[redacted] Network Equipment Refresh

George J. Lemere

Western Governors University

Table of Contents

Summary

[redacted] is a medium-sized school district in [redacted] Texas with an enrollment of 3500 students in grades K-12. The district consists of a Primary School, Elementary School, Junior High School, and High School, along with Central Office, Transportation, and Technology buildings. Their network is a mix of multi-vendor equipment that lacks standardization and includes equipment that the manufacturers no longer support. The district network suffers from poor performance, frequent network crashes, and the ability to support any future growth.

As the Director of Technology for the district, I was tasked with documenting, upgrading, and standardizing the network infrastructure. This process included compiling an inventory of the current network equipment, discussing future growth with campus principals and district leadership, and designing a network that will support that growth consisting of equipment from a single manufacturer. Once the network design and equipment list were finalized, the district solicited bids from vendors to purchase and install the new network equipment.

This project began with interviews of district leadership and campus principals to determine the needs and expectations of the network, as well as discuss the possibility of future growth of the district. While these interviews were going on, district IT staff was documenting existing network equipment and analyzing the current environment, such as ensuring adequate power and cooling was available in each of the equipment closets and the fiber optic cabling that connects each of those closets. At this time, the fiber optic cabling that connects the campuses to the technology building was tested and verified to handle the new equipment's transmission speeds.

Phase 2 of the project consisted of designing the network, including IP address schemes/VLANS, and compiling a finalized equipment list for each location. Once this list was

complete, it was emailed to various vendors and posted on the district website for two weeks. After the 2-week period ended, the bids were evaluated, and a vendor was selected. Once the vendor was selected and the scope of work was determined, the equipment was ordered.

Phase 3 began with receiving, verifying, and configuring the new equipment. The new equipment was powered up and configured at the technology building and installed at the proper campus location. The process was carried out one campus at a time, beginning with the campus's main distribution frame (MDF) and then progressing to each intermediate distribution frame (IDF) within the building. Throughout this document, the main distribution frame (MDF) refers to the central connection point for the campus or building to the rest of the network, and the intermediate distribution frame (IDF) refers to the smaller network closets within the campus or building that provide connectivity to the end user devices. The reasoning for this approach was that it minimized the downtime of each of the campuses, and any problems that arose would be addressed without affecting the rest of the district.

Review of Other Work

Migrating and standardizing on a manufacturer for network equipment simplifies the administration and reduces network management overhead. During this project, extensive research was done to search for advice, tips, and similar outcomes to gauge the success of the project. According to the Cisco Enterprise Campus Infrastructure Best Practices Guide, it is a recommended best practice to deploy a three-tier LAN design when numbers of distribution blocks are greater than two (Cisco, 2014). The three-tier LAN design consists of a Core, Distribution, and Access tier. The access layer is the first tier of the campus, where end user devices such as computers, printers, VOIP telephones, IP-based security cameras attach to the wired portion of the campus network. The distribution or aggregation layer is the network boundary between the campus and the routed campus core network. The campus core layer is the heart of the network backbone. This document was extremely helpful in communicating the needs and expectations of the district to the vendors.

After the physical design of the network was completed, it was time to investigate the logical layout. The old network was a flat network with no IP segmentation or VLANs. A VLAN is a logical group of workstations, servers, and network devices that appear to be on the same Local Area Network (LAN) despite their geographical distribution (Cisco, 2020). It was determined that [redacted] would benefit by creating VLANs for similar devices on the network, including VOIP phones, Wireless Clients, and IP-based security cameras. The default VLAN would be configured for management purposes only and separated from the user data traffic. Another best practice is to create a "dead end" VLAN to place unused ports in until they are needed and to either not enable routing between the VLANs or using Access Control Lists (ACLs) to servers or other devices that may contain confidential information.

After the information was gathered for the physical and logical design of the new network it was time to look at prioritizing and routing traffic. Since [redacted] has switched over to a VOIP phone system, it is extremely important to be able to prioritize that traffic. For VOIP transmissions to be intelligible to the receiver, voice packets should not be dropped, excessively delayed, or suffer varying delay (otherwise known as jitter) (Cisco, 2001). All modern networking equipment support the classification and marking of packets. Classification is the process of identifying the class or group to which a packet belongs. The most common way to accomplish this is by enabling an Ethernet 802.1p class of service (COS) tag to the traffic. This allows all voice traffic to be identified and prioritized over user data traffic to allow for clear communication between phones without having any pauses, drops, or jitter.

Changes to the Project Environment

[redacted] had a fundamental network setup. Within the technology center, there was a single 3Com 7906E 8 slot chassis core switch that connected to the internet via a 1 Gbps (Gigabits per second) fiber connection to a SonicWALL NSA 6600 firewall, which also had a 1Gbps uplink to their internet service provider. There were also two 3Com 4400 48 port switches that provided connectivity to the servers located in the center and the endpoints that the technology department uses. This core switch connected to each of the campuses and support buildings via single-mode fiber optic cable at 1Gbps speeds. The High School campus consisted of an MDF and 8 IDFs with a mix of 3Com and HP 48 port switches. These switches were stacked where applicable, and each IDF connected to the MDF at 1Gbps via multi-mode fiber optic cable. All the switches delivered 1Gbps to the endpoint devices. The Junior High campus had an MDF and 4 IDFs with the same mix of 3Com and HP switches. Once again, each IDF connected to the MDF at 1Gbps via multi-mode fiber optic cable and delivered 1Gbps speed to the endpoints. The other two campuses shared a similar configuration to these, just at a smaller scale. The one common theme was the mix and match of vendors with equipment over ten years old. Although this equipment was still functioning, it was running at total capacity and could not keep up with the volume of devices that have appeared over the last few years.

The current network design was a flat network with no IP segmentation. The problem that this caused was that if a broadcast packet is sent out from one of the High School clients, that broadcast packet was sent to every campus and building connected to the network. This also made the network susceptible to network loops which crashed the network. A network loop is caused when a patch cable is plugged in from one network port directly to another. This caused the packets to reflect back to the source which locked up the switch and, in this case, the entire network.

The new equipment installed in the technology center consists of two 8 slot chassis core routers that connect to the campuses at 10Gbps. Each campus has two connections running into the technology center, one for each core router. This adds redundancy to the network backbone in the event that if one connection fails, the other will continue to pass traffic. On the campuses, the MDFs were also connected to each IDF via 10Gbps redundant links where applicable. The new network design segmented each campus into its own IP subnet and went a step further by segmenting each IDF within the campus into its own subnet as well. Along with this network segmentation, VLANs (Virtual Local Area Networks) were configured for wireless access points and clients, VOIP (Voice over IP) telephones, and IP-based security cameras.

Methodology

As project manager, I chose the waterfall methodology model as this is a straightforward, well-defined project management methodology suitable for a project with a well-defined goal that will not change. The waterfall model consists of 6 phases: Requirements, System Design, Implementation, Integration and Testing, Deployment of System, and Maintenance. This is a common model to follow with projects such as this since it has clearly defined stages that begin when the preceding stage ends.

The Requirements phase of this project was satisfied by gathering relevant stakeholders from across the district. These meetings discussed the current state of the network, the issues to overcome, and a plan for future growth. This lead directly into the System Design phase, where based on the information gathered, a new network design was developed to include number of switches needed, the performance of those switches, and how they will be configured.

The Implementation phase began by generating a list of equipment needed from the System Design phase and ordering that equipment from the selected vendor. This equipment was delivered to the Technology building and grouped according to location. Once this equipment was added to the district inventory, it was unboxed and configured according to the destination and network best practices. The equipment was allowed to run for at least 24 hours to protect against failures directly from the manufacturer.

The Integration and Testing phase began by installing the new core switches alongside the current core switch and verifying connectivity to the existing firewall and internet. From this point forward, the Integration and Testing phase was immediately followed by the System Deployment phase per location. This meant that staff began at the site's MDF and replaced all existing equipment with new equipment. The new equipment was installed, powered on, and connected to the network backbone. Once connectivity with the new core had been established, the endpoint equipment was plugged into ports on the switch. After the endpoints' connectivity was verified, staff moved on to the next IDF and repeated the process until the entire location ran on the new network. Verification of endpoint equipment included computers connecting to the internet, security cameras recording to the security servers, and voice-over IP phones being able to make and receive calls.

This brought us to the Maintenance phase of the project, which included the monitoring and day-to-day management of the new network equipment.

Project Goals and Objectives

	Goal	Supporting objectives	Met/Unmet
1	Network Design & Upgrade	1.a. Inventory and document existing network equipment	Met
		1.b. Design new network and order hardware	Met
		1.c. Configure network switches	Met
		1.d. Install network switches and test connectivity.	Met
2	Improve network management	2.a. Verify network documentation and install management software	Met

Goal 1: Network Design and Upgrade. Create a new network design and replace all outdated, end-of-life hardware. Completing this goal entailed designing an efficient, robust network, selecting a single hardware manufacturer for networking hardware, and was qualified by increased network throughput, stability, and ease of management. This was the project's primary goal and consists of four supporting objectives.

Objective 1.a. Inventory and document existing network equipment. This was mainly needed for the number of switches, port count, and evaluating the network's future growth. One of the main problems with the current network was that it was a "flat" network not consisting of any IP segmentation or VLANs. Therefore, the current design of the network was not needed. This objective was met when an inventory of all the existing network equipment was completed along with the documentation, labeling, and testing of all fiber optic cabling performed.

Objective 1.b. Design new network and order hardware. The next step in this process was to create a new network design for the district. This network design was created to be secure, efficient, and adhere to industry best practices. Based on this design, an equipment list was created, ordered, and received at the Technology Center.

Objective 1.c. Configure network switches. All network hardware was shipped to the technology center. Upon arrival, all equipment was inventoried and configured. The equipment was then grouped by location and allowed to run for at least 24 hours to ensure there were no failures or defective modules.

Objective 1.d. Install network switches and test connectivity. Fortunately, [redacted] had the space in the district MDF to allow the installation of the new core switches alongside the existing core switch. This enabled both old and new core switches to be up and running and connected to the internet. The district also had spare fiber running to each location, allowing technology staff to replace switches one location at a time without bringing down the rest of the district. As the technology department staff installed the new equipment at the campuses, they tested the connectivity of all wired and wireless devices. The also tested the functionality of the VOIP phone system and IP-based security cameras before they moved on to the next campus.

Goal 2: Improve Network Management. The next goal was aimed at improving the management and helping with troubleshooting issues at the network level. [redacted] was always reactive to network issues instead of proactive. This was accomplished by a single objective and was qualified by being able to monitor and manage the network from the technology center.

Objective 2.a. Verify network documentation and install management software. Once the new networking equipment was installed and functioning properly, the technology staff updated and verified the network design along with IP address and VLAN configurations. This documentation was stored in all disaster recovery and operational notebooks for future reference. The new network monitoring software was installed as the last step to this objective. This new software allows technology staff to backups of switch configurations and monitor the health of the network.

Project Timeline

Milestone or deliverable	Planned Duration (Hours or days)	Actual Duration (Hours or days)	Actual start date	Actual end date
Project Kickoff Meeting	1 Day	1 Day	8/1/2019	8/1/2019
Inventory and Document existing network equipment	2 Days	20 Days	8/2/2019	8/30/2019
Design New Network	1 Day	1 Day	8/5/2019	8/5/2019
Create list of new equipment	1 Day	1 Day	8/8/2019	8/8/2019
Send list of new equipment to vendors	14 Days	14 Days	8/9/2019	8/23/2019
Evaluate bids	3 Days	3 Days	8/24/2019	8/26/2019
Select vendor and order equipment	1 Day	1 Day	8/29/2019	8/29/2019
Receive hardware at Technology Center	14 Days	21 Days	8/30/2019	9/27/2019
Inventory and configure new equipment	3 Days	3 Days	9/28/2019	10/1/2019
Install new equipment	14 Days	14 Days	10/3/2019	10/17/2019

During this project, there were two obstacles that caused the project to take longer than initially expected. The first was a problem that was discovered while the technology staff was completing the inventory of the existing network equipment and testing the existing fiber optic cabling. It was discovered that the existing fiber optic cabling would not support the transmission speed of newer network equipment and give us the results that were expected. To rectify the situation a cabling vendor was called in to provide an estimate to replace the fiber optic cabling within the campuses. After the scope of work was accepted a purchase order was generated to allow the vendor to complete the necessary work. Fortunately, the work was completed quickly and since the problem was discovered so early in the process, it really did not have a major effect on the project timeline. The next issue that did influence the timeline was supply chain issues on some of the switches that were ordered, approximately half of the new switches were on back order and were not received until a week after the other equipment arrived in the district technology center.

Unanticipated Requirements

While documenting the existing network equipment and testing the fiber optic cabling across the district, it was discovered that the fiber optic cabling within the campuses was not capable of supporting the higher transmission speeds of newer equipment. Once this was discovered, a cabling vendor was called in to inspect the environment and provide a quote to run new fiber optic cabling between the MDF and IDF closets within the campus buildings. Once the quote was accepted the vendor was able to complete the work in just under three weeks. Since this issue was discovered so early in the project it did not interfere with the schedule but did cause the project to be slightly over budget.

Conclusions

The success of this project was determined by the positive response from district staff and students. Another determining factor is that not a single network crash has occurred since the installation of the new equipment. District staff has commented on the increased speed of the network and how it has helped them deliver instructional material on platforms that were not possible with the previous network. They have also commented on the lack of dropped phone calls on the district's VOIP phone system as well as the clarity of those calls.

Project Deliverables

Appendix A contains final network diagrams of the physical topology of the technology center, the district backbone, and the high school campus. Included on these diagrams are the design notes and the connection speeds between the switches.

Appendix B contains screenshots of the spreadsheets that document the IP address and VLAN schemes of the campuses and support buildings for the district.

Appendix C contains screenshots of the network monitoring software that was installed to assist with the configurations, troubleshooting, and day to day monitoring of the new network equipment.

References

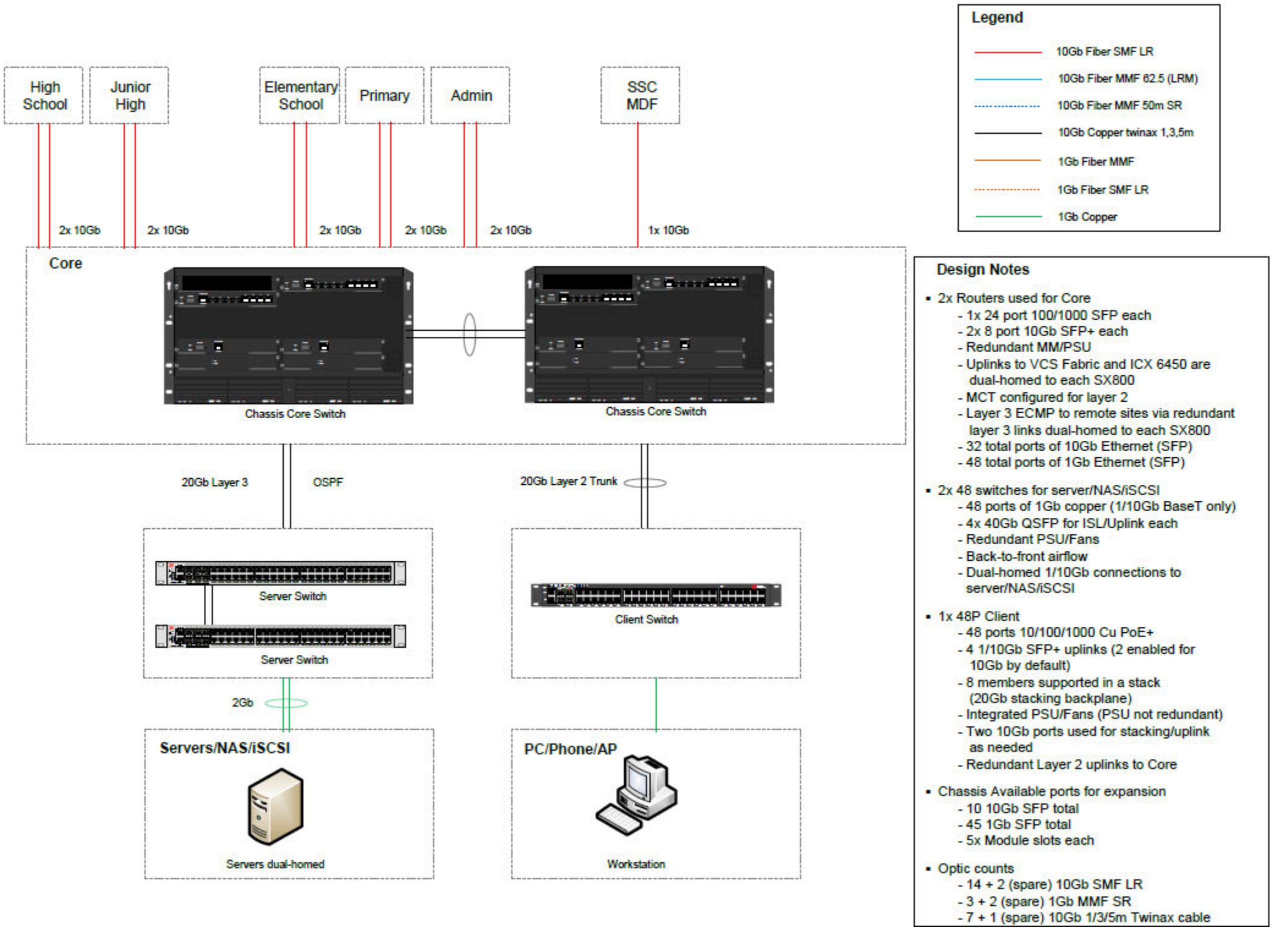
Cisco. (2001, June 30). *Quality of Service for Voice over IP.* Retrieved from Cisco: https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/qos_solutions/QoSVoIP/QoSVoIP.html

Cisco. (2014). *Cisco Enterprise Campus Infrastructure Design Guide.* Retrieved from Cisco.com: https://www.cisco.com/c/dam/global/shared/assets/pdf/cisco_enterprise_campus_infrastructure_design_guide.pdf

Cisco. (2020, January 27). *VLAN Best Practices and Security Tips for Cisco Business Routers.* Retrieved from Cisco.com: https://www.cisco.com/c/en/us/support/docs/smb/routers/cisco-rv-series-small-business-routers/1778-tz-VLAN-Best-Practices-and-Security-Tips-for-Cisco-Business-Routers.html

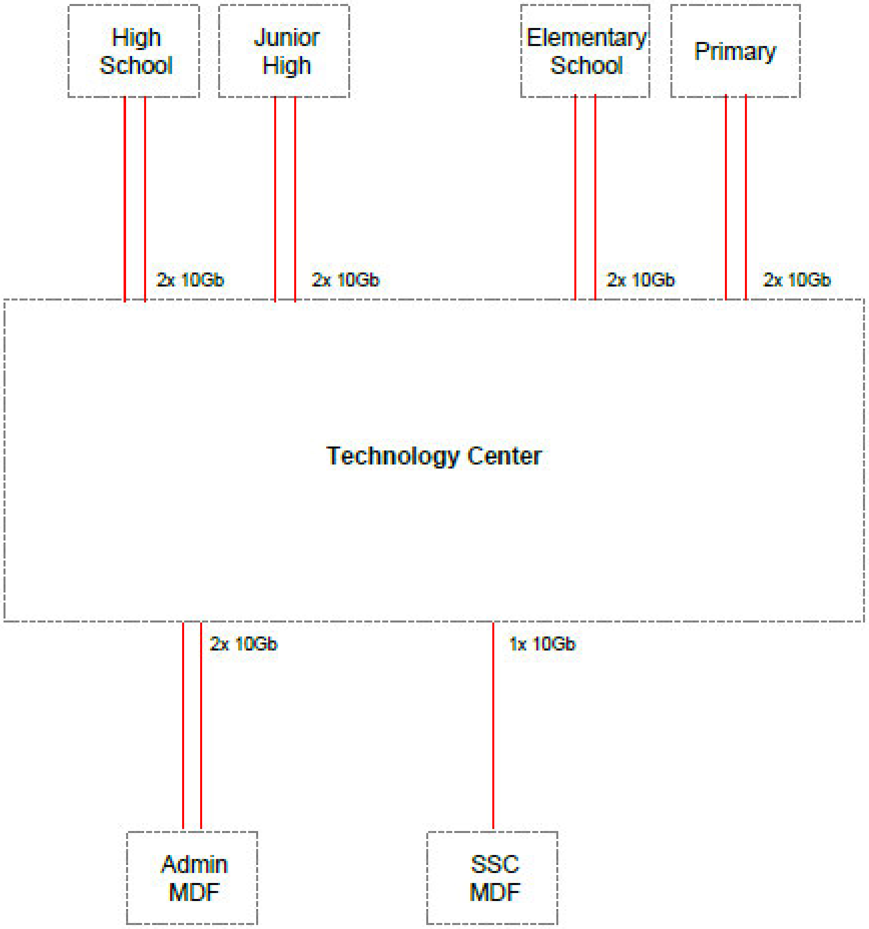
Appendix A

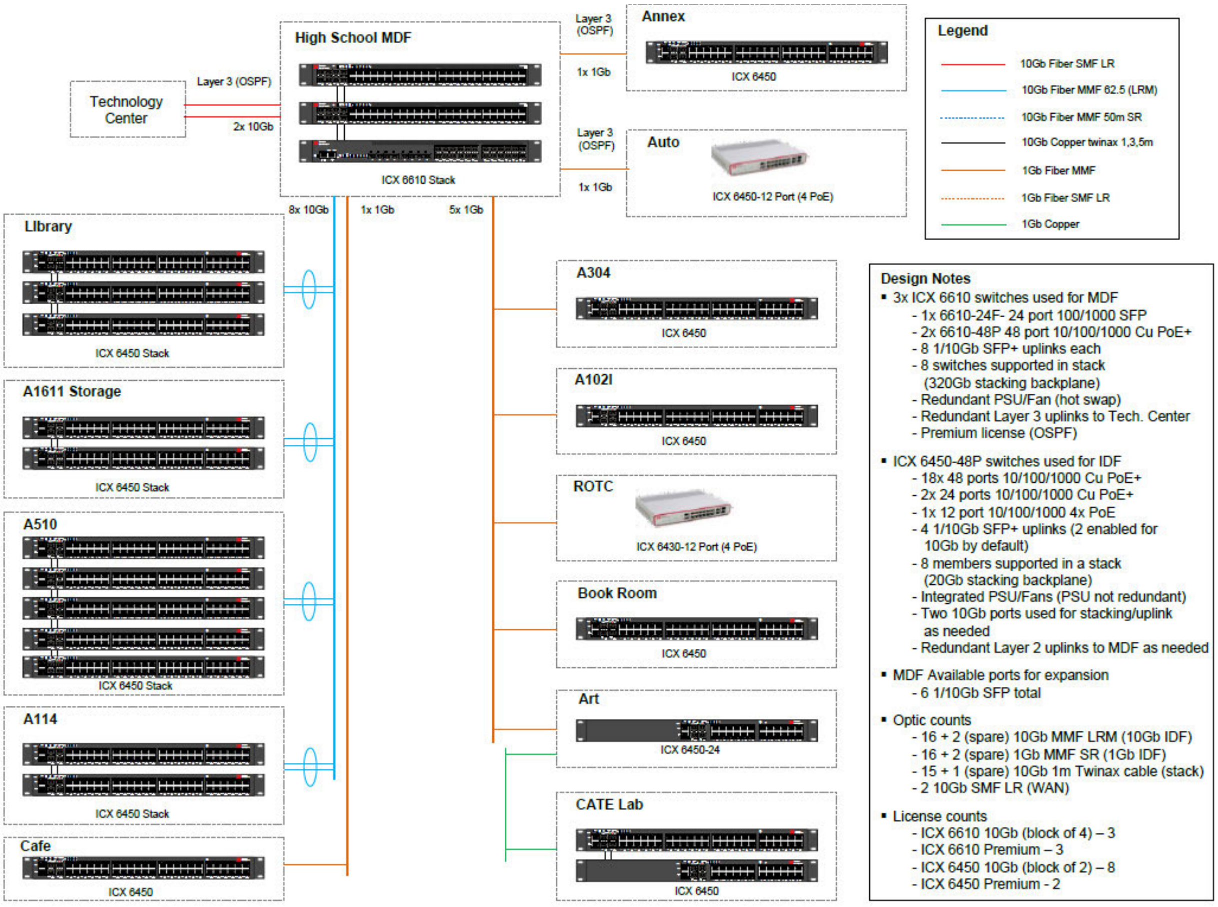
[redacted] Network Diagrams



Design Notes

- 2x Routers used for Core
  - 1x 24 port 100/1000 SFP each
  - 2x 8 port 10Gb SFP+ each
  - Redundant MM/PSU
  - Uplinks to VCS Fabric and ICX 6450 are dual-homed to each SX800
  - MCT configured for layer 2
  - Layer 3 ECMP to remote sites via redundant layer 3 links dual-homed to each SX800
  - 32 total ports of 10Gb Ethernet (SFP)
  - 48 total ports of 1Gb Ethernet (SFP)
- 2x 48 switches for server/NAS/iSCSI
  - 48 ports of 1Gb copper (1/10Gb BaseT only)
  - 4x 40Gb QSFP for ISL/Uplink each
  - Redundant PSU/Fans
  - Back-to-front airflow
  - Dual-homed 1/10Gb connections to server/NAS/iSCSI
- 1x 48P Client
  - 48 ports 10/100/1000 Cu PoE+
  - 4 1/10Gb SFP+ uplinks (2 enabled for 10Gb by default)
  - 8 members supported in a stack (20Gb stacking backplane)
  - Integrated PSU/Fans (PSU not redundant)
  - Two 10Gb ports used for stacking/uplink as needed
  - Redundant Layer 2 uplinks to Core
- Chassis Available ports for expansion
  - 10 10Gb SFP total
  - 45 1Gb SFP total
  - 5x Module slots each
- Optic counts
  - 14 + 2 (spare) 10Gb SMF LR
  - 3 + 2 (spare) 1Gb MMF SR
  - 7 + 1 (spare) 10Gb 1/3/5m Twinax cable


High School
Junior High
Elementary School
Primary
2x 10Gb
2x 10Gb
2x 10Gb
2x 10Gb
Technology Center
2x 10Gb
1x 10Gb
Admin MDF
SSC MDF



Legend

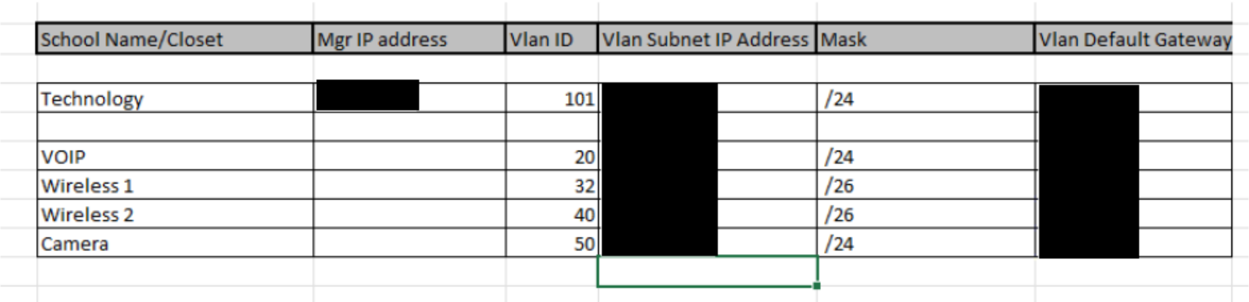
10Gb Fiber SMF LR
10Gb Fiber MMF 62.5 (LRM)
10Gb Fiber MMF 50m SR
10Gb Copper twinax 1,3,5m
1Gb Fiber MMF
1Gb Fiber SMF LR
1Gb Copper

Design Notes

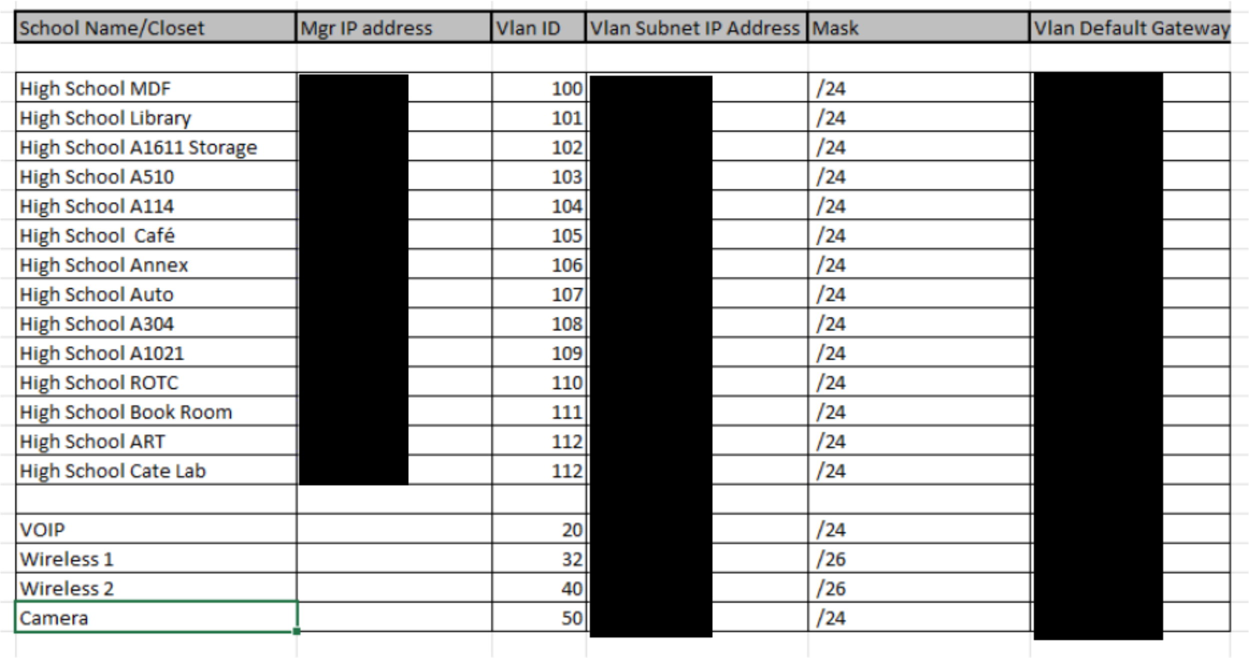
- 3x ICX 6610 switches used for MDF
  - 1x 6610-24F- 24 port 100/1000 SFP
  - 2x 6610-48P 48 port 10/100/1000 Cu PoE+
  - 8 1/10Gb SFP+ uplinks each
  - 8 switches supported in stack (320Gb stacking backplane)
  - Redundant PSU/Fan (hot swap)
  - Redundant Layer 3 uplinks to Tech. Center
  - Premium license (OSPF)
- ICX 6450-48P switches used for IDF
  - 18x 48 ports 10/100/1000 Cu PoE+
  - 2x 24 ports 10/100/1000 Cu PoE+
  - 1x 12 port 10/100/1000 4x PoE
  - 4 1/10Gb SFP+ uplinks (2 enabled for 10Gb by default)
  - 8 members supported in a stack (20Gb stacking backplane)
  - Integrated PSU/Fans (PSU not redundant)
  - Two 10Gb ports used for stacking/uplink as needed
  - Redundant Layer 2 uplinks to MDF as needed
- MDF Available ports for expansion
  - 6 1/10Gb SFP total
- Optic counts
  - 16 + 2 (spare) 10Gb MMF LRM (10Gb IDF)
  - 16 + 2 (spare) 1Gb MMF SR (1Gb IDF)
  - 15 + 1 (spare) 10Gb 1m Twinax cable (stack)
  - 2 10Gb SMF LR (WAN)
- License counts
  - ICX 6610 10Gb (block of 4) – 3
  - ICX 6610 Premium – 3
  - ICX 6450 10Gb (block of 2) – 8
  - ICX 6450 Premium - 2

Appendix B

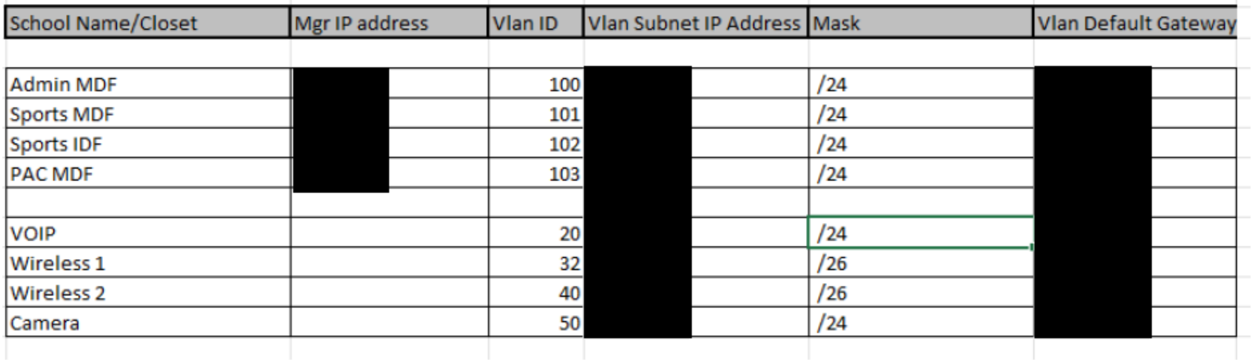
IP Addresses and VLANs



School Name/Closet	Mgr IP address	Vlan ID	Vlan Subnet IP Address	Mask	Vlan Default Gateway
Technology	[redacted]	101	[redacted]	/24	[redacted]
			[redacted]		[redacted]
VOIP		20	[redacted]	/24	[redacted]
Wireless 1		32	[redacted]	/26	[redacted]
Wireless 2		40	[redacted]	/26	[redacted]
Camera		50	[redacted]	/24	[redacted]



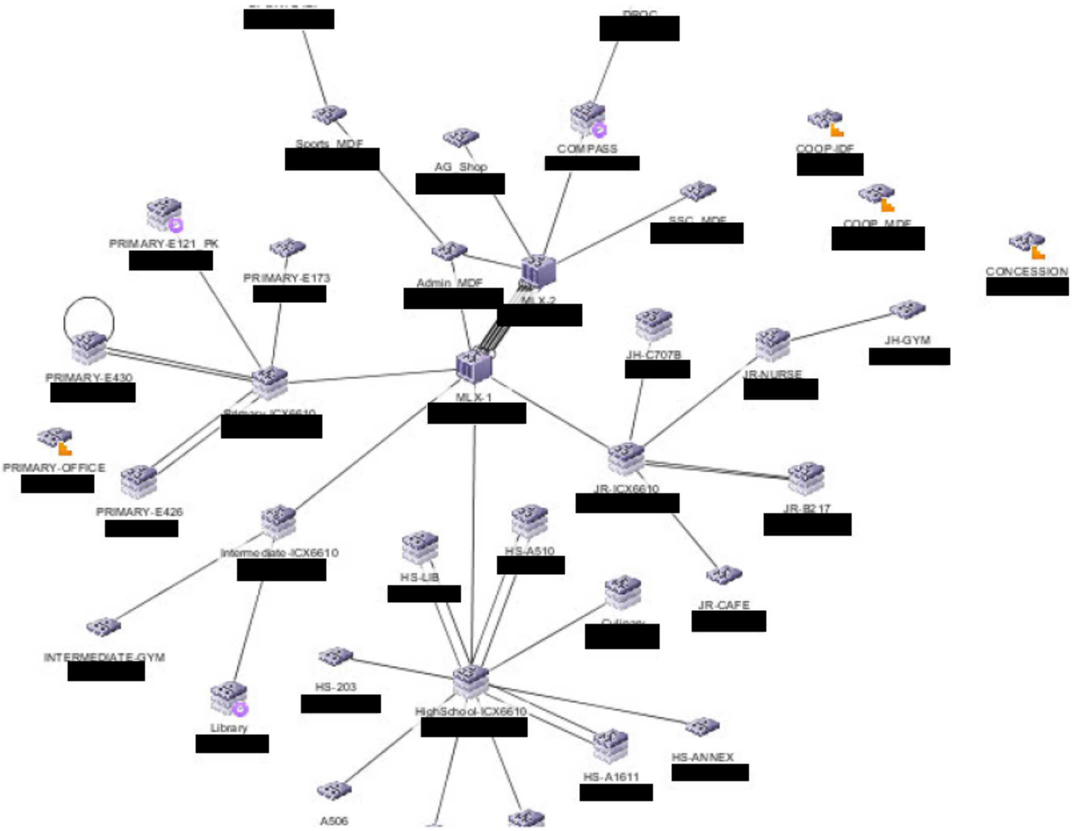
School Name/Closet	Mgr IP address	Vlan ID	Vlan Subnet IP Address	Mask	Vlan Default Gateway
High School MDF	[redacted]	100	[redacted]	/24	[redacted]
High School Library	[redacted]	101	[redacted]	/24	[redacted]
High School A1611 Storage	[redacted]	102	[redacted]	/24	[redacted]
High School A510	[redacted]	103	[redacted]	/24	[redacted]
High School A114	[redacted]	104	[redacted]	/24	[redacted]
High School Café	[redacted]	105	[redacted]	/24	[redacted]
High School Annex	[redacted]	106	[redacted]	/24	[redacted]
High School Auto	[redacted]	107	[redacted]	/24	[redacted]
High School A304	[redacted]	108	[redacted]	/24	[redacted]
High School A1021	[redacted]	109	[redacted]	/24	[redacted]
High School ROTC	[redacted]	110	[redacted]	/24	[redacted]
High School Book Room	[redacted]	111	[redacted]	/24	[redacted]
High School ART	[redacted]	112	[redacted]	/24	[redacted]
High School Cate Lab	[redacted]	112	[redacted]	/24	[redacted]
			[redacted]		[redacted]
VOIP		20	[redacted]	/24	[redacted]
Wireless 1		32	[redacted]	/26	[redacted]
Wireless 2		40	[redacted]	/26	[redacted]
Camera		50	[redacted]	/24	[redacted]

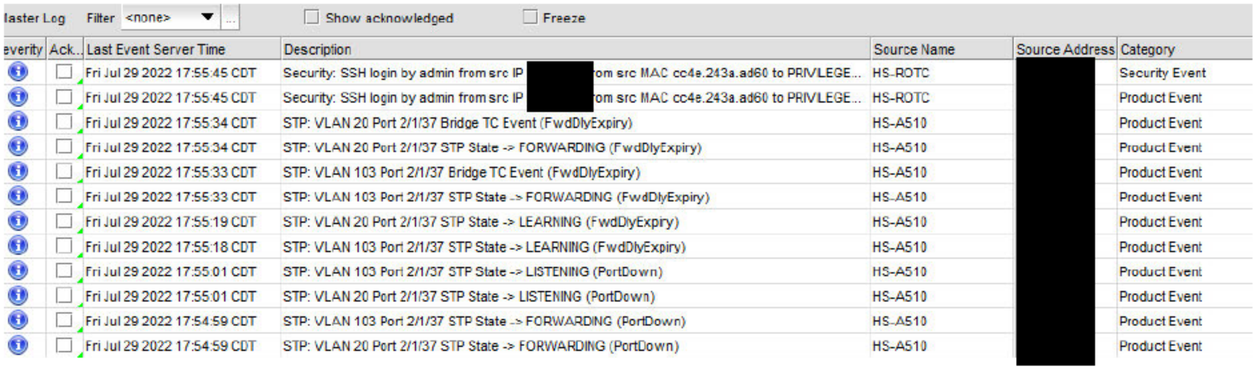


School Name/Closet	Mgr IP address	Vlan ID	Vlan Subnet IP Address	Mask	Vlan Default Gateway
Admin MDF	[redacted]	100	[redacted]	/24	[redacted]
Sports MDF	[redacted]	101	[redacted]	/24	[redacted]
Sports IDF	[redacted]	102	[redacted]	/24	[redacted]
PAC MDF	[redacted]	103	[redacted]	/24	[redacted]
			[redacted]		[redacted]
VOIP		20	[redacted]	/24	[redacted]
Wireless 1		32	[redacted]	/26	[redacted]
Wireless 2		40	[redacted]	/26	[redacted]
Camera		50	[redacted]	/24	[redacted]

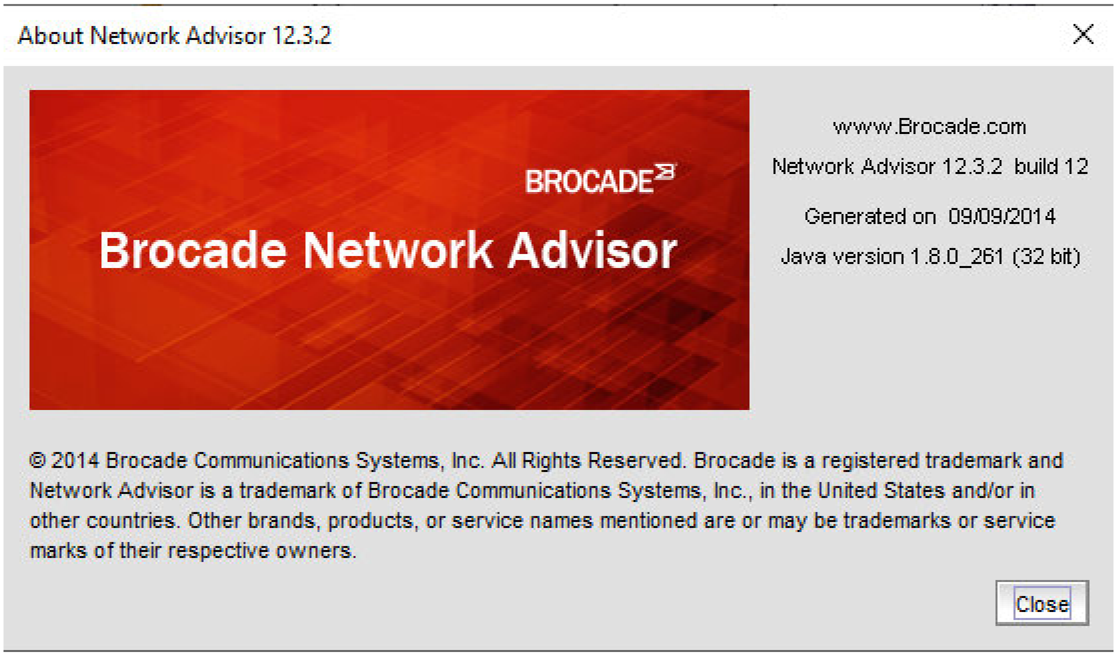
Appendix C

Network Monitoring Screenshots





everity	Ack...	Last Event Server Time	Description	Source Name	Source Address	Category
ⓘ	□	Fri Jul 29 2022 17:55:45 CDT	Security: SSH login by admin from src IP [redacted] om src MAC cc4e.243a.ad60 to PRIVLEGE...	HS-ROTC	[redacted]	Security Event
ⓘ	□	Fri Jul 29 2022 17:55:45 CDT	Security: SSH login by admin from src IP [redacted] om src MAC cc4e.243a.ad60 to PRIVLEGE...	HS-ROTC	[redacted]	Product Event
ⓘ	□	Fri Jul 29 2022 17:55:34 CDT	STP: VLAN 20 Port 2/1/37 Bridge TC Event (FwdDlyExpiry)	HS-A510	[redacted]	Product Event
ⓘ	□	Fri Jul 29 2022 17:55:34 CDT	STP: VLAN 20 Port 2/1/37 STP State -> FORWARDING (FwdDlyExpiry)	HS-A510	[redacted]	Product Event
ⓘ	□	Fri Jul 29 2022 17:55:33 CDT	STP: VLAN 103 Port 2/1/37 Bridge TC Event (FwdDlyExpiry)	HS-A510	[redacted]	Product Event
ⓘ	□	Fri Jul 29 2022 17:55:33 CDT	STP: VLAN 103 Port 2/1/37 STP State -> FORWARDING (FwdDlyExpiry)	HS-A510	[redacted]	Product Event
ⓘ	□	Fri Jul 29 2022 17:55:19 CDT	STP: VLAN 20 Port 2/1/37 STP State -> LEARNING (FwdDlyExpiry)	HS-A510	[redacted]	Product Event
ⓘ	□	Fri Jul 29 2022 17:55:18 CDT	STP: VLAN 103 Port 2/1/37 STP State -> LEARNING (FwdDlyExpiry)	HS-A510	[redacted]	Product Event
ⓘ	□	Fri Jul 29 2022 17:55:01 CDT	STP: VLAN 103 Port 2/1/37 STP State -> LISTENING (PortDown)	HS-A510	[redacted]	Product Event
ⓘ	□	Fri Jul 29 2022 17:55:01 CDT	STP: VLAN 20 Port 2/1/37 STP State -> LISTENING (PortDown)	HS-A510	[redacted]	Product Event
ⓘ	□	Fri Jul 29 2022 17:54:59 CDT	STP: VLAN 103 Port 2/1/37 STP State -> FORWARDING (PortDown)	HS-A510	[redacted]	Product Event
ⓘ	□	Fri Jul 29 2022 17:54:59 CDT	STP: VLAN 20 Port 2/1/37 STP State -> FORWARDING (PortDown)	HS-A510	[redacted]	Product Event



About Network Advisor 12.3.2

www.Brocade.com
Network Advisor 12.3.2 build 12
Generated on 09/09/2014
Java version 1.8.0_261 (32 bit)

© 2014 Brocade Communications Systems, Inc. All Rights Reserved. Brocade is a registered trademark and Network Advisor is a trademark of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned are or may be trademarks or service marks of their respective owners.