Yellowjacket-Ultra

Wi-Fi Tester User Manual 1.8

Table of Contents

Yellowjacket-Ultra Overview ……. 2

Unpacking ……..……. 6

Dimensions and Weights …….……6

Omni Antenna Specifications …….…… 7

Direction Finding Antenna …….…… 9

Quick Start Guide ……..……. 10

Yellowjacket-Ultra Screen Navigation Tree ……..…… 11

Main Menu Screen …….…… 12

Wi-Fi Scan List Screen…… 13

Wi-Fi Networks Screen…….....……...……....14

Authorized APs ……..……..…….……..... 15

Wi-Fi Channels Screen…….....……...…….... 16

Channel Configuration Screen…….....…….....17

Scan Setup Screen…….....…...……....18

Direction Finding Screen ….……..……..... 19

MAC Hunter Screen ….……..……..... 21

Unit Information Screen…….…….... 22

Hardware Status Screen…….…….... 23

Storage Space Screen…….…….…….... 24

Whitelist Editing Screen…….……..…….…….…….... 25

Blacklist Editing Screen…….…….…….…….....26

Screenshot Management Screen ……...……..... 27

GPS Recordings Management …….…….…….....28

Data Recordings Management…..……..…….…….....29

Unit Settings Screen ……..…….…….……..... 30

Wi-Fi Overview…….…….…….....31

Yellowjacket-Ultra Overview

The **Yellowjacket-Ultra** by Berkeley Varitronics Systems is a professional-grade wireless threat detection and direction-finding platform engineered for security personnel tasked with protecting sensitive data and controlled environments. In today's threat landscape, any wireless technology can become an unmonitored pathway for data exfiltration, credential harvesting, and classified information compromise. The Yellowjacket Ultra provides the RF visibility required to detect, analyze, and physically locate these threats in real time.

Purpose and Mission

Modern facilities handling sensitive intellectual property, regulated data, or classified information—including corporate data centers, research labs, defense contractors, and Sensitive Compartmented Information Facilities (SCIFs)—require more than traditional network monitoring tools. Many wireless threats operate outside managed infrastructure:

- Unauthorized access points installed under desks
- Rogue cellular hotspots bypassing perimeter firewalls
- "Evil Twin" SSIDs impersonating trusted networks
- MAC-spoofed devices attempting to evade monitoring
- Hidden or non-broadcast SSIDs
- Deauthentication attack platforms

The Yellowjacket Ultra bridges the gap between digital cybersecurity monitoring and **physical RF investigation**, enabling operators to move from detection to physical interdiction.

Operational Capabilities

The Yellowjacket Ultra is designed to provide:

1. Wireless Device Discovery

The Wi-Fi Scan List displays detected access points and clients, sortable by SSID, MAC/BSSID, RSSI (dBm) and channel. This enables rapid identification of unauthorized or suspicious transmitters.

2. Channel Analysis & Congestion Mapping

The Wi-Fi Channels overview provides a graphical representation of 2.4 GHz and 5 GHz spectrum activity. Operators can identify channel overlap, congestion, and anomalous transmitters.

3. Direction Finding (DF)

When paired with the directional antenna, the Yellowjacket Ultra transforms into a precision location tool. The dynamic RSSI needle provides real-time signal strength feedback, allowing operators to:

- Track signal gradients
- Isolate rogue APs
- Locate hidden transmitters
- Identify external threats leaking into secure facilities

Signal strength interpretation (RSSI in dBm) allows operators to estimate proximity, with stronger signals (e.g., -40 dBm) indicating closer physical distance than weaker signals (e.g., -80 dBm). Understanding RF propagation characteristics—including attenuation caused by steel, concrete, glass, and human bodies—is critical for accurate direction finding.

4. Evil Twin & Rogue AP Detection

Duplicate SSIDs with differing BSSIDs and unexpected channel assignments are flagged for rapid investigation. This capability is vital for preventing credential harvesting and man-in-the-middle (MITM) attacks.

5. MAC Hunter & Targeted Tracking

Operators can manually input specific MAC addresses to track known devices of interest—useful in forensic investigations, insider threat monitoring, or compliance sweeps.

6. Logging & Documentation

Integrated screenshot capture and logging features support evidentiary documentation, compliance audits, and after-action reporting.

National Security & SCIF Applications

In environments handling classified, controlled unclassified information (CUI), export-controlled technical data, or proprietary intellectual property, unmanaged wireless signals pose unacceptable risk.

The Yellowjacket Ultra supports:

- SCIF perimeter validation
- Detection of unauthorized PEDs/mobile devices
- Identification of covert hotspots
- Signal leakage assessments
- Quarterly RF security sweeps
- Incident response investigations

Understanding propagation characteristics is critical. For example:

- **2.4 GHz signals** travel farther and penetrate walls more effectively but are more prone to congestion.
- **5 GHz / 5.8 GHz signals** provide higher throughput but attenuate more quickly and are more susceptible to obstruction loss.
- Reinforced concrete and steel significantly reduce signal strength.
- Reflections and multipath can create false signal peaks during hunts.

Effective operators move slowly, rotate deliberately, and confirm consistent signal increases when closing in on a device.

Bridging Cybersecurity and Physical Security

Traditional cybersecurity tools monitor network logs and endpoint telemetry. However, they cannot:

- Physically locate a rogue access point hidden in a ceiling tile
- Identify a hotspot broadcasting from a vehicle in a parking lot
- Detect a cloned BSSID transmitting from an unexpected physical location
- Confirm signal leakage beyond facility boundaries

The Yellowjacket Ultra empowers security teams to translate digital anomalies into physical action.

Intended Operators

This manual is written for:

- Corporate security teams
- Government security officers
- SCIF managers
- Defense contractors
- Law enforcement investigators
- IT and network security administrators
- RF security auditors

Proper training in RF fundamentals, Wi-Fi architecture, and secure facility procedures is recommended prior to deployment.

Operational Philosophy

Wireless threats are dynamic. Devices move. Attackers adapt. Signals reflect.

The Yellowjacket Ultra is not merely a scanner—it is an investigative instrument. Its effectiveness depends on:

- Systematic sweep methodology
- Accurate interpretation of RSSI
- Awareness of environmental RF behavior
- Validation against authorized device inventories
- Thorough documentation

Used properly, the Yellowjacket Ultra becomes a critical component in layered defense strategy—protecting sensitive data, intellectual property, classified information, and national security assets.

Unpacking

Your Yellowjacket-Ultra ships with unit and all accessories in a rugged Pelican transport case. The items include:

- (1) Yellowjacket-Ultra unit
- (1) Omni directional antenna
- (1) Direction finding antenna
- (1) USB-C power adapter and cable
- (1) USB-A to USB-C cable
- (1) Pelican 1500 rugged transport case

Dimensions and Weights

Yellowjacket-Ultra ships in a 20” x 15” x 6” box weighing 12 pounds (51cm x 38cm x 15.24cm and 5.44 kg)

Omni Antenna Specifications

ANT-DB1-LCD-ccc

Data Sheet

Linx TECHNOLOGIES

Product Description

The Linx LCD Dipole Antenna is a superior solution for users searching for best-in-class performance for WLAN devices using Dual-Band WiFi (802.11ac, 802.11n, 802.11ax) or U-NII applications.

With a compact package and low price, the LCD's high peak gain and superior efficiency make it an excellent option for high volume, cost sensitive applications.

Dipole design means that no additional ground plane is required.

Features

- Excellent performance
- Dual-band
- Very low VSWR
- Omni-directional pattern
- Tilt and swivel base
- Standard SMA or Part 15 compliant RP-SMA connector

Ordering Information

ANT-DB1-LCD-RPS (with RP-SMA connector)
ANT-DB1-LCD-SMA (with SMA connector)

Electrical Specifications

Parameter	2.4GHz WiFi	U-NII	5.8GHz WiFi/ U-NII-3 Band
Recommended Frequency Range	2.4 – 2.5GHz	5.125 – 5.725GHz	5.725 – 5.875GHz
VSWR	<2:1	<2:1	<2:1
Peak Gain (max in the band)	2.8dBi	4.5dBi	2.92dBi
Average Gain (typical)	–0.6dBi	–1.5dBi	–2.2dBi
Efficiency (typical)	85%	70%	65%
Polarization	Linear		
Radiation	Omni-Directional		
Max Power	10W		
Wavelength	1/2-wave		
Impedance	50 ohms		
Connection	SMA Plug (Male) or RPS (Reverse Polarity Male)		
Weight	7.4g (0.26oz.)		
Operating Temperature Range	-40°C to +80°C		

Measurements taken on a 100 x 100mm ground plane, mounted on the edge, bent 90°.

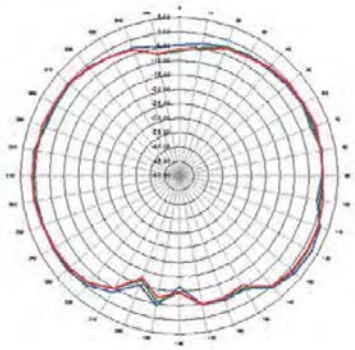
Gain Plots - Edge of Plane, Bent 90°

XZ-Plane Gain

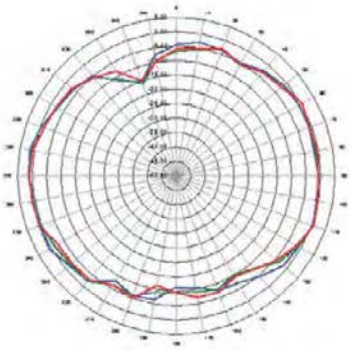
YZ-Plane Gain

XY-Plane Gain

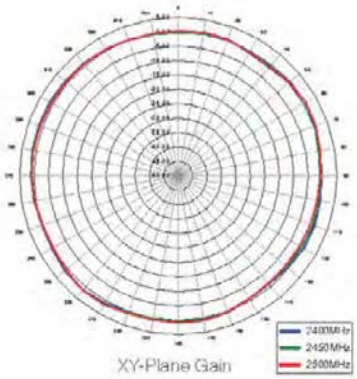
2400 - 2500MHz



XZ-Plane Gain

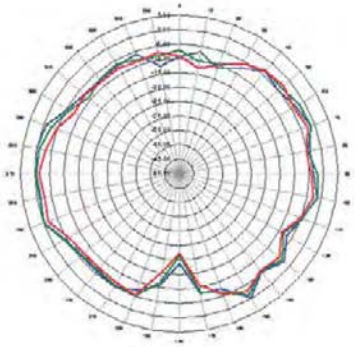


YZ-Plane Gain

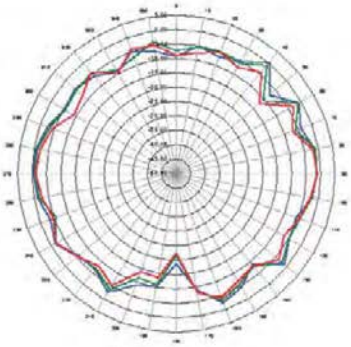


XY-Plane Gain

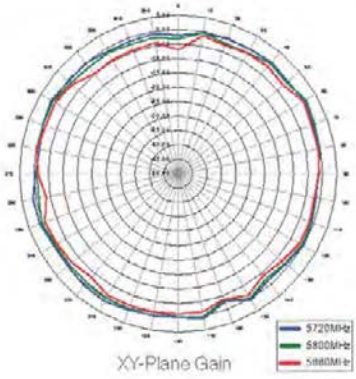
5720 - 5880MHz



XZ-Plane Gain



YZ-Plane Gain



XY-Plane Gain

Direction Finding Antenna

Yellowjacket-Ultra includes an omni-directional antenna and direction finding antenna. Initial measurements are taken using the small omni-directional antenna. Once you have an overview of the Wi-Fi signals in your area and want to concentrate on a particular AP or device, connect the direction finding antenna and bracket to your unit. Screw in the SMA antenna connector and secure the bracket to your unit using the embedded thumb screws. Note that while there are two different antenna connectors, it does not matter which one is used for direction finding.

Dual Band Directional Patch Antenna

High gain directional antenna

Covers 2.4 & 5GHz for WIFI/WLAN

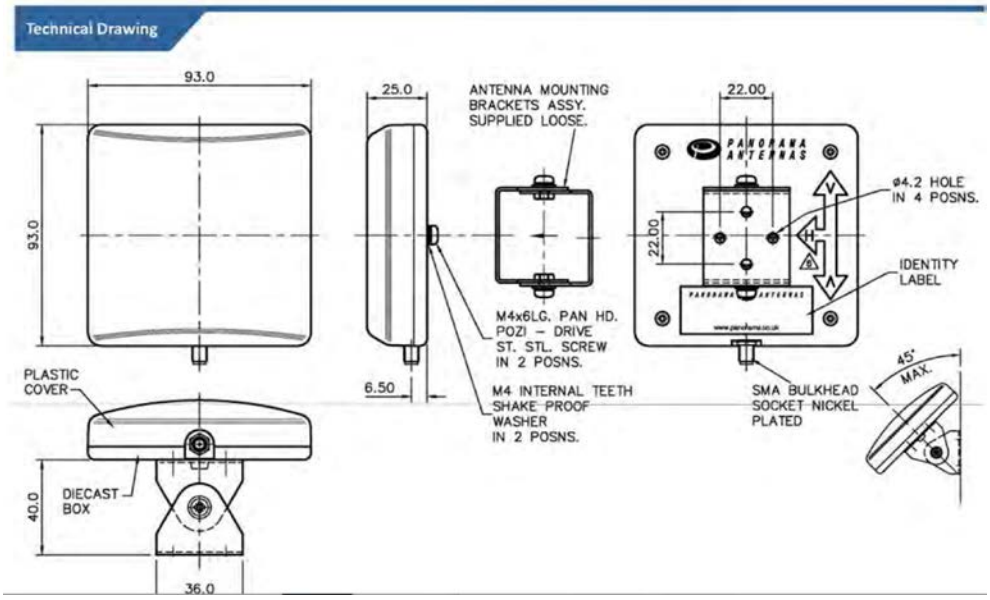
Ideal WIFI coverage extender for large rooms, car parks & warehouses

The Panorama client patch antenna is a directional wall or mast mounted antenna covering 2.4 & 5GHz for WIFI / WLAN applications.

This antenna is ideal for point to point communications or can be used to cover a wide area thanks to its relatively wide beamwidth in the horizontal and vertical planes. Several of these antennas can be used to provide cost effective sectored coverage.

The antenna is supplied with a 90 degree adjustable wall / mast mount angle bracket to give optimal mounting flexibility.

Ideal to infill network coverage black spots or to provide a consistent connection for subscriber terminals the W24-58-CP-9 is a cost effective solution to network coverage issues.



Yellowjacket-Ultra Field Quick Start Guide

Portable RF visibility and Wi-Fi direction finding

SCAN **IDENTIFY** **TRACK**

Quick Start Guide

1. Power On: Press and hold the power button until the device boots.
2. Attach Omni Antenna: Use the small antenna for initial scanning.
3. Start Scan: From Main Menu, select 'Wi-Fi Scanner' to view detected devices.
4. Identify Targets: Sort by RSSI or SSID to find unknown or suspicious devices.
5. Select Device: Tap a device to enter Direction Finding (DF) mode.
6. Switch to Directional Antenna: Attach patch antenna for tracking.
7. Locate Signal: Rotate slowly and follow increasing signal strength (e.g., -80 to -50 dBm).
8. Confirm Source: Physically locate device and verify against authorized list.
9. Document Findings: Capture screenshots or start data logging if needed.

Field Quick Guide (1-Page Reference)

Quick Indicators

- Strong signal (-40 dBm) + unknown device = investigate
- Duplicate SSID + different BSSID = possible Evil Twin
- Rapid RSSI changes = reflections or movement

RSSI Guide

- -30 dBm = Very close
- -50 dBm = Strong
- -70 dBm = Moderate
- -80 dBm = Weak

Direction Finding Tips

- Move slowly
- Rotate device steadily
- Follow strongest consistent signal
- Avoid body blocking antenna

Antenna Use

- Omni: initial scan
- Directional: locating target

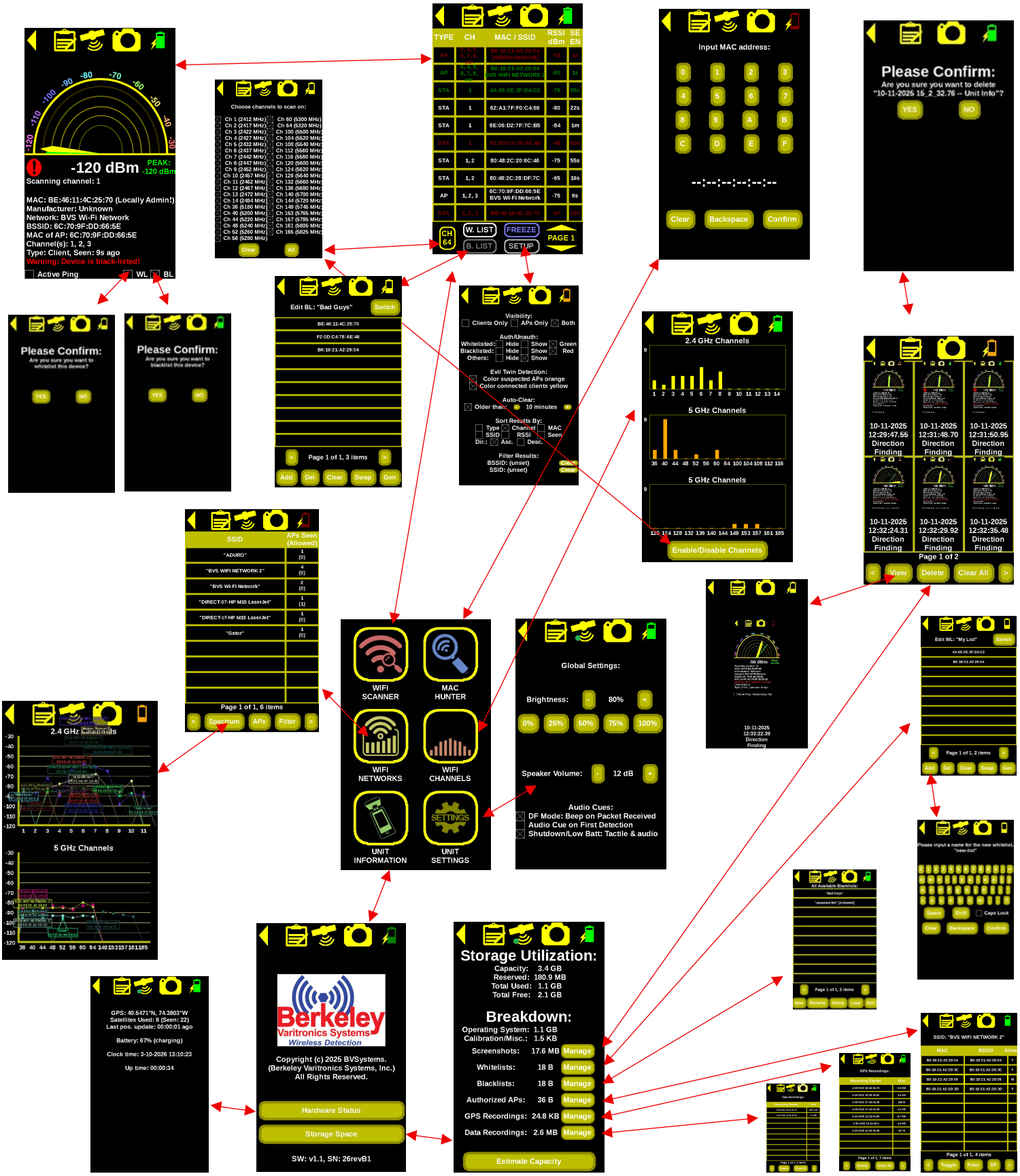
Common Issues

- No devices: check antenna connection
- Weak DF response: switch antenna
- GPS not working: move outdoors

Best Practices

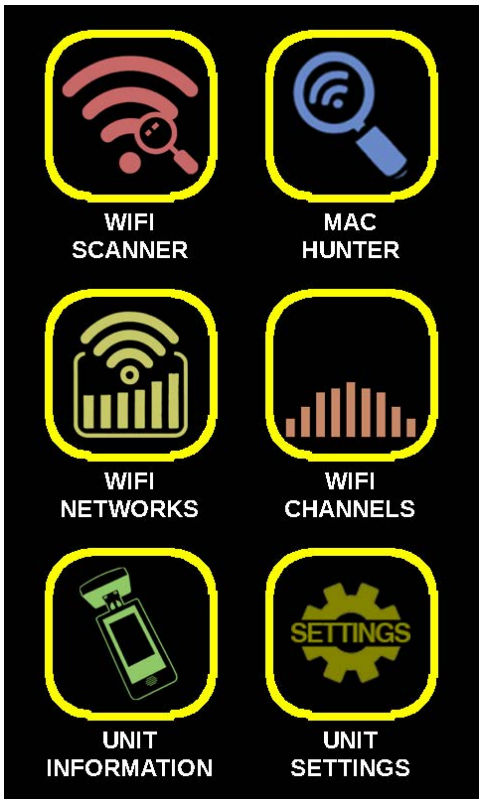
- Always verify against whitelist
- Log findings for reports
- Re-check suspicious signals from multiple angles

Yellowjacket-Ultra Screen Navigation Tree



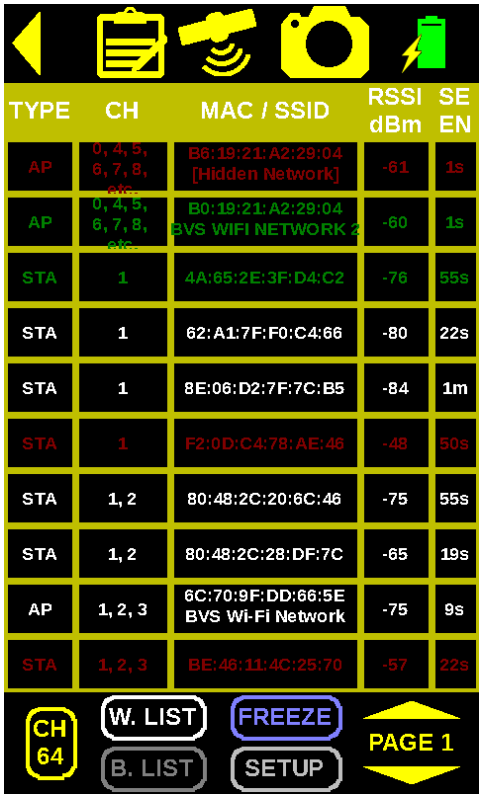
Main Menu Screen

This screen allows users to navigate directly to one of the six areas: Wi-Fi Scanner, MAC Hunter, Wi-Fi Networks, Wi-Fi Channels, Unit Info and Unit Settings. Touch the back arrow on the upper left of any screen to return back to this main menu screen.



Wi-Fi Scan List

This screen lists all currently detected Wi-Fi access points and clients. Devices are listed and can be sorted by type, channel, MAC/SSID, RSSI (dBm) and last seen by entering the SETUP screen to adjust preferences. Users may also sort all these columns by simply tapping the column header names at the top. The buttons along the very top are common to all screens in the Yellowjacket-Ultra. On the top left is the back arrow which takes users back to the previous screen. Next to that is the data logger (clipboard and pen icon) which allows users to start and stop all data recordings (standard .PCAP file). The data logging button flashes red while data recording is in progress. The GPS button (satellite icon) takes users to a screen displaying the number of satellites that are visible / in-use and the current GPS positioning. When the unit has GPS lock, a green indicator will appear on the bottom-right of this icon, and a red flashing indicator will appear when a GPS data recording is in progress (standard .CSV file). Note that GPS position tracking may not work indoors or in areas where the signal strength is low. Next to that is the screen snapshot (camera icon) which takes a single screen snapshot each time the user touches it. On the top right is the current battery level indicator (battery icon) which changes dynamically. A lightning bolt indicates that the unit is currently being charged. A fully charged battery delivers 4 to 5 hours of runtime. A row of buttons on the bottom also appear only on this screen.



CHANNELS – Touch this button to go directly to the CHANNEL CONFIGURATION screen. This button is dynamic so the channel number currently displayed is also currently being scanned.

WHITELIST – Touch this button to navigate to a whitelist of friendly or known Wi-Fi devices to avoid unwanted detection alerts.

BLACKLIST – Touch this button to navigate to a blacklist of unknown or suspicious Wi-Fi devices to reduce gratuitous detection alerts.

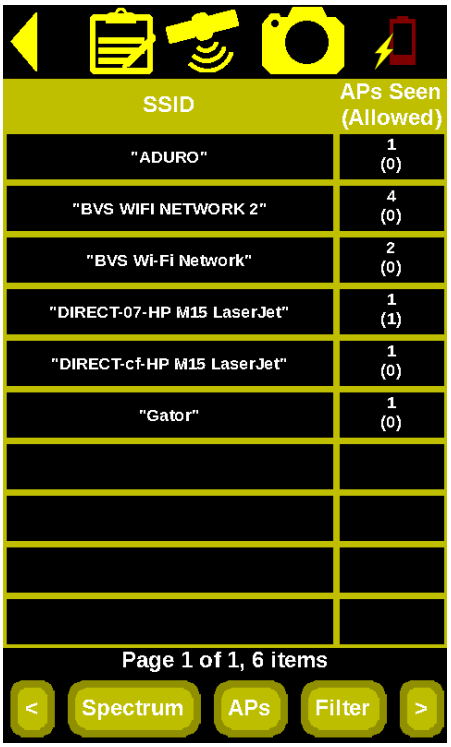
FREEZE – Touch this button to get a better look at an active screen by "freezing" it until you are ready to resume viewing live measurements.

SETUP – Touch this button to enter the SCAN SETUP screen to access additional settings.

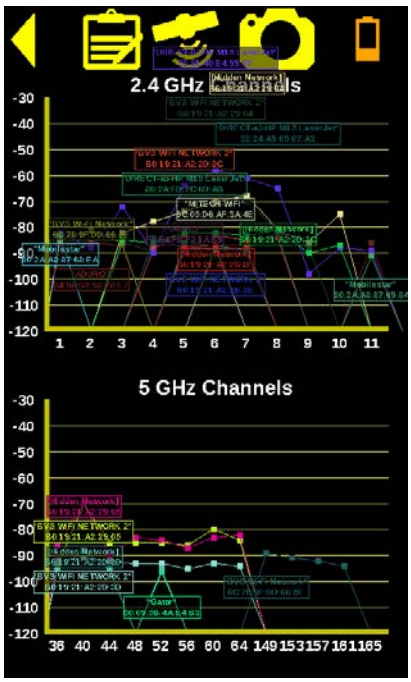
PAGE – Touch the top and bottom arrows to navigate between pages.

Wi-Fi Networks Screen

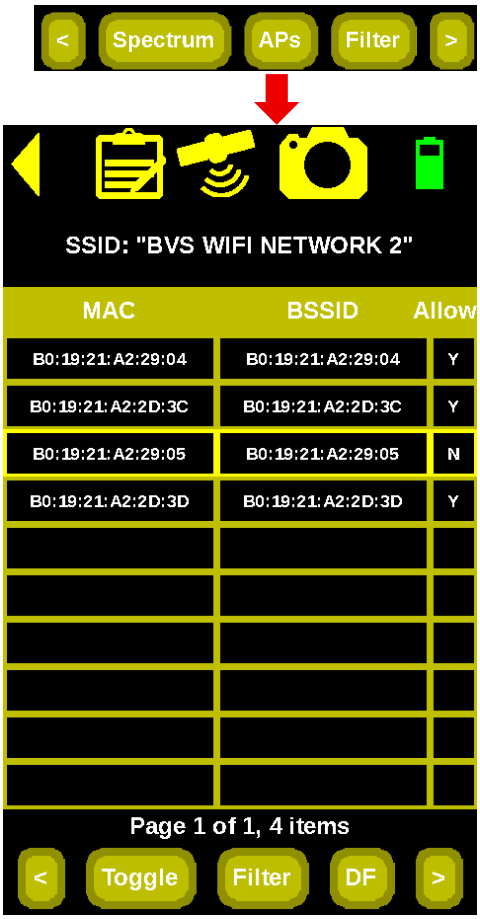
This screen displays a list of all "known networks" (a network is "known" if any APs have been detected broadcasting its SSID since the unit has booted up, or if any APs have been "authorized" to broadcast that SSID). Some of these SSIDs may also appear on the Wi-Fi Scan List screen of devices as well. Alongside the SSID, the list shows how many APs have been detected broadcasting that SSID, and how many have been "allowed" to broadcast that SSID. By clicking the "Filter" button, the user can filter their scan results to only show APs and devices associated with that SSID in the Scan Results screen (clearable using the "Clear SSID filter" button in Scan Setup). By clicking the "APs" button, the user is taken to the list of APs for that network.



The "Spectrum" button takes the user to the Spectrum View screen which diplays all APs by signal strength on both 2.4 GHz and 5 GHz channels.



Authorized APs



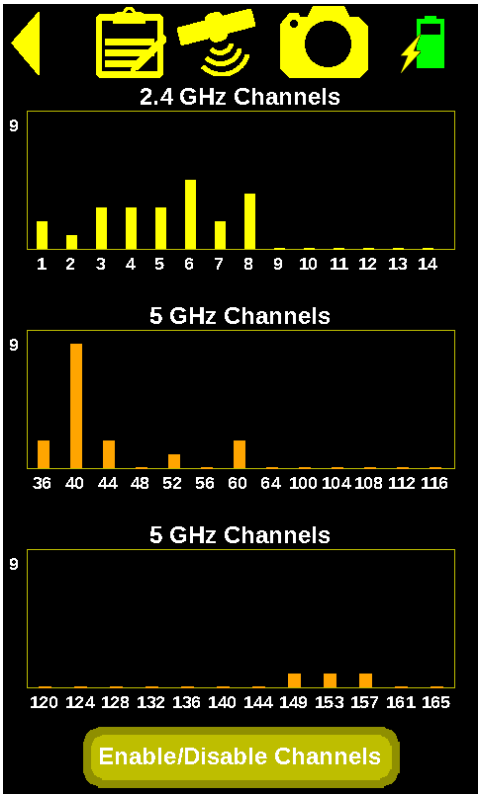
This screen shows a list of all APs associated with a given network, by the AP's BSSID. That includes both APs that have been detected broadcasting its SSID since the unit has booted up, and any APs that have been "authorized" to broadcast that SSID.

The purpose of "authorizing" APs to transmit a given SSID is for Evil Twin detection: if a given SSID has one or more APs "authorized", then any APs which are not "authorized" are potential Evil Twin APs masquerading as a legitimate AP to trick unknowing devices into connecting. This is accomplished by first selecting a MAC and then selecting “Toggle” to authorize each AP on a given Wi-Fi network indicated by Y/N in the "Allow" column.

The "DF" button takes the user to the Direction Finding screen to look for a given AP. The "Filter" button works similarly to the one on the Networks screen, except it filters by the selected AP's BSSID instead of the network's SSID.

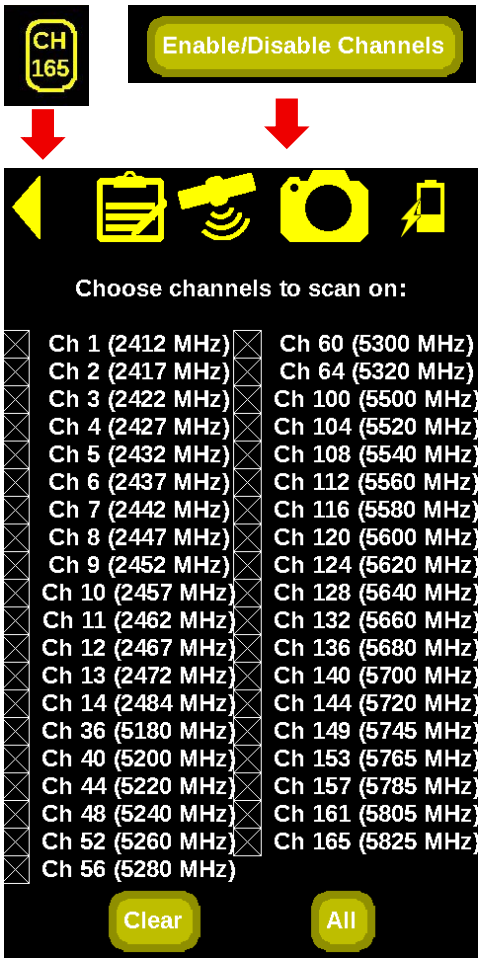
WiFi Channels Screen

This screen allows users to get an overview of 2.4 GHz and 5 GHz activity on all channels. The column height indicates the number of devices seen on each channel. For instance, the number (9) at the top left of each set of channels is the maximum number of devices seen on any channel. Touch the Enable/Disable Channels button on the bottom to navigate to the CHANNEL CONFIGURATION SCREEN.

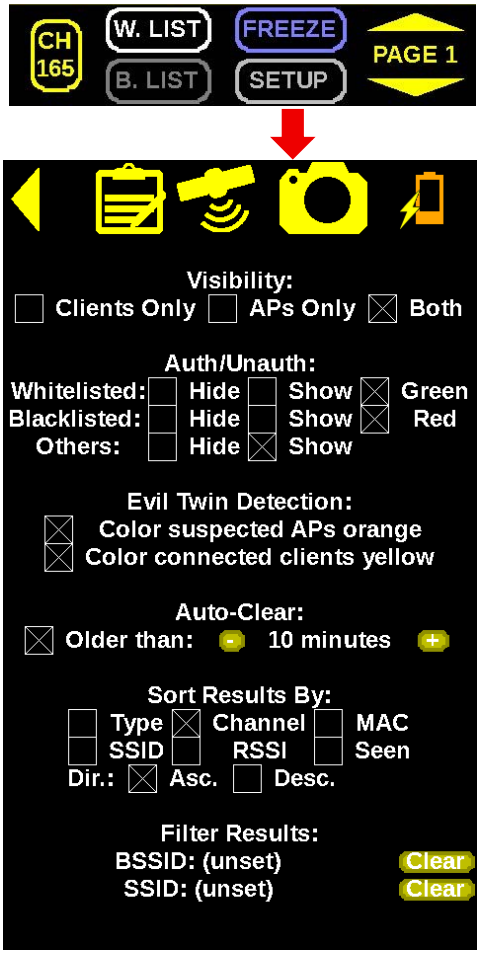


Channel Configuration

This screen allows users to select and deselect any channel to be scanned. This not only frees up visual clutter by reducing the number of pages in the SCAN LIST screen but also decreases the scan time slightly depending upon how many channels are being simultaneously. This screen also allows the user to easily see the frequency that is associated with each channel. Select each channel individually and choose CLEAR to deselect all. Selecting ALL will select all visible channels at once.



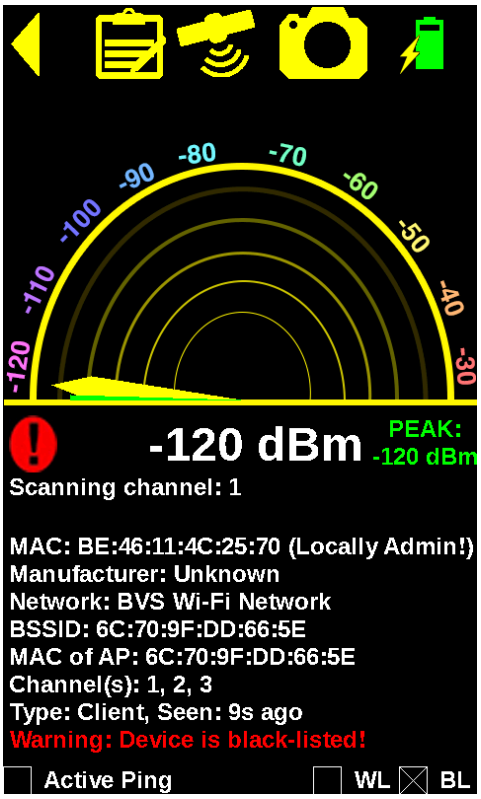
Scan Setup Screen



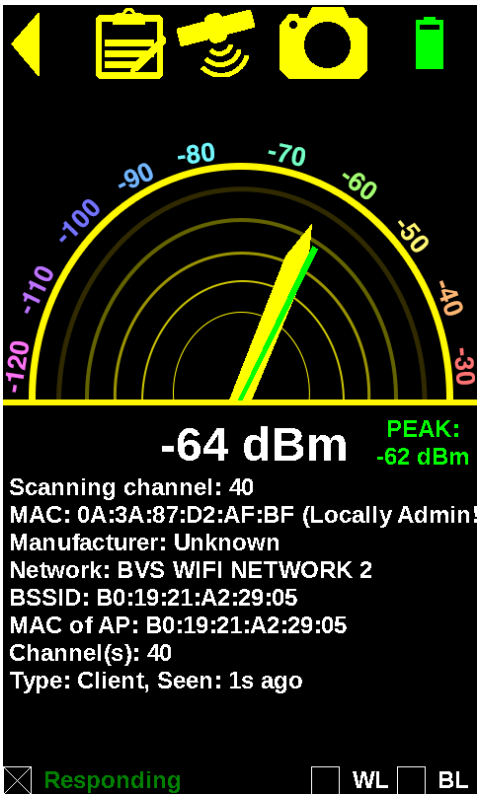
This screen allows all kinds of preferences for displayed, scanned or sorted measurements. To reduce clutter, users can select clients only, APs only or both for the most comprehensive view. Users may adjust visibility preferences for whitelisted and blacklisted measurements. Color coding for evil APs can be adjusted as well. An auto-clear function allows measurements to be automatically removed after a user-specified time increment to keep the scan list updated and fresh. The ‘sort results by’ in the scan list can be organized by their respective column headers in ascending or descending order. Finally, users can clear filters set on the Wi-Fi Networks screen for BSSID and SSID by touching the “Clear” buttons at the bottom.

Direction Finding Screen

Touching any AP or client in the SCAN LIST will take users directly to this DF (Direction Finding) screen for more measurement data. If you do not already have the direction finding antenna connected to your Yellowjacket-Ultra, be sure to connect it now to ensure the best measurements. The thicker yellow needle (and larger, white text just below it) adjusts dynamically across the scale as RSSI is measured in dBm. On the bottom left is the lowest signal strength at -120 dBm with the highest signal strength at -30 dBm. These measurements are the result of a combination of variables including distance from the receiver, Wi-Fi transmission strength and other environmental factors that typically cause RF interference. The thin, green needle (and green text to the right) indicates the strongest signal detection so far. As you move around and turn, this green needle might travel further to the right, but it will not move to the left unless you leave this screen which resets this indicator or unless the device has not been seen in several seconds. Both needles will drop to -120 after the selected device hasn't been seen in some time.



The flashing red exclamation point in the left center indicates a possible evil twin detected or if the device is blacklisted. The scanning channel (channel currently being scanned), MAC, manufacturer, network, SSID, BSSID and MAC of AP are all associated with the current signal strength measurement. Below them is a full list of all channels that have also been associated with the device being measured. “Type” indicates whether the Wi-Fi device is a client or access point and when it was last seen. Below that, red text warning appears if the device has already been blacklisted or if the device is suspected an evil twin AP (green text if device has already been whitelisted) Finally, at the very bottom, an Active Ping checkbox indicates if the Wi-Fi device is responding to Active Ping frames (shown here as ‘responding’) sends out packets to interrogate a device to determine its status. This typically identifies hidden client devices that do

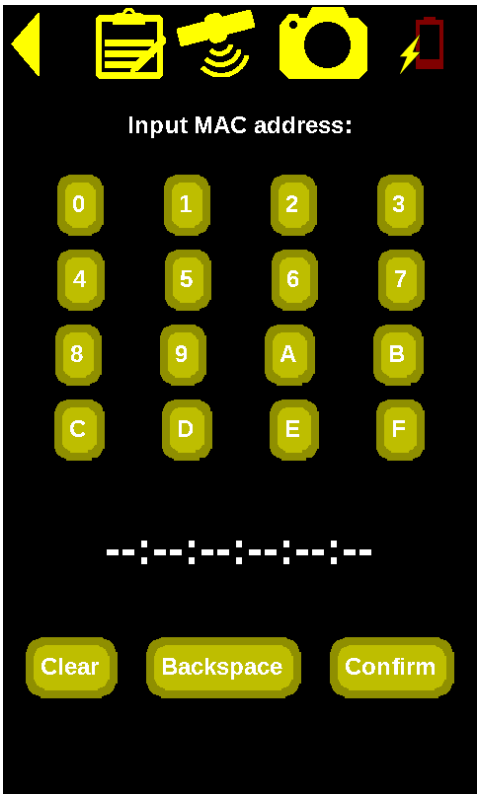


not normally transmit without being prompted first. Finally, users may also add the currently measured device into a whitelist or blacklist from this screen as well.

When “Active Ping” box is checked, it will change to "Responding" (in green) or "Not Responding" (in red) to indicate whether or not the device is replying to the Active Ping frames. Note, not all devices will respond to Active Ping.

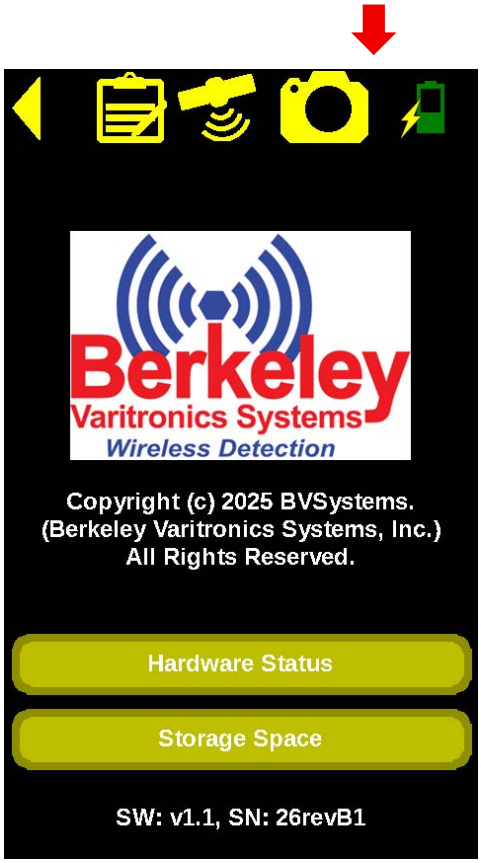
MAC Hunter Screen

MAC Hunter is accessed via the MAC Hunter button on the home screen. When the user has keyed in a valid MAC address and pressed the confirm button, the user is then brought to the Direction Finding screen. This functions similarly to tapping a device in the SCAN RESULTS list, but allows the user to select a known MAC manually, even if it hasn't been detected yet. Users enter MAC addresses manually using the “Clear”, “Backspace” and “Confirm” buttons at the bottom.

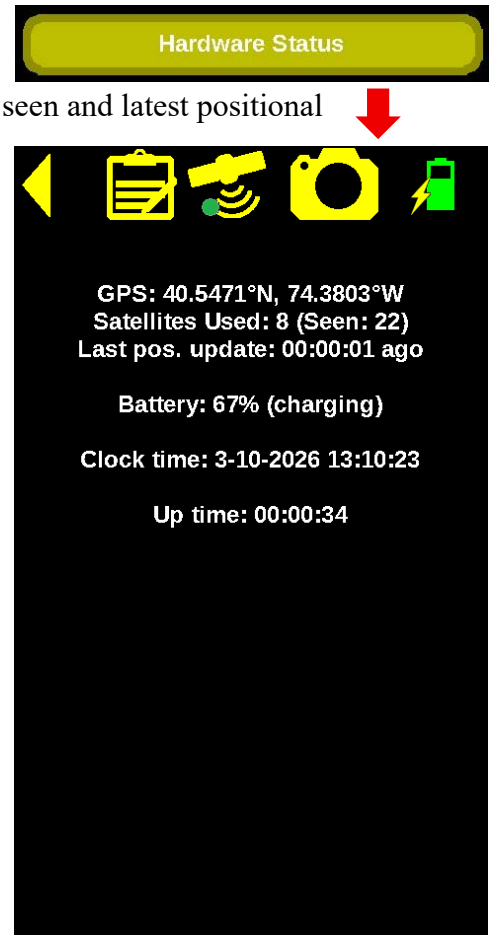


Unit Information

Select UNIT INFORMATION from the main menu screen and you will see this screen. Choose between Hardware Status and Storage Space to view more information about your unit.



Hardware Status

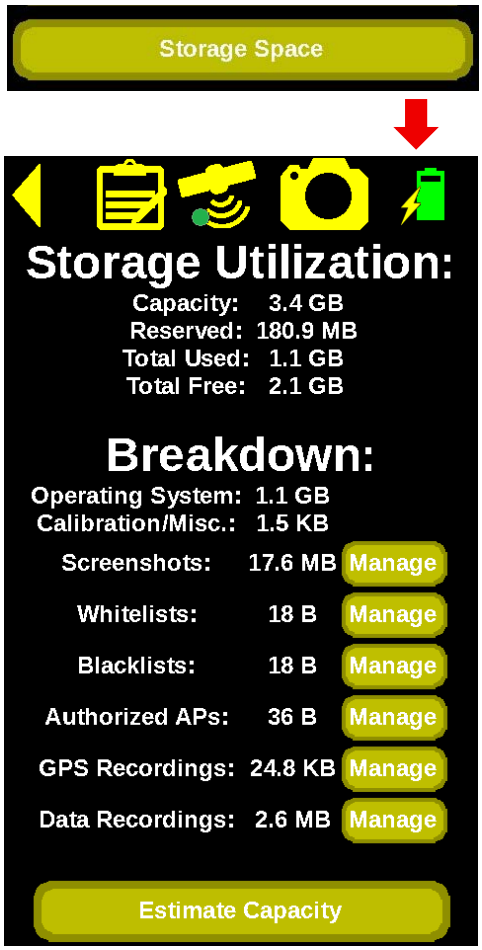


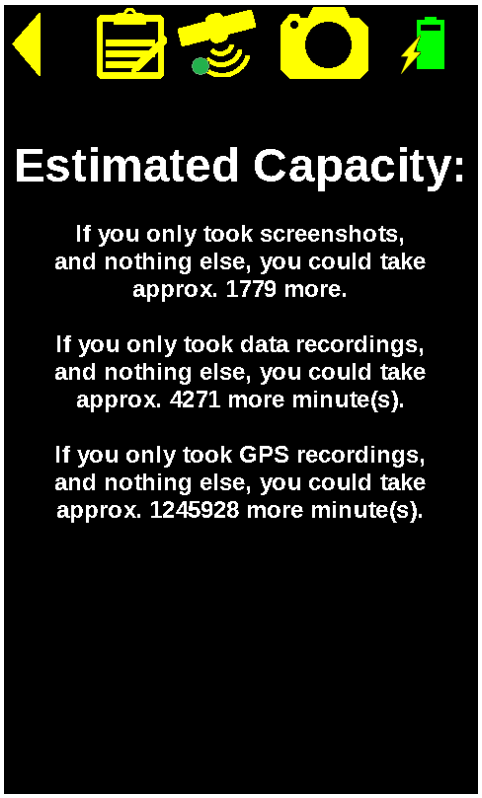
Select Hardware Status from the Unit Information screen to view hardware information including the GPS coordinates, satellites used and seen and latest positional update. Just below that, battery status is shown. Clock time and date (derived from GPS) appears below that and “Up time” shows the duration of the unit powered on below that.

Storage Space

Select Storage Space from the Unit Information screen to view a comprehensive breakdown of storage utilization including overall storage capacity, reserved storage, total storage currently used and free storage available. Below that, a more detailed breakdown displays operating system and calibration data and allows management of screenshots, user generated whitelists, user generated blacklists, authorized APs, GPS recordings and data recordings.

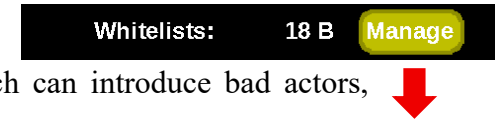
At the bottom, touching the “Estimate Capacity” button takes users to a new screen detailing storage estimates for screenshots, data recordings and GPS recordings.





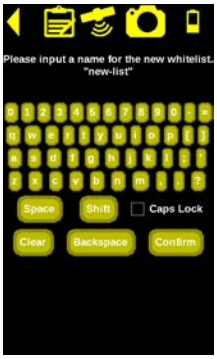
Whitelist Editing

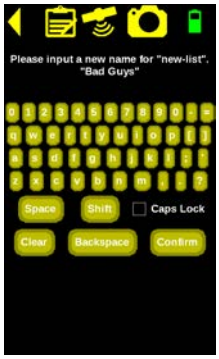
Whitelists (WL) are initially created by touching the “whitelist“ button at the bottom of the Wi-Fi Scan List screen. Whitelists are standard use in the security sector because they allow users to label known devices as “friendly” which can save a lot of time and effort when frequently scanning for new, unknown devices which can introduce bad actors, malware and general network insecurities.

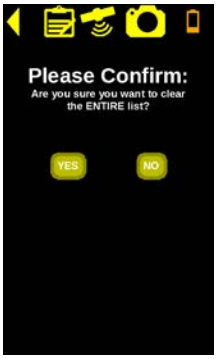


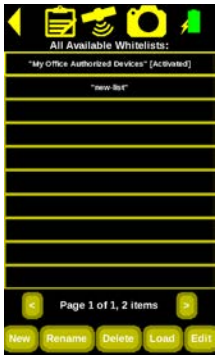
On this screen, the user can see the name of the active list, and add and remove MAC addresses from their currently loaded whitelist. "Switch" brings the user back to the "Manage Whitelists" screen to allow them to choose a different list. The left and right arrows allows the user to scroll through pages of MAC addresses. The "Add" button allows the user to key in a MAC address to add to the list manually. (MACs can also be added from the checkbox on the DF screen.) "Del" removes a MAC from the list, after requesting confirmation. "Clear" removes all MACs, leaving the list empty, after requesting confirmation. "Swap" moves a MAC to the active blacklist and removes it from the whitelist. Finally, "Gen" copies ALL MAC addresses from the scan results (as seen in the Scan Results screen) to the list.

The unit can support an arbitrary number of different, independent whitelists for the user to use in different scenarios or locations, for different security clients for example. Only one whitelist is active at any given point in time, and the user can select from among them using the "Load" button. The "Edit" button takes the user to the "Edit Whitelist" screen.







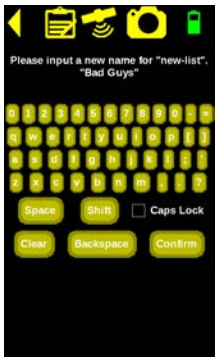


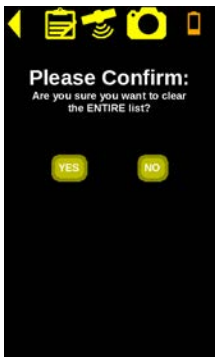
Blacklist Editing

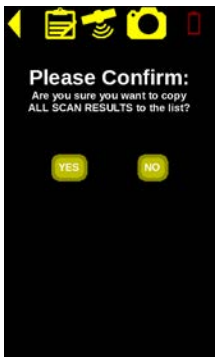
Blacklists (BL) are initially created by touching the “blacklist“ button at the bottom of the Wi-Fi Scan List screen. Blacklists are standard use in the security sector because they allow users to label devices as “unfriendly” which can save a lot of time and effort when frequently scanning among known “friendly” devices

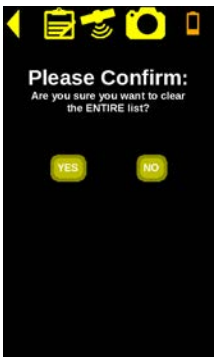
On this screen, the user can see the name of the active list, and add and remove MAC addresses from their currently loaded blacklist. "Switch" brings the user back to the "Manage Blacklists" screen to allow them to choose a different list. The left and right arrows allows the user to scroll through pages of MAC addresses. The "Add" button allows the user to key in a MAC address to add to the list manually. (MACs can also be added from the checkbox on the DF screen.) "Del" removes a MAC from the list, after requesting confirmation. "Clear" removes all MACs, leaving the list empty, after requesting confirmation. "Swap" moves a MAC to the active whitelist and removes it from the blacklist. Finally, "Gen" copies ALL MAC addresses from the scan results (as seen in the Scan Results screen) to the list.

The unit can support an arbitrary number of different, independent whitelists for the user to use in different scenarios or locations, for different security clients for example. Only one whitelist is active at any given point in time, and the user can select from among them using the "Load" button. The "Edit" button takes the user to the "Edit Whitelist" screen.

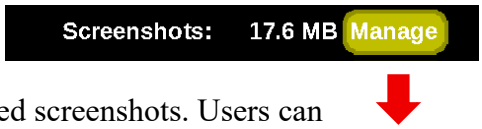




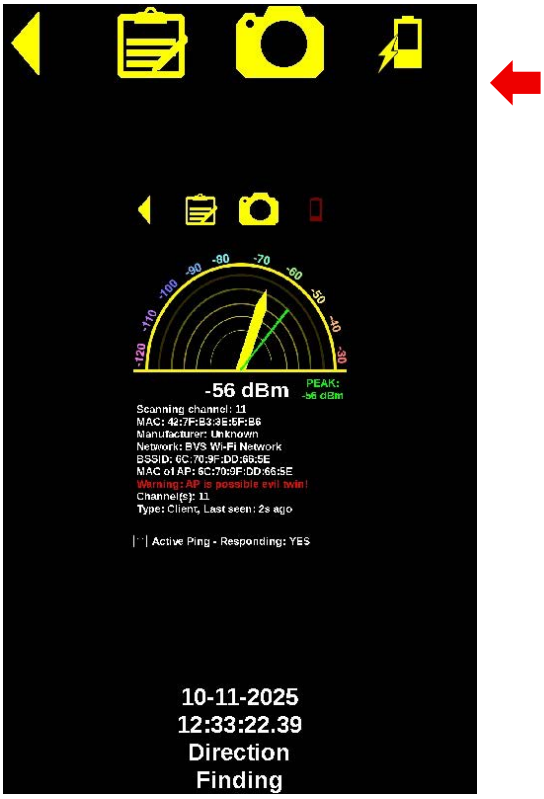




Screenshot Management



Touch the “Manage” button next to Screenshots to view and manage stored screenshots. Users can navigate among, “View”, “Delete” and “Clear All” individually timestamped screenshots.

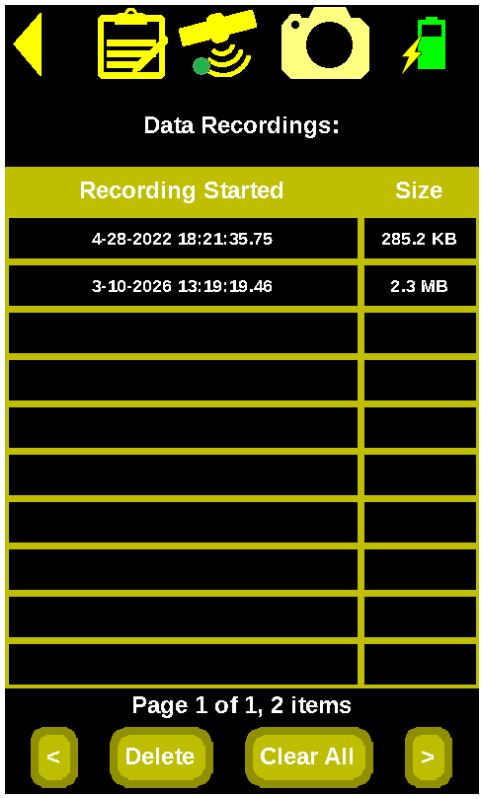


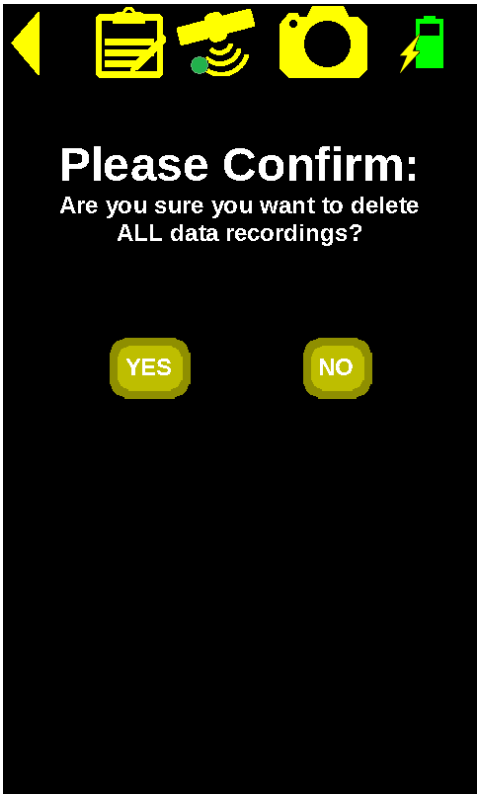
GPS Recordings Management

Touch the “Manage” button next to GPS Recordings to manage exisitng GPS recordings. GPS data can be exported into a .CSV file to view and edit in a spreadsheet.

Data Recordings Management

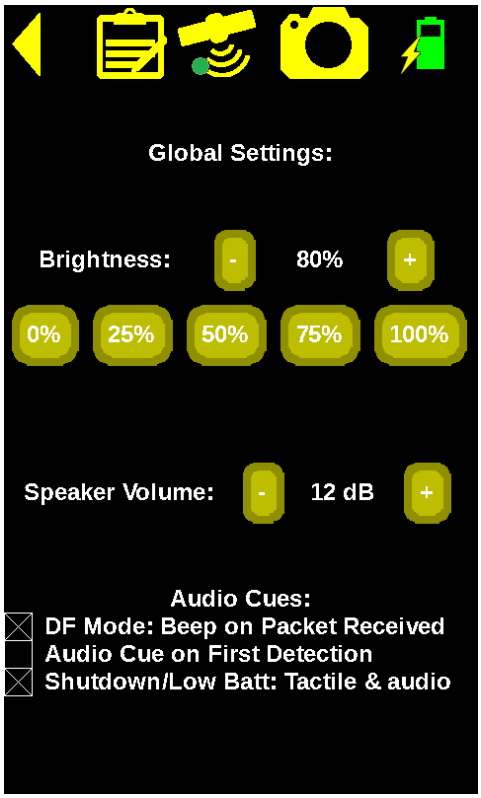
Touch the “Manage” button next to Data Recordings to view and manage each recording file.





Unit Settings

Select Unit Settings from the main menu screen and you will see this screen. This screen allows for brightness display settings and audio volume. It also includes checkbox options to select audio alerts for packets received while in the direction finding mode, audio alert upon first detection and a low battery warning audio alert.



"DF Mode: Beep on packet received": When enabled, when the user is on the DF screen, whenever a frame is received, the unit will play a beep, with the frequency proportional to the RSSI (higher pitch for higher signal strength) to aid in intuitive tracking of targets.

"Audio Cue on first detection": When enabled, when the user is on the scan results screen, if a blacklisted or possible evil twin device is detected for the first time since the unit has booted up (or the first time since scan results were auto-cleared), a voice clip of "blacklisted device detected" or "possible evil twin AP detected" will be played.

"Shutdown/Low Batt: Tactile & audio": when enabled, when the device is going to shut down (either because the battery is critically low, or because the user pressed the power button), tactile (unit vibration) warnings will occur at the start of the shutdown countdown, and audio (beep) warnings will be played each second until the unit powers off. If the user pressed the power button accidentally, there is a one-minute countdown where the user can cancel the shutdown (or select "shut down now"). If the battery is critically low, the user cannot cancel the shutdown and must plug the unit in to charge first.

Wi-Fi Overview

Signal Strength & RSSI Interpretation

RSSI (Received Signal Strength Indicator) is measured in dBm:

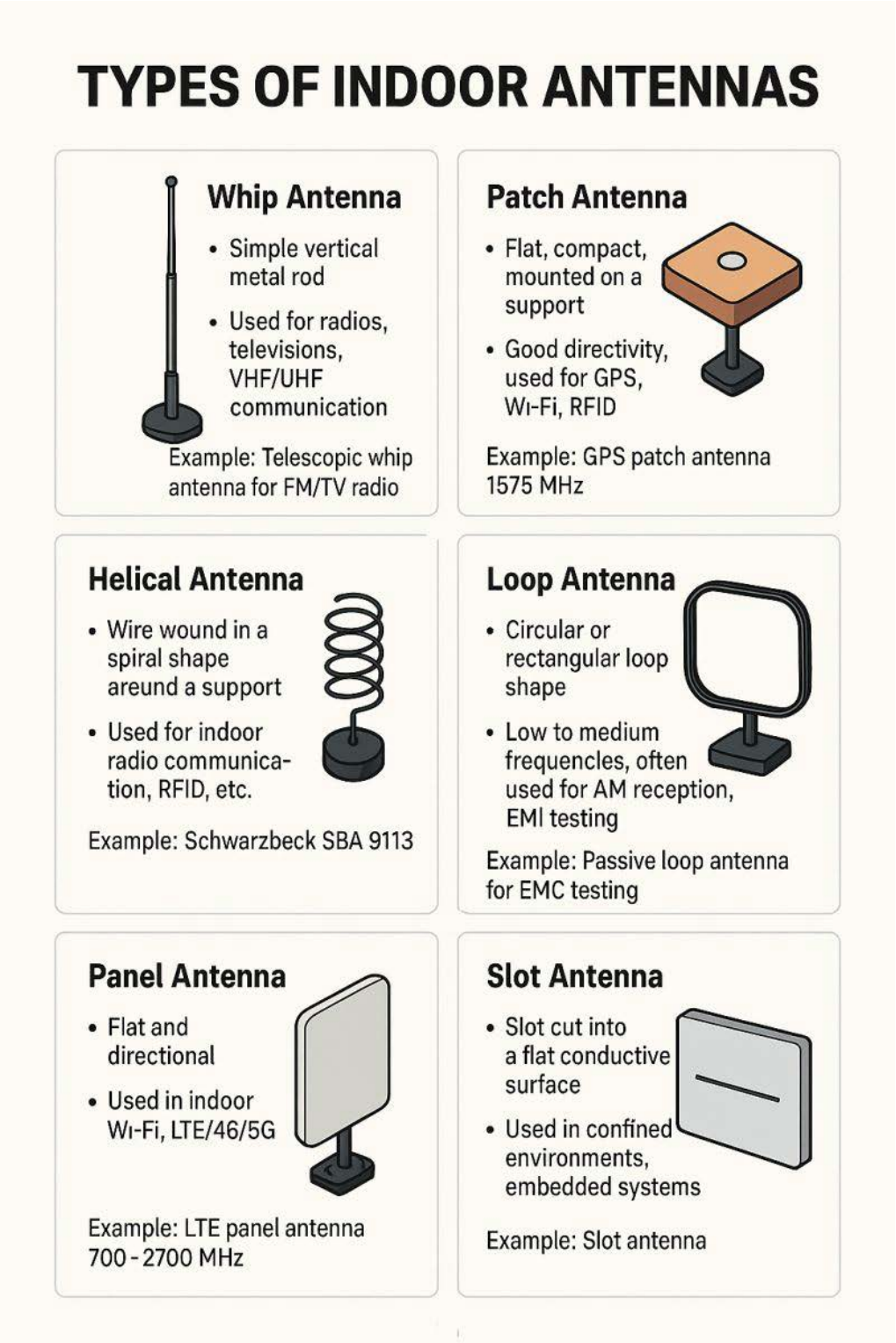
Signal Strength	Interpretation
-30 dBm	Extremely strong
-50 dBm	Excellent
-67 dBm	Reliable
-80 dBm	Weak
-90 dBm	Unstable
-120 dBm	Barely detectable

Direction finding accuracy improves as signal strength increases and environmental reflections decrease

Operational Use Cases: Security & Direction Finding Applications

The Yellowjacket-Ultra is designed for RF visibility, wireless threat detection, and physical location of suspicious Wi-Fi devices. The following use cases outline practical field deployment scenarios.

1. Locating a Rogue Access Point Inside a Facility



Scenario

An employee installs an unauthorized wireless router under a desk, bypassing corporate firewall protections.

Risk

- Creates backdoor into internal network
- Bypasses NAC and perimeter security controls
- Enables data exfiltration

Yellowjacket-Ultra Procedure

Step 1 – Scan List Review

- Open Wi-Fi Scan List
- Sort by SSID or Manufacturer
- Look for unknown or non-approved vendors
- Compare against Whitelist

Step 2 – Identify Suspicious AP

- Confirm it is not part of authorized infrastructure
- Observe channel assignment

Step 3 – Enter Direction Finding Mode

- Select device → DF screen
- Attach directional antenna
- Rotate slowly to identify peak RSSI
- Follow signal strength gradient

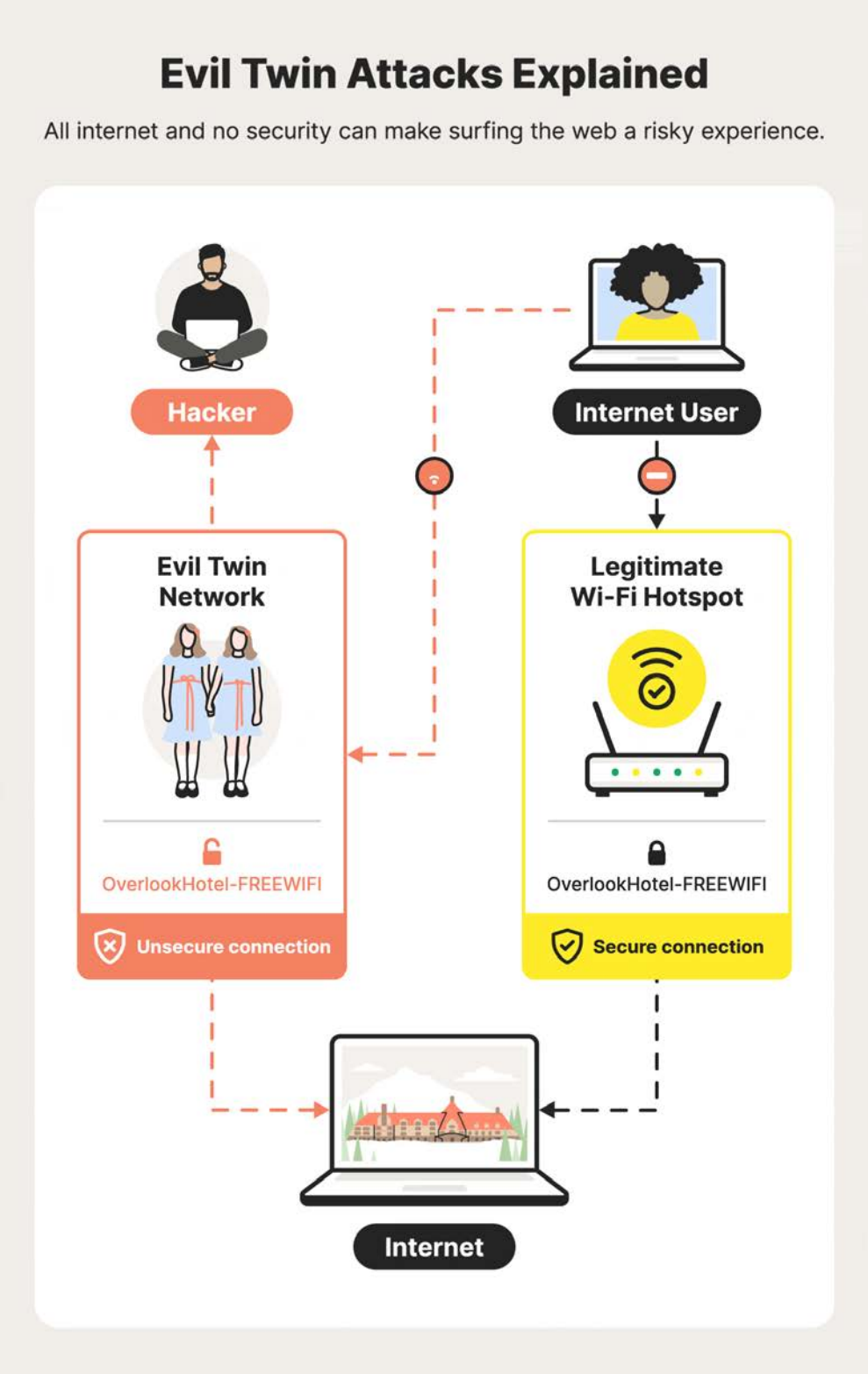
Step 4 – Physical Isolation

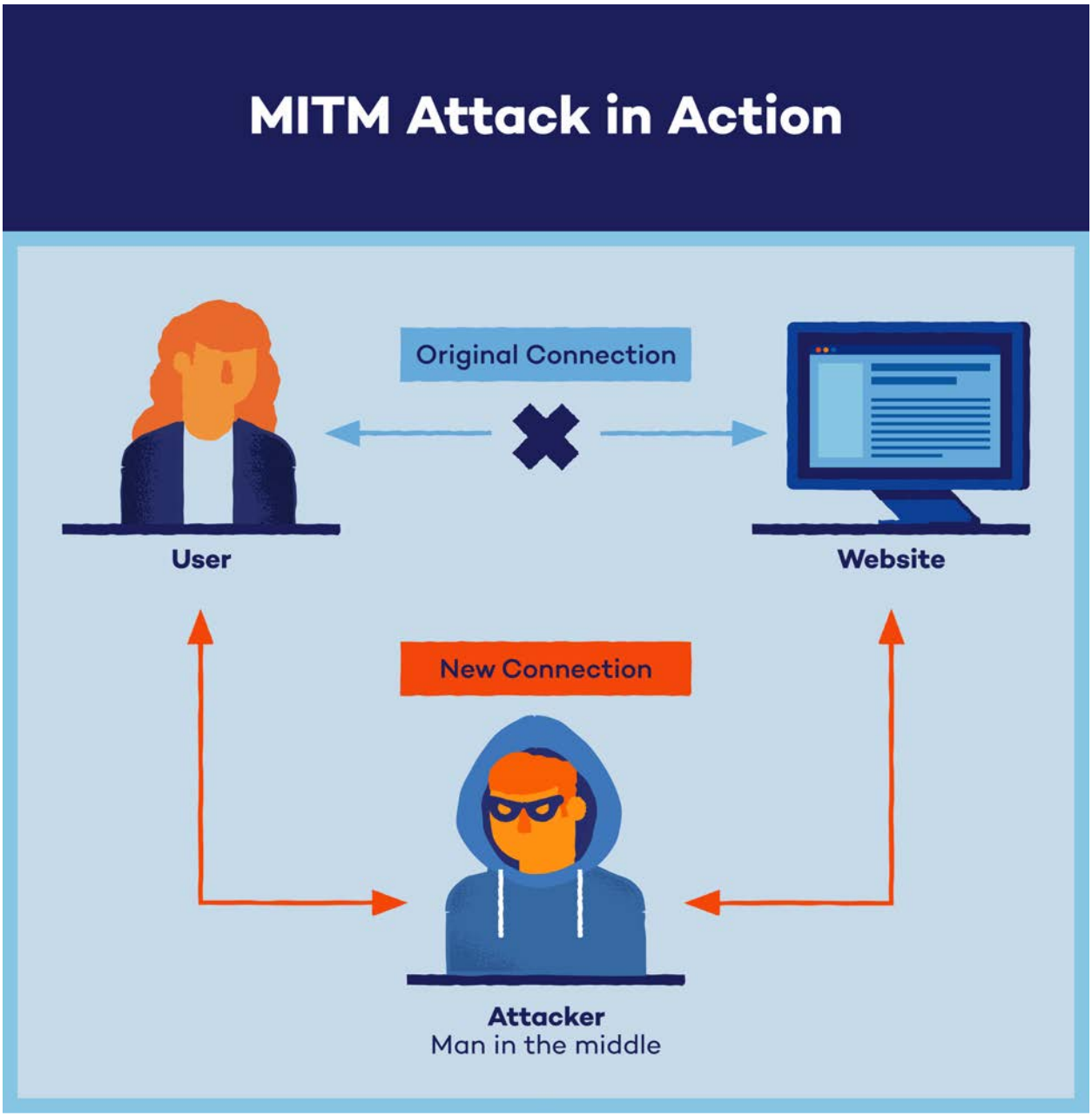
- Move toward increasing dBm (e.g., from -75 to -45 dBm)
- Narrow down to specific office, cubicle, or ceiling tile

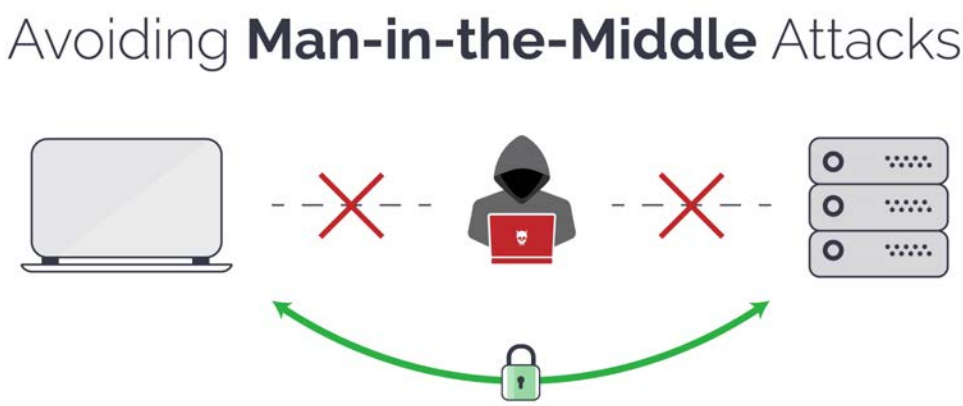
Result

Security can physically locate and remove unauthorized hardware.

2. Investigating an Evil Twin Attack




MITM Attack in Action
Original Connection
User
Website
New Connection
Attacker
Man in the middle



Scenario

Users report intermittent login prompts on the corporate SSID.

Threat Model

An attacker deploys a rogue AP broadcasting the same SSID as the legitimate network.

Detection Indicators in Yellowjacket-Ultra

- Duplicate SSID with different BSSID
- Stronger RSSI than expected
- Unexpected channel shift
- Red Evil Twin warning indicator

Direction Finding Workflow

1. Compare legitimate AP BSSID list
2. Identify unauthorized duplicate
3. Enter DF mode
4. Track strongest signal path
5. Monitor channel hopping behavior

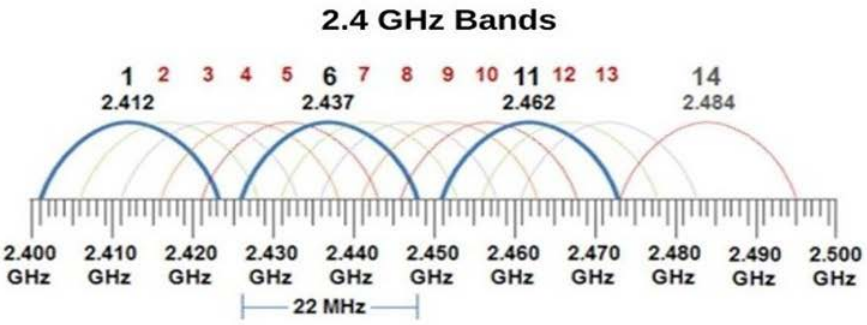
Field Example

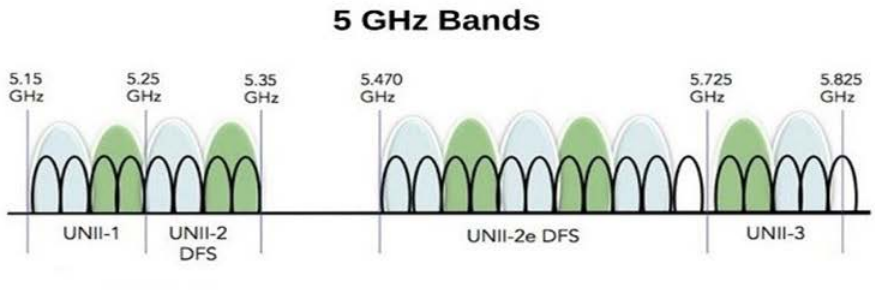
If the legitimate APs operate on Channel 36 and 44, but a duplicate appears on Channel 149 with unusually strong signal near a lobby, this may indicate a malicious portable hotspot device.

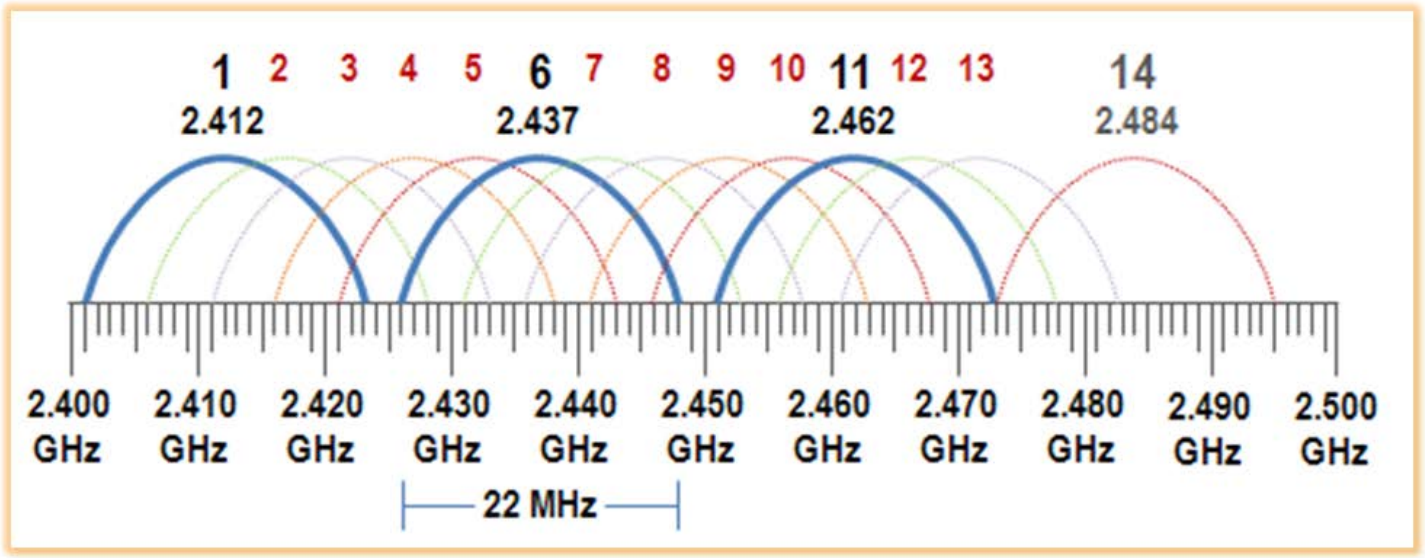
Outcome

Rapid location and neutralization prevents credential harvesting or MITM attacks.

3. Verifying Wi-Fi Interference & Congestion







Scenario

Users report slow throughput and dropped connections.

Possible Causes

- Channel overlap (2.4 GHz congestion)

- Adjacent-channel interference
- Too many APs on bonded 80 MHz channels
- Nearby RF emitters

Yellowjacket-Ultra Process

Channel Overview Screen

- Review activity across 2.4 GHz and 5 GHz
- Identify overpopulated channels
- Confirm non-overlapping usage (1,6,11 in 2.4 GHz)

Scan List Sorting

- Sort by channel
- Count AP density per channel

Signal Analysis

- Observe fluctuating RSSI
- Look for abnormal noise patterns

Outcome

- Recommend channel reassignment
- Reduce bonded channel width
- Rebalance AP power levels

---

4. Detecting MAC Spoofing Attempts

Scenario

An attacker clones the MAC address of an authorized AP.

Risk

- Impersonation
- Network trust bypass
- Confusion in monitoring systems

Yellowjacket-Ultra Indicators

- Observed on unexpected channels
- Vendor OUI mismatch

- RSSI inconsistent with known AP physical location

Direction Finding Method

- Compare known AP location vs detected signal source
- Use DF needle to determine if signal originates elsewhere

---

5. Identifying Deauthentication Attacks

Scenario

Multiple users are abruptly disconnected.

Threat

Attacker sends forged deauth frames to force reauthentication.

Detection Clues

- Frequent reconnect events
- Clients rapidly appearing/disappearing
- Signal stable but session unstable

Security Action

- Scan for suspicious nearby devices
- Investigate portable attack devices
- Use DF to locate source

---

6. Locating Hidden or Non-Broadcast SSIDs

Scenario

Sensitive area requires detection of covert APs.

Yellowjacket-Ultra Capability

- Detect BSSID even when SSID suppressed
- Identify associated clients
- Use Active Ping to prompt hidden devices

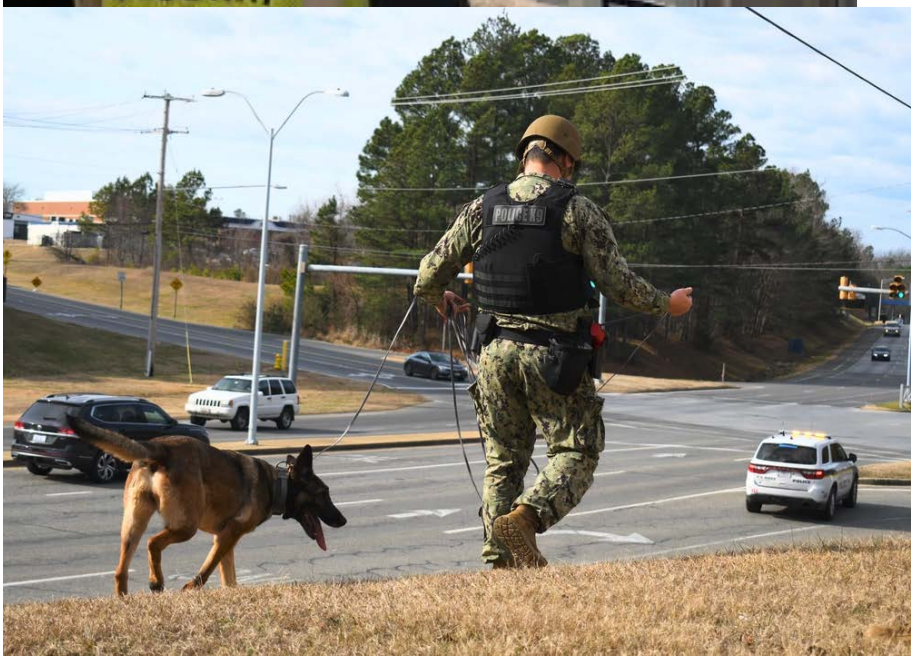
Operational Approach

- Scan area methodically
- Sort by last seen

- DF on unknown BSSIDs

---

7. Perimeter Security Sweep



Scenario

Security team performs proactive quarterly sweep.

Objectives

- Detect external rogue transmitters
- Identify parking lot Evil Twin attempts
- Confirm signal leakage beyond perimeter

Procedure

- Walk perimeter with DF antenna

- Monitor signal bleed from internal APs
- Identify unusually strong signals outside

Outcome

- Adjust AP power levels
- Improve containment
- Remove malicious devices

---

8. Law Enforcement / Forensic Application

Scenario

Investigation requires locating source of illicit wireless activity.

Application

- Track portable hotspots
- Locate hidden transmitters
- Identify device movement patterns

Method

- Log RSSI over time
- Use peak needle tracking
- Correlate signal strength with physical movement

Operational Best Practices

- Move slowly when direction finding
- Minimize body blocking and reflections
- Validate against authorized AP inventory
- Use whitelist/blacklist to reduce false positives
- Document findings with screenshot capture
- Log measurements during investigations

Summary

The Yellowjacket-Ultra supports:

• Physical location of rogue access points
• Evil Twin attack detection and tracking
• Wireless congestion diagnostics
• MAC spoofing identification
• Deauthentication event investigation
• Perimeter RF security sweeps
• Forensic wireless investigations

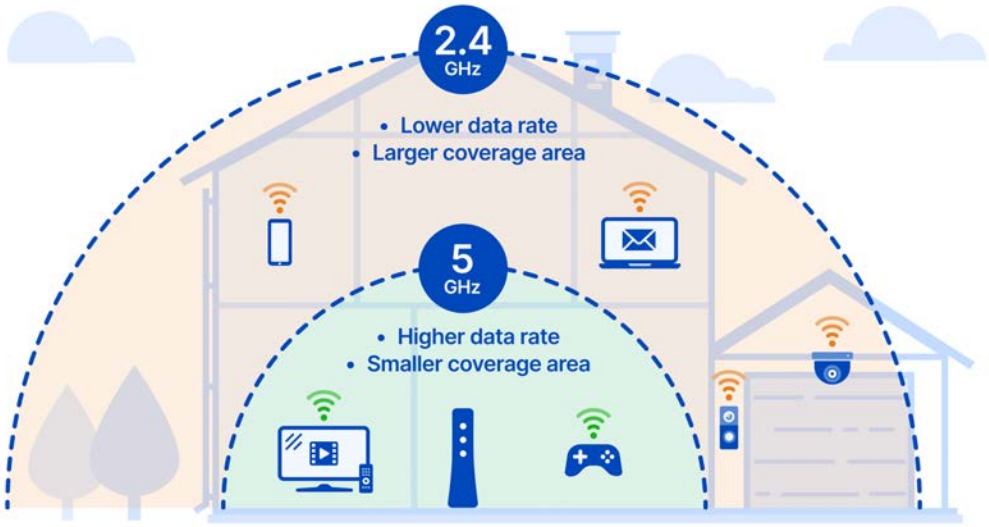
It bridges the gap between digital network monitoring and physical RF investigation.

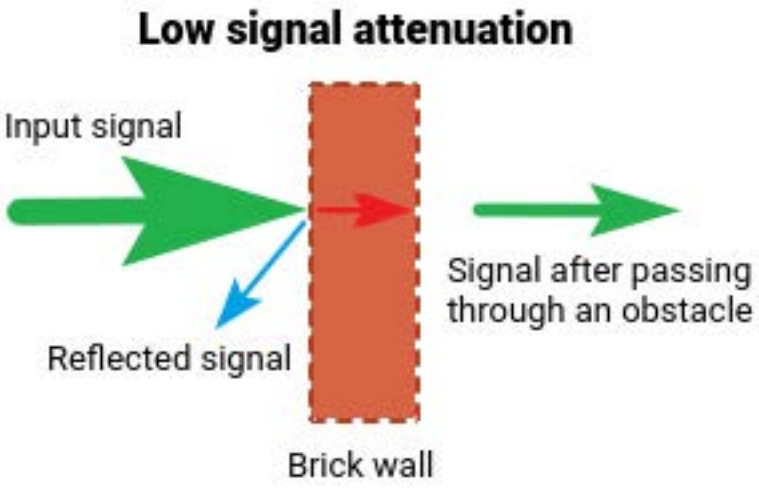
Wi-Fi Signal Range & Propagation Characteristics

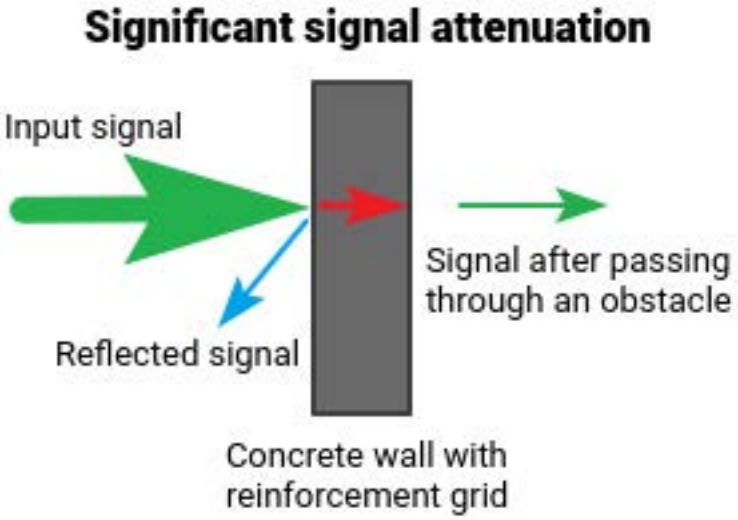
(2.4 GHz vs 5 GHz / 5.8 GHz)

Wi-Fi range depends on frequency, transmit power, antenna gain, environment, and physical obstructions. Higher frequencies attenuate (lose power) faster than lower frequencies.

2.4 GHz Wi-Fi Range







4

Typical Range

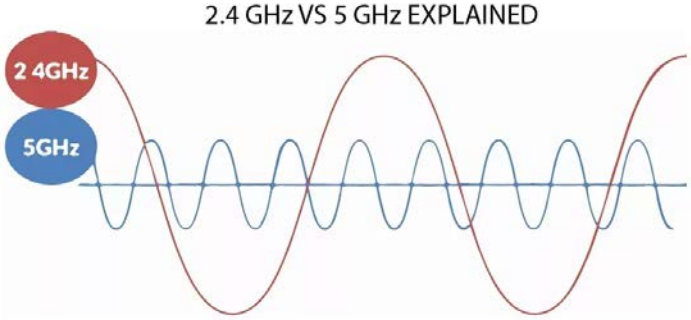
Environment	Approximate Range
Indoors (home/office)	100–150 ft (30–45 m)
Open indoor line-of-sight	150–200 ft (45–60 m)
Outdoors line-of-sight	300–1000+ ft (90–300+ m)

Characteristics

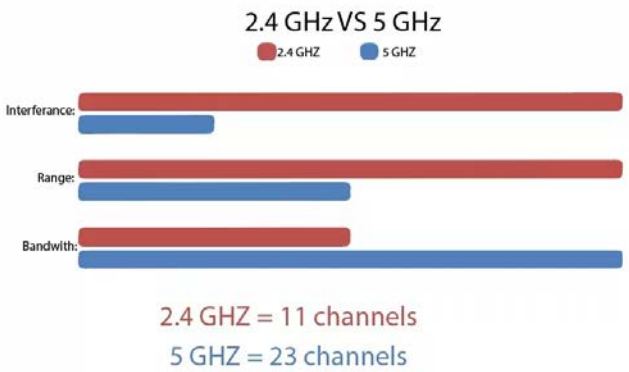
- Longer wavelength (~12.5 cm)
- Better wall penetration
- More prone to congestion and interference
- Travels farther than 5 GHz at same power level

---

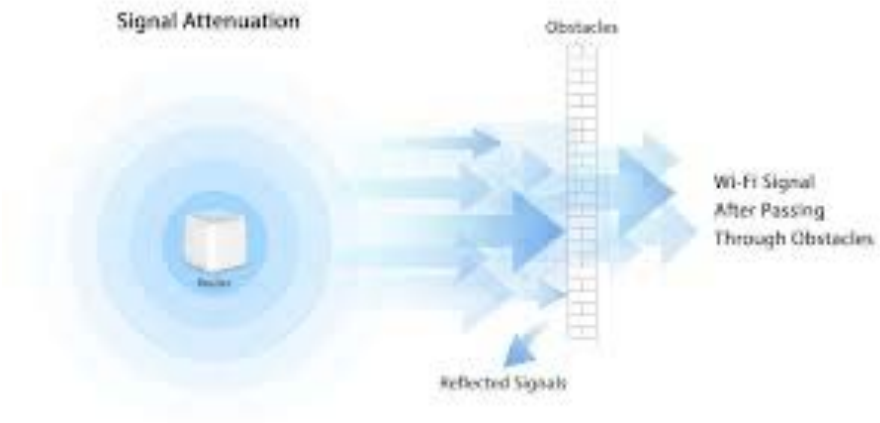
5 GHz / 5.8 GHz Wi-Fi Range



2.4GHz has a broader wavelength and has the advantage of covering a farther distance.
5GHz has a more compact wavelength which gives it the ability to provide faster data rates over a shorter distance.



5 GHz band has less overcrowding than the 2.4GHz band because fewer devices use it ,
while the 2.4GHz band has only 11 channels, however it will give you a greater Wi-Fi coverage range than 5GHz.
Your Router will auto select channels.



Typical Range

Environment	**Approximate Range**
Indoors (home/office)	50–100 ft (15–30 m)

Environment	Approximate Range
Open indoor line-of-sight	100–150 ft (30–45 m)
Outdoors line-of-sight	200–800 ft (60–240 m)

Characteristics

- Shorter wavelength (~6 cm)
- Higher data throughput
- More susceptible to obstruction loss
- Less congestion than 2.4 GHz

Why 2.4 GHz Travels Farther

Lower frequency = longer wavelength
Longer wavelength = better diffraction around objects
Lower free-space path loss

5 GHz signals attenuate more quickly due to:

- Increased free-space path loss
- Greater absorption by materials
- Reduced diffraction around obstacles

What Reduces Wi-Fi Range?

1. Building Materials (Major Impact)

Material	Signal Reduction (Approximate)
Drywall	3–5 dB
Glass	2–4 dB
Wood	4–6 dB
Brick	6–12 dB
Concrete	10–20 dB
Reinforced concrete	20–40+ dB
Steel / metal walls	30–100% reflection/blocking

Steel and reinforced concrete are the most significant attenuators.

Metal reflects RF energy instead of absorbing it, causing:

- Dead zones
- Multipath reflections
- Signal nulls

---

2. Water & Human Bodies

Water absorbs RF energy efficiently, especially at 5 GHz.

Examples:

- Aquariums
- Water pipes
- Large crowds (each human body is ~60% water)
- Indoor plants

This is why conference rooms packed with people often see reduced Wi-Fi performance.

---

3. RF Interference

Common 2.4 GHz Interference Sources

- Bluetooth
- Microwave ovens
- Cordless phones
- Baby monitors
- Wireless cameras

Common 5 GHz Interference

- Radar systems (DFS channels)
- Other enterprise APs
- Point-to-point wireless links

---

4. Antenna Type & Orientation

Omnidirectional antenna:

- Radiates 360°
- Shorter reach in one direction

Directional antenna:

- Focuses RF energy
- Increased range in specific direction
- Ideal for direction finding (as used with Yellowjacket-Ultra)

---

5. Transmit Power & Regulatory Limits

Wi-Fi transmit power in the U.S. typically ranges:

- 2.4 GHz: up to 1 Watt (30 dBm) EIRP
- 5 GHz: varies by band (often 200 mW – 1 W depending on sub-band)

Enterprise APs adjust power automatically to optimize coverage and reduce interference.

Real-World Example: Office Environment
Example building:

- Steel studs
- Concrete core
- Glass offices
- Cubicle partitions

Typical behavior:

- 2.4 GHz may cover multiple offices
- 5 GHz may require additional AP density
- Elevators (metal shaft) create RF shadow zones
- Parking garage below may still receive detectable 2.4 GHz leakage

---

Outdoor Propagation
Line-of-sight is critical.

If unobstructed:

- 2.4 GHz can travel 1000+ feet
- 5 GHz can travel several hundred feet

With high-gain directional antennas:

- Distances can extend several miles (point-to-point links)

However, foliage significantly reduces range — especially when wet.

How This Relates to Yellowjacket-Ultra
Understanding propagation helps during:

Rogue AP Hunts
If signal is -40 dBm in hallway but -70 dBm in adjacent office, the AP is likely closer to hallway.

Evil Twin Detection

If a “corporate SSID” is unusually strong near lobby entrance but weak near internal AP cluster, suspect external transmitter.

Perimeter Security

If 2.4 GHz corporate SSID is detectable 500 ft into parking lot, AP power may be too high.

Practical Direction Finding Insight

When hunting a device:

- Signal increases ~6 dB every time distance halves (approximate rule of thumb in free space).
- Moving from -80 dBm to -50 dBm represents a very significant reduction in distance.
- Reflections can create false peaks — rotate antenna slowly and verify consistency.

Quick Comparison Summary

Characteristic	**2.4 GHz**	**5 GHz / 5.8 GHz**
Range	Longer	Shorter
Wall Penetration	Better	Reduced
Congestion	High	Lower
Throughput	Moderate	Higher
Interference Sensitivity	Higher	Lower (except DFS radar)

Thank you for your purchase, we look forward to supporting you and your team.

Customer Support

Berkeley Varitronics Systems, Inc.
Liberty Corporate Park
255 Liberty Street
Metuchen, NJ 08840

8:00 AM to 6:00 PM EST
Toll Free: 888-737-4287
Phone: 732-548-3737
Fax: 732-548-3404

24/7 (expect a reply within one day)
email: support@bvsystems.com
www.bvsystems.com