data delivered

WES5

Wireless Ethernet System

WES5-AX Series

WES5-AX-AF

WES5-AX-BF

WES5-AX-CF

WES5-KT (Pre-Configured Point-to-Point Kit)

Installation & Operations Manual

Table of Contents

For full product line and support, visit: https://www.kbcnetworks.com

1. Product Overview

The WES5 Series is a rugged, outdoor-ready dual-radio wireless Ethernet system based on Wi-Fi 6 (802.11a/n/ac/ax). It supports point-to-point and multipoint wireless networking at up to 2.4 Gbps throughput.

Typical Applications:
- IP surveillance and remote gate access
- Building-to-building network extension
- Industrial plants, parking lots, or perimeter detection
- Off-grid deployments with solar or UPS power

2. Package Contents

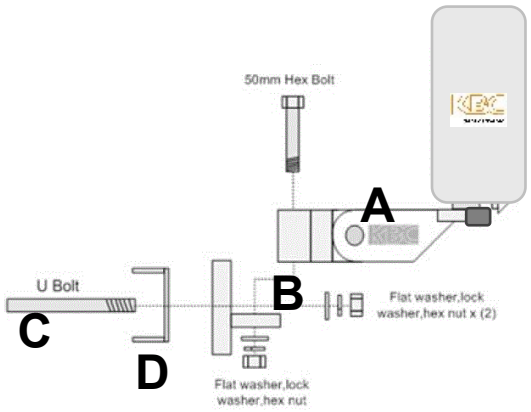
For **WES5-KT** Kit (pre-configured point-to-point kit models):
- (2) WES5-AX-CF radio units
- (2) each - Mounting kits: baseplates, pole clamps, U-bolts, washers, and brackets
- Cable gland attached to each unit

For **WES5-AX-AF**
- (1) WES5 omni-directional node
- (2) external 5dBi omni antennas
- (1) Mounting kit: baseplates, pole clamps, U-bolts, washers, and brackets
- (1) Cable gland attached to each unit

For **WES5-AX-BF** and **WES5-AX-CF** models:
- (1) WES5 directional node
- (1) Mounting kit: baseplates, pole clamps, U-bolts, washers, and brackets
- (1) Cable gland attached to each unit

⚠ Note: PoE injectors not included. Requires 802.3af PoE or 48V passive PoE.

3. Hardware Installation



Mounting Steps:

1. Attach baseplate (A) and swivel plate (B).
2. Use U-bolt (C) and pole clamp (D) to secure on a 2" pole.
3. Affix the WES5 unit to the mount using screws from its base.
4. Remove the cable gland, pass the Ethernet cable through, plug into the LAN port, then re-seal the gland. Finger tight is sufficient. A wrench, or other tool, is not needed to tighten the cable gland.
5. Align and tighten all components for optimal signal.

4. LED Status Indicators

Each WES5 radio has a window on the back with green LEDs. The LEDs do not change color, and one light may be lit, but it is to be ignored as it is not used on this product. (ie, “N/A”). If no LEDs are lit then the unit is not powering up, in which case a PoE injector is recommended. If no PoE source can power the WES5 radio, contact KBC for warranty status and potential return for repair.

PWR ● 48V PoE Power applied.
O No power to unit.

1G ● Link activity established
★ Link activity (flashing)
O No link to device.

N/A – Not used

(All S1~S4 LEDs should be lit, i.e., S2 will not light if S1 is not on; S3 will light if S1 and S2 are both on.)

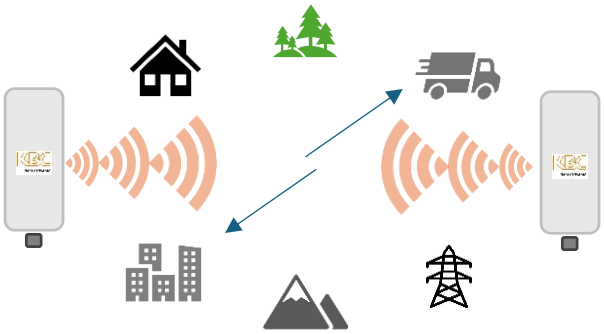
S1	● Weak RF signal	O No RF link
S2	● Weak RF signal	O No RF link / poor link *(ie, if just S1 is on)*
S3	● Mediocre signal	O No RF link / weak link *(if S1 and S2 are on)*
S4	● Ideal RF signal	O No RF link / okay but not ideal link *(if all others are on)*

5. Line-of-Sight Defined & Illustrated

5 GHz requires clear line-of-sight to connect with ideal signal strength numbers and associated data rate transfer speeds. When obstructions are in the wireless line-of-sight paths, the signal can be attenuated causing less than ideal signals and potential for negatively impacted performance.

5a. Line-of-sight:

Clear Line-of-Sight Example 1:



Clear Line-of-Sight Example 2:

The radio frequency (RF) signal, if it could be seen, expands in the shape of an American football as it transmits. The further distance needed, the more open space is also required. The antenna should be mounted so that no portion of the signal will be obstructed by physical things. See Section 4 regarding LED activity for more information.

5b. NOT line-of-sight:

Obstructed Line-of-Sight Example 1

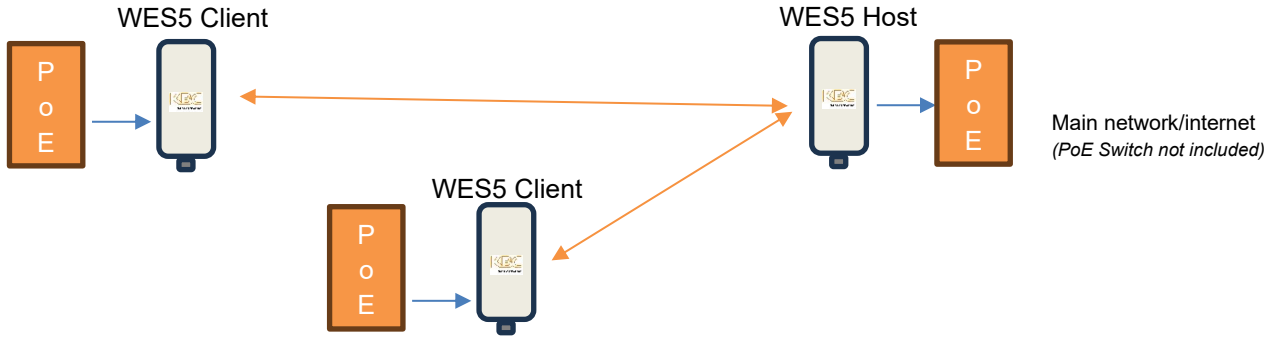
Obstructed Line-of-Sight Example 2

6. Typical System Configurations

WES5 offers two radios in each node. A wifi0 radio that supports 802.3bgn 2.4 GHz and wifi1 radio that supports 802.3axa 5 GHz. In the drawings below, the main Host to Client(s) connections are assumed to be operating on wifi1 (5GHz).

6a. Point-to-Point (PtP)

6b. Point-to-Multipoint (PtMP) with Example Configuration Settings



💡 **KBC Recommendation:** In the above PtP and PtMP diagrams, **disable wifi0 on the Host while using wifi1 for Host/Client communication**. In addition, it is advised to disable the DHCP Server functionality found on Network/Interfaces/Edit (see Section 7)

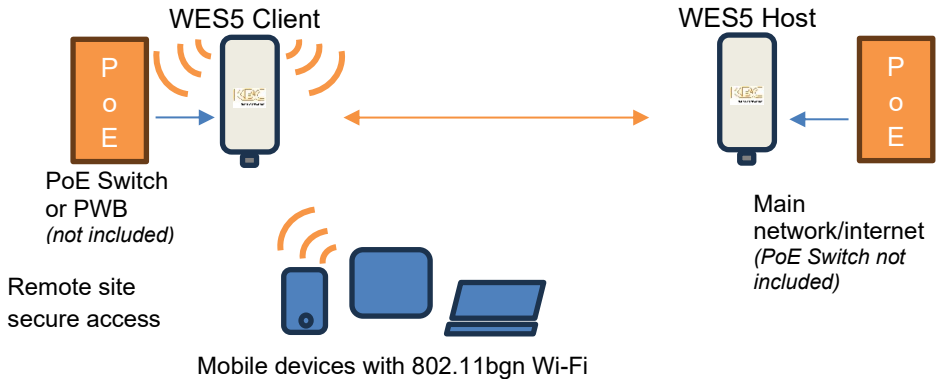
📝 Note: In PtMP applications, the Host 'receiver' can link to Client 'transmitters' within varying beamwidth degrees of the common Host device. Refer to the chart below to determine the degree of separation that each type of antenna will support in a multipoint configuration:

Host Model*	Antenna type	Beamwidth Degrees (Horizontal plane)	Max expected distance**
WES5-AX-AF	(2) External 5 dBi omni	360	1000 ft
WES5-AX-BF	Integrated 9 dBi directional	65	5000 ft
WES5-AX-CF	Integrated 17 dBi directional	30	1.5 miles

** The model ordered on its own will be set as Host/Access Point but each WES5 radio is able to be configured as Host or Client. The above assumes that wifi1 is set into Host/AP WDS mode. Refer to supplied documentation when ordered as part of a kit or pre-configuration.*

*** This is not a specification. It is a general, conservative example based on prior observations in optimal wireless conditions, assuming use of WES5-AX-CF client models.*

6c. Point-to-Point with Wi-Fi Access Point at Remote Site *(wifi0 remains enabled on the WES5 Client and DHCP Server Mode is also still enabled in this example)*



7. GUI Configuration Sections

7a. Log In

The default IP of the WES5 is 192.168.1.202. After setting your computer to a static IP on the same 192.168.1.x subnet, use a web browser to access the interface at 192.168.1.202 and enter “password” to access the interface.

📝 If you are working with a Host from a WES5-KT then the IP is 192.168.1.200 and a Client from a default configured WES5-KT is 192.168.1.201

7b. Status

7b.1 Overview

Indicates the configured settings and connection status as a display screen only. Configuration changes are not performed on this page.

7b.2 Firmware Version

The WES5 supports the following firmware versions:
- WES5-500A.1a (recommended if still running the original WES5-500A)
- WES5-500A.1b (new updated version)

⚠️ If you are using the original WES5-500A firmware, it is recommended to upgrade to

WES5-500A.1a or WES5-500A.1b current firmware version.

Download the latest firmware from:
https://www.kbcnetworks.com/component/zoo/wireless-ethernet-systems/wes5-series
Navigate to the 'Downloads - Firmware' section on the right side of the page.

7b.3 Wireless Radio Configuration Overview

This section provides configuration options for the two radios (wifi0 and wifi1), including band selection, channel width, encryption, and SSID settings. Wifi0 is typically used for local access, while **wifi1 is optimized for long-range or high-throughput links** – KBC recommends the wifi1 setting for long distance wireless point-to-point and multipoint links whereas wifi0 is used for local Wi-Fi access in Access Point mode.

📝 wifi0 is not typically used in Client mode. When setting up two WES5 units in a point-to-point link, make sure the unit with **wifi1** when set to **Access Point** (i.e. Host) also has **wifi0** either set to **Access Point** (Host) *or* ***disabled***. If **wifi0** is set to **Client**, it can create a network loop, which may cause connectivity issues.

7b.4 Wireless Connections

Shows signal strength, connection status, MAC address of linked units, and link quality metrics.

If a device has no connections, the user will see this message on the Status page:

As mentioned above, these fields populate when a mate unit is connected. We can tell the screenshot below is from the Host side because the Network field shows “Master,” which reflects the Host’s perspective. The Client side will show “Client” then the SSID.

7b.4a Understanding the Wireless Connection information:

MAC Address: This is the radio MAC address of the *other* unit that is wirelessly connected to the device you are currently viewing in the GUI.

Network: On the **Host** unit, this field will display **“Master”** followed by the network name (SSID).
On the **Client** unit, it will display **“Client”** followed by the network name it’s connected to.

Noise: This value shows the amount of background noise in the wireless environment. A reading around **-95 dBm** is typical. For optimal performance, the

noise level should ideally fall between **-90 dBm and -100 dBm**—the lower (more negative), the better.

Signal: The signal values are shown as positive numbers for simplicity but represent negative dBm values (e.g., 50 = –50 dBm). Using positive numbers makes signal strength easier to interpret at a glance. In the example above, the signal is strong. The numbers mean:

- **50** – Current signal strength
- **48** – Average strength since connection began
- **47** – Minimum strength during that time

RX Rate: A **real-time snapshot** of connection performance, showing the **current data rate** (in Mbps) at which the device is receiving data over the wireless transmission.
Note: This is not the actual throughput—it's the theoretical maximum speed based on current signal quality and network conditions.

TX Rate: same as above but for transmitting data in the opposite direction of the RX rate.

TxCCQ: or Transmit Client Connection Quality; a percentage value (0–100%) that represents the **quality of the wireless transmission** from a device to its connected peer (typically an access point or another wireless device).

- **100%** = Excellent connection quality (clean signal, minimal retransmissions)
- **Below 75%** = May indicate problems (interference, weak signal, noise, hardware issues, etc.)
- **0 to 25%** = Very poor connection; likely unstable or unusable

Up Time: The amount of time that the link has been established.

7c. System

On this tab a user can set administrative actions and utilize the tools and services that the WES5 unit has to offer.

7c.1 System Properties

This area lets users:
1. Set the local system time or sync it to the browser's time.
2. Set a hostname that appears in the browser tab for identification.
3. Set the time zone by selecting a major city (default is America/Los Angeles).

⚠️ If a user in eastern time syncs local time but forgets to change the time zone to America/New York, the displayed time will match the West Coast time equivalent.

📝 Clicking “Save” only will keep changes until exiting the GUI interface web browser pages. Once the user exits the GUI, all changes will revert to the last applied properties unless “Save & Apply” is clicked.

7c.2 Administration

7C.2a Password

This section is where the admin user can change the GUI login password.

- Use the green “refresh” arrows to toggle password visibility.
- Default password is 'password'.
- Enter the new password and confirm it by typing it again in the 'Confirmation' field. The password entries must match. There are no password requirements such as character length or special characters etc.
- Click 'Save & Apply'. The user will be logged out and must re-login with the new password.

⚠️ **Record all password changes!**

🔄 If the password is forgotten, the unit must be restored to defaults.
1. Remove the screw plug to access the button.
2. Using a small screwdriver, press the reset button on the underside of the unit for 5–10 seconds while powered on.
3. After reset, the unit returns to default IP 192.168.1.202 and password 'password'. Re-insert the screw into the hole to seal.

See “Restore” section below for default configurations.

7c.2b Services

Includes:
- Ping Watchdog
- Auto Reboot
- Log DUMP

7c.2c SNMP

Configure Simple Network Management Protocol settings for remote monitoring.

7c.2d MQTT

Enable and configure MQTT for device messaging and integration with IoT platforms.

7c.2e Backup / Flash Firmware

Upload new firmware or download backup configurations.

7c.2f Reboot

Performs a soft reboot. This will disconnect clients temporarily but will not reset any settings.

7c.2g Restore

Restores the WES5 to factory default settings, equivalent to pressing the internal reset button.

Regardless of how a WES5 unit is configured—**even if it's part of a pre-configured WES5-KT point-to-point kit**—using the restore function or resetting physically with the reset button will return the unit to the following default settings:

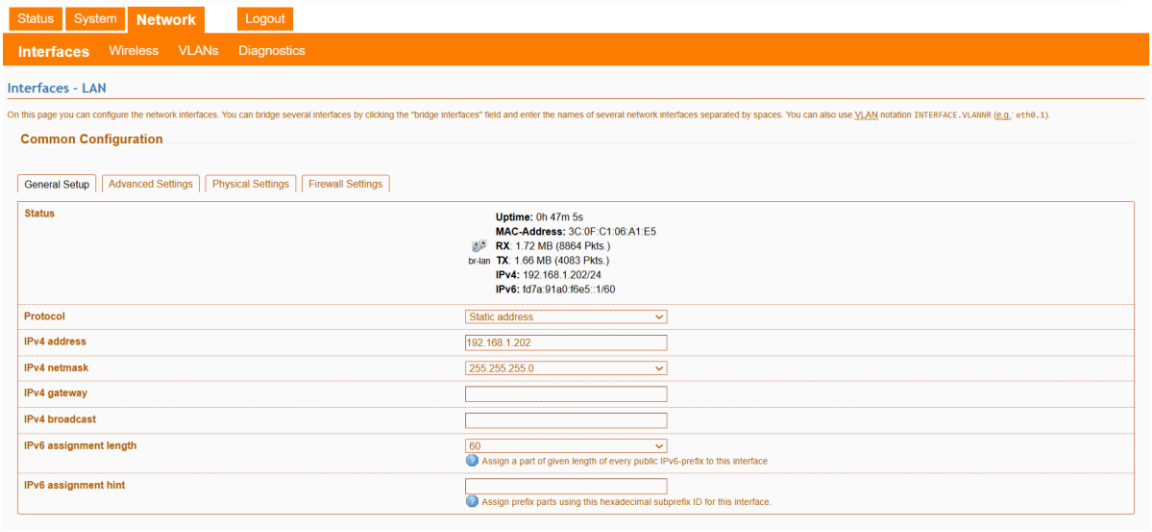
Parameter	Setting
LAN IP Address	**192.168.1.202**
GUI User ID	**admin**
GUI Password	**password**
DHCP Server Mode	**Enabled**
DHCP Server IP range	**192.168.1.100 ~ 150**
WiFi-0 Mode	**Access Point WDS**
WiFi-0 SSID	**WES5-2.4G**
Pre-shared Key	**KBCnetworks**
Mode/Frequency	**802.11axg / auto**
Chan Spectrum Width	**40MHz**
WiFi-1 Mode	**Access Point WDS**
WiFi-1 SSID	**WES5-5G**
Pre-shared Key	**11111111**
Mode / Frequency	**802.11axa / auto**
Chan Spectrum Width	**160MHz**

7d. Network

7d.1 Interface Overview

This screen shows the wired LAN interfaces. The MAC address displayed is for Ethernet and is **not** used in wireless MAC filtering. Click **"Edit"** to configure LAN settings like the IP address.

7d.2 Interfaces – LAN (Configuration)



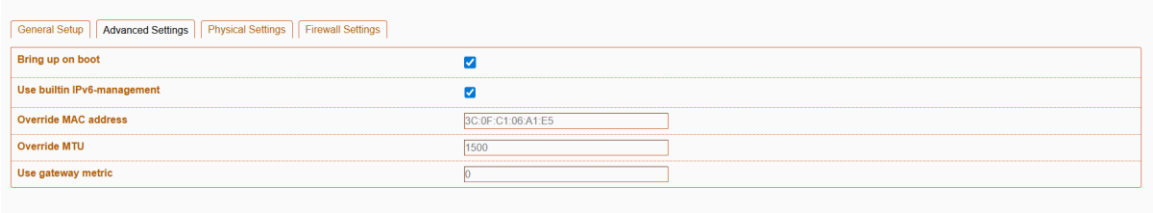
7d.3 General Setup

Configure the IPv4 address and click “save & Apply”. The interface will bring you to the new IP if the computer IPv4 setting is the same subnet as the new WES5 unit LAN IP.

Always click “Save & Apply” to activate changes

7d.4 Advanced Settings

Click the tab to show the advanced Ethernet configuration settings.



7d.4a Bring up on boot:

This setting determines whether the LAN interface (e.g., Ethernet port) is automatically enabled and activated each time the WES5 powers on or reboots.

7d.4b Use built-in IPv6-management:

A network configuration option that, when enabled, allows the device to automatically handle **IPv6 address assignment and management** using its **internal tools and services**, rather than relying on external systems or manual configuration.

When **"Use built-in IPv6-management"** is **enabled**, the device can:

- Assign **IPv6 addresses** to interfaces
- Handle **routing and neighbor discovery**
- Respond to or send **Router Advertisements (RA)**
- Manage **link-local and global IPv6 prefixes**

When you might use it:

- You want the device to **self-manage IPv6** on its interfaces without needing an external DHCPv6 server.
- You're setting up a **standalone or isolated network** where the device must provide IPv6 configuration to clients.
- You're using **OpenWRT** or similar firmware, which supports internal IPv6 stack management.

When you might not use it:

- Your network already has a **dedicated IPv6 router or DHCPv6 server**, and you want to avoid conflicts.
- You're running a **manual/static IPv6 configuration**.

7d.4c Override MAC address:

Using an **"Override MAC Address"** in the network configuration of a Wi-Fi device allows you to manually set a **custom MAC address** for that interface instead of using the device's factory-assigned one.

Here's **why** and **when** you might want to do this:

✅ **1. Avoid MAC-based Restrictions**

Some networks (like corporate or university environments) only allow devices with **pre-approved MAC addresses** to connect. Overriding the MAC lets your device appear as one of those approved devices.

✅ **2. Preserve IP Assignments (Static DHCP)**

If a network uses **MAC-to-IP mapping** (DHCP reservations), changing the MAC can:

- Help a device **retain a specific IP address**
- Allow multiple interfaces to cycle through reserved IPs

✅ **3. Device Replacement / Failover**

When replacing a Wi-Fi device or setting up a backup unit, you can match the original device's MAC so the network:

- Recognizes it the same way
- Continues routing or firewall rules without changes

✅ **4. Privacy or Testing Purposes**

- Mask your device's identity on public or semi-trusted networks
- Simulate another device for testing configurations or network behavior

---

✅ **5. Bypass MAC Filters or Licensing**

Some systems use MAC-based access control or licensing. Overriding the MAC can temporarily work around those limits—though this should only be done ethically and with permission.

⚠️ **Caution:**

- Using duplicate MACs on the same network can cause conflicts.
- Overriding MACs may violate some network policies or terms of service.

7d.4e Override MTU:

Network configuration option that allows you to manually set a custom **MTU (Maximum Transmission Unit)** size for a specific network interface, instead of

using the system default or auto-detected value. **Override MTU** lets you manually define the maximum packet size for a network interface, giving you greater control over how data is transmitted across the network.

🔧 **What is MTU?**

MTU (Maximum Transmission Unit) is the largest size (in bytes) of a single data packet that can be sent over a network interface without needing to be fragmented.

- WES5 Default: **1500 bytes** for Ethernet
- Smaller MTUs may be used for **VPNs**, **tunnels**, or **certain ISPs**

✅ **Why use "Override MTU"?**

You might override the MTU to:

- **Avoid packet fragmentation** in networks with lower MTU limits (e.g., VPN or PPPoE connections)
- **Resolve performance or connectivity issues** related to large packets
- **Match MTU settings** on other devices in your network
- **Optimize throughput** on specific links or protocols

⚠️ **Caution:**

- Setting the MTU too low can **decrease performance**
- Setting it too high may cause **packet loss** or **connectivity issues** if intermediate devices can't handle larger packets

---

Override MTU lets you manually define the maximum packet size for a network interface, giving you greater control over how data is transmitted across the network.

7d.4f Use gateway metric:

Enter a number that determines the **priority** or **preference** of a route in the routing table:

- **Lower metric = higher priority**
- **Higher metric = lower priority**

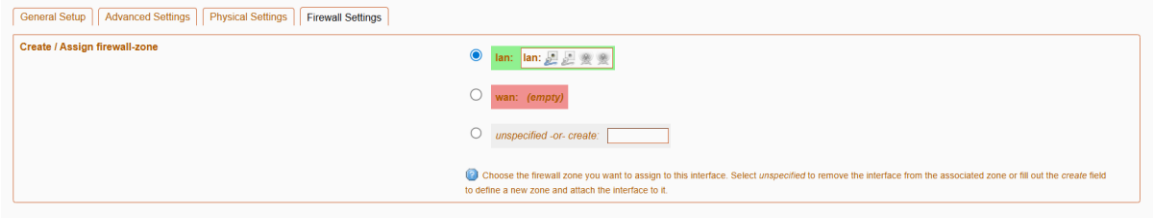
7d.5 Physical Settings

This section allows you to set the unit to **bridge mode** (the default setting). If using redundant links with managed switches, you can enable **STP (Spanning Tree Protocol)** under the **Physical Settings** tab.

⚠️ **Caution:** Avoid disabling active Ethernet or wireless interfaces, as this can lock you out of the GUI. If that happens, a factory reset will be required to regain access.

7d.6 Firewall Settings

To set up firewall zones. Click “Save & Apply” to save changes.



Setting up **firewall zones** in the network configuration of a Wi-Fi device allows you to **control traffic flow between different network interfaces or segments**, enhancing **security, performance, and isolation**.

✅ **1. Improve Network Security**

- **Prevent unauthorized access:** For example, you can block traffic from a guest Wi-Fi network to your internal LAN.
- **Limit exposure:** Keep vulnerable or less-trusted devices (like IoT or public access points) isolated from sensitive systems.

✅ **2. Control and Filter Traffic**

- Apply **firewall rules** to specific zones to restrict certain types of traffic (e.g., block SSH from guest devices, allow only HTTP/S).
- Prevent unnecessary communication between zones unless explicitly allowed.

✅ **3. Segment the Network**

- Create separate zones for:
  - **LAN (trusted internal network)**
  - **WAN (internet)**
  - **GUEST (untrusted devices)**
  - **DMZ (public-facing services)**
- Each zone can have different rules and policies.

✅ **4. Enhance Performance and Stability**

- Isolating noisy or bandwidth-heavy devices (like security cameras or streaming devices) can prevent them from affecting other parts of the network.

✅ **5. Required for Advanced Routing**

- If you're routing traffic between interfaces or using VLANs, zones help manage those paths securely and intentionally.

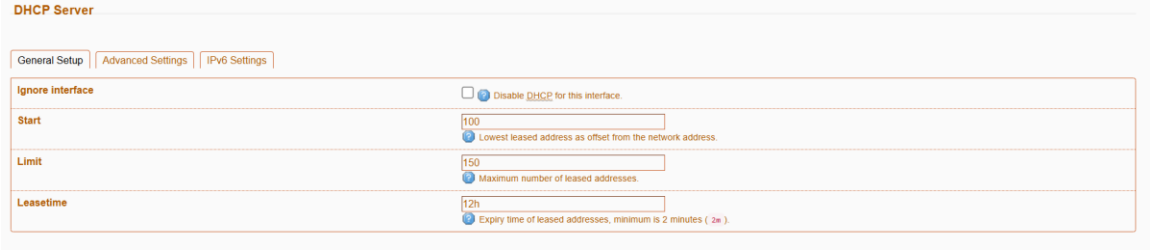
Example:

You might configure:

- **LAN zone** to have full access
- **GUEST zone** to only access the internet
- **WAN zone** to be tightly firewalled from all internal networks

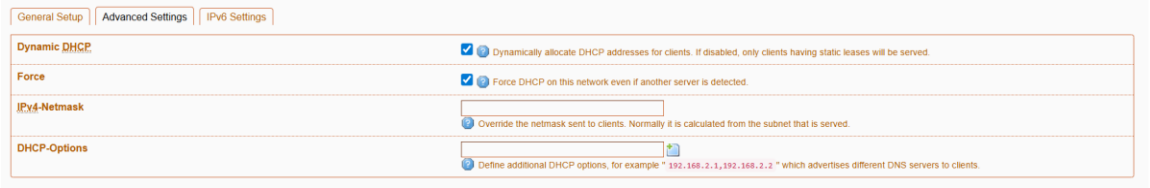
7d.7 DHCP Server

This function enables the WES5 unit to act as a **DHCP server**, automatically assigning IP addresses to connected devices within a specified range. Devices must have DHCP enabled to receive an address. The assigned IP addresses will follow the same subnet as the WES5 network setting, starting with the value entered in “Start” and continuing sequentially until the specified number of devices is reached.



7d.8 Advanced Settings

This section outlines the advanced configurable parameters available when enabling the DHCP server function on the WES5 device. These settings control how the device assigns IP addresses and related network information to connected clients. By adjusting options such as **Dynamic DHCP**, **Force**, **IPv4-Netmask**, and **DHCP-Options**, administrators can tailor DHCP behavior to meet specific network design and management requirements. Each setting below includes a description of its function and guidance on how it impacts the network's address assignment and client configuration process.



7d.8a Dynamic DHCP:

When enabled, the WES5 automatically assigns IP addresses to client devices upon connection. These addresses are allocated from a predefined pool configured in the General Setup tab and are leased for the duration specified there. Operating in DHCP server mode, the WES5 dynamically distributes available IP addresses to clients as requested, with each device receiving an address for a set lease period. Addresses may change if a client reconnects after the lease expires.

7d.8b Force:

When enabled, this setting compels the WES5 to act as the DHCP server for the network, assigning IP addresses to clients even if another DHCP server is detected on the same network segment. This ensures the WES5's DHCP service takes precedence, overriding any conflicting DHCP responses from other servers.

7d.8c IPv4-Netmask:

This setting allows the user to manually specify an IPv4 subnet mask to override the default netmask sent to DHCP clients. Normally, the netmask is automatically derived from the subnet configured on the network. Overriding the netmask enables customized subnetting for clients as needed.

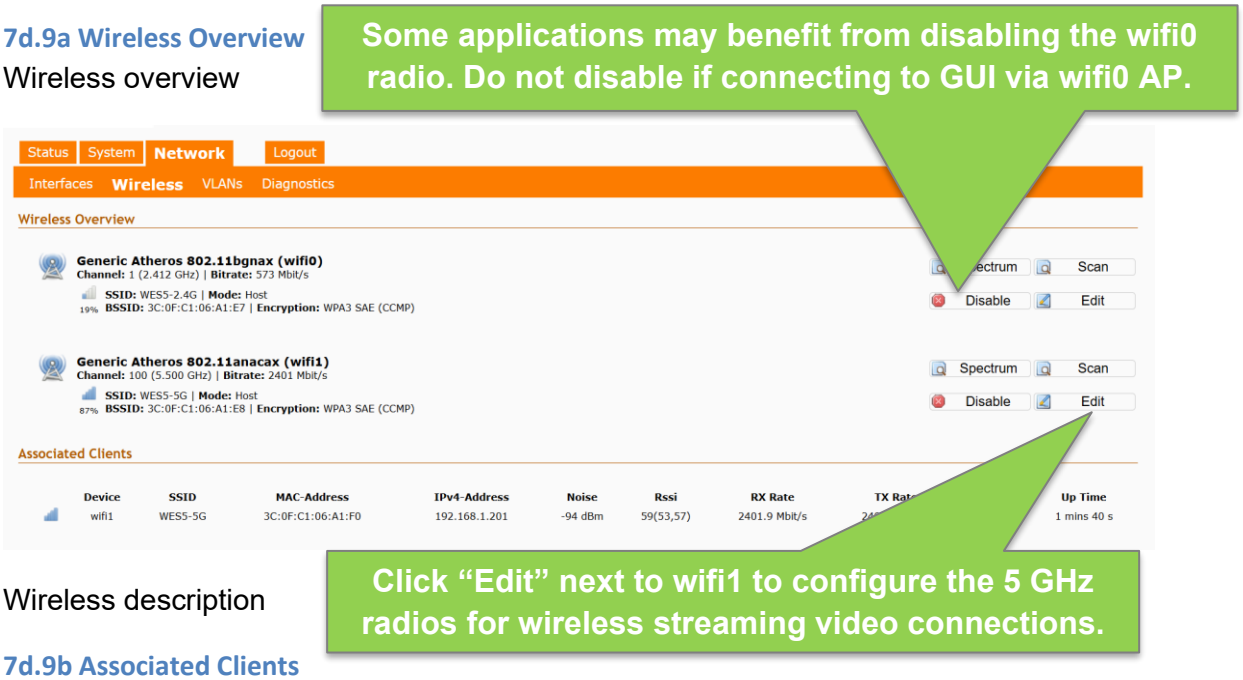
7d.8d DHCP-Options

This setting allows the user to define additional parameters to be included in DHCP responses. These options can customize the network configuration provided to clients. For example, specifying "192.168.2.1, 192.168.2.2" under this setting advertises alternate DNS servers to DHCP clients. Values must follow the appropriate format for the desired option type.

7d.9 Wireless

7d.9a Wireless Overview

Wireless overview



Wireless description

7d.9b Associated Clients

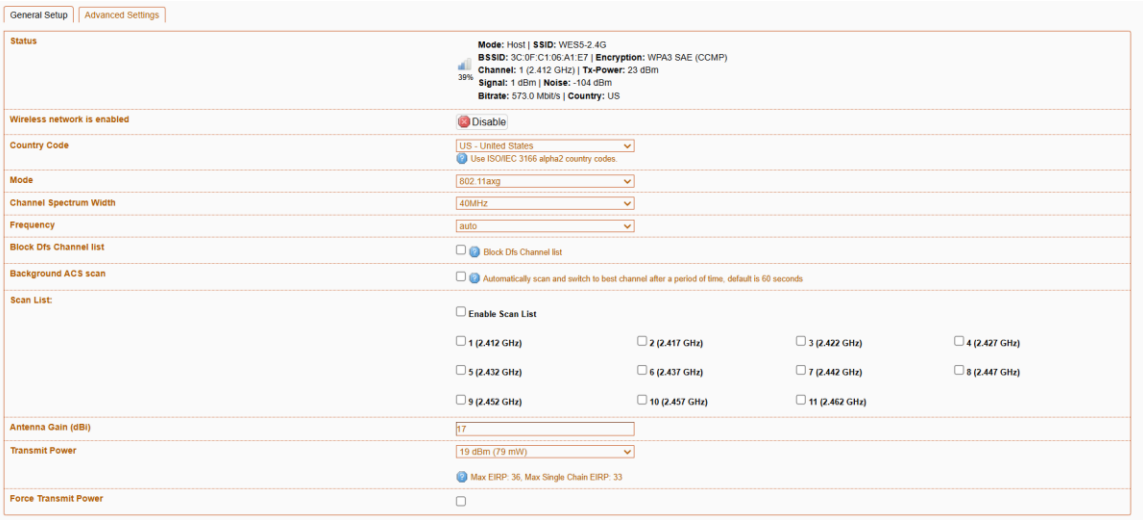
This information has been defined previously. See “Understanding the Wireless Connection information” on pages 6-7 in this manual.

7d.9c Wifi0 Device Configuration

The Device Configuration section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which are shared among all defined wireless networks. Per network settings like encryption or operation mode are grouped in the “interface configuration.”

📝 **Note:** The instructions and definitions below are the same for wifi1. Wifi1 is 5 GHz which is the radio and frequency most commonly used for long-distance streaming video applications.

7d.9d General Set Up



7d.9d.1 Status

This window shows the current wireless configuration status. BSSID displays the radio MAC address of the Host AP. In Host mode, it shows the unit's own MAC; in Client mode, it shows the MAC of the connected Host. Other settings reflect the current configuration from this screen. Some changes, like the channel on the Host, will auto-sync with the Client.

7d.9d.2 Wireless Network is enabled/disabled

Click this button to disable (or re-enable) wifi0.

💡 **KBC Recommendation: DISABLE wifi0 if not using as a local Wi-Fi hotspot Access Point.** Turning off wifi0 is useful in solar-powered setups to help lower power consumption. When disabled, it can be turned back on at any time. Keep in mind that disabling the radio means the unit can no longer be accessed wirelessly and will require a direct cable for access.

7d.9d.3 Country Code

Select from the list of countries to set the regional requirements and limitations for the wifi0 radio power output and channel operation.

7d.9d.4 Mode

The WES5 wifi0 radio supports various 2.4GHz IEEE 802.11 wireless standards. The most commonly used mode is **802.11axg**, as it supports multiple standards and maximizes compatibility with 2.4GHz Access Points and Clients. When set to "Auto," the radio defaults to 802.11axg. If the Access Point is an older device, you may need to manually select the matching standard used by the Host for proper wireless linking.

WES5 wifi1 is 5 GHz and will be the radio to enable and configure for most applications. The default mode is 802.11axa but can be set to the older methods for backward compatibility. If attempting to link to WES4, this option should be set to 802.11ac.

7d.9d.5 Channel Spectrum Width

Refers to the amount of frequency space used by a wireless signal to transmit data. It is typically measured in megahertz (MHz) and determines how much data can be carried at once. Wider channels can support higher data rates but may be more susceptible to interference, especially in crowded environments.

WES5 wifi0 options:

- **20 MHz** – More stable and better for avoiding interference in congested areas
- **40 MHz** – Offers higher throughput but can be more prone to interference
- **Auto** – The device will select the best width based on available channels and network conditions

WES5 wifi1 options:

- **40 MHz** – More stable and better for avoiding interference in congested areas
- **80 MHz** – Offers higher throughput but can be more prone to interference
- **160 MHz** – default channel spectrum width with maximum throughput capacity potential. Uses large 160 MHz frequency channels which could have the most chance of being affected by interference.
- **Auto** – The device will select the best width based on available channels and network conditions

*Actual real-world throughput is typically lower and is determined by several environmental factors. Allow for a usual 60~70% due to over-head and environmental factors.

📝 **Note:** Wider channels are best used in environments with minimal wireless congestion, while narrower channels are preferred for reliable performance in noisy or shared frequency spaces.

⚠️ The Host and Client Channel Spectrum Width settings must match.

📝 When the “Mode” is set to “Auto,” the **Channel Spectrum Width** option will no longer be visible because the system automatically uses a predefined channel width based on the selected mode.

⚠️ When in 160 MHz mode, the Dynamic Frequency Selection channels must be used. If you select the option to avoid those channels then the max channel width is 80.

7d.9d.6 Frequency

WES5 wifi0 supports 11 individual channels. The specific channel (or frequency) is determined by the Host (Access Point). When a device is set as a Client, it will automatically match the channel of its Host. Therefore, on a Client device, the channel setting shown on this page may not reflect the actual channel in use—because the Client ignores this setting and follows the Host’s configuration.

Wifi1 supports 25 individual 5 GHz frequencies. The larger the channel spectrum width, the less overall frequencies to choose from.

7d.9d.7 Block DFS Channel List

DFS is “Dynamic Frequency Selection” meaning that the system is allowed to change its frequency automatically. Click the checkbox to stay on static frequencies only.

As mentioned above, this option is not allowed for 160 MHz channel spectrum width. Enabling this will eliminate the ability to use 160.

DFS requires the ability for the unit to scan and change frequencies when affected by environmental RF activity on/near the transmitting channel. The unit could also change channels upon a restart of the Host. The wifi1 DFS frequencies are 5280~5725 MHz.

7d.9d.8 Background ACS Scan

Automatically scan the environment and switch frequencies based on the present impact of potential interfering RF signals that can be found on the scan.

⚠️ When the scan is performed, the wireless connection to its mate may be lost.

7d.9d.9 Scan List

This setting is disabled by default, allowing the device to scan and operate on all available channels. To limit operation to specific channels, manually enable this setting and select the desired channels. Leaving it blank will continue to allow use of all channels.

- **On the Host (AP) side**: the device will be limited to only the selected channels for operation.
- **On the Client side**: the device will only scan the selected channels when searching for a Host.

If the Host is using a channel that is not included in the Client's scan list, the Client will not detect or connect to it.

7d.9d.10 Antenna Gain

The antenna gain setting ensures the radio stays within FCC transmit power limits based on the built-in antenna. It defaults to 17 for WES5-KT and WES5-AX-CF. For WES5-AX-BF, it should be set to 9, and for WES5-AX-AF, to 5—both will reset to 17 by default and must be manually corrected.

7d.9d.11 Transmit Power

Transmit Power refers to the strength of the radio signal sent from the wireless device. It is measured in dBm (decibels relative to 1 milliwatt). Higher transmit power increases signal range and penetration but can also cause more interference and may exceed regulatory limits if not configured properly.

For the 2.4 GHz radio, the transmit power can be adjusted from **3 dBm (1 mW)** to **17 dBm (approximately 79 mW)**.

- **Lower settings** (e.g., 3–10 dBm) are useful for short-range, low-interference environments or when using high-gain antennas.
- **Higher settings** (e.g., 14–17 dBm) may improve range and reliability in open or obstructed areas but should be used with care to stay within legal limits and minimize interference with other devices.

User-selectable level	Approx. conducted power	Resulting EIRP (conducted + 17 dBi)	Typical use-case
0 dBm	1 mW	17 dBm (50 mW)	Very short links or lab testing
3 dBm	2 mW	20 dBm (100 mW)	Short indoor / campus hops
6 dBm	4 mW	23 dBm (200 mW)	Medium links with minimal noise
9 dBm	8 mW	26 dBm (400 mW)	General PTP links up to a few hundred meters
12 dBm	16 mW	29 dBm (800 mW)	Longer rural links, light foliage

User-selectable level	Approx. conducted power	Resulting EIRP (conducted + 17 dBi)	Typical use-case
15 dBm	32 mW	32 dBm (1.6 W)	Long LOS links; still 4 dB below FCC limit
17 dBm (default)	50 mW	34 dBm (2.5 W)	Factory default; safe margin for most U-NII-3 PTP installs
19 dBm (max)	80 mW	36 dBm (4 W)	Longest LOS links; **absolute maximum** allowed in the US for 5 GHz point-to-point with high-gain antennas (eCFR)

Always balance transmit power with antenna gain to comply with FCC regulations and ensure optimal performance.

7d.9d.12 Force Transmit Power

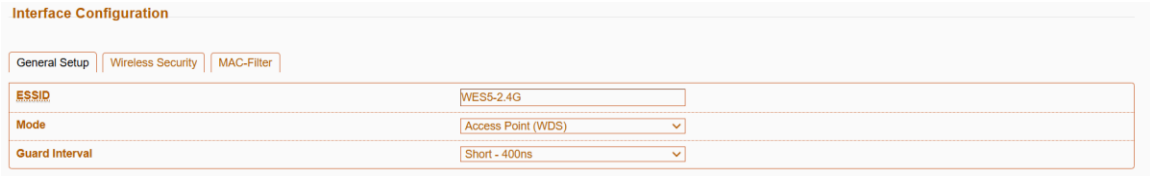
The Force Transmit Power option overrides the automatic power control features of the radio and locks the transmit power at the user-selected level. Normally, the radio may adjust its output power based on regulatory constraints, antenna gain, or environmental conditions.

When Force Transmit Power is enabled:

- The radio will transmit at the exact dBm value set in the Transmit Power setting, regardless of antenna gain or other system factors.
- This setting should be used only when necessary, such as for controlled test environments or specialized deployments, as it can increase the risk of violating FCC power limits if antenna gain is not accounted for.

Important: Use this feature with caution. When using high-gain antennas, forced high transmit power may exceed legal Effective Isotropic Radiated Power (EIRP) limits.

7d.9e Interface Configuration



7d.9f General Set Up

7d.9f.1 ESSID (Extended Service Set Identifier)

The **ESSID** is the name of the wireless network that the device will broadcast (in Access Point mode) or connect to (in Client mode). It acts as a unique identifier to distinguish one wireless network from another.

- In **Access Point mode**, this is the network name that client devices will look for and connect to.
- In **Client mode**, this setting must **match the ESSID** of the Access Point it is trying to connect to.

Wifi0 default: WES5-2.4G

Wifi1 default: WES5-5G

Key Points:

- The ESSID is **case-sensitive** and can include letters, numbers, and symbols.
- All devices in the same wireless network must use the **exact same ESSID** to communicate.
- Choose a unique ESSID to avoid conflicts with nearby wireless networks.

Example:
If the Access Point's ESSID is set to BridgeLink24, then all Client radios must also be set to BridgeLink24 to connect successfully.

7d.9f.2 Mode

The **Mode** setting defines how the radio behaves in the wireless network. Choose the mode based on the device's role and network design:

- **Access Point**
  Broadcasts a wireless signal for other radios (Clients) to connect to. Used when this radio is the central point in a point-to-point or point-to-multipoint setup.
- **Client**
  Connects to an Access Point. Use this when the radio is the remote end of a point-to-point or point-to-multipoint link.
- **Ad-Hoc**
  Creates a peer-to-peer connection without using an Access Point. Rarely used;

suitable for temporary or mesh-style networks where each device connects directly to others.

- **Access Point (WDS)**
  Functions like a standard Access Point, **but with WDS (Wireless Distribution System)** enabled, allowing transparent bridging of Ethernet networks across the wireless link. Use this to pass **MAC addresses**, multicast, and broadcast traffic seamlessly to Clients with WDS enabled.
- **Client (WDS)**
  Connects to an Access Point (WDS) and supports **transparent Layer 2 bridging**, preserving MAC addresses and allowing full network visibility across the wireless link.
- **Static (WDS)**
  A fixed WDS link where both sides are manually configured with each other's MAC address. Useful in secure, static deployments where automatic peer discovery is not needed or not supported.

When to Use WDS Modes:

Use **WDS modes** when you need:

- **Transparent Layer 2 bridging** (preserve MAC addresses across the link)
- **Full network visibility** (for protocols that rely on broadcasts, e.g., DHCP, VoIP, or some access control systems)
- A network that behaves as if devices are on the **same Ethernet switch**, just over wireless

Avoid WDS if you only need basic IP connectivity and want simpler configuration but **choose WDS** if you're extending a LAN or connecting systems that rely on MAC-level traffic.

7d.9f.3 Guard Interval

The **Guard Interval (GI)** is a small-time buffer inserted between transmitted symbols to reduce signal interference caused by reflections or multipath propagation (common in wireless environments). It helps the receiver distinguish between overlapping signals.

Available Options:

- **Short – 400 ns:**
  - **Faster data rates** due to less overhead.

  - Best for **short-distance** links with **clear line-of-sight** and minimal interference or reflections.
  - Offers higher throughput but is **less tolerant** of multipath environments.

- **Long – 800 ns (Standard):**
  - Balanced option with good **performance and reliability**.
  - Suitable for **most deployments**, including modest reflections or moderate distances.

- **Very Long – 1600 ns:**
  - Use in **long-range links** or **areas with high multipath interference** (e.g., urban or reflective environments).
  - Reduces symbol overlap, improving stability and reducing errors at the cost of **slightly lower throughput**.

- **Ultra Long – 3200 ns:**
  - Best for **very long-distance point-to-point links** or **highly reflective environments**.
  - Maximizes signal clarity in challenging RF conditions but adds the most overhead, reducing data rate.

Summary Recommendation:

- **Use Short** for clean, close-range environments where speed is critical.
- **Use Long** as the default for general use.
- **Use Very/Ultra Long** for long-range or harsh RF conditions where stability is more important than speed.

7d.9g Wireless Security

7d.9g.1 Encryption

This setting determines how wireless data is encrypted and secured. Choose the level of encryption based on the requirements of your network, compatibility with client devices, and the level of security needed.

📝 **Note:** When deploying multiple WES5 radios in a wireless network, all units should use **WPA3 encryption** for optimal security.
If **WES5 needs to communicate with WES4 radios**, set the WES5 **Encryption Mode** to **"WPA-PSK / WPA2-PSK Mixed Mode"** and ensure the **pre-shared key (PSK)** matches the one used on the WES4 units.
This setting applies only to **wifi1**, the 5 GHz radio, since all WES4 and WES4HTG radios operate on the 5 GHz band only.

WPA3 (Wi-Fi Protected Access 3)

- **Description:** Uses **SAE (Simultaneous Authentication of Equals)** for stronger protection against password-guessing attacks and supports **forward secrecy**.
- **When to Use:**
    - For **modern networks** needing the highest level of security.
    - When **all client devices support WPA3**.
- **Note:** Not compatible with older Wi-Fi devices.

WPA-PSK / WPA2-PSK Mixed Mode

- **Description:** Supports both **WPA (TKIP)** and **WPA2 (AES)** for backward compatibility.
- **When to Use:**
    - In **transitional environments** with a mix of old and new client devices.
    - When you're unsure what encryption the client devices support.
- **Note:** Offers broad compatibility but not the strongest security.

WPA2-PSK (Wi-Fi Protected Access 2 – Pre-Shared Key)

- **Description:** Industry standard for many years; uses **AES encryption** for strong security.
- **When to Use:**
    - In most modern deployments where **WPA3 is not required or supported**.
    - Provides a good balance of security and compatibility.

- **Note:** Still secure for most applications when used with strong passwords.

WPA-PSK (Wi-Fi Protected Access – Pre-Shared Key)

- **Description:** Early version of WPA; uses **TKIP encryption**, which is now considered weak.
- **When to Use:**
    - Only if required to support **very old legacy devices**.
- **Note:** Not recommended for secure environments.

WEP Shared Key (Wired Equivalent Privacy)

- **Description:** Outdated and insecure encryption method using a **shared key** for access.
- **When to Use:**
    - Only if **legacy equipment requires it** and cannot be upgraded.
- **Note:** Easily broken with modern tools; should be avoided whenever possible.

WEP Open System

- **Description:** Similar to WEP Shared Key, but the key is not used in the initial authentication, only in data encryption.
- **When to Use:**
    - Same as WEP Shared Key – **only for legacy compatibility**.
- **Note:** Offers **no meaningful security**; not recommended.

No Encryption

- **Description:** The network is completely **open**, and no password is required.
- **When to Use:**
    - Only in **controlled environments** like temporary demos, testing, or public access where security is not a concern.

- **Note: Not secure**—data can be intercepted by anyone within range.

Recommended Best Practices

- **Use WPA3** whenever possible for maximum security.
- If compatibility is a concern, use **WPA2-PSK** or **WPA2/WPA Mixed Mode**.
- **Avoid WEP and WPA (TKIP)** unless absolutely necessary.
- **Never use No Encryption** on production or sensitive networks.

7d.9g.2 SAE (Simultaneous Authentication of Equals)

When using WPA3, check this box to enable SAE which is the **authentication method used in WPA3-Personal** security mode. It replaces the traditional pre-shared key (PSK) exchange used in WPA2 with a more secure, password-based key exchange protocol.

SAE provides the following benefits:

- **Stronger protection against password guessing** (resistant to offline dictionary attacks)
- **Forward secrecy**, ensuring past sessions remain secure even if the password is later compromised
- **Mutual authentication**, treating both client and access point as equal participants in the authentication process

SAE enhances overall wireless security and is **required for WPA3 connections**.

7d.9g.3 SAE Password

The SAE password is the **shared passphrase** used in **WPA3-Personal** mode to authenticate devices via **Simultaneous Authentication of Equals (SAE)**. Each **Client device** must enter the **same passphrase** as configured on the **Host/Access Point** to establish a connection.

For the 2.4 GHz radio (**wifi0**), the **default SAE password** is:
KBCnetworks

When configuring this setting on the Host/AP:

- The passphrase must be **8 to 63 characters long**
- Only **ASCII characters** are allowed

- It may include **upper/lowercase letters, numbers, symbols, and spaces**

While the system does not enforce complexity rules, it is strongly recommended to use a **strong, non-obvious password** to ensure security.

7d.9g.4 SAE PWE (Password Element)

SAE PWE stands for **Simultaneous Authentication of Equals Password Element**. It refers to the method used to derive the cryptographic element from the password during the WPA3 authentication process.

The **PWE** is a core part of the **Dragonfly key exchange** used in WPA3, and it ensures that the password is securely converted into a cryptographic value without exposing it to attackers. Different methods for generating the PWE are available to improve compatibility or enhance security.

Common SAE PWE Methods:

- **Hunting and Pecking (Default):**
  The standard method defined in the WPA3 specification. It uses a trial-and-error algorithm to securely derive the password element from the shared password.
- **Hash-to-Element (optional):**
  A newer method based on hashing, offering more consistent and efficient password-to-element conversion. May be used in some implementations for improved performance or compliance with updated standards.

When to Configure SAE PWE:

In most deployments, this setting can be left at its default (usually **Hunting and Pecking**). Advanced users or those in regulated environments may choose a different method to match security or interoperability requirements.

SAE MFP (Management Frame Protection)

SAE MFP stands for **Simultaneous Authentication of Equals – Management Frame Protection**. It is a feature required by **WPA3-Personal** to enhance wireless network security by protecting **management frames** from being spoofed or tampered with.

Management frames are essential for network operation (e.g., beacons, deauthentication, disassociation messages). Without protection, attackers can exploit these frames to disrupt communication or trick devices into disconnecting.

Key Functions of SAE MFP:

- **Authenticates management frames**, ensuring they come from a trusted source.
- **Prevents spoofed deauthentication/disassociation attacks**, often used in denial-of-service (DoS) scenarios.
- **Mandatory in WPA3-Personal**: SAE MFP is always enabled when using WPA3 and does not require manual activation.

Operational Notes:

- No configuration is typically required; **SAE MFP is enforced automatically** with WPA3.
- Both the **Access Point and Client** must support MFP for the WPA3 connection to succeed.

7d.9h MAC-Filter

The **MAC-Filter** controls network access based on a device's **MAC address** (Media Access Control address), which is a unique identifier assigned to each network interface. This feature allows or blocks specific devices from connecting to the wireless network.

MAC-Filter Options:

- **Allow Listed Only**
  - **Only devices with MAC addresses on the list are allowed** to connect.
  - All other devices will be blocked, even if they have the correct password.
  - Use this for **maximum access control** in secure environments.
- **Denied MAC List**
  - Devices with MAC addresses on the list are **explicitly blocked** from connecting.
  - All other devices are allowed if they have the correct credentials.
  - Use this to **block known unwanted devices** without limiting access for others.

- **Disable**
    - **No MAC filtering is applied.**
    - Any device with the correct network credentials can connect.
    - Use this when **MAC-based access control is not needed**.

Important Notes:

- Though MAC addresses can be **spoofed** by advanced users, the Client does not broadcast its radio MAC address. That said, MAC filtering should not be relied on as the only layer of security.
- Always combine MAC filtering with strong encryption (e.g., WPA3) for better protection.

7d.9i Advanced Settings

7d.9i.1 802.11h *(Enable with checkbox)*

Enables support for **Dynamic Frequency Selection (DFS)** and **Transmit Power Control (TPC)**, required in certain regulatory domains (like Europe) for 5 GHz operation.

- **Use when:** Operating in DFS-required regions or to reduce interference.

7d.9i.2 UAPSD Enable (Unscheduled Automatic Power Save Delivery) *(Enable with checkbox)*

Enables **Wi-Fi power-saving features** for compatible client devices (mainly phones and tablets), allowing them to wake only when needed.

- **Use when:** You want to optimize battery life for mobile clients on low-traffic networks.

7d.9i.3 Multicast Rate *(Enter numeric value)*

Sets the **transmission rate for multicast and broadcast traffic**. Higher rates reduce airtime usage but may limit range.

- **Typical values:** 6–24 Mbps (depending on environment and reliability needs).

- **Use when:** You want to tune performance for video multicast or reduce low-rate traffic overhead.

Fragmentation Threshold *(Enter numeric value)*

Specifies the **maximum packet size before fragmentation** occurs. Lower values can improve reliability in noisy environments but reduce throughput.

- **Default/Recommended:** 2346 (disables fragmentation).
- **Use when:** Experiencing interference or high packet error rates.

7d.9i.4 RTS/CTS Threshold *(Enter numeric value)*

Sets the packet size that triggers **Request to Send / Clear to Send** handshaking, which helps avoid collisions in congested or hidden node scenarios.

- **Default:** 2347 (RTS/CTS disabled).
- **Use when:** There are many clients or potential hidden nodes.

7d.9i.5 WMM Mode (Wi-Fi Multimedia) *(Enable with checkbox)*

Enables **traffic prioritization** for voice, video, best-effort, and background traffic. Required for proper QoS in modern networks.

- **Use when:** Using VoIP, video streaming, or other latency-sensitive services.

7d.9i.6 Number of Spatial Streams *(Enter numeric value)*

Defines how many **MIMO spatial streams** are used for transmission. More streams = higher data rates (if both radio and client support it).

- **Values:** 1, 2, or 3 (depending on hardware).
- **Use when:** You want to limit or match spatial stream usage to client capabilities or interference conditions.

7d.9i.7 LDPC (Low-Density Parity Check) *(Enable with checkbox)*

Enables advanced **forward error correction** for improved signal reliability and throughput in noisy environments.

- **Use when:** You want maximum throughput and robustness, especially on weak or long links.

7d.9i.8 RX STBC (Receive Space-Time Block Coding) *(Enable with checkbox)*

Improves receiver performance by using **redundant data streams** sent over multiple antennas.

- **Use when:** Clients support it and you're optimizing receive sensitivity on long/complex links.

7d.9i.9 TX STBC (Transmit Space-Time Block Coding) *(Enable with checkbox)*

Increases transmission reliability by sending **redundant data** over multiple antennas to help clients better decode signals.

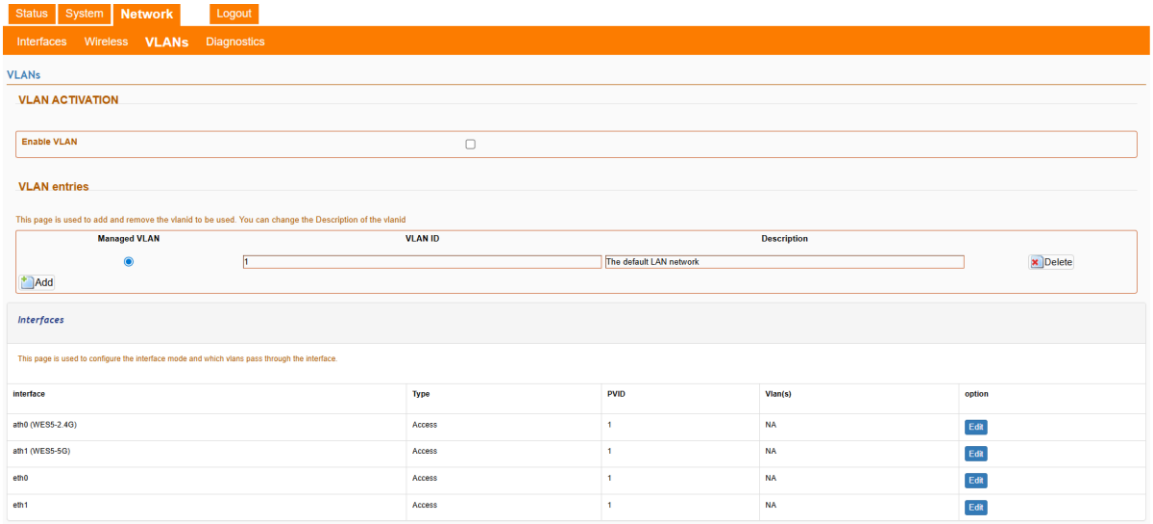
- **Use when:** Serving clients with poor signal quality or limited receive capabilities.

7d.9i.10 Roaming to Select Better AP *(Enable with checkbox)*

Allows the device to **automatically disconnect and reconnect** to a stronger access point when signal strength drops below acceptable levels.

- **Use when:** Deploying in a multi-AP environment and want seamless roaming between coverage zones.

7d.10 VLANs



7d.10a VLAN Configuration Page Overview

The VLANs configuration page allows you to enable VLAN functionality and manage virtual LANs on the WES5 device. To activate VLAN support, simply check the **"Enable VLAN"** box at the top of the page.

Under the **VLAN entries** section, you can define and manage VLANs by clicking the **"Add"** button. For each VLAN, enter a unique **VLAN ID** and an optional **Description** to help identify its purpose or role in the network (you may also assign a name for management clarity). Once saved, any defined VLAN can be removed at any time by clicking the **"Delete"** button next to its corresponding entry.

7d.10b Interfaces Section Overview

The **Interfaces** section displays all physical and wireless interfaces available on the WES5 unit, including:

- **ath0** – the 2.4 GHz Wi-Fi radio (WES5-2.4G)
- **ath1** – the 5 GHz Wi-Fi radio (WES5-5G)
- **eth0** – Ethernet Port 1
- **eth1** – Ethernet Port 2

Each interface is shown with its current configuration, including:

- **Type**: The operating mode of the interface, either **Access** or **Trunk**

- **PVID**: The Port VLAN ID – defaulted to **1**
- **VLAN(s)**: Indicates VLAN membership (currently shown as **N/A**)

To modify an interface's VLAN behavior, click the **"Edit"** button next to the desired interface. From there, you can change the **Type** to either **Access** (for untagged VLAN traffic) or **Trunk** (to allow tagged VLAN traffic). The **PVID** setting identifies the default VLAN ID for untagged packets; in this system, **1** is the only available option. After making your changes, be sure to click **"Save Changes"** to apply them.

7d.11 Diagnostics

7d.11a Ping Network Utility

The **Ping Network Utility** allows you to test connectivity to any device with a pingable IP address on the network. If the device connected to the WES5 is on the same subnet, this tool can help confirm the following:

- Whether the WES5 can successfully ping the directly connected device.
- If the response time matches what you see using a standard command prompt ping.
- If the WES5 can ping a device that cannot be reached from a command prompt on another network device, this may indicate a broader network issue not related to the WES5.

7d.12 Log Out

Click the Log Out button to immediately sign out of the GUI interface. You will be returned to the Login screen.

8. Set Up Step-by-Step Configuration Processes

8a Setting Up a Host to Client Link on wifi1

Basic Host/Client Setup Instructions

Before starting, set your laptop's LAN to a **static IP in the 192.168.1.x subnet**.

8a.1. Identify the Radios

Use at least two WES5 radios. If one is a **WES5-AX-BF**, use it as the **Host/AP**. Others will be Clients.

8a.2. Prepare the Host

- Power the Host via PoE and connect it to your laptop.
- Confirm it's at default settings (IP: **192.168.1.202**, both Wi-Fi interfaces in **Host/AP mode**).
- Default SSIDs: WES5-2.4G (wifi0), WES5-5G (wifi1).
- If not default, use the **System > Restore** function.

Note: If only one Host is needed, skip to step 4.

8a.3. Set Unique SSID (if multiple Hosts)

- Go to **Network > Wireless > Edit (wifi1)**.
- Under **General Setup**, change the **ESSID** from WES5-5G to a unique name for this Host/Client group.
- Record the new SSID.
- If using multiple Hosts, assign a different static IP to each via **Network > Interfaces > Edit**, and record those IPs.

Click **Save & Apply** when done.

8a.4. Set Up the Client

- Disconnect the Host and connect the Client unit via PoE (do not connect both at the same time).
- Access the GUI at **192.168.1.202**, password: password.
- Go to **Network > Wireless > Edit (wifi1)**.
- Set **Mode** to **Client (WDS)**.
- Enter the Host's SSID if it was customized.
- Click **Save & Apply**.

8a.5. Assigning a New IP to the Client

- Go to **Network > Interfaces > Edit** and set a static IP **different** from the Host (still in the same subnet).
- Click **Save & Apply**.
- If you change the subnet, update your PC's IP settings to match.

8b. Setting Up a New WES5 Client to Link to an Existing WES4 Host

🔧 Converting a Default WES5-AX-CF to a Client (WDS) to Link to WES4 Host

---

✅ PREPARATION

1. **Power the WES5-AX-CF Client** via PoE and connect it directly to your laptop.
2. **Set your laptop's IP** to a static address in the **192.168.1.x** range (e.g., 192.168.1.50).
3. Access the WES5 GUI at **http://192.168.1.202**.
   Default password: password.

⚙️ STEP 1: Disable MAC Filtering on the WES4 Host (if possible)

Since the existing WES4 Host is configured to only allow devices with a specific MAC address (that is now inactive), you **must either**:

- **Option A (easier):** Temporarily disable MAC filtering on the WES4 Host.
- **Option B:** Add the **WES5-AX-CF MAC address** (visible on the device label or from **Status > Overview** in the WES5 GUI) to the WES4's Allow List.

If MAC filtering remains enabled and the WES5's MAC is not listed, the link will fail regardless of other correct settings.

⚙️ STEP 2: Set WES5-AX-CF to Client (WDS) Mode

1. In the WES5 GUI, go to **Network > Wireless**.
2. Find the second wireless interface (**wifi1**, which is the 5 GHz radio).
3. Click **Edit** next to wifi1.
4. Scroll to **Interface Configuration > General Setup**.
5. Set **Mode** to **Client (WDS)**.
6. In the **ESSID** field, enter the **exact SSID of the WES4 Host** (case-sensitive).

7. Set **Encryption**:
    - Choose **WPA2-PSK** (or match the WES4's setting exactly).
    - Enter the **WPA2 passphrase** used on the WES4 Host.
8. Click **Save & Apply**.

⚙️ STEP 3: Change the IP Address of the WES5 Client

To avoid IP conflict with the WES4 Host (assuming it is also on **192.168.1.202** or similar):

1. Go to **Network > Interfaces**.
2. Click **Edit** next to the LAN interface (likely eth0 or br-lan).
3. Change the **static IP** to another unique IP on the same subnet (e.g., **192.168.1.203**).
4. Click **Save & Apply**.
5. Update your laptop's IP (if needed) so it's in the same subnet to maintain GUI access.

✅ STEP 4: Final Checks and Testing

1. Reboot the WES5 (or manually restart wifi1 if reboot isn't needed).
2. In the WES5 GUI, check **Status > Wireless**:
    - Look for **Signal Strength (RSSI)** and **Connection Time** to confirm the link to the WES4.
3. Try pinging the WES4 Host from **System > Diagnostics > Ping** using the WES4's IP address.
4. If the ping works and the signal is present, the link is successful.

✅ TROUBLESHOOTING NOTES

- **If there is no link**: Double-check the ESSID, passphrase, encryption type, and MAC filtering status on the WES4.
- **If signal is low or link unstable**: Verify line-of-sight and antenna alignment between the devices.

- **If Client shows connected but no data flow**: Verify IP settings and subnet compatibility.

8c. Configuring a WES5-AX-CF (or WES5-AX-BF) as a Host to Link to a WES4 / WES4HTG Client

⚙️ **Scenario:**

- **WES5-AX-CF or WES5-AX-BF** is the new **Host/AP**.
- **WES4-AX-CF** (or WES4HTG-AX-CA) remains in the field as the **Client**.
- **WES4 / WES4HTG Client** is using **5 GHz**, in **802.11ac mode**, with **WPA2/WPA Mixed Mode**, and is currently set to **SSID: WES4** *or WES4HTG* (default for those series).

✅ **PREPARATION**

1. Power the WES5-AX-CF via PoE.
2. Connect a laptop directly to the WES5 via PoE switch or injector.
3. Set your laptop's IP to a **static address on the 192.168.1.x subnet** (e.g., 192.168.1.50).
4. Access the WES5 GUI at **http://192.168.1.202**.
   Default login password: password.

⚙️ **STEP 1: Configure WES5 wifi1 Interface as Host (AP)**

1. In the WES5 GUI, go to **Network > Wireless**.
2. Locate the second wireless interface — **wifi1** (5 GHz radio).
3. Click **Edit** on wifi1.
4. Under **Interface Configuration > General Setup**:
   - Set **Mode** to **Access Point (WDS)**.
   - Change **ESSID** to WES4 to match the default SSID expected by the WES4 Client.
     - ⚠️ If the WES4 Client is not using the default SSID, change either it **or** this WES5 setting so they match **exactly** (case-sensitive).

- Confirm **Wireless Mode** is **802.11ac** (WES4 needs 802.11ac capability).

5. Scroll down to **Wireless Security**:
   - Set **Encryption** to **WPA2/WPA Mixed Mode**.
   - Set the **passphrase** (PSK) to match what the WES4 Client is using. The default is 11111111
6. Click **Save & Apply**.

⚙️ STEP 2: Adjust Channel & Transmit Settings (Optional, but recommended)

1. Still in the **wifi1 Edit** screen:
   - Set a fixed **Channel** (preferably a clean 5 GHz channel like 36, 40, 44, or 149).
     - ⚠️ The WES4 Client may not support DFS channels, so choose a **non-DFS** channel unless you've confirmed support.
   - You can also fine-tune **Transmit Power**, **Country Code**, and **HT Mode** (e.g., VHT80 for 80 MHz width if supported by the WES4).

⚙️ STEP 3: Optional - Change LAN IP of the WES5 Host (Avoid Conflict)

If the WES4 Client is also set to the default IP (192.168.1.202), you may want to **change the WES5 Host's IP** to avoid future confusion.

1. Go to **Network > Interfaces**.
2. Click **Edit** next to LAN interface (likely br-lan).
3. Change the **static IP** (e.g., to 192.168.1.210).
4. Click **Save & Apply**.
5. Update your laptop's IP if needed to remain in the subnet.

⚙️ STEP 4: Confirm Link from WES4 Client

Once settings are applied:

1. Ensure the **WES4 Client** is powered and within range.

2. On the WES4 GUI, check:
    - **SSID** matches (WES4).
    - **Encryption** is set to **WPA2/WPA Mixed Mode**.
    - **Wireless Mode** is **Client WDS**, and band is 5 GHz with 802.11ac enabled.
3. Watch for link-up status on the WES4 or ping from its Diagnostics page to the WES5 Host.

✅ **TROUBLESHOOTING TIPS**

- If there is no link:
    - Confirm SSID, channel, and encryption match exactly.
    - Ensure WES5 Host isn't set to WPA3 or DFS-only channels.
    - Check signal strength and antenna alignment.
- If WES4 Client doesn't support your selected WES5 channel, try switching to a different **non-DFS** 5 GHz channel.

9. System Management

This section covers essential system management functions for maintaining and supporting your WES5 device over time. It includes instructions for backing up and restoring configurations, performing factory resets, and updating firmware. Proper use of these tools ensures system stability, simplifies recovery, and helps maintain compatibility with future features and security updates.

9a Backups and Restores

Creating a backup of your WES5 configuration is recommended before making significant changes or deploying multiple units with a common setup.

To back up the current configuration:

1. **Log in** to the WES5 web interface using the device's IP address (default is 192.168.1.202).
2. From the top menu, click **System**.
3. In the left-hand menu, select **Backup / Flash Firmware**.

4. Under the **Backup** section, click the **Generate archive** button.
5. Your browser will download a .tar.gz file containing the full configuration.

🗂️ **Tip:** Rename and store the backup file securely with a descriptive name and date for easy identification later.

This file can later be restored on the same unit or uploaded to another WES5 to replicate the settings. See Section 9b for restoration steps.

9b Resetting to Default

If you need to restore the WES5 to factory default settings (such as when troubleshooting or repurposing a unit), you can do so through the web interface.

To perform a factory reset via the GUI:

1. Log in to the WES5 web interface.
2. Click the **System** tab from the top menu.
3. In the left-hand menu, select **Backup / Flash Firmware**.
4. Scroll to the **Reset to defaults** section at the bottom of the page.
5. Click the **Perform reset** button.

The unit will reboot and return to factory settings, including:

- Default IP: 192.168.1.202
- Default username/password
- Default SSIDs and wireless settings

⚠️ **Warning:** All configuration changes will be lost. Make sure to back up your configuration (see Section 9a) before resetting if needed.

9c Updating Firmware

Firmware updates provide new features, security patches, and compatibility improvements. Always ensure the device remains powered during the firmware upgrade process.

To update firmware on the WES5:

1. Download the latest WES5 firmware file (.bin or .img) from the KBC Networks support site or your authorized distributor.
2. Log in to the WES5 web interface.

3. Click the **System** tab, then choose **Backup / Flash Firmware** from the left-hand menu.
4. Under the **Flash new firmware image** section:
    - Click **Browse** to select the downloaded firmware file.
    - (Optional) Uncheck **Keep settings** if you want to perform a clean install.
5. Click **Flash image**.
6. On the next page, click **Proceed** to confirm.

The device will install the firmware and reboot automatically. This may take several minutes.

✅ **Tip:** After reboot, clear your browser cache or use a fresh browser session to avoid issues loading the updated GUI.

10. Troubleshooting and Best Practices

This section provides guidance for diagnosing common issues and optimizing performance in WES5 wireless deployments. It includes tips for evaluating link quality, identifying configuration conflicts, and ensuring stable, long-term operation. Following these best practices can help reduce downtime, simplify support, and ensure a reliable wireless connection in both point-to-point and point-to-multipoint environments.

10a Link Quality and Signal Strength

To ensure optimal performance, regularly monitor the signal strength and link quality between WES5 units.

How to check link quality:

1. Log into the **Client** unit's GUI.
2. Go to **Status > Wireless**.
3. Look for:
    - **Signal Strength (RSSI)**: Ideal is between **–40 dBm to –65 dBm**.
    - **Signal-to-Noise Ratio (SNR)**: Aim for **25 dB or higher**.
    - **TX/RX Rate** and **Uptime**.

📶 **Tip:** Poor signal quality (RSSI weaker than –75 dBm) can cause drops or slow speeds. Consider antenna adjustments or moving the units for better line-of-sight.

10b Antenna Alignment

Proper alignment is critical for stable links, especially for directional antennas like those on WES5 radios.

To align antennas:

1. Mount both radios securely at the desired elevation.
2. Use **visual line-of-sight** and remove any obstacles if possible.
3. On the **Client** radio:
    - Go to **Status > Wireless**.
    - Use **Signal Strength (RSSI)** as a live reference.
4. Slightly adjust the angle of the antenna while watching the RSSI update.
5. Lock antennas in place once optimal signal is reached.

🧭 **Tip:** Small adjustments (even 1–2 degrees) can significantly improve performance.

10c IP Conflicts and Subnet Mismatch

A common issue in deployments is overlapping IP addresses or incompatible subnets, which can block GUI access or communication.

Avoiding IP conflicts:

- Ensure each WES5 unit has a **unique static IP**.
- Avoid duplicating **192.168.1.202**, the default address, across multiple devices.
- When linking units, ensure all are on the **same subnet** (e.g., 192.168.1.x with subnet mask 255.255.255.0).

If you suspect a conflict:

- Disconnect the suspected unit from the network.
- Connect it directly to a PC with a static IP.
- Access it at 192.168.1.202 or the IP you previously assigned.
- Change its IP if needed.

10d Common Setup Mistakes

Avoid these frequent missteps that can prevent successful operation:

- ❌ **Host and Client in the same switch**: Once a Host and Client are configured to one another to link in a Host/Client wireless relationship, they cannot be powered via the same switch. This will cause a network loop.
- ❌ **SSID mismatch**: Ensure the SSID on the Client exactly matches the Host's (case-sensitive).
- ❌ **Incorrect MAC Address in MAC-Filter**: If the MAC-Filter is enabled, be sure to use the correct radio MAC address. If this is disabled and the units connect then you can know that the MAC-Filter was set incorrectly.
- ❌ **Encryption mismatch**: WPA3 on a WES5 won't connect to a WES4 Host; use **WPA2/WPA Mixed Mode** instead.
- ❌ **Incorrect SAE (or PSK)**: If you notice a MAC address briefly appearing on the Status screen "Wireless Connections" then it could be failing the Host's authentication process due to the SAE (or Pre-shared Key if WPA2) not matching the Host.
- ❌ **Incorrect Wi-Fi Interface**: When configuring the 5 GHz radio for long range wireless video applications, be sure to click "Edit" next to wifi1, not wifi0 which is 2.4GHz. The 2.4GHz wifi0 radio and antenna will not be strong enough for long range ptp connectivity and is intended for local "HotSpot" usage. The wifi0 interface can be disabled if not using for that purpose.
- ❌ **Incorrect Mode**: Be sure the Host is set to **Access Point (WDS),** and the Client is **Client (WDS)**.
- ❌ **DFS Channel issues**: If it is noticed that the frequencies are changing too often then the Host is on a Dynamic Frequency Selection channel and there are 3rd party RF sources stepping on the frequencies being used. To remain on a static frequency, use **non-DFS 5 GHz channels** (e.g., 36~48, 149~161).
- ❌ **Client unit cannot be seen from Host**: If you run a scan on any WES5 or previous generation, the only devices that will appear are other Host/Access Points so no Clients will show up on the scan feature. If the Client cannot be seen meaning that there are no Wireless Connections or the IP will not ping, then there is no RF link from Host to Client.

✅ **Best Practice:** Configure units one at a time on a bench, verify connectivity, then deploy in the field.

✅ **Best Practice:** Ensure wide-open line-of-sight between Host and Client(s) and use in environments free of harsh third-party RF interference.

✅ **Best Practice:** Use outdoor rated Cat5e or Cat6 Ethernet cabling.

✅ **Best Practice:** Align antennas until all 4 RSSI LEDs (i.e. S1~S4) are lit up. For fine tuning antenna alignment, use the Status Page Signal indicator under Wireless Connections. The ideal signal strength is 40~65 with a TxCCQ of 80~100%