Report For Friendly Limited

Contents

[Introduction 1](#_Toc99387414)

[Requirements Gathering Process and The Assumptions 1](#_Toc99387415)

[Network Design 2](#_Toc99387416)

[Topology Diagram 3](#_Toc99387417)

[Discuss security aspects and measures 4](#_Toc99387418)

[Physical Network Security 4](#_Toc99387419)

[Technical Network Security 4](#_Toc99387420)

[Administrative Network Security 4](#_Toc99387421)

[IP Addressing Scheme 6](#_Toc99387422)

[Features 7](#_Toc99387423)

[References 7](#_Toc99387424)

# Introduction

In this report I will design a network for Friendly Limited and also discuss any security measures that the company should consider in order to keep their business safe while also allowing staff and customers to be able to use their network safely.

# Requirements Gathering Process and The Assumptions

This type of network avoids the unauthorized access from guests and should only allow authorized access to staff. All the routers should allow staff to use the same password that they use for the other routers in order to login. This network connects the different departments of the company or many Offices and combines them in a single network. The routers must choose the best route for the packets and make the communication quickly and securely. In the developed scenario adaptive bitrate technology needs to be used as many people will be using their devices for streaming and searching on the internet mainly. A distance vector protocol will be applied in the project and the routers should be password protected for safety purpose.  
Gray castles consist of three floors, Ground floor reserved for IT Facilities workplaces and server rooms. Second and 1/3 floor have six departments, however there’s not enough space for all departments. Company is highly conscious for security so; we have adjusted some departments to the white tower because it doesn’t have enough space.

We can assume that we have to shift two public departments (marketing and finance) from gray fortress to white tower.

The Gray castle building is over 100 meters away therefore copper cable will not be useful so we need to take that into account and change which type of cables will be used.

This setup will require NAT as we will need to translate live IP into local IP.

# Network Design

* Router0 is main router which is connected to ISP as well as white tower (router1) and Gray Castle(router2).
* We use firewall with router0 for the connectivity to the internet.
* Firewall is used to protect org from hackers.
* Router0 placed in gray castle and router1 placed in white tower.
* White tower consists of Four Floors. So, we can use four switches.
* On the ground floor we have installed 3 Wi-Fi Routers in Conference room, cafeteria and show room.
* We have installed three Wi-Fi router because there are three different sections (Conference room, cafeteria and showroom) but if we installed one Wi-Fi router it won’t be efficient.
* On the first, second and third floor we have Lan connectivity from switches to PC’s.
* In local area network when we have connected more than two PC’s so we have used a switch.
* Gray Castle Consist of three floors.
* Ground Floor reserved for It Facilities and servers.
* We can also install IT center on 1st floor or 2nd floor but on the ground floor its temperature is more compatible compared to upper floors. In documents its mentioned that IT facilities and server rooms remain on ground floor.
* Second and third floor consist of different departments, so we have connected through switches which have been installed on the 2nd and 3rd floor.

## Topology Diagram

In this Scenario we have used star topology because we are connecting desktop/workstation directly to the switch.

A screenshot of a computer

Description automatically generated with medium confidence

**Figure 1 – Network Design for Friendly Limited**

* In this architecture we have installed, Switches (Cisco 2960 switches), 3 Router (Cisco 2811 routers) Wireless Routers, WLC, access points, Computer Systems(workstations), Firewalls and servers.
* Switches are connected to servers, routers and computer system with straight through cables. Routers are connected to other routers with cross over cable.
* We can use cross over cables connectivity of same devices, and straight through cables for connectivity of different devices.
* Cross over and straight through cables used because they are easy to install, low noise(coaxial) and better budgeted then other cables(fiber).
* We use three routers because one router is used in white tower second router is used in gray castle, but the third router is used for secure communication and connectivity of the two routers as well as internet. We use Administrator password for login purpose and Firewall is used for security purposes.
* We have used multimode optical fiber from router1 to router0 because its more than 100m.
* We have used multimode fiber because the length of the cables needed is over 100 meters so a standard copper cable would not be viable, also many signals will be carried at the same time so we need a cable that can send multiple packets in the same cable at once.
* In two routers we have used OM5 fiber for standard 50µm micron glass.
* ‘’OM5 fiber, also known as WBMMF (wideband multimode fiber), is the newest type of multimode fiber... at a minimum speed of 28Gbps per channel through the 850-953 nm window.’’ (John, September 2021, FS Community)
* We can use NM-1FE-FX network module in cisco 2811 router for optical communication. In routers/ switches we always use NIC (network interface card) for twisted pair cable connecter, but in fiber cable we use fiber connecters. for conversion of optical signals to electrical signals.

Routing Protocols

In router we use routing protocol RIP for routing and DHCP protocol for assigning Ip addresses, gateways and DNS servers automatically.

NAT (Network Address Translation)

We can use network address translation in router0 for private addresses to public address. (For local area network to public area network).

Recommended Hardware For systems

CPU: core2duo 2.20 GHz

Display resolution: 1280 × 1024

Storage: 500GB RAM: > 4GB

# **Discuss** **security aspects and measures**

**The main Security aspects for company**

### Physical Network Security

‘Physical security controls are designed to prevent unauthorized personnel from gaining physical access to network components’ (Unknown Author, Forcepoint). For this scenario we can keep servers and routers hidden away behind locked rooms with constant CCTV operations to ensure that the safety of the company data is not compromised.

### Technical Network Security

‘Technical security controls protected data that is stored on the network or which is in transit across, into or out of the network’ (Unknown Author, Forcepoint). Data also needs to be kept safe from malicious employees as you never know who wants to harm the company. Therefore, we can install firewalls and IPS (intrusion protection system) in order to prevent unauthorized access.

### Administrative Network Security

‘Administrative security controls consist of security policies and processes that control user behavior, including how users are authenticated, their level of access and how IT staff members implement changes to the infrastructure’ (Unknown Author, Forcepoint). So, we have installed Active Directory (AD) for access of users. This will control what files and data is given to specific users. Preventing low level staff from getting information that only high-level staff should be seeing.

More Security Aspects and measures that should be taken into account:

* Staff should make sure their passwords are strong and unique.

This shouldn’t be hard to be put into place. The staff should make sure their passwords are a good length and have a god combination of unique symbols, punctuation and capital letters.

* Set up a firewall.

To make sure our network is protected, we are installing cisco ASA firewalls. ‘Cisco ASA is a security device that combines firewall, antivirus, intrusion prevention, and virtual private network (VPN) capabilities’ (Rick, October 2021, cxtec, p.1) Antivirus protection.

* Updating is important.

Devices need to be updated and patched regularly. This ensures that the data is kept upto date and secure.

* Secure every portable device.

Laptops and phones have a high rate of being stolen so make sure they’re encrypted with strong passwords to prevent sensitive data being stolen along with your phone.

* Schedule backups.

We can schedule backup data to external hard drives or in the cloud in order to keep your data stored safely.

* Monitor steadily.

Conduct regular audits. Internal audits check the implemented systems and processes.

* **Educate your employees about Data Security**

We can educate our employs how we can prevent/secure data from hackers. Prevention is the best way to keep your Data safe.

In security aspects and measures first, we can install CCTV cameras, then we can install well-known techniques to prevent any physical unauthorized access.

Use different Wi-Fi networks for customers and visitors. Wireless routers we can use are cisco WLC (wireless LAN controller) because it offers central control over network elements, increases network visibility, and greatly simplifies individual component monitoring.

* When a customer connects to the Wi-Fi, they will get a prompt to log in
* If they are not a customer and they are staff then they can sign in with their username and password.
* If not, they can sign in as guest.
* All this traffic will be sent to Anchor WLC through the Mobility Tunnel.

For customers/visitors we have used wireless routers, but company employs we can also use LAN (ethernet) cables.

This method makes sure guests cannot have free roam to do whatever they want on the Wi-Fi and will be limited to just browsing the web and not uploading and downloading to prevent any cyber-attacks.

Having staff sign in with their username will allow the company to monitor if any staff are doing anything malicious.

# IP Addressing Scheme

We are using class C IP addressing scheme. This class of addressing is mostly used in LAN’s.

In ipv4 address we have used class C addressing scheme in this network. Ipv4 address consists of 32 bits in 4 portions. Total 32 bits are divided into network and host portion. Class C network first 24 bits represents network portion, and last 8 bits are representing to the host portion.

== 256

In class C one IP address contains 256 addresses. In which first IP used for network and last IP used for broadcast. So total useable IP address are 254.

Total we have used two IP addresses

192.168.0.0 (contains 254 addresses)

192.168.1.0 (contains 254 addresses)

254+254=508

Total IP addresses 508, so we have need 400 addresses.

So, we use class C addresses as we will have enough addresses for the 400 employees and there will be some spare for any guests that come and go.

So, total we have need 400 but we have accessible for expansion of our company employs.

These addresses are private addresses in ipv4

Class (A) 10.0.0.0 — 10.255.255.255

Class(B)172.16.0.0 — 172.31.255.255

Class(C)192.168.0.0 — 192.168.255.255

We can use any IP address from these classes but we can use class c IP address. When we need more host address, we use class B or Class A addresses.

|  |  |  |
| --- | --- | --- |
| Router’s name | Interfaces | IP Address |
| Router0 | Fa1/0 | 192.168.100.2 |
| Router0 | Fa0/0 | 192.168.102.1 |
| Router0 | Fa0/1 | 192.168.101.1 |
| Router1 | Fa1/0 | 192.168.100.1 |
| Router1 | Fa0/3/0-Fa0/3/3 | 192.168.0.1 |
| Router2 | Fa0/0 | 192.168.101.2 |
| Router2 | Fa0/3/0-Fa0/3/3 | 192.168.1.1 |
| Firewall | Gig1/1 | 192.168.102.2 |

# 

For PCs Ip address assign automatically from DHCP (dynamic host configuration protocol).

# Features

# This is a client-server architecture

# There are 3 routers used for the two sites of the company

# When a request is made by anyone on any system in the network, it is forwarded to a client switch on the network, which then send the data to the router then the server.

# WLC used for Wi-Fi connectivity

# Router acts as a DHCP server to assign Ip’s to the host devices and makes sure the data gets to desired destination.

# References

(John. September, 2021. Multimode Fiber Types: OM1 vs OM2 vs OM3 vs OM4 vs OM5.) <https://community.fs.com/blog/advantages-and-disadvantages-of-multimode-fiber.html>

(Unknown Author. NA. What is Network Security?)

<https://www.forcepoint.com/cyber-edu/network-security#:~:text=Physical%20Network%20Security,is%20essential%20in%20any%20organization>.

(Rick. October 2011. What is Cisco ASA?)

<https://www.cxtec.com/resources/blog/what-is-cisco-asa-security-appliance/>