In this Word document file, it conveys, articulates, and explains commodities of Cisco Packet tracer and the reasoning behind each step I had taken. I decided to create a small university campus network on MacOS using Cisco Packet Tracer software.

All usernames will use Clinton, and password as Computerscientist. The small University networks IP addresses are:

IT Services Network – 192.168.0.0/24

Administration Network – 192.168.1.0/24

Accounts Network – 192.168.2.0/24

Lecturer Network – 192.168.3.0/24

Student Network – 192.168.4.0/24

The email and web server will be configured in the IT Services switch to ensure that these services are centrally located and easily accessible to all networks within the campus. Additionally, this helps to minimize network traffic and provides a more efficient use of resources. The IT Services switch will also be configured with VLANs to separate different services and to ensure the security of the network.

Each switch will be given a name to convey each network they are of. For instance, ITServices switch named after ITServices network.

Copper Cable wiring:

I used copper cables to connect the various devices in the network, including PCs and switches. The copper cables were used to establish connections between devices that operated at different layers of the OSI model.

For instance, I connected each PC to the switch using fast Ethernet ports and copper cables. This helped to ensure a reliable and stable connection between the devices. The use of copper cables is a common practice in networking as it provides a cost-effective and efficient means of transmitting data between devices.

Overall, the use of copper cables helped to establish a robust and reliable network infrastructure that facilitated seamless communication between the various devices on the network.

Graphical user interface, application

Description automatically generated

In order to secure access to the command line interface (CLI) and console port, I implemented encrypted and plain text passwords. I achieved this by configuring a local username and password for each switch and enabling login for the local user. Additionally, I configured messages for users logging into the switch to inform unauthorised users that access is prohibited.

To begin, I created a basic switch configuration for each switch by assigning a name to them using the hostname command from global configuration mode. This is accessed by typing "config t" or "configure terminal".

Next, I configured an encrypted password to secure access to privileged mode using the command "enable secret password" in privileged exec mode ("en"). This encrypts the password and ensures that unauthorised users cannot access privileged mode.

For further security, I also encrypted all password information for each switch in the router using the command "service password-encryption". This encrypts the passwords in the configuration file and ensures that they cannot be easily accessed or read.

Overall, these measures helped to secure access to the CLI and console port, as well as prevent unauthorised access to privileged mode and password information.

Graphical user interface, application

Description automatically generated

Graphical user interface, application, Word

Description automatically generated

Securing access to the control line involved configuring the access to the virtual terminal lines (vty) for remote access to the switch. Configuring a password for Telnet access to the switch through the line vty configuration mode.

To secure access to the vty lines, an encrypted password is configured using the command "line vty 0 15" to access the vty configuration mode, followed by the command "password Computerscientist". This ensures that only authorised users with the correct password can access the switch remotely.

In addition to configuring a password, a message of the day (MOTD) banner is also configured for users logging in remotely to the switch via Telnet. This banner serves as a warning message to unauthorised users: “AUTHORISED ACCESS BY CLINTON ONLY” is displayed to users attempting to gain access to the switch remotely. The MOTD banner is configured using the "banner motd" command.

Finally, after configuring all the necessary security settings, the configuration files are saved to the non-volatile memory (NVRAM) using the "copy running-config startup-config" command. This ensures that all the configurations are saved and not lost in case of a power failure or other issues.

Command line Login local for security reasons was used because need two pieces of information are needed to gain access which is username and password. The output can be conveyed below: 

To configure the initial settings on the network, I started by securing access to the command line interface and console ports using encrypted and plain text passwords. This is done to restrict unauthorised access to the switches and routers in the network.

To configure messages for users logging into the switch and banners for authorised access only, I used the motd (message of the day) command. This command allows you to display a message to users when they log in to the device, which can be used to provide important information or warnings.

To secure access to privileged mode, I used the "enable secret" command followed by the desired password. This encrypts the password and provides an additional layer of security.

To secure access to the console line, I accessed the configuration mode and used the "line console" command followed by the desired password. This ensures that only authorised personnel can access the console port.

Finally, I encrypted the enable and console passwords using the "service password-encryption" command, which ensures that the passwords are not visible in plain text.

Again, after completing the configuration, I saved the configuration files to non-volatile random access memory (NVRAM) using the "copy running-config startup-config" command once more. As before, this ensures that the configuration changes are not lost if the device is restarted.

For security reasons, additional measures, such as access control lists (ACLs), firewalls, and intrusion detection systems (IDSs), will also be implemented to provide comprehensive network security.

After entering global configuration mode, I used the command "config t" and configured the IP address of the router to 192.168.0.1 with a subnet mask of 255.255.255.0. Then, I entered the interface configuration mode for gigabitethernet1/0 using the command "int g1/0" and added the IP address 192.168.3.1 with a subnet mask of 255.255.255.0, which granted me access into the port in the router. To ensure connectivity, I entered the "no shutdown" command.

To avoid connectivity issues, I also configured the IP address for each switch by accessing the local interface configuration mode and entering the IP address and subnet mask using the command "ip address." Lastly, to prevent data loss, I saved the configuration files to nvram by entering the command "copy run start."

Cisco switches by default forward ethernet configuration without any additional configuration. I assigned an IP address to each switch; configuring it under a local interface.

Ip address for switches is configured under a local interface.

After assigning IP addresses to the switches, I entered the VLAN 1 configuration mode using the "interface vlan" global configuration command. This allowed me to configure virtual LAN interfaces for the switches.

Once in VLAN 1 configuration mode, I added the IP address and subnet mask using the "ip address" and "subnet mask" commands respectively. This allowed me to specify the network address and subnet mask for each switch.

After configuring the VLAN interfaces and IP addresses for the switches, I was able to remotely manage and monitor the switches using network management protocols such as Simple Network Management Protocol (SNMP), Telnet, or Secure Shell (SSH).

By assigning IP addresses to the switches, I was able to perform switch management tasks such as configuring switch ports, VLANs, and Quality of Service (QoS) policies. This also enabled me to remotely monitor switch performance and troubleshoot network issues as they arise. This is conveyed in the below capture in Realtime.

Graphical user interface, text, application, Word

Description automatically generated

Below is the whole Network that I computed.

Graphical user interface, diagram, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Below shows how I configured the web servers. Graphical user interface, application

Description automatically generated

Below shows how I configured the email for each PC of my Network.

Graphical user interface

Description automatically generated

Then, to ensure that the network was functioning properly, network diagnostics were performed. This involved sending data packets from a PC to different devices on the network and then receiving data packets back. This process confirmed that the devices on the network were properly connected and were able to communicate with one another.

In addition to this, a ping test was performed to determine the reliability and general speed of the connection. The ping test measures the time it takes for a data packet to travel from the source (in this case, the PC) to the destination (the network device) and back again. The results of the ping test showed that the PC was indeed connected to the network and also displayed the latency, or the time it took for the data packet to travel to and from the destination.

By performing these tests, we were able to ensure that the network was functioning properly and that data could be transmitted effectively between devices. This allowed us to identify any potential issues and troubleshoot them in a timely manner.