Title

**Final Project**

CIS 3347-1

Submitted to University of Houston

College of Technology

Information and Logistics Technology

by

John Joshua Izuegbu

Cell Phone: *832-232-1592*

April 20, 2020

Instructor: Dr. Ron Viseh

**Table of Contents**

[Introduction 1](#_Toc502167584)

[Topology 1](#_Toc502167585)

[Internet Protocol Addressing 1](#_Toc502167586)

[Network Address Translation (NAT) 3](#_Toc502167587)

[Internet Access 3](#_Toc502167588)

[Network Components 3](#_Toc502167589)

[Network Circuits 4](#_Toc502167590)

[Twisted pair. 4](#_Toc502167591)

[Wireless. 4](#_Toc502167592)

[Fiber optic. 4](#_Toc502167593)

[Communication Components 4](#_Toc502167594)

[Voice over IP. 4](#_Toc502167595)

[Video conferencing. 4](#_Toc502167596)

[Network Operating Systems (NOS) 4](#_Toc502167597)

[Clients. 4](#_Toc502167598)

[Servers. 4](#_Toc502167599)

[Third Party Applications. 4](#_Toc502167600)

[Security 4](#_Toc502167601)

[Audit. 4](#_Toc502167602)

[NAT Proxy Servers. 4](#_Toc502167603)

[Physical Security. 4](#_Toc502167604)

[Security Holes. 5](#_Toc502167605)

[Anti-Virus Software. 5](#_Toc502167606)

[Virtual Private Networks (VPN). 5](#_Toc502167607)

[Encryption Techniques. 5](#_Toc502167608)

[Public Key (PK). 5](#_Toc502167609)

[Certificate Authority. 5](#_Toc502167610)

[Pretty Good Privacy (PGP). 5](#_Toc502167611)

[Secure Sockets Layer (SSL). 5](#_Toc502167612)

[IP Security Protocol (IPSec). 5](#_Toc502167613)

[User Authentication. 5](#_Toc502167614)

[Network Authentication. 5](#_Toc502167615)

[Intrusion Prevention. 5](#_Toc502167616)

[Intrusion Recovery. 5](#_Toc502167617)

[Risk Analysis 5](#_Toc502167618)

[Disaster Recovery Plan 5](#_Toc502167619)

[Unrestricted power supply (UPS) 5](#_Toc502167620)

[Physical Layout 6](#_Toc502167621)

[Data Communication 6](#_Toc502167622)

[Cost Assessment 6](#_Toc502167623)

[Conclusions or Recommendations 6](#_Toc502167624)

[References 7](#_Toc502167625)

[Appendix A: Categories 8](#_Toc502167626)

# Introduction

The Electric Point is a Houston based startup web hosting company with a mission to bring premium features at an affordable cost and offering an array of hosting products to a wide range of customers. Therefore, the new Electric Point facility data communication requirements need to be fulfilled with the latest technologies to compete with established U.S. web hosting companies. These technologies will include 10 Gbps wired fully shielded twisted-pair cable category (CAT) 7, 10 Gbps Cisco backbone switches, high security data center, Cisco ASA firewall, servers with solid-state drive (SSD), latest version of Microsoft and Linux servers operating systems, and many more top enterprise web hosting software and hardware (Cisco, 2020). This proposal depict the different aspects of how this network will be setup and equipped with current technology provided through Cisco technology. Additionally, the design will exhibit the network layout that will be beneficial for the company when trying to solve problems or when planning a new system. The first thing that needs to be considered is the layout of the building and the main distribution facility (MD) location for all the network components and wiring techniques.

**Main Distribution Facility (MDF)**

The distribution of network feedback and traffic over the feedback will go from a few different mediums. From the outside coming in: the connection will be Outside Internet to Cisco Firewall. Then from there it will be Firewall protection or screening going into a Core Network router. After so it will break off into the switch backbone layers, we will set up for the building. From those twenty-four ports switches those mediums will provide network bandwidth to the ports and mediums in every room that has been accounted for. Each backbone switch will lead into an array of floor switches accounted for on every floor this pattern will go up all the way A close up of text on a black background

Description automatically generatedfrom the bottom floor to the top 8th floor.

# Topology

Now for a few diagrams depicting the network topology for the building. Starting on the First-floor lobby and management area. We map out the network design layout of the sever room leading into the supporting rooms adjacent to the wiring room. We were able to map out the wiring overlay and divvied out the respective IP addresses needed for ports and devices, on each respective floor. Here is an excerpt of the designs:

1st Floor Design:

A close up of text on a white background

Description automatically generated

2nd Floor Design:

A picture containing text, map

Description automatically generated

3rd through 8th Floor Designs:

A close up of text on a white background

Description automatically generated

A screenshot of a cell phone

Description automatically generated

A close up of text on a white background

Description automatically generated

# Internet Protocol Addressing

Transmission control protocol/internet protocol (TCP/IP) is one of the most commonly used network worldwide. The reason for its popularity includes certain features and capabilities: (a) TCP/IP performs error checking, (b) it can send large files across even unreliable networks with great assurance that the data will arrive uncorrupted, and (c) TCP/IP is compatible with a variety of data link protocols (FitzGerald et al., 2012). Internet protocol (IP) is the network layer protocol that performs addressing and routing to identify a computer or a device on a TCP/IP network (FitzGerald et al., 2012). Table 1 and table 2 are proposed IP addressing for this new facility (IP Calculator, 2017).

Table 1

*IPv4 Subnet Result for 172.16.0.0*

|  |  |
| --- | --- |
| Network Address | 172.16.0.0 |
| Usable Host IP Range | 172.16.0.1 - 172.16.64.254 |
| Broadcast Address | 172.16.15.255 |
| Total Number of Hosts | 4,096 |
| Number of Usable Hosts | 4.094 |
| Subnet Mask | 255.255.240.0 |
| Binary Subnet Mask | 11111111.11111111.11110000.00000000 |
| IP Class | B |
| CIDR Notation | /20 |
| IP Type | Private |

Table 2

*All Possible /18 Networks for 172.16.x.x*

|  |  |  |
| --- | --- | --- |
| Network Address | Useable Host Range | Broadcast Address |
| 172.16.0.0 | 172.16.0.1 - 172.16.63.254 | 172.16.63.255 |
| 172.16.64.0 | 172.16.64.1 - 172.16.127.254 | 172.16.127.255 |
| 172.16.128.0 | 172.16.128.1 - 172.16.191.254 | 172.16.191.255 |
| 172.16.192.0 | 172.16.192.1 - 172.16.255.254 | 172.16.255.255 |

# Network Address Translation (NAT)

Dynamic Network Address Translation (NAT) and Port Address Translation (PDT) for the building allows for the users in the network to communicate with entities and users outside the network without that much of cost to the client. We will utilize a dynamic nat system that will choose a pool of different ips. “The NAT device will consist of a pool of IP addresses. This time though the pool of IP addresses will be used when needed and then given back to the pool. So if computer A needed a public address, it would take one from the pool, then hand it back when done. The next time the same computer wanted an IP address it may be assigned a different public address from the pool, because the one used previously may be in use by another computer, hence the name "dynamic". So users who want to communicate on the internet at any one time will be limited by how many public IP addresses are available in the NAT pool”. All we need for our client to do is supply a sizeable amount of PUBLIC IP’s for the network to use for the users within the network. Here’s an example of

A close up of a device

Description automatically generated

# Internet Access

For internet access to the network an individual will have to be an approved user on the network to have access to internet privileges. If not, the user will have to use a guest account/Wi-Fi login credentials. We will utilize a from of IP route filtering to allow access to our network and services. If an individual user does not have a proper IP address the network will not allow him to traverse the internet using the client’s credentials.

# Network Components

The network components (Hardware) that will be utilized in the building are as listed in the table below:

Table 3

*Hardware Recommendations*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Hardware | IP | VLAN | Type | Location |
| Routers | 172.16.0.2 – 172.16.0.10 | N/A | Network | MDF |
| Core Switch 1 | 172.16.0.20 | N/A | Network | MDF |
| Core Switch 2 | 172.16.0.31 | N/A | Network | Server Farm |
| Switche1 | 172.16.0.100 | 1 | Network | MDF |
| Firewall | 172.16.0.2 | N/A | Network | MDF |
| Access point 1 | 172.16.0.120 | 40 | Network | Hallway |
| Active Directory 1 | 172.16.0.150 | 1 | Server | MDF |
| Active Directory 2 | 172.16.0.151 | 1 | Server | MDF |
| Web | 172.16.0.152 | 1 | Server | MDF |
| FTP | 172.16.0.15 | 1 | Server | MDF |
| Mail | 172.16.0.17 | 1 | Server | MDF |
| Windows PC(s) | 172.16.13.74–172.16.14.20 | N/A | Network | 1-8 |
| Secure WAP(s) | 172.16.32.100-172.16.34.17 | N/A | Network | 1-8 |
| HP All-In-One Printers | 172.16.0.72-172.16.0.100 | 1 | Network | 1-8 |
| Cisco VoIP Phone | 172.16.64.2 – 172.16.0 |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Network Circuits

We will use different network cabling methods that will run through the building from different in Ethernet (twisted), fiber optic, and wireless connection.

Twisted pair - a type of cabling that is used for telephone communications and most modern Ethernet networks. A pair of wires forms a circuit that can transmit data. Two basic types of twisted-pair cable exist: unshielded twisted pair (UTP) and shielded twisted pair (STP) UTP cable relies solely on the cancellation effect produced by the twisted wire pairs to limit signal degradation caused by electromagnetic interference (EMI) and radio frequency interference (RFI). To further reduce crosstalk between the pairs in UTP cable, the number of twists in the wire pairs varies.

Wireless. *Wireless communication* uses radio frequencies (RF) or infrared (IR) waves to transmit data between devices on a LAN. For wireless LANs, a key component is the wireless hub, or access point, used for signal distribution we will have Wireless Access Points (WAP’s) with varying speeds at 2.5 GHZ and 5 GHZ for the residents, staff, and invited guests.

Fiber optic. Fiber optic cable is completely immune to EMI and RFI. This cable can transmit data over a long distance at the highest speed. It can transmit data up to 40 kilometers at the speed of 100Gbps. Fiber optic uses light to send data. It reflects light from one endpoint to another. Based on how many beams of light are transmitted at a given time, there are two types of fiber optical cable: SMF and MMF. We will use fiber to connect the outside internet connection to the peripherals inside the backbone and core components.

# Communication Components

Voice over IP. Voice over IP (VoIP) defines a way to carry voice calls over an IP network including the digitization and packetization of the voice streams. IP Telephony utilizes the VoIP standards to create a telephony system where higher level features such as advanced call routing, voice mail, contact centers, etc., can be utilized. We will use Cisco VoIP components for the design.

# Network Operating Systems (NOS)

A network operating system is a specialized operating system for a network device such as a router, switch or firewall.

Clients. Students and Teachers will have their own login, to the organizations OS.

Servers. Servers will have a terminal OS that will handle the server functioning for the building and network facility.

Third Party Applications. Will need to be approved by the NAT and other pools for functioning. A dealing with Least Privileges will be used as well.

# Security

Audit. We will utilize Risk Assessments, Vulnerability Assessments, Penetration Test, and a compliance Audit. For safety purpose and security for the network.

NAT Proxy Servers. We will utilize a web proxy to handle HTTP request from users, DNS proxy to help with queries, and a plethora of server proxy from our server farm/room.

Physical Security. Card and Lock access to rooms and desk with privileges given.

Security Holes. Security holes are going to be unregistered users in system, with guest that never been to the facilities.

Anti-Virus Software. Latest ant-virus software from MacAfee or secondary product.

Virtual Private Networks (VPN). Will be used on the network security camera and some other components on the network.

Encryption Techniques. Advanced Encryption Standard is a symmetric encryption algorithm that encrypts fixed blocks of data (of 128 bits) at a time. The keys used to decipher the text can be 128-, 192-, or 256-bit long. The 256-bit key encrypts the data in 14 rounds, the 192-bit key in 12 rounds, and the 128-bit key in 10 rounds. Each round consists of several steps of substitution, transposition, mixing of plaintext, and more.

Public Key (PK). As a public-key encryption scheme, its users encrypt data with the public key of their intended recipient, which can only be decrypted with the recipient’s private key. RSA is slow and uses a lot of computational resources, so it is generally only used to encrypt symmetric keys, which are much more efficient.

Certificate Authority. An [SSL Certificate](https://www.globalsign.com/) is a popular type of Digital Certificate that binds the ownership details of a web server (and website) to cryptographic keys. These keys are used in the [SSL/TLS protocol](https://www.globalsign.com/en/ssl-information-center/what-are-certification-authorities-trust-hierarchies) to activate a secure session between a browser and the web server hosting the SSL Certificate. In order for a browser to trust an SSL Certificate, and establish an SSL/TLS session without security warnings, the SSL Certificate must contain the domain name of website using it, be issued by a trusted CA, and not have expired.

Pretty Good Privacy (PGP). Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. Which we will use for this building.

Secure Sockets Layer (SSL). We will utilize a OV SSL model. The Organization Validation SSL certificate’s primary purpose is to encrypt the user’s sensitive information during transactions. This version of SSL certificate has a high assurance similar to the EV SSL certificate, which is used to validate a business’ creditably.

IP Security Protocol (IPSec). This section starts here…

User Authentication. After entering their username and a password, users have to clear an additional hurdle to login: they need to input a one-time code from a particular physical device.

Intrusion Prevention. IPS might scan the headers of emails to determine whether an email being sent to your company is safe or unsafe. If it detects anything suspicious or risky, it can prevent the email from being delivered to its intended recipient.

# Risk Analysis

This section starts here…

# Disaster Recovery Plan

* Back up network configuration files
* **Create an IT recovery team and assign responsibilities**
* **Assess potential risks and threats**
* **Reconfigure network infrastructure**
* **Regularly test and update the plan**
* **Determine critical network components and the impact of their failure**

# Data Communication

# A close up of a piece of paper Description automatically generatedCost Assessment

This section starts here…

# Conclusions or Recommendations

From this project I learned setting up a network infrastructure of multiple levels. Factoring in safety precautions and hardware capabilities of multiple different product for the build. Some things that should be recommended and taking account for is the different components needed to finish this project. And the sheer understanding of what goes into a network design for a facility. I will also look into different ways of building out a design of this magnitude for a client.

# References

CISCO (2017). Products and Services. Retrieved from https://www.cisco.com/

FitzGerald, J., & Dennis, A., Durcikova, A. (2012). *Business Data Communications and Networking* (11ed.). Hoboken, NJ: Wiley.

Kennedy, S. (2017). *Best Practices for Wireless Network Security.* Retrieved from https://www.computerworld.com/article/2573986/mobile-wireless/best-practices-for-wireless-network-security.html

IP Calculator (2017). *IP Subnet Calculator.* Retrieved from http://www.calculator.net/ip-subnet-calculator.html

NetSpot (2017). *Wi-Fi Site Surveys, Analysis, Troubleshooting*. Retrieved from https://www.netspotapp.com/

Metageek (2017). *Wi-Fi non-overlapping channels*. Retrieved from https://www.metageek.com/training/resources/design-dual-band-wifi.html

CISCO (2017). *Wi-Fi Overlapping Coverage Cells*. Retrieved from https://documentation.meraki.com/MR/WiFi\_Basics\_and\_Best\_Practices/Channel\_Planning\_Best\_Practices

NAT - <http://www.internet-computer-security.com/Firewall/NAT.html>

Wires - <https://www.ciscopress.com/articles/article.asp?p=31276>

Fiber - <https://www.computernetworkingnotes.com/networking-tutorials/network-cable-types-and-specifications.html>

NAT secrurity -<https://www.educba.com/types-of-proxy-servers/>

Encryption - <https://lab.getapp.com/common-encryption-methods/>

Certificates - <https://www.globalsign.com/en/ssl-information-center/what-are-certification-authorities-trust-hierarchies>

SSL - <https://www.liquidweb.com/blog/ssl-certificates/>

# 

# Appendix A: Categories

* Topology
* Internet Access
* Virtual Private Networks (VPN)
* Network Components
  + Router
  + Switches
  + Access points
  + Firewall
  + Workstations
    - Desktops
    - Laptops
  + Servers
    - Active Directory (AD)
    - Domain Name System (DNS)
    - Email Server
    - Database Server
    - File Server
    - Printer Server
    - Web Server
* Network Circuits
  + Twisted pair
  + Wireless
  + Fiber optic
* Communication Components
  + Voice over IP
  + Video conferencing
* Network Operating Systems (NOS)
  + Clients
  + Servers
* Third Party Applications
* Security
* Audit
* Network Address Translation (NAT)
* NAT Proxy Servers
* Physical Security
* Security Holes
* Anti-Virus Software
* Encryption Techniques
* Public Key (PK)
* Certificate Authority
* Pretty Good Privacy (PGP)
* Secure Sockets Layer (SSL)
* IP Security Protocol (IPSec)
* User Authentication
* Network Authentication
* Intrusion Prevention
* Intrusion Recovery
* Risk Analysis
* Disaster Recovery Plan
* Unrestricted power supply (UPS)