WEBER'S APARTMENTS

Project 6

Our company will be providing networking services for an apartment complex. There will be 5 apartment buildings at each property, along with a leasing office and amenities. The buildings at the property will have the same layout and each will also have eight apartments per floor and three floors. This gives us 120 apartments at each property with each apartment housing around four people on average. This means that there will be around 480 people that can live at the property and the property could have ten to fifteen employees who need internet access as well.

At the property the leasing office will hold a pool, gym and lounge area that will be available for residents to use. This building will need to provide a wifi connection that any resident can connect to, as well each apartment providing network access for their pertaining residents to be able to use. All staff and tenants will be expected to comply with and follow the Acceptable use policy pertaining to them when it comes to device use and misuse.

For our network design each building will have three floors and there will be eight apartments per floor. Each apartment will have four ethernet jacks placed throughout the apartment. In every apartment we will provide a wireless router or access point for residents to use. Each building will have an IDF that all apartments will connect to. For our switch in each building we will use four Ubiquiti UniFi Switch USW-48-POE rack mountable switches with 48 manageable ports[8]. The first three switches will each support a floor level and be connected to the fourth switch. Our IDF will then connect to our MDF switch using a fiber optic connection and the MDF will connect to the public wide area network (WAN). Our MDF core switch will be

the Ubiquiti US-16-xg that has 10G aggregation capability because it has 12 1G/10G SFP+ ports for our fiber connections.[10]

The wiring will allow for use of coaxial or ethernet devices and wireless access points that use coaxial or ethernet. Residents may provide their own modems or other devices for coaxial connectivity, but we will not be contouring to that end.

There will also be cameras found throughout each floor. The cameras will be placed at the end of each hall and there will also be cameras monitoring the entrance of the networking closet on every floor of the building for security purposes. We chose the Ubiquiti G5 Dome cameras because of the high quality resolution, night vision, and weather resistance.(5)

The max distance that any cable should have to go is 166ft which should be able to be supported by a single cable run to each jack without needing to use any repeaters. We will be using CAT6 cable to connect from the IDF to the apartments. This cabling standard provides up to 10Gbps which should be more than enough for many years. Using CAT6 over CAT5e will help us future proof our wiring. The cameras will also have their cables connected to the IDF for the building. The distance for cables includes distance added to take the cables to the ceiling of each floor in networking closets and bring them to each room and be two feet off of the ground.

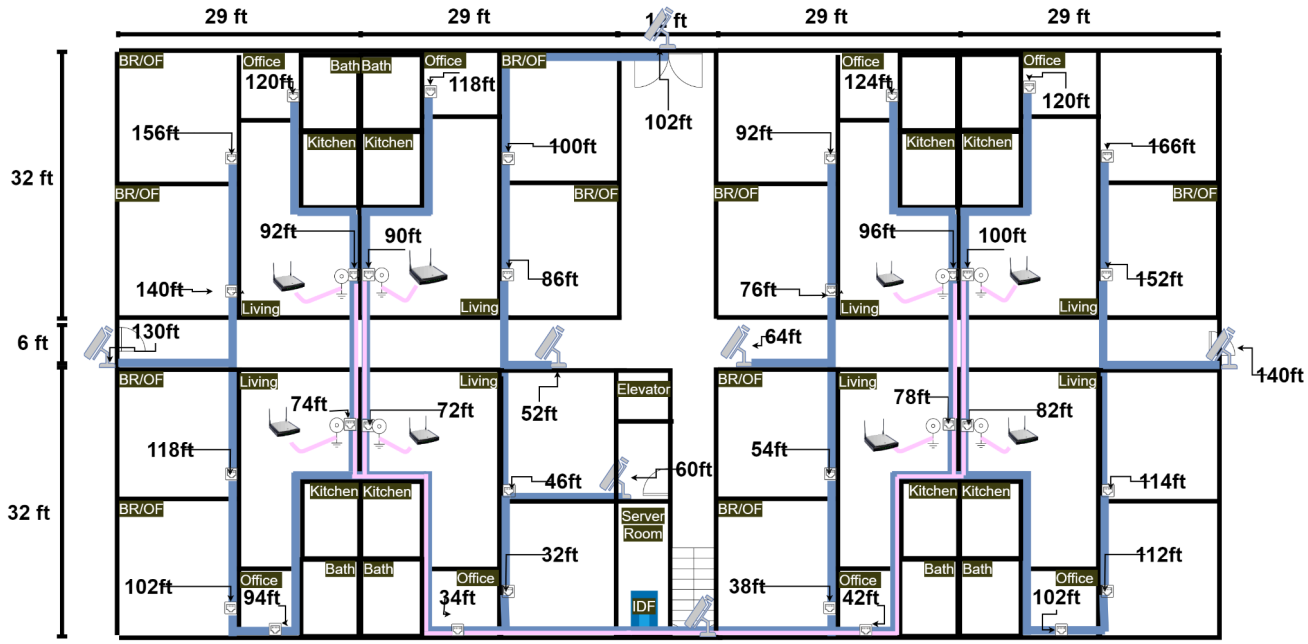

Figure 1 Floor Plan of apartment buildings.

We also have a community building that holds offices for employees of the apartments, and it also holds a pool and gym that will be used by residents of the apartments. This building will need wiring so all employees can have ethernet access at their desks. In our community building we will use wireless access points to provide internet access to residents while they are in the building. We will use the TP-Link EAP653 - Omada True WiFi 6 AX3000 Wireless Gigabit Ceiling Mount Access Point because of the Central Management system, or cloud management system if we choose, the backwards compatibility with 8.02.11 a/b/g/n for any device the residents choose to use, and for the MU-MIMO capability.[7] These locations will also have the Avaya J139 - VoIP phones that will be connected to the Ubiquiti UniFi USW-48-POE leasing office switch as well.[8] The lines will run from the switch to the patch panel and then from there through to the individual RJ-45 ports in the offices and around the leasing office.

Only one of our locations will hold the NVR to store all video recordings. It is the same brand as some of our other equipment and can be connected to the network to view in real time if needed. The hybrid Ubiquiti NVR system allows us to both store video data physically on the premises and be able to view it over the cloud from any location as well. [9]

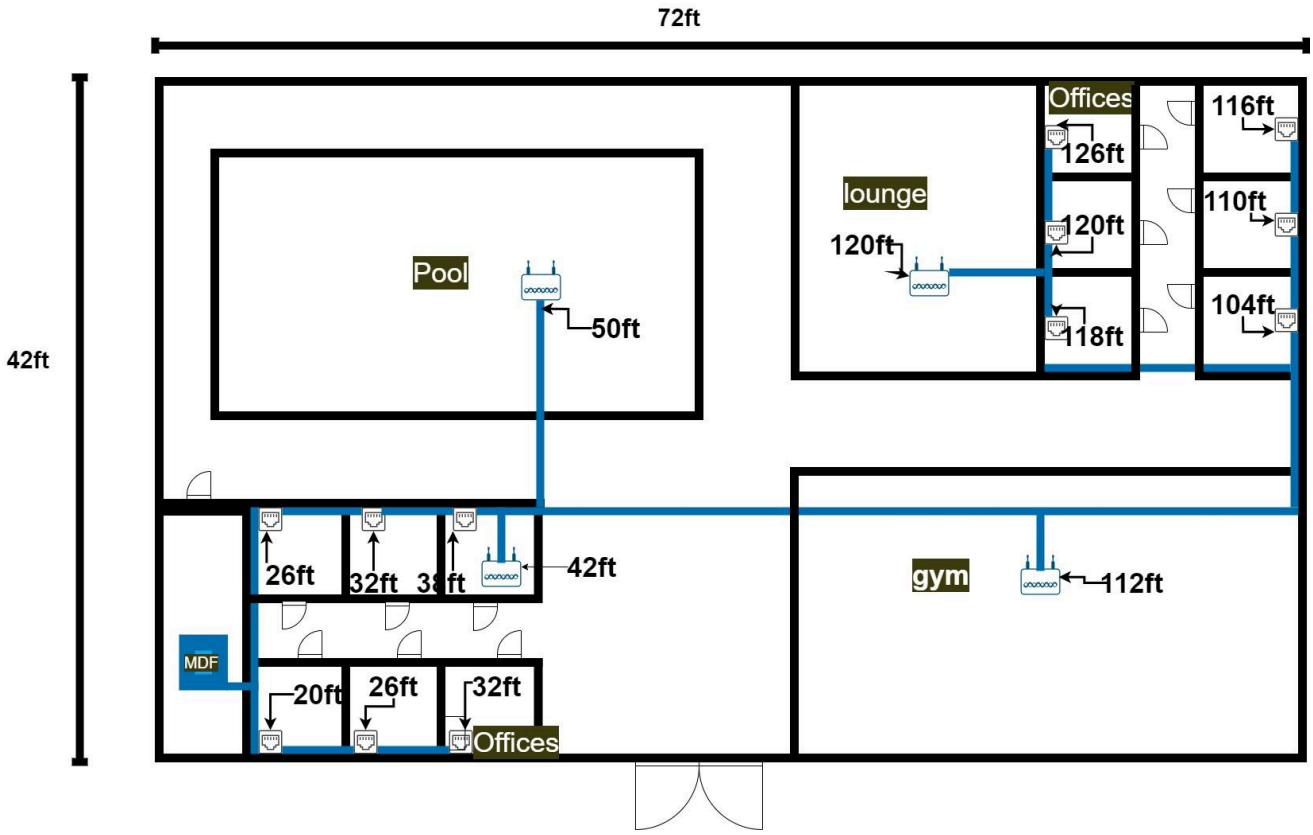

Figure 2 Floor plan of community building.

Each building will be connected together with cables running underground in conduit to get to the networking closets of each building. All of the buildings will go to a community building where the MDF will be located. The edge router will go here in this closet and act as our demarcation point. For our edge router we will use the Lantronix Edge Management Gateway EMG8500 - security appliance. This will provide us with a 2GB connection which should be more than adequate for our needs.(6)

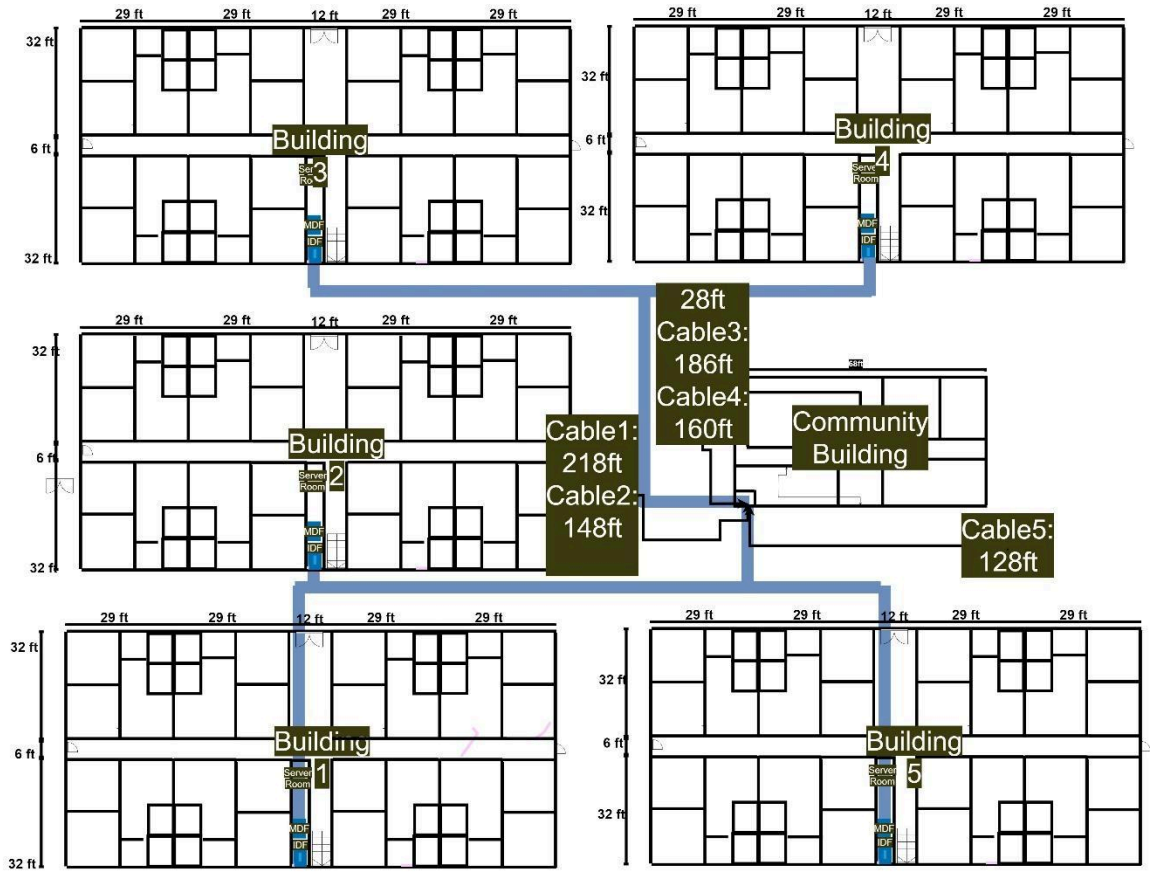

Figure 3 Plan of campus layout.

For our service provider, our first option would be Google Fiber 2 Gig for $250/month[1]. It has almost twice the bandwidth of the next competitor we are looking at. With 2 gigabits download and 1 gigabit upload speeds, we feel focusing on speed and bandwidth is more important than the extra additions with our second choice. We would offer a standard of 20 Mbps guaranteed per customer. That should allow around two devices streaming HD content at the same time whether it be TV, movies, or gaming. With this plan we could offer more bandwidth if the customer wanted to pay a little more. The extra bandwidth could also be used during peak times when more people would be streaming or using the Wi-Fi connections in the

lobby, gym, and lounge areas. This would also offer us more bandwidth for our servers regarding the cameras and VoIP phones.

We would have a choice to use the Wi-Fi 6 router they offer or our own. They also have 2 Wi-Fi mesh extenders if we choose to use them. Google comes with a static IP assignment, so we could later subnet if we were to expand any services or build more units. The 2 Gigabit plan comes with a 99.9% SLA as well.[2]

For our second internet service provider, we would choose to go with Business Internet Gigabit Extra 1.25 Gbps. With the option of unlimited devices, and up to 1250 Mbps for downloads and 200 Mbps uploads at $365/ month[3]. We will charge a flat rate per apartment or residence guaranteeing them 20 Mbps also. This will also allow around two devices streaming HD content at the same time whether it be TV, movies, or gaming. They will have the option of paying more if they want more bandwidth, but the 20 mbps will be included in their apartment rate just like our first choice.

Comcast Business also comes with redundancy if the power or internet goes out with their 4G LTE wireless backup connection. It also comes with some security regarding devices and scanning every 5 minutes if we decided to use their gateway instead of our own. The service level agreement is also 99.9 percent reliability[4]. You can also have a static Ip address for a little extra as well. With the lower total bandwidth, If we chose or in the future choose this one, we may have to put extra effort into monitoring the bandwidth or lower the Mbps guarantee, or raise the cost if customers want more bandwidth.

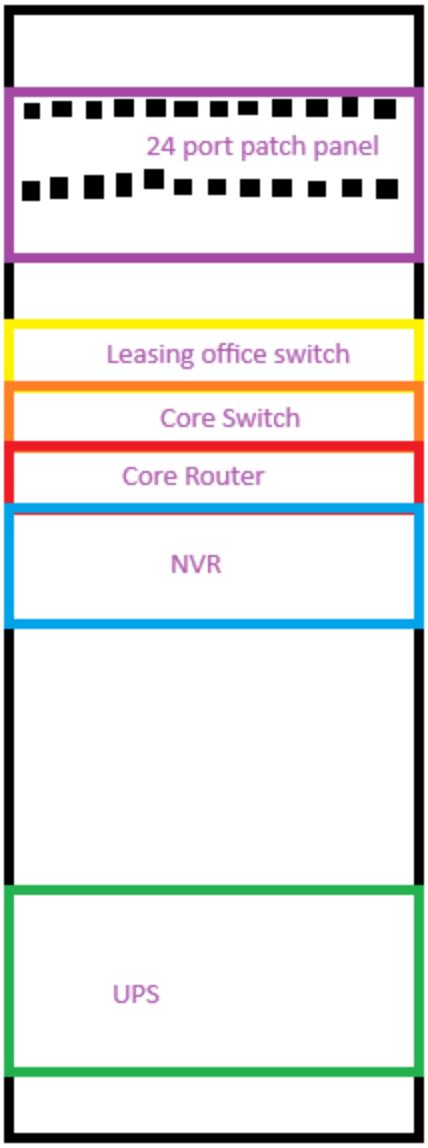

Figure 4 Plan of MDF Rack with Associated Devices

To control all of this we will have multiple spots to implement software on the core router itself, the switches in each complex unit, or on the router in each unit. Extra bandwidth will be dispersed between the overhead from the residential throughput, people that pay for more, or during peak hours on the Wi-Fi network in the lounge, swim, and gym areas.

We will monitor the bandwidth and make sure where it goes depending on QoS with voice, streaming, or video but also control it with Bandwidth Management so users can't consume too much. We will use traffic shaping during peak hours depending on what the baseline is for our network such as video or gaming during the evening hours.

For our network design each apartment will be put on its own VLAN. Every VLAN will be numbered based on the location and building at the location. All VLANs will use private IP address pools with a scope that is 64 addresses in size. This will give each VLAN a range of 10.X.X.X/26. This should be more than adequate for any need that will arise in any apartment. Some devices that could be used by residents on the wireless network include cell phones, video game consoles, TVs, printers, and laptops. All devices in the wireless network connect to the access point that will connect to the switch over a wired connection.

Wired network devices that could be connected to the network include game consoles, PCs, phones, and printers. The wired and wireless connections will all be on the same VLAN for each apartment.

One option for wireless authentication is that each apartment will have a wireless router that residents of an apartment can connect to. Each apartment will have its own SSID and password setup. The routers will use WPA version 2 or 3 with a PSK for authentication. The residents of the router will be able to control who they give the password to.

The community building will have the APs connected on a guest network that residents will be able to connect to using a username and password. The network will be set up so no devices on the network can communicate with each other or see what traffic the other devices are generating. There will also be a network that will be used by employees of the apartment

complex known as the leasing network. They will be separated so that we can ensure ideal bandwidth and speed for those who work there especially, as internet connection is essential to their daily tasks and duties. This also ensures that those on the guest network have an ideal connection as their network isn't being burdened by those working on the premises with the various phones and computers connected to the network.

Another option for wireless authentication is each apartment will have a wireless access point that connects to a RADIUS server found in the MDF that users will connect to for access. Each apartment will get its own account that all residents of the apartment use to connect to both the wireless and wired networks. This will allow use of 802.1x to dynamically assign a user a VLAN, which is based on their apartment no matter where they are connecting to the network. This will allow residents to connect to the network in any apartment and in the community building as well.

In the community building we will provide access points for users to connect to the network. The access points will connect to a RADIUS server using the same login credentials that residents use to connect to the network in their own apartments. This will allow us to use one SSID across the entire campus. There will also be a guest network that could be used in the community building that will use separate authentication credentials and be put on different VLANs and given different IP addresses than the authentication credentials that are used in the apartments. There will also be a network that will be used by employees of the apartment and it will also use a RADIUS server for authentication.

For wired internet connections there does not need to be any authentication methods. The ports that are used for wired connections will be designated on the VLAN they go to. This will make wired devices go to the VLAN of the apartment that they are connected to. Devices that are

connected to an ethernet jack are assumed to be trusted because only residents should be able to access the ethernet jacks.

We will assign addresses to each apartment in each building individually. Building 1 will be the start of subnetting the network. It will use the ranges from 10.0.0.0/26 – 10.0.5.192/26. This will give each of the 24 apartments in the building a subnet of 64 addresses to allow for both wired and wireless connections. The VLANs will start at VLAN101 and end at VLAN124.

Apartment	**VLAN**	**Address Pool**
1	101	10.0.0.0/26
2	102	10.0.0.64/26
3	103	10.0.0.128/26
4	104	10.0.0.192/26
5	105	10.0.1.0/26
6	106	10.0.1.64/26
7	107	10.0.1.128/26
8	108	10.0.1.192/26
11	109	10.0.2.0/26
12	110	10.0.2.64/26
13	111	10.0.2.128/26
14	112	10.0.2.192/26
15	113	10.0.3.0/26
16	114	10.0.3.64/26
17	115	10.0.3.128/26
18	116	10.0.3.192/26
21	117	10.0.4.0/26

22	118	10.0.4.64/26
23	119	10.0.4.128/26
24	120	10.0.4.192/26
25	121	10.0.5.0/26
26	122	10.0.5.64/26
27	123	10.0.5.128/26
28	124	10.0.5.192/26

Figure 5 Building 1 addressing table

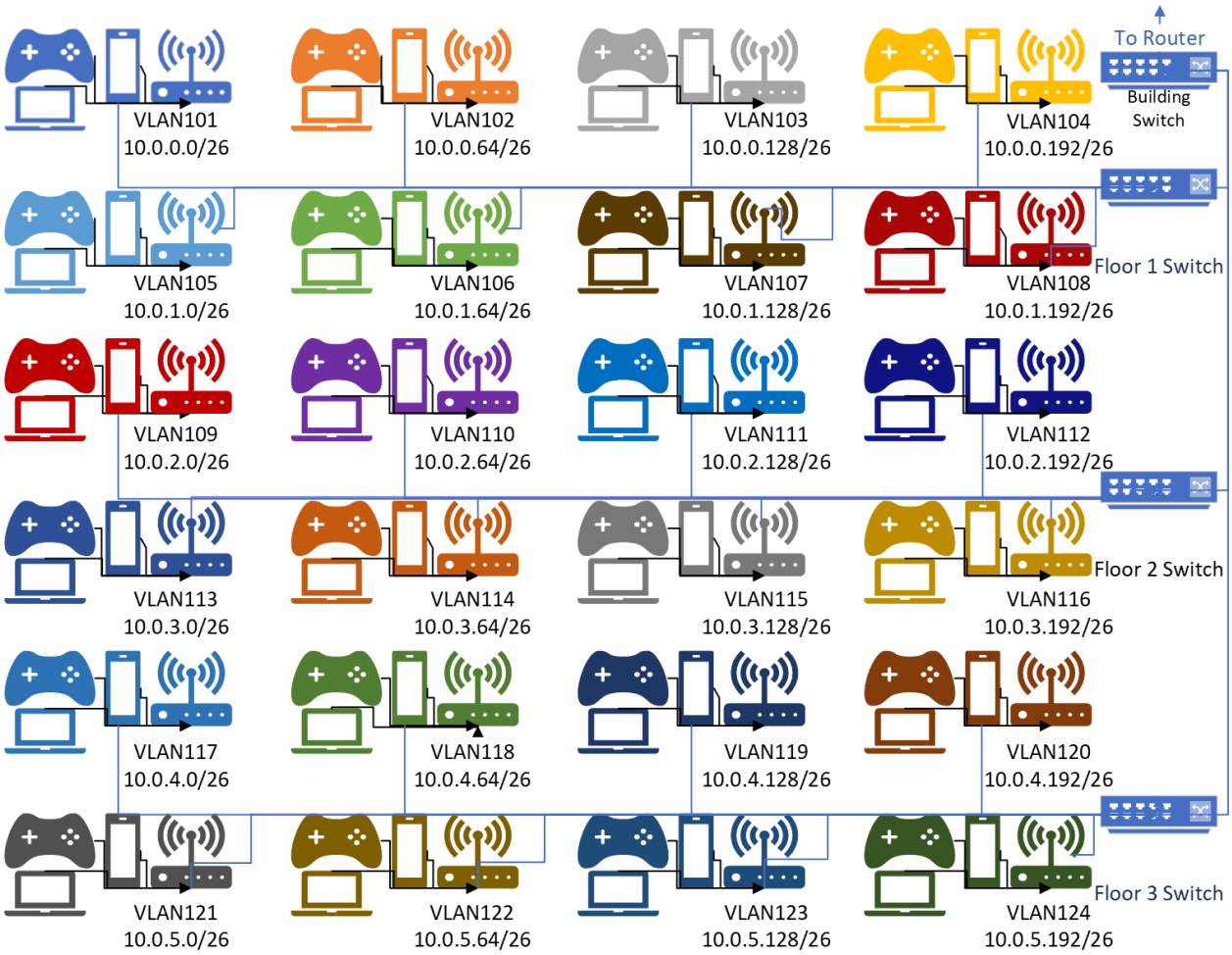

Figure 6 Building 1 wireless network.

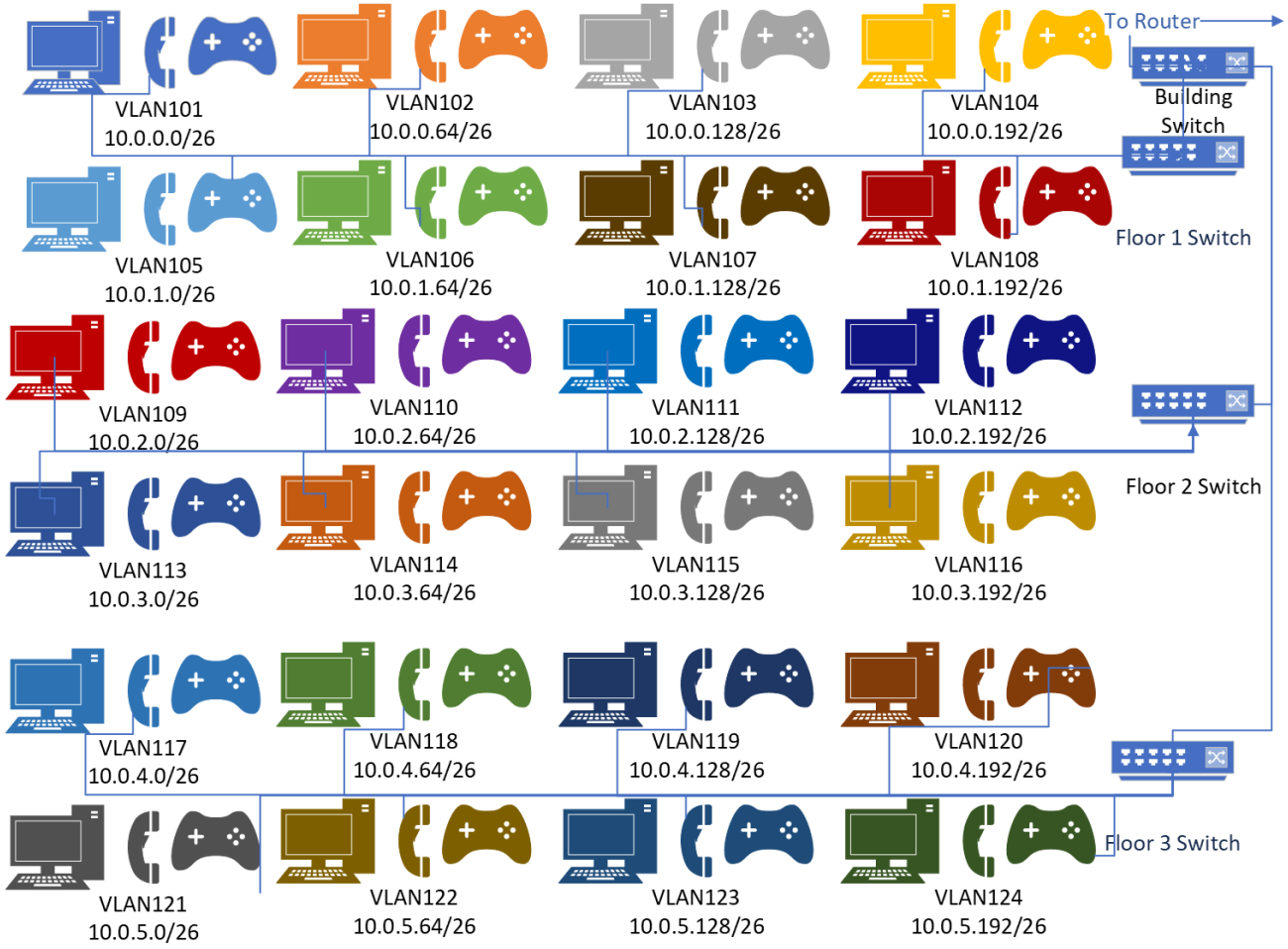

Figure 7 Building 1 wired network.

For Building 2 the subnets will be set up the same way with each apartment getting a range of 64 private addresses. The first network will use 10.0.6.0/26 and the last address range used in this building will be 10.0.11.192/26. This provides 24 address pools for each apartment to get its own. The VLAN range will start at VLAN125 and end at VLAN148. In Building 3 the first apartment will use an address range of 10.0.12.0/26 and the last apartment will use a range of 10.0.17.192/26. The VLAN range will be VLAN149 – VLAN172. Building 4 will use both wired and wireless connections and like the other buildings all connections will go to a

networking closet on the first floor of the apartment. The first range that will be used is 10.0.18.0/26 and the last range that will be used is 10.0.23.192/26. The VLAN range will be VLAN173 – VLAN196. In Building 5 the first range that will be used by a VLAN in this apartment building will be 10.0.24.0/26 and the last range will be 10.0.29.192/26. The VLAN range will be VLAN197 – VLAN220.

In the community building there will be two ranges of addresses. They will be 10.0.30.0/24 for employees and 10.1.0.0/16 for members of the community who need internet access in this building. In the community building there will be 15 VLANs available. They will be VLAN221 - VLAN 235. VLANs 222-225 will be used for wired connections that are used by employees on company devices. VLAN 222 will be used for the property manager and assistant manager. VLAN 223 will be used for offices of leasing agents. VLAN 224 will be used for the maintenance crew and vendors if necessary. VLAN 225 will be used to provide wireless access points for residents to have internet access while they are in this building.VLANs 226 - 235 will be set aside for use for community members and residents as needed.

For each of our other properties we will use a similar addressing scheme but provide a way to distinguish between which location the addresses belong to. In our first location we will use addresses in the range of 10.0.0.0 - 10.9.255.255. In our second location we will use a range of 10.10.0.0 -10.19.255.255. In location 3 we will use a range from 10.20.0.0 - 10.29.255.255. In location 4 we will use a range of addresses from 10.30.0.0 - 10.39.255.255. In location 5 we will use the range of 10.40.0.0 - 10.49.255.255.

The addressing will be assigned the same way at every location to make it simple to set up and understand but the addresses we assign will be different so locations can be identified

based on addresses used internally and the VLANs will be assigned in the same way at each location with different numbers used to identify the location.

For the VLANs that we use in each location we will also use a similar layout as to the first location. We will provide 135 VLANs to use for apartments and other needs with 165 addresses provided to be used in case of future growth and needs. Location 1 will use VLANs 101 - 235 with VLANs 236 - 400 set aside for growth. Location 2 will use VLANs 401 - 535 with VLANs 535 - 700 set aside. Location 3 will use VLANs 701 - 835 and VLANs 836 - 1000 will be set aside. Location 4 will use VLANs 1001 - 1135 with VLANs 1136 -1300 set aside. Location 5 will use VLANs 1400 - 1535 with VLANs 1536 - 1700 set aside.

Building	**Address Range**	**VLANs**
1	10.0.0.0 - 10.0.5.255	101 - 124
2	10.0.6.0 - 10.0.11.255	125 - 148
3	10.0.12.0 - 10.0.17.255	149 - 172
4	10.0.18.0 - 10.0.23.255	173 - 196
5	10.0.24.0 - 10.0.29.255	197 -220
Community Building	10.1.0.0/16	226 - 235
Offices	10.0.30.0/24	221-225
Future Needs	10.0.31.0 - 10.0.255.255 10.2.0.0 - 10.9.255.255	236 - 400

Figure 8 Location 1 Addressing

Building	**Address Range**	**VLANs**
1	10.10.0.0 - 10.10.5.255	401 - 424
2	10.10.6.0 - 10.10.11.255	425 - 448
3	10.10.12.0 - 10.10.17.255	449 - 472

4	10.10.18.0 - 10.10.23.255	473 - 496
5	10.10.24.0 - 10.10.29.255	497 - 520
Community Building	10.11.0.0/16	526 - 535
Offices	10.10.30.0/24	521 - 525
Future Needs	10.10.31.0 - 10.10.255.255 10.12.0.0 - 10.19.255.255	536 - 700

Figure 9 Location 2 Addressing

Building	**Address Range**	**VLANs**
1	10.20.0.0 - 10.20.5.255	701 -724
2	10.20.6.0 - 10.20.11.255	725 - 748
3	10.20.12.0 - 10.20.17.255	749 - 772
4	10.20.18.0 - 10.20.23.255	773 - 796
5	10.20.24.0 - 10.20.29.255	797 - 820
Community Building	10.21.0.0/16	826 - 835
Offices	10.20.30.0/24	821 - 825
Future Needs	10.20.31.0 - 10.20.255.255 10.22.0.0 - 10.29.255.255	836 - 1000

Figure 10 Location 3 Addressing

Building	**Address Range**	**VLANs**
1	10.30.0.0 - 10.30.5.255	1001 - 1024
2	10.30.6.0 - 10.30.11.255	1025 - 1048
3	10.30.12.0 - 10.30.17.255	1049 - 1072
4	10.30.18.0 - 10.30.23.255	1073 - 1096
5	10.30.24.0 - 10.30.29.255	1096 - 1120
Community Building	10.31.0.0/16	1126 - 1135

Offices	10.30.30.0/24	1121 - 1125
Future Needs	10.30.31.0 - 10.30.255.255 10.32.0.0 - 10.39.255.255	1136 - 1300

Figure 11 Location 4 Addressing

Building	**Address Range**	**VLANs**
1	10.40.0.0 - 10.40.5.255	1401 - 1424
2	10.40.6.0 - 10.40.11.255	1425 - 1448
3	10.40.12.0 - 10.40.17.255	1449 - 1472
4	10.40.18.0 - 10.40.23.255	1473 - 1496
5	10.40.24.0 - 10.40.29.255	1497 - 1520
Community and Offices	10.41.0.0/16	1526 - 1535
Offices	10.40.30.0/24	1521 - 1525
Future Needs	10.40.31.0 - 10.40.255.255 10.42.0.0 - 10.49.255.255	1536 - 1700

Figure 12 Location 5 Addressing

In order to allow residents to connect to the wide area network or internet, we will use ISP provided public IPs along with port address translation (PAT). This will allow us to use only a few public IPs while providing connections to many devices inside our network. Port address translation works by assigning ports to a device and using that port with a public IP so many devices can communicate while using the same public IP address. Using port address translation would be cheaper than getting a large enough address pool for each device to have its own public IP address. It might not even be possible to purchase a large pool of public IP addresses that we could even use to meet our needs. We need to offer IPv4 addressing because IPv6 is still a new technology and there are devices that do not support IPv6 addressing.

The entire property will be connected as each building has a switch that has a fiber optic connection coming from outside of the building and these connections will lead to the MDF that is in the leasing office. They will all connect to a core switch that is located in the aforementioned MDF. The core switch will connect to a core router which will be placed at the demarcation point where the connection to the WAN will be provided.

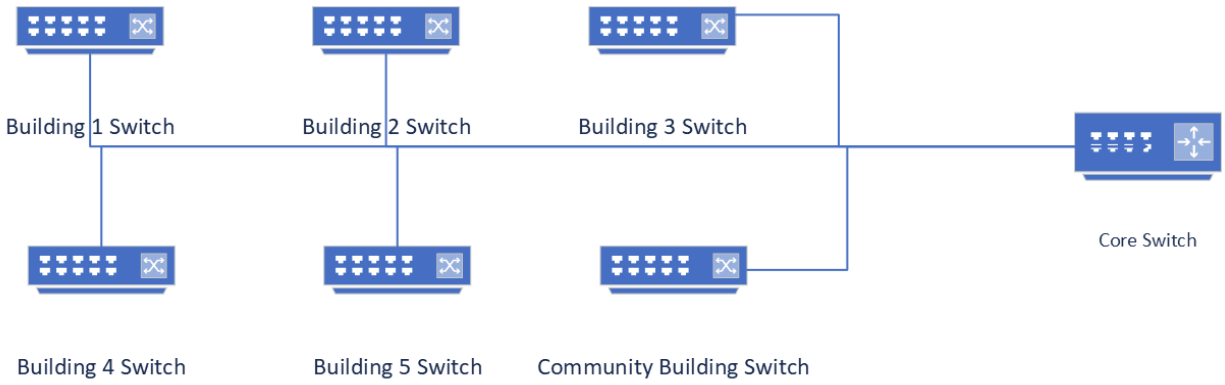

Figure 13 Overview of how switches connect to routers.

For our wide area network we will have five locations where employees will have client to site VPNs installed on their workstations. The devices will use the VPN software to connect to the VPN at the main location. The main location will hold all storage and information that could need to be accessed at any location. The VPN solution will use a regular WAN connection and go over the public infrastructure that already exists. For traffic from residents they will directly connect to the WAN and will not have to go through the VPN.

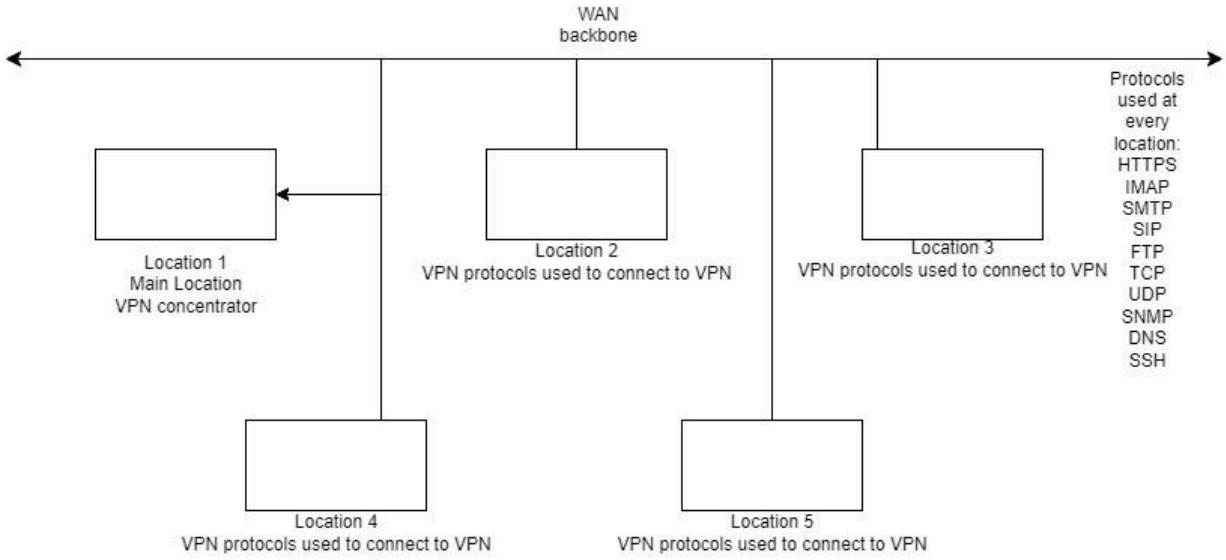

Figure 14 Protocol Diagram

Regarding our access control list or ACL policy, we are basing our solution on The National Institute of Standards and Technology or NIST baseline. In this configuration, we intend to cover access control policies, and mechanisms to assist in securing our network and computer applications. Due to the way in which our organization is set up we have implemented an hierarchical role based access control based on the roles that are outlined in our acceptable usage policy. As for the ACL itself we intend to implement a policy of least privilege, with ports enabled only on inbound connections for our VPN solution which we will be utilizing for remote access to internal systems such as the core switch, and server infrastructure.

Residents will expect to be able to use many protocols when they are connected to the network. They will expect to be able to stream videos, play video games, download files, browse the internet, send and receive emails, and other things that need to be kept secure. Protocols used

on the network will be secure and need access to the WAN so residents can do everything they want to be able to that is safe and secure.

In alignment with standard operating procedure we have outlined two acceptable usage policies. One policy will be business facing and shall exclusively affect employees, while the second usage policy pertains to tenants of the business. These policies were created with the intention of providing security, goals, and expectations of how users should conduct themselves whilst using business resources such as the internet or corporate devices. The employee facing policy reads as follows:

POLICY

All company information and information resources, shall be used in an approved, ethical, and lawful manner to avoid loss or damage to the business operations, image, and financial interests. All users are required to comply with official acceptable use policies and procedures. Employees, personal, and users shall contact the Chief Information Security Officer, or if unavailable the Chief Privacy Officer prior to engaging in any activities not explicitly covered by these policies.

ROLES AND RESPONSIBILITIES

The roles and responsibilities for acceptable use are defined as follows:

CHIEF PRIVACY OFFICER

The chief privacy officer shall be responsible for developing, updating, and maintaining policy on security and privacy issues.

MANAGERIAL STAFF

Managers at all levels shall be responsible for the following:

a) Informing personnel of corporate policies on acceptable use of information resources.

b) Ensuring that personnel under their supervision comply with these policies.

c) Monitoring the physical security, and maintenance of all business property.

SYSTEM ADMINISTRATORS

System administrators shall be responsible for the following:

a) Monitoring systems for misuse.

b) Immediately reporting suspicion or occurrence of any unauthorized activity or security incidents.

c) securing and maintaining all systems, to ensure security policies are being upheld.

CHIEF INFORMATION SECURITY OFFICER

The chief information security officer (CISO) shall be responsible for the following:

a) Developing and maintaining the acceptable use policy.

b) Developing awareness and training materials.

c) ensuring users and employees receive and understand the policies/training provided.

ALL PERSONNEL

All personnel shall be responsible for the following:

a) Abiding by official company policies on acceptable use of information resources.

b) Promptly reporting suspicion or occurrence of any unauthorized activities.

c) Any use made from their accounts.

d) Securing and proper utilization of logon ID's, passwords, PINs, or any other security or access information that pertains to themselves or others.

ENCRYPTION

Encrypting electronic mail or messages shall comply with the following:

Use encryption software and the methods approved by official sources.

a) Place the key or other similar file for all encrypted electronic mail in a directory or file system that can be accessed by management personnel prior to encrypting email.

b) Supply the key or other device needed to decrypt the electronic mail upon request by authorized corporate management.

c) Business related communications both internal and external shall be encrypted to acceptable company standards whenever possible.

INTERNET

Access to the Internet is available to employees, contractors, subcontractors, and business partners, whose duties require it for the conduct of corporate business. Since Internet activities may be monitored, all personnel accessing the Internet shall have no expectation of privacy.

ACCEPTABLE USE

The business provides internet access to facilitate business only. Occasional and minor personal Internet use shall only be permitted if it does not interfere with the work of themselves and others, or the business's ability to perform its needs and duties.

PROHIBITED USE

Prohibited activities when using the Internet or business devices include, but are not limited to, the following:

a) Browsing explicit pornographic or hate-based web sites, hacking or cracking sites, or other sites or environments that the corporation has determined to be off-limits.
b) Posting, sending, or acquiring sexually explicit or sexually oriented material, hate-based material, hacker-related material, or other material determined to be off-limits.
c) Posting or sending sensitive information such as PII or PHI, outside of the business requirements without management authorization.
d) Using other services available on the Internet, such as FTP or Telnet, on unauthorized systems.
e) Posting commercial announcements or advertising material not related to the business requirements.
f) Promoting or maintaining a personal or private business using business resources.
h) Using non-work related applications or software that can cause a degradation or high utilization of workstation or network processing time.
i) Posting, viewing, or otherwise utilizing other persons personally identifiable information (PII) outside of authorized business needs.

j) Stealing or copying of electronic files.

k) Violating copyright laws.

l) Browsing the private files or accounts of others, except as provided by appropriate authority.

m) Performing unofficial activities that may impact the performance of systems.

n) Performing activities intended to circumvent security or access controls of any organization, including the possession or use of hardware or software tools intended to defeat software copy protection, discover passwords, identify security vulnerabilities, decrypt encrypted files, or compromise information security by any other means.

o) Writing, copying, executing, or attempting to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of or access to any corporate computer, network, or information.

p) Accessing the corporate network via modem or other remote access service without the approval of corporate management.

s) Using someone else's logon ID and password.

t) Conducting fraudulent or illegal activities, including but not limited to: gambling, trafficking in drugs or weapons, participating in terrorist acts, or attempting unauthorized entry to any computer or electronic device.

u) Conducting fundraising, endorsing any product or service, lobbying, or participating in any partisan political activities.

v) Disclosing any corporate information that is not otherwise public.

w) Performing any act that may defame, libel, abuse, embarrass, tarnish, present a bad

image of, or portray in false light, the business or any person.

Below is our usage policy that is provided to our tenants as part of their lease:

TENANT(S) ACCEPTABLE USE POLICY

If Applicable, internet and network access may be provided by our service provider Weber Apartments to each dwelling within the apartment complex, and shall be managed by the company. The use of these services by the tenant(s) is subject to the following terms and conditions:

a) Tenant(s) acknowledges that Tenant(s) is receiving the Services selected directly from the respective providers, Weber Apartments is not the internet provider, and has no liability to Tenant(s) for availability, or outages of the Services. However Weber Apartments shall make best efforts to maintain and provide local networking equipment.

b) To provide these services, certain equipment, including amplifiers, distribution cables, lock boxes, connectors, splitters, wall plates, routers, cabling, and other related devices may need to be installed in Tenant's apartment. Tenant(s) shall allow each provider's service personnel reasonable access to the Tenant's apartment for purposes of installing, maintaining, repairing, replacing, or removing this equipment.

c) Tenant(s) agrees not to damage the equipment, and agrees to indemnify, defend, and hold Owner harmless from and against any and all claims, demands, costs, expenses (including legal fees and court costs), and causes of action arising out of, or in any way relating to, actions or

inactions by Tenant(s), including, but not limited to, any amounts Owner is required to pay to cover the costs of any such damage to any provider.

d) Owner reserves the right to switch providers at any time for any reason, change the quantity and quality of the Services provided, or discontinue the Services to the Property at any time and for any reason at its sole discretion.

e) Any breach of this Addendum is a default under the Lease. Additionally, if any portion of Tenant's rent is delinquent, and Owner provides Tenant written notice of the delinquency, and Tenant fails to pay the delinquent amounts within three days after receipt of notice, Owner may be permitted by applicable laws to request that the providers interrupt or terminate the provision of Services to Tenant's apartment (even if Tenant subscribes to enhanced services beyond those Services covered by this Addendum) until all delinquencies are brought current.

INTERNET SERVICES PROVISIONS

The use of the Internet Services by Tenant(s) is subject to the following terms and conditions:

a) Tenant(s) agrees to contact the Provider directly should they desire to order any additional video-related services such as television or on demand video services.

b) Tenant(s) agrees to contact the Provider directly to order any additional Internet-related services other than the Internet Services described and for all concerns involving the connection, operation, or repair of the Internet Services with the exception of repair or assistance with Weber Apartment’s equipment.

c)Tenant(s) agrees to contact Weber Apartments directly in such cases where the user is experiencing issues with equipment provided by Weber Apartments. This includes ports, routers, cables, or otherwise provided equipment.

d) Any use of the Internet Services that inordinately drains bandwidth, such as hosting one or more web sites, operating peer-to-peer file-sharing software, or running one or more servers directly from the Property, is prohibited. Tenant(s) may not use the Services to operate an Internet-based business without prior authorization from Weber Apartments.

e) Any Tenant(s) who receives the Internet Services in his or her apartment shall not install network devices, whether wireline or wireless, to enable any person who does not reside in Tenant's apartment to access the Internet Services. Any wireless network device installed by a Tenant must comply with applicable FCC rules and regulations, and must not interfere with the Services or wireless systems operated by Weber Apartments or any service provider at Weber Apartments properties.

f) Tenant agrees to install, operate, and regularly update anti-virus software on Tenant's computer and install and regularly update any operating system patches available for the operating system running on Tenant's computer to the best of their abilities. If, as a result of any failure to comply with the preceding sentence, the Internet Services provider's ability to provide the Internet Services to Tenant(s) or others at the Property is adversely affected, Tenant(s) may be disconnected from the Internet Services until such time as Tenant(s) demonstrates to the Internet Services provider's reasonable satisfaction that Tenant(s) computer is free of viruses and the operating system is updated.

g) Weber Apartments is not responsible or liable for any activity performed by the Tenant(s), and any illicit activities such as copyright infringement, hacking/cracking, theft, or any other illegal activity utilizing Weber Apartments network infrastructure is strictly prohibited. Failure to adhere to this policy will result in potential legal action, and/or the notification of law enforcement.

h) Weber Apartments is not liable to Tenant(s) for any losses incurred as a result of day trading, e-commerce, or other financial transactions and activities engaged in by Tenant using the Internet Services. If Tenant(s) uses the Internet Services to engage in any of these activities, Tenant(s) does so at Tenant's own risk.

TENANT NETWORK PACKAGES

The following is a detailing of the various packages and services we would offer to our tenants. The flexibility of which allows them to pick and choose the plan and services that apply best to them. This will help ensure quality of life for them and hopefully keep overall property morale high.

ROUTER PACKAGES:

We will offer two router packages to our residents for lease. The first will be the Zyxel NWA1123ACv3. This router covers only a 2.4 gHz bandwidth, although this would be perfect for a resident opting to use the Plus Service Package (detailed below). It has a range such that it will cover the entire apartment unit of a resident, but it will not cover much into the hall. This router is available for lease to tenants at the cost of $15 per month.

We will also offer a TP-Link EAP653 access point for $30 per month. This access point supports up to 2400 mbps (more than adequate to cover the speeds by our network). It also provides a much larger range than the alternative package as it will cover the entire unit strongly, and even cover out into the hallways.

SERVICE PACKAGES:

The service packages would be two-fold. For families whose interests don't require high bandwidth of speeds, we would offer a Plus package. This would include speeds of up to 100 mbps. This would cost the tenant $20 per month and comes with the same security and privacy guarantees as the rest of our network; the sole difference being the reduced speed. This package is ideal for families either of smaller size, of ages outside of peak network usage (assuming the highest ages of network-using people to be 12-50 years old), or other demographics that would use networks less than the average.

Alternatively, the Pro package would include speeds of up to 1000 mbps. This would be the ideal package for your average unit, offering speeds capable of streaming multiple instances of 4K video, gaming, or research capabilities. We recommend this package to everyone as it is the most reliable and strongest signal available. This package comes at the cost of $30 per month and guarantees the same privacy and security that we have always offered.

[1]https://business.comcast.com/shop/offers/detail/9326103044?services=All&internetdownloadspeed=All&contractlength=All&price=All

[2]https://support.google.com/fiber/answer/12143194?hl=en

[3]https://fiber.google.com/business/?gad_source=5&gclid=EAIaIQobChMI2PXiz_6fhQMVDQitBh0IHQaQEAAYASADEgI2vvD_BwE

[4]https://www.business.com/internet/comcast/review/

[5]https://store.ui.com/us/en/pro/category/cameras-dome/products/uvc-g5-dome

[6]https://www.cdwg.com/product/lantronix-edge-management-gateway-emg8500-security-appliance/6183693?pfm=srh#TS

[7]https://www.cdwg.com/product/tp-link-eap653-omada-true-wifi-6-ax3000-wireless-gigabit-ceiling-mount-ac/7363837?pfm=srh

[8]https://www.cdwg.com/product/ubiquiti-unifi-switch-usw-48-poe-switch-48-ports-managed-rack-mount/6150815?fta=1

[9]https://store.ui.com/us/en/collections/unifi-camera-security-nvr-large-scale/products/unvr-pro

{10]https://rspsupply.com/p-27145-ubiquiti-us-16-xg.aspx

[11]https://www.cdwg.com/product/avaya-j139-voip-phone/6907757?pfm=srh