Connecting State College Apartments

IST 220

4/28/23

Mendola | McMillen | Nwauche | Tosatti | Weicker

Table of Contents

[Overview/Executive Summary 3](#_Toc133573454)

[Needs and Requirements 4](#_Toc133573455)

[Security Requirements 6](#_Toc133573456)

[Network Design 8](#_Toc133573457)

[Team Member Responsibilities 15](#_Toc133573458)

[Sources 16](#_Toc133573459)

# Overview/Executive Summary

The town of State College has a large number of apartment buildings that require reliable connection. To provide connectivity between these buildings our team plans to create a network to do so. This network aims to provide a reliable source of connectivity that also ensures the safety of the apartment residents data as a whole. Throughout this document our team will describe important factors that go into this network like description of needs and requirements. This will include important information like network segments, computer systems that will be connected, the site locations, and information about Wi-Fi access. After that, we will be diving into the security requirements necessary for our network and also how our network will comply with many laws. For example, we will be identifying areas that need a special type of security and look into important laws like FERPA, HIPAA, and PCI-DSS. Next, this document will look into the bulk of our networks design with explanations and diagrams of the overall network. This network design will dive into three main aspects being Site-to-Site connectivity, Main site, and Typical Local Site. To end off the network design will be describing our security apparatus which shows the locations for VPN servers, firewalls, intrusions detection system, and more security systems. This makes up the portion of our useful content and the final pages contain information regarding team member duties and sources used during our research. Our network looks to ensure a high level of data security for many apartment residents across the State College area while still having extremely efficient connectivity year-round.

# Needs and Requirements

**List of Computer Systems Connected**

When looking into the computer systems that would need to be connected to the network, this would include gaming consoles, desktops, laptops, televisions, cellphones, printers, firewalls, VPN and more. This network is crucial for students and professors because they will need the ability to use these devices to access the internet, conduct research, and complete homework/tests. These devices will allow the apartment residents to stay educated while also having access to communication and entertainment leaving them fully available to use all of their resources. The software requirements will include certain applications like web browsers, operating systems, email, office or corporate programs, and other niche applications that would apply specifically to the certain apartment resident.

**List of network segments and their uses**

When analyzing the network segments, we wanted to be able to use public Wi-Fi and servers to connect to the apartments. We have decided to use a public ISP to connect the computer systems. This will be the most cost-effective network segment to use since the infrastructure has already been put in place. The public Wi-Fi we will be using is the Xfinity network. Our goal is to connect the public cable internet to each of the apartment’s locations. This will allow the apartment residents to access the internet with each of their devices. Additionally, since we are using public Wi-Fi to connect to each resident’s computer systems, we will need to protect their security. A Virtual Private Network (VPN) must be put in place to ensure security of their data. This will also provide a private network connection for the public Wi-Fi between the individual device and Xfinity server. We also need to place the servers in one main apartment site, specifically one that’s large and in an area that is centrally located between the apartments downtown. Having the servers placed on one main site will permit each building’s local area network to connect to the servers, allowing them to connect to the internet. Finally, we must

**Include Phone (voice), Video, Data, corporate Wi-Fi and "public" Wi-Fi access**

We also need to incorporate corporate Wi-Fi and “public” Wi-Fi access when designing our layout. Corporate Wi-Fi will need to be put in place for the employees in each building. This means it will only be available in the main office of the buildings. Additionally, phone access must be put in place on the first floor of all of the buildings. We must incorporate a voice and video service that will be connected through the internet. As far as “public” Wi-Fi goes, we must ensure that our infrastructure allows for a wireless connection that all residents can connect to. Residents must be able to connect their own devices to this public Wi-Fi right when they enter the building. **List of locations of each site (street address, location, etc).**

* + The Standard- 330 W College Ave, State College, PA
  + The Maxxen- 131 Hiester St, State College, PA
  + Beaver Hill- 340 E Beaver Ave, State College, PA
  + The Metropolitan- 412 W College Ave, State College, PA
  + Diplomat- 329 E Beaver Ave, State College, PA
  + Penn Tower- 255 E Beaver Ave, State College, PA
  + Cedarbrook- 320 E Beaver Ave, State College, PA
  + The Meridian- 646 E College Ave, State College, PA
  + The Rise- 532 E College Ave, State College, PA
  + Bryce Jordan Tower- 463 E Beaver Ave, State College, PA
  + The Legacy- 478 E Calder Way, State College
  + The Graduate- 125 S Atherton St, State College, PA
  + Nicholas Towers- 301 S Pugh St, State College, PA

# Security Requirements

* Pertaining to the VPN in the network, split-tunneling in the network must be disabled especially in the Xfinity server because multiple connections will be concatenated to that server. That way users will not be able to access unsecure and secured networks which could breach the security of the server and cause problems on the site.
* Making sure there is a strong presence of a VPN in the network should align with the guidelines of the HIPAA, this is a policy set in place to safeguard and ensure sensitive information to users will be protected. In accordance with this, the HIPAA Security and Privacy rule should be instilled as a security standard for *Protection of Electronic Protected Health Information.*
* The public ISP to connect the computer systems in the environment should have firewalls in place to prevent unauthorized access while blocking incoming traffic and outgoing traffic. These *must* be installed correctly; only authorized administrators should have control over the systems and data which would inevitably warrant access controls in the environment.
* **FERPA** guidelines will be set in place and followed due to the sites corresponding to a university. The guidelines include security compliances focusing on efforts to protect and safeguard student data, especially when the university is using identifiable information for the student that attends the university. Network Security Policy will be tied into most of the guidelines, particularly with the handling of the firewalls. More implementations to make the network more secure will include intrusion detection/prevention and encryptions.
* Electronic Communications Privacy Act (ECPA): These must be followed for the safety of the students around campus. Guidelines include the prohibition of intercepting electronic communications like emails and telephone calls on the network. The activities of this organization will always comply with the provisions of this law.
* Organization must comply with State and Local privacy and data protection laws. Data retention, breach notifications and data disposal laws. This will be implemented for the protection of personal information which could be accessed by unauthorized users, which could lead to violating legal compliances. Risk management will be set in place to prevent cyber breach attacks to make for secure networks.
* The Computer Fraud and Abuse Act (CFAA) is issued to ensure unauthorized use of the network will be prevented in the computer systems and network. With compliance to these guidelines, malware distribution and hacking will cease completely with the correct implementation of the law’s guidelines in the network.

# Network Design

The first step in implementing our full network design is choosing the most effective way to connect the different apartments with each other. In today’s world, there is a wide range of possibilities when making this choice, such as proprietary fiber, point to point wireless, or in our case, utilizing an ISPs prior infrastructure. More specifically, we have chosen to use the Xfinity network, which consistently appeared in the top three when researching the top ISPs in the area (Top 5, Top 8, 8 Best, 2023). This selection beat out other options such as Windstream’s Kinetic fiber network, Verizon’s DSL option, and T-Mobile's 5g network for a variety of factors, such as speed, cost, reliability, and connection type. Additionally, Xfinity is one of the largest cable internet providers in the United States and offers both cable and fiber connections. In our case, we will be connecting via their cable infrastructure, as service is provided at all our apartment addresses. The cable choice is also much more cost effective, as the infrastructure Is already there, and would not require further installation of the already more expensive fiber service.

Being that we have chosen to use a public ISP, it has become necessary to ensure the security of user data. While there may not be any one specific type of confidential information, residents could be using the internet with a variety of sensitive data, such as payment information or other personal info. Unfortunately, Xfinity does not allow for commercial VPN use on their cable network but states that users “can use a Virtual Private Network (VPN) connection just as long as it’s for your personal, non-commercial use” (Xfinity, 2023). This means that we could provide residents with the information for configuring their own VPNs if desired, which will be explained in greater detail later.

**Site-to-Site Diagram (link provided if too small):**

[**https://pennstateoffice365-my.sharepoint.com/:wb:/g/personal/pjm6188\_psu\_edu/EcgHCAF55OhNuiokWzZNBEsBvWnBx8p7GTF2d2rHMgadRw?e=UmzWcd**](https://pennstateoffice365-my.sharepoint.com/:wb:/g/personal/pjm6188_psu_edu/EcgHCAF55OhNuiokWzZNBEsBvWnBx8p7GTF2d2rHMgadRw?e=UmzWcd)

****

Another critical decision in the project was the proper location for the main site that would function as our primary connection point to the ISP and in turn, the rest of the internet. Given the layout of downtown State College, and the individual locations of our chosen apartments, we have decided to use The Maxxen as our main site. This means that we will house our main infrastructure in this building. This includes devices such as the commercial modem for the direct connection to Xfinity, along with the primary firewall, servers, router, and switches with connections to other buildings. We have chosen this location because it is one of the largest and newest on our list, ensuring space for equipment and a lower chance to be demolished/replaced any time soon. Additionally, it is in a relatively central location downtown. Speaking from a more technical point of view, our network will function as a metropolitan area network, with each building acting as its own local area network. As stated, each of these LANs will flow into The Maxxen’s core network station, where they will be connected to the rest of the internet via Xfinity. While we could simply have each site directly connected to Xfinity’s servers, the project requires a main site, meaning our connections must funnel to one location.

Again, this main site needs to house a variety of important equipment. This includes things such as a web server, which all residents could access to make payments, request maintenance, and complete other necessary tasks related to living within the apartment system. This server will be located in the DMZ as it could be accessed by non-residents looking to live at the apartments in the future. We also want to house our own DNS server for address translation. While this is not directly required considering Xfinity has multiple, it could prove to be faster in certain scenarios, and also provide redundancy case of a failure on Xfinity’s end. We also will house a DHCP server at our main site as a backup in case the integrated router DHCP service fails. Also, being that VoIP is required for the project, we are going to again use Xfinity’s voice service, as this will be provided directly through the modem.

**Main Site Network Diagram:**

[Main-Site Diagram](https://pennstateoffice365-my.sharepoint.com/:u:/g/personal/pjm6188_psu_edu/EVv8cZPZQsNBmvBitVRprbwB3PuYXzusAI9EWc3eFAl_IA?e=FAtET0)

**Diagram

Description automatically generated**

Now that we have determined our network’s core, we can begin to design the “typical local site”, which in our case, is any of the apartment buildings in our network. While each of the buildings may vary slightly in design, the general layout is very similar. Our apartments are generally laid out with an office and common area on the bottom floor, followed by multiple rooms per floor until you reach the roof. Again, while individual rooms may have varied designs, the layout generally consists of a kitchen/living room along with a few bedrooms. For our design, each room will have a wireless access point for all residents to connect, along with ethernet ports in each bedroom. In our case, this infrastructure will act as the “public Wi-Fi” with a connection to the wired network, where residents will bring their own devices to connect. As far as “corporate Wi-Fi” and VoIP telephone service goes, they will be accessible to building employees in the main office, as it is not necessary or cost-effective to have telephone service for each room in 2023. More broadly speaking, each building will have a firewall and router directly connected to our main site. From there, each floor will have its own switch connected to the wireless access points and ethernet ports in each room. For further security and network efficiency, each room will act as its own dedicated VLAN, meaning the switches on each floor will be configured in such a way that segments each room into an “individual network”

**Site Network Diagram:**

[Local Site Diagram.vsdx](https://pennstateoffice365-my.sharepoint.com/:u:/g/personal/pjm6188_psu_edu/EcwyK2dN4bRNukbQho3WFl8BqilquS1To6VRYvcg1cpOOg?e=4QKNA8)

**Diagram

Description automatically generated**

**Security Apparatus**

The locations for firewalls, VPN servers, intrusion detection systems, packet capture systems, as well as logging servers greatly varies. Starting with the Firewalls that need to be implemented within our network design, firewalls will need to be placed as the perimeter of the network, this way the firewalls are able to filter the traffic that is traveling in and out of our network. This is to ensure that all traffic traveling through our newly implemented network on the Xfinity Wi-Fi does not contain any harmful packets going in or out of our design. This will protect the users that are connected within any of the apartments listed in our design. Furthermore, there will need to be firewalls that are implemented within the boundaries of these apartments therefore monitoring the traffic internally ensuring a safe a viable connection option for all our users. Next will be the implementation of VPN (Virtual Private Network). These servers will be implemented within the boundaries of our network, which will make sure that even users outside of the network, if they are within the boundaries can access all resources in our network design without trouble. This will also allow users outside of the network to have full privacy from that outside of the network which will ensure that all packets exchanged within the network cannot be directly accessed from a location far away. Intrusion detection systems are greatly important due to the possibility of hackers from outside of the network. This will ensure we are able to recognize that the network has been compromised (if so) where these systems can monitor and analyze suspicious activity. These intrusion systems will be placed inside and outside of the network and all our critical points. Packet Capture systems will be placed at all important points of the network, ensuring our design efficiently and clearly capture all traffic and analyze the status of all the packets traveling through the network. Finally, the logging servers will be placed internally within the network, this ties into all of the previously mentioned security systems so these servers can receive the logs from the different systems within the network like those of firewalls, VPNs, and Intrusion Detection systems. This will allow us to ensure that all the saved logs are verified and any issues within the network will be analyzed, and the data will be available for further inspection, so that these issues can be recognized, and we can prevent the issue from happening at a later time for any of the users within this network. This allows the Network monitors to gain the knowledge of the issues and gives us the insight to reconstruct the network and ensure all users of the Xfinity network will have an easy and smooth experience within State College. After all, this is the end goal, to have users be able to connect with all apartment buildings allowing for the students at the university to have a seamless connection no matter where they are off campus, and not have to travel to a third-party location to be able to do schoolwork, or conduct business.

# Team Member Responsibilities

* Ian Mendola-Network Design
* Patrick McMillen- Network Design and Diagrams
* Miracle Nwauche-Security Requirements
* David Tosatti- Description of Needs
* Brendan Weicker- Executive Summary, Description of Needs, Overviewing project

# Sources

*8 best internet providers near you: State college, pa April 2023*. InMyArea.com. (2023). Retrieved April 23, 2023, from https://www.inmyarea.com/internet/pennsylvania/state-college

*Top 5 internet providers in State College, PA*. HighSpeedInternet.com. (2023). Retrieved April 23, 2023, from https://www.highspeedinternet.com/pa/state-college

*Top 8 internet providers in State College, PA*. BroadbandNow. (2023, April 21). Retrieved April 23, 2023, from <https://broadbandnow.com/Pennsylvania/State-College>

Xfinity. (2022, September 21). *Use VPN with your Xfinity Internet Service*. Xfinity Help & Support. Retrieved April 24, 2023, from https://www.xfinity.com/support/articles/using-a-vpn-connection

(OCR), O. for C. R. (2022, October 20). *Summary of the HIPAA security rule*. HHS.gov. Retrieved April 26, 2023, from <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>

Davis294, D., Staff, T. R., Crouse, M., Abdullahi, A., Greenberg, K., Okeke, F., & Wallen, J. (2007, June 8). *The importance of an effective VPN security policy*. TechRepublic. Retrieved April 26, 2023, from <https://www.techrepublic.com/article/the-importance-of-an-effective-vpn-security-policy/>

*Research & policy*. National Conference of State Legislatures. (n.d.). Retrieved April 26, 2023, from <https://www.ncsl.org/research/telecommunications-and-information-technology/state-cybersecurity>