CMPE2000 Group Assignment

NETWORK DESIGN FOR EECMS BUILDING (314) AND THE LAB BUILDING (207)

Miri Campus: Group 4	
Name	**Student ID**
Michael Chai Chon Yun	21186114
Lina Yeo	21204647
Elena Lim Jou Lyn	21089213
Sherlyn Hwang Sing Yue	21200344

Table of Contents

1 Introduction

1.1 Objectives

This report details the network design for the EECMS building (314) and the lab building (207). Conveyed through a well-designed Local Area Network (LAN) topology between the two buildings, and configured via an array of industry-standard network devices.

The LAN topology is drawn up on the buildings' floor plan, with an IP addressing scheme to feature the network's interconnections between labs, classrooms, offices, and server rooms. All computers and printers are connected to the LAN, allowing for inter-communications and remote manageability from the control rooms.

1.2 Scope

This report will showcase the network design on the floor plan through a topology diagram and packet tracer, IP addressing scheme, and list of network devices to be utilised. All of which will be justified, and with relevant referencing if found needed.

The network's characteristics will also be detailed through four aspects. Those being performance, reliability, security, and manageability.

1.3 Assumption

Five assumptions have been provided in the assignment detail, those being the following:

a) There will be 2 buildings - 314 and 207.
b) Each building has two floors.
c) There are 4 departments and about 40 employees.
d) It has a maximum of 180 users including staff, lecturers, and students at the same time.
e) The server room and control room can be accessed by technicians and some staff only.

1.4 Limitation

After meeting network requirements, or exceeding them in certain cases. Potential limitations of this network are

a) Up to a maximum of 240 devices can run simultaneously on this network.
b) A WLAN network is configured to support up to 30 devices.
c) As a star topology network, network segments are susceptible to failure when the central hub breaks down, however necessary steps have been taken to minimise recovery time.
d) Two VLANs supporting 30 devices each remain unutilised, for future use.

2 Floor Plan Layout

2.1 Floor Plan & Legend

2.1.1 EECMS Building (314), Floor 1

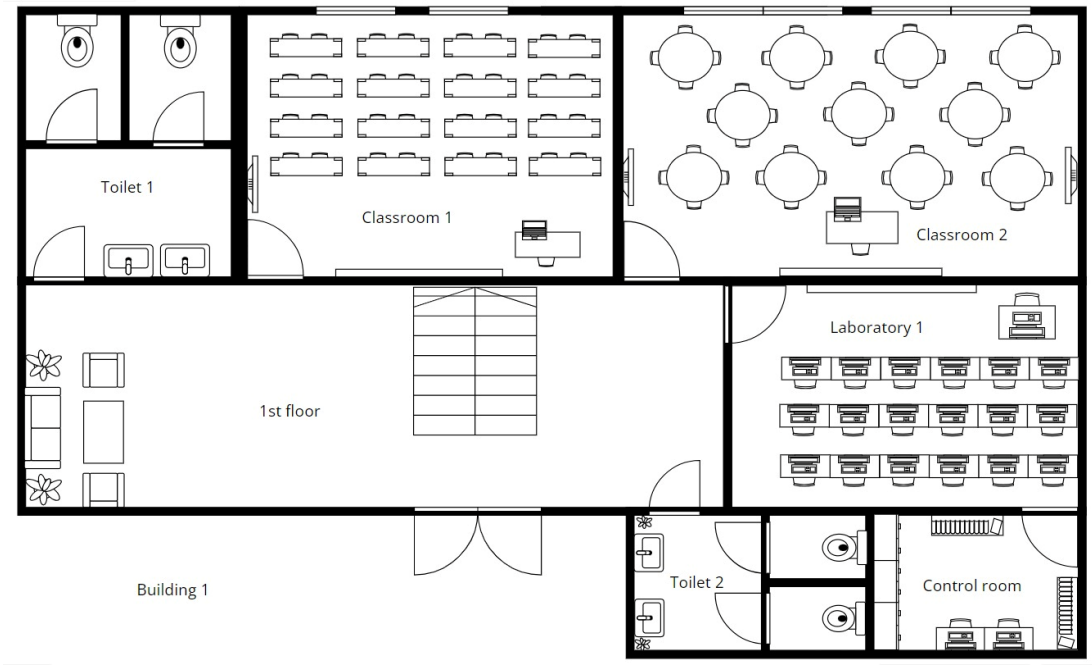


Figure 1: Floor Plan

2.1.2 EECMS Building (314), Floor 2

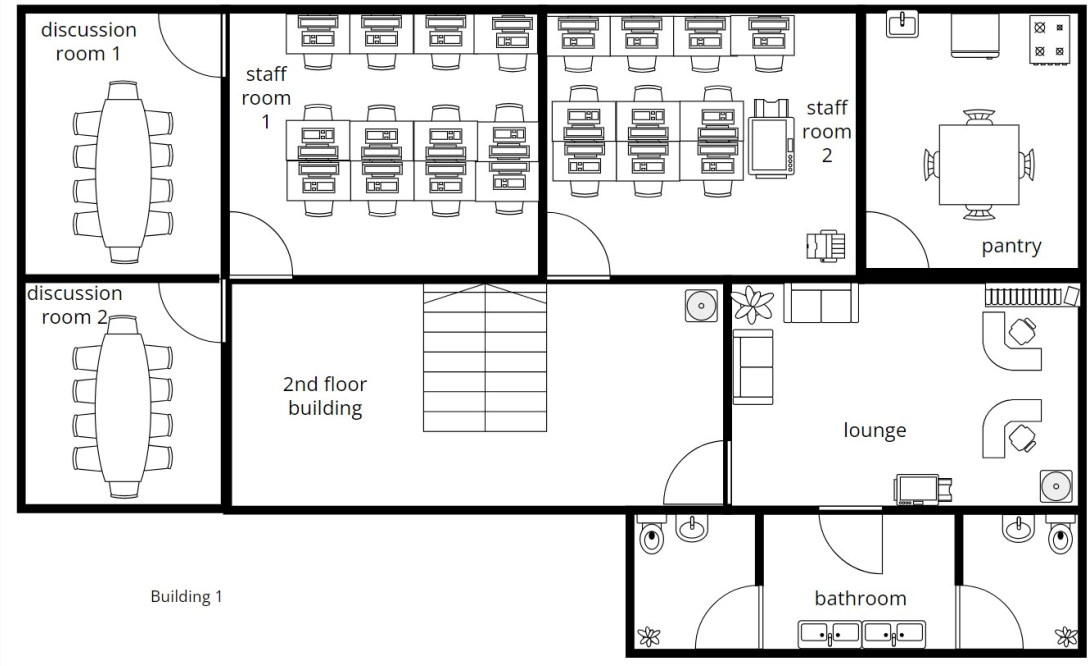


Figure 2: Floor Plan

2.1.3 Lab Building (207), Floor 1

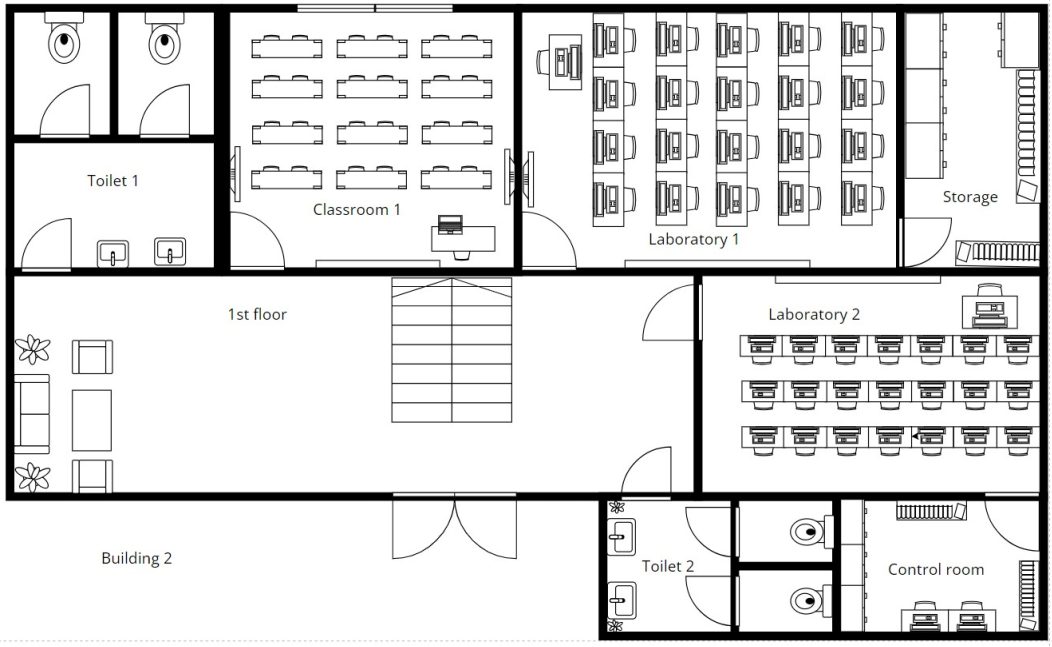


Figure 3: Floor Plan

2.1.4 Lab Building (207), Floor 2

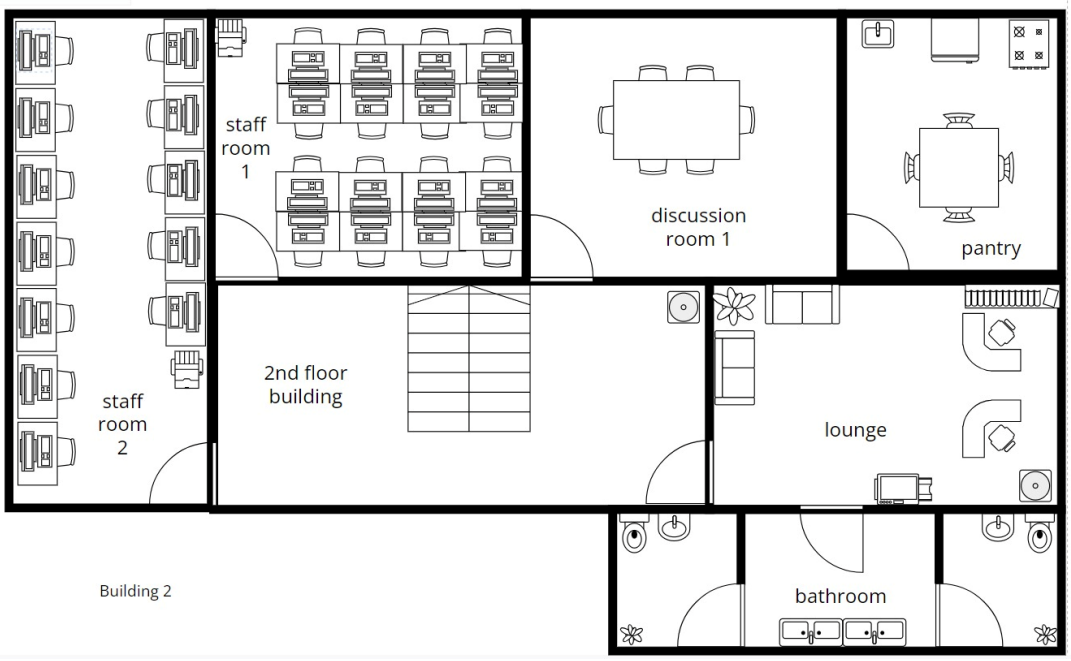


Figure 4: Floor Plan

2.1.5 Legend

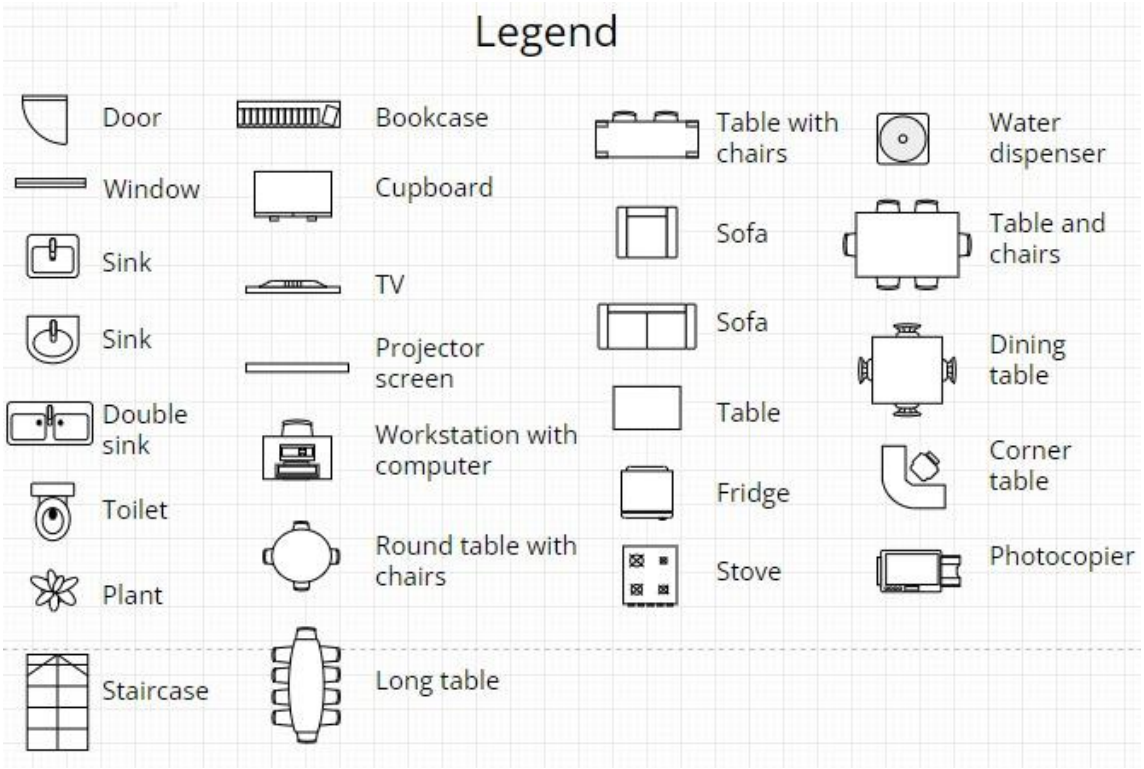


Figure 5: Floor Plans' Legend

2.2 Justification of Floor Plan Design

Following the assumptions made in the assignment brief, a detailed floor plan is designed. Floor plan is designed for two buildings which are, building 314 representing EECMS Building and building 207 representing lab building, which acts as the main building for network control. Each of the buildings have two floors with the first floor consisting of a classroom(s), laboratory and server room while the second floor consists mostly of staff rooms. The building was designed this way to give more privacy for staff and lecturers on the second floor and to avoid any disruption for the students on the first floor.

The first floor of building 314 or EECMS building was designed to have more, and larger classrooms compared to building 207 or lab building. Building 314 is designed in such a way to act as the learning space where lecture classes will be conducted, so it is prepared to fit in more students. While building 207 has more laboratories as the name suggests, it is a laboratory building. Next, on each first floor of the buildings, there is a server room or control room which has restricted access and only accessible by authorised staff. The server room has multiple cupboards to store the network devices for server connections and bookcases to store records and guidance books. All the classrooms and laboratories are also equipped with a projector screen and television for learning and teaching purposes.

The second floor of both buildings have two staff rooms for one department each, so both buildings combined have four staff rooms in total for four departments. Both buildings have a pantry for the staff's welfare and also a photocopier for office purposes. Building 314 is designed to have two discussion rooms with a bigger table for bigger meetings, while building 207 was designed with one discussion room with a smaller table for smaller meetings.

3 Network Devices

Device	Model	No. Total Devices	Justification for No. of devices	Purpose of device
Router	ROUTER-PT	3	· 2 routers to connect to each of the switches in each LAN. · 1 router to connect to the internet and switch.	· To allow devices on LANs to connect to the internet. · To allow communication across devices on the all LANs.
Switch	2960 IOS15	5	· The NO switches used are based on the NO ports available on each switch which is 24 in this case. · Hence, NO of computers, laptops and printers connected influence the NO of switches for each building. · 2 switches in building one to connect to a total of 46 printers, laptops and computers. · 3 switches in building two to connect to a total of 68 printers, laptops and computers.	· To connect together printers, laptops and computers within the same building. · To connect devices within the same LAN and allow communication between them.

4 Network Design

4.1 Side View of Network Diagram

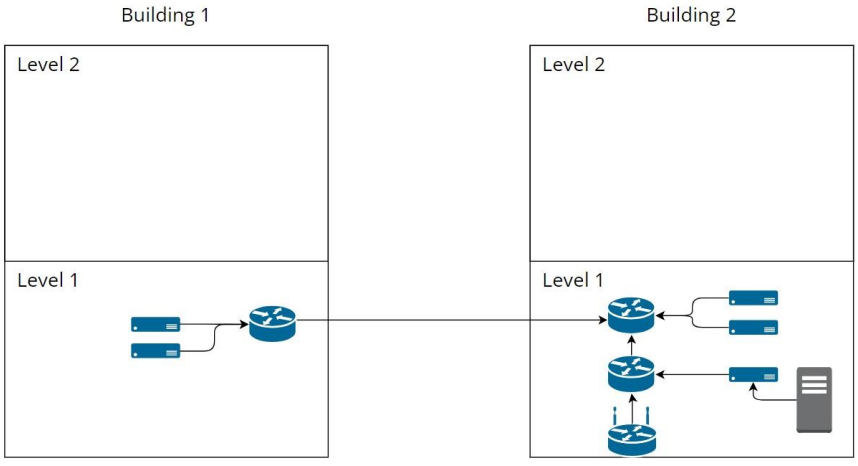


Figure 6: Network Diagram Side View

4.2 Aerial View of Network Diagram

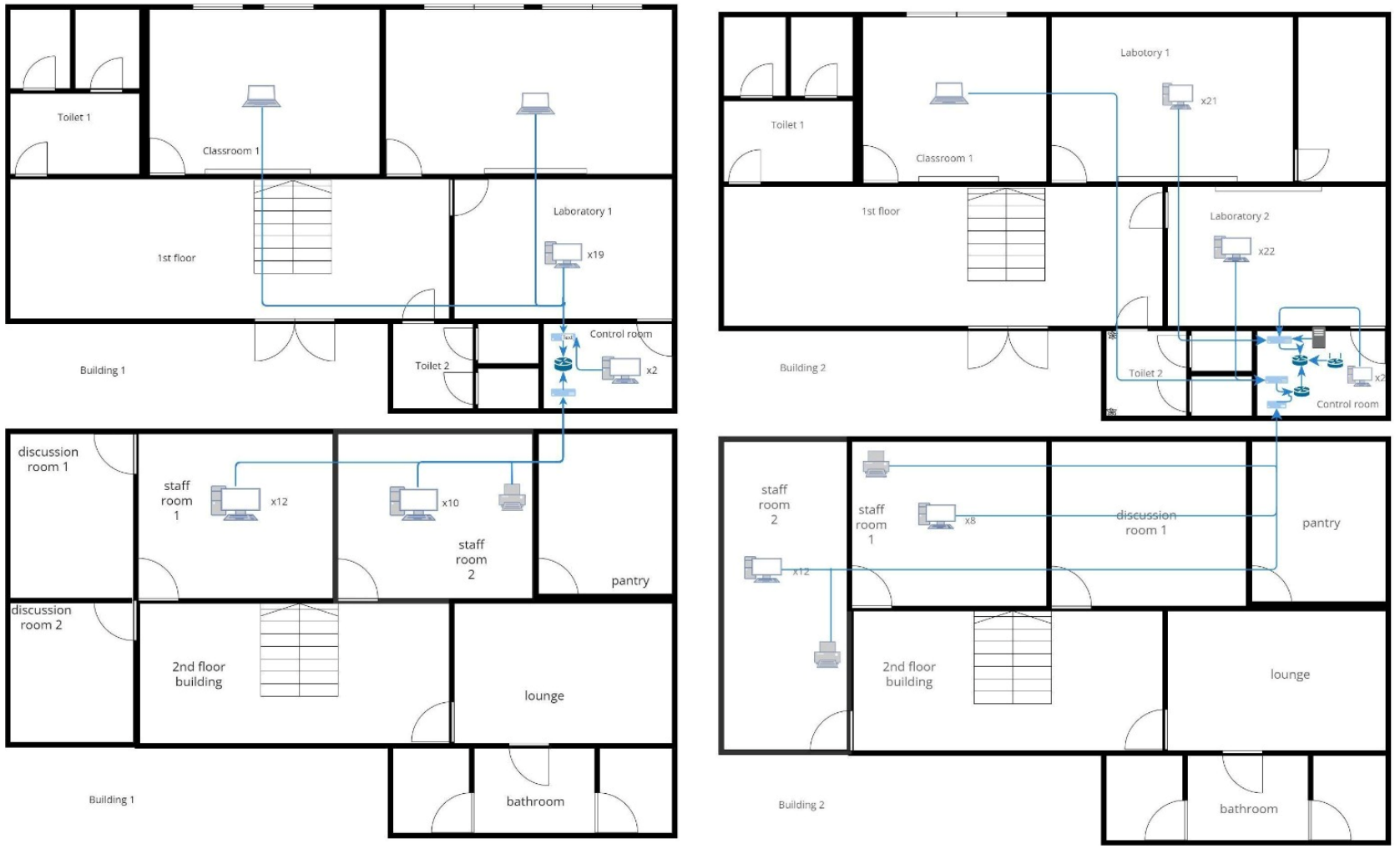


Figure 7: Network Diagram Aerial View

4.3 Network Design (Packet Tracer)

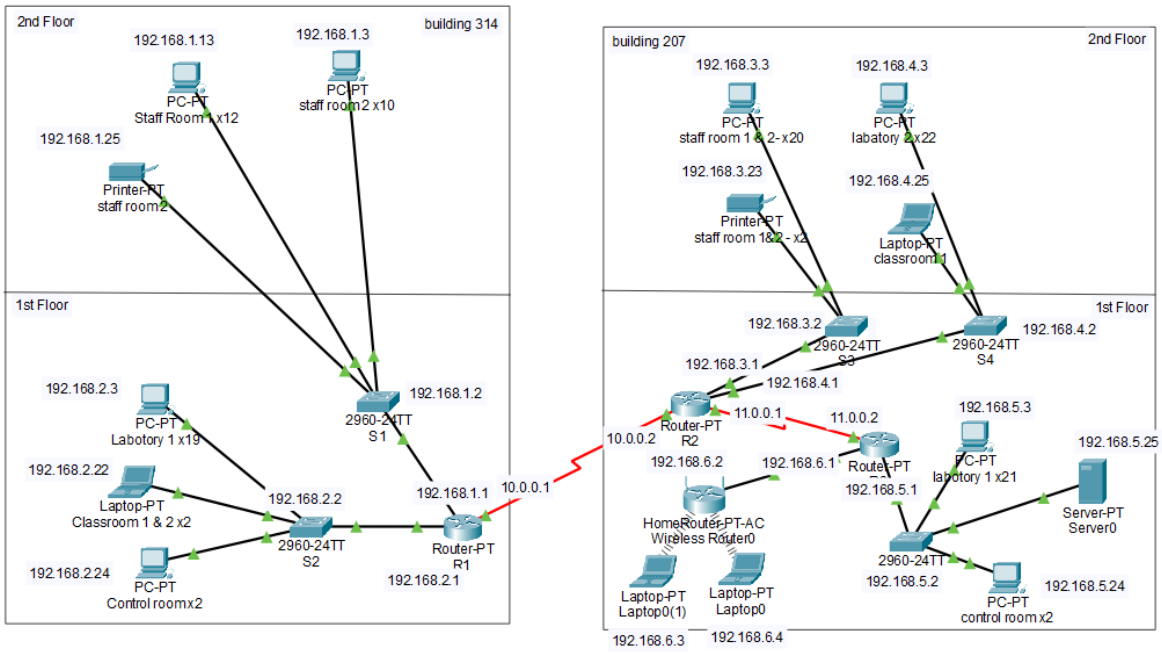


Figure 8: Logical Packet Tracer

5 Topology Justification

In building 314, there are a total of two switches. The reason for this is as there are a total of 46 different devices connected in this LAN and each switch consists of 24 ports. As the building consists of two floors, there is a switch for each floor. On the first floor, there are two classrooms each consisting of one laptop, a computer laboratory consisting of 19 computers and a control room consisting of an additional two computers resulting in 23 devices being connected to the S2 on the first floor. As for the second floor, there are two staff rooms where one consists of 10 computers and a printer while the other consists of 12 computers. Similarly to the first floor, there are a total of 23 devices that would be connected to S1. Of which, in both cases, the switches would offer a sufficient number of ports to connect to the devices on each respective floor. Additionally, a router named R1 is used to connect both S1 and S2 together, enabling communication between devices connected to each switch and to form the LAN.

As for Building 207 or Laboratory Building, there are three switches, with each switch having 24 ports. In order to have better understanding, the three switches will be called, S3, S4 and S5. Building 207 has more switches than Building 314 because Building 207 has more devices than building 314, thus, more switches are required for the LAN connection. The first floor of Building 207 has more devices than the second floor. There are 46 devices on the first floor of Building 207, one PC in classroom 1, 21 PCs in Laboratory 1, 22 PCs in Laboratory 2 and two PCs in the server/control room. Because of that, the first floor of Building 207 has two switches to connect all the devices together, a total of 23 devices across Classroom 1 and Laboratory 2 are connected to Switch S4, then, 23 devices in Laboratory 1 and the server room are connected to Switch S3. The second floor of Building 207 which has 22 devices; 20 PCs and two

printers in the two staff rooms will be connected to Switch S5, as 24 ports of one switch is sufficient for the second floor's devices' LAN connection. Switch S5 will also be connected to the server.

Other than switches, building 207 also has two routers. Router is used to manage the traffic between the networks and for Internet connection. Each router has four ethernet ports and two serial ports, serial port is used to connect a router to another router, while the ethernet port is used to connect switches to the router. One router is connected to switch S3, switch S4 and the router for building 314. Then, the second router is connected to switch S5 and the first router in Building 207. Although one router is sufficient to connect all three switches, the connection is divided into two separate routers to increase fault tolerance. In case of any router breaking down, there will still be one router that is functional. The second router will then be connected to the wireless router.

In addition, the reason for the number of switches used is to ensure that the use of all ports is efficient and fully maximised as opposed to having each switch allocated to each of the devices in each room which saves overall costs.

6 IP Addressing Justification

IP Addressing Table for Devices Shown in Packet Tracer				
Device	**Interface**	**IP Address**	**Subnet Mask**	**Default Gateway**
R1	Fa 0/0	192.168.1.1	255.255.255.224	N/A
	Fa 0/1	192.168.2.1	255.255.255.224	N/A
	S2/0	10.0.0.1	255.0.0.0	N/A
R2	Fa0/0	192.168.3.1	255.255.255.224	N/A
	Fa 0/1	192.168.4.1	255.255.255.224	N/A
	S2/0	10.0.0.2	255.0.0.0	N/A
	S3/0	11.0.0.1	255.0.0.0	
R3	Fa 0/0	192.168.5.1	255.255.255.224	N/A
	Fa 0/1	192.168.6.1	255.255.255.224	N/A
	S2/0	11.0.0.2	255.0.0.0	N/A
Wireless Router 0	Fa 0/0	192.168.6.2	255.255.255.224	192.168.6.1
S1	VLAN 1	192.168.1.2	255.255.255.224	192.168.1.1
S2	VLAN 2	192.168.2.2	255.255.255.224	192.168.2.1
S3	VLAN 3	192.168.3.2	255.255.255.224	192.168.3.1

S4	VLAN 3	192.168.4.2	255.255.255.224	192.168.4.1
S5	VLAN 4	192.168.5.2	255.255.255.224	192.168.5.1
Server 0	Fa 0/0	192.168.5.25	255.255.255.224	192.168.5.2
PC1 (Staffroom 2 x 10)	Fa 0/0	192.168.1.3	255.255.255.224	192.168.1.1
PC2 (Laboratory 1 x19)	Fa 0/0	192.168.2.3	255.255.255.224	192.168.2.1
PC3 (Staff room 1 & 2- x20)	Fa 0/0	192.168.3.3	255.255.255.224	192.168.3.1
PC4 (Laboratory 2 x 22)	Fa 0/0	192.168.4.3	255.255.255.224	192.168.4.1
PC5 (Laboratory 1 x 21)	Fa 0/0	192.168.5.3	255.255.255.224	192.168.5.1
Laptop 0	Wireless	DHCP		
Laptop 1	Wireless	DHCP		

IP Address Range per VLAN				
VLAN	**Utilised by (Building/Room)**	**Network Address**	**Usable Range**	**Broadcast Address**
1	B-314/Staff-1&2	192.168.1.0	192.168.1.1-30	192.168.1.31
2	B-314/Lab-1, Class-1&2, CR*	192.168.2.0	192.168.2.1-30	192.168.2.31
3	B-207/Staff-1&2	192.168.3.0	192.168.3.1-30	192.168.3.31
4	B-207/Class-1, Lab-2	192.168.4.0	192.168.4.1-30	192.168.4.31
5	B-207/Lab-1, CR*	192.168.5.0	192.168.5.1-30	192.168.5.31
6	B-207/1st-Floor Wi-Fi	192.168.6.0	192.168.6.1-30	192.168.6.31
7	Unutilised	192.168.7.0	192.168.7.1-30	192.168.7.31
8	Unutilised	192.168.8.0	192.168.8.1-30	192.168.8.31

*CR, Control-Room

The network is assigned a subnet within the 192.168.1.0/27 network. A /27 subnet mask provides eight subnets with 30 hosts each, which allows for up to 240 devices to be used simultaneously in the network. This way, there will be more than enough IP addresses to suit the needs of building 314 and 207, as well as enough VLANs for organised segmentation based on each department or room's needs.

The IP addresses are assigned statically to each permanent device on the network, to ensure consistent network identity and mapping. This is crucial for ease of communication between end devices, as well as for troubleshooting (Einorytė, 2023). An exception is made for network 192.168.6.0 on the first floor of building 207, as that network is specifically for WLAN, so IP addresses are assigned dynamically for the non-permanent devices entering and leaving the network frequently.

7 Network Characteristics

7.1 Network Performance

Based on the simulated design in the packet tracer to test if the network works as expected, various connectivity tests are performed between respective devices in the network. Ping tests are performed by testing if communication can be established between various layers in the topology. Subsequently, to conclude that a test is successful, the success rate of packets transferred shall be above 50% and vice versa. The below table displays the results of the tests.

Test Case	**Description**	**Source**	**Destination**	**Expected Result**	**Test Result**
1	Testing connection of devices connected to S1	Staffroom 1 PC (Building 314)	Staffroom 2 PC (Building 314)	Success	Success
2	Testing connection of devices connected to S2	Classroom 1 laptop (Building 314)	Lab 1 PC (Building 314)	Success	Success
3	Testing connection of devices across buildings	Control room PC (Building 314)	Control room PC (Building 207)	Success	Success
4	Testing connection of devices connected to S3	Staffroom 1&2 PC (Building 207)	Staffroom 1&2 Printer (Building 207)	Success	Success
5	Testing connection of devices connected to S4	Control Room PC (Building 207)	Server 0 (Building 207)	Success	Success
6	Testing connection of devices connected to the wireless router	Laptop 0	Laptop1	Success	Success
7	Testing connection of devices connected together within building 314	Control room PC (Building 314)	Staffroom 2 PC (Building 314)	Success	Success
8	Testing connection of devices connected together within building 207	Control room PC (Building 207)	Lab 2 PC (Building 207)	Success	Success

*NOTE: Screenshots of each test case has been attached below in the appendix.

As seen in the screenshots included in the appendix, nearly all of the tests' success rates are 100% except for test case 3 and 8 where there is 1 packet lost from each, resulting in a 75% success rate. The potential cause of packet loss could be due to various factors including network congestion, faulty network hardware, security measures, latency or QoS settings where it could then impact the network's performance through reduced throughput as data would need to be re-transmitted and an increased

latency where it could cause delay in data transmissions. However, research has shown that not all packet loss is avoidable and a certain level of packet loss is to be expected (Lamberti, 2024).

7.2 Network Reliability

To achieve optimal network reliability, appropriate designs or steps must be taken to keep the network functional when a device goes out-of-order, whether it be an end device, or a network device.

In regards to end devices, the network is designed based on a star-topology, using switches and routers to act as central hubs. Reason being, so that the network may resume normal operations when one or more host(s) experiences an issue. To simply put, when one computer is down, other computers will not be affected (Roy, 2020).

For network devices such as routers and switches, configuration backup has been taken as a step to minimise network down-time and resolution when a network device breaks down. Every switch and router's configuration has been saved and backed-up to the PC of their respective building's control room, allowing the network administrator to quickly replace and configure broken network devices.

*NOTE: Screenshots of configuration backups can be found in the appendix.

7.3 Network Security

Network security is crucial in order to protect data from threats and ensure the network reliability and trustworthiness (Barney & Lutkevich, 2022). With that being said, the simulated network in Packet Tracer is designed with the consideration of network security. Passwords are configured for all the routers and switches in the buildings to secure the network. For this simulated network in Packet Tracer, the generic password "cisco" is configured for the switches. This is to let the network administrator change or update the password configuration to a stronger password later on. For any attempt to access the switches and routers, warning messages will be displayed.

Next, the access to the server or control room is restricted. Only authorized staff have access to the control room. The staff will need to have a special ID in order to open the access room, and the time they are entering and leaving the server room will be recorded. Any changes or updates made on the servers and routers inside the server room will also need to be recorded accordingly.

The network also implements the Secure Shell (SSH) protocol. SSH protocol is a method to safely transmit commands to a computer across a vulnerable network. (SSH) offers robust password authentication and public key authentication. It also allows encrypted data transmission between two devices establishing a connection across an unrestricted network like the Internet (Loshin, 2021).

As for website access, the network is set to be able to access both https and http website as can be referred to in the Appendix. It is designed this way to allow access to all websites because not all websites have a Secure Socket Layer (SSL) port for https.

*NOTE: Screenshots of security configurations can be found in the appendix.

7.4 Network Manageability

Network administrators may easily configure network devices, switches and routers, from the comfort of the control room via Telnet as shown in Figure 9 & 10 below.

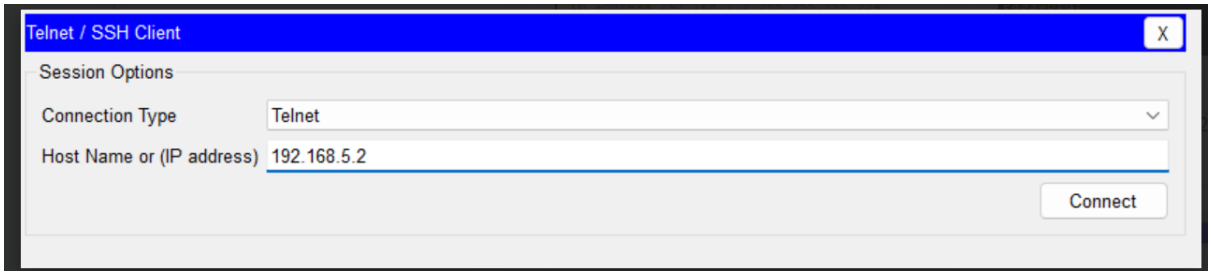


Figure 9: Telnet to 192.168.5.2

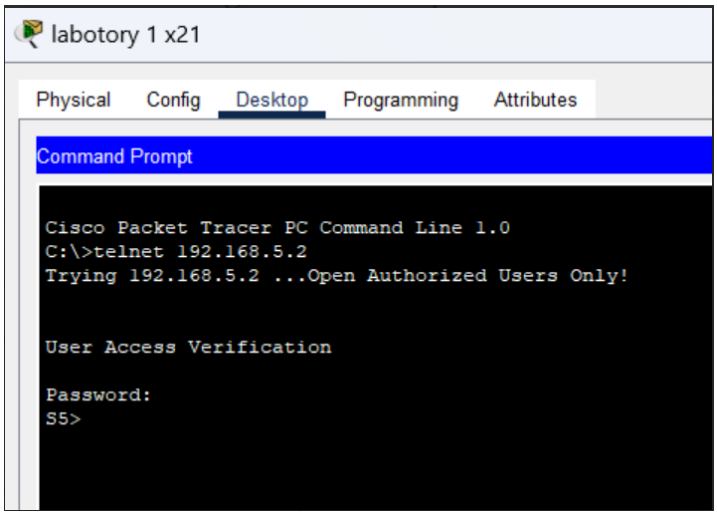


Figure 10: Telnet login to S5

Network administrators can also configure the Domain Name Service (DNS) for the network. As shown in the example in Figure 11, where DNS is configured for *server.com.au*. and later accessed in Figure 12 & 13.

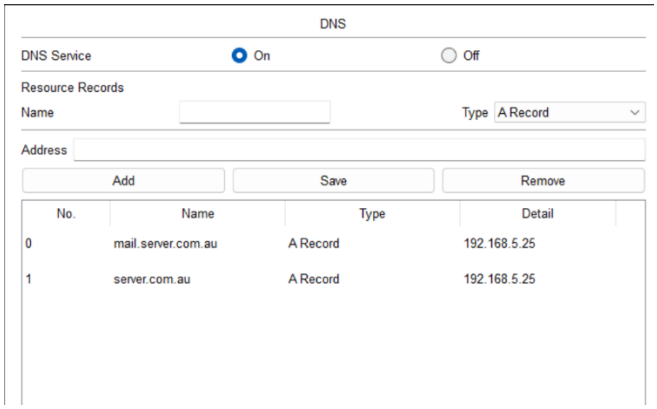


Figure 11: server.com.au is configured in DNS

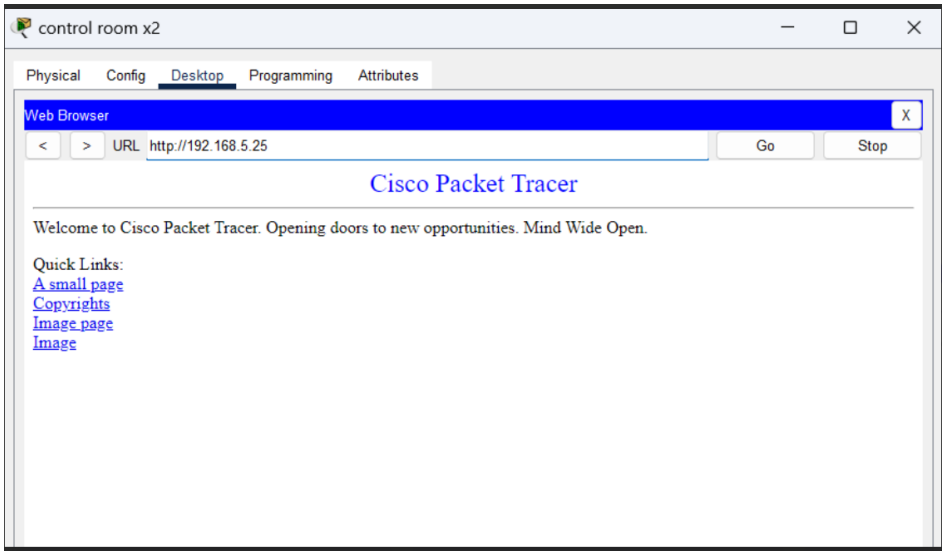


Figure 12: Accessing server.com.au using IP address

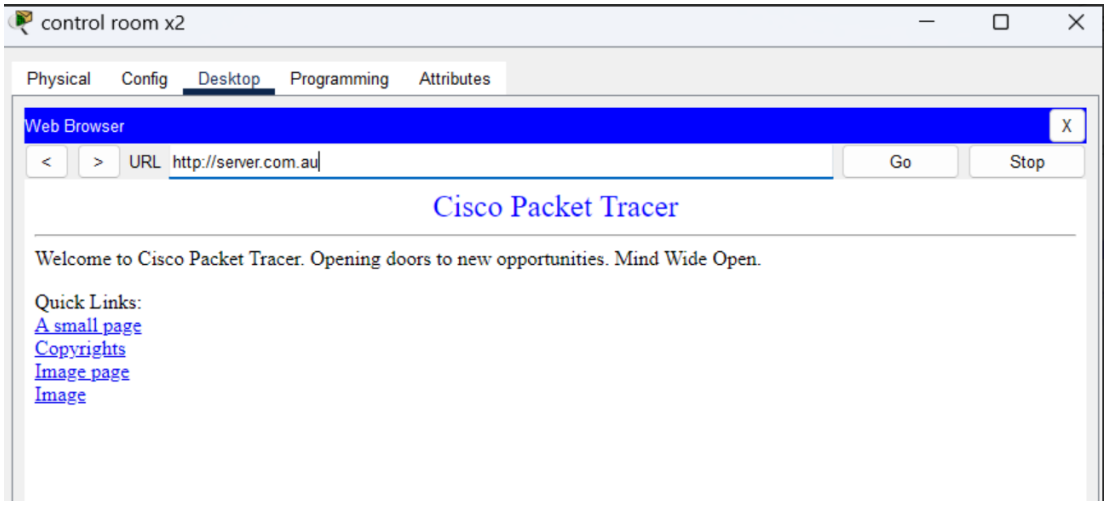


Figure 13: Accessing server.com.au using URL

8 Conclusion

A network has been designed specifically to address the needs of the EECMS Building (314) and the Lab Building (207). It can accommodate all required 180 hosts simultaneously, with an additional overhead of 60 devices for future scalability. Every end device can communicate with each other based on their static IP within the LAN, for both user communication and as well as for configuration by system and network administrators. Necessary steps and precautions have been taken to optimise the network's performance, reliability, security, and manageability.

9 References

Barney, N., & Lutkevich, B. (2022, October). What is Network Security? SearchNetworking. https://www.techtarget.com/searchnetworking/definition/network-security

Einorytė, A. (2023, November 24). Static IP vs. dynamic IP addresses. NordVPN. https://nordvpn.com/blog/static-ip-vs-dynamic-ip-address/

Lamberti, A. (2024, March 29). What Is Packet Loss & How Does It Affect Network Performance? Obkio. https://medium.com/obkio/what-is-packet-loss-how-does-it-affect-network-performance-c38fe32ce2e7#:~:text=Reduced%20Throughput%3A%20Packet%20loss%20can

Loshin, P. (2021, September). What is SSH (Secure Shell)? Definition from SearchSecurity. SearchSecurity. https://www.techtarget.com/searchsecurity/definition/Secure-Shell

Roy, J. (2020, March 22). What is Star Topology? Definition | Examples | Advantages | Disadvantages. Topology Network. https://topologynetwork.com/what-is-star-topology-definition-examples-advantages-disadvantages/

10 Appendix

Appendix A: Work Breakdown Structure

<table>
<tr><td colspan="5">Work in a team to propose a network design based on the given scenario
(Social Skills, Team Skills & Responsibility)</td></tr>
<tr><td colspan="2">Section 1 (Team)</td><td colspan="3">Introduction
- Objective / Scope / Limitations
- Assumptions (number of hosts, departments etc.)</td></tr>
<tr><td colspan="2"></td><td colspan="3">Floor Plan (Layout)
- Justification
- Network Devices</td></tr>
<tr><td colspan="5"></td></tr>
<tr><td rowspan="3">Section 1 (Individual)</td><td>Elena Lim Jou Lyn</td><td>Sherlyn Hwang Sing Yue</td><td>Lina Yeo</td><td>Michael Chai Chon Yun</td></tr>
<tr><td>Topology Justification</td><td>IP Addressing Justification</td><td>Topology Justification</td><td>IP Addressing Justification</td></tr>
<tr><td>Network Performance</td><td>Network Reliability</td><td>Network Security</td><td>Network Manageability</td></tr>
<tr><td colspan="5">Follow instruction to design a local area network and segmenting a network using simulation tools
(Practical Skills)</td></tr>
<tr><td>Cisco Packet Tracer</td><td colspan="2">Building 314</td><td colspan="2">Building 207</td></tr>
</table>

Appendix B: Peer Evaluation Forms

Write the name of each of your group members in a separate column. For each person, indicate the extent to which you agree with the statement on the left, using a scale of 1-4 (1=strongly disagree; 2=disagree; 3=agree; 4=strongly agree). Total the numbers in each column.

Peer Evaluation Form for Group Work by Michael Chai Chon Yun (21186114)			
Evaluation Criteria	Lina Yeo	Elena Lim Jou Lyn	Sherlyn Hwang Sing Yue
Attends group meetings regularly on time.	4	4	4
Contributes meaningful to the group discussions.	4	4	4
Prepares a quality of work and completes on time.	4	4	4
Demonstrates a cooperative and supportive attitude.	4	4	4
Contributes significantly to the success of the project.	4	4	4
Total	20	20	20

Peer Evaluation Form for Group Work by Lina Yeo (21204647)			
Evaluation Criteria	Michael Chai Chon Yun	Elena Lim Jou Lyn	Sherlyn Hwang Sing Yue
Attends group meetings regularly on time.	4	4	4
Contributes meaningful to the group discussions.	4	4	4
Prepares a quality of work and completes on time.	4	4	4
Demonstrates a cooperative and supportive attitude.	4	4	4
Contributes significantly to the success of the project.	4	4	4
Total	20	20	20

Peer Evaluation Form for Group Work by Elena Lim Jou Lyn (21089213)			
Evaluation Criteria	Lina Yeo	Michael Chai Chon Yun	Sherlyn Hwang Sing Yue
Attends group meetings regularly on time.	4	4	4
Contributes meaningful to the group discussions.	4	4	4
Prepares a quality of work and completes on time.	4	4	4
Demonstrates a cooperative and supportive attitude.	4	4	4
Contributes significantly to the success of the project.	4	4	4
Total	20	20	20

Peer Evaluation Form for Group Work by Sherlyn Hwang Sing Yue (21200344)			
Evaluation Criteria	Lina Yeo	Elena Lim Jou Lyn	Michael Chai Chon Yun
Attends group meetings regularly on time.	4	4	4
Contributes meaningful to the group discussions.	4	4	4
Prepares a quality of work and completes on time.	4	4	4
Demonstrates a cooperative and supportive attitude.	4	4	4
Contributes significantly to the success of the project.	4	4	4
Total	20	20	20

Appendix C: Network Performance Testing

Test case 1: Testing connection of devices connected to S1

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Pinging Staffroom 2 PC (192.168.1.3) from Staffroom 1 PC (192.168.1.13)

Test case 2: Testing connection of devices connected to S2

```
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Pinging Lab 1 PC (192.168.2.3) from Classroom 1 Laptop(192.168.2.22)

Test case 3: Testing connection of devices across different buildings

```
C:\>ping 192.168.5.24

Pinging 192.168.5.24 with 32 bytes of data:

Request timed out.
Reply from 192.168.5.24: bytes=32 time=2ms TTL=125
Reply from 192.168.5.24: bytes=32 time=2ms TTL=125
Reply from 192.168.5.24: bytes=32 time=29ms TTL=125

Ping statistics for 192.168.5.24:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 29ms, Average = 11ms
```

Pinging Building 207 Control room PC (192.168.5.24) from Building 314 Control room PC (192.168.2.24)

Test case 4: Testing connection of devices connected to S3

```
C:\>ping 192.168.3.23

Pinging 192.168.3.23 with 32 bytes of data:

Reply from 192.168.3.23: bytes=32 time<1ms TTL=128
Reply from 192.168.3.23: bytes=32 time<1ms TTL=128
Reply from 192.168.3.23: bytes=32 time=1ms TTL=128
Reply from 192.168.3.23: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.3.23:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Pinging Building 207 Staffroom 1&2 Printer (192.168.3.23) from Building 207 Staffroom 1&2 PC (192.168.3.3)

Test case 5: Testing connection of devices connected to S4

```
C:\>ping 192.168.5.25

Pinging 192.168.5.25 with 32 bytes of data:

Reply from 192.168.5.25: bytes=32 time<1ms TTL=128
Reply from 192.168.5.25: bytes=32 time<1ms TTL=128
Reply from 192.168.5.25: bytes=32 time<1ms TTL=128
Reply from 192.168.5.25: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.5.25:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Pinging Building 207 Server0 (192.168.5.25) from Building 207 Control room PC (192.168.5.24)

Test case 6: Testing connection of devices connected to the wireless router

```
C:\>ping 192.168.6.4

Pinging 192.168.6.4 with 32 bytes of data:

Reply from 192.168.6.4: bytes=32 time=72ms TTL=128
Reply from 192.168.6.4: bytes=32 time=46ms TTL=128
Reply from 192.168.6.4: bytes=32 time=42ms TTL=128
Reply from 192.168.6.4: bytes=32 time=42ms TTL=128

Ping statistics for 192.168.6.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 42ms, Maximum = 72ms, Average = 50ms
```

Pinging Laptop1 (192.168.6.4) from Laptop0 (192.168.6.1)

Test case 7: Testing connection of devices connected together within building 314

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=127
Reply from 192.168.1.3: bytes=32 time<1ms TTL=127
Reply from 192.168.1.3: bytes=32 time<1ms TTL=127
Reply from 192.168.1.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Pinging Staffroom 2 PC (192.168.1.3) from Building 314 Control room PC (192.168.2.24)

Test case 8: Testing connection of devices connected together within building 207

```
C:\>ping 192.168.4.3

Pinging 192.168.4.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.4.3: bytes=32 time=10ms TTL=126
Reply from 192.168.4.3: bytes=32 time=5ms TTL=126
Reply from 192.168.4.3: bytes=32 time=25ms TTL=126

Ping statistics for 192.168.4.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 25ms, Average = 13ms
```

Pinging Building 207 Lab2 (192.168.4.3) from Building 207 Control room PC (192.168.5.24)

Appendix D: Configuration Backups

R1 Configuration Backup

```
R1#enable
R1#copy running-config tftp
Address or name of remote host []? 192.168.2.24
Destination filename [R1-confg]?

Writing running-config....!!
[OK - 1003 bytes]

1003 bytes copied in 3.002 secs (334 bytes/sec)
R1#
```

R2 Configuration Backup

```
R2#enable
R2#copy running-config tftp
Address or name of remote host []? 192.168.5.24
Destination filename [R2-confg]?

Writing running-config....!!
[OK - 1008 bytes]

1008 bytes copied in 3.004 secs (335 bytes/sec)
R2#
```

R3 Configuration Backup

```
R3#enable
R3#copy running-config tftp
Address or name of remote host []? 192.168.5.24
Destination filename [R3-confg]?

Writing running-config...!!
[OK - 982 bytes]

982 bytes copied in 0 secs
R3#
```

S1 Configuration Backup

```
S1#copy running-config tftp
Address or name of remote host []? 192.168.2.24
Destination filename [S1-confg]?

Writing running-config....!!
[OK - 1261 bytes]

1261 bytes copied in 3.014 secs (418 bytes/sec)
S1#
```

S2 Configuration Backup

```
User Access Verification

Password:

S2>enable
Password:
S2#enable
S2#copy running-config tftp
Address or name of remote host []? 192.168.2.24
Destination filename [S2-confg]?

Writing running-config....!!
[OK - 1311 bytes]

1311 bytes copied in 3.004 secs (436 bytes/sec)
S2#
```

S3 Configuration Backup

```
S3#copy running-config tftp
Address or name of remote host []? 192.168.5.24
Destination filename [S3-confg]?

Writing running-config....!!
[OK - 1311 bytes]

1311 bytes copied in 3.009 secs (435 bytes/sec)
S3#
```

S4 Configuration Backup

```
S4#copy running-config tftp
Address or name of remote host []? 192.168.5.24
Destination filename [S4-confg]?

Writing running-config....!!
[OK - 1311 bytes]

1311 bytes copied in 3.001 secs (436 bytes/sec)
S4#
```

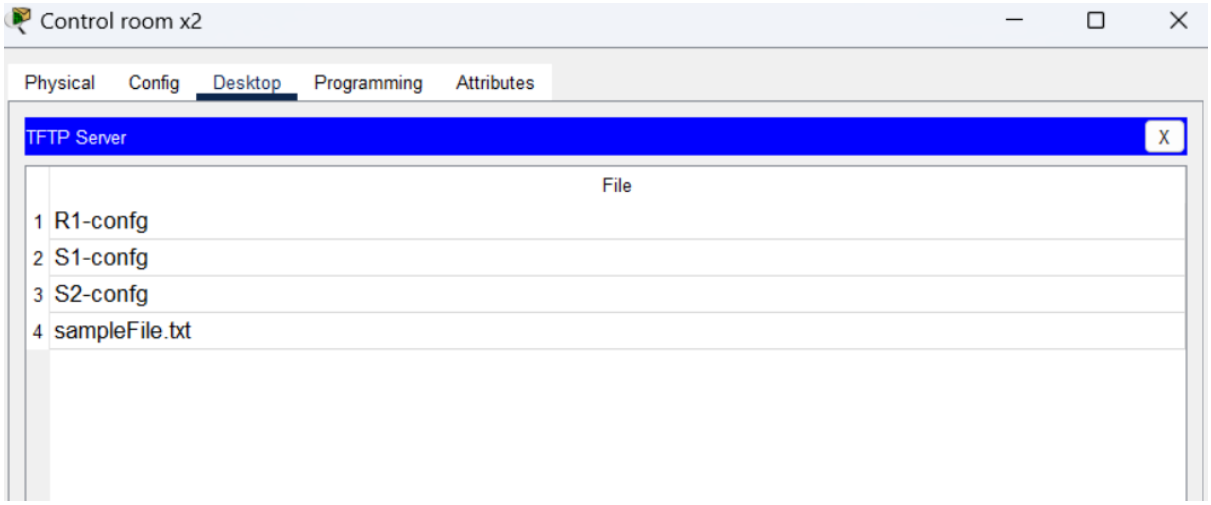
S5 Configuration Backup

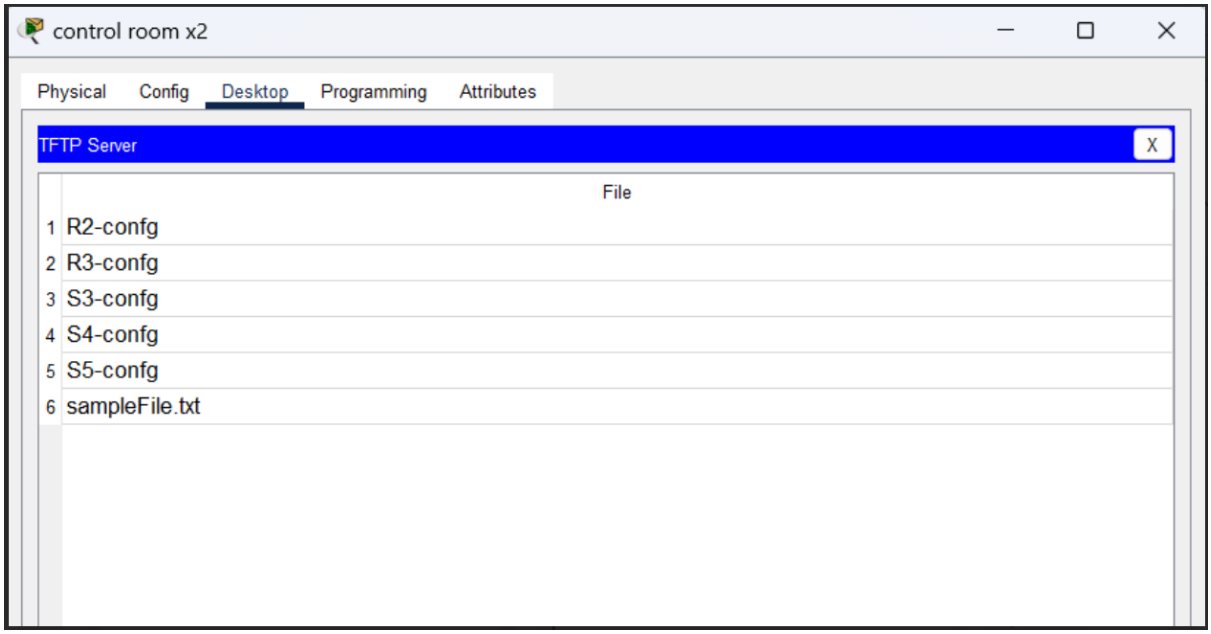
```
S5>enable
Password:
S5#enable
S5#copy running-config tftp
Address or name of remote host []? 192.168.5.24
Destination filename [S5-confg]?

Writing running-config....!!
[OK - 1291 bytes]

1291 bytes copied in 3.005 secs (429 bytes/sec)
S5#
```

Configuration Backups Saved on TFTP Server in Control Room PC





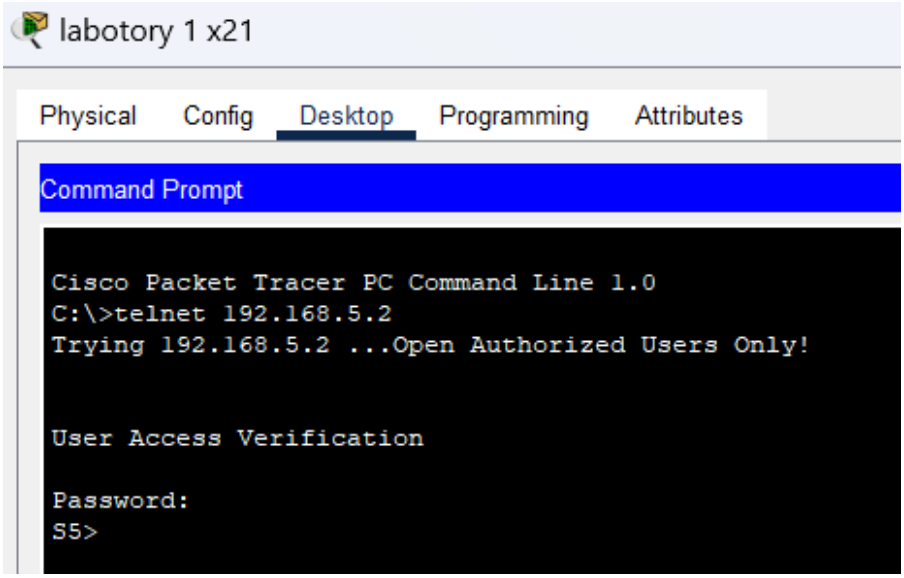
Appendix E: Security Configurations

Switch password configuration:

```
Building configuration...

Current configuration : 1261 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S1
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
no ip domain-lookup
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.2 255.255.255.224
!
ip default-gateway 192.168.1.1
!
banner motd ^C Authorized Users Only! ^C
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end
```

Warning messages for unauthorized access:



Router password configuration:

```
Current configuration : 1003 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R1
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
!
!
!
!
!
no ip domain-lookup
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.224
 duplex auto
 speed auto
!
interface FastEthernet1/0
 ip address 192.168.2.1 255.255.255.224
 duplex auto
 speed auto
!
interface Serial2/0
 ip address 10.0.0.1 255.0.0.0
 clock rate 2000000
!
interface Serial3/0
 no ip address
 clock rate 2000000
 shutdown
interface FastEthernet4/0
 no ip address
 shutdown
!
interface FastEthernet5/0
 no ip address
 shutdown
!
router rip
 network 10.0.0.0
 network 192.168.1.0
 network 192.168.2.0
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^CUnauthorized access is prohibited!^C
!
!
!
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 password 7 0822455D0A16
 login
!
!
!
end
```

HTTP and HTTPS website access: