Title

**Final Project**

CIS 3347-1

Submitted to University of Houston

College of Technology

Information and Logistics Technology

by

John Smith

Cell Phone: *xxx-xxx-xxxx*

April 25, 2018

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 EZ-Hosting 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 EZ-Hosting 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, 2017). This proposal will break down the different aspects of how the network will be setup and equipped for 21st century 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 (MDF) location for all the network components.

**Main Distribution Facility (MDF)**

This section starts here…

# Topology

This section starts here…

# 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 | 172.16.0.0 - 172.16.63.254 |
| Broadcast Address | 172.16.63.255 |
| Total Number of Hosts | 16,834 |
| Number of Usable Hosts | 16,832 |
| Subnet Mask | 255.255.192.0 |
| Binary Subnet Mask | 11111111.11111111.11000000.00000000 |
| IP Class | B |
| CIDR Notation | /18 |
| 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)

This section starts here…

# Internet Access

This section starts here…

# Network Components

This section starts here…

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 |
| … | … | … | … | … |
| … | … | … | … | … |

# Network Circuits

This section starts here…

Twisted pair. This section starts here…

Wireless. This section starts here…

Fiber optic. This section starts here…

# Communication Components

This section starts here…

Voice over IP. This section starts here…

Video conferencing. This section starts here…

# Network Operating Systems (NOS)

This section starts here…

Clients. This section starts here…

Servers. This section starts here…

Third Party Applications. This section starts here…

# Security

This section starts here…

Audit. This section starts here…

NAT Proxy Servers. This section starts here…

Physical Security. This section starts here…

Security Holes. This section starts here…

Anti-Virus Software. This section starts here…

Virtual Private Networks (VPN). This section starts here…

Encryption Techniques. This section starts here…

Public Key (PK). This section starts here…

Certificate Authority. This section starts here…

Pretty Good Privacy (PGP). This section starts here…

Secure Sockets Layer (SSL). This section starts here…

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

User Authentication. This section starts here…

Network Authentication. This section starts here…

Intrusion Prevention. This section starts here…

Intrusion Recovery. This section starts here…

# Risk Analysis

This section starts here…

# Disaster Recovery Plan

This section starts here…

# Unrestricted power supply (UPS)

This section starts here…

# Physical Layout

This section starts here…

# Data Communication

This section starts here…

# Cost Assessment

This section starts here…

# Conclusions or Recommendations

This section starts here…

# 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

# 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)