NCCD Coursework 2

SAFEBI Ltd. Network Design

5551408 – Hedley Benaiges

Contents

Network Design

The diagram seen in *Figure 1* shows a rough plan for the network which will be created. With each floor of the building being connected by a separate router and switch, which will connect to each department. The use of the switch will help when it comes to physically implementing or managing the network.

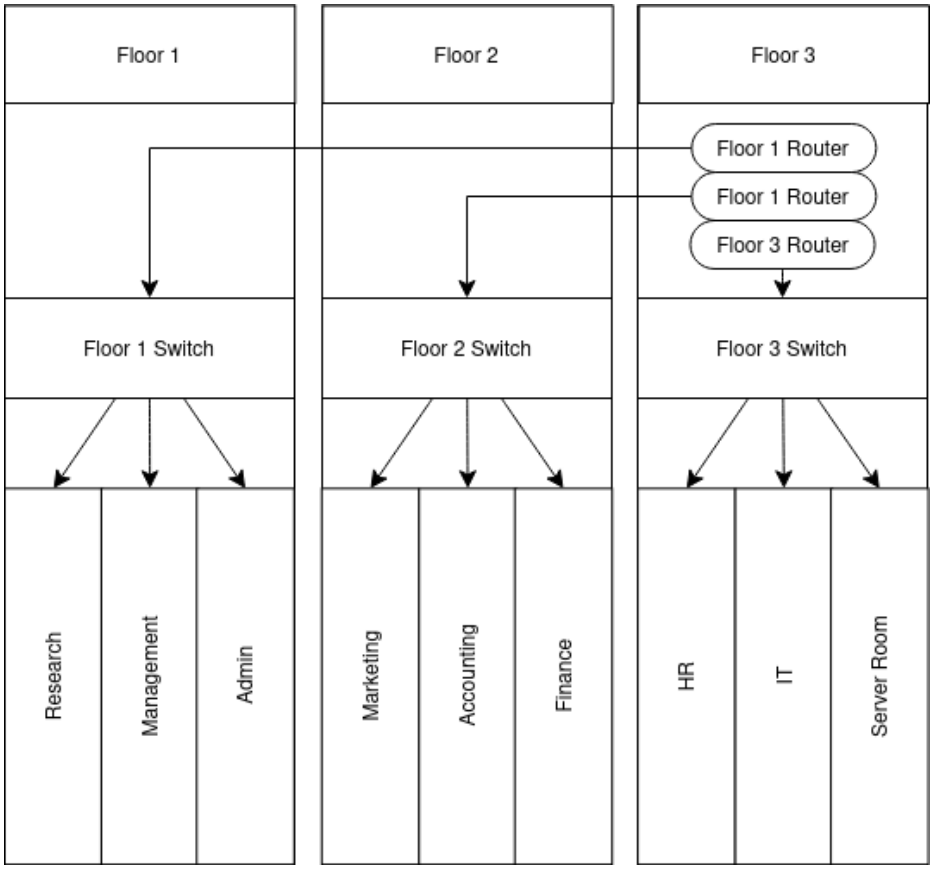

Figure 1: A rough design for the network.

Topology

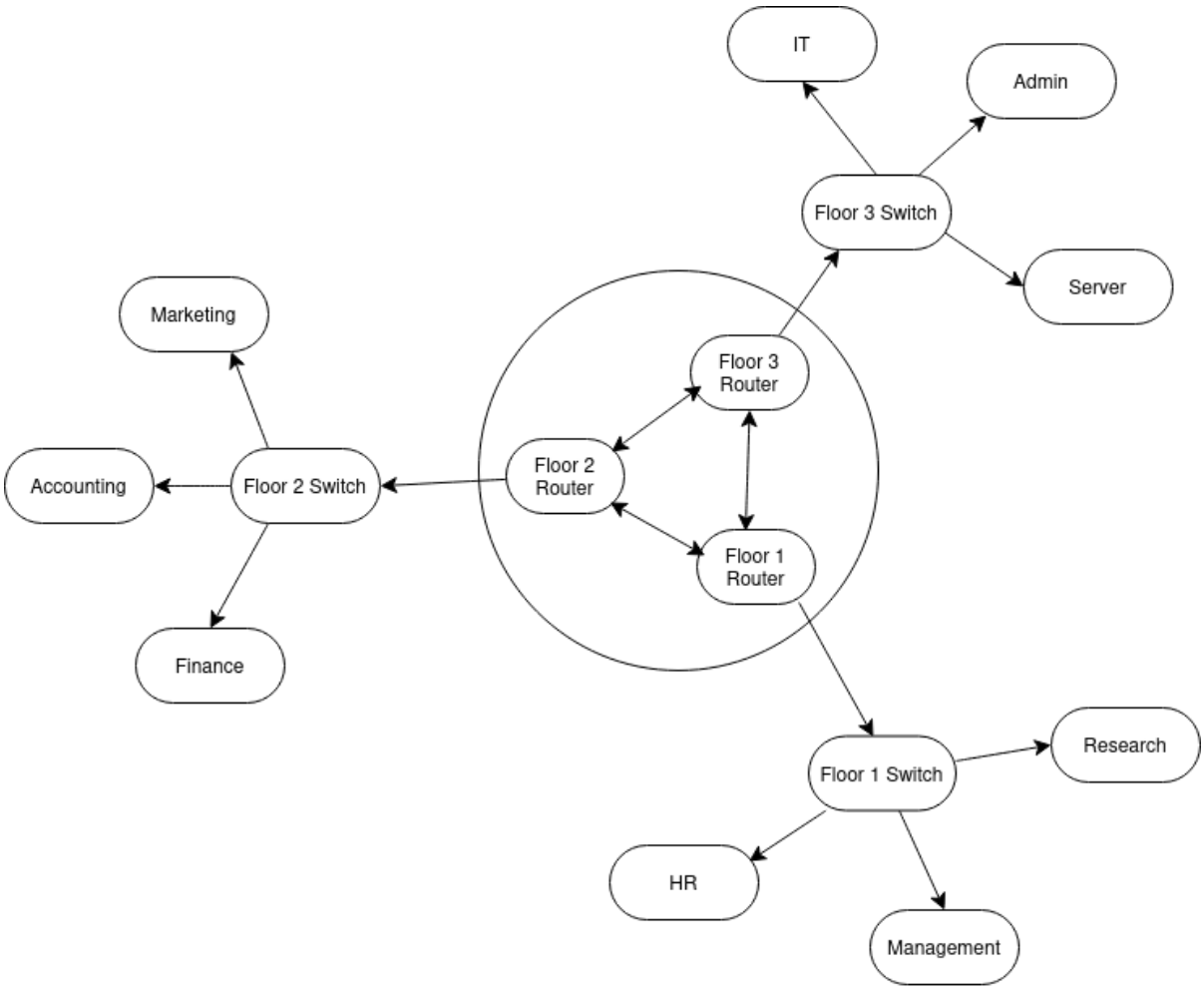

Figure 2: A Diagram of the Holistic Topology

The network (as seen in *Figure 2*) has been configured using an extended star topology, which uses a ring of routers in the middle. An extended star topology is ideal in this scenario, it combines good performance (due to low collision rates) with robustness (any failure excluding the central router will not affect the entire network). The main drawback of a star topology is the single point of failure in the middle. This, however, has been remediated by using a ring of routers in the middle. Here, if a connection between routers fails, the network will function as intended, and if a router fails, the other two floors should function with no issues.

IP Addressing Scheme

The departments are assigned IP addresses using variable-length subnetting (VLSM). VLSM is used to segment the address range 192.168.10.0/24 in a way that best fits the size of each department, while keeping the number of unused hosts to a minimum. *Figure 3 shows how these IP addresses were split up and assigned to each department*

Floor	Departments	No. Hosts	Nearest 2^x	Network Address	Broadcast Address	Subnet Mask
1	Research	30	32	192.168.10.0	192.168.10.31	/27
	Management	20	32	192.168.10.32	192.168.10.63	/27

3	Admin	20	32	192.168.10.64	192.168.10.95	/27
2	Marketing	20	32	192.168.10.96	192.168.10.127	/27
	Accounting	20	32	192.168.10.128	192.168.10.159	/27
	Finance	20	32	192.168.10.160	192.168.10.191	/27
1	HR	10	16	192.168.10.192	192.168.10.207	/28
3	IT	10	16	192.168.10.208	192.168.10.223	/28
	Server Room	5	8	192.168.10.224	192.168.10.231	/29
1 – 2	Routers	2	4	192.168.10.232	192.168.10.235	/30
2 – 3		2	4	192.168.10.236	192.168.10.239	/30
1 – 3		2	4	192.168.10.240	192.168.10.243	/30

Figure 3: The IP Addressing Scheme given to each department (sorted by Network Address)

VLANs

As well as subnets, VLANS are used to segment each department in the network. This helps to separate and control the traffic in the network.

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig0/1, Gig0/2
11   Research                         active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24
1002 fddi-default                     active
```

Figure 4: The VLAN for the Research department on the 'Research Switch'

Note how in *Figure 4,* Fa0/1 does not show up on the VLAN table, this is because it is being used for trunking.

Implementation and Device Configuration

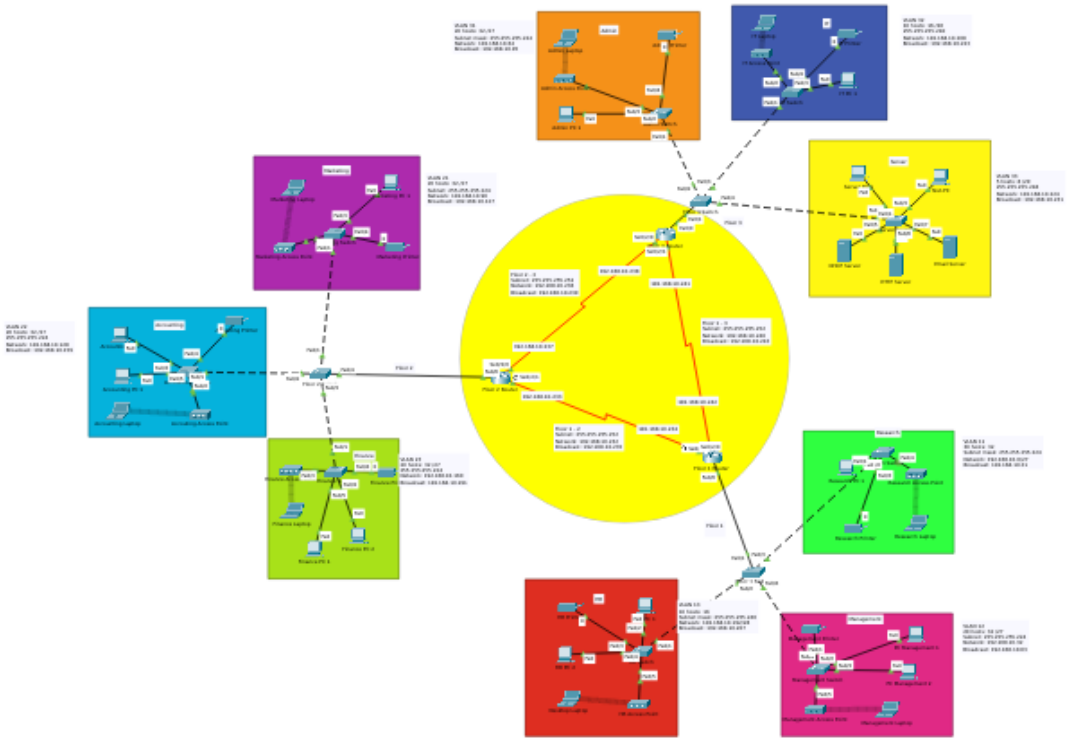

Figure 5: The network implemented in Cisco Packet Tracer

Wireless Access Points

A Wireless Access Point (WAP) can be found in almost every department in the building. With the only exception being the server room, where devices must be physically connected to the network. The server room should be a physically secure and access-controlled environment, however, a WAP could allow for a device to connect from outside the server room which may pose as a security risk. For this reason, the WAP has been omitted from the server room.

Despite this, every other department in the network has a functioning WAP. Allowing employees to bring their own devices such as laptops and phones, and seamlessly connect them to the network. Each wireless access point has WPA2-PSK security, with a password of 'SAFEBIaccess1'

The following images (*Figures: 6, 7, 8*) show a laptop connecting wirelessly to the network and pinging a PC in a different department.

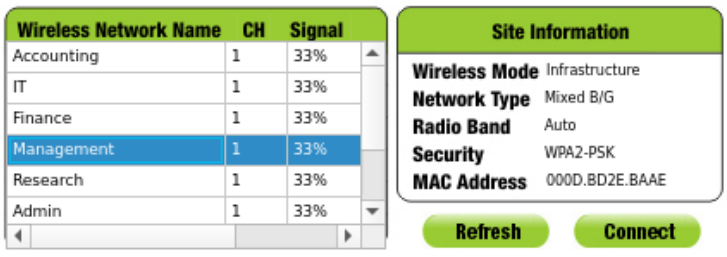

Figure 6: The Wireless Access Points from a Laptop

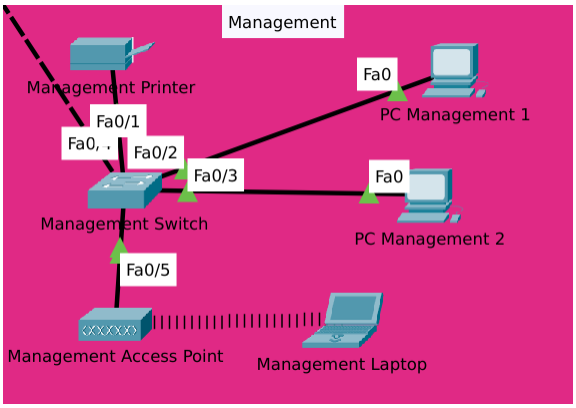

Figure 7: A Laptop connecting Wirelessly

Fire	Last Status	Source	Destination	Type
	Successful	Management Laptop	Marketing PC 1	ICMP

Figure 8: A Successful Ping from a Wirelessly Connected Laptop

SSH

All the routers have been configured with SSH, which will allow a PC to connect remotely to configure settings. It is useful for network administrators to access, configure, and troubleshoot routers from any device in the network.

Using the PC named 'TestPC' in the server room, we can test SSH on the routers. As seen in Figure 9, we can successfully login to the router using the username 'SAFEBIuser1' and the password 'SAFEBIpass1'. To go any further, the password 'SAFEBIenable1' is needed.

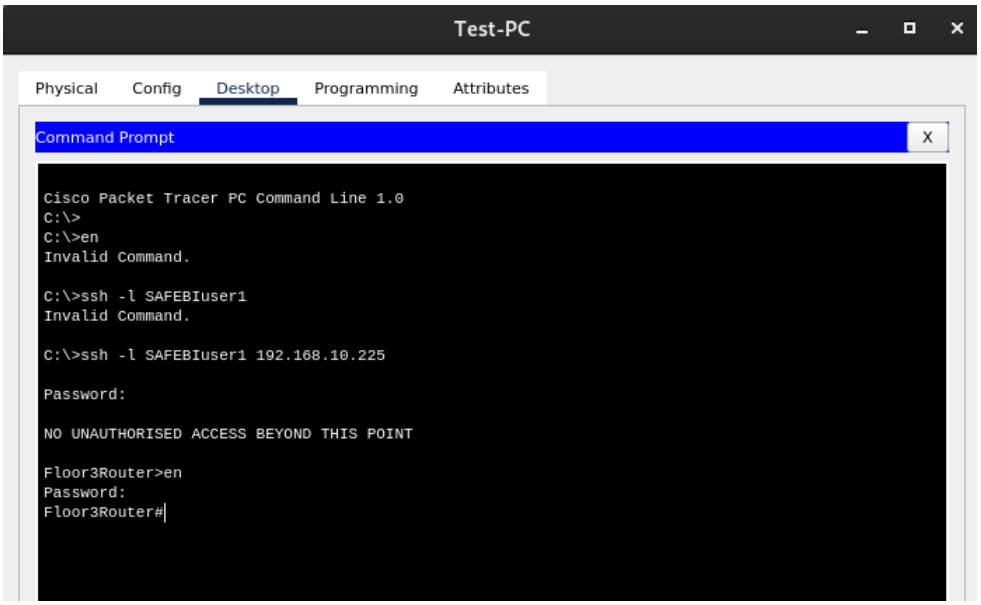

Figure 9: Accessing 'Floor 3 Router' from 'TestPC' using SSH

Servers

The network also contains 3 physical servers. These manage DHCP, Email, and a HTTP site (with a DNS running on the same device). All the servers use static IP addresses, this is to ensure DHCP does not lease out the server addresses to other devices, which could potentially make the servers unreachable in the network.

HTTP (and DNS) Server

A HTTP server has also been set up. When connected to, this will bring up a small web page (*see Figure 1*) which anyone on the network can access. In conjunction with this, DNS is running on the same machine, which has an entry to change the domain of 'safebi.local' to the IP address '192.168.10.227' (This can also be seen in *Figure 10*).

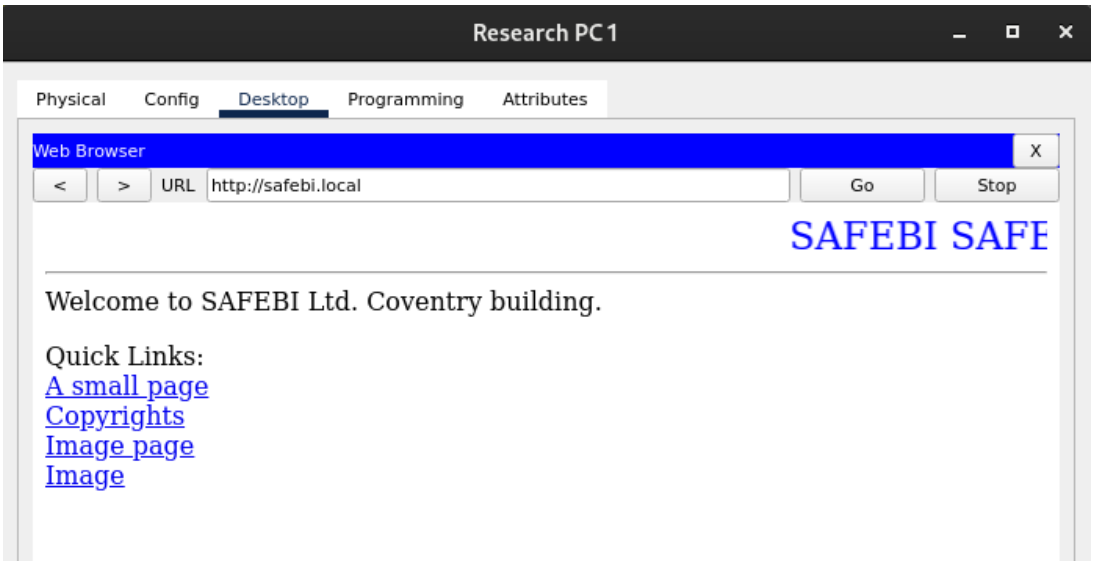

Figure 10: The website running on the HTML server

DHCP Server

DHCP is used to dynamically allocate IP addresses in the network. This is useful for adding devices to the network, aiding scalability, as it will automatically assign each device a working IP address within the subnet that they are in.

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
Server	192.168.10.225	192.168.10.227	192.168.10.229	255.255.255.248	2	0.0.0.0	0.0.0.0
HR	192.168.10.193	192.168.10.227	192.168.10.194	255.255.255.240	13	0.0.0.0	0.0.0.0
IT	192.168.10.209	192.168.10.227	192.168.10.210	255.255.255.240	13	0.0.0.0	0.0.0.0
Admin	192.168.10.65	192.168.10.227	192.168.10.66	255.255.255.224	29	0.0.0.0	0.0.0.0
Marketing	192.168.10.97	192.168.10.227	192.168.10.98	255.255.255.224	29	0.0.0.0	0.0.0.0
Accounting	192.168.10.129	192.168.10.227	192.168.10.130	255.255.255.224	29	0.0.0.0	0.0.0.0
Finance	192.168.10.161	192.168.10.227	192.168.10.162	255.255.255.224	29	0.0.0.0	0.0.0.0
Management	192.168.10.33	192.168.10.227	192.168.10.34	255.255.255.224	29	0.0.0.0	0.0.0.0
Research	192.168.10.1	192.168.10.227	192.168.10.2	255.255.255.224	29	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168.10.224	255.255.255.248	0	0.0.0.0	0.0.0.0

Figure 11: DHCP pools for each department

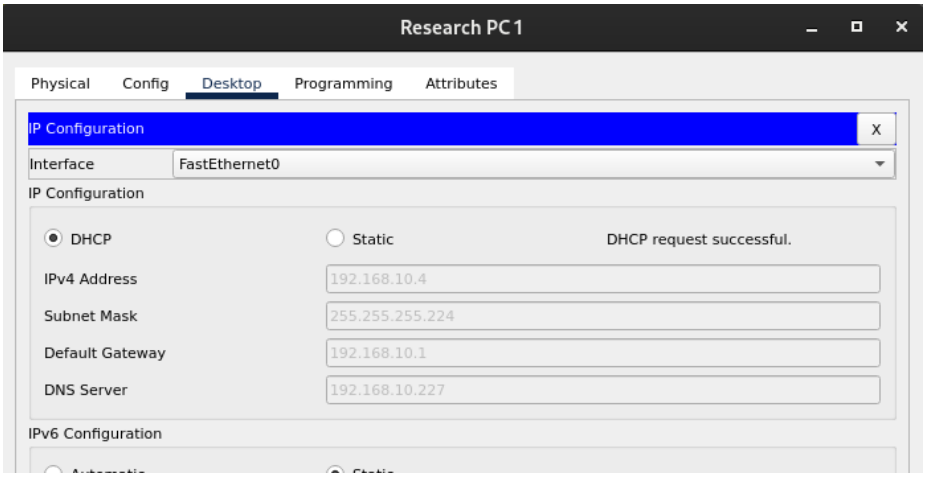

Figure 12: Successful DHCP request

E-Mail Server

An email server has also been implemented. This will allow employees to send files and messages across departments. To do this, the domain name 'safebi.com' is used.

When testing, two users were created. Username 'admin' password 'admin' and username 'test' password 'test'. *Figure 13* shows the test email sent from TestPC to Admin PC 1

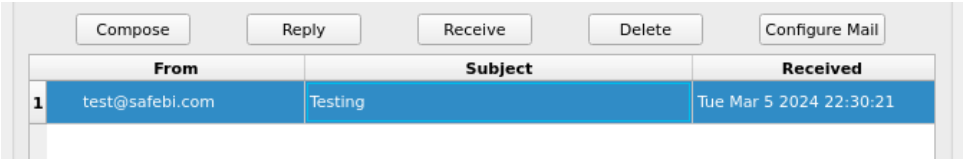

Figure 13: An email received by 'admin@safebi.com' from 'test@safebi.com'

OSPF Routing

OSPF (Open Shortest Path First) is a routing protocol that routes packets via the shortest path available (found with the Dijkstra algorithm). This makes it ideal as it will ensure quick and efficient delivery of packets from source to destination.

```
Floor3Router#show ip route ospf
     192.168.10.0/24 is variably subnetted, 17 subnets, 5 masks
O       192.168.10.0 [110/65] via 192.168.10.242, 01:41:28, Serial0/2/1
O       192.168.10.32 [110/65] via 192.168.10.242, 01:41:28, Serial0/2/1
O       192.168.10.96 [110/65] via 192.168.10.237, 01:41:28, Serial0/2/0
O       192.168.10.128 [110/65] via 192.168.10.237, 01:41:28, Serial0/2/0
O       192.168.10.160 [110/65] via 192.168.10.237, 01:41:28, Serial0/2/0
O       192.168.10.192 [110/65] via 192.168.10.242, 01:41:28, Serial0/2/1
O       192.168.10.232 [110/128] via 192.168.10.242, 01:41:28, Serial0/2/1
                       [110/128] via 192.168.10.237, 01:41:28, Serial0/2/0
```

Figure 14: OSPF routing protocols on Floor 3 Router

Security Features

Upon entering the CLI of a device, a message of the day (motd) banner is displayed warning the user not to attempt to log in if they are not authorised (see *Figure 15*).

```
Press RETURN to get started!

NO UNAUTHORISED ACCESS BEYOND THIS POINT

User Access Verification

Password:
```

Figure 15: Motd banner and Password prompted

As well, all hardware devices have been secured with a password:

- *Switches use the password 'SAFEBIswitch1' to enter initially*

- *Routers use the password 'SAFEBIrouter1' to enter initially*

- *Both Routers and Switches use the password 'SAFEBIenable1' to enter privileged execution mode*

- *Wireless Access Points use the password 'SAFEBIaccess1'*

Furthermore, '*service password-encryption*' was used on every device to encrypt the passwords in the '*startup-config*' (see *Figure 16*).

```
!
banner motd ^CNO UNAUTHORISED ACCESS BEYOND THIS POINT^C
!
!
!
!
line con 0
 password 7 08126D682C3B2C051D1E1801387A
 login
!
```

Figure 16: A snippet of the 'startup-config' of 'Floor 3 Router' showing a banner message of the day and an encrypted password.

Test and Verify Network Communication

Every client can communicate with each other. This can be seen in *Figure 17* where pings are sent across the network to test communication.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodi	Num
	Successful	HR PC 1	Research PC 1	ICMP		0.000	N	0
	Successful	Test-PC	Finance PC 2	ICMP		0.000	N	1
	Successful	Admin PC 1	Accounting Laptop	ICMP		0.000	N	2
	Successful	HR PC 1	IT PC 1	ICMP		0.000	N	3
	Successful	IT Laptop	Finance Printer	ICMP		0.000	N	4

Figure 17: Successful pings across the network