**Secure Network Services – Final Assessment**

**Student Name:** Eryk Gloginski **(L00157413)**

**Course:** BSc Computing

**Module:** Secure Programming

**Lecturer:** Mark Melling

**Submission Date:** 04/04/2023

## **1. Introduction:**

We have been asked to create a Cisco Packet Tracer network design using the **class B network 172.16.0.0/16** for a company called “**Corona Fightback Solution**” which has a total of **200 staff** **members**. There are 6 departments, and each are named **Medical** **Research**, **Marketing**, **Accounts**, **Technical**, **Managers**, and **Receptionists**. They all have a specific number of staff members that we need to account for.

To make sure of **efficient network management** and to avoid IP address wastage, I will implement **Variable Length Subnet Masking (VLSM)** to segment the network into smaller subnets based on the respectable department sizes. The **Medical Research** department with 140 staff members requires the largest subnet, while **Marketing** with 20 staff members, **Accounts** with 10, **Technical** with 10, **Managers** with 10, and **Receptionists** with 10, require smaller subnets. Each department should also have its own **VLAN** to further divide the network and create logical networks but unfortunately it seems very difficult to do.

In addition to **network segmentation**, all of the staff members need to have **access to the internet** and an **email server**, and each department should have access to its own customized **HTTP WEB server**. To ensure that the network is **secure**, **basic security features** will be **implemented** on the **network**, **based on the practical classes that we have covered**. This will help to protect the network from unauthorized access, data breaches, and other potential security threats.

With this approach, I am confident that I will be able to create a reliable and efficient network for the company “**Corona Fightback Solution**”.

## **2. Network Design:**

The network for the company “**Corona Fightback Solution**” requires us to have roughly **200 hosts**. With servers added such as the **application** servers, **WEB** servers, **DHCP** servers and an **email** server, that number of **200** changes to **223**, which is a significant number of devices to manage.

To make sure that the network can handle the traffic across a **large geographical area**, such as a city, a **Wide Area Network (WAN)** will be implemented. This allows us to connect **departments** that could potentially be located on the **opposite** sides of a city, providing a seamless experience for end users.

To handle this, I’m going to create **subnets** for each **department**. This allows for **better organization** and segmentation of traffic which in turn makes it easier to manage and troubleshoot any problems that may come. It is best to keep in mind that while **designing** this network, we require **redundancy**. If one of the switches on the bigger departments is to go down, it could potentially mean that half of the network would go down. One solution for implementing **redundancy** into the network is to have multiple interconnected switches. By doing this, we basically create a mesh network that allows traffic to be routed through alternative paths if one of the switches fails. This approach does not only improve **availability**, but it also provides **scalability** which allows additional switches to be added to the existing network without disrupting it.

In addition to **redundancy** and **scalability**, the network also requires **security**. I will ensure that the network at least implements **basic security features** such as **passwords** and **password encryption** while using **switches** and **routers**.

## **3. Subnetting:**

We are going to start off by deciding how many subnets for the network do we need. Since there are at least 6 departments, we will need to use **at least 6 subnets**. To **efficiently allocate** IP addresses and prevent the **wastage** of IP addresses for the 6 departments, we will be using **Variable Length Subnet Masking (VLSM)** This technique allows us to create subnets with different sizes, based on the number of devices in a subnet. Additionally, each one of the subnets listed below will have its own VLAN to ensure network traffic is appropriately segmented.

The subnet **#0** needs to support **at least 151 hosts**, so we will borrow **8 bits**, which leaves us with 256 - 2 = **254 hosts**. This will make the network **172.16.0.0** with the **C.I.D.R.** mask 24.

The subnet **#1** needs to support at least 26 hosts, so we will borrow **5 bits**, which leaves us with 32 - 2 = **30 hosts**. This will make the network **172.16.1.0** with the **C.I.D.R.** mask 27.

The remaining subnets **#2**, **#3**, **#4**, and **#5** all need to support **at least 11 to 12 hos**ts, so we will borrow **4 bits per subnet**, which leaves us with 16 - 2 = **14 hosts**. This will make the networks **172.16.1.32**, **172.16.1.48**, **172.16.1.64**, and **172.16.1.80**, each with the **C.I.D.R** mask 28.

The table below shows information about the departments and WANs. If more information is required, please refer to the Excel spreadsheet that was submitted along with this report.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Department** | **Network Address** | **First Usable** | **Last Usable** | **Broadcast** |
| Medical Research | 172.16.0.0/24 | 172.16.0.1/24 | 172.16.0.254/24 | 172.16.0.255/24 |
| Marketing | 172.16.1.0/27 | 172.16.1.1/27 | 172.16.1.30/27 | 172.16.1.31/27 |
| Accounts | 172.16.1.32/28 | 172.16.1.33/28 | 172.16.1.46/28 | 172.16.1.47/28 |
| Technical | 172.16.1.48/28 | 172.16.1.49/28 | 172.16.1.62/28 | 172.16.1.63/28 |
| Managers | 172.16.1.64/28 | 172.16.1.65/28 | 172.16.1.78/28 | 172.16.1.79/28 |
| Receptionists | 172.16.1.80/28 | 172.16.1.81/28 | 172.16.1.94/28 | 172.16.1.95/28 |
| **R1 to R2** | 172.16.1.96/30 | 172.16.1.97/30 | 172.16.1.98/30 | 172.16.1.99/30 |
| **R2 to R3** | 172.16.1.100/30 | 172.16.1.101/30 | 172.16.1.102/30 | 172.16.1.103/30 |
| **R3 to R4** | 172.16.1.104/30 | 172.16.1.105/30 | 172.16.1.106/30 | 172.16.1.107/30 |
| **R4 to R1** | 172.16.1.108/30 | 172.16.1.109/30 | 172.16.1.110/30 | 172.16.1.111/30 |

## **4. VLANs:**

As previously mentioned, each subnet should have their own **VLAN**. **VLAN** stands for **Virtual Local Area Network**. **VLANs** play an important role in **network segmentation**, which is why I wanted to **implement** them in this network. By using VLANs, it is possible to **group network devices** such as **switches** and **routers** together to create virtual networks, that are **isolated** from one another. This allows me to **segment** the network based on **department**, which can help to further **improve the network performance**, **simplify network management,** and **enhance the overall security** of the network.

In this case, I’d like to use **VLANs** to correspond to each of the six departments present for the company “**Corona Fightback Solution**”: **Medical Research**, **Marketing**, **Accounts**, **Technical**, **Managers** and **Receptionists**. Each **VLAN** should be assigned a unique **VLAN ID**, which will allow network administrators to easily identify and manage the traffic flowing from within each network. To ensure **consistency** and **organization**, I will be numbering the **VLANs** from 11 to 66, that use **increments** of 11.

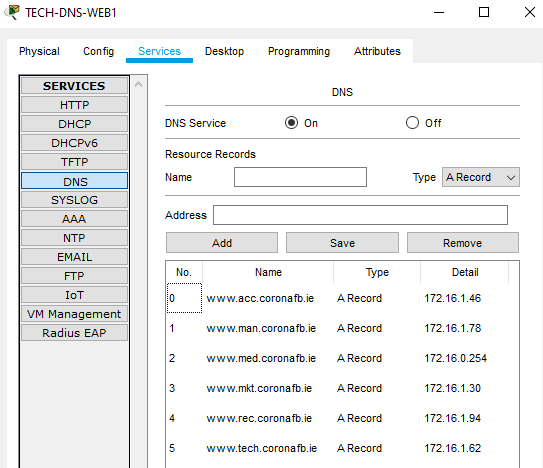
This is a list of the **VLAN IDs**, their **name**, and their **associated IP**:

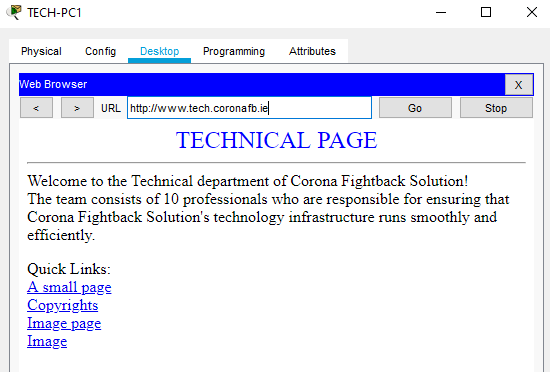
1. **VLAN 11** will be designated for the **Medical Research** Department and will be assigned the IP address of **172.16.0.2**.
2. **VLAN 22** will be designated for the **Marketing** Department and will be assigned the IP address of **172.16.1.2**.
3. **VLAN 33** will be designated for the **Accounts** Department and will be assigned the IP address of **172.16.1.34**.
4. **VLAN 44** will be designated for the **Technical** Department and will be assigned the IP address of **172.16.1.50**.
5. **VLAN 55** will be designated for the **Managers** Department and will be assigned the IP address of **172.16.1.66**.
6. **VLAN 66** will be designated for the **Receptionists** Department and will be assigned the IP address of **172.16.1.82**.

By implementing **VLANs** in the network, we can effectively segregate the traffic in the network, reduce network congestion, and improve overall network security. Unfortunately, I was unable to implement **VLANs** into the final network design due to the fact that there was an error with VLANs not being able to communicate with the other servers and with each other after going through the **default gateway**.

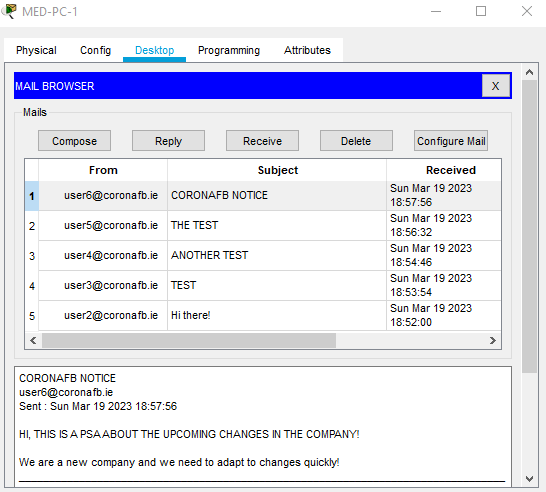
## **5. WEB SERVERS AND DNS:**

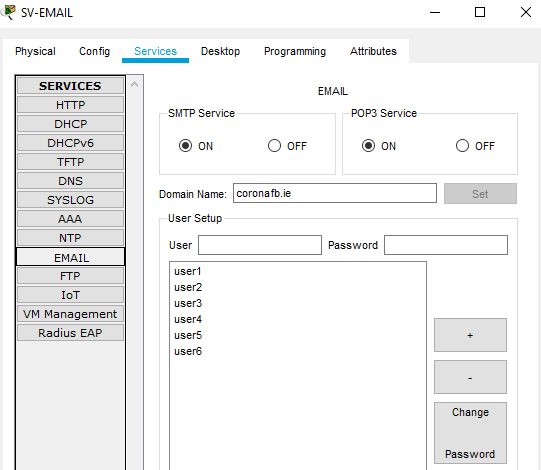
As a part of my network design for the company “**Corona Fightback Solution**”, I have included a **customized** **http web server** for each department in the network. The **web servers** overall are designed to provide each department with their own unique web presence and facilitate communication with the other departments that are in the company.

In order to make the accessing the web servers easier, I have enabled a **Domain Name System (DNS)** on the **TECH-DNS-WEB1** server. This allows users to use **6 different domains** that are currently defined, each that are corresponding to a specific department. By using these domains, users can easily access the web servers of various departments without having to remember the IP address of the **web server**.  


The use of **web servers** also allows for better **collaboration** and **information sharing** between departments. By having a **web server**, each department can easily share information about their projects, research findings and other important updates with other departments in the company. This helps to facilitate a better **communication** and **collaboration**, which ends up leading to **improved** **productivity** and **efficiency** across the organization.  


## **6. EMAIL SERVER:**

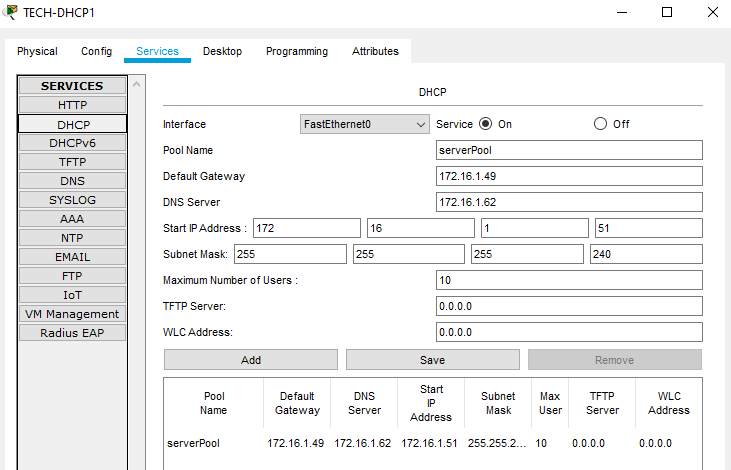
In order to facilitate for better **communications** and **collaboration** among the different departments that are present in the company, an email server would be essential. With a **dedicated email server**, staff members in the company can easily **send and receive** messages, documents, and other important files, regardless of their physical location.  


The **email server** acts as a central hub for all internal and external communication, providing a **secure and reliable** platform for exchanging information. With the ability to set up different **accounts** for each staff member, the email server makes sure that messages are delivered to the intended recipient fast.  


## **7. DHCP:**

**Dynamic Host Configuration Protocol (DHCP)** is a powerful network protocol that simplifies the task of assigning and managing resources on a network. With **DHCP**, network administrators can automatically assign **IP addresses**, **subnet masks**, **default gateways**, and **DNS servers** to devices that join the network.

In **Cisco Packet Tracer**, we can easily configure a DHCP server to automatically assign IP addresses and other configuration details to devices on the network. The beauty of **DHCP** is that it operates on a **client-server model**, where the **client device** sends a request to the **DHCP server** for the **network configuration data** and the server responds with the **required** network configuration data.

I will be using a **DHCP server** on the **technical subnet (or subnet #3)** to assign these resources **dynamically**. The pool name will be kept as the default of **serverPool**, and this server will have a **maximum** of **10 hosts**, starting from **172.16.1.51**. This means that any device connected to the technical subnet will **automatically** **receive** an IP address, subnet mask, default gateway and DNS server information from the **DHCP server**. This greatly **reduces** the **administrative burden** of manually assigning these resources to each **individual** device.  


Additionally, using a **DHCP server** provides more **flexibility** in terms of managing network resources. For example, if the company needs to renumber the network or change the **DNS server**, they can easily update the **DHCP server’s** configuration, and all the devices connected to the network in that specific subnet will **automatically** receive the **new configuration details**.

## **8. OSPF:**

**Open Shortest Path First (OSPF)** is a **routing protocol** used in networks. It is designed to determine the best path for data packets to travel between network devices by **calculating the shortest path** based on various metric such as **bandwidth**, **delay**, and **cost**, making it an efficient and reliable method for routing data.

In the network topology that I have created, **OSPF** can be used to **dynamically** **distribute** **routing** **information** between the routers **R1**, **R2**, **R3** and **R4**. **OSPF** would allow each **router** to **discover** the best path to each network, and to **update** that information in **real time** as changes occur in the network. This would ensure that the **packets** are always **routed** along the most **efficient** path and would also provide **redundancy** if one of the **connected** routers supposedly fails.

## **9. PORTFAST:**

In order to improve the speed of **forwarding physical ports** for **end devices**, **PortFast** is going to be used. **PortFast** is a feature in **Spanning Tree Protocol(STP)** that minimizes the amount of time it takes for a port to **transition** from the **blocking state** to the **forwarding state**. By **default**, when a **switch port** is first **enabled** or when a **link state** is **changed**, the port goes through a lot of steps before it reaches the **forwarding state**. In some cases, when a **switch port** is connected to an **end point** device like a **computer** or a server, the delay caused by STP can be problematic. This is where **PortFast** comes in, as it allows the **port** to **instantly** **transition** into the **forwarding state**, without going through the **STP process**.

In the scenario of this network design for “**Corona Fightback Solution**”, **PortFast** is going to be used on the **ports** connected to **end points** such as the **PCs** and **Servers** as they are not expected to be part of a **loop in the network**. This can **improve network performance** by reducing the time it takes for a device to connect to the network and start communicating. It is **important** to note that **PortFast** shouldn’t be used on ports that are connected to **switches** or **routers**, as it could lead to **loops** in the network. These **loops** refer to a **situation** where a **packet** is **forwarded continuously** between two or more **network devices** in a circular path, leading to **network congestion or failure**.

## **10. VTP:**

In order to improve the **management** of the **VLANs**, I had planned to use **VLAN Trunking Protocol (VTP)**. **VTP** is a protocol that allows switches to **share** their **VLAN configurations** with **other switches** on the same network. By enabling **VTP** on a switch, it can be assigned as the **VTP server** and it can be given a **VTP domain** name, such as “**coronafb**”. The **VTP server** is responsible for maintaining the **VLAN database**. Other switches on the network can be assigned as **VTP clients** to receive the **configuration** **updates** from the **VTP server**. However, due to the **limitations** with the **software** that we are using for the assignment (**Cisco Packet Tracer**), I am unable to implement **VTP** for the entire network as intended in the original plan.

Initially in the network design, I had planned to configure all switches, with one switch acting as the **VTP** **server** and the other switches as **VTP clients**. However, I discovered that **VTP** implementation in **Cisco Packet Tracer** had a limitation regarding the **hop** **counts** of **VTP**. Regardless of Version 1 or 2 of **VTP**, I could only get it to **hop one time** onto the next switch. Just to clarify, Version 3 of **VTP** cannot be used in **Cisco Packet Tracer**. This means that the **VTP updates** can only be sent to **directly connected switches** and **cannot propagate beyond** them. As a result of this, I had to **abandon** the use of **VTP** in a **major part** of the network design and find an alternative solution for this, which was the use of **WANs**.

Despite this **setback**, the network design will still utilize **VLANs** to **segment** the network into multiple logical networks. Although I am not able to use **VTP** in a major part of the network design, I can still potentially **utilize** it in the **Marketing** department at the very least as it only has 2 switches. This was another method or **protocol** that I wanted to **implement**. Unfortunately, I was unable to implement VTP due to me not being able to get the VLANs to work as I wanted them to.

## **11. BASIC SECURITY:**

In order to ensure that the basic **security measures** are in place, **several commands** have been **applied** to the **switches and routers** in the entire network. These **basic security features** will help to **prevent** **unauthorized access** to the network devices, ensuring the **security and integrity** of the network.

Firstly, the **enable password** is set to “**cisco**” and the **enable secret** is set to “**class**”. Additionally, the **service password-encryption** command has been used to **encrypt all the plain-text passwords**, which prevents **unauthorized** access to sensitive information. To ensure that the authorized users are aware of which switch or router they are currently connected to or attempting to connect to, a banner message has been configured using the banned **motd command**, which displays a **message** that looks like “**Corona Fightback Solution Router/Switch <INSERT NAME HERE>**”.

Furthermore, the **password protection** has been used for the **console and virtual terminal** **(VTY) lines**. The **password** for the **console line** has also been set to “**cisco**” and access to the line is **restricted** to **authenticated** users only through the **login command**. Similarly, the **line vty 0 4 command** has been used to configure the password “**cisco**” for the virtual terminal lines and the **login command** has been enabled to ensure that only authenticated users can access the device remotely.