Concept Guide

Secure Wireless

4D

DEFINE / DESIGN / DEPLOY / DEMO

Table of Contents

Change Log

Date	Change Description
2022-01-19	Initial release.
2022-06-08	Updated Signal on page 11, Channels and channel planning on page 14, and Wi-Fi 6 specific improvements with FortiAPs on page 25.

Introduction

This document provides a general overview of Wireless concepts and introduces Fortinet Secure Wireless products.

Fortinet Secure Wireless LANs

"How do I get on the Wi-Fi?" It is a cliché because it is true: the most common network access technology is Wi-Fi. Other wireless technologies, such as LTE for long range and BLE for short range are also vital to modern networks, but they complement Wi-Fi rather than compete with it.

The evolution Wi-Fi has undergone over the last 20+ years, and continues to undergo, has not just been about the network standards, but also the way we use it. Physically, all Wi-Fi connections are the same, and follow the same primarily network Layer 1 and Layer 2 standards, but securing the ever-growing variety of devices that connect over the Wi-Fi keeps getting more complex.

Authorized end users with organization issued devices are not the same as authorized users with personal devices (BYOD, Bring Your Own Device), which are not the same as short term guest users, or public access users, let alone the enormous number of evolving IoT devices that don't have a user associated with them at all—and were usually designed by companies with no real cybersecurity expertise. Fortinet brings unique strengths to address network

and security administrator's needs to secure WLANs, providing cyber security that is both strong and simple to administer without burdening customers with complex licensing.

Intended audience

This guide is intended for an audience who is interested in learning about Fortinet's Secure Wireless LAN concepts. Readers should have a basic understanding of networking, wireless and security concepts before they begin. Interested audience may include:

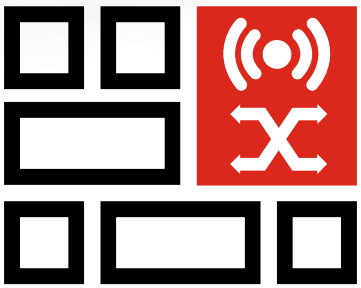
- *Network, Wireless and Security architects*
- *Network, Wireless and Security engineers*

About this guide

This guide aims to provide a broad overview of Wireless concepts, and introduce products in the Fortinet portfolio that work together to implement a scalable Secure Wireless solution. Industry standard terminologies are used, with introductions to Fortinet specific terms, concepts and technologies. Readers can move on to the Wireless Architecture Guide and other Wireless Deployment Guides when they are familiar with the concept and terminology and is ready to explore different designs to use in their environment.

Fortinet is a networking company

Fortinet is one of the most premier and well-recognized providers of cybersecurity solutions in the world. Traditionally, security has been thought of as something to add 'on top' of IP networks—deploy (or at least design) the network, and then secure it at the edge (or edges). However, that paradigm started to break down with the first laptop, with the increase of BYOD, public networks, guest networks, cloud applications, public clouds, IoT, and the evolution and expansion of remote work. Network edges are everywhere, and network security needs to be enforced everywhere.



FortiGate NGFW appliances (and VMs) are known primarily as Security Appliances, but they are also Network Appliances. They combine routing, SD-WAN, DHCP and DNS services and more with a Wi-Fi and Switch controller as well as the extensive cybersecurity functions. The convergence of all this functionality enables *Security Driven Networking*—described in more detail below.

FortiAPs are high performance purpose-built Wi-Fi 6 access points. They are 3 radio models, which means they can service both Wi-Fi bands while the 3rd radio serves as a monitor, tracking RF conditions and scanning for neighbor and rogue APs. When managed by a FortiGate, they become extensions of the FortiGate Network Security Platform. All network access, regardless of where is comes from can have a full security stack applied. We call this the *LAN Edge*—the border between the LAN and the client devices the LAN serves.

FortiAP U-series are premium APs with 2 additional features. For Bridge Mode SSIDs, where traffic is bridged directly to the network instead of tunneled to the FortiGate, UTP (Unified Threat Protection) enforcement can take place on the AP, such as Web Filtering, Anti-Virus scanning, and others. This is most commonly used with APs deployed remotely for teleworkers. The second important feature is that one of the client-serving radios is band selectable, meaning the AP can have one 2.4 GHz radio and one 5 GHz radio, or both can be tuned to channels in 5 GHz. The advantages of this will be discussed below.

FortiSwitches are feature rich yet cost-effective Ethernet switches. FortiSwitches behave similarly to FortiAPs, in that they form a fabric with a FortiGate and extend NGFW functionality throughout the LAN and to the LAN Edge.

FortiWiFi units are FortiGates for small offices that incorporate an AP directly into the FortiGate hardware. These are similar to many home all-in-one systems, although much more secure and with a higher level of network functionality.

Security driven networking—the LAN Edge and FortiLink

The LAN Edge

Traditionally, networks were perceived to have an 'inside', the LAN, and an 'outside', the WAN or Internet boundary. This provided a clearly defined perimeter where security policies of all kinds were applied. However, in our more recent and more complex networking world, it has become clear that there are multiple perimeters or network "edges". End devices are separate from the LAN that grants them access and network services, and it is necessary to differentiate and apply security policies to ALL devices that access our networks. This is the LAN Edge, the border between wired and wireless clients and the LAN, where clients receive authorization and access to network resources.

FortiGate, FortiSwitches and FortiAPs are the core components of the Fortinet Secure LAN Edge. FortiGate is the base of a unified Security Fabric that extends via FortiLink over FortiAPs to the wireless LAN, or over FortiSwitches to the wired LAN or both. (For example, a FortiGate and FortiAPs without FortiSwitches, or the other way around, are reasonable architectures.)

FortiLink is the mechanism that extends NGFW functionality to the LAN Edge. FortiLink is a control and tunneling protocol for FortiAPs and FortiSwitches. Through FortiLink, FortiAPs remain in communication with the FortiGate at all times to get any configuration changes. By default, they also tunnel all traffic to the FortiGate, which then applies any configured Firewall and other security policies, routes the traffic and otherwise treats it as if the AP was directly connected to the FortiGate.

Wireless Controller (WiFi & Switch Controller in the GUI) is a feature of FortiOS (the FortiGate Operating System) that manages wireless networking and APs. WLANs (SSIDs) can be configured and deployed to all access point, access point radios configured, clients monitored, etc.

FortiLink NAC is a feature included with FortiOS that identifies devices connected to a FortiLink managed device and assigns them to a specified VLAN. Criteria can include MAC address, operating system, device type, etc. This is particularly useful for devices for IoT devices that only support WPA2/WPA3 personal security for WLAN access.

Security-driven Networking is Fortinet's strategy of tightly integrating network infrastructure and security architecture. The above features are simply included in all FortiGates, with no special licensing. The unification of FortiGate, FortiSwitch and FortiAP via FortiLink drives the highest level of security. The FortiGate WiFi & Switch Controller enables a true single pane of glass for the entire network. The tight integration of both security networking simplifies both areas of operation where other vendors require complex combinations of overlay products.

Scalability, flexible management, and analytics

FortiGate models range from being appropriate for small offices to large campuses of thousands of APs. There are management options for multiple locations, whether the need is a few retail locations, a small school district, up to a major Managed Service Provider (MSP) with thousands of customers.

FortiGate Cloud is a service portal that provides remote cloud management of multiple FortiGates and the LAN Edge components connected to them. It has a multi-tenant option that can be used either by service providers to separate customers, or even by a single organization to divide administration. It includes configuration, backup and upgrade, as well as reporting, log retention and traffic analysis.

FortiLAN Cloud – Needs are not the same for every network. There may be any number of reasons to deploy FortiAPs or FortiSwitches, or both, in standalone mode rather than FortiGate controlled. FortiLAN Cloud not only provides simple cloud management of FortiAPs and FortiSwitches, but also monitoring, reporting, and analytics.

FortiManager is the ultimate NOC-SOC operations tool, built from the ground up with from a security perspective and supporting a massive scale of devices—10,000 or more. Granular Administrative Domains and Management extensions support the most demanding Service Provider environments, but the analytics and management extensions often make it a good choice for small organizations, depending on their needs. FortiManager is available as an appliance, as a VM and as FortiManager Cloud.

FortiAnalyzer provides massive log retention, security fabric analytics, and automation to provide better detection and response against cyber risks and network anomalies. FortiAnalyzer can gather and analyze logs from Fortinet and over 25,000 third-party devices. It is a necessary component when deploying FortiAIOps. It is available as an appliance, virtual machine or, if the log volume is not excessive, FortiAnalyzer Functionality can be enabled on FortiManager.

FortiWLM provides enhanced and aggregated monitoring of FortiGate administered wireless networks. It includes an extensive set of troubleshooting and reporting tools. FortiWLM is available as an appliance or a Virtual Machine, or as a FortiManager Management Extension.

ABOUT THIS GUIDE

FortiAIOps is an Artificial Intelligence with Machine Learning (AI/ML) solution for network troubleshooting. In conjunction with FortiAnalyzer's quick collection of data, FortiAIOps provides identification of network anomalies and event correlation, identifying wireless and wired connection problems, all while performing network operations center (NOC) optimizations.

FortiPresence is a Wi-Fi Presence and Analytics and Customer Engagement Solution for public venues. FortiPresence leverages existing onsite Fortinet access points to detect visitors' smartphone Wi-Fi signals. Analytics provides insight into the behaviors of visitors within a site both in real time and across time periods. Data from FortiPresence can be used to increase business efficiencies, improve visitor experiences, and positively impact the business' bottom line.

FortiPlanner is a graphical Wireless LAN planning and post-deployment site survey tool. Using FortiPlanner ensures planning accuracy through sophisticated signal propagation ray-tracing algorithms. After deployment, a real-time coverage heat map shows the areas that need fine-tuning, such as coverage holes or especially congested areas.

Important Wi-Fi concepts

This section contains the following topics:

Wi-Fi Organizations and terms

The Wi-Fi Alliance

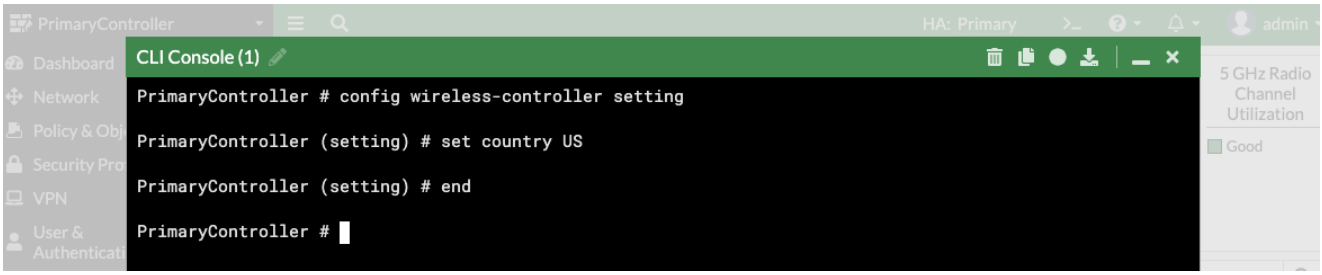
Wi-Fi does not mean "Wireless Fidelity", although it was coined to take advantage of its similarity to "Hi-Fi." It is a pure marketing term, and the trademark is owned by the Wi-Fi Alliance (https://www.wi-fi.org). The Wi-Fi Alliance is a non-profit industry organization whose primary purpose is to ensure interoperability of Wi-Fi products. There are a number of certifications, but the essence is that a Wi-Fi certified device will work with any other certified device regardless of vendor. Fortinet is a member of the Wi-Fi Alliance and our products are certified.

Recently, the Wi-Fi Alliance simplified the generational names of Wi-Fi standards. Previously, Wi-Fi generations had been labeled only with the IEEE (Institute of Electrical and Electronics Engineers) technical standards, or the letter

portion of the amendment—i.e., 802.11n, 802.11ac, 802.11ax. the alliance has renamed these to "Wi-Fi 4, Wi-Fi 5, and Wi-Fi 6," respectively. Wi-Fi 6E will soon add more channels to Wi-Fi 6, and Wi-Fi 7 (802.11be) is in development. Generally, every generation of Wi-Fi is required to be backwards compatible with previous generations.

Regulatory agencies like the FCC in the US set the rules for what channels and the allowed transmit power for Wi-Fi. There is no technological reason for the channels used; they are chosen for regulatory reasons. Radio and TV stations and mobile phones license the spectrum (channels) they use from governments, but Wi-Fi occupies **unlicensed spectrum**. Unlicensed spectrum can be used by anyone and any technology so long as the transmit power is below the legal threshold and other regulations are obeyed.

Country code is a FortiGate setting that aligns the AP radio settings with a country's regulations. By default, FortiGates are set to US. The Country Code can be changed in the CLI.



Signal

Any wireless communication system depends on a modulated signal. A transmitted signal is spread over a large volume of space, and is always much stronger than the signal actually received at the client radio. The receiver can only get 1 millionth of the original signal and consider it excellent. With Wi-Fi, the clearer the signal, the faster the data transmission rate because smaller changes in signal strength and phase (modulations) can be used to encode more data.

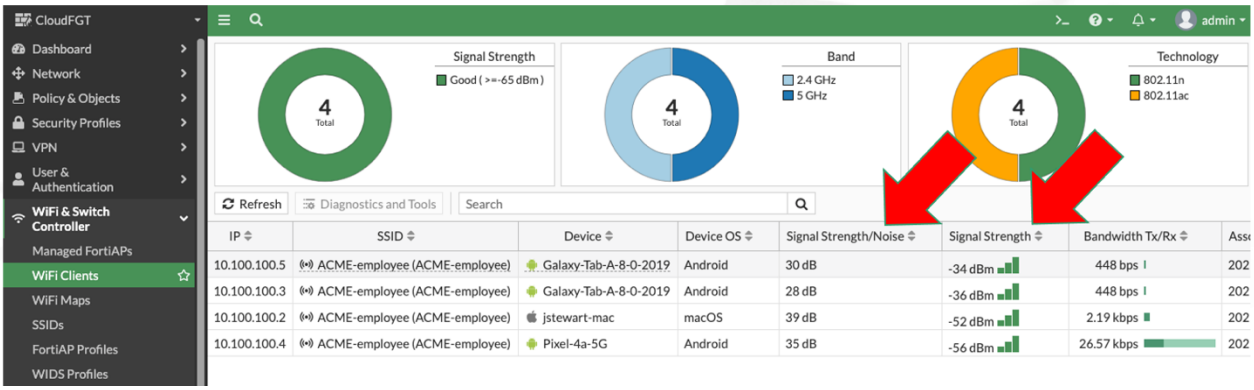
MCS rate (Modulation and Coding Scheme) is the list of available data rates for Wi-Fi transmissions. There are fixed modulation types—that is, 6.5 Mbps and 13 Mbps are possible at the low end, but not 12 Mbps. Signal strength must be high enough relative to background RF-noise to achieve high throughput rates.

You can refer to Modulation and Coding Scheme (MCS) index tables such as https://mcsindex.com. Wi-Fi performance is dependent on signal strength, noise, number of streams, and channel width.

SNR (signal-to-noise ratio) is the difference between received signal and the background RF. Even a very clean environment has some undifferentiated signal. RF noise is analogous to the noise in an environment when two people are talking. Compare conversing in a library vs a restaurant during the lunch rush. In the first case, whispers are easily understood, in the latter, people have to speak up. The equivalent RF background could mean the it takes a higher signal to maintain the same MCS rate.

SIGNAL

RSSI (Received Signal Strength Indicator) is just what the name implies, and used by Wi-Fi radios, along with the SNR, to determine what MCS they can negotiate. However, it is a relative number (1-252) and every Wi-Fi vendor has their own implementation of it.

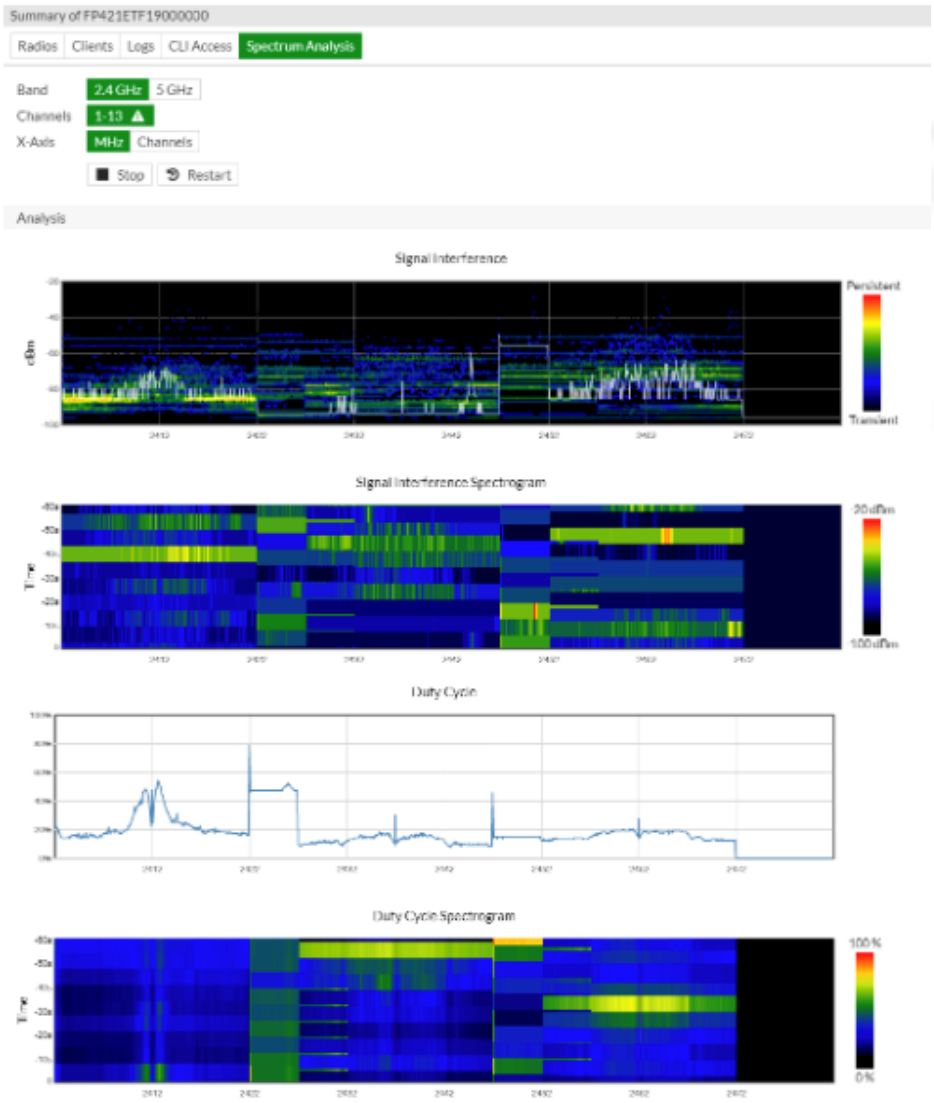


dBm (decibel milliwatts) is used for the absolute value of a Wi-Fi signal. Decibels are a logarithmic scale (actually 10 times the log base 10), so 10 dBm is 10 milliwatt, but 20 dBm is 100 milliwatts. Another way of thinking about that is 10 is one zero, 20 is two zeros, 30 is three zeros, etc. Because signal strength changes so drastically, decibels are considered easier to work with than absolute milliwatts. Furthermore, our concern is usually with dropping signal so it is more important to focus on negative values: -10dBm is 0.1mW, -30dBm is 0.001mW, etc. Usually for Wi-Fi, because we are using negative dB values, the bigger the absolute value of a dB measurement, the weaker the signal.

You do not have to be skilled at dB math for the overwhelming majority of Wi-Fi concerns, you just have to know a couple general rules:

- + 26dBm is 400 mW and the top signal emitted by most FortiAPs in the US
- + 23dBm or 200 mW is a more typical FortiAP emitted signal (FortiAPs adjust for environment)
- **-67dBm** or higher is the usual received signal strength design goal—this should allow quality voice over Wi-Fi calls
- -50 dBm, is much stronger than -67 dBm, and -30dBm is an outstanding received signal
- A dB difference of 3 is double or half. -70 dB is half of -67 dB and -64dB is twice -67 dB
- Background noise is typically around -87 dBm, but very location dependent

A Spectrum Analyzer is necessary to measure how much noise is on a channel. FortiAP radios can be put in Spectrum Analyzer mode and the results viewed in the FortiGate UI. Another advantage of the Wi-Fi 6 APs over some earlier models is the 3rd monitor radio is always available for troubleshooting without having to use the client service radios.



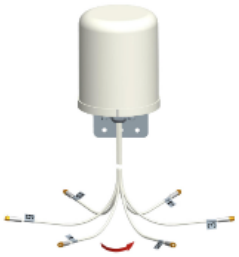
Signal Loss is the drop in signal strength for various reasons. Signal drops with the square of the distance ($1/r^2$), but in most indoor environments the most important consideration is wall penetration. Wall material matters with Wi-Fi. Drywall blocks less signal than brick, at a typically -8dB. Cinder block is pretty transparent, but solid concrete and rebar are very opaque. One common problem is unexpected metal such as leaded glass, or plaster over chicken wire. These will obstruct Wi-Fi penetration. Another factor is that 5 GHz signals generally penetrate less than 2.4 GHz.

Antennas shape and direct signal. The integrated antennas in FortiAPs are omni-directional (360 degree) and ideally suited for ceiling mount in the middle of most spaces. FortiAPs with external antenna connectors can accept a number of directional options. You can compare omni antennas to direction antennas as similar to standard light bulbs compared to spotlights. An indoor space is usually best served by an omni in the middle. If for some reason APs can only be hung on the sides of a space—which is very common when covering an outdoor area—the directional option will work better. Antennas do not increase total signal, but direct it. A directional antenna with a 60 beamwidth will have roughly twice an omni's signal within the 'spotlight' area, but much weaker signal behind it.

Fortinet offers many different antenna options that can be used with our FortiAP line of products. These antennas can help to optimize coverage and overall wireless performance in a range of installation settings. Antennas come in a variety of patterns and with various numbers of antenna elements to help installers find the best match for their equipment.


FANT-04ABGN-2504-O-R


FANT-04ABGN-0606-O-R
FANT-04ABGN-0606-O-N


FANT-06ABGN-0606-O-R


FANT-06ABGN-2504-O-R


FANT-06ACAX-8509-D-N


FANT-04ABGN-8065-P-N


FANT-04ABGN-1414-P-N


FANT-04ABGN-0606-P-R

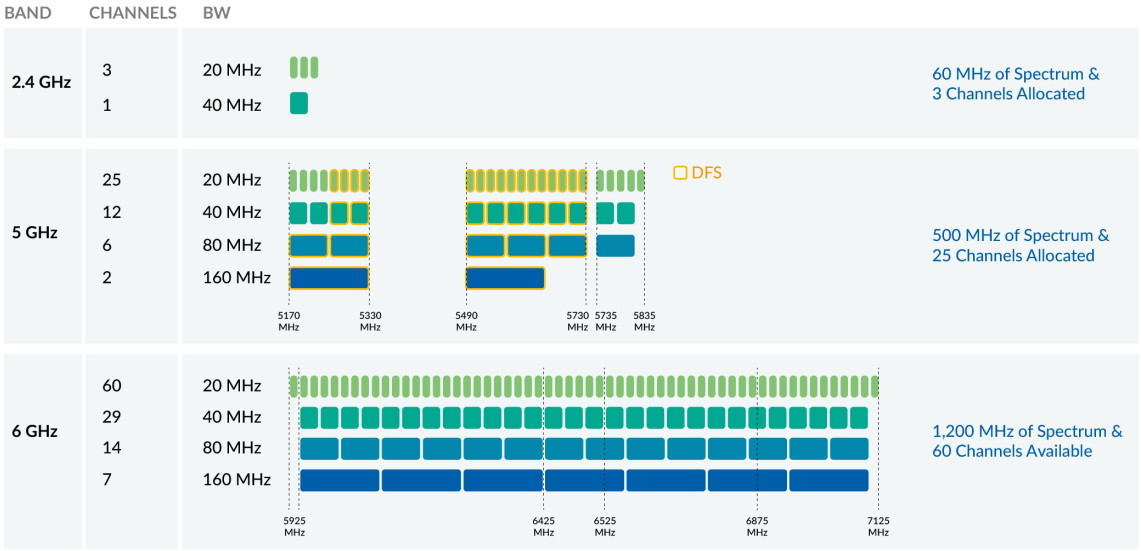

FANT-08ABGN-1213-D-R

FANT-10ACAX-1213-D-N

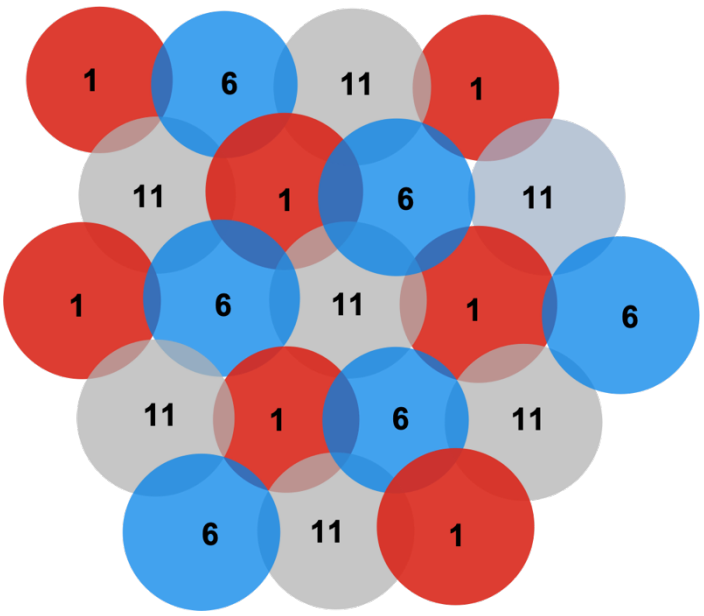
Channels and channel planning

Wi-Fi Channels are available over two, soon to be three (with Wi-Fi 6E), bands of unlicensed spectrum. A band is a group of adjacent frequencies. The **2.4 GHz band** (sometimes call the b/g band because 802.11b and 802.11g used it) has only 3 'non-overlapping channels'—1, 6 and 1—in most of the world. The reason these three channels aren't numbered as 1, 2, and 3 is because they were named before Wi-Fi existed.

Wi-Fi is a spread spectrum technology, which means unlike an FM radio, it sends redundant signals over multiple small channels at low power. For the non-RF engineers, the important point is **a Wi-Fi channel must spread over 20 MHz** (or more, see below). Three channels are the minimum necessary for a channel plan.



Wi-Fi is a half-duplex technology – only one radio can talk at a time. Exceptions, when the physics works out, are part of Wi-Fi 6, but the primary approach is one AP can talk to one client device at a time. However, if the AP radio cells are on different channels, then they can use both channels, and two APs on two channels can each talk to one client at the same time. Finally, 2 APs can use the same channel if they are far enough apart that they do not hear each other. The illustration below shows why 3 channels are the minimum for any channel plan.



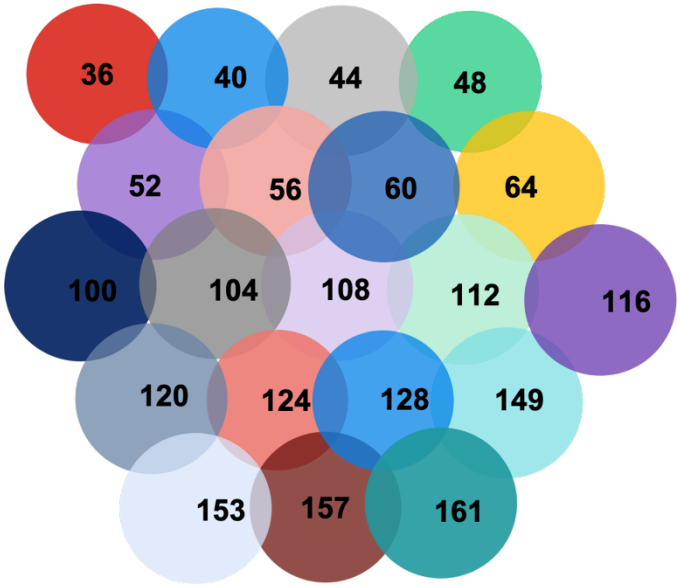
2.4 GHz channel plan

Interference is why channel planning is so important. For our purposes, there are two kinds of interference—noise and other Wi-Fi. **Noise** is when another RF source is putting energy out on the frequency we want to use—a microwave oven, baby monitor or Bluetooth are common sources. Other Wi-Fi, often called **co-channel**

interference, may interfere on the Wi-Fi protocol level. APs may be forced to wait their turn according to the Wi-Fi protocol. Two APs on the same channel that can clearly 'hear' each other will perform worse than a single AP, because they will contend for the medium and be forced to back off when the other is sending. When APs on the same channel are far enough apart, the co-channel interference just adds to the background noise level, and that can be transmitted over.

Understanding that devices contend for a shared medium might be the single most important concept in good Wi-Fi design. In one case study, a hotel wanted a very redundant Wi-Fi network, so they deployed the equivalent of the above channel plan but with 40 instead of 20 APs 2.4 GHz in the same space. With two APs covering the same spatial area on the same channel, constantly contending for media access, performance was miserable. In many environments, the biggest interference problem is *your own network interfering with itself*, although in dense urban environments, neighboring networks become significant.

The 5 GHz band has MUCH more capacity, with 25 available channels. The example channel plan above could have every single AP on a different channel in 5 GHz, resulting in NO co-channel or self-interference. However, there are other factors to consider in distributing channel capacity.

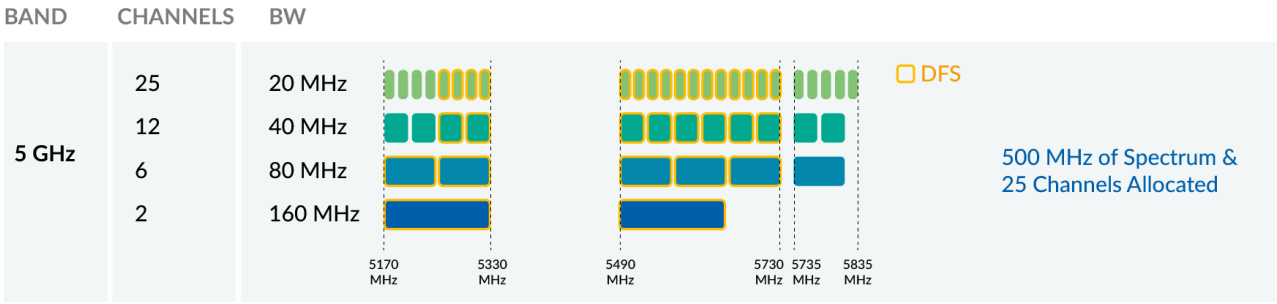


5 GHz channel plan

Channel bonding - Because Wi-Fi is a spread spectrum technology, with data encoded into multiple subcarriers, two 20 MHz wide channels can be combined into a 40 MHz channel to deliver twice the throughput to a client. Notice, that's not twice the total throughput. The theoretical throughput total of two 20 MHz channels is the same as the throughput of one 40 MHz channel, but the throughput peak to a single client is higher, and that total throughput can be achieved with fewer radios (APs). 80 MHz and even 160 MHz wide channels are defined in the standard, but 160 is impractical in 5 GHz unless you are deploying a single AP to a building in an isolated location. Wi-Fi 6 FortiAPs support 20, 40 and 80 MHz wide channels in 5 GHz, but only allow 20 MHz channels in 2.4 GHz.

Channel bonding is a way of redistributing the available capacity for fewer and faster devices. The total capacity of a multiple FortiAP LAN is roughly the same if all channels are used, regardless of the bonding plan. As a general rule, use 40 MHz wide channels in 5 GHz. In high density deployments, consider dropping to 20 MHz wide. For example, in a large conference room or auditorium, a single FortiAP can easily cover the room, but it cannot have 1000 devices connected to it. 20 MHz channels allow you to throw more APs at the capacity problem until you run out of channels. On the other hand, an office with 5 FortiAPs and a dozen devices each could consider 80 MHz wide channels.

Dynamic Frequency Selection (DFS) channels are another complication to be aware of. Sixteen of the twenty-five 5 GHz channels are used by military, weather radar, and satellite communications. Such use predate the development of Wi-Fi. Several Wi-Fi generations ago, it was unusual to make use of the DFS channels, but that is no longer the case. FortiAPs will automatically choose channels on boot up, and if a radar event is detected, will change to another channel automatically, as is required by regulation. The main point is that a network administrator should not be afraid to use the DFS channels. These channels represent a great deal of additional capacity and FortiAPs will automatically allocate channels around any radar.



Design for 5 GHz over 2.4 – because 2.4 GHz is the lowest common denominator, there is a tendency to design for 2.4 GHz first. However, it's much better to design with 5 GHz as the primary access, and use 2.4 as a kind of auxiliary band. Virtually all Wi-Fi client devices, even older ones, support 5 GHz, and there is just too much additional capacity to not focus on 5 GHz. 2.4 GHz is effectively becoming the **IoT band**. Bluetooth uses 2.4 GHz, and even the very small number of 2.4 only Wi-Fi devices are because they are very cost conscious IoT devices. IoT devices usually have low throughput needs so they can operate at lower data rates (see below).

Distributed Automatic Radio Resource Provisioning (DARRP) is a Fortinet Wireless Controller technology that assigns radio channels automatically to APs, and updates regularly to account for changing conditions. DARRP ensures the wireless infrastructure is optimized for maximum performance. Wi-Fi 6 FortiAPs include a third monitoring radio so that this advanced feature has all the necessary data to make intelligent decisions. The third radio can continuously monitor the RF environment for interference, noise, and signals from neighboring APs. With this data, the FortiGate WiFi Controller is able to determine the optimal channel and RF power levels for each AP on the network, without a need for administrator intervention.

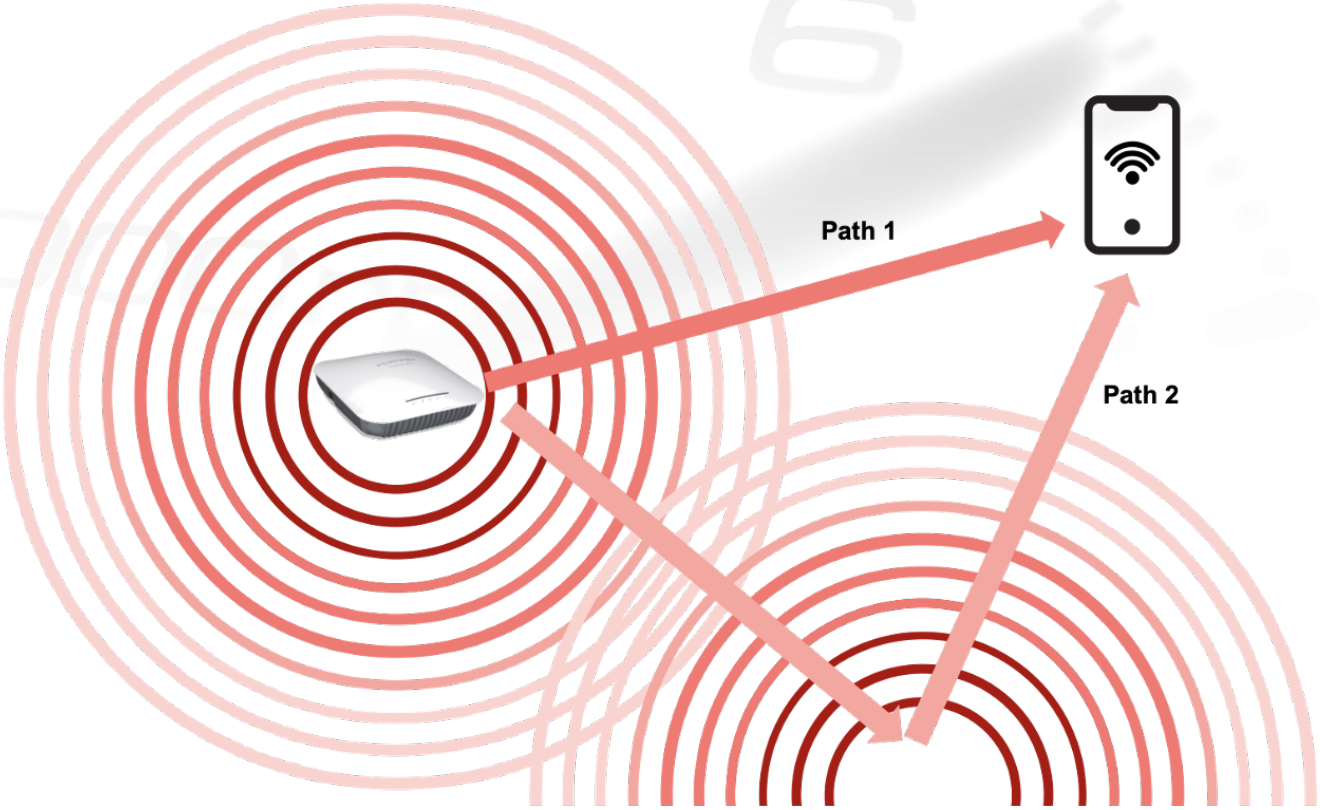
Frequency Band Handoff (Band Steering) - Every Wi-Fi device that operates in 5 GHz not only gains for itself, but it also leaves behind capacity for 2.4 GHz only devices. The FortiOS WiFi Controller can tell from a client's Wi-Fi probes if a device is dual band capable, and it will respond on 5 GHz, balancing the use of spectrum if signal strength is high enough.

Client Load Balancing across APs is a related idea supported by FortiAPs. In this case, clients are balanced across different APs, rather than different radios in the same AP. If the client count exceeds the configurable threshold (default of 30), clients are moved to another AP with sufficient signal strength.

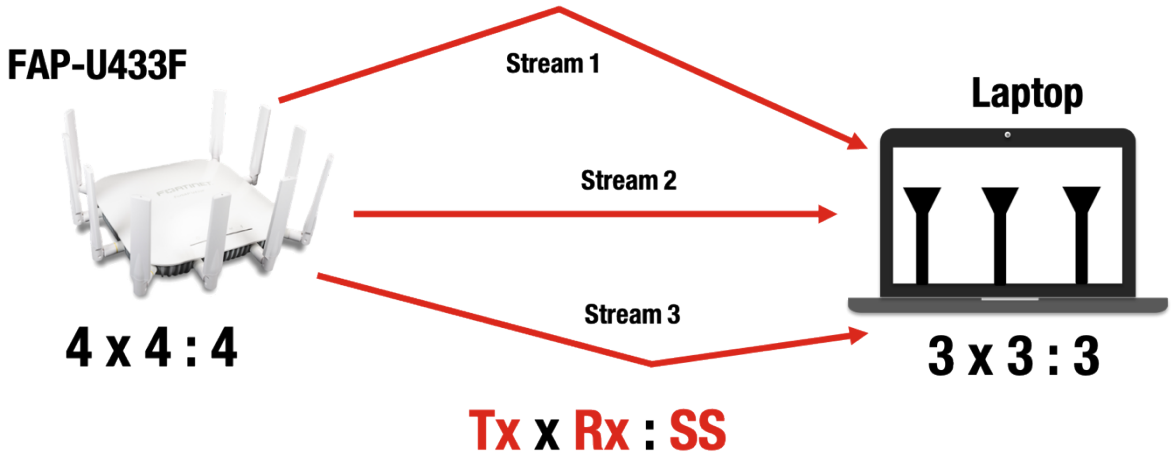
MIMO

MIMO (Multiple Input, Multiple Output) uses slightly different signals between multiple sending and receiving antennas to increase throughput. Introduced in Wi-Fi 4 (11n), it turned an RF liability into an advantage. Indoor Wi-Fi results in a lot of reflections; very little signal goes directly to the receiving antenna and much of it bounces off of the

walls, ceiling, and etc. The bounced signal arrives at a later time because it followed a different path, so this is called **multi-path**.



The problem is that this distorts signal. It is exactly analogous to trying to talk in an echoing chamber. In an amazing feat of engineering, Wi-Fi standards have been developed to take advantage of this by using multiple antennas. Advanced signal processing, which is part of every FortiAP, can take advantage of multi-path so that different transmit antennas can align with different receive antennas to each carry a different data stream. Two antennas on each end have the potential to double the data rate, three to triple it, etc.

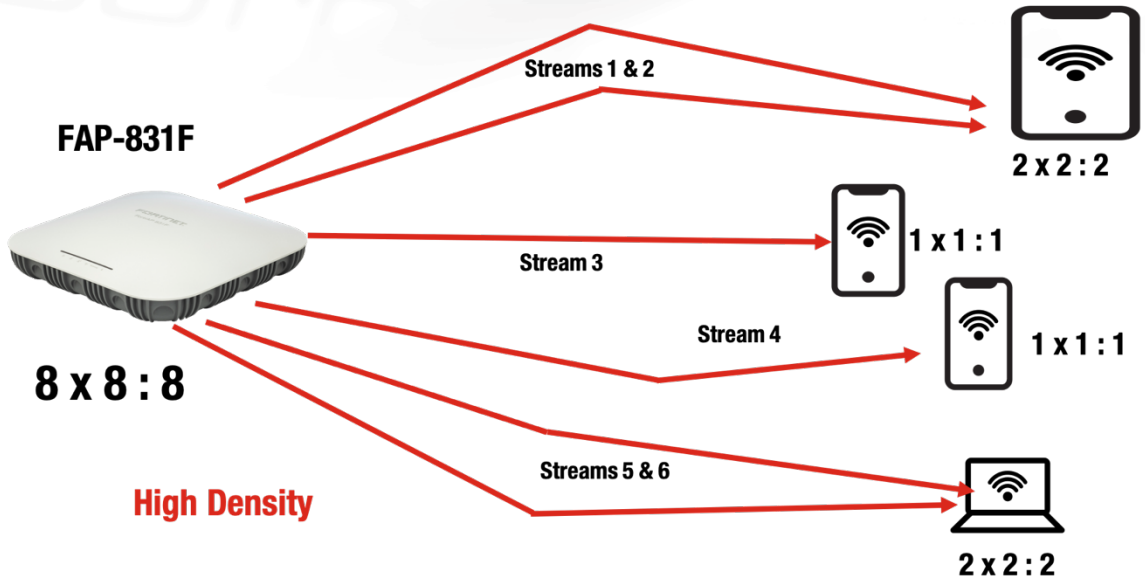


The nomenclature 'Tx X Rx : SS' where Tx is the number of transit antennas, Rx is the number of receivers and the S is the number of **spatial streams**, or simply streams. There must be at least enough antennas to support the streams, but there can be more antennas than streams. Wi-Fi 4 (11n) MIMO was AP to one client only, and earlier APs often supported 3 antennas but only 2 streams.

MIMO

Client capabilities always matter with Wi-Fi. While it is pretty reasonable to get 3 streams to a laptop, smart phones just do not have the space and battery power for enough antennas for effective multipath. Smart phones are generally not capable of simple MIMO and have a much lower capacity than laptops.

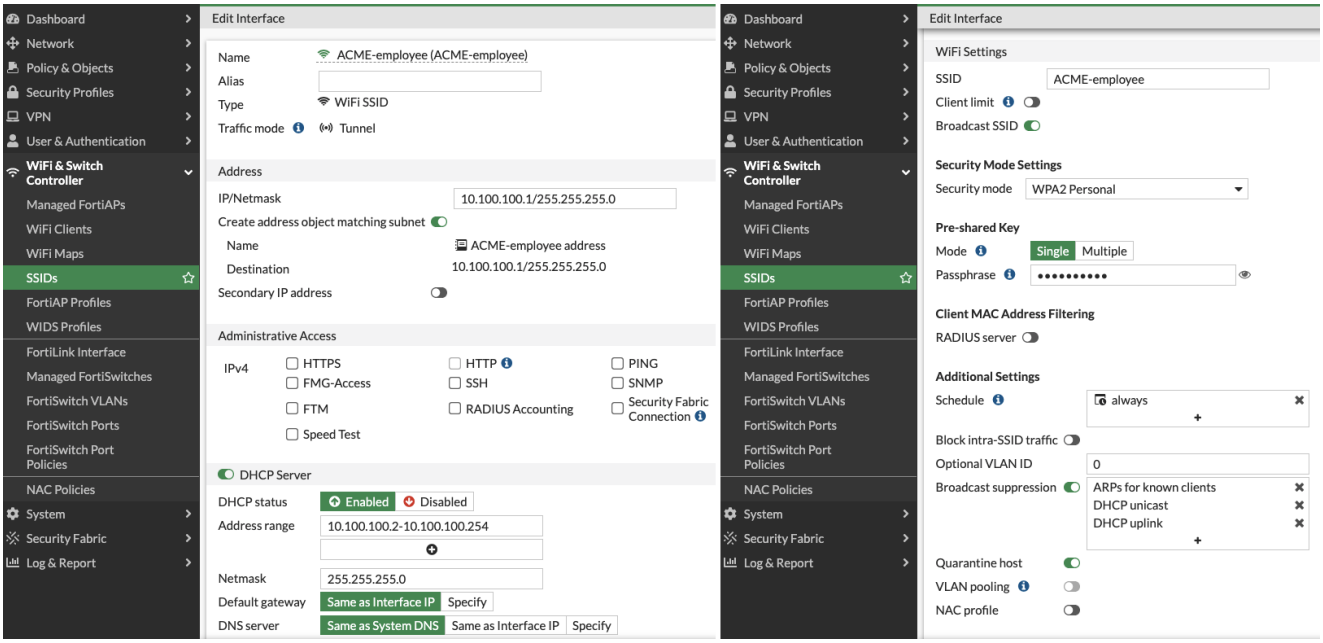
MU-MIMO (Multi-User MIMO), is the next evolution of the technology. MU-MIMO allows the AP transmit streams to be divided up among multiple clients. With MU-MIMO, an AP can transmit to one client with one or some antennas, and use other antennas to simultaneously transmit to another client. Fortinet's Wi-Fi 6 FortiAPs include support for both Uplink MU-MIMO as well as Downlink MU-MIMO.



WLAN configurations

The previous topics have mostly covered the physical layer aspects of Wi-Fi, the wireless equivalent of the number of wires in an Ethernet cable, the correct voltages, etc., but more complex and with more variables. As a networking device, a FortiAP is fundamentally a Layer 2 device with wireless equivalents to switches such as 'virtual ports.' It provides access to the network, hence "Access Point", and usually translates Wi-Fi into Ethernet.

SSID (Service Set Identifier) is the over-the-air name of the WLAN, so that users can find it and connect to it. Every AP that serves that WLAN will carry an SSID. The FortiOS WiFi Controller simplifies the creation and security integration of an SSID by making it part of configuring an interface on the FortiGate. The DHCP server, firewall address object, routing, and NGFW policies can easily be configured through the same single pane of glass interface.



BSSID (Basic Service Set Identifier) is best thought of as the AP's Wi-Fi MAC address. The SSID is the same for the entire WLAN, but the BSSID is specific to an AP radio and WLAN. FortiAPs will generate these automatically.

MIMO

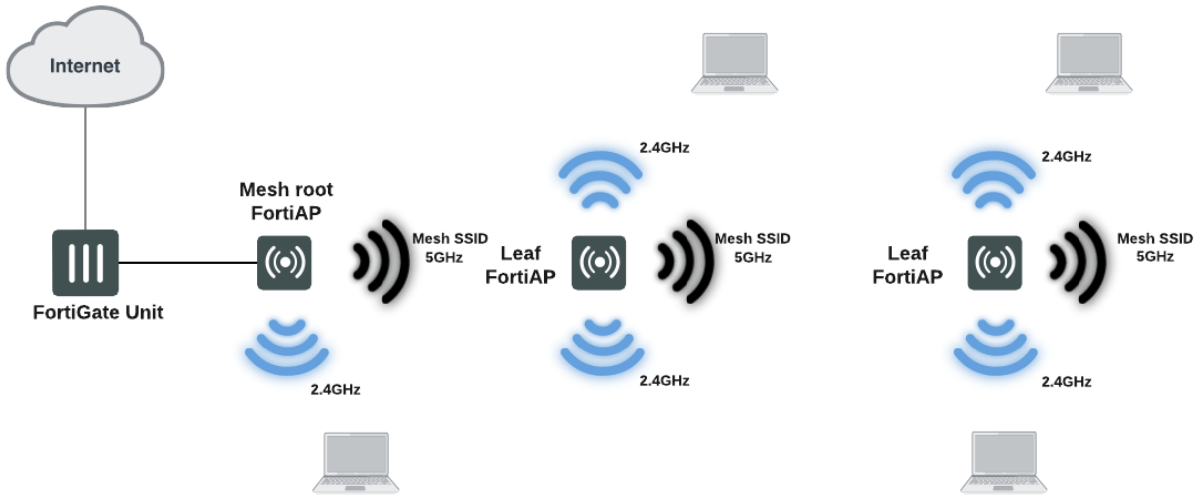
All | 2.4 GHz | 5 GHz | Open | Secure

BSSID	Network Name	Anno...	Vendor	Signal	Channel	Channel Width	Band	Generation
00:0C:E6:F0:85:31	ACME-employee		Fortinet Inc.	-56 dBm	112	20 MHz	5 GHz	Wi-Fi 6
00:0C:E6:F0:85:32	ACME-guest		Fortinet Inc.	-56 dBm	112	20 MHz	5 GHz	Wi-Fi 6
00:0C:E6:F0:85:33	NAC-wifi		Fortinet Inc.	-56 dBm	112	20 MHz	5 GHz	Wi-Fi 6
00:0C:E6:F0:85:34	Cloud-SSID		Fortinet Inc.	-56 dBm	112	20 MHz	5 GHz	Wi-Fi 6
00:0C:E6:F0:85:41	ACME-employee		Fortinet Inc.	-43 dBm	11	20 MHz	2.4 GHz	Wi-Fi 6
00:0C:E6:F0:85:42	ACME-guest		Fortinet Inc.	-43 dBm	11	20 MHz	2.4 GHz	Wi-Fi 6
00:0C:E6:F0:85:43	NAC-wifi		Fortinet Inc.	-43 dBm	11	20 MHz	2.4 GHz	Wi-Fi 6
00:0C:E6:F0:85:44	Cloud-SSID		Fortinet Inc.	-43 dBm	11	20 MHz	2.4 GHz	Wi-Fi 6
00:0C:E6:F2:3A:B1	ACME-employee		Fortinet Inc.	-53 dBm	120	20 MHz	5 GHz	Wi-Fi 6
00:0C:E6:F2:3A:B2	ACME-guest		Fortinet Inc.	-53 dBm	120	20 MHz	5 GHz	Wi-Fi 6
00:0C:E6:F2:3A:B3	NAC-wifi		Fortinet Inc.	-53 dBm	120	20 MHz	5 GHz	Wi-Fi 6
00:0C:E6:F2:3A:B4	Cloud-SSID		Fortinet Inc.	-56 dBm	120	20 MHz	5 GHz	Wi-Fi 6
00:0C:E6:F2:3A:C1	ACME-employee		Fortinet Inc.	-46 dBm	1	20 MHz	2.4 GHz	Wi-Fi 6
00:0C:E6:F2:3A:C2	ACME-guest		Fortinet Inc.	-45 dBm	1	20 MHz	2.4 GHz	Wi-Fi 6
00:0C:E6:F2:3A:C3	NAC-wifi		Fortinet Inc.	-46 dBm	1	20 MHz	2.4 GHz	Wi-Fi 6
00:0C:E6:F2:3A:C4	Cloud-SSID		Fortinet Inc.	-46 dBm	1	20 MHz	2.4 GHz	Wi-Fi 6
00:0C:E6:F3:A5:71	ACME-employee		Fortinet Inc.	-60 dBm	128	20 MHz	5 GHz	Wi-Fi 6

Traffic modes include the default '**Tunnel**', where all traffic is tunneled to the FortiGate via FortiLink. This effectively VLANs all traffic without having to tag or define VLANs on the intervening switch network. Every tunneled WLAN goes to the FortiGate which can then inspect the traffic and route it according to the configured rules.

Bridge Mode bridges WLAN traffic directly to the AP Ethernet port. Logically, this works like plugging into the switch the AP is plugged into, so that interface must have the necessary DHCP server, etc. configured. This is most commonly used for remote APs and or guest networks where there is reason NOT to send the traffic directly to the FortiGate.

Mesh Mode enables FortiAPs to use a radio as a back-haul. The client traffic is bridged from one radio, with normal SSIDs available for client connection (usually the 2.4 GHz), to the other radio (usually the 5 GHz). This is useful when it is impractical to run an Ethernet cable but power is available, such as with portable classrooms or temporary structures, or a bridge is otherwise needed to another building.

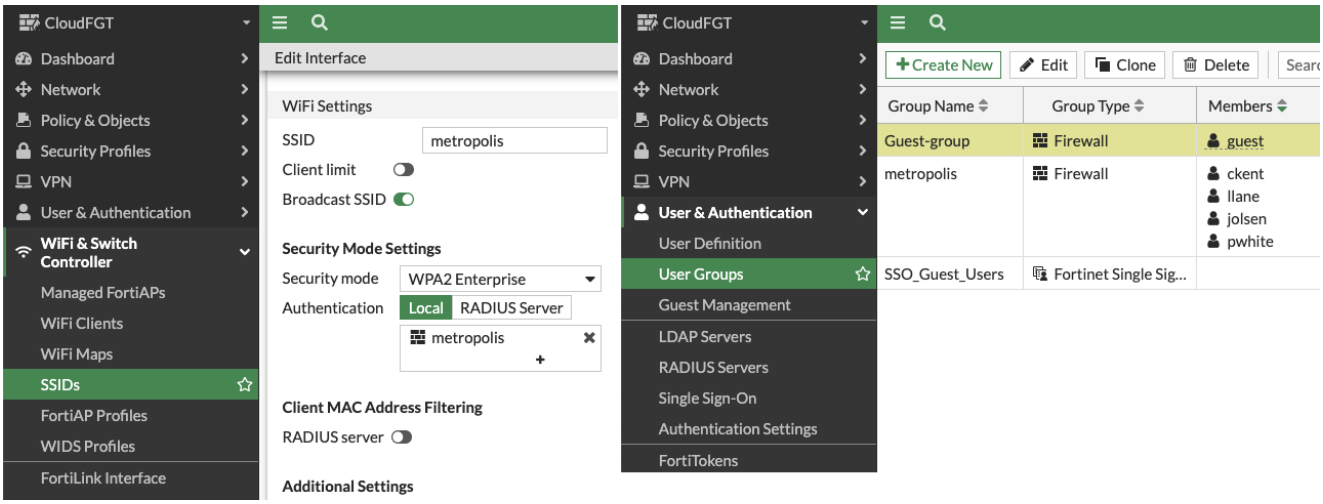


Security

Wi-Fi Security is a subset of network security. The great advantage of using a FortiGate based Wi-Fi system is that the entire security stack is easily available behind a single pane of glass—Security Driven Networking. However, Wi-Fi specific security differs from more general network security. Because Wi-Fi is over the air, there is no reliable way to limit physical access to the network, and because the network can be sniffed, it needs encryption if it is to be private. Nevertheless, open networks are common for guest use or in public venues, possibly with Captive Portals (see below) included.

WPA2 and WPA3 Enterprise are RADIUS based. These are the standards any enterprise class network should be using. If you have a database of users with a RADIUS front end, this is what to use. Encryption and authentication are strongest. We are in a transition period, as there are still many clients out there that do not support WPA3 enterprise. Windows 11 with a compatible Wi-Fi card, Mac computers after 2013, iPhone 11, and more should support it, but you may need a transition plan for your network.

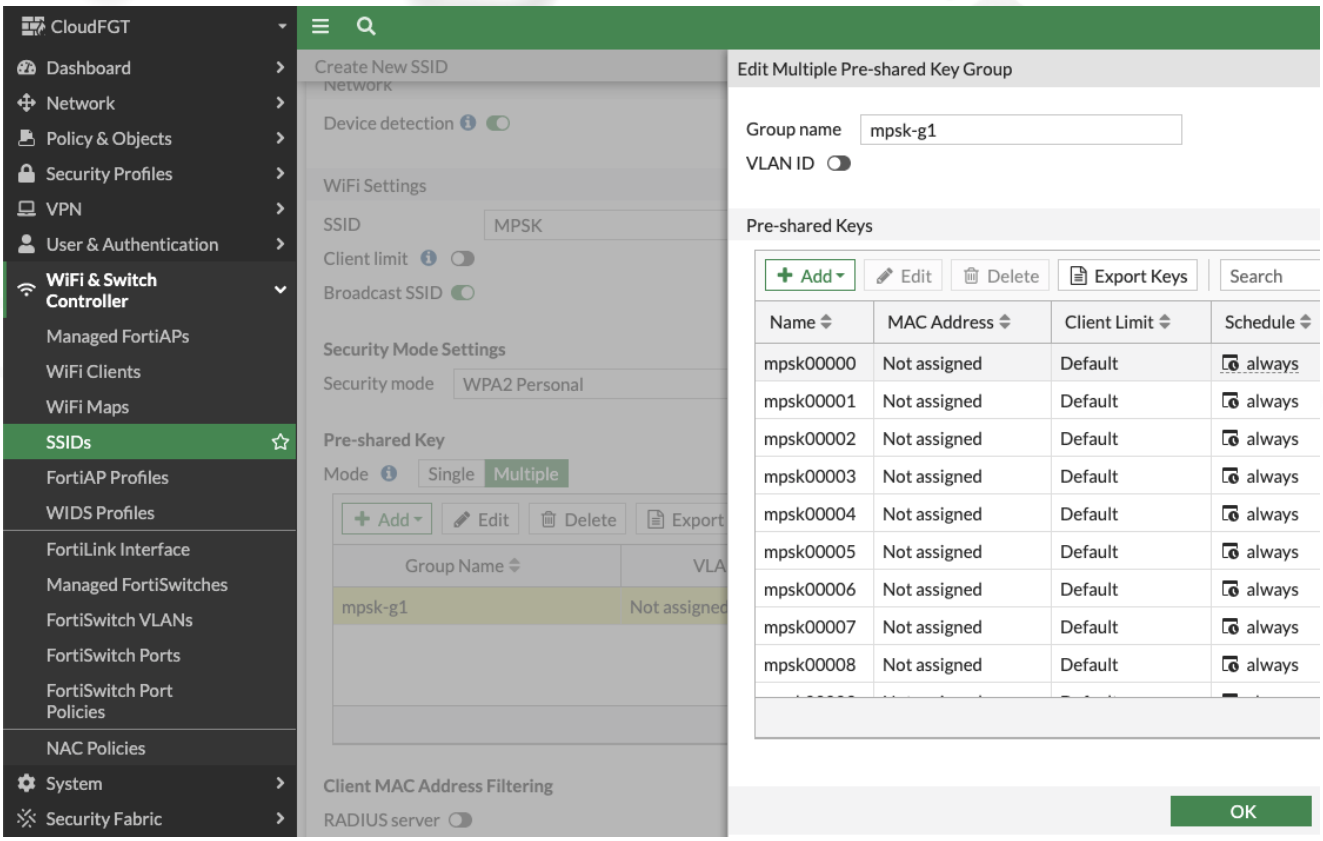
FortiGate As RADIUS server - The locally defined users and user groups on the FortiGate can be used as the RADIUS server by choosing the local authentication option. A handy option for many environments or special cases.



WPA2 Personal and WPA3 SAE use a *Pre-Shared Key* (PSK) for authentication and encryption. This is usually referred to as "the Wi-Fi password". This is meant for home use and small offices and should be avoided in locations where more than a few users are to be authenticated.

A WPA2 Personal/WPA3 SAE SSID may be necessary even in large environments because of IoT devices that do not support the enterprise options. If so, security best practices are to isolate such WLANs to a specific VLAN.

MPSK (Multiple PSK) - A Fortinet Wi-Fi option when creating a WPA2 Personal network is to use multiple keys. In this case, not every device uses the same PSK, sharing the keys among groups of devices or even a unique entry for each device. WPA3 SAE does not need this option. SAE (Simultaneous Authentication of Equals) generates a unique encryption key for each session/device.



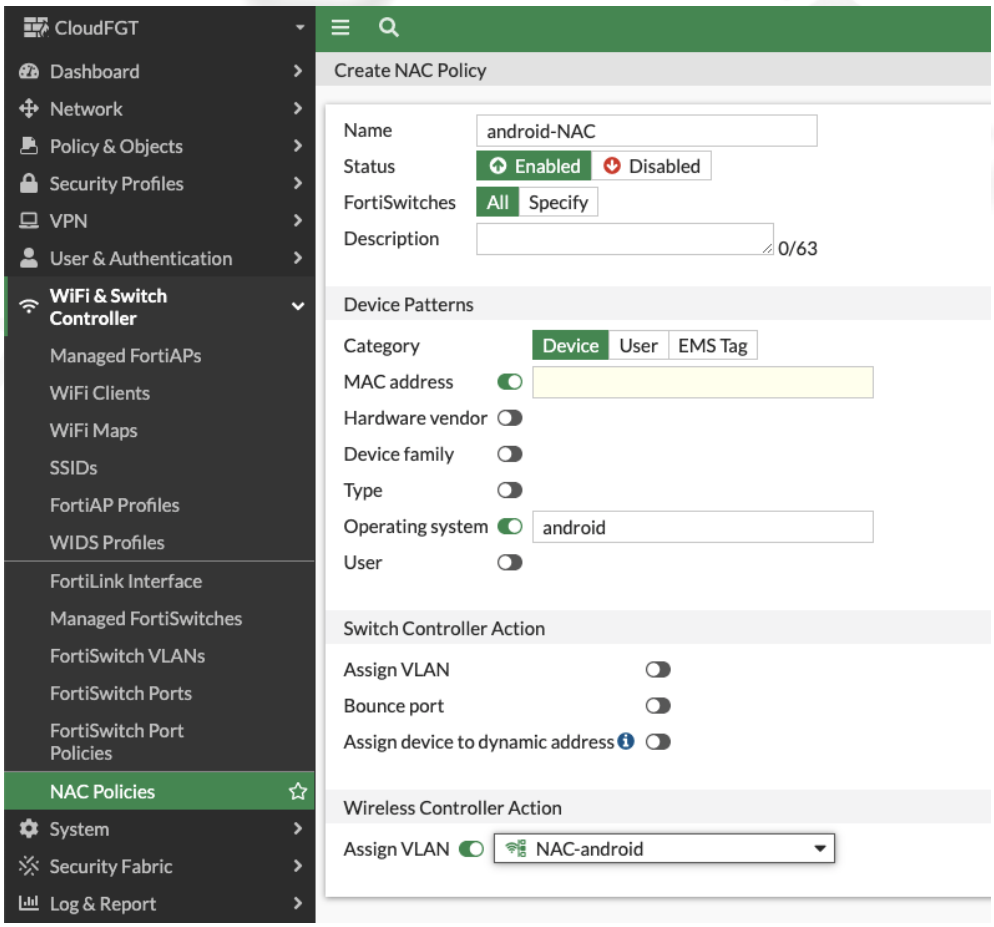
Captive Portals and Open Networks – Open Networks have no Layer 2 encryption or authentication, while a Captive portal is a web page than can be used for authentication above Layer 2, or simply present a click through disclaimer page. The authentication portal can be hosted at the FortiGate or use an external 3rd party portal. Captive Portal can also be combined with WPA2 Personal.

- **Public Networks**, such as the local coffee shop, make frequent use of Captive portals, sometimes with a minimal disclaimer only, sometimes with self-registration. Fortinet Wi-Fi supports email capture during self-registration via captive portal
- **Guest Networks** are more what one finds in Enterprise environments, where guests need permission from someone like a lobby administrator. Fortinet Wi-Fi supports this and several variations, such as a guest sponsorship.

Hotspot 2.0 uses the OSEN security option in the SSID configuration screen. This is a standard for public hotspot registration across large service providers.

Wireless Intrusion Detection System (WIDS) with Rogue AP Detection WIDs profiles can be enabled on a per radio basis in AP profiles. WIDS profiles monitor and alert for a number of Wi-Fi attacks such as EAPOL and other floods, deauthentication attacks and similar. All Wi-Fi 6 FortiAPs have a third radio for monitoring purposes and it is highly recommended to enable Rogue AP scanning on the monitoring radio, which can scan the entire channel space while the service radios support network clients. Rogue APs can also be suppressed automatically over-the-air.

FortiLink NAC with an onboarding VLAN can be enabled on a WLAN. A Wi-Fi connected device can be allowed onto an initial onboarding VLAN and then automatically identified by criteria such as operating system, MAC address, hardware vendor and more. Once identified it can be moved to a specific VLAN designated for such devices. For instance, VoIP phones could be moved to a VoIP VLAN secured specifically for such devices.



Security Driven Networking – While we focus on Wi-Fi specific security, don't overlook the central security advantage. The FortiOS WiFi Controller runs on a FortiGate, and ALL the security power of the FortiGate is integrated in a single pane of glass. The normal flow is for Wi-Fi SSID to be automatically isolated from the rest of the network, tunneled to the FortiGate without the need to configure any VLANs, and fully inspected before being allowed anywhere else.

Wi-Fi 6 specific improvements with FortiAPs

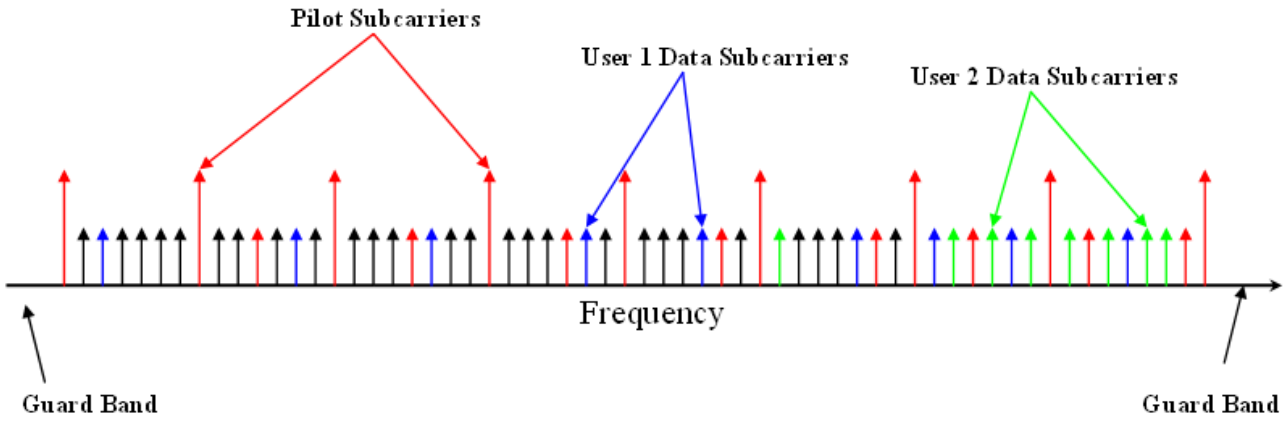
Wi-Fi 6 improvements over previous generations

Wi-Fi 6 changes includes higher data rates, spatial stream improvements and general enhancements to previous Wi-Fi generations. However, it also includes completely new techniques to improve high-density environments. As previously mentioned, when all clients were laptops, adding spatial-streams greatly increased capacity. Smart phones and tablets are more limited. More spatial streams require more antennas, and more antennas require not only more space in these smaller form factors, but more battery power. MU-MIMO is one way to improve the total networks capacity, but Wi-Fi 6 also introduces completely new technologies.

OFDMA

Wi-Fi is a spread spectrum technology. That means that a 20 MHz Wi-Fi channel is actually the sum of a number of smaller channels—about 48 per 20 MHz, depending on how you count. This is called OFDM (Othogonal Frequency Division Multiplexing). Channel bonding uses a bigger stretch of subcarriers, and so can carry more information. OFDMA (Orthogonal Frequency Division, Multiple Access) does the opposite, splitting the channel into smaller channels (called Resource Units) with fewer subcarriers, but it can use those smaller channels at the same time, from the same antenna.

With OFDMA a Wi-Fi channel can be divided up among multiple clients. Instead of using the entire channel for one client at a time, with OFDMA, subcarriers are divided into 'resource units' that can be directed at specific clients. This reduces contention and overhead resulting in more efficient use of the channel, especially for lower speed clients. Of course, the clients must be Wi-Fi 6 to support this.



https://wikipedia.org/wiki/Orthogonal_frequency-division_multiple_access#/media/File:OFDMA_subcarriers.png

8 stream MU-MIMO

MIMO (Multiple Input, Multiple Output) for single clients with multiple antennas was introduced in Wi-Fi 4 (802.11n). While OFDM and OFDMA are *frequency multiplexing*, MIMO is *spatial-multiplexing*, depending on multi-path (different paths) to the target antennas for each stream.

Wi-Fi 5 introduced MU-MIMO, or Multi-User MIMO, where each antenna stream could send data to antennas on different devices, allowing simultaneous downstream to multiple devices. The standard defined up to 8 streams, but no APs were deployed with more than 4.

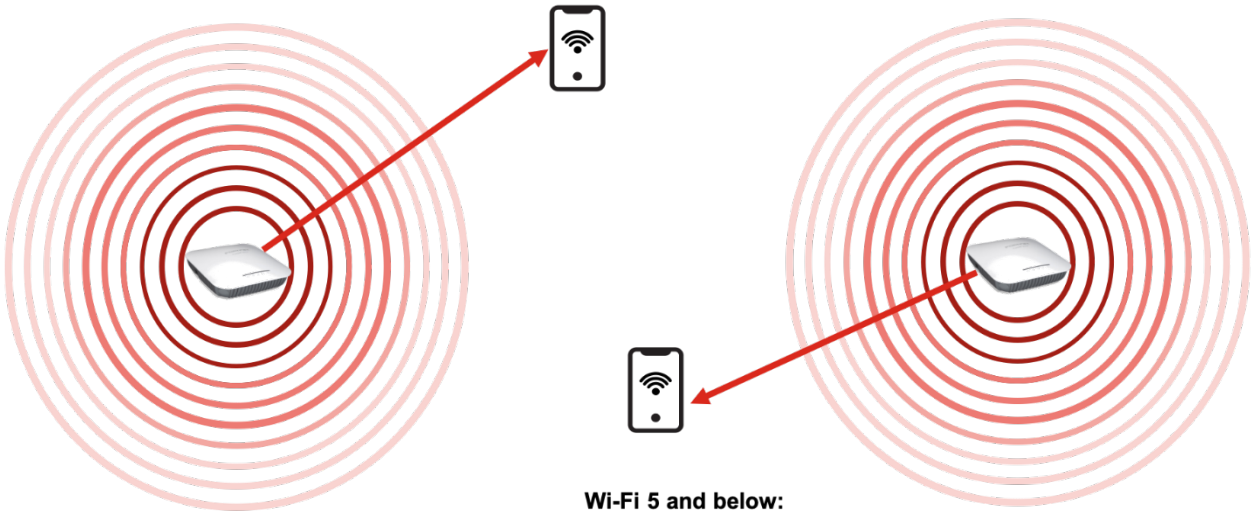
Wi-Fi 6 extends MU-MIMO to 8 streams, and enables simultaneous uplink from multiple clients. MU-MIMO is supported on all Wi-Fi 6 FortiAPs, but the number of streams available depends on the number of antennas: 2 for an FAP-231F, 4 for an FAP-431F, and the FAP-831F has 8 antennas and supports 8 streams.

It is important to understand that MU-MIMO only works when the clients have enough 'spatial diversity.' If 2 smart phones are physically close together, it is unlikely that there is enough of a difference to mathematically resolve one antenna to one, one to another at the same time, while if the hypothetical smart phones are on opposite sides of the AP, a solution is much more likely. That's why the FAP-831F is considered a high-density AP. In an office environment with fewer devices, the 2 and 4 antenna APs are going to cover most of the possible MU-MIMO options. However, in a high-density deployment, like an auditorium with many client devices surrounding an FAP-831F, it is much more likely that MU-MIMO will provide a solid performance boost.

BSS coloring

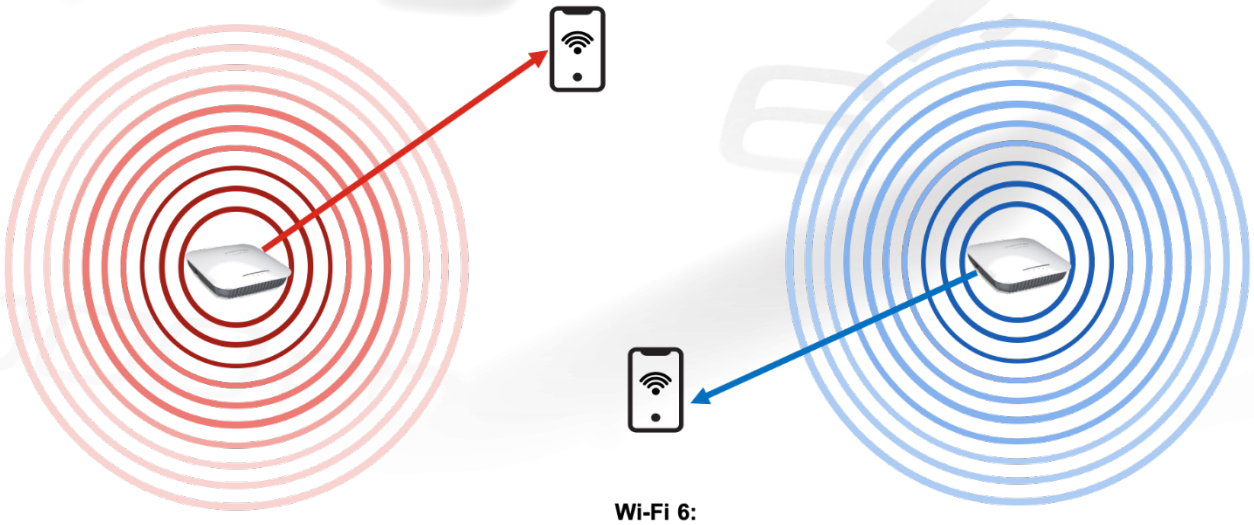
As a reminder, there are two kinds of interference to be concerned with in a Wi-Fi network: Wi-Fi and non-Wi-Fi. Non-Wi-Fi interference is 'noise,' RF energy interfering with the medium. The classic example is a microwave oven disrupting a Wi-Fi connection. It is interference at layer 1 or the physical layer of the OSI model. However, Wi-Fi is no longer new. It is everywhere. Now the more important concern is other Wi-Fi signals on channel, including the local WLAN self-interfering.

If a signal is recognizable as Wi-Fi, then a Wi-Fi radio has to wait its turn (this function is called a CCA of Clear Channel Assessment). It interferes because of the way the protocol works; the medium is not clear and the radio has to wait its turn. It is fairly described as layer 2 interference because it is a media access issue. In a campus environment, your own APs on the same channel, or clients connected to them, may cause contention in other AP cells.



Wi-Fi 5 and below:
Same channel + too close = must take turns

BSS coloring adds some header information, or a 6-bit 'color' tag. If a Wi-Fi packet is detected that has a *different* color, it is part of a different AP-client combination and the listening Wi-Fi radio can go ahead and transmit, treating the signal as if was background noise. Both signals can be transmitted simultaneously, network capacity goes up, and APs can be spaced closer together.



Wi-Fi 6:
Same channel + different colors = simultaneous Tx

FortiAP Wi-Fi 6 Standard and UTP Access Points

FortiAP U431F and U433F - 4x4:4 MIMO Indoor

These enterprise class Wi-Fi6 (802.11ax) indoor APs provide three radios. These top-of-the-line access points provide OFDMA, a 2.5 Gigabit Ethernet port plus an additional 1 Gbps Ethernet port for PoE diversity. The APs can be configured for dual 5 GHz band access while still providing coverage for devices on the 2.4 GHz band, or can be configured to offer dedicated scanning. The integrated BLE radio can be used for beacons and locationing applications.

FortiAP U432F - 4x4:4 MIMO Outdoor/Ruggedized

This enterprise class 802.11ax ruggedized indoor/outdoor AP provides three radios. As a top-of-the-line Wi-Fi 6 access point it provides OFDMA, a 2.5 Gigabit Ethernet port, plus an additional 1 Gbps Ethernet port with PoE out. The AP can be configured for dual 5 GHz band access while still providing coverage for devices on the 2.4 GHz band, or can be configured to offer dedicated scanning. The integrated BLE radio can be used for beacons and locationing applications.

FortiAP U231F - 2x2:2 MIMO Indoor

This enterprise class Wi-Fi 6 (802.11ax) indoor AP provides three radios as well as features such as OFDMA and dual 1 Gbps Ethernet ports for PoE diversity. The APs can be configured for dual 5 GHz band access while still providing coverage for devices on the 2.4 GHz band, or can be configured to offer dedicated scanning. The integrated BLE radio can be used for beacons and locationing applications

FortiAP U234F - 2x2:2 MIMO Outdoor/Ruggedized

This enterprise class Wi-Fi 6 ruggedized indoor/outdoor AP provides three radios with internal antennas as well as features such as OFDMA and dual 1 Gbps Ethernet ports. The AP can be configured for dual 5 GHz band access while still providing coverage for devices on the 2.4 GHz band, or can be configured to offer dedicated scanning. The integrated BLE radio can be used for beacons and locationing applications.

FortiAP 831F - 8x8:8 MU-MIMO Indoor/High Density

This high throughput enterprise class 802.11ax indoor AP provides three radios and 8 spatial streams. This top-of-the line access point supports OFDMA, a 5.0 Gigabit Ethernet port, plus an additional 1 Gbps Ethernet port for PoE diversity. The AP can provide 24/7 scanning across both bands while still providing access on both the 2.4 GHz and 5 GHz bands. The integrated BLE radio can be used for beacons and locationing applications.

FortiAP 431F and 433F

These enterprise class 802.11ax indoor APs provide three radios. These top-of-the-line access points provide OFDMA, a 2.5 Gigabit Ethernet port, plus an additional 1 Gbps Ethernet port for PoE diversity. The APs can provide 24/7 scanning across both bands while still providing access on both the 2.4 GHz and 5 GHz bands. The integrated BLE radio can be used for beacons and locationing applications.

FortiAP 432F - 4x4:4 MU-MIMO, Outdoor/Ruggedized

This enterprise class 802.11ax ruggedized indoor/outdoor AP provides three radios. As a top-of-the-line Wi-Fi 6 access point it provides OFDMA, a 2.5 Gigabit Ethernet port, plus an additional 1 Gbps Ethernet port with PoE out. The AP can provide 24/7 scanning across both bands while still providing access on both the 2.4 GHz and 5 GHz bands. The integrated BLE radio can be used for beacons and locationing applications.

FortiAP 231F - 2x2:2 MU-MIMO Indoor

This enterprise class Wi-Fi 6 indoor AP provides three radios as well as features such as OFDMA and dual 1 Gbps Ethernet ports. The AP can provide 24/7 scanning across both bands while still providing access on both the 2.4 GHz and 5 GHz bands. The integrated BLE radio can be used for beacons and locationing applications.

FortiAP 234F - 2x2:2 MU-MIMO, Outdoor/Ruggedized

This enterprise class Wi-Fi 6 ruggedized indoor/outdoor AP provides three radios with internal antennas as well as features such as OFDMA and dual 1 Gbps Ethernet ports. The AP can provide 24/7 scanning across both bands while still providing access on both the 2.4 GHz and 5 GHz bands. The integrated BLE radio can be used for beacons and locationing applications.

FortiAP 23JF - 2x2:2 MU-MIMO Wall Plate

This enterprise class Wi-Fi 6 wall plate AP provides three radios with internal antennas as well as features such as OFDMA and is PSE-capable. The AP can provide 24/7 scanning across both bands while still providing access on both the 2.4 GHz and 5 GHz bands. The integrated BLE radio can be used for beacons and locationing applications. Additional features include PoE out for downstream devices and RJ45 passthrough. This access point can be installed in minutes, right over the existing wall plate.

Appendix A: Documentation references

Feature Documentation

- FortiSwitch Product Documentation Library
- FortiAP/FortiWiFi Product Documentation Library

Solution Hub

- Secure Access Solution Hub

www.fortinet.com

20-700-767598-20220608