assignment 6

SAAD1002 – TEAM 3

Courtney Hagen, Mitch Jean, Nick Lucyk, Nick White

November 14, 2019

Contents

[Background 3](#_Toc24635150)

[Business Process and Information Flow 6](#_Toc24635151)

[Cross Functional Flowchart 6](#_Toc24635152)

[Admin Group Flowchart 7](#_Toc24635153)

[Lab Technician Group Flowchart 8](#_Toc24635154)

[Nurses Group Flowchart 9](#_Toc24635155)

[Doctors Group Flowchart 10](#_Toc24635156)

[Network Design Methodology/Topology 11](#_Toc24635157)

[What are the benefits of a Hierarchical Network Design? How would they apply to Friendswood Hospital? 11](#_Toc24635158)

[What activities and logical network functions would be occurring at each of the layers in a hierarchical network at Friendswood Hospital? 11](#_Toc24635159)

[What is a Collapsed Core Design? Do you think it is appropriate for Friendswood hospital? 12](#_Toc24635160)

[Will we employ elements of mesh designs or simply stick to a hub-and spoke design? Why? 12](#_Toc24635161)

[High Availability Network Resources 12](#_Toc24635162)

[Do we anticipate a need for Virtual LANs? If so, how will they be used? 13](#_Toc24635163)

[What are the design considerations for the Wireless LANs? 13](#_Toc24635164)

[What elements of Cisco’s SAFE Security Reference Architecture do you think may apply to the design of this network? 13](#_Toc24635165)

[Network Diagrams 14](#_Toc24635166)

[Network Topology – High Level 14](#_Toc24635167)

[Network Topology – Basement Floor (Floor 1) 15](#_Toc24635168)

[Network Topology – Main Floor (Floor 2) 16](#_Toc24635169)

[Network Topology: Lab Floors (Floors 3-5) 17](#_Toc24635170)

[Network Topology – Patient Floors (Floors 6-10) 18](#_Toc24635171)

[Floorplan: Basement Floor (Floor 1) 20](#_Toc24635172)

[Floorplan – Main Floor (Floor 1) 21](#_Toc24635173)

[Floorplan – Lab Floors (Floors 3-5) 22](#_Toc24635174)

[Floorplan – Patient Floors (Floors 6-10) 23](#_Toc24635175)

[Rack Diagrams 24](#_Toc24635176)

[Time & Cost Estimates 25](#_Toc24635177)

[Information Graphs 25](#_Toc24635178)

[Pivot Tables 26](#_Toc24635179)

[Labor Estimation, Cabling Cost, and Final Total 27](#_Toc24635180)

[Ongoing Plan 27](#_Toc24635181)

[Scalability Plan 27](#_Toc24635182)

[Growth Points  27](#_Toc24635183)

[Chokepoints  27](#_Toc24635184)

[Granular Plan  27](#_Toc24635185)

[Security Plan 27](#_Toc24635186)

[Maintenance & Security Plan 28](#_Toc24635187)

[Equipment System Maintenance Tasks:  28](#_Toc24635188)

[Network Management Tasks:  29](#_Toc24635189)

[Maintenance Schedule 30](#_Toc24635190)

[References 31](#_Toc24635191)

[Appendix A – Complete Time & Cost 33](#_Toc24635192)

[Appendix B – Work Journals 34](#_Toc24635193)

[Courtney Hagen 34](#_Toc24635194)

[Mitch Jean 34](#_Toc24635195)

[Nick Lucyk 34](#_Toc24635196)

[Nick White 35](#_Toc24635197)

[Totals 35](#_Toc24635198)

# Background

Friendswood Hospital:

Friendswood Hospital is a 10-floor hospital in a medium-sized city. Ms. Zia Oleg, the IT director is responsible for the network at the medical facility and it has been determined that the current network infrastructure is completely inadequate for the needs of the organization, its employees, and its patients. Your team has been tasked with creating a network system design proposal that Ms. Oleg can present to the hospital’s board of directors for their approval.

As the first step of constructing the system design proposal, we need to understand the fundamental business processes that staff will regularly perform on the network. While there are a variety of other business functions such as accounting, payroll, and technical support to name a few, we will focus our attention on the core patient care and tracking aspects of the organization.

The following groups form the main, patient-facing employee groups of the organization:

* Administrative staff working at desktop computers on the second (main) floor will access the proprietary patient tracking software (PTS) to enter new patients into the data store, control admissions, and schedule appointments.
* Laboratory technicians on floors 3-5 will use desktop computers to access the PTS to view appointments as well as to store documents, scans, and reports related to the results of patient tests.
* Nurses working with patients on floors 6-10, where all patient rooms are, will use mobile devices and/or laptops to access the PTS via wireless connections primarily to track the administration of medication and other treatments.
* Doctors working with patients on floors 6-10, will also utilize the wireless network to access the PTS to maintain patient charts, track patient progress, and specify patient discharge dates.

While the network infrastructure at Friendswood Hospital is wholly outdated and obsolete, and the goal is to replace all of the network components, cabling, and computer devices, knowledge of the existing network setup may help to inform the new design.

The first floor (i.e. basement) of the hospital currently contains the server room/data centre, and WAN connection. There are also approximately 25 desktop client machines on this floor to support some Managerial and Support (e.g. HR & Tech Services) personnel.

The second (i.e. main) floor contains about 40 client machines, which mostly supporting hospital Administrative staff with some additional Managerial and Support personnel.

Floors 3-5 contain approximately 20 desktop machines each to support Laboratory technicians and their Administrative personnel.

On each of the patient floors, there are currently only two to three desktop client machines at the nurses’ stations with an additional 4-5 per floor in doctor’s offices.

Friendswood Hospital hopes to provide secure wireless access within patient rooms so doctors and nurses may enter information in the patient tracking software (PTS) on mobile devices without having to take notes and enter data back on their respective desktop machines. However, the desktop machines would remain for use when in the offices or at the nurses’ stations.

The Friendswood Hospital building has external dimensions of 200-by-100 feet, with ten stories as mentioned before. Every floor of the hospital has some common characteristics:

* Stairwells on all corners
* Two Elevators in the center of the floor
* Washrooms in the center of both east and west walls opposite the elevators
* A wiring closet on the back side of the elevators that is paired with a utility room
  + Can assume the wiring closet will have conduits for running cabling between floors

On the first floor (basement) we have:

* A large, 20-by-30 foot server/data room on the south side of the building in the center of the floor, near the wiring closet
* Three other slightly smaller utility rooms near the server room for furnace, storage, etc.
* Approximately 25 cubicles for some Managerial and Support staff

On the second floor (main) we have:

* A large open entrance area along the north wall in the middle which we can assume has space for the cafeteria as well
* Approximately 40 cubicles/small offices/work areas for mostly Administrative staff with some additional Managerial and Support personnel

On Floors 3-5 we have:

* Three large laboratory areas, with an administrative office with a single workstation and partitioned room for three technicians with lab spaces and workstations for each (so, 3 x 4 = 12 workstations)
* Four smaller lab spaces with spaces for two technicians to work and workstations for each (so, 4 x 2 = 8 workstations)

On each of the patient floors, there are:

* Six 2-room patient rooms along north wall
* Four single patient rooms along both sides
* Two Nurses’ stations: each in the middle of both halves of the building with either one or two workstations
* Five Doctor’s offices each with a single workstation along the south walls, behind an interior wall or partition

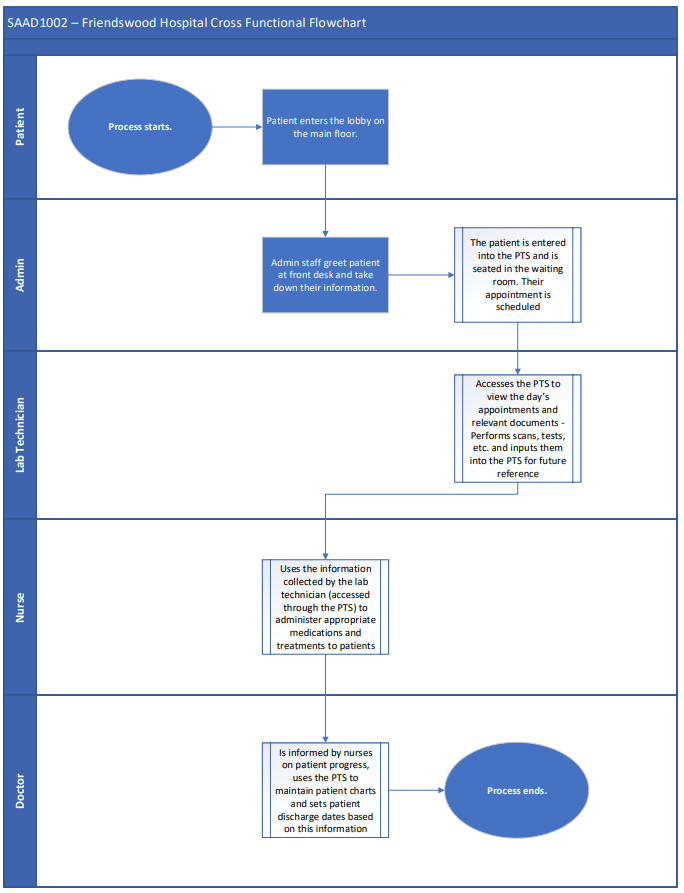
As an addendum to the previously mentioned dimensions and architectural details of Friendswood Hospital, it should be noted that the **floors are ten feet in height**. While, with any dropped ceilings or raised floors on a particular floor the ceiling height might vary, each floor is essentially 10 feet above the previous one.

Friendswood Hospital has agreements in place to receive discounts by exclusively purchasing their equipment with both Cisco (10%) for networking devices such as routers, switches, hubs, and access points and Dell (15%) for servers and workstations. All other necessary equipment will be purchased at retail prices and, preferably, locally whenever possible.

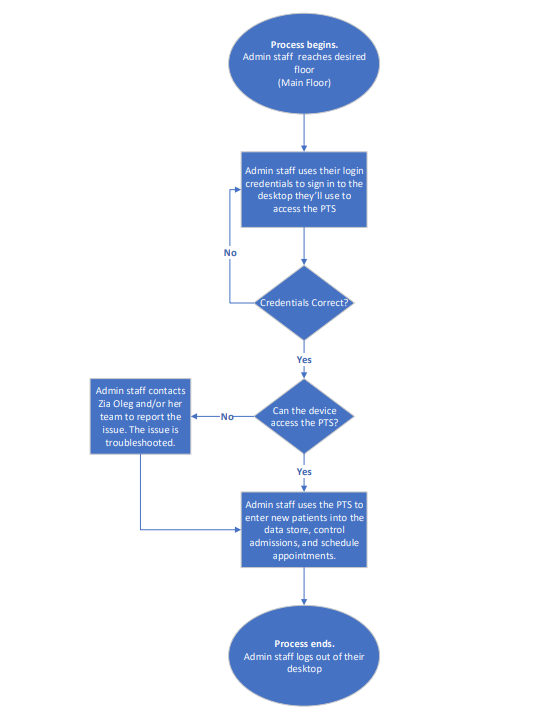
Due to cutbacks of a few years’ previous, Friendswood Hospital maintains a minimal Network Administration and Tech Support staff, with only one full-time employee onsite for each shift with off duty staff on-call in case of emergency and some part-time staff added during peak times. Given the overtime rates specified in the union contract and the downtime mandated for each employee before returning to shift work, the management has decided to outsource the network installation tasks to an outside contractor. Once the new network is in place, the existing employees will be tasked with supporting and maintaining it.

# Business Process and Information Flow

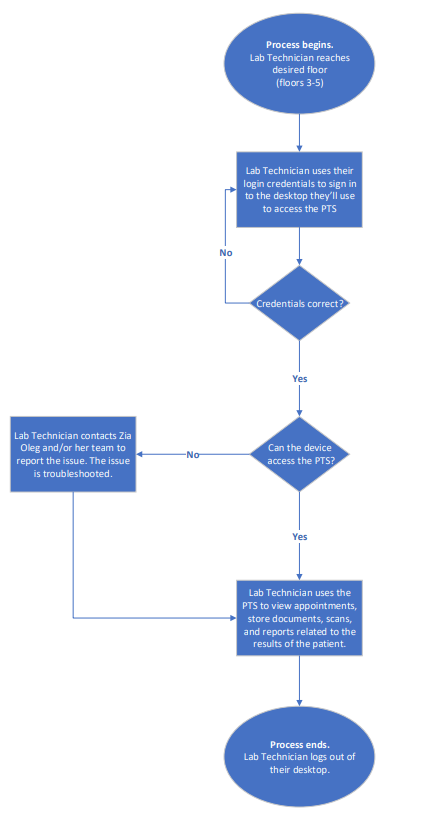
## Cross Functional Flowchart



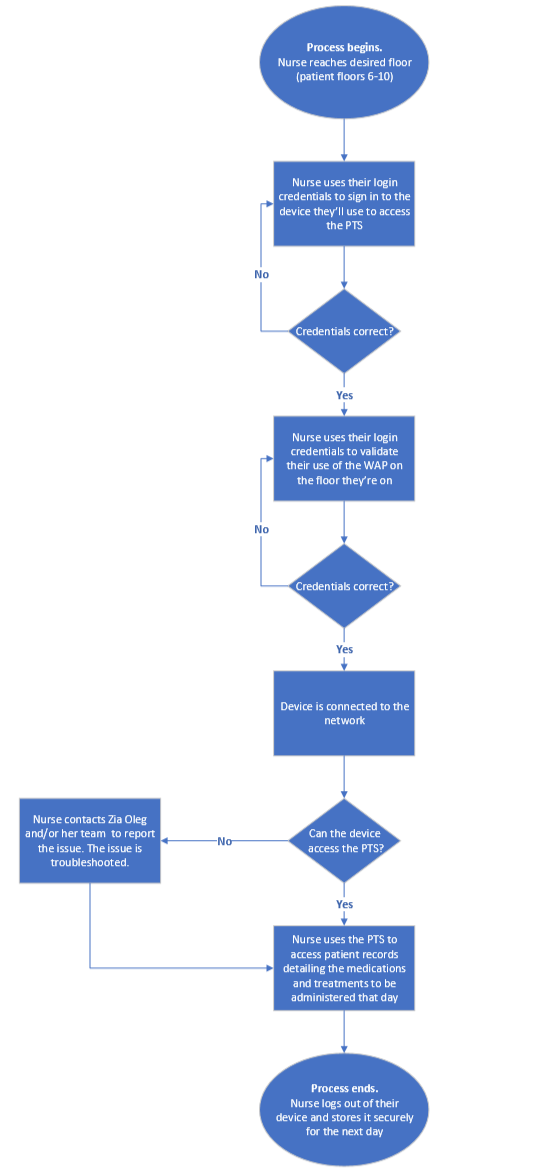
## Admin Group Flowchart



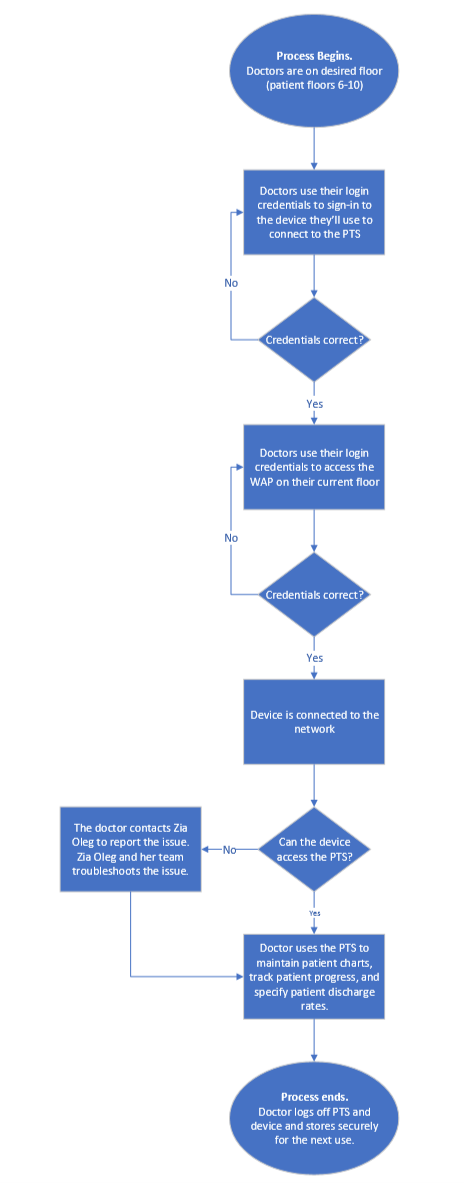
## Lab Technician Group Flowchart



## Nurses Group Flowchart



## Doctors Group Flowchart



# Network Design Methodology/Topology

## What are the benefits of a Hierarchical Network Design? How would they apply to Friendswood Hospital?

Hierarchical network design, as it applies to Friendswood hospital, would mostly be a benefit to scalability/fostering future growth of the network, and providing fault tolerance (through redundancy) to the core systems (the PTS, essentially). This would be accomplished through setting up redundant links, possibly running multiple servers to host the PTS, and segmenting the network into VLANs according to the department or method of connection to the PTS. Using a model of Core > Distribution > Access in a smaller network like Friendswood would, as previously stated, mostly just make it easier to expand the network in the future. The core wouldn’t really be established until a remote office or another branch of the hospital is developed (the “high speed backbone” to get information across to the distribution layer on the other side). The access layer, as expected, would simply facilitate the different departments to access the PTS for their own purposes.

## What activities and logical network functions would be occurring at each of the layers in a hierarchical network at Friendswood Hospital?

Core Layer – The Core layer is the highest layer in the Hierarchical network model. It contains the fastest data transportation equipment and is the final stop before data is routed out to the WAN. It would contain the router that is connected to the WAN as well as high-level switches. This is the most important point in the model because if any parts fail the whole network will be affected, so it must be reliable and easy to fix if there is an issue. There would not be much in the way of activity within this layer once it is set up. System Admins would access this layer to make sure things were connecting properly out to the WAN and would need to access it if there were network issues.

Distribution Layer – The Distribution layer is in the middle of the Hierarchical network model. This layer connects the Access layer to the Core layer. This layer would be where the hospital’s server room and data center reside. As well as many switches that would connect all the of switches in the wiring closets on each floor up to the Data layer. These switches will split up the different parts of the network from each other so that if there is an issue with one part it won’t necessarily disrupt all the network. Network policies are often applied at this level because of its location in the network model. Activities at this level would include System Admins managing policies and troubleshooting issues with parts of the network. Also, they would need to manage any issues or updates to the server room and data center.

Access Layer – The Access layer is the lowest layer in the Hierarchical network model. It is the busiest part of the model and sits on the edge of the network where host devices are connected. All user access points to the network would be here such as computers, printers, VoIP phones, WAPs and wirelessly connected devices like cell phones and laptops. These access points would be connected to Network closets on each floor that contain switches that connect all the devices to the distribution layer. There would be a large amount of activity at this layer as this is where all end-users are accessing the network through their devices. As well System Admins will spend most of their time here making sure that users have proper connection to the network. (NetworkDirection.net, 2018)

## What is a Collapsed Core Design? Do you think it is appropriate for Friendswood hospital?

A Collapsed Core Design is a Hierarchical network design that takes the core and distribution layer and combines them. The reason for using a collapsed core design over a Hierarchical network design would be for cost reduction which we believe Friendswood would benefit from as a healthcare institution. However, if the building plans to expand, this may not be the best method. We believe that going for cost efficiency over a potential growth issue in the future is a better decision, therefore Friendswood should go with the collapsed core design over a hierarchical network design. (Small Enterprise Design Profile Reference Guide, 2013)

## Will we employ elements of mesh designs or simply stick to a hub-and spoke design? Why?

A Hub-and-spoke network design is a network design that uses no redundant wires to connect different nodes. A mesh design uses additional wires to create redundant links between nodes, creating little to no down time. There are two different version of the mesh design, partial and full. The difference between them is that either every node has a redundant link or only some do, the first being a full mesh design and the latter being a partial mesh design. We should go with a full mesh design for Friendswood because reliability should be the hospitals primary concern. (Hub-and-spoke Wide Area Network (Wan) network topology, n.d.) (Partial-Mesh Wide Area Network (WAN) topology, n.d.)

## High Availability Network Resources

**Reliability** is a key concept we have to consider for Friendswood. The hospital operates with every department’s reliance on a single system: the PTS. We need to put in place every measure possible to ensure the PTS stays up, as it services the entire building (mostly), but if it goes down, we also need a solid system in place to mitigate against down time. This is where **redundancy**comes into play; if we’re hosting the PTS off of multiple servers, and possibly storing the core files and database in a RAID array, we’d ensure that hardware failure is something that we can recover from in a situation of emergency. Budget is something we have to consider here, but some proactive spending will ensure we don’t have to spend even more down the line. In simpler terms, if we have a system in place to facilitate **fault tolerance**, we can avoid catastrophe AND save money. The PTS also has to work quickly and diligently across the network, being **accessible** anywhere it’s needed, and as **fast** as possible in the case of time sensitivity (considering we’re working with patients that may need immediate care, or access to relevant information). This would simply constitute intelligent design of the network, avoiding collisions and optimizing where we can. As mentioned in previous parts of this document, we also have to consider **scalability**when designing our network, as we need to account for potential growth in the network for any given reason. If any remote offices are to pop up, it’s not a stretch to assume that they’ll also need to access information from the PTS (hosted in the datacenter at Friendswood). The Core > Distribution > Access model is inherently scalable, so as long as we adhere to a hierarchical design, this shouldn’t be an issue. Lastly, the entire system needs to be as **secure** as possible, considering we’re dealing with sensitive (and at times confidential) patient data that cannot be leaked without consequence. Also, we provide an essential service to the public, so if attackers are able to bring down parts of our network it could be debilitating to our entire operation. By adhering to best practices (securing lines on switches and routers, hardening servers, etc.) we can mitigate against malicious actors to the best of our ability. This would also include a DMZ and potential WAPs for visitors/patients to get a WiFi connection.

## Do we anticipate a need for Virtual LANs? If so, how will they be used?

We do anticipate a need for Virtual LANS. It is a good practice to separate different departments into different VLANs for increased security so that we can modify who can access what data.

For the VLANs, we would make an Admin VLAN, a Lab Technician VLAN, a Wireless VLAN for nurses and doctors, a Management VLAN and a Server VLAN. This would allow the servers to be isolated and have proper security configured with the Management VLAN able to gain access only. Nurses and doctors will share a VLAN as they both use the wireless connections and access the same data. (Lorenzen, 2018)

## What are the design considerations for the Wireless LANs?

There are multiple things to take into consideration when it comes to the design of Wireless LANs. The first one being the Range/Coverage of the Wireless network. It’s important to make sure that there is enough Wireless Access Points (WAP) spread throughout the hospital so that there are no areas where the signal drops, also known as dead zones. If WAP placements are planned properly and tested, then it is possible to avoid these dead zones. Another thing is to consider how much traffic there will be on the wireless networks, if the Doctors and Nurses are only using the Wi-Fi to input patient data it wouldn’t need too much bandwidth. However, if they are using it for more than just that or there are a lot of hospital staff accessing it at once it could require a good amount of bandwidth. The ideal amount of bandwidth could be determined with proper testing. Security is another very important thing to consider, strong security settings such as long passwords and user logins will help to keep the network secure. Lastly, scalability is important to think about when designing a WLAN. It is possible that the hospital could have some renovations and add another wing to the building that would need to have the WLAN extended to it. This would require new WAPs connected to the previous ones that were set up. (Vacca, 2001)

## What elements of Cisco’s SAFE Security Reference Architecture do you think may apply to the design of this network?

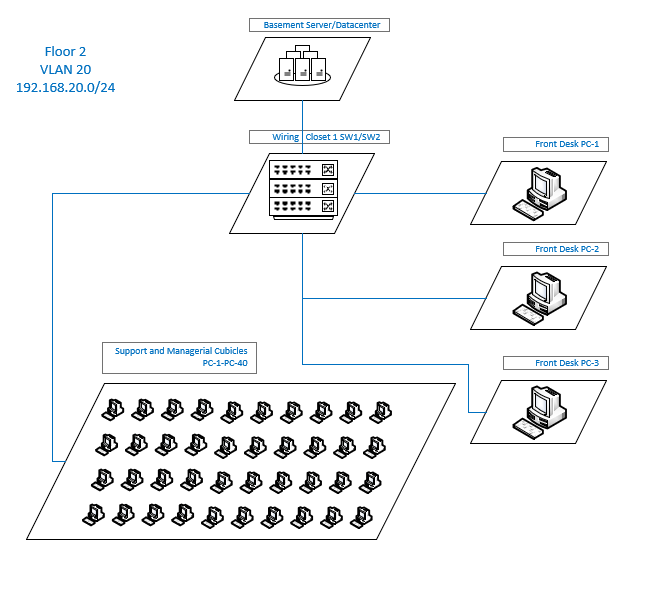
In reference to Cisco’s SAFE architecture, this hospital would need to be planned to be a Secure Campus. This is because it physically holds all the networking equipment for the company and the employees need to physically be connected to that network as there is no identified branches. The functional controls that then need to be considered are secure applications, access, remote access, communications, and web access. Remote Access has not been identified as something the hospital has plans on using, so this does not need to be planned for. Secure applications are important as the hospital uses their applications to host sensitive information on the patients. As for secure access, it is also equally important as the employees are using their access to use applications that store sensitive information. For secure communications, each department will need to communicate with each other and this may include private information, so it is equally important to implement. Finally, with secure web access, the internet may be used for research, so it is important secure web access is implemented so threats from accessing the internet may not obtain private hospital records. (SAFE Architecture Guide, 2018)

# Network Diagrams

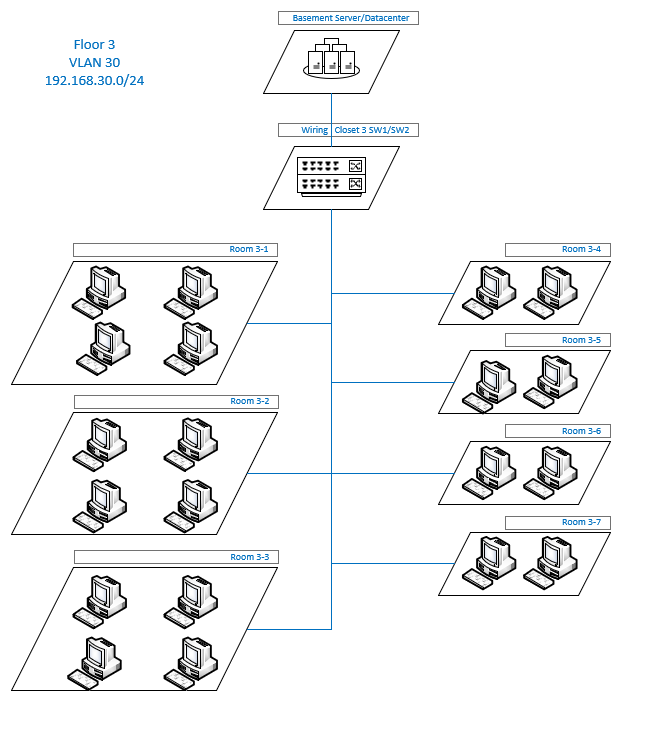
## Network Topology – High Level

## C:\Users\w0415917\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\A6DE0823.tmpNetwork Topology – Basement Floor (Floor 1)

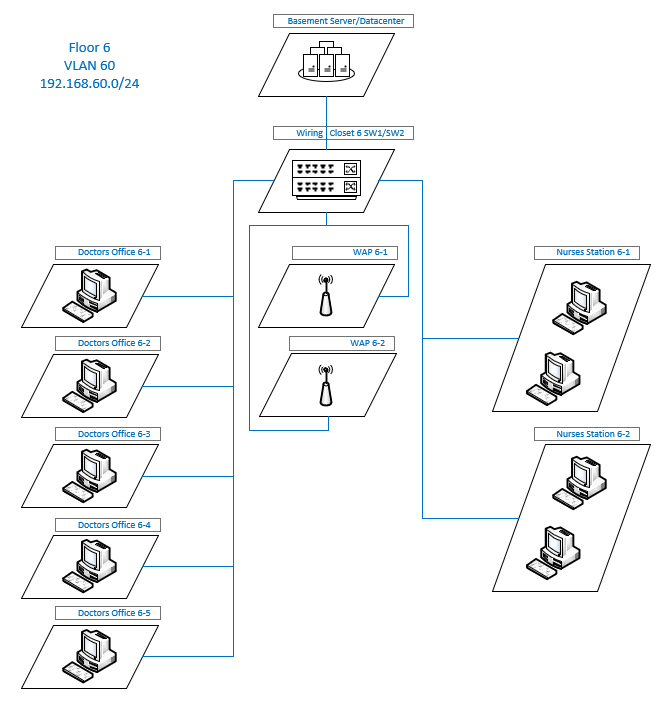
## Network Topology – Main Floor (Floor 2)



## Network Topology: Lab Floors (Floors 3-5)

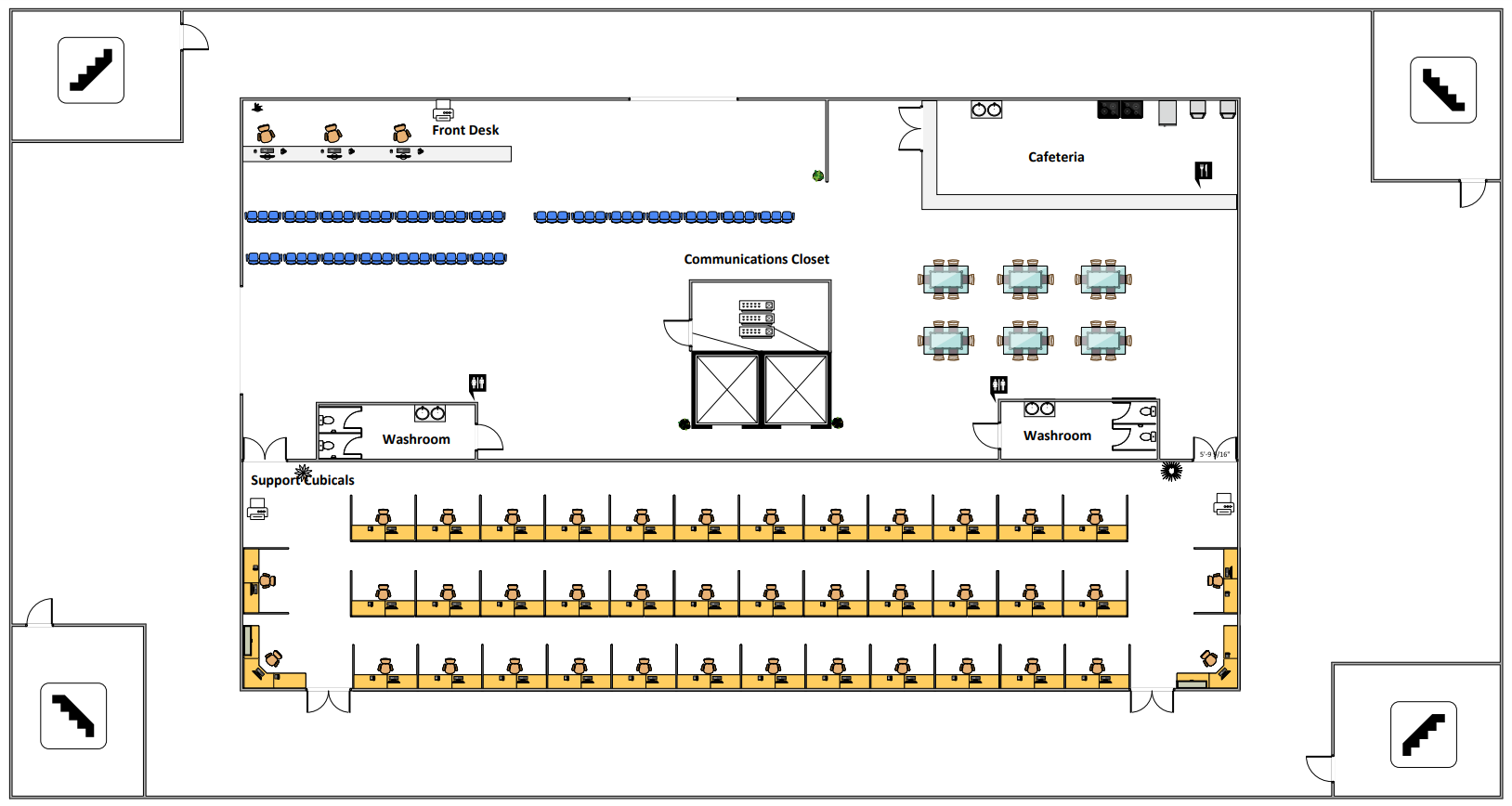


## Network Topology – Patient Floors (Floors 6-10)



## Floorplan: Basement Floor (Floor 1)

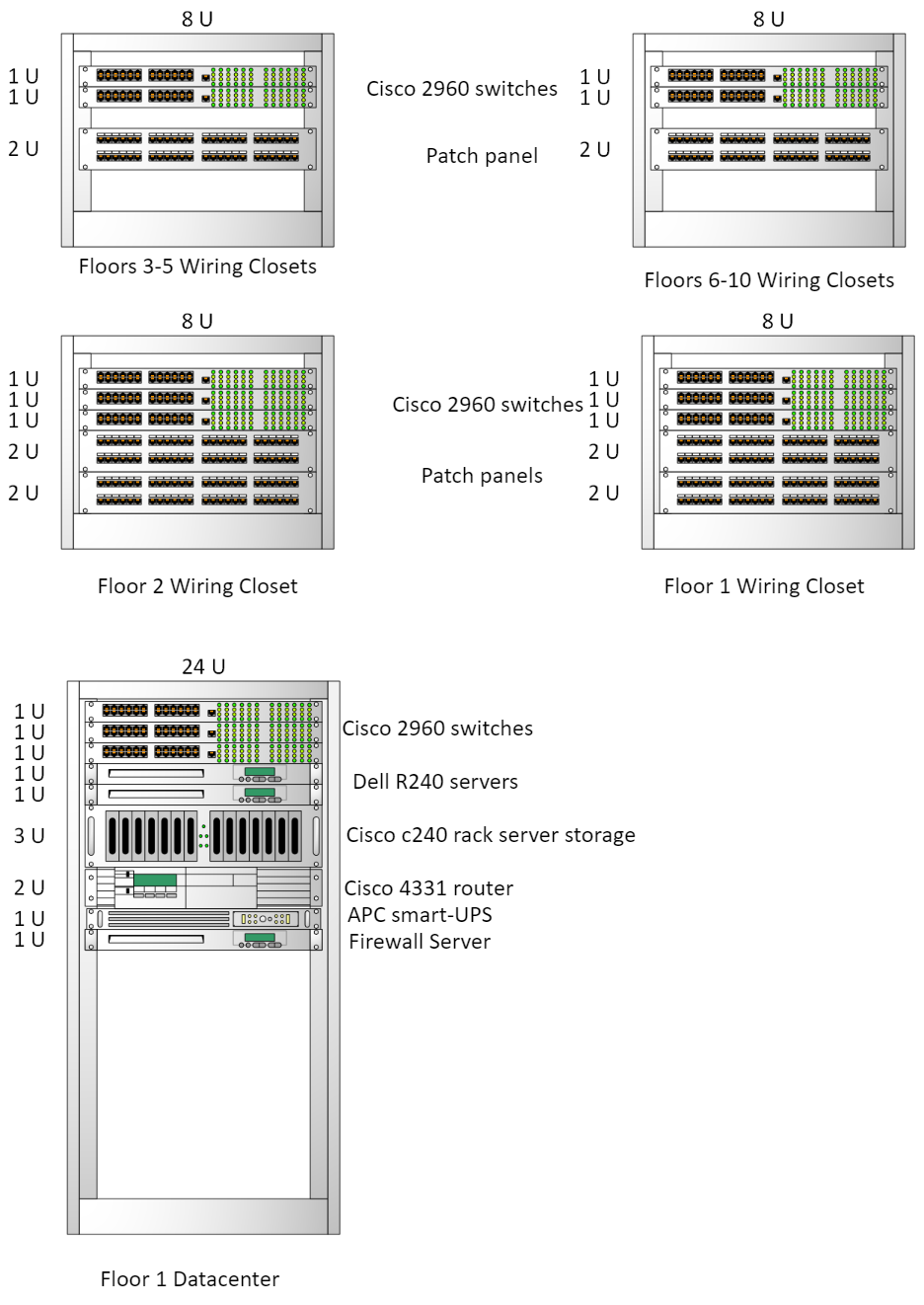
## Floorplan – Main Floor (Floor 1)



## Floorplan – Lab Floors (Floors 3-5)

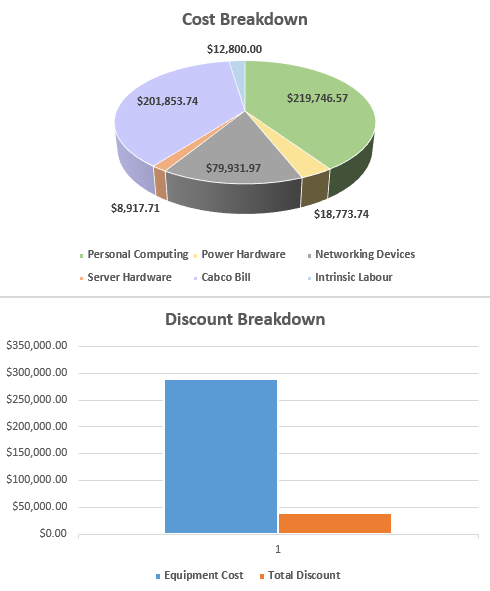
## Floorplan – Patient Floors (Floors 6-10)

## Rack Diagrams

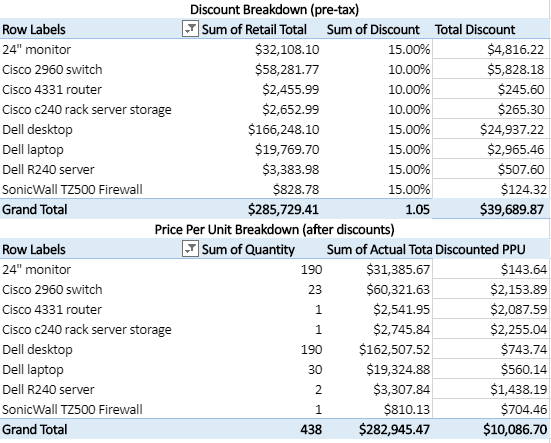


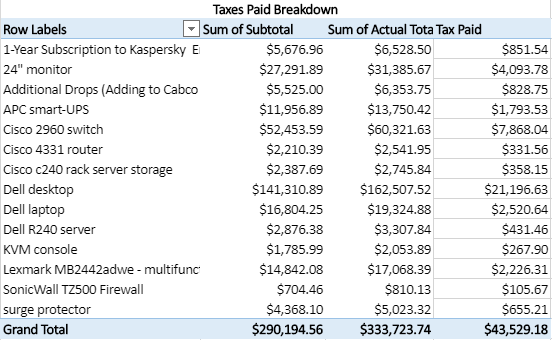
# Time & Cost Estimates

## Information Graphs



## Pivot Tables





## Labor Estimation, Cabling Cost, and Final Total

# Ongoing Plan

## Scalability Plan

### Growth Points

The growth areas for the Friendswood would be the workstations for employees, planning for an increase of 25% over a 5-year period, and adding switches to add those potential new workstations to the network.

### Chokepoints

Our current design of Floor 2 does not have the capacity to add any additional workspaces for potential growth.

### Granular Plan

The current network for the hospital will be designed to accommodate for potential growth on all floors by creating new drops for additional workspaces, a 25% increase of the current amount of workspaces on the floor, adding additional switches to all closets as required to accommodate the new potential work spaces, and pre purchasing additional desktops, monitors, and surge protectors for the potential increase of staff.

## Security Plan

The Personal Information Protection and Electronic Documents Act in Canada states that the level of security an organization uses must reflect how private the information being stored is. (Wood, n.d.) As hospital information is incredibly private, the hospital must do its absolute best to protect this information. Fortunately, as the hospitals network is not connected to the internet and is confined, there will be less risks to contend with. However, there are still many security issues to consider. 

The first security concern for any organization is teaching the users in the company good security practices. If the entire network itself is secure, there is still the potential for maliciously acquiring information from users. Some examples of this include writing passwords down around work areas, leaving their workstations unlocked, and allowing other users to use their accounts. These issues are best avoided through user education. Initially, it can be in the form of a presentation, with reminder emails being sent out by the IT staff monthly in the future. (Brook, 2018) 

Another factor to consider is the physical security of the equipment. Firstly, all communications closets and the basement datacenter should be physically locked with only the IT person and a member of Management with keys to access them. Next, all doors for communications closets and the data center should give access alerts so any suspicious entry into these areas can be monitored. Not only should the doors to the rooms be locked, but the racks themselves should remained closed and locked when not in use by the IT department. Lastly, all physical IT equipment such as workstations and monitors should be cable locked in place to prevent theft and damage. 

In terms of mobile devices such as the laptops, they should be configured to be able to be remotely wiped. They should also be configured to have the data on them encrypted. This will help in the event a mobile device is stolen and removed from the hospital, making the data useless if it is taken off before it is wiped.

For network security, the primary change that should be made is the implementation of a firewall. This could be a firewall and router combination such as a Dell SonicWALL to make it easier on the small IT staff at the hospital. Dell SonicWALL comes with network monitoring tools that should also be implemented to be proactive in terms of network infiltrators Along with the VLANs already planned, port security should be implemented to only allow for the MAC addresses of the workstations and devices already plugged into ports and to shutdown otherwise to prevent unauthorized individuals to connect to the network. There should also be protocol to shut down any ports not in use to prevent unauthorized access. Along with the VLANs, there should be ACLs in place to separate different departments that do not need to access files from one another. This will help if there is a breach in one VLAN to contain it in that VLAN and not have the entire network compromised. 

Lastly, to maintain security, it is important to schedule regular updates for all equipment and software. Updates are not only to make the equipment and software function more affectively; they are also there to patch security holes that have been discovered. Of course, these updates should be tested first, but once they are tested with no issues found then they should be implemented on a regular basis.

## Maintenance & Security Plan

### Equipment System Maintenance Tasks:

* **Keeping Network equipment up to date (switches, routers, servers)**
* Performing routine updates to networking equipment, making sure they are all up to date and all on the same update
* **Reading and dealing with submitted issues by users**
* Users will submit issues by e-mail to an e-mail shared by the full time IT staff which they can then decide on priority and respond when they can
* **Maintaining equipment (cleaning, testing backup drives and UPS)**
* Maintaining equipment to make sure that there is nothing wrong and preventable issues aren’t slowing things down
* **Schedule backups**
* Backing up important information such as patient data is a very important task, however as hospitals never close, finding an opportune time to do it can be hard
* **Updating equipment inventory**
* Keeping a detailed inventory list will help keep track of what equipment might be running low and need ordering

### Network Management Tasks:

* **Documenting changes to network**
* Anytime a change is made to the network it needs to be documented in the necessary logs
* **Documenting changes to image**
* Anytime a change is made to the image it needs to be documented in the necessary logs
* **Researching potential security threats**
* Researching potential security threats to stay ahead of potential attacks is very important and a worthwhile use of time
* **Researching potential hardware/software issues**
* Knowing that other IT professionals are dealing with a certain version of software or OS is good as it lets our network admin avoid update to that version
* **Testing new updates for software and OS**
* Doing our own testing on software and OS before pushing them out is an important task in order to prevent potential down time
* **Reading and dealing with submitted issues by users**
* Users will submit issues by e-mail to an e-mail shared by the full time IT staff which they can then decide on priority and respond when they can
* **User management**
* Making sure that users have proper permissions, removing users when they leave. HR can let IT know if anyone employees are leaving

* **Checking event logs / monitoring network resources**
* Checking to make sure that the network isn’t struggling to keep up with usage and there aren’t any unusual events occurring
* **Virus scanning, firewall maintenance**
* Keep the firewall up to date and checking for viruses is very important to make sure the hospital stays secure

## Maintenance Schedule

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday |
| **Morning**    **AM** | - Check Event Logs / Network Diagnostics  - Check submitted issues for anything urgent    - Research for potential security threats    - Respond to any issues submitted by users | - Check Event Logs / Network Diagnostics  - Check submitted issues for anything urgent    - Research hardware / software issues    - Respond to any issues submitted by users | - Check Event Logs / Network Diagnostics  - Check submitted issues for anything urgent    - Test new updates for software and OS    - Respond to any issues submitted by users | - Check Event Logs / Network Diagnostics  - Check submitted issues for anything urgent    - Apply any necessary tested updates to software and OS    - Respond to any issues submitted by users | - Check Event Logs / Network Diagnostics  - Check submitted issues for anything urgent     - Apply any necessary tested updates to software and OS    - Respond to any issues submitted by users | - Check Event Logs / Network Diagnostics  - Check submitted issues for anything urgent    - Check network documentation to confirm it is up to date    - Respond to any issues submitted by users | - Check Event Logs / Network Diagnostics  - Check submitted issues for anything urgent  - Check that backup was successful    -Update equipment inventory list    - Respond to any issues submitted by users |
| **Afternoon**    **PM** | - Maintain network equipment    - Respond to any issues submitted by users | - Maintain any network equipment that couldn’t be finished Sunday    - Respond to any issues submitted by users | - User management if necessary    - Respond to any issues submitted by users | - Check firewall rules are up to date  - Run virus scan    - Respond to any issues submitted by users | - Update or replace network equipment if necessary    - Respond to any issues submitted by users | - Schedule backup of patient data for nighttime    - Respond to any issues submitted by users | - Catch up on anything missed during week    - Respond to any issues submitted by users |

* *\*make sure that any changes to network are properly documented in the applicable change log*
* *\*if there are issues outside of the full-time personnel’s hours the on-call number will be listed to cal*

# References

Brandall, B. (2017, April 5). BPMN Tutorial: Quick-Start Guide to Business Process Model and Notation: Process Street: Checklist, Workflow and SOP Software. Retrieved from https://www.process.st/bpmn-tutorial/

Create a basic flowchart. (n.d.). Retrieved from <https://support.office.com/en-us/article/create-a-basic-flowchart-e207d975-4a51-4bfa-a356-eeec314bd276>

Create a cross-functional flowchart. (n.d.). Retrieved from <https://support.office.com/en-us/article/create-a-cross-functional-flowchart-4a403033-9787-454f-b87e-b88452c47a21>

Hebb, N. (n.d.). Cross Functional Flowcharts. Retrieved from https://www.breezetree.com/articles/cross-functional-flowchart

Barracuda (n.d.) What is a DMZ Network? Retrieved from    
https://www.barracuda.com/glossary/dmz-network

Cisco, *Best Practices – Location-Aware WLAN Design Considerations*, retrieved from: <https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/WiFiLBS-DG/wifich5.pdf>

Cisco (n.d.) Cisco Medical Grade Network: Providing Foundational Architectures for Healthcare [Infographic]. Retrieved from   
<https://www.cisco.com/c/dam/global/en_ca/solutions/strategy/healthcare/assets/docs/09CS2124-MGN.pdf>

Cisco Networking Academy (2014), *Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design*, retrieved from: <http://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4>

Edraw (n.d) Hierarchical Network Design - Access Layer of the Hierarchical Network Design Model. Retrieved from <https://www.edrawsoft.com/Hierarchical-Network-Design.php>

Lorenzen, M. (2018, June 20). The Importance of Using VLANs to Segment Network Traffic. Retrieved from https://www.linkedin.com/pulse/importance-using-vlans-segment-network-traffic-mike/

NetworkDirection.net (2018), *Hierarchical Network Model*, retrieved from: <https://networkdirection.net/articles/network-theory/hierarchicalnetworkmodel/>

Rouse, M. (Last revision: 2019, May) RAID (redundant array of independent disks). Retrieved from <https://searchstorage.techtarget.com/definition/RAID>

SAFE Architecture Guide. (2018, January). Retrieved from <https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/safe-architecture-guide-secure-campus.pdf>

Small Enterprise Design Profile Reference Guide. (2013, October 31). Retrieved September 29, 2019, from <https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Small_Enterprise_Design_Profile/SEDP/chap2.html#wp1054292>

Vacca, J. (2001), *Wireless Design Considerations*, retrieved from: <http://www.informit.com/articles/article.aspx?p=24483&seqNum=5>

Warner Reese, C. (2010, April 15) Designing a Medical Grade Network. Retrieved from   
<https://netcraftsmen.com/designing-a-medical-grade-network/>

Brook, C. (2018, December 4). 20 Information Security Tips for Hospitals. Retrieved October 29, 2019, from <https://digitalguardian.com/blog/20-information-security-tips-hospitals>.

Wood, J. (n.d.). The Personal Information Protection And Electronic Documents Act. Retrieved October 29, 2019, from <https://www.colleaga.org/article/personal-information-protection-and-electronic-documents-act-pipeda-canada>.

TechDonut (n.d.) Network management tasks. Retrieved November 4, 2019 from <https://www.techdonut.co.uk/buy-and-manage-it/regular-it-maintenance/network-management-tasks>

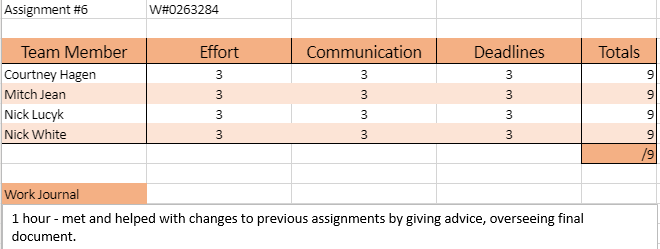
Welcher, P. (2018, June 21) Network Maintenance Best Practices. Retrieved November 4, 2019 from   
<https://www.networkcomputing.com/networking/network-maintenance-best-practices>

# Appendix A – Complete Time & Cost

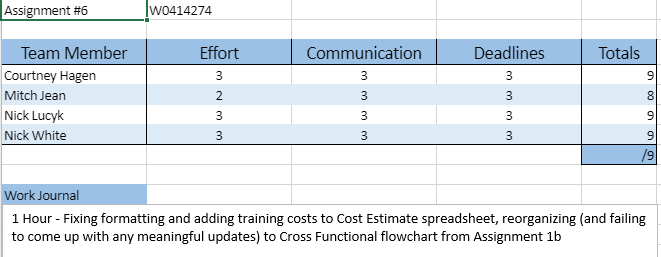


# Appendix B – Work Journals

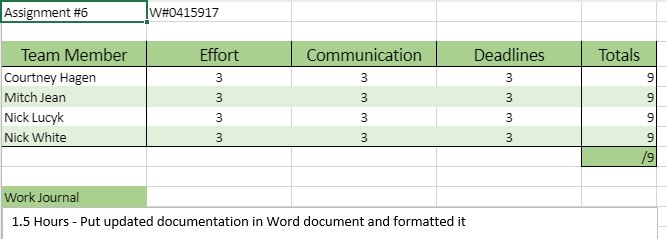
## Courtney Hagen



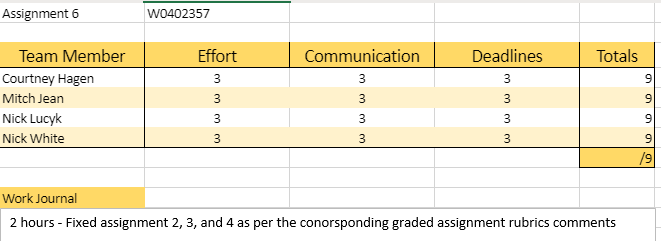
## Mitch Jean



## Nick Lucyk



## Nick White



## Totals

