Healthcare Data Compliant Network

Cisco Team 12: Justin Tecson, Kaan Baltaci, Luke DaSilva, Maciej Jedryczka

The New Jersey Institute of Technology

IT491 - 004, IT/CS Senior Capstone Project

Instructor: Dr.Eljabiri

Due Date: 4/30/24

Table of Contents

Chapter 1: Introduction **Author: Maciej Jędryczka**

1.1 Glossary of Terms

- Bad Actor - A person who means to infiltrate or cause harm.
- HIPAA - Health Information Protection and Accountability act
- Packet Tracer - Cisco owned network building platform.
- VLAN - Virtual Local Access Network.
- FTP - File Transfer Protocol.
- TFTP - Trivial File Transfer Protocol.
- RFID - Radio Frequency Identification.
- Switch - A device that allows the creation of VLANs and to expand interconnections from a router.
- Router - A device that facilitates packet routing.
- Computer - Device for storing and processing various types of data.
- Gantt Chart - A type of chart that displays multiple events that occur simultaneously.
- FDD - Feature Driven Development.
- IP - An address for a computer.
- IoT - Internet of Things
- MCU - Micro-Controller Unit

1.2 Project Background

Health clinics are becoming more under threat in recent days. As bad actors are beginning to realize that hospitals and health clinics are more likely to pay or fulfill any demands, it makes them more likely to be targeted again.The healthcare industry is already reliant on technological solutions for handling patient information, streamlining processes, and to enhance patient care. To have any of these functions under threat will directly affect the patient's care and the financial stability of the health facility.

A health facility relies critically on network infrastructure for many things. One very important role is to handle patient information. This is on the top of the list because patients trust healthcare providers with their most sensitive information. Such includes medical histories, test results, and personal information. Maintaining this trust and privacy is one of the pillars and legal obligations in healthcare. In the United States, HIPAA exists as a set of strict standards for protecting patient health information and carries heavy punishments for any occurrences of violation. For good reason. HIPAA works to force health organizations to implement appropriate security measures to protect and safeguard personal health information. This specifically includes protected electronic health information (ePHI). A good, robust network within a health facility must at the very least follow HIPAA standards. Also to not only to protect patient information, but to also protect the infrastructure itself from any attacks or subversion of security. Another critical role the network infrastructure must meet the requirements for is to facilitate secure and reliable communications channels. It is important to maintain seamless interactions between healthcare workers and their patients.

1.3 Problem Definition

For this project, the healthcare facility we're preparing is a small health clinic. Able to provide care for a handful of people at a time and to allow staff to efficiently do their work with little to no down time. The infrastructure in plan should be easy to implement in order to be easily adopted by current facilities, have the ability to expand to better adapt to changes, and to be robust without being too complicated and to be easily manageable. The network must have secure channels for communications, servers to facilitate different functions that might be useful for the facility like network storage, web server hosting, and remote access capabilities. The network must also accommodate patients and visitors with guest WiFi as well as secure WiFi for facility staff, devices, and IoT devices. Lastly, for physical security, the facility must have the ability to secure sensitive rooms with RFID technology.

1.4 Revision Updates

Milestone 1: Research and Design

- In order to better ascertain the scope of the project and what needs to be done and how, individuals in the group were tasked with finding resources related to constructing a healthcare security compliant network. After finding examples about existing network infrastructures, resources about healthcare security, and network best practices, we were ready to move onto the next phase of the project.

Milestone 2: Prototyping and Testing

- Packet Tracer is a great testing ground for Cisco related networks. The first thing we built was a map of the health clinic. This is to keep us grounded to the project and to think closely to what a healthcare facility might need. Then devices were laid around the map. Routers, switches, servers, and computers; things that any network needs. Then we

designed the topology and how the VLANs must work by assigning ip addresses to the devices. After making sure every device can communicate with the devices they're allowed to communicate with, it was time to secure the network. This was done by giving every Cisco device passwords and different elevations of access.

Milestone 3: Final Touches

- After making sure that the network works as designed, it was time to add the finishing touches by adding the required functionality. This included configuring the servers to facilitate FTP functionality, allowing remote connections to the network for privileged users, and the facitlie's ability to host their own web server. Lastly, a final addition to the simulated network were some quality of life features. Some of which were working fire suppression sprinklers, RFID locks, and RFID keycards.

Chapter 2: Project Management

Author: Kaan Baltaci

2.1 Task Analysis:

The task analysis was needed for setting the steps and actions needed for completing our project. Our first step was identifying these tasks, such as the solutions we needed to implement, and assigning roles. The next step involved breaking these tasks down into smaller and more manageable steps. Such as doing research on the HIPAA laws or assigning VLANs. This helped us formulate the time frame for completing these tasks and assign responsibilities to each member of the team. The task analysis also consisted of reviewing and refining our tasks. We achieved this by going over our tasks and fixing or improving our network infrastructure if needed.

2.2 Roles:

Justin Tecson - Project Manager

- Designer & Developer
    - Created network topology and architecture, added configurations to networking devices such as the switches, routers, and servers.

Kaan Baltaci - Co-Project Manager

- Developer
    - Configured the networking devices such as routers, switches and servers.

Luke DaSilva - Individual Contributor

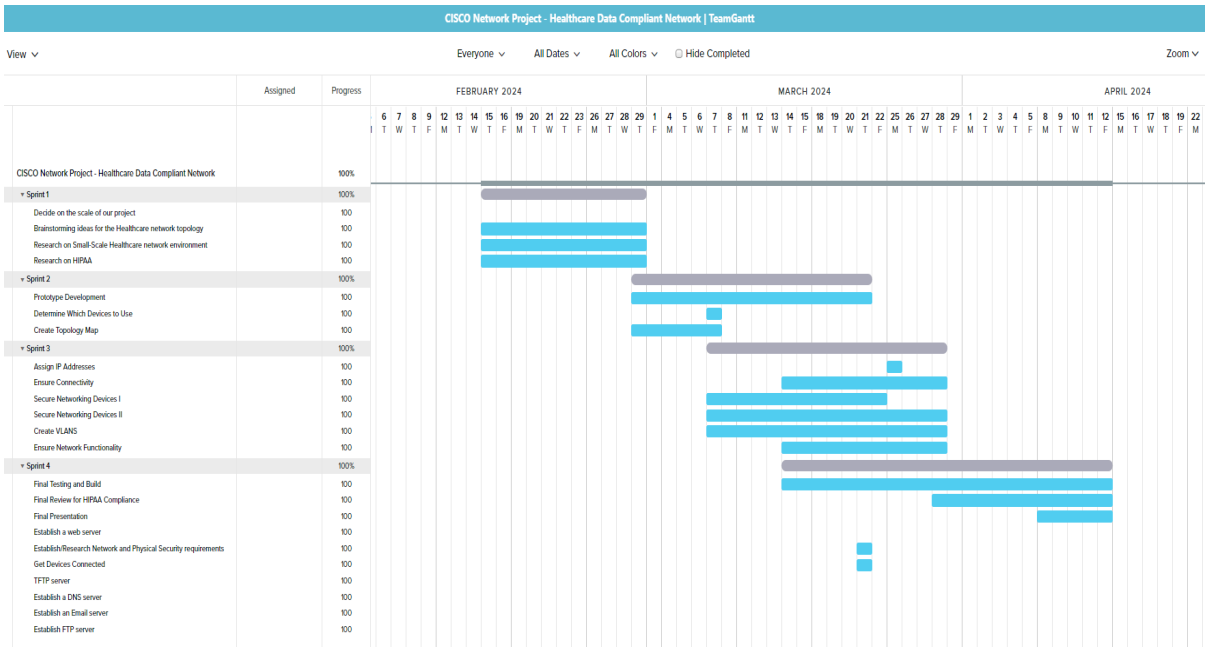
- Designer

- Created the network topology layouts and added devices throughout the network architecture.

Maciej Jędryczka - Individual Contributor

- Developer
  - Configured the networking devices such as routers, switches and servers.

2.3 Gantt Chart:



CISCO Network Project - Healthcare Data Compliant Network		100%
▾ Sprint 1		100%
Decide on the scale of our project		100
Brainstorming ideas for the Healthcare network topology		100
Research on Small-Scale Healthcare network environment		100
Research on HIPAA		100
▾ Sprint 2		100%
Prototype Development		100
Determine Which Devices to Use		100
Create Topology Map		100
▾ Sprint 3		100%
Assign IP Addresses		100
Ensure Connectivity		100
Secure Networking Devices I		100
Secure Networking Devices II		100
Create VLANS		100
Ensure Network Functionality		100
▾ Sprint 4		100%
Final Testing and Build		100
Final Review for HIPAA Compliance		100
Final Presentation		100
Establish a web server		100
Establish/Research Network and Physical Security requirements		100
Get Devices Connected		100
TFTP server		100
Establish a DNS server		100
Establish an Email server		100
Establish FTP server		100

To create an extensive work breakdown structure, we used the Gantt chart and split our process into 4 sprints. By dividing our project into four sprints, we were able to establish a good workflow to ensure project completion. We were able to track our progress and manage the tasks that needed to be completed.

2.4 Risks Identification:

- Communication
    - Can we, as a team, work effectively, efficiently, and communicate with one another?

- Time Management
    - Staying on track with our tasks and completing them on time
- Ensuring Healthcare Compliance
    - Is our project HIPPA compliant?
- Technical Knowledge
    - Our team members need to have technical knowledge to complete their individual and group tasks.

2.5 Risk Mitigation:

- Usage of online social platforms
    - By using platforms such as Discord, we actively communicated with each other.
- In-depth Research
    - Doing constant research into reliable resources for implementing and maintaining healthcare compliance.
- Learning the material
    - Learning the material from Cisco Academy and completing our assignments. As well as reading outside information to gather the necessary knowledge to do our tasks for the project. It is important to maintain technical advantage when implementing solutions for our network infrastructure.
- Time Management
    - It is important to use platforms such as Trello, Gantt Charts, and the SCRUM methodology to create a time frame suitable for our group and project goals. These platforms helped us formulate time frames such as completion deadlines,

assigning tasks, and setting meetings. All of this combined helped us create visibility and accountability.

Chapter 3: Define

Author: Kaan Baltaci

3.1 Stakeholders Identification

- Cisco Team 12 - Our team members
- Cisco NetAcademy Instructor - Omar Firas
- NJIT Faculty - Professors, Judges, Admin
- Students - in the capstone class
- Hypothetical End Users - Nurses, Doctors, Patients

3.2 Hardware used:

- 11 PCs: Allows the employees to do their work, such as accessing patient data and setting up appointments.
- 3 Switches (2960 IOS 15): A hardware device used to connect multiple networking devices within our network. They are used for VLAN support, port connectivity, and functionality.
- 1 MultiLayer Switch (3650-24PS): Creates communication between the router and the other switches.

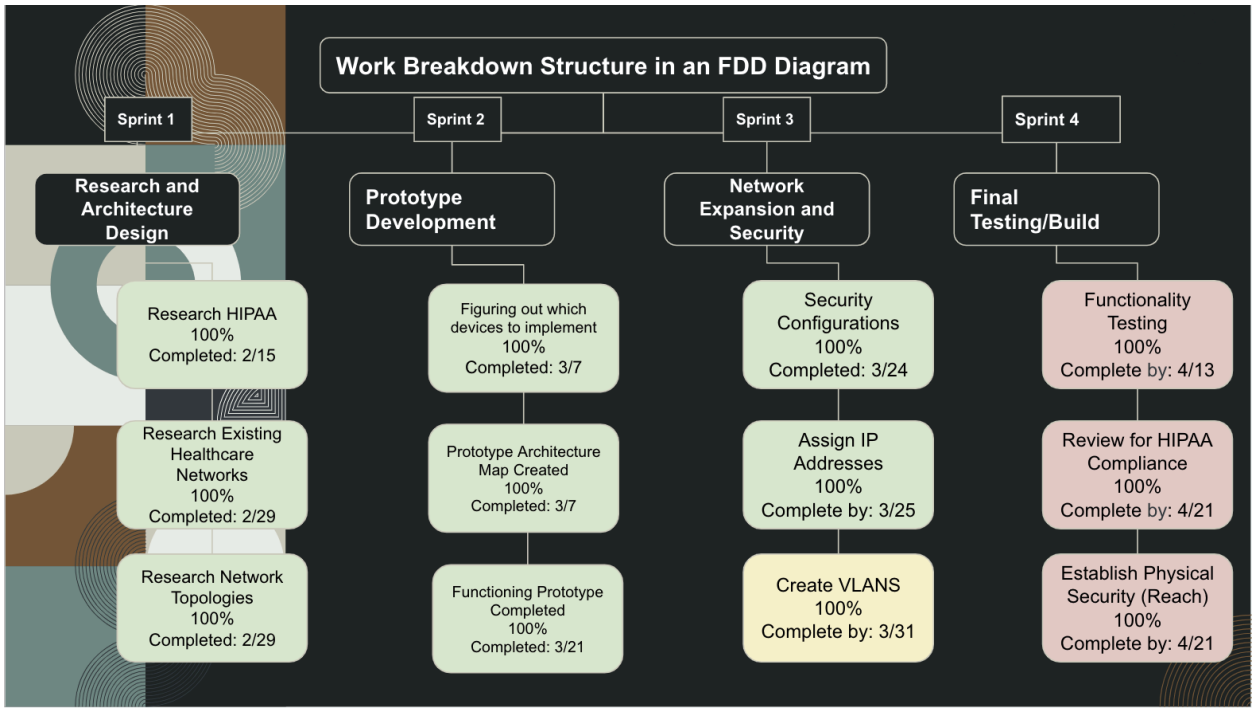
- 3 Printers: The employees need access to printers to print required documents. There is a printer located in the lobby, the headquarters room, and the doctor's office.
- 5 Servers
    - Web Server: It delivers web content over the internet.
    - E-Mail: A server that manages the storage, sending, and receiving of email messages.
    - TFTP: Trivial File Transfer Protocol server is used for transferring files between devices on our network.
    - FTP: File Transfer Protocol server enables the transfer of files between the PCs over our network.
    - IOT Registration Server: The Internet of Things registration server manages and registers IoT devices that are connected to the network.
- 1 Router (2911): A networking device that forwards data packets in a network. It connects all the switches and other devices on our network.
- Door Security
    - RFID Reader: It is a radio frequency device that is used to read RFID cards. It can be accessed only by authorized RFID cards.
    - RFID Card: It is used for identification purposes; only authorized personnel have access to these cards.
    - MCU boards: Microcontroller unit boards are used to create the connection between the door and the RFID reader.
    - Door: Physical security to stop unauthorized access with the assistance of the RFID reader.

- Fire Suppression System
    - Fire Monitor: Used for fire detection, it sends signals to the fire sprinklers in case of a fire.
    - Fire Sprinklers: When fire is detected, it unleashes water strong enough to extinguish or control the fire in the building.
    - MCU boards: Microcontroller unit boards are used to create the connection between the fire monitoring system and the fire sprinkler system.

3.3 Project Scope:

Our project objective is to create a healthcare data compliant network that takes into account HIPAA laws. It needs full network functionality to handle and protect sensitive patient data. Our project scope consists of creating a network architecture, device configurations, network connectivity, and security implementations. All the elements mentioned together create a working network suitable for protecting sensitive patient information and compliant with healthcare data laws.

FDD Diagram :



The FDD diagram details how we allocated different large tasks or goals under several overarching sprints. Our entire process spans 4 sprints, starting with our research into the architecture and design, the prototype development of our network, the expansion of that network as well as the implementation of security features, and the final testing of our network

Chapter 4: Design

Author: Luke DaSilva

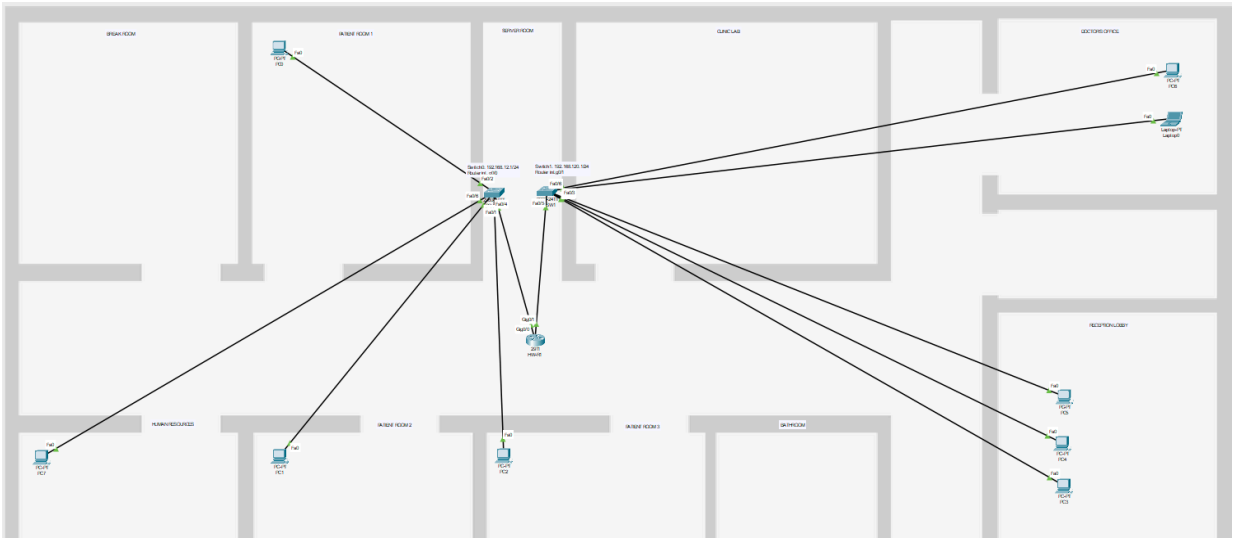
4.1 Design Process

Early on in our design process, we made the decision to split our network into two distinct sections: one section we labeled “internal”, and the other section we called “public-facing”. This division would remain a principal feature of our network moving forwards, and throughout the different prototypes we had created it slowly evolved into the final product you will see at the end.

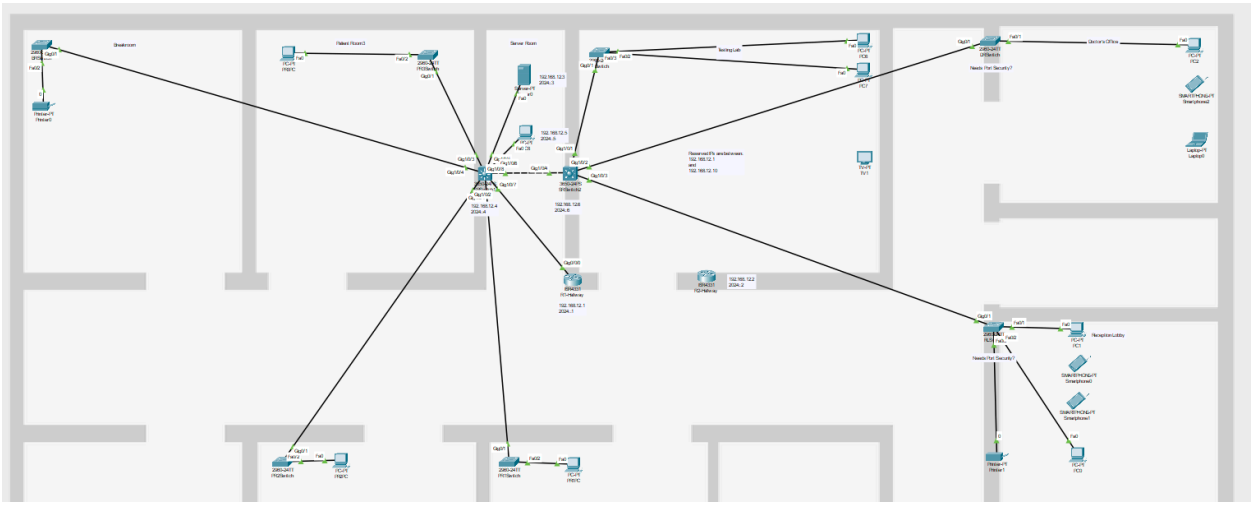
Another feature with our network that we had settled on was the simple structural details that would satiate the needs of a simple, small clinic: a break room with a printer, each exam room having a single PC, devices in a testing lab, a receptionist’s desk having a printer and a PC, and the head doctor’s office. Once we settled on roughly where devices would be, we moved towards early prototyping.

4.2 Prototyping Stages

The first prototype we designed had the network’s backbone segmented into two switches, joined by a router. We had originally planned to statically assign IPs and segment the network into two VLANs for security, so that the computers at the receptionists desk couldn’t access any sensitive patient data from the internal VLAN. Below is a picture of the network.



The only positives with this model was the segmentation of the network into the two desired VLANs, but setting up and maintaining that segmentation proved to be more trouble than it was worth. One of the most glaring issues we had with this network was that the router would act as a single point of failure for the network **as a whole**. While the architecture's layout was inspired by security-minded ideas, this implementation of the core idea of segmentation failed. We would need Layer 3 switches (multilayer switches) in order to truly bring this idea to fruition.



This version of the model saw the introduction of multilayer switches, and a small, but major architectural change. To start, one change between this model and the previous one are that

each room hosting devices had a switch between the devices inside the room, and the multilayer switch outside the room. This was so that we could configure port security for each room dynamically, and avoid overwhelming the multilayer switch with too many rules and restrictions in one place. However, our caution had caused more problems than it was worth, and we had ended up scrapping the room-by-room switch implementation after this.

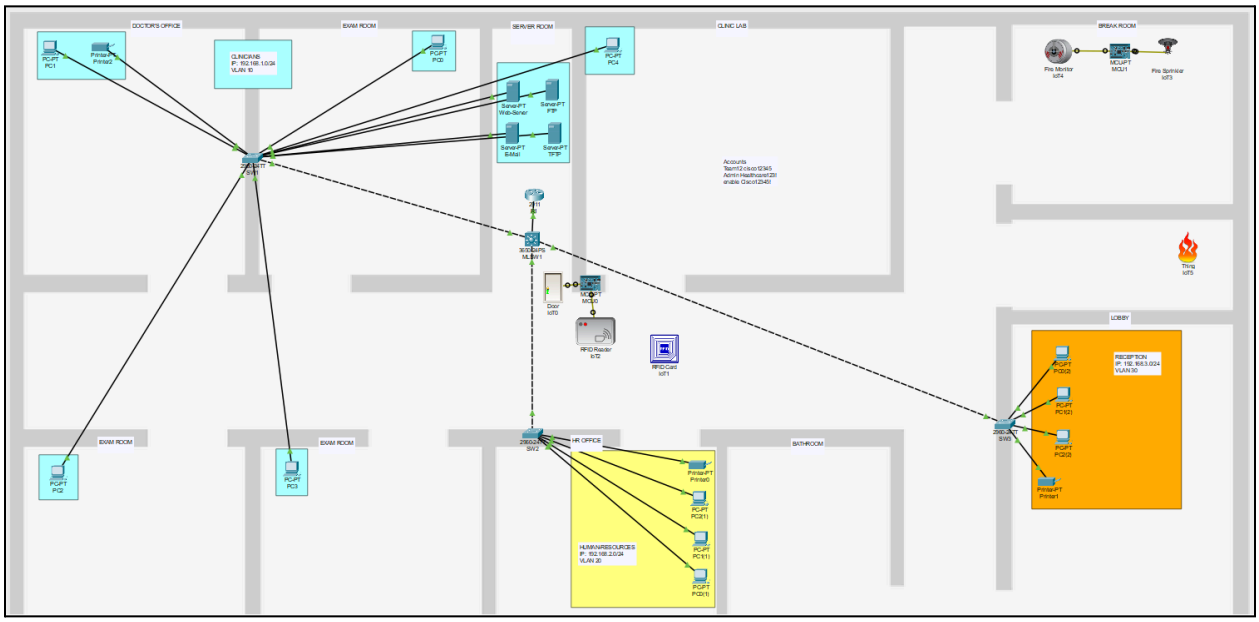
The major yet small change was the replacement of the backbone with multilayer switches, and the introduction of a second (albeit disconnected) router. We experimented with using two routers (one for each VLAN), but eventually decided it was simply too much trouble and added unnecessary complexity to the network. At this point in our process, we realized that we had been a little bit too careful with our designs, and trying to future-proof designs and problems before they were faced was being taken a little to the extreme here. While we did a good amount of experimentation, we had to face the fact that we could be holding ourselves back. After this iteration, we decided to scrap excessive devices and take steps towards centralizing the network in order to increase efficiency and decrease problems with deployment.

One last breakthrough we had before creating our final design was that we had originally largely focused on physical segmentation of the network, via switches, routers, and cables, but we had yet to capitalize on the logical segmentation of the network. While we utilized VLANs, we had created them on separate switches and had not bridged them on a single device, which had long been the cause of many headaches during development. With all these lessons learned, we moved towards our final design

Chapter 5: Development **Author:** Justin Tecson

5.1 Our Solution

As you can see in the image below, our network architecture in Packet Tracer represents our overview of the intended solution we developed for a small healthcare clinic for a doctor, clinician staff, and reception staff departments.



Each department is assigned a different VLAN: the Clinicians department which would in theory consist of doctors, nurses, and clinical technicians as VLAN 10 (blue) with starting IP address of 192.168.1.0 , the Human Resources department as VLAN 20 (yellow) with starting IP address of 192.168.2.0, and lastly the front reception department as VLAN 30 (orange) with starting IP address of 192.168.3.0. With DHCP configured on our main router, these starting IP addresses allocated to each VLAN on the switch will help determine the addresses that will be assigned to each device on the respective VLAN. For example, the first network device

connected on VLAN 20 will have an IP address of 192.168.2.11 and the next device to be connected will automatically be assigned 192.168.2.12 and so on. It starts from ".11" onwards because we configured DHCP pools to have the first ".1-.10 " addresses to be reserved for devices that need static rather than dynamic configuration.

All of these VLANs are configured to communicate with each other through inter-VLAN routing. If communication needs to be restricted, inter-VLAN routing is temporarily disabled. The purpose of VLANs is to segment the network to limit network traffic to their respective departments only and to increase security by compartmentalizing the network.

For our 2911 Router's configuration, we implemented credentials for User Access Verification in order to ensure that only those who are authorized can access and make changes to our networking devices. In the image below, the router prompts the user for a Username and Password.

```
 (Sunset Clinic Authorized access only)
(Warning this is a restricted access network. Unauthorized access is prohibited)

User Access Verification

Username:
Username:
Username: Admin
Password:

R1#show running-config
Building configuration...

Current configuration : 1994 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 10
!
hostname R1
!
!
!
enable secret 5 $1$mERr$qvQ4xEW18PRaHS0uXVe8v.
!
```

The result of the “show running-config” command outputs all current configurations on the router. It can be seen in our configuration that we enforced password lengths as well as password encryption. The next image represents how our passwords (encrypted with a hash) are displayed. This is true for both our Admin account (highest privilege) and Team12 user account (lowest privilege).

```
!
username Admin privilege 15 secret 5 $1$mERr$Eup4LwMH6quteNms4Zrbz/
username Team12 secret 5 $1$mERr$WvpW0n5HghRrqnrwXCUU1.
!
```

By maintaining accounts with access controls for different levels of access as well as data encryption, we safeguard data at rest as well as determine only those with the proper credentials can be using our networking devices. Another security measure implemented for management of the router is the configuration and use of SSH, which is the secure shell protocol. By having SSH configured, an authorized user can on their workstation open up a command line interface and remotely manage the router using the command ‘SSH -l (router’s IP address)’. The user would then be prompted to enter credentials such as the Admin account’s credentials. By using SSH, we ensure that remote management of networking devices is secure, leaving behind such deprecated methods like Telnet (an older remote-in feature succeeded by SSH).

Additional security measures taken would also be on our switches. Like the router, configurations exist where accounts with varying privileges are present on the devices. There are also multiple port interfaces present on any given switch, which allows for networking devices like PCs and other devices to be connected. In order to prevent unauthorized devices from being connected to a switch, we implemented port security.

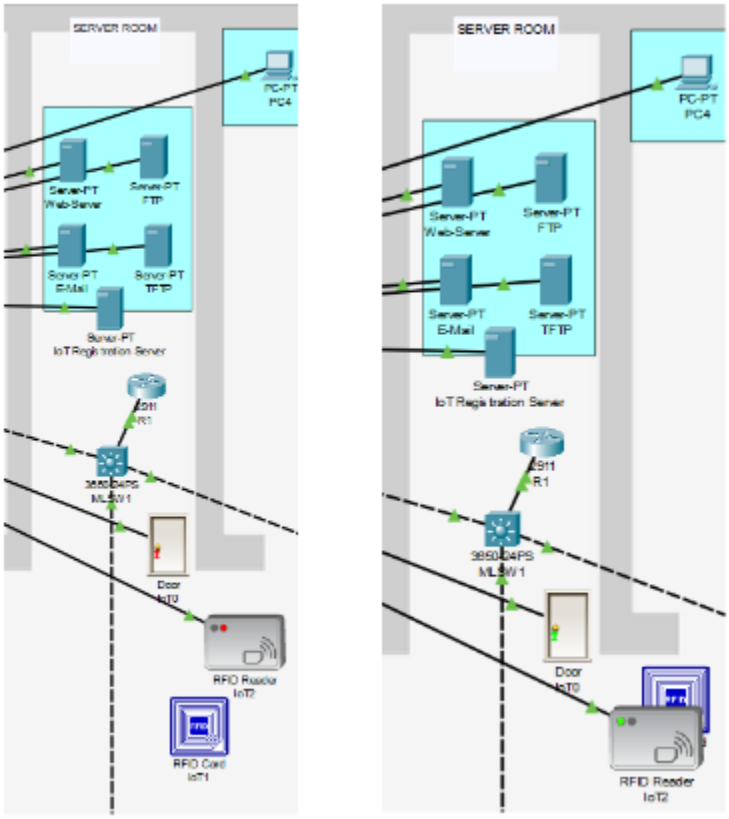
Author: Justin Tecson

```
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 00E0.A3A1.122C
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0001.C918.C7A7
!
interface FastEthernet0/4
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 000C.CF1C.234E
!
interface FastEthernet0/5
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
```

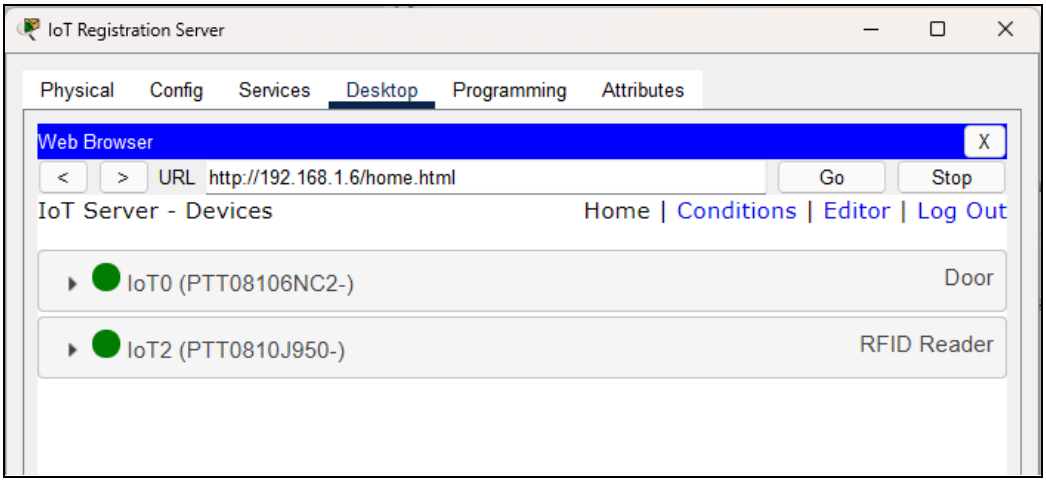
Each port on the switch is labeled as “interface FastEthernet” and is configured with port security. The purpose of configuring port security as “mac-address sticky” is to dynamically record the MAC address of the device it is currently connected to. An example of this is connecting a PC to a switch. The port that the PC is connected to will automatically register the PC’s MAC address as being the only MAC address allowed on that port. Each device has a MAC address, and that can be used as its unique identifier. If another device connects to the port with the incorrect MAC address, the connection is dropped.

Some physical security enhancements we implemented involved the use of an RFID reader to access the server room as well as a fire suppression system. The image below

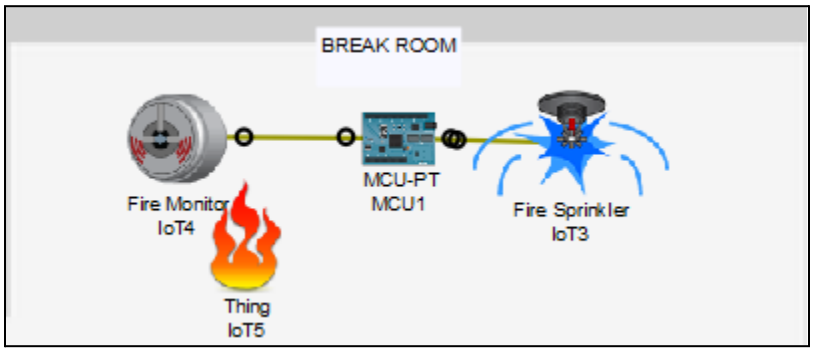
demonstrates how we can use an RFID card to access the server room.



This ensures that only those with the proper credentials can access and manage servers within the room. How this was achieved was using IoT devices in the form of a smart door and the RFID reader itself. Both devices were also registered into the IoT Registration Server for remote management and configuration.

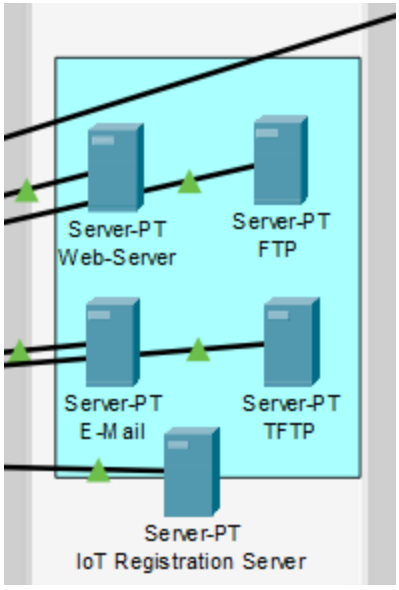


As for the fire suppression system, it is configured using an MCU board. The MCU board is programmed with a python script to ensure that when a fire is detected by the Fire Monitor, the Fire Sprinkler activates.



Beyond security, our solution also utilizes the use of different servers for multiple types of functionality within our network. These servers include an FTP server, TFTP server, Web Server, IoT Server and E-Mail server.

Author: Justin Tecson

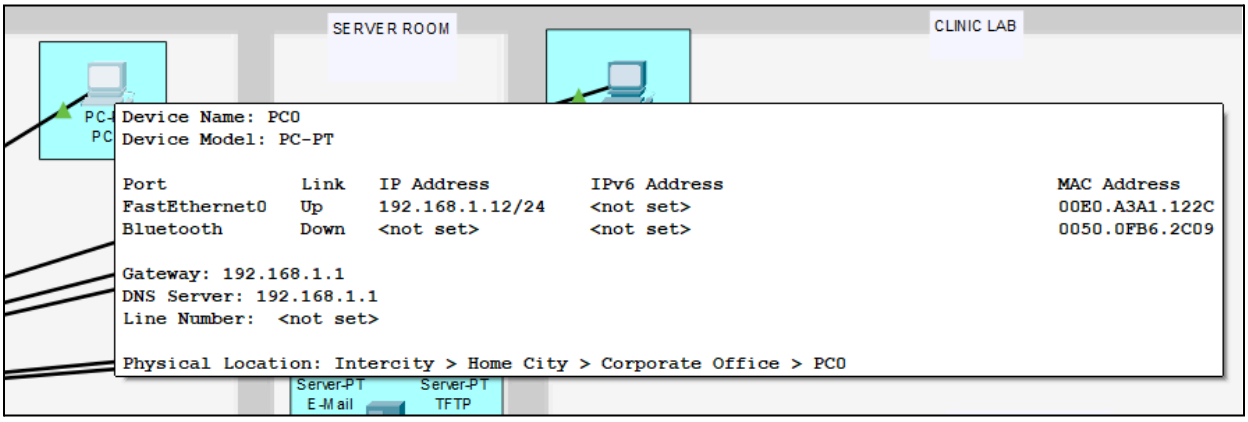


As seen on the image to the left, these are our servers present in the server room. Of course, the Web-Server allows us to host a website in order to interface and interact with clients looking for services. Our E-Mail server allows for users to send email across different rooms such as with the doctor and other nurses. The FTP server governs the File Transfer Protocol, which essentially is how files are delivered throughout the network. A TFTP server also contains a list of configuration files needed to back up or configure new networking devices like routers. The IoT server, which was mentioned before, contains a list of registered IoT devices that can be configured and managed.

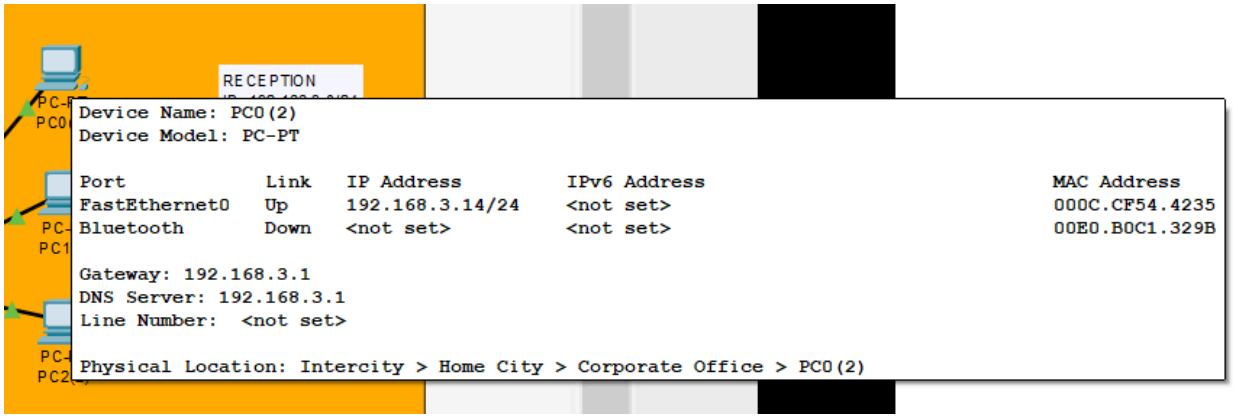
5.2 User Manual

Testing Connectivity

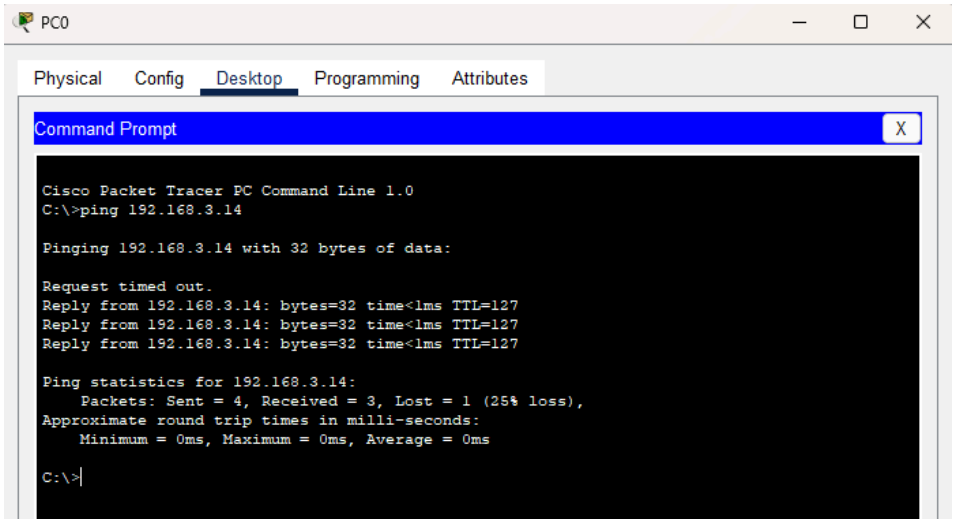
To test connectivity of devices on the network, such as with inter-vlan communication, a user at a workstation needs to utilize the ping command. Let's say a user at PC0 in the Clinicians VLAN wanted to communicate with PC0 in the Receptionist's VLAN.



Author: Justin Tecson



By navigating to PC0 → Desktop → Command Prompt , the user can input commands.

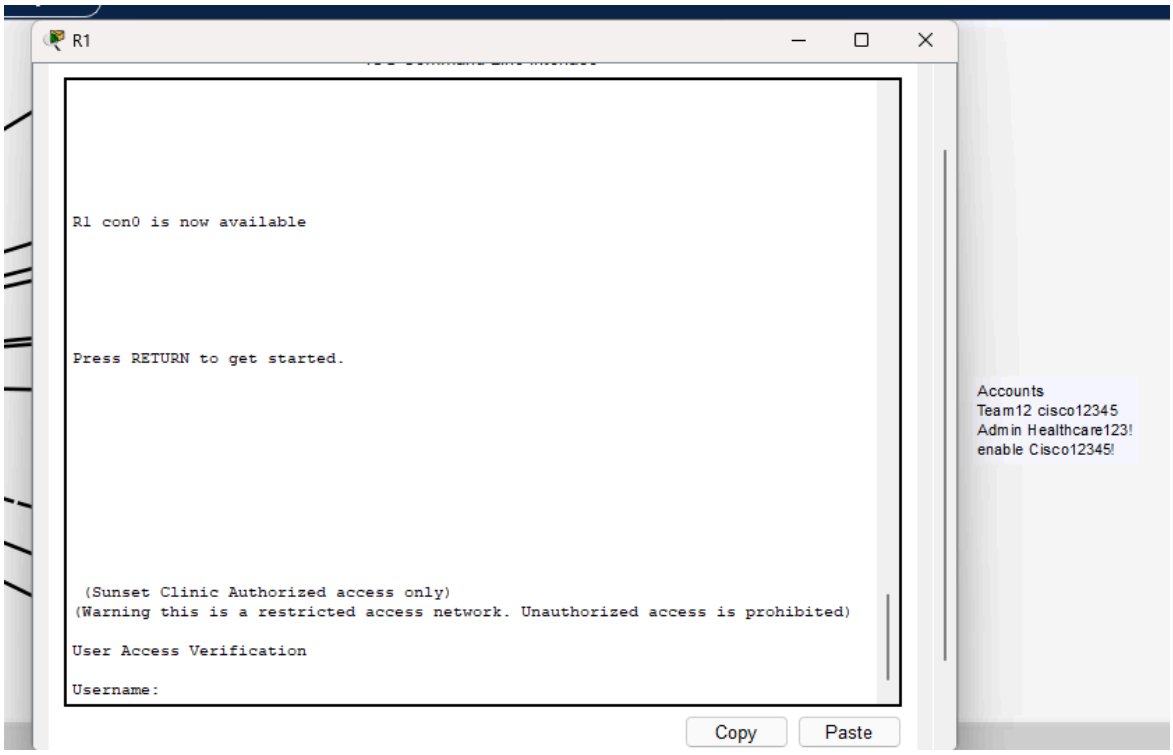


The image on the left demonstrates usage of the ping command. By knowing the IP address of the device you want to communicate with, the ping command can be used as such “ping 192.168.3.14”.

User Accounts

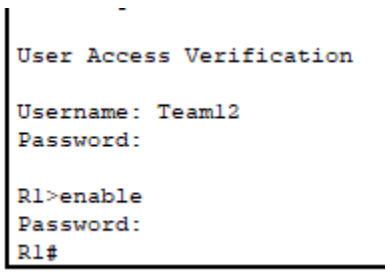
To log into a device for management such as the router, the following needs to be achieved: User Account Verification. There are currently two privilege levels that we have configured, a Team12 account which has the lowest privilege levels and an Admin account that has all privileges. The purpose of the Team12 account is the basic management of switches and routers, with no ability to completely change configuration files present within the device. The Admin account of course has full permissions to make changes to the configuration files. The Team12 account does have

the ability to elevate their privileges using the “enable” command. There is an additional password required to use the “enable” command on the Team12 account.



The image above shows the username login prompt. On the right of the image, we have our account credentials listed out. In order to log in as any account, the credentials are as follows:

- Username: Team12 (least privileged) | Password: cisco12345
- Username: Admin (most privileged) | Password: Healthcare123!
- Enable password (for use once logged into a least privileged account)
    - Cisco12345!

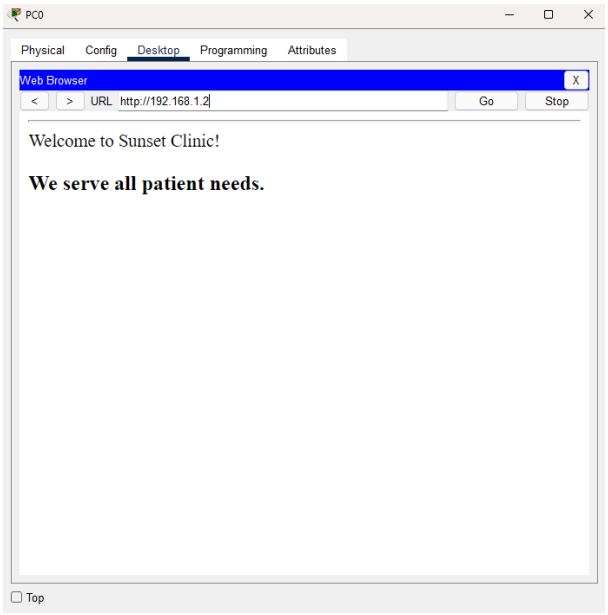


This image demonstrates using the enable command on the Team12 account. Passwords are obviously not visible when entering through the command line.

Author: Justin Tecson

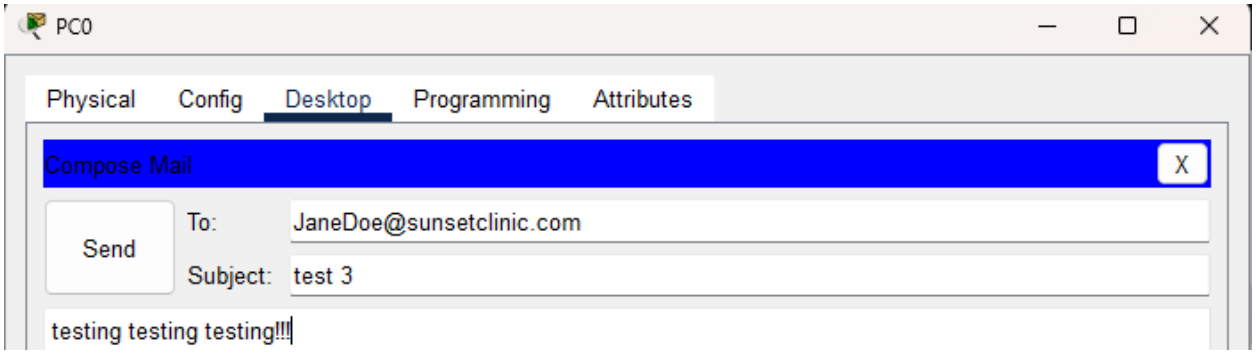
Accessing the Website

To access the website for the healthcare clinic, which we named Sunset Clinic, one would have to navigate onto their workstation or other device then “desktop”, and then “ web browser”. The website’s current IP address is 192.168.1.2, the address for the web server.



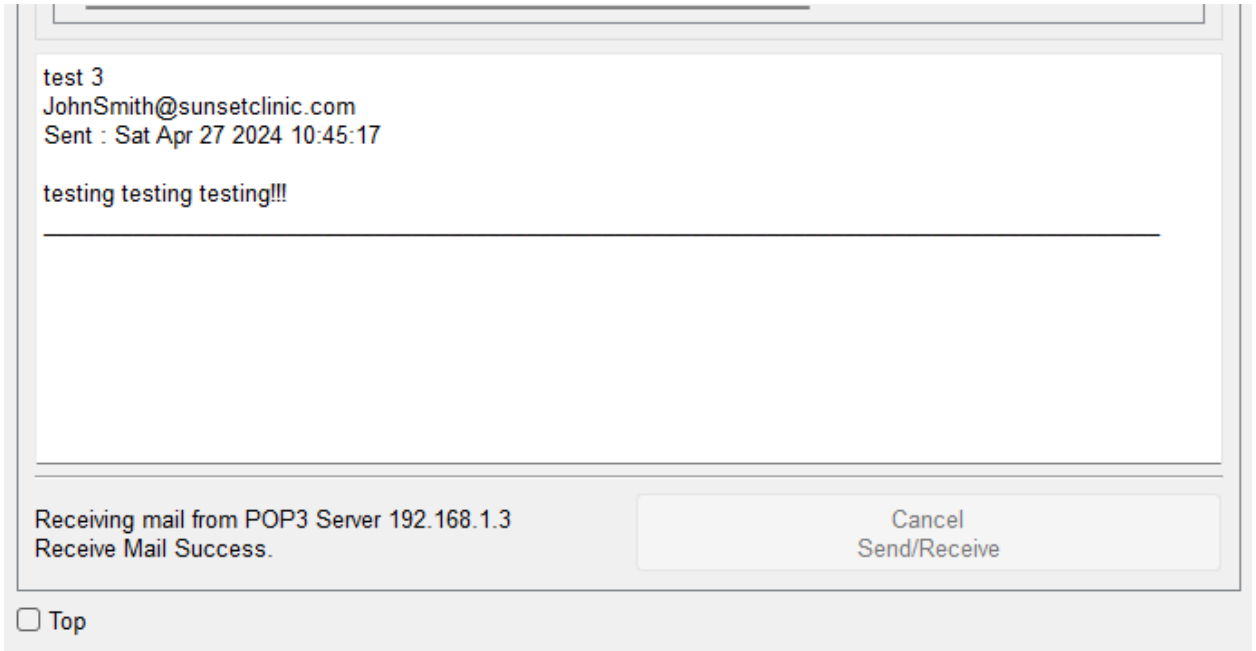
Composing E-Mails

To utilize our E-Mail system, we’ll use PC0 and PC1 as an example. PC0 is logged into the email account JohnSmith@sunsetclinic.com. PC1 is logged into the email account JaneDoe@sunsetclinic.com. PC0 needs to navigate to “Desktop” → “E-Mail”, where the currently logged in user can select “compose” to create an email.



To compose the email, of course all necessary fields must be filled and then the “Send” button is hit. Below is a successful sending of the email.

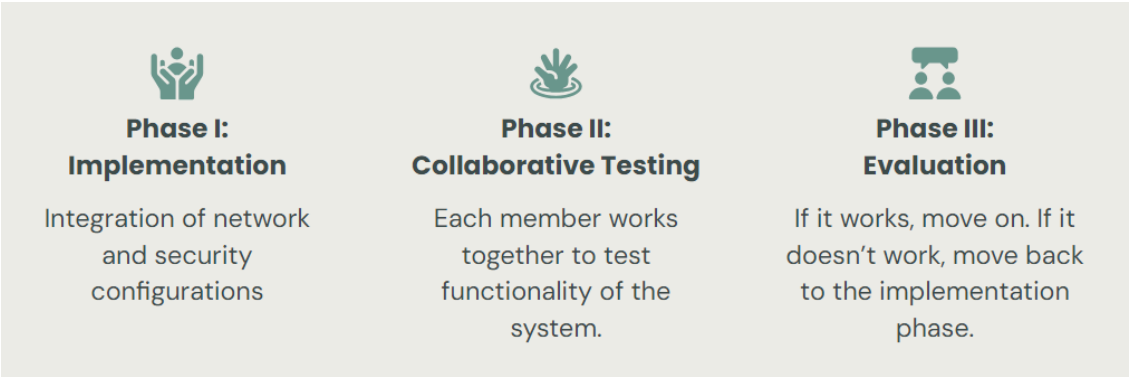
On JaneDoe@sunsetclinic.com’s end, they will see the following email once “Receive” is hit.



Chapter 6: Evaluation and Conclusion **Author: Justin Tecson**

6.1 Solution Testing

To test our solution, our group generally followed this methodology:



Of course, our implementation was the solution outlined in Chapter 5. To test this, we would each individually test every new component added into the network. Based on the functionality, and if it worked, we would move on to test the next component. An example of this would be testing DHCP services. Once the router was configured, each of us added a workstation to the project. If a workstation was able to have an automatically assigned IP address, move on to the next workstation and so on until all workstations were configured in our topology.

6.2 Verification & Validation

To verify our solutions met the requirements of a Healthcare Data Compliant Network, we consulted various resources such as the Centers for Disease Control and Prevention's (CDC) Health Insurance Portability and Accountability Act (HIPAA) guidelines. This is because HIPAA is one of the most prolific healthcare data laws in the United States, and following through with those standards would suffice as a Healthcare Data Compliant Network. "A major goal of the Privacy Rule is to make sure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high-quality healthcare,

and to protect the public's health and well-being"(CDC, 2022). Other resources would include guidelines set forth by compliance firms Algosec, the Compliancy Group, and Kiteworks. By combining knowledge from both official law and third-party compliance group guidelines on how to maintain HIPAA standards, we were able to create a checklist for a Healthcare Data Compliant Network.

Our Verification & Validation Checklist:

1. Creating security solutions to ensure the secure transmission of sensitive patient data
2. Implementing access control rules within the network infrastructure
3. Deploying physical security measures to protect critical infrastructure from environmental hazards or unauthorized access
4. Presenting training material to staff to educate them on best practices for security awareness
5. Disclosure for data breaches if they do happen

In terms of our project, elements such as the use of encryption, switchport security, and other measures against network vulnerabilities fulfilled the first point. For the second point, access controls were fulfilled by the fact that we had privileged accounts with varying access configured on the network devices. Physical security measures were also fulfilled through the implementation of environmental hazard countermeasures like fire suppression systems. The RFID scanner for access into the server room also sufficed to restrict access to the server room only to those who were authorized to maintain the room. This could not be fully realized within packet tracer, but theoretically our training material would be delivered through the FTP server, E-Mail server, and possibly the website. Disclosures would also be conducted via the E-Mail server and the Web Server.

6.3 Team Conclusions

We learned that within network architecture design there needs to be an adequate amount of configurations in order to meet the standards that we need our network to perform at. This is especially true when designing our healthcare network to meet the needs and guidelines set forth by HIPAA law as well as other compliance groups.

Throughout this project, we had to make a few tough decisions with regards to including features. If given the chance to do things differently, we would likely reassess our exclusion of firewalls. The exclusion was due to both time constraints and the inability to properly configure it into our network. This would be a feature that would not be discarded in future iterations of the network architecture. A packet sniffer also could have been implemented, in order to monitor inbound and out of bounds connections, as well as monitor which resources are being used by who on the network. Both a firewall and packet sniffer would have been effective network safeguards when their capabilities are combined.

Instead of relying on our internal network's isolation to provide security, we could have instead connected a portion of the network to an ISP, set up a DMZ between our sensitive data servers and the rest of the internal network, and then configure firewalls to protect our network.

Despite these shortcomings, we were successful in making a secure network. We were able to configure our VLANs to be resistant to VLAN hopping, maintain encryption for data at rest, configure servers to be able to maintain the flow of information within the network, and provide access controls to securely maintain and configure devices to only those who had the proper privileges.

Works Cited

CDC, C. (2022, June 27). *Health Insurance Portability and accountability act of 1996 (HIPAA)*. Centers for Disease Control and Prevention. https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge.

Compliancy Group. (2024, February 13). *The ULTIMATE HIPAA network compliance requirements checklist: Ensuring your architecture is secure*. https://compliancy-group.com/the-ultimate-hipaa-network-compliance-checklist/

Ertl, B. (2024, January 22). *Your complete checklist for achieving HIPAA compliance*. Kiteworks. https://www.kiteworks.com/hipaa-compliance/hipaa-compliance-requirements/#:~:text=To%20meet%20HIPAA%20compliance%20requirements,audit%20logging%2C%20and%20activity%20monitoring.

HIPAA Network Compliance & Security Requirements explained. algosec. (2023, June 21). https://www.algosec.com/resources/hipaa-compliance/

Larsson, D. (2017). *networking-terminology-understand-what-you-say*. Cisco Learning Network. https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKRHEA4/networking-terminology-understand-what-you-say

Cisco packet tracer - networking simulation tool. Networking Academy. (2023, April 23). https://www.netacad.com/courses/packet-tracer