Edge Hill University

Faculty of Arts and Science

The Department of Computer Science

CIS2707

Computer Networks

Level 5

Coursework 1 Home Wireless Network Scenario 2024/2025

Thomas Mason

26040247

Module Leader: Hamed Balogun

☎ 01695 65 6795

Email: hamed.balogun@edgehill.ac.uk

Administrators:

☎ 01695 65 7603

Table of Contents

Introduction:

This report presents the evaluation and testing of the home wireless network which was designed and built for a three bedroomed student accommodation. The network is designed to support multiple smart devices, laptops, and streaming/gaming equipment across two floors. Overall, this report focuses on covering the testing of the network, assessing the security features, identifying potential limitations, and providing recommendations for further improvement.

Testing Methodology:

Multiple tests were performed using Cisco Packet Tracer to evaluate the performance and security of the wireless network. The primary objective in testing is to assess how well the network is able to handle a wide range of various devices across different parts and locations, focusing on key metrics such as latency, packet loss and signal strength (Digital Samba, 2023).

The following devices were included in the test:

- 5 Laptops (3 Main, 2 Guest)
- 1 Gaming Console
- 1 Smart 4K TV
- 5 Smart Lights (3 Main, 2 Guest)
- 3 Smartphones
- 2 Smart Speakers
- 4 Tablets (3 Main, 1 Guest)

Note: Devices on the Main Network were on VLAN 10, while the Guest Network was on VLAN 20.

The tests were carried out as follows:

Latency ICMP Ping Test:

The latency was measured by using the ping command, it allows for the measurement of round-trip time between devices and the router (e.g, Laptop0 to Router, Gaming Console to Router) and between devices as well (e.g, Laptop 0 to Gaming Console); getting consistently low ping times indicates a responsive network (Bocco, 2024).

Packet Loss:

Implementing extended ping sessions (e.g., 100 packets) validates the network's reliability and stability; if any packets fail, it shows the network is inconsistent. However, if all packets are received, it shows the network is stable and reliable (Garn, 2024).

Connectivity to the Internet:

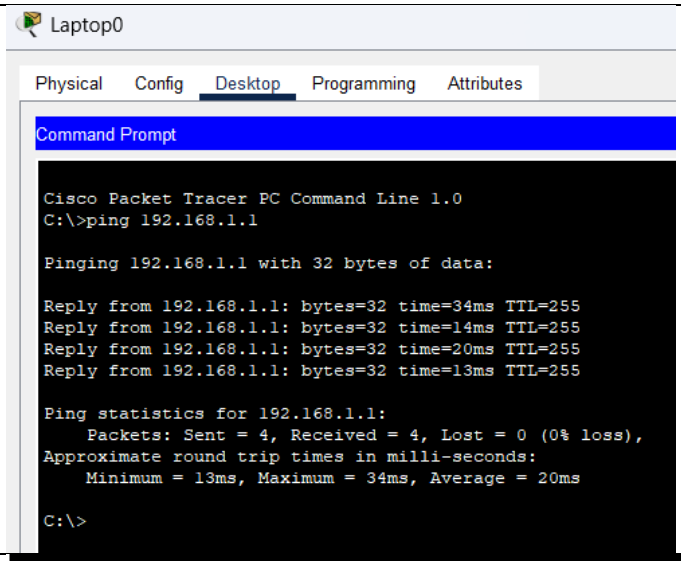
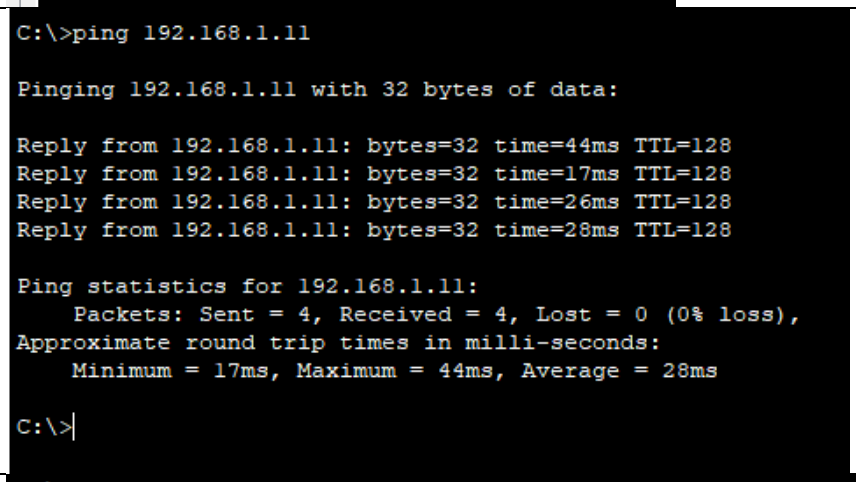
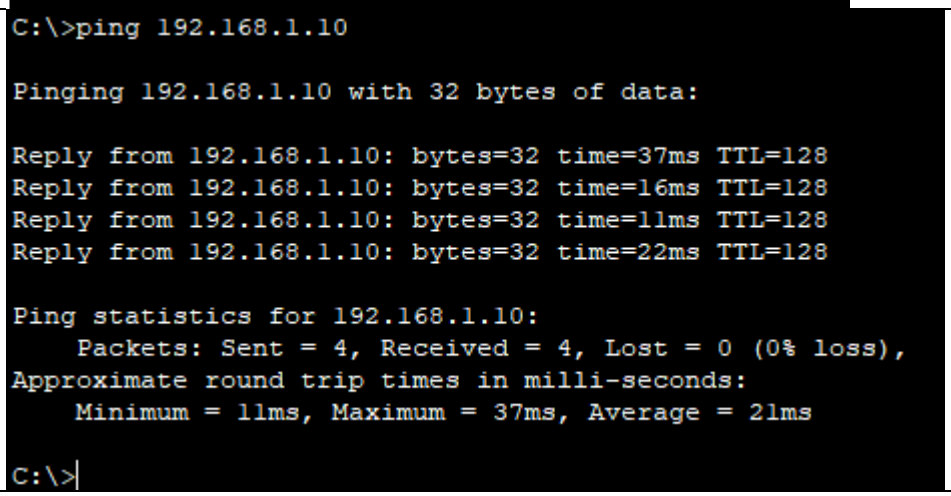
Internet Access was simulated using a static PC configured to a second router to represent an external web server with an IP address of '8.8.8.8'. Devices attempt to ping this to verify connectivity to the internet.

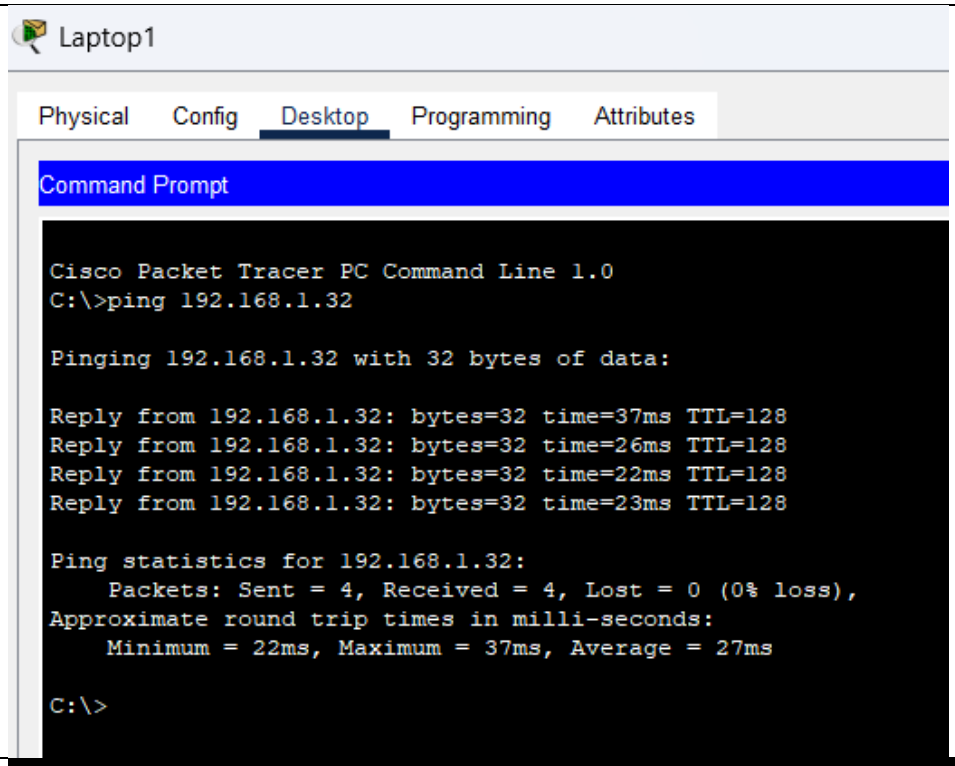
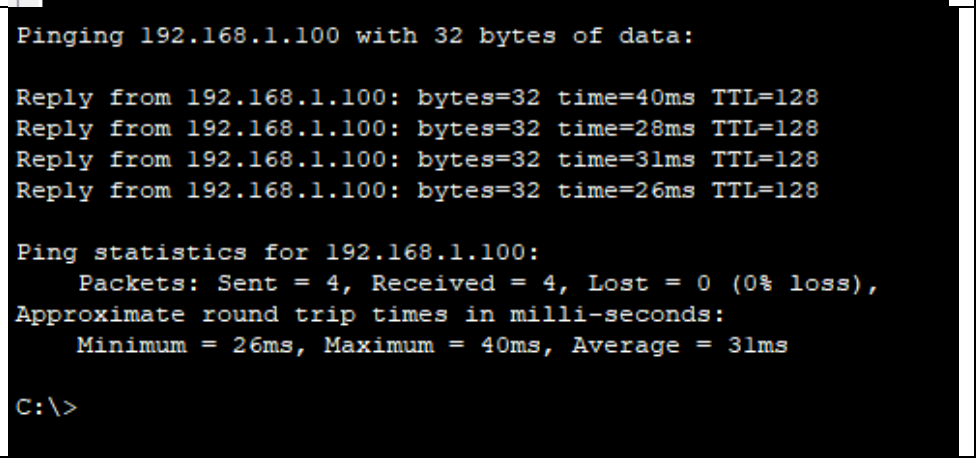
Signal Strength and Coverage:

Testing the Signal Strength can be replicated using the Laptop's PC Wireless GUI on the connect page to represent the signal strength and coverage with a visual strength indicator when scanning for the available networks to represent a realistic Wi-Fi coverage simulation.

Network Performance Evaluation:

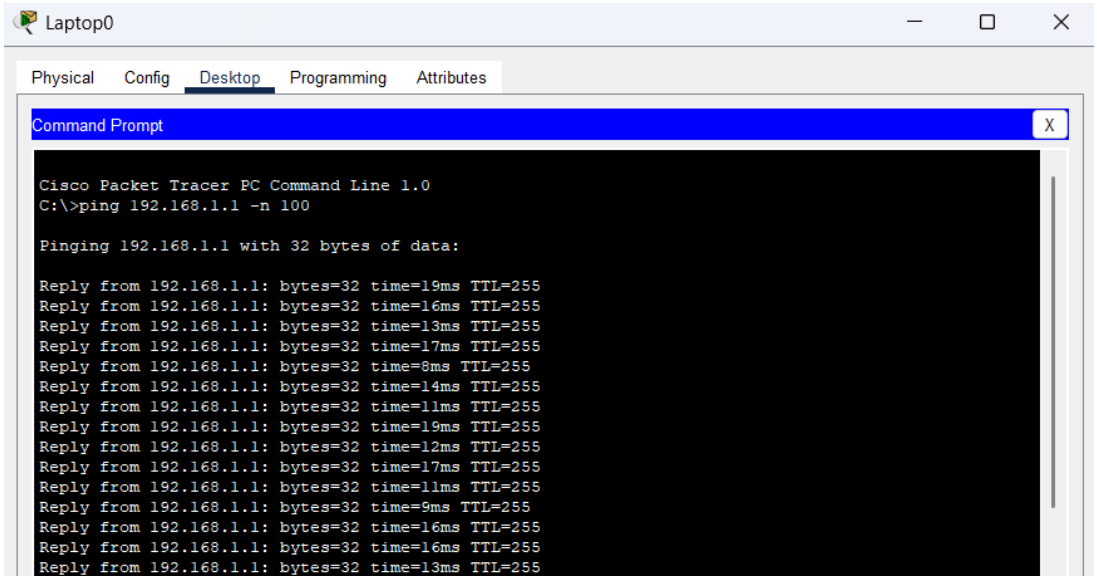
Latency ICMP Ping Test:

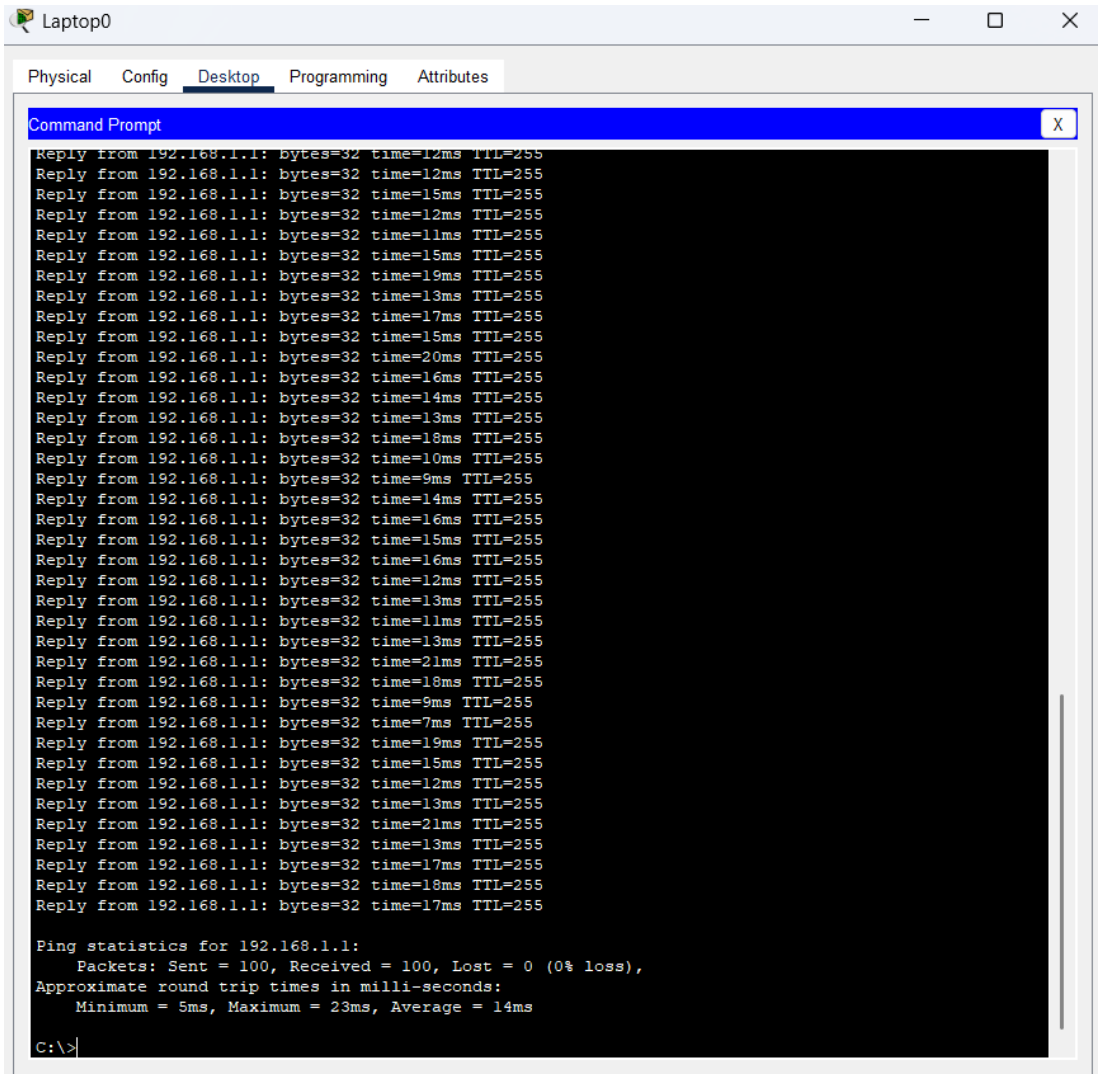
Ping Test	Screenshot
Laptop0 to 192.168.1.1 (Router). Average 20ms. 0% Packet Loss.	
Laptop0 to 192.168.1.11 (Gaming Console). Average 28ms. 0% Packet Loss.	
Laptop0 to 192.168.1.10 (4K Smart TV). Average 21ms. 0% Packet Loss.	

Laptop1 to 192.168.1.32 (Smart Light 3) Average 27ms. 0% Packet Loss.	
Laptop1 to 192.168.1.100 (Smartphone 2) Average 31ms. 0% Packet Loss.	

Packet Loss Test:

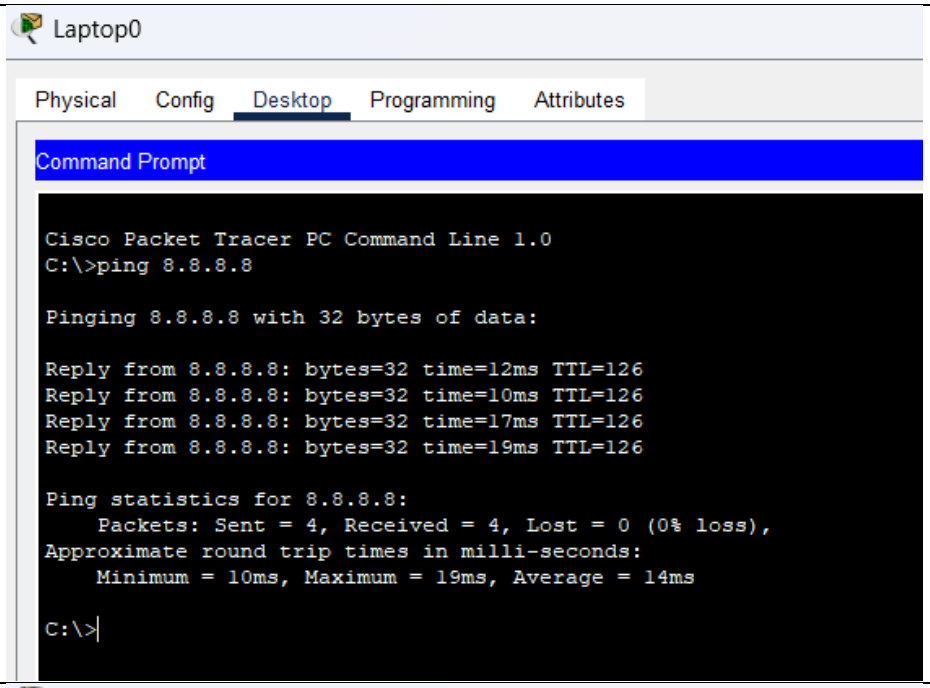
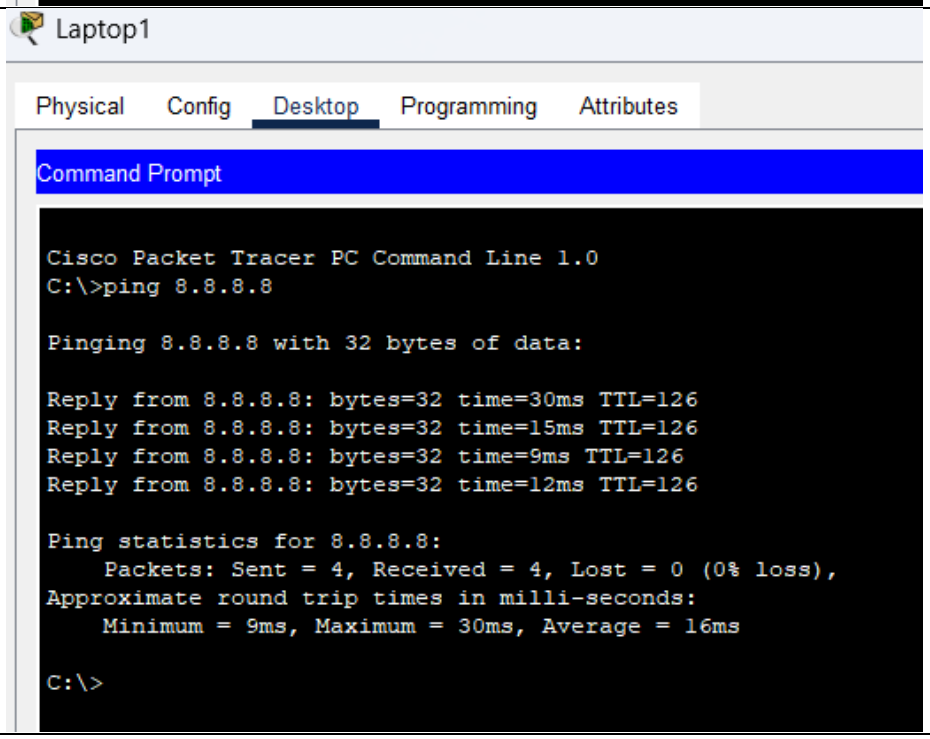
The image shows the testing of the stability of the network with 100 ping tests between the Laptop0 and router for any packet loss.

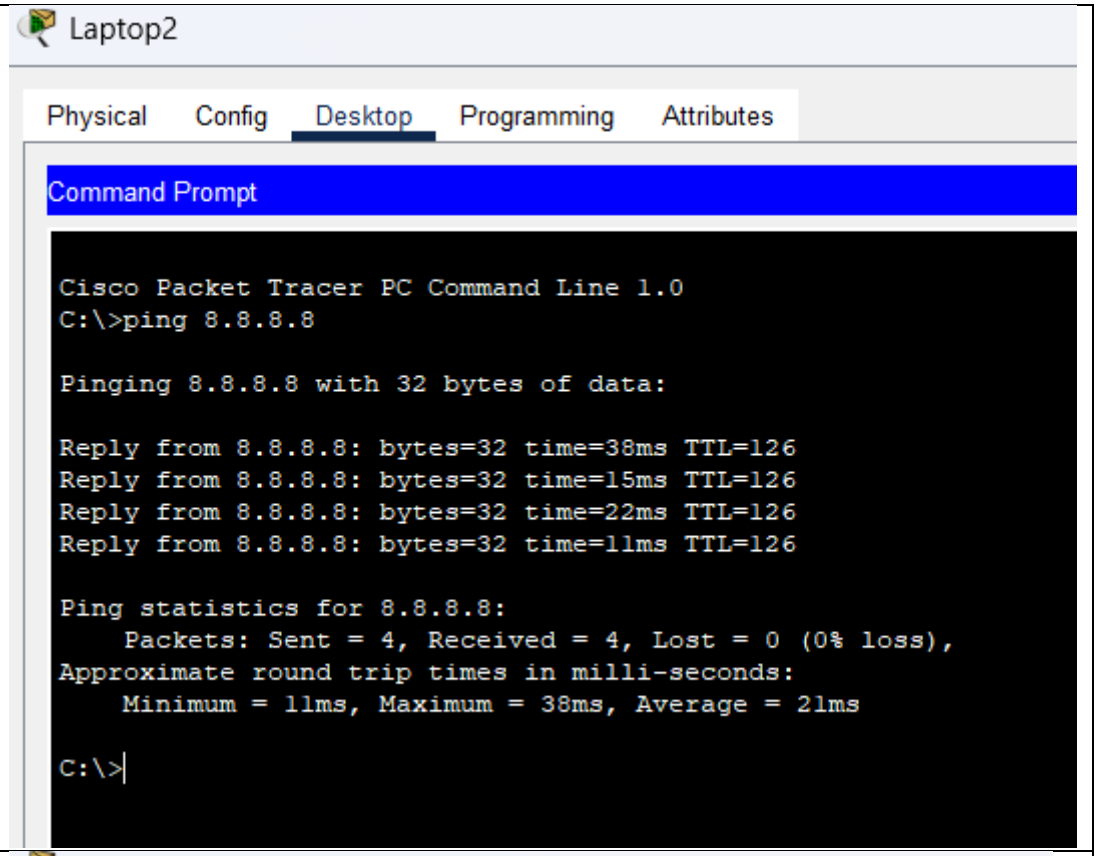
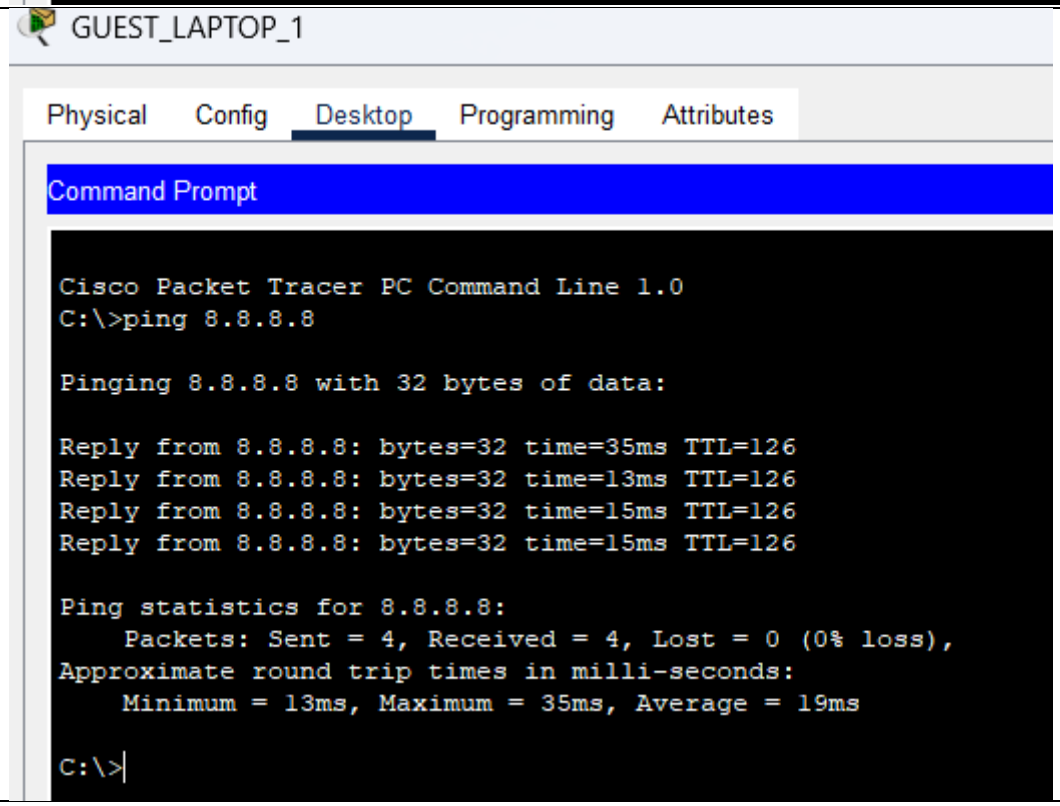


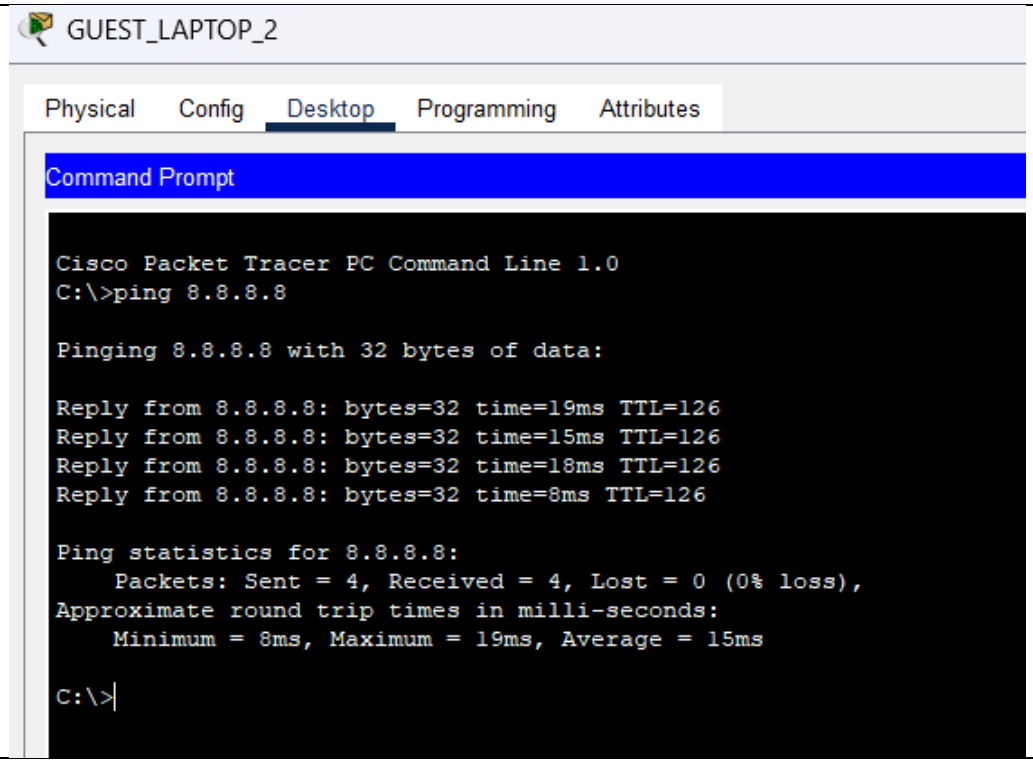


Device Connectivity to the Internet:

Pinging 8.8.8.8 to simulate an internet connection for the devices.

Device	Screenshot
Laptop0 to 8.8.8.8 Average 14ms. 0% Packet Loss.	
Laptop1 to 8.8.8.8 Average 16ms. 0% Packet Loss.	

Laptop 2 to 8.8.8.8 Average 21ms. 0% Packet Loss.	
Guest_Laptop1 to 8.8.8.8 Average 19ms. 0% Packet Loss.	

Guest_Laptop2 to 8.8.8.8	

Guest Network Security Test:

Testing the ACL 110 firewall between VLAN 10 and VLAN 20.

Device	Screenshot
VLAN 10 Main Network can successfully ICMP ping.	PDU List Window Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num | Edit Successful | Laptop0 | Smartphone1 | ICMP | 0.000 | N | 0 | (edit) Successful | Tablet PC1 | Smart Light 4 | ICMP | 0.000 | N | 1 | (edit) Successful | Smart Light 1 | 4K Smart TV | ICMP | 0.000 | N | 2 | (edit) Successful | Gaming Console | Tablet PC0 | ICMP | 0.000 | N | 3 | (edit) Successful | Laptop0 | Home_Router | ICMP | 0.000 | N | 4 | (edit)
VLAN 20 Guest Network can successfully ICMP ping.	PDU List Window Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num | Edit Successful | GUEST_LAPTOP_2 | GUEST_LAPTOP_1 | ICMP | 0.000 | N | 0 | (edit) Successful | GUEST_LAPTOP_1 | GUEST_PHONE_2 | ICMP | 0.000 | N | 1 | (edit) Successful | GUEST_TABLET_1 | GUEST_PHONE_1 | ICMP | 0.000 | N | 2 | (edit) Successful | GUEST_TABLET_1 | GUEST_LAPTOP_1 | ICMP | 0.000 | N | 3 | (edit) Successful | GUEST_PHONE_1 | Home_Router | ICMP | 0.000 | N | 4 | (edit)
The Guest Network (VLAN 20) can successfully ping the router but cannot ping any of the devices within the Main Network (VLAN 10).	PDU List Window Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num | Edit Successful | GUEST_TABLET_1 | Home_Router | ICMP | 0.000 | N | 0 | (edit) Failed | GUEST_TABLET_1 | Tablet PC0 | ICMP | 0.000 | N | 1 | (edit) Failed | GUEST_LAPTOP_2 | Laptop1 | ICMP | 0.000 | N | 2 | (edit) Failed | GUEST_LAPTOP_1 | Smartphone1 | ICMP | 0.000 | N | 3 | (edit) Failed | GUEST_TABLET_1 | Smart Light 4 | ICMP | 0.000 | N | 4 | (edit)

Network Load Test (Simulation Mode):

The image shows the simulation of network traffic to represent load on the router.

PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Laptop0	Smartphone0	ICMP		0.000	N	0	(edit)	
	Successful	Laptop1	Gaming Console	ICMP		0.000	N	1	(edit)	
	Successful	Laptop2	Smart Speaker 1	ICMP		0.000	N	2	(edit)	
	Successful	Smart Light 2	Tablet PC0	ICMP		0.000	N	3	(edit)	
	Successful	Smart Speaker 2	Smartphone1	ICMP		0.000	N	4	(edit)	
	Successful	Gaming Console	Tablet PC2	ICMP		0.000	N	5	(edit)	
	Successful	Smartphone2	Tablet PC1	ICMP		0.000	N	6	(edit)	
	Successful	Tablet PC2	Smartphone0	ICMP		0.000	N	7	(edit)	
	Successful	Tablet PC1	Smartphone2	ICMP		0.000	N	8	(edit)	

PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	GUEST_LAPT...	GUEST_LAPT...	ICMP		0.000	N	0	(edit)	
	Successful	GUEST_LAPT...	GUEST_TABL...	ICMP		0.000	N	1	(edit)	
	Successful	GUEST_TABL...	GUEST_PHON...	ICMP		0.000	N	2	(edit)	
	Successful	GUEST_PHO...	GUEST_LAPT...	ICMP		0.000	N	3	(edit)	

Signal Strength and Coverage:

Testing the signal strength of the network with the Laptops on the GUI PC Wireless Interface.

Device and Signal	Screenshot
Laptop0 5GHz 66% 2.4GHz 86%	

Laptop1 5GHz 69% 2.4GHz 89%	
Laptop2 5GHz 69% 2.4GHz 89%	

Security Evaluation:

The implemented network was designed with multiple security measures, which was tailored to the limitations of Cisco Packet Tracer. The evaluation of the security setup focuses on encryption, network segmentation and access control.

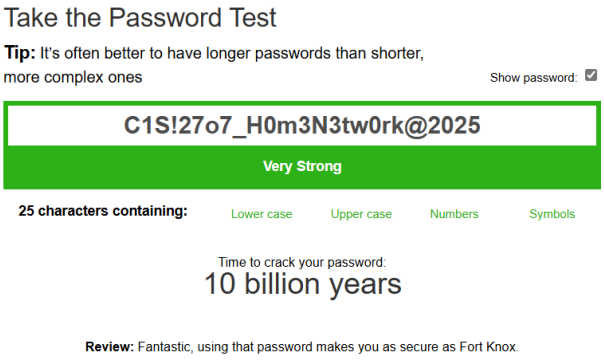
Encryption & SSID Security:

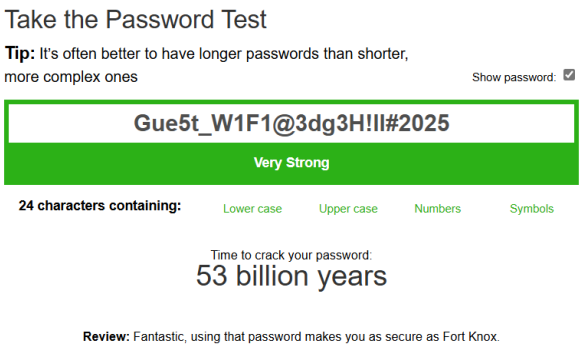
The wireless network uses WPA2 Encryption on both the Main (5GHz) and Guest (2.4GHz) networks. While WPA3 would have been a better solution for further enhanced protection against brute force dictionary attacks and stronger encryption (Šlekytė, 2023), it is not supported within Cisco Packet Tracer and therefore, WPA2 was the best choice available.

Furthermore, the SSID would have been typically hidden within real-world applications, eliminating the unnecessary broadcast for a potential vulnerability. However, this was not possible in Packet Tracer due to save restrictions.

Password Policies:

Both passwords were designed to meet the best practices for a home network and were set for both SSIDs, with a minimum of 12 characters and a mix of upper/lower-case characters, numbers, and symbols. This reduces the risk of brute force and dictionary attacks on the network, as seen in the screenshots from the password tester.





MAC Address Filtering:

While MAC address filtering was considered for the main 5GHz network for devices that are consistently on the network to create further security and integrity, this feature could not be implemented due to the limitations of AccessPoint-PTs not having this feature. However, in the real world, this feature would have been enabled to restrict access to only approved devices; however, note that this security feature can be bypassed with MAC address spoofing (Šlekytė, 2024).

Network Segmentation and VLANs:

Two VLANs were created to separate the network:

- VLAN 10 is the main network for trusted regular users and personal devices.
- VLAN 20 is the guest network for visitors.

By enforcing this segmentation using an Access Control List (ACL 110) applied inbound on VLAN 20, it blocks traffic from the guest devices on VLAN 20 attempting to reach the main devices on VLAN 10 while still allowing the created artificial internet connection. This prevents the guest network from becoming a vulnerability to the main network with the trusted devices, improving the internal security.

Firewall/Access Control:

While Cisco Packet Tracer does not support advanced firewall features, ACL 110 acts as a firewall by filtering traffic on the router. The ACL blocks multiple VLANs' access/communication with each other while allowing outbound communication for both VLANs (Simulationexams.com, 2025), creating a zone/bubble-based network.

Performance Limitations of the Network:

While the wireless network performed well under simulation conditions and met the core fundamentals and security requirements for the assignment, there are several limitations due to

both the design restrictions and Cisco Packet Tracer's capabilities. These particular limitations could have more of an impact on real-world usage in terms of coverage, performance, scalability, and security.

Signal Coverage Limitations:

- 2.4GHz on Channel 6
- 5GHz on Channel 36

Although dual-band access points were designed for floor-based coverage (5GHz Downstairs, 2.4GHz upstairs), using a 2.4GHz signal can cause interference with other household electronics and the neighbours (especially in urban student housing) due to its long range and high congestion, making it highly vulnerable to interference causing slower speeds and intermittent connections (Burrell, 2024). Theoretically, 5GHz is better in most cases due to its higher frequency speed. However, its range ability has lower wall penetration, causing potentially lower performance upstairs (www.alternativewireless.com, 2025).

No Real-Time Monitoring:

There are no monitoring systems or dashboards to track statistics such as:

- Device performance,
- Network utilisation
- Unexpected disconnections.

This limits the ability to monitor the network consistently, troubleshoot issues, and improve performance.

Packet Tracer Simulation Limitations:

Due to Cisco Packet Tracer's limitations, real-world networking simulations are not possible. Therefore, it paints an inaccurate picture of how a network could perform due to constraints such as:

- Walls, floors, and appliances such as microwaves all interfere with a wireless network and are not modelled correctly.
- Tests such as ICMP ping are simulated without actual network traffic flow and therefore are not accurate for variables such as latency, jitter and packet loss.
- Modern Wi-Fi 6 is not supported, which limits a real-world modern wireless internet.

Proposed Improvements:

Based upon the network's current performance and design, as well as considering the limitations of Cisco packet tracer, several improvements can be made in the real-world scenario to optimise the network for both performance and security.

Upgrade to a WPA3-compatible router:

While WPA2 is sufficient for this simulation, modern real-world routers support WPA3 encryption, which has increased protection for simple passwords and increased encryption against brute force attacks (Gillis, 2023). Overall, upgrading to a WPA3 router would improve security and future-proof the network against emerging threats.

Mesh Wi-Fi or Range Extenders:

While the current dual-band network provides decent coverage, 5GHz coverage could be a potential real-world issue when factors such as walls and a physical upstairs are taken into consideration. Therefore, a network typology like a mesh system could provide a much stronger signal throughout the household. Wi-Fi extenders could be used in key areas if the coverage isn't too much of an issue.

Enable MAC Address Filtering:

Due to the limitations of Cisco Packet Tracer, implementing MAC Filtering in my setup was not possible because the AccessPoint-PTs did not have that implementation. However, in a physical real-world network, this feature would be enabled to whitelist only the approved devices. While it may be able to bypass with MAC spoofing, it adds another layer of protection (Šlekytė, 2024).

Conclusion:

The home wireless network designed and tested within this report successfully met the requirements of supporting multiple users and devices for a three-bedroomed student accommodation. With the use of VLAN segmentation, DHCP configuration and simulated internet access, the network provided reliable performance across the board, with various devices providing consistent latency, zero packet loss and good signal coverage.

The security of the network was handled by multiple factors such as WPA2 encryption, strong password policies for the access points, and the segmentation between the Guest and Main network with ACLs to isolate the two VLANs, creating a very strong security configuration.

Despite all of these successes, there were limitations because of Cisco Packet Tracer's lack of support, including not including WPA3, Wi-Fi 6 and real-time monitoring. Gaps such as these highlight how while simulated environments are often helpful for concepts, they don't truly reflect the true complexities and features of real-world networking.

In conclusion, the network is well-designed, secure, and functional for the scenario's simulation. With the proposed improvements, such as mesh Wi-Fi, WPA3 routers, MAC filtering and monitoring tools, this network has the potential to be a high-performance, secure and future-proof real-world network.

Referencing:

Bocco, D., 2024. *What is ping?* [online] UptimeRobot Knowledge Hub. Available at: https://uptimerobot.com/knowledge-hub/devops/ping-explained/ [Accessed 10 Apr. 2025].

Burrell, S., 2024. *Understanding 2.4 GHz ISM Bands: A Practical Guide for Everyone.* [online] Wray Castle. Available at: https://wraycastle.com/blogs/knowledge-base/2-4-ghz-ism [Accessed 10 Apr. 2025].

Digital Samba, 2023. *A Deep Dive into the Network Performance Monitoring Metrics.* [online] Available at: https://www.digitalsamba.com/blog/a-deep-dive-into-the-network-performance-metrics [Accessed 10 Apr. 2025].

Garn, D., 2024. *How to perform packet loss tests and how they work.* [online] SearchNetworking. Available at: https://www.techtarget.com/searchnetworking/answer/How-to-test-for-packet-loss-on-a-broadband-connection [Accessed 10 Apr. 2025].

Gillis, A., 2023. *What is WPA3? - Definition from WhatIs.com.* [online] SearchSecurity. Available at: https://www.techtarget.com/searchsecurity/definition/WPA3 [Accessed 10 Apr. 2025].

Simulationexams.com, 2025. *Cisco Access Control Lists (ACL): Sim-ExTM Study Guide for CCNA.* [online] Available at: https://www.simulationexams.com/tutorials/ccna/Cisco-access-control-lists.htm [Accessed 10 Apr. 2025].

Šlekytė, I., 2023. *WEP, WPA, WPA2, and WPA3: Main Differences | NordVPN.* [online] NordVPN. Available at: https://nordvpn.com/blog/wep-vs-wpa-vs-wpa2-vs-wpa3/ [Accessed 10 Apr. 2025].

Šlekytė, I., 2024. *What is a MAC spoofing attack? Here's all you need to know | NordVPN.* [online] NordVPN. Available at: https://nordvpn.com/blog/mac-spoofing/ [Accessed 10 Apr. 2025].

www.alternativewireless.com, 2025. *5GHz WiFi Disadvantages vs 2.4GHz - Compare Two WiFi Freq.* [online] Available at: https://www.alternativewireless.com/resources/wifi-networking/5ghz-vs-2-4ghz-wireless-lan/5ghz-wifi-disadvantages.html [Accessed 10 Apr. 2025].