19L055 – WLAN TECHNOLOGY

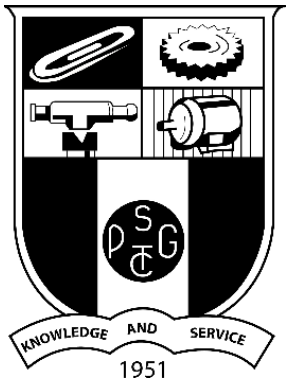
CREATING MULTIPLE VAPs

Dissertation submitted on Partial Fulfilment of the requirements of the degree of

BACHELOR OF ENGINEERING

Branch: ELECTRONICS AND COMMUNICATION ENGINEERING

Affiliated to Anna University



APRIL 2025

SUBMITTED BY

JAISURYA S (22L225)

AKASH S (22L285)

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

PSG COLLEGE OF TECHNOLOGY

(Autonomous Institution)

Coimbatore – 641 004

Contents

1. INTRODUCTION

In modern wireless networking, the demand for multiple, segregated networks within the same environment has steadily increased. Traditionally, achieving this required deploying multiple physical access points (APs), each broadcasting a separate network. However, this approach led to higher hardware costs, increased power consumption, network interference, and complex maintenance overhead. As wireless standards evolved from Wi-Fi 4 (802.11n) to Wi-Fi 5 (802.11ac) and now to Wi-Fi 6 (802.11ax), the need for smarter, more efficient network management solutions became critical — particularly in environments like offices, campuses, hospitality, and public spaces.

This is where Virtual Access Points (VAPs) emerged as a scalable, cost-effective alternative. VAPs allow a single physical AP to broadcast multiple SSIDs, each functioning as an independent network with its own security settings and policies. Introduced widely with the maturing of Wi-Fi 5 infrastructure, and further refined in Wi-Fi 6 networks, VAPs leverage software-defined networking techniques to virtualize wireless interfaces. This not only reduces physical hardware requirements but also enhances network segmentation, client isolation, and bandwidth management — critical for handling dense, multi-device environments seen in today's Wi-Fi 6 deployments.

To implement such advanced configurations, open-source firmware platforms like **OpenWrt** have become increasingly popular. OpenWrt is a Linux-based firmware designed for routers and embedded devices, offering users far greater control than typical stock firmware. By flashing OpenWrt onto a Wi-Fi 6 router **TP-Link Archer AX23**, network administrators can unlock capabilities like creating multiple VAPs, advanced VLAN management, firewall configurations, and bandwidth optimization — effectively transforming a standard consumer router into a professional-grade networking tool tailored for modern, high-density wireless environments.

2. PROBLEM WITH MULTIPLE PHYSICAL APs

In traditional wireless network setups, when there's a requirement to create multiple isolated networks — for example, separating an internal corporate network from a guest network or

segmenting IoT devices from business-critical systems — the most straightforward solution was to deploy multiple physical Access Points (APs). While this may initially seem like a reliable approach, it introduces several operational challenges. First and foremost, it significantly increases the initial investment in hardware, cabling, and power infrastructure. In large-scale environments such as office complexes, educational campuses, hotels, or hospitals, deploying multiple APs for each network requirement leads to unnecessary hardware redundancy and elevated capital expenditure.

Beyond the financial aspects, managing multiple physical APs adds layers of complexity to network administration. Each AP requires separate configuration, firmware updates, security patches, and performance monitoring. This makes network management time-consuming and prone to human error, especially when scaling up to dozens or hundreds of APs. Furthermore, with multiple APs operating within close proximity, there's a heightened risk of signal overlap and channel interference. This degrades the overall wireless performance, resulting in unstable connections, reduced throughput, and poor user experience. Additionally, maintaining physical APs for different SSIDs limits network flexibility, as any changes in the network structure would require hardware modifications, physical relocation, or additional cabling — making it inefficient in dynamic or rapidly growing environments.

3. VIRTUAL ACCESS POINTS

A **Virtual Access Point (VAP)** is a software-based networking technique that allows a single physical Access Point (AP) to broadcast multiple SSIDs, each functioning as an independent wireless network. This concept gained momentum alongside the evolution of Wi-Fi standards — particularly from Wi-Fi 5 (802.11ac) onward — as the demand for dynamic, scalable, and secure wireless environments increased. VAPs operate by virtualizing the wireless radio interface of the AP, enabling it to simultaneously support multiple logical networks over the same physical hardware. Each SSID created through a VAP can have its own set of security protocols, authentication mechanisms, Quality of Service (QoS) policies, and access restrictions, offering precise control over how devices connect and interact within a shared wireless environment.

From a networking architecture perspective, each VAP can be linked to a different **VLAN (Virtual Local Area Network)**, ensuring complete traffic isolation between networks. This means guest devices can connect to a dedicated SSID without gaining access to sensitive internal systems, while IoT devices can be restricted to a separate, bandwidth-limited network with custom firewall rules. In Wi-Fi 6 deployments, where high device density, security segmentation, and bandwidth optimization are critical, the use of VAPs significantly enhances operational flexibility. Network administrators can efficiently segment traffic, enforce tailored security policies, and manage diverse device groups — all without adding extra hardware. This makes VAP configurations an ideal choice in environments like enterprise campuses, educational institutions, healthcare systems, and smart buildings, where reliable, high-performance, and scalable wireless infrastructure is essential.

4. OPENWRT

OpenWrt is a game-changer in the world of wireless networking, enabling advanced users and network administrators to push the boundaries of what consumer routers are capable of. At its core, OpenWrt is an open-source, community-driven operating system built on the Linux kernel, designed specifically for embedded devices such as routers, gateways, and wireless access points. Unlike stock firmware typically provided by router manufacturers, which often limits users to basic settings, OpenWrt provides complete access to the underlying system, enabling advanced configuration and optimization of network performance. This flexibility is especially crucial in environments that require customized network setups and performance tuning, such as when multiple Virtual Access Points (VAPs) need to be managed on a single device.

OpenWrt's architecture allows users to customize almost every aspect of their router's functionality. Whether it's configuring multiple SSIDs, setting up different VLANs, controlling bandwidth per client, or optimizing security protocols, OpenWrt gives complete control over how the router behaves. This becomes particularly important in Wi-Fi 6 networks, where high-density usage, improved throughput, and stringent security demands require fine-tuned configurations. The ability to create multiple VAPs on a single router through OpenWrt is one of its standout features, allowing businesses, educational institutions, and service providers to segment traffic efficiently without investing in additional hardware. For example, a single TP-Link Archer AX23

running OpenWrt can serve as several isolated wireless networks, each with its own policies, access rules, and security settings.

A key advantage of OpenWrt is its extensive package management system. The router can be expanded with additional features or customized services by installing packages directly from the OpenWrt repository, offering flexibility that proprietary firmware simply cannot match. The system supports everything from advanced firewall configurations, VPN setups, and custom routing protocols to traffic shaping and load balancing — all of which contribute to a more robust and adaptable network infrastructure. In enterprise or service provider settings, OpenWrt also ensures that the network is always up-to-date with security patches and new feature implementations, thanks to the active, open-source community that constantly contributes to its development.

Moreover, OpenWrt offers dual interfaces: the **LuCI web interface** for easier, more intuitive management and the **command-line interface (CLI)** for power users who need more granular control. The latter allows for in-depth configuration of network services, routing, and monitoring, making it perfect for professionals who require a tailored, high-performance networking setup. The combination of usability and depth makes OpenWrt ideal for not only those experimenting with custom network setups but also for businesses that need a reliable, secure, and scalable solution to meet their growing networking needs.

Finally, OpenWrt's open-source nature means there are no licensing fees, offering a highly cost-effective alternative to proprietary solutions. It can be flashed onto a wide range of routers, including the **TP-Link Archer AX23**, providing businesses and individuals with a feature-rich, customizable platform without the need for expensive enterprise-grade hardware. As Wi-Fi 6 networks become the standard in high-density environments, OpenWrt provides the necessary tools to ensure that these networks remain flexible, efficient, and secure, ultimately helping organizations meet their growing demands without sacrificing performance or budget.

5. INSTALLING OPENWRT ON TP-LINK ARCHER AX23

Step 1: Verify Router Compatibility Before proceeding, ensure that your **TP-Link Archer AX23** router is supported by OpenWrt. Visit the official OpenWrt Table of Hardware and search for the

Archer AX23 to confirm that OpenWrt has a stable release for your router model. Make sure to note the specific OpenWrt build version that corresponds to your router's hardware revision.

Step 2: Download OpenWrt Firmware

- Go to the OpenWrt Downloads page and select the appropriate firmware for the TP-Link Archer AX23.
- Choose the **stable release** and download the **factory image** suitable for your router model. The factory image is used for the initial installation of OpenWrt.

Step 3: Prepare the Router

- Ensure that the router is plugged in and connected to a computer or laptop via an Ethernet cable. It's important to use a wired connection to avoid any disruptions during the firmware installation.
- Make sure you have access to the router's **web interface** (this is typically accessible at **192.168.0.1** or **192.168.1.1**).

Step 4: Access the Router's Admin Interface

- Open a browser and enter the IP address of the router's web interface (e.g., **192.168.0.1**).
- Log in to the admin panel using the default credentials. The default login is usually:
    - **Username**: admin
    - **Password**: admin or the one on the label of your router.

Step 5: Backup Current Configuration Before flashing OpenWrt, it's always recommended to back up the current configuration in case you need to restore it later:

- In the router's admin interface, navigate to the **System Tools** or **Backup/Restore** section.
- Click **Backup** to save the current router configuration to your computer.

Step 6: Flash OpenWrt Firmware

- In the router's web interface, navigate to the **Firmware Upgrade** or **System Upgrade** section.
- Click on **Choose File** and select the OpenWrt **factory image** that you downloaded earlier.
- Confirm the upgrade by clicking **Upgrade**. The router will begin the firmware flashing process. **Do not disconnect** the router or interrupt the process, as doing so could result in a bricked device.

Step 7: Wait for Reboot

- The router will automatically reboot after the firmware is flashed. This may take a few minutes.

- Once the router has rebooted, the OpenWrt firmware will be running on your TP-Link Archer AX23.

Step 8: Access OpenWrt Web Interface (LuCI)

- After the router has rebooted, open your browser again and navigate to **192.168.1.1** (the default IP address for OpenWrt).
- You should now see the OpenWrt web interface (**LuCI**).
- The default login credentials for OpenWrt are:
    - **Username**: root
    - **Password**: (no password by default; you will be prompted to set one upon first login).

Step 9: Set Up a New Password

- The first time you log into OpenWrt, you'll be prompted to set a new password for the **root** user. Set a strong password to secure your router.

Step 10: Configure Basic Settings

- Once logged into the LuCI web interface, configure the basic settings:
    - Set the **hostname** for your router.
    - Adjust **WAN** and **LAN** interfaces if necessary.
    - Set up the **Wi-Fi** settings (SSID, security type, etc.) under the **Wireless** tab.

Step 11: Install Additional Packages (Optional)

- OpenWrt provides a rich set of features, but additional packages can be installed to extend functionality. For instance, you can install **VAP (Virtual Access Points)** packages or any other services you need (e.g., VPNs, traffic management tools).
- To install additional packages, go to the **System** menu > **Software**, and use the **opkg** package manager to install desired software.

Step 12: Reboot the Router After configuring your router to your liking, reboot it to ensure that all settings take effect correctly. You can reboot through the **System** > **Reboot** menu in the LuCI interface.

6. CREATING VIRTUAL ACCESS POINTS

6.1. Understanding Wireless Configuration in OpenWrt

In OpenWrt, all wireless settings are stored in /etc/config/wireless, which is managed using the Unified Configuration Interface (UCI) system. Wireless configuration - two major components:

- config wifi-device: Describes physical radio hardware (e.g., radio0 for 2.4 GHz, radio1 for 5 GHz).
- config wifi-iface: Describes individual logical interfaces (VAPs) that operate on a radio.

Each VAP is defined as a separate config wifi-iface section with unique settings. Some of those settings are:

- option ssid: Name of the wireless network
- option network: Assigned logical interface (LAN, guest, etc.)
- option encryption: Security mode (e.g., WPA2-PSK)
- option mode: Typically set to ap for Access Point mode

By creating multiple wifi-iface entries under the same radio, we can broadcast multiple SSIDs (VAPs) on a single physical wireless interface. It also shares bandwidth and airtime but can be isolated at the IP/network layer.

6.2.Creating VAPs using LuCI (GUI)

LuCI (Lua Configuration Interface) provides a simple and user-friendly way to configure the router. Step-by-step procedure for creating VAPs using LuCI is given below.

i. Login to LuCI:

- Connect to the router via browser at 192.168.1.1
- Use your root password to log in.

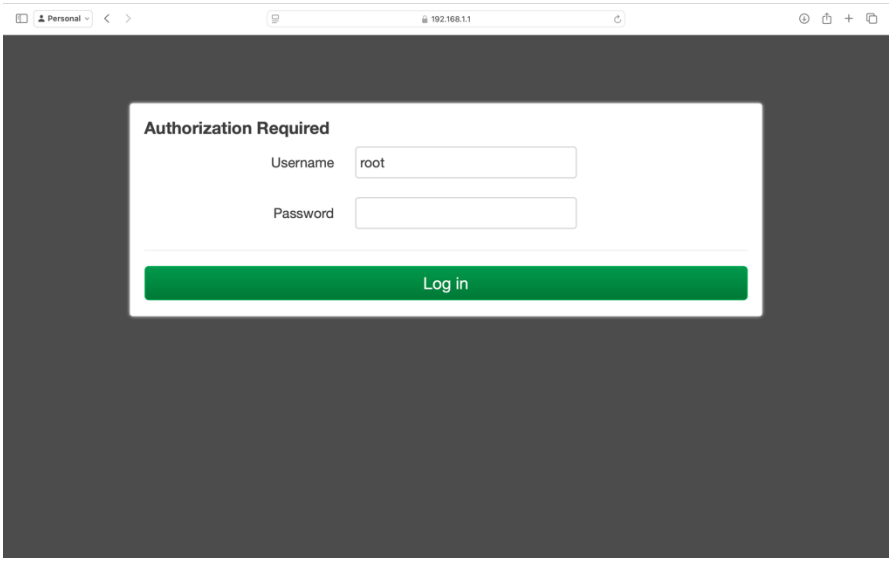


Fig 1. User login page of LuCI

ii. Navigate to Wireless Settings:

- Go to Network → Wireless.
- You will see available radios (e.g., radio0, radio1) and existing SSIDs.

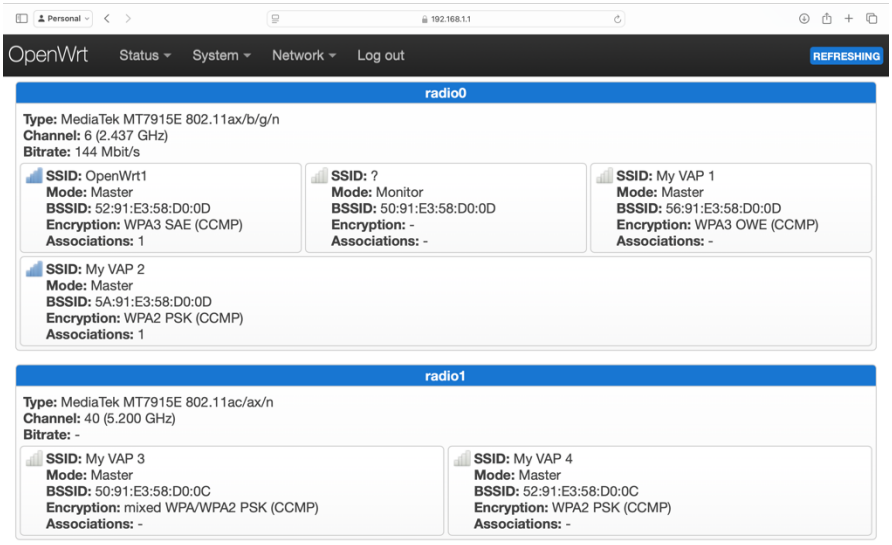


Fig 2. List of active SSIDs in respective radios in Home page

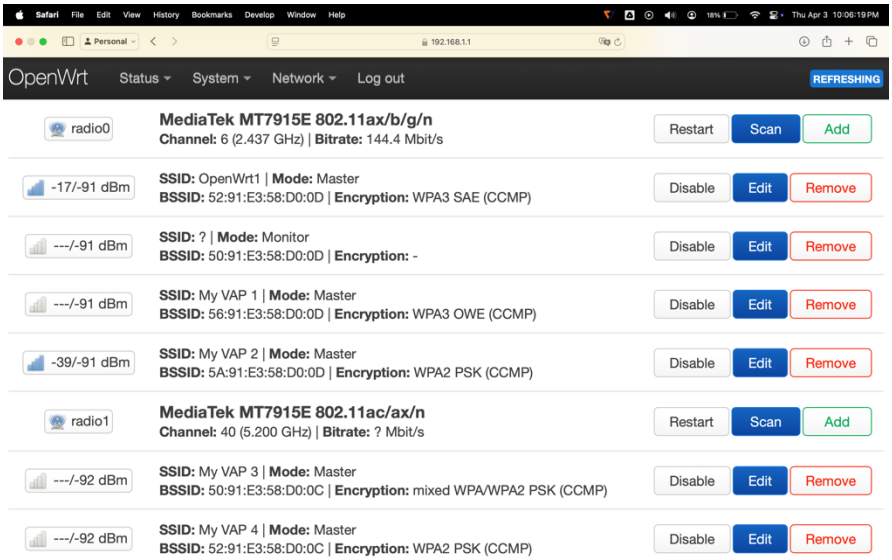


Fig 3. List of radios and configured SSIDs in Wireless configuration page

iii. Add a New VAP:

- Click “Add” next to the desired radio
- Set the SSID: e.g., “My VAP 1”

- Mode: Set to Access Point
- Network: Choose the network interface (e.g., lan)

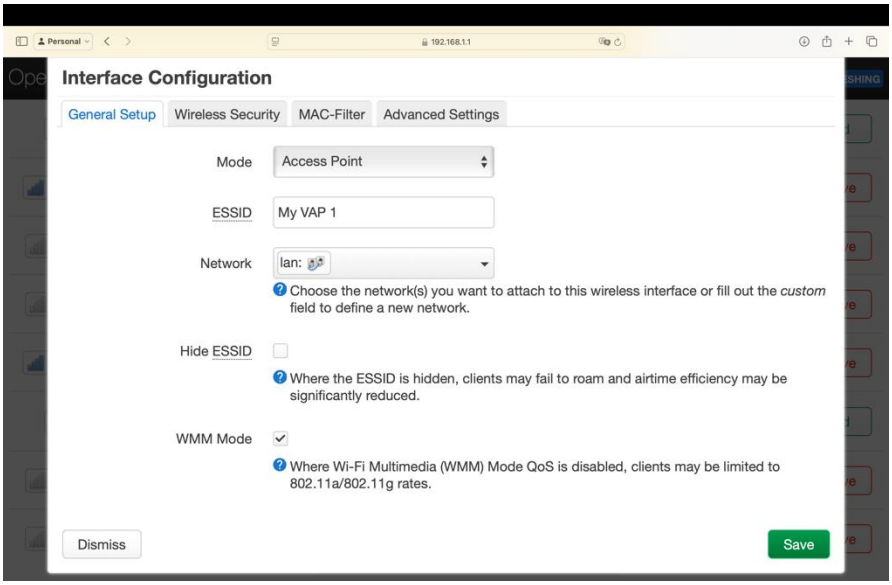


Fig 4. General Setup tab of Interface Configuration window

- Encryption: Choose the security protocol (e.g., WPA3-SAE)
- Key: Enter the password for this SSID

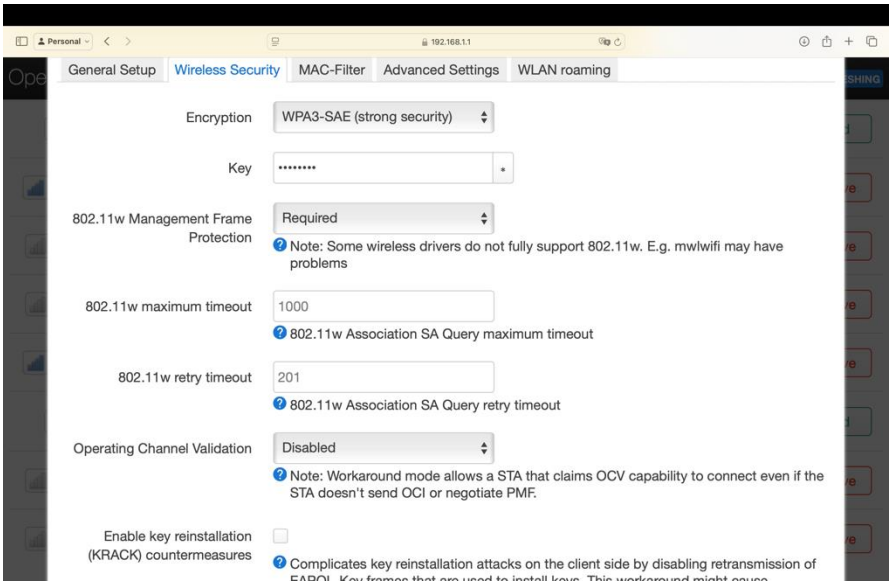


Fig 5. Wireless Security tab of Interface Configuration window

iv. Optional Settings:

- The mode used, channel and bandwidth of the radio can be configured in General Setup tab under Device Configuration window. Legacy 802.11b rates can be enabled. Maximum transmit power can be changed according to the requirement.

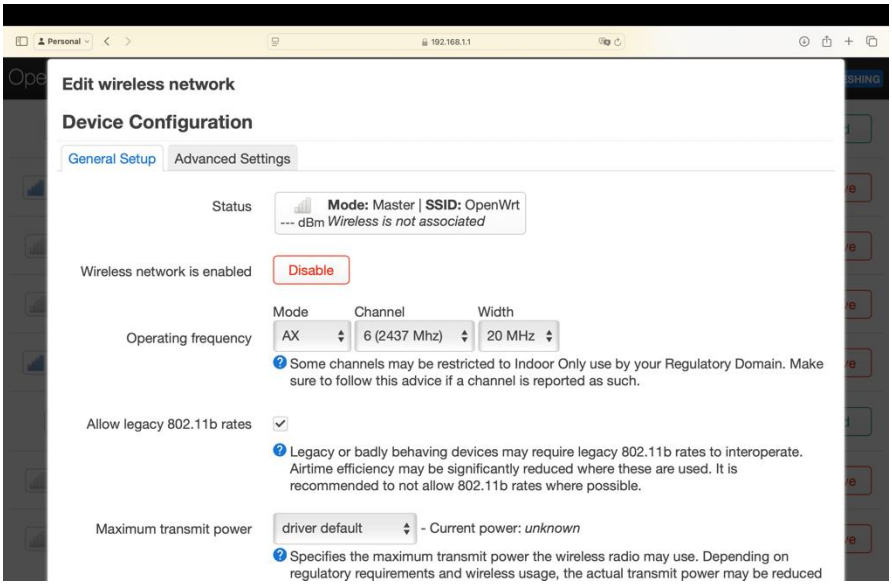


Fig 6. General Setup tab of Device Configuration window

v. Save and Apply Settings

vi. Verify:

- Check if new SSID is visible to client devices
- Connect and test IP assignment and internet access

6.3. Creating VAPs using CLI

Creating VAPs through SSH is preferred for advanced users. Step-by-step procedure for creating VAPs using CLI is given below

i. SSH into the Router:

(base) username@host ~ % ssh root@192.168.1.1

BusyBox v1.37.0 (2025-03-07 13:03:12 UTC) built-in shell (ash)

```
 _______                     ________        __
|       |.-----.-----.-----.|  |  |  |.----.|  |_
|   -   ||  _  |  -__|     ||  |  |  ||   _||   _|
|_______||   __|_____|__|__||________||__|  |____|
         |__| W I R E L E S S   F R E E D O M
```

```
 OpenWrt SNAPSHOT, r28947-213799e33e
 -------------------------------------------------
=== WARNING! =====================================
There is no root password defined on this device!
Use the "passwd" command to set up a new password
in order to prevent unauthorized SSH logins.
--------------------------------------------------
```

ii. Add New VAP via Vim editor (Option 1):

```
root@OpenWrt:~# cd /etc/config
root@OpenWrt:/etc/config# vim wireless

config wifi-device 'radio0'
        option type 'mac80211'
        option path '1e140000.pcie/pci0000:00/0000:00:01.0/0000:02:00.0'
        option band '2g'
        option channel '6'
        option htmode 'HT20'
        option legacy_rates '1'
        option cell_density '0'

config wifi-iface 'default_radio0'
        option device 'radio0'
        option network 'lan'
        option mode 'ap'
        option ssid 'OpenWrt1'
        option encryption 'sae'
        option key 'password'
        option ocv '0'

config wifi-device 'radio1'
```

```
        option type 'mac80211'
        option path '1e140000.pcie/pci0000:00/0000:00:01.0/0000:02:00.0+1'
        option band '5g'
        option channel '40'
        option htmode 'HE20'
        option cell_density '0'

config wifi-iface 'default_radio1'
        option device 'radio1'
        option network 'lan'
        option mode 'ap'
        option ssid 'My VAP 3'
        option encryption 'psk-mixed'
        option key 'password'

config wifi-iface 'wifinet0'
        option device 'radio0'
        option mode 'monitor'

config wifi-iface 'wifinet4'
        option device 'radio0'
        option mode 'ap'
        option ssid 'My VAP 1'
        option encryption 'owe'
        option network 'lan'

config wifi-iface 'wifinet4'
        option device 'radio0'
        option mode 'ap'
        option ssid 'My VAP 2'
```

```
        option encryption 'psk2'
        option key 'password'
        option network 'lan'

    config wifi-iface 'wifinet5'
        option device 'radio1'
        option mode 'ap'
        option ssid 'My VAP 4'
        option encryption 'psk2'
        option key 'password'
        option network 'lan'
```

iii. Add New VAP via UCI (Option 2):

```
root@OpenWrt:~# uci add wireless wifi-iface
root@OpenWrt:~# uci set wireless.@wifi-iface[-1].device='radio0'
root@OpenWrt:~# uci set wireless.@wifi-iface[-1].mode='ap'
root@OpenWrt:~# uci set wireless.@wifi-iface[-1].ssid='My VAP 1'
root@OpenWrt:~# uci set wireless.@wifi-iface[-1].encryption='owe'
root@OpenWrt:~# uci commit wireless
```

iv. Reload Wireless & Network:

```
root@OpenWrt:~# wifi reload
root@OpenWrt:~# /etc/init.d/network restart
```

6.4.Common Configuration Mistakes

- SSID Confilcts: Using the same SSID for multiple VAPs can confuse clients and create roaming issues.
- Forgetting to Assign VAP to a Network Interface: If a VAP is not linked to a logical network (e.g., lan), clients will connect but won’t get an IP or internet access.

- Radio Device Disabled: option disabled '1' is set for the radio or interface, causing the VAP/SSID to not broadcast.
- Missing wifi reload or uci commit: Changes made via CLI don't apply if you forget to commit and reload the wireless config.
- SSID Not Broadcasting: SSID is hidden by setting option hidden '1' or due to beacon timing misconfigurations.
- LuCI Changes Not Applied: Not clicking "Save & Apply" after making changes in LuCI leads to unsaved configurations.

7. BEACON FRAME ANALYSIS OF VAPs

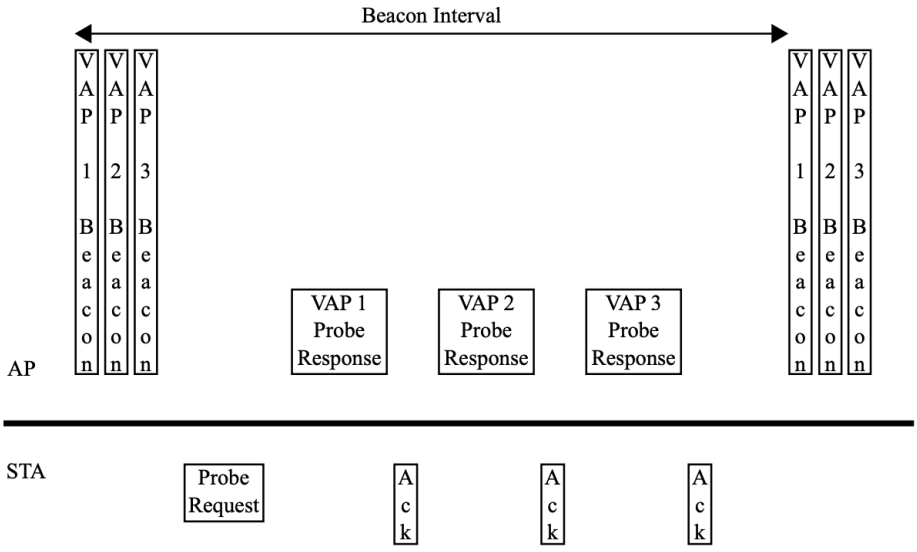


Fig 7. Co-hosted mode of multiple VAP operation

When multiple Virtual Access Points (VAPs) are configured on a single physical wireless radio in OpenWrt, each VAP functions as a distinct Basic Service Set (BSS), with its own unique BSSID. Since all these virtual interfaces operate on the same physical hardware, the wireless driver schedules beacon transmissions for each VAP sequentially. The physical radio does not transmit all beacons simultaneously—instead, it interleaves them within the same beacon interval window. This results in each VAPs beacon frame being broadcast at slightly staggered times, though the configured interval (e.g., 100 ms) is maintained per VAP.

No.	Time	Source	Destination	Protocol	Info
14	0.054362	52:91:e3:58:d0:0d	Broadcast	802.11	Beacon frame, SN=2319, FN=0, Flags=........C, BI=100, SSID="OpenWrt1"
15	0.058366	56:91:e3:58:d0:0d	Broadcast	802.11	Beacon frame, SN=2317, FN=0, Flags=........C, BI=100, SSID="My VAP 1"
16	0.063228	5a:91:e3:58:d0:0d	Broadcast	802.11	Beacon frame, SN=2313, FN=0, Flags=........C, BI=100, SSID="My VAP 2"

(a)

No.	Time	Source	Destination	Protocol	Info
77	0.163388	52:91:e3:58:d0:0d	Broadcast	802.11	Beacon frame, SN=2320, FN=0, Flags=........C, BI=100, SSID="OpenWrt1"
78	0.165579	56:91:e3:58:d0:0d	Broadcast	802.11	Beacon frame, SN=2318, FN=0, Flags=........C, BI=100, SSID="My VAP 1"
79	0.167027	5a:91:e3:58:d0:0d	Broadcast	802.11	Beacon frame, SN=2314, FN=0, Flags=........C, BI=100, SSID="My VAP 2"

(b)

Fig 8. Beacons of 2.4 GHz band VAPs

From fig 8. we can infer that each VAP has its unique BSSID. The beacon frame of for each VAP is transmitted sequentially. Fig 8. (a) is the first set of beacons transmitted, and Fig 8. (b) is the second set of beacons transmitted. Comparing the time of beacon frame of same VAP, we can conclude that there is approximately 100 ms interval before broadcasting the next beacon. Fig 9. shows the beacon frames of 5 GHz VAPs.

No.	Time	Source	Destination	Protocol	Info
57	0.093138	TPLink_58:d0:0c	Broadcast	802.11	Beacon frame, SN=1139, FN=0, Flags=........C, BI=100, SSID="My VAP 3"
58	0.097152	52:91:e3:58:d0:0c	Broadcast	802.11	Beacon frame, SN=1136, FN=0, Flags=........C, BI=100, SSID="My VAP 4"

(a)

No.	Time	Source	Destination	Protocol	Info
148	0.195607	TPLink_58:d0:0c	Broadcast	802.11	Beacon frame, SN=1140, FN=0, Flags=........C, BI=100, SSID="My VAP 3"
149	0.200993	52:91:e3:58:d0:0c	Broadcast	802.11	Beacon frame, SN=1137, FN=0, Flags=........C, BI=100, SSID="My VAP 4"

(b)

Fig 9. Beacons of 5 GHz band VAPs

This beaconing strategy, while effective in virtualizing multiple SSIDs on a single radio, does require careful consideration of airtime efficiency. Too many VAPs on a single radio can lead to excessive management traffic, which competes with client data transmissions, ultimately affecting throughput and latency.

8. DATA TRANSMISSION ANALYSIS

8.1. Packet Flow between VAPs and Clients

In the conducted experiment, three Virtual Access Points (VAPs)—OpenWrt1, My VAP 1, and My VAP 2—were configured on a 2.4 GHz band, each associated with one client station (STA).

Each STA was actively streaming a YouTube video during the packet capture. The captured .pcap file was analyzed to study the traffic pattern, with a focus on the volume and type of frames transmitted by each VAP.

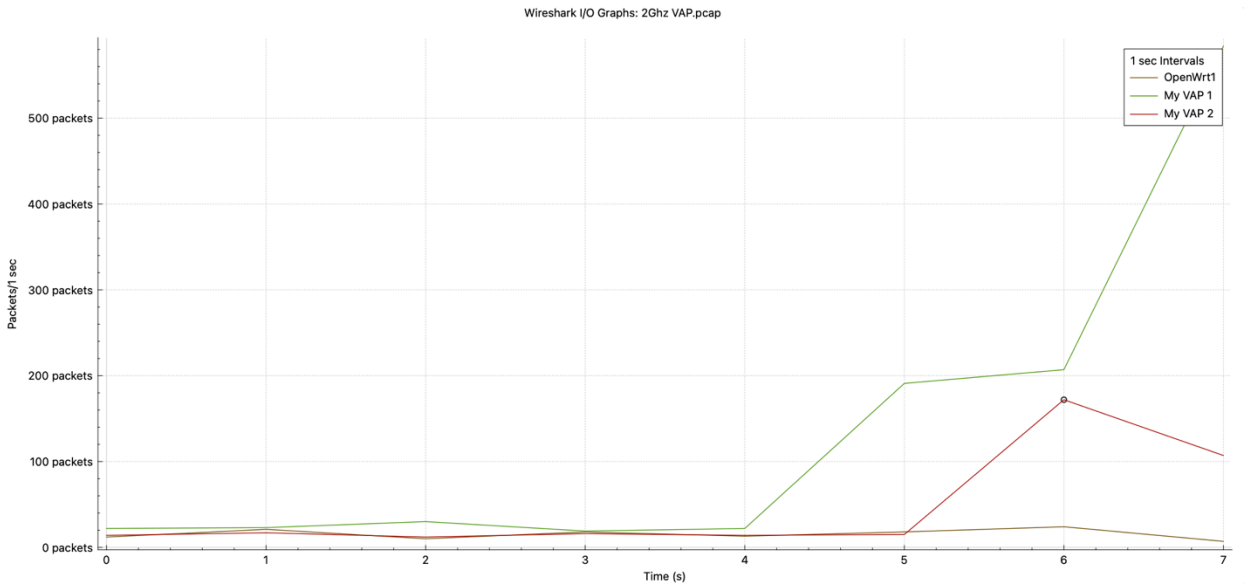


Fig 10. IO Graph for 2.4 GHz VAP Frames

From fig 10. we can infer that initially, during the setup phase, the number of frames observed from each BSSID was roughly equal. This corresponds to the standard management frame activity such as beaconing, probe requests/responses, and initial connection handshakes, which are uniform across all VAPs at startup. As the streaming sessions began, divergence in the number of frames associated with each VAP became evident. Notably, My VAP 1 exhibited a significantly higher number of data frames compared to the others, followed by My VAP 2, while OpenWrt1 showed only a slight increase. This trend can be attributed to several possible factors like variation in streaming behaviour of YouTube, client capability or distance. The IO graph for similar experiment conducted in 5GHz band is given fig 11.

Thus, while multiple VAPs offer logical network separation and configuration flexibility (e.g., different SSIDs or VLAN mappings), their data transmission performance is tightly coupled to the limitations of the underlying shared physical medium. Efficient VAP deployment must consider not just logical configuration but also client behaviour, signal conditions, and total expected traffic to maintain balanced performance.

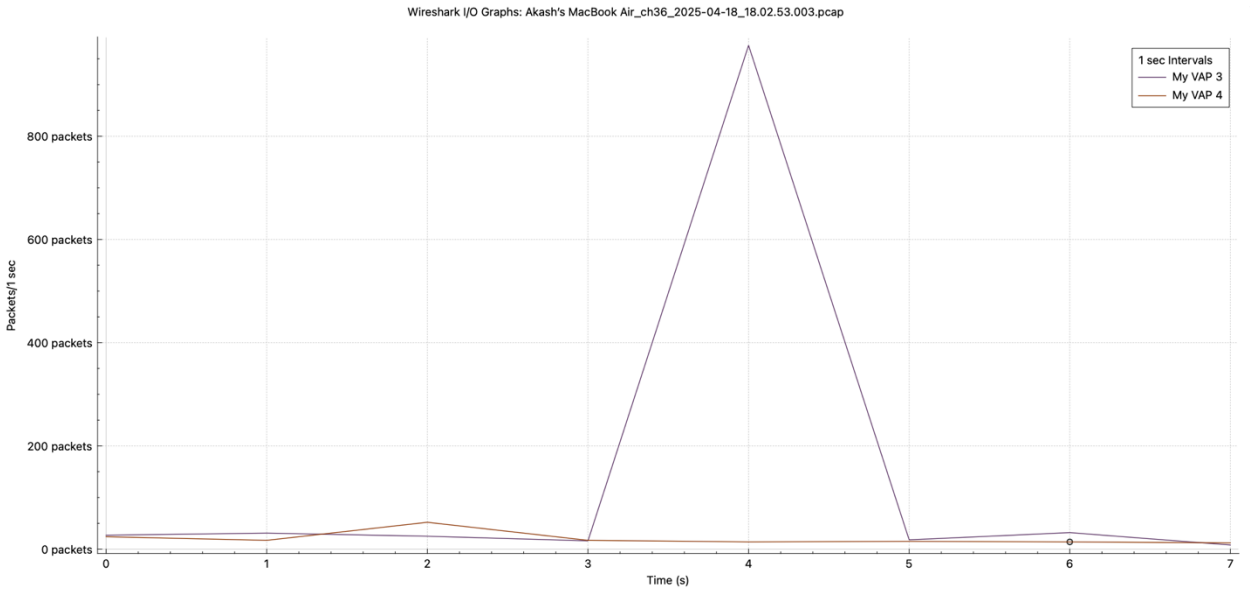


Fig 11. IO Graph for 5 GHz VAP Frames

9. CONCLUSION

In this study, we explored the behaviour and performance of multiple Virtual Access Points (VAPs) configured on a single OpenWrt-based router (TP-Link Archer AX23), with a focus on beacon behavior, data transmission patterns, and overall feasibility for real-world applications. Some observations from this study are:

- Each VAP operates with a unique BSSID and broadcasts its own beacon frames, which increases management overhead. These beacons are transmitted sequentially since they share the same radio, leading to additional airtime consumption.
- Each VAP operates with a unique BSSID and broadcasts its own beacon frames, which increases management overhead. These beacons are transmitted sequentially since they share the same radio, leading to additional airtime consumption.
- Each VAP operates with a unique BSSID and broadcasts its own beacon frames, which increases management overhead. These beacons are transmitted sequentially since they share the same radio, leading to additional airtime consumption. Each VAP operates with a unique BSSID and broadcasts its own beacon frames, which increases management overhead. These beacons are transmitted sequentially since they share the same radio, leading to additional airtime consumption.

VAPs have a wide range of applications in real world, including guest networking in homes, isolating IoT devices from personal networks, creating separate staff and student networks in educational institutions, segmenting departments in enterprises, offering dedicated SSIDs for visitors and employees in co-working spaces, and enabling bandwidth or access control in public venues like cafes and libraries—all using a single physical access point for cost-effective and secure wireless management.

In conclusion, while VAPs provide flexibility and logical segmentation in wireless networks, care must be taken to account for the shared nature of the radio channel. Traffic patterns, management overhead, and physical limitations can impact performance, especially when several VAPs are actively used on bandwidth-constrained bands like 2.4 GHz. Proper planning, monitoring, and understanding of client behavior are essential for optimal deployment.

10.REFERENCES

[1] OpenWrt Project. (n.d.). OpenWrt Project [Online]. Available: https://openwrt.org

[2] OpenWrt Forum. (n.d.). “Vlan tagging/VAP on whr-hp-gn (latest AA 12.09 ar71xx)” [Online]. Available: https://forum.archive.openwrt.org/viewtopic.php?id=51325

[3] S. R. Gulasekaran and S. G. Sankaran, Protocol and Network. Norwood, MA: Artech House, 2021.

[4] Wireshark Wiki. (n.d.). *Wireshark Wiki* [Online]. Available: https://wiki.wireshark.org/