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: Network Scenario.

This document outlines the fundamental concepts and principles of designing a home wireless network for a three-bedroom student-shared accommodation. The network must provide sufficient connectivity throughout the household, including the shared living space on the ground floor, where activities such as studying, virtual meetings and online gaming/ streaming will happen.

The network must support multiple devices, including laptops, smartphones, smart TVs, smart speakers, smart lights, gaming consoles, and tablets, which all require stable and sufficient high-speed bandwidth. Additionally, the implementation of strong security measures is essential for protecting the network and minimising the potential for unauthorised access and cyber-attacks, ensuring a safe and reliable connection (CISA.gov, 2021).

Network Requirements Analysis.

Identifying Devices:

The home network must support a variety of devices within the network for the students within the household. Below, I have outlined what devices are going to be within the network and what students will use the devices for.

Device	User	Function	Bandwidth Needs
Laptop (x3)	All	Studying / Video Streaming / File Downloading	Medium - High
Smartphones (x3)	All	Communication / Video Steaming	Medium
Tablets (x3)	All	Studying / Video Streaming	Medium
Smart 4K TV	Shared	Video Streaming	High
Gaming Console	Shared	Online Gaming	High
Smart Speakers (x2)	Shared	Music / Voice Assistant	Low
Smart Lights (x4)	Shared	Home automation	Low

Table 1 – Devices within the network.

Laptops:

Each student has a single laptop for both their academic and personal use, and therefore, the laptops will need to require a stable Wi-Fi connection for multiple tasks such as:

- Online research and coursework – Browsing the internet and using cloud storage.
- Online meetings and camera streaming – Using platforms such as Microsoft Teams or Zoom for group discussions with other students for coursework.

- File downloads/uploads – Uploading and submitting assignments and downloading coursework and larger files such as software or big research files.
- Browsing and Video streaming – Watching Netflix, YouTube, lectures and other streaming platforms for entertainment and study purposes.

Smartphones:

Each student also has a single phone that connects to the Wi-Fi with common uses such as:

- Instant messaging and VoIP calls – Using FaceTime, WhatsApp or Skype to communicate with friends and family regularly.
- Social Media – Browsing Instagram, TikTok, Snapchat and Facebook.
- Background app activity – Automatic cloud backups and updates.
- Video Streaming and music – Watching Netflix, YouTube or streaming music on Spotify and Apple Music.

Tablets:

Each Student may use tablets for:

- Downloading e-books and PDFs and browsing the Web – Accessing textbooks and academic papers and researching.
- Taking Notes using programs such as OneNote for their coursework.
- Video streaming and browsing – watching Lectures, Netflix, YouTube, or browsing the internet.

Smart 4K TV:

A shared TV in the living room will require a high-speed Wi-Fi connection for:

- There is a shared Smart 4K TV in the living room, which will require a high-speed Wi-Fi connection for:
- Streaming 4K & HD Content – Used for services like Netflix, Amazon Prime and Disney+.
- Screen mirroring and casting – connecting smartphones or laptops for entertainment or presentations.
- Software firmware and app updates – The TV will need to be updated regularly to fix any security issues and keep apps up to date.

Gaming Console:

A shared gaming console within the living room requires a high-speed Wi-Fi connection for:

- Stable low-latency connectivity – essential for reliable online gaming.
- Large game downloads and updates – Frequent software updates and game installations.
- Voice chat – Online multiplayer communication.

Smart Speakers:

Smart speakers such as Amazon Echo or Google Nest Hubs require constant connectivity for:

- Voice commands and automation – controlling music, setting alarms and responding to users.
- IoT integration allows smart devices to automate processes and integrate with other devices (Griffith, 2024).

Smart Lighting:

Smart Lighting, such as smart bulbs or LED strips, connects through Wi-Fi and requires:

- Remote Control and Automation – App control and voice activation through smart speakers.
- Voice Adjustment – Altering the brightness and colour settings.

WLAN Devices and Security Solutions.

To build an efficient and secure WLAN, Wi-Fi security is needed to protect devices in the wireless network. Without Wi-Fi security, devices such as routers or wireless access points are unsecured and can be accessed by anyone within the range of the wireless signal (Cisco, 2025).

WLAN Devices:

- ISP Modem – Provides an internet connection from the service provider. (Hitron, 2025)
- Wireless Router (Cisco 1941) – This is a simple high bandwidth router that offers flexibility and efficiency (Cisco, 2017).
- Access Points (AccessPoint-PT-AC) – A reliable access point for home networks that provides stable connectivity and a strong connection across all rooms with supported Wi-Fi 5.

Security Solutions:

- WPA2-PSK (Wi-Fi Protected Access 2 - Pre-Shared Key) – This encryption helps prevent unauthorised users from accessing the network by a security protocol that uses a four-way handshake to establish encryption keys securely for protecting data on the WLAN connection. WPA2-PSK operates with a pre-shared passphrase that all the users within the Wi-Fi network share to enable encrypted communication (J. Guo, 2020). *Note: Cisco packet tracer (8.2.2.0400) does not support WPA-3; therefore, WPA2 is being used.*
- MAC Address Filtering – Improves wireless security by allowing devices that match the list of pre-approved addresses to be allowed. This, in theory, improves security

as it performs an additional check before accepting devices onto the network (Mitchell, 2021).

- Router Firewall Configuration – Protects the internal network from the external by analysing the incoming and outgoing traffic by preset rules. This creates a protective bubble for the network against potential software or hardware threats (Anon., 2025).
- Strong Password Policy – Using a complex and strong password is the first part of defence in a wireless network. To prevent the risk of password-related attacks to the network, a strong password with a variety of characters and upper and lowercase letters should be implemented (D'Andrea, 2024).
- Guest Network Setup – This helps to secure and simplify the network, giving the ability to run a separate network from the main. This added security benefit means users will not have access to the leading Wi-Fi network or devices connected to it, protecting shared folders, NAS drives or printers. Another advantage is that the guest Wi-Fi password can be simplistic for users to access as it is entirely separate from the leading home network (Crawford, 2023).

Wireless Network Design & Requirements.

Coverage:

- Dual-band Wi-Fi: 2.4Ghz for range, 5Ghz for speed
- 2.4 GHz to be used for devices upstairs.
- 5 GHz is to be used downstairs.
- Additional access points if coverage issues arise.

Bandwidth Requirements:

The household consists of three students and multiple devices actively using the bandwidth at any given time. For this reason, the network must have adequate bandwidth and latency. Below are the network types of traffic with varying bandwidth and latency requirements:

Activity	Bandwidth Requirement	Latency Requirements
Web Browsing	1-3Mbps	Low
Video Calling	2-5Mbps	High
HD Video Streaming	5-10Mbps	Medium
4K Video Streaming	15-25Mbps	High
Online Gaming	3-10Mbps	High
Large file downloads	10-50Mbps	Low

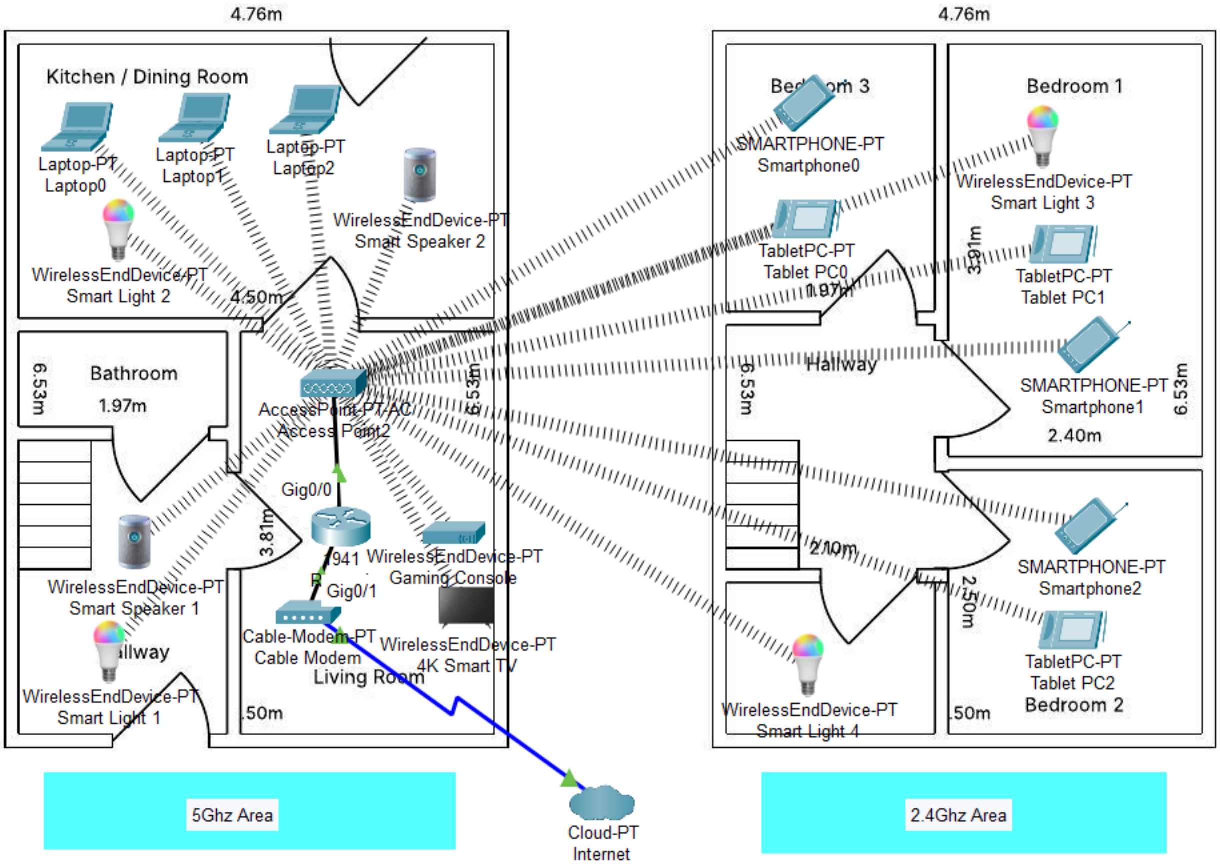
Table 2 – Types of Network Traffic

Because the network demands, such as online gaming video streaming, are latency-dependent and file downloads are bandwidth-intensive, the network design must have sufficient speed and coverage for multiple intensive tasks. For this reason, I plan to have an ISP bandwidth of at least **150Mbps** to handle multiuser usage.

User Requirements:

The wireless network for the three users (students) must be reliable and have a fast connection so students have an uninterrupted connection for studying, online classes and research. Security is another significant requirement for the privacy of the students, and therefore, WPA2 (Wi-Fi Protected Access 2) encryption and MAC address filtering should be implemented to prevent unauthorised access. The network should also be able to handle multiple devices simultaneously without performance drops and packet loss and have minimal lag and stable bandwidth for online gaming. Furthermore, the Wi-Fi should have a separate network with limited access for guests for security. Finally, the network needs to be scalable and allow for additional devices, such as new smart home devices in the future.

Network Diagram:



IP Addressing Scheme.

IP Addresses Static:

Device Type	IP Assignment Type	IP Address
Router	Static	192.168.1.1
4K Smart TV	Static	192.168.10
Gaming Console	Static	192.168.11
Smart Speakers	Static	192.168.20, 192.168.21
Smart Lights	Static	192.168.30, 192.168.31, 192.168.32, 192.168.33

Table 3 – Static IP Addresses

Dynamic IPs (DHCP Assigned):

Device Type	DHCP Pool	IP Range
Students Laptops, Phones, and Tablets	Main Network	192.168.1.100 – 192.168.1.149
Guest Devices (Visitors, Friends, etc)	Guest Network	192.168.150 – 192.168.1.200

Table 3 – Dynamic IP Ranges

Security Protocols:

WPA2-PSK Encryption (Wi-Fi Protected Access 2 – Pre-Shared Key) – The wireless access point will use WPA2-PSK along with a strong password, providing the network with 128-bit encryption. This provides a high level of protection against brute force attacks and offline password cracking (Sr., 2023). *Note: Cisco packet tracer (8.2.2.0400) does not support WPA-3; therefore, WPA2 is being used.*

Firewall Configuration – Using the router's built-in firewall will monitor and filter the incoming and outgoing traffic as well as configure devices to restrict access for further protection, which will protect against unauthorised access attempts and prevent DDos attacks.

Guest Network Setup – There will be a separate SSID from the network for the guests, which will have restricted bandwidth and no access to the internal devices. This, in turn, will prevent access to devices within the leading network, reducing the potential vulnerabilities from untrusted devices.

MAC Address Filtering – The devices with preapproved MAC Addresses that are registered on the router will only be able to connect to the network. However, on the Guest network, there will be no restriction to joining, but this is a separate network from the main one.

MAC filtering prevents authorised users from joining the network without being registered, even if they know the password.

SSID Naming and Hiding – The leading network will not be broadcasted, and the guest SSID will not be identifiable from the house name/number (e.g. "Network5Ghz"), which reduces the chances of Wi-Fi snooping and targeted attacks.

Conclusion.

The wireless network design ensures that the connectivity, security and efficiency aspects of the network are all covered within the student shared home. The security of the network will be more than adequate for the student home network with WPA2-PSK encryption and MAC address filtering, the implementation of dual band Wi-Fi, static and dynamic IP addresses, and a guest network reassures users/devices that they can use the network and guarantee a high performance and reliable experience without interference and security issues. Furthermore, the router firewall and the SSID protection further improve the security aspects against unauthorised access and potential threats.

Overall, this wireless network offers potential scalability within the future with more devices or higher bandwidth and provides a secure, stable and high-performance network for the students relying on it for their work and entertainment.

References

Anon., 2025. *What is a firewall?.* [Online]
Available at: https://www.cisco.com/site/uk/en/learn/topics/security/what-is-a-firewall.html
[Accessed 28 02 2025].

CISA.gov, 2021. *Securing Wireless Networks.* [Online]
Available at: https://www.cisa.gov/news-events/news/securing-wireless-networks#:~:text=So%2C%20if%20your%20neighborhood%20is,traffic%2C%20or%20steal%20personal%20files.
[Accessed 27 02 2025].

Cisco, 2007. *Cisco 1800 Series Integrated Services Routers.* [Online]
Available at: https://www.andovercg.com/datasheets/cisco-1841-router.pdf

Cisco, 2014. *Cisco Aironet 3700 Series Access Points.* [Online]
Available at:
https://www.cisco.com/c/dam/global/en_ph/solutions/smb/velocity/Downloads/ap3700_datasheet.pdf
[Accessed 27 02 2025].

Cisco, 2017. *Cisco 1941 Series Integrated Services Routers Data sheet.* [Online]
Available at: https://www.cisco.com/c/en/us/products/collateral/routers/1900-series-integrated-services-routers-isr/data_sheet_c78_556319.html
[Accessed 27 02 2025].

Cisco, 2025. *What Is Wi-Fi Security?.* [Online]
Available at: https://www.cisco.com/c/en/us/products/wireless/what-is-wi-fi-security.html
[Accessed 27 02 2025].

Crawford, D., 2023. *What is a guest network? – Why you need one and how to set one up.* [Online]
Available at: https://protonvpn.com/blog/guest-networks
[Accessed 28 02 2025].

D'Andrea, A., 2024. *The Importance of Strong Passwords in 2024.* [Online]
Available at: https://www.keepersecurity.com/blog/2024/07/10/the-importance-of-strong-passwords-in-2024/
[Accessed 28 02 2025].

Griffith, B., 2024. *What Is IoT Integration? A Comprehensive Guide.* [Online]
Available at: https://www.workato.com/the-connector/iot-integration/#:~:text=IoT%20integration%20connects%20smart%20devices,and%20analyze%20your%20activity%20data.
[Accessed 27 02 2025].

Hitron, 2025. *The Difference Between a Modem and a Router.* [Online]
Available at: https://us.hitrontech.com/learn/the-difference-between-a-modem-and-a-router/#:~:text=A%20modem%20is%20a%20device,computer%2Flaptop%20or%20your%20router.
[Accessed 27 02 2025].

J. Guo, M. W. H. Z. a. Y. Z., 2020. A Secure Session Key Negotiation Scheme in WPA2-PSK Networks. *2020*, 25-28 May, p. Section 1.

Mitchell, B., 2021. *MAC Address Filtering: What It Is and How It Works.* [Online]
Available at: https://www.lifewire.com/enabling-mac-address-filtering-wireless-router-816571
[Accessed 28 02 2025].

Sr., M. A. F., 2023. *WPA2-PSK Wi-Fi Encryption: The Ultimate Guide.* [Online]
Available at: https://firewalltimes.com/wpa2-psk/
[Accessed 01 03 2025].