Network Facility Design Proposal

Medical Facility Network Hardware Deployment

Shannon B. Caldwell
Shannon Caldwell12/8/2011

Executive Summary

Overview and Recommendations

Our report will lay out our recommendations for hardware, software, policies, and implementation for a network infrastructure of a small hospital. The recommendations found in this report will focus on redundancy (no less than 99.99% uptime) and compliance with HIPAA requirements for wireless networks first and foremost. This report will talk about our recommendations for the physical layout and logical topologies for the medical facility for whom we are designing the network.

Server virtualization is becoming much more prevalent in Health care I.T. system configuration where it is excellent for helping reduce costs of hardware. With this advantage, however, it also poses some risks and can be difficult to configure. Most notably, virtualization can be challenging when server clustering is used for the physical set up in which it is utilized.
For our Medical Facility Network Design, we will employ server virtualization by running two virtual machines: RedHat Linux Enterprise (version 6) for the Hospital Information System and Windows server 2001 for imaging, communication, and the computerized practitioner order entry system (CPOE.)

With the critical nature of the systems we will run, the configuration's reliability is paramount and will require considerable forethought to ensure the goal of 99.99% up-time. The decision to utilize server virtualization will allow for consolidation and reduce the take away from the server's workload placing less stress on its overall capacity, therefore increasing reliability. Server virtualization will also allow for hardware upgrades without changes to each application or the operating system when more processing power or storage capacity is needed. The virtual machine's Live migration also allows for upgrades to the operating system with no interruption to applications or users.

Another advantage of virtualization is disaster recovery with its ability for point-in-time rollbacks. This allows for setting the virtual machine back to a point in time in which the system was known to be in a good state (prior to data corruption.)

Written Description

Network Constraints

There are a few considerations we had to take into account for this network:

- The network must have no less than 99.99% uptime
- 200 of the 220 users need wireless access
- The wireless access must meet HIPAA compliance
- The datacenter for the hospital is located across the street from the hospital, but no networking cables can be run between the two

Hardware

Datacenter

To connect the data center to the hospital across the street we have chosen a Cisco Aironet 1400 Wireless Bridge. The Aironet supports both point-to-point and point-to-multipoint connections, range from 2.75-20 miles, and 128 or 256 bit encryption (Figure A-2).

In the datacenter there will be a NAT device on the internet side of our servers with a firewall on the internal network side of our servers to provide protection to our network. A router and switch will be connected to our five servers which connect to our Aironet Wireless bridge and a room with workstations (Figure A-2).

Hospital

Coming into three routers from the datacenter we split up wireless network (Fig. B-3), VOIP (Fig. B-2B), and hardwired workstations (Fig. B-2A).

Network Policies

The following standard operating procedures are to be met by all of the hospital's technology equipment. These SOP are designed to reduce the risk of loss of sensitive and confidential information, or exposure of the hospital and information to outside threats, which may occur from unauthorized and incorrect use of hospital resources. The policy defines standards for ownership, configuration, and operation of equipment.
The SOP policies that are outlined must be met by all hospital technology equipment, both currently owned and operated and any future acquisitions by the hospital, equipment must be configure and set up according to this policy unless there is an exemption given by the IT department. All technology equipment, applications, and network policies mentioned in the following SOP policies will be administered and under control by the IT department.

Internet Access

Users located inside the confines of the hospital and its facilities using a terminal or other device will be considered on the hospital computer network and must use the network for appropriate business pertaining to the hospital and it entities. All employees and terminals will have access to the Internet in order to perform daily work functions and procedures as need, only specifically specified terminals will not have a connection to the internet due to there purpose and for security. Any person accessing the hospital network and/or Internet has a responsibility to use it in an appropriate manner and way that will not be harmful, degrading or offensive to any other employee or individual in or out of the hospital network. Additionally any person accessing the Internet from the hospital network may not use it to perform or assist in any form of illegal action. These actions being similar to but not exclusively limited to, distributing copyrighted/illegal material, transmitting, copying or distributing proprietary confidential or sensitive information to an outside source, and installing, downloading sending any form of software or code that may be considered malicious or harmful to other individuals and property on the network. Violation of this standard may result in revocation of network access permissions and or termination of employment.

Finally any individual who accesses the Internet from the hospital network waives their right to privacy for anything crated accessed or sent as all Internet traffic will be monitored and filtered by the IT department and can be recalled in the future to assist in the determination and or investigation as to if a violation of policy has occurred.

Printing

Printing will be restricted and allocated based on the need to the department. Access to printers will be limited to individuals for whom it is necessary for them to complete their day-to-day tasks and to ensure that possibly sensitive or confidential information being leaked and improperly controlled. All print jobs must relate to appropriate hospital business, and those without access

must ask an area supervisor for permission and access to print. Any sensitive being printed must be printed in office areas that are not publically available and have a cover page.

Storage Allocation

Each user on the network is responsible for saving their individual documents and work on a daily basis. Users will have their own individual network storage folder that will be sized at 25 gigabytes of storage for documents and other files related to their job function that will be stored and backed up on the server. These network folders will be linked to the individual users accounts so that they will be able to access them from any terminal connected to the network. Users will also be allocated 1 gigabyte of storage for each individual email account; this storage will be on the server for universal access on and off the hospital network.

Wireless Access Policy

There will be two wireless networks setup within the hospital network, one primary wireless network to be used by wireless devices owned and operated by the hospital, and guest account to be used by devices temporarily at the site and that do not fully meet the security standards of the IT department. The primary wireless network will be encrypted by WPA2 Enterprise, the SSID will not be broadcast, and each device will have a set static IP address established by the IT department. This will allow for easier monitoring and controlling of network traffic and to isolate where a possible threat or issue is located. The second wireless network will be for guest and temporary access encrypted by WPA2 Enterprise and will require a username and password that will be generated for temporary access by thy IT department. This network will be separated by the primary networks of the hospital by a firewall and have its own DHCP server for allocating IP addresses. Users on this network will have only have access to the Internet, and the possibility for access to a printer if permission and need is granted by the IT department.

E-Mail Usage

Employees will each be given their own individual company email address for official hospital business communication internally and externally, to fellow employees and any contractors or vendors. All users of the hospital email system are expected to uphold a standard of professionalism and not use the system in any way that may be offensive demeaning and harmful to others both internally and externally. In addition all users are to not use the email system to distribute and produce any form of harmful, confidential materials. Employees who use the hospital email system give up any right to privacy for anything that the send or receive including any form of attachment. All email communication will be monitored and stored and may be reviewed at anytime.

User Administration

All users will be required to logon to any terminal and the hospital network through use of a username and password that will be established by the IT department for each user. By logging in each user will activate their predetermined access controls and permissions, we will be using a role based access control (RBAC) system for user administration. Each user depending on their level and role within the hospital will have increased or decreased levels of access to patient medical records and resources on the network.

Naming Conventions

All technology equipment located within the hospital will be named with the similar standard. All portable and stationary computer terminals will be named in sequential order preceded by which department, the equipment is primarily located in. For example a laptop located in the lab are will be named LABLT1 followed by LABLT2.

Devices such as routers and servers the will be physically permanent will be named based on the region of the building that they are located in, sequentially if there is more then one device of similar nature in the location. For example a switch located in the lab area would be named SWLAB1 followed by SWLAB2.

Protocol Standards

The main protocol standard that will be used on the network will be TCP/IP protocol, his will allow the network to utilize multiple types of technology and equipment, such as VOIP phone systems and IP based printers. This will allow for easy adaptation and expansion on the network and also easier monitoring and controlling of traffic and bandwidth usage. The other main protocol that will be used will be Remote Authentication Dial In User Service (RADIUS), this protocol will be used to allow centralized managed authentication for users to login and access network resources.

Workstation Configuration

All workstations will be equipped basic peripherals and either a wireless or wired network interface card (NIC) in order to connect to the network and services. Depending on the location of specific terminals within the network specific modifications will be made in order for expansion by adding specialized medical equipment to the terminals and increased performance for medical imaging and test processing.

Environmental Issues

In order for the technology infrastructure to function properly all server and datacenter locations must be kept at appropriate environmental levels. Dedicated air conditioning and venting fans will be used for each server and data server to keep all equipment in a cool environment and low humidity. This will help extend the longevity of the servers and datacenters, and prevent self-induced damage.

Power

All computer terminals and laptops will be connected to UPS power supply devices as to reduce the risk of possible damage done by a power surge and or improper shutdown. All servers will be connected to large-scale UPS devices that will protect against power surges and carry the power load until backup generators will be able to engage incase of power failure. This will allow adequate time for non-essential services to be shutdown and the servers to be properly shutdown.

Applying Patches

In order to effectively apply patches to the multiple devices located on the network, a server will be running Windows Server Update Services (WSUS). This will allow for the IT department to download any need updates or hotfixes and push them out over the network to all terminals needing the update. This will save on bandwidth and drag on network traffic because the update will only have to be downloaded once and can be applied over the network during downtime as to not interfere with normal operations.

Security Policies

User Account Access/ Passwords

- Each employee will be given a username and will be required to set a password upon arrival.
- Upon termination, the employee's username and password will be deactivated. If the employee returns to work they will get a new username and will be required to make a new password. The old account is just kept for the purpose of its records.
- Users can log into any computer in the building with their account name and password, but cannot log into more than one computer at a time unless given special permission from the administrator.
- Passwords much be at least 12 characters long
- Passwords will be comprised of any combination of letters, numbers, and symbols as long as there is at least one of each in the password
- Users must create a new password with the IT department on the first business day of each month
- New passwords cannot be the same as any previous password.
- If a user fails to enter their password correctly 5 times than they will be locked out of their account and must contact the administrator.

Network Access

- Network access is for hospital employees only
- No personal devices are allowed on the network for any reason
- For access outside of the office, employees will use ssh protocol 2 connections only
- The idle timeout for user logins will be 10 minutes
- We will disable root login over SSH

Hardware/ Firewalls

- We will use SELinux as our system firewall
- SELinux uses a combination of MAC scheme and a discretionary access control scheme
- If a request passes the permission of the users "role" in the DAC scheme it then is passed through the MAC scheme. If it passes through the MAC scheme than the user can access the data or file which they asked permission to see.

Encryption Use

We will use SSL certificates for Encryption

Logging practices

- An Auditing infrastructure will be used to log all user data and low level events that occur throughout the system.
- Back-ups will be kept off site just in case of a malware infection so the logs can be used to find the infection if necessary.

Physical Access Rules

- The building will have security cameras set up in the halls of the hospital, and at each door leading from the exterior of the building.
- All network equipment will be kept in a secure room protected by biometric scanners that scan the individual's finger print. Only the network admin or other IT employee's whom the admin deems has a legitimate reason will have access to this room.
- Each room of the hospital will require access cards to enter during business hours and after hours a physical key will also be required to unlock the doors of the hospital.
- During business hours, employees are responsible for their workstation and making sure no one gains access to it other than themself.
- There will be a 24 hour security team making sure that all the equipment is safe and secure at all times of the day.
- At the end of each day each user must log out of their work station.

IDS/IPS regular Vulnerability Assessment

- We will use both IDS and IPS in order to catch and stop malicious traffic from coming into the network.
- We will log all network traffic so that it can be analyzed to find were the break in occurred if there is an attack

Disciplinarian Policies

- If any illegal activity occurs the user's account will be immediately deactivated and the employee will be suspended without pay while an investigation is undergone.
- If the employee indeed is guilty than their employment will be terminated and legal action may or may not be taken depending on the circumstances.
- If the employee is not guilty of the crime but his/her account was used for the intrusion, than they may come back to work from their unpaid break and must set up a new account with restricted access for 2 weeks
- If an employee just breaks a minor rule than they must have a meeting with the system admin and restrictions may or may not be placed on their account depending on what the administrator deems necessary for punishment.

Disaster Recovery Policies

Disaster Recovery Policy

Disaster – For our purposes, a "disaster" is declared by the Information Technology Administrator or by a higher authority. This includes, but is not limited to, Electrical Failure, Fire, Flood, Tornado, Tropical Storm/Hurricane, or Earthquake.

Disaster Preparation

Electrical Failure - Tools

- The first step in recovering from a disaster is to work to prepare for them. To this end, we must have the appropriate tools in case of a disaster.
- 150kW Generac Generator - $28,999.99 – This will be enough to keep the medical facility running in case of emergency – whether it be a power failure due to simple loss, a brownout, or a hurricane. They will run on either propane or natural gas, so it will only depend on the amount of fuel we have on hand.
- 2 - 24,000W TRIPP LITE SmartOnline UPS - $11,399.99 each – It will take a few minutes to get the generators on-line. In the process, we cannot lose the servers at any point during a power failure. These UPS's will be sufficient to bridge the gap until the generators kick on. We should have one in every building we have a server – at present, 2.
- 2 – Tripp Lite External Battery Frame - $3,204 each – In case we find that we need more power, these will connect to the UPS's and provide housing for extra batteries.
- 10 – Tripp Lite Internal Battery Pack - $650 each – These will be housed inside the Battery Frames for more power.

Preparatory Measures

- The fuel meter for the generator must be checked once every 2 weeks for fill.
- The generator and all UPS's must be tested once every month, except in case of failure; in which case, the generator must be tested after repairs for 4 consecutive weeks to make sure it does not fail again.
- Every workstation will be connected to a well-rated surge protector.

Fire - Tools

- At least 30 fire extinguishers - $45 each

Preparatory Measures

- Follow OSHA standards of having a fire extinguisher every 75 feet. At least 1 fire extinguisher should be available for every 3000 square feet.
- Fire extinguishers must be checked for fill every 6 months by a licensed professional.
- Fire sprinklers must be checked for proper working condition according to OSHA Standards.
- Fire drills must be conducted every month for moveable patients, every 6 months for immoveable patients.
- Fire exits and proper exiting procedures must be covered by management once every 6 months.

Tropical Disturbance/Hurricane – Preparatory Measures

- Follow proper procedures for hospitals as it relates to evacuation orders.
- Check all UPS's and the generator for proper function at least 7-10 days in advance of any and all Tropical Storms or higher in which the city lies within the cone of uncertainty.
- Take all precautions deemed necessary and proper by authorities and board of directors to further secure the hospital.

Other Preparatory Measures

- Server room must be in a fireproof and watertight room on the first floor near the center of the building.

<u>Disaster Endurance</u>

Tools

- IBM Infrastructure Recovery Services: Rapid Recovery – 52 month contract, $120,000/month – this will keep the hospital's data backed up and readily accessible through any disaster. This package includes encrypted data in a dedicated IBM Recovery Center (hot site). This is completely necessary to ensure that all patients are served to the best of our ability, no matter what the circumstances.

Policies

- Recovery Services must be contacted 5-7 days ahead of time, if possible, in case of any disaster. If this time is not possible, then the service must be contacted as soon as possible so to get the Recovery Process started.

Disaster Recovery

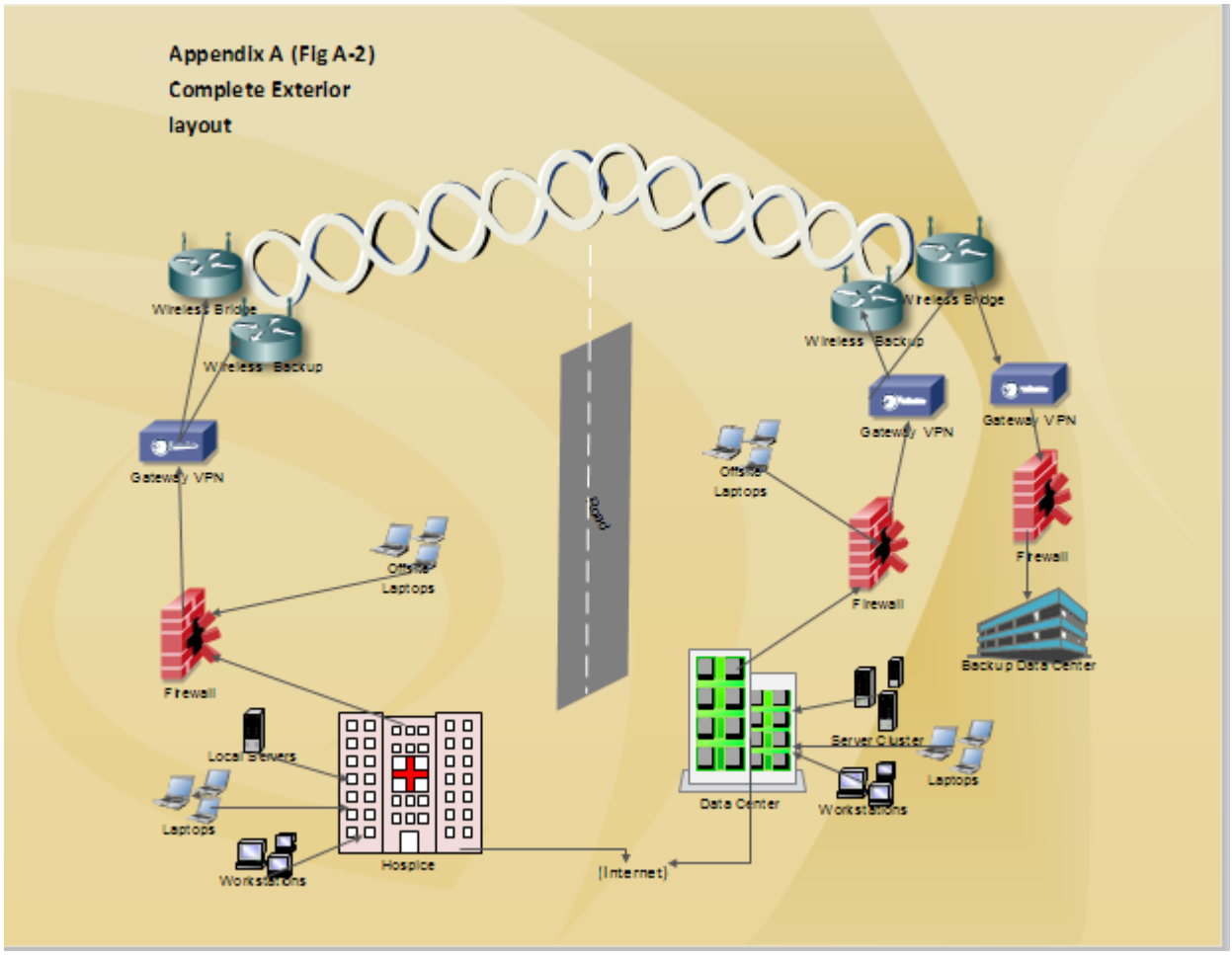
Policies

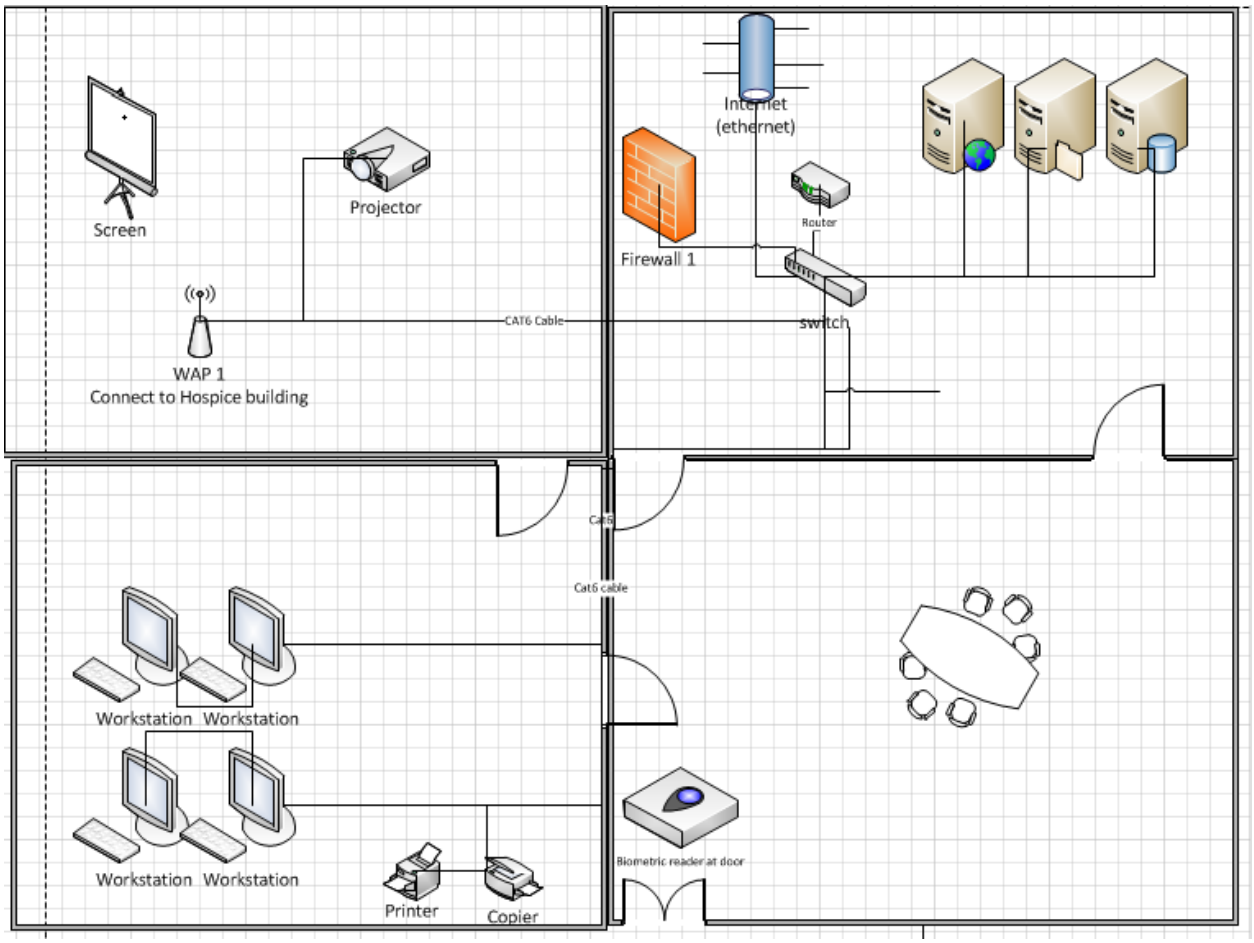
- As soon as it is deemed safe by authorities to be in the area, inspect any and all damage caused by the disaster.
- All damages must be inspected and notated, no matter how small.
- Damage reports must be turned in to the Head of Disaster Recovery of the Information Technology Department and to any other hospital heads as the Information Technology Administrator deems necessary. Reports must be turned in no more than one (1) business week after a disaster is declared.
- Besides damages, damage reports must include lessons learned from the disaster and/or strategies that could prevent the damage in future disasters.
- The Recovery Services Center must be contacted as soon as possible after their services are no longer needed for disaster recovery.

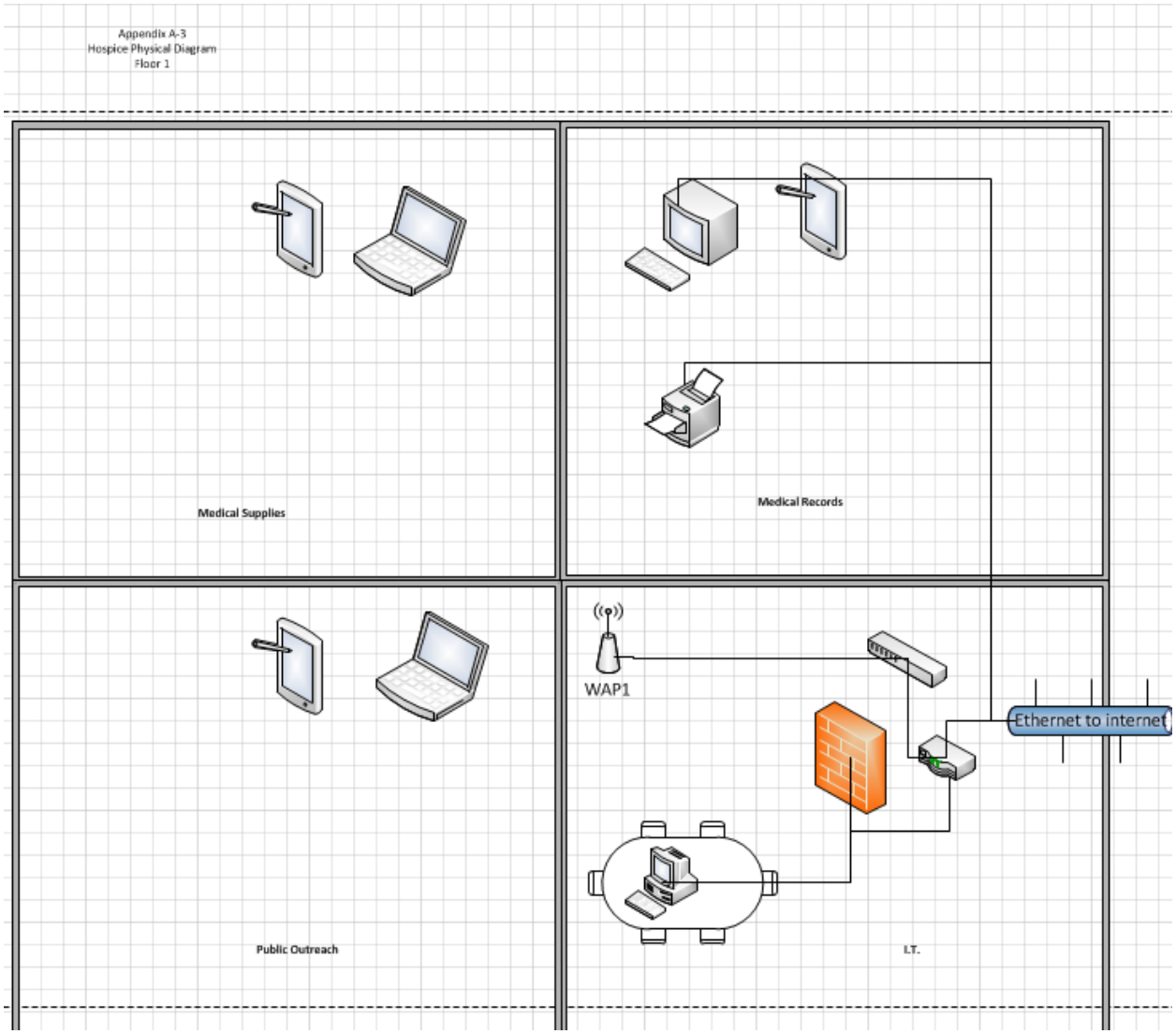
Miscellaneous Policy

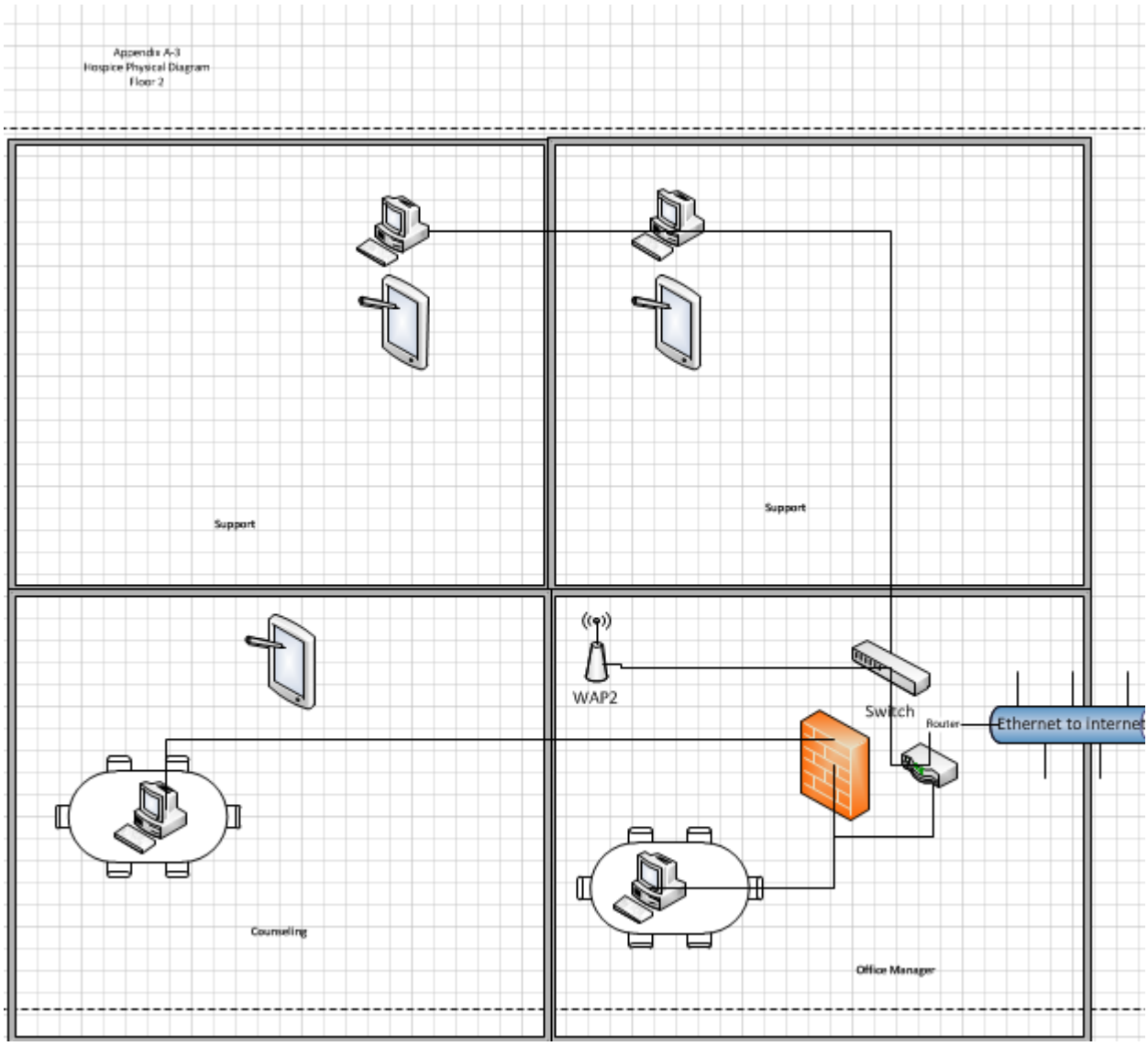
- If not stated above, all backup situations and equipment must be tested every 6 months or sooner if prescribed by OSHA, Board of Directors, or another governmental authority.
- Only the Information Technology Administrator or higher authority may amend this Disaster Recovery Policy. Additions may include, but are not limited to, strategies to help recover from future disasters, new equipment, more disaster recovery categories, and other categories as deemed necessary and proper by the Information Technology Administrator. These policies must be ratified by the Board of Directors for good fit to the hospital.

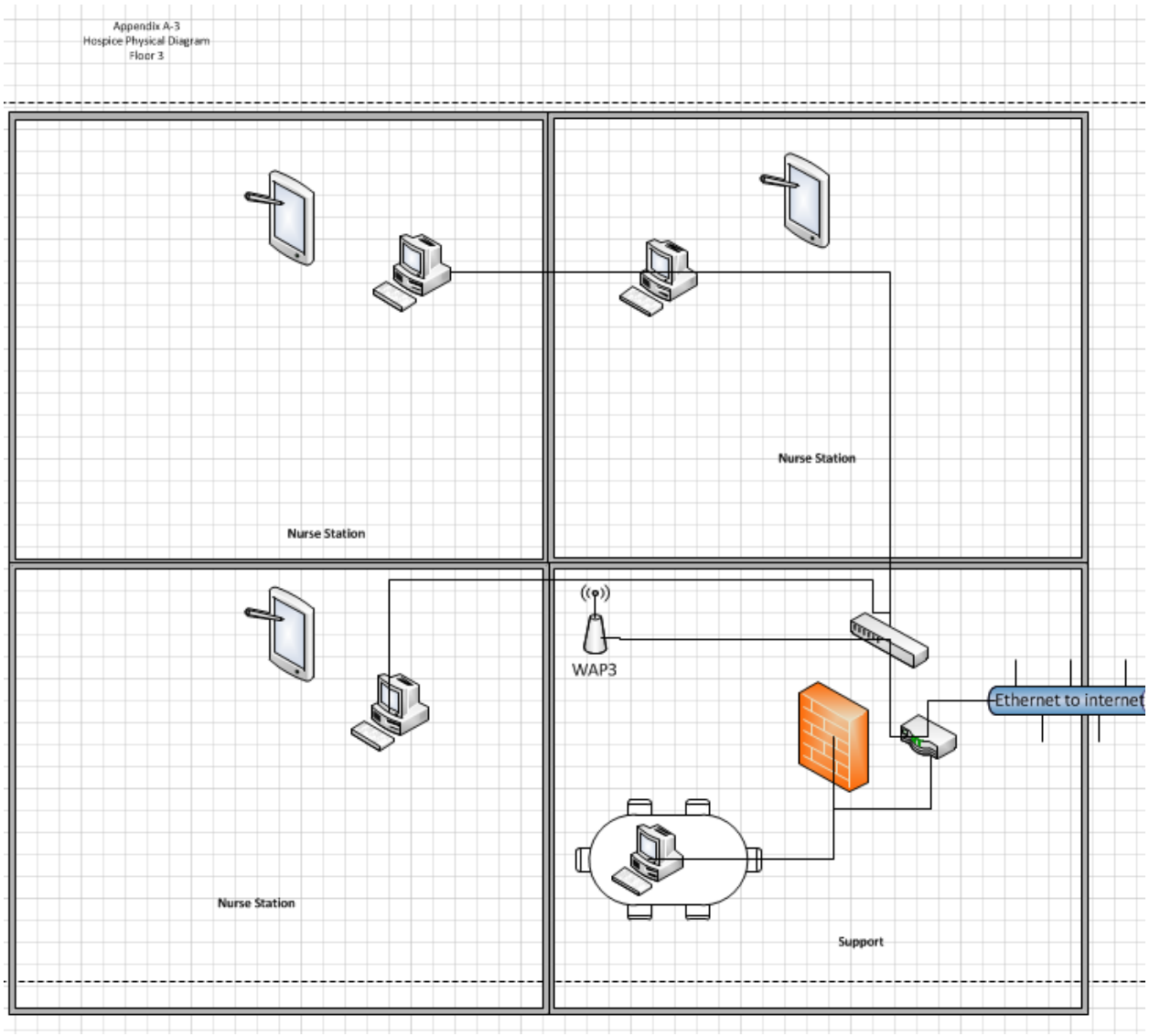
Appendix A. Physical Topology

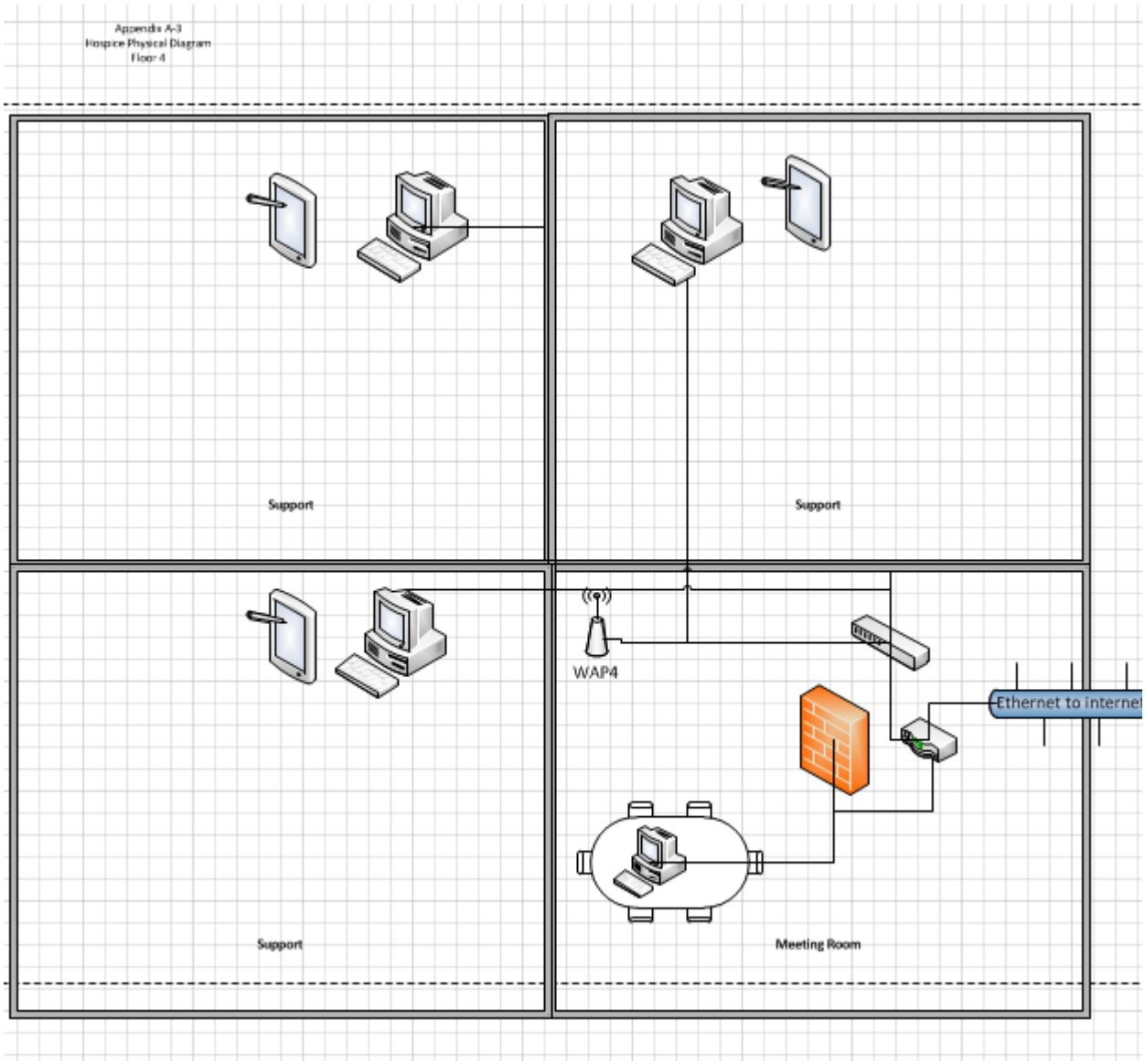


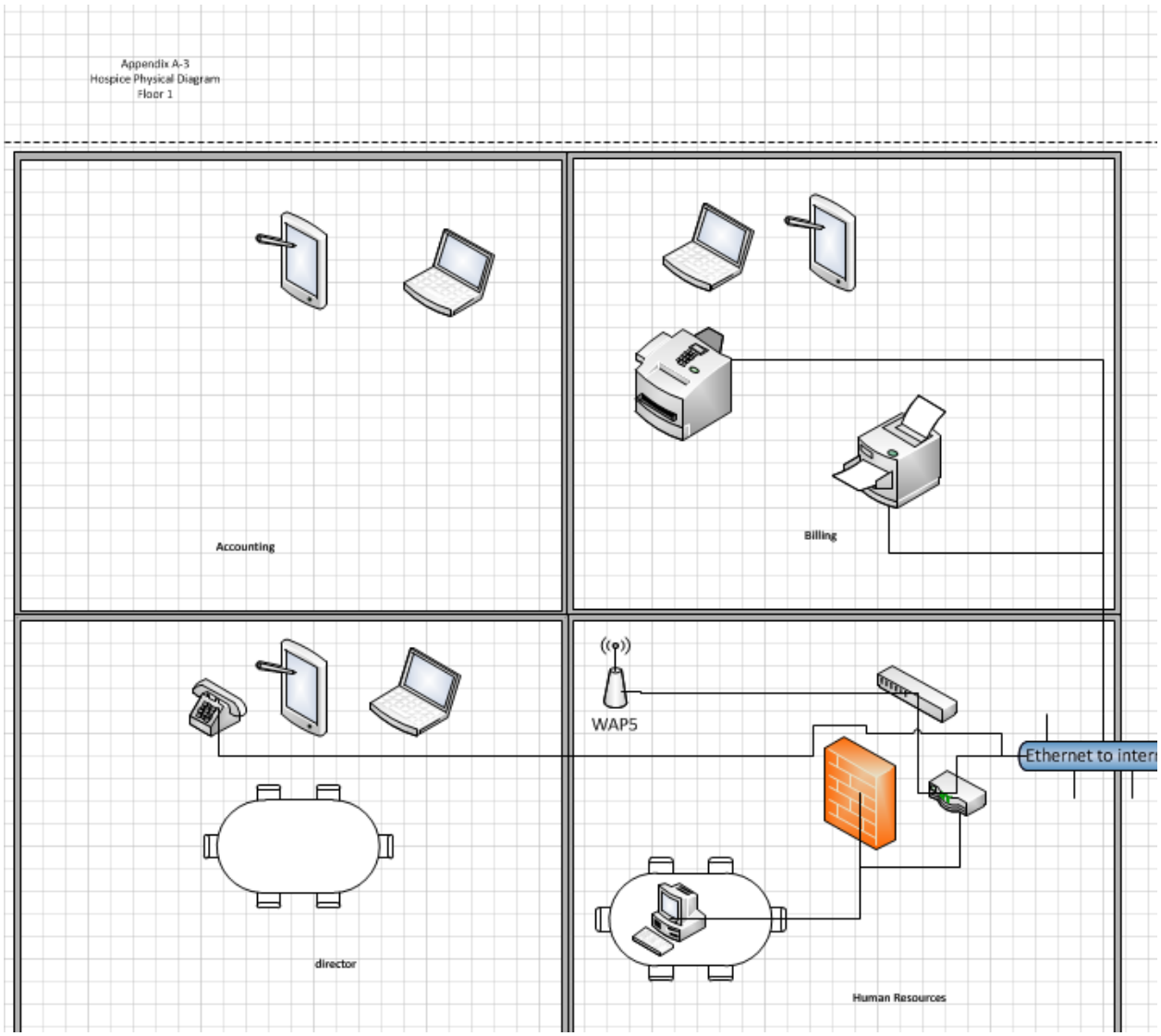

Screen
Projector
Internet
(ethernet)
Firewall 1
Router
switch
CAT6 Cable
WAP 1
Connect to Hospice building
Cat6
Cat6 cable
Workstation
Workstation
Workstation
Workstation
Printer
Copier
Biometric reader at door

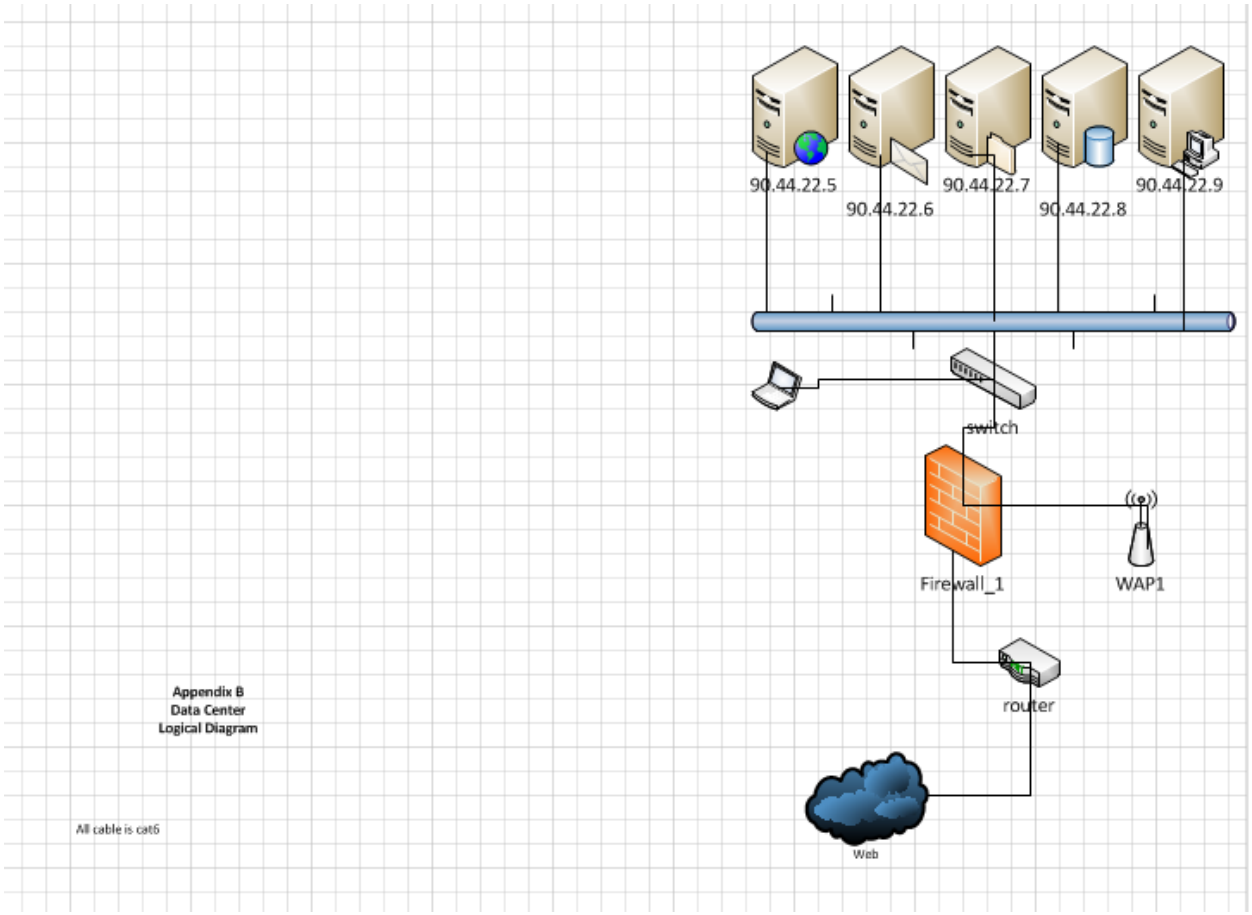

Appendix A-3
Hospice Physical Diagram
Floor 1
Medical Supplies
Medical Records
Public Outreach
WAP1
Ethernet to internet
I.T.

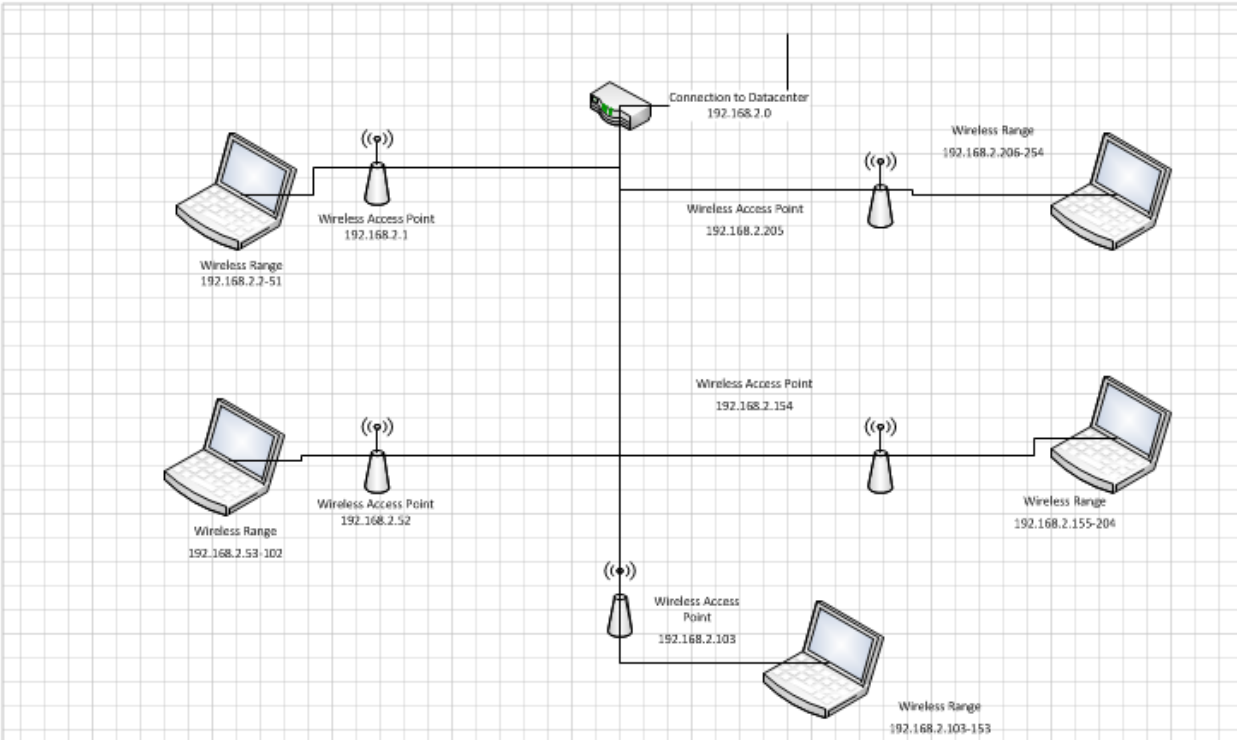

Appendix A-3
Hospice Physical Diagram
Floor 2
Support
Support
WAP2
Switch
Router
Ethernet to Internet
Counseling
Office Manager


Appendix A-3
Hospice Physical Diagram
Floor 3
Nurse Station
Nurse Station
Nurse Station
WAP3
Ethernet to internet
Support


Appendix A-3
Hospice Physical Diagram
Floor 4
Support
Support
Support
WAP4
Ethernet to internet
Meeting Room


Appendix A-3
Hospice Physical Diagram
Floor 1
Accounting
Billing
director
WAP5
Ethernet to inter
Human Resources


90.44.22.5
90.44.22.6
90.44.22.7
90.44.22.8
90.44.22.9
switch
Firewall_1
WAP1
router
Web
Appendix B
Data Center
Logical Diagram
All cable is cat6



Appendix Fig. B-3
Hospital Wireless Logical Layout