Team 4 Integration Services

Final Project Report

for

DTX Manufacturing

Rising Phoenix

Version 3.0 approved

Prepared by Team 4

David Dollan (Team Lead)
Jeffery Wilson
Jamish Patel
Brian Snyder

11/21/2020

Table of Contents

Revision History

Name	Date	Reason For Changes	Version
David Dollan	11/1/2020	Document Creation	1.0
Jamish Patel	11/7/2020	Main Document Editing	1.1
David Dollan	11/7/2020	Final Draft Editing	2.0
David Dollan	11/21/2020	Review Editing and adding presentation slides	3.0

Group Members

Name	Role	Responsibilities
David Dollan	Team Lead, Wireless Systems Lead	• Oversees entire project • Records meeting notes (if applicable) • Provides wireless systems design and input
Jeffery Wilson	Project Manager, WAN Systems Lead	• Documents customer needs, deliverables, documents project dependencies • Ensures schedules are followed and deadlines are kept using the project timeline or Gantt Charts • Identifies project constraints and priorities • Provides WAN systems design and input
Jamish Patel	Document Specialist, Network Security Lead	• Maintains revision history, document repository, and collaboration method • Creates overall layout and design for written reports • Organizes team documentation into the Project Vision & Scope and Final Report • Provides Network Security architecture design and input
Brian Snyder	Presentation Specialist, LAN Systems Lead	• Creates the presentation template used for the final readout • Organizes team documentation into a final presentation • Takes on the role of backup presenter in case a team member is unable to join for the final presentation • Provides LAN systems design and input

1. Final Project Summary

DTX Manufacturing company is based out of Florida with 200 employees and specializes in the making of complex and intricate parts and subcomponents for a wide variety of industries. Recently, DTX has contracted with a new customer based out of Texas which is creating components for rocket motors and other aerospace propulsion systems. Due to the unique relationship between DTX and this new customer, DTX has decided to open a remote location near their new customer. The new location is a leased building that needed a complete network solution before normal operations begin.

Team 4 Integration Services had been chosen by DTX to install a complete network that included provisions for WAN, LAN, wireless, and network security. All systems included a base configuration as defined by the project vision and scope document. Once DTX has indicated substantial completion of the project, DTX's IT department will configure each system in accordance with DTX IT standards.

1.1. Content Summary

The following information provides a summary of the overall project in terms of scope, schedule, risks, costs, and IT systems deployed. For more detailed information on these topics, please refer to the project vision and scope document in Appendix A.

Scope
Since DTX planned on leasing a building at a new location, there needed to be a deployment of a full network to include WAN, LAN, wireless, and network security. All four of these systems also needed all accompanying hardware, cabling, installation, and initial configuration of each system. Team 4 Integration Services has provided these four systems and all connectivity to ensure interoperability with DTX's main facility in Florida based on the bill of materials presented to DTX. Team 4 Integration Services has also provided a Meraki Dashboard that will be used as the monitoring platform for the Meraki systems that have been chosen. This was an important feature for DTX as this arrangement is the first time the company has stood up a remote location. As such, monitoring is crucial to ensure that the remote site's IT systems related to WAN, LAN, wireless, and network security are taken care of and remain in a high state of availability with little to no onsite IT support.

Due to the agreements set forth by DTX and Team 4 Integration Services, there were a few items that were out of scope which included the following:

- Integration with telephony systems
- High voltage installation and/or conveyance
- Network Protection System (NPS)

These additions to the network were the responsibility of DTX and the installation of such equipment has happened after substantial completion.

Schedule
The Rising Phoenix project started on Sunday, September 20th, 2020 and is scheduled to run to December 20th, 2020. At this time, on December 20th, 2020, final testing will have been completed and all project deliverables and configurations will be handed over to DTX Manufacturing. For a detailed breakdown of the schedule, please see Appendix A, Vision and Scope document for the complete project schedule.

Business Risks
Several risks had been identified for this project and are shown below in Table 1. This same list has also been called out in the Vision and Scope document and is also available for review in Appendix A.

Table 1: List of business risks

Risk	Severity Level	Mitigation
WAN failure	High	Alternate carrier Selection (Possible Point to Point Wireless)
Not enough throughput / bandwidth	High	Calculate bandwidth by adding capacity for maximum usage also use the MX traffic-shaping feature. Business-grade SLA on WAN links
Cable failure/incorrect cabling termination.	High	Qualify each network drop after installation with Fluke qualification tester and repair any deficient drops. Ensure spare drops as appropriate for growth and potential failure.
Hardware failure - Switch	High	Deploy switch in a failover configuration with adequate port availability. Ensure support contracts are in place for replacement hardware.
Wireless frequency saturation in the surrounding area	Medium	Utilize the highest radio power for 2.4G and ensure 5G channels do not interfere with surrounding radios
A wireless site survey does not accurately reflect radio attenuation	Low	Add additional APs and adjust radio power if needed
Phishing attacks	High	DTX to provide the necessary training to all employees regarding the dangers of Phishing attacks and how to recognize and report such attacks on security

Weak Password, Unpatched Devices, Plugin USB drives, Rogue insiders, Malware	Medium & High	DTX will provide the necessary training and policies to all employees to ensure passwords meet minimum requirements based on industry standards. Patching, drivers, Malware, and Rogue insiders will be monitored by the DTX IT department and with the Meraki Cloud Dashboard
Initial migration to a new Firewall and switches could result in a large network outage.	High	A configuration backup will be taken of the current environment and any migration maintenance will be complete during off-hours.

Costs

DTX had set the master budget at $530,000 for the entire remote site development. The budget for the Rising Phoenix project was set at $100,000 and is a subsection of the master budget. DTX leadership had also authorized a 10% increase to the Rising Phoenix budget in the event changes to the scope or equipment was needed but this was not required. Had additional budgeting been needed approval from DTX leadership would have been solicited.

Team 4 Integration Services had quoted DTX $92,950.56 for all hardware, integration, and shipping which also included subcontracting for the installation of all cabling. For a detailed breakdown of all costs, please see Appendix A.

IT Systems Deployed

The IT systems deployed include different technologies needed to ensure a remote site has the means to communicate with the main campus. This includes WAN, LAN, wireless, and security devices that work together to provide the right type of connectivity for the employees and guests. The following is a summary of the systems deployed:

WAN

Meraki MX100 and MX84 devices have been set up to provide SDWAN capabilities for both internet and connectivity back to the head office. These devices have been installed at both the main site in Florida (MX100) and the remote site (MX84) to allow for this connectivity. Licenses have also been purchased and configured for each device and are set to a three-year cycle. WAN system management is set up in such a way that DTX can deploy the new WAN links more efficiently than traditional WAN links (Wilson, 2020). Additionally, all monitoring for this technology is being handled through the Meraki dashboard.

LAN

Two Meraki MS350-48 switches with a total of 96 switch ports have been installed at the remote site which provides the necessary network connectivity between all wired devices within the building. These devices are PoE and will be able to provide the capacity for all equipment needing network connectivity. These devices also included 10 Gb SFP+ modules for uplink purposes. Each switch has a seven-year license subscription and management has been configured in the Meraki dashboard with the WAN devices.

Wireless
Employee and guest access for the wireless network will be through 5 Meraki MR55 wireless access points which will also be managed through the Meraki dashboard (See Appendix C, Figure 8). Each MR55 device has been purchased with a five-year license. The wireless network also includes a captive portal for guest access and an example of this portal can be viewed in Appendix C, Figure 1.

Security
The primary security for the new location is now handled by a machine-learning Palo Alto Firewall which has been installed at the head office in Florida. Traffic via the remote site's WAN is now managed by the new firewall for both inbound and outbound traffic. Group policy and Active directory have also been adjusted to allow integration with the new security system.

1.2. Lessons Learned

Throughout this project, there have been several situations that shaped Team 4's decisions and processes. First, Team 4 needed to produce the scenario on which the project should be based on. Since each team member had different expertise in WAN, LAN, wireless, and security, it was decided that the project would revolve around the creation of a complete networking solution. From this decision, Team 4 was challenged to produce a specific scenario that would involve this holistic network solution. This was our biggest challenge of the project as several paths could have been taken and Team 4 did not want to overreach our capacity to produce deliverables. This challenge was eventually solved by focusing on a smaller scenario (like a remote site) and then building up the background information until the requirements of the project became easier to identify.

As the project requirements started to unfold, several decisions were made such as what responsibilities were to be filled by each team member, what equipment was going to be quoted in the project, and how the team was going to communicate and document progress. All these decisions were made with input from the team, so everyone agreed on how to proceed. Progress for the deliverables went smoothly and peer review information came back incredibly positive. The business practitioner also thought that the project was on the right track, but recommended changes to clarify the scope pertaining to end-user devices (PCs, phones, etc.). These changes were welcomed into the project and the scope was updated accordingly.

Overall, this project has been a success for Team 4 but there is always room for improvement. If more time had been available, additional integrations with other systems could have been explored such as network-driven security, PoE (Power Over Ethernet) lighting, and integrated facilities monitoring. Lastly, if more time were available, this project could have produced deliverables with even greater detail such as additional Meraki configurations or API deployments.

1.3. Learning Outcomes Summary

Communications outcome
The communications outcome was met through Team 4's use of email, live meeting sessions in Microsoft Teams, and the use of OneDrive as a collaboration platform. All team members participated in meetings and tasks assigned were completed.

Critical thinking outcome
The critical thinking outcome was met through Team 4's proposed solutions to the requirements noted in the Vision and Scope document (See Appendix A). The solutions that were proposed by the team were the result of significant research as to what would work in the specific situation that was presented and represented technologies that were current and up to date.

Network design outcome
The network design outcome was fulfilled by Team 4's creation of the WAN, LAN, wireless, and security documentation and architecture needed to install a complete networking solution. This included all the specifications needed to maintain the required bandwidth, latency, availability, security posture, and physical connectivity of all devices.

Management information systems outcome
The management information systems outcome was met by highlighting the need for alerting and access information that can shape both short-term and long-term actions. Understanding the overall health and function of a network is crucial in understanding how to allocate resources to better serve the organization.

Systems administration and scripting outcome
The systems administration outcome was met by Team 4's inclusion of the Meraki Dashboard element to the project. The dashboard is an interface that allows for the overall administration and configuration of the system. This feature is part of the cloud capabilities of the Meraki system and is highly accessible by system administrators.

Employability outcome
The employability outcome was met by the drive of Team 4 to create a solution that was not only relevant for the scope requirements but able to meet the needs of the future. Additionally, this project was completed with a focus on cost and the requirement of not exceeding the budget threshold (See Appendix A).

1.3.1 Communications

During the project, all team members have completed the communications required for this project. The team lead conducted meetings per the agreed to terms noted by the project charter and meeting notes were generated as needed. The collaboration method chosen for live meetings was Microsoft Teams where schedules could be coordinated with all team members and the ability to share meeting information improved communication within the group. Live team meetings were held every Monday at 8:00 PM (EST) where agenda topics centered around weekly deliverables. Outside of Microsoft Teams, team members utilized Microsoft Outlook for all communications outside of the regular meeting schedules. These communications included project updates, schedule changes, instructor updates, and other general communications. For documentation storage, OneDrive was chosen to both retain deliverables, but also serve as a collaboration tool so all team members could work on the project at the same time. Prior to the submission of major deliverables, team members had the opportunity to voice concerns or make suggestions. This allowed all participants to have a say in the final product before final copies were submitted.

1.3.2 Critical Thinking

The critical thinking objective was fulfilled in several ways. After the project scenario was created, Team 4 needed to begin the process of designing a solution that would fit the needs of DTX based on the requirements called out in the Vision and Scope document (See Appendix A). The solutions provided for each technology were researched based on these requirements to ensure that the proposed systems would have the correct capacity to provide connectivity. An example of this is the design of the LAN configuration. Based on the layout of the proposed building, it was determined that two network switches would be needed to provide the correct connectivity but also allow for the requirement of 20% scalability for future needs. Another example is the deployment of the wireless system where the design needed to consider current trends in mobile device needs. The solution not only gives ample capacity for current connectivity but again allows for the required scalability and future growth.

1.3.3 Network Design

The Rising Phoenix Project is a complete design and installation of a network for DTX's Remote site. As such, there were several categories of network design. These categories and design parameters are detailed below.

WAN

The installation of diverse path fiber was completed for two DIA (Dedicated Internet Access) 50 Mbps circuits (100 Mbps total). The winning bids came from two carriers Spectrum and AT&T with an SLA not to go below the 50 Mbps threshold (25 Mbps for each carrier). The fully redundant Meraki MX solution was completed at HQ in Florida and the new Texas office. Both circuits were provided with business-grade SLA guarantees. Monitoring has proved SLA has been met and both circuits are voice grade service with Latency <= 37 ms, jitter <= 1.0 ms, and loss <= 3.3%. Working with DTX technical team, Team 4 Integration Services was able to remotely configure headend MXs. The failover has been successfully tested at both sites. Currently, no-load balance issues have been noted. The physical installation documents for both sites and security system settings can be reviewed in Appendix C, Figures 2 and 3.

LAN

Dual Cisco MS350-48FP switches were installed using VRRP for high availability and redundancy. Each switch was connected to a separate WAN device for fault tolerance. Devices were configured using the Meraki Cloud Dashboard and will also utilize the monitoring and alert capability of the console. CAT 6 cables have been certified using various available tools including Fluke testers. Stress testing has been completed from the PC to switch on all ports. The MS350 switches handled the load without issue. POE functionality has been tested and the switches are providing adequate power for all devices (AP, Phone, etc.) Technologies such as

VPN are functioning normally. Connections from workstations to the main office are working as expected.

Wireless
The wireless network has been designed and implemented in accordance with the requirements and building layout shown in the Vision and Scope document (See Appendix A). A predictive site survey was performed (See Appendix C, Figure 6). This shows that five wireless access points were needed for the 100 percent coverage at –60 DB for both the 2.4 GHz and 5 GHz frequencies. From this site survey, Team 4 Integration services chose to use MR33 wireless access points (WAPs) that were connected back to the MS350-48 network switches using CAT 6 cabling. However, after DTX leadership reviewed the 802.11ax Whitepaper (See Appendix D), DTX decided to instead use MR55 Wifi 6 WAPs to allow increased speed, future growth, and IoT capabilities in the 1 GHz and 7GHz frequency ranges (Dollan, 2020). This change was an increase of $3,810.05 from the original budget, but even with the increase, the total cost of the project is under budget.

1.3.4 Management Information Systems

The Management Information Systems requirement of the project was met by the configuration of system alerts and the implementation of a wireless captive portal. These features are important as they can provide a significant amount of metrics about the network environment. For example, there Meraki Dashboard has been configured to log parameters that are out of specification such as WAN bandwidth. Such a data point can be used to determine if the internet service provider chosen is meeting the service level agreement. Furthermore, these alerts have been set up to notify IT personnel of undesirable situations via email or SMS text. This is an important feature as IT personnel may not be onsite and will be able to handle troubleshooting issues remotely (Synder, 2020).

As part of the wireless system, access for DTX employees and guests alike must provide the correct amount of connectivity for mobile devices. DTX employees will connect to the wireless systems through integration with Active Directory which will handle normal user authentication. Guest access to the wireless system will be maintained by a captive portal that is set up through the Meraki Dashboard. The captive portal gateway (See Appendix C, Figure 1) includes the ability for the guest user to sign up for wireless access using their full name, email address, phone number, and their organization. Additionally, terms of use information will be displayed to indicate acceptable use and to note that there is no expectation of privacy while using the guest wireless network.

1.3.5 Systems Administration and Scripting

Once installed, the full network solution was configured by Team 4 Integration Services to comply with providing a base configuration. After the Base configuration was complete, full control was given to DTX IT employees to configure the systems to their standards and specifications. The main system administration platform is achieved through the Meraki Dashboard. This user interface (UI) is designed as a "single pane of glass" that acts as the central point for system activity, status, and management. As part of the Meraki licensing, DTX will have the ability to monitor all functions of both the WAN, LAN, Wireless, and elements of the network security structure. The Dashboard was set up to integrate both the main facility in

Florida and the remote site in Texas so network operations can be monitored and controlled as if it were a single system. For screenshots of the Meraki Dashboard for both the Florida and Texas locations, see Appendix C, Figures 4 and 5.

1.3.6 Security

When implementing a network infrastructure, it is important to consider what methods will be used to protect the network. Controlling access to privileged information and safeguarding the network against malicious activity ensures that data is accessed securely with minimal threats. To address security concerns Team 4 Integration Services has focused on upgrading network authentication and authorization. By addressing authorization and authentication Team 4 Integration Services will enhance DTX and Palo-Alto security methods. Additionally, the structuring of the domain organizational structure will mimic DTX manufacturing company organizational structure and prevent multiple futures re-organizing efforts. This project has also included new policies and procedures that will enhance the security of resources as well as increase the reliability of the network.

Team 4 Integration Services has recommended and installed a version of the Palo Alto firewall as a Security appliance that will provide firewall services to the company. In addition to firewall services, the Meraki security system will provide DTXwith VPN servers, which can provide digital privacy and encryption (Meraki Auto VPN, 2020). By utilizing a firewall and Meraki solution DTX will be able to secure the network from attempts to access local network resources as well as assist in virus prevention by scanning traffic (See Appendix C, Figure 7).

The best way to protect a network is to combine multiple security technologies to create a single holistic solution. Team 4 Integration Services is offering DTX a simple solution for complex security needs with minimal cost and maximum protection.

1.3.7 Employability

The Rising Phoenix project was created in response to a need for a complete network solution that was realistic, up-to-date, and that satisfied the needs of DTX Manufacturing's strategic priorities. The budget for this project was set at $100,000 with a 10% overspend available. Even though the cost could go over $100,000, Team 4 Integration Services was able to complete the project under budget for $96,760.61. Additionally, Team 4 Integration Services deployed the SDWAN architecture to allow for the network overhead created by the various applications required by DTX employees while also integrating redundancy for high availability. The LAN infrastructure was also designed not only with speed and bandwidth in mind, but also scalability where future considerations were built into the system from the start. The same is true regarding the wireless system as newer 802.11ax WAPs were installed to take advantage of increased spectrum usage and IoT capabilities using the 1 GHz and 7 GHz frequency ranges (Dollan, 2020). Lastly, security was a major priority for Team 4 Integration services which is an ever-increasing concern for any organization. Team 4 Integration Services recommended and installed both Meraki security elements and Palo Alto infrastructure to shape and control traffic at the Florida and Texas locations. All of these features within the Rising Phoenix project would be a great asset to any organization but they are especially vital to DTX Manufacturing as they seek a greater market share in the aerospace industry.

2. Future directions

The Rising Phoenix project was intended to provide a fully functional network system for the DTX organization. While there was a specific endpoint to the actions that took place, there are a few directions the project could take in the future. One such direction is integrating physical building security into the Meraki cloud environment. This addition to the Meraki solution suite would be able to integrate security cameras into the already existing Meraki environment. Another enhancement to the system could also be the integration of third-party applications into the Meraki API suite. This could expand on the monitoring possibilities already included with the Meraki cloud platform by building business insights in applications such as DOMO or PowerBI. Having this additional information can give business leaders detailed information as to ROI and predictive planning measures.

3. Annotated Bibliography

Meraki Auto VPN General Best Practices. (2020, July 16). Retrieved October 01, 2020, from https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Best_Practice_Design_-_MX_Security_and_SD-WAN/Meraki_Auto_VPN_General_Best_Practices
This site provides information on the deployment best practices for Meraki secure VPN solution. This Meraki guide was created to help installers follow best practices when deploying Meraki auto VPN service. It lists best practices focused on the most common deployment scenarios for most topologies.

Cisco. (2018). *Conducting Site Surveys with MR Access Points*. Retrieved October 2, 2020, from Meraki Documentation: https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Conducting_Site_Surveys_with_MR_Access_Points
This document provides ways systems administrators are able to conduct a site survey utilizing the features of the MR series WAPs. In lieu of dedicated site survey hardware or software, a systems administrator would be able to measure RSSI strength and map out the various readings at different locations within the building

Dollan, D. (2020). *Current Wireless Standards and the Shift to 802.11AX.* Retrieved November 7, 2020
This white paper explores the differences between the current IEEE 802.11ac and the IEEE 802.11ax standards. Recommendations for choosing one standard over the other needs to be a well thought out decision, but if an organization is looking to stand up a new location, the recommended decision is to use the 802.11ax standard.

Patel, J. (n.d.). Windows Server & Network Security of Benefits for a Company. Retrieved November 7, 2020
This white paper provides information related to the deployment of Windows Server 2019 and the integration of Hypervisor as a way to run multiple virtual machines. This functionality of Windows server 2019 allows for efficient deployment of server infrastructure while having the smallest available footprint.

Pierce, M. (2020, March 10). *Why is a Captive Portal Important for Wireless Guest Access?* Retrieved November 7, 2020, from SecureEdge: https://www.securedgenetworks.com/blog/why-is-a-captive-portal-important-for-wireless-guest-access

This article explains the need for providing a legal disclaimer for an open or guest WiFi service. Many times, a guest WiFi is configured in such a way that users are able to intercept traffic of other users which can lead to privacy concerns. It is important to note that privacy should not be assumed on guest networks.

Synder, B. (2020). *Cloud Management and Monitoring.* Retrieved November 7, 2020

This white paper serves as an example for organization looking to utilize cloud based services for remote management and monitoing. As an example the Meraki monitoring service is able to provide the necessry level of information to correct issues before they become realy problems. This helps IT organizations as no dedicated resources need to be present for troubleshooting and corrective actions to take place.

Wilson, J. (2020). *SDWAN Whitepaper.* Retrieved November 7, 2020

This white paper provides a history of broadband services and goes into detail about the characteristics of dedicated internet access. The latest version of WAN technology is SDWAN which provides an overal better and more manageable way for organizations to use WAN services.

4. Response to Reviewers

This document has been reviewed by class peers and the following comments have been selected by Team 4 to include as part of the editing process. There are two parts to each review. The first part is the peer review, and the second part is the team's response.

1. **Review:** their writing is perfect in my idea, and the interesting thing is that there are 19884 words in 85 pages in their project. So they spent too much time on their project good job.

   Response: A lot of work went into this project and is what would be required for a complete network installation using the solutions that were called out.

2. **Review:** I'm nitpicking, because I'm not seeing any glaring issues, but in the WAN section does Jitter and Loss need to be capitalized? I'm questioning the employability section though, I'm not sure it fits based on my understanding of that section. I understood that section to be more of a "How will this project help with employability for those working on it?"

Response: The section where jitter and loss are capitalized has been corrected. The section regarding employability will not be changed as the instructions were to document "concerning the scope, quality, and technical depth of your project. This should be persuasive, referencing other sections of the document as if you were showing a potential employer this project in an effort to be hired." The section was written specifically with "showing a potential employer" in mind.

3. **Review:** The need to implement a new network is clearly defined and is significant to the industry. The writing flows nicely and is consistent throughout the document. The sources that are included are relevant, appropriate, and current. The use of the sources help support the arguments of the writers. The sources are all in APA format. The document overall follows the appropriate format and not adjustments need to be made there. There were a few typos in the document, but they are minor fixes. By running a quick spelling and grammar check all the grammar and spelling mistakes can be identified and corrected. Overall, the writing is excellent and little maintenance needs to be completed

   Response: Spelling, grammar, and punctuation have been corrected as per the review.

4. **Review:** The introduction does a good job at mentioning that there is a need to gather metrics about the network environment. One feature that could be tracked included the internet service provider was meeting the level mentioned in the service level agreement. Another feature mentioned that is great for the IT personnel is receiving email and SMS text alerts when undesirable conditions occur. It was mentioned that user access will be controlled using active directory. Additionally, guests can access the network by providing some required information. One thing that can enhance this section would be to include some specific service levels that need to be met. For example, what is the minimum data point the internet service provider agreed to provide. Another area could be including testing for each group or team that uses the network resources. This could be used to determine whether more or less resources will be needed in the future, or if one team does not seem to be using the network then their resource allotment can be reduced.

   Response: Added information about the SLA agreement with the two carriers has been added to provide context to the other SLA statements in the WAN section. Monitoring was also a big part of this project and the Meraki Dashboard and monitoring tool would cover whether more or less network resources would be needed. Team 4 is declining the addition of provisions that would throttle network resources based on usage.

5. **Review:** There are formatting issues with APA 7, specifically with indenting and line spacing after headings and subheadings. There are misspelled words within the paper.

There are no in-text citations. They include a bibliography, but do not cite the sources within the paper.

> **Response:** Formatting issues have been corrected within the annotated bibliography. Spelling, grammar, and punctuation have been corrected as per the comment. Cited sources are, in fact, present within the document and exist where needed as per the instructions.

5. Appendix A: Vision and Scope

Vision and Scope Document

For

DTX Manufacturing
Rising Phoenix Project

Version 2.1 approved

Prepared by Team 4:

David Dollan (Team Lead)
Jeffery Wilson
Jamish Patel
Brian Snyder

9/15/2020

Table of Contents

Revision History

Name	Date	Reason For Changes	Version
David Dollan	9/14/20	Document Creation	1.0
David Dollan	9/28/20	Formatting Changes	1.1
Jamish Patel	10/2/20	Major editing and content changes	2.0
David Dollan	10/3/20	Final draft editing	2.1

6. Business Requirements

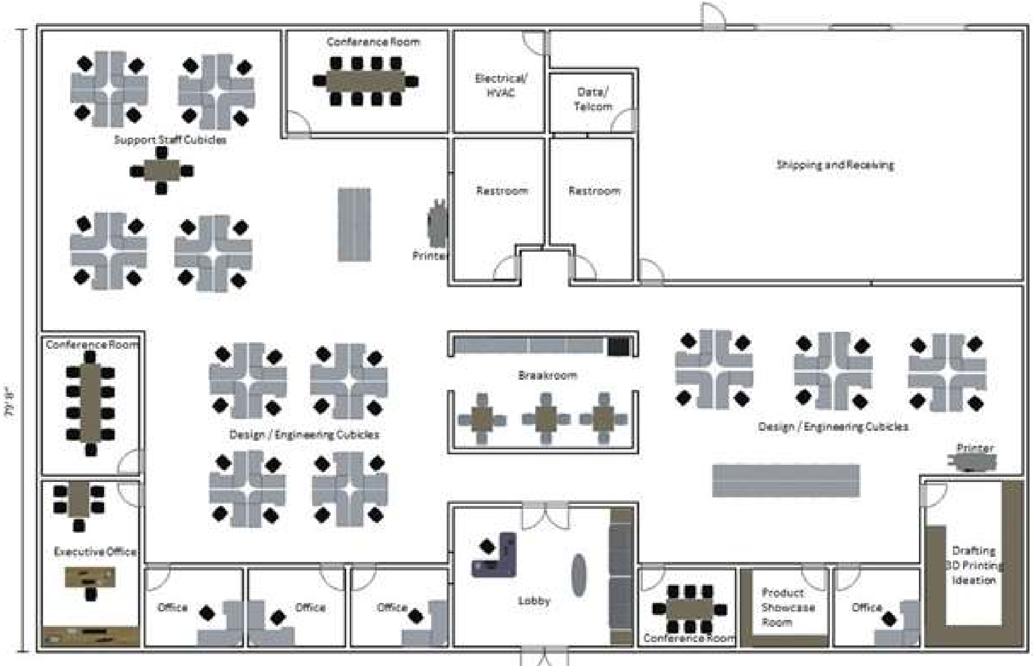
DTX is a manufacturing company from Florida with 200 employees that have recently secured a new customer located in Texas. Due to the nature of the contract, DTX will need to have a presence in Texas to be near the new customer to collaborate on various, large-scale projects. While there are ample ways to perform remote collaboration, the customer's projects will need on-site engineers and support staff from DTX to ensure quality and product specifications. As such, DTX has decided to lease a building that is located close to the customer to provide the needed support required by the contract.

6.1. Background

According to the new contract, DTX will be providing several parts for a project that is in development by the customer. Several components of the customer's project have already been built, but DTX will be providing specialty components that will require regular on-site visits to the customer by DTX engineers. These engineers will then design mock-ups of the components needed before full production begins.

Since these engineers will be working very closely with the customer and the logistics of travel and the shipping of prototypes is not feasible, DTX has decided to lease a building in the immediate area of the customer which will provide a remote base of operations for DTX. The proposed layout for this location is detailed in Figure 1. Since this is a new location, DTX has contracted with Team 4 Integration Services to provide a holistic network solution to sustain approximately 50 employees. The full solution should include provisions for WAN, LAN, wireless, and network security for the new location.

Figure 1: Remote site layout



6.2. Business Opportunity

The customer that DTX has contracted with has been developing innovative solutions for the aerospace industry and has developed new technology that will assist in the production of more efficient turbojet engines. Additionally, the customer is working on state-of-the-art compression systems that have application in reusable rocket motors for space flight.

For DTX this is an opportunity to produce components that have a wide range of applications and opens future work within the aerospace industry, a market that DTX has not entered yet. Being able to enter this market could mean the potential for 14.7 million dollars in market share, and the successful collaboration with the new customer is the essential first step to this goal.

In order to begin this process, DTX will need a remote site near the customer's location in Texas. This new site must have a robust network that has WAN, LAN, wireless, and network security elements which will be key in collaborating with both the home office and with DTX's customer.

6.3. Business Objectives and Success Criteria

The main business objective for this project is to deliver a holistic network solution that incorporates WAN, LAN, wireless, and network security provisions by December 20th, 2020. Since operations will begin shortly after the installation of the new network, it is very important that the solution is delivered on time. In addition, the full network will need to seamlessly integrate into the networking environment that DTX already has at their main site. This is to ensure maximum uptime and reliability for all communications between DTX and the customer. Lastly, the solution will need to provide adequate bandwidth for the internal network and WAN connectivity to ensure that both software and hardware are able to operate at maximum capacity.

6.4. Customer or Market Needs

DTX has indicated that there will be several requirements for this remote site. First, the solution should also integrate with DTX's main office and should include 100Mbps connectivity with the Internet Service Provider (ISP). Transfer speeds between the main office and the remote office should not drop below 50 Mbps and should include applicable firewall hardware and base configuration ACLs. Second, the solution should allow for the proper connectivity and bandwidth to the various cloud environments that are used by DTX such as Microsoft Azure Services, Microsoft Office 365, Adobe Creative Cloud, Solid Works, and AutoCAD. Third, the remote office will need a robust LAN infrastructure which will need provisions for 50 employees. This should include infrastructure that can support employee computers, desk phones, and conferencing equipment. Additional provisions will need to also support applicable VLANs, data security, and room for up to 20% increased scalability. Lastly, the solution should also include a wireless network that has the capability to provide full building coverage with signal loss of no greater that -60 dB. Wireless security should include integration to Active Directory for DTX employees and a separate network with captive portal capability for guests. Table 1 details these requirements from DTX.

Table 1: List of customer needs

Customer Needs	Proposed Solution
Provide required bandwidth for traffic communicating with cloud services and between the main and remote site.	Minimum 50Mps, Recommended 100Mps allows for speed burst Estimated 50 low scale usage 100 Kbps (kilobits per second) Devices: VIOP phones E-Fax machines Estimated 50 Medium 500 Kbps (kilobits per second) Services: streaming, cloud application, emailing downloading
Provide VPN capabilities for offsite work including BCP operations	Core equipment sized to allow for the deployment of Teleworker Gateway Devices for BCP operations
Provide a baseline firewall and applicable ACLs.	Palo alto Firewall will be installed and utilized with ACLs
Provide a robust LAN infrastructure that includes both physical wiring and all switching hardware	Cisco switches will be installed in a stacked warm spare configuration with redundant WAN circuits. Port speed will be a minimum of 1Gb/s. Cat6 cable will be installed and qualified with Fluke test equipment.
Provide adequate VLAN segmentation for the organization of various network needs	VLAN implementation will mirror main corporate office with appropriate segmentation (LAN, Management, VOIP, Wireless, etc...)
Provide a wireless network setup for DTX employees that allows for all current wireless standards	Install dual band access points for wireless coverage that utilizes Active Directory for employee authentication and a captive portal for guest access.
Provide a methodology to allow wireless authentication for DTX employees through Active Directory	Microsoft Network Policy Server will be utilized with RADIUS technology to authenticate with Active Directory. Appropriate security groups and policies will be configured.

6.5. Business Risks

Since a full network solution will be implemented during the life of the project, there are many risks that may occur including but not limited to the following:

Table 2: List of business risks

Risk	Severity Level	Mitigation
WAN failure	High	Alternate carrier Selection (Possible Point to Point Wireless)
Not enough throughput / bandwidth	High	Calculate bandwidth by adding capacity for maximum usage also use MX traffic shaping feature. Business grade SLA on WAN links
Cable failure/incorrect cabling termination.	High	Qualify each network drop after installation with Fluke qualification tester and repair any deficient drops. Ensure spare drops as appropriate for growth and potential failure.
Hardware failure - Switch	High	Deploy switch in failover configuration with adequate port availability. Ensure support contracts are in place for replacement hardware.
Wireless frequency saturation in the surrounding area	Medium	Utilize the highest radio power for 2.4G and ensure 5G channels do not interfere with surrounding radios
Wireless site survey is does not accurately reflect radio attenuation	Low	Add additional APs and adjust radio power if needed
Phishing attacks	High	Advise employees to never click hyperlinks in suspicious or unverified emails, especially ones requesting information or payments. Keep in mind that legitimate institutions that offer payment options will always have HTTPS websites equipped with SSL protection.
Weak Password, Unpatched Devices, Plugin USB drives, Rouge insiders, Malware	Medium & High	Weak Password: Passwords containing at least eight characters, one number, mixed-case letters, and non-alphanumeric symbols were once believed to be robust. Malware: Ensure that your software is updated with the

		latest patches and that all applications, email programs, and browsers are covered.
Initial migration to new Firewall and switches could result in a large network outage.	High	All Current Firewall and Switches will have their current configuration copied and applied to new switches. All maintenances work will be taken place after business hours, allowing the ability to test the network changes. In the event of a failure, the old equipment can be swapped back into the network back online.

7. Vision of the Solution

Team 4 Integration Services has proposed a solution for DTX that addresses the four major areas that are needed which include WAN, LAN, wireless, and network security. The following sections summarize each area of the solution which will tie into the overall IT structure at the DTX's main office in Florida.

7.1. Vision Statement

DTX's network solutions will contain the following:

WAN Integration:
The WAN solution consists of two Meraki model number MX100s located in the DTX Florida Headquarters location. Devices will be configured in high availability pair (HA) with one acting as a warm spare. The Texas location will consist of two Meraki MX84s also in (HA) pair. Circuit will consist of two DIA WAN links to be ordered by the customer for the Texas site for SDWAN capabilities and failover

LAN Integration:
The LAN solution will consist of Dual Cisco MS350-48FP switches in a warm spare (VRRP) configuration. These switches will also perform routing functions at layer 3 with WAN circuit failover. The MS350-48FP will provide ample POE for WAP and VoIP applications. Network cable drops will use Cat6 cable and provide 1Gb/s connections from the switch to desktop with ability to provide a limited amount of 10Gb/s connections if necessary. Servers (AD, DNS, DHCP, FS, NPS) will use standard ports or SFP+ ports as necessary. Cisco switches will integrate with the proposed Meraki Cloud Dashboard.

Wireless Integration:

The wireless network will also be Meraki solution that uses dual band MR33 access points which connect back to a centralized control system. This controller is cloud based and will have at least a 5-year license for each of the access points that are connected. Once the wireless solution is in place, it will be capable of providing a, b, g, n, and ac wireless standards using both 2.4GHz and 5GHz frequencies. Connectivity in the wireless network will enter through the "DTX_MFG" SSID and will authenticate through DTX's existing Active Directory environment. A guest network will also be provided and will include a captive portal for the entry interface.

Network Security:
Microsoft provides the security controls, which force an end user to meet password complexity requirements. The out of box configuration will not be changed during implementation unless the client administration policy is required to change. Other security controls can be implemented utilizing Microsoft Azure Active Directory such as limitations to non-business functions of the operating environment of the workstation. Microsoft Windows Server 2019 also offers Hybrid capability with Azure, Advanced multilayer security, Unprecedented hyperconverged infrastructure, Network Policy Server and much more, which enables client security to be validated before network access is granted to a workstation. NPS is only documented as a feature to the implementation of this project and is outside the scope of work for this project. The implementation of an Active Directory environment does also provide some security controls such as:

- SSO to both cloud and on-premises resources
- Conditional Access through MDM enrollment and MDM compliance evaluation
- Self-service Password Reset
- Enterprise State Roaming across devices
- Resource Security
- Application Security
- Workstation Security
- User and Group Security

7.2. Major Features

WAN Integration:

- SDWAN cloud managed security appliances
- High Availability Pair (HA)
- Diverse Dedicated Internet Access (DIA)

LAN Integration:

- 48 × 1G port models x 2
- 4 × 10G SFP+ uplinks x 2
- 740W total, 30W per port POE
- Layer 3 routing with OSPF
- Warm spare redundancy (VRRP)
- Voice and Video QoS

Wireless Integration:

- Dual Band (2.4 GHz and 5 Ghz) radios per access point
- 802.11 a,b,g,n,ac standards
- 1.3 Gbps aggregated throughput
- Active Directory Integration
- Captive Portal
- Always on monitoring via Meraki Cloud Dashboard

Network Security:
The authentication and authorization project will include the following key Installations:

- Install new Palo Alto Firewall:
  - The industry's only complete ML-based IoT Security product discovers and secures every unmanaged device in your network (Palo Alto, 2020)
  - Inline Machine Learning-based malware and phishing prevention to stop most unknown attacks (Palo Alto, 2020)
  - ML-Powered NGFW for your Kubernetes container environment with CN-Series - another industry first (Palo Alto, 2020)
  - Deploy and maintain TLS decryption with ease. Now with support for TLS 1.3 and up to 2X performance boost (Palo Alto, 2020)
- Installation and configuration of Hyper Vison on host system
- Installation and configuration of new file server
- Consolidate and secure network file shares
- Configuration of group policy to help with network security

7.3. Assumptions and Dependencies

Based on all current information, Team 4 Integration Services makes the following assumptions:

- Rack Space ,2U available for MX appliances at Headquarters location.
- Rack environment Headquarters, Dual UPS power sources available for redundancy.
- Climate controlled environment for network and server hardware.
- Adequate space between network and electrical cable to minimize interference.
- Conditioned reliable power source with UPS backup.
- The space above the drop ceiling will have the appropriate structural supports that can be used for access point mounting hardware.
- Light modification to the building is permissible to run low voltage cabling.
- Appropriate modifications to system configurations would take place to comply with DTX IT standards. These additional modifications would be performed by DTX IT personnel.
- Ample frequency space exists for both the 2.4 GHz and 5 GHz ranges and interference is minimal in the surrounding area.
- Security assumptions for a network security hardware appliance
    - A function and secure Website and database for our customers

- Palo Alto Firewall, Cisco Router and Switches
- Ad or SAM type of security on our networks
- A robust Network security that will meet the need of our company environment Network safety protocols.

In addition to the assumptions, the following dependencies have been identified:

- Existing Headquarters DIA circuit 100Mbps or greater.
- A vetted Internet Service Provider contract will be in place by the time Team 4 Integration Services starts installation work at the site
- Palo Alto Firewall and Cisco switches contracted by HBS and will be in place when Team 4 Integration Services begins installation work at the site

8. Scope and Limitations

The scope of this project is to provide a full network solution that will include WAN, LAN, wireless, and network security provisions for DTX's new remote site. The integration that will be provided by Team 4 Integration Services will include all hardware, cabling, installation, and initial configuration of all components. Additionally, Team 4 Integration Services will guarantee that the installed solution will provide a fully configured Meraki Dashboard that will serve as the monitoring platform. This dashboard can be used to ensure that the needed throughput and bandwidth requirements (internal and external) are achieved and available for future use and troubleshooting.

8.1. Scope of Initial Release

The scope of the initial release is broken down into the following categories and will satisfy all requirements put forth by DTX:

WAN Scope:
The WAN scope will include the installation and configuration of headend and remote location. DTX will provide IP addressing schema, for the two headend appliances and all VLANs at the remote location. With guidance from DTX content filtering and firewall blacklisting and whitelisting will be enabled. Team 4 Integration Services will provide training on adjusting these setting to DTX staff. Circuit requirements for HA environment also call for both DIA circuits be delivered from LEC with /29 addressing.

LAN Scope:
The LAN scope will include network topology maps including enough drops for all PCs and peripherals such as network printers. CAT 6 cabling and hardware installation will be subcontracted to a locally licensed provider in conjunction with construction of walls and drop ceilings (provisions for the cost of the subcontractor have been built into the bill of materials below). Switch configuration will be applied as well as ports qualified to the desktop with a minimum 1Gb/s speed. Switch ports will be appropriately segmented by VLAN as designed by existing corporate office network.

Wireless Scope:
The wireless scope will encompass the initial site survey that will determine the location of each access point and system variables such as radio transmit power and frequency selection. Next, the installation of all hardware will include the mounting and cabling of the APs back to the appropriate network drop. Lastly, the initial configuration will be applied to the installed APs in order to communicate back to the Meraki cloud environment. This configuration will also include the deployment of a captive portal, Active Directory integration, and full systems monitoring.

Network Security Scope:
The network security scope will include deploying the new Windows 2019 servers and promoting all four servers to domain controllers and firewall. Servers in the Texas office will be read only domain controllers and will receive replicated domain changes from the Florida office.

8.2. Scope of Subsequent Releases

While the initial scope satisfies the immediate needs of DTX, there will eventually be a need to adjust the overall network as business demands are realized. These future business needs may include an overall increase in throughput, increase in LAN or wireless capacities, network security upgrades or changes in Internet service providers. Team 4 Integration Services can meet all these needs and will be available to discuss future projects.

8.3. Limitations and Exclusions

The following list summarizes the limitations and exclusions that should not be considered part of this project and can either be addressed during subsequent releases or via change order (after approval from all parties):

- Telephony integration – All telephony hardware, setup, and integrations with existing CUCM or PBX services will be the responsibility of DTX.
- Electrical installation and conveyance - All electrical connectivity (except specifications related to Power over Ethernet (PoE) will be handled and performed by certified electricians.
- Network Protection System (NPS) - the primary NPS will be considered a part of the project only as it applies to the integration of DTX's main office to the remote office, but the configuration will be outside of this scope.

9. Business Context

The main business context resides in the contractual agreement that DTX has with its new customer and the unique business relationship that will be needed for operations. DTX will need to provide onsite support for the new customer so there will be a need for increased collaboration between these two businesses. While onsite visits will be a must, the customer will need to transfer data to DTX in the form of communications and files to the remote site. Additionally, DTX will need to further collaborate with personnel from the main office in Florida to be successful with the project. The digital network that will allow these communications to happen is vital to both DTX and its new customer and management from both businesses have taken a great interest in the solution's development. The budget for the overall acquisition and occupancy of the new building has been set at $530,000 in which $110,000 has been set aside for the Rising Phoenix project. The organization would, however, like to try to keep spending below $100,000 if possible.

9.1. Stakeholder Profiles

Table 3: List of stakeholder profiles

Stakeholder	Major Value	Attitudes	Major Interests	Constraints
DTX organization	Increase company footprint into new consumer area	Bring value to customer base in an area of increasing opportunity	Develop closer relationship with customers and also reduce travel time and expense of employees	Maximum building budget = $530,000
Project Team	Deliver customer driven IT solutions	Focus on customer needs in designing solutions and delivering on time and on budget	Solutions should be cost effective, manageable, secure and expandable	Timetable is aggressive with no option for delay. Employees are currently be hired
Users	Quick access to data and applications	Timely access to applications critical for users day-to-day operations	Time is better spent focusing on customers not working with support to resolve access issues	35% of the users at site will be new to the organization
DXT CIO	Reliable, secure and cost-effective IT solutions.	Information technology solutions need to work and be for the most part, transparent to user	Transition point in organization for technology solutions. Makes sure solutions are correct fit for the organization	Has little time for meetings has several IT projects in motion.
DTX CEO	Encourage Growth of the organization	Very excited about this venture, hopes it the first of many	Will watch project closly and want it to be as successful as possible, not interested in technical problems only solutions.	Will want frequent updates just on project status.
DTX CFO	Budget for the project	Besides implementation budget interested in MRC or monthly recurring charges	MRC cost for circuits and Maintenace, wants to develop a greater understanding not only for want the added cost might mean for customers charges	Does not want to be involved in weekly updates only in budget and charges

		could affect customer cost	but also for budgeting future expansions	

9.2. Project Priorities

Table 4: List of priority profiles

Dimension	**Driver (state objective)**	**Constraint (state limits)**	**Degree of Freedom (state allowable range)**
Discovery and customer requirements	Start DTX engagement 9/27/2020	Clarity of customer requirements and documented could cause solution rejection 10/4/2020	With short time frame for solution and to be able to have equipment and circuits delivered solution development cycle will be transparent to customer to lower risk
Circuit orders	Circuits must be ordered before the 10/4 date to ensure delivery before testing 12/5	Risk of delay will impact DTX H/R hiring project scheduled 12/15	If delay is greater than week risk missing project completion date
Equipment orders	Confirmed that equipment is in stock and can be delivered 10/18 for Headend installation	Headend must be completed before remote site testing 12/5	2-week possible delay
Remote LAN MDF	LAN MDF equipment cabinet and UPS must be installed before 11/5 for remote equipment install	Team travel plans and other internal projects will be impacted	Would need to change team travel plans and look at impact on other Team4 projects if delay over two days
Cost	Bring project in under the projected 100K budget	Circuit buildout cost could impact DTX budget	budget overrun up to 10% acceptable without executive review

9.3. Operating Environment

The installation of the complete network at proposed remote site is a big investment for DTX and it will serve as a base of operations in a new region and industry. As such, the network that is proposed will need to be robust enough to handle day to day operations, but also reliable enough to maintain communications between the main office in Florida and the remote office in Texas. A VPN solution has also been identified as being an integral part of the project due to the possibility of travel and offsite work that may be performed from time to time by DTX employees. Additionally, VPN connectivity is included in BCP operations should a local or national emergency happen which will provide a means of further productivity while DTX employees are working from home.

The LAN deployment will need to provide at minimum 1 Gbps connectivity to each of the 50 proposed DTX employees that will be onsite at the remote office. At a minimum, each employee will have a laptop and cell phone, but for connectivity to the LAN, laptop docking stations will be provided to interface with the network. Each employee's workstation will have at least one network drop that will be connected to their Cisco desk phone, which will then be connected to the employee's docking station. All network cabling will terminate in the data closest which is near the rear middle of the building and the appropriate network switches will be installed to handle 50 DTX employees with a scalability option of up to 20%.

The wireless network will further enhance the capabilities of the overall network deployment by providing access for laptop and mobile devices. DTX is planning on each of their 50 employees to have at least two devices that will need wireless access which includes a laptop and a mobile device. Current wireless standards are a must and all access points installed must be capable of 802.11ac with backwards compatibility for 802.11a, b, g, and n. A wireless network that is capable of a logical air gap must be provided for DTX guests for security purposes and shall include a captive portal for access control.

Lastly, network security is a critical component for any organization and will a part of this project. DTX currently has its own IT staff that will be performing the final changes to the security configuration; however, Team 4 Integration Services will need to provide a base configuration to provide interim data protection. This includes a base configuration to the Palo Alto firewall and the ACLs within the Meraki cloud management environment.

10. Human Resources

Human resources and personnel management for this project will be the responsibility of Team 4 Integration Services and covers the team charter, skills of team members, assigned roles, and information regarding the communications format that will be used during this project.

10.1.Team Charter

To prepare for this project, a team consisting of David Dollan, Jeffery Wilson, Jamish Patel, and Brian Snyder was assembled and began work on the details on September 13, 2020. David Dollan was voted as Team Leader and will oversee all aspects and deliverables of the project. Both technical and non-technical roles have also been established and assigned to each team member and is listed in section 5.3. Since every member of the team has a wide range of expertise, all decisions will be as a collective to ensure quality. The workload of the project will be evenly distributed and approved by the team. Regular team meetings via Microsoft Teams will be scheduled for every Monday at 8:00 PM (EST) and will have a duration of one hour. Meeting notes will be recorded (if applicable) and distributed to the team for review. Any change to the meeting schedule may be initiated by an individual team member but will be approved by the whole team. Communications outside of the recurring team meetings will be conveyed through email and will be addressed to everyone within the team. Conflicts within the group will be handled professionally and any disagreements that cannot be solved by the team will be forwarded to the class instructor as a last resort. Lastly, underperforming team members will be acknowledged by the rest of the team prior to any actions taking place and if needed peer grading will be adjusted.

10.2.Technical Skills and Attributes

Table 5: Team member skills and attributes

Name	Skills	Attributes
David Dollan	Networking, cabling, systems design, technical writing, hands on experience	Attention to detail
Jeffery Wilson	Network Engineer	Creative
Jamish Patel	Network administrator, Network Security, programing	Attention to editing
Brian Snyder	Network & Systems Engineer, CCNA, MCITP:SA, Security+	Enthusiasm and personal drive

10.3.Roles and Responsibilities

Table 6: Team member roles and responsibilities

Name	Role	Responsibilities
David Dollan	Team Lead, Wireless Systems Lead	• Oversees entire project • Records meeting notes (if applicable) • Provides wireless systems design and input
Jeffery Wilson	Project Manager, WAN Systems Lead	• Documents customer needs, deliverables, documents project dependencies • Ensures schedules are followed and deadlines are kept using the project timeline or Gantt Charts • Identifies project constraints and priorities • Provides WAN systems design and input

Jamish Patel	Document Specialist, Network Security Lead	• Maintains revision history, document repository, and collaboration method • Creates overall layout and design for written reports • Organizes team documentation into the Project Vision & Scope and Final Report • Provides Network Security architecture design and input
Brian Snyder	Presentation Specialist, LAN Systems Lead	• Creates the presentation template used for the final readout • Organizes team documentation into a final presentation • Takes on the role of backup presenter in case a team member is unable to join for the final presentation • Provides LAN systems design and input

10.4.Communication Strategies

Communication for this project will primarily consist of email. Where possible, the team will respond to the same email thread as to ensure all members have the same information. Email will be checked frequently and if questions or concerns come up, the team leader should be notified immediately. Team meetings will also be schedule for every week on Monday's at 8:00 PM EST by the team leader and will be facilitated in Microsoft Teams. These meetings will also allow each member of the team a chance to report on progress and to provide feedback as necessary. Project files that are produced by the team will be stored in OneDrive with all members of the team having access to the documentation. These project documents will be live and editable while old files will be placed into the project archive.

11. Project Management

The project management section is broken into deliverables, dependencies, and an overall view. An additional Gantt chart has been provided (Appendix A and B) to clarify project schedules that have been produced by Team 4 Integration Services in partnership with DTX. This project requires experts in several fields WAN, LAN, wireless and security. Team 4 Integration Services has assigned team members with the required background in the specified fields to this project. Overall project management team lead has been accepted by David Dollan as well as the wireless design role. The team lead's responsibilities are to keep the team on task and adjust as necessary to see the project to successful completion. The WAN responsibilities will be managed by Jeff Wilson as well as the project manager role. The project manager role set dates for task and meetings, confirms task completion, monitors cost and ensures all members have the time needed to successfully complete assignments. Jamish Patel has the roles of document specialist and security design. The document specialist's responsibilities are to review team created documents and confirm content meets requirements before being shared with customer or other teams peer review. Brian Snyder has the roles of presenter and LAN specialist for the team. The presenter will manage documents so they can be presented to the customer and for peer review.

11.1.Deliverables

DTX Deliverables

Project plan to include:

- DTX requirements and goals of project
- Gantt scheduling chart
- Staffing management plan
- Risk register

Hardware and Labor

- All hardware and labor costs are specified in the bill of materials in section 6.4.

Technical Documents

- Detailed WAN diagram
- Detailed facility wiring diagram
- Detailed MDF cabinet equipment layout
- Detailed LAN diagram
- Detailed wireless diagram

11.2.Dependencies

Items below are dependent on the previous task

- Network Diagram from DTX
- DTX recommended Network IP addressing
- Core equipment at headend site in Florida
- Circuit installation at Texas location
- Power LAN cabling and MDF cabinet at Texas Location
- Remote MX and switching infrastructure
- Wireless survey

11.3.Schedule

Table 7: Capstone Deliverables

Rising Phoenix				
Team 4				
Team Lead: David Dollan		Project Start:	Sun, 9/20/2020	
TASK	**ASSIGNED TO**	**PROGRESS**	**START**	**END**
Vision and Scope Draft	Team 4	100%	9/20/20	10/4/20

Aropa Peer Review	Individuals	0%	10/4/20	10/11/20
Aropa Revised Vision & Scope	Individuals & Team Leader	0%	10/11/20	10/18/20
White Paper Draft	Individuals	0%	10/18/20	10/23/20
White Paper Peer Review	Individuals	0%	10/23/20	10/25/20
Final Report Start /Include Presentation Draft	Team 4	0%	10/25/20	11/8/20
Final Report Peer Review	Individuals	0%	11/8/20	11/15/20
Presentation Draft	Team 4	0%	11/8/20	11/14/20
Final Report Revision	Team 4	0%	11/16/20	11/22/20
Presentation Revised	Team 4	0%	11/23/20	11/28/20

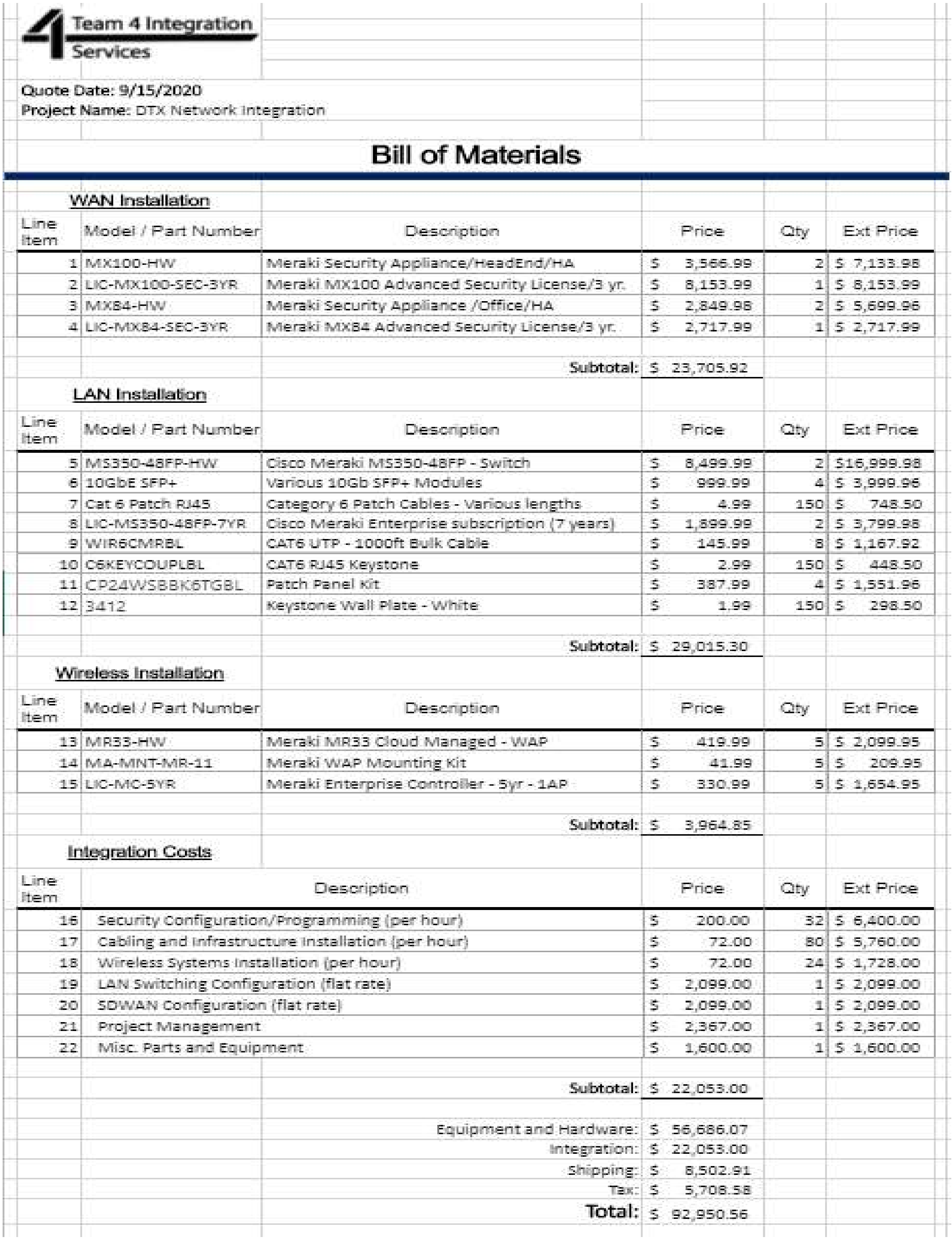
Table 8: DTX Deliverables

Rising Phoenix				
Team 4				
Team Lead: David Dollan		Project Start:	Sun, 9/20/2020	
TASK	**ASSIGNED TO**	**PROGRESS**	**START**	**END**
Customer Meet /Gather Requirements	DTX staff and Team 4	100%	9/20/20	9/27/20
Request Current Network Design Documents	DTX IT Staff	100%	9/27/20	10/2/20
Proposed Solution Review	DTX staff and Team4	100%	10/2/20	10/4/20
Place circuits orders per Team 4 specifications	DTX	0%	10/4/20	12/3/20
Place equipment orders	Team 4	0%	10/4/20	10/6/20
Cabling begins at Location starting with MDF equipment	Team 4	0%	10/6/20	11/15/20
Install Headend Equipment	Team 4 /DTX IT staff	0%	10/18/20	10/25/20
Install remote office Equipment	Team 4	0%	11/15/20	11/21/20
Test circuit and equipment	Team 4	0%	12/5/20	12/11/20
User testing	DTX TEAM 4	0%	12/12/20	12/17/20
Complete project	Team 4		12/17/20	12/20/20

11.4.Budget

The budget in as shown in Figure 2 is to be reviewed by the finance department and is an estimate of the overall project cost. This estimate may change. Therefore, the organization needs to be prepared in order to adapt to any changes within the budget. However, if there are any costs that greatly exceed these budget guidelines the project manager is required to submit an inquiry to the finance department. These issues will be dealt with specifically on a case to case basis.

Figure 2: Copy of the Bill of Materials list provided to DTX



Team 4 Integration Services

Quote Date: 9/15/2020
Project Name: DTX Network Integration

Bill of Materials

WAN Installation

Line Item	Model / Part Number	Description	Price	Qty	Ext Price
1	MX100-HW	Meraki Security Appliance/HeadEnd/HA	$ 3,566.99	2	$ 7,133.98
2	LIC-MX100-SEC-3YR	Meraki MX100 Advanced Security License/3 yr.	$ 8,153.99	1	$ 8,153.99
3	MX84-HW	Meraki Security Appliance /Office/HA	$ 2,849.98	2	$ 5,699.96
4	LIC-MX84-SEC-3YR	Meraki MX84 Advanced Security License/3 yr.	$ 2,717.99	1	$ 2,717.99
		Subtotal:	$ 23,705.92		

LAN Installation

Line Item	Model / Part Number	Description	Price	Qty	Ext Price
5	MS350-48FP-HW	Cisco Meraki MS350-48FP - Switch	$ 8,499.99	2	$16,999.98
6	10GbE SFP+	Various 10Gb SFP+ Modules	$ 999.99	4	$ 3,999.96
7	Cat 6 Patch RJ45	Category 6 Patch Cables - Various lengths	$ 4.99	150	$ 748.50
8	LIC-MS350-48FP-7YR	Cisco Meraki Enterprise subscription (7 years)	$ 1,899.99	2	$ 3,799.98
9	WIR6CMRBL	CAT6 UTP - 1000ft Bulk Cable	$ 145.99	8	$ 1,167.92
10	C6KEYCOUPLBL	CAT6 RJ45 Keystone	$ 2.99	150	$ 448.50
11	CP24WSBBK6TGBL	Patch Panel Kit	$ 387.99	4	$ 1,551.96
12	3412	Keystone Wall Plate - White	$ 1.99	150	$ 298.50
		Subtotal:	$ 29,015.30		

Wireless Installation

Line Item	Model / Part Number	Description	Price	Qty	Ext Price
13	MR33-HW	Meraki MR33 Cloud Managed - WAP	$ 419.99	5	$ 2,099.95
14	MA-MNT-MR-11	Meraki WAP Mounting Kit	$ 41.99	5	$ 209.95
15	LIC-MC-5YR	Meraki Enterprise Controller - 5yr - 1AP	$ 330.99	5	$ 1,654.95
		Subtotal:	$ 3,964.85		

Integration Costs

Line Item	Description	Price	Qty	Ext Price
16	Security Configuration/Programming (per hour)	$ 200.00	32	$ 6,400.00
17	Cabling and Infrastructure Installation (per hour)	$ 72.00	80	$ 5,760.00
18	Wireless Systems Installation (per hour)	$ 72.00	24	$ 1,728.00
19	LAN Switching Configuration (flat rate)	$ 2,099.00	1	$ 2,099.00
20	SDWAN Configuration (flat rate)	$ 2,099.00	1	$ 2,099.00
21	Project Management	$ 2,367.00	1	$ 2,367.00
22	Misc. Parts and Equipment	$ 1,600.00	1	$ 1,600.00
	Subtotal:	$ 22,053.00		

Equipment and Hardware:	$ 56,686.07
Integration:	$ 22,053.00
Shipping:	$ 8,502.91
Tax:	$ 5,708.58
Total:	$ 92,950.56

12. Educational/Program Outcomes

Overall, educational outcomes will require students to develop a successful functioning team. Teamwork will be critical in completion of the project. The assignment has project management and business aspects. Critical skills in understanding business needs, defining, and aligning goals while working within a scope will test student's abilities to adapt to and perform in a real-world type of project. Communication, task ownership, and agreement will be an important feature in the success of this exercise.

12.1.General Education

In this project, Team 4 will need to turn customer driven business needs into a customized technical solution that is not only robust but is also manageable and secure. In doing so, the team will need to work both individually and together to produce well written documentation that meets all requirements of the project. These skills have been learned over several classes at Franklin University and will be essential in the production of this deliverable. Team members will also face challenges in turning ideas into actionable items, working within schedules, maintaining documentation and using effective communications in order to deliver a comprehensive project targeted to the customer requirements. Critical thinking and practical application skills that have been acquired by all team members will be utilized to combine all aspects of the project and to ensure project objective meet real-world scenarios. Throughout the process, risk and limitations will be identified and mitigated. These risks could be either technical in nature or resource driven and are in line with project management principles that are needed to advance team goals.

12.2.Information Technology

This project includes many different technology categories that will require research into many aspects of information technology. For all subsections of this project (WAN, LAN, wireless, and network security) systems design is critical and starts with computer systems fundamentals. On this foundation is built more refined areas of Information technology such as networking components, security protocols, system configuration standards, and industry best practices. These subjects and past course load provide the guidance needed to create a project that combines many Information Technology disciplines into a single product that can be an imitation of real-world situations. The team will also need to justify that the technology solution meets the business requirements, is cost effective, and conforms to project management best practices. This is essential as an educational outcome as all organizations will have a focus on what is being produced, the overall cost breakdown, and the effort needed for the production. These concepts have been clearly defined in several Information Technology classes at Franklin University and will be fully applied during this project.

13. Annotated Bibliography

Cisco. (2018). *Conducting Site Surveys with MR Access Points*. Retrieved October 2, 2020, from Meraki Documentation: https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Conducting_Site_Surveys_with_MR_Access_Points
This guide provides some best practices for conducting site surveys with Meraki MR access points. The information allows administrators of Meraki MR systems to perform a basic site survey without expensive equipment and while using the same access points that would be used in the deployment. This can be accomplished by using the broadcast SSID of the access point and then measuring signal strength on a computer. Additionally, this guide provides further tips for site surveys such as understanding the building layout and the types of devices or clients that may be connecting to the system.

Cisco. (2018). *MX Warm Spare - High Availability Pair*. Retrieved October 1, 2020, from Meraki Documentation: https://documentation.meraki.com/MX/Deployment_Guides/MX_Warm_Spare_-_High_Availability_Pair
Used in WAN configuration (HA)

Cisco. (2018). *Signal-to-Noise Ratio (SNR) and Wireless Signal Strength*. Retrieved October 2, 2020, from Meraki Documentation: https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Signal-to-Noise_Ratio_(SNR)_and_Wireless_Signal_Strength
This online document provides an overview of the importance of understanding the signal-to-noise ratio when deploying a wireless system. Signal noise can come from various devices in the immediate area to the wireless deployment and needs to be accounted for to ensure that connected devices are able to receive the correct wireless signal at the maximum strength possible. For a Meraki deployment, the signal to noise ratio information can be found on both the Meraki Dashboard and through each access point interface.

Cisco. (2018). *Splash Page Details for Meraki MR*. Retrieved October 2, 2020, from Meraki Documentation: https://documentation.meraki.com/MR/MR_Splash_Page/Splash_Page_Details_for_Meraki_MRThis document provides information on the various ways that a Meraki wireless system is able to deploy a captive portal environment for guest users. This can be accomplished in several ways to allow system administrators to take advantage basic levels of security for their WIFI guests. Additionally, the captive portal can also be set up as a pay-per-access model where guest would need to submit payment information prior to accessing the guest network.

Charfi, E., Chaari, L., Ben Hlima, S., & Kammoun, L. (2017). Multi-user access mechanism with intra-access categories differentiation for IEEE 802.11ac wireless local area networks. Retrieved October 2, 2020, from Telecommunication Systems, 64(3), 479–494. https://doi-org.links.franklin.edu/10.1007/s11235-016-0187-x
This periodical explores the 802.11ac wireless standard and how the technology is able to allow for multiple methods for communications by multiple devices at once. The

802.11 AC standard has much greater speed, bandwidth, and quality of service than previous standards by utilizing DL MU-MIMO transmitters and receivers. This provides simultaneous streams of data that allow devices better connectivity and transfer rates than in other 802.11 standards.

Meraki Auto VPN General Best Practices. (2020, July 16). Retrieved October 01, 2020, from https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Best_Practice_Design_-_MX_Security_and_SD-WAN/Meraki_Auto_VPN_General_Best_Practices
This site provides information on the deployment best practices for Meraki secure VPN solution.
This Meraki guide was created to help installers follow best practices when deploying Meraki auto VPN service. It lists best practices focused on the most common deployment scenarios for most topologies. The document provides recommended SD-WAN architecture for most deployments and gives detailed examples and the purpose of selecting features and options

MX Sizing Guide, (2020, April 2020). Retrieved October 01, 2020, from https://meraki.cisco.com/lib/pdf/meraki_whitepaper_mx_sizing_guide.pdf
This guide provides information on sizing Meraki MX security appliance to meet customer needs
This document released by *Meraki* list and compares the different models of the *MX* security devices. The document provides benchmark testing using industry standards that are designed to help you compare MX security appliances to firewalls from other vendors and the recommended MX product for your environment. This is good for scaling for the correct number of users, example if you have 550 users choose and *MX* that supports 1000 user.

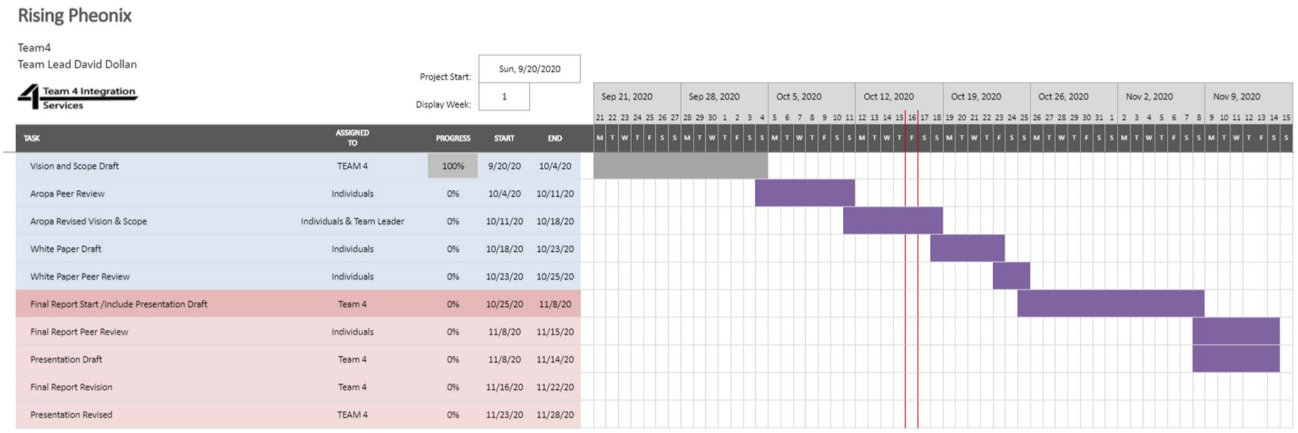
Trounce, D. (2019, November 30). *How to Estimate Bandwidth Requirements for a Business Site or Network*. Retrieved October 1, 2020, from Help Desk Geek: https://helpdeskgeek.com/networking/how-to-estimate-bandwidth-requirements-for-a-business-site-or-network/
This information aligned with Microsoft 0365 research and Cisco for bandwidth calculations.

The World's First ML-Powered NGFW. (n.d.). Retrieved October 17, 2020, from https://www.paloaltonetworks.com/network-security/next-generation-firewall
This document provides the information about Palo-Alto next generation firewalls, features. it’s also talks about how this firewall being beneficial to other organization and protect their network environment with security threats and attacks.

Walker, J. (2017, October 10). Top 7 security risks that small businesses should know about. Retrieved October 03, 2020, from https://www.monitis.com/blog/top-7-security-risks-that-small-businesses-should-know-about/

This document provides the information about security risks that business should know about. In this document they also talk about that cyber-criminals have scaled up their efforts they've also discovered that small businesses are easy pickings for stealing data. Lack of robust security infrastructure, less cyber-security tools and resources, and little or no prevention training often amount to an open invitation for a data breach.

Appendix A – Class Project Gantt Chart



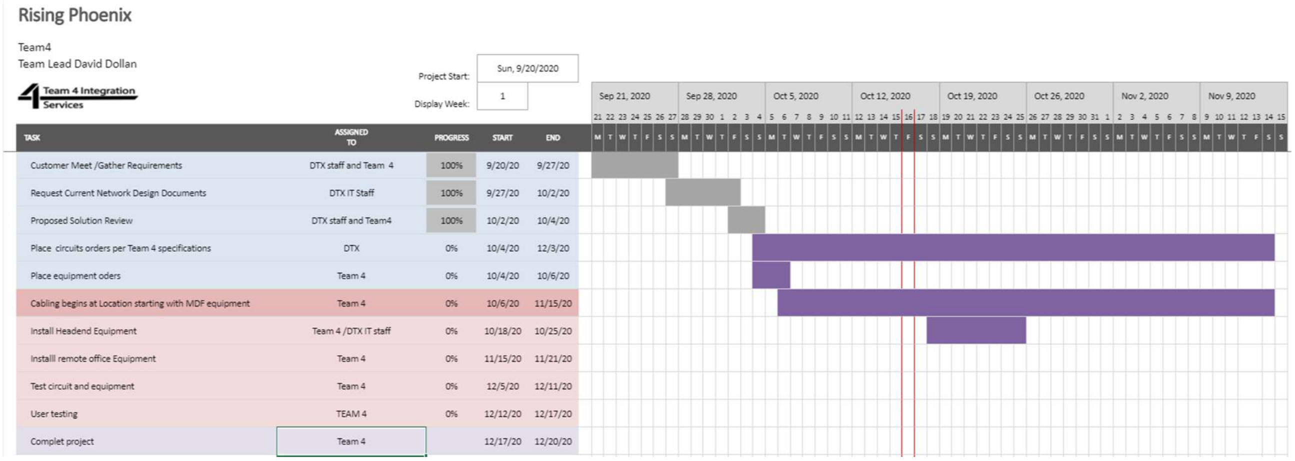
Rising Pheonix

Team4
Team Lead David Dollan

Project Start: Sun, 9/20/2020
Display Week: 1

TASK	ASSIGNED TO	PROGRESS	START	END
Vision and Scope Draft	TEAM 4	100%	9/20/20	10/4/20
Aropa Peer Review	Individuals	0%	10/4/20	10/11/20
Aropa Revised Vision & Scope	Individuals & Team Leader	0%	10/11/20	10/18/20
White Paper Draft	Individuals	0%	10/18/20	10/23/20
White Paper Peer Review	Individuals	0%	10/23/20	10/25/20
Final Report Start /Include Presentation Draft	Team 4	0%	10/25/20	11/8/20
Final Report Peer Review	Individuals	0%	11/8/20	11/15/20
Presentation Draft	Team 4	0%	11/8/20	11/14/20
Final Report Revision	Team 4	0%	11/16/20	11/22/20
Presentation Revised	TEAM 4	0%	11/23/20	11/28/20

Appendix B – Customer (DTX) Gantt Chart



Rising Phoenix

Team4
Team Lead David Dollan

Project Start: Sun, 9/20/2020
Display Week: 1

TASK	ASSIGNED TO	PROGRESS	START	END
Customer Meet /Gather Requirements	DTX staff and Team 4	100%	9/20/20	9/27/20
Request Current Network Design Documents	DTX IT Staff	100%	9/27/20	10/2/20
Proposed Solution Review	DTX staff and Team4	100%	10/2/20	10/4/20
Place circuits orders per Team 4 specifications	DTX	0%	10/4/20	12/3/20
Place equipment oders	Team 4	0%	10/4/20	10/6/20
Cabling begins at Location starting with MDF equipment	Team 4	0%	10/6/20	11/15/20
Install Headend Equipment	Team 4 /DTX IT staff	0%	10/18/20	10/25/20
Installl remote office Equipment	Team 4	0%	11/15/20	11/21/20
Test circuit and equipment	Team 4	0%	12/5/20	12/11/20
User testing	TEAM 4	0%	12/12/20	12/17/20
Complet project	Team 4		12/17/20	12/20/20

Appendix C – Response to Reviewers

This document has been reviewed by class peers and the following comments have been selected by Team 4 to include as part of the editing process. There are two parts to each review. The first part is the peer review, and the second part is the team's response.

<u>Review 1</u> - Team 4 did great work in articulating the client needs and discussing the means in which they attend to address these concerns. The writing was solid, particularly in the early sections of the document. There are a handful of typos and grammatical errors within the document such as "VIOP" instead of "VoIP", or "greater that" instead of "greater than", among others. One of the most frequent issues with grammar was the consistency in capitalizing letters. Some terms, such as "Network Security" are arbitrarily capitalized, despite not being proper nouns. Bullet point items would sometimes contain capitalized letters, other times they would not. The section regarding the Palo Alto firewall is a current concern, as it is copied from the manufacturer site without citation. Additionally, that section mentions jargon such as being "ML-based" without detailing that this means machine-learning, or what that means to DTX. In my opinion, the solution itself is well-designed, the appliances and circuits that were chosen should accomplish the goals if this organization without being unreasonable regarding time or budget. The bibliography contained enough references, and they were properly formatted.

> **Response -** The team review the document for grammar, consistency, and verbiage and corrected issues seen by the reviewer. The section regarding the Palo Alto Firewall has been modified to include APA citations and information about machine learning have been modified to include how it applies to the project.

Review 2 - The scope and limitations section were thorough and successfully covered many of the aspects of the project. One item that is currently unclear is the "monitoring platform". What is the chosen monitoring solution for this project, and how will it help DTX address their needs? Later in the document, this system is not included in the budget, however, it is advertised as being part of the scope of initial release. If both are true, this will result in either hidden costs for DTX, a need for Integration Services to cover these expenses out of pocket, or an adjustment of the scope post-implementation. Generally speaking, the project seems right sized for the team and schedule. The limitations section is wise to include items outside of the scope of the project.

> **Response -** The team has made clear in the final version that Meraki Cloud Dashboard will be used as the full monitoring solution which comes with the purchase of the chosen solution.

Review 3 - The business context sections are straightforward and aligned with the requirements. The stakeholders that are listed in table 3 does a good job of encapsulating the goals of each involved party. I was a bit confused on table 4 and the time limitations of the project. The stakeholder table mentions no flexibility with delays, then the subsequent table goes on to detail that there are degrees of freedom after all. The cost concerns are similar, the project stakeholders budget is listed as 150k, the priorities table projected budget is 100k, and budget overruns allows 10%, which is 110k. I am not suggesting this is incorrect, I just feel it could be explained more succinctly in the introductory paragraph.

Response - Budgetary conditions have been reviewed and clarified in the stakeholders' table. This notes the overall budget for DTX's office move versus the budget for the network integration.

Review 4 - The section regarding educational outcomes could use some extra substance. The area regarding general education highlights the ways in which project management education has been obtained and will be utilized. I feel this draft document was robust and inclusive of a great deal of material. With that said, it contained plenty of additional general education outcomes that could be included in this summary. The section regarding information technology is even more scarce despite having exceptionally more applicable content. It might be difficult to tie all four of the IT program aspects into the project, but certainly at least three of those bullet points could be expanded on.

Response - The team reworded educational outcomes and added content that clarified the team's position.

Review 5 - This team composed a thorough analysis of their "customer." They have evaluated all areas of need for the project and provided scope and depth for each area. They have included substantial figures and tables that document each of the areas to be included in the project. They have a detailed schedule that includes a timeframe for each deliverable as well as a substantially detailed budget. Their annotated bibliography is correct, except the second one down doesn't have details in it that include the literary review. The left out their team logo.

Response - The bibliography has been modified to include additional synopsis information for three of the references in question.

Review 6 - Better description on the installation of cat 6. A complete infrastructure overhaul (Including cat 6 cable running) seems a little bit crazy for a team of 8. Are contractors handling that?

Response - The team has clarified that the cabling of the CAT 6 infrastructure will be handled by third party contracted by Team 4 Integration Services.

Review 7 - The business context presents the issues DTX must address. The stakeholder profiles need work. These are too generalized to be appropriate. Who are the stakeholders in the DTX Organization and what are their interests in this project? The document just states that DTX as an entire organization is a stakeholder. The CEO, CFO, or perhaps a technology related position such as a CIO if they have one may be potential stakeholders within the organization. These varying positions would have different attitudes and interest in the project. That is one of the things that make it so difficult to perform a project is how to make all aspects of an organization satisfied. The rest of the section looks well and the previous issue can be easily adjusted.

> **Response -** The team has added additional stakeholder information to address this concern.

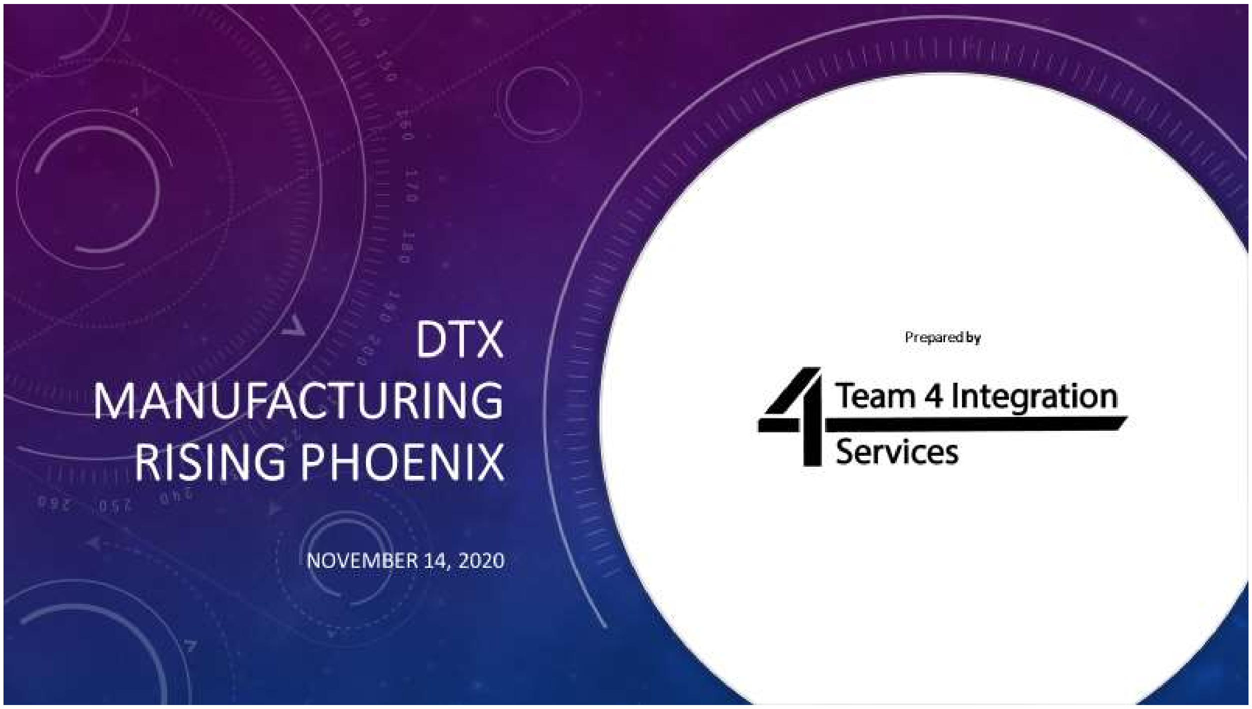
Review 8 - In the team charter section, the responsibilities of the team are presented well. Regular team meetings are brought up so an idea to enhance this section is providing what platform is being used for the team meetings. If the team is using Zoom, Microsoft Teams, Google Meet, or whatever other platform maybe just mention that here. Another thing is where are all files being stored? I know email is mentioned as the primary form of communications, but are all documents from the team being sent directly to the team lead? Section 5.4 does a nice job at explaining the communication strategy for the class project. How communications regarding the Team 4 Integration project can be included here as well. Things like how will progress reports be sent out to stakeholders, what training, if any, will be provided, what is someone from DTX has a question who will they contact, can all be addressed in a paragraph or two here.

> **Response -** Communication strategies have been clarified to include collaboration platforms used and how project documents are stored and maintained.

Review 9 - The human resource part of the project is well defined, the team structure is explained and how each member of the team will contribute to the success of the project. A method of communication was established, and an alternate method of communication was also put in place. The team meeting schedule is a very good idea, one issue that was not address is what actions should be taken in case the team notices that a team member is under-performing this is something that needs to be mentioned and thought of but overall the method of resolving conflicts and the team setup is good.

> **Response -** Information about under-performing team members have been added to this section

14. Appendix B: Presentation Slides

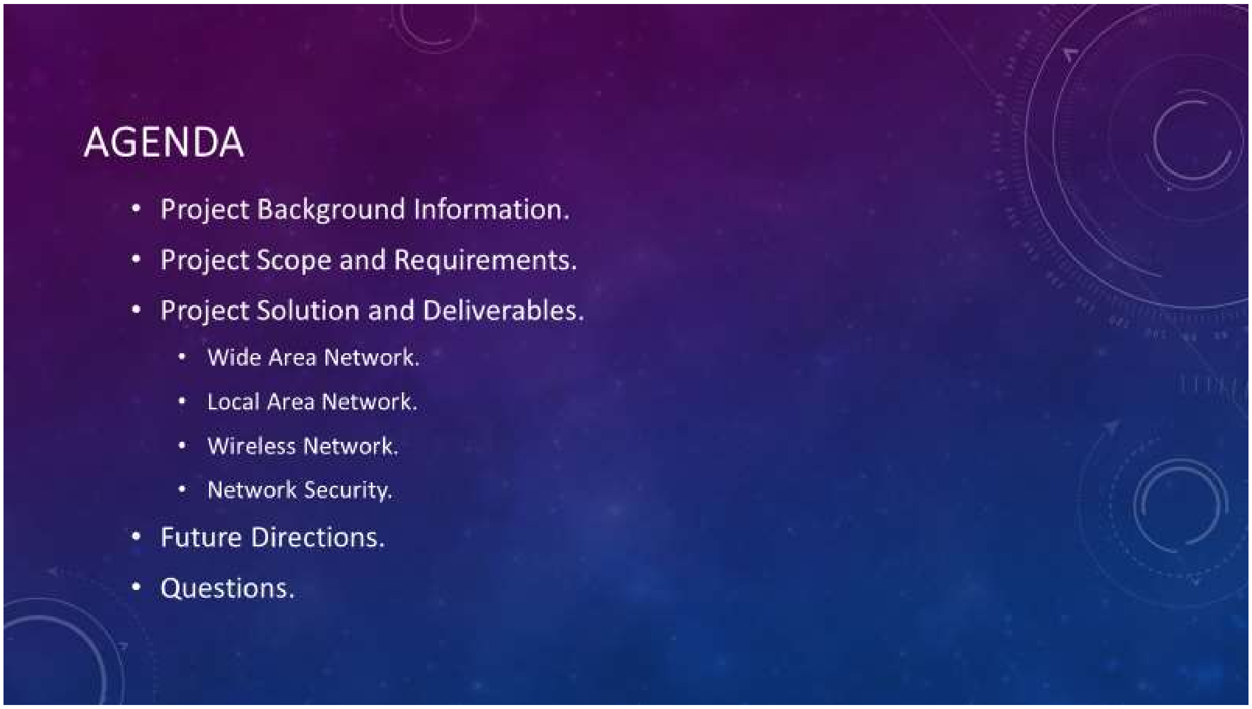


DTX MANUFACTURING RISING PHOENIX

NOVEMBER 14, 2020

Prepared by

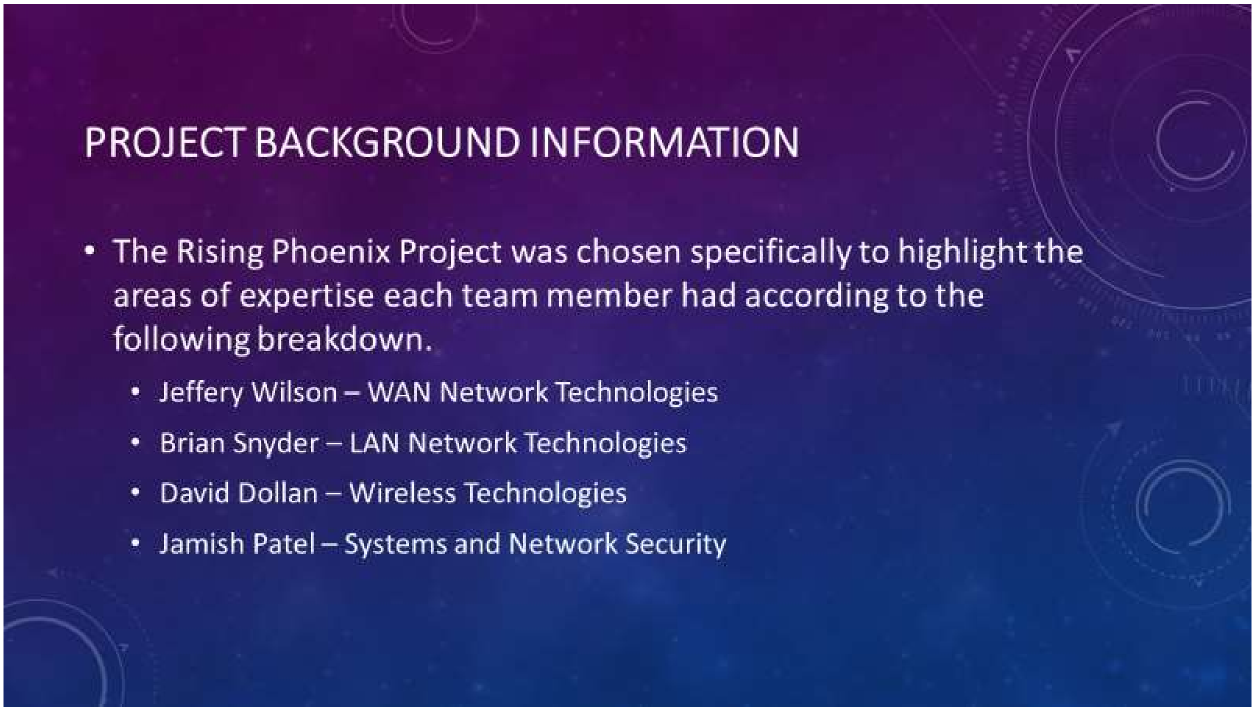
Team 4 Integration Services



AGENDA

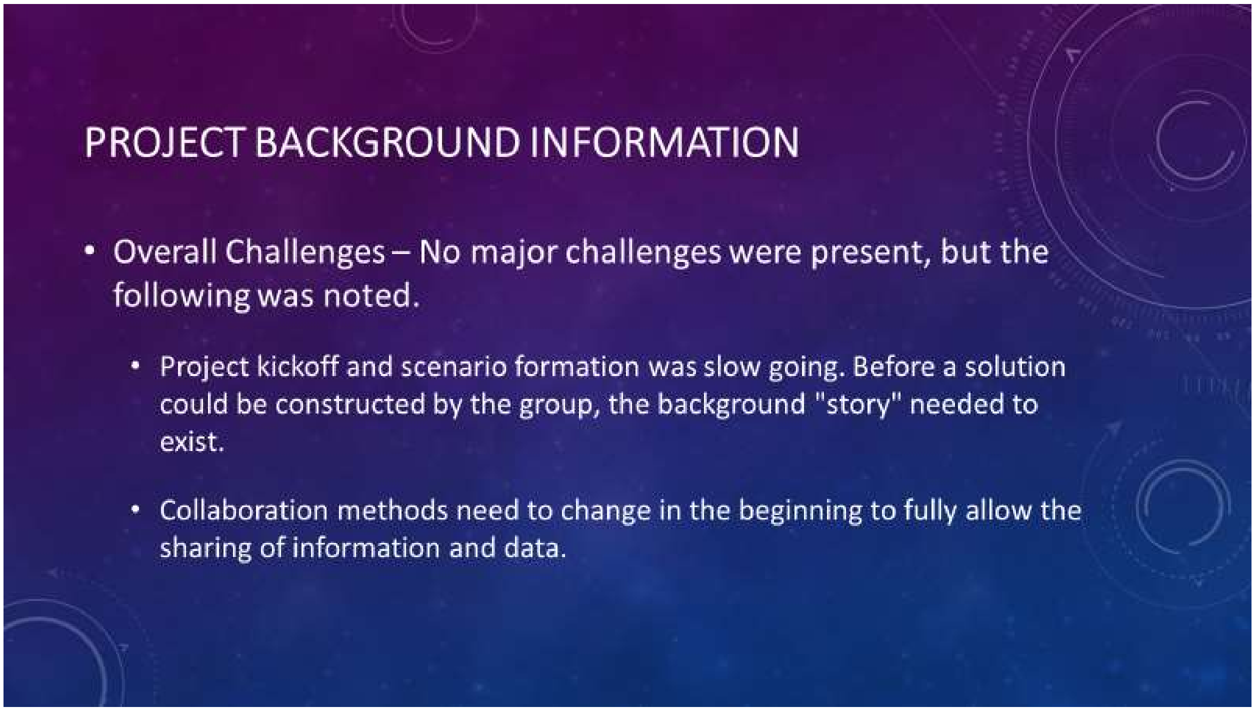
- Project Background Information.
- Project Scope and Requirements.
- Project Solution and Deliverables.
  - Wide Area Network.
  - Local Area Network.
  - Wireless Network.
  - Network Security.
- Future Directions.
- Questions.

PROJECT BACKGROUND INFORMATION



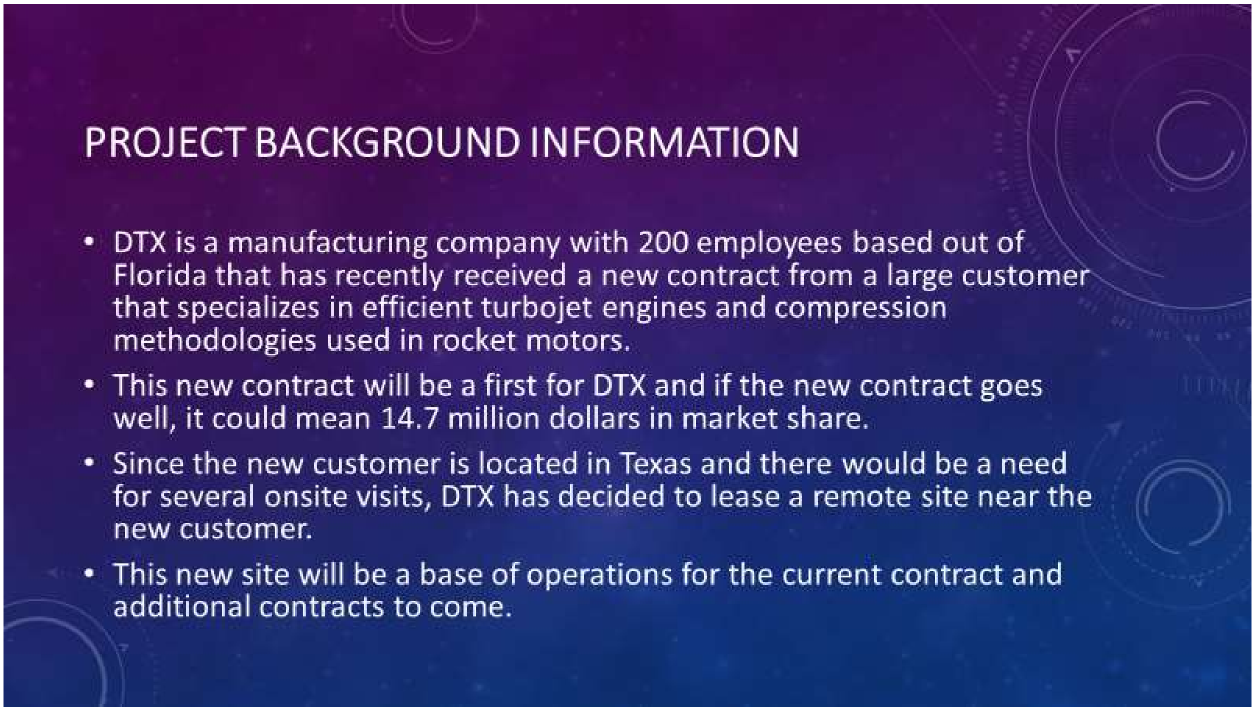
PROJECT BACKGROUND INFORMATION

- The Rising Phoenix Project was chosen specifically to highlight the areas of expertise each team member had according to the following breakdown.
  - Jeffery Wilson – WAN Network Technologies
  - Brian Snyder – LAN Network Technologies
  - David Dollan – Wireless Technologies
  - Jamish Patel – Systems and Network Security



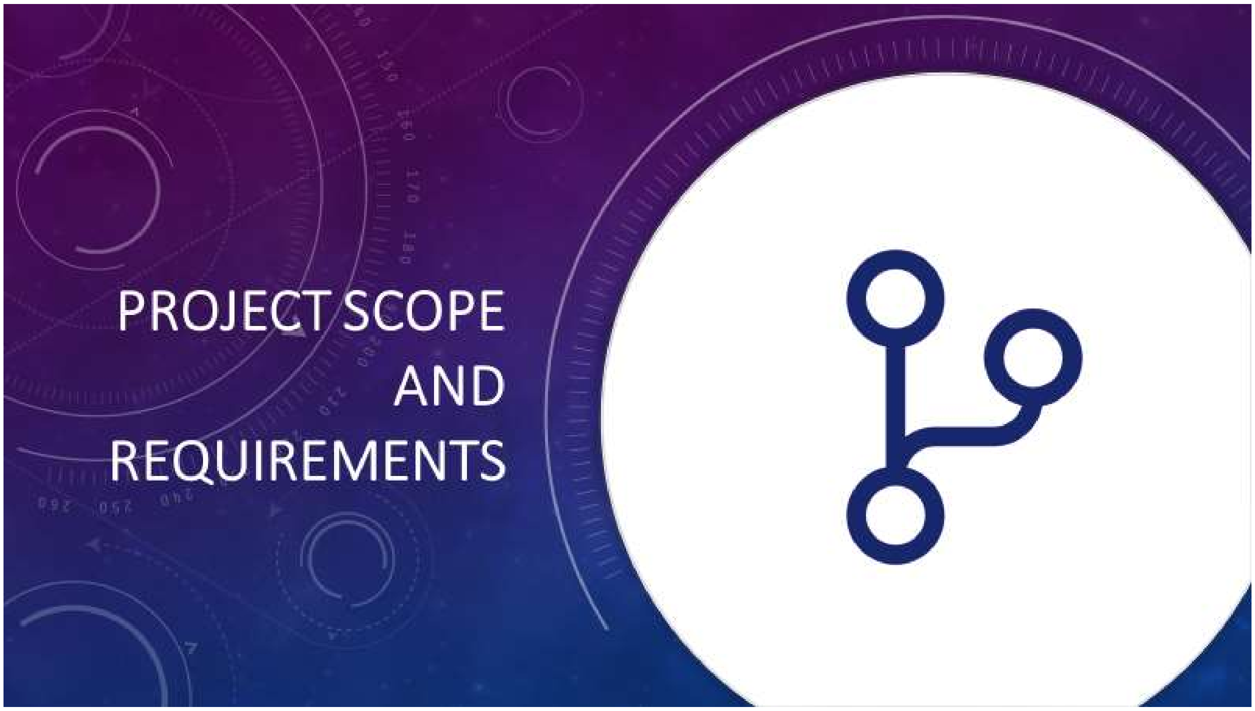
PROJECT BACKGROUND INFORMATION

- Overall Challenges – No major challenges were present, but the following was noted.
  - Project kickoff and scenario formation was slow going. Before a solution could be constructed by the group, the background "story" needed to exist.
  - Collaboration methods need to change in the beginning to fully allow the sharing of information and data.

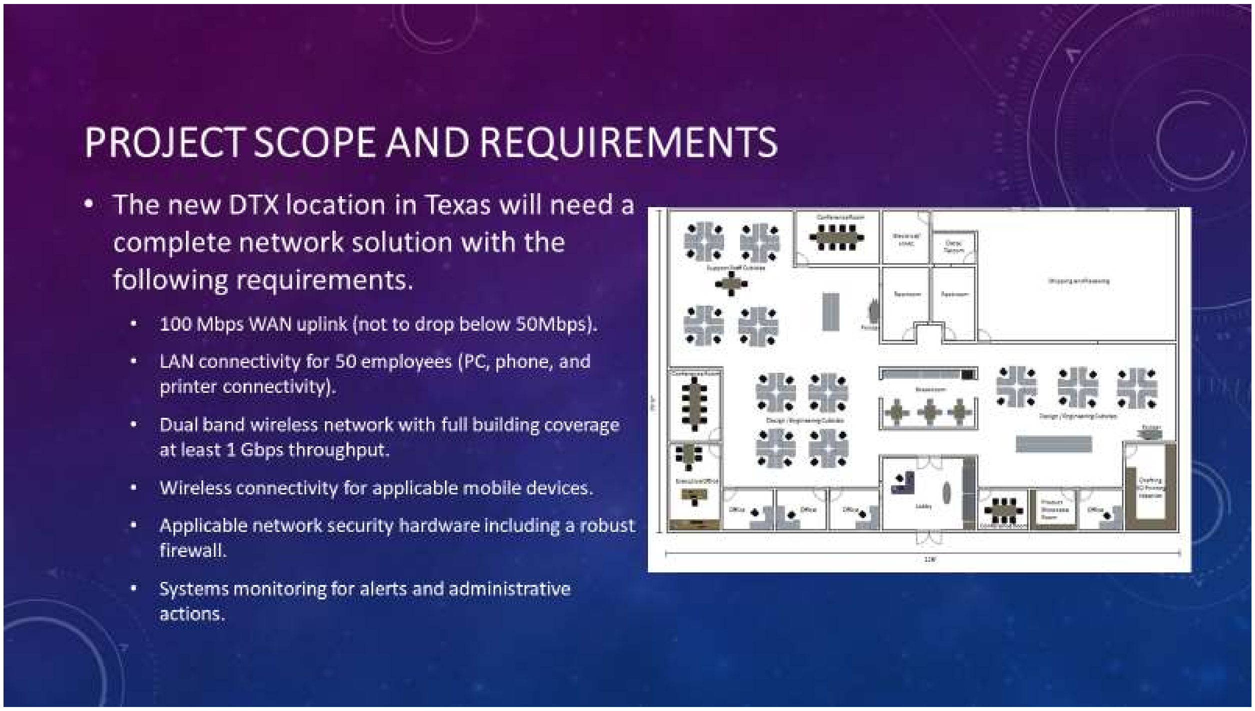


PROJECT BACKGROUND INFORMATION

- DTX is a manufacturing company with 200 employees based out of Florida that has recently received a new contract from a large customer that specializes in efficient turbojet engines and compression methodologies used in rocket motors.
- This new contract will be a first for DTX and if the new contract goes well, it could mean 14.7 million dollars in market share.
- Since the new customer is located in Texas and there would be a need for several onsite visits, DTX has decided to lease a remote site near the new customer.
- This new site will be a base of operations for the current contract and additional contracts to come.

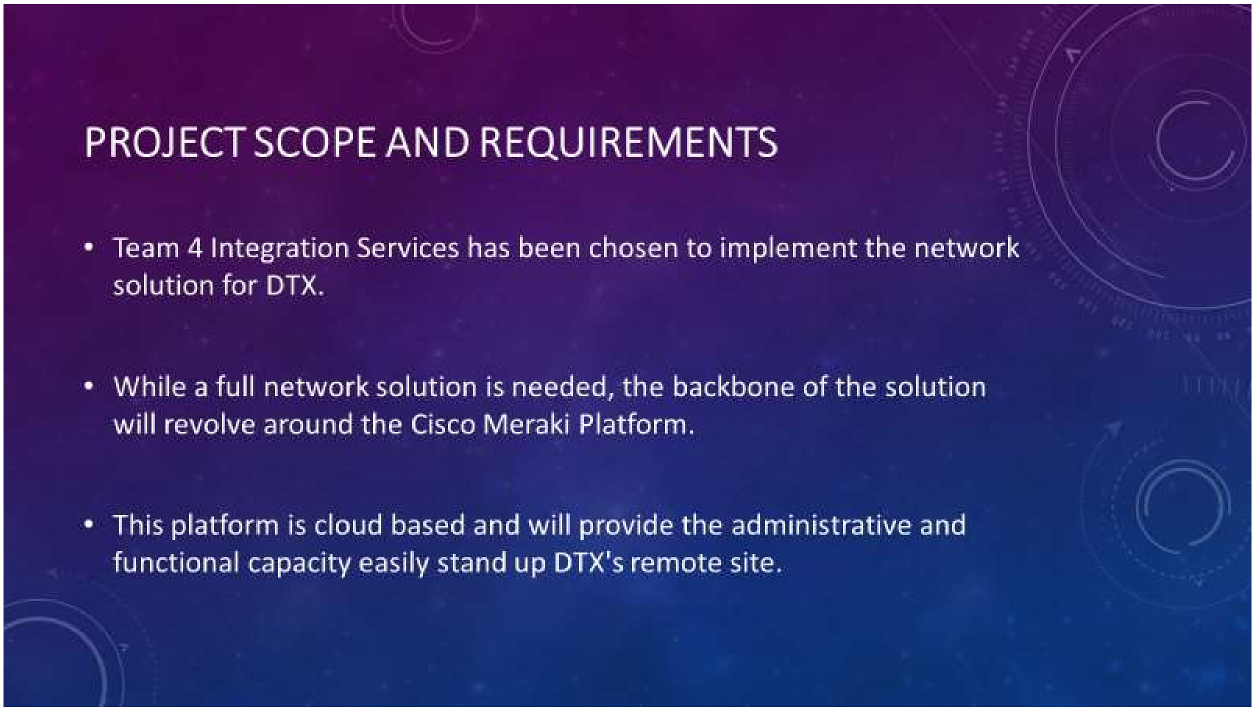


PROJECT SCOPE AND REQUIREMENTS



PROJECT SCOPE AND REQUIREMENTS

- The new DTX location in Texas will need a complete network solution with the following requirements.
  - 100 Mbps WAN uplink (not to drop below 50Mbps).
  - LAN connectivity for 50 employees (PC, phone, and printer connectivity).
  - Dual band wireless network with full building coverage at least 1 Gbps throughput.
  - Wireless connectivity for applicable mobile devices.
  - Applicable network security hardware including a robust firewall.
  - Systems monitoring for alerts and administrative actions.



PROJECT SCOPE AND REQUIREMENTS

- Team 4 Integration Services has been chosen to implement the network solution for DTX.
- While a full network solution is needed, the backbone of the solution will revolve around the Cisco Meraki Platform.
- This platform is cloud based and will provide the administrative and functional capacity easily stand up DTX's remote site.

PROJECT SCOPE AND REQUIREMENTS

Budget Information

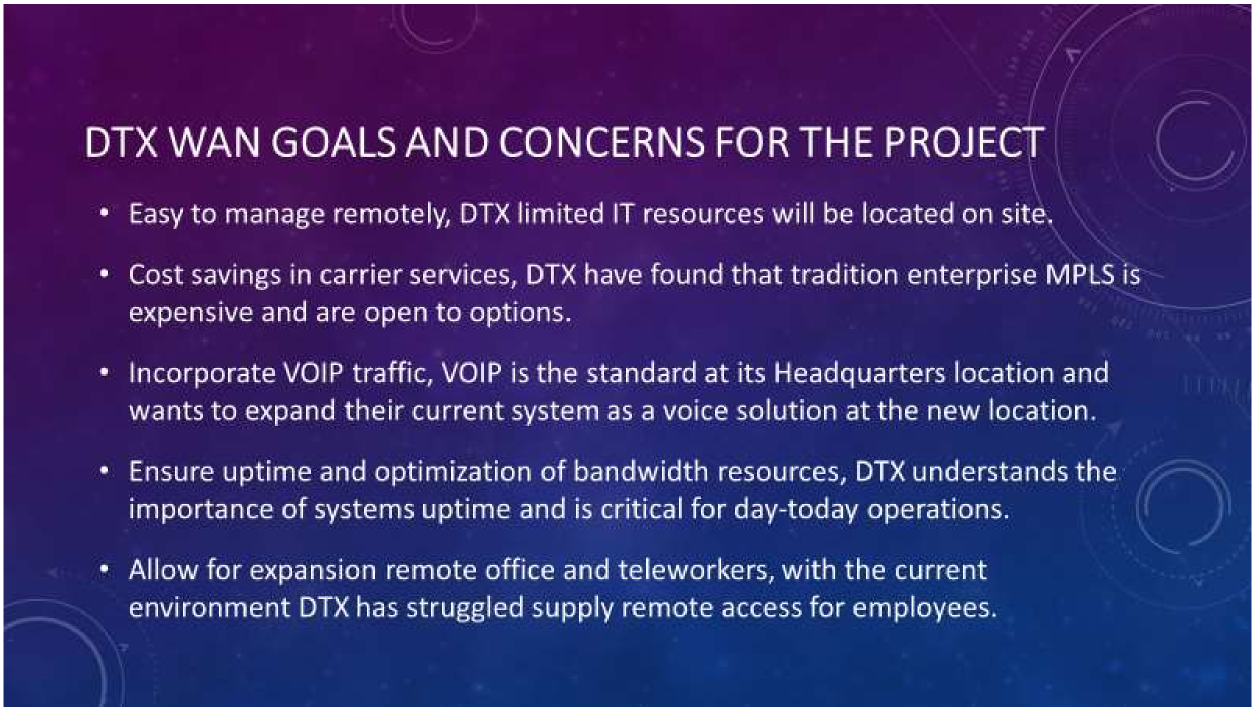
- Remote site total = $530,000
- Rising Phoenix Budget = $100,000
- Overage = 10%
- Delivered Solution Cost = $96,760.61
- Under Budget = $3,239.39

Risks

- WAN Failure
- Insufficient Bandwidth
- Hardware Failures
- Wireless Frequency Saturation
- Network outage during Firewall Migration

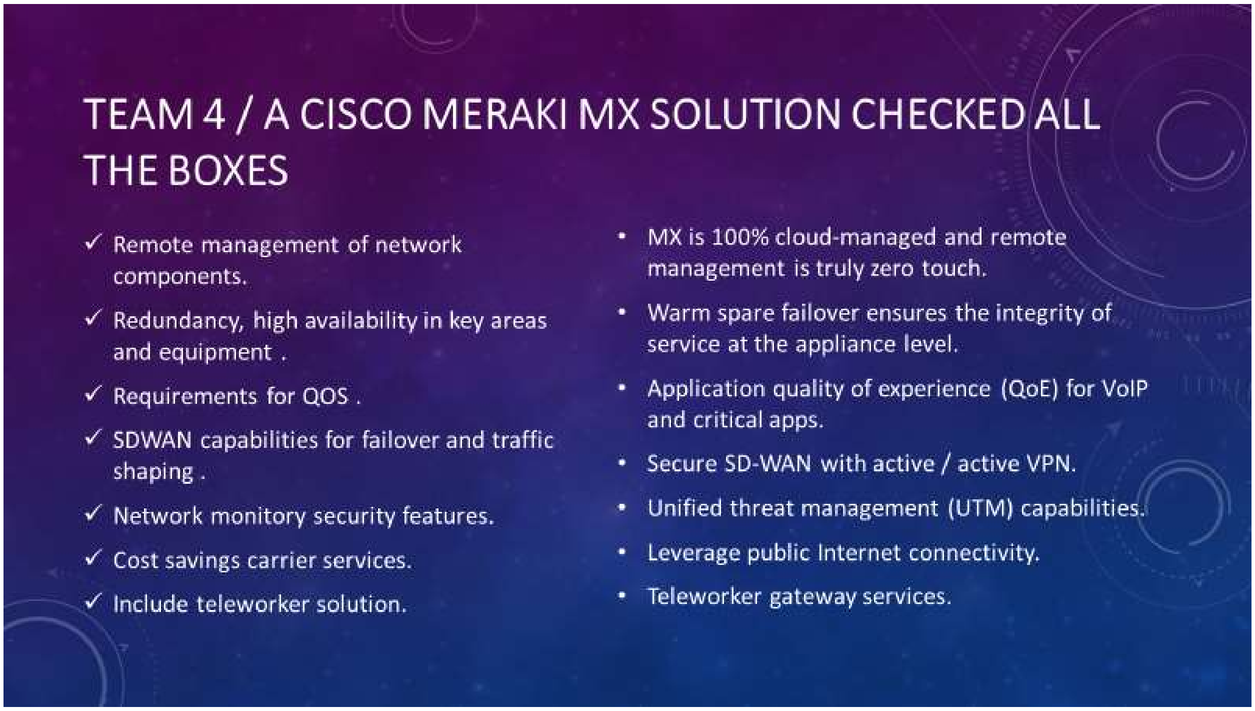
PROJECT SOLUTION AND DELIVERABLES

WAN SOLUTION AND INFRASTRUCTURE



DTX WAN GOALS AND CONCERNS FOR THE PROJECT

- Easy to manage remotely, DTX limited IT resources will be located on site.
- Cost savings in carrier services, DTX have found that tradition enterprise MPLS is expensive and are open to options.
- Incorporate VOIP traffic, VOIP is the standard at its Headquarters location and wants to expand their current system as a voice solution at the new location.
- Ensure uptime and optimization of bandwidth resources, DTX understands the importance of systems uptime and is critical for day-today operations.
- Allow for expansion remote office and teleworkers, with the current environment DTX has struggled supply remote access for employees.



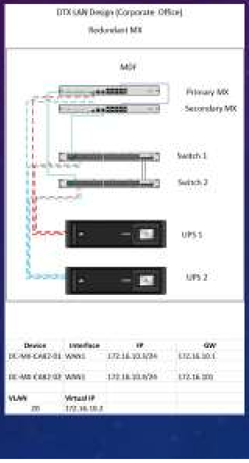
TEAM 4 / A CISCO MERAKI MX SOLUTION CHECKED ALL THE BOXES

- ✓ Remote management of network components.
- ✓ Redundancy, high availability in key areas and equipment .
- ✓ Requirements for QOS .
- ✓ SDWAN capabilities for failover and traffic shaping .
- ✓ Network monitory security features.
- ✓ Cost savings carrier services.
- ✓ Include teleworker solution.

- MX is 100% cloud-managed and remote management is truly zero touch.
- Warm spare failover ensures the integrity of service at the appliance level.
- Application quality of experience (QoE) for VoIP and critical apps.
- Secure SD-WAN with active / active VPN.
- Unified threat management (UTM) capabilities.
- Leverage public Internet connectivity.
- Teleworker gateway services.

TEAM 4 MERAKI MX HA INSTALLATION OVERVIEW

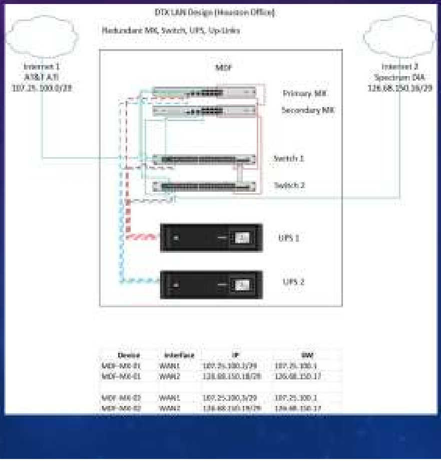
Installation DTX Corporate site



Device	Interface	IP	GW
DC-MX-CAB2-01	WAN1	172.16.10.3/24	172.16.10.1
DC-MX-CAB2-02	WAN1	172.16.10.4/24	172.16.101

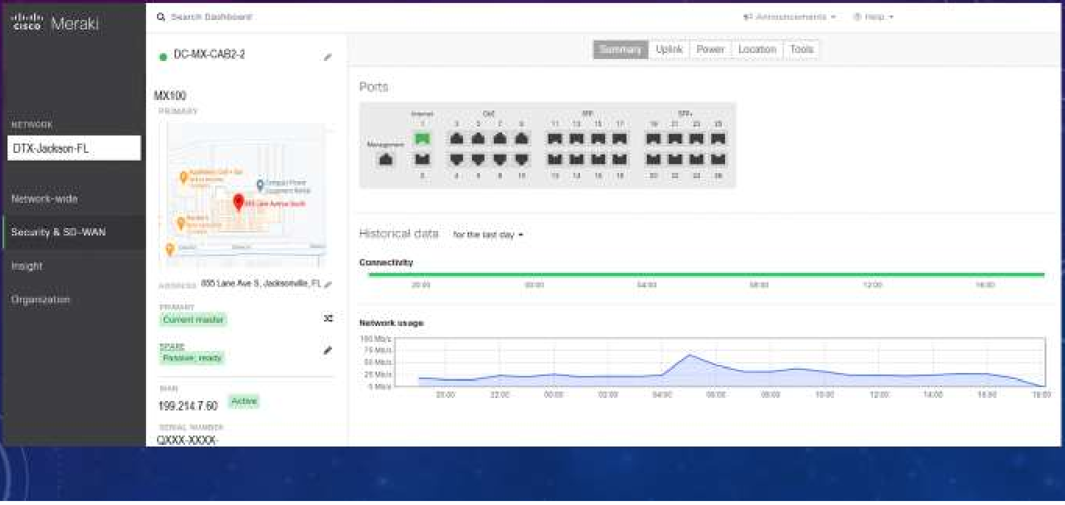
VLAN	Virtual IP
20	172.16.10.2

Installation DTX Texas site



Device	Interface	IP	GW
MDF-MX-01	WAN1	107.25.100.2/29	107.25.100.1
MDF-MX-01	WAN2	126.68.150.18/29	126.68.150.17
MDF-MX-02	WAN1	107.25.100.3/29	107.25.100.1
MDF-MX-02	WAN2	126.68.150.19/29	126.68.150.17

MERAKI CLOUD DASHBOARD DTX FLORIDA SITE



DC-MX-CAB2-2

MX100
PRIMARY

ADDRESS 835 Lane Ave S, Jacksonville, FL

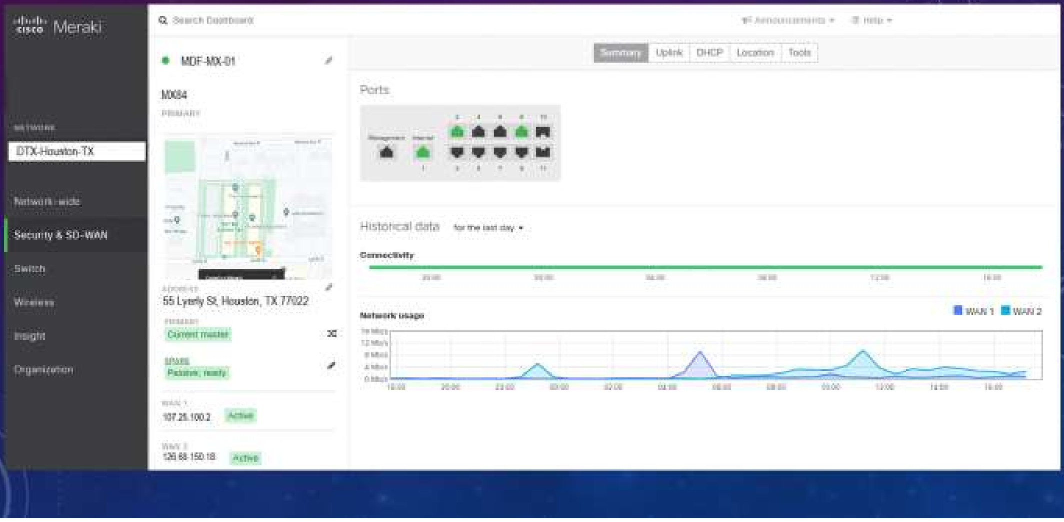
PRIMARY
Current master

SPARE
Passive; ready

WAN
199.214.7.60 Active

SERIAL NUMBER
QXXX-XXXX-

MERAKI CLOUD DASHBOARD TEXAS SITE



MDF-MX-01

MX84
PRIMARY

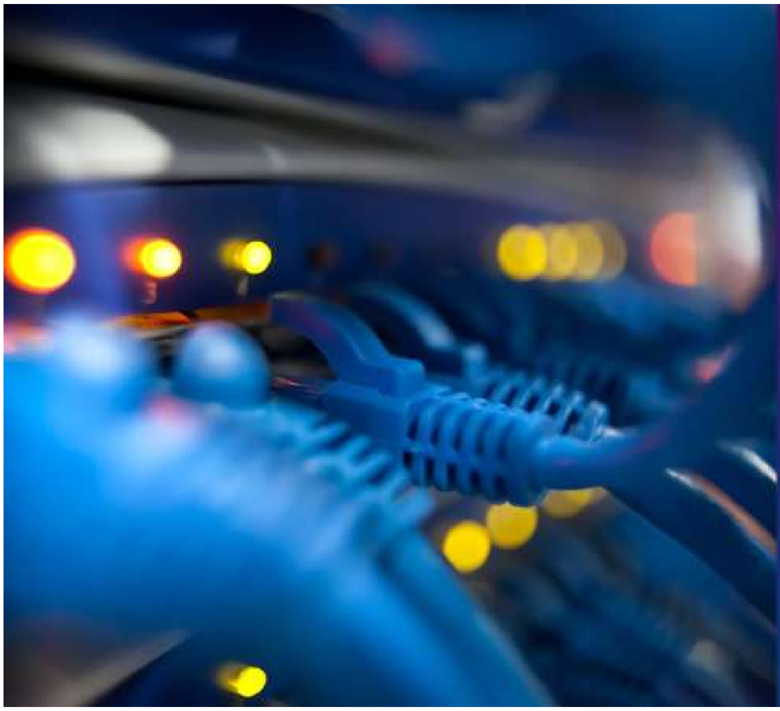
ADDRESS
55 Lyerly St, Houston, TX 77022

PRIMARY
Current master

SPARE
Passive; ready

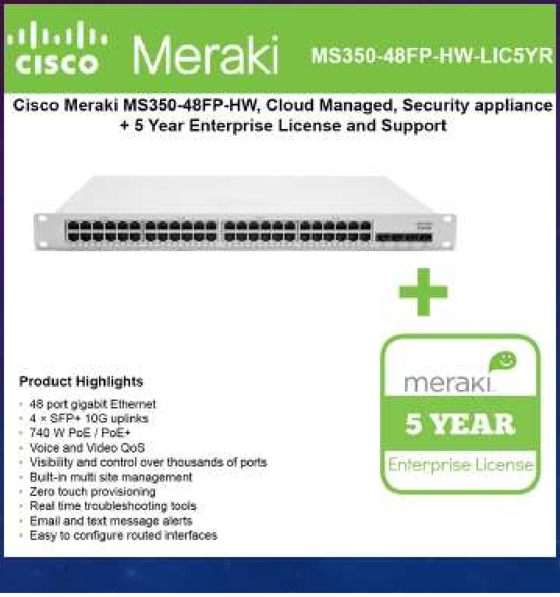
WAN 1
107.25.100.2 Active

WAN 2
126.68.150.18 Active



LAN SOLUTION AND INFRASTRUCTURE

MERAKI MS350-48FP



MS350-48FP-HW-LIC5YR

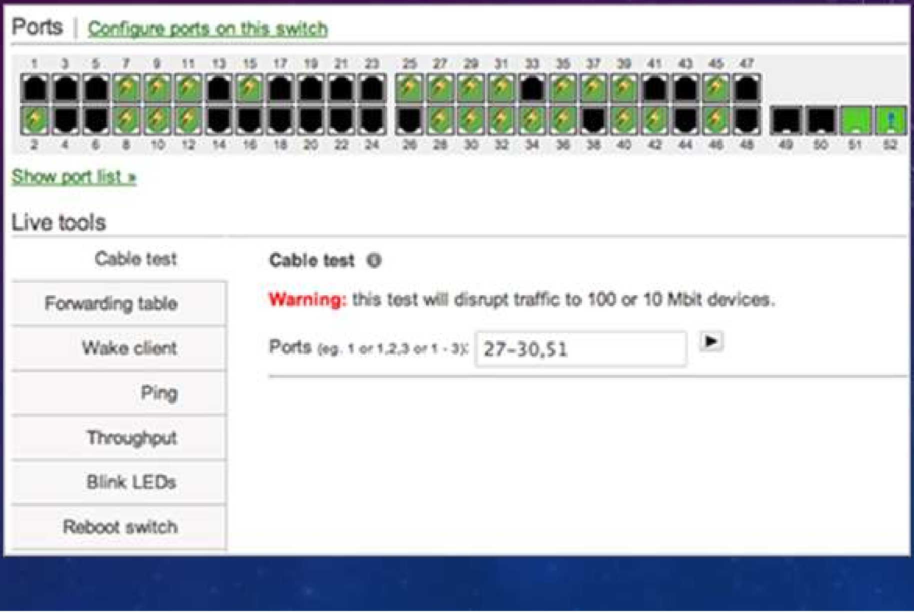
Cisco Meraki MS350-48FP-HW, Cloud Managed, Security appliance + 5 Year Enterprise License and Support

Product Highlights

- 48 port gigabit Ethernet
- 4 × SFP+ 10G uplinks
- 740 W PoE / PoE+
- Voice and Video QoS
- Visibility and control over thousands of ports
- Built-in multi site management
- Zero touch provisioning
- Real time troubleshooting tools
- Email and text message alerts
- Easy to configure routed interfaces

HIGH AVAILABILITY

MERAKI DASHBOARD INTEGRATION



Ports | Configure ports on this switch

Show port list »

Live tools

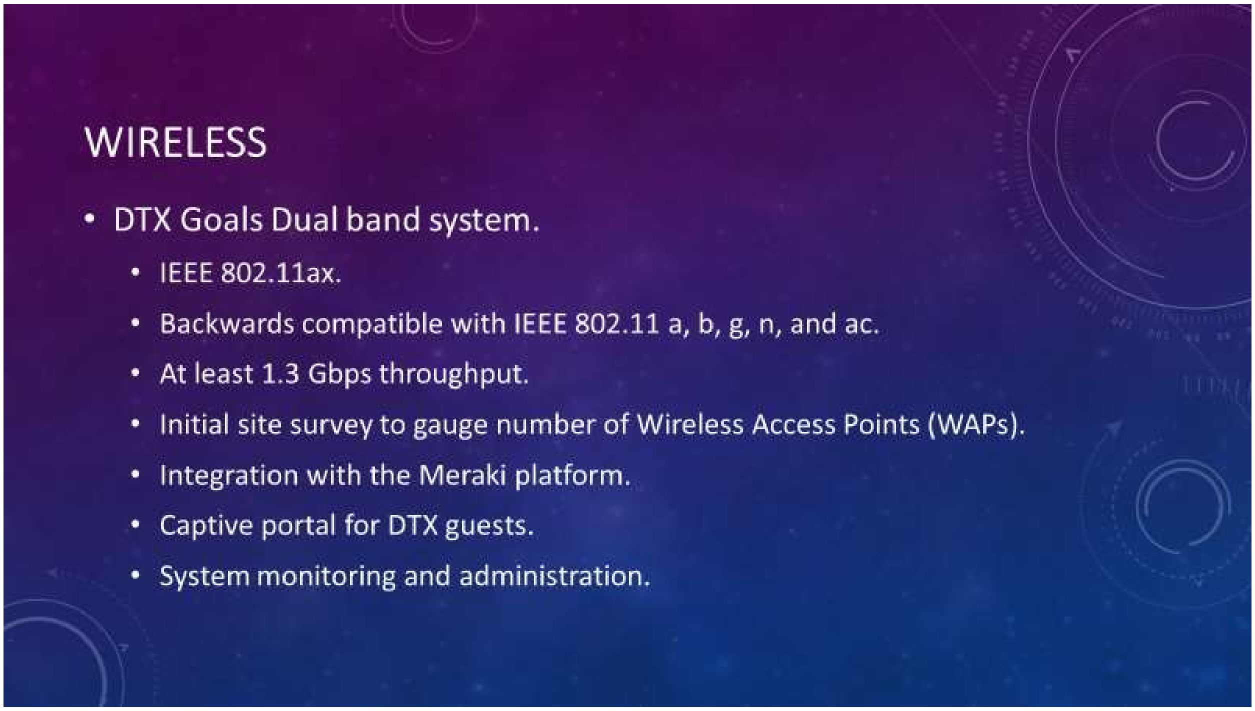
Cable test

Cable test

Warning: this test will disrupt traffic to 100 or 10 Mbit devices.

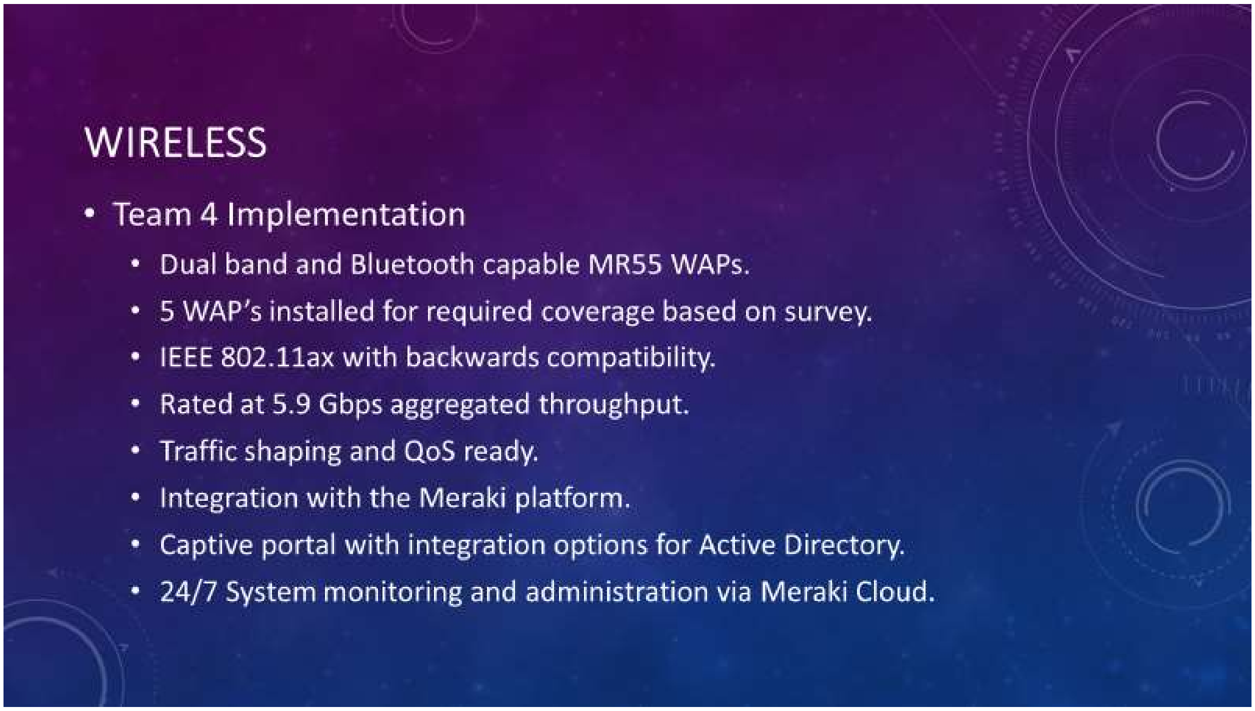
Ports (eg. 1 or 1,2,3 or 1 - 3): 27-30,51 ▶

WIRELESS SOLUTION AND INFRASTRUCTURE



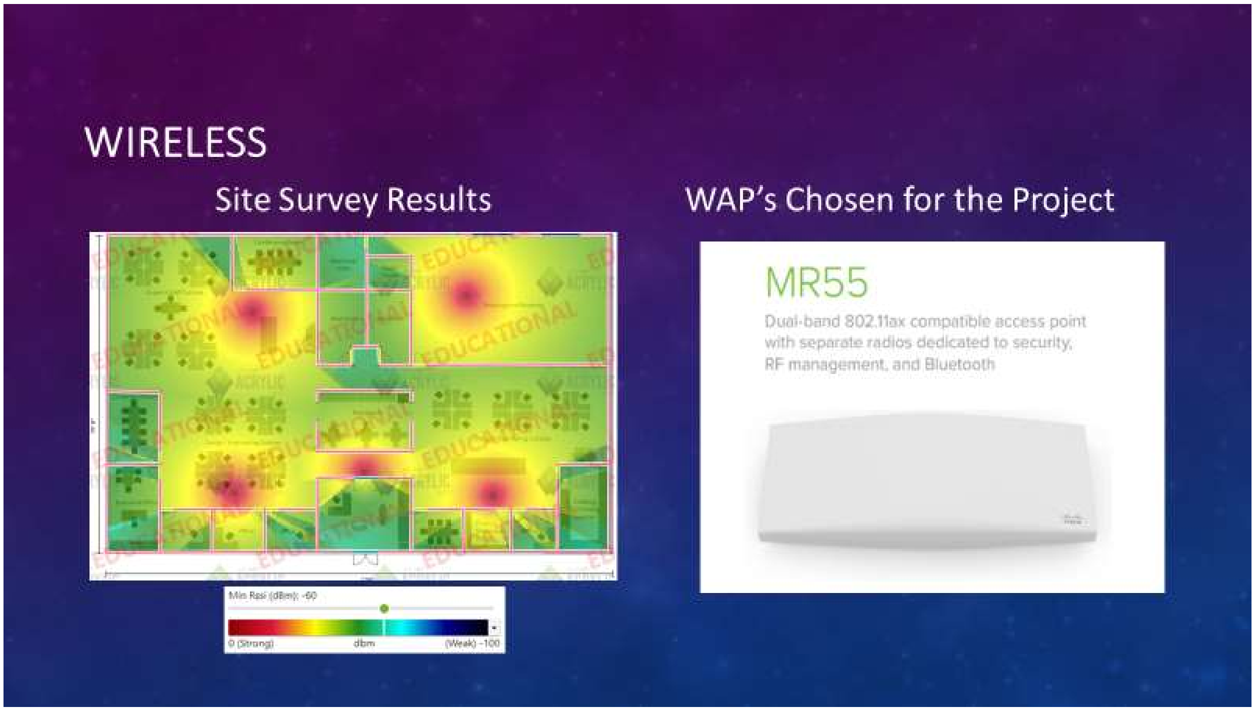
WIRELESS

- DTX Goals Dual band system.
  - IEEE 802.11ax.
  - Backwards compatible with IEEE 802.11 a, b, g, n, and ac.
  - At least 1.3 Gbps throughput.
  - Initial site survey to gauge number of Wireless Access Points (WAPs).
  - Integration with the Meraki platform.
  - Captive portal for DTX guests.
  - System monitoring and administration.



WIRELESS

- Team 4 Implementation
  - Dual band and Bluetooth capable MR55 WAPs.
  - 5 WAP’s installed for required coverage based on survey.
  - IEEE 802.11ax with backwards compatibility.
  - Rated at 5.9 Gbps aggregated throughput.
  - Traffic shaping and QoS ready.
  - Integration with the Meraki platform.
  - Captive portal with integration options for Active Directory.
  - 24/7 System monitoring and administration via Meraki Cloud.



WIRELESS

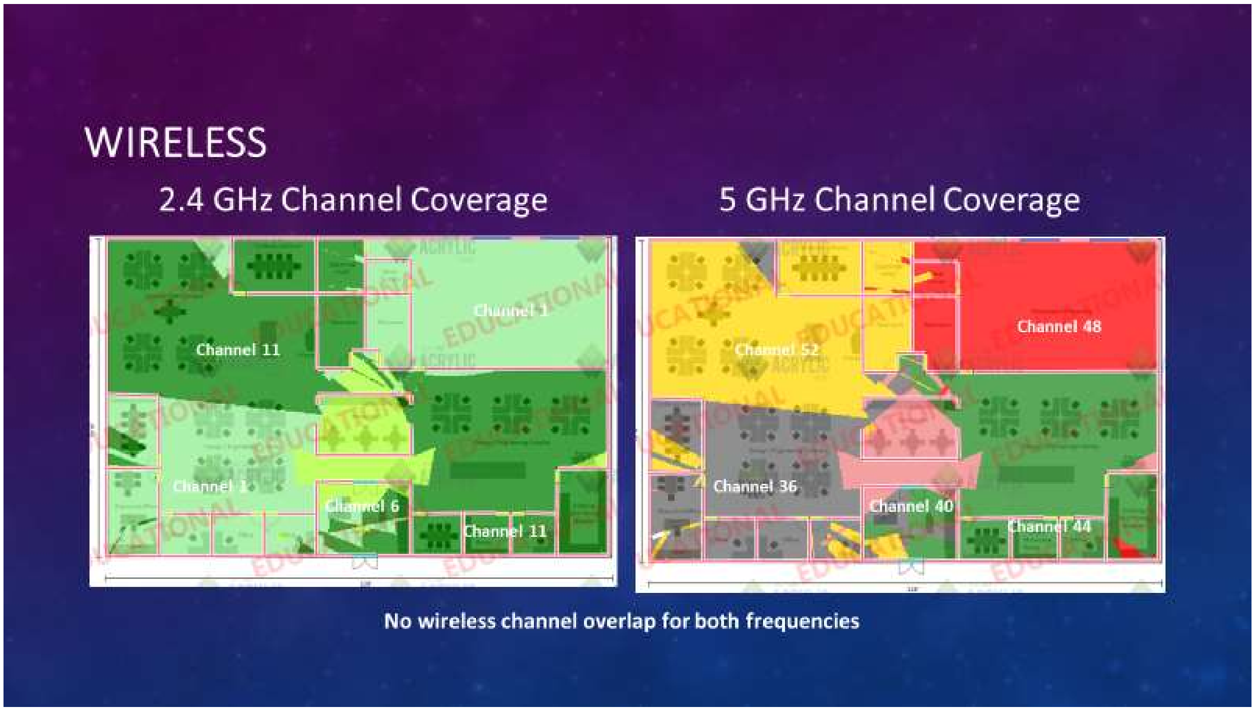
Site Survey Results

WAP's Chosen for the Project

MR55

Dual-band 802.11ax compatible access point with separate radios dedicated to security, RF management, and Bluetooth

Min Rssi (dBm): -60
0 (Strong)
dbm
(Weak) -100



WIRELESS

2.4 GHz Channel Coverage

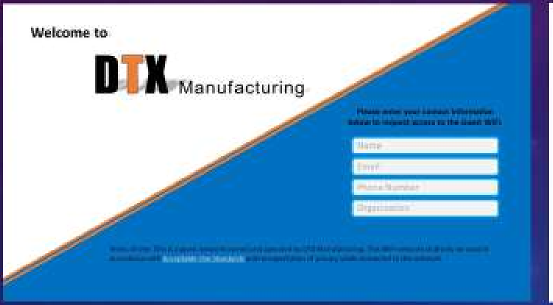
5 GHz Channel Coverage

Channel 1
Channel 11
Channel 1
Channel 6
Channel 11
Channel 48
Channel 52
Channel 36
Channel 40
Channel 44

No wireless channel overlap for both frequencies

WIRELESS

Captive Portal Landing Page



Welcome to

DTX Manufacturing

Please enter your contact information below to request access to the Guest WiFi

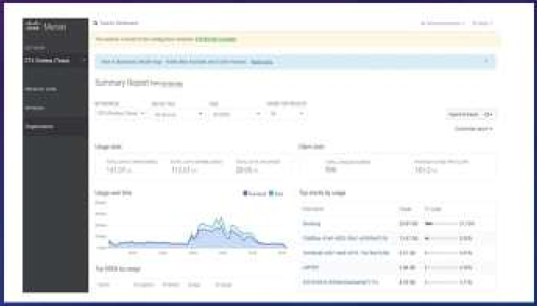
Name

Email

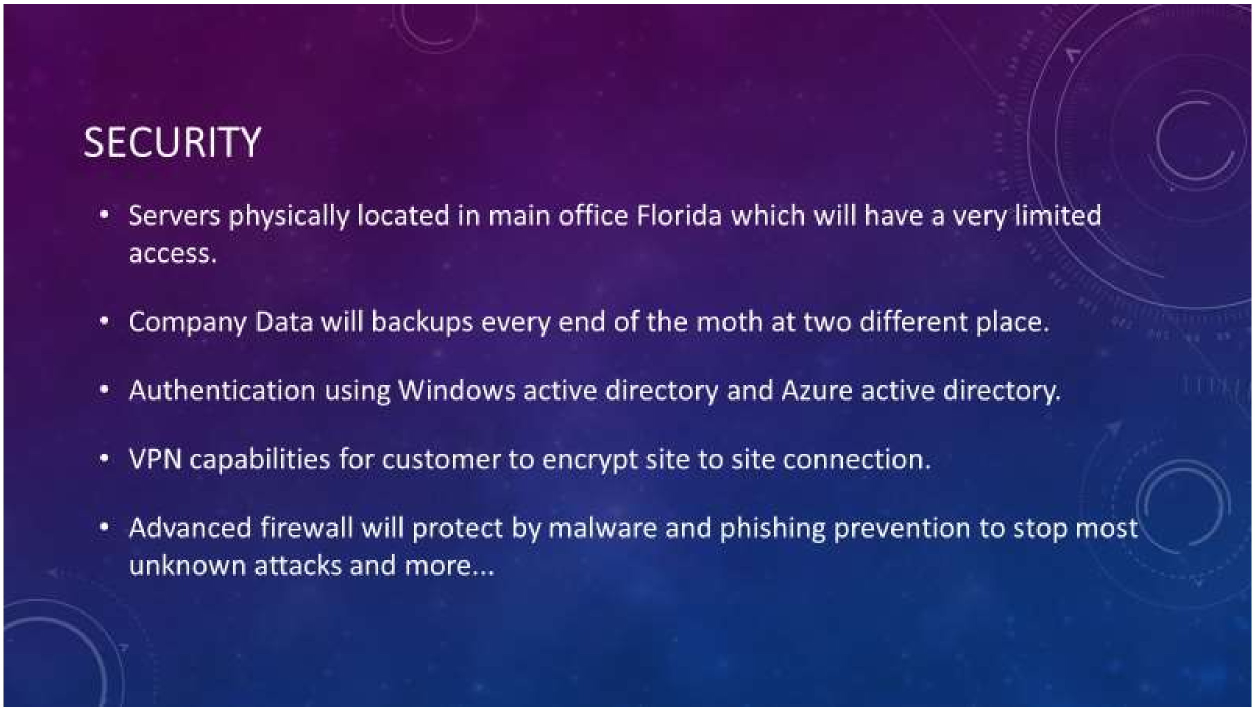
Phone Number

Organization

Meraki Wireless Dashboard

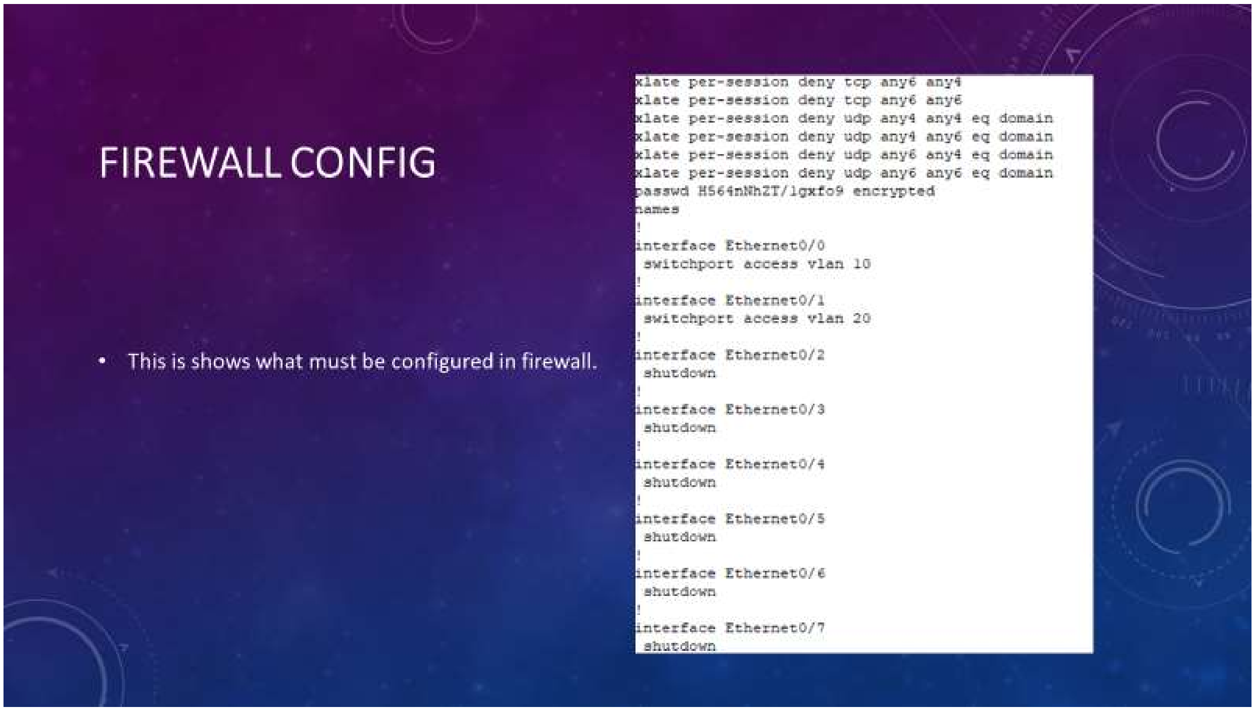


NETWORK SECURITY SOLUTION



SECURITY

- Servers physically located in main office Florida which will have a very limited access.
- Company Data will backups every end of the moth at two different place.
- Authentication using Windows active directory and Azure active directory.
- VPN capabilities for customer to encrypt site to site connection.
- Advanced firewall will protect by malware and phishing prevention to stop most unknown attacks and more...

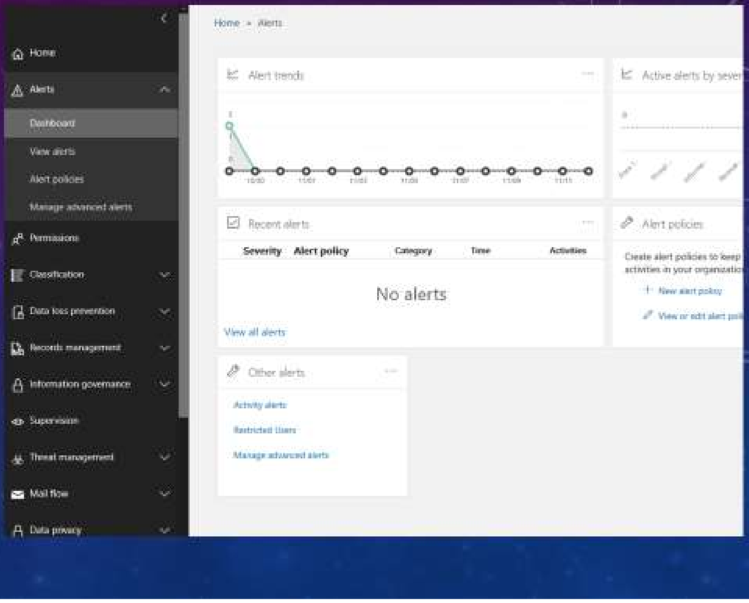


FIREWALL CONFIG

- This is shows what must be configured in firewall.

```
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
passwd H564nNhZT/lgxfo9 encrypted
names
!
interface Ethernet0/0
 switchport access vlan 10
!
interface Ethernet0/1
 switchport access vlan 20
!
interface Ethernet0/2
 shutdown
!
interface Ethernet0/3
 shutdown
!
interface Ethernet0/4
 shutdown
!
interface Ethernet0/5
 shutdown
!
interface Ethernet0/6
 shutdown
!
interface Ethernet0/7
 shutdown
```

SECURITY AND COMPLIANCE

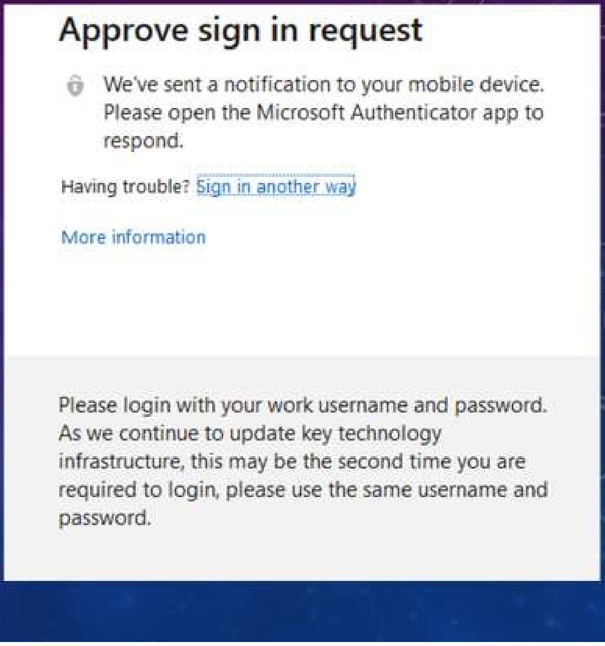


Severity Alert policy Category Time Activities

No alerts

Create alert policies to keep activities in your organizatio

MULTIFACTOR AUTHENTICATION



Approve sign in request

We've sent a notification to your mobile device. Please open the Microsoft Authenticator app to respond.

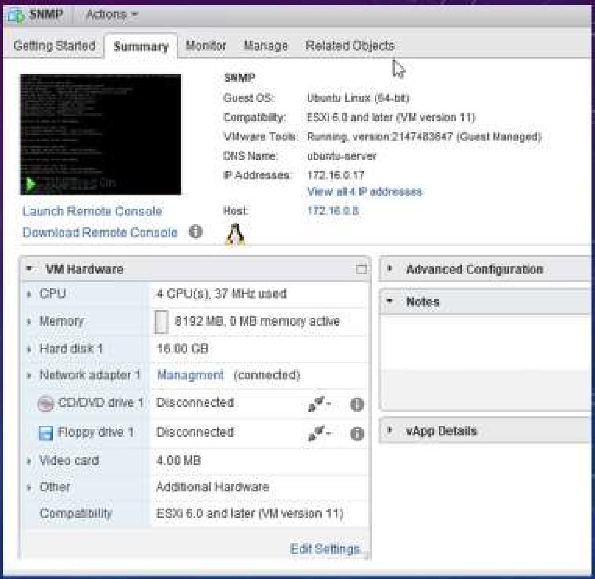
Having trouble? Sign in another way

More information

Please login with your work username and password. As we continue to update key technology infrastructure, this may be the second time you are required to login, please use the same username and password.

SNMP

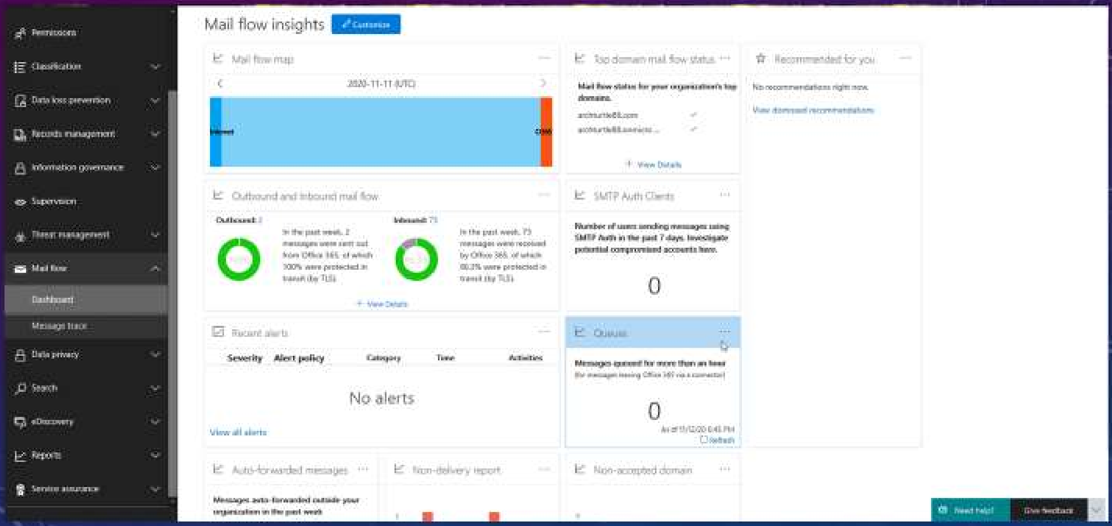
- Summary of SNMP VM server.



SNMP
Guest OS: Ubuntu Linux (64-bit)
Compatibility: ESXi 6.0 and later (VM version 11)
VMware Tools: Running, version:2147483647 (Guest Managed)
DNS Name: ubuntu-server
IP Addresses: 172.16.0.17
View all 4 IP addresses
Host: 172.16.0.8

CPU	4 CPU(s), 37 MHz used
Memory	8192 MB, 0 MB memory active
Hard disk 1	16.00 GB
Network adapter 1	Managment (connected)
CD/DVD drive 1	Disconnected
Floppy drive 1	Disconnected
Video card	4.00 MB
Other	Additional Hardware
Compatibility	ESXi 6.0 and later (VM version 11)

EMAIL SECURITY



Mail flow insights

Mail flow map
2020-11-11 (UTC)

Outbound and inbound mail flow
Outbound: 2
In the past week, 2 messages were sent out from Office 365, of which 100% were protected in transit (by TLS).
Inbound: 73
In the past week, 73 messages were received by Office 365, of which 80.2% were protected in transit (by TLS).

Recent alerts

Severity	Alert policy	Category	Time	Activities

No alerts

Top domain mail flow status
Mail flow status for your organization's top domains.
archturtle88.com ✓
archturtle88.onmicro... ✓

SMTP Auth Clients
Number of users sending messages using SMTP Auth in the past 7 days. Investigate potential compromised accounts here.
0

Queues
Messages queued for more than an hour (for messages leaving Office 365 via a connector)
0
As of 11/12/20 6:45 PM
Refresh

Recommended for you
No recommendations right now.
View dismissed recommendations

Auto-forwarded messages
Messages auto-forwarded outside your organization in the past week

Non-delivery report

Non-accepted domain

FUTURE DIRECTIONS

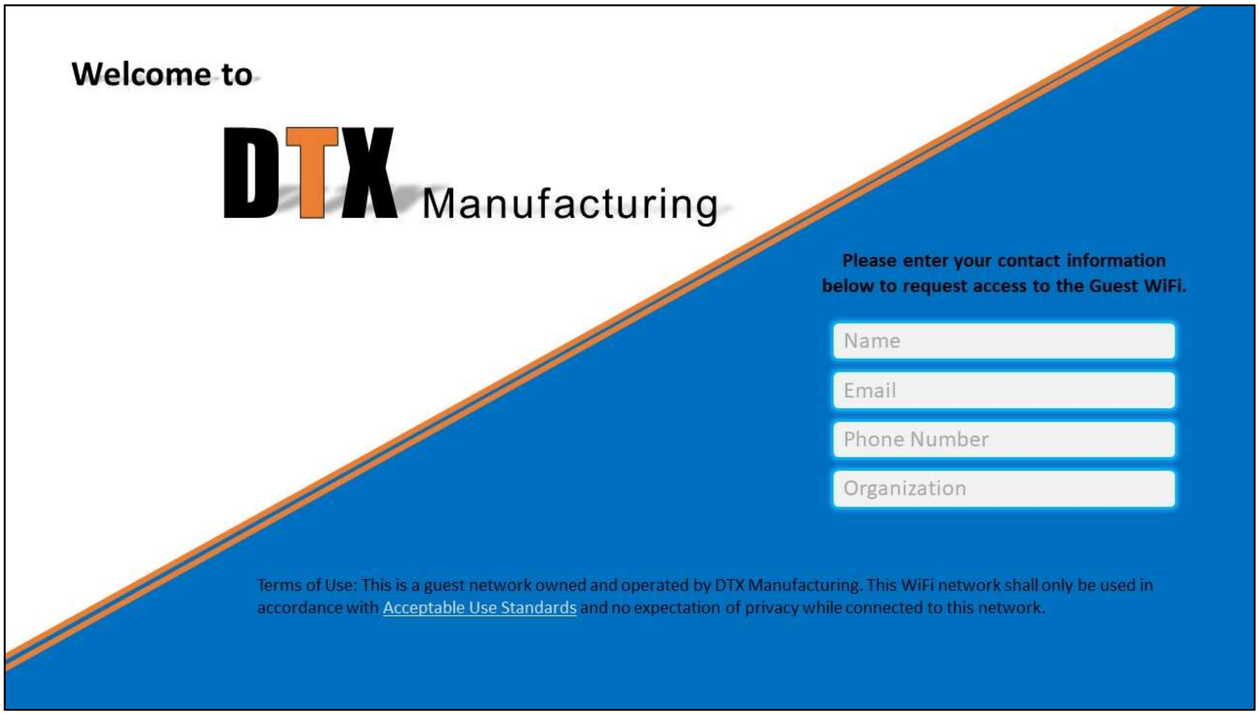
FUTURE DIRECTIONS

- This project scope was to provide a full network solution for a remote site, but there are several enhancements that can be considered for the future such as:
  - Physical building security.
  - Security cameras.
  - API integrations with Meraki.
  - Enhanced analytics for business decisions.

QUESTIONS?

15. Appendix C: Figures and Illustrations

Figure 1 - Captive Portal



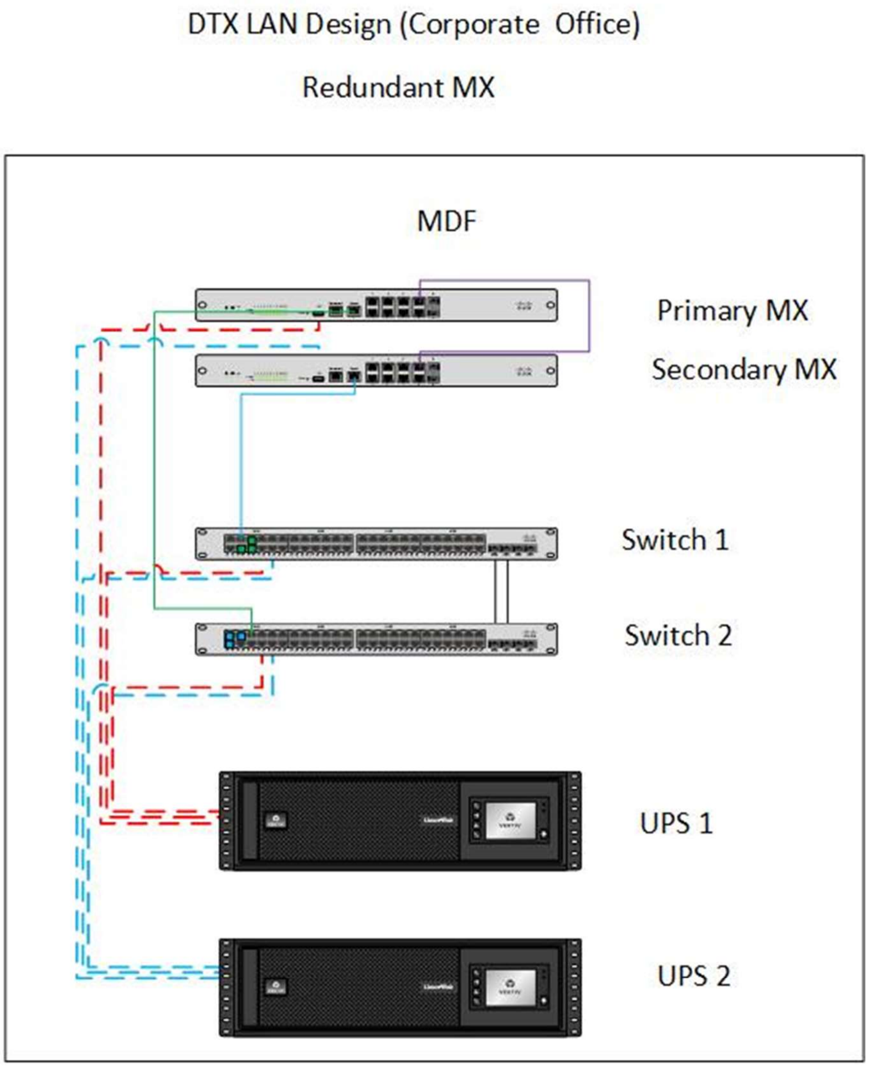
Welcome to

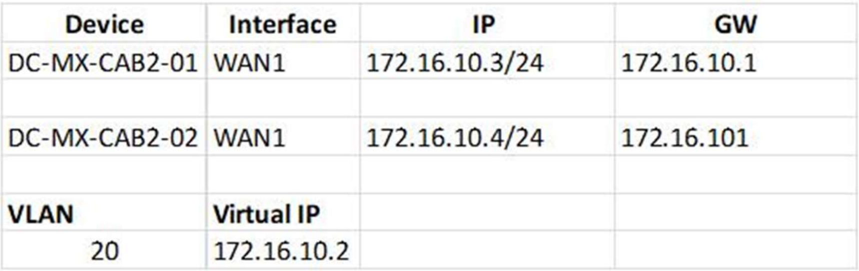
DTX Manufacturing

Please enter your contact information below to request access to the Guest WiFi.

Terms of Use: This is a guest network owned and operated by DTX Manufacturing. This WiFi network shall only be used in accordance with Acceptable Use Standards and no expectation of privacy while connected to this network.

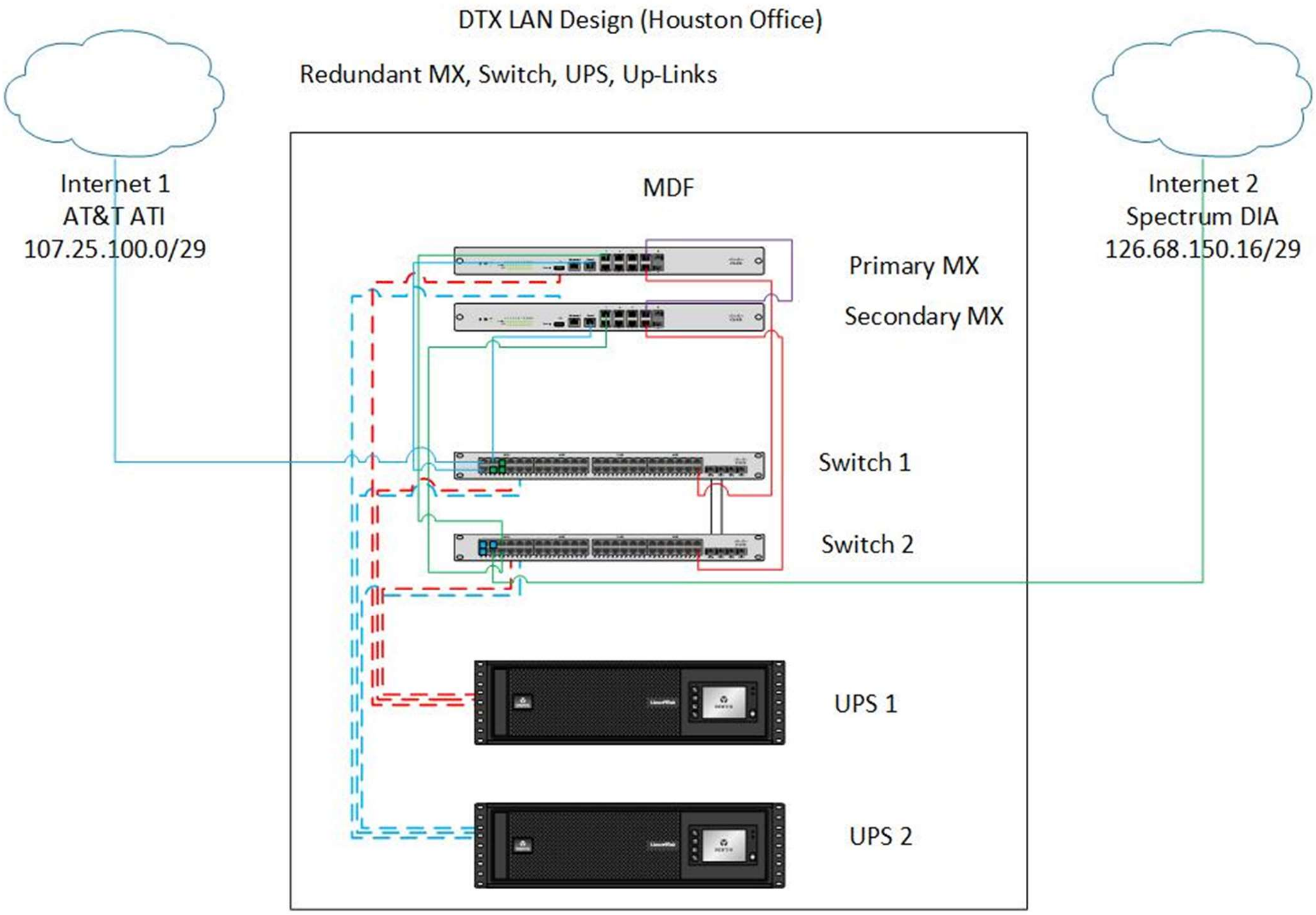
Figure 2 – DTX Redundant MX Configuration (Florida Office)

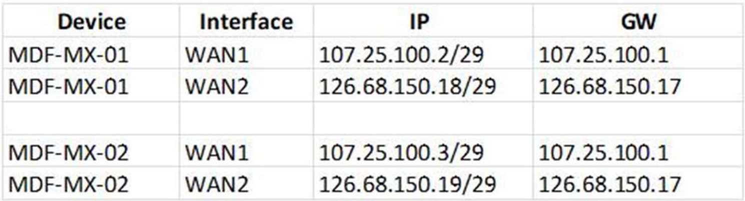




Device	Interface	IP	GW
DC-MX-CAB2-01	WAN1	172.16.10.3/24	172.16.10.1
DC-MX-CAB2-02	WAN1	172.16.10.4/24	172.16.101
VLAN	**Virtual IP**		
20	172.16.10.2		

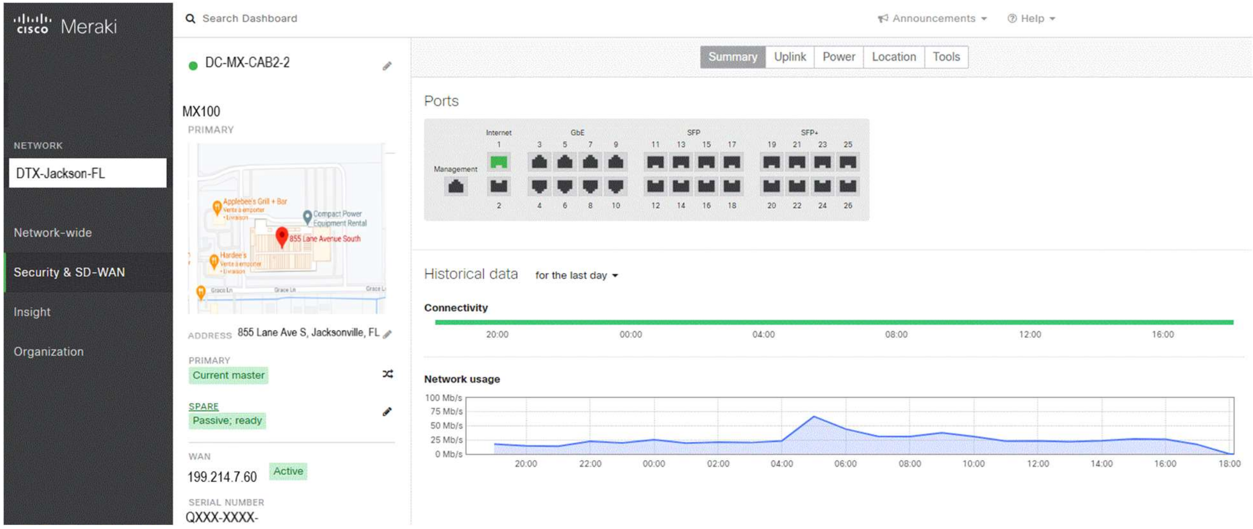
Figure 3 – DTX Redundant MX Configuration (Texas Office)





Device	Interface	IP	GW
MDF-MX-01	WAN1	107.25.100.2/29	107.25.100.1
MDF-MX-01	WAN2	126.68.150.18/29	126.68.150.17
MDF-MX-02	WAN1	107.25.100.3/29	107.25.100.1
MDF-MX-02	WAN2	126.68.150.19/29	126.68.150.17

Figure 4 – Meraki Dashboard (Florida Office)



DC-MX-CAB2-2

MX100
PRIMARY

ADDRESS 855 Lane Ave S, Jacksonville, FL

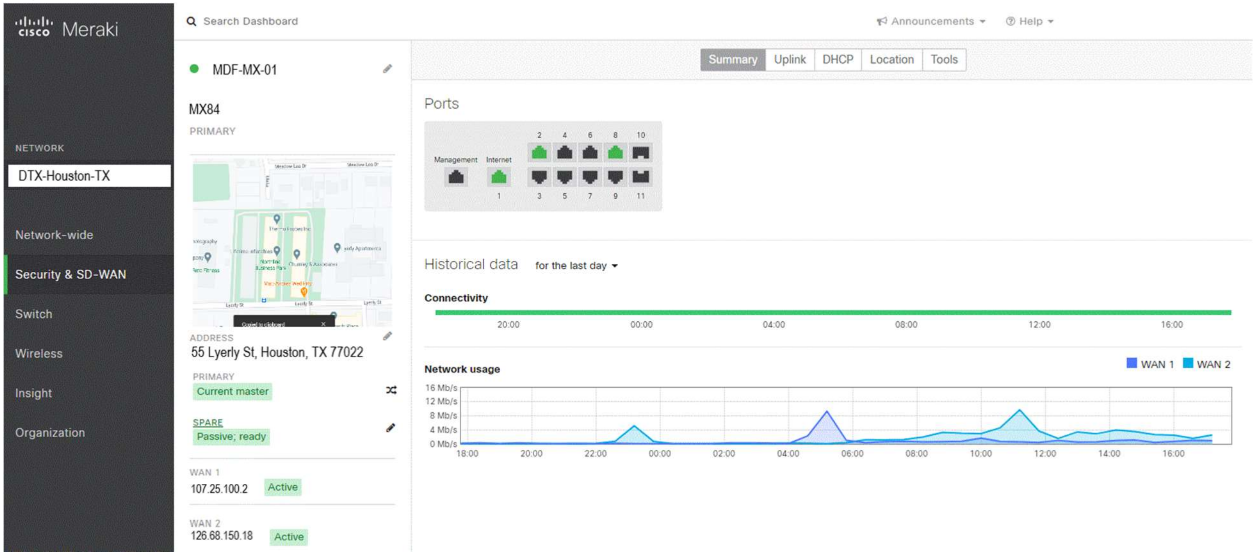
PRIMARY
Current master

SPARE
Passive; ready

WAN
199.214.7.60 Active

SERIAL NUMBER
QXXX-XXXX-

Figure 5 – Meraki Dashboard (Texas Office)



MDF-MX-01

MX84
PRIMARY

ADDRESS
55 Lyerly St, Houston, TX 77022

PRIMARY
Current master

SPARE
Passive; ready

WAN 1
107.25.100.2 Active

WAN 2
126.68.150.18 Active

Figure 6 – Wireless Site Survey Heat Map

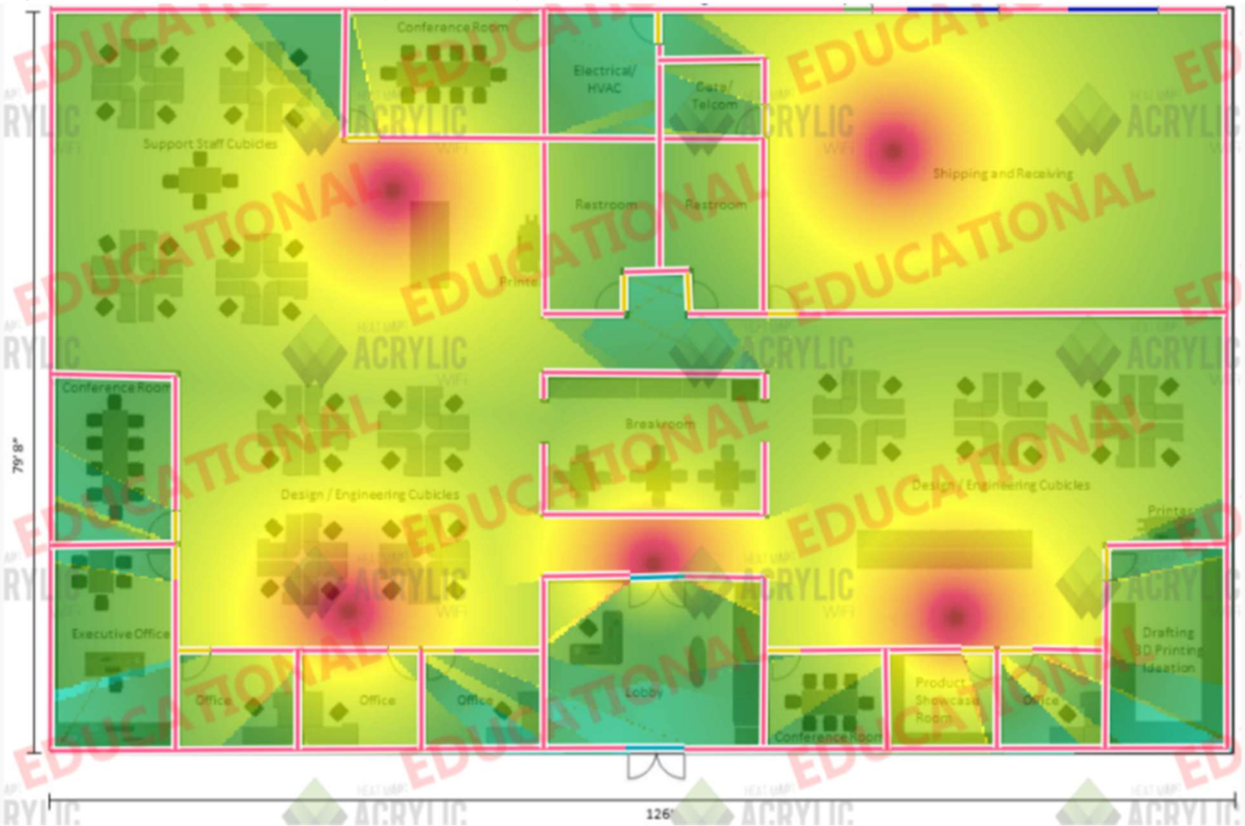
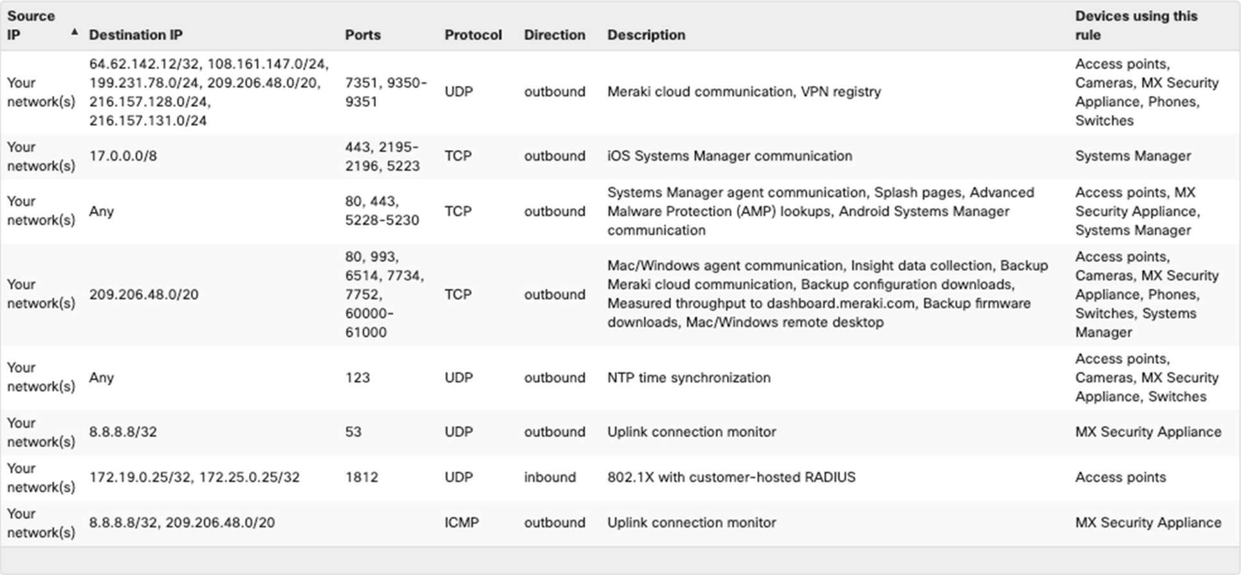
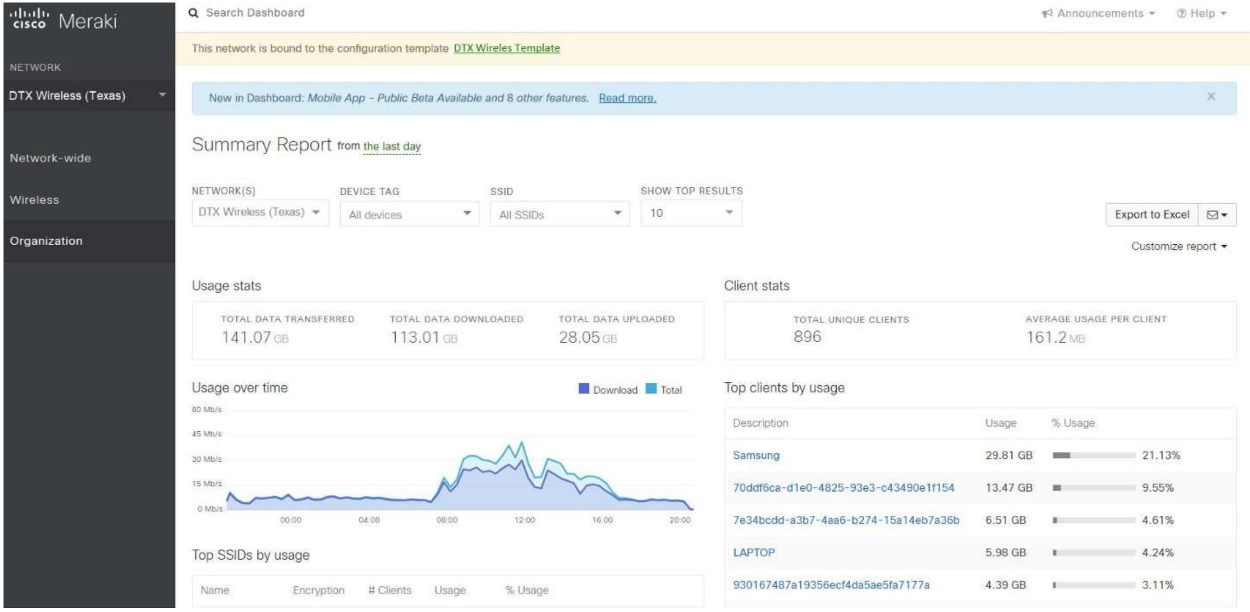


Figure 7 – Meraki Firewall



Source IP ▲	Destination IP	Ports	Protocol	Direction	Description	Devices using this rule
Your network(s)	64.62.142.12/32, 108.161.147.0/24, 199.231.78.0/24, 209.206.48.0/20, 216.157.128.0/24, 216.157.131.0/24	7351, 9350-9351	UDP	outbound	Meraki cloud communication, VPN registry	Access points, Cameras, MX Security Appliance, Phones, Switches
Your network(s)	17.0.0.0/8	443, 2195-2196, 5223	TCP	outbound	iOS Systems Manager communication	Systems Manager
Your network(s)	Any	80, 443, 5228-5230	TCP	outbound	Systems Manager agent communication, Splash pages, Advanced Malware Protection (AMP) lookups, Android Systems Manager communication	Access points, MX Security Appliance, Systems Manager
Your network(s)	209.206.48.0/20	80, 993, 6514, 7734, 7752, 60000-61000	TCP	outbound	Mac/Windows agent communication, Insight data collection, Backup Meraki cloud communication, Backup configuration downloads, Measured throughput to dashboard.meraki.com, Backup firmware downloads, Mac/Windows remote desktop	Access points, Cameras, MX Security Appliance, Phones, Switches, Systems Manager
Your network(s)	Any	123	UDP	outbound	NTP time synchronization	Access points, Cameras, MX Security Appliance, Switches
Your network(s)	8.8.8.8/32	53	UDP	outbound	Uplink connection monitor	MX Security Appliance
Your network(s)	172.19.0.25/32, 172.25.0.25/32	1812	UDP	inbound	802.1X with customer-hosted RADIUS	Access points
Your network(s)	8.8.8.8/32, 209.206.48.0/20		ICMP	outbound	Uplink connection monitor	MX Security Appliance

Figure 8 – Meraki Wireless Dashboard



This network is bound to the configuration template DTX Wireles Template

New in Dashboard: *Mobile App - Public Beta Available and 8 other features.* Read more.

Summary Report from the last day

NETWORK(S): DTX Wireless (Texas)

DEVICE TAG: All devices

SSID: All SSIDs

SHOW TOP RESULTS: 10

Usage stats

TOTAL DATA TRANSFERRED	TOTAL DATA DOWNLOADED	TOTAL DATA UPLOADED
141.07 GB	113.01 GB	28.05 GB

Client stats

TOTAL UNIQUE CLIENTS	AVERAGE USAGE PER CLIENT
896	161.2 MB

Usage over time

Top clients by usage

Description	Usage	% Usage
Samsung	29.81 GB	21.13%
70ddf6ca-d1e0-4825-93e3-c43490e1f154	13.47 GB	9.55%
7e34bcdd-a3b7-4aa6-b274-15a14eb7a36b	6.51 GB	4.61%
LAPTOP	5.98 GB	4.24%
930167487a19356ecf4da5ae5fa7177a	4.39 GB	3.11%

Top SSIDs by usage

Name	Encryption	# Clients	Usage	% Usage

16. Appendix D: Other Deliverables/Artifacts

White Paper

Jeffery Wilson

Information Technology Capstone

ITEC495-R1WW

Professor Wayne Smith

November 1st 2020

Abstract

SD-WAN is an acronym for software-defined networking in a wide area network. The technology was designed to simplify the management and operation of a wide area network and to improve data center management and operation. The concept is not unique in that it is similar other virtualization technologies as it decouples the networking hardware from its control mechanism.

Introduction

As organizations expand, businesses require the ability to communicate between geographically separated sites. As an organization expands WAN connections become necessary, a WAN operates beyond the geographic scope of a LAN. WAN reliability and improving the efficiency can increase a business's profitability by lowering operation cost. In order to understand the technology we need to understand the history of WAN connections. This whitepaper will review the advancements and options in circuit technology and demonstrate how SDWAN take advantage of certain various characteristics to bring value to an organization communication needs.

History: Early Solutions

Choosing a WAN solution (Wide Area Network) for your organization can be a daunting task. We know what we want to accomplish. To connect a remote location back to the organization to share applications, data voice, video the demands continue to grow. Understanding and purchasing the correct technology solutions can be critical to the success of the endeavor. Communication circuits or connections have evolved over the years. It started out simply with point-to-point (PPP) leased lines often running at only 56K in the 1980s. In the

1990s faster, but more expensive T1/E1 or T3/E3 connections were available from providers, but they were still point to point circuits (11-2 Point-to-Point WANs: Layer 1 2014). This required that each remote location connection coming into a central location needed its own circuit even at the head-end. This could quickly prove to be a headache for engineers and costly for the organization. As each circuit would need is own interface or a channel service unit/data service unit (CSU/DSU), which could or could not be integrated into the router or customer-premises equipment (CPE); this term is commonly used by communication providers to refer to the equipment installed at the customer site (Networks 2020) .

History: MPLS arrival

In the early 1990s, Frame Relay service for WAN connections was introduced. What this did was remove some complexity and cost. You could still use your PPP connection, but it connected to the service provider’s cloud, you no longer needed all the individual physical links between locations. This allowed for the sharing of the media connection for the last-mile connection to remote sites. The last mile term is used telecommunications, cable television and internet industries and it is to reference the final leg of the network that deliver services to retail end-users. In addition, Frame Relay also lowered the cost of the CPE by not needing as many (CSU/DSU) devices or integrated CSU/DSU WAN interface cards to terminate a T1 or fractional T1 service and lowered the amount of circuits needed. Frame Relay was so successful that the vast majority of corporate WANs were migrated to it within five years of its introduction. In the mid-2000s Multiprotocol Label Switching (MPLS) came along which, is the successor to Frame Relay. The technical differences are not substantial between Frame Relay and MPLS. Frame Relay is a connection-oriented, circuit-switched protocol, and MPLS is a connectionless protocol the major exception was for voice over Internet Protocol (VoIP). The connectionless nature of

MPLS provided quality of service (QOS) reducing latency, which improves call quality of VOIP over the WAN links (Gottlieb &amp; Gottlieb, 2012).

History: SLA

All of these services PPP, Frame Relay, and MPLS are available with a service level agreement (SLA) with the service provider. SLAs guarantee aspects of performance and reliability for latency, packet delivery, and availability. In the event of an outage, the provider resolves the issue within a stated period or pays the requisite penalties. For a business, this is a critical agreement because downtime can cost a business in the loss of revenue. Some examples of these costs could be a service an example a corporate website. Other losses would be time, opportunities, and customers all of these items come with a heavy cost. The high reliability and quality of MPLS makes it expensive. It also takes time to get it provision, as many times the service provider will need to build out their network to support it at a specific location. The cost of the build-out is either passed on to the customer, in a one-time charge or added to the monthly recurring charge (MRC) (Gottlieb &amp; Gottlieb, 2012).

History; Internet Broadband

Lower cost higher speed internet connections or broadband came along in the early 1990s in the form of ADSL and cable modem replacing T1-based access. At first, many large enterprises did not deploy broadband technology at their central locations instead they were deployed at branch sites for either internet connectivity or for backup IPsec virtual private network or VPN connection in the event of the failure of the primary MPLS connection. ADSL and cable modems broadband services are best effort and do not provide an SLA for latency or jitter also upstream bandwidth is limited and it is shared media and bandwidth received cannot guarantee. IPsec VPNs introduced in the mid-1990s the technology made site-to-site secure connections over the internet possible. Latter development accelerated with the introduction of SSL VPN. The VPN service made it possible for workers to access the organization's network resources from anywhere from a broadband connection. A downside to VPN over the internet is you cannot get end-to end SLA over the public internet. Despite the ability of a price advantage of broadband using a VPN the unpredictable performance of broadband connection VPN connections were relegated as failover solution in an active and passive configuration, remote worker or partner connectivity solutions.

History: Dedicated Internet Access

Service providers have worked to improve on the broadband shortcomings and have developed Dedicated Internet Access (DIA) circuits. DIA circuits predominately use Metro Ethernet Fiber from companies like Spectrum, Comcast, AT&T, Windstream, CenturyLink, Cincinnati Bell, Nitel, and others. DIA comes with the benefits of guarantees missing in broadband products. Some of the guarantees included circuit will receive the bandwidth you purchased, 100% of the time. Synchronous upload and download speeds meaning that both your download and upload speed/bandwidth are always to be that same and guaranteed, example a 100Mps second DIA upload speed is 100Mpbs same as the download. This differs from broadband products that when developed the bulk of traffic originated on the internet and uploading was less of a concern. DIA provides better throughput in the Internet Service Provider ISP's high-capacity under-subscribed backbone network. A typical DIA SLA will guarantee network uptime, latency, packet loss, and jitter. These guarantees equal better response time, ISP's typically provide a 4-hour guaranteed response time verse 24-hour for broadband type of circuits. If your company has Dedicated Internet Access and your ISP fails to meet its SLA, they will give you a refund (Smith &amp; Smith, 2017).

SDWAN

Now that we have an understanding of WAN links we can dive into software-defined wide-area networks or SDWAN. SDWAN uses software to control the connectivity, management, and services between data centers and remote branches or cloud instances. One of the chief features SD-WAN's is the ability to manage multiple connections from MPLS to broadband to DIA. Another important piece is the ability to segment, partition and secure the traffic traversing the WAN. The driving principle of SDWAN is to simplify the way organizations turn up new links to remote offices and to better manage the way those links are utilized for data, voice or video while also potentially saving money in the process. SD-WAN can exploit two or more WAN links in an active-active manner. This means that data can be utilizing sent and received on both links at the same time. This is in contrast from traditional enterprise WAN designs that normally place secondary links in a passive mode until the primary link fully drops because of failure (Cooney, 2019). Other benefits SDWAN continuously monitors all WAN links in real time to determine the optimal data flow path, data can be prioritized and also disturbed across WAN links so at any given moment it is traveling the fastest path. SDWAN also provides fewer network outages compared to traditional active-passive setup. Traditional redundancy and failover mechanisms cannot properly handle degraded circuits, a primary link may be significantly degraded, while not technically being down, or a situation could form where constantly flapping between active and passive links. Both of these situation results in a poor end user experience. SDWAN also allow for mission-critical data flows that can be easily identified, allowing administrators to give preferential treatment over the

WAN links. This important now that many of our applications are web based. Prioritizing traffic to the company's web-based business app over general web browsing improves users experience for internal application. Ease of deployment having an active-active architecture organizations no longer need to wait or pay for expensive WAN connections such as MPLS, instead two or more broadband or DIA circuits can be used just as effectively. SD-WAN can squeeze more performance from these inferior technologies. Many instances to where performance and reliability differences are negligible over the more expensive circuit solution (SD-WAN Solution - Bringing SD-WAN benefits to user experience 2019).

Conclusion

With the many communication circuit options available to organizations, it is clear to see the value in SDWAN technologies. The SDWAN active- active status of communications links over active-passive provides for seamless failover caused by circuit outages. The ability to route and prioritize traffic to match circuit pros and cons brings value in low cost DIA circuits can be used for large transfers saving valueable bandwidth on MPLS for VoIP and other loss sensitive applications. The inherit flexibility of SDWAN gives organizations the options of using lower cost links over higher cost point-to-point links that were required in the past while also improving the end user experience. Using low cost links also cut the time needed to bring a remote location on-line as point-to point requires a longer period from the service provider to complete in comparison to a DIA or broadband connection.

References

Networks, C. (n.d.). A History of SD-WAN. Retrieved October 18, 2020, from https://www.catonetworks.com/sd-wan/a-history-of-sd-wan

11-2 Point-to-Point WANs: Layer 1. (2014, January 06). Retrieved October 18, 2020, from https://www.freeccnastudyguide.com/study-guides/ccna/ch11/11-2-point-point-wans-layer-1/

Gottlieb, N., &amp; Gottlieb, A. (2012, April 06). A Brief History of the Enterprise WAN. Retrieved October 18, 2020, from https://www.networkworld.com/article/2222089/a-brief-history-of-the-enterprise-wan.html

Cooney, M. (2019, October 09). SD-WAN - What it means for enterprise networking, security, cloud computing. Retrieved October 18, 2020, from https://www.networkworld.com/article/3031279/sd-wan-what-it-is-and-why-you-ll-use-it-one-day.html

Smith, P., &amp; Smith, M. (2017, September 07). What is Dedicated Internet Access? Retrieved October 18, 2020, from https://www.networkworld.com/article/3221478/what-is-dedicated-internet-access.html

SD-WAN Solution - Bringing SD-WAN benefits to user experience. (2019, March 25). Retrieved October 18, 2020, from https://www.cisco.com/c/en/us/solutions/enterprise-networks/sd-wan/sd-wan-benefits-user-experience.html

Current Wireless Standards and the Shift to 802.11ax

David Dollan

ITEC495-R1WW (F20)

Professor Wayne Smith

October 31, 2020

Abstract

Wireless connectivity for the organization has been around for a few decades and standards were created to ensure interconnectivity between devices. The two most recent standards, IEEE 802.11ac and IEEE 802.11ax are now at the forefront of options available for upgrading wireless infrastructure. The 802.11ac standard was a significant upgrade over 802.11n which added an increased amount of throughput. Now, the 802.11ax standard expands the features of 802.11ac by adding methods for transmission sharing which allows for a greater number of devices in a densely populated network. Organizations that can upgrade to wireless infrastructure that uses the new 802.11ax standard would be advised to do so to allow for future-proofing of the organization and to cope with the potential for interference from nearby wireless networks.

Current Wireless Standards and the Shift to 802.11ax

Introduction

Wireless technologies have made significant advances over the last several decades and have given mankind countless benefits that range from lifesaving equipment to a proliferation of mobile computing devices. The latter is a well-documented journey that culminates into the standards that we know today created by the Institute of Electrical and Electronics Engineers (IEEE) and the WiFi Alliance. Wireless technologies would not be where it is today without the progression of these standards and the ever-changing requirements of new technology. For organizations using wireless connectivity, the problem then becomes a matter of when to upgrade wireless hardware to take advantage of features within the new standard. This white paper will focus on this problem in relation to the IEEE 802.11ac and the new IEEE 802.11ax standards and will provide technical guidance to organizations that are thinking about upgrading or installing new wireless hardware.

IEEE 802.11ac and its Current Feature Set

Each jump that has taken place between the different 802.11 standards has seen several benefits over previous versions and the deployment of 802.11ac was no exception. Incorporated into the IEEE standards in 2013, 802.11ac boasted significant features that now prove to be invaluable to millions of WiFi users (IEEE, 2020). The first of these features discussed is data throughput, followed by network capacity, and lastly power efficiency.

The amount of data that can be transmitted or received over a medium is always reliant on the hardware performing the communication and the medium that communication is attached to. In the case of a wireless medium for data transmissions, the traditional definition used for how much data (or payload) can transverse over a medium at a given speed is known as throughput (Ciampa, 2013). For the 802.11ac standard operating on the 5 GHz frequency band, throughput is specified for at least 1 Gbps (Perahia & Stacey, 2013). While the original 802.11ac standard does not include usage on the 2.4 GHz frequency band, backward compatibility is possible which can add to the overall throughput upwards of 1.4 Gbps (Perahia & Stacey, 2013). Much of the increased speed is due to the various forms of Multiple Input Multiple Output (MIMO) which is the utilization of several radio transmitters and receivers to accept more than one signal from a device at a time (Ciampa, 2013). This method of sending and receiving wireless transmission is nothing new to the IEEE standards as MIMO was a major part of 802.11n. However, 802.11ac brought this method one step further with Multiple-User MIMO (MU-MIMO). The new strategy adds the ability for multiple devices capable of multiple radio transmissions to be able to access wireless access point radio streams which increases the overall speed to 1 Gbps per device (Perahia & Stacey, 2013). This is a 40% increase in theoretical speeds from 802.11n (Ciampa, 2013). With devices that cannot transmit multiple radio transmissions at once, 802.11ac uses methods within MU-MIMO to provide backward compatibility for older devices with less wireless provisions (Perahia & Stacey, 2013). It also allows the wireless transmissions from these devices to prevent a bottleneck in throughput to the rest of the wireless network due to the limited capabilities of one device (Perahia & Stacey, 2013). The 802.11ac standard has seen several improvements that allow a wide variety of devices to connect wirelessly without causing a loss in throughput and the ability of faster devices to co-exist with older devices within the same wireless network. This has allowed for better performance and an increase in the consumption of applications that depend on wireless transmissions.

IEEE 802.11ax

At the time of this writing in 2020, it is estimated that there will be approximately 31 billion wireless devices that need network connectivity (Allison, 2019). Five years later in 2025, those figures will double which will cause serious issues for wireless networks trying to provide access for an increased number of wireless clients (Allison, 2019). Wireless networks do have limits in the amount of usable connectivity that can be provided. For example, in a large hotel where all rooms are booked, guests may have difficulty accessing the wireless network due to the large number of devices that are attempting to obtain a usable connection. What makes the situation more difficult is that the number of wireless devices that a single person carries has also increased so it would be a common sight to see a single person carrying, for example, a laptop, cell phone, and a tablet such as an iPad. The 802.11ax standard was designed to address these issues and build on the successful 802.11ac standard that will allow organizations to make gains in the overall capabilities their wireless networks can offer (Allison, 2019).

The first of these capability gains are the potential data rates that could theoretically be achieved. As mentioned in the paragraph on 802.11ac, MU-MIMO allows for multiple transmissions to be received by a wireless access point for increased data traffic but with 802.11ax, multi-user orthogonal frequency division multiple access (MU-OFDMA) is added to gain as much efficiency as possible (Allison, 2019). MU-OFDMA works by subdividing transmission bandwidth into subcarriers that allow the different transmissions of multiple devices to occupy the same transmission space (Teckchandani, 2019). To compare this concept in terms of vehicle traffic, 802.11ac would be the equivalent of an intersection with a traffic light. Vehicles take turns traversing the intersection but only when it is their turn and when the traffic light turns green. 802.11ax with MU-OFDMA would thus be the equivalent of a roundabout where vehicles can uniformly merge and transverse a shared space with other vehicles in the intersection without coming to a complete stop. This method using MU-OFDMA in conjunction with MU-MIMO allows a 37% increase in transmission throughput and increases the overall efficiency (Allison, 2019).

Another capability that 802.11ax has over the previous standard is an increased emphasis on wireless network deployment in a dense and frequency diverse environment. When deploying any wireless network, it is a best practice to perform a wireless site survey to understand if there would be any interference from other wireless devices located in the surrounding areas (Ciampa, 2013). With 802.11ac deployments, attention was given to make coexistence with other wireless networks possible while continuing to drive toward increase speeds and better power consumption (Allison, 2019). This is accomplished by frequency spectrum sharing in situations that exhibit a large number of dissimilar wireless networks.

Lastly, 802.11ax introduces the next level of security with the addition of Wi-Fi Protected Access (WPA3). As more and more devices need to access these wireless networks, security for dense environments are crucial to ensure only the right people are accessing the right information. WPA3 builds upon the success of WPA2 with better management of open networks while maintaining 256-bit encryption using Advanced Encryption standards (AES) (Allison, 2019).

Switching to IEEE 802.11ax

The 802.11ax wireless standard adds a lot of capability to an organization looking to start down a wireless upgrade path, but the question is whether or not an organization should make the investment. As with many other situations, challenges, and changes within IT, the choice to upgrade hardware is certainly dependent on the specific scenario that is being played out. If an organization is not expanding its footprint (i.e. they are not adding wireless hardware to their inventory) adjusting the organization's plans to adopt early may not be the best idea (Allison, 2019). However, if that same organization is adding wireless infrastructure due to a new building addition or remote office, it would be recommended to invest in 802.11ax devices to take advantage of newer features while maintaining backward compatibility. From an aspect of planning for the future, and 802.11ax deployment makes a lot of sense as the number of client devices has been steadily increasing and will continue to do so. Additionally, future amendments to the 802.11ax could see the use of additional frequencies such as the 1 GHz and 7 GHz bands (Allison, 2019). The possible increase in frequencies could mean even more bandwidth for services such as video streaming or other IoT devices needing separation from an already established 2.4 GHz and 5 GHz spectrum. While switching to 802.11ax does carry a lot of benefits in terms of future-proofing an organization, there is a question about what to do with current wireless clients such as computers and other mobile devices that exist in the organization. For the benefits of the features within the 802.11ax standard to be fully taken advantage of, the devices that are connecting to a new wireless deployment need to also be certified with 802.11ax. While backward compatibility exists, features such as speed and special stream sharing through MU-OFDMA would not be possible. Overall, any organization should seriously consider making the switch from other 802.11 standards to the 802.11ax standard if the operational environment of the organization allows.

Conclusion

As with any technology, the demand for improvements gives rise to additional functionality that is driven by ever-changing standards. IEEE 802.11ax is a great example of this change that provides a rich feature set to address the challenges in density, security, and speed that is needed in technologically capable devices. Organizations that identify these challenges have the choice to upgrade to the new standard, but careful consideration of organizational needs must take place. If needs are warranted, an upgrade to the 802.11ax standard would be advisable.

17. References

Allison, P. (2019). What 802.11AX Means for Your Network. *Computer Weekly*(23). Retrieved October 18th, 2020, from https://links.franklin.edu/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=f5h&AN=134706746&site=eds-live

Ciampa, M. (2013). *CWNA Guide to Wireless LANs* (3rd ed.). Boston , MA: Cengage Learning.

IEEE. (2020, September 24). *Official IEEE 802.11 Working Group Project Timelines - 2020-09-24*. Retrieved October 13, 2020, from IEEE 802 LAN/MAN Standards Committee: https://www.ieee802.org/11/Reports/802.11_Timelines.htm#tgac

Perahia, E., & Stacey, R. (2013). *Next Generation Wireless LANs.* Cambridge, United Kingdom: Cambridge University Press. Retrieved October 13, 2020, from https://ebookcentral-proquest-com.links.franklin.edu/lib/franklin-ebooks/reader.action?docID=1139677&ppg=6

Teckchandani, A. (2019, March 13). *What's the Difference between OFDMA and MU-MIMO in 11ax?* Retrieved October 18th, 2020, from NetworkWorld: https://www.networkworld.com/article/3366216/what-s-the-difference-between-ofdma-and-mu-mimo-in-11ax.html

Response to Reviewers

This white paper has been reviewed by class peers and the following content was chosen to be included in the editing process. This section is presented in two parts. The first is the original comments or critiques made by the reviewer and the second part is the response to the reviewer.

1. A few minor punctuation and gramitcal errors but overall very well done. These are very minor, the paper is written well. A simple run through of a grammatical checking software will assist with these issues easily.

Exmaples:

"Wireless connectivity for the organization has been around for a few decades and standards were created to ensure interconnectivity between devices."

Should have a comma before the "and" in this case.

"Now, the 802.11ax standard expands the features of 802.11ac by adding methods for transmission sharing which allows for a greater number of devices in a densely populated network."

Should have a comma before "which" in this. The word "which" is used throughout the document in a situation where some punctuation may be required.

Or a sentance rephrase for example here...

"Much of the increased speed is due to the various forms of Multiple Input Multiple Output (MIMO) which is the utilization of several radio transmitters and receivers to accept more than one signal from a device at a time (Ciampa, 2013)."

rephrase to

"Much of the increased speed is due to the various forms of Multiple Input Multiple Output (MIMO), which utilizes several radio transmitters and receivers to accept more than one signal from a device at a time (Ciampa, 2013)"

Response:

I disagree with this assessment of the correct use of commas. The use of commas is to indicate a natural pause in a sentence structure or to combine stand-alone thoughts into a single sentence. The original sentences of the examples given do not require a natural pause and the use of an additional comma would force a single thought into two that would not otherwise be able to exist on their own. An additional look at grammar, spelling, and punctuation has been completed, but no changes have been made based on the critique.

2. This whitepaper provided good referenced coverage of both 802.11ac and 802.11ax and proper comparisons and contrast.

Examples of each technology that are relatable and accurate are present.

Proper recommendation with a caveat as to who the recommendation is a good touch as one recommendation will not work for all.

Response:

This critique was marked as “Good” with no indications of what may need to be corrected to create a better white paper. As such, no changes have been made regarding this comment.

3. While some examples of jargon are present, each example gives a definition or explanation of what the jargon refers to.

There is a single use of "you" that I noticed during the reference to network traffic being compared to a traffic roundabout. Could be reworded to something similar to "Thinking of this concept as..." Instead of "If you think of this concept..."

Paragraphs in specific sections flow pretty well, but perhaps a transitional sentence between sections may be helpful.

Response:

The use of the word “you” has been removed to maintain professional consistency. The sentence now starts with, “To compare this concept in terms of vehicle traffic…”

4. I'm not sure that this whitepaper fits the desired format. While the abstract, introduction, and conclusions are present. There really isn't a definition of the problem, analysis of possible solutions, and how the possible solutions will be evaluated and chosen. From a strickly informational paper on 802.11ac/ax, it is good, however I believe this just misses the mark on what was expected.

Response:

Originally, this white paper was set up to present a choice between two standards and to provide background information an organization might use to make an educated decision. A problem description was never specifically called out but was implied. I reworded some parts of the writing to make this clearer and to call out a specific recommendation.

Cloud Management and Monitoring

Brian Snyder

Franklin University

Abstract

The adoption of cloud-based applications, also known as Software as a Service (SaaS) has become commonplace, with over ninety percent of midsize businesses currently using one or more to deliver business services. Many branch offices do not have the resources to manage and monitor network devices and services. Cloud management and monitoring of various networks have become commonplace. This approach has many benefits over classic on-site configuration and updates. This paper will compare and solve different problems with new cloud technologies. This paper will also attempt to compare and contrast different management and monitoring systems and determine an appropriate solution for a small branch office.

DTX is a Florida manufacturing company with 200 employees. DTX has recently secured a new customer located in Texas. Due to the nature of the contract, DTX will need to have a presence in Texas to be near the new customer. DTX will need to collaborate on various, large-scale projects. While there are ample ways to perform remote collaboration, the customer's projects will need on-site engineers and support staff from DTX to ensure quality and product specifications. As such, DTX has decided to lease a building that is located close to the customer to provide the needed support required by the contract.

DTX will have minimal on-site IT support in the new branch location. It will be imperative that the configuration and management of network equipment be as seamless as possible. The on-site support will also be tasked with other functions and may have little time to monitor network systems regularly. A high availability system with alerts would be very beneficial to minimize downtime. A cloud management system would be ideal for this situation. The bulk of the configuration could be done by the central IT staff at the main office as well as monitoring uptime. This document will focus on the cloud solution offered by Cisco Meraki.

Simplified configuration

Cisco Meraki Systems Manager is a complete endpoint management solution that provides deep visibility and control over your Android, Chrome OS, iOS, macOS, and Windows devices. It unifies endpoint management into a single pane of glass through an easy-to-use, cloud-based Dashboard shared with the rest of the Meraki stack and is the only solution to bring network-level security and visibility to the endpoint.

Key capabilities include:

- Manage and monitor endpoint devices

- Manage and distribute mobile and enterprise applications
- Investigate and change device functionality based on device status

This technology will greatly simplify configuration for the new branch office. The bulk of the configuration can be accomplished by the staff at the main corporate office before the equipment arrives. This consolidated view of all network technologies including clients can give a high-level view of current network health and potentially stop and issues before they arise.

Limited IT Staff/Budget

Upgrading network switches is often a significant financial and technological commitment. Switches are the foundation of any network and are expected to last anywhere from five to ten years or more. In today's modern networks switches must be highly reliable, easy to manage at scale, and compatible with the latest technologies for the foreseeable future.

As networks grow in size and complexity, decision-makers are beginning to look beyond the upfront hardware costs to include operational expenses, which can become a significant, recurring cost. This is often referred to as Total Cost of Ownership (TCO). Initial configuration, network complexity, troubleshooting, security, and revision management can add up to a substantial cost each year. Selecting the right solution can pay massive dividends and often significantly recover the costs of a network refresh over the lifetime of the deployment.

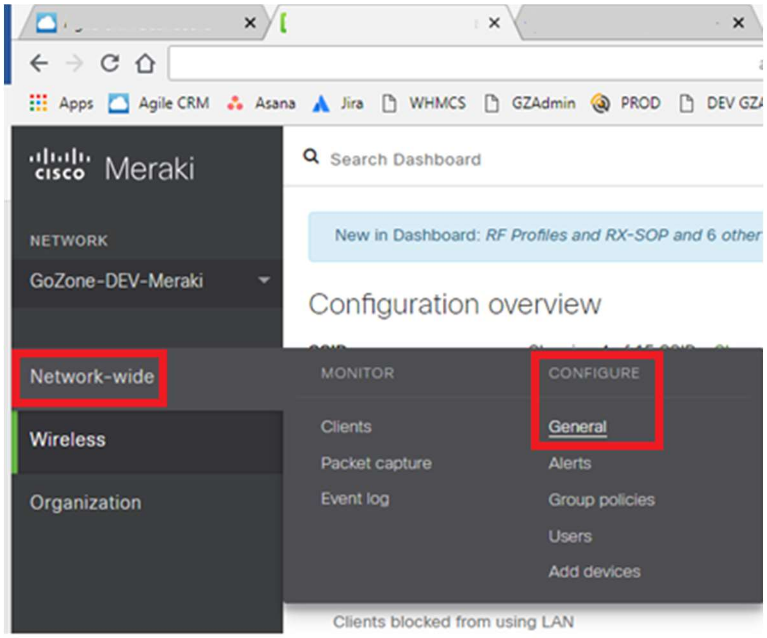
Solutions such as zero-touch provisioning can greatly save on installation time and budget. Hardware no longer needs to be pre-staged to be effectively installed. The DTX branch office will need to be installed and online as rapidly as possible with very little interaction from support staff. This technology will facilitate that goal.

Network Health and Alerts

When managing a large campus or many remote sites, getting a general overview of all networks and devices can be a daunting task. Adding reporting and visibility per site often requires additional solutions to be set up and maintained, increasing up-front and operational costs. Meraki has built-in alerting and reporting features so there is no need for maintaining yet another solution.

Meraki will allow staff at the DTX main office to monitor network health without the need for another on-site IT staff member. The Meraki Dashboard offers several alert options such as email and dashboard. Alerts can be effectively communicated to on-site staff for prompt remediation.

Figure 1. Meraki Configuration and Alerts



Security

Automatic cloud updates: When managing many remote sites, keeping devices updated with the latest software can be a daunting task. Any time a new software update or patch is released, it can require significant downtime and weeks of work before the entire switch network has been updated. With Meraki, simply select the desired upgrade window and when a new software update becomes available, the cloud will seamlessly upgrade network devices while you sleep!

Do the math: Company Profile: Retailer with 150 locations At 150 locations with 2 switches per store, each switch takes approximately one hour of installation and configuration. This would add up to 300 hours or $30,000 in wages at an average onsite rate of $100 per hour. Use Meraki switch clone and automatic software updates to reduce install time to just 10 minutes and save $25,000 in provisioning costs.

DTX would like to take advantage of the cost-saving security features provided by the Meraki solution. The automatic security updates are of great benefit due to the prevalence of ransomware and other malware. The branch office site will have limited IT support and a proactive approach will be needed.

The reduced installation time will also be of great benefit. This will allow replacement switches to be installed and configured in a matter of minutes by on-site staff. This is especially useful if spare hardware is available in the server rack.

In conclusion, Cisco Meraki offers a suite of cloud products that can simplify installation, reduce costs, and the need for on-site IT staff for the new DTX branch office. Real-time monitoring and seamless security updates will also avoid any potential downtime. Any issues will be communicated almost instantly via email or other alert systems. The majority of issues could be repaired from the main corporate office with little need to disrupt the staff at the branch office. The complete network health will be available at a glance from a convenient and user-friendly dashboard.

References

General Systems Manager Deployment Guide. (2020, July 20). Retrieved October 19, 2020, from https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Best_Practice_Design_-_Endpoint_Management/General_Systems_Manager_Deployment_Guide

Getting Started. (2020, May 27). Retrieved October 14, 2020, from https://documentation.meraki.com/Getting_Started

Reducing Cost & Complexity with Cisco Meraki Switches. (n.d.). Retrieved October 18, 2020, from https://meraki.cisco.com/wp-content/uploads/2020/05/meraki_switch_cost_savings_guide.pdf

SIMPLE CLOUD-MANAGED NETWORKING. (n.d.). Retrieved October 18, 2020, from https://www.arubanetworks.com/assets/so/SO_Cloud.pdf

Response to reviewers

I have fixed the indentation on the references page to match proper APA formatting. I did not have the paragraph set to hanging indentation.

Reread the whitepaper and corrected some grammar issues and made the paper overall easier to read and understand.

ITEC495
Windows Server & Network Security
Implementation of Benefits for a Company
Assignment: White Paper
Jamish Patel
Professor Wayne Smith
10/18/20

Abstract

The purpose of the report is to discuss the benefits of implementation to Windows Server 2019, Hyper-V, and network security in a mid-size company setting and to recommend, based on research, that implementation is a beneficial and cost-efficient solution for a mid-size company. The new enhanced features that windows server 2019, and Hyper-V offers allow a company the ability to make the most of current resources. However, many company's maybe deterred to new implement due to cost or lack of compelling rationale.

Introduction

Recent reviews of Windows Server 2019 have shown the reason for the hesitation of implementation could be primarily due to the increase in cost (Keizer, 2018). Businesses will purchase licenses based on the number of activated processor cores located in each server (Keizer, 2018). Furthermore, repeatedly mid-size businesses have become comfortable relying on Office 365 (Bruzzese, 2018). Nevertheless, many mid-size businesses are looking for a server solution that will fit their tight budget and offer all of the features they need to continue to be competitive.

Background

Microsoft released windows server 2019 Technical Preview in March 2018 (Team, 2018) The new Windows Server 2019 rolls up many incremental updates that Microsoft introduced over the past three years and packs in many new features as well, especially in areas of security, administration, storage and integration with Microsoft's Azure cloud (Henderson, 2019). The new features that are most beneficial to the company is a Windows Server 2019 goes too far greater lengths than ever before to prevent attacks. Windows Defender is included by default and has new features designed to plug security holes and make administration easier. Although Defender won't stop a trigger-happy email recipient from opening an attachment harboring a zero-day threat, Windows Advanced Threat Protection adds another layer of security designed to protect against several kinds of malware behaviors, including a method of "bolting down" folder access to prevent ransomware-like mass file encryption (Henderson, 2019). Another feature also beneficial to a company is a Hyper-V and a network security

Hyper-V

Hyper-V quick for hypervisor is essentially software that allows multiple virtual machines to run while controlling the hardware and allocating resources to each virtual machine operating system (Shinder, 2008). Hyper-V servers allow for the consolidation of resources which help small businesses improve server operation and reduce cost (Branimir, Zlatko, Bundalo, & Palic, 2016). Additional key benefits of having a virtualized infrastructure are, business continuity and disaster recovery, development and test systems, and a dynamic data center (Branimir, Zlatko, Bundalo, & Palic, 2016). Previous versions of Windows Server have included Hyper-V. However, the new enhancements included in Windows Server 2019 have caught the attention of many organizations.

One of the enhanced features that Windows Server 2019 now offers is nested virtualization, which is one of the newest features in Microsoft virtualization tools (Branimir, Zlatko, Bundalo, & Palic, 2018). This feature allows a mid-size company to create development or testing environments which completely removes the cost of having to use dedicated hardware (Posey, 2016). Secondly, nesting can be used for IT training (Posey, 2016). Every mid-sized business today has an IT department, instead of unleashing administrators on a current production server, an environment can be created in which administrators can safely learn and experiment (Posey, 2016).

Microsoft has included hot add and removes for network adapters and memory (Microsoft, 2018 B). This new feature allows users to add or remove a network adapter while the virtual machine is running which decreases downtime (Microsoft, 2018 B). Additionally, the amount of memory assigned to a virtual machine can be changed while it is running (Microsoft, 2017 B).

Lastly, Windows Containers allow isolated applications to run on a single computer system (Microsoft, 2018 B). Hyper-V Windows Containers are scalable, fast, and portable using a light-weight virtual machine for each container (Microsoft, 2018 B). This new feature provides small businesses with the support they need for websites and applications, including the ability to manage data through container shared folders, and the capability to restrict container resources (Microsoft, 2018 B).

These are just several of the more prominent new features of Hyper-V included in Windows Server 2019. Other new features included in Windows Server 2019 Hyper-V are Windows admin center, Desktop experience, System Insight, Security Advanced Threat Protection (ATP), and Hybrid Cloud start order priority for clustered virtual machines, shielded virtual machines, rolling Hyper-V cluster, production checkpoints, discrete device assignment, encryption support for virtual machines and host resource protection (JasonGerend, 2019 B)

Network Security

In today's world, data security is a central concern for organizations of any size. With attacks happening more frequently and with greater sophistication, organizations must take an increasingly aggressive stance towards protecting their cyber networks and assets against unauthorized access. At the forefront of this effort to combat new and emerging threats has grown a reliance on the tools and best practices utilized to protect enterprise systems from attacks that originate both externally and internally (RSI Security, 2019). Cisco is one of the best products for mid-size and a large size network. Cisco convergence of security and networking can help the company leverage the network's intelligence and visibility to make more-informed decisions on policy and threats. The feature of Cisco Intent-Based Networking Security is that the Cisco DNA Center and its streamlined security integrations, can Enable automated access policies, Stop propagation of data breaches, Streamline visibility, and Automate threat responses from the SOC which can help the company to protect their data and devices from threats (Cisco, 2020).

Features as Business Solution

Windows Server 2019 was created for cloud deployment (Anderson, 2018). These new features meet the needs of many small businesses. According to a study done on cloud computing and its effects on small businesses, the cost of cloud computing is estimated to be at least three to five times less than that of traditional data management (Alijani, Fulk, Omar, & Tulsi, 2017). In a recent study to discover small businesses' motivation for using cloud computing, cost efficiency was the highest reason for utilizing the technology (Alijani, Fulk, Omar, & Tulsi, 2017). Window Server 2019 addresses the top priorities of today's technological landscape with more advancement to cloud computing and Introducing new Advanced threat protection (ATP) than any previous major Window Server release (Anderson, 2018). This has brought Windows Server 2019 into the age of cloud computing which is in line with most business models.

Recommendation

Based on this research there is evidence to propose that mid-size companies are involved in pursuing cloud computing implementation to Windows Server 2019. Although there may be an increased cost of licenses the new features make implementation a beneficial long-term investment. The Cisco Intent-Based Networking Security is also evidence to propose the mid-size company to secure their company network infrastructure.

Response to Reviewers

Reviewer two pointed out that there was a sentence that used first-person "Based on this research I propose...", this statement has been changed to “Based on this research there is evidence to propose…”. The cover page has been edited to ensure APA format has been followed. Reviewer two also stated that adding a list of keywords to the abstract is necessary however, APA guidelines state that this is optional, and therefore the decision was made not to include it. Reviewer three commented that the in-text citations were not displayed. After reviewing OWL Purdue as suggested by the reviewer, all citations meet APA guidelines. No changes were made to the in-text citations. Reviewer three also suggested a cover page format change that did not meet APA guidelines therefore it was not utilized in the final draft. However, a change to the reference formatting to include a hanging indentation was applied to the final draft. Reviewer four suggested that fewer sources be used, however, the use of these sources is crucial to support the claims made within the paper. Therefore, there were no changes to the number of references used.

References

DNA), C., 2020. Enterprise Network Security Solutions – Cisco DNA Security. [online] Cisco. Available at: <https://www.cisco.com/c/en/us/solutions/enterprise-networks/enterprise-network-security/index.html> [Accessed 14 October 2020].

Anderson, T. (2018). What's New in Windows Server 2019. Computer, 18-21.

Alijani, G., Fulk, K., Omar, A., & Tulsi, R. (2017). Cloud Computing Effects on Small Business. Entrepreneurial Executive, 35-45.

Henderson, T. (2019, November 19). Review: Microsoft Windows Server 2019. Retrieved October 17, 2020, from https://www.idginsiderpro.com/article/3454599/review-microsoft-windows-server-2019.html

JasonGerend. (n.d.). What's new in Windows Server 2019. Retrieved October 17, 2020, from https://docs.microsoft.com/en-us/windows-server/get-started-19/whats-new-19

Keizer, G. (2018, March 22). Microsoft begins push for Windows Server 2019. Retrieved October 17, 2020, from https://www.computerworld.com/article/3265061/microsoft-begins-push-for-windows-server-2019.html

Security, written by RSI. “What Are The Main Benefits Of Enterprise Network Security Solutions?” RSI Security, 23 Feb. 2019, blog.rsisecurity.com/what-are-the-main-benefits-of-enterprise-network-security-solutions/.

Solutions - Intent-Based Networking Security At-a-Glance. (2020, July 13). Retrieved October 17, 2020, from https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/intent-based-network-security-aag.html

Team, M. (2018, September 18). Introducing Windows Server 2019 – now available in preview. Retrieved October 17, 2020, from https://cloudblogs.microsoft.com/windowsserver/2018/03/20/introducing-windows-server-2019-now-available-in-preview/