Fast Lane
Consulting and Education Services Inc.

Intro to Enterprise Wi-Fi Troubleshooting

Chris Avants
Sr. Cisco Instructor
CCIE Wireless #45272

About this White Paper

To limit the scope of this White Paper, we will assume readers are currently or will soon be using a Cisco Unified Wireless Network with Cisco Light Weight APs, and Wireless LAN Controller in what is also referred to as a Split MAC design. This white-paper will be focused around the basics of troubleshooting Enterprise Wireless Networks (Wi-Fi), some of the most common issues seen in these environments, and common tools used to troubleshoot Wi-Fi.

October 2015

Background

Enterprise Wireless LAN’s, and Wi-Fi Troubleshooting hasn’t changed much in the last 15 years… Who am I kidding? Wi-Fi has become the number one network access medium for enterprises in the US and around the globe. Guest Access, BYOD, and IoE, IoT, trends are ensuring Wi-Fi and related Wireless technologies will continue to be the leader and some of these trends are in their infancy. While Wi-Fi technology has historically progressed slower than it’s wired Ethernet counterparts, Wi-Fi has seen a number of new enhancements in just the last 5 years allowing Wi-Fi speeds and security to rival that of it’s wired brother. Wi-Fi is now the first-choice for network access, which Enterprises rely on for day-to-day business. IT departments are charged with ensuring the Wi-Fi network can support increasing end user demands, and an increasing number of endpoints per user, while providing an optimal end-user experience.

Before we begin talking about Wi-Fi issues and troubleshooting, let’s ensure we’re on the same page about what modern Wi-Fi should be. Enterprise Wireless (Wi-Fi) today should be:

- Secure
- Allow simple on boarding of users, and devices
- Allow simple administration of users and network services
- Support Line of Business Applications
- Allow Seamless Mobility (moving around the enterprise)
- Provide a good end-user experience

NOTE: Line of business applications could be anything companies use for business operations and communications and may include Web/E-mail, to time sensitive applications like Voice, Video, Database Applications, Video Streaming and Location based applications.

Wifi Troubleshooting

Change in User Demands

1

Today’s workforce is mobile, there’s no two ways about it. Thanks once again to Apple and trends like IoT/IoE, users are now more connected than ever. By more connected I’m referring to more devices, where it’s common for a single user to easily have three different Wi-Fi connected devices and most likely twice as many wireless connections. Just about every device that has Wi-Fi also has two or more other Wireless technologies like Cellular, Bluetooth, NFC, IR, etc.

Let’s do some quick counting, a typical user has a smart phone, laptop, tablet, and possibly a wearable like Apple’s iWatch. Granted not everyone has come around to the iWatch yet, but that list has four Wi-Fi WLAN adapters and potentially eight to twelve other types of wireless connections we will discuss later, but you get the point.

Change in Applications

2

Line of Business applications used to refer to a few simple distinct categories, for example
Web/E-Mail, office productivity, which were not too time sensitive, and then collaboration applications like Voice and Video which were very time sensitive.

NOTE: Real-time applications like Voice (VoIP) and Video conferencing, video streaming, and collaboration apps etc., have network performance requirements which must be met to provide the end-user with a good experience while using these applications. A good end-user experience is the ultimate goal of any network architecture including Wi-Fi.

Before smartphones and softphones, specially designed Wi-Fi VoIP phones where the only way to make a phone call over a Wi-Fi network. Today the lines have been blurred between business applications, personal applications and, just as if not more important, time sensitive vs non time sensitive traffic. For example a typical smartphone provides web/e-mail access and office productivity (which is not time sensitive), while at the same time provide collaboration apps and features for interactive video streaming, video calls and of course voice calls.

If not considered early in the planning and design stages of the Wireless Network lifecycle, modern trends will create real challenges for admins and potentially poor end-user experiences. Wi-Fi is still at its heart a Half-Duplex Technology.

Wi-Fi 101 Review

3

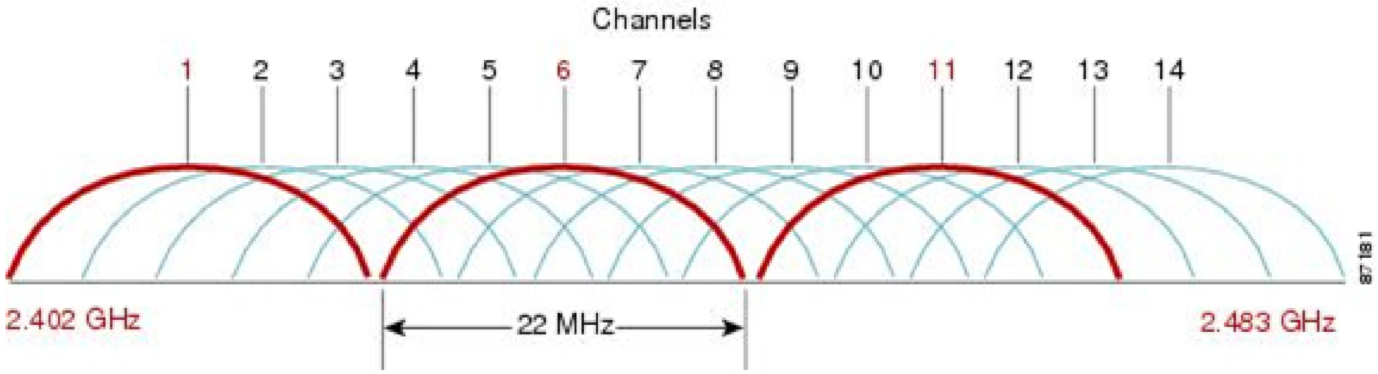
Wi-Fi is comprised of a suite of protocols, many of which are standards under the Institute of Electrical and Electronic Engineers (IEEE) 802.11 working group operating in two main “unlicensed” bands in the RF spectrum. The Federal Communications Commission (FCC) regulates the use of the RF spectrum in the U.S. and each country has its own regulatory authority.

Figure 101

Protocol	Band	Ratified	Speed	Modulation
802.11	2.4Ghz	1997	2mb	FHSS / DSSS
802.11b	2.4Ghz	1999	11mb	HR-DSSS
802.11g	2.4Ghz	2003	54mb	OFDM / DSSS
802.11a	5Ghz	1999	54mb	ERP-OFDM
802.11n	2.4Ghz or 5Ghz	2009	600mb	OFDM - HT
802.11ac w1	5Ghz	2014	7GB	OFDM - VHT

Figure 101 shows Wi-Fi standards beginning with 802.11, and is sorted and color coded by frequency range or band. Notice 802.11, 802.11b, and even 802.11g all operate in the 2.4 GHz Industrial Scientific and Medical unlicensed bands. The 2.4 GHz band is plagued by several issues, one of the primary issues is there are only three non-overlapping channels useable (1, 6, 11) in the U.S. (4 channels in some parts of the world). 802.11a and 802.11ac operate in the 5 GHz band only, where more real-estate "channels" for communication exist (20+ in the US). 802.11n is an odd-ball that can work in 2.4 GHz with some performance limitations (due to the limited number of channels), or can operate in 5GHz and reach more of its potential.

Figure 102



In figure 102 you can see the three non-overlapping channels in red. Each channel in the 2.4 GHz spectrum is 5 MHz wide, and 802.11b for example, uses a 22 MHz wide channel. Therefore channel 1 overlaps with 2, 3, 4, and 5. Using any of the other channels in blue means you would be overlapping with multiple other non-overlapping channels. For example, if you were to configure your AP to operate on channel 3, you would interfere with any Wireless stations (STA's) or APs operating on both channel 1 and channel 6. It is only in very rare instances such as some RFID location deployments which could require you to operate in channels other than 1, 6, or 11 in the ISM bands and should only be done with a vendor approved recommendation to do so. The rule of thumb is if you must use the 2.4 GHz spectrum today, use only channels 1, 6, or 11.

Figure 103

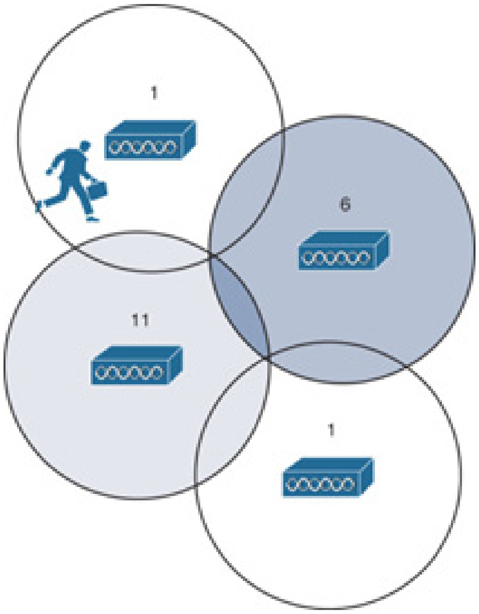
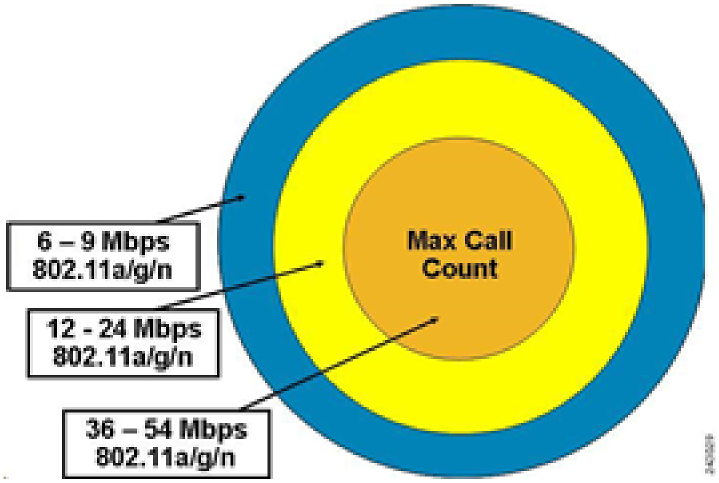


Figure 104



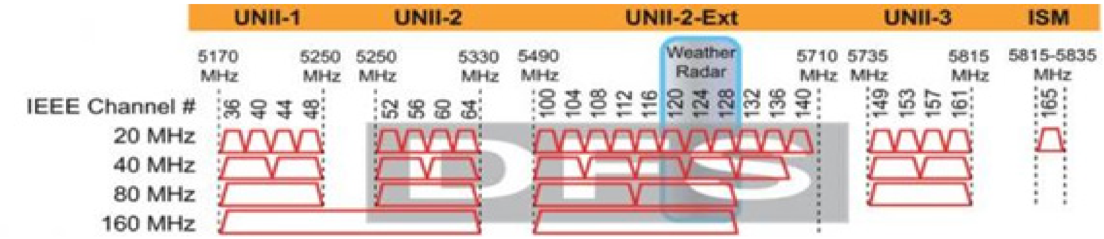
APs provide a coverage area called a cell (see figure 104). The coverage area provided by a single cell varies depending on regulatory domain, band, transmit power, and also the receiver's ability to hear the signal (WLAN client power). Unlike 802.3 based Ethernet networks, 802.11 allows for Dynamic Rate shifting so the closer you are to the center of the cell the better rate you can achieve, but as you move further away your client will not hear the signal as well and may have to use simpler coding schemes, which equal a slower connection (see figure 104 blue area) until you ideally roam to a cell with better performance, or roam outside of the coverage area until no signal is heard at which point you are disconnected.

Enterprise deployments provide coverage by placing APs in a way so there is cell overlap from APs operating on different (adjacent) channels, which allows users to roam from cell to cell, ideally without losing connectivity (see figure 103). The amount of overlap depends on the type of deployment, environment or other factors, but when APs hear other APs operating on the same channel it's known as Co-Channel Interference (CCI) and too much CCI is problematic for Wi-Fi and can lead to a poor user experience.

The 5GHz spectrum is comprised of several Unlicensed National Information Infrastructure bands which are collectively and commonly referred to as UNII bands. 5 GHz offers much more real-estate for Wi-Fi than the ISM band does, with over 20 channels available in the US, and even more available in other countries.

Without question, the 5GHz spectrum is what all Enterprises with mission critical Wi-Fi in the U.S. should be using.

Figure 105



802.11n / 802.11ac

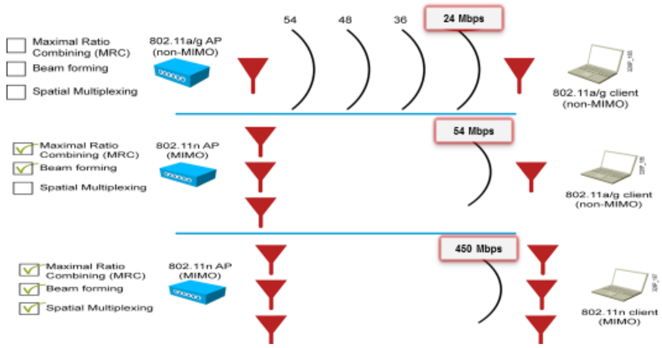
4

In 2009 Wi-Fi took a huge step forward with the release of 802.11n. Until 802.11n everything in Wi-Fi was Single-In, Single-Out communication (SISO). 802.11n brought with it many new features, and theoretical PHY speeds of 600mb although most vendor deployments support PHY speeds up to 450Mbs. 802.11n uses multiple-input multiple-output (MIMO) and 40Mhz wide channels at the physical (PHY) layer, and frame aggregation at the MAC layer to achieve these faster speeds. Although it's possible to bond channels in the 2.4GHz ISM band, it would consume over 80% of the available bandwidth and is un-realistic in any urban areas.

Where 802.11n really shines is in the 5GHz spectrum where there is enough channels to bond and still produce good designs without excessive CCI. Even bonding to 40 MHz wide channels with 802.11n, would leave you with over 10 unique channels to design your RF environment. 802.11ac builds off of the techniques developed with 802.11n including channel bonding, where 802.11ac supports channel bonding of, 40Mhz, 60 MHz, 80 MHz, and 160 MHz wide channels. 802.11ac is 5 GHz only, as there is simply not the real-estate (channels) available in 2.4GHz to bond and reach these higher PHY speeds. Most Enterprises today implement 802.11n and 802.11ac not just for the faster speeds, but for their ability to improve performance for non 802.11n/ac clients as well. 802.11n/ac offer several features to increase non 802.11n/ac Wi-Fi client performance by as much as 40% thanks to techniques like Transmit Beam Forming (TBF), Maximal ratio combining (MRC) and spatial multiplexing.

In reference figure 106 the top AP is non MIMO (802.11n), and the client is non MIMO, and is able to connect at 24Mbs. The second example is an 802.11n AP with 3SS, communicating with a non 802.11n client at over double the performance (54MBs) thanks to MRC and Beamforming. Finally in the bottom example, you have an 802.11n AP and 802.11n client operating in 5GHz at 450Mbs. Of course this is just an example of how using 802.11n capable APs provide much more value than these theoretical peak PHY data rates.

Figure 106

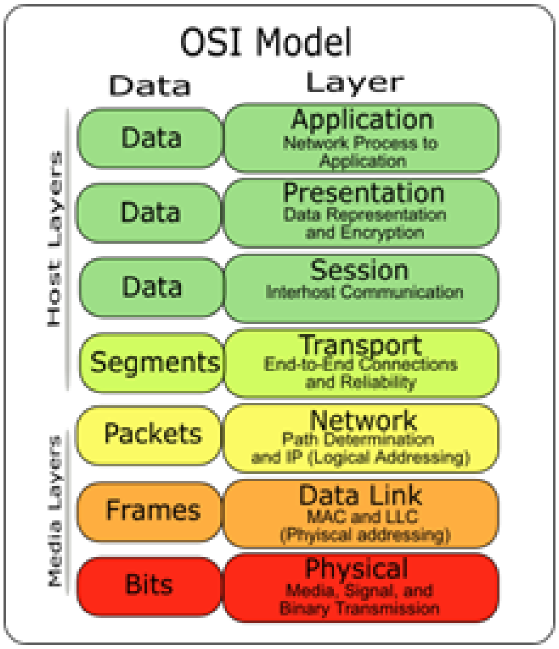


Wifi Troubleshooting Strategies

There are several strategies for troubleshooting networks today which can save valuable time, provide consistent results and provide faster problem resolutions with incidents if followed correctly. Several methodologies are based on using a Layered Approach. A layered approach refers to systematically testing network connectivity alongside the Open Systems Interconnect (OSI) model.

Note: While we are providing a reference to the OSI here, this white paper assumes you are aware of the OSI model as well as the 4 layer TCP/IP model which is a separate model on the mechanics of IPv4. If you are not familiar with the OSI or TCP/IP models, we recommend attending a CCNA R/S course such as ICND1 and ICND2 or CCNAX.

Figure 107


OSI Model
Data
Layer
Host Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation and Encryption
Data
Session
Interhost Communication
Segments
Transport
End-to-End Connections and Reliability
Media Layers
Packets
Network
Path Determination and IP (Logical Addressing)
Frames
Data Link
MAC and LLC (Phyiscal addressing)
Bits
Physical
Media, Signal, and Binary Transmission

Troubleshooting Strategies

1. Bottom Up – refers to testing each layer of connectivity using the OSI model as a reference beginning at the bottom.

2. Top Down – refers to testing each layer of connectivity beginning at the top, Application Layer.

3. Shoot from the Hip – refers to using your instinct to choose a layer in the middle to start with, for example an ICMP Echo or PING at Layer 3. If your host can ping a remote host using the correct source and destination ports, you can assume network reachability is not the issue and to look at upper layers beginning at Layer 4. Now if the ping fails, you realize there is likely a network issue, and you can begin troubleshooting layer 3 (network layer) and below until the problem is identified.

Adopting a troubleshooting strategy like the layered approach above is considered best practice, provides a methodical approach to Troubleshooting Wireless Networks and avoids jumping to conclusions and wasting time.

Using a Layered Approach for basic Wi-Fi Troubleshooting

1 While the OSI and TCP/IP models can be used in troubleshooting networks across any type of medium, Wi-Fi has some special considerations. First of all it's important to understand Wi-Fi (802.11) is a network transport medium, which operates at layer 1 (Physical) and 2 (Data Link, aka MAC) of the OSI model. Past the Wi-Fi operation at L1, and L2 the Network layer (IPv4/IPv6) operates at Layer3 of the OSI, which we will also be touching in the series, but it's important to remember Wi-Fi itself operates at Layer 1 and Layer 2 only, although most wireless engineers are expected to know and troubleshoot issues through layer 7. For the purpose of this paper, we will use the bottom up approach for troubleshooting below.

Layer 1 (OSI - Physical) has 2 sub layers with Wi-Fi, the Physical Layer Convergence Procedure (PLCP), and Physical Medium Dependent (PMD). The PLCP role adds a preamble and PHY header to the transmission. Transmitted in 1's and 0's sent on the channel to indicate a pending frame and synchronize radios that communication is about to take place. The PMD layer uses coding techniques like CCK, BPSK, QPSK, QAM, and many others which are algorithms to use as many bits as possible in a transmission.. The PMD layer uses modulation techniques (DSSS, OFDM, etc.) to deliver coded bits. When any RF is heard by a client's WLAN adapter that cannot be processed by a modulation and coding schemes (MCS) above, the adapter considers it noise. The only way to view Wi-Fi at Layer 1 is to use a Spectrum Analyzer, which will be discussed later.

Layer 2 (OSI - Data Link) also has 2 sub layers with Wi-Fi, Logical Link Control (LLC), and Mac Access Control (MAC). The MAC layer aka Mac Protocol Data Unit (MPDU) adds the mac addresses. In Wi-Fi there are 4 MAC addresses: Source Address (SA), Destination Address (DA), Transmitter Address (TA), and Receiver Address (RA). The LLC layer communicates with the upper layers via a Mac Service Data Unit (MSDU) which includes all the information from the upper layers 3-7. When troubleshooting Wi-Fi at Layer 2, you need WLAN adapters or APs that can operate in Monitor mode to capture 802.11 frames. Wi-Fi/802.11 frame capture tools will be discussed later.

Layer 3 (OSI - Network) the network layer is where IPv4/IPv6 comes in, and where many pain points /trouble tickets can come from, but it's important to remember issues at this layer are no longer part of Wi-Fi itself, and have become a general network issue. There are many ways to troubleshoot Layer 3 issues, some of which will be discussed later in the series.

Let's look at using a layered approach.

Bottom Up Approach – Starting with Layer 1

2

In the OSI model Layer 1 deals with the “media” and binary transmission of data. With wired 802.3 based Ethernet networks, a Layer1 issue typically means you need to check the cable. Wi-Fi has no cables of course, but there is transmission via Radio Frequencies (RF), described above, so verifying Layer 1 connectivity could involve things like ensuring the WLAN adapter is installed and enabled? If its dual-band that the correct band or both bands are enabled that the AP is using? After the WLAN adapter is verified as functioning, the question becomes can I see the Wireless LAN’s Service Set ID (SSID) I need to connect to?

If you see other Wi-Fi networks available, but not the SSID/WLAN you are looking for, you need to ensure you are within range of an Access Point (AP) advertising the SSID you’re looking for. If you know you’re within range, and you’re still not seeing the correct SSID the WLAN could be hidden or may not be advertised by the Access Point (AP) or Wireless LAN Controller (WLC) and you should check the controller for those settings.

Terminology Review

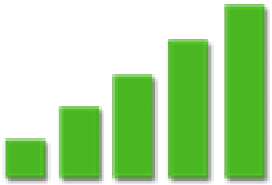
•**RSSI** – Received Signal Strength Indicator – Measured in dBm decibels/milliwatt, values are measured in a negative where -0 would be a theoretical perfect. One rule of thumb for RSSI measurements are typically -40dBm through -67dBm is a good signal, -68 through -75 is useable for web/email and anything below that is considered a poor connection.

•**Noise** – Any signal received by the adapter, which is not understood.

•**SNR** – Signal to Noise Ratio

One of the challenges with standard WLAN adapters and Operating Systems is that they don’t allow you to see a true numerical representation of the actual RF. Most OS vendors have adopted the “bars” strategy (see figure 108) to simplify users understanding of how good the connection is. Many vendors use their own formulas and algorithms based on Received Signal Strength Indicator (RSSI) where 4 bars is good, 1 bar is bad, etc., but a problem with using RSSI only, is it is only part of the story of how good your connection is. The other major factor is noise. Noise is any RF heard by the WLAN adapter which it cannot understand and modulate. An easy example of noise we can use is microwave ovens which operate in the 2.4 GHz ISM band with Wi-Fi, but would be considered noise as Microwaves are not talking Wi-Fi. An indication you may have a lot of non-802.11 interferers on your network would be a high noise floor, or low Signal to Noise Ratio (SNR). SNR is another key value, which tells you the audible good signal strength RSSI compared to the bad noise. You can think of SNR as having a conversation with someone in a crowded room. If the noise is too loud, you may have to repeat parts of your conversation. The higher the Signal to Noise Ratio (SNR), the better.

Figure 108



When designing Wi-Fi for voice (VoIP) devices, a common design rule of thumb is to have an RSSI of -67dBm at the cell edge with an SNR of 25dB which is said to allow the client to offer the best performance for voice and video deployments, (max rate RSSI's do vary for different technologies) however RSSI is not the only part of this equation. If you have a good RSSI while having too much interference or noise, your device may not be able to communicate at the fastest data rate, and will attempt transmitting at lower data rates if no acknowledgements are received which is called Dynamic Rate Shifting (DRS). Rate shifting down to a slower supported MCS/ data-rate can allow clients to remain connected even at different distances from the AP, until the signal is too weak for the client to identify as Wi-Fi. Ideally clients should roam before rate shifting down to undesirable speeds, or network performance could be impacted.

AP/Client Power Mismatches

Another thing which can cause issues at Layer 1 is power mismatches between AP and clients. APs can have transmit powers of 23dBm or more but varies depending on regulatory domain and channel. Mobile device vendors have been constantly struggling to find the best balance between portability, battery life, and performance. Unfortunately these super portable, battery powered devices like smartphones and tablets just can't keep up. In fact many smartphones have Effective Isotropic Radiated Power (EIRP) values of 10 – 14dBm depending on channel and regulatory domain. To put this in prospective, a +/-3dBm difference equates to double the power (+), or 50% reduction in power (-).

What this means is the client may see a great RSSI from the AP, but the AP may not be able to hear the client as well. In these cases clients may attempt transmitting at the best data-rate, and retry until the AP can understand the client. If you have a BYOD deployment, and Wi-Fi packet captures show this is a common occurrence, AP power should be lowered to the power level of the worst client your organization supports. This is one of those issues that should ideally be discussed before APs are deployed, as reducing AP to these levels can change coverage areas and may require more APs. Put simply you must consider the WLAN client capabilities during network planning and design phases. Otherwise you may be spending extra money on moves, ads, and changes if discovered after the fact.

We have learned the key values (RSSI, Noise, and SNR) are used to determine if our connection is good, or maybe experiencing issues. Now where can we find them on our clients when we need to verify these values? That's one of the downfalls with Wi-Fi currently, as mentioned earlier most Operating Systems vendors only show you bars, which is the vendors own algorithm for what a good connection is, and unfortunately the algorithms used can differ from vendor to vendor.

Although there are several tools and Wi-Fi survey utilities which can be installed to show you these values (RSSI, Noise, SNR), there is only 1 type which can help identify the source of noise, which is a Spectrum Analyzer.

Noise and Non-802.11 Interferers

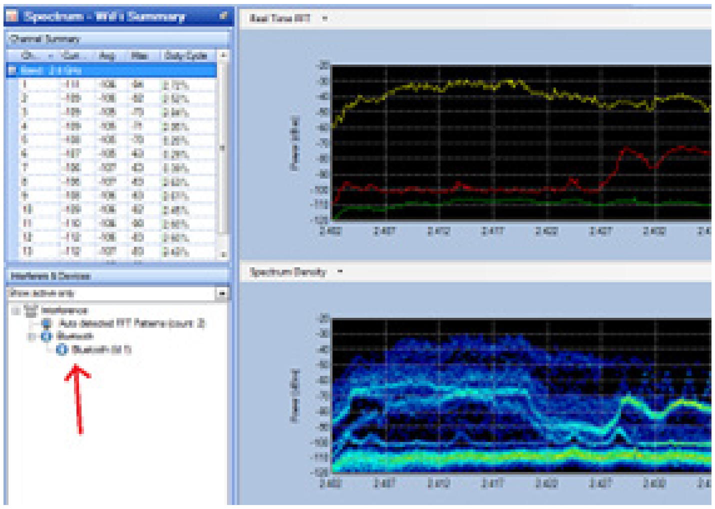
As Wi-Fi operates in the unlicensed spectrums, there are many devices, which can interfere with your wireless connections including:

- Microwaves
- Bluetooth
- Zigbee
- Dect Phones
- Video Cameras
- Invalid Channels
- Inverted Channels

One of the issues with problems caused by non-802.11 interferes is that they are difficult to identify if you don't have the proper tools. As discussed earlier, WLAN adapters are "tuned" to transmit and receive signals which conform to 802.11 standards, and look at any other audible non-conforming RF as noise. The only way to identify non-802.11 interference sources is with a Spectrum Analyzer. Spectrum Analyzers are devices which are focused 100% on listening to the RF in a particular band, and reporting on the signals heard for a specific band the device is designed for such as 2.4GHz or 5GHz.

Good Spectrum Analyzers designed for Wi-Fi will also attempt to identify any 802.11 interference sources by name. There are many spectrum analyzers on the market today geared towards Wi-Fi troubleshooting, some of my favorites are Fluke Networks AirMagnet Spectrum XT software with AirMagnet Spectrum XT USB adapter, and MetaGeek Chanalyzer Pro with Meta Geek's Wi-Spy dBx adapter. Below is an example I ran which identified Bluetooth from my cell phone to illustrate some of the features Spectrum Analysis tools provide. Notice we get a real-time view of the RF spectrum, in this case 2.4GHz ISM band, with time lapsed channel utilization and performance details, as well as identification of the non-802.11 device by name "Bluetooth".

AirMagnet Spectrum XT



Spectrum - WiFi Summary

Channel Summary

Ch.	Cur.	Avg.	Max	Duty Cycle
Band: 2.4 GHz				
1	-111	-106	-64	2.72%
2	-109	-106	-62	2.52%
3	-109	-106	-75	2.44%
4	-109	-105	-71	2.28%
5	-108	-105	-70	2.20%
6	-107	-105	-43	2.29%
7	-106	-107	-43	2.36%
8	-106	-107	-43	2.62%
9	-108	-106	-43	2.67%
10	-109	-106	-42	2.48%
11	-110	-106	-90	2.60%
12	-112	-106	-43	2.60%
13	-112	-107	-43	2.43%

Interferers & Devices

Show active only

Interference
Auto detected FFT Patterns (count: 2)
Bluetooth
Bluetooth (id 1)

Non-Standard Channels/ Invalid Channels

If after performing any survey you find APs operating on non-standard channels in the 2.4GHz ISM band you should change the configuration on the AP/WLC to use the proper bands, or remove the device from the network. If the AP is found to be a neighbors AP, you should make the request they do the same. In multi-tenant environments you will no doubt have situations where neighbors will also be using Wi-Fi, and these areas would be essentially shared air space, especially problematic for 2.4GHz with limited channels. If you must support 2.4GHz ISM it's much better that everyone use the standard non-overlapping channels (1, 6, and 11) to limit channel overlap interference as it only adds to the problem. Once again the ideal solution is to use the less crowded 5GHz spectrum, I've seen enterprises with major noisy neighbor issues essentially disappear after ensuring their clients are operating on the 5GHz spectrum. (See dual band clients below). Invalid channels can come from non-802.11 devices,

Bottom Up Approach – Looking at Layer 2

3

After you have verified things discussed with Layer 1, that the adapters are enabled and SSIDs are seen for the networks you want to join, the next step is to look at Layer 2. While there are many issues that could develop at this layer, some of the more common issues arising from Layer 2 is supported technology, sticky clients, supported data-rates, and security issues so we will focus on these.

Technology Review:

- **802.11 Frame Types** – 3 Types (Management, Control, Data)
- **Management Frames** – Beacon, Probe Request, Probe Response, Authentication Request, Authentication Response, Association Request, Association Response.
- **Control Frames** – Request to Send (RTS), Clear to Send (CTS), Power-Save Poll (PS-Poll)
- **Data Frames –** Data being transmitted

Supported Technology

This concept is super easy to grasp, your AP and client must be able to speak the same language i.e. 802.11a, 802.11b, 802.11g, 802.11n etc. Most client adapter's software attempts to make them dynamic in nature (to provide the best user experience), but let's say your client was set to 802.11b only for some reason and you have implemented best practices which was to disable 802.11b and 802.11b data rates of 1mb, 2mb, 5.5mb, and 11mb. Then any 802.11b clients would not see the network at all, and would not be able to communicate on it which is actually an ideal scenario, but you get the point. The reason you want to disable 802.11b is 802.11b clients degrade the performance of an 802.11g cell by as much as 30%, as 802.11g clients use backward compatibility, legacy techniques to co-operate in the cell. The take away here is protocols must be enabled on both the client and adapter to function, so checking the WLC/AP settings and WLAN client settings would be a logical step here.

Sticky Clients

This is a fun issue to this very day. When clients join a cell/AP, and the user moves within better range of a better AP but the client tries to remain connected to the original AP it's referred to as a sticky client. Ideally clients would join APs with best signal strength and least loaded, but some wLAN client vendors algorithms are to maintain connectivity to a single AP even though it would receive better performance by roaming. If you're wondering why vendors would do this, a lot has to do with the environment the device was made for. For example Apple iPhones were originally designed as personal devices (designed for homes). As most people have a single AP at home, the best user experience would be to keep a user connected to that single AP even with a poor connection, as the majority of end-users had a single AP. Modern smart devices, designed for Enterprise ala BYOD have started re-thinking their algorithms for what a good user experience is.

Supported Data Rates

Adaptive Data rates are an important part of Wi-Fi, and allows users to roam and remain connected at different distances and at different speeds from the cell. APs/WLCs have settings for Mandatory, Supported, and Disabled Data Rates. For Wi-Fi to function, 802.11 management frames must be heard by devices operating with different signal quality and performance, so management frames are sent at the lowest mandatory data rate to ensure anyone in the supported area could receive the signal, most APs/WLCs default to 1Mbs as the lowest which can create performance problems from DAY 1. Its best practice to disable data rates of 1, 2, 5.5, and 11Mbs (802.11b data rates), make 6Mbs mandatory, which disables 802.11b, and also creates a smaller cell size, with better performance and can help reduce co-channel interference in 2.4GHz ISM band Ideally you would avoid the 2.4GHz ISM band all together, but until that's a reality for your business optimizing the band and 802.11g should still show major performance improvements for what 2.4GHz clients remain.

Note: Before disabling any data-rates, it's recommended to ensure you're not disabling protocols that certain devices require. It's also recommended to perform a site-survey to validate that removing these lower data rates will not create coverage holes, or other coverage issues as disabling rates can greatly reduce cell coverage.

Dual-Band Adapters

One of the great things 802.11ac brought us is a huge increase in number of dual band 2.4GHz and 5GHz compatible client adapters on the market today. 802.11n helped start this trend, but as 802.11n could operate in 2.4GHz with limited performance, many vendors marketed 802.11n capable devices but operated in 2.4GHz only. 802.11ac is a 5GHz only technology, so client device vendors cannot make the claim a device is 802.11ac compatible without it supporting 5GHz. Even with dual-band APs and dual-band adapters, there is still a struggle to move clients to 5GHz.

How can this be you ask? Well most dual band adapters send 802.11 probe with the 2.4GHz radio first, so naturally the 2.4GHz radio gets the response first and clients which should be operating in the better 5GHz are further overloading the problems with 2.4GHz. So how can you avoid this? Well Cisco offers a feature called Band Select, also known as Band Steering, which helps to steer dual band clients to 5GHz by delaying the probe response on the 2.4GHz just enough so clients can receive the response on 5GHz and join the 5GHz. Band Select is enabled per WLAN on Cisco WLCs, but use caution when enabling Band Select on any WLAN supporting real-time communication like Voice or Video. Another solution is configure the WLAN adapter to 5GHz only mode, but this can be problematic to support if employees need to use their devices on Wi-Fi networks where 5GHz is not an option.

Security Issues

Some of the most common tickets from Enterprise Wireless users relate to security. Enterprise Wi-Fi security like WPA2/Enterprise utilizes 802.1x with EAP, where users authenticate to a centralized Authentication, Authorization, and Accounting (AAA) server using Remote Access Dial-up Networking (RADIUS) protocol. With Wi-Fi this all happens at Layer 2 where users must successfully authenticate before an IP address is assigned. Due to the number of protocols and technologies which deal with L2 Wi-Fi security we are going to simplify this to a simple scenario. If a single users is failing authentication, it’s likely an issue with credentials or client device. If multiple issues are failing authentication, it’s likely an issue with AP/WLC settings, AAA server settings, or networking between AP/WLC and AAA server. Another common type of Enterprise Wireless Security is Web-Auth, where users are re-directed to a web page for authenticate before being allowed access to the rest of the network. This happens at Layer 3, after IP Addressing, and DNS information is assigned. A common issue with this is when users fail to get re-directed to the Web-Auth-page for authentication.

Identifying issues at Layer 2

There are a couple of ways to identify issues relating to Layer 2 with Wi-Fi. One is for Cisco customers using a WLC, reviewing client details under the monitor page, and looking at the Policy Manager state.

The Policy Manager has a few key states to help admins identify issues with WLAN clients which are:

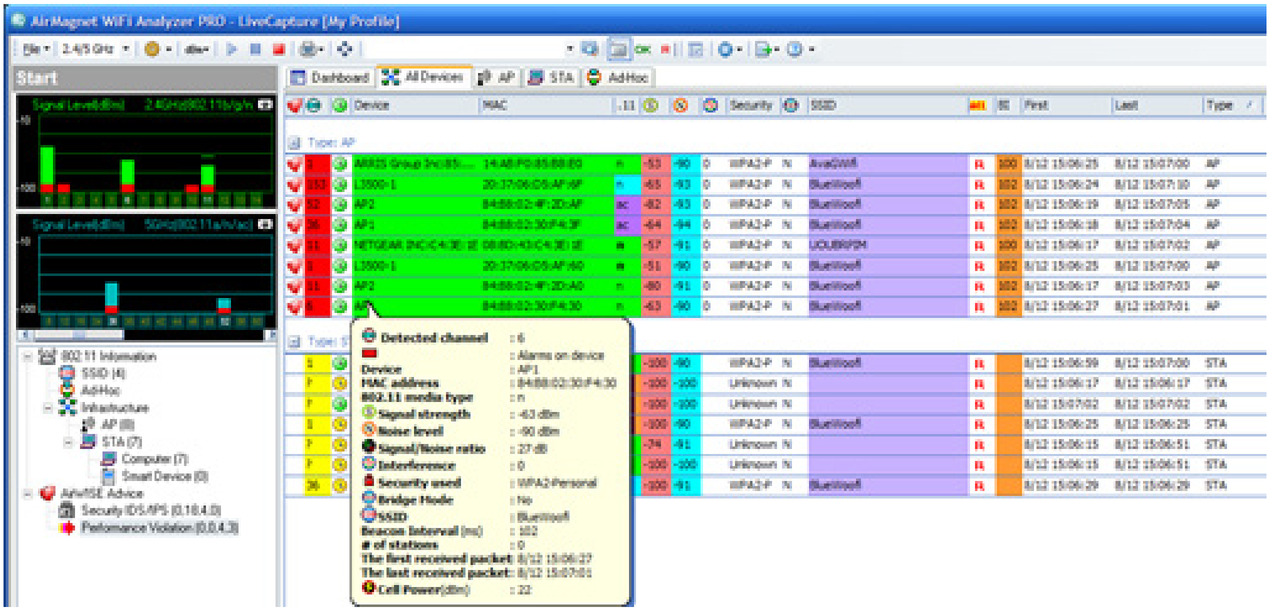
802.1X_REQD – 802.1x (L2) Authentication Pending
DHCP_REQD – Clients have not attained an IP
WEBAUTH_REQD – (L3) Web Authentication Pending
RUN – Client traffic forwarding

These states are pretty self-explanatory and an easy way to identify why clients are not able to connect to the WLAN. If you have a Cisco Prime Infrastructure Server, there is a great Client Troubleshooter tool, which will help identify issues relating to layers 1-3, and even give the technician proposed next steps to fix the issue. There is also just using the layered approach itself from the problematic device, i.e. we have successfully joined the SSID, do I have an IP address, gateway and DNS? Can I ping anything? Can I reach the Web-Auth page and see what I should? Another “more detailed” way to troubleshoot issues at Layer 2 is with a wireless packet capture.

Wireless Packet Capture

Capturing 802.11 frames with a laptop requires a WLAN adapter, and software capable of putting the WLAN adapter in Monitor mode. Running a WLAN adapter in Monitor mode on a Windows PC requires software and a 3rd party adapter, like the riverbed AirPcap adapter which works with WireShark. You can use Apple Mac Book Pro’s integrated Airport WLAN adapter, with Wireshark in Monitor mode natively with a few required supporting apps installed. There is a saying in the network industry “packets never lie” which is true, but there should also be a statement “packets can be time consuming to review”. While AirPcap adapters and WireShark, or MacBooks/Linux and Wireshark do give you the ability to see 802.11 frames, and even higher level frames, Netscout’s AirMagnet Wi-Fi Analyzer Pro (see figure 109) gives you the same visibility with an analysis engine designed for Wi-Fi. Wi-Fi Analyzer pro has algorithms to help quickly isolate issues found in the packet capture, and can save valuable time. There is a 3rd option for 802.11 packet capture for customers with Cisco Unified Wireless Network, and that is to use an existing AP in Sniffer Mode which converts the AP from serving client data into a Wireless capture device useable with WireShark or AirMagnet Survey Pro see Figure 109.

Figure 109



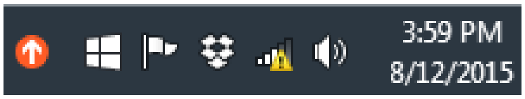
AirMagnet WiFi Analyzer PRO - LiveCapture [My Profile]
File
2.4/5 GHz
dBm
Start
Signal Level(dBm) 2.4GHz(802.11b/g/n)
Signal Level(dBm) 5GHz(802.11a/n/ac)
-10
-100
802.11 Information
SSID (4)
AdHoc
Infrastructure
AP (8)
STA (7)
Computer (7)
Smart Device (0)
AirWISE Advice
Security IDS/IPS (0,18,4,0)
Performance Violation (0,0,4,3)
Dashboard
All Devices
AP
STA
AdHoc
Type: AP
Type: STA

			Device	MAC	.11				Security		SSID			First	Last	Type
	3		ARRIS Group Inc:85...	14:AB:F0:85:B8:E0	n	-53	-90	0	WPA2-P	N	AvaGWifi	R	100	8/12 15:06:25	8/12 15:07:00	AP
	153		L3500-1	20:37:06:D5:AF:6F	n	-65	-93	0	WPA2-P	N	BlueWoofi	R	102	8/12 15:06:24	8/12 15:07:10	AP
	52		AP2	84:B8:02:4F:2D:AF	ac	-82	-93	0	WPA2-P	N	BlueWoofi	R	102	8/12 15:06:19	8/12 15:07:05	AP
	36		AP1	84:B8:02:30:F4:3F	ac	-64	-94	0	WPA2-P	N	BlueWoofi	R	102	8/12 15:06:18	8/12 15:07:04	AP
	11		NETGEAR INC:C4:3E:1E	08:BD:43:C4:3E:1E	n	-57	-91	0	WPA2-P	N	UOUBRP2M	R	100	8/12 15:06:17	8/12 15:07:02	AP
	3		L3500-1	20:37:06:D5:AF:60	n	-51	-90	0	WPA2-P	N	BlueWoofi	R	102	8/12 15:06:25	8/12 15:07:00	AP
	11		AP2	84:B8:02:4F:2D:A0	n	-80	-91	0	WPA2-P	N	BlueWoofi	R	102	8/12 15:06:17	8/12 15:07:03	AP
	6		AP1	84:B8:02:30:F4:30	n	-63	-90	0	WPA2-P	N	BlueWoofi	R	102	8/12 15:06:27	8/12 15:07:01	AP
	1					-100	-90		WPA2-P	N	BlueWoofi	R		8/12 15:06:59	8/12 15:07:00	STA
	F					-100	-100		Unknown	N		R		8/12 15:06:17	8/12 15:06:17	STA
	F					-100	-100		Unknown	N		R		8/12 15:07:02	8/12 15:07:02	STA
	1					-100	-90		WPA2-P	N	BlueWoofi	R		8/12 15:06:25	8/12 15:06:25	STA
	F					-74	-91		Unknown	N		R		8/12 15:06:15	8/12 15:06:51	STA
	F					-100	-100		Unknown	N		R		8/12 15:06:15	8/12 15:06:51	STA
	36					-100	-91		WPA2-P	N	BlueWoofi	R		8/12 15:06:29	8/12 15:06:29	STA

```
Detected channel           : 6
                           : Alarms on device
Device                     : AP1
MAC address                : 84:B8:02:30:F4:30
802.11 media type          : n
Signal strength            : -63 dBm
Noise level                : -90 dBm
Signal/Noise ratio         : 27 dB
Interference               : 0
Security used              : WPA2-Personal
Bridge Mode                : No
SSID                       : BlueWoofi
Beacon Interval (ms)       : 102
# of stations              : 0
The first received packet: 8/12 15:06:27
The last received packet:  8/12 15:07:01
Cell Power(dBm)            : 22
```

Bottom Up Approach – Troubleshooting Layer 3

4 This is where Wi-Fi itself ends, and network troubleshooting begins. After troubleshooting Layer 1 and 2, you should be able to identify the SSID's you are looking for, and successfully connect to them with the correct security, and receive what's called an Association ID (AID). Of course you don't see this AID on your clients, most OS's say simply, you've successfully connected. Even still you may receive the dreaded windows icon that indicates there is a problem.



If your reading this you have likely seen the Wi-Fi alarm before, but what you may not realize is although you can't reach the internet your Wi-Fi is still connected, and layers 1 and 2 likely worked as they should. The problem here could be a couple of things, most commonly the client not receiving IPv4 information via DHCP. This could be due to no DHCP server being present on the network the user was placed on, or no IP helper address. Point being is you are likely associated to the wireless network even though you can't reach anything, or have limited connectivity. If this is the case, you have validated Wi-Fi itself is working and are now troubleshooting network issues.

Troubleshooting Using Layered Approaches

By using a layered approach, in this case a bottom up approach we have methodically validated layers 1 and 2 and could continue all the way through layer 7 until the exact cause of the problem is found, duplicated, documented and resolved. If you find issues where the network seems to be functioning, but other issues are occurring you may consider a Top Down approach where you start with the Application layer and work your way down. If you are new to Troubleshooting networks, and Wi-Fi networks I highly recommend starting with these two approaches and use patience, the answers are there if we leave nothing to assumption. Being methodical, using a layered approach is a great way to solve problems, learn, and sharpen troubleshooting skills at the same time. After you build experience troubleshooting Wi-Fi, you may opt for other methodical approaches like Shoot from the Hip, or Follow the Path both of which I'll be discussing in Wireless LAN Troubleshooting Part 2 White Paper, coming soon.

Save Time Troubleshooting Wi-Fi

In this whitepaper you have no doubt learned troubleshooting many issues with Wi-Fi requires special tools. Having the right tools available when troubleshooting Wireless Networks can save valuable time and of course money from lost productivity.

There are three main categories of tools all Wi-Fi Engineers should have when designing, deploying, or troubleshooting an Enterprise Wireless Network including:

Site Survey tools - AirMagnet Survey Pro, or Ekahau Site Survey Pro
Spectrum Analysis/Analyzers - AirMagnet Spectrum XT or MetaGeek Chanalyzer
Wi-Fi Packet Capture – AirMagnet Wi-Fi Analyzer Pro, riverbed AirPcap / Wireshark, MAC OSX or Linux / Wireshark

All the products mentioned above are used by many Wi-Fi professionals/experts, myself included. There is one more product I wanted to mention which can help save time troubleshooting certain issues which is a handheld device, NetScout's AirMagnet Air Check unit. Which is a handheld device designed to quickly identify and troubleshoot issues relating to Wi-Fi. The reason I wanted to give this device a special shout-out is due to the fact it's a handheld and doesn't require you to carry around a laptop, and has a ton of useful features for quickly identifying issues with Wi-Fi earning this device the ultimate Wi-Fi portable troubleshooting tool award. Just kidding there is no such award, but there should be Net Scout, there should be.

Troubleshooting Day to Day

For day to day troubleshooting of Wireless Networks, Enterprises should use and regularly monitor a Centralized Network Management System (NMS), for example Cisco Prime Infrastructure. When Prime is properly deployed, and managed, it is one of the best tools for monitoring and troubleshooting deployed Cisco Enterprise Wireless Networks providing a centralized command and control center for both the Wired and Wireless network.

Take Away

Why so much talk early on about design in a troubleshooting paper? Because many enterprises who complain of constant problems with their Wi-Fi deployments are due to improper planning or poor design choices. Before deploying any Enterprise Wireless solution a full on premise pre-deployment Site Survey should be performed, and should include analysis of customer facilities, coverage areas, user base, line of business applications, supported devices, network load, security policies, etc. Design the RF Environment for your worst client's performance and power settings. After this thorough design process is done, a second post-deployment validation Site Survey should be performed which essentially verifies the design met its required objectives.

Cover the basics -

- Control the RF environment
  - Establish a Data Rate Policy to optimize cell size and performance
  - BAN 802.11b devices
  - BAN the 2.4GHz entirely (if possible)
  - Use BAND Select to steer dual-band clients to 5GHz
  - Use Enterprise Security ONLY, WPA2/Enterprise (EAP-PEAP, EAP-TLS, EAP-FAST) or L3 Web-Auth / wACL's. If WPA2/Personal pre-shared key is a requirement use complex passwords 20+ characters of alphanumeric, and special characters.
- Once the architecture is in place, a centralized NMS like Cisco Prime should be used for centralized monitoring and reporting of the network infrastructure.
- Ensure you have the wireless tools to properly survey and troubleshoot issues relating to Wi-Fi, this includes tools described above, Site Survey, Spectrum Analysis, and Wi-Fi packet capture.
- Be cognizant about devices you're allowing on the network, and make dual-band or 5GHz a requirement.
- Ensure you and your team(s) have the proper training.

How can I learn more?

There are many courses available to help students who are interested in learning how to design, deploy, secure, and troubleshoot Cisco Enterprise Wireless solutions. Whether you care about becoming certified or not, these courses can help you become a Wi-Fi Masta! Cisco has laid out career paths focused on Wireless networking beginning at the associate level (CCNA Wireless), continuing through the Expert level (CCIE Wireless). There are dozens more courses around specific skillsets within Wi-Fi, like Design, Security, or Location Services. To learn more speak to a Fast Lane training advisor today.

Vendors mentioned in this whitepaper – product images and graphics used with permission.
Chris Avants http://chrisavants.com
Cisco Systems https://www.cisco.com
NetScout AirMagnet https://www.flukenetworks.com
Ekahau http://www.ekahau.com
Riverbed http://www.riverbed.com
Wire Shark http://www.wireshark.org