GROUP PROJECT

GROUP 4 (PART 2)

COMPUTER NETWORKING

BIC21303

BY

GROUP MEMBERS

No	Name	Matric No
1.	Rusdi bin Abd Rashid	AI230025
2.	Danish Assafi bin Nor Saidi	AI230062
3.	Muhammad Zulhilman bin Tarmizi	AI230047
4.	Muhammad Nur Faiz bin Alistini	CI230041
5.	Adam Muqri bin Zulkifli	AI230062
6.	Alkhattab Shehabaddin Abdullah Abdulwadod Al-Dubai	AI230209

ISI KANDUNGAN
TABLE OF CONTENT

Table of Contents

1.0 Project Title

1.1 Project Title

A campus network design for a college

1.2 Project Scope

This project aims to design and implement a secure, high-performance campus network infrastructure for a college. The network will serve 230 users across three buildings and 100 users in a remote branch campus. The college has 160 users in the Main building, 20 users in Building 1, and 50 users in Building 2. Every building has a lobby which is 500 square feet of open space, where wireless access to the network is required and only authorized personnel should have access to the wireless network.

The distance from Building 1 to the main building is 500 meters. Building 2 is located 100 meters away from the main building, and the distance between Building 1 and Building 2 is 200 meters. The main building has access to a high-speed cable internet connection that needs to be shared with all users in the other buildings.

A branch campus situated approximately 10 kilometers away from the main campus network serves around 100 users, all located within a single building. The campus features a lobby equipped with Wi-Fi access, which is available exclusively to registered students. The design includes secure wireless access in lobbies, centralized internet sharing, and a dedicated server farm subnet for key services (web, email, DNS, DHCP).

2.0 Campus Diagram

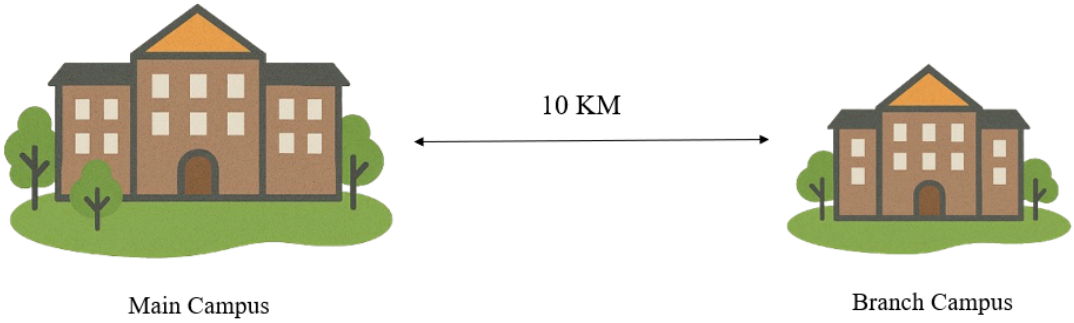


Figure 2.1 *Campus diagram for Main Campus and Branch Campus*

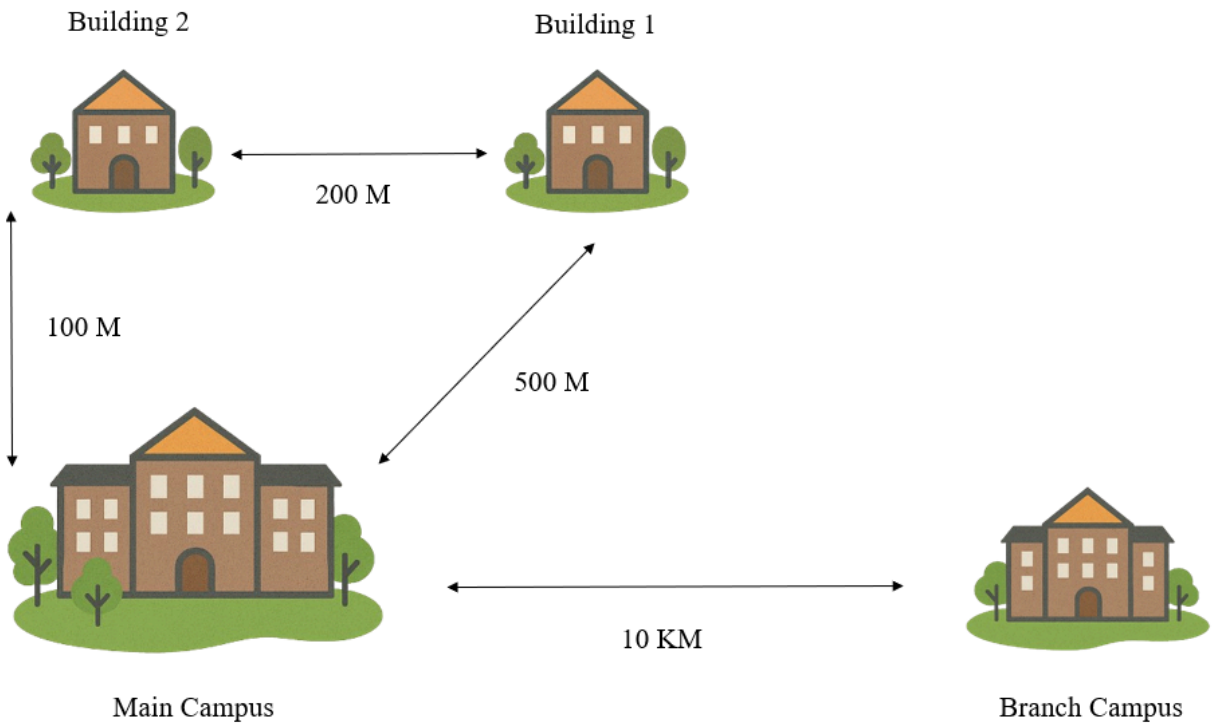


***Figure 2.2** Overview of Campus diagram*

3.0 Network requirement analysis

- **User and Device Distribution**

Location	Wired Users	Wireless Users	Total Users	Remarks
Main Building	160	20 (Lobby)	180	Core location, internet connection, server farm
Building 1	20	10 (Lobby)	30	Connected via fiber (500m)
Building 2	50	10 (Lobby)	60	Connected via fiber (100m)
Branch Campus	100	20 (Lobby)	120	Located 10 km away, connected via VPN or dedicated WAN link
Total	**330**	**60**	**390**	

This network requirement analysis outlines the necessary components and considerations for designing and implementing a campus network infrastructure to support a college consisting of multiple buildings and a branch campus. The main building hosts 160 wired users and a 500 square feet lobby requiring secure wireless access for 20 additional users. Building 1 accommodates 20 wired users and a lobby serving 10 wireless users, located 500 meters from the main building. Building 2, located 100 meters from the main building, supports 50 wired users and 10 wireless users in its lobby. The branch campus, 10 kilometers away, houses 100 wired users and a lobby for 20 wireless users. In total, the network must support 330 wired users and 60 wireless users, amounting to 390 users altogether.

A high-speed internet connection is available in the main building and will be shared across the entire network. Each building, including the branch campus, will be assigned its own subnet using private IP address space, such as 192.168.0.0/16. DHCP servers will be used for dynamic IP allocation, while static IPs will be reserved for critical infrastructure like servers, routers, and switches. The main building will host a server farm that includes a web server, email server, DNS server, and DHCP server, which will be allocated a dedicated subnet. Security protocols like WPA2 or WPA3 Enterprise will be enforced for wireless networks, allowing only authorized users to access the system.

The campus network will employ a Core-Distribution-Access layered topology, with a star connection from the main building to other buildings via fiber optic cables. Building 1 and Building 2 will connect through fiber due to the distance and performance requirements. The branch campus will be linked using either a VPN over the public internet or a dedicated leased line. At least two routers will be deployed for inter-building routing and WAN access. Layer 3 switches will be used at the distribution level, and Layer 2 switches at the access level to manage VLANs and segment traffic between students, staff, servers, and Wi-Fi networks.

Network security will include firewall implementation at the internet gateway, MAC filtering, access control lists (ACLs), and the use of a RADIUS server for identity authentication. Services such as DHCP, DNS, NAT, file sharing, and network monitoring will be provided to ensure efficient operation and communication within the network. The network will be scalable, allowing for future expansion through subnetting and virtualization. Redundancy measures, such as a backup WAN connection and failover configurations, will be put in place for reliability.

Centralized network management will be implemented using tools that support SNMP, SSH, and web-based interfaces. Proper documentation, labeling, and cable management will aid in troubleshooting and maintaining the network efficiently. This comprehensive plan ensures a secure, scalable, and high-performance network to support the operational needs of the college.

Below are the list of network requirements:

No	Item	Quantity	Justification
1	ISR 4331/K9 Routers	2	One for main campus gateway, one for branch campus or redundancy
2	Cisco Catalyst Switch 2960-24TT-L	10	Reasonable: Main building (6+), Building 1 (2), Building 2 (2), branch (3)
3	CAT7 Straight-through LAN Cable	265	Good for connecting end devices to access

			switches
4	Multilayer Switch 3560-24 PS	1	Used at the distribution/core layer (Main Building, Server Farm, Inter-Building)
5	Crossover Ethernet Cable	25	For direct device-to-device connections

4.0 Physical Network Design

A physical network design describes the tangible elements of a network for the campus, including hardware, cables, and physical connections. It focuses on the actual layout and arrangement of network devices and how they are physically connected.

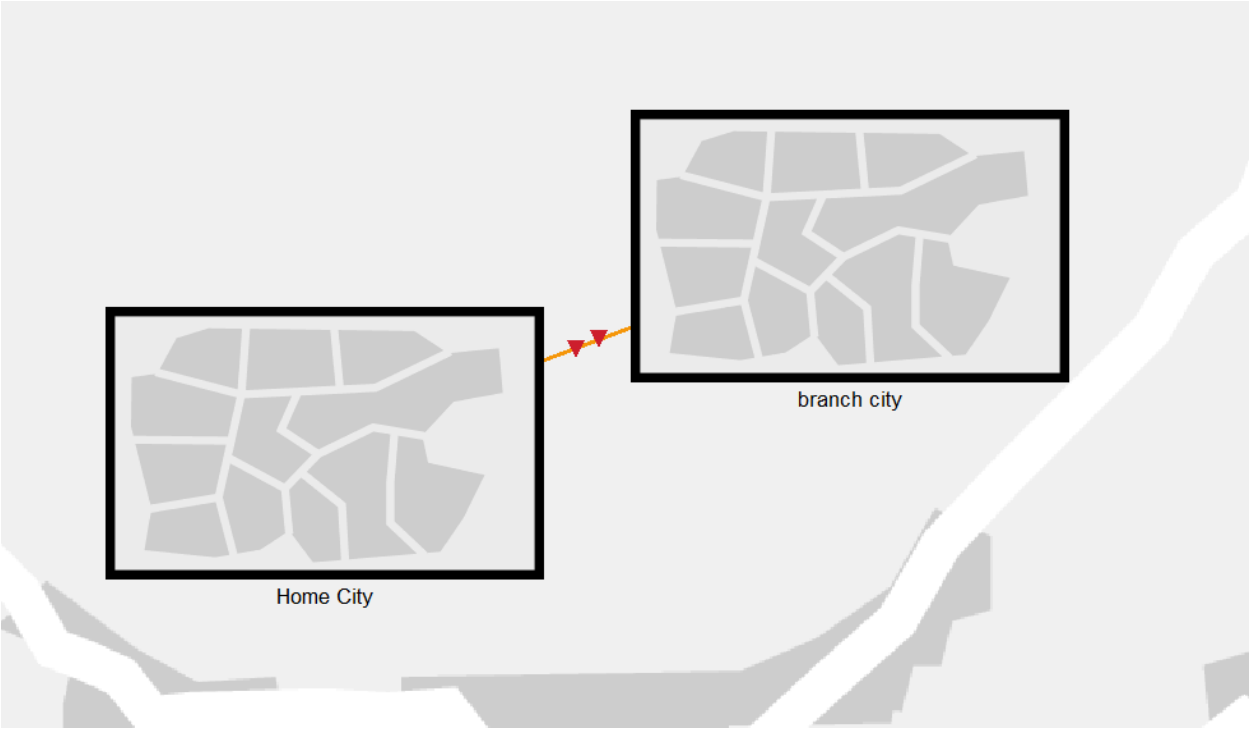


Figure 4.0.1 *Intercity physical network topology*

This network topology illustrates the connection between the main campus (located in the home city) and a branch campus situated 10 kilometers away. The main campus router provides connectivity to both the internet and the branch campus. Similarly, the branch campus router connects the branch campus to the main campus. A high-speed fiber optic link is used to establish the connection between the two campuses over the 10-kilometer distance.

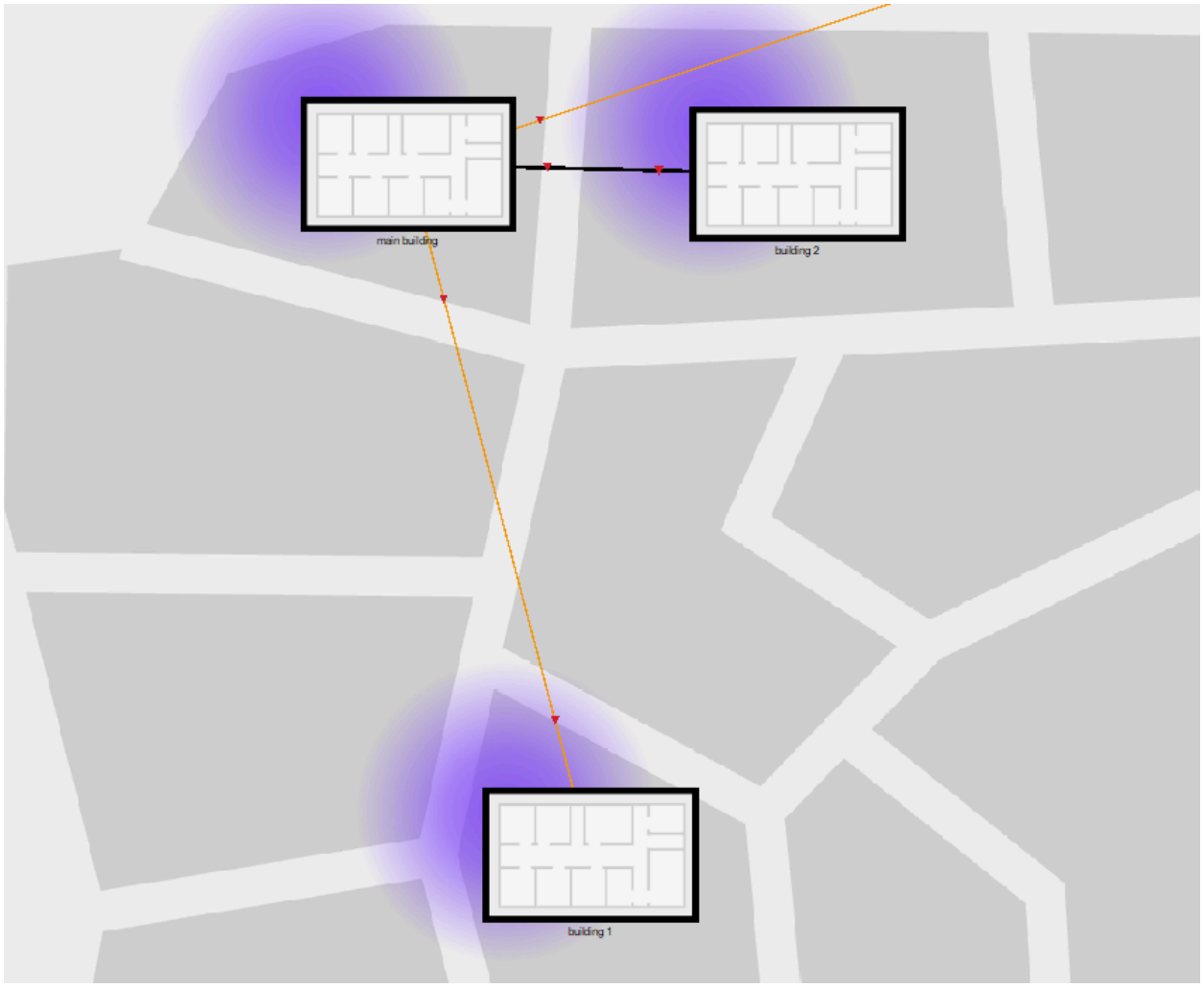


Figure 4.0.2 *Inter-college physical network topology*

This topology depicts the network connections among the Main Building, Building 1, and Building 2 within the main campus. The core switch located in the Main Building functions as the central backbone for that building. Each switch in Building 1 and Building 2 is responsible for connecting devices within its respective building. Additionally, Access Points (APs) are installed in the lobbies of each building to provide wireless network access.

Figure 4.0.3 *Branch campus city physical network topology*

This topology represents the internal network structure of the branch campus. Access Points (APs) are installed in the lobby area to provide wireless connectivity. User devices, such as laptops and desktops, are connected to the network through both wired and wireless connections. Rack-mounted equipment is installed in wiring closets located on various floors of the building.

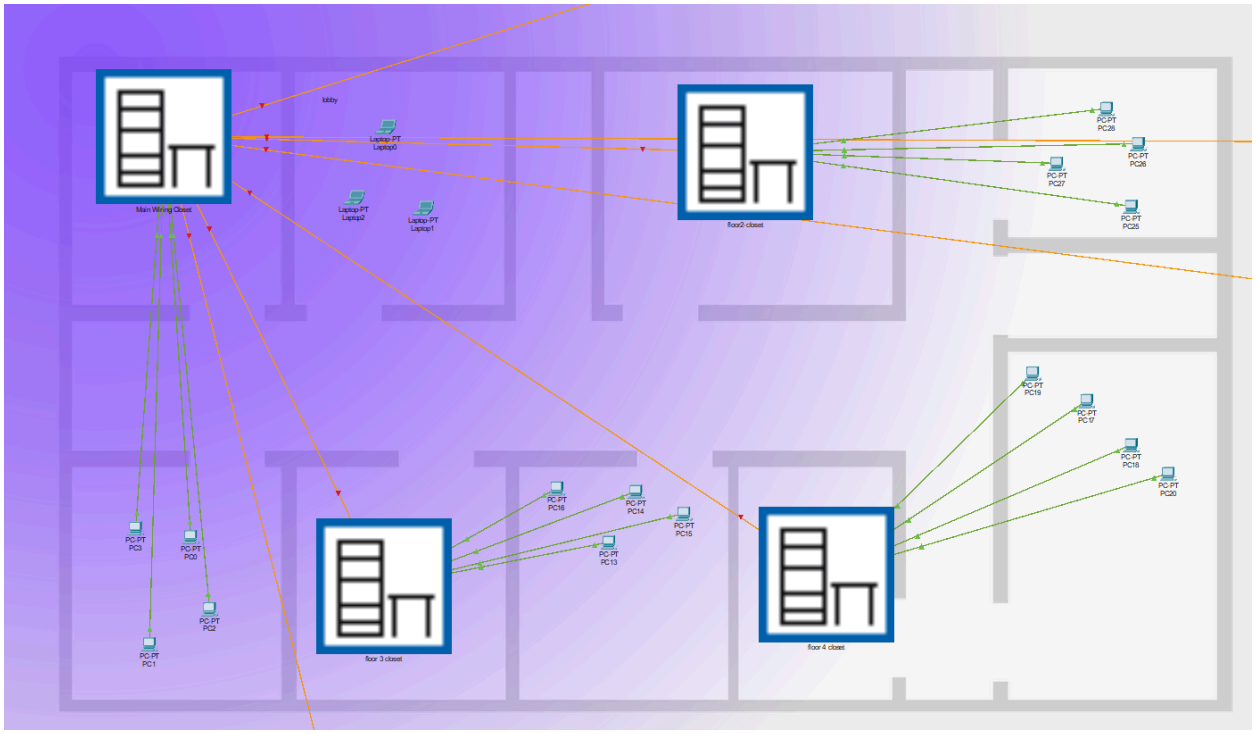


Figure 4.0.4 *Main building physical network topology*

The Main Building's physical network topology is designed to support 160 users, with a ratio of one PC for every ten users. As a result, approximately 16 PCs or laptops are active at any given time. The network infrastructure includes a core switch (Core-Switch-Main) that serves as the central hub for connectivity within the building. Floor-level switches are deployed to distribute network access across different floors. Additionally, Access Points (APs) are strategically installed in open areas such as lobbies and common spaces to provide wireless connectivity. User devices, including laptops and desktops, connect to the network through both wired and wireless connections.

Figure 4.0.5 *Floor 1 wiring room rack*

This rack functions as the central hub for network connectivity within the main building. It houses core networking components and servers that deliver essential services to users across the campus. Key components within the rack include the main router, core switch, and a server farm consisting of the Web Server, Email Server, DNS Server, and

DHCP Server. The main router acts as the central gateway, connecting the internal network to the internet and to remote locations such as the branch campus. It also manages routing between various subnets, including those for the Main Building, Building 1, Building 2, and the Branch Campus. The core switch serves as the backbone of the network, interconnecting all floor-level switches, servers, and the router. It is connected to floor switches (e.g., Switch-Floor2, Switch-Floor3), the server farm, the firewall, and the main router, ensuring efficient data flow and centralized network management.

The server farm consists of several critical servers that provide centralized network services, including a Web Server, Email Server, DNS Server, and DHCP Server. The Web Server hosts both internal and external websites, such as the college portal. The Email Server manages email communications for both staff and students. The DNS Server is responsible for resolving domain names into IP addresses for internal and external access. The DHCP Server dynamically assigns IP addresses to client devices within the network. Additionally, the Web Server and Email Server are placed in a Demilitarized Zone (DMZ) to protect the internal network from direct exposure to untrusted external networks. This setup allows secure and controlled access to specific services while safeguarding the internal infrastructure.

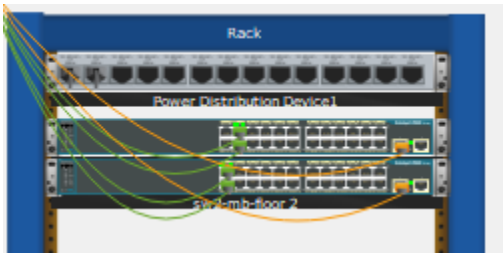


Figure 4.0.6 *Floor 2 wiring room rack*

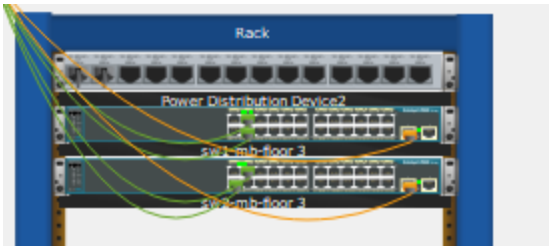


Figure 4.0.7 *Floor 3 wiring room rack*

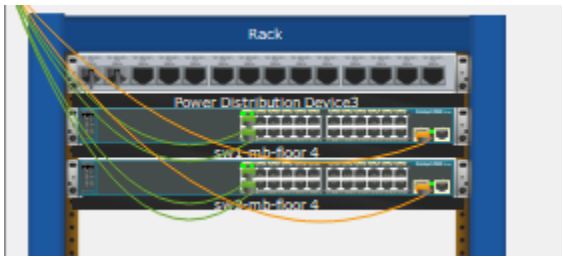


Figure 4.0.8 *Floor 4 wiring room rack*

Figure 4.0.6, Figure 4.0.7 and ***Figure 4.0.8*** illustrate the racks that support network connectivity for Floors 2, 3, and 4, respectively. Each rack includes a Layer 2 or Layer 3 switch dedicated to managing network connections on its corresponding floor.

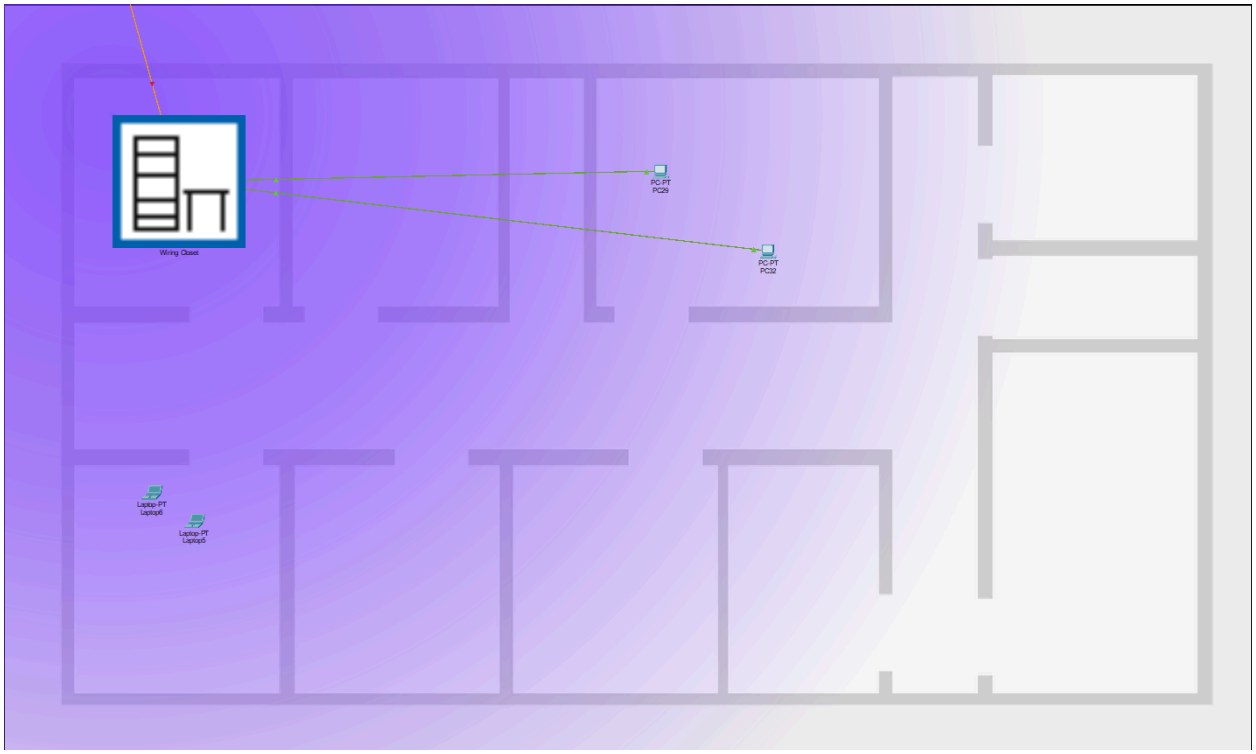


Figure 4.0.9 *Building 1 physical network topology*

The physical network topology of Building 1 supports 20 users and is connected to the Main Building through Ethernet cabling. A Layer 2/Layer 3 switch (Switch-Building1) is deployed to manage network traffic within the building. Access Points (APs) are installed in the lobby to provide wireless connectivity. User devices, including laptops and desktops, connect to the network via both wired and wireless interfaces.

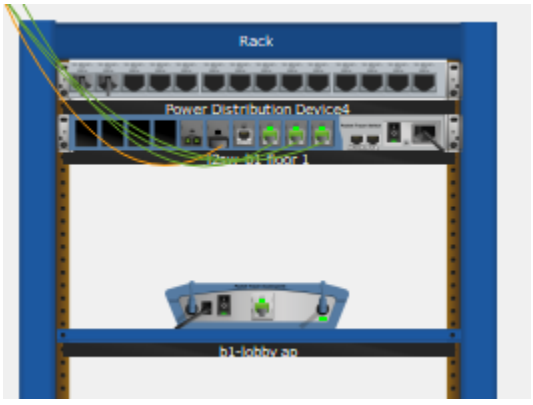


Figure 4.0.10 *Floor 1 wiring closet rack*

Figure 4.0.10 show the wiring closet on Floor 1 of Building 1 contains networking equipment includes a Layer 2 switch for Floor 1.

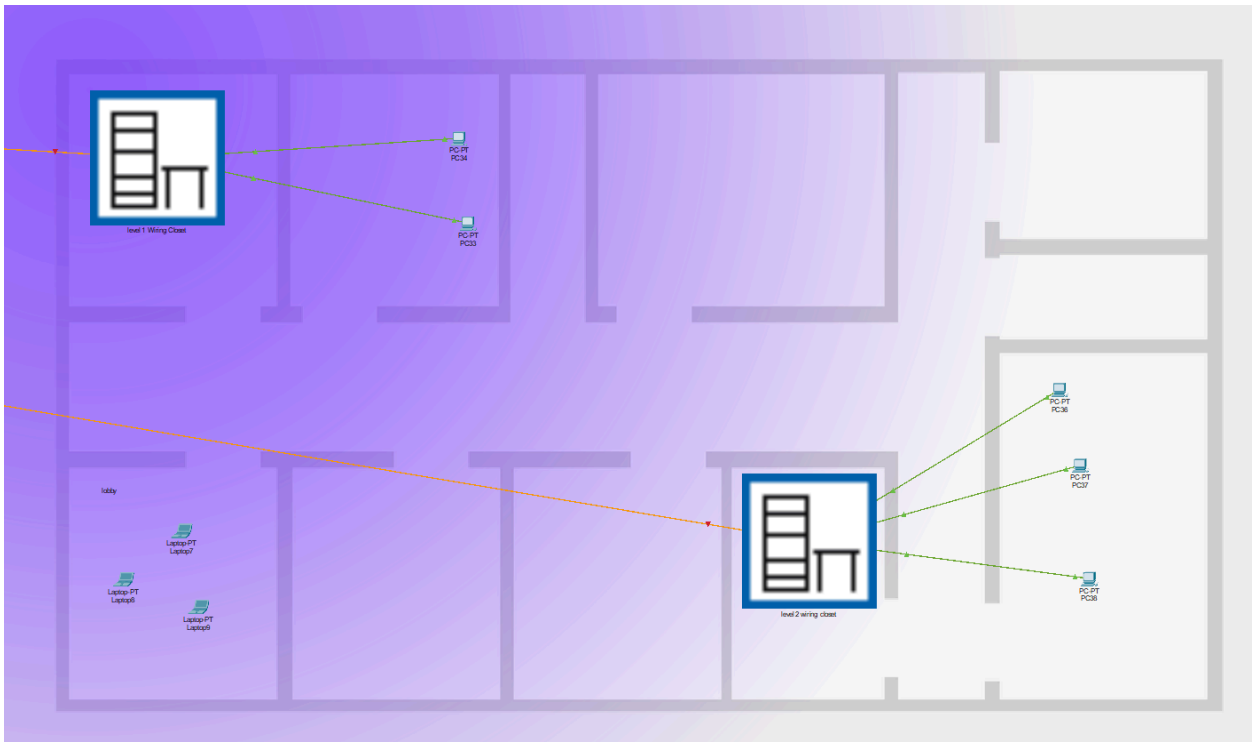


Figure 4.0.11 *Building 2 physical network topology*

Building 2's physical network topology supports 50 users and is connected to the Main Building via Ethernet cabling. Similar to Building 1, a Layer 2/Layer 3 switch (Switch-Building2) is deployed to handle network operations within the building. Access Points (APs) are installed in the lobby to provide wireless connectivity. User devices, including laptops and desktops, connect to the network through both wired and wireless connections.

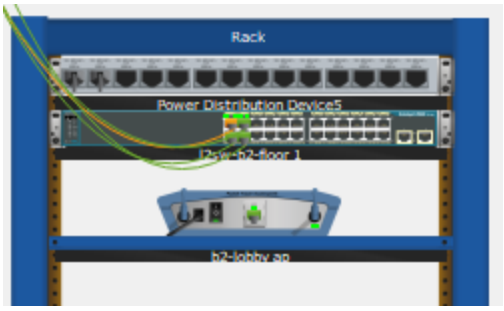


Figure 4.0.12 *Floor 1 wiring closet rack*

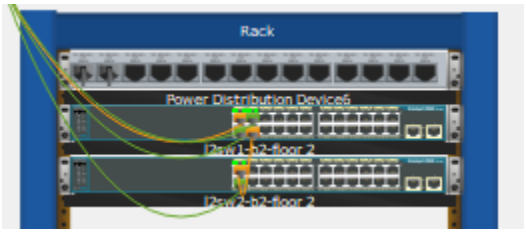


Figure 4.0.13 *Floor 2 wiring closet rack*

The wiring closet on Floor 1 and Floor 2 of Building 2 houses essential networking equipment that supports connectivity for that floor. Additionally, Floor 1 features an Access Point (AP) to provide wireless connectivity in the lobby area.

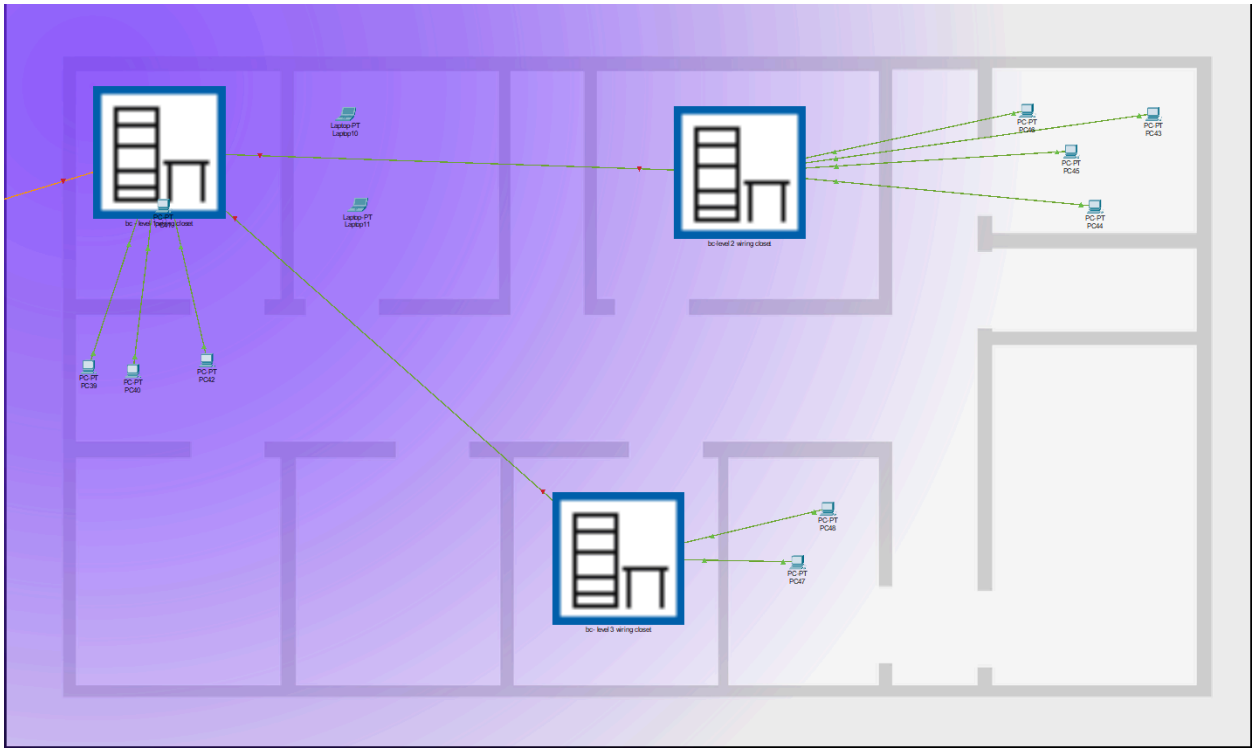


Figure 4.0.14 *Branch campus physical network topology*

The physical network topology of the branch campus, which is located 10 kilometers from the main campus, supports 100 users. At the core of the network is the Core-Switch-Branch, which manages connectivity within the branch campus. Access Points (APs) are installed in the lobby area to provide wireless network access. User devices, including laptops and desktops, connect to the network through both wired and wireless interfaces. The Router-Branch serves as the gateway, linking the branch campus to the main campus via a leased line or high-speed fiber optic connection.

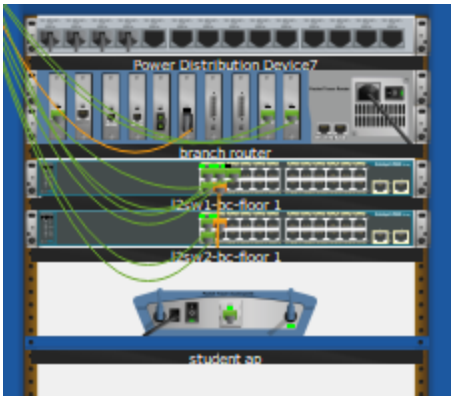


Figure 4.0.15 *Branch campus's First floor wiring room rack*

The wiring room on the first floor of the branch campus contains essential networking equipment that supports connectivity for the building. It includes a Layer 2 switch (Switch-Branch-Floor1) dedicated to managing network traffic on the first floor. An Access Point (AP) is also installed to provide wireless coverage in the area. Additionally, the branch router is housed in this room, serving as a critical component of the building's network by managing communication between the branch campus and the main campus, as well as routing traffic within the local network.

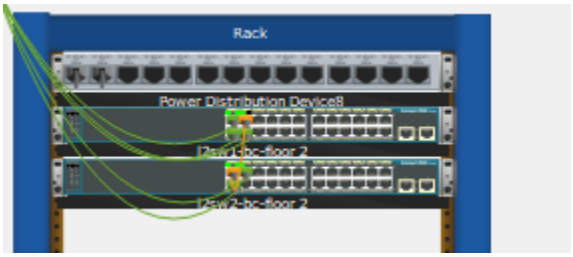


Figure 4.0.16 *Branch campus's second floor wiring room rack*

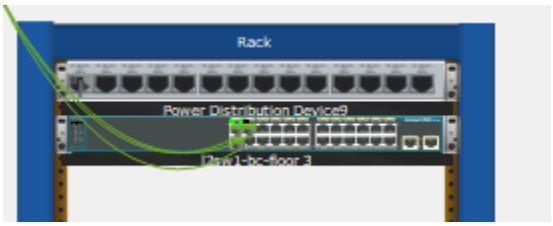


Figure 4.0.17 *Branch campus's third floor wiring room rack*

5.0 Logical network topology

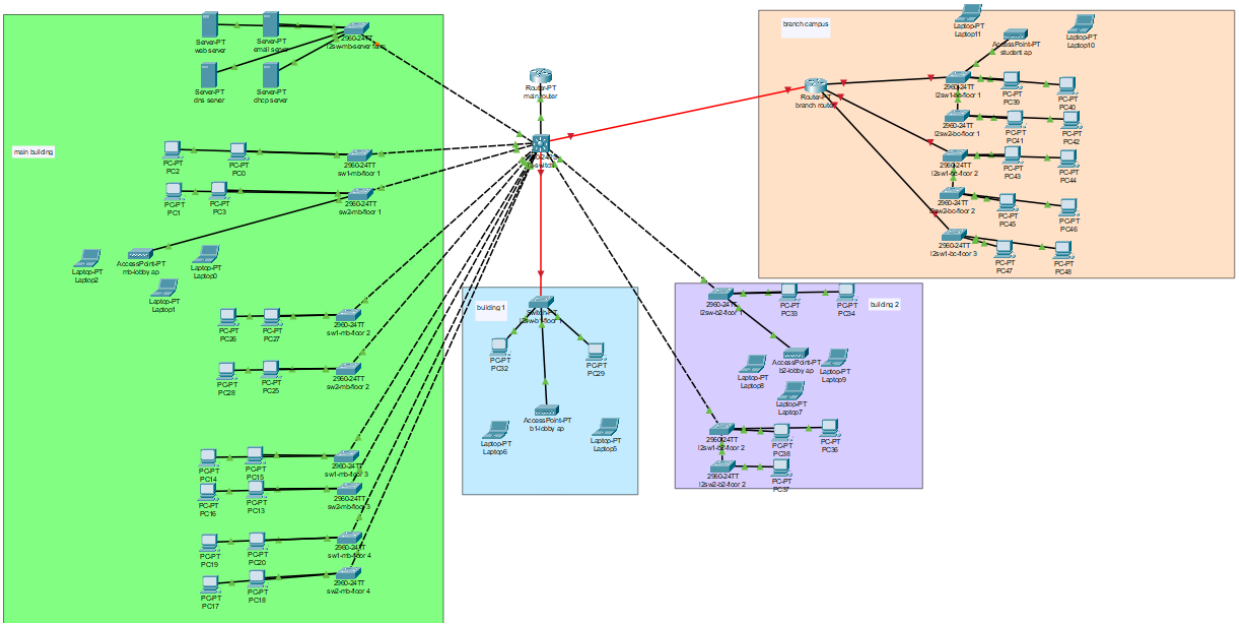


Figure 5.0.1 *Complete view of logical network topology simulated on CISCO packet tracer*

Device	Vlan	IP address	Subnet mask	Default gateway	DNS server
Main Building – User_VLAN (VLAN 10)					
PC1	10	199.40.40.2	255.255.255.0	199.40.40.1	199.40.41.2
PC2	10	199.40.40.3	255.255.255.0	199.40.40.1	199.40.41.2
...	...	...	...	...	...

PC60	10	199.40.40.62	255.255.255.0	199.40.40.1	199.40.41.2
Main Building – Lobby_WiFi_VLAN (VLAN 50)					
Laptop1	50	199.40.41.162	255.255.255.224	199.40.41.161	199.40.41.2
Laptop2	50	199.40.41.163	255.255.255.224	199.40.41.161	199.40.41.2
...	...	...	...	...	...
Laptop12	50	199.40.41.190	255.255.255.224	199.40.41.161	199.40.41.2
Main Building – Server_VLAN (VLAN 60)					
Web_Server	60	199.40.41.2	255.255.255.192	199.40.41.1	199.40.41.2
Email_Server	60	199.40.41.3	255.255.255.192	199.40.41.1	199.40.41.2
DNS_Server	60	199.40.41.4	255.255.255.192	199.40.41.1	199.40.41.2
DHCP_Server	60	199.40.41.5	255.255.255.192	199.40.41.1	199.40.41.2

Main Building – DMZ_VLAN (VLAN 100)					
FTP_Server	100	199.40.41.66	255.255.255.192	199.40.41.65	199.40.41.2

Device level ip table

The IP network design table outlines the logical addressing scheme used across the campus, ensuring efficient and secure communication between different network segments. Each VLAN is assigned a unique subnet from the provided 199.40.40.0/24 and 199.40.41.0/24 address space, with clearly defined ranges for user devices, wireless access, servers, and management traffic. Gateways are set to the first usable IP in each subnet and are configured on the Layer 3 switch to enable inter-VLAN routing. This structured approach supports scalability, simplifies troubleshooting, and allows for security policies such as ACLs and DMZ implementation.

6.0 IP network Design Table

Vlan	Network address	Subnet mask	First usable IP	Last usable IP	Number of usable IP
User_VLAN (Main Users)	199.40.40.0	255.255.255.0 (/24)	199.40.40.1	199.40.40.254	254
Lobby_WiFi_VLAN	199.40.41.160	255.255.225.224 (/27)	199.40.41.161	199.40.41.190	29
Server_VLAN (DNS/DHCP)	199.40.41.0	255.255.255.192 (/26)	199.40.41.1	199.40.41.62	62
DMZ_VLAN (Web/Email)	199.40.41.64	255.255.255.192 (/26)	199.40.41.65	199.40.41.126	61
Management_VLAN	199.40.41.128	255.255.225.240 (/28)	199.40.41.129	199.40.41.142	13

Table 5.1 IP network Design Table for Main building

Vlan	Network Address	Subnet Mask	First usable IP	Last usable IP	Number of usable IP
B1_VLAN (Users)	199.40.41.32	255.255.255.224	199.40.41.33	199.40.41.62	30
Lobby_WiFi_B1	199.40.41.64	255.255.255.192	199.40.41.65	199.40.41.126	62

Table 5.2 IP network Design Table for building 1

Vlan	Network Address	Subnet Mask	First usable IP	Last usable IP	Number of usable IP
B2_VLAN (Users)	199.40.41.96	255.255.255.192 (/27)	199.40.41.97	199.40.41.1126	29
Lobby_WiFi_B2	199.40.41.160	255.255.255.224 (/27)	199.40.41.161	199.40.41.190	30

Table 5.3 IP network Design Table for building 2

Vlan	Network Address	Subnet Mask	First usable IP	Last usable IP	Gateway
B_Campus_VLAN (Users)	199.40.41.192	255.255.255.128 (/25)	199.40.41.193	199.40.41.254	126
Lobby_WiFi_Branch	199.40.40.64	255.255.255.192 (/26)	199.40.40.65	199.40.40.126	62

Table 5.4 IP network Design Table for branch campus building

The IP addressing scheme used across all the buildings in the network design demonstrates an efficient application of Variable Length Subnet Masking (VLSM). VLSM allows for the allocation of different subnet sizes based on the specific needs of each VLAN, which helps maximize IP address utilization and reduce waste.

In the Main Building, the User_VLAN is assigned a /24 subnet (255.255.255.0), providing 254 usable IP addresses, which is suitable for supporting a large number of users. In contrast, the Lobby_WiFi_VLAN only requires a smaller subnet, so it uses a /27 mask (255.255.255.224), giving 29 usable IPs—just enough for public or guest access points in the lobby. The Server_VLAN and DMZ_VLAN are both assigned /26 subnets, allowing 62 and 61 usable IPs respectively, which accommodate multiple internal services (like DNS, DHCP, and web/email servers) while keeping them isolated for better security and management. The Management_VLAN, which likely supports a small number of administrative interfaces (such as switch or access point management), uses a much smaller /28 subnet with only 13 usable IPs.

In Building 1, a /27 subnet (255.255.255.224) is used for the user VLAN, offering 30 usable addresses, while a larger /26 subnet is allocated for Lobby WiFi, indicating a higher demand for guest or mobile connections there.

Similarly, Building 2 applies a /27 subnet to the user VLAN and again uses a /27 for the lobby WiFi. This shows consistent planning where lobby areas are given just enough IPs for their devices, while user VLANs are tailored to expected client counts.

In the Branch Campus, more users are expected, so a larger /25 subnet (255.255.255.128) is used for the main user VLAN, offering 126 usable IPs. For the Lobby WiFi, a /26 subnet provides 62 usable IPs, indicating moderate access needs.

Overall, VLSM enables the network designer to assign subnet sizes precisely based on demand—larger subnets for high-density user areas and smaller ones for management or public WiFi zones. This strategy preserves IP address space, supports scalability, improves routing efficiency, and ensures logical network segmentation for security and performance.

Vlan ID	Vlan name	User
10	User_VLAN	Internal staff/users
20	B1_VLAN	Building 1 users
30	B2_VLAN	Building 2 users
40	Branch_VLAN	Branch campus users
50	Lobby_WiFi_VLAN	Guest or wireless access
60	Server_VLAN	Internal servers (DNS, DHCP)
70	Management_VLan	Upper Management
100	DMZ_VLAN	Servers in demilitarized server (Web, Email)

Vlan ID classification

The VLAN configuration in the network design is strategically organized to provide logical segmentation, security, and manageability. Each VLAN serves a distinct purpose based on user roles and network functions. VLAN 10, named User_VLAN, is designated for internal staff and general users within the main building. By isolating user devices from other functions, it enhances performance and security within the main campus. VLAN 20 (B1_VLAN) and VLAN 30 (B2_VLAN) are assigned to users in Building 1 and Building 2, respectively. This separation allows location-based network management and prevents broadcast traffic from spreading unnecessarily between buildings.

VLAN 40 (Branch_VLAN) is used for users in the branch campus. As this site is geographically separated, having its own VLAN enables independent control while maintaining connectivity to the central infrastructure. VLAN 50 (Lobby_WiFi_VLAN) is dedicated to guest or public wireless access. Placing wireless users in a separate VLAN allows for tight access control and the implementation of security policies such as firewalls or bandwidth restrictions, ensuring guests cannot access internal resources.

For core network services, VLAN 60 (Server_VLAN) is reserved for internal servers like DNS and DHCP. This segregation protects essential services and facilitates better monitoring and maintenance. VLAN 70 (Management_VLAN) is used exclusively by network administrators or upper management to access network devices and perform administrative tasks. Limiting access to this VLAN safeguards critical configurations and

management interfaces. Lastly, VLAN 100 (DMZ_VLAN) is allocated for publicly accessible services such as web and email servers. The DMZ provides an additional layer of security by isolating these servers from the internal network, reducing the risk of external attacks affecting internal resources. Overall, this VLAN setup demonstrates the use of logical network segmentation through VLSM and security zoning to build an efficient, scalable, and secure network.

7.0 Network Configuration

In this segment, the methods of configuring each device in each building to connect it into a network will be shown.

7.1 Main building configuration

Main router

Erase router's initial configurations	Router>enable Router#erase startup-config Router#reload
Disable DNS lookup to prevent the router form attempting to translate incorrectly entered commands as though they were host names	Router(config) #no ip domain-lookup
Assign class as the privileged EXEC encrypted password	Router(config) #enable secret class
Assign cisco as the console password and enable login	Router(config)#line console 0 Router(config-line)#password cisco

Layer 3 switch

Naming virtual interface and separating it by function	Switch(config)# vlan 10 Switch(config-vlan)# name User_VLAN Switch(config)# vlan 50 Switch(config-vlan)# name Lobby_WiFi_VLAN Switch(config)# vlan 60 Switch(config-vlan)# name Server_VLAN Switch(config)# vlan 100 Switch(config-vlan)# name DMZ_VLAN Switch(config)# vlan 70 Switch(config-vlan)# name Management_VLAN
Assign each vlan with IP addresses which act as gateway	interface vlan 10 ip address 199.40.40.1 255.255.255.0

	no shutdown interface vlan 50 ip address 199.40.41.161 255.255.255.224 no shutdown interface vlan 60 ip address 199.40.41.1 255.255.255.192 no shutdown interface vlan 100 ip address 199.40.41.65 255.255.255.192 no shutdown interface vlan 70 ip address 199.40.41.129 255.255.255.128 no shutdown
Allow for more than 1 vlan to be able to be accessed through each port	interface gigabitEthernet1/0/1 switchport mode trunk no shutdown interface gigabitEthernet1/0/2 switchport mode trunk no shutdown interface gigabitEthernet1/0/3 switchport mode trunk no shutdown interface gigabitEthernet1/0/4 switchport mode trunk no shutdown interface gigabitEthernet1/0/5 switchport mode trunk no shutdown interface gigabitEthernet1/0/6 switchport mode trunk no shutdown interface gigabitEthernet1/0/7

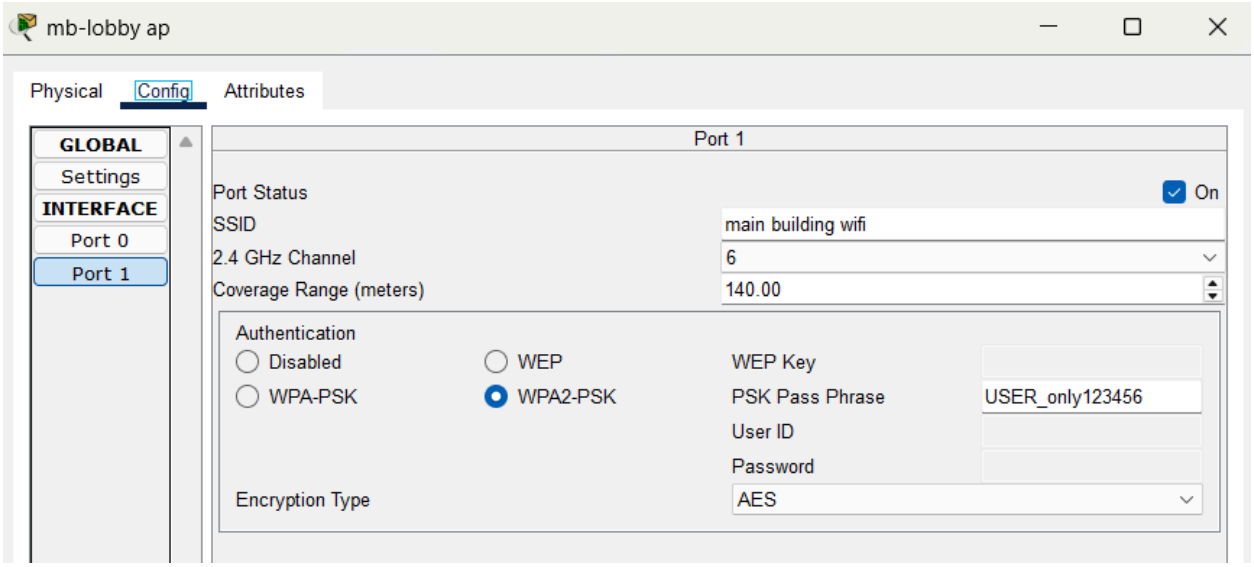
	switchport mode trunk no shutdown interface gigabitEthernet1/0/8 switchport mode trunk no shutdown
Enable inter-Vlan routing	Ip routing

```
Device Name: l3-switch
Device Model: 3650-24PS
Hostname: Switch

Port                  Link   VLAN   IP Address         IPv6 Address                              MAC Address
GigabitEthernet1/0/1  Up     1      <not set>          <not set>                                 0003.E4DB.4701
GigabitEthernet1/0/2  Up     --     <not set>          <not set>                                 0003.E4DB.4702
GigabitEthernet1/0/3  Up     --     <not set>          <not set>                                 0003.E4DB.4703
GigabitEthernet1/0/4  Up     --     <not set>          <not set>                                 0003.E4DB.4704
GigabitEthernet1/0/5  Up     --     <not set>          <not set>                                 0003.E4DB.4705
GigabitEthernet1/0/6  Up     1      <not set>          <not set>                                 0003.E4DB.4706
GigabitEthernet1/0/7  Up     1      <not set>          <not set>                                 0003.E4DB.4707
GigabitEthernet1/0/8  Up     --     <not set>          <not set>                                 0003.E4DB.4708
GigabitEthernet1/0/9  Up     --     <not set>          <not set>                                 0003.E4DB.4709
GigabitEthernet1/0/10 Up     --     <not set>          <not set>                                 0003.E4DB.470A
GigabitEthernet1/0/11 Up     --     <not set>          <not set>                                 0003.E4DB.470B
GigabitEthernet1/0/12 Up     --     <not set>          <not set>                                 0003.E4DB.470C
GigabitEthernet1/0/13 Down   1      <not set>          <not set>                                 0003.E4DB.470D
GigabitEthernet1/0/14 Down   1      <not set>          <not set>                                 0003.E4DB.470E
GigabitEthernet1/0/15 Down   1      <not set>          <not set>                                 0003.E4DB.470F
GigabitEthernet1/0/16 Down   1      <not set>          <not set>                                 0003.E4DB.4710
GigabitEthernet1/0/17 Down   1      <not set>          <not set>                                 0003.E4DB.4711
GigabitEthernet1/0/18 Down   1      <not set>          <not set>                                 0003.E4DB.4712
GigabitEthernet1/0/19 Down   1      <not set>          <not set>                                 0003.E4DB.4713
GigabitEthernet1/0/20 Down   1      <not set>          <not set>                                 0003.E4DB.4714
GigabitEthernet1/0/21 Down   1      <not set>          <not set>                                 0003.E4DB.4715
GigabitEthernet1/0/22 Down   1      <not set>          <not set>                                 0003.E4DB.4716
GigabitEthernet1/0/23 Down   1      <not set>          <not set>                                 0003.E4DB.4717
GigabitEthernet1/0/24 Down   1      <not set>          <not set>                                 0003.E4DB.4718
GigabitEthernet1/1/1  Down   1      <not set>          <not set>                                 00D0.97CC.CE01
GigabitEthernet1/1/2  Down   1      <not set>          <not set>                                 00D0.97CC.CE02
GigabitEthernet1/1/3  Down   1      <not set>          <not set>                                 00D0.97CC.CE03
GigabitEthernet1/1/4  Down   1      <not set>          <not set>                                 00D0.97CC.CE04
Vlan1                 Down   1      <not set>          <not set>                                 0030.A349.AC08
Vlan10                Up     10     199.40.40.1/24     <not set>                                 0030.A349.AC01
Vlan50                Up     50     199.40.41.161/27   <not set>                                 0030.A349.AC02
Vlan60                Up     60     199.40.41.1/26     <not set>                                 0030.A349.AC03
Vlan70                Up     70     199.40.41.129/28   <not set>                                 0030.A349.AC04
Vlan100               Up     100    199.40.41.65/26    <not set>                                 0030.A349.AC05

Physical Location: Intercity > Home City > main building > Main Wiring Closet > Rack > l3-switch
```

The Layer 3 switch (L3 switch) is configured to handle inter-VLAN routing and trunking between Layer 2 switches. It uses SVIs (Switched Virtual Interfaces) as gateways for each VLAN, ensuring proper communication between users, Wi-Fi clients, servers, management devices, and public-facing services. Trunk ports (GigabitEthernet1/0/1 and GigabitEthernet1/0/2) carry multiple VLANs, while access ports are assigned to specific VLANs based on their function. This design ensures efficient routing, security, and scalability for the campus network.

Layer 2 switch

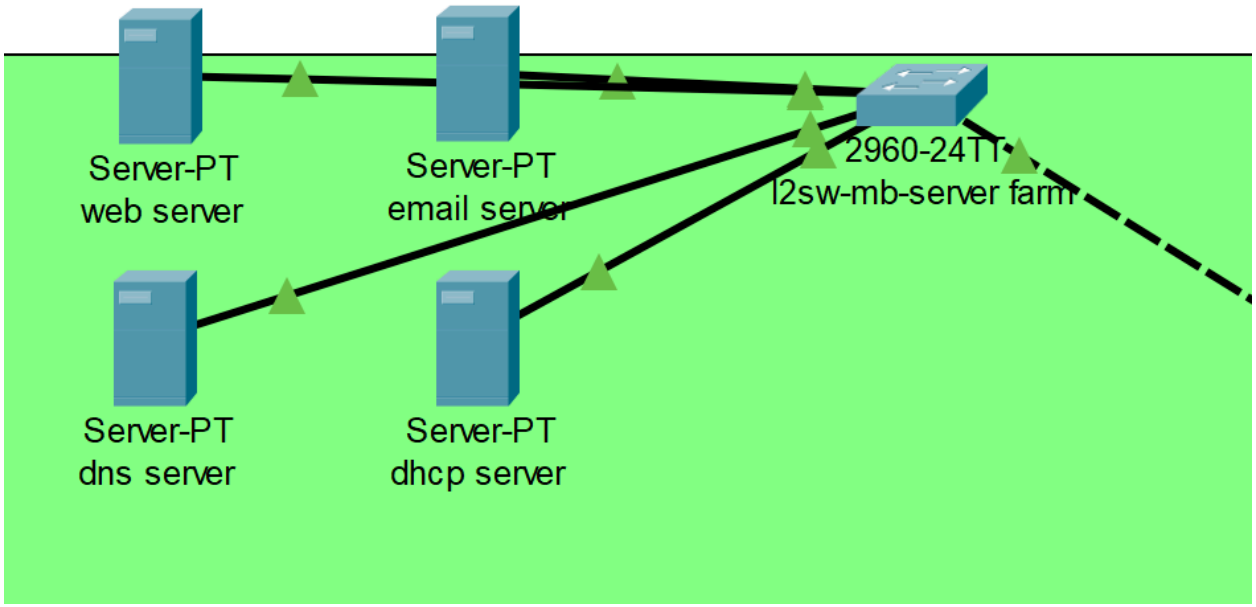
Create VLan in layer 2 switches	Switch> enable Switch# configure terminal vlan 10 name User_VLAN
Assign all user connected through all port in switches in the first floor into the User_VLan	interface range fa0/1 - 23 switchport mode access switchport access vlan 10
Assign all user connected to the network via lobby access point to into the wifi_VLan	interface fa0/24 switchport mode access switchport access vlan 50
Allow all port to be in trunk mode to be able to access multiple vlan type	interface fa0/24 switchport mode trunk



Main lobby access point configuration

As WPA2-PSK authentication is enabled along with PSK Pass Phrase, the access to the wireless access point in the main building's lobby is only granted to authorized users.

Server Farm



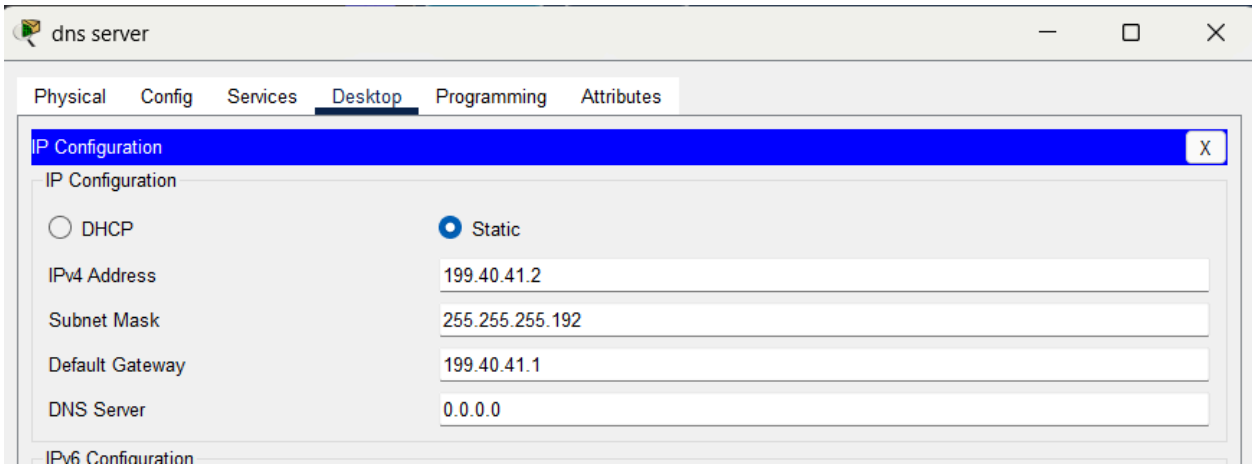
Server farm located in the main building

Create and assign Server_VLan for dns server and dhcp server	Switch> enable Switch# configure terminal vlan 60 name Server_VLAN interface range fa0/3 - 4 switchport mode access switchport access vlan 60
Create and assign DMZ_VLan for email and web server	Switch> enable Switch# configure terminal vlan 100 name DMZ_VLan interface range fa0/1 - 2 switchport mode access switchport access vlan 100
Enable switches port tot transport multiple vlan	 interface fa0/24 switchport mode trunk

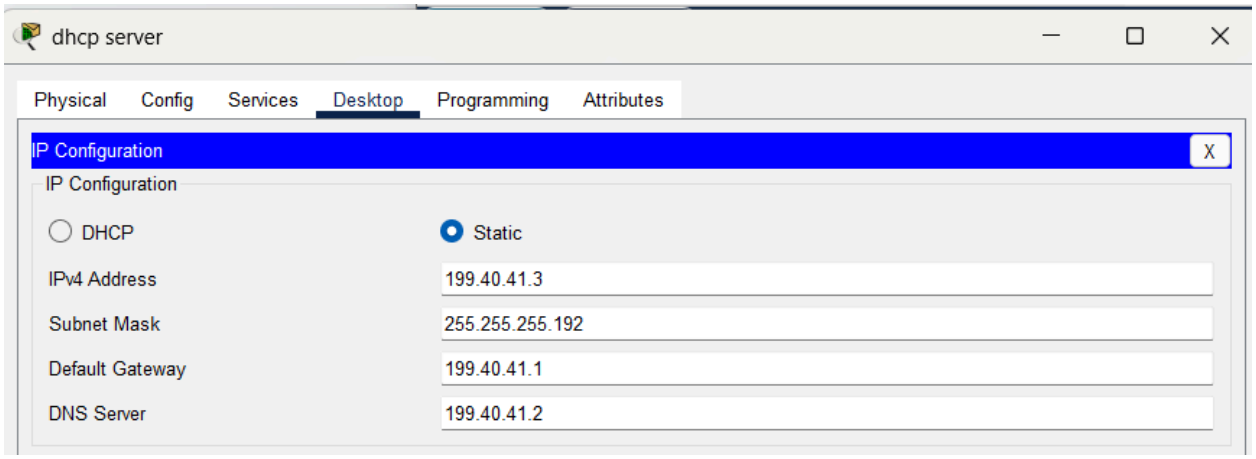
Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Up	100	--	0001.C774.9601
FastEthernet0/2	Up	100	--	0001.C774.9602
FastEthernet0/3	Up	60	--	0001.C774.9603
FastEthernet0/4	Up	60	--	0001.C774.9604
FastEthernet0/5	Down	1	--	0001.C774.9605
FastEthernet0/6	Down	1	--	0001.C774.9606
FastEthernet0/7	Down	1	--	0001.C774.9607
FastEthernet0/8	Down	1	--	0001.C774.9608
FastEthernet0/9	Down	1	--	0001.C774.9609
FastEthernet0/10	Down	1	--	0001.C774.960A
FastEthernet0/11	Down	1	--	0001.C774.960B
FastEthernet0/12	Down	1	--	0001.C774.960C
FastEthernet0/13	Down	1	--	0001.C774.960D
FastEthernet0/14	Down	1	--	0001.C774.960E
FastEthernet0/15	Down	1	--	0001.C774.960F
FastEthernet0/16	Down	1	--	0001.C774.9610
FastEthernet0/17	Down	1	--	0001.C774.9611
FastEthernet0/18	Down	1	--	0001.C774.9612
FastEthernet0/19	Down	1	--	0001.C774.9613
FastEthernet0/20	Down	1	--	0001.C774.9614
FastEthernet0/21	Down	1	--	0001.C774.9615
FastEthernet0/22	Down	1	--	0001.C774.9616
FastEthernet0/23	Down	1	--	0001.C774.9617
FastEthernet0/24	Down	--	--	0001.C774.9618
GigabitEthernet0/1	Up	--	--	0001.C774.9619
GigabitEthernet0/2	Down	1	--	0001.C774.961A
Vlan1	Down	1	<not set>	0090.2198.E240
Vlan60	Up	60	199.40.41.1/26	0090.2198.E202
Vlan100	Up	100	199.40.41.65/26	0090.2198.E201

Internal network

DNS and DHCP servers should generally remain in the internal trusted network for security reasons. The DNS server may have a public-facing component (e.g., for authoritative DNS records) hosted in the DMZ or with a third-party provider, while internal DNS resolution stays behind the firewall. The DHCP server, which assigns IP addresses to internal devices, should always reside in the secure internal network to prevent unauthorized access.



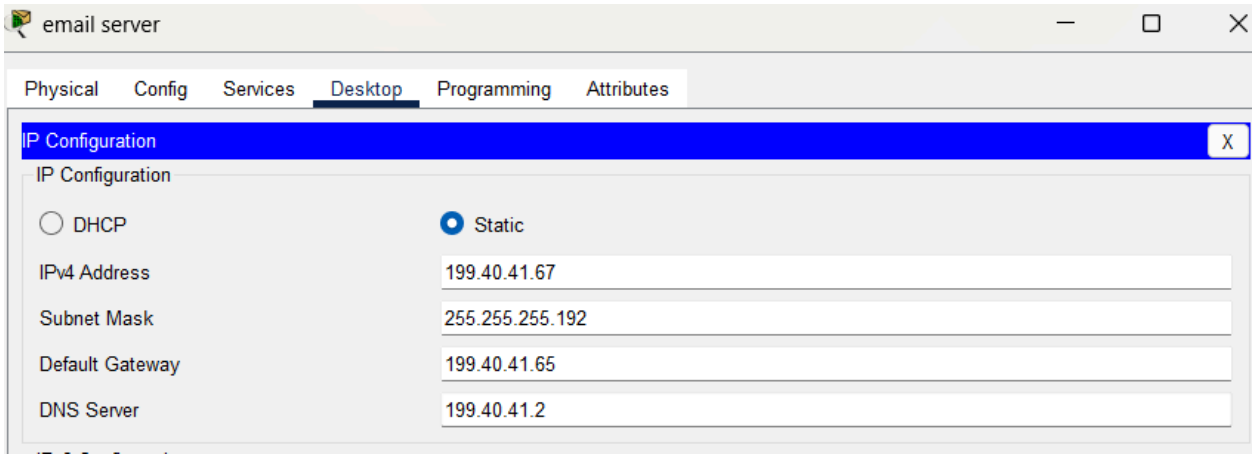
DNS server ip configuration



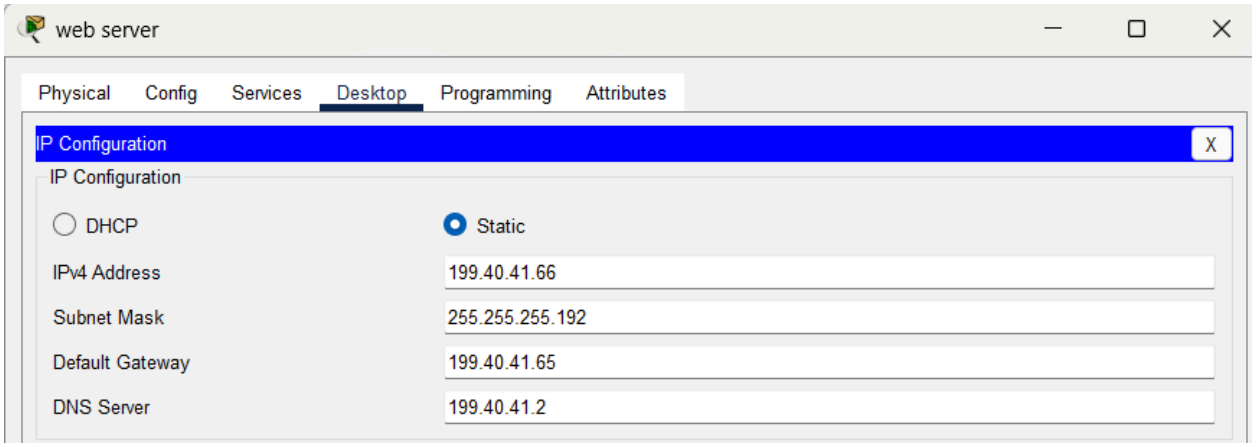
DHCP server ip configuration

Demilitarized zone

A Demilitarized Zone (DMZ) was implemented to securely host public-facing services such as the Web_Server and Email_Server . The DMZ acts as an isolated network segment, separating these servers from the internal network to prevent direct access to sensitive resources like the DNS and DHCP servers. By placing the Web and Email servers in VLAN 100 (DMZ_VLAN) with a dedicated subnet 199.40.41.64 /26, external users and guests can access these services while being restricted from reaching internal systems. An Access Control List (ACL) was applied to further secure the DMZ by allowing only specific traffic (such as HTTP, HTTPS, and SMTP) into this zone, ensuring both availability and security of critical services. This design mirrors real-world enterprise practices and earned bonus marks for advanced network configuration.



Email server ip configuration



Web server ip configuration

Access control list

```
Switch(config)#access-list 101 permit tcp any host 199.40.41.66 eq www
Switch(config)#access-list 101 permit tcp any host 199.40.41.66 eq 443
Switch(config)#access-list 101 permit tcp any host 199.40.41.67 eq smtp

Switch(config)#access-list 101 deny ip any 199.40.41.64 0.0.0.63
Switch(config)#access-list 101 permit ip any any
Switch(config)#access-list 101 remark Allow HTTP to Web Server
Switch(config)#access-list 101 remark Allow HTTPS to Web Server
Switch(config)#access-list 101 remark Allow SMTP to Email Server
Switch(config)#access-list 101 remark Deny all other traffic to DMZ
Switch(config)#access-list 101 remark Allow all other traffic
Switch(config)#
Switch(config)#interface vlan 100
Switch(config-if)#ip access-group 101 in
```

Access Control List Configuration

To enhance security in the network design, an extended Access Control List (ACL) was implemented on the Layer 3 switch to control traffic entering the DMZ_VLAN

(VLAN 100), which hosts the public-facing servers, specifically the Web Server and Email Server. The ACL ensures that only necessary services are accessible from external or unauthorized networks, while all other traffic is restricted.

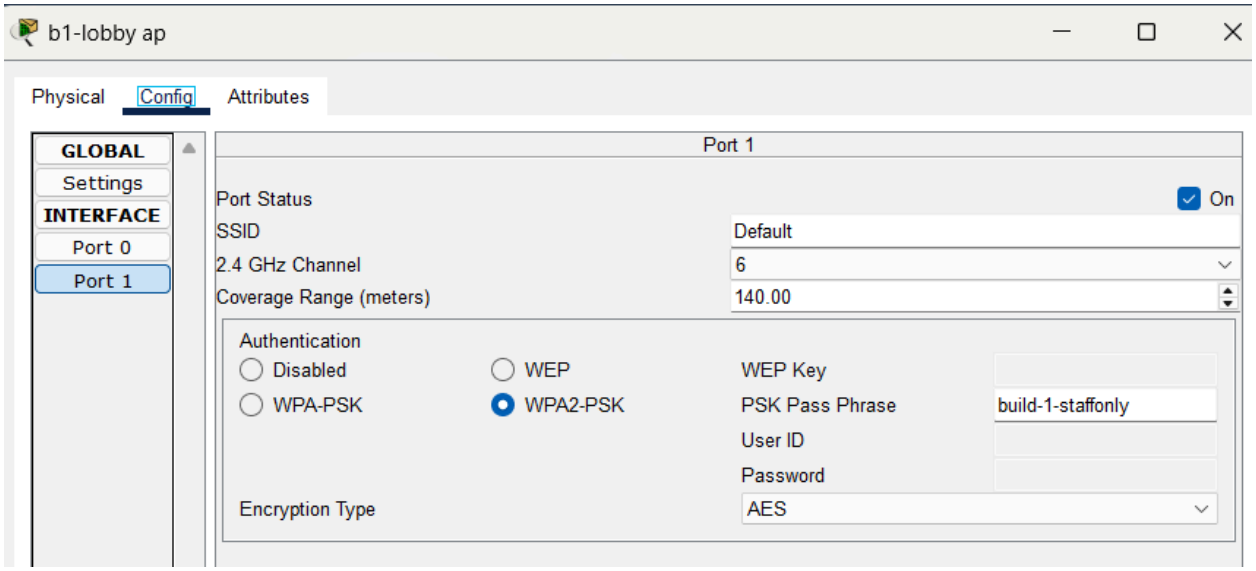
In this setup, the keyword any allows traffic from any source IP address, making it flexible for users inside and outside the campus to access these services. The host 199.40.41.66 refers to the Web Server, and access to it is permitted via TCP port www (port 80) for HTTP and port 443 for HTTPS traffic. Similarly, the Email Server (199.40.41.67) is allowed to receive SMTP traffic (port 25) from any source. All other types of traffic targeting the DMZ_VLAN were explicitly denied using a deny statement with the network range 199.40.41.64 0.0.0.63, which covers all usable IPs in the DMZ subnet. A final permit ip any any statement was added to allow unrestricted outbound traffic from the DMZ to internal networks or the internet, ensuring normal communication is maintained while inbound access remains tightly controlled.

7.2 Building 1 configuration

Layer 2 switch

Create VLANs	Switch(config)# vlan 20 Switch(config-vlan)# name B1_User_VLAN, Switch(config-vlan)#interface vlan 20 Switch(config-vlan-if) ip address 199.40.41.33 Switch(config)# vlan 50 Switch(config-vlan)# name B1_Lobby_WiFi_VLAN
Assign all user-connected ports to User_VLAN	interface range fa0/1 - 20, switchport mode access, s switchport access vlan 20
Assign wireless AP port to WiFi_VLAN	interface fa0/21, switchport mode access, switchport access vlan 50
Configure trunk port to connect back to Main Campus	interface fa0/24, switchport mode trunk

```
Device Name: l2sw-b1-floor 1
Device Model: Switch-PT
Hostname: Switch

Port              Link   VLAN   IP Address         MAC Address
FastEthernet0/1   Up     1      --                 00D0.D39E.BEB8
FastEthernet1/1   Up     1      --                 0001.C7E3.D3D8
FastEthernet2/1   Up     1      --                 0030.A323.1171
FastEthernet3/1   Down   1      --                 0030.F2A2.8492
FastEthernet4/1   Down   1      --                 0060.5C28.35E8
FastEthernet5/1   Down   1      --                 0060.3EEE.7160
Vlan1             Down   1      <not set>          0030.A3AE.1185
Vlan20            Up     20     199.40.41.33/27    0030.A3AE.1101
```



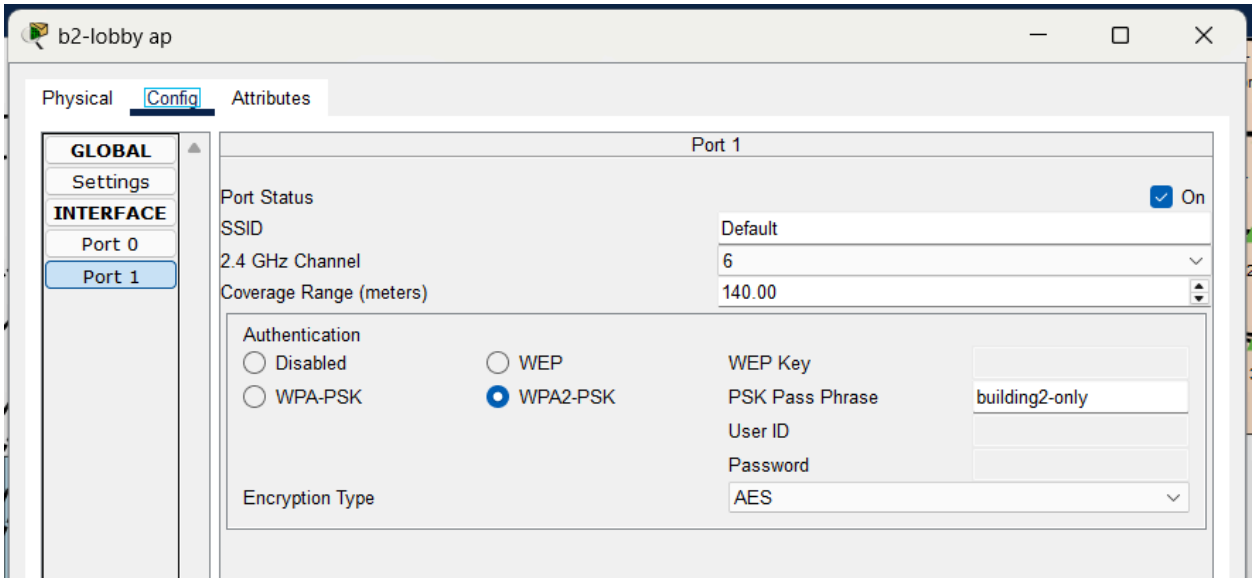
Building 1 wireless access point configuration

7.3 Building 2

Layer 2 switch

Create and assign user connected directly wired port to B2_user_VLAN	Switch> enable Switch# configure terminal ! Create VLANs vlan 30 name B2_User_VLAN

	interface range fa0/1 - 20 switchport mode access switchport access vlan 30
Create and assign user connected through wireless access point to wifi_VLan	vlan 50 name WiFi_VLAN interface fa0/21 switchport mode access switchport access vlan 50
Allow port to carry multiple vlan	interface fa0/24 switchport mode trunk
Enable and apply access list restriction to guest using wireless access point	access-list 102 remark Allow FTP to internal server access-list 102 permit tcp any host 199.40.41.5 eq ftp access-list 102 remark Deny all other traffic to LAN access-list 102 deny ip any 199.40.40.0 0.0.0.255 access-list 102 deny ip any 199.40.41.0 0.0.0.63 access-list 102 deny ip any 199.40.41.64 0.0.0.63 interface vlan 50 ip access-group 102 in



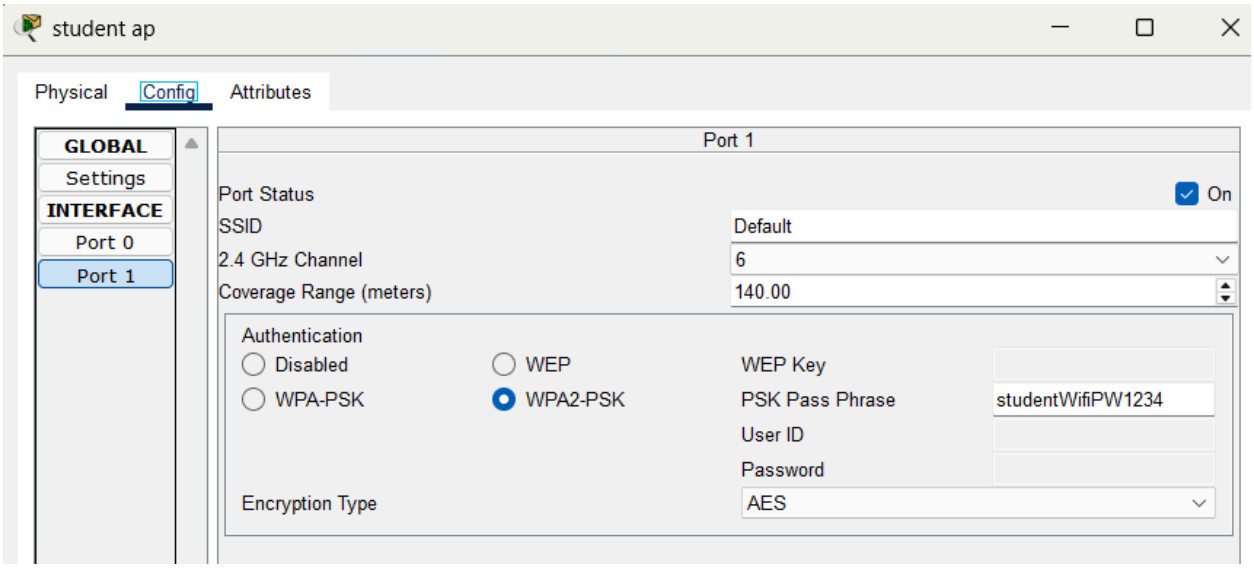
Wireless access point configuration for building 2's lobby

Branch Campus
Router

Enable configuration and Set hostname	Router> enable Router# configure terminal hostname Branch_Router
Disable DNS lookup	no ip domain-lookup
Set encrypted privileged EXEC	password enable secret class

Layer 2 switch

Create and assign user into Branch_User_VLanon	Switch> enable Switch# configure terminal vlan 40 name Branch_User_VLAN vlan 50 name WiFi_VLAN interface range fa0/1 - 20 switchport mode access switchport access vlan 40
Assign user connected through access point into wifi_VLan	interface fa0/21 switchport mode access switchport access vlan 50
Allow port to carry multiple vlan	interface fa0/24 switchport mode trunk

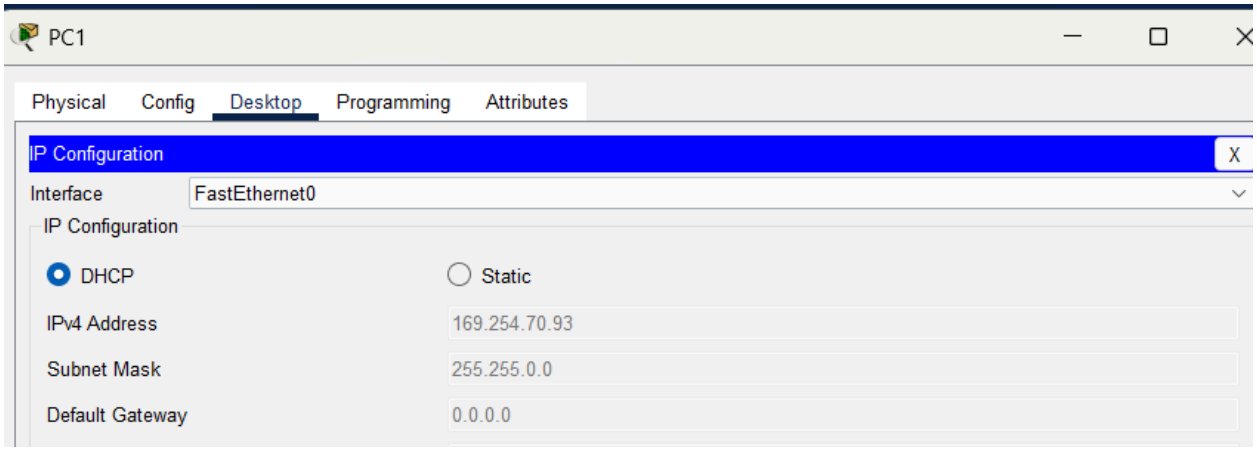


Branch campus wireless access point configuration

8.0 Network testing and verification

```
C:\>ping 199.40.40.26

Pinging 199.40.40.26 with 32 bytes of data:

Reply from 199.40.40.26: bytes=32 time<1ms TTL=128
Reply from 199.40.40.26: bytes=32 time<1ms TTL=128
Reply from 199.40.40.26: bytes=32 time<1ms TTL=128
Reply from 199.40.40.26: bytes=32 time<1ms TTL=128

Ping statistics for 199.40.40.26:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Successful connection from main building



Successful dhcp IP assignment

9.0 Bill of Materials

Item	Qty	Model / Brand	Unit Price (MYR)	Total (MYR)
Core Routers	2	Cisco ISR 4331	4800	9600
Access Switches (24-port)	10	Cisco Catalyst 2960-X	1500	15000
Wireless Access Points (APs)	5	Cisco Aironet 1832i	600	3000
Wireless Controller	1	Cisco 3504 WLC	1050	1050
Firewall	1	Cisco ASA 5506-X	2541	2541
Server Hardware (Rackmount)	1	Dell PowerEdge R640	4362	4362
Fiber Modules & Transceivers	6	Cisco GLC-LH-SM	880	5280
Patch Panels + Cat6 Cabling	1	Legrand/Panduit	17131	17131
UPS (Uninterruptible Power Supply)	3	APC Smart-UPS 1500VA	2800	8400
Network Rack + Cooling	2	42U Rack with fans	4999	9998

Windows Server Licenses	4	Windows Server 2022 Standard	20	80
Endpoint Security (Antivirus)	230	Microsoft Defender (Business Plan)	$2.4 per user per month	6624 annually
Network Monitoring Software	1	PRTG 2500 sensors	$675 per month	8100 annually
Multilayer Switch	1	Cisco Catalyst 3560-24PS-S	13899	13899

The details of each material are as follows:

Cisco ISR 4331

Cisco Catalyst 2960-X

Cisco Access Point AIR-AP1832I-K-K9 (Refurbished)

Price	RM600.00 ~~RM4,862.00~~
Product SKU	AIR-AP1832I-K-K9
Brand	Cisco
Size (L x W x H)	24 cm x 24 cm x 8 cm
Availability	8

Cisco Aironet 1832i

Cisco AIR-CT2504-K9 (Refurbished)

Price	RM1,050.00 ~~RM5,520.00~~
Product SKU	AIR-CT2504-K9
Brand	Cisco
Size (L x W x H)	23 cm x 30 cm x 7.5 cm
Availability	1

Cisco 3504 WLC

Cisco Asa 5506-x Firewall With Control License Asa5506-k9 12vdc 5a

Product SKU: 149343
Available: Only 1 item in stock
Condition: New

ADD TO WISHLIST

$599.57

Cisco ASA 5506-X

(Refurbished) Dell PowerEdge R640 Rack Server (XS4110.32GB.240GB)

Model : Dell PowerEdge R640 Rack Server
Processor: 1 x Intel Xeon Silver 4110 Processor
Memory: 1 x 32GB RAM
HDD: 1 x 240GB SSD
RAID Controller: Dell PowerEdge RAID Controller H330
Power Supply:1 x 750W
Warranty: 1 year Parts warranty

Part Number: R640-XS4110

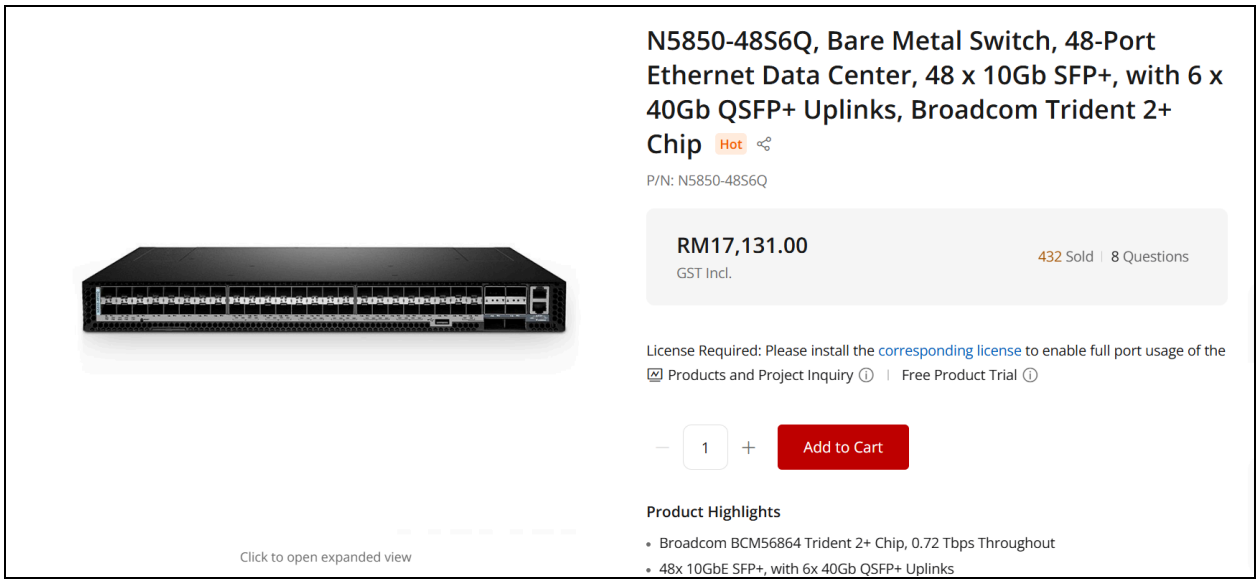
RM 4,361.50

Dell PowerEdge R640

Cisco GLC-LH-SMD (Refurbished)

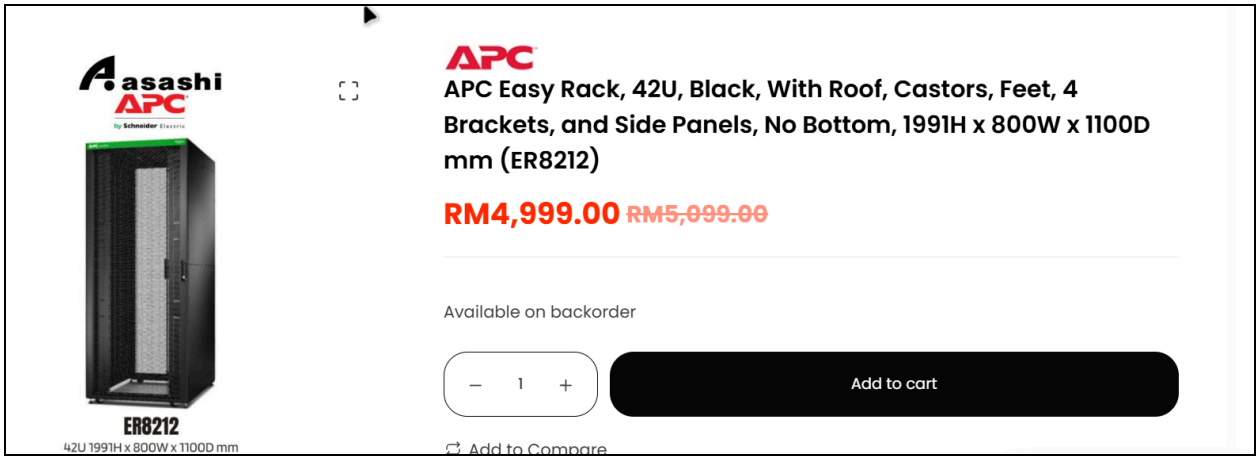
Price	RM880.00 ~~RM5,454.45~~
Product SKU	GLC-LH-SMD (Cisco)
Brand	Cisco
Size (L x W x H)	12.1 cm x 7 cm x 3.1 cm
Availability	4

Cisco GLC-LH-SM

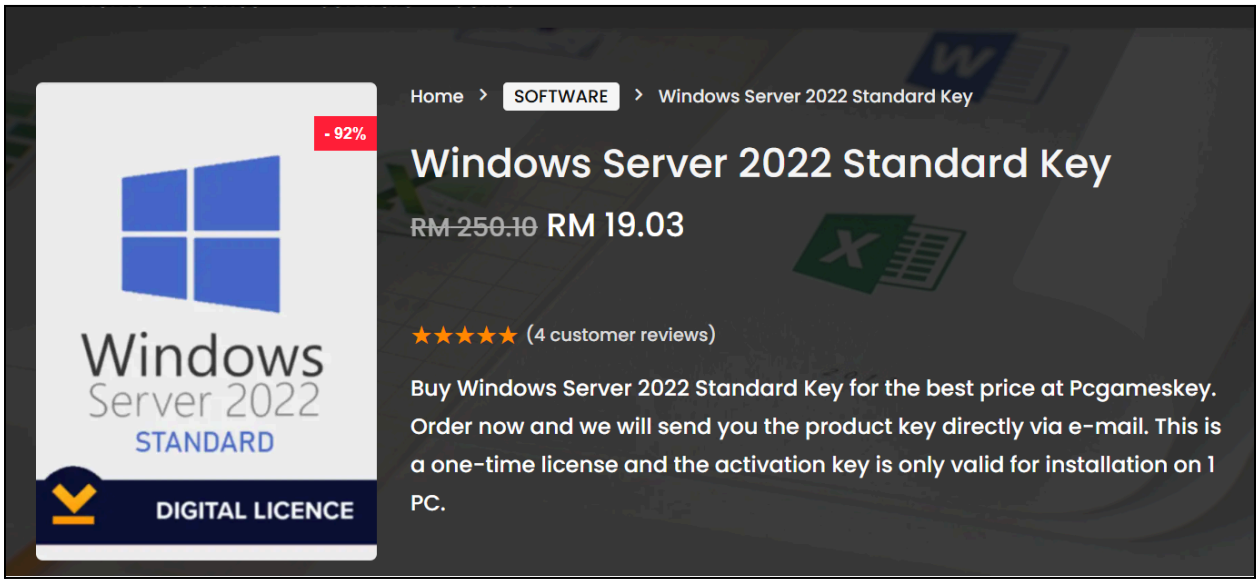


Legrand/Panduit

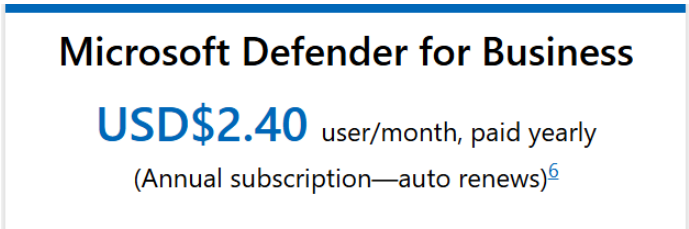
APC Smart-UPS 1500VA



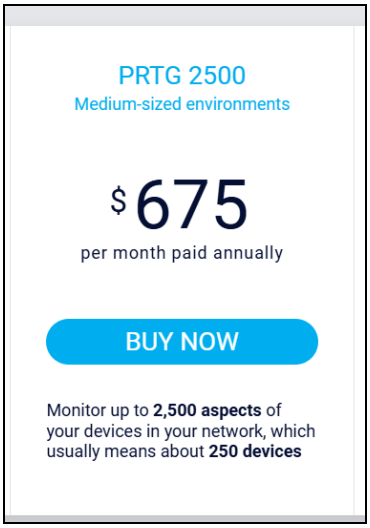
42U Rack with fans



Windows Server 2022 Standard



Microsoft Defender (Business Plan)



PRTG 2500 sensors

Cisco Catalyst 3560-24PS-S

Categorization of Estimated Budget :

1. Network Hardware

Includes:

- Core Routers: RM 9,600
- Access Switches: RM 15,000
- Wireless APs: RM 3,000

- Wireless Controller: RM 1,050
- Firewall: RM 2,541
- Fiber Modules & Transceivers: RM 5,280
- Network Rack + Cooling: RM 9,998
- Multilayer Switch: RM 13899

Total: RM 60,368

---

2. Server Infrastructure

Includes:

- Server Hardware (Dell R640): RM 4,362
- UPS (3x APC Smart-UPS): RM 8,400

Total: RM 12,762

---

3. Software & Licensing

Includes:

- Windows Server Licenses: RM 80
- Endpoint Security (Microsoft Defender): RM 6,624 annually
- Network Monitoring (PRTG): RM 8,100 annually

Total: RM 14,804

---

4. Cabling & Installation

Includes:

- Patch Panels + Cat6 Cabling (Legrand/Panduit): RM 17,131

Total: RM 17,131

---

5. Accessories

- Rack + Cooling: RM 9,998

Total: RM 9,998

---

6. Security & Monitoring

Already included under **Software & Licensing**, but broken out for clarity:

- Firewall (ASA 5506-X): RM 2,541
- Antivirus (Defender): RM 6,624
- Monitoring (PRTG): RM 8,100

Total: RM 17,265

Gross Total: ~ RM 178,797