element14 ESSENTIALS

# Wireless Protocol II: Wi-Fi

*Sponsored by* CYPRESS EMBEDDED IN TOMORROW™

1. Introduction | 2. Objectives | 3. Wi-Fi and the 2.4/5.0 GHz ISM Bands | 4. Wi-Fi Basics | 5. CSMA, CSMA/CD, CSMA/CA | 6. Coordination Functions and Wi-Fi Topologies | 7. Wi-Fi Evolution: Alphabet Soup | 8. Wi-Fi Security: WEP, WPA, and Beyond | 9. Other Wi-Fi Considerations and Some Explanations | Related Components | **Test Your Knowledge**

## 1. Introduction

Hedy Lamarr is well known as an actress during Hollywood's Golden Age (1930s-40s), starring with famous actors Clark Gable and Spencer Tracey. What is less well known is that she also made critical contributions to the development of the communication technique that is now known as Frequency Hopping Spread Spectrum (FHSS), in collaboration with musician George Antheil. FHSS was used in early versions of Wi-Fi, with more contemporary versions using Direct Sequence Spread Spectrum (DSSS). The original patent for FHSS was not picked up by anyone until many years after its release, when the US Navy began using FHSS for communications. It took decades before she was recognized for her contributions to wireless technology. In this learning module, we will briefly discuss both FHSS and DSSS, along with the Essentials of Wi-Fi, including networks, topologies, CSMA, Wi-Fi evolution, security, and examples of Wi-Fi devices available today.

## 2. Objectives

*The objective of this learning module is to acquaint you with Wi-Fi. Upon completion of this learning module, you will be able to:*

- Understand the basic architecture, networks, and elements of Wi-Fi
- Explain some key features of the IEEE 802.11 standard
- Explain the alphabet soup of 802.11 standards, viz. a, b, g, n, ac, etc.
- Explain CSMA, CSMA/CD, and CSMA/CA

## 3. Wi-Fi and the 2.4/5.0 GHz ISM Bands

We have previously discussed the 2.4 GHz ISM band in the Essentials of Bluetooth. As a review, the 2.4 GHz band is an unlicensed band in which any device can transmit, provided it does not exceed the maximum output power restrictions. As a result, there are many different devices and technologies in the 2.4 GHz band, including our beloved Microwave Oven. All of these devices and technologies have to coexist, and this is what

makes the use of advanced wireless communication techniques such as Spread Spectrum essential to understanding Wi-Fi.

### *- 3.1 Wi-Fi and the 2.4 GHz Band*

When Wi-Fi technology was first deployed, it was in the 2.4 GHz band and it has remained in that band for many years. Over the years, the technology has advanced enough such that not a lot of wireless communication issues are experienced due to other nearby 2.4 GHz devices and technologies. When issues do arise, they usually revolve around range, signal power (and its reduction due to the presence of walls), the number of simultaneous users, and the number of co-located Basic Service Sets (BSSs; or networks in layperson's terms). The advances in the different versions of the IEEE 802.11 standard have been in Modulation and MIMO techniques that have led to better speeds and more robust performance. We will discuss this evolution in a later section. The advances have actually gone so far that the 2.4 GHz band and its characteristics are no longer sufficient to support today's wireless LAN needs. Since Wi-Fi is the Wireless LAN technology of choice worldwide, the evolution of Wi-Fi has placed it firmly now in the 5 GHz band.

### *- 3.2 Wi-Fi and the 5 GHz Band*

| **Band Specs** | **2.4 GHz** | **5.0 GHz** |
|---|---|---|
| Standard | IEEE 802.11 b, g and n | IEEE 802.11 a, n, ac |
| Channels | Three non-overlapping | 23 non-overlapping |
| Data Rate | Lower | Higher |
| Network Range | Wider Range | Shorter Range |
| Interference | Higher | Lower |

*Table 1: Comparison of 2.4 GHz and 5 GHz Wireless Bands*

The 5 GHz band is also an unlicensed band; however, there are fewer devices and technologies vying for that space. More importantly, there is more bandwidth available in the 5 GHz band, and with the advent of more advanced engineering making up for the limitations of the 5 GHz band, this has made it more attractive for current and future evolutions of Wi-Fi.

Wi-Fi will continue to operate in the 2.4 GHz band (as you may have noticed on 802.11 ac networks), but there is better performance available at the 5 GHz band.

## 4. Wi-Fi Basics

Wi-Fi stands for Wireless Fidelity, which is simply a trademarked term for devices operating using the IEEE 802.11 standard. Other variants of Wi-Fi are Wi-Fi, WLAN

(short for Wireless LAN), and 802.11. IEEE 802.11 is more likely to be encountered in technical, engineering and academic circles. Most laypersons know it simply as Wi-Fi.

### *- 4.1 The Last Hop Technology*

It is now common to have not only Wi-Fi enabled laptops and cellphones, but toasters and washers as well. What this means is that these are devices or appliances capable of accessing the Internet through the use of Wi-Fi as the last hop access technology. This is accomplished by the device making a wireless connection (via Wi-Fi) to a wireless access point (AP), which in turn is usually connected to the Internet through the use of Ethernet or another technology (that other technology could also be Wi-Fi, by the way). For the time being, it is good to simplify and think of an access point as somehow being connected to the Internet (for example, literally through a wire), and then providing wireless access (to the Internet) to devices that are within range.

### *- 4.2 Basic Service Set (BSS)*

When an access point is set up, it is usually set up as part of a local network. In Wi-Fi terminology, such a network is called a Basic Service Set (BSS), and the network is identified by a BSS id. The human readable name that we use (ex: "Element14-Secure) that you see pop up when your device informs you that there are Wi-Fi networks available, is the SSID (Service Set Identifier), and it applies to both BSSs and ESSs (below) depending on the context.  When set up in a home, the BSS is often just the one access point (AP) and the devices that are connected to it. This connection in Wi-Fi terminology is called an association; thus, devices are associated with the AP.

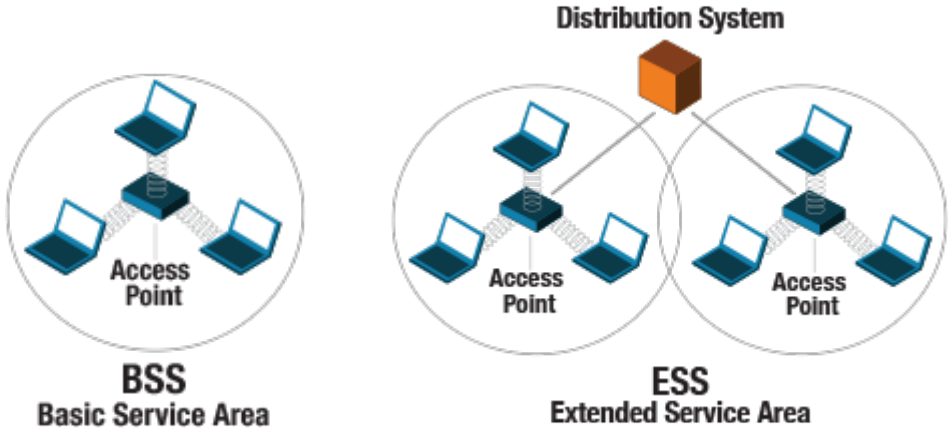


*Figure 1: Wi-Fi: Basic Service Area versus Extended Service Area (Source: Cisco)*

### *- 4.3 Extended Service Set (ESS)*

In enterprise systems, where the same wireless network is seen throughout an office or university campus, it should be obvious that not all devices are being serviced by the same AP. In this situation, the wireless network is accessed usually by a device accessing the closest AP—though it is more accurate to say the best AP, because the

closest AP is determined not by distance but by signal quality. All the APs in this scenario are part of a larger wireless network. This extension of the BSS concept is called an Extended Service Set (ESS). It is common nowadays to see multiple ESSs in the same physical space, for example, Element_14_Guest and Element_14_Secured. In those situations, the same AP is capable of servicing clients on both Service Sets.

Enterprise APs provide the capability for provisioning such that bandwidth (BW) distribution and Quality of Service (QoS) can be handled according to policy. For example, there might be more BW dedicated to the secure network vs. the guest network. Also, in many such situations, the "guest" might be open, while the "secured" might need higher level authentication. (We will discuss wireless security in Section 8.)

### *- 4.4 Access Point vs. Wi-Fi Router*

For the purposes of this learning module, we will use the term access point (AP) to refer to the device that is providing end user connectivity. It is common to hear the term Wireless Router, or Wi-Fi Router, so let us briefly explain the difference between the terms and clarify why we will use the term AP throughout.

Both an AP and a Router provide wireless access. The only difference is that a Router will have Ethernet ports in addition to providing wireless access through Wi-Fi. Thus, it is an AP with Ethernet ports. You should note that the term Router in networking means something very specific, that is, the capability to participate in a Routing Protocol (ex: Internet Routers participate in the Internet Protocol or IP). Since a Wireless Router performs no Routing function, it should not be called a Router. A Wireless/Ethernet Hub or Switch (depending on the AP device's capability) would be a better name. However, marketing/sales specialists have determined that the device is to be called Wireless Router, thus we are stuck with that term despite its lack of technical exactness.

*Note: It is worth mentioning that when an Internet Service Provider (ISP) hands you a Wireless Gateway that, in fact, is an accurate description of that product. A Gateway is a bridge between different Layer 2 technologies (in this case, probably Wi-Fi/Ethernet and cable or fiber).*

## 5. CSMA, CSMA/CD, CSMA/CA

Wi-Fi was inspired by Ethernet, or as a wireless replacement for LANs. In fact, the 802.11 suite of standards was often referred to as Wireless LAN or WLAN technologies. Wi-Fi uses CSMA, so let's discuss this key concept in this section.

CSMA stands for Carrier Sense Multiple Access, a system in which multiple devices in a broadcast domain listen-before-transmitting. If the channel is busy, you do not transmit; if the channel appears to be free, then you transmit. There are several variants on the precise protocol for transmitting, but that's out of the scope of this learning module. CSMA was developed by building on the random broadcast channel concept of the ALOHA protocol.

### *- 5.1 CSMA and CMSA/CD*

Since there is a possibility that more than one node is ready to transmit at a given moment, there is a chance for collisions in CSMA. To address the problem of collisions, in Ethernet, which uses CSMA but with Collision Detection (CSMA/CD), you do the same thing as CSMA but are actively detecting collisions. So, if a collision is detected, then the transmission is aborted, thereby not wasting the entire transmit time of a packet. Once a collision occurs, a Randomized Exponential Backoff (REB) process begins. That is, you start throwing dice and then wait as many slot times as the dice tell you to before you try to transmit. Each time you try to retransmit and encounter a collision, you double your dice size. Thus, when the first collision is experienced you start with [0, 1] as being your dice (or number set if you want to be mathematical). The next collision you can randomly choose from [0, 1, 2, 3], and so on. The network should stabilize according to the number of nodes and the amount of offered traffic – mathematically, the dice range will stabilize to account for the number of collisions being experienced. In modern Ethernet, which is typically Switched Ethernet, there are almost no collisions, and so even though the devices/interfaces are operating as CSMA/CD, the Backoff is not very likely to take effect.

### *- 5.2 Wi-Fi and Collision Avoidance*

While Wi-Fi uses CSMA, there are two reasons why Collision Detection is difficult while the packet is in flight. The first and more debilitating reason is that early on the 802.11 standardizers decided to make Wi-Fi half-duplex, i.e. a Wi-Fi radio is capable of transmitting or receiving at a given instant of time but cannot do both. So, even if the transmission is garbled or there is a simultaneous transmission from some other node, the transmitting node has no way of detecting this.

From its beginnings, Wi-Fi was made to reduce cost and power consumption; however, it also kept in mind the future evolution of the technology for making critical, far-reaching decisions. The second reason why collision detection is difficult for a packet-in-flight has to do with the nature of the Wireless domain. There is a problem wherein a transmitter cannot hear another transmission, either because of distance or because of topography: both transmissions collide at a receiver who can hear both transmitters, but neither transmitter is within hearing range of the other, which is known as the hidden node problem.

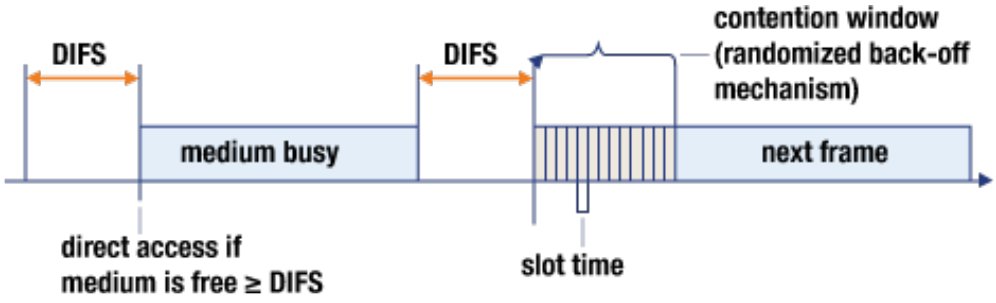


*Figure 2: The Distributed Coordination Function (DCF) uses a CSMA/CA with binary exponential backoff algorithm. When a station is ready to send it begins sensing the medium. If the medium is free during an IFS, the station starts sending. If the medium is busy, the station has to wait for a free IFS, and then the station must wait a random backoff time.*

To deal with being unable to detect collisions, Wi-Fi takes the approach of using CSMA with Collision Avoidance (CSMA/CA). The probability of collisions is reduced by using Randomized Exponential Backoff (REB) right away. In other words, you're assuming that there might be other nodes that are ready to send information at the same time as the channel is perceived to be idle and thus you do not wait for a collision to begin playing the game of dice. The number set or dice is called a Contention Window. The size of the Contention Window is controlled by a CWmin parameter, which is typically set to 15. Thus, Wi-Fi starts the Exponential Backoff with a number set of [0, 15] right from the start. Thereafter, the Contention Window is usually doubled each time there is a collision up to a CWmax (typically 1023)[1].

[1] There are always more details in a standard the size of 802.11. The increase in Contention Window size is actually controlled by a Persistence Factor that is typically set to 2. 802.11e, which was developed to support Quality of Service (QoS) on Wi-Fi, and prescribes different CW parameters for different classes of traffic.

## 6. Coordination Functions and Wi-Fi Topologies

The CSMA/CA scheme discussed above is what is used by default in Wi-Fi, and is part of the Distributed Coordination Function (DCF). DCF is default inasmuch as every access point (AP) and device is required to support it. We will discuss DCF in a little bit more detail shortly, once we have made a brief mention of some optional components of the standards.

### *- 6.1 Point Coordination Function (PCF)*

Like many other standards, Wi-Fi has optional pieces that some devices/APs can choose to deploy. Like many other standards, the optional pieces are almost never used. One of those pieces is Point Coordination Function (PCF). DCF is in contrast to the Point Coordination Function (PCF), in which the AP controls the channel by assigning transmit slots to nodes. Apart from being optional, PCF is almost never used because it is designed to be used in conjunction with DCF, and, in practice, results in the AP being late in sending beacon frames (See section 6.4), which are the frames assigning the time slots in the first place.

### *- 6.2 Request-to-Send/Clear-to-Send (RTS/CTS)*

In DCF, there is an optional Request-to-Send/Clear-to-Send (RTS/CTS) feature to alleviate the hidden node problem. Since the receiver sends the CTS message, the transmitter can be confident that no one else is going to transmit simultaneously; if there were a hidden node transmission, then the CTS would not be sent; if there were a hidden node looking to transmit, a CTS would be an indication to it to hold off. However, it is a significant performance overhead and still susceptible to problems.

### *- 6.3 Acknowledgement Message (ACK)*

With half duplex radios, how does a node know if its transmission has succeeded? How are collisions inferred? These lingering questions are answered by means of an acknowledgement (ACK) message. The receiver whom the message was meant for will respond with an ACK if it successfully received the message. If an ACK is not received, then that indicates that the packet was garbled. This may be due to a collision, due to interference from other Wi-Fi sources (not part of the BSS but on the same channel), or interference from other non-Wi-Fi sources in the unlicensed band. There is no way to tell these apart. The response is always going to be to adjust the contention window (CW). We discussed earlier that CWmax is set to 1023, i.e., once the dice is [0, 1023] you do not expand it further. It is likely that if there is something untoward occurring on the channel (i.e., popcorn in the microwave) causing not only the original packet's transmissions to fail, then its retransmissions may fail as well, leading to repeated failures. To ensure this doesn't continue for too long, a retransmission limit for an individual packet is set to 7. After that many tries, Wi-Fi gives up, and the packet is lost.

The bigger issue is intermittent interference, because then all the repeated transmissions might fail. As such, if when a node is ready to transmit, it finds the medium BUSY (either because of a Wi-Fi transmission, or otherwise), then it will refrain from doing anything until the medium is found to be IDLE. Something like a microwave or other non-Wi-Fi interference can pose a significant problem because the channel is not necessarily perceived as BUSY all of the time that the microwave is going – home microwaves in particular only work for one cycle of the alternating current (AC), which means that while the microwave is ON, 50% of the time it is not emitting radiation in the 2.4 GHz band; additionally, the emitted power level will also vary with the rising and falling of the AC sinewave. In short, it's complicated. One thing that Spread Spectrum enables is that it makes the Wi-Fi signal more resistant to narrow-band interference by spreading out the signal over the 22 MHz, but a microwave emission is easily wider than a Wi-Fi channel wide and may overlap all 3 non-overlapping Wi-Fi channels (see section 9.1).

ACK frames are given priority through a timing mechanism. Even though we said earlier that a node checks to see if the channel is idle before it begins a REB, it actually needs to wait for a DCF Interframe Spacing (DIFS) time period before it can begin that. There is a Short Interframe Spacing (SIFS) which is used to send ACKs, and a PCF Interframe

Spacing (PIFS) that can be used by the AP to take control of the channel. The relationship between the 3 time periods is thus:

**SIFS < PIFS (SIFS + 1 slot time) < DIFS (SIFS + 2 slot times)**

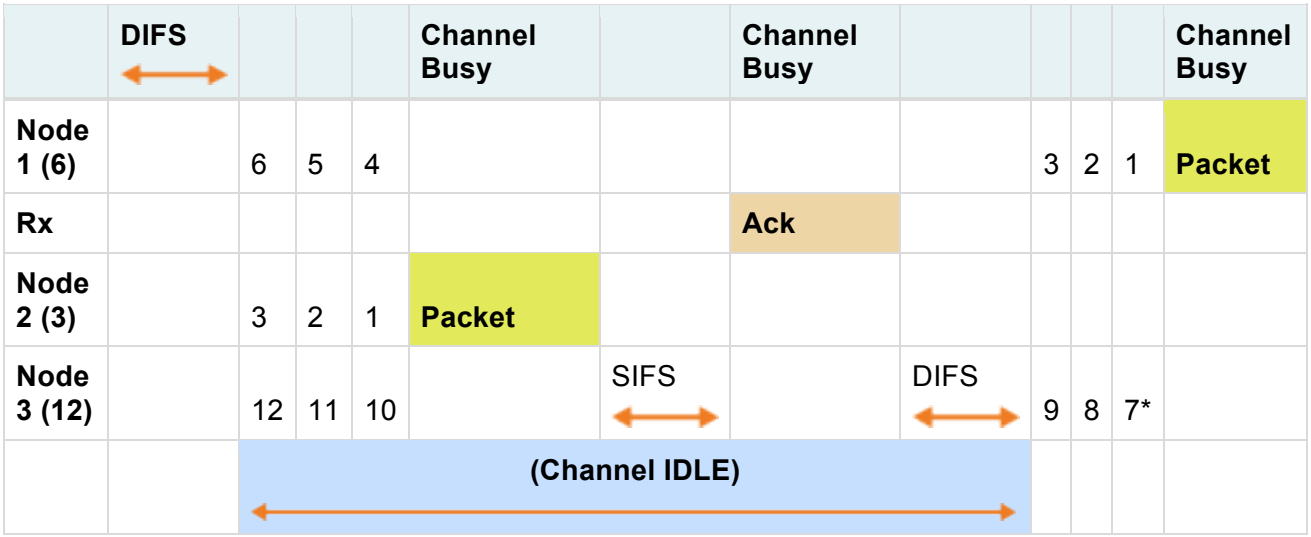


*Figure 3: An illustration of DCF CSMA/CA with Randomized Exponential Backoff.*
**Countdown will resume at 6 when channel is IDLE (i.e., no transmission for a DIFS period).*

Figure 3 shows three nodes (1, 2, 3) are ready to transmit and detect the channel as IDLE simultaneously. Since each one picks from the CW of [0.31] at random, node 1 picks 6, node 2 picks 3, and node 3 picks 12. Node 2 counts down to 0 quickest and is able to transmit. Once Node 2 begins transmitting, the other 2 nodes pause their countdowns (otherwise the game of dice would be really unfair). After the packet is received by the receiver Rx, it acknowledges (ACK) after a SIFS time period. Thereafter, after a DIFS period, when the channel is detected as IDLE again, the countdowns for node 1 and node 3 resume at their paused values.

In the meantime, it is possible that a 4th node became ready to transmit, in which case, it would pick a number from the CW. It could potentially be smaller than 9 or 3 (the paused count), in which case it will get precedence. If a failure occurs at any point (i.e. no ACK is received for a packet,) the failed transmitter will double its CW.

Note that although there is some reduction in efficiency, the 3 nodes that are simultaneously ready to transmit do not result in collisions because of the Collision Avoidance REB mechanism.

### *- 6.4 Beacon Frames*

As we can see from the above example, timing is crucial in a Wi-Fi network. An AP periodically sends out a Beacon frame (typically 10 times per second) that announces its presence and which BSS/ESS it is servicing. This lets a device know that there are BSSs available at a given spot. (Note: This is typically what is used, and there are many

variations possible.) For example, an AP may not want to advertise its BSS for security reasons.  Again, the vastness of all 802.11/Wi-Fi possibilities is beyond the scope of even a 600-page book!  The Beacon frame also allows all nodes in the BSS to resynchronize their clocks with that of the AP. Clock Drift is a major issue in networks of all kinds. In fact, every frame that is sent on Wi-Fi has a preamble portion that is part of the Wi-Fi PLCP (Physical Layer Convergence Protocol) that enables the receiver to synchronize to the transmitter's clock. One last thing worth mentioning here is that the Wi-Fi header announces how long a packet is going to be so that receivers other than the intended destination can choose to go to sleep to save power.

***- 6.5 Ad Hoc Mode***

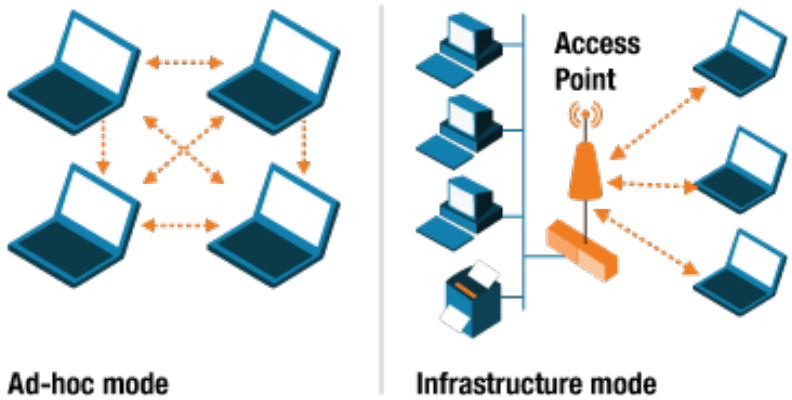


*Figure 4: Ad Hoc Mode vs Infrastructure Mode*

Depending on your operating system, Wi-Fi can also work in ad hoc mode without an AP. Two devices can communicate directly with each other in ad hoc or peer mode. In this case, one of the devices acts as a temporary AP sending beacons to keep the connection alive. Ad hoc mode is also used in Wi-Fi Direct in which a secondary device (such as a remote) communicates with a primary (TV/Roku). Whether you are in ad hoc mode when using wireless streaming depends on the underlying technology.  Even if your operating system does not allow you to create an ad hoc network with another computer, it may still use ad hoc mode with something like Wi-Fi Direct.

## 7. Wi-Fi Evolution: Alphabet Soup

The first version of Wi-Fi (1997) did not arrive with an alphabet subscript and had a data rate of 1 Mbps or 2 Mbps. The alphabets have been added as the technology and standard have evolved. Here's a summary of the Wi-Fi versions with subscripts:

- **802.11b (1999):** Enhanced the modulation for the DSSS variant at 2.4 GHz to support data rates up to 11 Mbps.

- **802.11a (1999):** Added an Orthogonal Frequency Division Multiplexing (OFDM) PHY at 5.8 GHz. This variant did not become common until after 802.11g. Data rates up to 54 Mbps.

- **802.11g (2003):** Brought OFDM from 802.11a to the 2.4-GHz band. Data rates up to 54 Mbps. Following the advent of g, it was extremely common to have 802.11b/g compliant devices, and over time 802.11a/b/g compliant devices (which were dual band – 2.4 and 5.8 GHz).

- **802.11n (2009):** Added Multiple Input Multiple Output (MIMO) antenna capabilities to Wi-Fi. Data rates of up to 600 Mbps. Prior to n, in 2007 letters a-j (except f) were merged into the base standard. MIMO enables the use of beamforming and Spatial multiplexing, thereby increasing the data rates (depending on antenna configuration). A similar merging occurred in 2012 as well.

- **802.11ac (2013):** This is the standard today. Data rates up to 1300 Mbps are possible with the use of wider channels along with Spatial multiplexing at the 5 GHz band.

Other subscripts of interest:

- **802.11af:** White-Fi: Use of Wi-Fi in TV White spaces.

- **802.11ah:** Use of Wi-Fi in sub-1GHz applications.

- **802.11ad/ay:** Use of Wi-Fi in 60 GHz. aj is ad at 45 GHz.

- **802.11ax:** The next mainstream version is currently under development with a goal of increasing data rates by up to 4 times.

## 8. Wi-Fi Security: WEP, WPA, and Beyond

In a broadcast medium such as Wi-Fi, where all transmissions can be heard by everyone, it is critical to have security to ensure privacy and integrity. During the time of 802.11b, security was available through a mechanism known as Wired Equivalent Privacy (WEP). WEP was extremely limited and had several problems, most egregious of which was that in Shared Key authentication, the AP sent clear text to the node requesting to authenticate, and the node was authenticated when it sent back an encrypted version of that clear text. Thus, the still overblown paranoia about Wi-Fi networks being open for all to hear (play your favorite radio commercial in your head).

WEP was deprecated when Wi-Fi Protected Access (WPA) was introduced as part the 802.11i draft in 2003. WPA was designed such that it could be implemented via a firmware upgrade. WPA was designed to bring Wi-Fi up to the security standards of the day, including 64-bit and 128-bit encryption and Temporal Key Integrity Protocol (TKIP). The base version of WPA has pre-shared keys (WPA-PSK). Intended for home use, WPA does not require the use of an authentication server. WPA-Enterprise requires the use of a RADIUS (Remote Authentication Dial-in User Service) Server. WPA-Enterprise supports a variety of EAP (Extensible Authentication Protocol) extensions.

WPA2 was the ratified standard version of 802.11i, circa 2004. There aren't many differences as compared to WPA, apart from the fact that WPA2 support is mandatory for products to be Wi-Fi certified and WPA2 has support for CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol/Counter Mode CBC-MAC protocol).

WPA3 was introduced earlier this year and enhances WPA/WPA2. WPA3 uses 128-bit encryption in personal mode and 192-bit encryption in Enterprise mode. WPA3 adds Forward Secrecy.

## 9. Other Wi-Fi Considerations and Some Explanations

This last section of the module provides a commentary on overlapping channel considerations, password security and spatial multiplexing.

### *- 9.1 Overlapping Channels in the 2.4 GHz band*

Some of you may use the default settings on a new Wi-Fi router/AP. One of the default settings is that of the default channel. This is often set to channel 6.

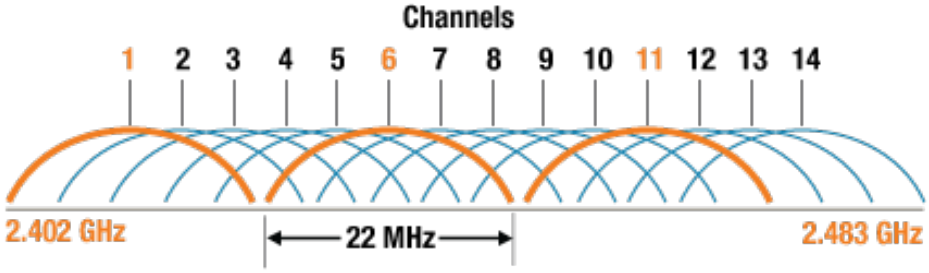


*Figure 5: 2.4 GHz Channels (Source: Cisco)*

When in the 2.4 GHz band, channel considerations are quite important. Worldwide, the Wi-Fi standard will say that there are 14 channels in the 2.4 GHz band, the lower 13 of which are in use in Europe, and the bottom 11 in the US. So, 11 channels, right? Pretty nice capacity. But the 2.4 GHz band, by definition, is 100 MHz. Wi-Fi channels are 22 MHz, then how does one get more than 5 channels from 100 MHz total? In fact, in the US, the Wi-Fi band stretches from 2401 MHz to 2473 MHz. That's about 70 MHz. The reason why this is possible is because the 11 channels are overlapping.

The center frequencies for Wi-Fi channels begin at 2412 MHz and go up in 5 MHz increments. This naturally means that there will be interference from adjacent channels. There will actually be interference from all overlapping channels to varying degrees. For example, Channel 6, which is the default, would receive a lot of interference from Channel 5 and Channel 7, a bit less from Channel 4 and 8, and so on, and no interference from Channel 1 and Channel 11. It is typical, therefore, to only use the 3 effective channels, both to improve your performance, but also to *play nice* with others.

Of the 3 effective channels (1, 6, 11) which one should you use? Should you remain with the default? The answer depends, but there is a good chance that your neighbors are using the default, so 6 may be a bad choice. When there are multiple BSSs on the same channel, the DCF works in such a way that all BSSs end up sharing the effective bandwidth.

The correct approach is to conduct a *Site Survey* using any number of free or open source tools to figure out what is the least occupied channel in your neighborhood and set your router to that channel. Note that contemporary routers often have the capacity to autodetect the least occupied channel; it is wise to make sure that it is automatic in such a way and not a default channel selection.

At 5 GHz, there is much less to worry about: not only is there an abundance of channels, but there are also non-overlapping channels (phew!).

In enterprise networks or ESSs, it is typical to configure nearby routers to have different channels in a rotating fashion.

### *- 9.2 Wi-Fi Passwords*

We have noted some of the security in Section 8, WPA and beyond. When setting up your Wi-Fi network it is important to note that the encryption key is based off the Wi-Fi password that you setup (in WPA-PSK). The password can be 8-63 characters long (ASCII, or 64 hex digits), and the the password along with the SSID is used to compute the 256 bit encryption key. The problem is that if your password is too short then it will be easier to attempt a brute force attack. So your password should be as long as possible; security experts recommend 15 characters or more. Long phrases are good.

### *- 9.3 MIMO and Spatial Multiplexing*

We have mentioned MIMO, beamforming, and Spatial Multiplexing in section 7 on Wi-Fi evolution. It is worth discussing briefly in layperson terms to get an intuition of how it works. Older Wi-Fi antennas used to be omni-directional (that is, the signal transmitted and received is from all directions). This made sense since the relative positioning of transmitters and receivers could be anywhere, bearing in mind obstacles and reflections.

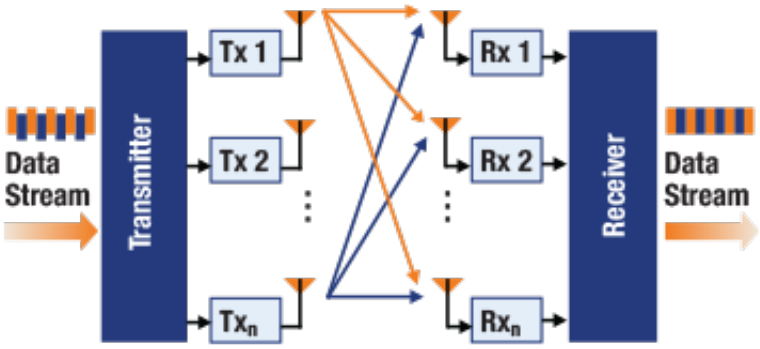


*Figure 6: Spatial Multiplexing*

With the advent of better antennas and the use of antenna arrays, it became feasible to have directionality with antennas such that they transmit and receive from specific directions. When a transmitter and receiver are tuned in such a way then a radio-beam is being transmitted that does not spread in all directions (a directional beam). This allows for the use of multiple beams simultaneously in different directions, thus allowing for multiple simultaneous communications (multiplexing) spatially (Spatial Multiplexing). You can get an intuitive feel for Spatial Multiplexing by looking at a Cellphone tower near you. The multiple antennas (of the same type/size) are breaking the geographic range of the tower by directions.



Take the Quiz