Table of Contents

Wireless Network Planning and Installation

Introduction

Immaculate Conception Catholic School has been educating students for 65 years and consists of students through eighth grade. In order to keep up with the ever-changing methods of education and the technology advancements as they become available, the school has decided to upgrade its wireless capabilities. This will make the upgraded technology readily available for all grades but will be utilized primarily in grades 6 through 8. The new wireless network will have the ability to encompass the entire student body, staff, and guests during special events such as graduations and presentations. The wireless must be powerful enough to support live streaming of any event. The system needs to be powerful enough to handle up to 500 concurrent connections and to be able to live stream events.

Because a large amount of cabling is involved, the project can only occur during the summer months when there are no students on campus, making the classrooms readily available. The project timeframe begins in mid-June and ends in mid-August. It is essential that the project is completed on time, as cabling cannot occur when classrooms and offices are occupied.

Background

During meetings between the IT department and administration, the network infrastructure, current software, and the use of iPad programs and electronic text books were reviewed in detail. Because teachers access the student information system, the current method of access was also reviewed. A more robust and highly secure process of access will be thoroughly investigated.

During the evaluation of the current system, it is vital that the project addresses the key issues that are lacking in the current system. These include student access throughout the entire

campus, determining safe and unsafe sites that students may visit, monitoring of the students to make sure they are on task in the classroom, and having sufficient bandwidth with which students, faculty and staff may operate.

Current software programs running on the network servers and controller will be evaluated and recommendations will be made for all necessary improvements. This will be done by an outside entity with no stake in the project. Currently the network servers are running a combination of Windows 2008 R2 and Windows 2016 R2. There is no need to upgrade the network servers or server Operating System.

Since students will be primarily working on iPads throughout the day, all necessary software will be evaluated such as online textbooks, online testing systems, word processing programs, presentation programs, and video programs. Currently the students are using eText books in Math, science, English, and History. Advanced Placement math utilizes an online learning system designed for schools in the Archdiocese of Miami. A list of iPad applications needed for classroom learning will be made by teachers to ensure resources are sufficient. To allow for this usage, updated software for both the firewall and wireless controller will be necessary. A strong mobile device manager that will safely deploy school applications to the students and enforce the necessary software restrictions on the iPads while they are on school grounds will be employed.

Currently Immaculate Conception School has 40 low end Enterasys Networks access points and an Enterasys Networks wireless network controller. The wireless controller is responsible for allowing wireless devices to connect to the network and monitors them to ensure security. The firewall consists of a Sonicwall mid-range firewall which controls access to the Internet. Currently both the wireless controller and firewall are running software that is out of

date and cannot be updated because they are both past their end of life. When software reaches, end of life, no further updates or support are provided by the manufacturer.

WLANs offer a convenient and economical way to expand a local area wired network (Walery, 2004). According to EdTech (n.d.) the steps for creating a new wireless network are to practice active management, use managed wireless products, prioritize usage, develop a guest policy, and build security from the start. Business consumers are expecting additional high speed options when connecting to a network. Since wireless networks give users the freedom to access network resources and the Internet, a wired cable is not necessary. This is extremely essential as many new devices such as iPads and notebooks, do not come with a wired network port. These devices require an alternative method of connection other than a wired connection.

Pierce (2019) addresses the importance of implementing a system that makes proper planning a priority in order to support technological initiatives. The author also points out that bad design is a major contributor to the majority of wireless network issues. Wireless network technology uses a router to allow laptops, cell phones and tablets to connect to the electromagnetic waves generated by the network (Yin, 2019). Once connected these devices use the resources provided by the wireless controller and router to access the Internet. It is up to the information technology (IT) department to determine whether or not internal network resources, such as drive shares, would also be accessible. The author adds that America appears to be changing the way learning is accomplished, as schools, libraries and universities are using WiFi technologies for video learning and video conferencing. A study done by ABIresearch (2019) states that over 20 billion devices will be added to networks across the nation within the next six years.

The IT department, in conjunction with administration, will review the features lacking in the current system. Safety of the students is foremost so the following recommendations will be made:

- 50 Aruba IAP-207 Wireless access points
- 4 Aruba AP-365 Outdoor wireless access points
- Enterasys C4110 Wireless controller running software version 9 or higher. The controller provides management for users, devices, and applications. It also provides added security and filtering.
- Fortigate 200E firewall and router. Currently the latest version of the Fortigate operating system is 6.0.5 which offers extremely powerful protection of resources, both incoming and outgoing. The software allows for advanced privileges for staff as well as a guest option with extremely limited access. Student access is configured based upon built in categories. Categories such as violence and pornography are automatically blocked and placed in a log file for administration to view.
- 11 Extreme Series 210 or 220 High Speed network switches
- 8 APC 2000 Uninterruptable Power Supplies. Power Chute Version 10 will be utilized to shutdown network servers safely in the advent of a power failure.
- Moyle Mobile Device iPad management system

All switches come with 5-year warrantee support and software updates. Each of the components come with a guaranteed 1-day replacement in case of a failure. As part of the assessment, a complete network analysis will be completed which will include application security for all student and software programs. Multi Browser support will be addressed as iPads and Windows workstations use different browser as their default. For example, iPads use the

Safari browser to connect to the Internet, while Windows computers use either Chrome or Edge browsers. Security for browsers is implemented through the network software and the mobile device management system. Applications for the iPad will include Showbie for assignments, Notability or Pages or word processing, Keynote for presentations, HMH and McGraw-Hill ConnectED for online textbooks, iMovie to videos, PicMonkey for photo editing, Prodigy for math, and Quizlet for online testing.

Problem Statement

Currently the school's wireless network does not offer the adequate bandwidth and controls necessary to ensure that sufficient learning and student protection occurs. This is a problem as education is becoming more and more dependent on wireless computing for learning. Schools are moving away from traditional hard textbooks (Leith, 2019) and are being replaced with electronic books from publishers such as Pearson, McGraw Hill, and Cengage for subjects such as math, science, and history.

This can definitely be a problem as insufficient network and Internet access can cause students to not be able to view electronic learning videos, complete eText assignments, take online tests, and communicate effectively within groups. Since parents are required to pay tuition, they expect that the school will keep up with current technology trends. Failure to do so can easily result in parents finding other schools with more advanced technology for their children to attend.

Current cabling is comprised of antiquated category 5 (Cat 5) cabling which does not meet the current standards. Clayton State University (2001) recommends a minimum of Cat 5e cable which became the new standard in 2001. Cat 5 cable is susceptible to interference which can easily cause a slowness to the network. In addition, the current cable does not offer the speed

that Cat 6 offers. This can compromise network security. The current controller does not allow for both 2.4 Ghz and 5.0 Ghz options which is necessary to avoid frequency overlaps between devices (Coextro, 2019). An extremely risky issue is the fact that the current firewall does not allow for separate rules for staff and students that are necessary to ensure the safety of the students.

Wired networks do not allow students to move their desks to another area of the classroom nor do they allow students to move their devices to another area of the school without disconnecting from the network itself. Wireless technology has been prevalent in education over 20 years. As early as 2002, schools have been using wireless technology to overcome the barriers of a wired network (Nagle, 2002).

In order to be competitive with advanced learning technologies, a new wireless network should be employed (Leung & Chan, 2003). The authors addressed that access to educational resources from any point in a school campus is a necessity. Greg LaBrie (2020) states that there are six benefits to implementing a wireless network.

1. Increased mobility allows real-time information while in a different area of a location. This allows a user to go from one area to another without losing connectivity, something which cannot be done with traditional wired devices.
2. Installation speed and simplicity is increased since only the access points in each room need to be cabled. No further cabling is necessary which allows for easy connection and eliminates unnecessary cables that can definitely be a safety risk.
3. Wider reach of the network can be achieved, such as outside areas of the building where network cables are not feasible.
4. More flexibility allows for changes and updates to the network to be fulfilled.

5. Reduced cost of ownership is realized overtime even though the initial cost may be higher.
6. Increased scalability is possible as the network can be configured to meet the requirements of changing application needs.

In addition to the benefits described above, implementing a wireless infrastructure in addition to keeping the existing wired network allows for the ability to promote educational opportunities that result in an extremely sophisticated learning environment (Fong, Hui & Lau, 2004).

Risks

Like any technological changes, there are always risks involved, however in this case the risks are virtually non-existent. This is due to the fact that there is already an operational network in place. The new network will be completely independent of the old one and the final stage will simply consist of moving a few cables from the other controller to the new one. Should there be any failure, the cables can be moved back to the original controller.

Return on Investment

A study prepared by Cisco, showed that productivity increased after a wireless network installation (MobileInfo, 2001). This claim is supported by a study done by Wirelss Lan association, which stated that a return on investment was achieved in less than 9 months. Although there is not an actual measureable monetary return in an educational environment, an increase in student enrollment is the desired outcome of more advanced technology. Jennifer Roland (2017) evaluated the return of investment due to technology in the classroom and concluded that students will be better suited to enter the business world. She added that advanced

technology allows for interaction and collaboration with other students and offers more interactive learning methods.

Audience

In order to have a successful implementation of the proposal, there are several vital groups of participants that need to be included. They include the administration of the school, the faculty, staff, students who will be using the new technology, and other stakeholders such as the school board and parent council. Since the school is a private institution whose primary income is student tuition, it is imperative that the parents be on board as the new system may result in an increase in their tuition payments. These groups should be extremely well informed of the needs, reasons, implementation timeframe, and the overall benefits. The school has a development director who may be able to acquire some or all of the funding needed for implementation. E-Rate funding for schools, which is designated to help fund internet access and the hardware and software necessary to access it, is available on the condition that the school abides by the CIPA regulations. This funding is applied for by the technology department as will supply approximately 50% of the total amount needed to complete the project.

Items to be addressed with administration and school board members will include the coverage area of the wireless network, the number of wireless access points, controllers, and routers. To ensure safety and security a more robust firewall and Internet filter will also be needed. Power protection will also be addressed as Florida is extremely prone to power surges which can be dangerous to electronic equipment.

When addressing these groups, the current state of the network will be explained in great detail. The results of the independent network analysis will be shown and each weakness will be explained in detail with the solutions necessary to resolve them.

The proposal will require that a comprehensive description of the recommended networking infrastructure and software be explained and will include both its advantages and disadvantages. In order to present a solution, a problem must exist and be made known. The needs of the students will be a key selling point as the lack of flexibility and learning potential is limited with a wired network and outdated software. Although the groups will more than likely be diverse, they all share a common goal of high quality education and safety of the students. To assist in relating this information to all stakeholders a complete strength, weakness, opportunity and threats analysis (SWOT) will be created. In addition, a high emphasis will be placed on the repercussions that will entail should the project not proceed.

System Requirements

Requirements Modeling

In order to justify the project proposal, an intense information gathering is vital. To gather the information several interviews will be conducted with all pertinent individuals. Feedback from other schools that have a similar student body will be evaluated. Publishers will also be contacted for resources needed for their eBooks. The information will be put together diligently to produce the systems requirements report.

Outputs

- Firewall security reports
- Open and closed ports report
- URL access reports
- Blocked sites report
- Usage by network protocols
- Network activity

- Firmware versions
- Bandwidth reports
- Listing of all connected devices
- Virtual Lan reports
- Email notifications
- Access Points connections
- Attempt at illegal access
- Signal strength
- Device IP address reports
- Device health reports
- Device App listing
- Proxy attempts on devices
- VPN reports

Inputs

- Vlan SSID
- Passwords for SSID
- Application installation to devices
- New devices
- Device restrictions
- Grade level restrictions
- Application restrictions

Processes

- The system must be able to monitor and control bandwidth usage by device or vlan

- The system must be able to monitor the device database
- The wireless controller must communicate with the Virtual Lan DHCP server to ensure IP address are consistent
- The system must keep track of guest usage to make sure that no internal access is granted
- The system must ensure that devices do not lose connection from an access point
- The system must allow devices to stay connected when a device moves from one access point's domain to another access point's domain

Performance

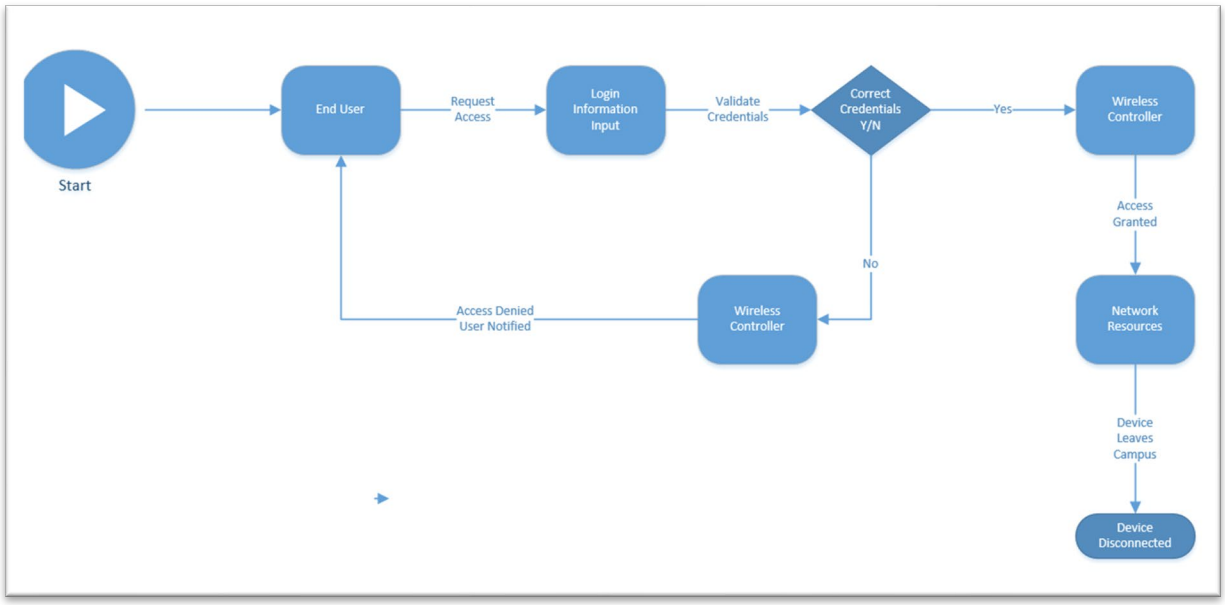
- The system must be able to support up to 1000 devices
- The system must allow access to a device within 2 seconds
- The system must be operational at all times

Controls

- All personal information must be secure
- All data being transferred, whether internally or externally, must be encrypted with the latest encryption methods and protocols
- Each controller and switches must be password protected.
- Devices that violate network policies can be blocked from the system
- The system must be able to set different levels of access based upon vlan
- Students have full set up restriction defined by school and as required by CIPA
- Students have no access to network resources
- Staff have predefined staff access as if they were on a network computer
- Guests have only Internet Access

- All Internet policies are defined in the firewall based upon whether user is a student, staff, or guest
- The system must be able to set different restrictions for individual devices

Data Process Model

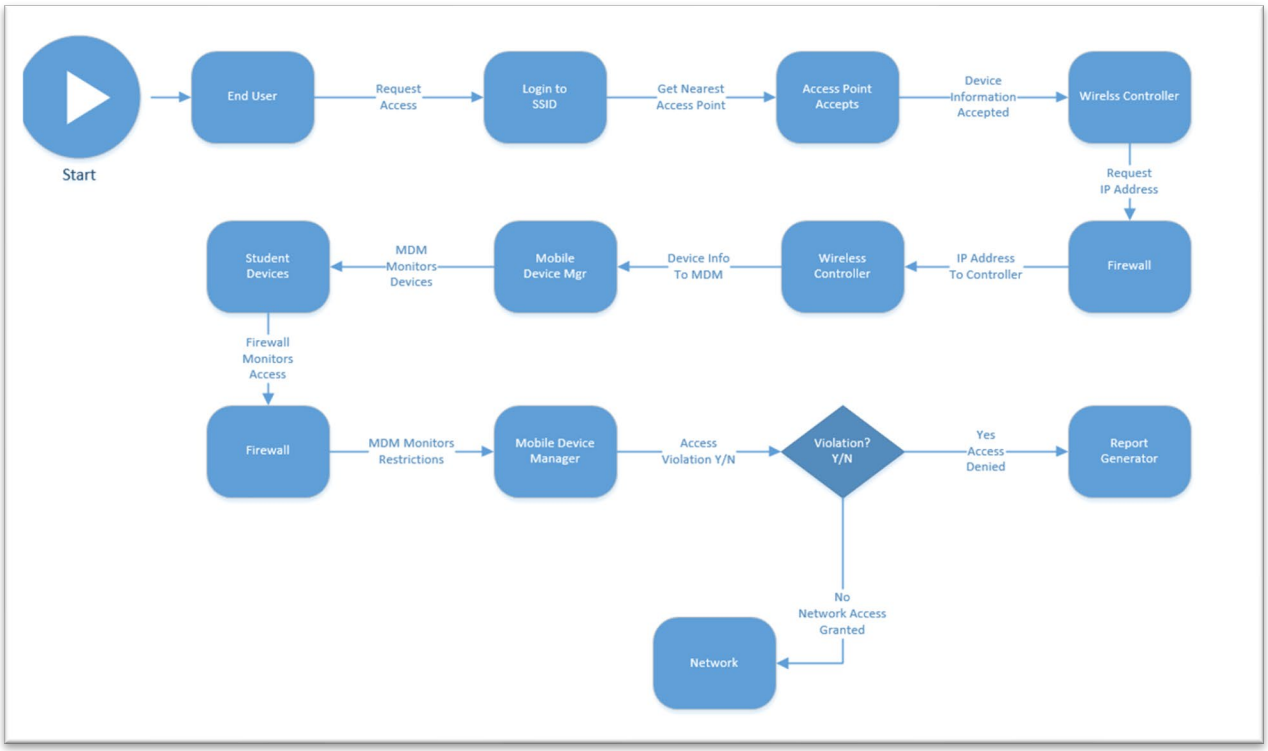


Data Flow Diagrams

There are three data flow diagrams as different users are granted different access and privileges. Students are granted full access to the Internet with the exception of sites that are deemed dangerous as defined either by the Child Information Protection Act (CIPA) or by school administration. In house restrictions are also placed by the Mobile Device Manager (MDM) and enforced by both the MDM and the firewall.

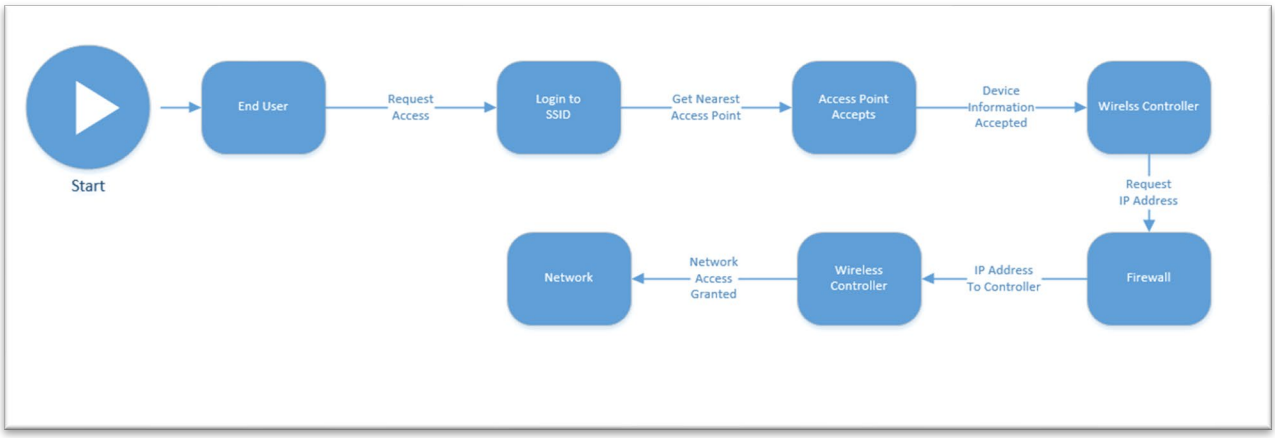
Student Data Flow Diagram

Students are granted only the access they need to access approved Internet sites and applications needed for them to process school work.



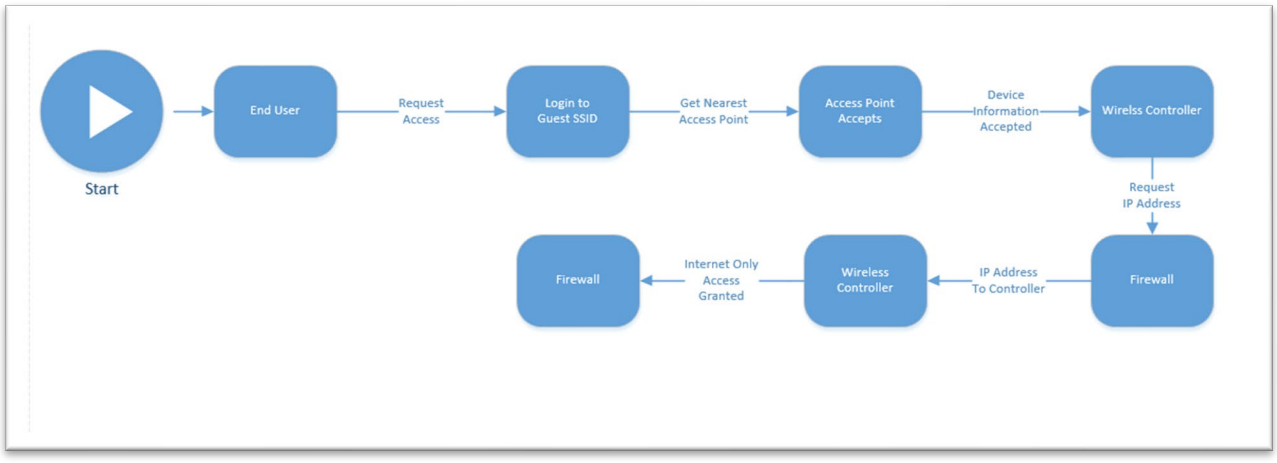
Staff Data Flow Diagram

Staff users are granted full access to the Internet with the exception of sites that are deemed inappropriate by school administration. These restrictions are enforced by the firewall. In addition, staff members have full access to the school's network resources. Authentication and authorization of the resources are granted by network group policy.



Guest Data Flow Diagram

Guest users are granted limited access to the Internet. These restrictions are enforced by the firewall.



Data Dictionary

Student Table

Attribute	Data Type	Description	Required? Y/N
Student_ID	Long Integer	Unique Primary ID	Y
Student_LName	Text	Lastname of Student	Y
Student_FName	Text	Firstname of Student	Y
Grade	Integer	Grade of Student	Y
Homeroom	Integer	Homeroom of Student	Y
Violations	Integer	Violations in term	Y
Num_Violations	Integer	Total Violations	Calculated
Last_Violation_Date	Date/Time	Date of last student violation	Auto Filled

Staff Table

Attribute	Data Type	Description	Required? Y/N
Staff_ID	Long Integer	Unique Primary ID	Y
Staff_LName	Text	Lastname of Staff	Y
Staff_FName	Text	Firstname of Staff	Y
Grade	Integer	Grade of Staff	Y
Homeroom	Integer	Homeroom of Staff	Y

Devices Table

Attribute	Data Type	Description	Required? Y/N
Device_ID	Long Integer	Unique Primary ID	Y
Student_ID	Integer	ID of Student, Links to student table	Y
Device_Name	NumericText	Names of device	Y
IP_Address	Text	IP_address of device, must be unique	Y

MAC_Address	Text	Hardware address of device, unique	Y
Battery_PCT	Numeric	Percentage of battery life remaining	Y
Last_Connection	Date/Time	Date and time of last connection	Y

Connections Table

Attribute	Data Type	Description	Required? Y/N
Connect_ID	Integer	Unique Primary ID	Y
Device_ID	Integer	Links to Device table	Y
Access_Point	Integer	Access Point connected to	Y
IP_Address	NumericText	IP_address of device, must be unique	Y
Vlan_ID	Integer	Vlan connected to	Y

VLANs Table

Attribute	Data Type	Description	Required? Y/N
VLAN_ID	Integer	Unique Primary ID	Y
SSID	Text	Service Set Identifier, normally referred to as the wireless name	Y
Num_Connected_devices	Integer	Number of devices currently connected – auto calculated	Y

Access Points Table

Attribute	Data Type	Description	Required? Y/N
Access_ID	Integer	Unique Primary ID	Y
Room_Numbr	Integer	Room Location of Access Point	Y
Num_Connected_devices	Integer	Number of devices currently connected – auto calculated	Y

Applications Table

Attribute	Data Type	Description	Required? Y/N
APP_ID	Integer	Unique Primary ID	Y
App_Desc	Text	Name of Application	Y
Device_ID	Integer	Linked to the device table	Y

Restrictions Table

Attribute	Data Type	Description	Required? Y/N
Restriction_ID	Integer	Unique Primary ID	Y
Restriction_Desc	Text	Complete description of restriction	Y
Student_ID	Integer	Links to student table	

Violations Table

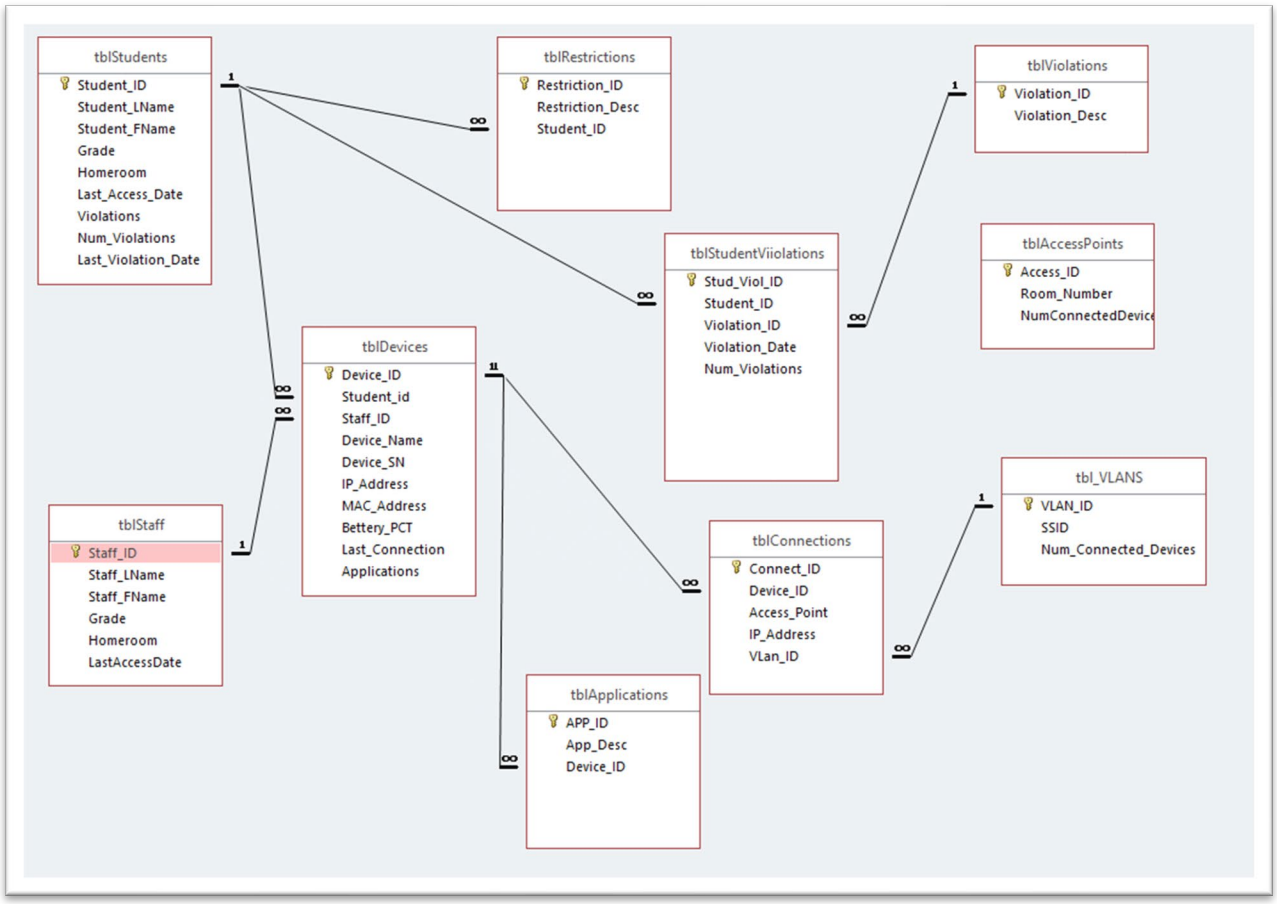
Attribute	Data Type	Description	Required? Y/N
Violation_ID	Integer	Unique Primary ID	Y
Violation_Desc	Text	Complete description of violation	Y

Student Violations Table

Attribute	Data Type	Description	Required? Y/N
Stud_Viol_ID	Integer	Unique Primary ID	Y
Student_ID	Integer	Links to student table	Y
Violation_ID	Integer	Links to violation table	Y
Violation_Date	Date/Time	Date and time of violations	Y
Num_Violations	Integer	Total number of violations - Calculated	Y

A more detailed data dictionary is attached.

Relationships Diagram



Object Modeling

Objects, Attributes and Methods

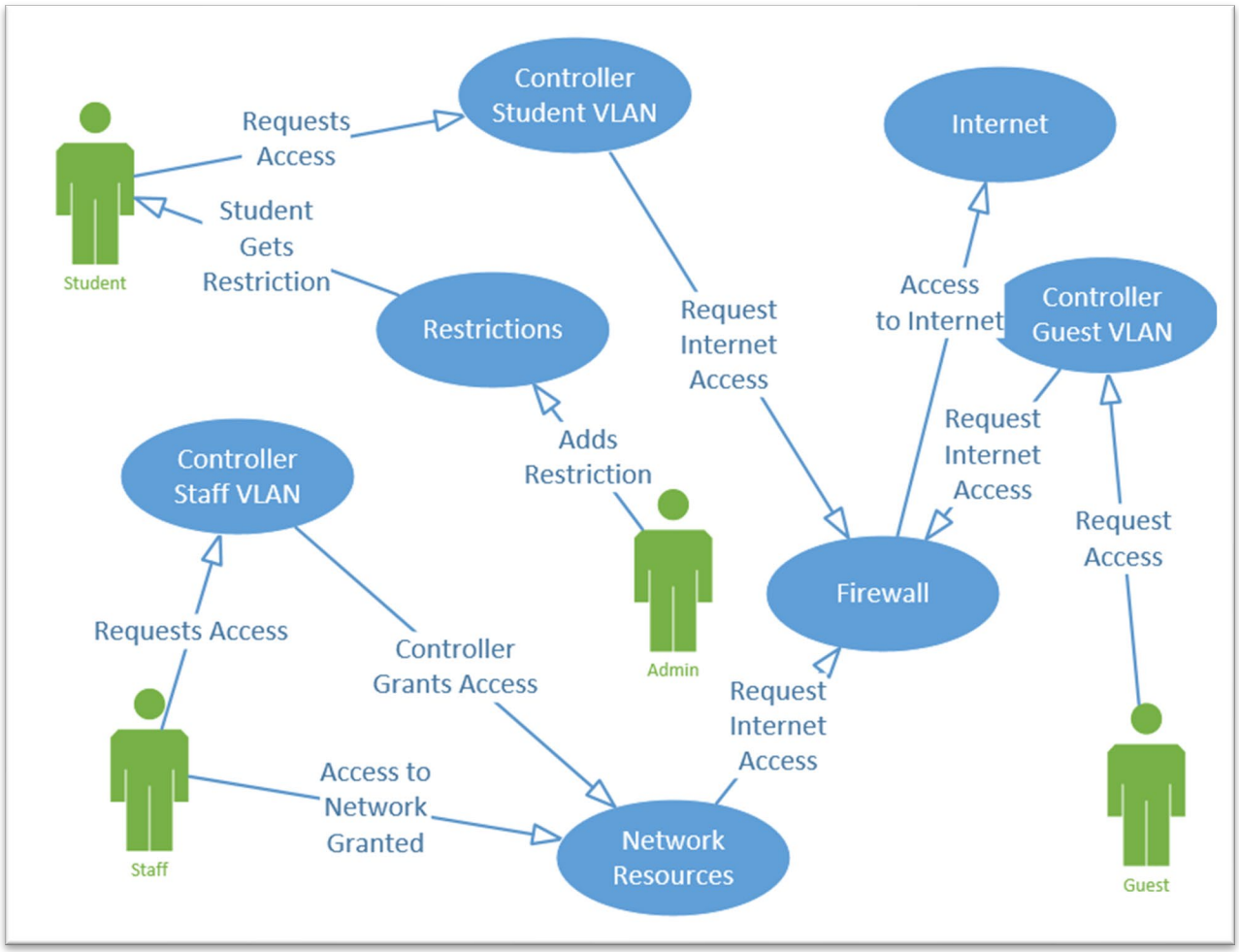
Students	Staff	Devices
Attributes	Attributes	Attributes
Student_ID Student_LName Student_FName Grade Homeroom Violations Num_Violations Last_Violation_Date	Staff_ID Staff_LName Staff_FName Grade Homeroom	Device_ID Student_ID Device_Name IP_Address MAC_Address Battery_PCT Last_Connection
Methods	Methods	Methods
Add Student Edit Student Information View Student Information Add Violation Remove Violation Inactivate Student	Add Staff Member Edit Staff Information View Staff Information Inactivate Staff Member	Add Device Edit Device Information Assign to Student View Device Information

Restrictions	Violations	Student Violations
Attributes	Attributes	Attributes
Restriction_ID Restriction_Desc Student_ID	Violation_ID Violation_Desc	Stud_Viol_ID Student_ID Violation_ID Violation_Date Num_Violations
Methods	Methods	Methods
Add Restriction Edit Restriction Add to student Remove from student	Add Violation Edit Violation Delete Violation	Add Violation to Student Remove Violation From Student

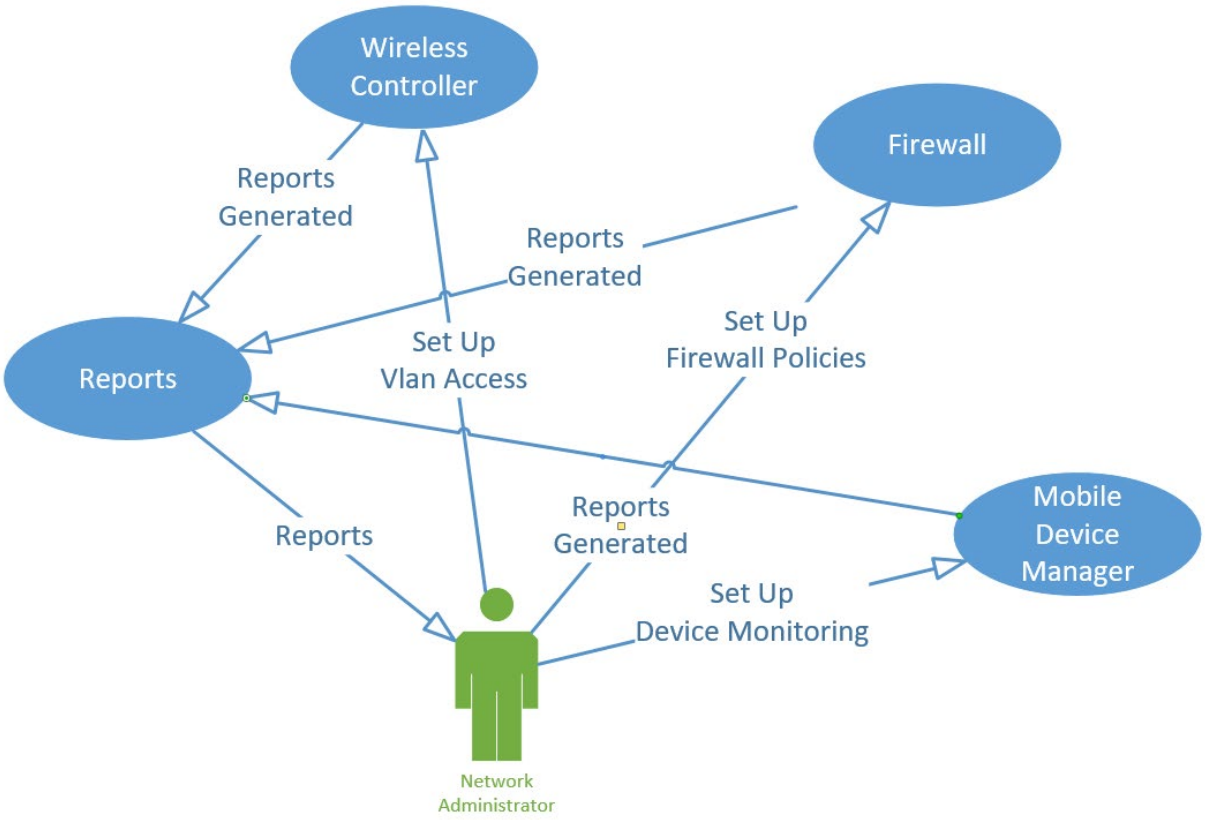
Access Points	VLANS	Connections
Attributes	Attributes	Attributes
Access_ID Room_Number NumConnectedDevices	VLAN_ID SSID Num_Connected_devices	Connect_ID Device_ID Access_Point IP_Address Vlan_ID
Methods	Methods	Methods
Add Access Point Edit Access Point View Access Information Remove Access Point	Add Vlan Add SSID View connected devices	View Connection Information

Applications
Attributes
APP_ID App_Desc Device_ID
Methods
Add Applications Edit Application View Assigned Devices

Use Case Diagram



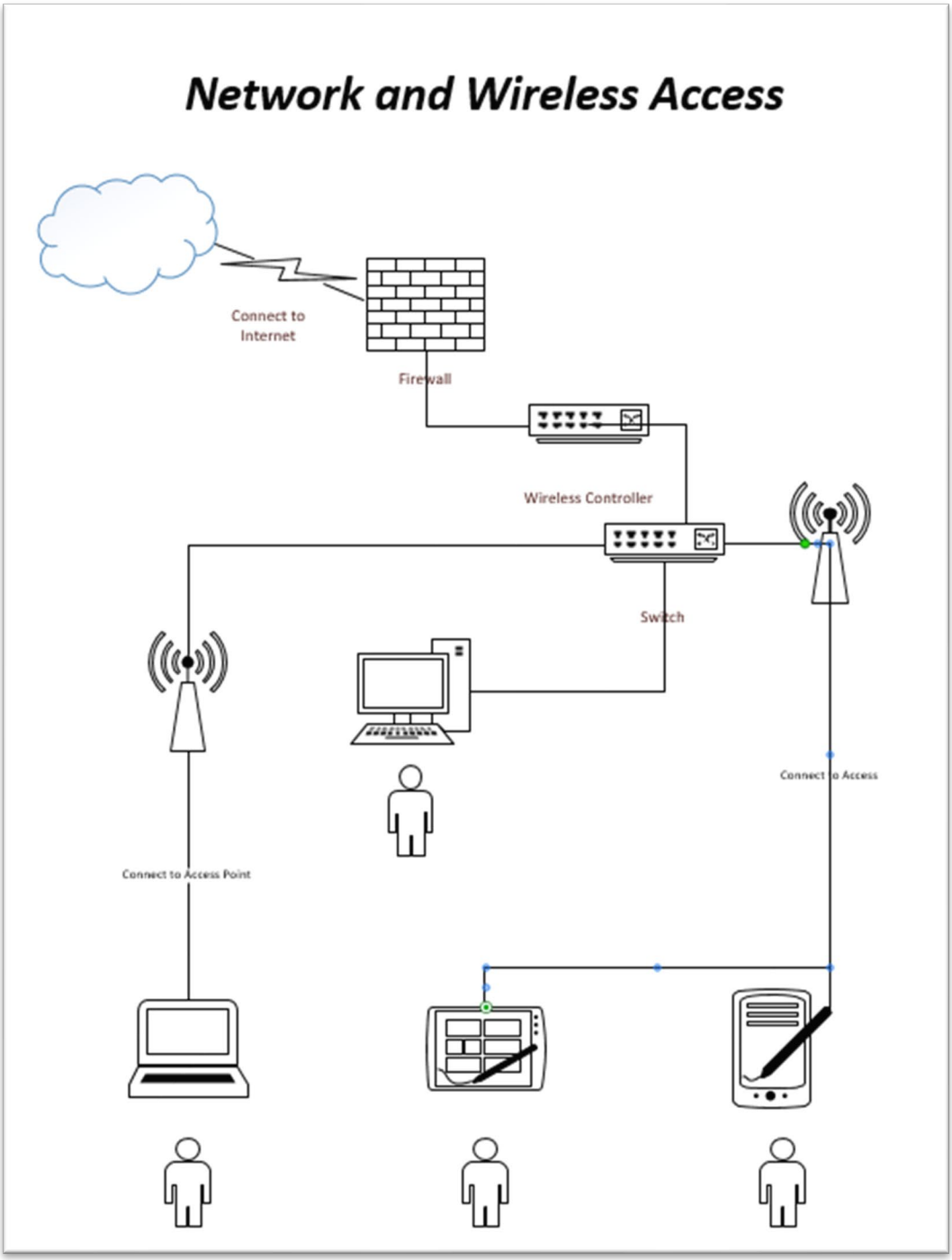
Admin Use Case Diagram



System Design

Specifications

Device Access



Hardware Requirements

- Workstations
  - Windows 8 or higher
  - Processor Intel I3 or Higher
  - 4GB or more Ram. 8 GB recommended
  - 80GB or higher hard drive
  - 1GB or higher Ethernet port
  - Optional 1GB or higher wireless lan card
- Laptops
  - Windows 8 or higher
  - Processor Intel I3 or Higher
  - 4GB or more Ram. 8 GB recommended
  - 80GB or higher hard drive
  - 1GB or higher wireless adaptor
- IPads
  - Apple iPad 4 or higher
  - 32 GB Ram. 128GB Recommended
- Switches
  - Layer 2 or Layer 3 manageable
  - 48 port auto negotiate
  - Trunk ports enabled
  - SFP Fibre optic ready
  - Cisco compatible

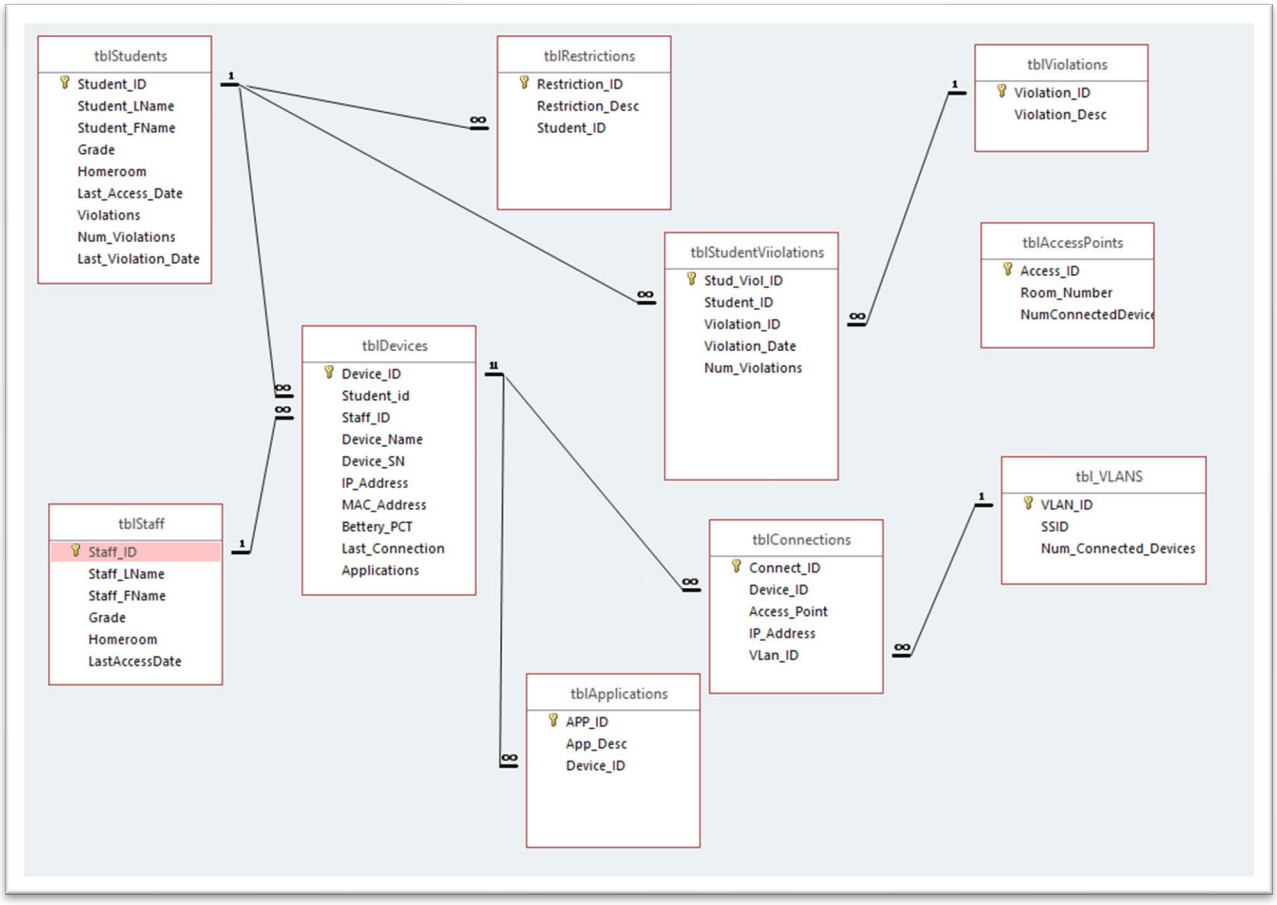
- Router and Firewall
  - 1000 connection capable
  - 10 GB bandwidth capable
  - Port, Protocol and Category control
- Wireless Controller
  - 1000 connections capable
  - Mac Filtering
  - DHCP ready

Data Design

The database server that controls the database is cloud based and can be accessed by any valid secured connection. The secure public and private keys are generated and maintained by Digicert Corporation. The firewall also has its own digital keys as an added level of security. The database consists of 10 tables with each table containing a single primary key. All tables are related to another table with the exception of the Access Points table, which is controlled strictly by the wireless controller. No other table or device has access to the table. All other tables are related by at least one foreign key that references the primary key of the related table. To guarantee data integrity, each table employs referential integrity, which ensures that a non-null foreign key entry can exist without a corresponding entry in the related table. Although by definition, a foreign key can actually contain a null value as long as it is not part of the table's primary key (Coronel & Morris, 2019), null values will not be allowed in any of the tables contained in the database. To make sure that each field has a valid entry, the property table will have nulls set to 'Not Allowed.'

Entity Relationship Diagram

The ERD shows all tables, attributes, and relationship. The diagram also shows that the all tables in third normalization form.



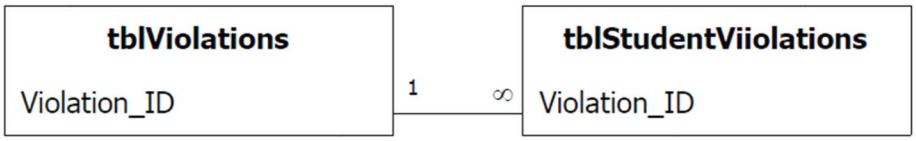
A relational database design requires that all tables be in at least 2NF, which states that no partial dependencies can occur. If a non-prime attribute can be derived from a part of the primary key or a candidate key, the table contains one or more partial dependences (Onsman, 2018), so the table would remain in 1NF. The database for this project will have tables that are all in 3NF, which means that the tables are in 2NF and also do not contain any transient dependencies. No table may contain values that are dependent on an indirect attribute. In other words, the value of attribute cannot be determined by a non-primary key value.

Relationships for each table are shown in the following diagram. All relationships are 1 to many (1:M). Many to Many (M:N) relationships are not allowed in this database. There are actually five levels of normalization, but it is rare that a robust database would need to go past the third level.

Indexes and keys for each table are shown in the following pages.

Relationships

tblViolationstblStudentViiolations



Attributes:	Enforced
RelationshipType:	One-To-Many

Table Indexes

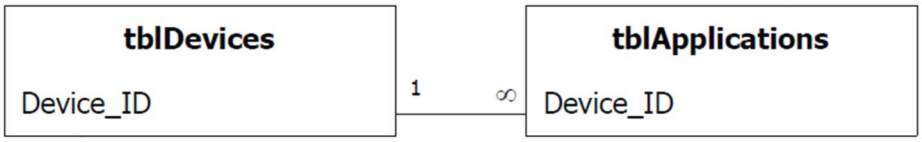
Name	Number of Fields
PrimaryKey	1
Fields:	
Violation_ID	Ascending

Table Indexes

Name		Number of Fields
NumConnectedDevices		1
	Fields:	
	NumConnectedDevices	Ascending
PrimaryKey		1
	Fields:	
	Access_ID	Ascending

Relationships

tblDevicestblApplications



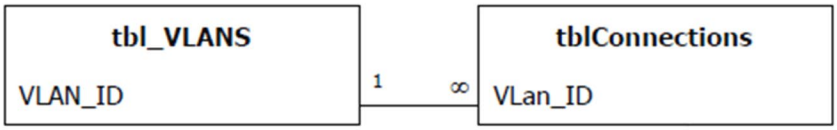
Attributes:	Enforced
RelationshipType:	One-To-Many

Table Indexes

Name	Number of Fields	
PrimaryKey	1	
Fields:		
APP_ID		Ascending
Student_ID	1	
Fields:		
Device_ID		Ascending
tblDevicestblApplications	1	
Fields:		
Device_ID		Ascending

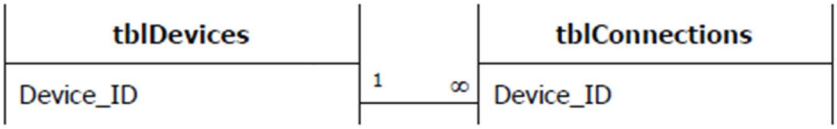
Relationships

tbl_VLANStblConnections



Attributes:	Enforced
RelationshipType:	One-To-Many

tblDevicestblConnections



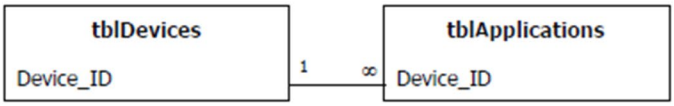
Attributes:	Enforced
RelationshipType:	One-To-Many

Table Indexes

Name	Number of Fields
Device_ID	1
Fields:	
Device_ID	Ascending
PrimaryKey	1
Fields:	
Connect_ID	Ascending
tbl_VLANStblConnections	1
Fields:	
VLan_ID	Ascending
tblDevicestblConnections	1
Fields:	
Device_ID	Ascending
VLan_ID	1
Fields:	
VLan_ID	Ascending

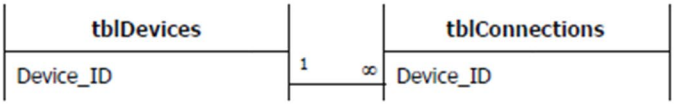
Relationships

tblDevicestblApplications



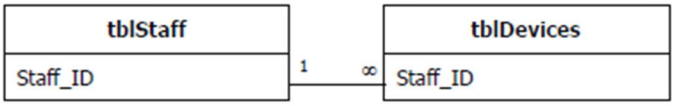
Attributes:	Enforced
RelationshipType:	One-To-Many

tblDevicestblConnections



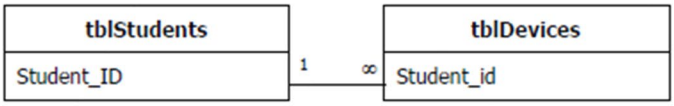
Attributes:	Enforced
RelationshipType:	One-To-Many

tblStafftblDevices



Attributes:	Enforced
RelationshipType:	One-To-Many

tblStudentstblDevices



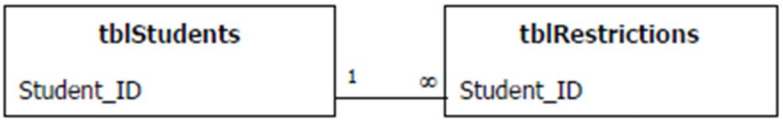
Attributes:	Enforced
RelationshipType:	One-To-Many

Table Indexes

Name	Number of Fields
PrimaryKey	1
Fields:	
Device_ID	Ascending
Student_ID	1
Fields:	
Staff_ID	Ascending
Student_id1	1

Relationships

tblStudentstblRestrictions



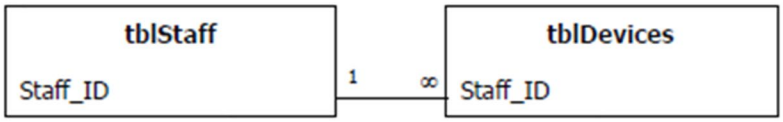
Attributes:	Enforced
RelationshipType:	One-To-Many

Table Indexes

Name	Number of Fields
PrimaryKey	1
Fields:	
Restriction_ID	Ascending
Student_ID	1
Fields:	
Student_ID	Ascending
tblStudentstblRestrictions	1
Fields:	
Student_ID	Ascending

Relationships

tblStafftblDevices



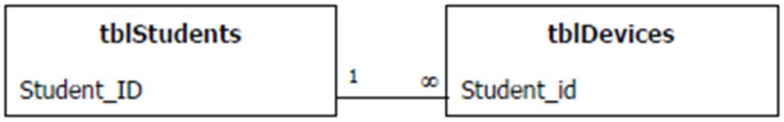
Attributes:	Enforced
RelationshipType:	One-To-Many

Table Indexes

Name	Number of Fields
PrimaryKey	1
Fields:	
Staff_ID	Ascending

Relationships

tblStudentstblDevices

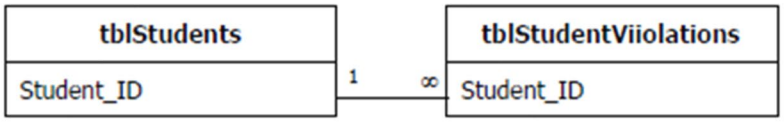


Attributes:	Enforced
RelationshipType:	One-To-Many

tblStudentstblRestrictions

Attributes:	Enforced
RelationshipType:	One-To-Many

tblStudentstblStudentViiolations



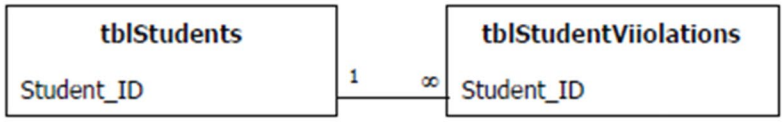
Attributes:	Enforced
RelationshipType:	One-To-Many

Table Indexes

Name	Number of Fields
Num_Violation	1
Fields:	
Num_Violations	Ascending
PrimaryKey	1
Fields:	
Student_ID	Ascending

Relationships

tblStudentstblStudentViiolations



Attributes:	Enforced
RelationshipType:	One-To-Many

tblViolationstblStudentViiolations

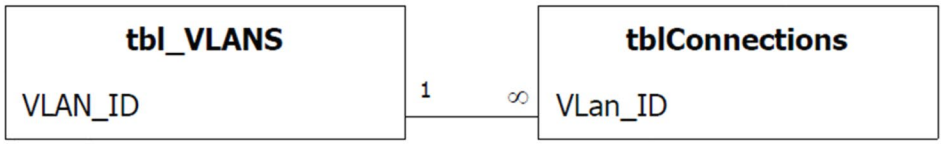
Attributes:	Enforced
RelationshipType:	One-To-Many

Table Indexes

Name	Number of Fields
Num_Violations	1
Fields:	
Num_Violations	Ascending
PrimaryKey	1
Fields:	
Stud_Viol_ID	Ascending
Student_ID	1
Fields:	
Student_ID	Ascending
tblStudentstblStudentViiolations	1
Fields:	
Student_ID	Ascending
tblViolationstblStudentViiolations	1
Fields:	
Violation_ID	Ascending
Violation_ID	1
Fields:	
Violation_ID	Ascending

Relationships

tbl_VLANStblConnections



Attributes:	Enforced
RelationshipType:	One-To-Many

Table Indexes

Name	Number of Fields
Num_Connected_Device	1
Fields:	
Num_Connected_Devices	Ascending
PrimaryKey	1
Fields:	
VLAN_ID	Ascending
SSID	1
Fields:	
SSID	Ascending

User Interface Design

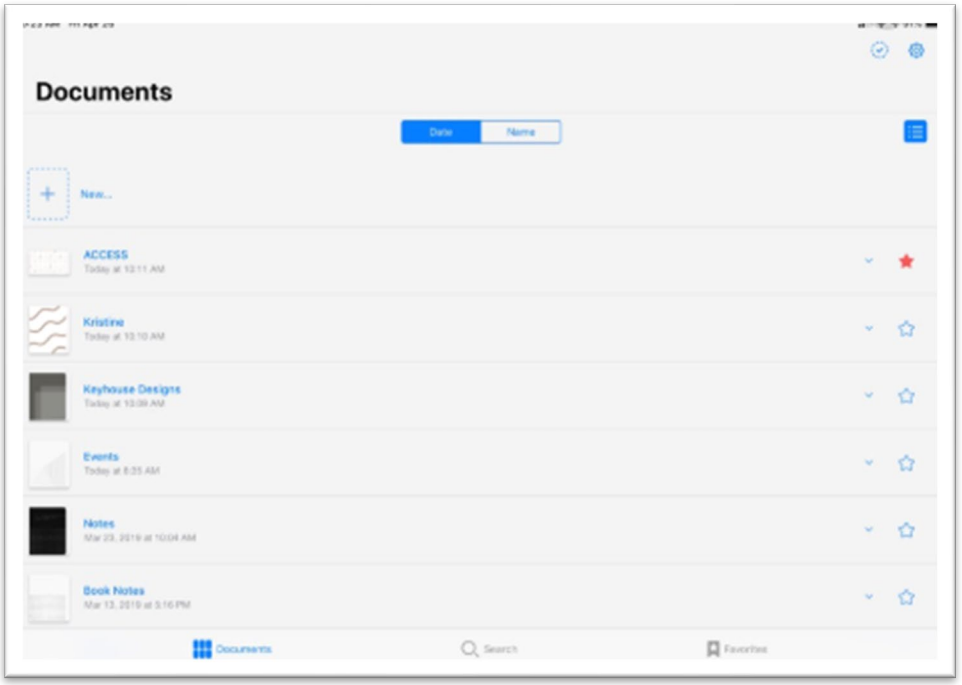
In order to maximize use of the wireless network, the users will need to access an application, which can be automatic or transparent, or initiated by either the device or by the user. A user application will employ a specific program such as a business software program to increase productivity (Tilley, 2020). An example of an automatic application would be a device connection automatically to the wireless network. Unless there is an issue, the user does not have to do anything other than have a device that enters into an area within an access point zone. For

example, a user with an iPad can connect to the school's wireless. When the device leaves the access area, it will be automatically disconnected until the device is within an access area to which it has previously been connected.

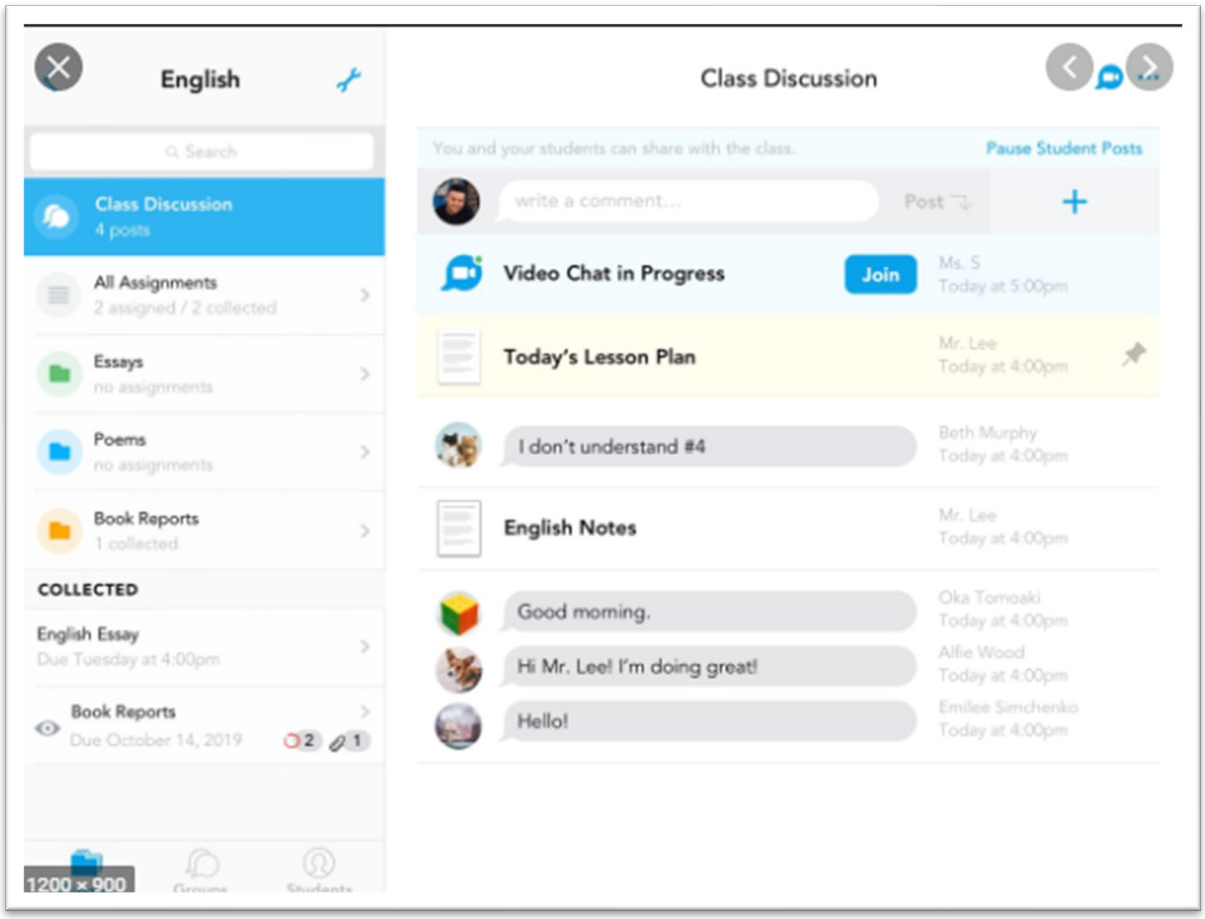
Other software applications must be initiated by the user. Workstations applications include Microsoft Office Programs, Browsers such as Edge and Chrome, Graphics programs, and many more. There are menu items or icons that allow the user to access these applications. For ease of access, all workstations and tablets will have a Graphical User Interface (GUI). For the most part the user will just need to point and click without any actual typing.

Examples of a workstation GUI and iPad GUI are show below.

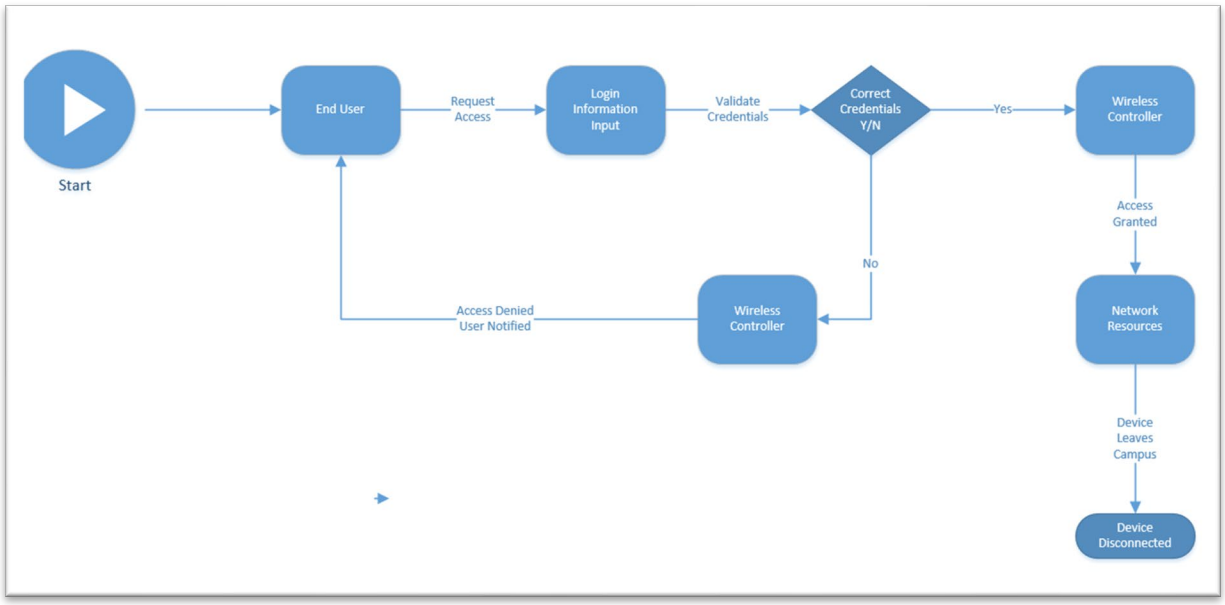
Document processing application for iPad



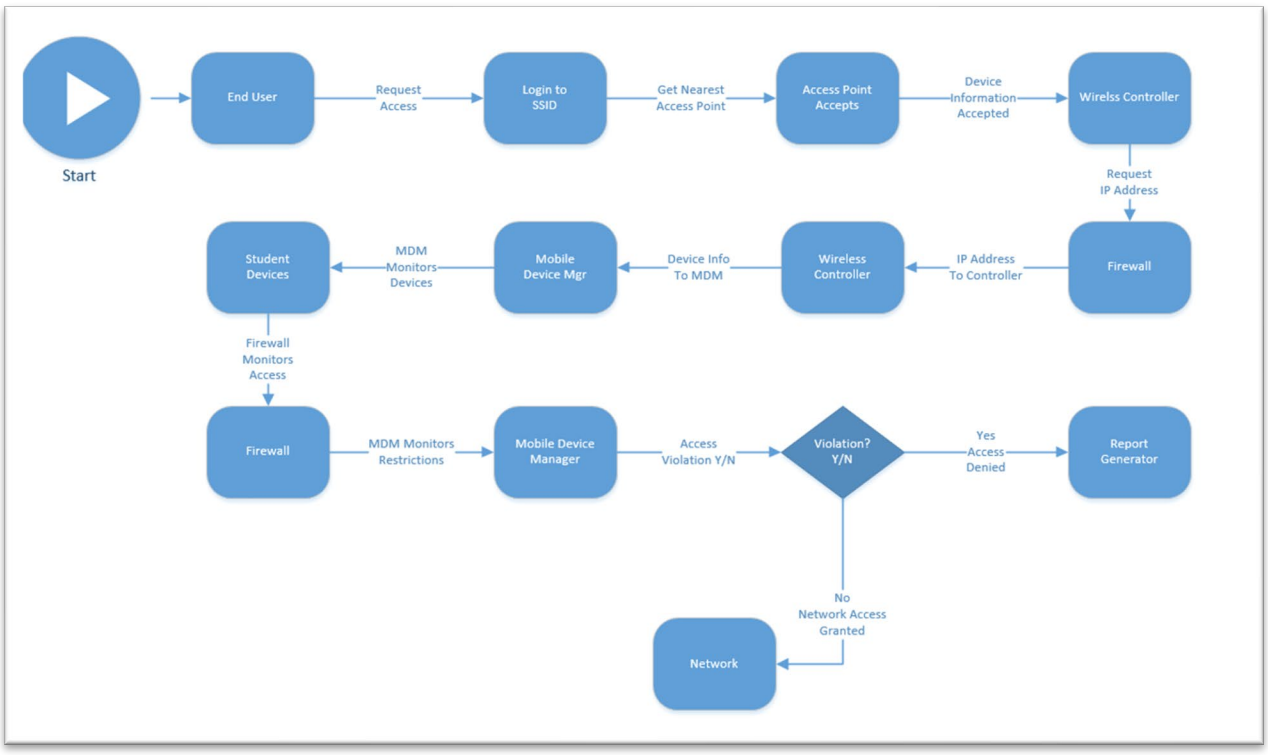
Classroom application user interface for iPad



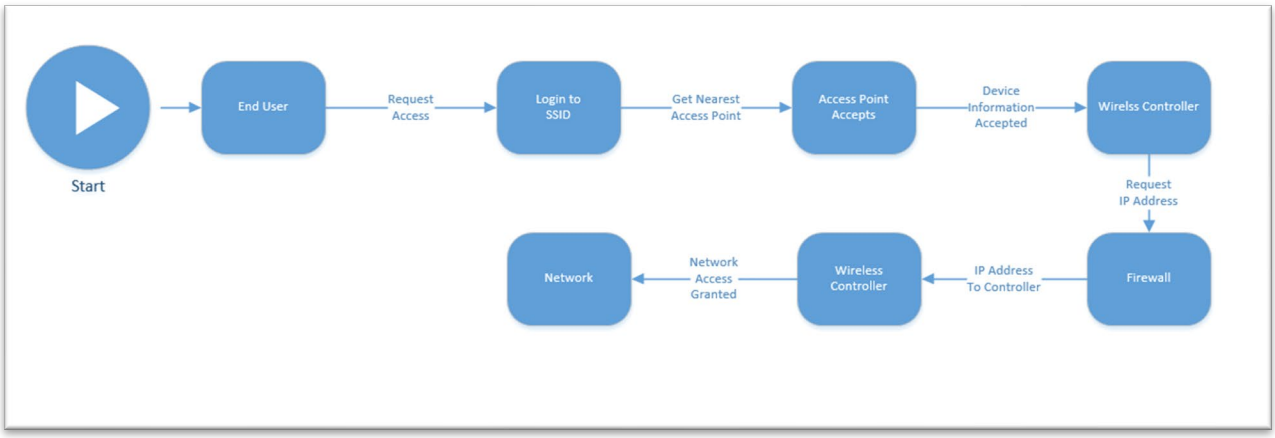
User Interactions



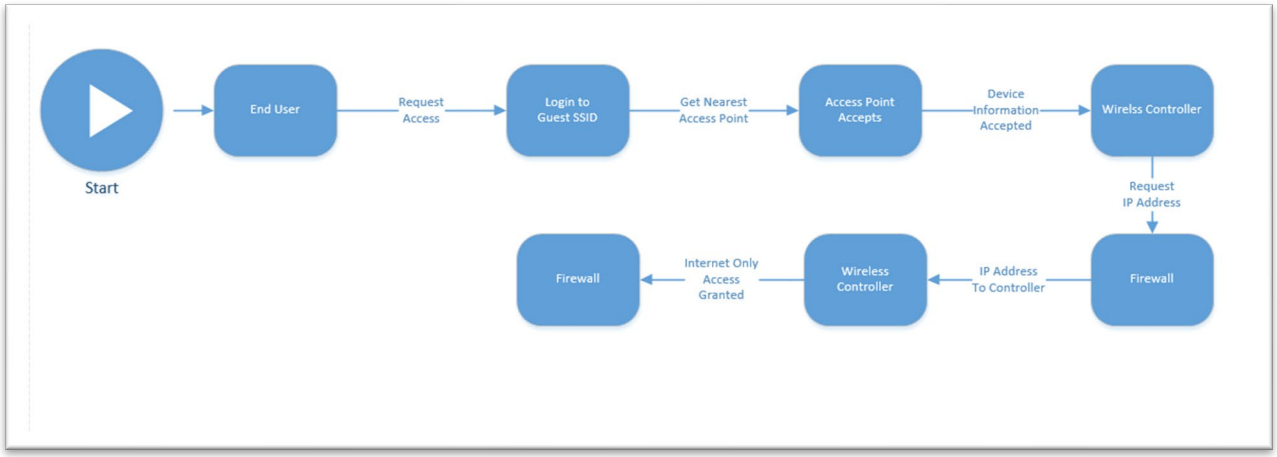
Student Diagram



Staff Diagram



Guest Diagram



System Architecture

Corporate Organization and Culture

To be successful, all wireless devices must operate with complete fluidity. Immaculate Conception School will have three in school wireless policies and one guest policy. Students will have the most restricted policies. Staff will have elevated access, but will not have any administrative access. Administrators will have total access to the system, but will also follow the Information Protection guidelines. Parents and other visitors to the school will receive access

only to the Internet, but the access will be restricted to proper sites and will not include email and shopping sites.

The architectural configuration of the wireless network is designed to boost productivity of both students and staff. Many of the productivity tools do not require a fee which will help to keep costs down. Charged licences for program applications will be reclaimed if the student leaves the school or graduates. The licences belong to the school and are managed by the mobile device manager.

The school's governing body consists of an assembly that is well aware of the diverse nature and needs of the students and the surrounding community. Decisions are made as a group with input from the Director of IT, the Pastor of the church, the financial manager and the principal.

Enterprise Resource Planning (ERP)

Companies that utilize an ERP will create a strategy that encompasses the entire company (Tilley, 2020). An ERP will establish standards that include network access, user interface, security, and how data is processed. Immaculate Conception will employ restricted user access for all students and staff. The firewall, wireless controller, and mobile device management system all produce reports that can be accessed by the database administrator and contain options to generate custom reports such as individuals that have connected to the system after a specific time of the day. The database administrator also has access to a report that shows every application accessed by an iPad during the day, the time of the day that it was accessed, and how long the application was open.

Cost of Ownership

The total cost of ownership which includes items such as equipment, licences and fees, and installation, are classified as hard costs (Tilley, 2020). The author added that training and support are considered as soft costs. Because technology is changing at a rapid rate, all of the equipment purchased comes with five year licencing and support. Comprehensive training to IT staff will be given during the final stages of the project and throughout the first year. Phone support and web training will remain in effect throughout the entire five years. In addition, the vendor chosen is a certified Schools and Libraries Erate vendor, which allows the school to receive a 50 percent discount on all products and services.

A major advantage of wireless devices for students is the fact that it will allow the school to take advantage of eBook licences which are much more economical than purchasing hard covered books. All eBook licences will be purchased with either a three or five year licence which are dramatically less expensive than one year licences.

Several different solutions were evaluated and the one that was the most cost effective and also the best suited for the school environment was chosen. A major factor in the decision was the vendor's close proximity to the school and their high level of expertise. Several of the systems to be implemented are in companies other schools that Immaculate Conception has close relationships with management, so getting a realistic review of the work quality and etiquette was a reality.

Time and Cost

Task	Duration	Description	Cost
Cabling	30 Days	Run new CAT 6 cable in all rooms and server rooms	$21,550.00
Access Points	2 Days	Install access points in locations including outside antennas	$13,446.72

Switches	2 Days	Install and configure network switches	$11,922.89
Controller	1 Day	Install and configure wireless controller	$4094.14
Firewall	1 Day	Install and configure firewall router	$12,208.78
iPad Software	3 Days	Install and configure mobile device management software	$2800.00
Testing	4	Complete testing of network components, internet bandwidth and software applications	$0.00

Scalability

A major consideration of the project was the system's ability to expand products and services. For example, the wireless controller will be initially handling approximately 500 devices at a time but has the capability to handle 1000 devices. Should the school expand at a rapid rate where there would be a need of more than 1000 devices, the controller and firewall would simply need to obtain an additional licence and have the firmware upgraded. This will allow for a seamless integration of the additional users.

All of the resources used by students will be online in cloud servers. This includes the full student information system as well as all eBooks, testing and classroom productivity applications. All current software and applications come with free upgrades for the duration of the licences, which includes all student productivity software applications.

Should the school purchase additional workstations or build a second computer lab, only an additional switch would be needed to connect them. The servers licences allows for connections from an unlimited number of workstations.

Web Integration

The purpose of the project is for a high degree of web integration. All switches communicate directly with the wireless controller, which communicates with a controller in the

cloud. Should there be a hardware issue, the cloud controller could take over the responsibilities of the in house controller until the issue is resolved. The firewall also has the same capabilities. These features prevent a single point of failure.

All iPads have the capability of running the latest mobile applications. When an application is updated by the manufacturer, the user is notified by the App Store application and given the option to update. The mobile device manager also has the option of updating all of the iPads at once. This is normally set to occur during the evening hours to avoid several hundred iPads updating at the same time. Users have access to devices with touch-screens but an optional blue tooth keyboard can be used.

The iPads will integrate automatically with the wireless controllers. The controller is the intermediary between the iPad and the firewall, which is responsible for web access. As an added level of productivity, most eBooks allow for downloading the book directly on the iPad. This allows a user to continue to work should the user be located in an area without wireless access. Productivity applications default setting is to have files stored in the cloud, but the user may also have them stored directly on the device. Should a student's device fail, all data will be readily available when the device is repaired or the student purchases a new one. The mobile device manager has the capability of upgrading the device to the last IOS. This is necessary as often an updated application will only function with the specific IOS or higher.

Interface requirements will be standard for all devices and a minimum amount of 64 GB storage is required, but 128GB is recommended. All icons on the devices are created and clearly labelled when an application is installed. To increase productivity, students are required to group all school related application icons.

Security

Students will be required to put a password on their iPad to prevent unauthorized use. The mobile device manager has the ability to determine any device that does not have an access password enabled and to lock the device until one is put on. The wireless controller has the ability to change the password to access the wireless network if determined that unauthorized users have been granted access. The controller will also have the ability to suspend access to any device for a period of time or until access is re-granted. The firewall has the ability to deny access to any device but this will allow the user to continue to use any in class productivity applications.

There will be several levels of protection and privileges on all switches, controllers, the firewall, and the mobile device manager. Access to these devices will be granted only to IT staff.

Feasibility Analysis

Bridges (2019) stated that if the feasibility study cannot support all of the components of the project, then the project should not be started. This is supported by (Simplilearn, 2020), which states the study will determine whether the project supports its investment. The project's analysis looked at the operational feasibility, the economic feasibility, the technical feasibility, and the schedule feasibility.

The operational analysis area is designed to look for any potential problems that the user may encounter. Access to the wireless is available from any area in the school. There are multiple points of entry so access will be available at all times. The firewall has multiple ports to connect to the Internet, so if one fails it is just a matter of moving a cable to another port. Each student does all the classwork on an iPad, so if the student's iPad fails, the school has several loaners configured and available for the student to use.

The economic analysis will be done to ensure that the benefits and success of the project will be well worth the actual cost. An important item that is initially hidden would be that some students may choose to attend another school with more advanced technology. Since the school income is 90% tuition driven, losing just three students will generate a loss of more than the cost of the entire project. If the school picks up three students because of the new technology, then the entire cost of the project covered in full. The cost of the project is fixed, so there would not be any additional expenditures.

The technical analysis determines what hardware and software devices are needed to complete the project. Each of these are outlined in detail with justification for the need of each piece of hardware and software.

Finally the scheduled is examined. The entire project will be done over the summer when there is minimal staff and no students. The project is slated for a maximum of 43 days. There is a 10 day buffer between the scheduled end of the project and the beginning of the school year.

Project Plan

Work Breakdown Structure

The project manager will begin the project by completely reviewing the project notes. After a comprehensive review the project manager, with assistance from the system analyst and appropriate stakeholders, will develop a comprehensive business case manuscript and identify the system requirements. The existing system environment will be thoroughly appraised to identify both the fully functional parts as well as the areas that need improvement. The project will consist of hardware, cabling, and software installation and configuration. The software for switches, controllers and firewalls is referred to as firmware, and not software. Firmware is actually special software that works with the hardware (Fisher, 2019). The project manager will

take into account that technology changes extremely rapidly and as a result, planning for growth and enhancements will be taken into consideration in the overall project.

It is imperative that the project manager and the system analyst work closely together so that the business requirements will be clearly defined, and the tasks needed to accomplish them will be realistic within the timeframe allowed. The project's vendor team, along with the project manager, will design the new wireless system and will be implemented as follows:

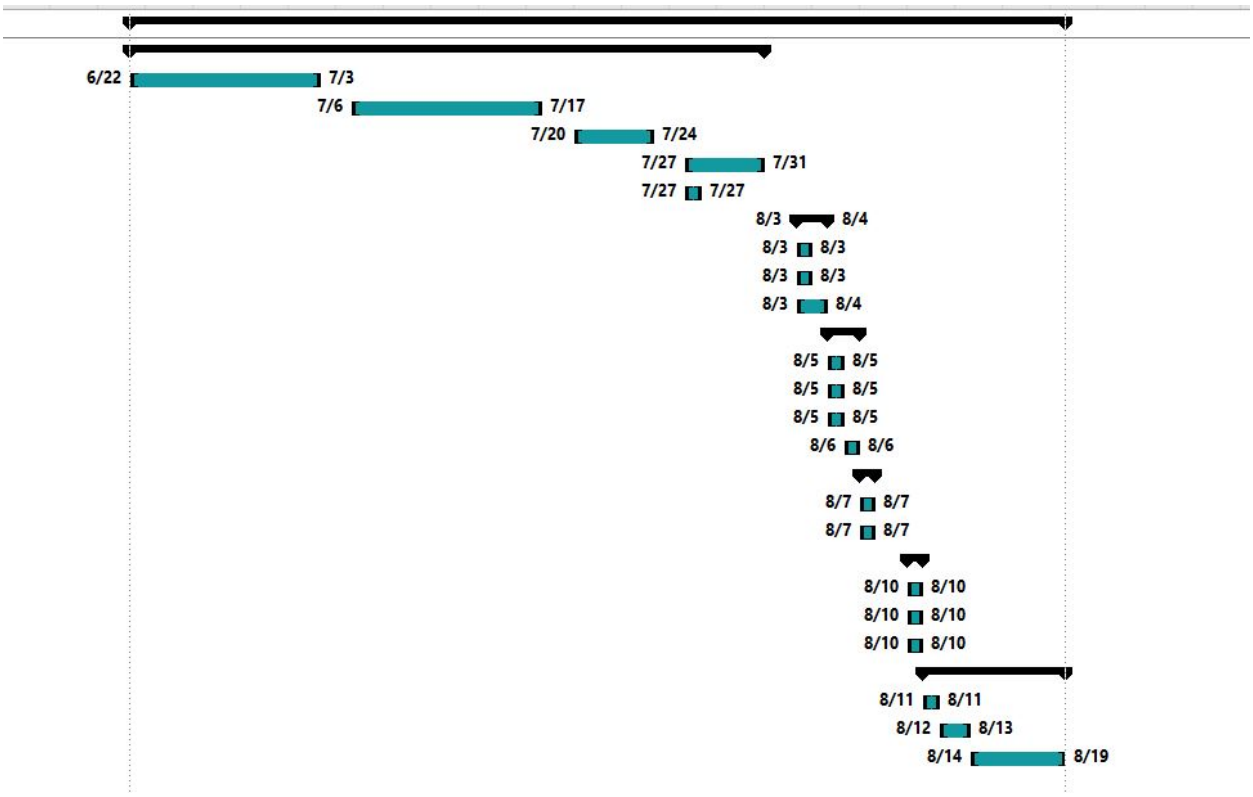
- Project Manager: Oversees the entire project making sure each phase is completed on time and is done with the quality required. The project manager will be onsite at least one day a week and will also be available as needed.
- Cabling: Two qualified individuals will do all of the cabling and make the proper connections of the ends to the switches and controllers.
- Hardware: A certified switch technician will mount the switches and wireless controller to the provided racks, will install the necessary firmware, and configure the routing to the network segments. A certified firewall technician will upgrade and install the necessary firmware, create the necessary wireless local area networks (WLANS), virtual local area networks (VLANS) and implement security
- System Analyst: The system analyst will have a major role throughout the entire project. The system analyst and project manager will meet one week prior to the start of the project to review each step.

In order to evaluate the overall project and to assure the timeframe is being adhered to Tilley (2020) states that individual tasks must be defined and grouped. Each group task is assigned a maximum number of days to be completed. It is necessary that both the beginning and

ending dates of each task be clearly defined. Since tasks durations are generally estimates, a buffer will be added to ensure that tasks will be completed on time.

The tasks chart is broken down into cabling, mounting of access points, mounting and configuring the switches and controller, and mounting and configuring the firewall. The wireless controller configures the access points. The vendor team will perform all of these tasks. The iPad mobile device manager software will be installed and configured by the IT director, who is also the system analyst.

Task Name	Duration	Start	Finish	Cost	Resource Names
Wireless Project	**43 days**	**Mon 6/22/20**	**Wed 8/19/20**	**$66,022.53**	
Cabling	**30 days**	**Mon 6/22/20**	**Fri 7/31/20**	**$21,550.00**	
Building 1	10 days	Mon 6/22/20	Fri 7/3/20	$6,400.00	Cabling
Building 2	10 days	Mon 7/6/20	Fri 7/17/20	$6,400.00	Cabling
Building 3	5 days	Mon 7/20/20	Fri 7/24/20	$3,200.00	Cabling
Admin	5 days	Mon 7/27/20	Fri 7/31/20	$3,200.00	Cabling
Cable Cost	1 day	Mon 7/27/20	Mon 7/27/20	$2,350.00	Cable[1 Box]
AccessPoint	**2 days**	**Mon 8/3/20**	**Tue 8/4/20**	**$13,446.72**	
AP Hardware	1 day	Mon 8/3/20	Mon 8/3/20	$10,584.00	Access Points[1
AP Antennas	1 day	Mon 8/3/20	Mon 8/3/20	$2,862.72	Antenna[1 Units
SW Installation	2 days	Mon 8/3/20	Tue 8/4/20	$0.00	Software Install
Switches	**2 days**	**Wed 8/5/20**	**Thu 8/6/20**	**$11,922.89**	
Hardware	1 day	Wed 8/5/20	Wed 8/5/20	$7,828.75	Switch[1 Units]
Controller	1 day	Wed 8/5/20	Wed 8/5/20	$3,094.14	Controller[1 Uni
Installation	1 day	Wed 8/5/20	Wed 8/5/20	$0.00	Installation
Software Configuration	1 day	Thu 8/6/20	Thu 8/6/20	$1,000.00	Switch Configura
Controller	**1 day**	**Fri 8/7/20**	**Fri 8/7/20**	**$4,094.14**	
Hardware	1 day	Fri 8/7/20	Fri 8/7/20	$3,094.14	Controller[1 Uni
Software Configuration	1 day	Fri 8/7/20	Fri 8/7/20	$1,000.00	Controller Confi
Firewall	**1 day**	**Mon 8/10/20**	**Mon 8/10/20**	**$12,208.78**	
Hardware	1 day	Mon 8/10/20	Mon 8/10/20	$11,208.78	Firewall[1 Units]
Intallation	1 day	Mon 8/10/20	Mon 8/10/20	$0.00	Installation
Configuration	1 day	Mon 8/10/20	Mon 8/10/20	$1,000.00	Firewall Configu
Ipad Software	**7 days**	**Tue 8/11/20**	**Wed 8/19/20**	**$2,800.00**	
Mobile Appications	1 day	Tue 8/11/20	Tue 8/11/20	$2,800.00	Mobie Device Sc
ipad SW Installation	2 days	Wed 8/12/20	Thu 8/13/20	$0.00	
Testing	4 days	Fri 8/14/20	Wed 8/19/20	$0.00	



The resources are as follows

Resource Name	Type	Material	Initials	Max.	Std. Rate	Ovt. Rate	Cost/Use	Accrue	Base
Access Points	Material	Units	A		$0.00		$10,584.00	Prorated	
Antenna	Material	Units	A		$0.00		$2,862.72	Prorated	
Cable	Material	Box	C		$0.00		$2,350.00	Prorated	
Cabling	Work		C	100%	$80.00/hr	$0.00/hr	$0.00	Prorated	Standard
Controller	Material	Units	C		$0.00		$3,094.14	Prorated	
Controller Configureation	Work		C	100%	$0.00/hr	$0.00/hr	$1,000.00	Prorated	Standard
Firewall	Material	Units	F		$0.00		$11,208.78	Prorated	
Firewall Configuration	Work		F	100%	$0.00/hr	$0.00/hr	$1,000.00	Prorated	Standard
Hardware	Material	Units	H		$0.00		$0.00	Prorated	
Installation	Work		I	100%	$0.00/hr	$0.00/hr	$0.00	Prorated	Standard
iPad	Work		i	100%	$0.00/hr	$0.00/hr	$0.00	Prorated	Standard
Misc Hardware	Material	Units	M		$0.00		$0.00	Prorated	
Mobie Device Softare	Material	Units	M		$0.00		$2,800.00	Prorated	
Software Install	Work		S	100%	$0.00/hr	$0.00/hr	$0.00	Prorated	Standard
Switch	Material	Units	S		$0.00		$7,828.75	Prorated	
Switch Configuration	Work		S	100%	$0.00/hr	$0.00/hr	$1,000.00	Prorated	Standard

All work is a fixed amount with the exception of the cabling. There will be a minimum of two persons doing the cable for a charge of $80 per hour. The maximum amount of billable hours will be 240. If the cabling takes less, then only the hours used will be billed. If the cabling takes longer, then the vendor will not charge any additional hours. Each hardware item is listed

as material and a fixed cost. Installation and configuration are listed as work but is also a fixed cost and not by the hour. Each task has its own resource in order to allow for cost breakdown by task group.

Project Monitoring and Control Plan

Chand (2014) addresses three types of necessary controls in a project, performance, cost, and time. Controls are extremely imperative in mid to large size projects, but should also be employed in all projects regardless of the size. He adds that the main purpose for controls is to identify both potential and actual problems and then make the necessary modifications in order to resolve them. He also mentioned that controls should be proactive in order to identify issues before they become a problem.

Both the project manager and the system analyst will supervise the development and overall progress of the project with an emphasis on timely task completion. Before moving to the next phase, both the project manager and the system analyst will inspect the work of the current phase and each of the individual tasks. The project manager will be responsible for providing additional cabling professionals at no additional cost in the event that any of the cabling tasks may possibly take longer than the allotted time.

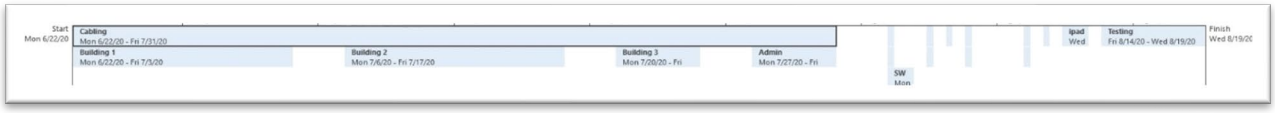
Each Monday during the cabling phase, the project manager will meet with the system analyst and the cabling professionals to discuss the overall cabling progress and the cabling implementation plan for the current building. The overall progress for each task will be evaluated to make sure it will be completed within the time allotted. At that time, a determination will be made whether to employ any additional persons qualified to do cabling. The cabling phase is the most complicated and time consuming. It must be completed before any of the other phases can begin. Upon completion of each building, a post performance check will be completed. During

the check, each cable and all connections will be thoroughly tested with a top grade tester, such as the Fluke Networks MicroScanner2 Cable Verifier and Network tester.

The project will have two defined critical paths, which are crucial to keeping the project on the specific timeline. The most important critical path will be the cabling, as the project cannot continue until the cabling has been thoroughly tested and approved. The second critical path will be the testing phase which will occur the week before classes start. Two extra days of testing have been added to allow for any modifications that may be necessary.

Timeline

The project will be implemented during the summer months when school is not in session and will be fully tested during student orientation in the days prior to the start of the new school year.



The timeframe for the project is 43 working days. It begins on Monday June 22, 2020 and ends on Wednesday August 19, 2020. The project work will be completed on August 13, 2020 and the testing phase will begin on August 14, 2020. Four full days of testing have been allocated, but since classes do not begin until August 24, 2020, there are an additional two days that can be used for supplementary testing. The vendors have agreed that they will charge for a fixed number of hours, and will work on weekends if necessary to ensure that the project is completed on or before the ending date.

The cabling will take a maximum of 30 days and the tasks are broken into separate buildings. Each building will be completed before starting the cabling on another building.

References:

ABIresearch. (2019, June 13). Wi-Fi Celebrates 20 Years with More Than 20 Billion Anticipated Device Shipments over the Next Six Years. Retrieved April 17, 2020, from https://www.abiresearch.com/press/wi-fi-celebrates-20-years-more-20-billion-anticipated-device-shipments-over-next-six-years/

Bose, R. (2004). Information technologies for education & training in e-government. *Proceedings of the IEEE International Conference on Information Technology: Coding and Computing*. Las Vegas, NV, 203-208.

Bridges, J. (2019, December 12). How to Conduct a Feasibility Study. Retrieved May 30, 2020, from https://www.projectmanager.com/training/how-to-conduct-a-feasibility-study

Caverly, & Mac. (2019, December 30). Children's Internet Protection Act. Retrieved from https://www.fcc.gov/consumers/guides/childrens-internet-protection-act

Caverly, D. & MacDonald, L. (2005). Techtalk: Wireless networking. *Journal of Developmental Education*, *28*(3), 38-39.

Chand. (2014, January 29). Project Control Mechanism: 3 Types of Project Control Mechanism. Retrieved May 1, 2020, from http://www.yourarticlelibrary.com/projects/project-control-mechanism-3-types-of-project-control-mechanism/24442

Children's Internet Protection Act. (2019, December 30). Retrieved April 18, 2020, from https://www.fcc.gov/consumers/guides/childrens-internet-protection-act

CIPA. What is Children's Internet Protection Act ? (n.d.). Retrieved April 18, 2020, from https://www.infoblox.com/glossary/childrens-internet-protection-act/

Clayton State University. (2019). Wiring Standards. Retrieved from https://www.clayton.edu/nes/wiring/

Coextro. (2019, September 24). Advantages and Disadvantages of the 2.4 GHz and the 5 GHz Wireless Networks. Retrieved April 17, 2020, from https://www.coextro.com/advantages-and-disadvantages-of-the-2-4-ghz-and-the-5-ghz-wireless-networks/

Coronel, C., & Morris, S. (2019). *Database systems: design, implementation, and management*. Boston, MA: Cengage.

EdTech (2019, May 1). 5 Best Practices for Implementing a New Wireless Network. Retrieved April 17, 2020, from https://edtechmagazine.com/higher/article/2013/09/5-best-practices-implementing-new-wireless-network

Fisher, T. (2019, November 27). Hardware vs Software vs Firmware: What's the Difference? Retrieved May 1, 2020, from https://www.lifewire.com/hardware-vs-software-vs-firmware-whats-the-difference-2624567

Fong, A., Hui, S., & Lau, C. (2004). On-demand learning for a wireless campus. *IEEE Multimedia*, 50-60.

Leith, S. (2019, July 16). School textbooks are on the way out. Retrieved April 21, 2020, from https://www.theguardian.com/commentisfree/2019/jul/16/electronic-textbooks-future-rude-drawings-pearson-digital-pupils

Leung, C. & Chan, Y. (2003). Mobile learning: A new paradigm in electronic learning. *Proceedings of the 3rd IEEE International Conference on Advanced Learning Technologies*. Athens, Greece, 76-81.

MobieInfo. (2019). Retrieved April 21, 2020, from http://mobileinfo.com/ROI/ROI_WLANs.htm

Moody, L. & Schmidt, G. (2004). Going wireless: The emergence of wireless networks in education. *Journal of Computing Sciences in Colleges*, *14*(4), 151-158.

Nagle, D. (2002, November 2). Wireless vs. Hard-Wired Network Use in Education. Retrieved April 16, 2020, from https://thejournal.com/Articles/2002/11/01/Wireless-vs-HardWired-Network-Use-in-Education.aspx

Onsman, A. (2018, July 3). Partial Dependencies in DBMS. Retrieved May 28, 2020, from https://www.tutorialspoint.com/Partial-Dependency-in-DBMS

Pierce, M. (2020, April 2). What Should be Included in a Wireless Network Design for Businesses? Retrieved April 16, 2020, from https://www.securedgenetworks.com/blog/what-should-be-included-in-a-wireless-network-design

Roland, J. (2017, August 14). Evaluating the ROI of Technology in the Classroom. Retrieved April 21, 2020, from https://insights.samsung.com/2017/08/14/evaluating-the-roi-of-technology-in-the-classroom/

Simplilearn. (2020, March 23). What is Feasibility Study and Its Importance in Project Management. Retrieved May 30, 2020, from https://www.simplilearn.com/feasibility-study-article

Tilley, S. R. (2020). *Systems analysis and design* (12th ed.). Boston, MA: Cengage Learning Asia Pte Ltd.

Walery, D. (2004). Wireless technology in K-12 education. *T.H.E. Journal*, *31*(8), 48-50.

Yin, J. (2019, June 17). The Future of Wi-Fi Is Coming. Retrieved April 16, 2020, from https://www.project-disco.org/innovation/061719-the-future-of-wi-fi-is-coming