**Torin Flanagan 1169130 ICT220 Wireless Communications Task 2**

**Network and Communications Skill-Based Assessment**

Contents

[Introduction 2](#_Toc197629443)

[Change of Default Settings on SOHO Router 2](#_Toc197629444)

[WLC Controller for the Enterprise Network 3](#_Toc197629445)

[Two Separate WLANs on the WLC Controller 3](#_Toc197629446)

[Implementing Dual Authentication Mechanism for the RADIUS Server 4](#_Toc197629447)

[Why WPA2-Enterprise Over WPA2-PSK on WLAN VLAN 5 4](#_Toc197629448)

[Conclusion 5](#_Toc197629449)

[Reference List 5](#_Toc197629450)

[Appendix A - SOHO Network PT Configuration Summary 5](#_Toc197629451)

[Appendix B - Enterprise Network PT Configuration Summary 7](#_Toc197629452)

[Figure 1: Final Successfully Configured SOHO and Enterprise Networks 2](#_Toc197629438)

[Figure 2: Ping results for Wireless Host 1 10](#_Toc197629439)

[Figure 3: Ping results for Wireless Host 2 11](#_Toc197629440)

### Introduction

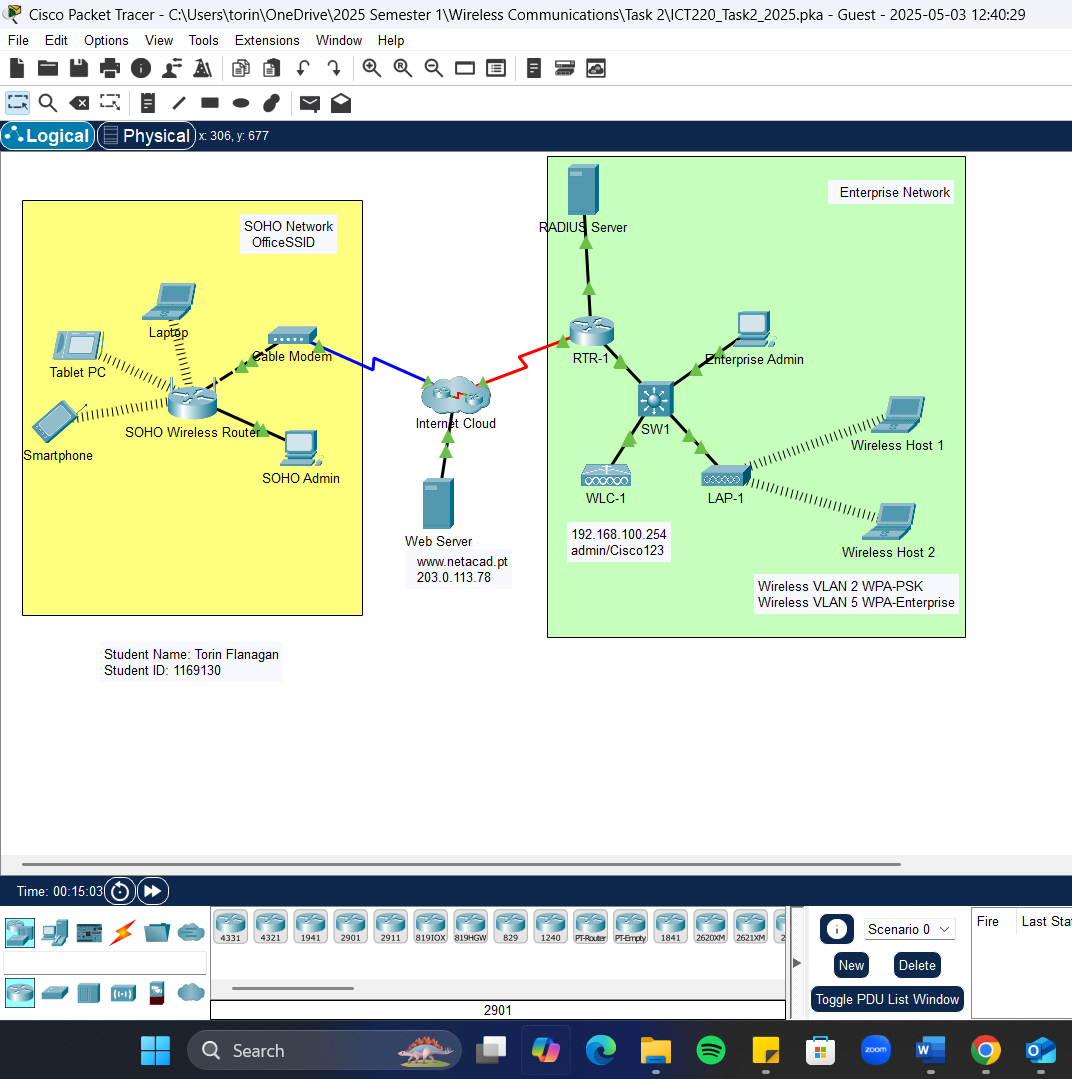
As wireless networks continue to grow in complexity and scale, both SOHO and enterprise environments must adopt modern security measures and maintain current connectivity standards. The following recommendations address essential aspects of network configuration, from basic router setup to advanced enterprise features, aimed at improving performance, scalability, and security. Each recommendation aligns with best practices in network design, with a central focus on building secure, efficient, and manageable infrastructure.

Figure 1: Final Successfully Configured SOHO and Enterprise Networks

### Change of Default Settings on SOHO Router

SOHO routers serve as consumer-grade gateways for internet access, with most data between a computer and the Internet passing through them. By default, they often lack strong security measures and offer limited network functionality.

Regarding network security with SOHO routers, everyday users of the network rarely change usernames, passwords, or IP addresses of their routers, exposing the network to brute-force attacks via the router’s web interface (as required for SOHO Network packet tracer configuration). Additionally, default wireless protocols like WEP or WPA are outdated and should be replaced with WPA2 or WPA3 using AES encryption for better protection (Davis and Chow, 2014).

From a performance perspective, changing the default SSID helps avoid accidental connections from nearby networks. Adjusting the wireless channel can also reduce interference and improve speed. On advanced SOHO routers, enabling QoS allows prioritisation of specific traffic types to optimise overall network performance (Davis and Chow, 2014).

### WLC Controller for the Enterprise Network

Implementing a WLC in an enterprise network provides a centralised approach to managing multiple wireless access points (APs). This architecture is well-suited to growing business environments with increasing demands for wireless connectivity. APs extend the network’s wireless coverage by relaying bandwidth from the central router, allowing client devices to maintain strong connections over greater distances (Cisco, 2019).

By using a WLC, the administration of these APs becomes centralised, streamlining tasks such as configuration, firmware updates, security policy enforcement, and load balancing. This improves network scalability, reduces configuration errors, and simplifies maintenance. Additionally, WLCs enable real-time monitoring of the wireless infrastructure, allowing quick detection and responses to performance issues or security threats (Cisco, 2019).

Overall, a WLC-based architecture enhances the efficiency, reliability, and security of enterprise WLANs by offering better control and visibility over wireless operations.

### Two Separate WLANs on the WLC Controller

WLAN’s enable multiple end-user devices to connect wirelessly, eliminating physical medium needs. Once configured through a WLC controller, WLAN functions become centralised, enhancing system operability and simplifying overall network management. Centralised control ensures consistent configuration across all WLANs, promoting stronger security and more reliable client connectivity (Smith, Woodhams, and Marg, 2010).

Segmenting the enterprise network into two distinct WLANs (typically via VLAN assignments) reduces the broadcast traffic and interferences. This segmentation enhances performance and isolates sensitive systems from unauthorised access. With the WLC controller managing both WLANs, administrators can then implement custom configurations, enforce bandwidths and security policies, and maintain greater control over user access. This structure significantly improves the scalability, security, and efficiency of the enterprise wireless network as an end result.

### Implementing Dual Authentication Mechanism for the RADIUS Server

Remote authentication dial-in user service (RADIUS) is a networking protocol that centrally manages authentication, authorisation, and accounting (AAA) for network access. Users are authenticated against a central database, and access is granted if credentials match policy requirements. RADIUS has extensible authentication protocol (EAP) support, enabling a variety of authentication methods (Szilagyi, Sood and Singh, 2009).

Because of EAP support, RADIUS packets can carry EAP messages through intermediary devices like APs. These devices act as pass-through points, without needing to understand or process EAP. Only the RADIUS server handles EAP authentication, simplifying the architecture while maintaining strong security (Szilagyi, Sood and Singh, 2009).

In terms of enhancing RADIUS server security, dual authentication should be implemented, using EAP support. This allows using multiple authentication factors without needing to increase network complexity. Because the APs act as pass-through devices, authentication will remain centralised and efficient, further reducing unauthorised access.

### Why WPA2-Enterprise Over WPA2-PSK on WLAN VLAN 5

The main difference between WPA2-Personal and WPA2-Enterprise lies in how the encryption keys are generated. WPA2-Personal uses a shared PSK (typically 8 characters) which is the same for all users, becoming vulnerable to password guessing and leaks. In contrast, WPA2-Enterprise uses dynamic session-based keys for each user, which is managed through a RADIUS server having the keys updated periodically during a session (Radivilova and Ali Hassan, 2017).

To achieve maximum data security, WPA2-Enterprise should be integrated with digital certificates and EAP methods. This ensures both the end user and authentication server verify certificates, providing strong protections against unauthorised access (Radivilova and Ali Hassan, 2017).

By implementing WPA2-Enterprise, it allows for improved system scalability, accountability, and policy enforcements with the enterprise network. Such security use enables IT administrators to track user access, revoke credentials when necessary, and apply custom access control policies for different user roles. Having such a high level of control by implementing WPA2-Enterprise for the enterprise network is crucial for a secure and manageable wireless enterprise environment.

### Conclusion

By implementing the targeted recommendations, wireless network administration will be significantly improved in terms of both security and operational efficiency. These measures reduce vulnerabilities, enhance scalability, and strengthen user access control. Such solutions are essential for maintaining secure, high-performing wireless environments across both small and large-scale deployments.

### Reference List

* Cisco (2019). What Is a WLAN Controller? (WLC). [online] Cisco. Available at: https://www.cisco.com/c/en/us/products/wireless/wireless-lan-controller/what-is-wlan-controller.html [Accessed 7 May 2025].
* Davis, M. and Chow, M. (2014). SOHO Router Security. [online] Available at: https://www.cs.tufts.edu/comp/116/archive/fall2014/mdavis.pdf [Accessed 8 Nov. 2021].
* Radivilova, T. and Ali Hassan, H. (2017). Test for penetration in Wi-Fi network: attacks on WPA2-PSK and WPA2-Enterprise. [online] p.3. Available at: https://arxiv.org/pdf/1805.06691 [Accessed 7 May 2025].
* Smith, J., Woodhams, J. and Marg, R. (2010). Controller-Based Wireless LAN Fundamentals. Pearson Education.
* Szilagyi, D., Sood, A. and Singh, T. (2009). RADIUS: A REMOTE AUTHENTICATION DIAL-IN USER SERVICE. Rivier Academic Journal, [online] 5(2), p.12. Available at: https://www2.rivier.edu/journal/ROAJ-Fall-2009/J286-RADIUS-Sood.pdf [Accessed 7 May 2025].

### Appendix A - SOHO Network PT Configuration Summary

* **The router IP and DHCP settings to be changed according to the information in the Addressing Table:**
  + Opened the **SOHO Admin PC**, navigated to the **Desktop** tab, and launched the **Web Browser**.
  + Entered the router IP **192.168.0.1**, found by setting the PC's IP to **DHCP** under **IP Configuration**, revealing the **Default Gateway** as the router's address.
  + Logged into the router GUI using (username; admin, password; admin).
  + In **Internet Setup**, changed **Connection Type** from Static IP to Automatic Configuration – DHCP.
  + In **Network Setup**, updated the **Router IP** from 192.168.0.1 to 192.168.1.1, and the **Subnet Mask** to 255.255.255.192.
* **DHCP settings on the router to permit a maximum of 22 addresses to be issued by the router.**
  + In **DHCP Server Settings**, increased the **Maximum Number of Users** from 10 to **22**, and changed the **IP Address Range** from 192.168.0.1–10 to 192.168.1.10–31.
* **The DHCP server to start with IP address .10 of the LAN network.**
  + In **DHCP Server Settings**, confirmed **DHCP Server** was enabled, then changed the **Start IP Address** from 192.168.0.1 to 192.168.1.10.
* **The internet interface of the router to receive its IP address over DHCP.**
  + Already set to **obtain IP via DHCP** under the **Internet Setup** tab, as noted in step 1.
* **The static DNS server to be configured to the address in the Addressing Table.**
  + In **DHCP Server Settings**, **Static DNS 1** was changed from 0.0.0.0 to 10.100.100.252.
* **The network to use a channel on the 2.4GHz Wireless LAN interface which does not interfere with Channels 1 and 6.**
  + In the **Wireless** tab (next to Setup), under **Basic Wireless Settings**, the 2.4GHz settings were adjusted:
    - **SSID** changed to OfficeSSID,
    - **SSID Broadcast** set to Enabled,
    - **Channel** changed from 1 – 2.412GHz to 11 – 2.462GHz,
    - **Channel Bandwidth** set to 20MHz (from Auto).
  + **5GHz – 1** and **5GHz – 2** settings were left as default with **SSID Broadcasts** disabled.
* **The Wireless LAN to use WPA2 Personal. Use information shown in the WLAN information table.**
  + In the **Wireless** section, under **Wireless Security**, the **2.4GHz** channel security was initially Disabled.
  + It was enabled by selecting **WPA2 Personal**, setting **Encryption** to *AES*, and entering the **Passphrase**: Office777.
  + Security for the **5GHz – 1** and **5GHz – 2** channels remained disabled.
* **The default password of the router to be changed to SoHo123#.**
  + In the **Administration** tab under **Management**, the default router password was changed from admin to SoHo123# by entering it in both the **Router Password** and **Re-enter to confirm** fields.
* **The laptop, Tablet PC and Smartphone to be connected to the wireless network.**
  + **Laptop**: Open the device, go to the **Desktop** tab, then **PC Wireless**. Under the **Connect** tab, select **OfficeSSID** and click **Connect**. Confirm connection in **IP Configuration**, the Default Gateway should show 192.168.1.1. Alternatively, use **Command Prompt** to ping 192.168.1.1 to verify communication.
  + **Tablet PC**: Go to the **Config** tab, select **Wireless0** under **INTERFACE**, set SSID to OfficeSSID. Choose **WPA2-PSK**, enter the passphrase Office777, and ensure encryption is **AES**. Confirm connection via **IP Configuration** or by pinging 192.168.1.1.
  + **Smartphone**: Follow the same steps as the Tablet PC.

### Appendix B - Enterprise Network PT Configuration Summary

* **The wireless LAN controller to include two WLANs using the following interfaces:**
  1. VLAN 2
     + Name: WLAN 2
     + VLAN Identifier: 2
     + Port Number: 1
     + Interface IP Address: 192.168.2.254/24
     + Gateway: RTR-1 G0/0/0.2 address
     + Primary DHCP Server: Gateway address
  2. VLAN 5
     + Name: WLAN 5
     + VLAN Identifier: 5
     + Port Number: 1
     + Interface IP Address: 192.168.5.254/24
     + Gateway: RTR-1 G0/0/0.5 address
     + Primary DHCP Server: Gateway address
* Access to **WLC-1** was achieved via **Enterprise Admin** using the **GUI** by entering **192.168.100.254** in the web browser, login credentials were (username; **admin** and password; **Cisco123**).
* Interfaces were added via **Controller > Interfaces > New**, with **IP** **settings** and **DHCP** **configuration** applied as required.
* **A DHCP scope to be configured for the wireless management network**
  + Scope Name: management
  + Pool Start Address: 192.168.100.235/24
  + Pool End Address: 192.168.100.245/24
  + Default Routers: RTR-1 G0/0/0.100 address
* Configured under **Internal DHCP Server > DHCP Scope > New**. **Address pool** and **default gateway** were applied to the **‘**management’scope.
* **The WLC to be configured to use the RADIUS server and send logs information to an SNMP server**

1. Configure the RADIUS server information as follows:
   * Sever Index: 1
   * Sever Address: 10.6.0.254
   * Shared Secret: RadiusPW
   * Configured via **Security > AAA > RADIUS > Authentication > New**.
2. Configure the WLC to send logs information to an SNMP server.
   * Community Name: WLAN
   * IP Address: 10.6.0.254

* Set up under **Management > SNMP > Trap Receivers**. SNMP protocols **v1, v2c, and v3** were enabled.

**The WLANs to be created using the information below:**

1. WLAN VLAN 2
   * Profile Name: Wireless VLAN 2
   * WLAN SSID: SSID-2
   * Interface: WLAN 2
   * ID: 2
2. WLAN VLAN 5
   * Profile Name: Wireless VLAN 5
   * WLAN SSID: SSID-5
   * Interface: WLAN 5
   * ID: 5
   * Created via **WLANs > Create New**. Each was enabled and assigned to the corresponding interface.

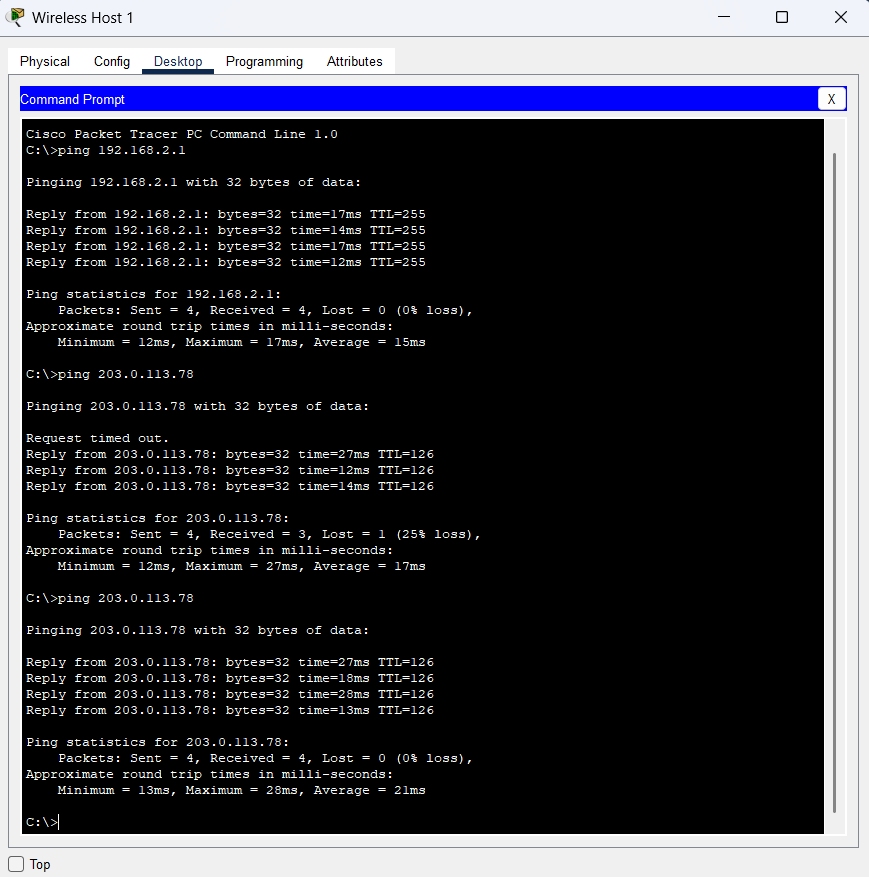
* **The WLANs to be secured using the information shown in the WLAN information table**
  1. Security settings for WLAN 2 (SSID-2):
  + Security: WPA2-PSK
  + Encryption: AES
  + Passphrase: Enterprise123
  1. Security settings for WLAN 5 (SSID-5):
  + Security: WPA2-Enterprise (802.1X)
  + Encryption: AES
  + RADIUS Server: 10.6.0.254 (Port 1812)
  + Both set under **WLANs > Security**. WPA2 and 802.1X authentication configured per WLAN requirements.
* **The FlexConnect settings to be appropriately enabled for both WLANs.**
  + For both WLANs, **Advanced > FlexConnect Local Switching** was enabled and applied.
* **Wireless Host 1 to connect to Wireless VLAN 2.**
  + Accessed WLC-1 via Enterprise **Admin > Command** to set the date, time, and time zone.
  + Configured WLAN 2 interface **(192.168.2.254, gateway 162.168.2.1, DHCP 192.138.2.1)** and created **SSID-2** using **WPA2-PSK** with password **Enterprise123**.
  + **LAP-1** registered to **WLC-1**, **CAPWAP tunnel** established, and **RTR-1** provided **DHCP** for **VLAN 2**.
  + On **Wireless Host 1**, connected to **SSID-2** via **PC Wireless** using correct profile settings.
  + **Ping results** confirmed successful connectivity from **Wireless Host 1**.

Figure 2: Ping results for Wireless Host 1

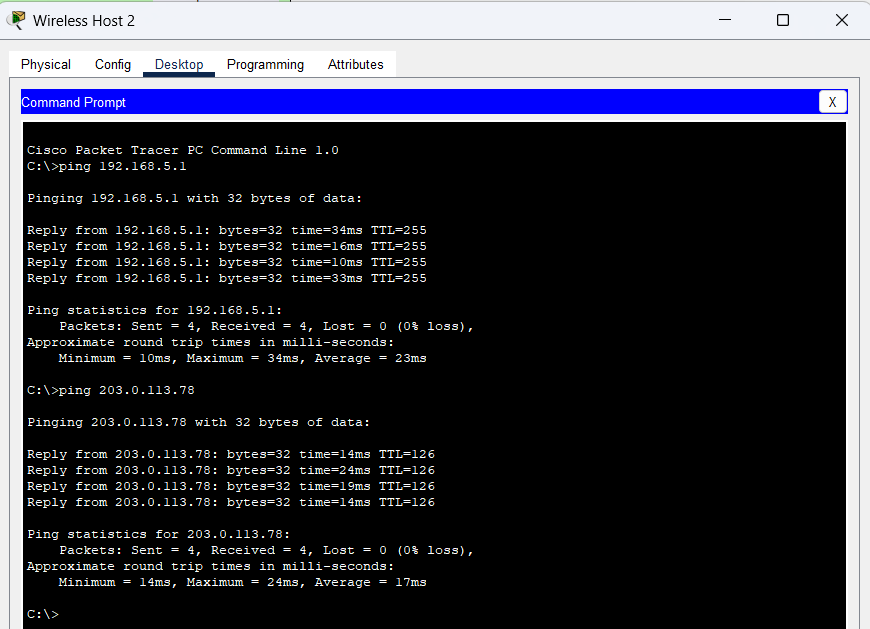
* **Wireless Host 2 to connect to Wireless VLAN 5.**
  + For Wireless Host 2 to connect to WLAN 5, **WLC-1 interface** was configured as **WLAN 5** **(192.168.5.254, gateway 192.168.5.1, DHCP 192.168.5.1)**.
  + **SSID-5** was set up under profile **Wireless VLAN 5** using **WPA2-Enterprise**.
  + **RADIUS server** configured at **10.6.0.254** with shared secret **RadiusPW**; credentials: **userWLAN5 / userW5pass**.
  + **LAP-1** registered to **WLC-1** and **CAPWAP tunnel** confirmed **active**.
  + On **Wireless Host 2**, a matching profile was created under **PC Wireless**, and a successful connection was established.
  + **Ping results** confirmed successful connectivity from **Wireless Host 2**.

Figure 3: Ping results for Wireless Host 2