FORTINET WIRELESS LAN CONTROLLER

SOLUTION GUIDE

TABLE OF CONTENTS

INTRODUCTION

WHY NOT A SINGLE SOLUTION FOR WI-FI?

Wi-Fi has become a commodity. Much like the auto industry, there are a range of products on the market which do mostly the same thing with little or no knowledge from the driver. Most cars can go faster than the speed limit in the same way that most access points (APs) can go faster than the internet connection they rely on.

But in certain circumstances, specialized knowledge is a requirement. For example, it would be unwise to put a standard family sedan into a Formula 1 race. It is the same with Wi-Fi. Some implementations are beyond the commonplace AP and a specialized solution is required. The Fortinet Controller is that specialized solution.

Of course, in the above analogy the standard family sedan would be able to complete a lap of the Formula 1 circuit but it would be far from optimized.

Continuing with a car theme, 50 years ago most car owners would need to have a reasonable working knowledge of their cars' components and how to do basic maintenance if they wanted to get to work each day. Wi-Fi is on a faster trajectory, but even 10 years ago anyone installing a simple Wi-Fi solution had to have a great understanding of the technology. Today, the average motorist might struggle to change a tire, let alone adjust the fuel / air mixture on their car. But modern cars have developed beyond needing that sort of owner maintenance and Wi-Fi has too, in most cases. Fortinet offers a range of Wi-Fi solutions which fit into the plug-and-play generation of Wi-Fi, where a standard subset of settings is presented for customization and details are taken care of automatically. Fortinet also offers a controller solution for scenarios where automation is not optimized for the particular environment.

THE CUSTOMERS HAVE CHANGED AND SO HAVE THE DEVICES

Seven years ago, the iPad did not exist. Ten years ago, the iPhone did not exist. Mobile devices were laptops or basic phones with simple email clients on them. Mobility was not a reality. Most users shut their laptop down before roaming around a building --if it took the radio card a couple of seconds to reconnect, no one cared.

Wi-Fi at its inception was intended to be a single transmitter and multiple clients. As things progressed, more transmitters (APs) were added to the network and the client was expected to decide which one to talk to. This remains one of the most contentious parts of any Wi-Fi solution today. As more mobile devices offer Voice over Wi-Fi and many cell phone operators expect to use Wi-Fi as a medium to cover inside buildings, the roam times and efficiency of client roam decisions are critical to the overall performance of the network. The problem is that many of these mobile devices are driven by cost, size, and battery life rather than great Wi-Fi, which can lead to poor performance.

But the Fortinet controller takes control of the situation and can even remove the roaming decision from the client.

SOME 802.11 BASICS

WI-FI RANGE – HOW FAR DOES YOUR ACCESS POINT COVER?

This question never seems to go away, and it is such a pointless question in most network deployments today. Even public access networks should not be based on how far an AP can transmit. An AP is a dedicated Wi-Fi device. It can transmit at the full power that is allowed in the local area and can be placed in an ideal location to maximize coverage.

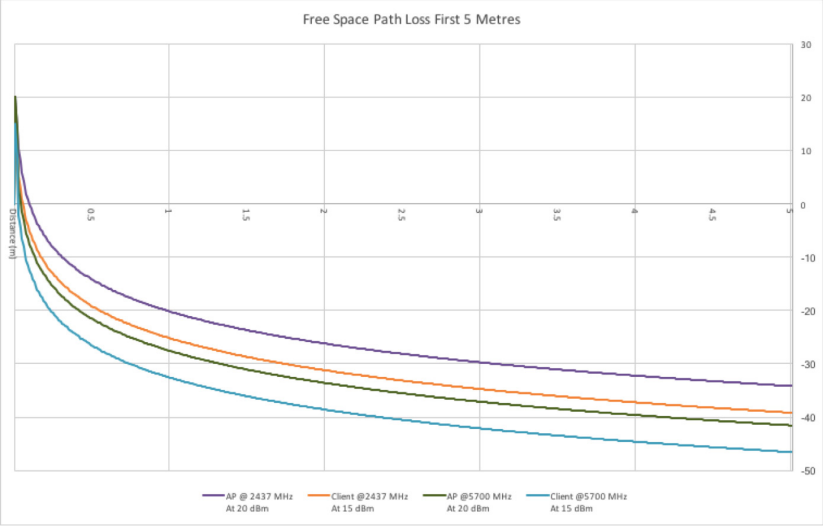
Great. But what about the other end of the Wi-Fi link: the client device? An iPhone 7 has the following radios:

- LTE/UMTS/CDMA/GSM/EDGE – Dependent on country/cell phone standards
- Bluetooth 4.2 – Wireless Headsets etc.
- Assisted GPS – Satellite Navigation etc.
- iBeacon – Location finding
- NFC – Mobile payments
- 802.11a/b/g/n/ac Wi-Fi with MIMO (20-50mW – Dependent on band)

These all have radios and antennas along with the EMC noise generated by the high-performance CPU. In addition to the above, the iPhone 7 also requires a Bluetooth headset. With all of this happening and the phone sitting in a jacket pocket next to a large bag of water (otherwise known as the user), trying to take a Voice over Wi-Fi call via the Bluetooth headset, is it reasonable to assume the AP's ability to transmit is not the main factor in the range decision?!

GREAT RANGE <> GREAT THROUGHPUT

Wi-Fi speeds reduce at an alarming rate as the range increases. The wireless signal decays very quickly – over just the first 5 meters:



The above chart shows:

AP running at full power (20dBm – 100 mW) on 2.4 GHz channel 6

Client running at 15dBm – 32 mW on 2.4 GHz channel 6

AP running at full power (20dBm – 100 mW) on 5 GHz channel 140

Client running at 15 dBm – 32 mW on 5 GHz channel 140

This chart is just using the standard free space path loss formula, so it does not take into account any special antennas or MU MIMO or walls, etc. This is just about the physics of a wireless signal going from a transmitter to a receiver.

FSPL (dB) = 20Log10(d) + 20Log10(f) +32.44

Where:

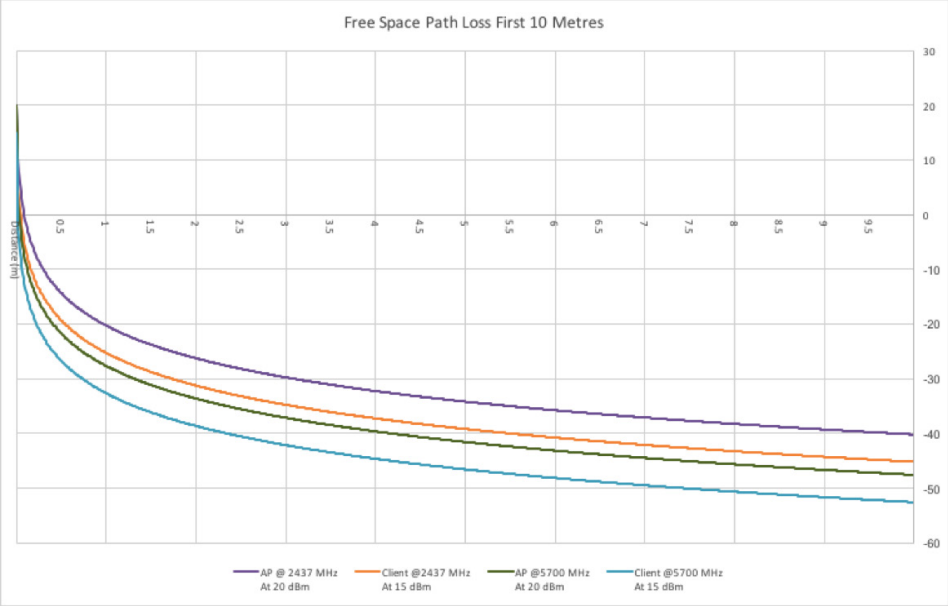
d is the distance in km between the receiver and transmitter and

f is the signal frequency in MHz

The chart shows a number of ideal world issues. The 2.4 GHz and 5 GHz radios, although starting at the same transmit power, after 5 m they have already diverged with the 5GHz still showing -41.5 dBm as opposed to the 2.4 GHz at -34.1 dBm. This is why site surveying for APs with dual radios can be a challenge.

What is also shown very clearly is the different power from the clients, and therefore the different range.

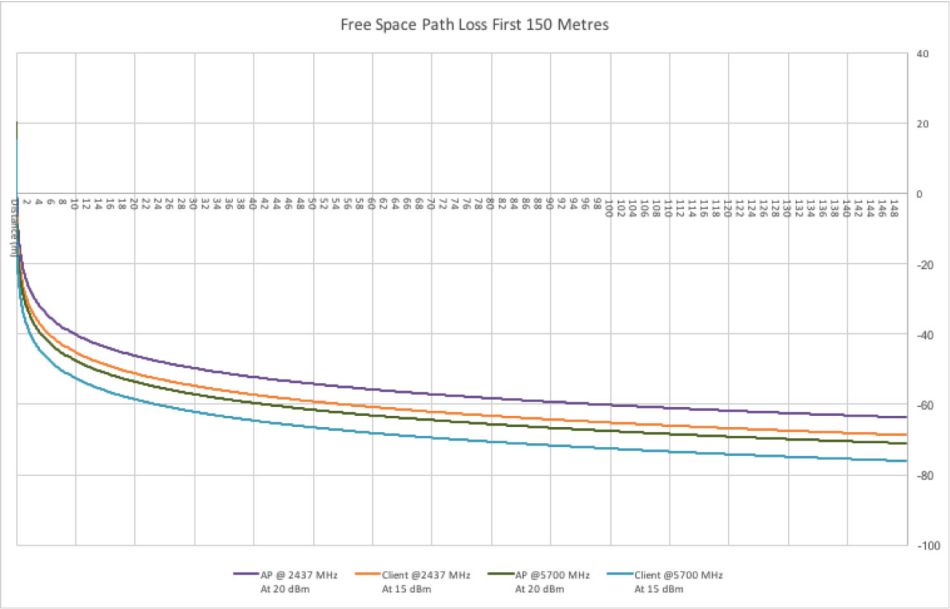
Consider over a longer distance.



The deltas (in dBm terms) start to remain constant as the distance increases, here showing the 2.4GHz AP at -40.1 dBm and the 5GHz AP at -47.5 dBm – a delta of 7.4 dBm. Bear in mind, an increase of 3 dBm doubles the power; this is a significant difference.

As the range increases, the signal strength reduces as one would expect. But the data rate at which the client and AP can communicate also has to change to deal with the reduced signal. So even at a range of 10 meters, the modulation rate may well have changed several times.

Longer range again:

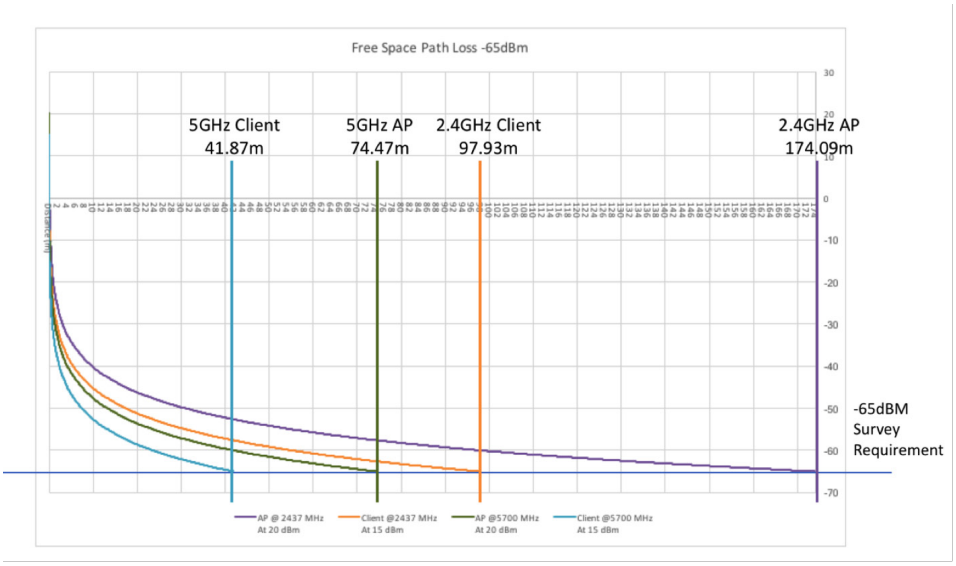


The 2.4GHz AP is at -63.6dBm and the 5GHz AP is at -71 dBm, maintaining the 7.4 dBm delta.

So, what does all this mean?

If you are planning a site survey for voice, a typical request would be for -65dBm coverage – which seems simple enough.

Referencing the graph above, however…



Making more (slightly extreme) assumptions that these are perfect radiators in 2 dimensions, this means:

2.4 GHz AP covers 95213.28 m2

5 GHz AP covers 17422.58 m2

So, a 300,000m2 warehouse needs 4 APs at 2.4 GHz or 18 APs at 5 GHz – just a 4.5x difference! This is one of the challenges that faces today's automated systems, and in some environments they are not able to deal with this kind of situation effectively.

CHANNEL PLANNING

In a SoHo environment, it is relatively simple to find a part of the spectrum that has some space available and automatically select a radio channel. But as the density of APs and users increases, then the available channels become a significant challenge.

The marketing speeds of wireless standards are always the maximum possible–which is not always practical. For example, 802.11ac Wave 2 supports 160 MHz channels to give astonishing speeds. Of course, to achieve these speeds you need phenomenal SNR and RSSI values, as shown below.

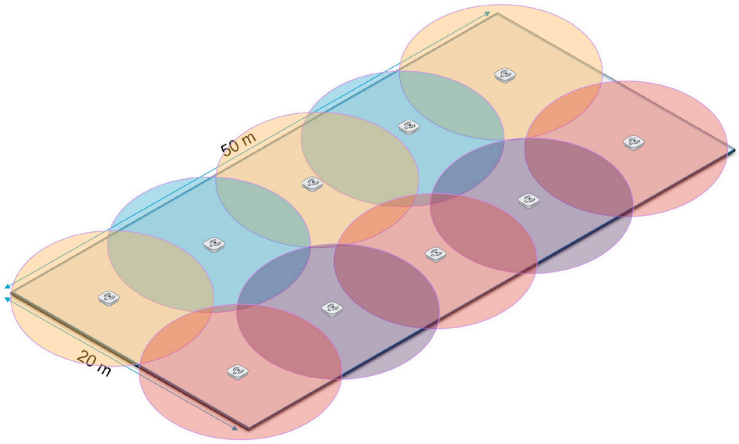
Modulation and coding schemes

MCS index[a]	Spatial Streams	Modulation type	Coding rate	Data rate (in Mbit/s)[8][b]							
				20 MHz channels		40 MHz channels		80 MHz channels		160 MHz channels	
				800 ns GI	400 ns GI	800 ns GI	400 ns GI	800 ns GI	400 ns GI	800 ns GI	400 ns GI
0	1	BPSK	1/2	6.5	7.2	13.5	15	29.3	32.5	58.5	65
1	1	QPSK	1/2	13	14.4	27	30	58.5	65	117	130
2	1	QPSK	3/4	19.5	21.7	40.5	45	87.8	97.5	175.5	195
3	1	16-QAM	1/2	26	28.9	54	60	117	130	234	260
4	1	16-QAM	3/4	39	43.3	81	90	175.5	195	351	390
5	1	64-QAM	2/3	52	57.8	108	120	234	260	468	520
6	1	64-QAM	3/4	58.5	65	121.5	135	263.3	292.5	526.5	585
7	1	64-QAM	5/6	65	72.2	135	150	292.5	325	585	650
8	1	256-QAM	3/4	78	86.7	162	180	351	390	702	780
9	1	256-QAM	5/6	N/A	N/A	180	200	390	433.3	780	866.7
0	2	BPSK	1/2	13	14.4	27	30	58.5	65	117	130
1	2	QPSK	1/2	26	28.9	54	60	117	130	234	260
2	2	QPSK	3/4	39	43.3	81	90	175.5	195	351	390
3	2	16-QAM	1/2	52	57.8	108	120	234	260	468	520
4	2	16-QAM	3/4	78	86.7	162	180	351	390	702	780
5	2	64-QAM	2/3	104	115.6	216	240	468	520	936	1040
6	2	64-QAM	3/4	117	130.3	243	270	526.5	585	1053	1170
7	2	64-QAM	5/6	130	144.4	270	300	585	650	1170	1300
8	2	256-QAM	3/4	156	173.3	324	360	702	780	1404	1560
9	2	256-QAM	5/6	N/A	N/A	360	400	780	866.7	1560	1733.4
0	3	BPSK	1/2	19.5	21.7	40.5	45	87.8	97.5	175.5	195
1	3	QPSK	1/2	39	43.3	81	90	175.5	195	351	390
2	3	QPSK	3/4	58.5	65	121.5	135	263.3	292.5	526.5	585
3	3	16-QAM	1/2	78	86.7	162	180	351	390	702	780
4	3	16-QAM	3/4	117	130	243	270	526.5	585	1053	1170
5	3	64-QAM	2/3	156	173.3	324	360	702	780	1404	1560
6	3	64-QAM	3/4	175.5	195	364.5	405	N/A	N/A	1579.5	1755
7	3	64-QAM	5/6	195	216.7	405	450	877.5	975	1755	1950
8	3	256-QAM	3/4	234	260	486	540	1053	1170	2106	2340
9	3	256-QAM	5/6	260	288.9	540	600	1170	1300	N/A	N/A

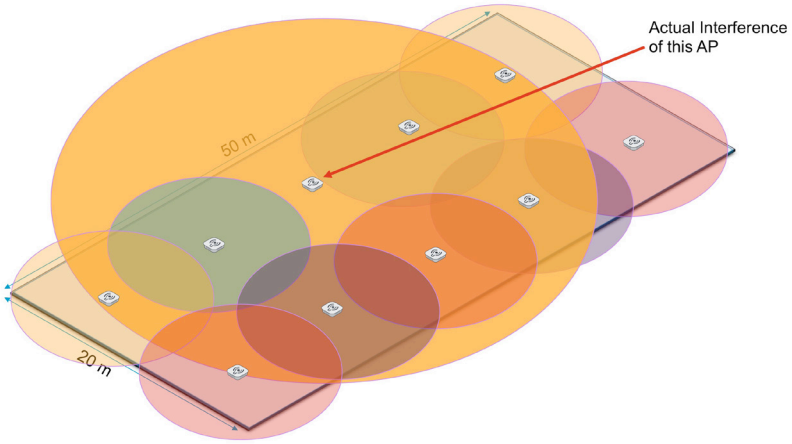
To obtain your golden 2,340 Mbps, you need a client that supports this configuration (note: there are no Wi-Fi certified clients as of today) and a very clean radio environment. In most homes today, 1,300 Mbps is achievable in the same room as the Wi-Fi router. In the enterprise space, however, things are a little different.

Planning has become more automated in simple deployments, relying on algorithms and automation between the APs to define a channel plan and power settings for the APs to minimize overlap. But this rarely takes into account client density, which has to be manually considered when looking at AP deployment decisions.

A typical wireless deployment in a dense environment may look like this:



As each color represents a different channel, this shows that a good channel plan has been deployed. The site survey would have specified -65dBm coverage and 80 MHz channels. The output power of the APs would be significantly reduced – the target coverage for the AP is around 8m – so even if the power is wound down to 1dBm, the coverage at lower data rates is still significantly more than the desired 8m.



This shows that as channel re-use increases, the co-channel interference becomes a real concern. Also bear in mind the above diagram considers only 2 dimensions. Within a building with multiple floors, the issue can be significantly worse.

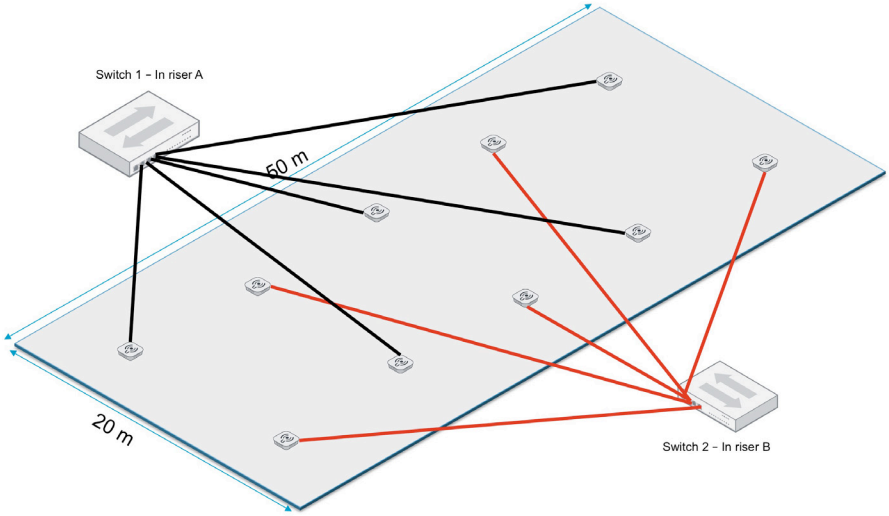
As shown in the diagram, three APs use the same channel and when any of those APs transmit (even at low power), that transmission is heard by the other APs. As each AP is responsible for its own clients, it must wait an uncertain length of time until the other APs stop talking before it can transmit. This lack of real-time coordination between APs is one of the main issues within a dense deployment. It is also worth noting that when a client transmits on this same channel, it may well be transmitting at its full power of 32 mW (15dBm), and so its interference pattern would be even greater still. If that client is mobile, then it may end up talking to one AP while directly under another on the same channel, dependent on its roaming capability.

For this reason, many enterprise deployments today use narrower channels (i.e., 40 MHz or even 20 MHz), which reduces the co-channel issue, as there are more channels available. But it also impacts the throughput of individual clients. 802.11ac Wave 2 allows for 160 MHz wide channels – but with only 2 channels available, the type of deployment shown above is not viable.

RESILIENCE

Wi-Fi has a great advantage over wired networks when it comes to resilience. If an AP fails, then as shown in the previous diagram, the neighboring APs have plenty of spare signal to go around. In most cases, the end users will not notice a single AP failure.

By either dual-homing the APs or simply wiring neighbors to resilient switches, almost any network issue can be mitigated by the wireless network. In the example below, if Switch1 failed completely, then half of the APs would still operate with reasonable service from Switch 2.



While this is a great feature and benefit of wireless, it comes with some issues. On the demo floor, several APs could fail and staff may notice their clients running a little slower. The issue is of course ensuring that all the equipment is working, not just on a power on level but at a detailed radio capability level. The management system of a wireless network needs to be proactive to ensure that critical environments remain operational at an optimal level.

INTERFERENCE

Wi-Fi operates in an ISM (Industry/Scientific/Medical) band and, as such, is license free. While this is good news, it also means that multiple other technologies also operate within the same bands. Most Wi-Fi solutions will show a signal quality which is basically a noise floor and interference indication. In order to formally mitigate the interference, it has to be understood. Fortinet's controller platform can utilize spectrum sensors and some APs to give a very detailed analysis of what is causing the interference. It also uses human readable reporting to identify the source of the interference, as well as the impact it is having on the APs.

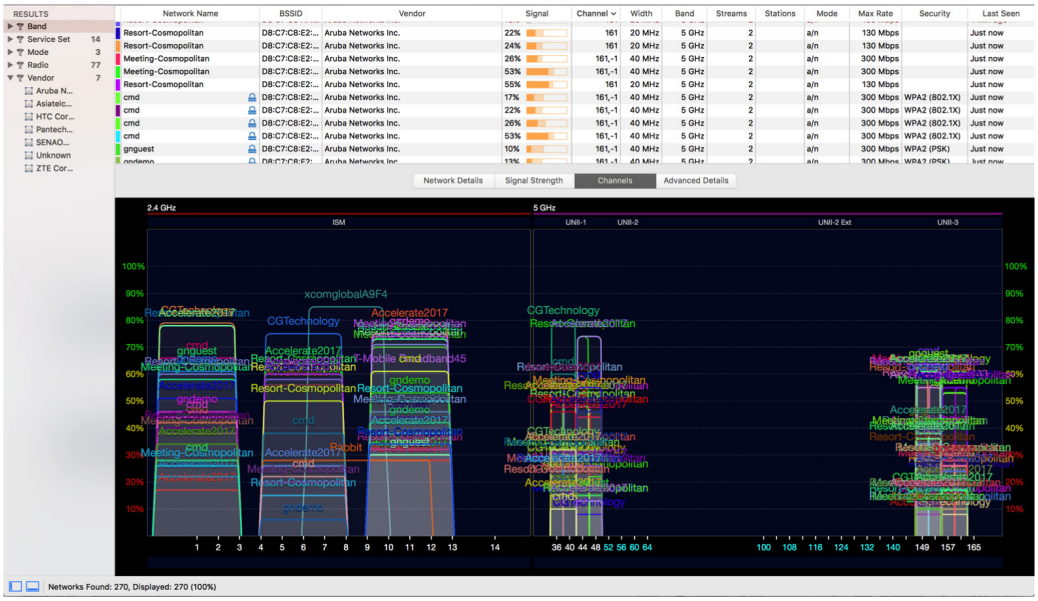
SO, DOES WI-FI WORK?

Absolutely. Wi-Fi clients and the APs are getting better and complying to more standards, which in turn improves overall performance. Wi-Fi is no longer the slowest link in the network; by some margin, the internet connection is the bottleneck. Consider a 'normal' office with 50 employees, each with a couple of connected devices. Add 4 APs and a standard internet connection of 100 Mbps. Even if the clients are basic 2x2 802.11n on 40 MHz channels, they are going to connect to the Wi-Fi at 270 or 300 Mbps (radio speed; actual speed is around 200 Mbps). Under these conditions, a single client could overload the internet connection. If clients have to resend transmissions 30- 50% of the time, the internet connection is still going to be the slowest part of the network. Generally, the internet is where clients want to go.

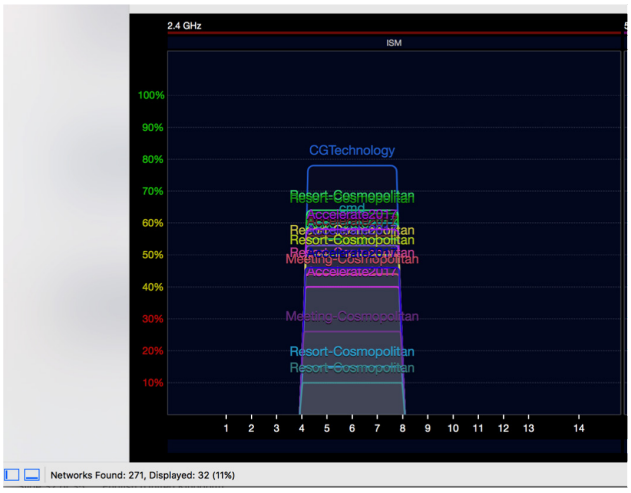
In hotels and public places, operators are very aware of the internet pipe issue and place per-client Wi-Fi restrictions of 1 or 2 Mbps, unless you pay a premium. Again, a connection of 300-1300 Mbps can deliver 1 or 2 Mbps with a huge retry rate. It does not mean it is a good way to deploy Wi-Fi, it just means it does what it needs to do.

HOW NOT TO DO IT

Below is a capture from a hotel--it does not matter which hotel or which Wi-Fi provider was used. This is a common view of most dense deployments today. The key point to understand here is the bottom left figure of 270 networks found. This scan was taken over 5 minutes while stationary in a corridor of the facility. The bottom graphic shows how congested the channels in use are. For whatever reason, they have decided to only use the non-DFS channels in the US, which does make the 5 GHz look a little busy.



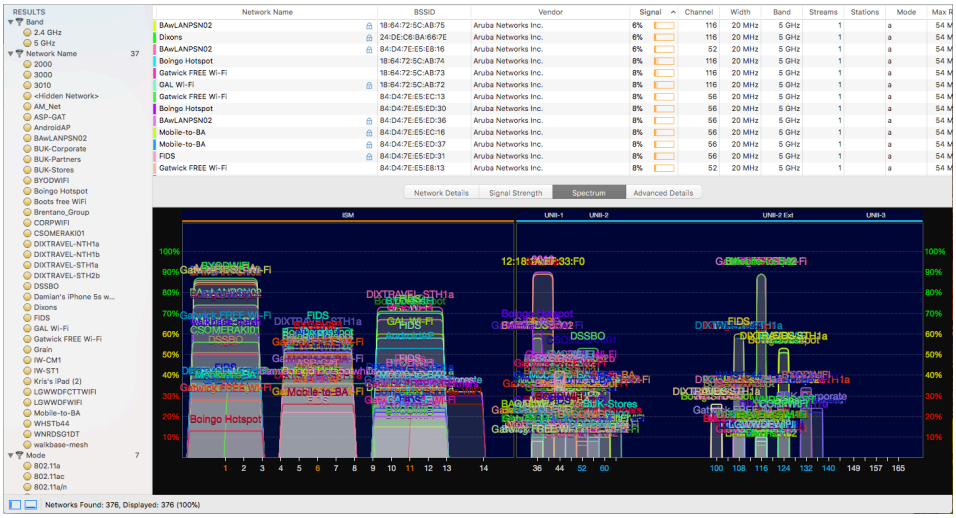
Just looking at one channel in the 2.4 GHz space:



Again, the key point is the displayed 32 networks. On this single, 2.4 GHz channel there are 32 different BSSIDs beaconing and trying to serve traffic.

Even with all of the above issues, annoyingly, the WiFi was ‘working’. We could all get Email and basic web access. But if the facility wanted to do anything intensive with the WiFi that would just not be an option.

Just to illustrate that this is not a one off, the same trace was taken at a large UK airport. Again, with the same idea of sitting in one location and passively listening to the air:



A total of 376 BSSIDs were visible from a single location.

Consider for a moment the client devices--how are they supposed to maintain a quality data connection and roam when they have to listen to 376 devices saying talk to me?

Once again, even in this melee, a Wi-Fi client was able to pass traffic. But the 1 Mbps limit imposed by the operator was probably not required with the noise and retries that were in progress.

WI-FI CONCLUSIONS

This section has focused on the worst of Wi-Fi in very difficult locations–but that is exactly when and where the Fortinet Controller solution can offer a completely different way to do Wi-Fi. In a large majority of installations, the number of APs and the automatic power and channel mechanisms of Fortinet's integrated and cloud-managed products work very well.

FORTINET'S CONTROLLER PLATFORM

INTRODUCTION

Like most controller-based solutions, the Fortinet Controller has been around for some years. It was originally developed by Meru to cope with Voice over Wireless in the days when clients were extremely poor, radio spectrum was scarce, and data rates were very low.

As speeds have increased and spectrum has extended with the 5 GHz band, the need for meticulous control of the radio environment receded. But now that speeds are using more and more of the 5 GHz spectrum in larger sections, there is a need in some cases to utilize an advanced solution, such as the Fortinet Controller.

VIRTUAL CELL

Virtual Cell is a key differentiator for the Fortinet Controller. The basic principle is to take control of both the air and clients to make decisions for the whole network from a central point of management. Most controllers today push configuration and software to the APs and manage channel planning and tunneling. The radio interface is left up to the APs. This is in contrast to Fortinet's approach.

In a standard AP, each Service Set IDentifier (SSID) it is asked to publish generates a unique Basic Service Set IDentifier (BSSID – basically a MAC address). In fact, if there are two radios (5GHz and 2.4GHz) and the AP will generate 2 BSSIDs, one for each radio.

A client requests all the SSIDs in the air and is then configured with a particular SSID (network name) to talk to. It then listens to all the APs publishing that SSID via the AP's BSSID, and when the client decides which AP it wants, it uses the BSSID to just talk to one radio of one AP.

In the examples shown earlier, some of the APs had been configured to publish seven different SSIDs on both radios, so each AP was publicizing 14 BBSIDs – which is why the number of BSSIDs can get out of hand very quickly.

When a client decides the signal on its current AP has degraded beyond use, it then probes for a better AP and initiates a roam. That roam is critical to voice and video services, as lost packets will be very evident. In a dense environment such as the office building we showed earlier, simply walking from one end of the office to the other for a coffee could make the Wi-Fi device roam four or five times.

The Virtual Cell concept changes this whole process. In each Virtual Cell, there could be anywhere from 10 to 500 APs, depending on the design criteria. All of the radios (typically two per AP) in the Virtual Cell operate on the same radio channel, and they all publish the same BSSID for any given SSID (per radio). This means that when a client looks for an SSID, it is only presented with one or two BSSIDs to choose from (most often one in the 5GHz range and one in the 2.4GHz range). The client makes the decision as to which of the two BSSIDs they wish to talk to (although the controller can even massage that decision if required) and associates to it.

The question, of course, is associates to what? The answer is the most appropriate AP radio, as defined by the controller. The controller is aware of all the APs and which ones can see one another. It is also aware of which APs are busy, so it tells the most appropriate AP to deal with this new client. If the client then moves and the AP radio is no longer the absolute best, then the controller simply tells the next AP radio to deal with the client. The client has no indication that anything has changed. It never asked to roam, and as far as it is concerned, it did not roam. The Virtual Cell changed the route of the traffic dynamically as the BSSID remains constant across all the radios.

HAPPY CLIENTS – HAPPY WI-FI

The Virtual Cell process of always keeping the best AP talking to the client on a packet-by-packet basis ensures the client can run

at its highest possible data rate – which also ensures that it spends as little time on the air as possible. This in turn means that there is space for other devices to talk. The client is always near to the AP, and so if it has the capability to reduce its transmit power then it can – which reduces interference and saves battery life for the client. This process has great advantages when considering clients that may not be at the premium end of the scale. Low-cost client devices with inferior drivers are designed for home networks and therefore are often poor at roaming. But in a Virtual Cell, it doesn't matter – they don't need to roam because the controller will take care of them. Internet of Things (IoT) devices will be the next influx of relatively dumb clients, and Virtual Cell will provide this unique benefit.

The client roaming decision is improved with new standards such as 802.11kvr—but as of today, most clients do not yet support this standard and a mixed environment can be difficult to manage.

SINGLE CHANNEL ARCHITECTURE – GOOD IDEA/BAD IDEA?

The obvious counterargument to Virtual Cell is that each one operates on a single channel and therefore must provide less throughput than lots of APs on different channels. So, is this the best approach to take? Well the answer is absolutely yes and definitely no – whichever you prefer. You can set up a test to categorically prove one is better than the other--it just depends on how you configure the test. Virtual Cell is one option on the controller platform. It can operate in Multi-Cell mode and be the same as the rest of the industry, but then apply Virtual Cell where appropriate. A single controller can operate some APs in Virtual Cell mode and others in Multi-Cell mode.

In general terms:

Radio Utilization

Multi-Cell APs suffer from co-channel interference when deployed with wide channels in a dense environment. In this configuration, the APs compete for the channel and as such do not use the radio spectrum efficiently.

Virtual Cell APs are all on the same channel. The controller ensures the clients are talking to the best AP and therefore at their highest data rate allowing the APs to make the best use of the radio Spectrum.

Client Roaming

Multi-Cell APs generate a lot of BSSIDs for clients to choose from, and by the design of the network, clients are expected to roam. Client roaming involves a lot of packets at the lowest data rate, which slows the overall network down. In order for clients to roam, they must also perform active and passive scans to look for better APs–all of which is time spent not sending useful data.

Virtual Cell clients always hear a strong signal and are therefore less likely to look for another AP, which means less active and passive scanning and more time to send data. Virtual Cell clients do not roam and so they can concentrate on sending data at the maximum rate. Virtual Cell APs can have the lower data rates completely disabled as they are not required.

Sticky Clients

Multi-Cell APs can cause clients to connect to the first AP they hear and then hang onto that AP, either because the driver is poorly written or because the client cannot hear a better AP for all the noise in the air. If a client does 'stick' to its first AP, it can drag the data rate of the link down to a very low level which slows the whole channel down.

Virtual Cell APs move the client to the best AP without the client's knowledge. This ensures the client device can always operate at the best data rate.

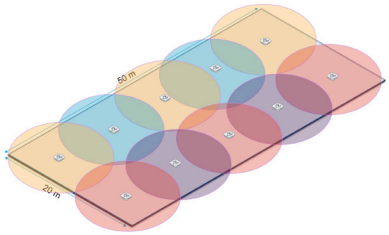
Summary

It is easy to dismiss Virtual Cell because it is unique—and if it were any good, everyone would be using it. There is a good reason why it is not widespread; it has taken years to develop to a successful product. There are no standards issues with Virtual Cell, there are no client specific drivers or conditions, and as a final check point the controller supports Multi-Cell as well if the environment does not require Virtual Cell.

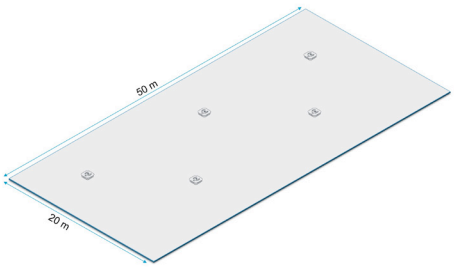
SINGLE CHANNEL? NOT EXACTLY…

It is true that a Virtual Cell requires a single channel, but that's not to say you can only have one Virtual Cell. In a Multi-Cell environment, every AP is expected to publish every wireless network—as there are not enough channels to have two sets of APs (one for public and one for private, for example). But with Virtual Cell, there are a lot more options, as only a single channel is required for each Virtual Cell.

Returning to the original sample design:

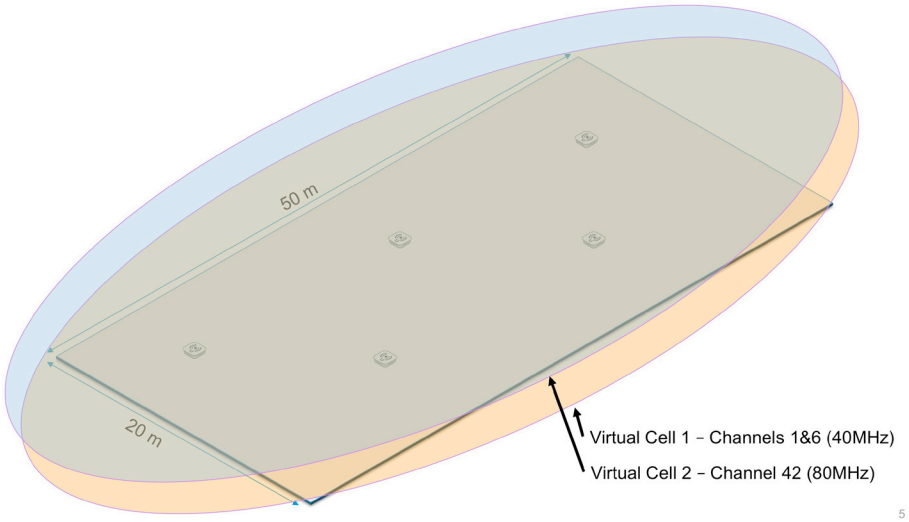


If we are considering all the APs on the same channel, then there is little point in placing them at the density shown for the Virtual Cell, as the laws of physics still apply and APs that are too close to each other cannot transmit at the same time on the same channel. With this in mind, let's place half the APs across the floor:



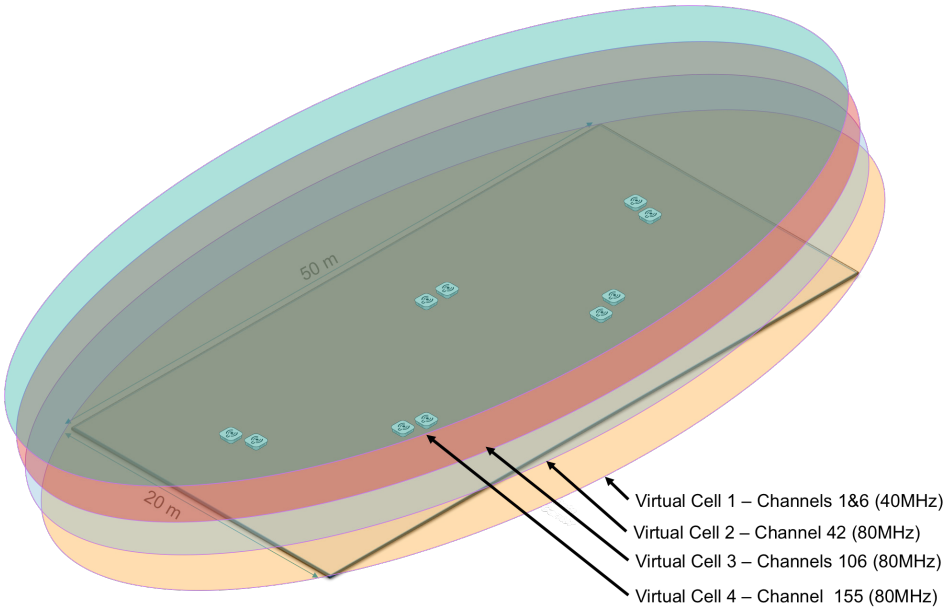
These five APs will provide more than enough coverage for the location. Each AP has two radios on board. For this first set of APs, one Virtual Cell will be on channel 1&6 (yes, we can bond channels at 2.4GHz as we don't need channel planning) and the second Virtual Cell will be on channel 42.

As can be seen here, we have the two Virtual Cells from the first five APs. The original design had 10 APs – so we can afford to add a second set of APs to add further Virtual Cells.



Now with four Virtual cells, we have a 240MHz band used in 5 GHz and 40 MHz used in 2.4 GHz and all of those bands are available everywhere with no roaming, as opposed to roaming from one 40MHz island to another every time you move.

But this is not the best part.



When a Multi-Cell AP offers two SSIDs, it publishes two BSSIDs as mentioned before–but the physical radio transmitter in the AP can only be one BSSID or the other. It cannot exist as both at the same time and so it cycles between all the BSSIDs in quick succession. So effectively, if four SSIDs are configured on a standard AP, each SSID only gets the radio for 25% of the time. Equally, if there is a guest client on an isolated SSID that is not obeying the QoS rules because it's a few years old and running at 6 Mbps because it's a long way from the AP and has not roamed correctly, that client will have an impact on the other SSIDs being published by the AP. The airtime that the poor client is wasting is not available for anyone else on your isolated 40 MHz island.

Consider now the same four SSIDs in the Virtual Cell world. Each Virtual Cell has a single SSID (it does not have to–it can have 16, the same as anything else–but this illustrates the point better). So, a VoIP client on Virtual Cell 2 and a guest client on Virtual Cell 3 have no impact on each other at all. The guest Virtual Cell can be running at 100% due to an exhibition running at that time, but the corporate systems have the same number of clients on their isolated Virtual Cell and get the same performance regardless of what is happening on the other Virtual Cells. It's as close to wireless switching as is possible today, providing real Wireless SLA capabilities.

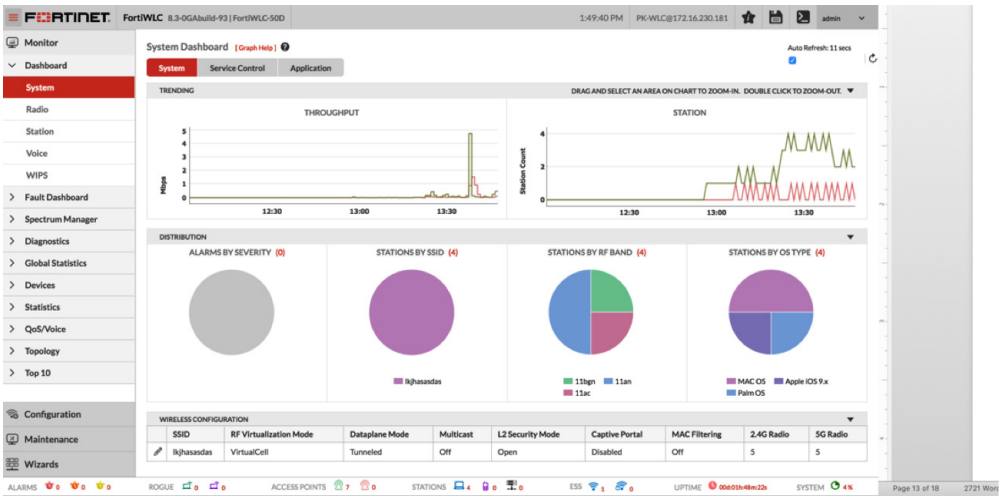
FORTIWLC–WIRELESS LAN CONTROLLER

OVERVIEW

The Wireless LAN Controller (WLC) is the brains of the wireless network, making real-time decisions about which AP should serve which client in the Virtual Cell mode, while also providing some management capability. The WLC can operate on its own or as part of a managed solution with FortiWLM (Wireless LAN Manager). The WLC is available in various sizes and forms, both virtual and physical. The WLC needs to be able to talk to the APs and the manager.

FORTIWLC GUI

In standalone mode, the GUI is a critical management tool and generally looks the same across the range. There are only a subset of the management functions to ensure there is significant benefit in procuring the WLM product.



Above you can see, the main system status provides a good overview of the current status of clients (stations) and access points. WLCs can be deployed in HA mode should resilience be required.

WIPS and Spectrum Analysis Management are available directly from the WLC, but also can be accessed from the WLM appliance so they will be covered there. There is no Service Assurance Manager in the WLC interface.

Each WLC is shipped with the maximum number of Access Point licenses enabled, apart from the virtual ones which have 50 APs enabled at installation. A one-off license is applied once the product is purchased.

FORTIWLM–WIRELESS LAN MANAGER

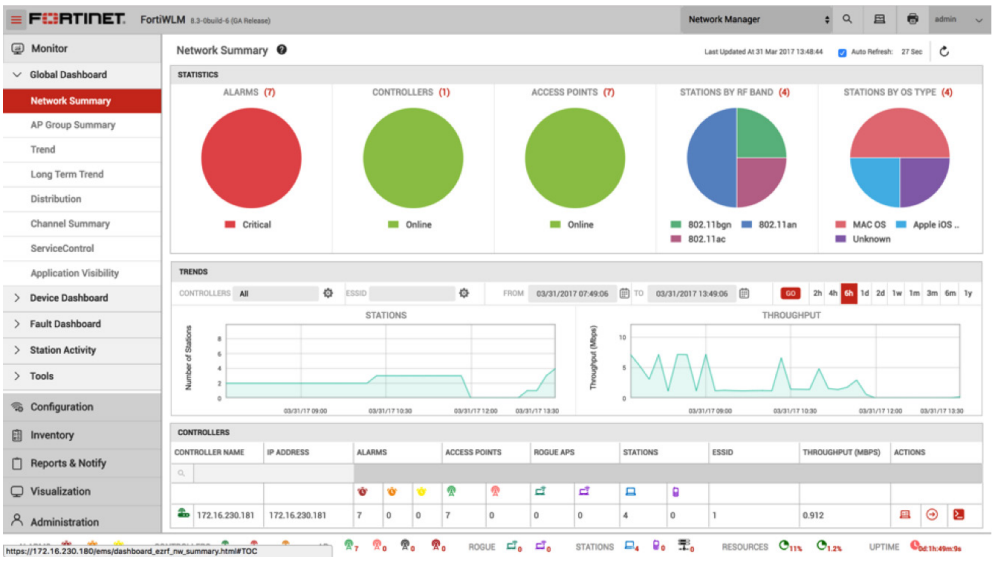
OVERVIEW

FortiWLM provides a full management and reporting platform for WLCs. It remains separate from mainstream Fortinet products, as the management information is very specific and it would be difficult to provide a consistent view. To return to the car analogy, the WLM is the steering wheel of the Formula 1 car, offering lots of extra controls and information that would be pointless if it were fitted to the family sedan.

A comprehensive API has been developed inside the WLM to allow the Fortinet Security Fabric to interrogate the WLM for extended visibility—but this is a project for a later release.

FORTIWLM GUI

The FortiWLM GUI aggregates multiple controllers into a single view as shown below:



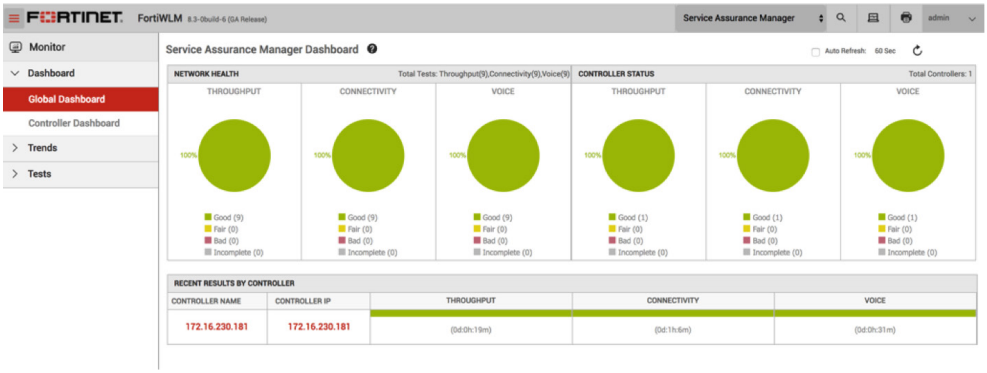
The data shown in the GUI above is identical to the information shown in the WLC on the previous page, so the similarities can be appreciated.

The key difference is history. The WLM can store a year of history for events such as client roams/probes/association requests, etc.—so when a client is reported as having an issue, its data can be scrutinized immediately and its current performance can be cross-referenced against a wealth of historical information.

SERVICE ASSURANCE MANAGER

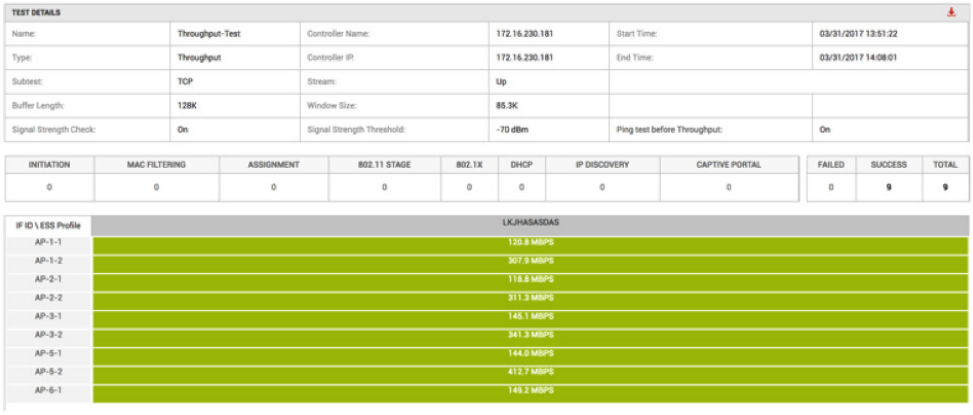
A key benefit of Virtual Cell is that APs have a very close relationship with their neighbors and can be used to validate their performance. Service Assurance Manager (SAM--a previously licensed feature which is now included) utilizes this neighbor relationship to perform a range of automated tests and provide alerts for issues that would be otherwise difficult to identify.

To take a real-world example, at the point of installation a baseline can be taken to measure the system's performance:



As would be expected, everything is well with the installation.

Various tests can now be run between the APs automatically to ensure that performance remains at a known level—for example an AP throughput test:



TEST DETAILS

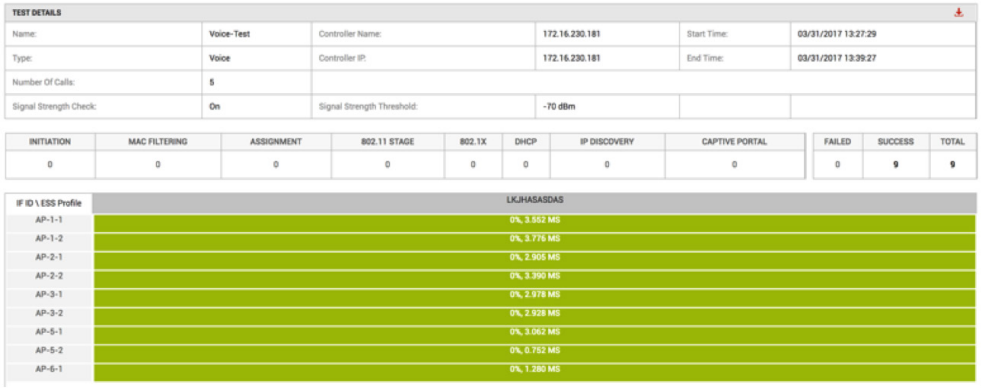
Name:	Throughput-Test	Controller Name:	172.16.230.181	Start Time:	03/31/2017 13:51:22
Type:	Throughput	Controller IP:	172.16.230.181	End Time:	03/31/2017 14:08:01
Subtest:	TCP	Stream:	Up		
Buffer Length:	128K	Window Size:	85.3K		
Signal Strength Check:	On	Signal Strength Threshold:	-70 dBm	Ping test before Throughput:	On

INITIATION	MAC FILTERING	ASSIGNMENT	802.11 STAGE	802.1X	DHCP	IP DISCOVERY	CAPTIVE PORTAL	FAILED	SUCCESS	TOTAL
0	0	0	0	0	0	0	0	0	9	9

IF ID \ ESS Profile	LKJHASASDAS
AP-1-1	120.8 MBPS
AP-1-2	307.9 MBPS
AP-2-1	118.8 MBPS
AP-2-2	311.3 MBPS
AP-3-1	145.1 MBPS
AP-3-2	341.3 MBPS
AP-5-1	144.0 MBPS
AP-5-2	412.7 MBPS
AP-6-1	149.2 MBPS

Above we can see the APs offering various throughputs as measured by their nearest neighbor, acting as a client.

A voice test can measure latency and packet loss in a similar fashion



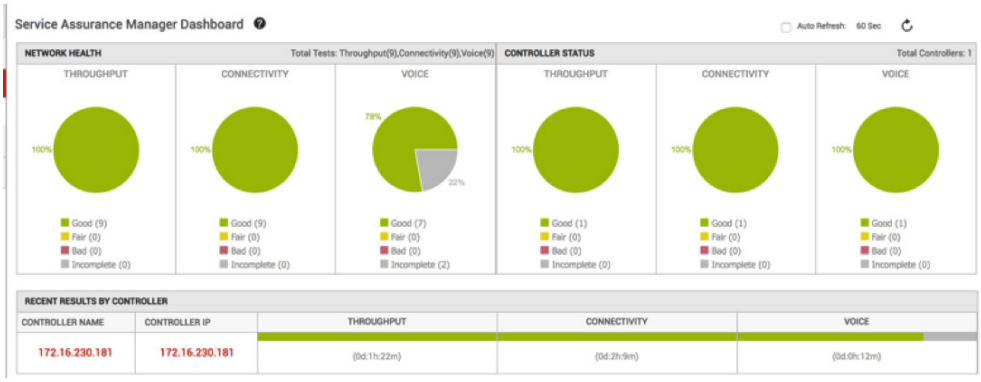
TEST DETAILS

Name:	Voice-Test	Controller Name:	172.16.230.181	Start Time:	03/31/2017 13:27:29
Type:	Voice	Controller IP:	172.16.230.181	End Time:	03/31/2017 13:39:27
Number Of Calls:	5				
Signal Strength Check:	On	Signal Strength Threshold:	-70 dBm		

INITIATION	MAC FILTERING	ASSIGNMENT	802.11 STAGE	802.1X	DHCP	IP DISCOVERY	CAPTIVE PORTAL	FAILED	SUCCESS	TOTAL
0	0	0	0	0	0	0	0	0	9	9

IF ID \ ESS Profile	LKJHASASDAS
AP-1-1	0%, 3.552 MS
AP-1-2	0%, 3.776 MS
AP-2-1	0%, 2.905 MS
AP-2-2	0%, 3.390 MS
AP-3-1	0%, 2.978 MS
AP-3-2	0%, 2.928 MS
AP-5-1	0%, 3.062 MS
AP-5-2	0%, 0.752 MS
AP-6-1	0%, 1.280 MS

So how does this help with fault finding? Consider a scenario where an AP is wall mounted and a large metal cupboard is placed directly in front of the AP. The AP is still connected to the network and is probably still servicing clients to some extent, but it is certain that the network coverage no longer matches the plan. To simulate this, the AP is placed in a metal trash can and the voice test immediately shows an issue:



The detailed test results show that two of the radios (both on the same AP) have a very poor signal to the neighbors:

TEST DETAILS

Name:	Voice-Constant	Controller Name:	172.16.230.181	Start Time:	03/31/2017 15:01:37
Type:	Voice	Controller IP:	172.16.230.181	End Time:	03/31/2017 15:11:14
Number Of Calls:	5				
Signal Strength Check:	On	Signal Strength Threshold:	-70 dBm		

INITIATION	MAC FILTERING	ASSIGNMENT	802.11 STAGE	802.1X	DHCP	IP DISCOVERY	CAPTIVE PORTAL	FAILED	SUCCESS	TOTAL
0	0	0	0	0	0	0	0	2	7	9

IF ID \ ESS Profile	LKJHASASDAS
AP-5-1	POOR SIGNAL
AP-5-2	POOR SIGNAL

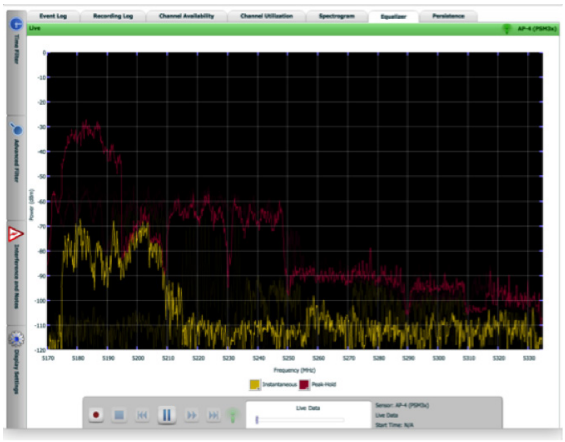
This automated test has quickly identified an issue and an email could have been sent to the network manager, even though no hardware has failed. These tests would pick-up up other anomalies such as damaged antennas or new walls being installed.

SPECTRUM ANALYSIS

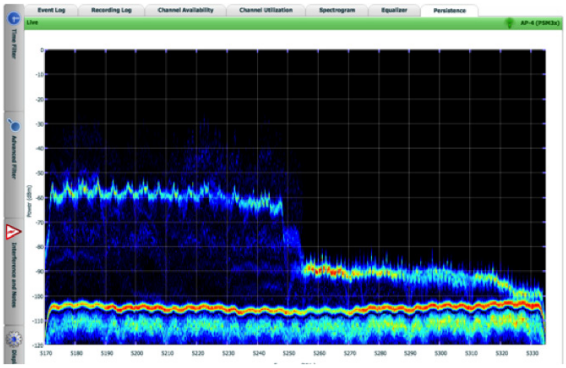
Wi-Fi operates in a shared band with many other technologies. In critical areas, understanding what is interfering can make problem resolution considerably easier.

A no cost option in both the WLC and WLM AP radios can be enabled as spectrum monitors or alternatively optimized spectrum analyzer APs, which can detect a much greater range of interference sources.

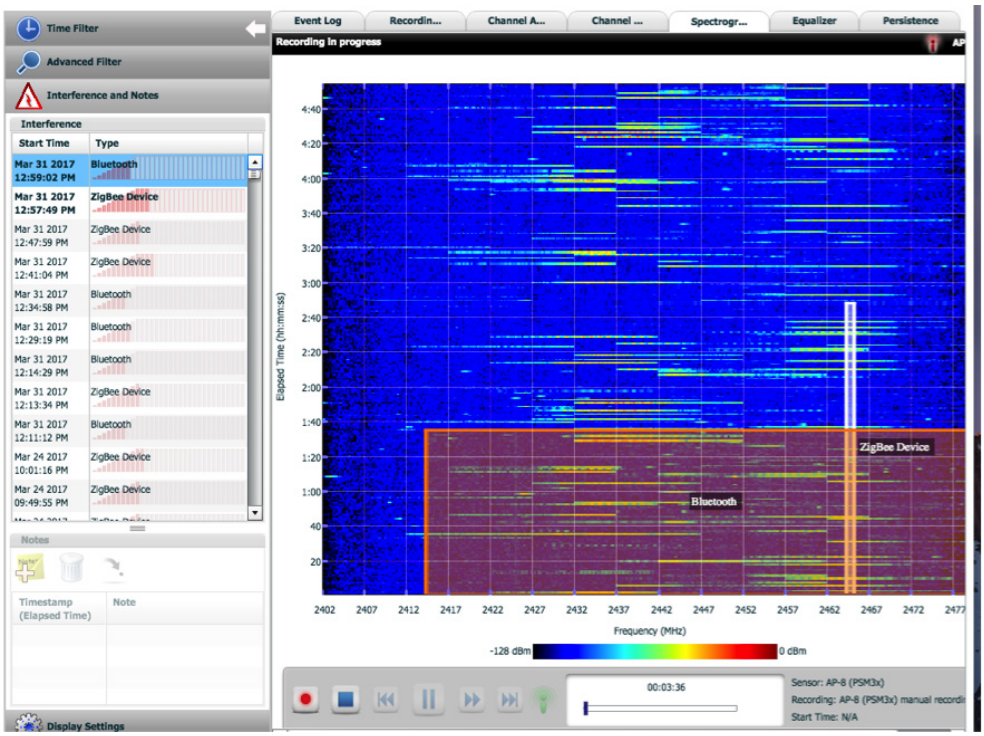
Below is a live view of the spectrum as a client operates on an 80 MHZ band:



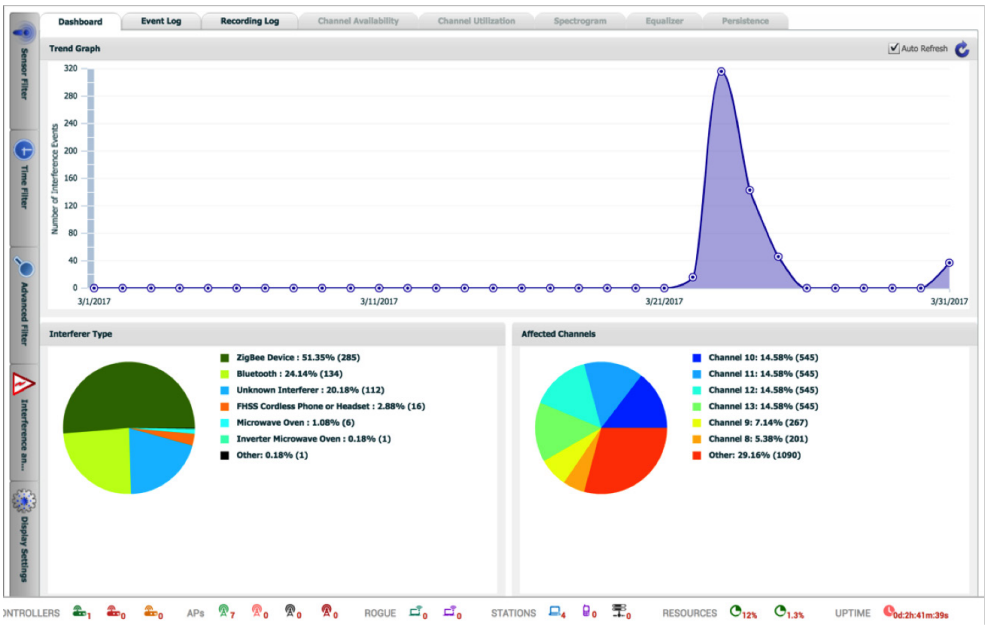
The system can also build a persistent picture of the signals to make them easier to read. See below for an example:



Looking now at the potential sources of interference, a live spectrogram can overlay the interference in real time, so the breadth and length of the interference can clearly be seen.



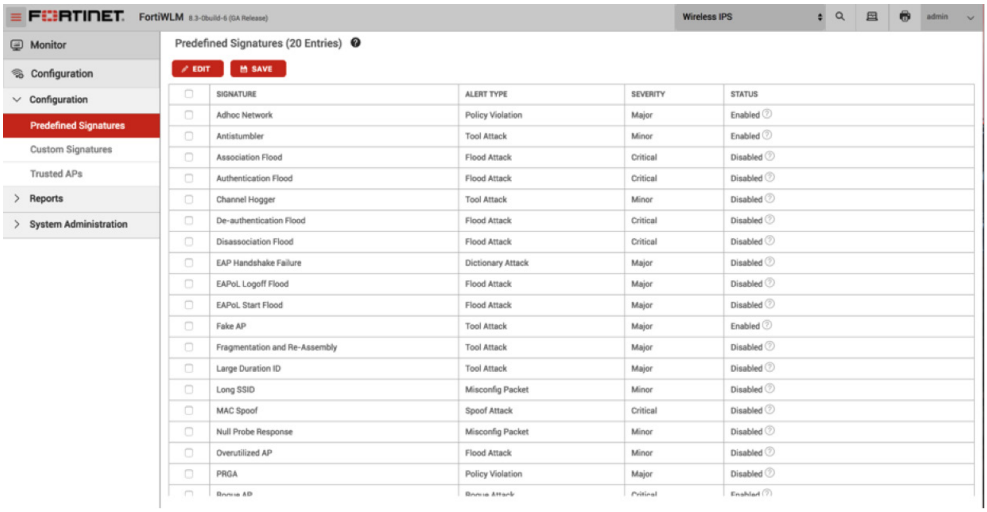
As the interference builds over time the Spectrum Manager can show the breakdown of interference sources in a number of different ways--as a list of events, graphically, or as an overall summary of the types of interference as shown below:



The above graphic shows the interference sources and also the channel utilization. More detail on the channels can also be shown in real time:

WIRELESS INTRUSION PROTECTION

The Fortinet Controller offers a full suite of WIPs with many built in signatures and the option to add new custom signatures if required.



OTHER FEATURES

FortiWLM & FortiWLC offer a full, enterprise-class solution. Features not detailed in this document include:

- Support for BLE (iBeacons)
- Hotspot 2.0 certification
- Integration with location vendors (it should be noted that any device inside a Virtual Cell can be rapidly located as every AP will hear that device as they are all on the same channel)
- PCI 3.0 Reporting
- Application visibility

CLOSING REMARKS

The Fortinet Controller solution is more complex than the plug and play solutions but it can deliver significant advantages where high performance is the requirement.

Some key applications to consider the Fortinet Virtual Cell include:

- Densely populated, mobile-focused environments where rapid roaming is required
- Large Stadiums
- Conference Centers
- Hotel Meeting Suites
- Exhibition Halls
- Universities/SLED

If the customer does not need the enhanced visibility that the controller and management platform provide, then a FortiGate and attached APs or FortiCloud may well be a better option.

If you need 100% of the performance that is possible with Wi-Fi, then the Fortinet Controller will deliver that.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

76757-B-0-EN **Oct 10, 2017**