Final Project Report

Course: CIS 2347

Submitted to

Information Science Technology

Technology Division, College of Engineering

University of Houston

by

Khang Nguyen

November 26, 2024

Prof. Peddoju

Table of Contents

1. Introduction

The luxury residence hall at the University of Houston needs a network design for a student housing apartment. The building would include 162 two-bedroom, one-bathroom apartments spanning 6 floors. The first floor features a lobby and an office area for employees. The second floor is dedicated only to conference rooms which are planned to be used for meetings, collaborative projects, and or a space to study. However, because a parking garage surrounds the buildings, floors 1 and 2 (100 feet by 70 feet) would have smaller dimensions than the residents' floors which are 240 by 150 feet. Furthermore, the first floor contains a server room for the university's network which is responsible for managing all campus residences, employees, and infrastructure components. A critical objective highlighted in this project was to design a secure, efficient network, but to isolate and segment the networks as much as possible from high-value data and infrastructure from unauthorized access. The design proposed would prioritize efficiency above all else while still being mindful of budget concerns and costs. Equipment and configurations of the network and cabling are carefully assessed beforehand, keeping in mind future growth and expansion while still delivering optimal performance. Information regarding each component, their purpose, benefits, and the reason behind each implementation will be provided as well as the layout of the building, and the placement of wireless access points. IP addresses assigned for each group of users will be thoroughly discussed and VLAN will also be an important factor in how the network is configured.

2. Recommendations

Ethernet Drops

To ensure network connectivity, this specific configuration for Ethernet drop across the building is recommended. For each office, it will be equipped with two Ethernet drops for standard office setup including the computer workspace and VoIP phone. Each dorm room, designed to house two residents, will feature four Ethernet drops to accommodate academic and personal needs. Even though there was no requirement to have Ethernet drops in the conference room, it is highly recommended as the space would be used for presentations, meetings, and other collaborative projects which may require direct high-speed internet access in the vicinity. Because of this needs analysis, each room will also include two Ethernet drops. For installation, a 2-port Ethernet wall plate would be used to optimize flexibility and ease of connection for multiple devices. To establish an Ethernet line, the circuits will utilize Cat5e cables which would support a maximum bandwidth of 1,000 Mbps (1 Gbps), sufficient enough for everyday applications across all users while maintaining cost-efficiency. These recommendations are designed to balance performance, scalability, and user convenience while ensuring the network meets the needs of all campus occupants.

Access Switches

The proposed access switches for the network are Cisco Catalyst 1200-48P-4X, chosen for its robust capability and ability to support current and future requirements. Each switch includes 48 ports compatible with 10/100/1000 Base-T, guaranteeing high-speed connections for users' devices and wireless access points. Because of the number of Ethernet ports used for establishing connections to all Ethernet drops and wireless access points, three switches will be used per floor to provide sufficient connectivity while still including spare ports for future expansion or IoT devices such as cameras. Furthermore, the switches also provide power over the Ethernet which would make setting up wireless access points easier without the need for separate power cords which simplifies network installation and labor costs. The switch also features SFP+ transceivers which support up to 10 Gbps, critical for connecting the access layer to the backbone network and ensuring high-speed communication between the distribution and core layers. To support the higher data capacity allowed by the SFP+ transceivers, CAT6A cabling would be recommended as it ensures it can manage high-speed data transfer while still being resistant to electrical interference. Lastly, the switches are multilayer, meaning that it can efficiently route traffic between different networks or in this case, VLANs which would make network segmentation, security, more granular than through the use of subnets.

Core Switches

The core switches picked out is the Cisco Catalyst 1300-24XS. Almost entirely supporting only SFP+ modules, this switch is highly optimized for being a part of the backbone network as it offers multiple inputs for low latency and high speeds of up to 10 Gbps. These would serve as the main switches which would distribute traffic across all floors and network traffic into the router which will lead and connect to other buildings and assets. Cabling from each of the switches on the floor will be routed through both the core switches for increased redundancy and load balancing. The core switches themselves will also both be connected to the router for further redundancy. However, because SFP+ on the switches will require transceivers, the use of SFP+ to RJ45 will then allow the use of copper Ethernet cables such as Cat6A to be routed into it which will be needed to support the higher available throughput. Furthermore, because the switch is managed, this will allow network administrators to easily configure and set rules for all direct connections via the command line.

Wireless Access Points

The wireless access points recommended is the Cisco Business 140AC which is incredibly affordable while still being sufficient enough to cater to the needs of the residential network. Having the capability of Wi-Fi 5, it is able to work in for 5 GHZ and 2.4 GHZ in order to establish the correct connections and configuration for employees, residents as well as visitors. It is ceiling mounted which would make setting up connection and expanding coverage way easier and furthermore, it is compatible with 802.1Q needed to segment VLANs from each other as well as inter-switch routing for communication. It has a data transfer of up to 1 Gbps which means that CAT5e cabling would be used to connect to the switch to facilitate the fastest speeds available.

Cabling

To facilitate all connections to the network, the correct cabling type must be used which provides the best speed when considering the usage, network traffic, and purpose. All circuits that form the access layer will utilize Cat5e cables as they provide sufficient bandwidth, supporting speeds up to 1 Gbps for daily work and network traffic. For the backbone which interconnects with other switches and the various buildings on campus, Cat6A cables would be used as it supports speeds up to 10 Gbps, making it ideal to handle the increased traffic and higher throughput demands of the backbone and core. However, because of the extreme amount of cabling needed to route through each Ethernet drop as well as the wireless access points, the amount of cabling dramatically shoots up. Because of this, cabling such as Cat5e and Cat6A would be bought in bulk to limit cost. This will require a lot of termination of the wires to fit the required length for cabling and organization. An RJ45 network connector will also need to be bought in bulk and the recommended product would be the Belkin network connector.

Uninterruptable Power Supply

To safeguard network devices against common power issues such as surges, blackouts, and brownouts, the implementation of an uninterruptible power supply (UPS) is essential. The recommended UPS is the CyberPower Smart App Intelligent LCD OR2200LCDRT2U which provides many features for not only current needs but in the future. This UPS features battery backup with a simulated sine wave to ensure uninterrupted power to network devices during outages. It also includes surge protection which would shield any network devices from power spikes and surges which may harm the lifespan of the hardware. In terms of output capacity, it contains eight output connections which is enough to power all three switches including power over Ethernet required for each of the residents' floor. This UPS will also be used in the main distribution frame. In terms of power ratings, it has a capacity of 2000VA, which is enough for the UPS to run for approximately 13 minutes at half load or 5 minutes at full load during a power outage. This would provide ample time for network administrators or on-site personnel to save their work and power down the devices in a controlled and safe manner which will minimize the risk of corruption and damage to equipment.

Wiring Closet's Server Rack

Proper organization and management of network equipment are critical to ensure operational efficiency and scalability. In consideration of this, each network device was picked in consideration of being rack-mountable which would help organize and centralize the management of the various equipment. To address these needs, A StarTech.com 4-Post 18U Mobile Open Frame Server Rack will be installed in each wiring closet which would provide sufficient space for current equipment while still allowing enough space for future expansion. For cable management, the use of Tripp Lite 24-port blank keystone patch panels will not only make the beginning of cabling and organization easier but will allow troubleshooting and expansion far easier. With six panels per rack, each switch will be flanked by a patch panel above and below, streamlining cable management and making troubleshooting more efficient. 6-inch patch cables will further enhance organization, reducing cable clutter and improving accessibility. Furthermore, this specific patch panel is compatible with the use of Cat5e cabling and Cat6 cabling which is future-proof. However, the usage of blank keystone patch panels instead of punch-down blocks would require the use of punch-down keystone jacks to work with the modularity and flexibility allowed by the blank keystone patch panels. The punch-down keystone proposed is the Tripp Lite Cat6/Cat5e punch-down keystone jack. For rack space allocation, because each floor will house three switches, each occupying 1U, the total allocated for only switches is a total of 3U. The six patch panels will occupy an additional 6U as each panel is 1U. The UPS for power backup chosen will take up 2U, ensuring the safety and stability of the equipment during power disruptions. After accommodating these components, 7U of space will remain, which can be used for future expansions, additional cable management trays, or even a computer for on-site configuration and monitoring.

Main Distribution Frame’s Server Rack

Following the same principles for the server rack on the residents’ floors, this too will be used to help organize the central network infrastructure of the building into one concise rack. However, instead of using the 18U server rack, the MDF will be supplied with an even larger server rack to account for additional space needed to house the servers, switches, UPS, and router. The server rack recommended is the Tripp Lite 24U Rack Enclosure Server which will house all of the network’s infrastructure. The router used will be placed at the very top which will connect to both the core switches. The core switches will follow just below the router which allows for more easy access to this important hardware. The access switches which supply the 1st and 2nd floor Ethernet drops and connections will lay just below it. However, it's important to keep in mind that there will be 1U of space in between each switch which we use for the blank patch panels to help with cable management. There will be a total of 6 panels needed to account for all the ports available. The router will take only 1U of space. All the switches will take the combined amount of 4U and the patch panels, 6U. The building's servers will be laid below the access switches which will then connect to core switches. Each server takes up 2U of space so a combined amount of 4U. Lastly, the UPS will be placed at the very bottom of the server rack which will then allow space for additional hardware components or hard drives space for backup systems, data storage, or processing. This UPS takes up 2U of space. Accounting for all these components, the minimal amount of space this used up is 16U of space. This leaves 8U of space left over for additional expansion, equipment, and more.

Servers

To ensure efficient management and separation of network services for residents and building employees, the deployment of two servers is recommended. Each server will manage Active Directory (AD) and Dynamic Host Configuration Protocol (DHCP) processes within its respective VLANs, with proper IP address assignments for segmented traffic control. Containing many powerful components such as an Intel Xeon E-2200 and 64GB of RAM, it also supports multiple hard drives for RAID configuration for local data redundancy. Because of the server's resources, it would be able to run multiple services including AD and DHCP with implementation of virtualization if space and budget were to be of high concern. Both servers are to run Windows Server 2022, which provides advanced features for Active Directory management and DHCP configuration. However, it is recommended to use the Cisco Prime network registrar as it offers a more comprehensive and scalable solution with advanced features like integrated DNS, IPv6 support, and centralized management across large networks. Active Directory will be set up alongside these multiple services, maintaining separate AD domains of residents and building employees for proper authentication, access control, and resource allocation for each group. This dual-server setup provides a secure, efficient, and scalable foundation for managing the building's network services, supporting both current and future demands.

Architecture

To prioritize segmentation, redundancy, and efficiency, the network design must utilize a combination of switched backbone and routed backbone networks. This hybrid approach ensures optimal data flow, bandwidth utilization, and scalability for the campus network. At the distribution layer, a switched backbone would be implemented to efficiently direct traffic between the different floors. To further increase redundancy, each residential floor's switches will connect to two central backbone switches located in the main distribution frame. Not only does this reduce single points of failure by creating multiple pathways for transmission, but traffic distribution across two backbone switches would prevent bottlenecks and enhance overall network performance. At the core layer which would connect the several buildings on campuses, a routed backbone would be used to allow additional segmentation of the network, future network expansion, and ease of troubleshooting. Routers will connect to both backbone switches, adding an additional layer of redundancy and ensuring continued network operation in the event of a single failure. This proposed architecture will support the campus network's current needs while taking into consideration future growth, such as the addition of new VLANs, devices, or floors. The segmentation provided by the routed backbone ensures that any updates or reconfigurations can be made with minimal impact on existing systems or networks.

IP addresses

This residential network will utilize the 172.16.0.0/18 network, offering four subnets with a total of 16,382 usable addresses per subnet. This design provides ample capacity for all network devices, including static IP addresses, and ensures scalability for future expansion. IP addresses will be handed out via the configured server which acts as an active directory that works alongside the dynamic host configuration server. To enhance security, segmentation, and efficiency, the network will employ Virtual Local Area Networks (VLANs), correctly configured for the appropriate VLAN access and trunk ports on the switches, routers, and circuits. There will be a total of four VLANs each with their respective IP pool, purpose, and typical devices which may fall into it. Infrastructure components such as the servers, printers, and IoT devices will be configured to be at VLAN 10. This would segregate critical infrastructure into one main network which would reduce exposure to potential threats and will make future reconfiguration and expansion easier due to the centralization of such devices. Employees' work devices and BYOD devices will be assigned VLAN 20 and have a gateway of 172.16.64.1 via the DHCP server. Authentication will be enforced through 802.1X with a RADIUS server for identification and verification of credentials. Office computers connected via the Ethernet drops can supplement validation through certificates tied to hardware ID or MAC addresses and are secured with WPA2-enterprise. For residents with their own personal devices and computers, they may want to directly connect via Ethernet, they will be connected through VLAN 30 which has a gateway of 172.16.128.1 via the DHCP server. Lastly, for visitors and guests who may just want to have access to the internet, they will connect to VLAN 40 which provides isolated internet access without interfering with other VLANs or internal resources. However, due to being a guest, lower speeds and access to resources will of course be addressed via permissions in the active directory. The benefits of this configuration VLAN segmentation prevents unauthorized access and minimizes the impact of potential breaches. The assignment of VLAN will be done automatically through what is called dynamic VLAN. This dynamic assignment will be done using VLAN protocols which work in tangent with the RADIUS, Active Directory, and the DHCP server.

<u>Securities</u>

To secure the network, a combination of services, protocols, and industry standards will need to be implemented. These strategies will aim to minimize exposure to attacks, prevent unauthorized access, and to ensure the security of data. The Cisco Identity Services Engine will be highly recommended as it is network access control software which will prove crucial in managing the network. Due to the high capability and interface, this will help in making insights into the network through analyzing traffic, assessing efficiency, and to help in iterating the network design or security for future growth. Furthermore, this platform will work in tangent with the active directory and DHCP to manage and enforce security policies to any devices before they connect to the network. This will mean the users must meet encryption and antivirus requirements and adhere to the operating system standards in order to connect. Furthermore, with the capability of dynamic VLAN, it will even be easier to segment the network and secure it by having the user first log in and then dynamically given their assigned VLAN, reducing the need to manually configure each interface which would have wasted time and resources. Stateful firewalls will be employed on the router which will have the purpose of denying or allowing requests through filling requirements such as IP addresses, data types, and port. Wireless network standards will use WPA-2 with Advanced Encryption Standard (AES) which will provide the industry standard for secure data transmission. This will also work in conjunction with the Active Directory for authentication, ensuring only those who provide the correct credentials will have access to the network and its resources. For additional security policies, network devices which support these policies will have the ability to filter only approved devices such as verifying MAC addresses which will be important for office computers. DHCP snooping will also be implemented to prevent unauthorized devices from obtaining a valid IP and Spanning Tree Protocol (STP) will help with preventing Address Resolution Protocol (ARP) spoofing. This network configuration will reduce the attack surface by allowing granular access controls to sensitive data and resources.

Backup System and Disaster Recovery

Backup systems will be implemented in a layered approach where there will be multiple options for backup and security to maximize reliability and accessibility given any circumstance. For instance, for faster recovery, local backup systems will be held on the two servers located locally in the main distribution frame. This close backup system will be reliable for quick restoration of systems or files given scenarios like accidental file deletion or minor data corruption. However, off-site protection through the use of a third-party service like Amazon Web Service will help protect against localized disasters which may impact the local backup systems such as if a fire or flood were to occur. Furthermore, data stored on the cloud service will be stored across multiple data centers, spanning continents or regions, and due to the ease of scalability that cloud service provides, it is an effective option for long-term data. Cloud backups will be highly preferential in scenarios following catastrophic events such as natural disasters. However, for data recovery to run smoothly, procedures must be created, assessed, and followed for the system in place to be effective. Both backup systems should be regularly tested to ensure that data remains accessible, and prioritization of certain users should be kept in mind such as the university's data, employees, and its students. Furthermore, staff should be assigned roles and responsibilities concerning certain disaster scenarios and maintain a communication plan to coordinate and notify those who handle the situation. Lastly, data should always be monitored to identify any weaknesses, points of failure, and performance.

3. Diagrams/Maps

Floor 1

The first floor of the building features an open lobby with a seating area and a separate office area. To accommodate the highest volume of users and network traffic, three wireless access points will be strategically placed in the area of the lobby, maximizing coverage and minimizing frequency interference. For more understanding of the visuals, the yellow circle corresponds to the coverage of 2.4 GHz and the red with 5 GHz. WAP #1 would be installed in the bottom left corner of the lobby, WAP #2 bottom right corner of the lobby, and WAP #5 at the center of the lobby. For the office area, WAP #3 will be positioned in Office M106 and WAP #4 in Office M102. For a better visual representation of how exactly the placement helps with minimizing channel interference, specifically 2.4 GHz, reference Figure 1. In terms of choosing the specific channels for 5 GHz, it won't exactly be discussed in detail due to how much easier it is to plan and configure due to the increase in the number of non-overlapping channels in 5 GHz. This specific pattern would continue to be a recurrence for the rest of the network layout as it provides robust coverage for both 2.4 GHz and 5 GHz frequencies while mitigating channel interference. Now, besides serving as the main lobby and office area, it also serves as the hub for the building's network infrastructure. Here in the main distribution frame, two core switches, a router, and two access layer switches are housed in the MDF to manage traffic across all floors. Two servers would also be included, designated for both the active directory, security protocols, and data storage. These servers will be configured in a way that supports segmentation and ensure secure management of network services for both residents and employees. For backbone cabling, Cat6A cabling, depicted in orange, connects the MDF to the backbone switches, ensuring high-speed data transfers and supporting inter-floor traffic. All Ethernet drops and wireless access points on the first floor will connect to Switch #1 with black arrows representing connections between network components for more visually readable connections. All Ethernet drops and wireless access points on the 2nd floor will connect to Switch #2 as shown by the green cabling coming out from the area of the north stairs and elevators.

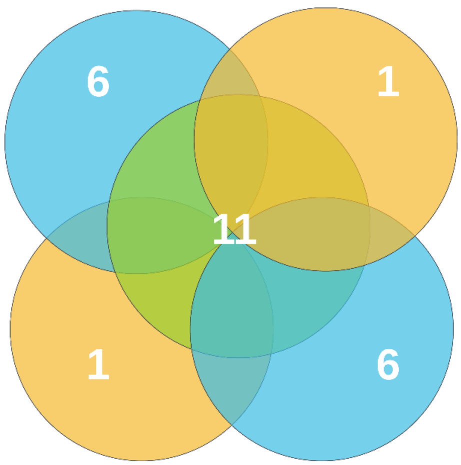
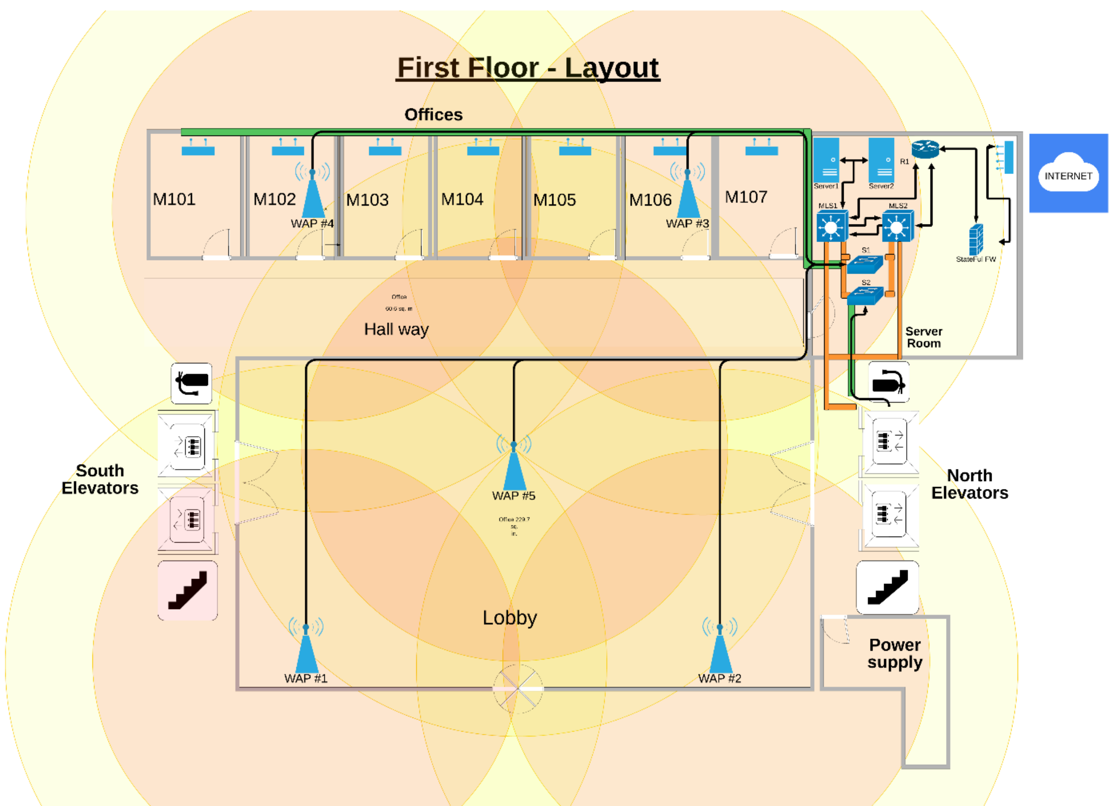
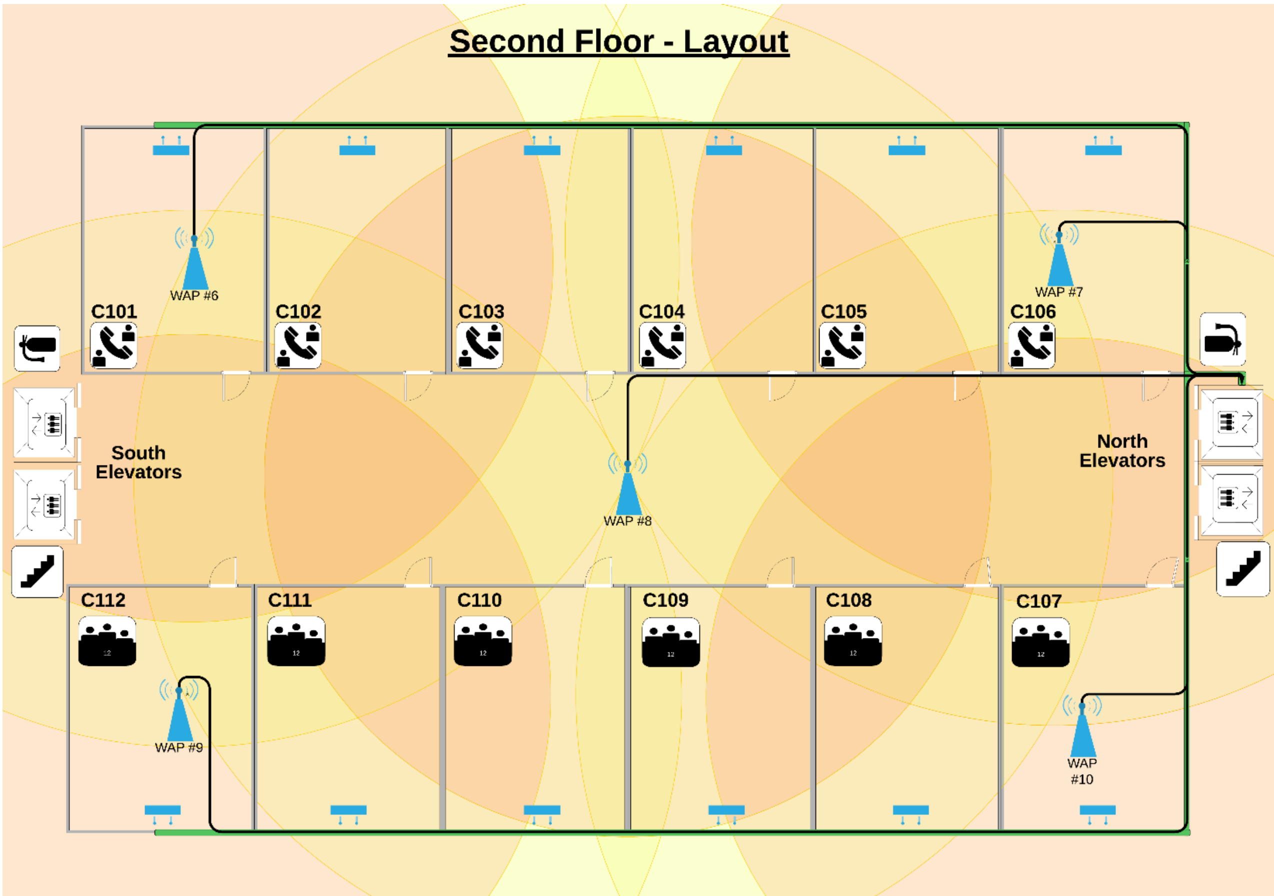


Figure 1. Visual representation of the WAPs configuration



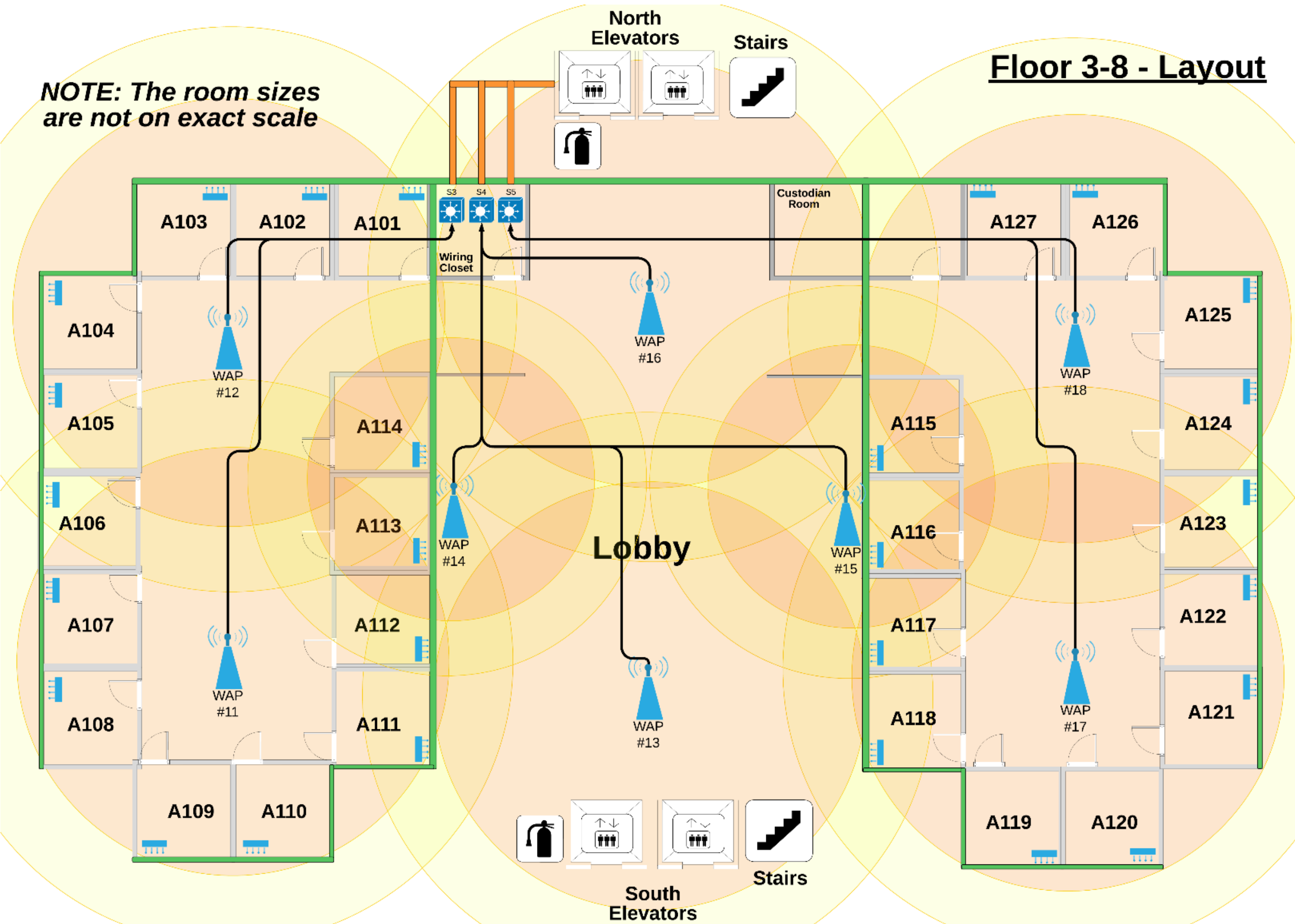
Floor 2

The second floor is designed to support conference rooms for meetings, collaboration, and project work. To connect the conference rooms, each room is provided with two Ethernet drops to support high-bandwidth applications, such as video conferencing and collaborative tools. Routing of the Ethernet drop is visually represented by the green cables and are routed through the dry walls following the building's stairwell or elevator shafts for efficient and concealed installation. The Ethernet drops on the 2nd floor, however, will connect to switch #2 which will be explained why later. To maintain the principles of maximum coverage, minimum frequency interference, and efficient traffic distribution, there will be a total of five wireless access points on this floor with strict placement. WAP #6 will be placed in conference room C101, WAP #7 in conference room C106, WAP #9 in conference room C112, and WAP #10 in conference room C107. An access point will be installed in the middle of the hallway to eliminate any potential dead zone for fast 5 GHz connectivity. In terms of cabling, all WAPs will connect to Switch #2, housed in the MDF on the first floor. Green cabling and black arrows, as illustrated in the first-floor layout, represent the routing of Cat5e cables to these WAPs and Ethernet drops. Connecting second-floor devices to Switch #2 preserves additional ports on the two access switches on the first floor. This ensures flexibility for future expansions, such as the integration of IoT devices like IP cameras and card scanners.

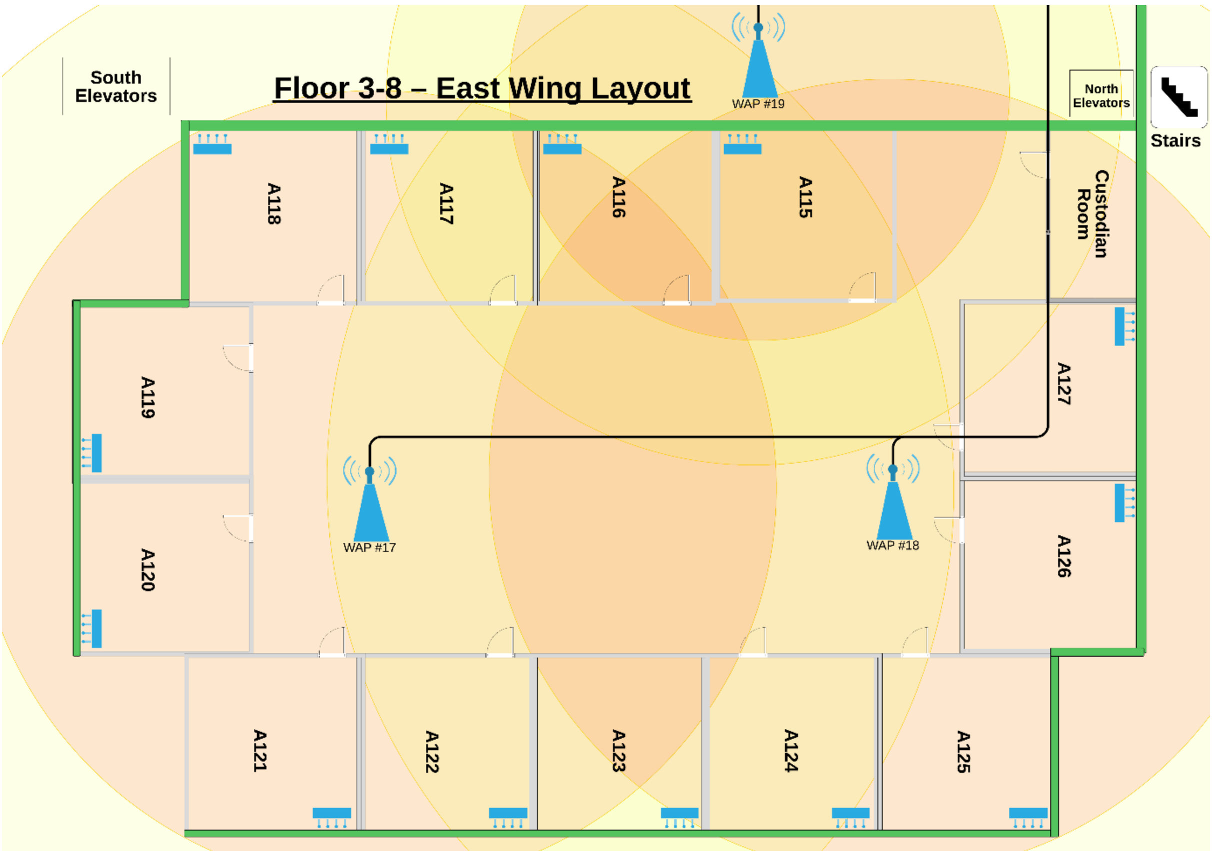


Floor 3-8

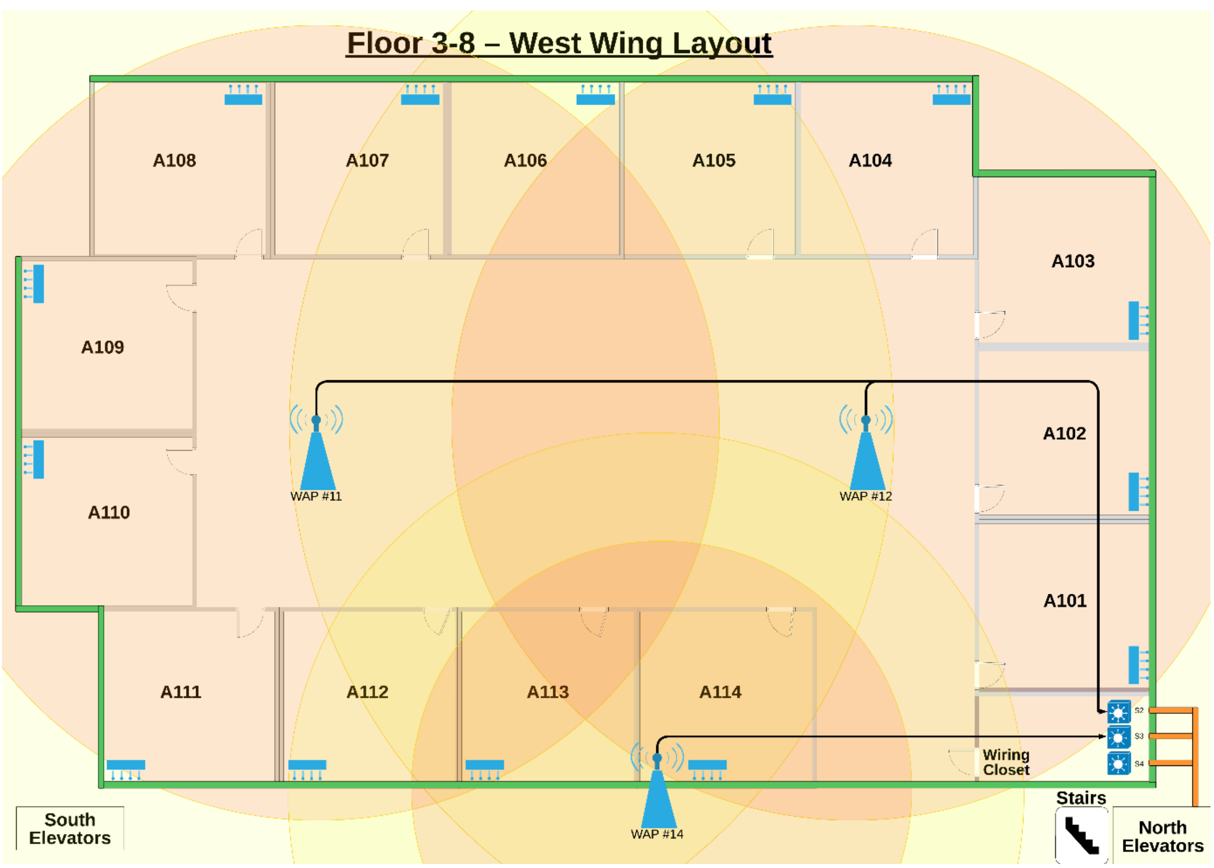
The residents' floors consist of 27 two-bedroom apartments which require 4 Ethernet drops per room. This would result in a total of 108 connections per floor which, to accommodate for the abundant number of Ethernet connections, will need 3 48-port switches per floor. The Ethernet drops will be evenly distributed across the switches, each receiving 36 connections to distribute the load. For wireless access, a total of 8 wireless access points will be deployed for complete coverage. In the west wing, WAP #11 will be placed at the end of the hallway and WAP #12 at the beginning of it. This placement allows maximum coverage of all the dorms as well as the hallway. This configuration will also be mirrored on the east wing with WAP #17 and WAP #18 following the same placement respectively. For the lobby area, WAP #16 would be placed in the middle of the hallway which connects the West and East wing of the building. WAP #13 would be positioned at the south end of the lobby, near the elevator. However, two additional WAPs will be installed on either side of the lobby to eliminate any potential dead zones. WAP #14 will be installed on the west side of the lobby while WAP #15 on the east side. To avoid channel interference with these additional access points, the power level specifically will be reduced to limit the effective range and therefore interference. To configure the port connection of the WAPs, switch 3 will handle the WAPs on the West wing, Switch 4 for the lobby area, and Switch 5 for the East wing. These switches will then connect to the backbone network located in the main distribution frame (MDF) located on the first floor. For redundancy, each switch will connect to both the main core switches on the first floor, reducing single points of failure and adding additional load distribution. This can be seen visualized in the map with the orange cabling, representing Cat6A for the additional speed required, routed down the walls of either the stairs or elevator.



Floor 3-8 - Layout
NOTE: The room sizes are not on exact scale
North Elevators
Stairs
S3
S4
S5
Wiring Closet
Custodian Room
A101
A102
A103
A104
A105
A106
A107
A108
A109
A110
A111
A112
A113
A114
A115
A116
A117
A118
A119
A120
A121
A122
A123
A124
A125
A126
A127
WAP #11
WAP #12
WAP #13
WAP #14
WAP #15
WAP #16
WAP #17
WAP #18
Lobby
South Elevators
Stairs



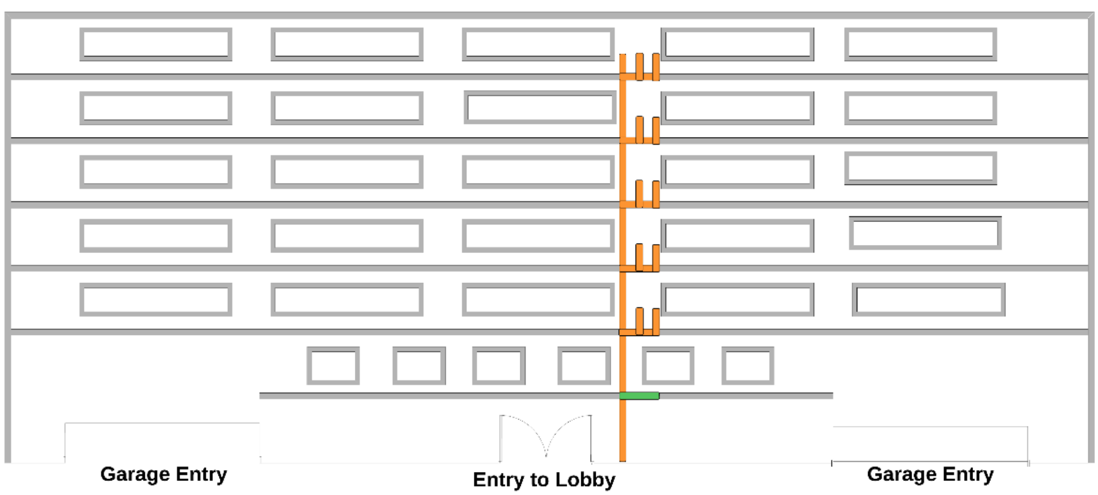
South Elevators
Floor 3-8 – East Wing Layout
WAP #19
North Elevators
Stairs
A118
A117
A116
A115
Custodian Room
A119
A120
A127
A126
WAP #17
WAP #18
A121
A122
A123
A124
A125



Floor 3-8 – West Wing Layout
A108
A107
A106
A105
A104
A103
A109
A110
A102
WAP #11
WAP #12
A101
A111
A112
A113
A114
Wiring Closet
WAP #14
South Elevators
Stairs
North Elevators

Building's Cabling

To connect all the floors, the switches on each floor will connect to the core switches in the main distribution frame to allow intercommunication between each floor. This cabling from the access switches can be routed either alongside the drywalls of the elevator or the stairs for direct connection and centralization of the cabling. This is shown in the layout below showing the residents' floor switches routing towards the bottom as well as all the Ethernet drops and wireless access points on the 2nd floor shown by the green cabling.



4. Cost Assessment

Equipment	Product Name	Quantity	Cost per Item	Total Cost
Wireless Access Points	Cisco Business 140AC	58	$88.99	$5,161.42
Switch	Cisco Catalyst 1200-48P-4X	20	$1,189.99	$23,799.8
Switch	Cisco Catalyst 1300-24XS	2	$2,243.99	$4,487.98
Router	Cisco Catalyst 8200-1N-4T	1	$1,739.99	$1,739.99
Uninterruptable Power Supply	CyberPower Smart App Intelligent LCD OR2200LCDRT2U	7	$604.95	$4,234.65
Wall Plate	C2G Two Port Cat5E RJ45	344	$9.12	$3,137.28
RJ45 Connectors	Belkin network connector (100 pack)	15	$19.99	$299.85
Network Access Control Software	Cisco Identity Services Engine Device Admin - license	1	$8,629.99	$8,629.99
DHCP Software	Cisco Prime Network Registrar DHCP	1	$16250.00	$16250.00
Server Rack	StarTech.com 4-Post 18U Open Frame Server Rack	6	$277.99	$1,667.94
Server Rack	StarTech.com 4-Post 24U Server Rack Cabinet	1	$839.00	$839.00
Cable	Monoprice Cat6 500ft Spool	4	$89.99	$359.96
Cable	Black Box GigaBase 350 CAT5e 1000ft Spool	120	$259.99	$31,198.8
Blank Patch Panels	Tripp Lite 24-Port 1U Rack-Mount Shielded Blank	36	$39.99	$1,439.64

	Keystone/Multimedia Patch Panel			
Patch Cable	Monoprice Cat5e 6in Black Patch Cable	744	$0.89	$662.16
Patch Cable (switches)	Monoprice Cat6A 6in Blue Patch Cable	36	$0.99	$35.64
Transceiver	Tripp Lite SFP+ Transceiver RJ45 Cat6a 98ft	84	$174.99	$14,699.16
Server	Dell PowerEdge R240	2	$2,074.00	$2,074.00
			Total	$120,017.3

5. Subnets

Table 1: IPv4 Subnet Result for 172.16.0.0

Network Address	172.16.0.0
Usable Host IP Range	172.16.0.0 - 172.16.63.254
Broadcast Address	172.16.63.255
Total Number of Hosts	16,834
Number of Usable Hosts	16,832
Subnet Mask	255.255.192.0
Binary Subnet Mask	11111111.11111111.11000000.00000000
IP Class	B
CIDR Notation	/18
IP Type	Private

Table 2: All Possible Networks for 172.16.x.x

Network Address	Useable Host Range	Broadcast Address
172.16.0.0	172.16.0.1 - 172.16.63.254	172.16.63.255
172.16.64.0	172.16.64.1 - 172.16.127.254	172.16.127.255
172.16.128.0	172.16.128.1 - 172.16.191.254	172.16.191.255
172.16.192.0	172.16.192.1 - 172.16.255.254	172.16.255.255

Table 3: Hardware Recommendations

Hardware	IP	Subnet	Type	Location
Router(s)	VLAN 10 (172.16.0.2)	172.16.0.0	Network	MDF
Core Switch 1 (TenGigE 1-18)	VLAN 20 (172.16.64.1) VLAN 30 (172.16.128.1) VLAN 40 (172.16.192.1)	172.16.0.0	Network	MDF
Core Switch 2 (TenGigE 1-18)	VLAN 20 (172.16.64.1) VLAN 30 (172.16.128.1) VLAN 40 (172.16.192.1)	172.16.0.0	Network	MDF
Switch 1 (Gi0/1-7, Gi0/25-31)	VLAN 20 (172.16.64.1)	172.16.64.0	Network	MDF
Switch 1 (Gi0/19-23)	VLAN 10 (172.16.0.1) VLAN 20 (172.16.64.1) VLAN 30 (172.16.128.1) VLAN 40 (172.16.192.1)	172.16.64.0 172.16.128.0 172.16.192.0	Network	MDF
Switch 2 (Gi0/1-12, Gi0/25-36)	VLAN 20 (172.16.64.1)	172.16.64.0	Network	MDF
Switch 2 (Gi0/19-23)	VLAN 20 (172.16.64.1) VLAN 30 (172.16.128.1) VLAN 40 (172.16.192.1)	172.16.64.0 172.16.128.0 172.16.192.0	Network	MDF
Switch 3-20 (Gi0/1-18, Gi0/24-42)	VLAN 30 (172.16.128.1)	172.16.128.0	Network	3rd-8th floor

AP 5 GHz	172.16.0.7 – 172.16.0.64	172.16.0.0	Network	1st-8th floor
AP 2.4 GHZ	172.16.0.7 - 172.16.0.64	172.16.0.0	Network	1st-8th floor
Active Directory 1	VLAN 10 (172.16.0.5)	172.16.0.0	Server	MDF
Active Directory 2 Printer Server	VLAN 10 (172.16.0.6)	172.16.0.0	Server	MDF

Table 5: All Possible DHCP Range for 172.16.x.x

Network Component	Host Range
Infrastructure Components	172.16.0.2 – 172.63.255.254
Employees	172.16.64.2 - 172.16.127.254
Residents	172.16.128.2 - 172.16. 191.254
Guests & Visitors	172.16.192.2 – 172.16.255.254

References

Cisco Business 140AC

Cisco Catalyst 1200-48P-4X

Cisco Catalyst 1300-24XS

Cisco Catalyst 8200-1N-4T

CyberPower Smart App Intelligent LCD OR2200LCDRT2U

C2G Two Port Cat5E RJ45

Belkin network connector (100 pack)

StarTech.com 4-Post 18U Open Frame Server Rack

Tripp Lite 24U Rack Enclosure Server

Monoprice Cat6 500ft Spool

Black Box GigaBase 350 CAT5e 1000ft Spool

Eaton Tripp Lite Series Cat6/Cat5e 110 Punch Down Keystone

Tripp Lite 24-Port 1U Rack-Mount Shielded Blank Keystone/Multimedia Patch Panel

Monoprice Cat5e 6in Patch Cable

Tripp Lite SFP+ Transceiver RJ45 Cat6a 98ft

Dell PowerEdge R240

Cisco Prime Network Registrar DHCP