UNIVERSITI KUALA LUMPUR
ASSESSMENT BRIEF

COURSE DETAILS	
INSTITUTE	UniKL BRITISH MALAYSIAN INSTITUTE
COURSE NAME	WIRELESS NETWORK ARCHITECTURE
COURSE CODE	BTB37303
COURSE LEADER	MOHD RAZIFF ABD RAZAK
LECTURER	MOHD RAZIFF ABD RAZAK
SEMESTER & YEAR	OCTOBER 2025

ASSESSMENT DETAILS	
TITLE/NAME	Lab 2
WEIGHTING	20%
DATE/DEADLINE	14/12/2025, 11.00PM
COURSE LEARNING OUTCOME(S)	CLO 4: **Prepare** wireless network design and documentation. (A4, PLO8)
INSTRUCTIONS	Perform the following tasks: 1. Submit the **individual report** as instructed by Course Lecturer. 2. All answers must be in English language only. 3. Submission of report through eLearning.

Student Name:	**ID:**	**Group:**
AHMAD NAFIS BIN MOHD ZULKIFLI	51224125264	L01
Assessor's Comment:		**Marks:**

Verified by: Course Leader [MRAR] **Prepared by: [MRAR]**	**QSC format verification**	**PC/HOS content validation**
I hereby declare that all my team members have agreed with this assessment. All team members are certain that this assessment complies with the Course Syllabus. Signature: _____ Date : 6 / 11 /2025	QUALITY ASSURANCE ACADEMIC 10 NOV 2025 VERIFIED	Dr. Nor Khairiah Ibrahim Head of Section Communication Technology 10/11/2025

TASK NO	CLO	MARKING SCHEME	MARKS
1	4	Physical Topology Design	*5*
1	4	Logical Topology Design	*5*
2	4	Network Configuration and Installation	*30*
3	4	Report Format	*10*
3	4	Introduction	*10*
3	4	Discussion	*10*
3	4	Conclusion	*10*
4		Video / Demo	*20*
		TOTAL	**100**

BTB37303 WIRELESS NETWORK ARCHITECTURE

LAB 2: IMPLEMENTATION OF AN SDN-BASED WIRELESS NETWORK USING LIGHTWEIGHT ACCESS POINTS

LECTURER: MR MOHD RAZIFF ABD RAZAK

DATE: 14 DECEMBER 2025

STATION 6

STUDENT NAME	STUDENT ID
AHMAD NAFIS BIN MOHD ZULKIFLI	51224125264

TABLE CONTENT

1.0 INTRODUCTION

A wireless network is a communication system that connects computers and devices using radio waves instead of physical cables, allowing users to access network resources and the internet while maintaining mobility. Wireless networks are widely used due to their flexibility, convenience, and cost-effective deployment, enabling seamless connectivity across homes, businesses, and public environments as the number of portable and smart devices continues to grow.

The objective of this lab is to design and implement a controller-based wireless network infrastructure that reflects real-world enterprise deployment practices. The network is designed using a Thin Access Point (AP) architecture, where multiple access points are centrally managed through a single wireless controller. Although the original design specified four access points, only three were deployed due to physical workspace limitations. Nevertheless, the implementation followed the same architectural principles and design requirements. The network incorporates a VPN router to provide secure internet connectivity and a network switch to support device interconnection and internal data flow. Four WLAN profiles which are ITStaff_6, Staff_6, Student_6, and Guest_6 were configured, where "6" represents the assigned workstation number. Each WLAN profile is designed to serve a specific user group with defined access permissions and network policies. The equipment used in this lab are shown in Table 1.

Lightweight Access Points (LWAPs) were selected for this experiment because they operate under centralized management through a wireless controller. Unlike standalone access points, LWAPs do not require individual configuration, enabling consistent policy enforcement, simplified deployment, and improved scalability. Centralized management allows administrators to control SSIDs, security settings, firmware updates, and traffic policies from a single interface. These capabilities are essential for larger campus or organizational networks but are difficult to manage using standalone access points.

In the context of this lab, LWAPs were chosen to provide hands-on experience with controller-based wireless architectures that are widely adopted in modern corporate, educational, and enterprise environments. Furthermore, the use of the TP-Link Omada Controller reflects Software-Defined Networking (SDN) principles, where the control plane is centralized and separated from the data plane. Through this SDN-based approach,

configurations, WLAN profiles, and security policies are dynamically distributed to all access points, improving automation, consistency, and operational efficiency.

The network design consists of both physical and logical topology components. The physical topology defines the hardware interconnections between the router, switch, controller, access points, and end devices, while the logical topology represents IP addressing, WLAN segmentation, routing, and traffic flow. Together, these designs establish a scalable and secure wireless network that supports controlled access and reliable internal and external communication. This lab activity supports the Course Learning Outcome (CLO) by providing practical experience in wireless network design, configuration, and documentation aligned with professional networking standards.

2.0 OBJECTIVES

1. To design wireless network.
2. To apply the Light Weight Access Point (LWAP) wireless network design.

3.0 EQUIPMENT & SOFTWARE

Equipment	Model	Function
Gigabit VPN Router	ER605	Provides internet access and routes network traffic.
Controller	OC200	Centrally manages and configures the access points.
Smart PoE+ Switch	TL-SG2008P	Connects network devices and distributes data.
Access Points	EAP115	Broadcast Wi-Fi and allow wireless device connections.
PC	Custom dekstop	Used for network configuration and testing
Smartphone	iPhone 16 Pro	Wireless client device
Software	Web Browser (Chrome)	Used to access and configure networking devices.

Table 1: Equipment and Software Used

4.0 NETWORK DESIGN

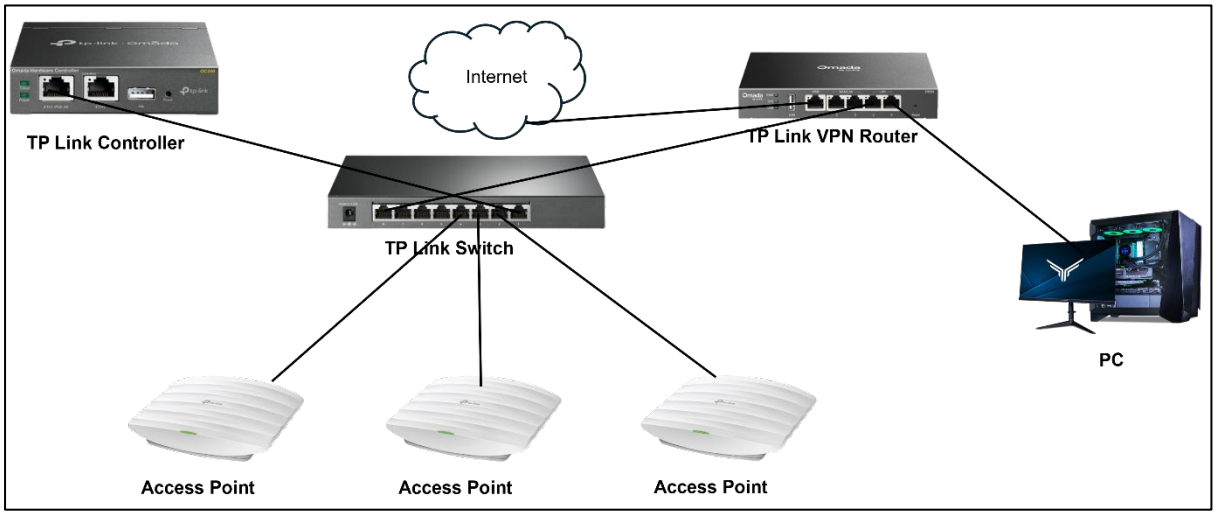

Figure 1: Physical Network Diagram

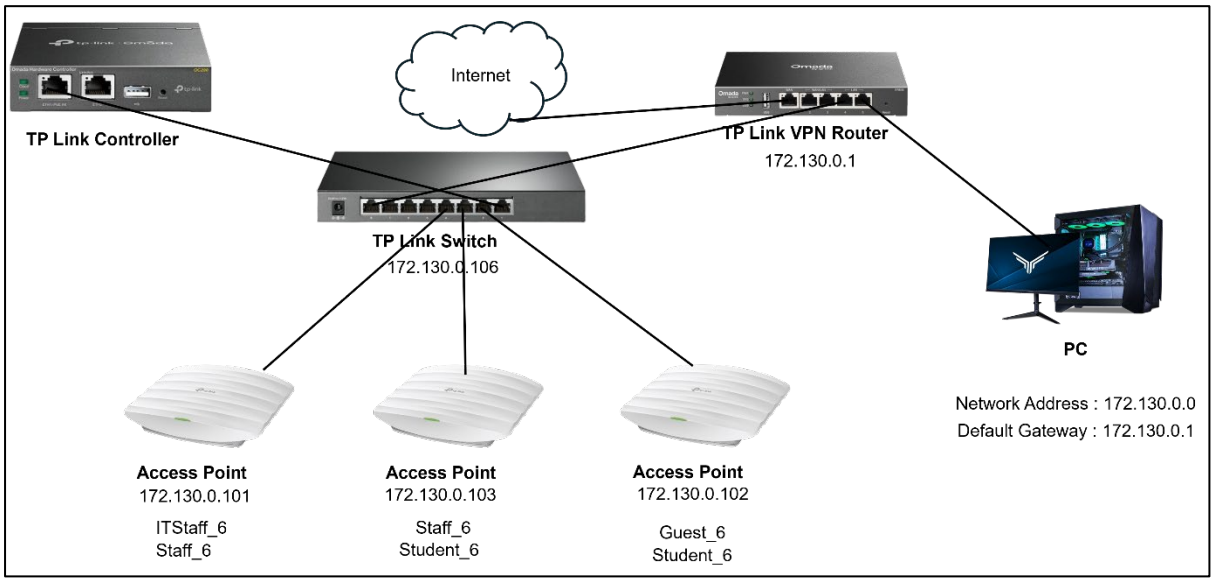

Figure 2: Logical Network Diagram

5.0 METHODOLOGY: NETWORK INSTALLATION & CONFIGURATION

5.1 Device Installation

All network devices within the Local Area Network (LAN) were physically interconnected to establish the wired backbone of the wireless infrastructure. The workstation PC was connected to the Gigabit VPN Router (ER605) via a LAN port to allow direct access for initial configuration and network management. The router was then connected to the Smart PoE+ Switch (TL-SG2008P) through its LAN interface to enable downstream device connectivity and traffic distribution. Both the router and the switch were powered using their respective external power adapters to ensure stable operation throughout the experiment. All physical connections between the PC, router, and switch were implemented using Unshielded Twisted Pair (UTP) Ethernet cables to support reliable data transmission. The completed physical interconnection of the LAN devices is shown in Figure 3.

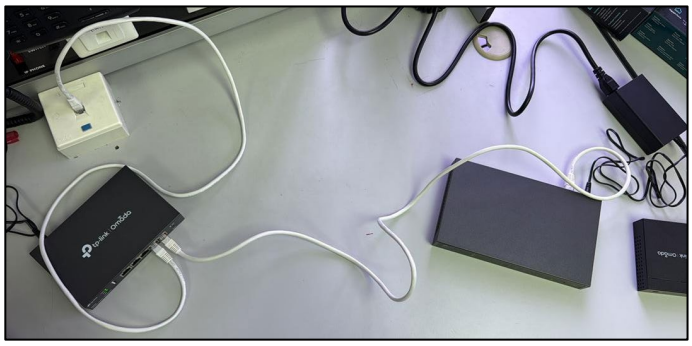

Figure 3: Physical LAN Network Connection Setup

The router was connected to the network switch using a non-PoE Ethernet port, excluding Ports 1 to 4, which were deliberately reserved for Power over Ethernet (PoE) devices. This port allocation strategy ensures that PoE resources are dedicated exclusively to devices requiring power delivery through the Ethernet link. The Omada Controller (OC200) and three Lightweight Access Points (EAP115) were connected directly to Ports 1 to 4 of the TL-SG2008P switch. These ports provide PoE capability, allowing the controller and access points to receive both power and data through a single Ethernet cable, thereby eliminating the need for external power adapters. This configuration supports a clean physical layout, simplifies installation, and ensures reliable operation of all PoE-dependent network devices. (refer Figure 4).

Figure 4: Switch Ports Connection

To provide external network connectivity, an Ethernet cable was connected from the Wide Area Network (WAN) port of the Gigabit VPN Router (ER605) to the internet. This WAN connection enabled the router to function as the gateway between the internal LAN and the external network, allowing all connected devices to access internet services. With the WAN link established, the router was able to perform routing, Network Address Translation (NAT) and traffic forwarding for both wired and wireless clients. As a result, all network devices including the switch, controller, access points and PC workstation were fully interconnected at the physical layer, forming a complete end-to-end network infrastructure as illustrated in Figure 5.

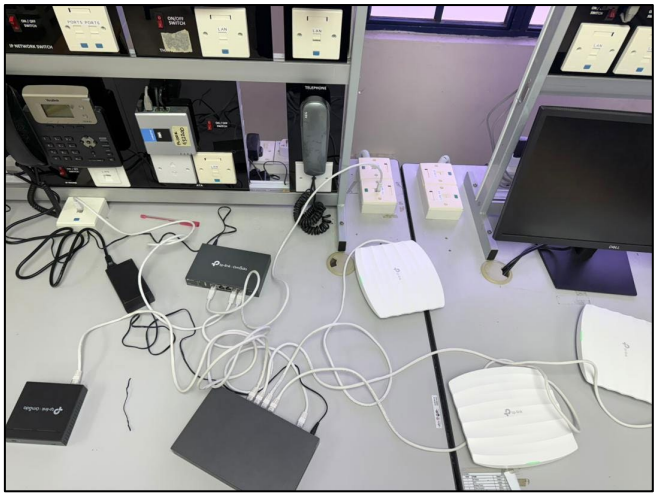

Figure 5: Complete Physical Network Interconnection with Internet Uplink

After completing the physical network setup, the PC was used to verify network connectivity and identify the router's management address. The Command Prompt was opened on the PC, and the *ipconfig* command was executed to display the assigned IP address, subnet mask and default gateway information. The default gateway address obtained from this output was then used to access the web-based configuration interface of the router through a web browser. This step confirmed successful Layer 1 and Layer 2 connectivity and ensured that the PC was correctly communicating with the router prior to further network configuration. The output of the ipconfig command is shown in Figure 6.

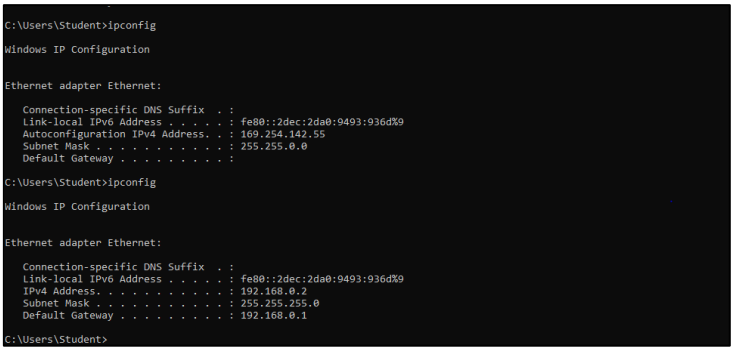

Figure 6: IP Configuration Verification Using Command Prompt

Upon successfully accessing the router's web-based configuration interface, the system prompted the creation of an administrator account as an initial security measure. This step is mandatory to protect the device from unauthorized access and to ensure that only authenticated users can perform configuration changes. The administrator credentials were defined by assigning a secure username and password, which were subsequently used for all future management sessions. Completing this step enabled access to the router's full configuration menu and marked the beginning of the logical network setup. The administrator account creation interface is shown in Figure 7.

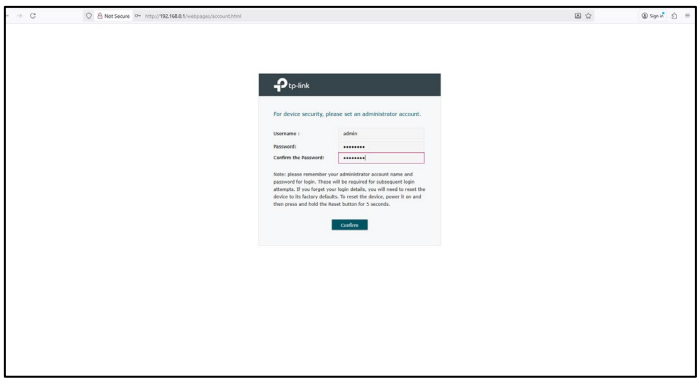

Figure 7: Administrator Account Creation Interface

5.2 Properly assign IP addresses

The router's LAN interface was configured according to the IP addressing scheme assigned to the workstation. The network was set to use the 172.130.0.0 address range and the router was assigned the static IP address 172.130.0.1, which also functioned as the default gateway for all devices within the LAN. A subnet mask of 255.255.255.0 was applied to define the network boundary. In addition, the Dynamic Host Configuration Protocol (DHCP) server was enabled on the router to automatically assign IP addresses to connected devices within the specified DHCP range. This configuration ensured consistent addressing, proper routing and seamless device communication within the network. The LAN and DHCP settings configured on the router are shown in Figure 8.

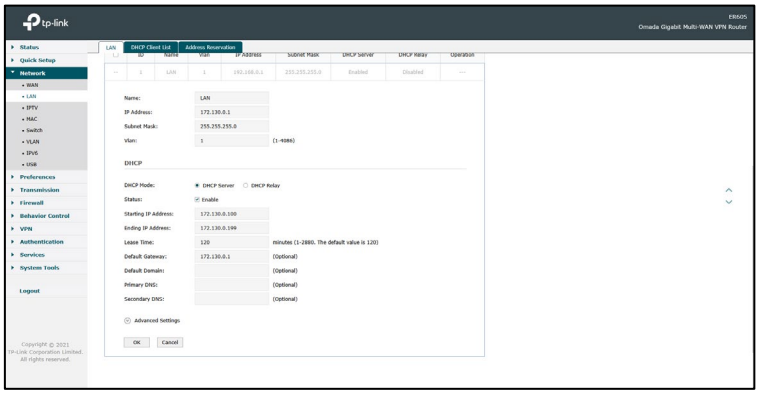

Figure 8: Router LAN IP Address and DHCP Configuration Interface

After configuring the LAN IP addressing and DHCP settings, the DHCP Client List on the router was reviewed to verify that all connected network devices had successfully obtained IP addresses. Each device including the switch, Omada Controller, access points and PC was confirmed to be assigned an IPv4 address within the designated 172.130.0.0 network range. This verification step ensured proper DHCP operation and confirmed that all devices were recognized by the router. To further validate end-to-end connectivity, each assigned IP address was tested using the ping command from the workstation's Command Prompt. Successful ping responses confirmed that all devices were correctly connected and reachable within the LAN. The DHCP Client List is shown in Figure 9, while the ping test results are provided in the Appendix (Figure 10).

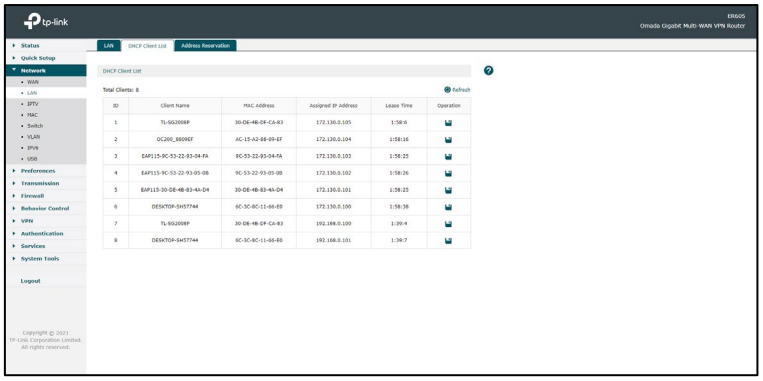

Figure 9: DHCP Client List Showing Assigned IP Addresses

Before proceeding to the next configuration stage, the PC's IP settings were verified to ensure correct network parameters had been applied. The Command Prompt was opened, and the *ipconfig* command was executed to display the assigned IPv4 address, subnet mask and default gateway. This verification step was necessary to confirm that the workstation had obtained an IP address within the designated 172.130.0.0 network range and that the default gateway was correctly set to the router's LAN IP address (172.130.0.1). Confirming these parameters ensured reliable communication with network devices and prevented configuration errors during subsequent steps. The IP configuration output is shown in Figure 11.

```
:\Users\Student>ping 192.168.0.1

inging 192.168.0.1 with 32 bytes of data:
eply from 192.168.0.1: bytes=32 time=1ms TTL=63
eply from 192.168.0.1: bytes=32 time=1ms TTL=63
eply from 192.168.0.1: bytes=32 time=1ms TTL=63
eply from 192.168.0.1: bytes=32 time=1ms TTL=63

ing statistics for 192.168.0.1:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
pproximate round trip times in milli-seconds:
   Minimum = 1ms, Maximum = 1ms, Average = 1ms

:\Users\Student>ipconfig

indows IP Configuration


thernet adapter Ethernet:

  Connection-specific DNS Suffix  . :
  Link-local IPv6 Address . . . . . : fe80::2dec:2da0:9493:936d%9
  IPv4 Address. . . . . . . . . . . : 172.130.0.100
  Subnet Mask . . . . . . . . . . . : 255.255.255.0
  Default Gateway . . . . . . . . . : 172.130.0.1

:\Users\Student>
```

Figure 11: Workstation IP Configuration Verification

5.3 Software Defined Networking Configuration

After verifying correct IP configuration, the IP address assigned to the Omada Controller was copied and entered into a new web browser tab to access the controller's web-based management interface. This interface represents the Software-Defined Networking (SDN) platform used in this lab, which enables centralized management of TP-Link Omada Access Points, switches, and routers through a single control interface. Accessing the SDN controller is a core objective of the experiment, as it demonstrates enterprise-level centralized network control and policy management. Upon initial access, the controller initiated its startup process, after which the controller name was configured according to the assigned workstation identifier (Station_6). In addition, the operating region and time zone were set to Malaysia to ensure correct regulatory compliance and accurate system time synchronization. The initial SDN controller startup interface is shown in Figure 12 and 13.

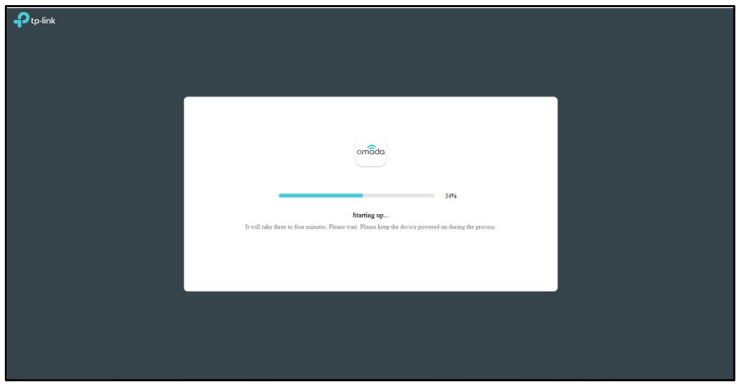

Figure 12: Initial Startup Interface of the Omada SDN Controller

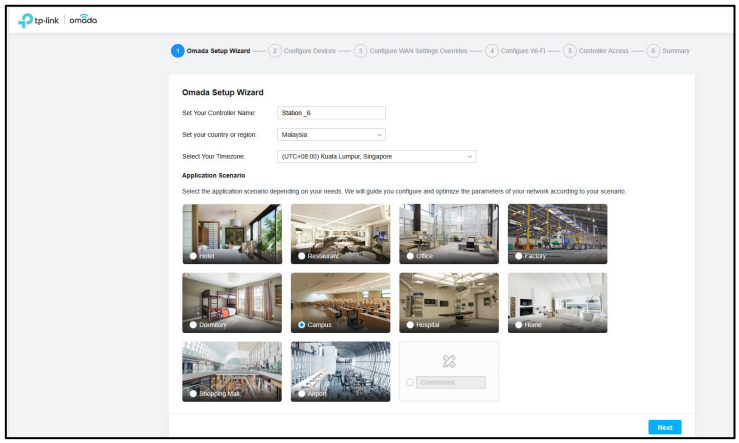

Figure 13: Omada SDN Controller Setup Wizard Interface

During the Omada Setup Wizard process, the configuration steps for device adoption, WAN settings overrides and Wi-Fi configuration were intentionally skipped, as these components were planned to be configured manually at a later stage. The setup process proceeded directly to the Controller Access configuration, where the administrator account credentials were defined to secure access to the SDN controller interface. This step established authentication control for centralized network management. Upon completing the controller access configuration, the setup wizard finalized the basic SDN initialization, confirming that the controller was successfully configured with the predefined parameters. The controller access configuration interface is shown in Figure 14, while the successful completion summary of the SDN basic configuration is shown in Figure 15.

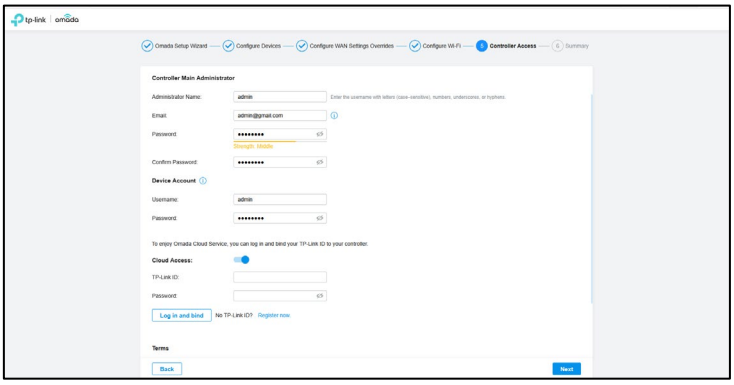

Figure 14: Controller Access Configuration Interface

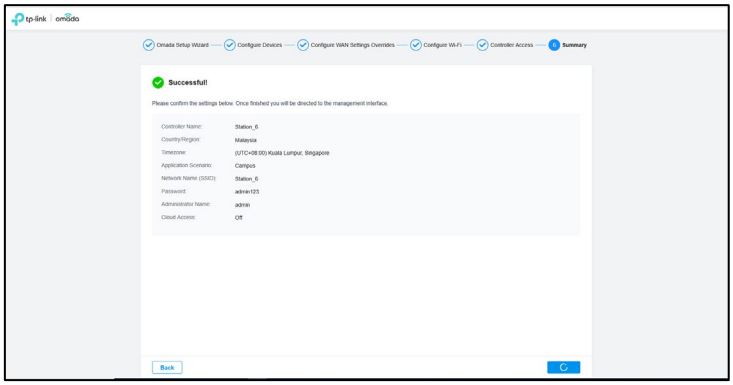

Figure 15: SDN Setup Summary and Successful Initialization

After completing the initial SDN setup, the LAN IP addressing was configured within the Omada SDN Controller based on the IP address scheme assigned to Station 6. This configuration was performed by navigating to Settings located at the bottom-left of the controller interface, followed by Wired Networks > LAN. The existing LAN network profile was edited to define the gateway IP address, subnet mask and DHCP parameters according to

the 172.130.0.0 network. The gateway address was set to 172.130.0.1 with a subnet mask of /24, and the DHCP server was enabled to automatically assign IP addresses to connected devices within the specified range. This step ensured consistent addressing and proper Layer 3 connectivity across all network devices managed by the SDN controller. The LAN configuration interface is shown in Figure 16.

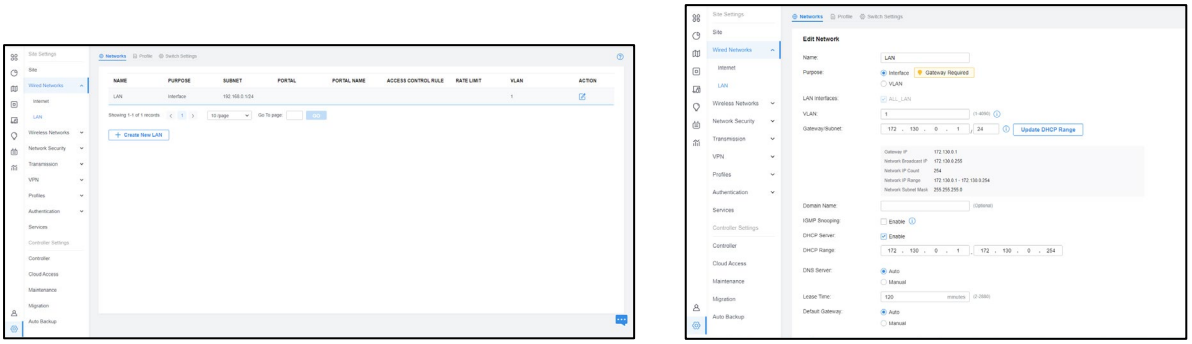

Figure 16: LAN IP Address Configuration in the Omada SDN Controller

After completing the LAN configuration in the SDN controller, all network devices were required to be adopted into the Omada SDN environment to enable centralized management. During the adoption process, certain devices prompted for authentication credentials, which were entered to authorize controller access. To verify basic network connectivity prior to successful adoption, the router's IP address was tested using the ping command from the PC, as shown in Figure 17. Successful ping responses confirmed that the router was reachable within the configured network.

Throughout the adoption process, the controller interface was refreshed periodically until each device status changed from *Pending* to *Connected*, indicated by a green status label in the controller dashboard. Once all devices were successfully connected, each network device was renamed via Device > Config > General to clearly identify its function (e.g., router, switch, AP1, AP2, AP3). This naming convention reduced management complexity and prevented configuration errors during subsequent network setup. The final adoption and renamed device status is shown in Figure 18.

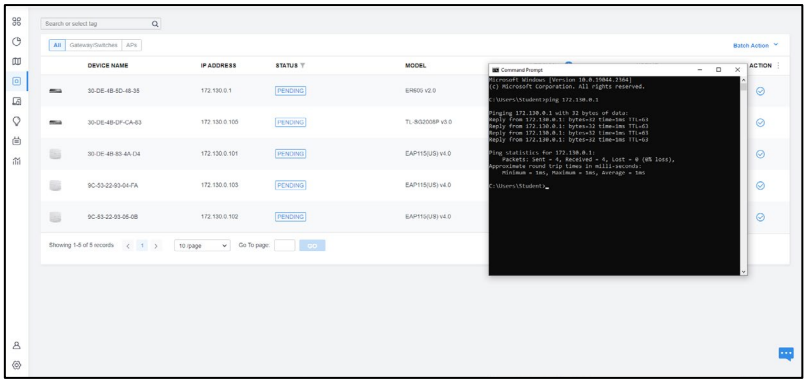

Figure 17: Device Connectivity Verification Using Ping Test

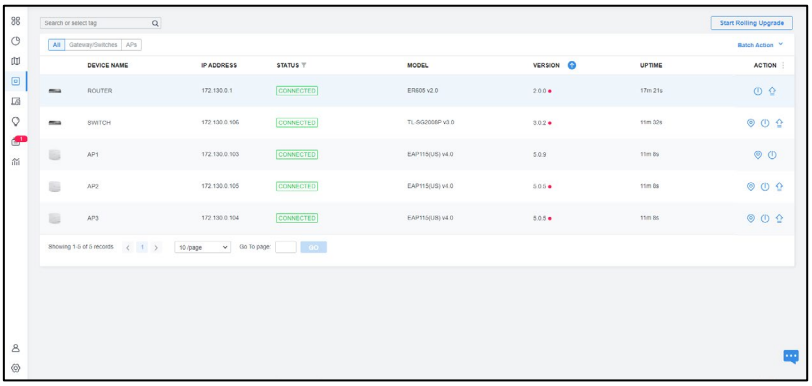

Figure 18: Successful Device Adoption and Renaming in Omada SDN Controller

5.4 Profile Configuration

After all network devices were successfully adopted into the SDN controller, wireless network profiles were configured to support different user groups. This process was performed by navigating to Settings > Wireless Networks > WLAN > Create New Wireless Network within the Omada SDN Controller interface. A new WLAN profile named Staff_6 was created and secured using WPA-Personal authentication to ensure controlled access. The wireless band settings were configured to support both 2.4 GHz and 5 GHz frequencies to optimize coverage and performance. The same configuration procedure was then repeated to create additional WLAN profiles which are ITStaff_6, Student_6, and Guest_6 where each serving a distinct category of users. These profiles enable logical segmentation of wireless access while maintaining centralized management through the SDN controller. The WLAN creation interface is shown in Figure 19, and the list of successfully created WLAN profiles is shown in Figure 20.

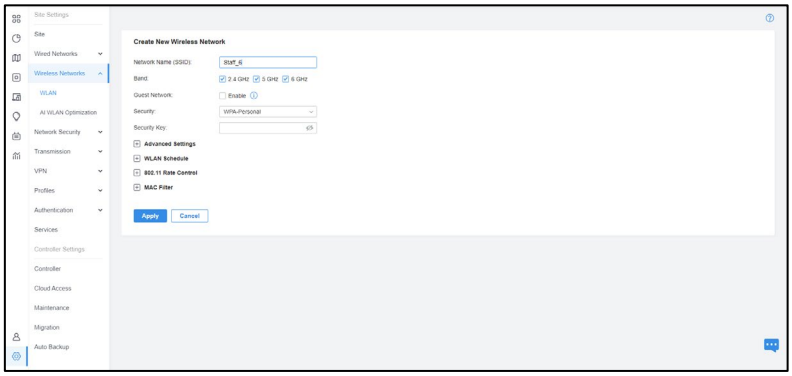

Figure 19: Create New Wireless Network (SSID) Configuration Interface

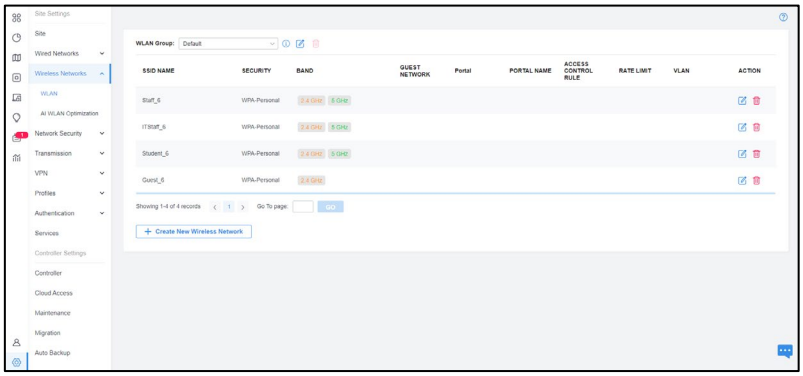

Figure 20: List of Configured WLAN Profiles in Omada SDN Controller

After creating all WLAN profiles, each Lightweight Access Point (LWAP) was configured to broadcast specific wireless networks based on its intended coverage area and user requirements. This configuration was performed by selecting the respective access point in the

Omada SDN Controller, navigating to Device > Config > WLAN, and enabling the required WLAN profiles. Each access point was assigned two WLAN profiles to support multiple user groups within the same coverage zone.

As shown in Figure 21, AP1 was configured to broadcast ITStaff_6 and Staff_6, representing areas such as administrative offices and staff-only floors where restricted access is required. In Figure 22, AP2 was assigned Staff_6 and Student_6, reflecting shared environments such as classrooms and departmental areas that require both staff and student access. Figure 23 shows AP3 configured with Guest_6 and Student_6, representing public-facing areas such as the ground floor and guest lobby. This selective WLAN assignment demonstrates efficient wireless segmentation and reflects real-world enterprise deployment practices where access control is enforced based on physical location and user role.

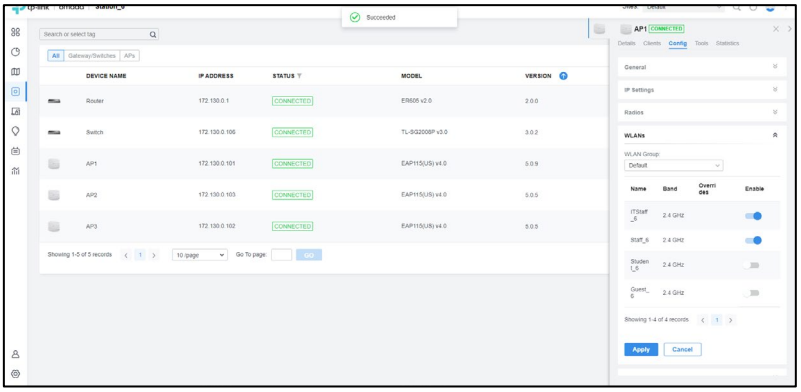

Figure 21: WLAN Profile Assignment for AP1

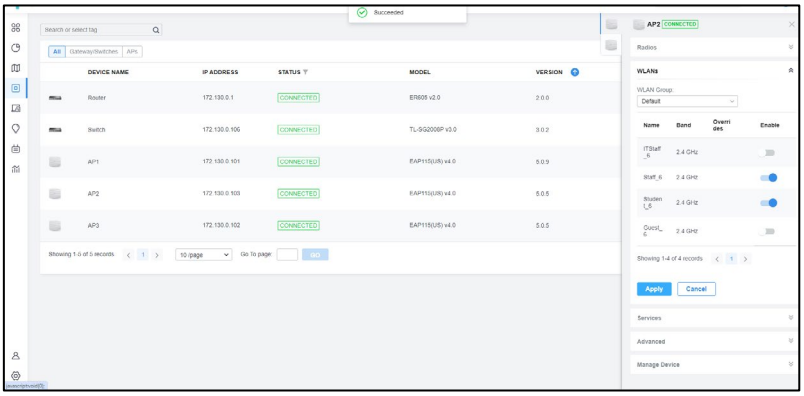

Figure 22: WLAN Profile Assignment for AP2

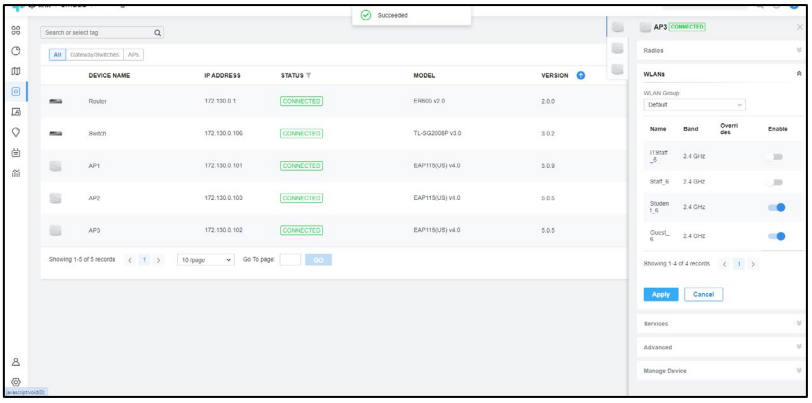

Figure 23: WLAN Profile Assignment for AP3

6.0 RESULT AND ANALYSIS

After completing the wireless network configuration, a series of validation tests were conducted to verify connectivity, SSID functionality, device association, and internet access across all WLAN profiles. The verification process focused on confirming that each SSID could successfully connect client devices, obtain valid IP addresses from the DHCP server and communicate both within the LAN and with external networks.

First, wireless clients were connected to each SSID, and the Topology Map feature in the Omada SDN Controller was used to visually confirm device associations. By navigating to Map, all connected devices were displayed graphically, showing the relationship between access points and their respective clients. This visual verification confirms correct WLAN-to-AP assignment and successful client association, as shown in Figure 24.

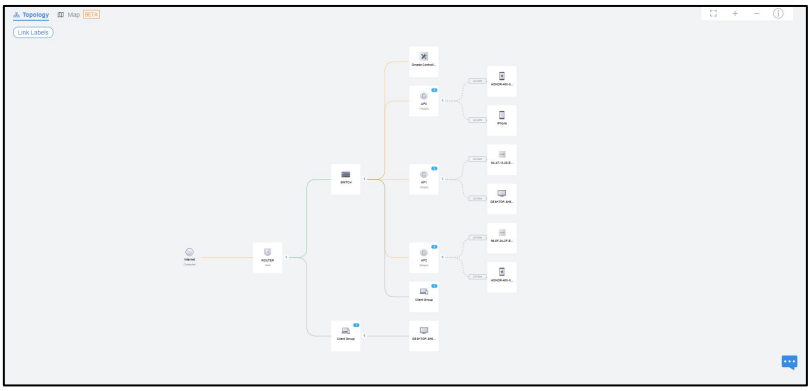

Figure 24: Wireless Client Associations

Next, a smartphone connected to AP2 was tested by identifying its assigned IP address from the controller and performing a ping test from the PC workstation. Successful ICMP (Internet Control Message Protocol) replies confirmed that the wireless client connected through AP2 was reachable within the LAN, as shown in Figure 25.

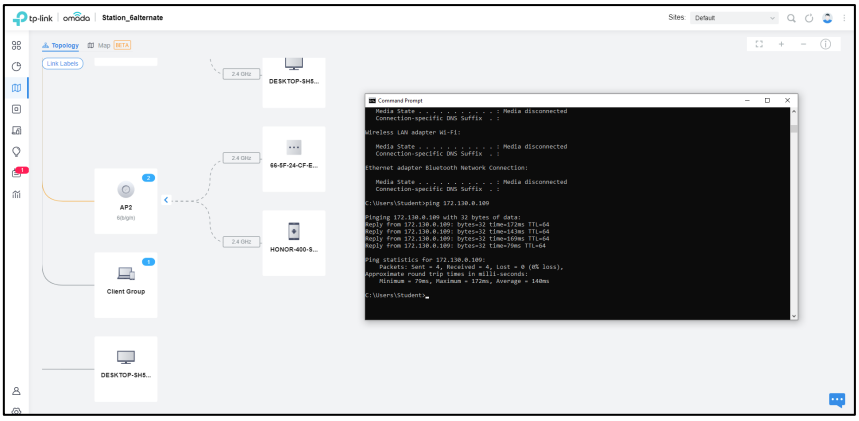

Figure 25: Ping Test to Smartphone Connected via AP2

To verify internet connectivity, the PC was connected wirelessly to the ITStaff_6 SSID. A ping google.com command was executed and successful replies confirmed that DNS resolution and external internet access were functioning correctly through the configured network gateway. This result is shown in Figure 26.

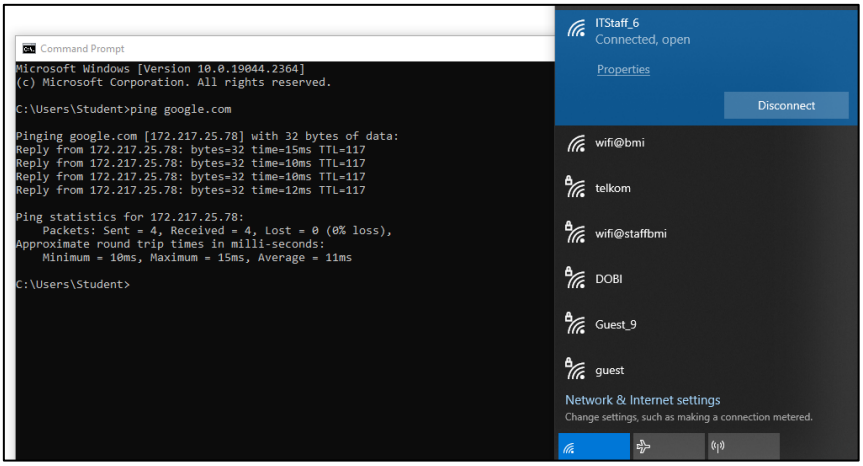

Figure 26: Internet Connectivity Test Using ITStaff_6 SSID

Further validation was performed using an iPhone by connecting sequentially to ITStaff_6, Staff_6, Student_6, and Guest_6 SSIDs. Each connection successfully obtained an IP address within the 172.130.0.0 network range and was able to browse the internet. These screenshots are combined and presented as Figure 27 to demonstrate that all WLAN profiles provide valid connectivity and internet access.

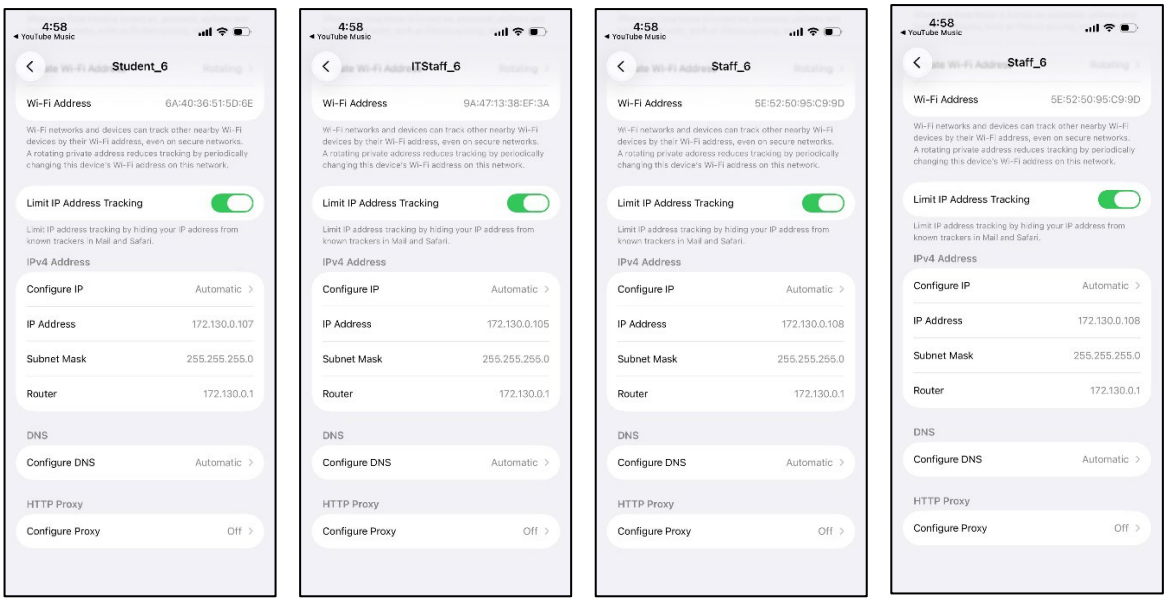

Figure 27: iPhone Connectivity Verification Across All WLAN Profiles

Subsequently, a wireless client connected to Student_6 (iPhone connectivity) was tested by pinging its assigned IP address from the workstation. Successful responses verified correct DHCP assignment and LAN communication, as shown in Figure 28.

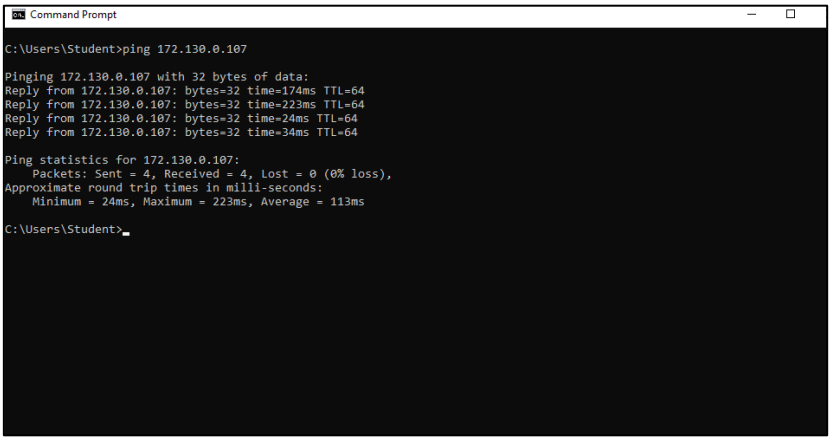

Figure 28: Ping Test to Client Connected to Student_6 SSID

Finally, an additional PC was connected to the Staff_6 SSID to further validate network reliability. A ping test was performed to the default gateway (172.130.0.1), and successful replies confirmed stable wireless connectivity and proper routing within the network. This final verification is shown in Figure 29.

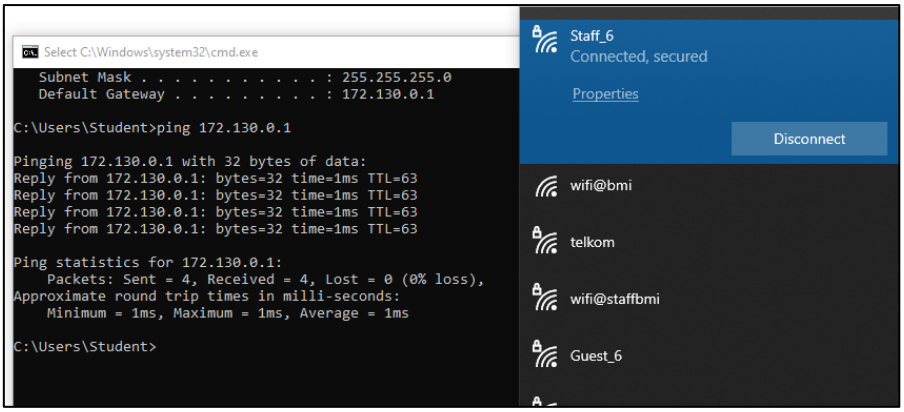

Figure 29: Gateway Connectivity Verification from Staff_6 SSID

In addition to connectivity testing, a wireless performance evaluation was conducted to assess the quality of the ITStaff_6 SSID. A speed test was performed using a mobile device connected to the ITStaff_6 wireless network. The results demonstrate that the SSID is capable of providing stable internet access with acceptable throughput, confirming that the wireless configuration supports not only connectivity but also practical network performance for end users. (refer Figure 30)

Figure 30: Wireless Speed Test Result for ITStaff_6 SSID

Overall, the results confirm that all WLAN profiles are operational, correctly segmented and capable of providing secure LAN and internet access according to the network design requirements.

7.0 DISCUSSION

During the configuration and deployment of the wireless network, several technical considerations and challenges were identified, particularly in relation to centralized, controller-based management. All access points required connection to Power over Ethernet (PoE) ports in order to power up and operate correctly. The TL-SG2008P switch provides PoE functionality only on Ports 1 to 4, therefore, each Lightweight Access Point (LWAP) had to be connected specifically to these ports. PoE is essential because it delivers both electrical power and data through a single Ethernet cable, simplifying installation and reducing cabling complexity. In scenarios where PoE ports are unavailable, access points can alternatively be powered using external power adapters or PoE injectors to ensure continuous operation without modifying the switch hardware.

A key observation from this lab is that once devices are adopted and configured through the Omada SDN Controller, further manual configuration at the router level is no longer recommended, as shown in Figure 31. This behavior reflects Software-Defined Networking (SDN) principles, where the controller functions as the centralized control plane and network devices operate as data-plane elements. Configuration, policy enforcement, and WLAN behavior are managed centrally through software, ensuring consistency and reducing configuration conflicts that may arise from distributed device management.

Figure 31: Router web-page

A significant challenge encountered during implementation was ensuring that all network devices obtained IP addresses from the required addressing class (172.130.0.X). In some instances, the controller or router assigned unexpected IP ranges, requiring the controller and occasionally the router to be reset. This process had to be repeated until all devices aligned

under the same IP addressing scheme. Although time-consuming, this step was necessary to ensure proper routing, device discovery, and reliable communication between the SDN controller and access points. This challenge highlights the importance of consistent network state management in controller-based architectures.

The implementation of both physical and logical network diagrams played a crucial role in supporting the SDN-based configuration process. The physical network diagram provided a clear representation of device placement, cabling paths, and PoE port assignments, reducing installation errors. The logical network diagram illustrated IP addressing, WLAN segmentation, and traffic flow as defined by centralized policies. Together, these diagrams helped validate that the SDN controller's logical configuration aligned correctly with the physical infrastructure.

The use of a static IP address for the workstation was also important in an SDN environment. Static addressing ensured that the configuration PC remained consistently reachable when accessing the controller and network devices. In contrast, access points were assigned dynamic IP addresses via DHCP to simplify deployment and allow automatic discovery and adoption by the controller. This approach supports scalability, as additional access points can be integrated into the network without manual IP configuration.

Compared to the previous lab, a major advancement in this experiment was the ability to assign multiple WLAN profiles (SSIDs) to a single access point through centralized control. In earlier labs, each router supported only a single SSID, limiting flexibility. In this lab, the Omada SDN Controller enabled the deployment of four WLAN profiles which are ITStaff_6, Staff_6, Student_6, and Guest_6 that allowing multiple user groups to coexist securely on the same wireless infrastructure. This reflects real-world enterprise network design, where access control and policy enforcement are managed centrally rather than per device.

An additional observation was made during the configuration of the Guest_6 WLAN profile. Initially, the guest network was configured without security, allowing devices to associate with the SSID but without internet access. After security was enabled, internet connectivity was successfully established. This behavior demonstrates how centralized SDN policies and security configurations directly influence user access and network behavior. Proper WLAN security configuration is therefore essential to ensure controlled access while allowing guest users to access external network resources as intended.

8.0 CONCLUSION

This lab successfully demonstrated the design, configuration and deployment of a controller-based wireless network using Lightweight Access Points (LWAPs), a centralized TP-Link Omada Controller, and supporting network infrastructure. Through the implementation of both physical and logical network diagrams, the lab provided a structured approach for planning device connectivity, IP addressing, WLAN segmentation and overall network behavior. The application of Software-Defined Networking (SDN) concepts through the controller reinforced modern enterprise practices by enabling centralized configuration, policy enforcement and unified network management.

The practical implementation highlighted the importance of proper PoE port allocation, consistent IP addressing, and strict adherence to controller-based configuration workflows. Several challenges were encountered, particularly in ensuring that all devices obtained IP addresses within the required 172.130.0.X network range. These challenges provided valuable troubleshooting experience and emphasized the need for systematic resets, verification steps, and careful configuration management. Additionally, the use of a static IP address for the PC workstation and DHCP-based addressing for access points strengthened understanding of device discoverability and network management principles.

A major advancement compared to previous labs was the ability to configure multiple WLAN profiles on a single access point, reflecting real-world enterprise environments where multiple user groups coexist with different access permissions. The successful deployment of four WLAN profiles which are ITStaff_6, Staff_6, Student_6, and Guest_6 that demonstrated the flexibility, scalability and efficiency of controller-based wireless architectures. Overall, this lab enhanced technical proficiency in wireless network design, IP addressing schemes and SDN-based configuration, thereby supporting the Course Learning Outcome (CLO) related to the preparation and implementation of professional wireless network documentation.

9.0 APPENDIX

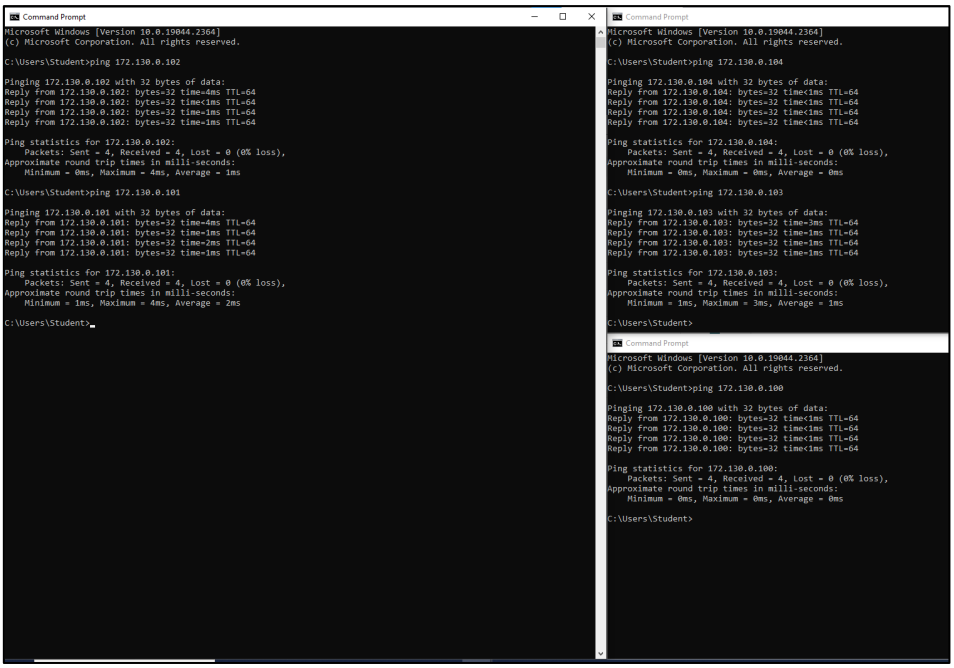

Figure 10: Network Connectivity Verification Using Ping Tests

UNIVERSITI KUALA LUMPUR
RUBRIC FOR LABORATORY REPORT

COURSE CODE & NAME	BTB37303 & WIRELESS NETWORK ARCH.
STUDENT NAME	AHMAD NAFIS BIN MOHD ZULKIFLI
STUDENT ID	51224125264

GROUP
L01

PERFORMANCE CRITERIA		**QUALITY OF WORK**					
		VERY POOR 1	**POOR** 2	**GOOD** 3	**VERY GOOD** 4	**EXCELLENT** 5	**TOTAL**
TASK 1: (10 marks) Network Design							
1.1	Physical Topology Design (x1)						
	Logical Topology Design (x1)						
TASK 2: (30 marks) Network Installation and Configuration							
2.1	Devices Installation (x2)						
2.2	Profile configuration (x2)						
2.3	Properly assign IP addresses (x2)						
TASK 3: (40 marks)							
3.1	Introduction. (x2)						
	Discussion. (x2)						
	Conclusion. (x2)						
	Report Format. (x2)						
TASK 4: (20 marks)							
4.1	Demo Physical (x2)						
4.2	Demo Configuration (x2)						
	Total marks						

ASSESSMENT COVERSHEET

Attach this coversheet as the cover of your submission. All sections must be completed.

Section A: Submission Details

Programme	:	BACHELOR OF TELECOMMUNICATION ENGINEERING TECHNOLOGY WITH HONOURS
Course Code & Name	:	BTB37303 WIRELESS NETWORK ARCHITECTURE
Course Lecturer(s)	:	MR MOHD RAZIFF ABD RAZAK
Submission Title	:	LAB 2 REPORT
Deadline	:	Day _____ Month _____ Year _____ Time _____
Penalties	:	• 5% will be deducted per day to a maximum of four (4) working days, after which the submission will **not** be accepted. • Plagiarised work is an Academic Offence in University Rules & Regulations and will be penalised accordingly.

Section B: Academic Integrity

Tick (√) each box below if you agree:

- ☑ I have read and understood the UniKL's policy on Plagiarism in University Rules & Regulations.
- ☑ This submission is my own, unless indicated with proper referencing.
- ☑ This submission has not been previously submitted or published.
- ☑ This submission follows the requirements stated in the course.

Section C: Submission Receipt

(must be filled in manually)

Office Receipt of Submission

Date & Time of Submission (stamp)	Student Name(s)	Student ID(s)
14 DECEMBER 2025	AHMAD NAFIS BIN MOHD ZULKIFLI	51224125264

Student Receipt of Submission

This is your submission receipt, the only accepted evidence that you have submitted your work. After this is stamped by the appointed staff & filled in, cut along the dotted lines above & retain this for your record.

Date & Time of Submission (stamp)	Course Code	Submission Title	Student ID(s) & Signature(s)
14 DECEMBER 2025	BTB37303	LAB 2 REPORT	51224125264