Network Design for Providence Medical Center

Joshua Marzan

Daniel Rivera

Miami Dade College

Professor Juan Avila

Dec. 9, 2023

Table of Contents

8.2 Routers (Core Layer)

8.3 Layer 3 Switch (Distribution Layer)

8.4 Layer 2 Switch (Access Layer)

8.5 Access Points

8.6 Servers

8.7 Uninterruptible Power Supply

8.8 Server Racks & Cooling Systems

8.9 Internet of Medical Things

1. Introduction & Executive Summary

A recent cyber (ransomware) attack halted critical operations and negatively impacted network performance. The executives at Providence Medical Center asked us to accommodate the network infrastructure to meet cybersecurity best practices in lieu of the network and data breaches. The healthcare industry is driven by the evolution of information systems, the sensitive data of every patient and data of research conducted in the field, and the system's ability to protect stored data. To meet these demands, a new network will be implemented with industry standards pertaining to security and manageability.

Cybersecurity training will be issued to employees to keep the network safe from outside attacks. In addition, we also plan to improve the wireless connectivity throughout the hospital in case users besides employees and staff would like to have internet connection while visiting loved ones. These improvements will not only yield a more stable and safeguarded atmosphere for hospital operations, but add quality-of-life improvements for those who use the network. Ultimately, our plan is to implement a well-balanced secure network that will achieve four-nines availability and support our customers.

2. Goals & Objectives

2.1 Goals

1. A more educated and aware user base less prone to making mistakes that could pose harm to the network and sensitive information such as medical research and patient data.
2. A secure, reliable, and available network that will meet the needs of medical personnel, staff, and patients.
3. Improved overall customer satisfaction stemming from improved network performance.

2.2 Objectives

1. **Securing Network:** Putting measures into place that ensures secure access of network resources, ample access control for servers, and HIPAA compliance. Integrating firewalls, IPS, VPNs (for remote access), monitoring and logging, endpoint security applications. Configuring network segmentation, encryption, and strong passwords/authentication policies. As far as physical security goes, we plan to have security contractors hired to monitor the area and invest in port security mechanisms such as port locks for unused ports on access layer switches and cable locks on systems used by staff. Additionally, for access to our MDFs/IDFs we will implement a two-person integrity system with key cards with a configured range of 60 seconds - the time in which the second individual has to scan their card so access can be gained.
2. **Improving Network Design:** Changing network architecture to enable reliable, available, resilient access for authorized users and devices. Laying the groundwork for a scalable, user-friendly, redundant network for IT staff/ network administrators. Employing site surveys to eliminate dead zones, change access point placement, improve

signal strength to create a network that can be accessed across most sections of the campus. Focusing on network segmentation to increase performance among endpoints, visibility for the network administrators, and isolation of key services and endpoints. After restructuring the network, periodic site surveys will take place so we can remain informed of the status of the network throughout various areas of the Providence Medical Center and implement changes as needed.

3. **User Security Training:** We are going to develop a user training program to educate staff about the dangers of surfing the web, recognizing phishing attempts that may arise from their emails, and provide necessary procedures to take when coming into contact with threats to the network and sensitive information.
4. **Disaster Recovery Plan/Risk Assessment:** We will have a disaster recovery plan to detail the actions that will be taken in the case of a security breach (physical/cyber) or natural disaster (i.e. hurricanes) to reduce downtime and prevent data loss as much as possible given the potential circumstances. We will discover what the acceptable risks are and determine mitigations for unsolvable risks. The presence of uninterruptible power supplies will supplement the network to ensure services remain running.
5. **Availability:** Design and secure a network that is capable of four nines (99.99%) availability which would amount to 52 minutes of downtime per year - which would be an improvement for Providence Medical Center.
6. **Inventory Tracking:** We will design an inventory system so we could keep track of all the devices that are critical to the infrastructure and provide effective maintenance.

3. Scope of Work

Our scope of work will be constrained to only one medical facility (Providence Medical Center). Executives, shareholders, and the board of directors should expect the project to be completed by the 15 month mark - by the end of Aug 2024 as we are essentially spearheading an overhaul of the network for the entire facility. Over the course of these 15 months, there will be several phases dedicated to the project's progress including assessing the network's current state and identifying areas for improvement, proposing a design and upgrade scheme, infrastructure upgrading (cabling, network devices), VLAN implementation and network segmentation, and providing documentation to the eventual IT staff for monitoring purposes and providing user training for the staff that will use the network. The network will accommodate the needs of 2000 employees including the physicians, nurses, technicians, and several others. Additionally, the network will be able to accommodate 500 patients and a family member of each patient. This accounts for an additional 500 users on the guest network segment - although we expect that we won't reach capacity on the guest network segment due to the more important circumstances that are presented with individuals when they come to a hospital in general.

3.1 Employee Description

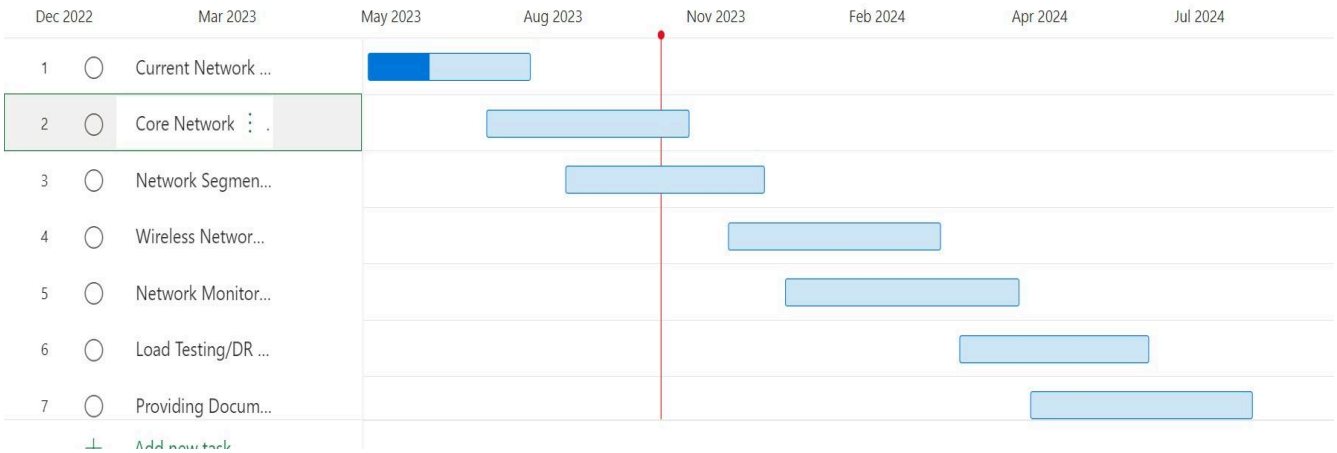
Personnel	
Employee Roles	**Number of Employees**
Doctors, Nurses, Students, Residents, Physical Therapists, Social Workers	**1700**
Janitors	**20**
IT	**20**
Clerical	**10**

Personnel	
Board of Directors/Legal/Admin	**30**
Billing	**25**
HR	**25**
Security	**30**

4. Project Timeline

Phase	**Start Date**	**End Date**	**Duration**
Phase 1 - Current Network Assessment, Design Proposal, Decommissioning	6/01/2023	8/23/2023	84 days
Phase 2 - Network Infrastructure Upgrades, Construction (Placement, Wiring)	8/01/2023	11/13/2023	105 days
Phase 3 - VLAN Implementation/Network Segmentation	9/11/2023	12/22/2023	103 days
Phase 4 - Wireless Network Enhancement	12/4/2023	3/22/2024	110 days
Phase 5 - Network Monitoring/Identifying Observability Gaps	1/2/2024	5/1/2024	121 days
Phase 6 - Load Testing/DR Exercises/Network Assessment	4/1/2024	7/8/2024	99 days

Phase 7 - Providing Documentation/Initial Runbooks, Training Program	5/8/2024	8/30/2024	115 days



4.1 Phase Details

Phase 1 of the project is essentially where the foundation will be laid with the board of directors, discussions of decommissioning legacy infrastructure, and an assessment of the network at its current stage will take place. Here we will also introduce our network design and our vision for the future of Providence Medical Center. Once approved, we will begin ordering the new equipment needed to upgrade the infrastructure according to our plans. While we are going through these preliminary activities, there will be a user migration (to another medical center) taking place as the facilities in the hospital will not be cleared for activity until the late stages of the project - approximately a year from the start of the project.

Phase 2 of the project is where the network infrastructure we ordered will start to come into play and the infrastructure upgrades will begin to take place. However, before installation of

the new equipment some construction must take place to accommodate the wiring needed for the network and create space for the infrastructure. Raised floors and fake ceilings will play an essential role in providing the space for the routing of the cabling along with PVC pipes and plenum-shielded cabling. This will allow for the wiring to remain untouched throughout the hospital which will prove to be beneficial as the less that the cables are touched, the slower it will take for them to degrade.

Phase 3 heavily involves the process of segmenting the network and implementing VLANs with the newly installed infrastructure. This is where we will execute a significant portion of the HIPAA/ePHI guidelines to make sure our legal requirements are met and the data of our customers remains secure.

The fourth phase is where site surveys will take place to see where improvements could be made in the wireless network. The site surveys will provide a gauge as to where access points could be added to provide sufficient coverage or if existing access points could be moved to a better spot to provide better coverage to users. Enhancements to the wireless network could also prove to be beneficial as IoMT devices will be used throughout the network for various purposes to service patients and relay health information to medical professionals.

The fifth and sixth stages are particularly crucial to the project as they serve the purposes of verifying the network works and give indications as to where improvements can be made after installation and implementation of the network. It is key to note that despite their ending dates in the project timeline, these phases never actually end because no network design is perfect - there are always adjustments that can be made to better accommodate the customers and assist them in their goals. These phases essentially highlight the importance of those periodic site surveys and

failover/disaster recovery (DR) test scenarios because it is realistic for such scenarios to come into fruition at one point or another.

These phases lead into the last portion of the project which is providing documentation and standard operating procedures. Documentation is everything in essentially any field that we work in and if created with clarity and detail, it can serve as a sufficient guide to address various scenarios and issues that may arise. Runbooks are a subset of documentation that is typically used in engineering/networking environments as they are valuable assets that enhance consistency, efficiency, and knowledge sharing within large organizations and corporate environments.

5. Technical Requirements

Scalability: user data, devices on networks, more sites

Availability: network redundancy across all major switches, diesel generators powering server room in case of outages,

Network Performance: 5Gbps bandwidth to allow for video calls, EHR search/transfer, real time image transfer (XRay/MRI), administrative work. 2nd ISP for network redundancy between sites

Security: HIPAA/ePHI framework, best practice for patching

a. Encryption: electronic health records (Ataman, A. 2023), patient monitoring devices, wireless
b. Access Control: accessing EHR, network resources, data files based on the principle of least privilege
c. Monitoring: server and database access, WLAN access, network
d. Employee Training: Cybersecurity training, KnowBe4 phishing attempts
e. Endpoint Protection: SentinelOne Antivirus Software, Fortinet Firewalls
f. Physical Security: locking ports, restricting access to server room, keycard access
g. Quarterly Meetings with IT Team: Pen Testing, improving security, planning out meetings

Manageability: track network changes, implementing patching schedule

6. Feasibility Analysis

6.1 Budget

Taking into consideration the extent of overhauling that will be done, the budget for $16 million. This includes the cost of hardware, implementation of equipment, software licensing, contractors working on the project, and other miscellaneous items. For a network that is being revamped to improve network performance and improve all-around security, this is feasible especially considering how much is spent on maintaining IT operations in this kind of environment.

NetShark Innovators Budget				
Equipment	**Model**	**Unit Price**	**# of units**	**Total**
Firewall	Fortinet FG-900G	887.99	8	7,103.92
Router	Cisco ASR 1002-HX Router	109,728.99	8	821,831.92
Multilayer SW	Cisco Catalyst 9600 Series Switch	7505.5	12	90,066
Access SW	Cisco Catalyst 9300 Series Switch	6939.99	40	277,590.60
APs	Cisco Catalyst 9166 Series APs	1685.99	96	323,710.08
Servers	Dell PowerEdge Rack Server R760	10,528.27	15	157,924.05
Racks	Vertiv VR Racks	2695.99	4	10,783.96
Enclosure	Vertiv SmartAisle	20,000	1	20,000
Cooling	Liebert Mini-Mate Precision Cooling	9,000	4	36,000
Badge Access System	HID Access Control	10,000	4	40,000
Remote User Monitoring	RocketCyber	7.95	2000	15,900
Remote Management Software	Kaseya	8.95	2500	22,362.50
Cybersecurity Training	KnowBe4	17.16	2000	343,202
Endpoint Protection	SentinelOne	45	600	27,000
Producitivity Application	Office 365 E3	23	2000	46,000
Windows Enterprise	Enterprise Volume Licensing	120	2000	2,000
AWS Various Service Hosting	Web/DNS/Backup	2,000,000	1	2,000,000
Microsoft Azure	Active Directory Domain Services	300,000	1	300,000
AT&T Dedicated Business Ethernet	Internet Service Provider	3420	4	13680
Comcast Ethernet Services	Internet Service Provider	2400	4	9600
			Year One Cost	**4,564,755.03**
			Maintenance	**2,779,744.50**

6.2 Legal and Compliance Considerations

Accounting for the fact that we will be handling patient data and research information, we will need to make sure our design meets HIPAA regulations and is compliant with the ePHI framework. HIPAA regulations outline that there are 18 various demographics that can identify a patient ranging from name, addresses, social security numbers, medical records, emails and much more (Berkeley, n.d.). With hashing out access controls, security, and encryption - we can ensure this project will be feasible in this regard.

6.3 Risk Assessment and Matrix

With handling such data and working in a facility where availability of services is paramount, several risks must be addressed and considered in the design scheme. Risks that have been identified that could have detrimental effects on availability are physical access control, cybersecurity threats, natural disasters (due to location in FL), drive failures for storage devices, switch failures, and power outages. The impact that these events could yield and the likelihood that they will occur are noted in the risk assessment diagram below.

Risk	Probability level (1-5)	Impact level (1-10)	Risk level (1-20)	Mitigation	Rating
Risk 1: Singular router connected in each buildings	2	5	10	Network redundancy - backup routers in storage to replace faulty devices and cable is unlikely to go bad due to no contact (running through the ceilings of the building).	Medium high
Risk 2: Natural disaster	2	5	10	Having UPSs on standby and battery backups for IT operations equipment. Additionally, implement a disaster recovery plan: SOPs, failover procedures. Given the location of the medical center, the likelihood that	Medium high

				something like this could occur is possible but the impact will be constrained to a medium level.	
Risk 3: Drive failure on storage devices	3	1	3	Spare drives will be ready; NAS will be hot-swappable.	Low
Risk 4: Power outage	2	4	8	Mitigation steps are similar to what is seen for the 2nd risk	Medium
Risk 5: Switch failure	2	3	6	Have a hot spare on deck and ready to swap in for the faulty switch.	Medium low
Risk 6: One ISP goes down	2	4	8	Contact the ISP for support but failover to secondary ISP in the meantime.	Medium
Risk 7: Physical access control	2	5-10 (depending on what is accessed	10-20 (depending on what is accessed)	Security personnel, port/cable locks, TPI locks with badge access. The PCs would have port and cable locks as well and settings would be configured for them to lock after inactivity after a short period.	High to Critical

Risk 8: User falls for phishing attempt	1	6	6	Disconnect device from network, run antivirus /anti-malware scan, and change information if necessary	Medium low

Note: (green - low, light green - low medium, yellow - medium, orange - medium high, red - high)

1. Risk: Singular router connected in each of the buildings Mitigation: Network redundancy - backup routers in storage to replace faulty devices and cable is unlikely to go bad due to no contact (running through the ceilings of the building).
2. Risk: Natural disaster. Mitigation: Having UPSs on standby and battery backups for IT operations equipment to make sure our monitoring stays online. Additionally, we would have a disaster recovery plan highlighting SOPs, failover procedures and detailing what departments would have priority service in this scenario. Given the location of the medical center, the likelihood that something like this could occur is possible but the impact will be constrained to a medium level.
3. Risk: Drive failure for storage devices. Mitigation: Spare drives will be ready; NAS will be hot-swappable. We are aiming for minimal server downtime and low resource use while the drive replication is taking place. The likelihood that drive failures would occur is possible and impact would be low due to the SOPs we have in place. However we must keep in mind the proper procedures we must follow to properly dispose of the drive within HIPAA compliance standards.

4. Risk: Power outage. Mitigation: Having UPSs on standby and battery backups for IT operations equipment to make sure our monitoring stays online. Additionally, we would have a response plan highlighting standard operating procedures and detailing what departments would have priority service in this scenario. Likelihood that this occurs is low but the impact could range from medium high to critical depending on the time such an event would occur.
5. Risk: Switch failure. Mitigation: Have a hot spare on deck and ready to swap in for the faulty switch. Likelihood that this will occur is unlikely but the impact would be medium because although operations for the affected network that supports a particular department would cease, the substitution would be quick. Additionally, there would be alerting/monitoring in place to provide a notification on a device's health.
6. Risk: One ISP goes down. Mitigation: Contact the ISP for support but failover to secondary ISP in the meantime.
7. Risk: Physical access control. Mitigation: Security personnel, port/cable locks, TPI locks with badge access. The PCs would have port and cable locks as well and settings would be configured for them to lock after inactivity after a short period. The likelihood that anyone will gain access to any network devices is very unlikely considering their secure placement. However, if an unauthorized figure gained access to any devices, the event could yield a medium-level impact.
8. Risk: User falls for phishing attempt. Mitigation: User training and regular cybersecurity/phishing exercises will be sent to employees to remind and educate them on the dangers of clicking on unknown links and identifying potential threats. Despite

these measures being put in place, if a user succumbs to phishing it could result in a medium level impact given the kind of information an attacker could gain access to.

6.4 Market Research

According to Definitive Healthcare, the average IT operating expense budget across over 4500 hospitals is approximately $8.4 million. Given the kind of project we are undertaking which involves decommissioning old devices and replacing it with new infrastructure, the budget for this project is well into the millions with $8 million.

6.5 Technical/Resource Feasibility

The technical requirements have been outlined in our scope of work and they coincide with what we need in regards to resources to ensure this project's completion will be feasible. Given the nature of what we are working with, we will need to make sure our network is available, secure, redundant, and able to be monitored and patched with efficiency. This means we will need to have the best devices/equipment to implement with the network, sufficient encryption to ensure data remains secure and also ensure that the network performance remains optimal (the monitoring aspect). With the selection of devices we will have at our disposal, the ground we need to cover (as far as connections go), and the cooperation of our partners (ISPs, ServiceNow, AWS, various contractors) we can ensure the technical aspect of this project is feasible.

6.6 Overall Feasibility Assessment

With the several aspects of this project considered, we at NetShark Innovators wholeheartedly believe this project is feasible and will be able to be completed within the 15-month deadline. As stated above, we have a plan to provide a suite of deliverables that will ensure increased network performance, increased security, a redundant and available network along with tools for monitoring and training to support it, and a program that will be used to educate the staff on best practices to use when utilizing the network.

7. Providence Medical Center - Network Design

7.1 Physical Topology

7.1.1 Cabling Methods

The plan with cabling is to have two ISPs contribute to providing our connections via fiber to the Internet for the sake of meeting our redundancy and availability requirements. Those connections the ISPs are providing will also have some presence on the core layer as we employ a network model reminiscent of hub and spoke. Between routers on the core layer, there will be two connections supported respectively by the ISPs connecting our main routers of the building to the Internet.We will be utilizing Cat6a cabling on the core layer On the distribution layer of our topology, we will continue to utilize Cat6a Ethernet cabling to the network for the router to multilayer switch connections. Beyond that, we are going to implement Cat6a Ethernet cabling between the distribution layer and the access layer. Then we will shift to utilizing Ethernet cabling once we get to the distribution layer and connect to the access layer switches since those will be in the same rooms physically. From there, we will run our Ethernet cabling through the ceilings/floor which will be protected by plenum/PVC pipes to allow for our devices to connect to the network.

7.1.2 MDF/IDF Layout & Floor Plan (Sample)

In our network, we will have main distribution frame (MDF) rooms in each of the buildings and two intermediate distribution frame (IDF) rooms in each of the buildings to complement the MDFs and the connections that are terminated in those MDFs. This will allow us to efficiently facilitate connections between each of the buildings for the private networks but also allow for a

structured routing approach for connections to the Internet and the various network services hosted by our vendors (Amazon, Microsoft, and RingCentral).

Below is a sample of our floor plans which represents a general idea of how things would be set up from a physical standpoint. The blue dots in the image represent where the ethernet (Cat6a cabling) drops would be in this building (building 3 - West general patient wing, first floor). The drops would allow the thin clients PCs to be connected physically to the network. The black rectangle shows where our MDF would be located and from there, the Ethernet cabling would be run through the ceilings and the floors utilizing plenum shielding along with PVC pipes to prevent physical damage to the cabling as they are routed throughout the building..

7.1.3 Server/Network Rooms

This will be hosted in building and it will contain essential servers that will host various mission critical applications and services such as our DMZ to act as a protection boundary for the network, the web servers to allow for customers/patients to inquire about the medical center's services. Additionally, this space will also include our domain controllers, file servers (for in-house storage purposes), and Hyper-V servers that will host the applications needed to best care for patients and update their information seamlessly.

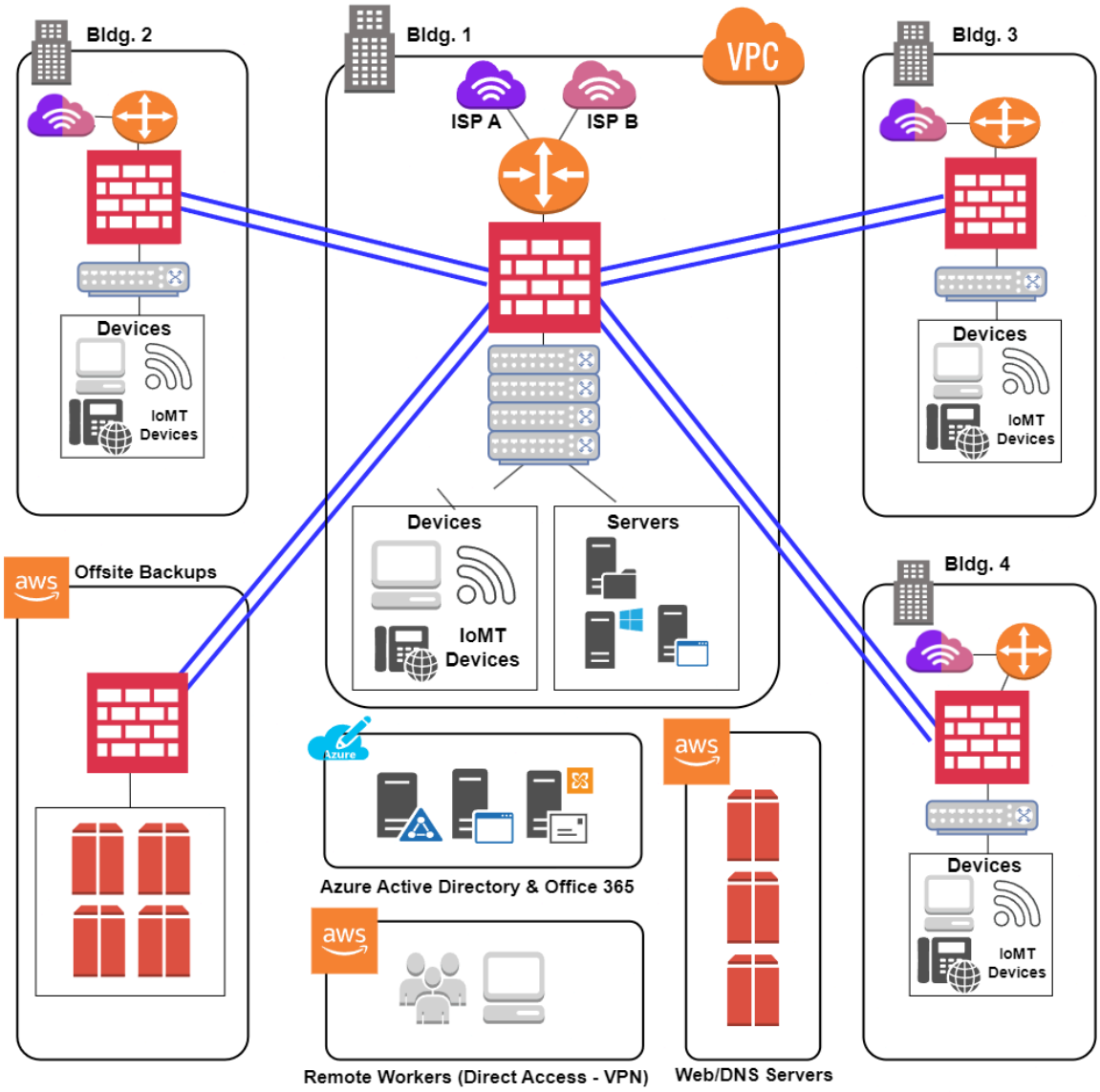
7.1.4 Access Point Deployments

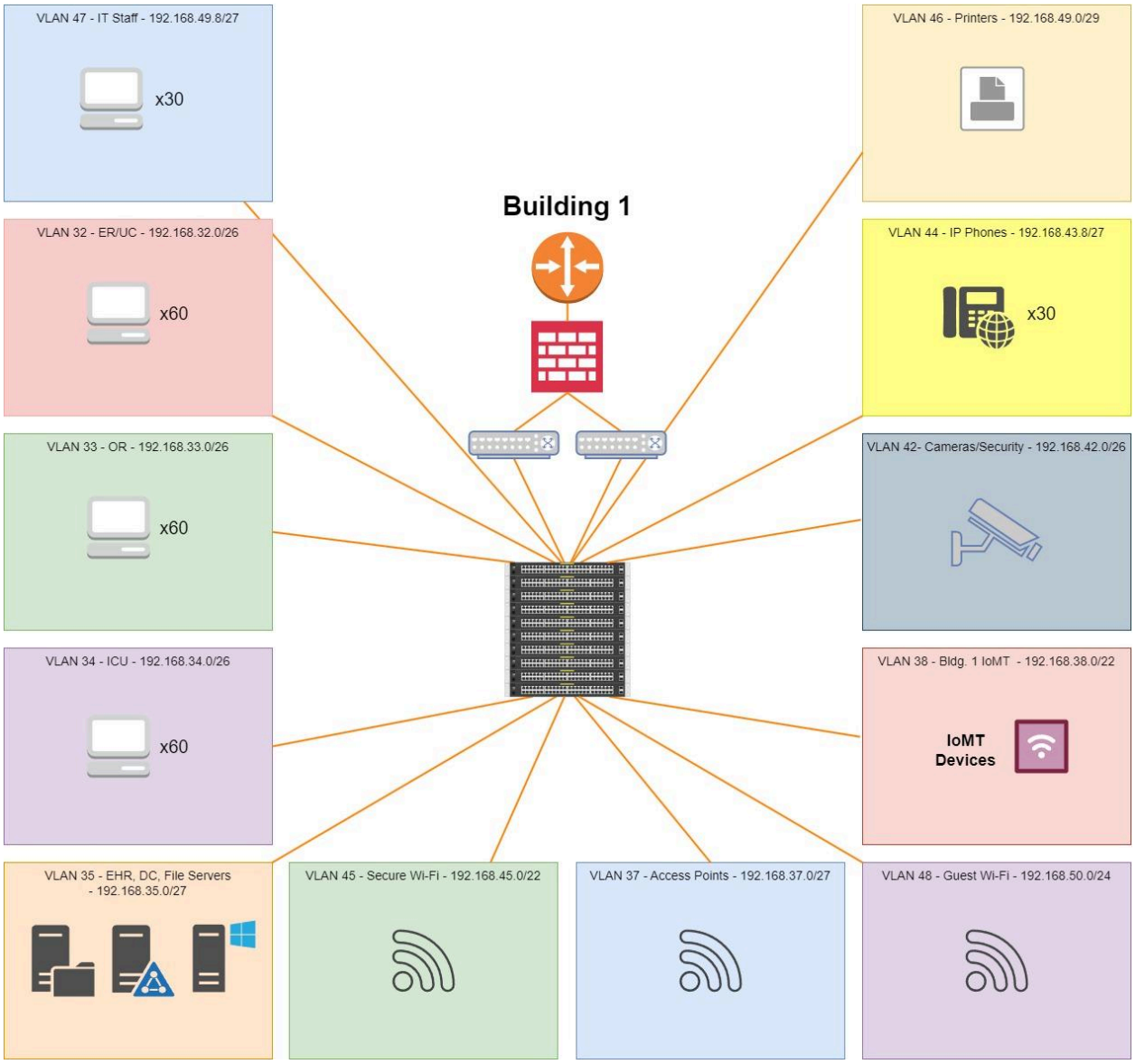
For our access point deployments, we are looking at six APs per wing as that will allow for devices to provide services whilst being mobile. This will prove to be beneficial in areas of the hospital where mobility is paramount like the ER and the ICU. In less-resource intensive areas like the Therapy section or the HR department, there will be less APs on the floor (three in this case) as the demand for resources in those areas is not as high compared to how it is in mission-critical areas of the facility. Access points will also be the point of connection for users to access the guest Wi-Fi if they desire as they await the status of their family members or if they are patients themselves.

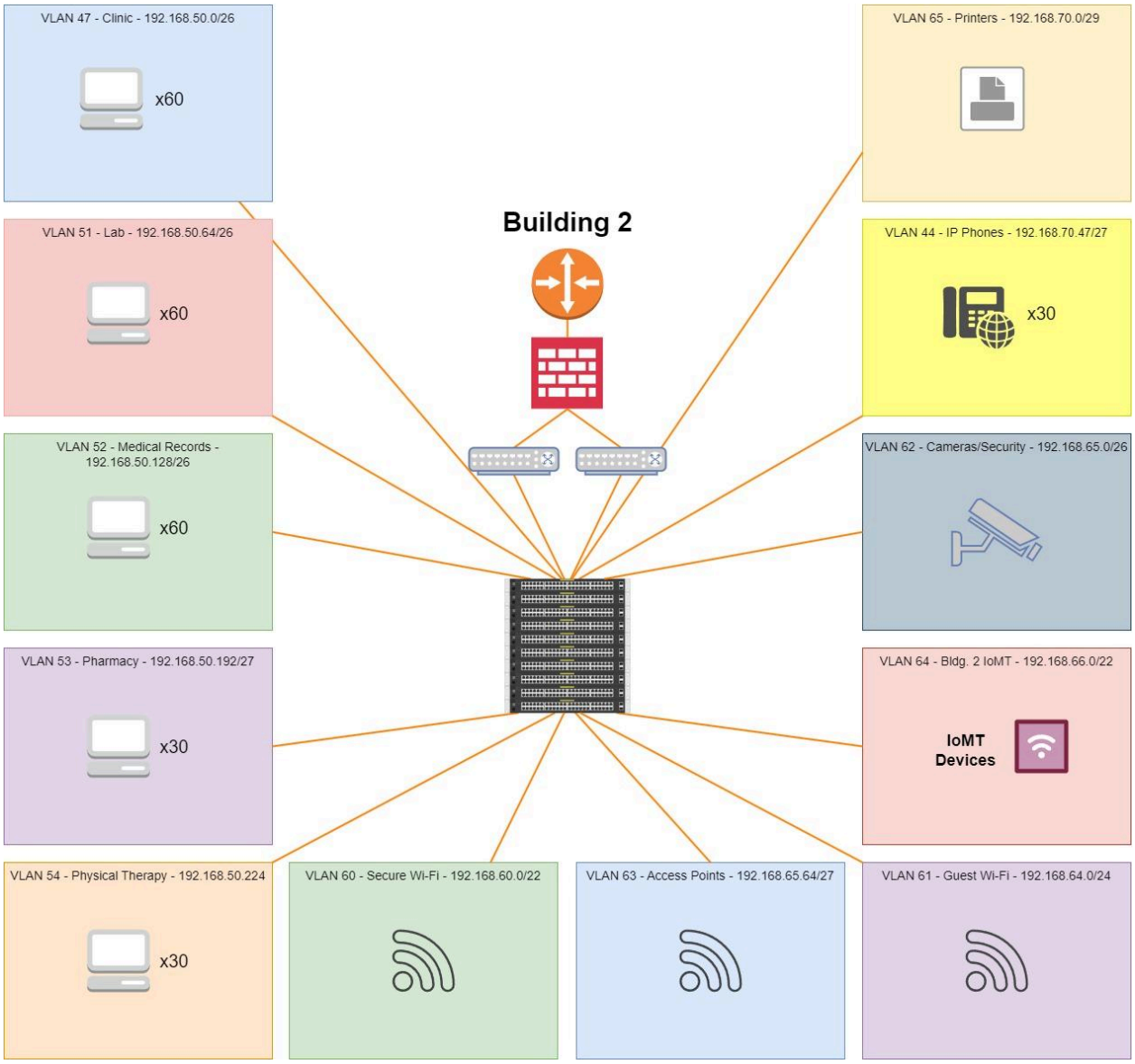
7.2 Logical Topology

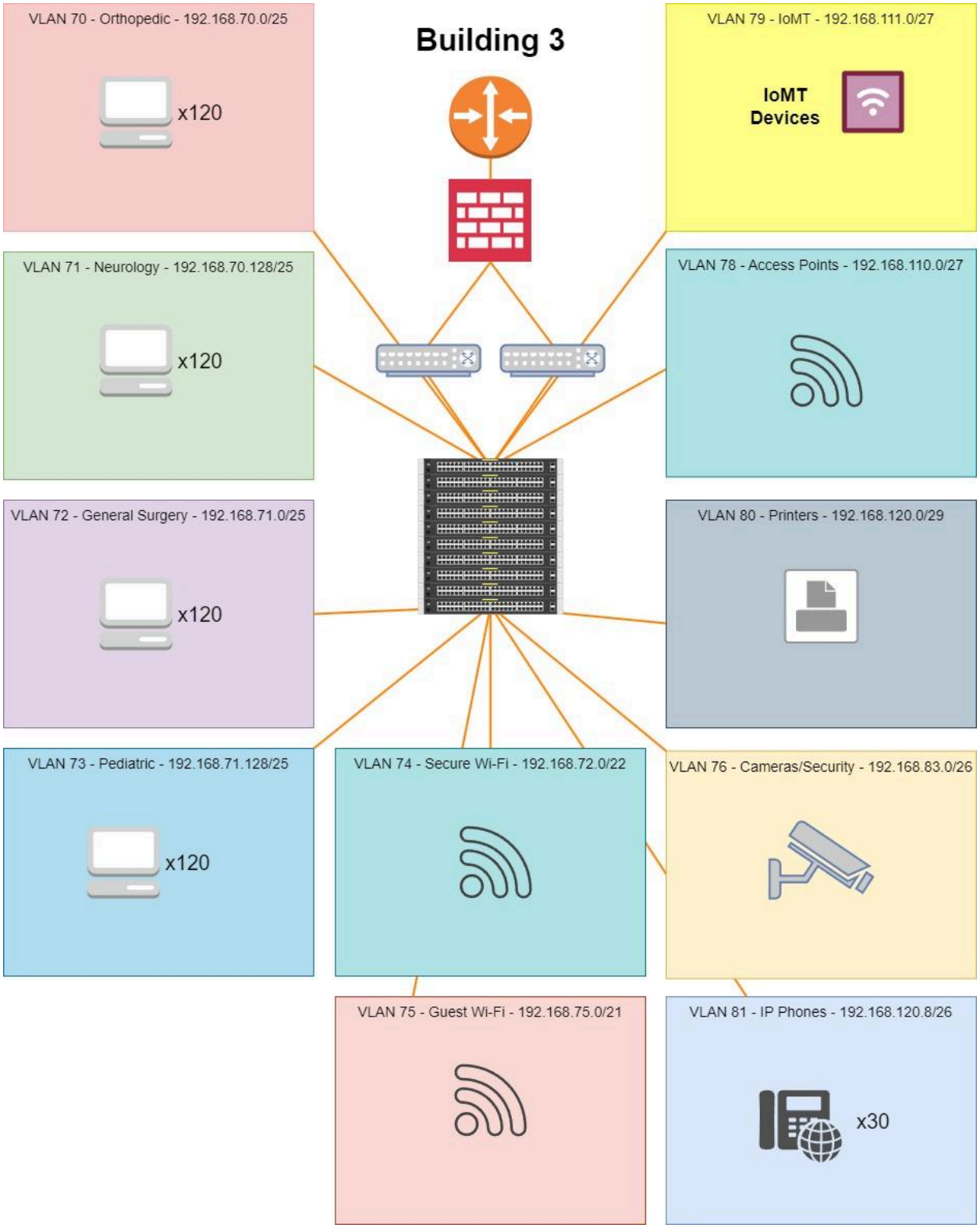
Our topology is based on a hub-and-spoke approach, where the hub (Building 1) houses the main firewalls, servers, and IT staff. The spokes are the secondary buildings (Buildings 2, 3, and 4), where a site-to-site VPN is implemented between the main FortiGate firewall at Building 1 and the secondary location's firewall. For more information on security implementations, see section 7.4 "Security Controls & Implementations".

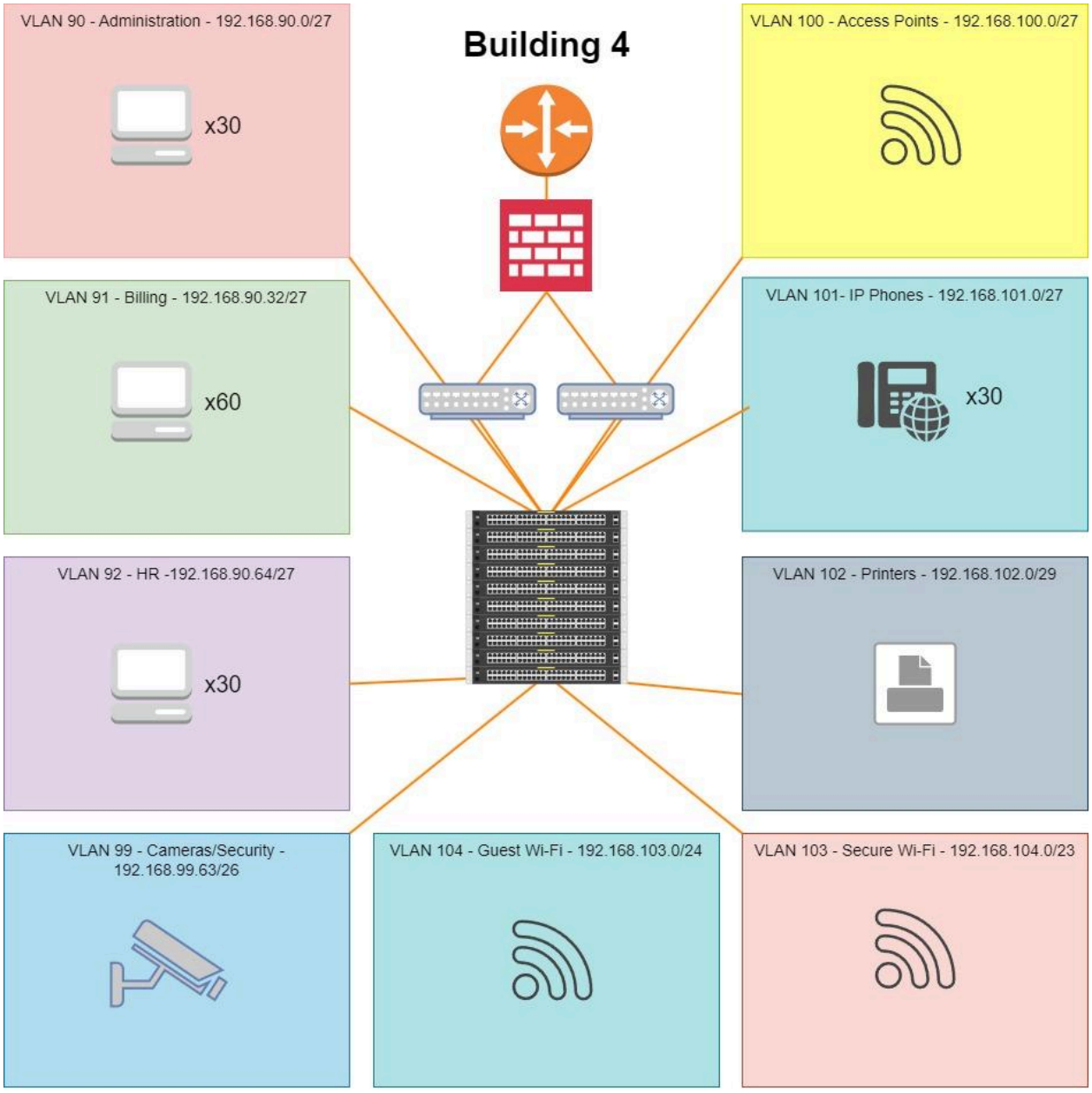
Overall Topology




VLAN 47 - IT Staff - 192.168.49.8/27
x30
VLAN 46 - Printers - 192.168.49.0/29
Building 1
VLAN 32 - ER/UC - 192.168.32.0/26
x60
VLAN 44 - IP Phones - 192.168.43.8/27
x30
VLAN 33 - OR - 192.168.33.0/26
x60
VLAN 42- Cameras/Security - 192.168.42.0/26
VLAN 34 - ICU - 192.168.34.0/26
x60
VLAN 38 - Bldg. 1 IoMT - 192.168.38.0/22
IoMT Devices
VLAN 35 - EHR, DC, File Servers - 192.168.35.0/27
VLAN 45 - Secure Wi-Fi - 192.168.45.0/22
VLAN 37 - Access Points - 192.168.37.0/27
VLAN 48 - Guest Wi-Fi - 192.168.50.0/24


VLAN 47 - Clinic - 192.168.50.0/26
x60
VLAN 65 - Printers - 192.168.70.0/29
Building 2
VLAN 51 - Lab - 192.168.50.64/26
x60
VLAN 44 - IP Phones - 192.168.70.47/27
x30
VLAN 52 - Medical Records - 192.168.50.128/26
x60
VLAN 62 - Cameras/Security - 192.168.65.0/26
VLAN 53 - Pharmacy - 192.168.50.192/27
x30
VLAN 64 - Bldg. 2 IoMT - 192.168.66.0/22
IoMT Devices
VLAN 54 - Physical Therapy - 192.168.50.224
x30
VLAN 60 - Secure Wi-Fi - 192.168.60.0/22
VLAN 63 - Access Points - 192.168.65.64/27
VLAN 61 - Guest Wi-Fi - 192.168.64.0/24


Building 3
VLAN 70 - Orthopedic - 192.168.70.0/25
x120
VLAN 71 - Neurology - 192.168.70.128/25
x120
VLAN 72 - General Surgery - 192.168.71.0/25
x120
VLAN 73 - Pediatric - 192.168.71.128/25
x120
VLAN 74 - Secure Wi-Fi - 192.168.72.0/22
VLAN 75 - Guest Wi-Fi - 192.168.75.0/21
VLAN 76 - Cameras/Security - 192.168.83.0/26
VLAN 78 - Access Points - 192.168.110.0/27
VLAN 79 - IoMT - 192.168.111.0/27
IoMT Devices
VLAN 80 - Printers - 192.168.120.0/29
VLAN 81 - IP Phones - 192.168.120.8/26
x30


Building 4
VLAN 90 - Administration - 192.168.90.0/27
x30
VLAN 100 - Access Points - 192.168.100.0/27
VLAN 91 - Billing - 192.168.90.32/27
x60
VLAN 101- IP Phones - 192.168.101.0/27
x30
VLAN 92 - HR -192.168.90.64/27
x30
VLAN 102 - Printers - 192.168.102.0/29
VLAN 99 - Cameras/Security - 192.168.99.63/26
VLAN 104 - Guest Wi-Fi - 192.168.103.0/24
VLAN 103 - Secure Wi-Fi - 192.168.104.0/23

7.2.1 Addressing Scheme/Segmentation

Our addressing scheme will be based on the device class and/or the department of the corresponding device/user. There will be slight variation across the network due to the varying needs of the departments and their respective demands.

We will be using the 192.168.0.0/16 private IP address space. This allows us to have just a bit over 65,000 usable IP addresses to assign which would be enough to cover the PCs, IoT devices, APs, and medical devices on the premises. With this address range at our disposal, we employ the method CIDR across the entire network to allocate IP space for the buildings and their varying requirements based on the departments housed in them and account for the scenario in which the hospital needs to scale. In that case, we would still have several thousand addresses we could assign to devices that would potentially connect to the network which enable us to smoothly address this particular situation.

When it comes to network segmentation in this project, VLAN implementation is an essential component of that and it will allow us to remain HIPAA compliant in our design. Given that we are designing our network to secure sensitive information, each department will have its own designated VLAN and ACLs will be configured to prevent network traffic from flowing into the other departments containing that information.

7.2.2 Addressing Scheme for Building 1

VLAN	Subnet ID / Net Address	IP Address Range	Broadcast Address	Total # of Usable Hosts	Description
32	192.168.32.0	192.168.32.1 - 192.168.32.62 /26	192.168.32.63	62	ER/UC
33	192.168.32.64	192.168.32.65 - 192.168.32.126 /26	192.168.32.127	62	ICU
34	192.168.32.128	192.168.32.129 - 192.168.32.190 /26	192.168.32.190	62	OR
35	192.168.35.0	192.168.35.1 - 192.168.35.30 /27	192.168.35.31	30	EHR App/File Servers
37	192.168.37.0	192.168.37.1 - 192.168.37.30 /27	192.168.37.31	30	Bldg. 1 APs
38	192.168.38.0	192.168.38.1 - 192.168.41.254 /22	192.168.41.255	1022	IoMT Building 1
42	192.168.42.0	192.168.42.1 - 192.168.42.62 / 26	192.168.42.63	62	Building 1 Cameras/Security
43	192.168.43.0	192.168.43.1 - 192.168.43.6 /29	192.168.43.7	6	DHCP Servers
44	192.168.43.8	192.168.43.9 - 192.168.43.38 /27	192.168.43.39	30	IP Phones
45	192.168.45.0	192.168.45.1 - 192.168.48.254 /22	192.168.48.255	1022	Secured WiFi
46	192.168.49.0	192.168.49.1 - 192.168.49.6 /29	192.168.49.7	6	Printers
47	192.168.49.8	192.168.49.9 - 192.168.49.38 /27	192.168.49.39	30	IT
48	192.168.50.0	192.168.50.1 - 192.168.50.254 /24	192.168.50.255	254	Guest WiFi

7.2.3 Addressing Scheme for Building 2

VLAN	Subnet ID / Net Address	IP Address Range	Broadcast Address	Total # of Usable Hosts	Description
50	192.168.50.0	192.168.50.1 - 192.168.50.62 /26	192.168.50.63	62	Clinic
51	192.168.50.64	192.168.50.65 - 192.168.50.126 /26	192.168.50.127	62	Lab
52	192.168.50.128	192.168.50.129 - 192.168.50.190 /26	192.168.50.191	62	Medical Records
53	192.168.50.192	192.168.50.193 - 192.168.50.222 /27	192.168.50.223	30	Pharmacy
54	192.168.50.224	192.168.50.225 - 192.168.50.254 /27	192.168.50.255	30	Physical Therapy
60	192.168.60.0	192.168.60.1 - 192.168.63.254 /22	192.168.63.255	1022	Secured WiFi (For personnel)
61	192.168.64.0	192.168.64.1 - 192.168.64.254 /24	192.168.64.255	254	Guest WiFi
62	192.168.65.0	192.168.65.1 - 192.168.65.62 /26	192.168.65.63	62	Security/Cameras Building 2
63	192.168.65.64	192.168.65.65 - 192.168.65.94 /27	192.168.65.95	30	Access Points Building 2
64	192.168.66.0	192.168.66.1 - 192.168.69.254 /22	192.168.69.255	1022	IoMT Building 2
65	192.168.70.0	192.168.70.1 - 192.168.70.6 /29	192.168.70.7	6	Printers
66	192.168.70.8	192.168.70.9 - 192.168.70.14 /29	192.168.70.15	6	DHCP Servers
67	192.168.70.16	192.168.70.17 - 192.168.70.46 /27	192.168.70.47	30	IP Phones

7.2.4 Addressing Scheme for Building 3

VLAN	Subnet ID / Net Address	IP Address Range	Broadcast Address	Total # of Usable Hosts	Description
70	192.168.70.0	192.168.70.1 - 192.168.70.126 /25	192.168.70.127	126	Orthopedic
71	192.168.70.128	192.168.70.129 - 192.168.70.254 /25	192.168.70.255	126	Neurology
72	192.168.71.0	192.168.71.1 - 192.168.71.126 /25	192.168.71.127	126	General Surgery
73	192.168.71.128	192.168.71.129 - 192.168.71.254 /25	192.168.71.255	126	Pediatric
74	192.168.72.0	192.168.72.1 - 192.168.74.254 /22	192.168.74.255	1022	Secured WiFi (For personnel)
75	192.168.75.0	192.168.75.1 - 192.168.82.254 /21	192.168.82.255	2046	Guest WiFi
76	192.168.83.0	192.168.83.1 - 192.168.83.62 /26	192.168.83.63	62	Security/Cameras
78	192.168.110.0	192.168.110.1 - 192.168.110.30 /27	192.168.110.31	30	Access Points Building 3
79	192.168.111.0	192.168.111.1 - 192.168.118.254 /21	192.168 118.255	2046	IoMT Building 3
80	192.168.120.0	192.168.120.1 - 192.168.120.6 /29	192.168.120.7	6	Printers Building 3
81	192.168.120.8	192.168.120.9 - 192.168.120.38 /27	192.168.120.39	30	IP Phones Building 3

7.2.5 Addressing Scheme for Building 4

VLAN	Subnet ID / Net Address	IP Address Range	Broadcast Address	Total # of Usable Hosts	Description
90	192.168.90.0	192.168.90.1 - 192.168.90.30 /27	192.168.90.31	30	Admin
91	192.168.90.32	192.168.90.33 - 192.168.90.62 / 27	192.168.90.63	30	Billing
92	192.168.90.64	192.168.90.65 - 192.168.90.94 /27	192.168.90.95	30	HR
99	192.168.99.0	192.168.99.1 - 192.168.99.62 /26	192.168.99.63	62	Security/Cameras Building 4
100	192.168.100.0	192.168.100.1 - 192.168.100.30 /27	192.168.100.31	30	Access Points Building 4
101	192.168.101.0	192.168.101.1 - 192.168.101.30 /27	192.168.101.31	30	IP Phones
102	192.168.102.0	192.168.102.1 - 192.168.102.6 /29	192.168.102.7	6	Printers Building 4
103	192.168.103.0	192.168.103.1 - 192.168.103.254/24	192.168.103.255	254	Guest Wi-Fi Building 4
104	192.168.104.0	192.168.104.1 - 192.168.105.254 /23	192.168.105.255	510	Secure Wi-Fi

7.3 Scalability

Scalability is a huge factor for us to consider in the scenario that the medical center has a need to expand. As stated before, with the private address space we are using, we will be able to accommodate that need in the case that the facility needs to potentially add another two departments or if extra users are expected to use the network in the next few years. Additionally, all of the floors in each building will not be used so there will still be plenty of physical space to allow for additional infrastructure if needed.

7.4 Security Controls & Implementations

In Building One, we will implement two firewalls configured in an active/passive configuration. After we receive data from the ISP, we will connect to our router, then into our firewalls. The firewall we will be deploying is the FortiGate 900G, as it is the Gartner Magic Quadrant Leader for network firewalls and WAN edge infrastructure (Fortinet, 2023, page 1).

Our Intrusion Protection System (IPS) will be included in our Fortinet firewalls. The FortiGate IPS is software based, to allow possible scaling through virtual machines. The logic behind this choice is to allow for scaling our IPS, which will eliminate a possible bottleneck if too much traffic is being analyzed, which will slow down the total throughput.

7.4.1 Access Control

The privilege of least-access will be implemented to segment the network flow, limit the accessible data (File Servers) to each user, and to best comply with HIPAA regulations. Each department will only have access to its own shared drive: administered through a logon script based on the user's department in Active Directory. Specific folders are determined by least privilege as well, requests may be sent to the IT team to provide access only if absolutely necessary.

7.4.2 Encryption Methods

Data will be encrypted in transit using Advanced Encryption Standard (AES-256) over the network, and implementing Transport Layer Security (TLS) through HTTPS for accessing web-based applications and ePHI. Data at rest will be encrypted using Volume Encryption at the endpoint level. For remote access encryption, see the Remote access section below.

7.4.3 Staff Training

Considering the large amount of general staff in the hospital, regular cybersecurity training will be implemented through KnowBe4. KnowBe4 trains users to avoid clicking unknown links, further investigate the sender and their domains, and keeps users on their toes while live phishing attempts are sent throughout the ranks of the company directory. Active training on HIPAA compliance will be addressed in quarterly meetings to all medical staff who access medical records throughout the network.

Without strong leadership and direction, any group's ideals and goals will not be achieved. The current IT Director will appoint a HIPAA Compliance Officer to oversee that the proper measures are being taken to ensure HIPAA compliance across local backups, endpoints, and our network. Additional IT staff (system administrators, technicians, cloud architects) will be included in the HIPAA compliance training to ensure proper administration of best practices.

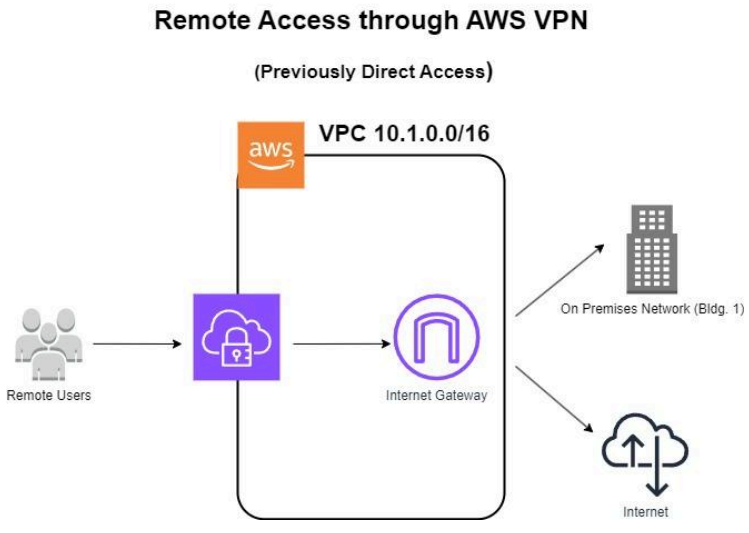
7.4.4 Physical Security

The main IT Room houses our server racks, network switches and firewalls and act as our Main Distribution Frame (MDF). The room is locked to the public, only accessible by personnel with the corresponding badge clearance. Our servers, switches, and local backups are locked to prevent tampering. Ports not in use will be closed to prevent security risks, manually opened when a new device needs a connection. Security cameras will be placed throughout the hospital to monitor personnel and in the server room to document anyone tampering with the server racks.

7.4.5 Remote Access

The previous IT administration team used Microsoft Direct Access to allow users to work remotely on company-provided devices. Currently, Microsoft recommends using another remote access solution over Direct Access (JasonGerend, *DirectAccess*). With that being said, we had to re-evaluate the current means of our remote access solution.

After careful consideration, remote access will be available through a Virtual Private Network administered by Amazon Web Services. VPNs make sure the data is encrypted when a user needs to work remotely and access the data within the hospital network.

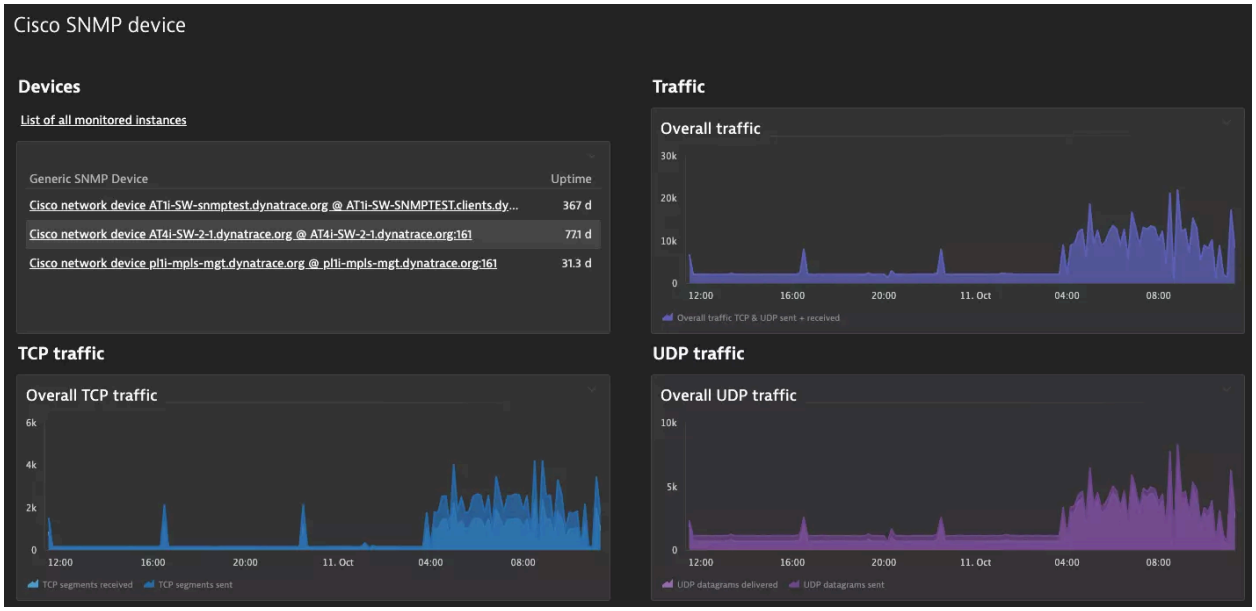


7.4.6 Wireless Network

Our wireless network (facing the client side) will be segmented through VLANs. Network segmentation will allow us to have a segregated network which has guest access separated from the main network which houses our servers.

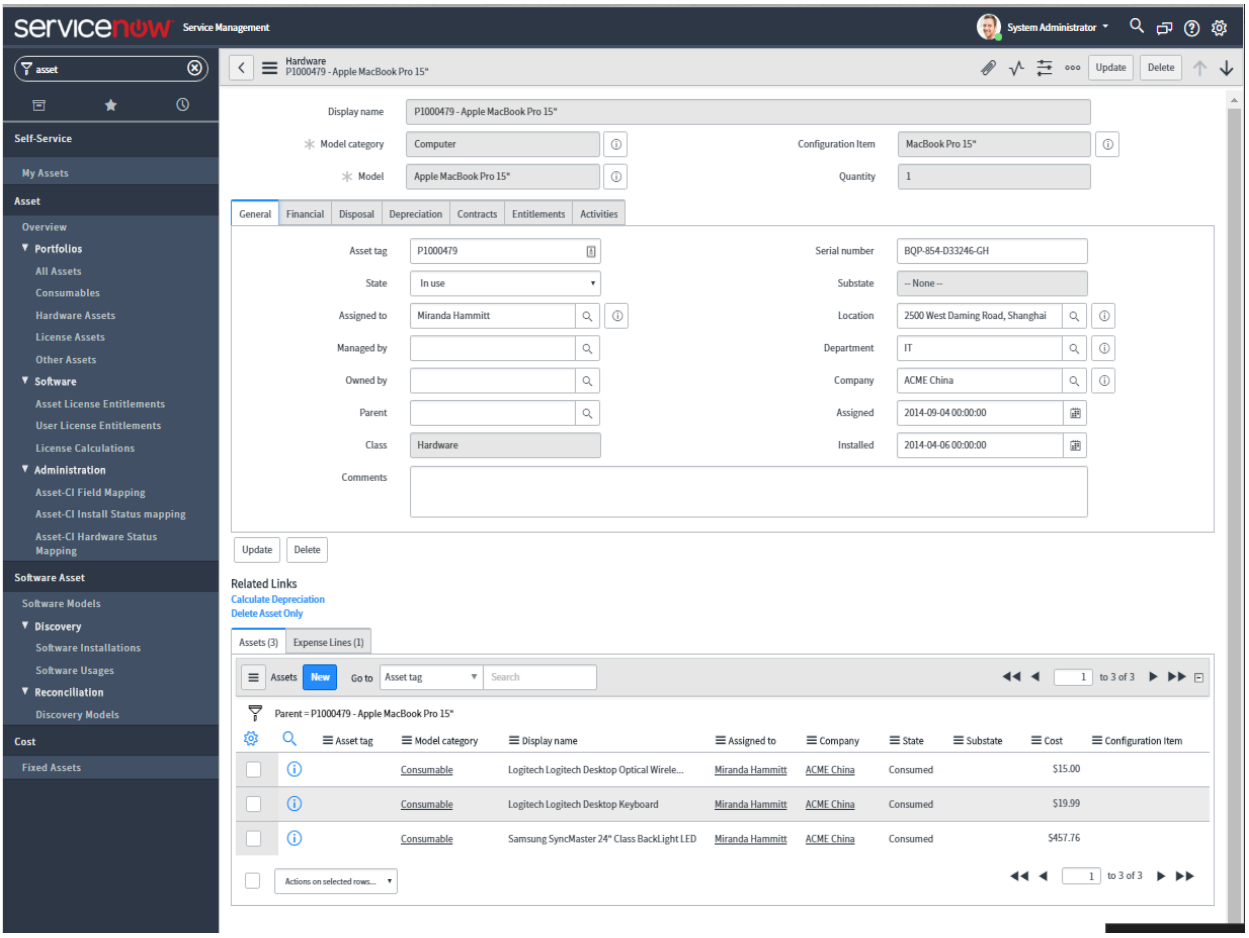
7.4.7 Monitoring & Asset Management

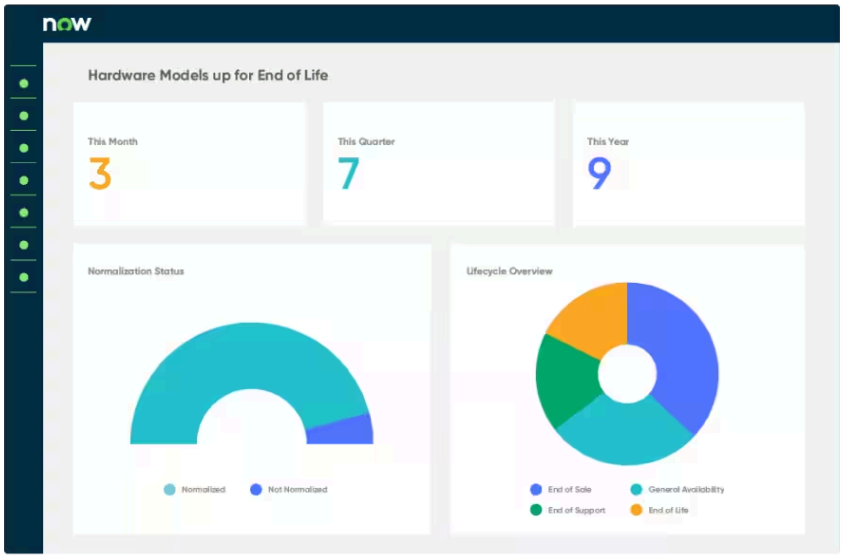
An essential step in monitoring our services is having some visibility into the health of our services being managed by other services such as AWS and Microsoft. Dashboards and metrics provided by Dynatrace would provide that essential insight needed to monitor the health of our applications being hosted by other services and on-premises and our networking devices via simple network management protocol (SNMP).



Another important aspect of network management we also have to consider is how we are going to keep track of our devices that are used throughout the network. If we are going to support the network to the fullest extent, it is paramount that we are aware of each and every asset. This will

be beneficial towards monitoring the overall health of our network as we would gain visibility on the life cycles of our hardware that the employees use. By utilizing ServiceNow's IT Asset Management (ITAM) system, their hardware asset management system (HAM), and their native configuration management database (CMDB) we would gain the transparency needed to effectively oversee the network and contribute to lowering financial risk for the medical center (ServiceNow, n.d).





7.4.8 IoMT Device Security

Internet of Medical Things (IoMT) devices will be placed in its own VLAN at each building. Segmenting IoMT traffic leads to a more secure network, as these devices may contain vulnerabilities that may compromise the main network if left unsupervised.

7.5 Redundancy & Availability/Reliability Efforts

7.5.1 Network Redundancy

To ensure we meet availability requirements (five nines - 99.999%), we will have hot spare routers and switches configured and ready to be swapped in the case one of the devices goes down. Swapping out of the devices will be seamless and downtime would be minimal.

7.5.2 Server Redundancy

A cold backup of mission critical servers will be off in case of any main server downtime. The Datto backup solution will keep local backups of servers and databases in case of any corruption or downtime. In regards to web and DNS servers, those services will be hosted by AWS and we will rely on them for support in that facet as we will utilize their cloud infrastructure. Microsoft Exchange will also be involved as we will utilize their email server software along with Microsoft 365 cloud suite for other office applications.

7.5.3 Data Backups

Data backups will be stored locally on attached storage, running RAID 5, with hot swappable drives ready in case of any emergency. Off-site backups will be stored at another AWS data center, the traffic between the main hospital and the backups will be protected by a VPN tunnel.

7.5.4 Quality of Service (QoS)

Quality of Service (QoS) will be implemented at the router level to address any bandwidth issues. Mission critical devices, health metric monitoring equipment, and selected endpoints will be allotted more bandwidth.

8. Hardware

Below is a table containing all of the hardware devices that will be used throughout all buildings.

Device Type	**Vendor**	**Model**
Firewall	Fortinet	FG-900 Firewall
Router	Cisco	Cisco ASR 1002-HX Router
Layer 3 Switch (Dist.)	Cisco	Cisco Catalyst 9600 Series Switch
Layer 2 Switch (Access)	Cisco	Cisco Catalyst 9300 Series Switch
Access Point	Cisco	Cisco Catalyst 9166 Series Access Point
Servers	Dell	PowerEdge R760 Rack Server
Uninterruptible Power Supplies	APC by Schneider Electric	Symmetra PX 125kW Scalable to 250kW with Right Mounted
Server Racks & Cooling Systems	Vertiv	Vertiv SmartAisle (1) Vertiv VR 42U Network Racks (4) Liebert Mini-Mate, Ceiling-Mounted Precision Cooling System, 3.5-28kW (4)

8.1 Firewalls

FortiGate FG-900G

Interfaces:

- 1 x 2.5/1 GE RJ45 HA Port
- 1 x GE RJ45 Management Port
- 16 x GE RJ45 Ports
- 8 x GE SFP Slots
- 4 x 10GE/GE SFP+/SFP Slots
- 4 x 25GE/10GE SFP28/SFP+ ULL (ultra-low latency) Slots

The Fortigate FG-900G firewall will serve as our key device for securing the entries into the network of Providence Medical Center. It yields the kind of high-performance that enterprises would need to protect their networks as it provides a number of features including intrusion detection and prevention (IDP), web-filtering, VPN support (which is an essential foundation of our network design), high availability and load balancing with failover capabilities, and logging and reporting functionalities. Versatility is a huge technical requirement we are striving for given the kind of data we are securing with this network - and this particular device provides just that

which makes it a critical asset for securing business assets and data, which includes patient data, various EHR data, and medical research in this case.

8.2 Routers (Core Layer)

Cisco ASR 1002-HX Router

Interfaces:

- Built-in front panel 4xGE and 4x10GE; can be upgraded to 8xGE amd 8x10GE with a license
- Extendable I/O with 1 Ethernet port adapter, and 1 single-wide network interface module (NIM) or 1 double-wide NIM

The Cisco ASR 1002-HX Router will serve as the foundation for routing within our network. It's versatile capabilities allow the device to handle the stress that comes with supporting data center infrastructures or branch network infrastructures that yield high usage (which is our use case for this project), and can adapt to the needs of the network it is part with its advanced QoS

capabilities, integrated services (VPN capabilities, intrusion prevention), and the redundancy (software redundancy) and high availability it offers (Cisco, 2020). Cisco provides some insight into how the software redundancy could positively feed into our four nines availability requirements - essentially stating how standby IOS processes can be available on the same route processor (the component that performs route processing and distributes forwarding tables) as the active IOS process and be switched over to in the event of a Cisco IOS failure in correspondence with the stateful switchover (SSO) and nonstop forwarding (NSF) capabilities.

8.3 L3 Switch (Distribution Layer)

Cisco Catalyst 9600 Series Switch

Interfaces: 48-port RJ45 - 10GE/5GE/2.5GE/1GE/100Mbps/10Mbps (Note: These interfaces are made available due to the line card C9600-LC-48TX)

The Cisco Catalyst 9600 Series Switches will serve as our devices on the distribution layer of our topology. These switches are built to withstand the demand that comes with bandwidth-intensive environments and large campus deployments. This will prove to be beneficial for our networking

environment particularly as the usage of IoT devices and IoMT devices continue to support medical personnel in their roles. The routing capabilities of this switch also makes it a great asset to our network as we are implementing the traditional network setup for an enterprise - which is having a core layer, a distribution layer, and an access layer. An important feature to also note that comes with this particular switch is the routing capabilities and its compatibility with the various interior routing protocols or interior gateway protocols (IGPs), this will be advantageous to our network design as the interior routing protocol that will be implemented throughout our design is Open Shortest Path First (OSPF) - mainly due to the fact that it is a non-proprietary protocol which enables compatibility among most if not all brands of modern networking devices. In general, it is also better for load balancing according to Cisco (Cisco, 2023c), which will further bolster the availability and reliability of our networking systems. Additionally, with the functionality of being able to work with the exterior routing protocol - Border Gateway Protocol (BGP) which will be implemented by Amazon in our use case, it will make routing throughout our network more efficient overall as it will tag those external routes.

8.4 L2 Switch (Access Layer)

Cisco Catalyst 9300 Series Switch

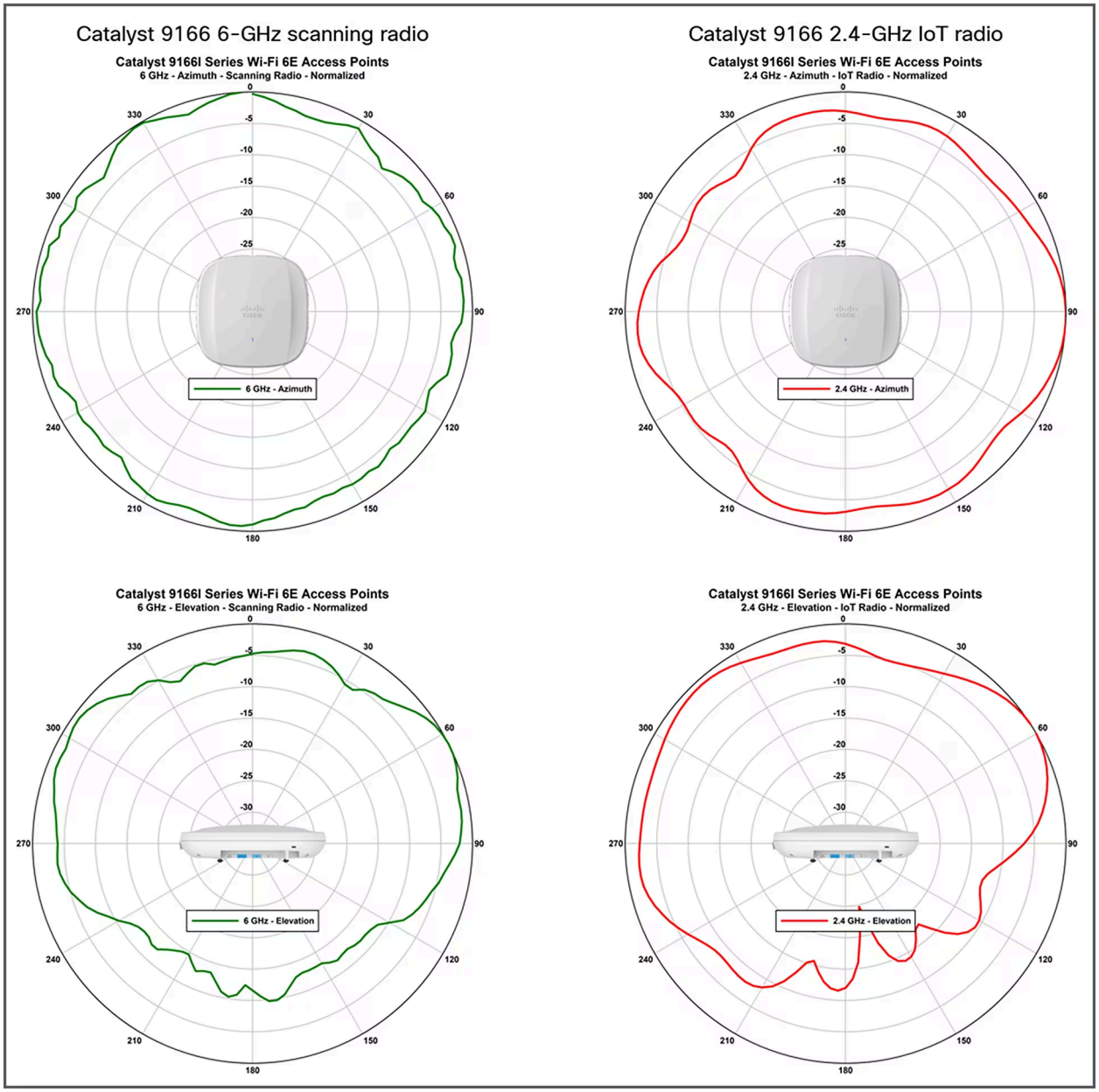
Interfaces: 48-port Multigigabit Ethernet

The Cisco Catalyst 9300 Series Switch is the perfect device for our access layer as it provides all the necessities for our enterprise network - most notably the scalability that comes with its interfaces and the amount of them and the Advanced Encryption Standard support at 256-bits (AES-256). Additionally, the Multigigabit technology would allow us to accommodate the needs that comes with running a hospital, yielding bandwidth speeds of up to 10 Gbps over traditional Cat6 (or higher standard) cabling (Cisco, 2023a). What's also been noted about this switch is the robust and reliable technical capabilities - which is perfect for the environment we're supporting considering it needs to be available 99.999% of the time (five-nines availability). This is bolstered by the redundant components and hot-swappable modules that would contribute to uninterrupted network operation.

8.5 Access Points

Cisco Catalyst 9166 Series Access Point

The Cisco Catalyst 9166 Series Access Points will serve as our vector for wireless connectivity throughout the network as according to Cisco they are capable of handling the environments posed by mission-critical deployments (Cisco, 2023b). With our application of IoT devices and IoMT devices, this particular access point with its management capabilities (compatibility with the Cisco Catalyst 9800 WLC and Meraki Dashboard) will allow us to control this particular aspect of the network with relative ease. The kind of antennas that will be used in the access points is the Catalyst 9166I which provide omnidirectional coverage. The image below displays how that coverage is provided when the access point is set up.


Catalyst 9166 6-GHz scanning radio
Catalyst 9166I Series Wi-Fi 6E Access Points
6 GHz - Azimuth - Scanning Radio - Normalized
6 GHz - Azimuth
Catalyst 9166 2.4-GHz IoT radio
Catalyst 9166I Series Wi-Fi 6E Access Points
2.4 GHz - Azimuth - IoT Radio - Normalized
2.4 GHz - Azimuth
Catalyst 9166I Series Wi-Fi 6E Access Points
6 GHz - Elevation - Scanning Radio - Normalized
6 GHz - Elevation
Catalyst 9166I Series Wi-Fi 6E Access Points
2.4 GHz - Elevation - IoT Radio - Normalized
2.4 GHz - Elevation

8.6 Servers

PowerEdge R760 Rack Server

Rack Server	R760
	
Key attributes	Provides performance and versatility for demanding applications
Target workloads	Mixed Workload Standardization Database and Analytics Virtual Desktop Infrastructure
Type of processor	2 x 4th Generation Intel® Xeon® S cores per processor
Memory (DDR5 DIMM slots & max)	32 (8 TB)
Disk drives up to:	12 x 3.5" 8 x 2.5" 16 x 2.5" 24 x 2.5" 2 x 2.5" or 4 x 2.5" (rear)
NVMe drives up to:	24
Gen5 PCIe slots up to:	4
Gen4 PCIe slots up to:	8
Accelerator support up to:	2 x 350 W DW or 6 x 75 W SW
Rack height (U)	2

The Dell PowerEdge R760 Rack Servers will serve as our devices responsible for our file services, database services, and EHR hosting. Due to their versatility and the fact they were designed to withstand the demands that come with extensive applications, this server will prove to be a benefactor for our network (Dell, n.d - a). The 8TB storage and the virtual desktop infrastructure capability are also significant features to note with the environment we are supporting.

8.7 Uninterruptible Power Supplies (UPSs)

Symmetra PX 125kW Scalable to 250kW with Right Mounted

The Symmetra PX 125kW Scalable to 250kW is a versatile and reliable UPS system known for its high-performance power protection in mission-critical deployments and enterprise IT environments in general. This particular UPS model will assist us in remaining HIPAA compliant as part of the guidelines is to ensure availability of our services. The hot-swappable

components and the N+1 redundancy will further bolster the availability of our networks. (Schneider Electric, n.d).

8.8 Server Racks/Enclosures & Cooling Systems

Vertiv SmartAisle

The Vertiv SmartAisle is an innovative integrated data center solution designed to improve overall performance, sustain reliability, and optimize airflow (Vertiv, n.d). Given we are hosting data/virtualization-intensive services in building 1, the SmartAisle is the perfect enclosure to utilize as it will coincide with our precision cooling system (that will be mentioned later) to maintain the temperature of our mini-datacenter (in the low 70s degree Fahrenheit) and relative

humidity at 50%. Additionally, with modifications the SmartAisle can accommodate over 40 RUs of networking/server hardware.

Vertiv VR Racks

The Vertiv VR Racks will serve as our enclosures for networking devices in the other buildings (2, 3, and 4). They will meet our needs when it comes to organization of devices, cable management, and optimization of airflow allowing for efficient cooling (Vertiv., n.d).

Liebert Mini-Mate, Ceiling-Mounted Precision Cooling System

The Liebert Mini-Mate Precision Cooling System will serve as our cooling systems in the MDFs/IDFs in all of the buildings. The ceiling mounted design along with the precision cooling capabilities makes it the perfect system to utilize in our networking environments as it would provide uniform cooling and maintain temperature and humidity consistency in the environments.

8.9 Internet of Medical Things (IoMT) Devices

The Internet of Medical (IoMT) is very crucial to our network given the kind of environment we are building this network to host and provide service to. The medical scene has evolved at a very quick rate with its increased usage of technology to monitor crucial patient information and sending that data to other devices that are used daily (essentially making that info more accessible). These devices include remote patient monitoring devices, glucose monitoring devices, miniature robotic devices (for surgery), heart rate monitoring devices, and point-of-care devices like ultrasound machines.

References

FortiGate 900G Series FG-900G and FG-901G AI/ML Security and Deep Visibility. (October 17, 2023). https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-900g-series.pdf

Ataman, A. (2023, February 24). Data Encryption in Healthcare: Importance, Benefits & Use Cases. Research.aimultiple.com. https://research.aimultiple.com/data-encryption-in-healthcare/

Healthcare Cybersecurity Solutions. (n.d.). Fortinet. Retrieved October 24, 2023, from https://fortinet.com/solutions/industries/healthcare

HIPAA. (n.d.). Fortinet. Retrieved October 25, 2023, from https://www.fortinet.com/corporate/about-us/product-certifications/hipaa

Federal Register :: Request Access. (n.d.). Unblock.federalregister.gov. https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C

https://www.pagerduty.com/resources/learn/what-is-a-runbook/#:~:text=A%20runbook%20is%20a%20detailed,configs%2C%20and%20opening%20ports).

Dynatrace. (2023, December 8). Generic Cisco Device Monitoring & Observability: Dynatrace Hub. Dynatrace. https://www.dynatrace.com/hub/detail/generic-cisco-router-snmp-extension/

ServiceNow. (n.d.). Hardware Asset Management. ServiceNow. https://www.servicenow.com/products/hardware-asset-management.html

Cisco. (2020, February 4). Cisco ASR 1002-HX aggregation services router. Cisco. https://www.cisco.com/c/en/us/products/routers/asr-1002-hx-router/index.html

IP routing: BFD Configuration Guide, Cisco Ios XE release 3S - bidirectional forwarding detection [cisco ios XE 3S]. Cisco. (2018, July 19). https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bfd/configuration/xe-3s/irb-xe-3s-book/irb-bi-fwd-det.html

Cisco Catalyst 9600 series switches Data Sheet. Cisco. (2023, October 25). https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9600-series-switches/nb-06-cat9600-series-data-sheet-cte-en.html

Cisco. (2023c, August 28). Understand open shortest path first (OSPF) - design guide. Cisco. https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html

Cisco Catalyst 9300 Series Switches Data Sheet. Cisco. (2023a, October 25). https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html

Cisco Catalyst 9166 Series Access Points Data Sheet. Cisco. (2023b, November 1). https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9166-series-access-points/catalyst-9166-series-access-points-ds.html

Dell. (n.d.-a). Poweredge R760 - Dell Technologies Partner Portal. https://www.delltechnologies.com/asset/en-us/products/servers/technical-support/poweredge-r70-spec-sheet.pdf

Dell. (n.d.-b). Quick Reference Guide Rack Server R760 R660 R7625 R6625 R7615 R6615 - Dell.

https://i.dell.com/sites/csdocuments/Product_Docs/en/poweredge-rack-quick-reference-guide.pdf

Schneider Electric. (n.d.). SY100K250DR-pd - symmetra PX 100kw scalable to 250kw with right mounted ... *https://www.se.com/us/en/product/SY100K250DR-PD/symmetra-px-100kw-scalable-to-250kw-with-right-mounted-maintenance-bypass-and-distribution*

Berkeley, U. (n.d.). *HIPAA PHI: Definition of phi and list of 18 identifiers*. UC Berkeley Human Research Protection Program. https://cphs.berkeley.edu/hipaa/hipaa18.html

Jason Gerend. (n.d.). DirectAccess. Microsoft Learn. *https://learn.microsoft.com/en-us/windows-server/remote/remote-access/directaccess/directaccess*

Vertiv. (n.d.). VertivTM VR Rack. Vertiv VR Rack | High Power Density Racking Systems. *https://www.vertiv.com/en-us/products-catalog/facilities-enclosures-and-racks/racks-and-containment/vertiv-vr-rack/*

Vertiv. (n.d.). SmartAisle. Smart Aisle | Vertiv IT Infrastructure. *https://www.vertiv.com/en-us/products-catalog/facilities-enclosures-and-racks/integrated-solutions/smartaisle/#/models*