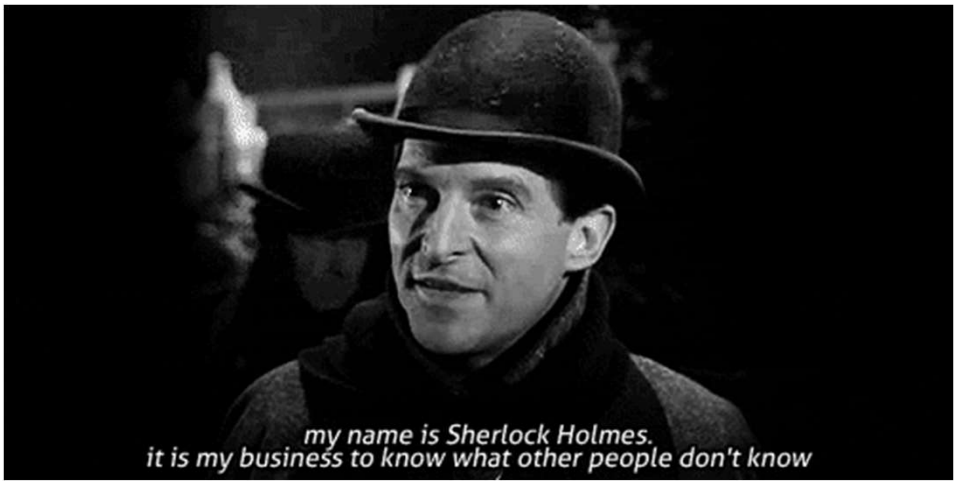
Hacking 101

Topic : Intro to Wi-Fi

SECURESET ACADEMY

Wi-Fi Introduction



SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

We all use Wi-Fi.

We see the network name, we click on it and boom, we are connected.

But how does it work? Most people have no idea and from a Cybersecurity standpoint, IT IS REALLY IMPORTANT TO KNOW.

In today's topic we are going to cover the basics of Wi-Fi, so buckle up and keep an open mind to learn how this technology works.

What is Wi-Fi

SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

(/ˈwaɪfaɪ/)

- **Wi-Fi** or **WiFi** is technology for radio wireless local area networking of devices based on the IEEE 802.11 standards.

- Wi-Fi is a trademark of the **Wi-Fi Alliance**, which restricts the use of the term Wi-Fi Certified to products that successfully complete interoperability certification testing.

- Phil Belanger, a founding member of the Wi-Fi Alliance who presided over the selection of the name "Wi-Fi", has stated that Interbrand invented *Wi-Fi* as a pun upon the word *hi-fi*

- **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers

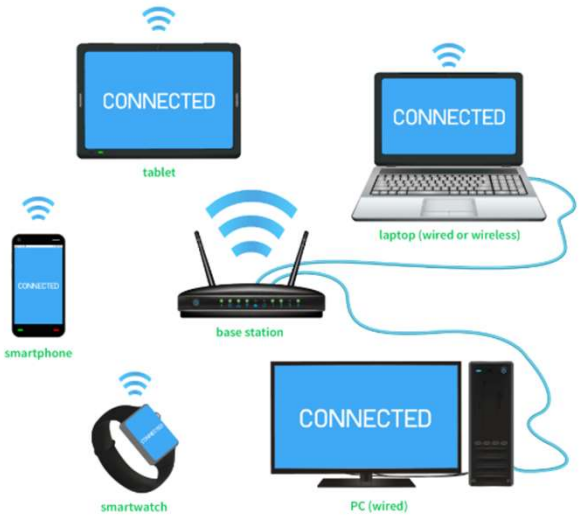
    - **Institute of Electrical and Electronics Engineers** (**IEEE**) is a professional association with its corporate office in New York City and its operations center in Piscataway, New Jersey. It was formed in 1963 from the

amalgamation of the American Institute of Electrical Engineers and the Institute of Radio Engineers.

- They come up with the networking standards that are accepted for the most part in WiFi.

- The IEEE 802.11 standard is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6, 5, and 60 GHz frequency bands.
- They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802). The base version of the standard was released in 1997, and has had subsequent amendments.

WLAN



SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

- Wi-Fi compatible devices can connect to the Internet via a WLAN and a wireless access point. Such an access point (or hotspot) has a range of about 20 meters (66 feet) indoors and a greater range outdoors.

- Hotspot coverage can be as small as a single room with walls that block radio waves, or as large as many square kilometers achieved by using multiple overlapping access points.

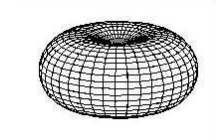
- Wi-Fi operational range depends on factors such as the frequency band, radio power output, receiver sensitivity, antenna gain and antenna type as well as the modulation technique. In addition, propagation characteristics of the signals can have a big impact.

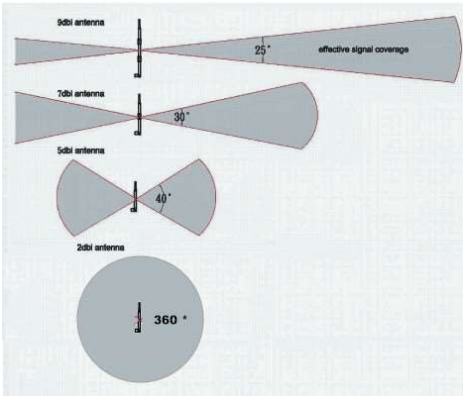
- At longer distances, and with greater signal absorption, speed is usually reduced.

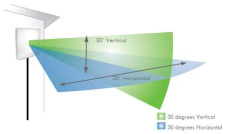
- Compared to cell phones and similar technology, Wi-Fi transmitters are low power devices. In general, the maximum amount of power that a Wi-Fi device can transmit is limited by local regulations,

- FCC Part 15 in the US. Equivalent isotropically radiated power (EIRP) in the European Union is limited to 20 dBm(100 mW).

Antennas





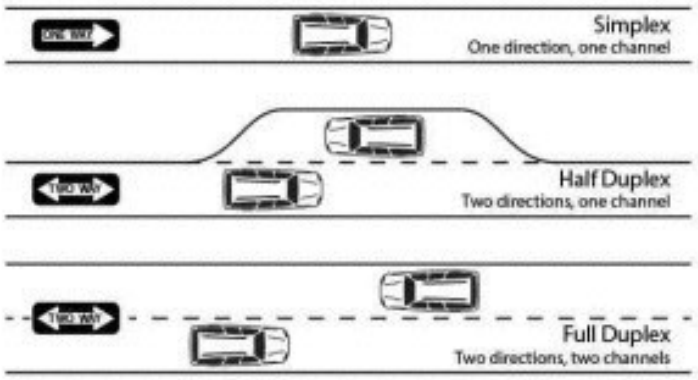


SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

- An access point compliant with either 802.11b or 802.11g, using the stock omnidirectional antenna might have a range of 100 m (0.062 mi).
- The same radio with an external semi parabolic antenna (15 dB gain) with a similarly equipped receiver at the far end might have a range over 20 miles.
- Higher gain rating (dBi) indicates further deviation (generally toward the horizontal)

Basics of Communication – Traffic Modalities

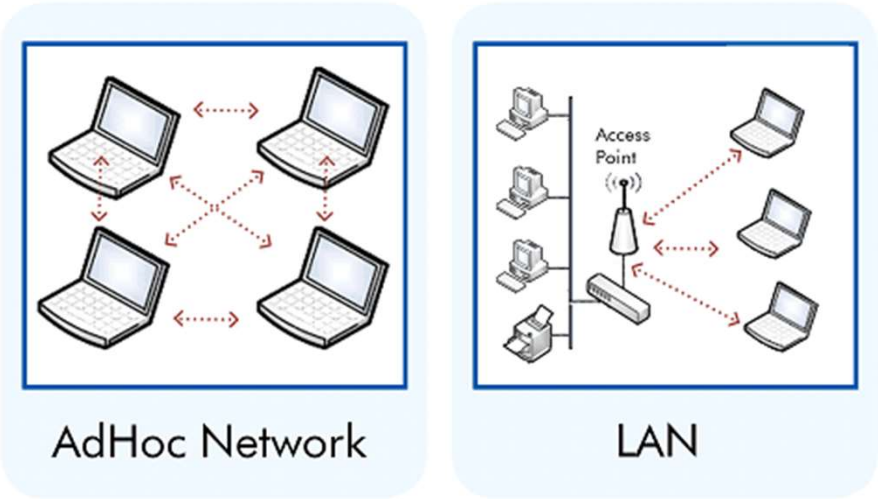


SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

- **TDD**
  - Time division duplex (TDD) refers to duplex communication links where uplink is separated from downlink by the allocation of different time slots in the same frequency band.
  - It is a transmission scheme that allows asymmetric flow for uplink and downlink data transmission.
- **FDD**
  - Frequency-division duplexing (FDD) is a method for establishing a full-duplex communications link that uses two different radio frequencies for transmitter and receiver operation.
  - The transmit direction and receive direction frequencies are separated by a defined frequency offset.

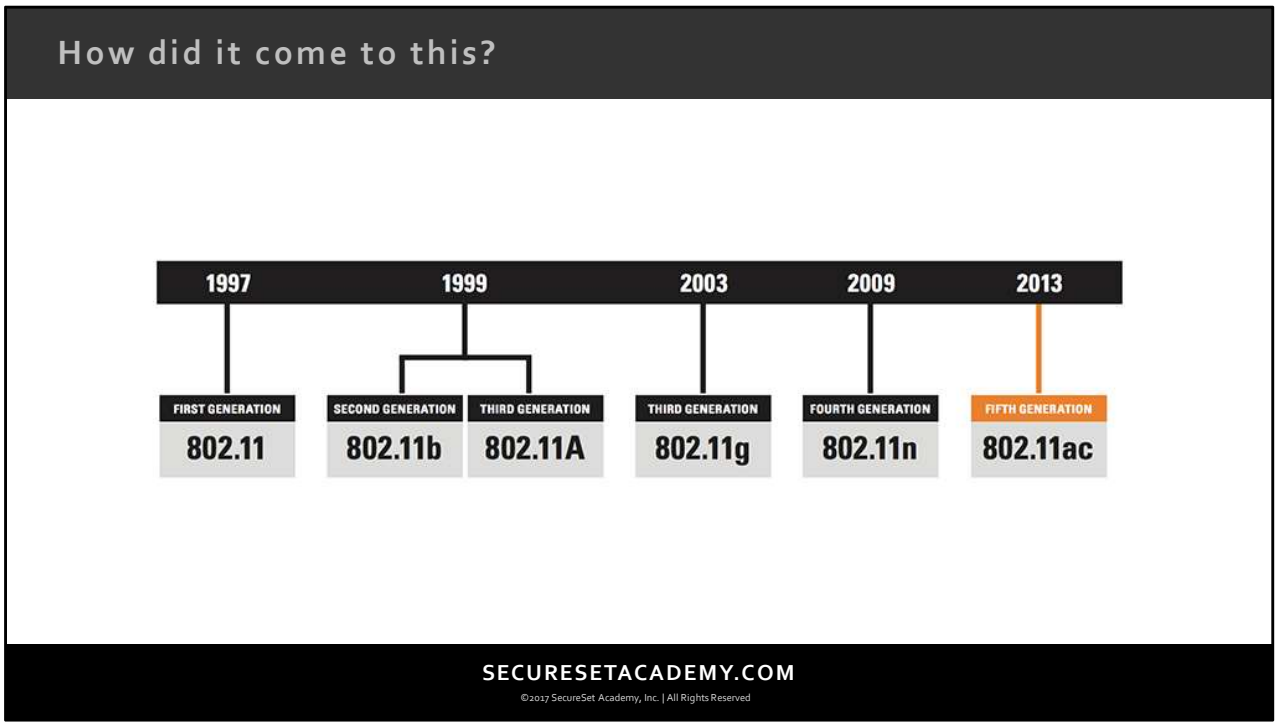
Basics of Communication – Traffic Modalities



SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

- In computer networking, infrastructure mode is when a network joins devices together, either through wired or wireless means, via an access point like a router. This centralization is what sets infrastructure mode apart from the ad-hoc mode.
- Setting up an infrastructure mode network requires at least one wireless access point (AP) and that the AP and all the clients be configured to use the same network name (SSID).
- The access point is cabled to the wired network to allow wireless clients access to resources like the internet or printers.
- Additional APs can be joined to this network to increase the reach of the infrastructure and support more wireless clients.
- Home networks with wireless routers support infrastructure mode automatically since these types of devices include a built-in AP.
- Newer equipment can create a “mesh” mode where you seamlessly get handed off from AP to AP and it works together to avoid generating interference.



Wi-Fi was first released to consumers in **1997**, its standards have been continually evolving – typically resulting in faster speeds and further coverage.

As capabilities are added to the original IEEE 802.11 standard, they become known by their **amendment (802.11b, 802.11g, etc.).**

Here we'll discuss the basics of each 802.11 Wi-Fi standard.

802.11b - 1999

- 802.11b uses the same 2.4 GHz frequency as the original 802.11 standard. It supports a maximum theoretical rate of 11 Mbps and has a range up to 150 feet. 802.11b components are cheap, but the standard has the slowest maximum speed of all the 802.11 standards.
    - And since 802.11b operates in the 2.4 GHz, home appliances or other 2.4 GHz Wi-Fi networks can cause interference. Today, routers that only support 802.11n are no longer manufactured.

802.11a - 1999

- The 'a' amendment to the standard was released at the same time as 802.11b. It

introduced a more complex technique, known as OFDM **(orthogonal frequency division multiplexing)** for generating the wireless signal. 802.11a offers a few advantages over 802.11b: it operates in the less crowded 5 GHz frequency band, making it less prone to interference.

- And its bandwidth is much higher than 802.11b, with a theoretical max of 54 Mbps.
- You probably haven't encountered many 802.11a devices or routers. This is because 802.11b devices were cheaper and became more popular in the consumer market. 802.11a was mainly used in business applications.

802.11g - 2003

- The **802.11g** standard uses the same OFDM technology introduced with **802.11a**. Like **802.11a**, it supports a maximum theoretical rate of **54 Mbps**.
    - But like 802.11b, it operates in the crowded **2.4 GHz** (and thus is subject to the same interference issues as **802.11b**). **802.11g** is backward compatible with **802.11b** devices: an **802.11b** device can connect to an **802.11g** access point (but at 802.11b speeds).
    - With 802.11g, consumers enjoyed a significant advance in Wi-Fi speeds and coverage. At the same time, consumer wireless routers were getting better, with higher power and better coverage than earlier generations.

802.11n

- With the **802.11n** standard, **Wi-Fi** became even faster and more reliable. It supports a maximum theoretical transfer rate of **300 Mbps** (and can reach up to **450 Mbps when using three antennae**).
    - **802.11n** uses **MIMO** (Multiple Input Multiple Output) where multiple transmitters/receivers operate simultaneously at one or both ends of the link.
    - This provides a significant increase in data without needing a higher bandwidth or transmit power. **802.11n** operates in both the 2.4 GHz and 5 GHz bands.

802.11ac - 2014

- **802.11ac** supercharges Wi-Fi, with speeds ranging from 433 Mbps all the way up to several Gigabits per second.
    - To achieve this kind of performance, **802.11ac** works exclusively in the **5 GHz band, supports up to eight spatial streams** (compared with 802.11n's four streams), doubles the channel width up to 80 MHz, and uses a technology called **beamforming**.
    - With beamforming, the antennae basically transmit the radio signals so they're directed at a specific device.
    - Another significant advancement with **802.11ac** is multi-user (**MU-MIMO**).

- As you can see Wi-Fi performance continues to evolve, with potential speeds and performance nearing wired speeds.

Standards

TABLE 1: IEEE 802.11 PHY STANDARDS

Release date	Standard	Band (GHz)	Bandwidth (MHz)	Modulation	Advanced antenna technologies	Maximum data rate
1997	802.11	2.4	20	DSSS, FHSS	N/A	2 Mbits/s
1999	802.11b	2.4	20	DSSS	N/A	11 Mbits/s
1999	802.11a	5	20	OFDM	N/A	54 Mbits/s
2003	802.11g	2.4	20	DSSS, OFDM	N/A	54 Mbits/s
2009	802.11n	2.4, 5	20, 40	OFDM	MIMO, up to four spatial streams	600 Mbits/s
2012 (expected)	802.11ad	60	2160	SC, OFDM	Beamforming	6.76 Gbits/s
2013 (expected)	802.11ac	5	40, 80, 160	OFDM	MIMO, MU-MIMO, up to eight spatial streams	6.93 Gbits/s

SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

Please note that 2.4GHz is licensed, 5 GHz is not.

Standards 2.0

802.11 Wireless Standards

IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Year Adopted	1999	1999	2003	2009	2014
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Max. Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Typical Range Indoors*	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Typical Range Outdoors*	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

- Wi-Fi most commonly uses the 2.4 gigahertz (12 cm) UHF and 5.8 gigahertz (5 cm) SHF ISM radio bands
- These bands are subdivided into multiple channels. Each channel can be time-shared by multiple networks.
- These wavelengths work best for line-of-sight. Many common materials absorb or reflect them, which further restricts range, but can tend to help minimize interference between different networks in crowded environments.
- At close range, some versions of Wi-Fi, running on suitable hardware can achieve speeds of over 1 Gbps.

Lets start talking Spectrum

Range	Center Frequency	Bandwidth
6.765–6.795 MHz	6.78 MHz	30 kHz
13.553–13.567 MHz	13.56 MHz	14 kHz
26.957–27.283 MHz	27.12 MHz	326 kHz
40.66–40.7 MHz	40.68 MHz	40 kHz
433.05–434.79 MHz	433.92 MHz	1.84 MHz
902–928 MHz	915 MHz	26 MHz
2.4–2.5 GHz	2.45 GHz	100 MHz
5.725–5.875 GHz	5.8 GHz	150 MHz
24–24.25 GHz	24.125 GHz	250 MHz
61–61.5 GHz	61.25 GHz	500 MHz
122–123 GHz	122.5 GHz	1 GHz
244–246 GHz	245 GHz	2 GHz

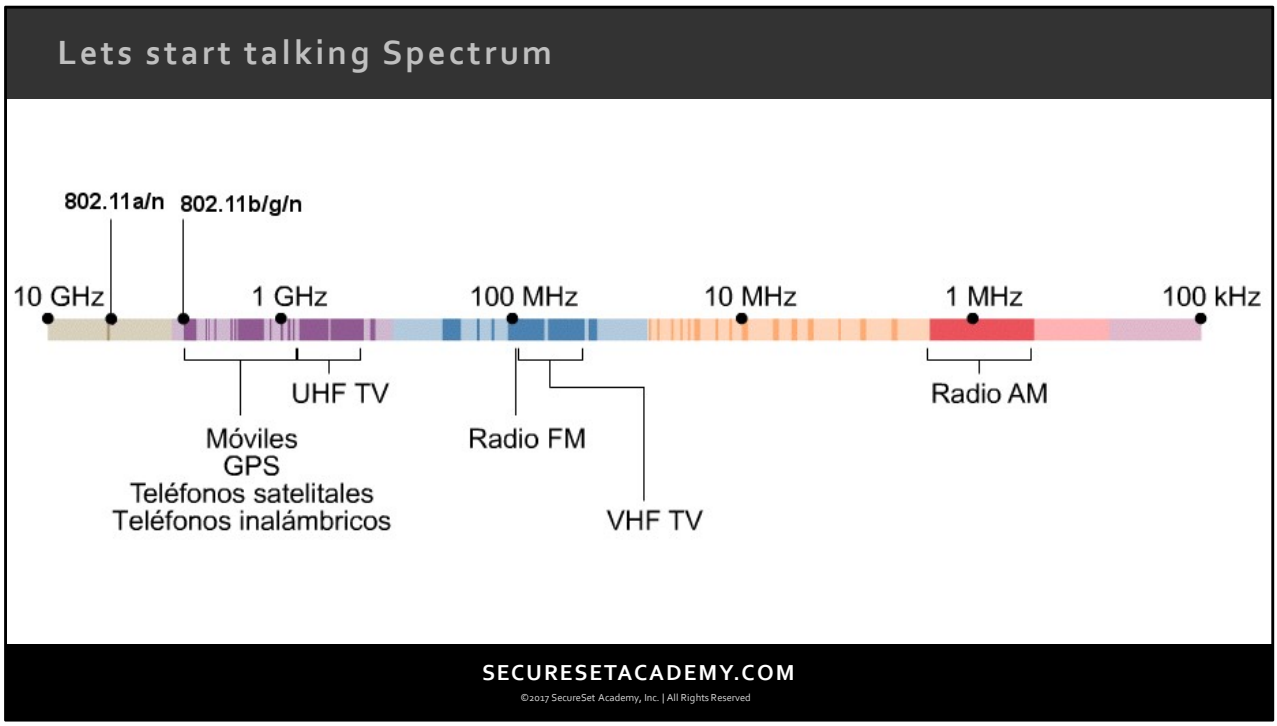
1.4.2. Multiple Channels Utilization

SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

6.765 MHz -> 246 GHz

The **industrial, scientific and medical (ISM) radio bands** are radio bands (portions of the radio spectrum) reserved internationally for the use of radio frequency (RF) energy for industrial, scientific and medical purposes other than telecommunications.



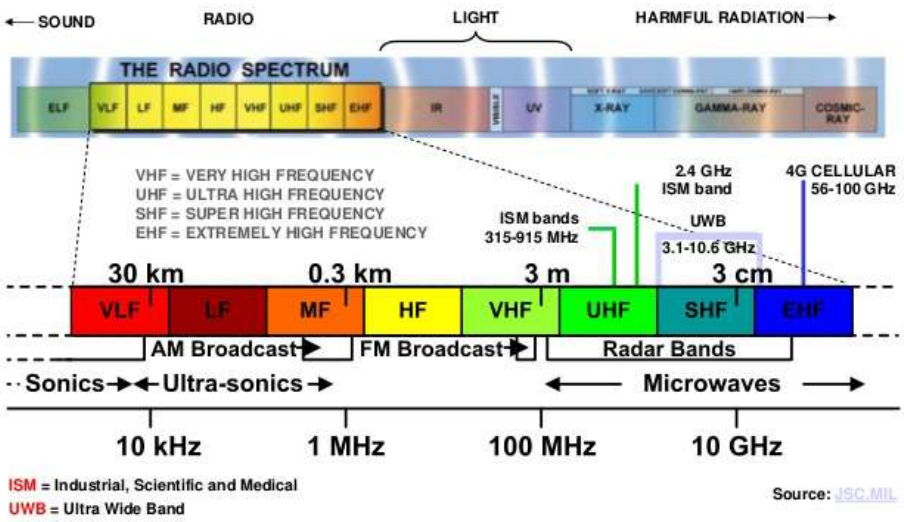
6.765 MHz -> 246 GHz

Different view of the spectra.

Understand that the spectrum that was released by Analog Television in 2009 ushered in a new age of Wireless communication. 2G Cellular jumped to 3G and 4G LTE by using the spectra that was given up by Analog Television.

Carriers spend billions of dollars to the FCC to obtain these frequencies.

Lets start talking Spectrum



SECURESETACADEMY.COM

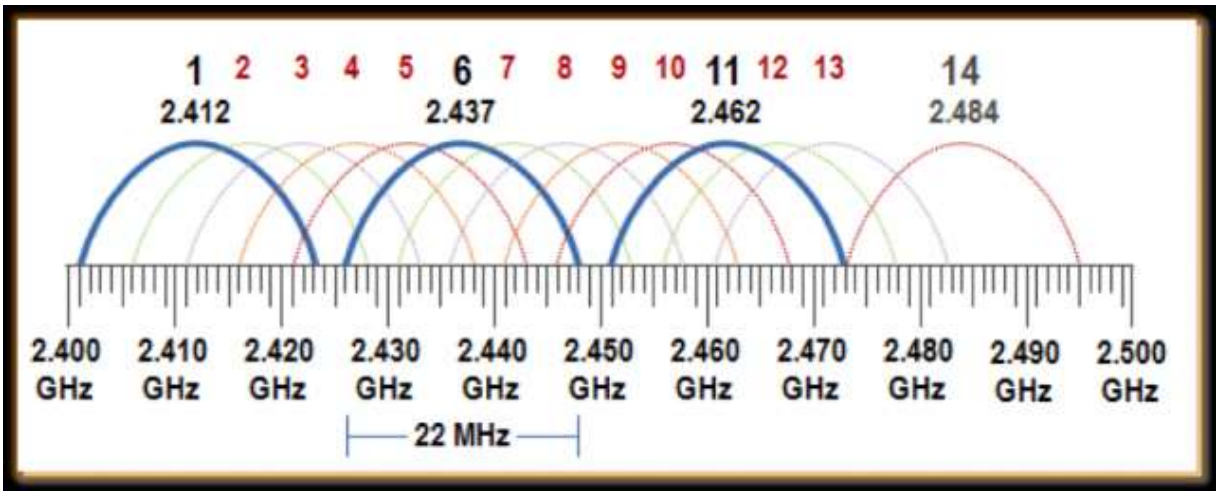
©2017 SecureSet Academy, Inc. | All Rights Reserved

6.765 MHz -> 246 GHz

Examples of applications in these bands include radio-frequency process heating, microwave ovens, and medical diathermy machines.

The powerful emissions of these devices can create electromagnetic interference and disrupt radio communication using the same frequency, so these devices were limited to certain bands of frequencies. In general, communications equipment operating in these bands must tolerate any interference generated by ISM applications, and users have no regulatory protection from ISM device operation.

2.4 GHz



SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

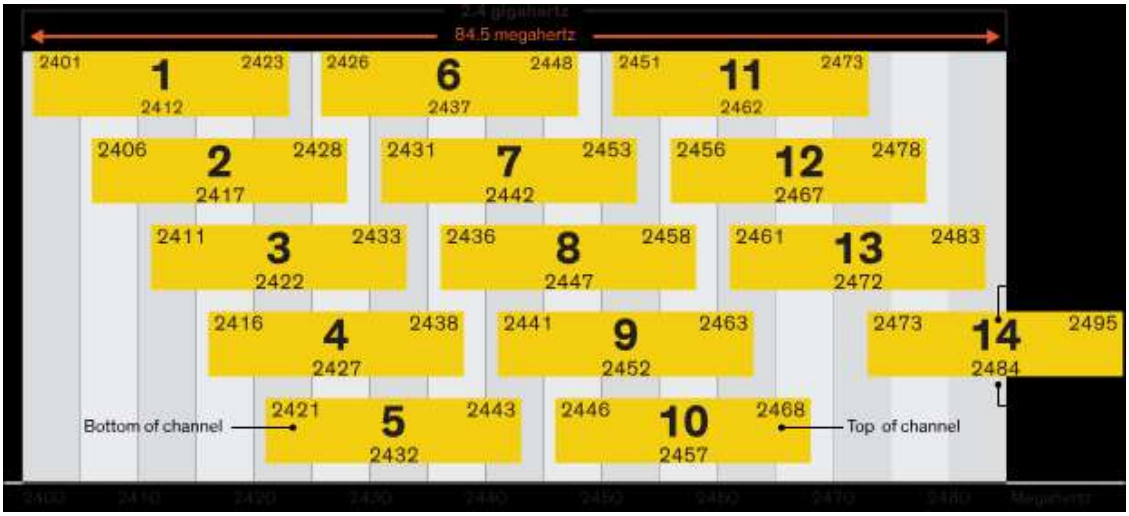
- 802.11b and 802.11g use the 2.4 GHz ISM band, operating in the United States under Part 15 Rules and Regulations.

- Because of this choice of frequency band, 802.11b and g equipment may occasionally suffer interference from microwave ovens, cordless telephones, USB3.0 hubs, and Bluetooth devices.

    - Spectrum assignments and operational limitations are not consistent worldwide: Australia and Europe allow for an additional two channels (12, 13) beyond the 11 permitted in the United States for the 2.4 GHz band, while Japan has three more (12–14).

    - In the US and other countries, 802.11a and 802.11g devices may be operated without a license, as allowed in Part 15 of the FCC Rules and Regulations.

2.4 GHz



SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

- A Wi-Fi signal occupies five channels in the 2.4 GHz band. Any two channel numbers that differ by five or more, such as 2 and 7, do not overlap.

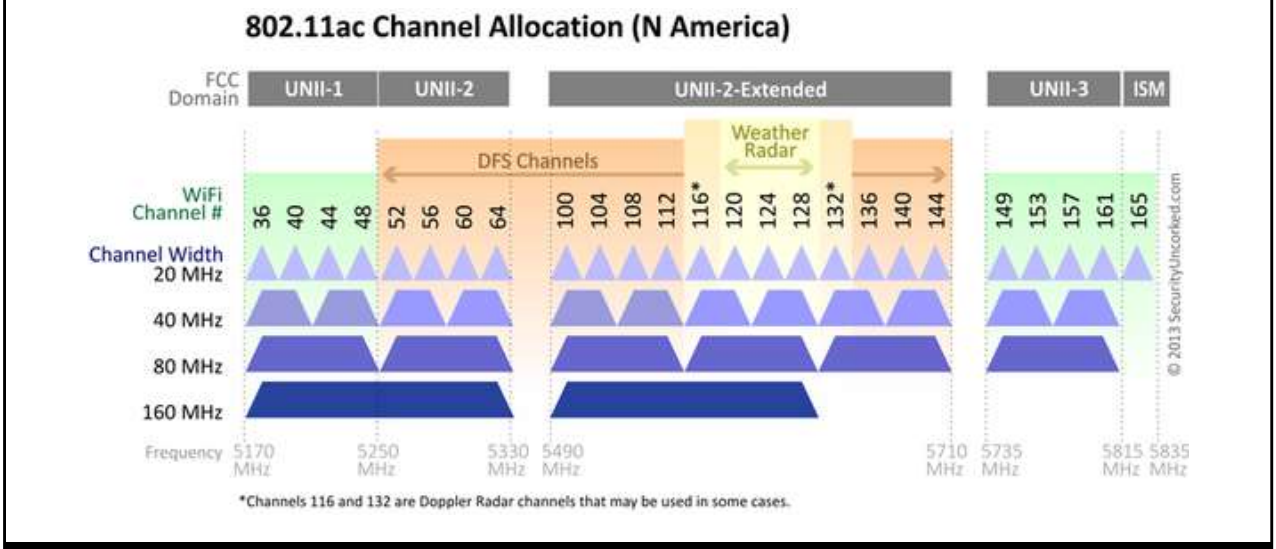
- The oft-repeated adage that channels **1, 6, and 11** are the *only* non-overlapping channels is, therefore, not accurate.

- However the **1, 6, and 11** are considered discrete and the most efficient channelization to use.

- Channels 1, 6, and 11 are the only *group of three* non-overlapping channels in North America and the United Kingdom.
- In Europe and Japan using Channels 1, 5, 9, and 13 for 802.11g and 802.11n is recommended.

- 802.11a uses the 5 GHz U-NII band, which, for much of the world, offers at least 23 non-overlapping channels rather than the 2.4 GHz ISM frequency band, where adjacent channels overlap.

5 GHz



SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

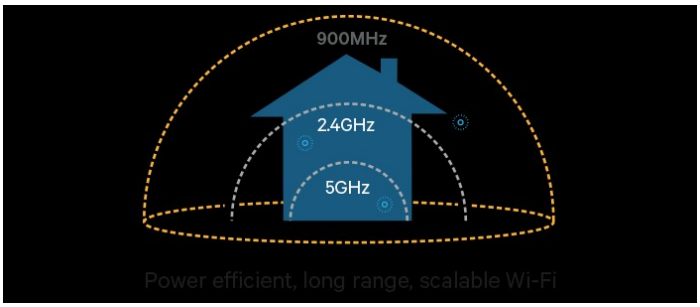
- As the 2.4 GHz band becomes more crowded, many users are opting to use the 5 GHz ISM band. This not only provides more spectrum, but it is not as widely used by Wi-Fi as well as many other appliances including items such as microwave ovens, etc.
- It will be seen that many of the 5 GHz Wi-Fi channels fall outside the accepted ISM unlicensed band and as a result various restrictions are placed on operation at these frequencies.

- **5GHz** there are four "**Bands**" available, each containing a bunch of WiFi channels.
- The first band, UNII-1, is designed mainly for domestic use because from Unii-2 upwards, your router needs to have DFS (dynamic frequency selection)
- and TPC (transmit power control) built in, which will automatically adjust the channel and power output of your router so it doesn't interfere with military, radar, weather station signals and so on.
- The 5GHz channels generally don't overlap (unlike many of the 2.4GHz ones), because in many countries contiguous channels are "bonded" to have a higher bandwidth.
- This means that on your router you may see that the channels are all four numbers apart. There are twenty-three non-overlapping channels at 5GHz, as opposed to

just three at 2.4GHz, making each channel equally good when it comes to not having interference from other channels.

- The higher channel numbers, operating at higher frequencies, tend to be used by radar, weather stations, and the military. If that happens while you're using your WiFi, then your signal may be bumped to another frequency.
    - This shouldn't be an issue, though it can cause momentary interference as your channel gets switched.
    - There are also some old phone models that still operate at the higher frequencies/channels, though the likelihood of this affecting your signal is very small.
- With all that said, **perhaps it's best to stick to the channels in the first "Band**" I talked about earlier (36, 40, 44, 48), because these are designated for domestic use and are least likely to get interference from exterior factors.
- As these tend to be the "default" channels, there will be more people using them, which is why you should use a WiFi checker to find which ones are least congested while offering you the best signal.

2.4 GHz vs 5GHz Ranges

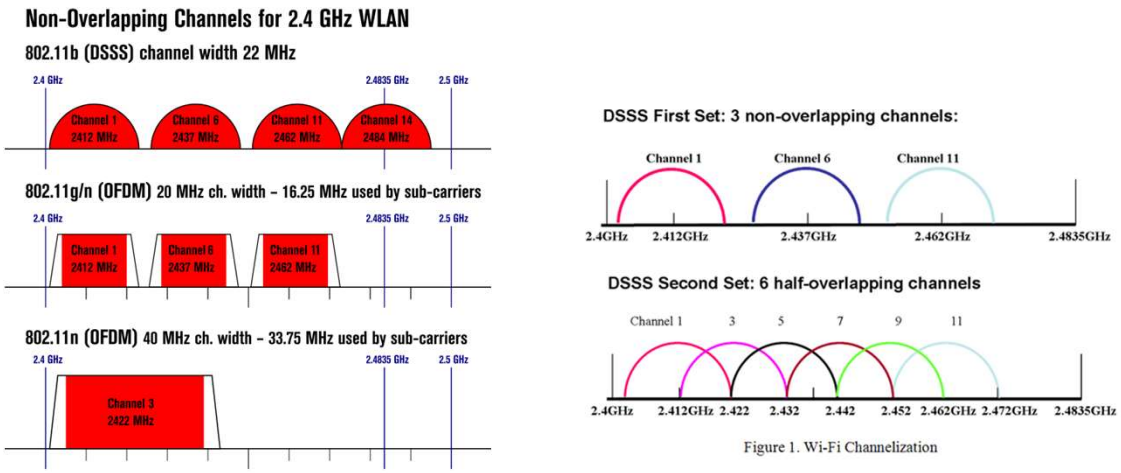


SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

- The primary differences between the 2.4 GHz and 5GHz wireless frequencies are range and bandwidth.
    - 5GHz provides faster data rates at a shorter distance
    - Whereas 2.4GHz offers coverage for farther distances, but may perform at slower speeds.

Frequency Technologies

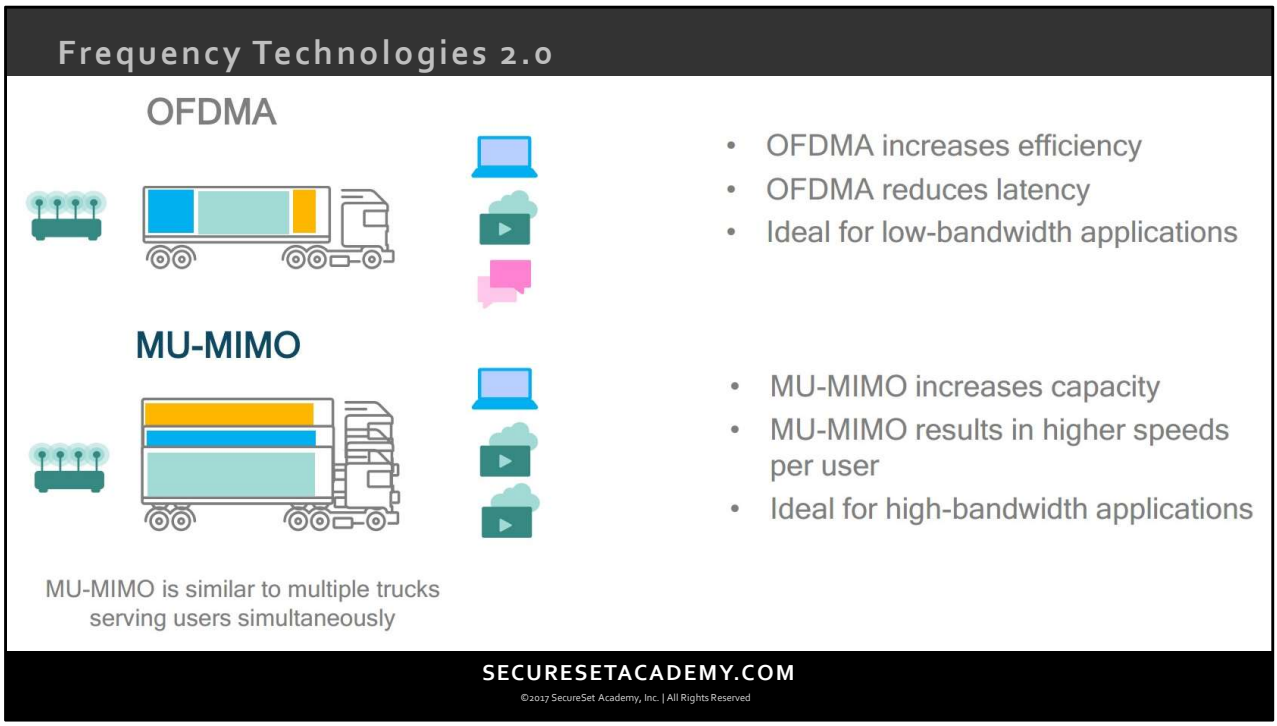


SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

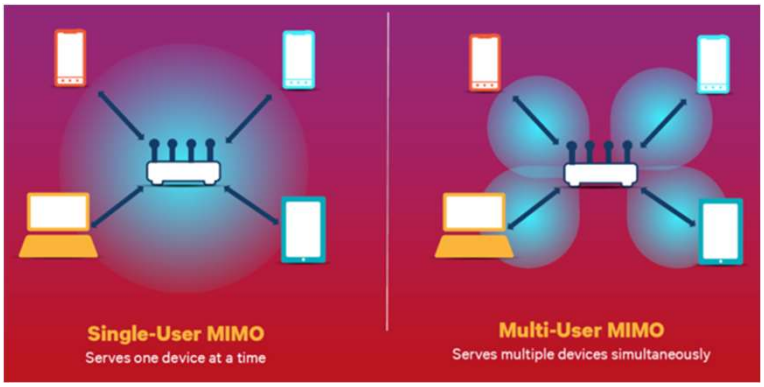
- (**DSSS**)
  - **direct-sequence spread spectrum**
  - is a spread spectrum modulation technique used to reduce overall signal interference. The spreading of this signal makes the resulting wideband channel more noisy, allowing for greater resistance to unintentional and intentional interference.

- **OFDM**
  - Orthogonal frequency-division multiplexing
  - a method of encoding digital data on multiple carrier frequencies. OFDM has developed into a popular scheme for wideband digital communication, used in applications such as digital television and audio broadcasting, DSL internet access, wireless networks, power line networks, and 4G mobile communications.



- **OFDMA**
  - **Orthogonal frequency-division multiple access**
  - is a multi-user version of the popular orthogonal frequency-division multiplexing (OFDM) digital modulation scheme. Multiple access is achieved in OFDMA by assigning subsets of subcarriers to individual users. This allows simultaneous low-data-rate transmission from several users.
- MU-MIMO
  - Multi-user MIMO
  - a set of multiple-input and multiple-output (MIMO) technologies for wirelesscommunication, in which a set of users or wireless terminals, each with one or more antennas, communicate with each other.[1] In contrast, single-user MIMO considers a single multi-antenna transmitter communicating with a single multi-antenna receiver. In a similar way that OFDMA adds multiple access (multi-user) capabilities to OFDM, MU-MIMO adds multiple access (multi-user) capabilities to MIMO. MU-MIMO has been investigated since the beginning of research into multi-antenna communication

MIMO



SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

So what is MIMO?
SU-MIMO = Single user, Multiple in-Multiple out
MU-MIMO = Multiple user, Multiple in-Multiple out

- Multiple Antennas - Ever wondered why the new WAP/MAP(s) look like spiders?

- The majority of Wi-Fi devices—especially in phones and tablets—are 1x1 devices, because the additional antennas and signal processing requires more space and power in the mobile devices, which adds extra cost and requires more power from the battery.

- Using multi-user multiple-input, multiple-output (MU-MIMO) technology, a wireless routers can transmit to and receive data from multiple Wi-Fi devices at the same time. Although the devices must also support MU-MIMO to utilize it, they aren’t required to have multiple antennas.

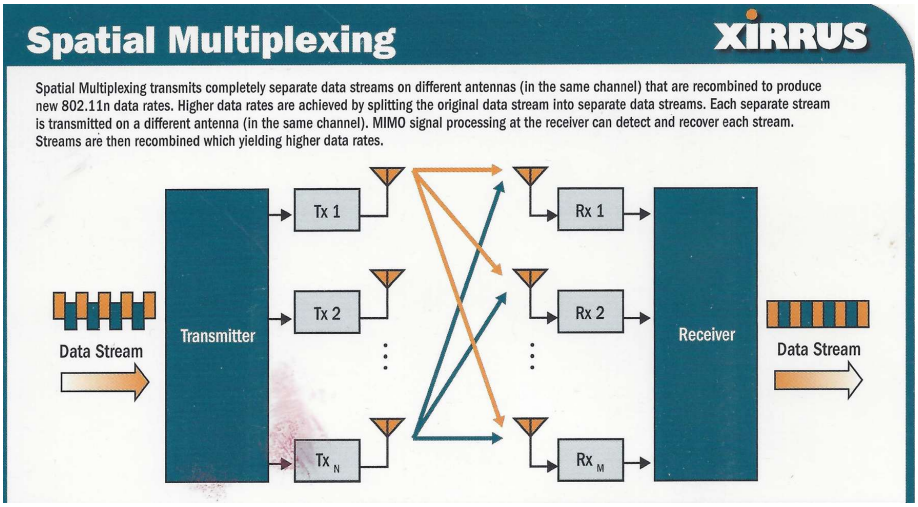
- It's important to remember that, unlike SU-MIMO, MU-MIMO currently works only with downlink wireless connections. Only wireless routers and APs are able to simultaneously send data to multiple users, whether it's one or more streams of

data to each.

- The wireless devices themselves (such as smartphones, tablets or laptops) still must take turns sending data to the wireless router or AP, although they can individually utilize SU-MIMO to send multiple streams when it's their turn.

- SU-MIMO works in both the 2.4GHz and 5GHz Wi-Fi frequency bands, but MU-MIMO doesn’t.

MIMO 2.0

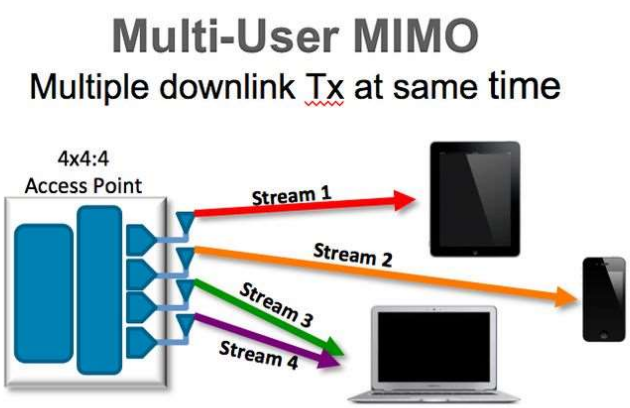


SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

- Wireless routers and APs can simultaneously serve multiple users only in the higher band.
- Unfortunately, a MU-MIMO router or AP can't simultaneously serve unlimited streams and devices. A router or AP has a certain number of streams it supports
- For instance, a four-stream AP may choose to simultaneously serve four different one-stream devices or a single one-stream device and a single three-stream device.
- You'll see the biggest advantages of MU-MIMO when there are simpler devices on the network that support just one or two streams vs. those supporting three or four streams. That's because the technology doesn't speed up individual connections, but rather increases total network throughput by serving multiple devices at once.

MIMO 3.0



SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

- Multi-user MIMO (MU-MIMO) can leverage multiple users as spatially distributed transmission resources, at the cost of somewhat more expensive signal processing.
    - In comparison, conventional, or single-user MIMO considers only local device multiple antenna dimensions. Multi-user MIMO algorithms are developed to enhance MIMO systems when the number of users or connections is greater than one. Multi-user MIMO can be generalized into two categories: MIMO broadcast channels (MIMO BC) and MIMO multiple access channels (MIMO MAC) for downlink and uplink situations, respectively. Single-user MIMO can be represented as point-to-point, pairwise MIMO.
- To remove ambiguity of the words *receiver* and *transmitter*, we can adopt the terms *access point* (AP; or, *base station*), and *user*. An AP is the transmitter and a user is the receiver for downlink environments, whereas an AP is the receiver and a user is the transmitter for uplink environments. Homogeneous networks are somewhat freed from this distinction.

Beamforming

SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

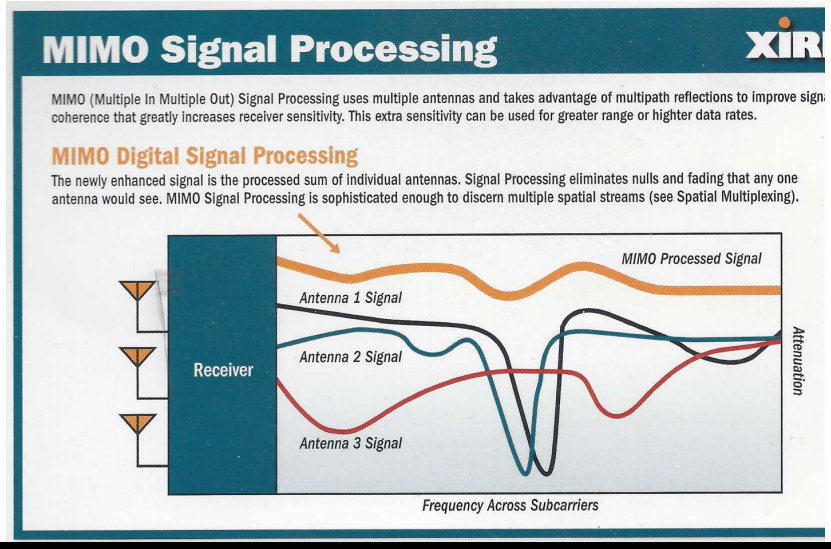
- Devices that support beamforming focus their signals toward each client, concentrating the data transmission so that more data reaches the targeted device instead of radiating out into the atmosphere.

- Think of putting a shade on the lamp (the wireless router) to reduce the amount of light (data) radiating in all directions. Now poke holes in the shade, so that concentrated beams of light travel to defined locations (your Wi-Fi clients) in the room.

- If the Wi-Fi client also supports beamforming, the router and client can exchange information about their respective locations in order to determine the optimal signal path.

- Any device that beamforms its signals is called a beamformer, and any device that receives beamformed signals is called a beamformee.

MIMO and Beamforming – Aggregation of Signal



SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

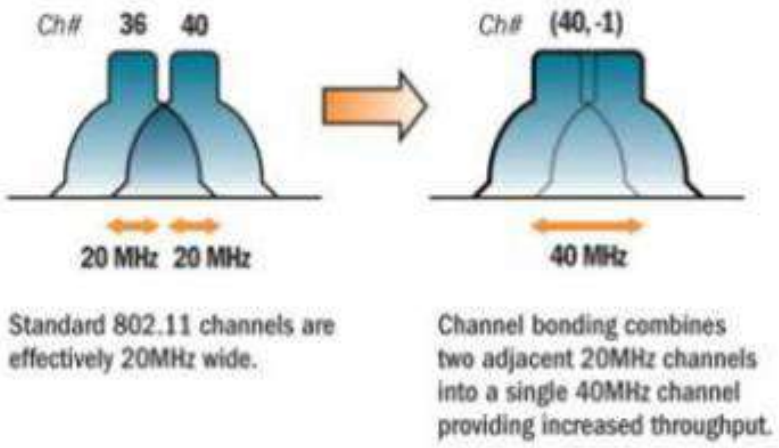
One caveat about MU-MIMO: It doesn't work well with rapidly moving devices, as the beamforming process becomes more difficult and less effective.

Thus, the technology might not provide much benefit in networks with constantly roaming devices.

However, these problem devices shouldn't affect the MU-MIMO transmissions to devices that are more stationary, nor their performance.

Digital Signal Processing the AGGREGATE of multiple signals to create a much better connection.

Channel Bonding



SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

- Channel bonding is a practice commonly used in IEEE 802.11 implementations in which two adjacent channels within a given frequency band are combined to increase throughput between two or more wireless devices.

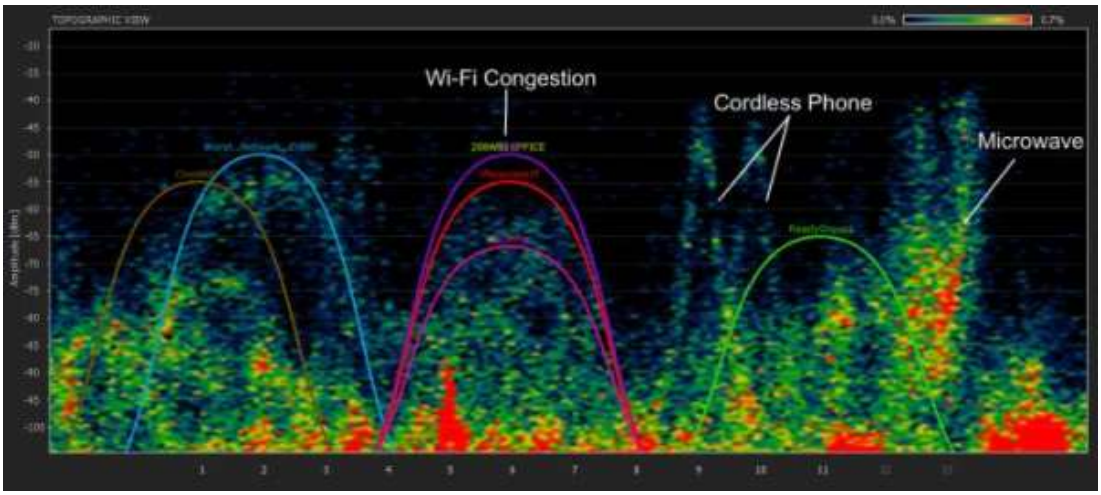
- It has become a very popular technique in the world of Wi-Fi because its increased throughput provides for more functionality within Wi-Fi deployments.

- Channel bonding is commonly practiced in Wi-Fi networks, which typically operate within the 2.4 GHz frequency band.

- The 2.4 GHz frequency band has room for three non-overlapping bonded channels. Within 802.11n deployments this translates into a theoretical throughput of 54 Mbps.

- The combination of these non-overlapping channels is often referred to as increasing the size of the pipe.
- 5GHz channel bonding works in 802.11ac

So why does Wi-Fi suck sometimes?

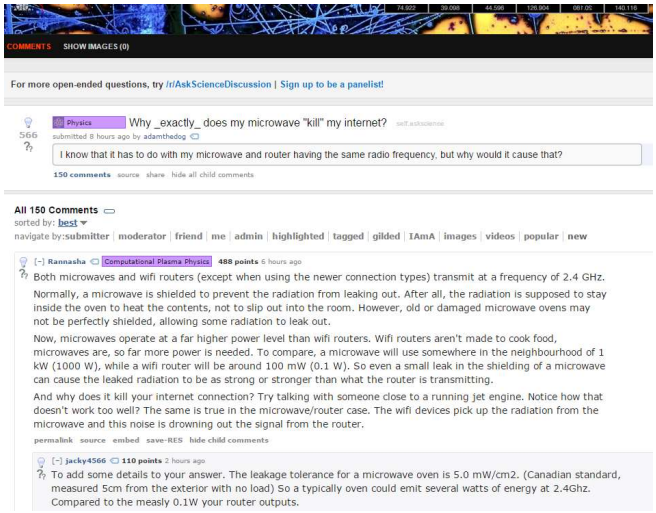


SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

- Wi-Fi connections can be disrupted or the Internet speed lowered by having other devices in the same area. Wi-Fi protocols are designed to share channels reasonably fairly, and will often work with little to no disruption.
- However, many 2.4 GHz 802.11b and 802.11g access-points default to the same channel on initial startup, contributing to congestion on certain channels.
- Wi-Fi pollution, or an excessive number of access points in the area, can prevent access and interfere with other devices' use of other access points as well as with decreased signal-to-noise ratio(SNR) between access points.
- In addition interference can be caused by overlapping channels in the 802.11g/b spectrum.
- These issues can become a problem in high-density areas, such as large apartment complexes or office buildings with many Wi-Fi access points.

Microwaves don't melt steel beams?



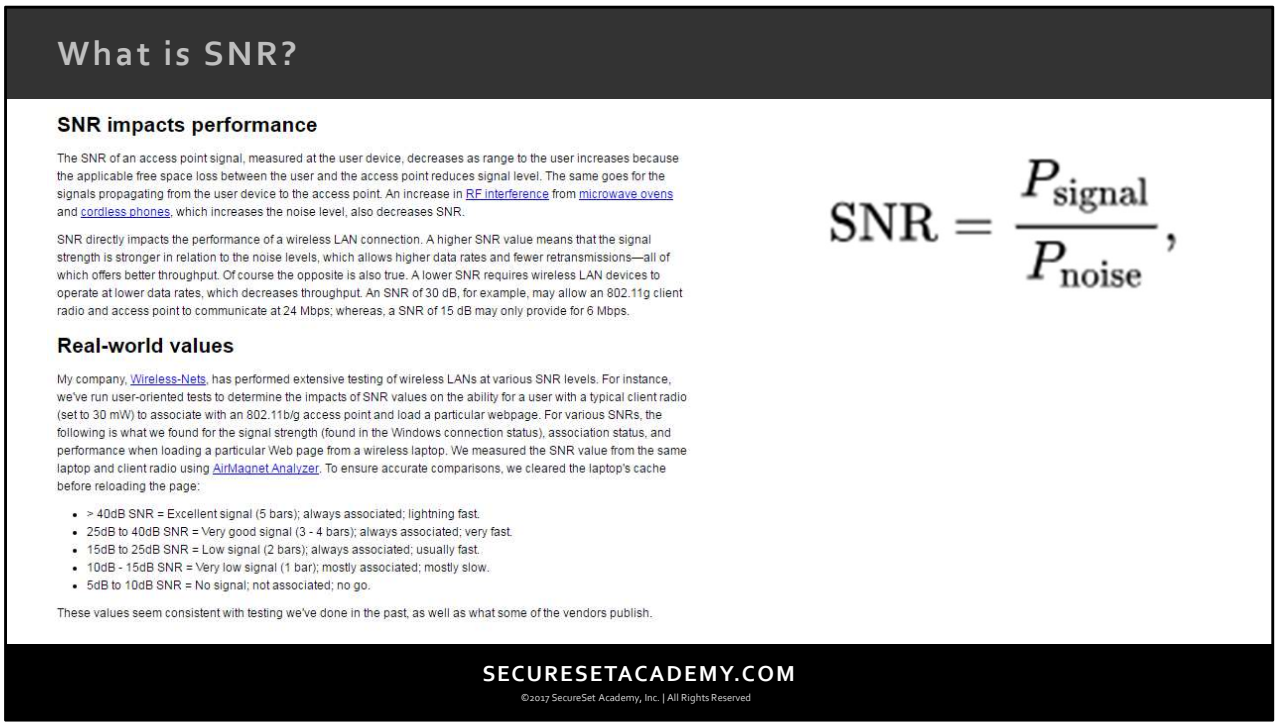
SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

- Additionally, other devices use the 2.4 GHz band: microwave ovens, ISM band devices, security cameras, ZigBee devices, Bluetooth devices, video senders, cordless phones, baby monitors, and, in some countries, amateur radio, all of which can cause significant additional interference.

- These bands are allowed to be used with low power transmitters, without requiring a license and with few restrictions.

- However, while unintended interference is common, users that have been found to knowingly cause deliberate interference to other users, particularly for attempting to locally monopolize these bands for commercial purposes, have been handed large fines.

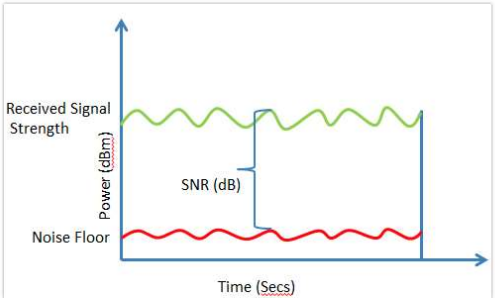


Signal-to-noise ratio (abbreviated **SNR** or ***S/N***) is a measure used in science and engineering that compares the level of a desired signal to the level of background noise. SNR is defined as the ratio of signal power to the noise power, often expressed in decibels. A ratio higher than 1:1 (greater than 0 dB) indicates more signal than noise.

Because many signals have a very wide dynamic range, signals are often expressed using the logarithmic decibelscale. Based upon the definition of decibel, signal and noise may be expressed in decibels (dB)

SNR and Noise Floor

SNR is not actually a ratio but the difference in decibels between the received signal and the background noise level (noise floor). For example, if a radio (client device) receives a signal of -75 dBm and the noise floor is measured at -90 dBm, the SNR is 15 dB. Data corruption and therefore re-transmissions will occur if the received signal is too close to the noise floor. In 802.11 networks, re-transmissions adversely affect throughput and latency.

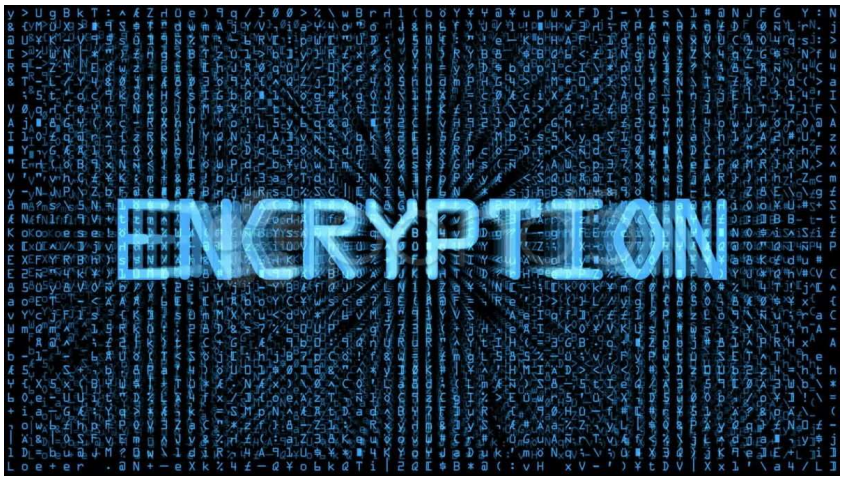


SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

SNR is usually taken to indicate an *average* signal-to-noise ratio, as it is possible that (near) instantaneous signal-to-noise ratios will be considerably different. The concept can be understood as normalizing the noise level to 1 (0 dB) and measuring how far the signal 'stands out'

Wi-Fi – Why do we use Encryption?



SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

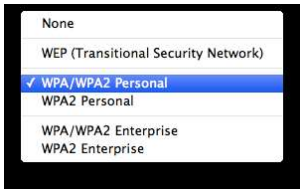
- Encryption protects our data.
    - It protects our data when it's sitting on our computers and in data centers, and it protects it when it's being transmitted around the Internet. It protects our conversations, whether video, voice, or text. It protects our privacy. It protects our anonymity.
    - This protection is important for everyone. It's easy to see how encryption protects journalists, human rights defenders, and political activists in authoritarian countries. But encryption protects the rest of us as well. It protects our data from criminals. It protects it from competitors, neighbors, and family members. It protects it from malicious attackers, and it protects it from accidents.
    - Encryption works best if it's ubiquitous and automatic. The two forms of encryption you use most often -- https URLs on your browser, and the handset-to-tower link for your cell phone calls -- work so well because you don't even know they're there.

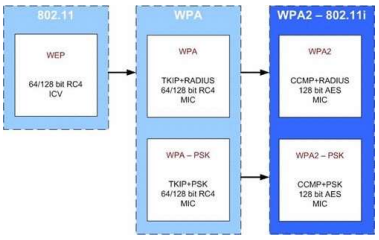
- Encryption should be enabled for everything by default, not a feature you turn on only if you're doing something you consider worth protecting.

- This is important. If we only use encryption when we're working with important data, then encryption signals that data's importance. If only dissidents use encryption in a country, that country's authorities have an easy way of identifying them. But if everyone uses it all of the time, encryption ceases to be a signal. No one can distinguish simple chatting from deeply private conversation. The government can't tell the dissidents from the rest of the population. Every time you use encryption, you're protecting someone who needs to use it to stay alive.

Wi-Fi Security

	Authentication	Encryption	Suitable for corporate WAN	Suitable for home and small business WLAN
WEP	none	WEP	poor	less than good
WPA (PSK)	PSK	TKIP	poor	best
WPA2 (PSK)	PSK	AES-CCMP	poor	best
WPA (full)	802.1x	TKIP	better	good (expensive)
WPA2 (full)	802.1x	AES-CCMP	best	good (expensive)





SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

Even though it is kind of logical to secure your WiFi network, it is sometimes a bit puzzling to understand which encryption protocol to implement with all the abbreviations.

- WEP
- WPA
- WPA2
- WPA3

Personal
Enterprise

Wi-Fi Security

SECURESETACADEMY.COM

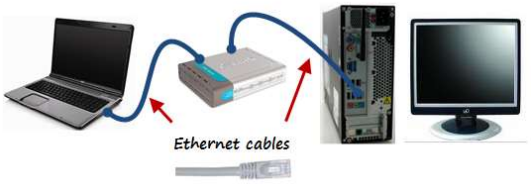
©2017 SecureSet Academy, Inc. | All Rights Reserved

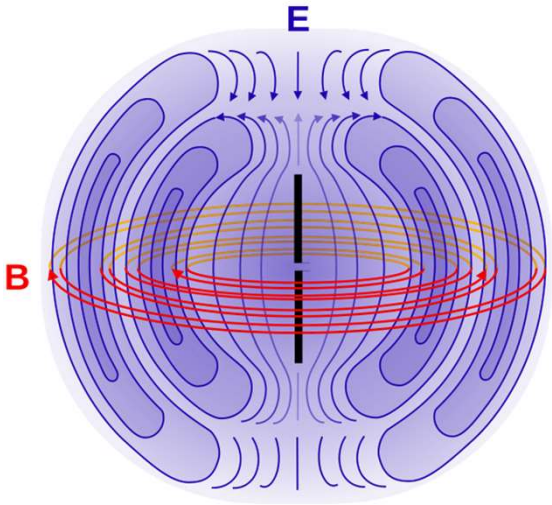
- WiFi security algorithms have been through many changes and upgrades since the 1990s to become more secure and effective.
- Different types of wireless security protocols were developed for home wireless networks protection.
- The wireless security protocols are WEP, WPA, and WPA2, serving the same purpose but being different at the same time.
- Not only do the protocols prevent unwanted parties from connecting to your wireless network, but also wireless security protocols encrypt your private data sent over the airwaves.

- WEP
- WPA
- WPA2
- WPA3

Personal
Enterprise

Wi-Fi Security





SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

- No matter how protected and encrypted, wireless networks cannot keep up in safety with wired networks.
- The latter, at their most basic level, transmit data between two points, A and B, connected by a network cable.
- To send data from A to B, wireless networks **broadcast it within their range in every direction to every connected device that happens to be listening**.

Wired Equivalent Privacy (WEP)

SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

- **Wired Equivalent Privacy (WEP)**

  WEP was developed for wireless networks and approved as a Wi-Fi security standard in September, 1999. WEP was aimed to offer the same security level as wired networks, however there are a bunch of well-known security issues in WEP, which is also easy to break and hard to configure.

- Passwords were in Hexadecimal

- Despite all the work that has been done to improve the WEP system it still is a highly vulnerable solution. Systems that rely on this protocol should be either upgraded or replaced in case security upgrade is not possible. WEP was officially abandoned by the Wi-Fi Alliance in 2004.

Wi-Fi Protected Access (WPA)

SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

- For the time the 802.11i wireless security standard was in development, WPA was used as a temporary security enhancement for WEP.
- One year before WEP was officially abandoned, WPA was formally adopted.
- Most modern WPA applications use a preshared key (PSK), most often referred to as WPA Personal, and the Temporal Key Integrity Protocol or TKIP (/tiːˈkɪp/) for encryption.
- WPA Enterprise uses an authentication server for keys and certificates generation.
- WPA was a significant enhancement over WEP, but as the core components were made so they could be rolled out through firmware upgrades on WEP-enabled devices, they still relied onto exploited elements.
- **WPA, just like WEP, after being put through proof-of-concept and applied public demonstrations turned out to be pretty vulnerable to intrusion.**
- The attacks that posed the most threat to the protocol were however not the

direct ones, but those that were made on Wi-Fi Protected Setup

- (WPS) - auxiliary system developed to simplify the linking of devices to modern access points.

Wi-Fi Protected Access Version 2 (WPA2)

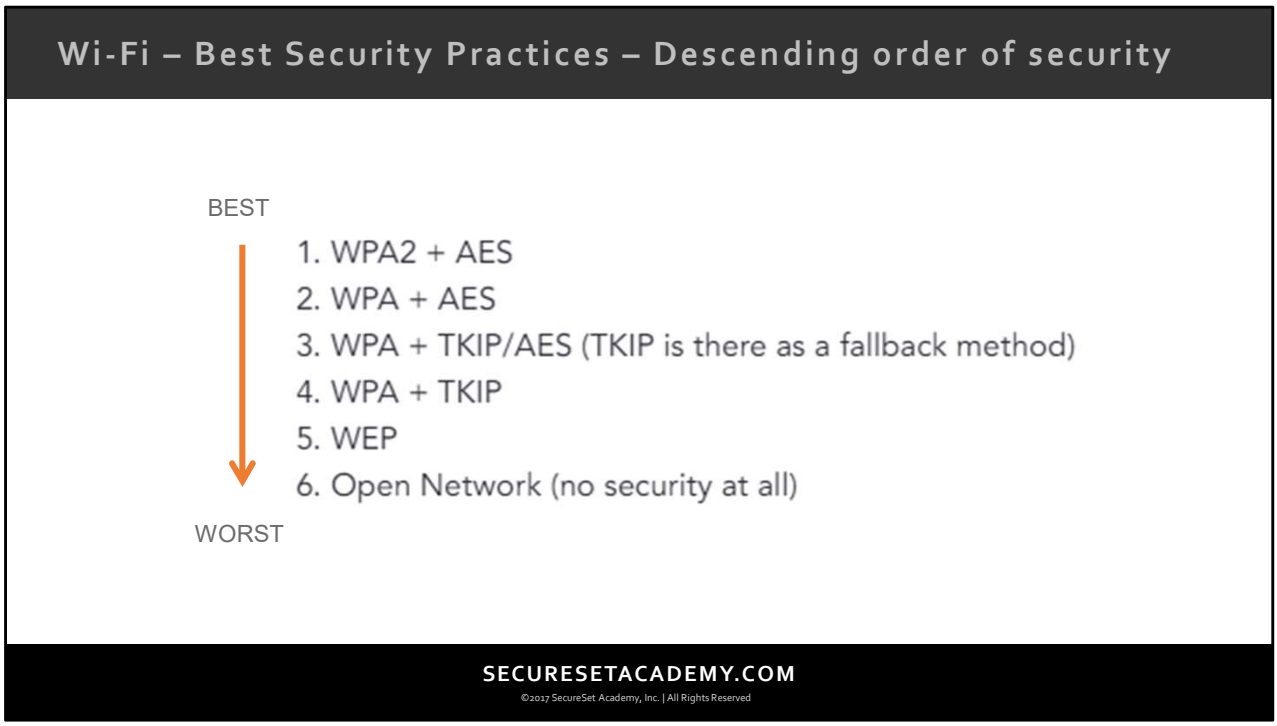
SECURESETACADEMY.COM

©2017 SecureSet Academy, Inc. | All Rights Reserved

- The 802.11i wireless security standard based protocol was introduced in 2004
    - The most important improvement of WPA2 over WPA was the usage of the Advanced Encryption Standard (AES) for encryption. AES is approved by the U.S. government for encrypting the information classified as top secret, so it must be good enough to protect home networks.
    - At this time the main vulnerability to a WPA2 system is when the attacker already has access to a secured WiFi network and can gain access to certain keys to perform an attack on other devices on the network. This being said, the security suggestions for the known WPA2 vulnerabilities are mostly significant to the networks of enterprise levels, and not really relevant for small home networks.
    - Unfortunately, the possibility of attacks via the Wi-Fi Protected Setup (WPS), is still high in the current WPA2-capable access points, which is the issue with WPA too.
    - And even though breaking into a WPA/WPA2 secured network through this

hole will take anywhere around 2 to 14 hours it is still a real security issue

- **WPS should be disabled and it would be good if the access point firmware could be reset to a distribution not supporting WPS to entirely exclude this attack vector.**



- The best way to go is deactivate Wi-Fi Protected Setup (WPS) and set the router to WPA2 +AES. And as you go down the list, the less secure your network is going to get.

- Most consumers will not have access to the enterprise methodology of AES, which requires a AAA or Radius server to authenticate vs a security schema such as Active Directory.

- Most if not all consumers will reasonably pick the TKIP methodology.

- TKIP (Temporal Key Integrity Protocol) is an encryption protocol included as part of the IEEE802.11i standard for wireless LANs (WLANs).

- TKIP is a suite of algorithms that works as a "wrapper" to WEP, which allows users of legacy WLAN equipment to upgrade to TKIP without replacing hardware.
    - TKIP uses the original WEP programming but "wraps" additional code at the beginning and end to encapsulate and modify it.

Wi-Fi – Hacking 102

SECURESETACADEMY.COM

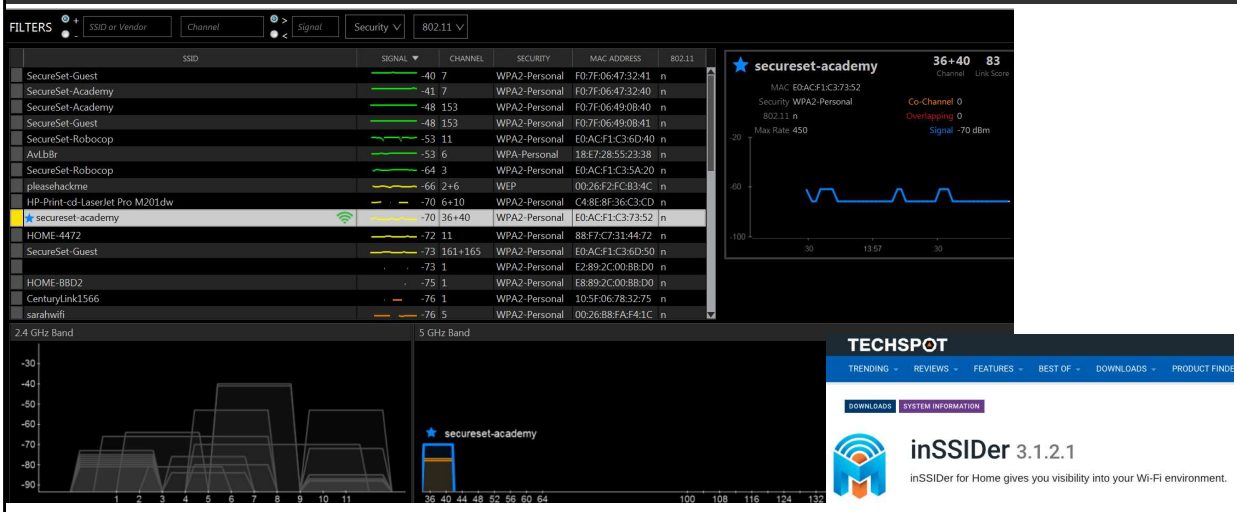
©2017 SecureSet Academy, Inc. | All Rights Reserved

Stay Tuned for our next iteration of Hacking 102 Wi-Fi – How does it break.

We will cover more in depth:

- Troubleshooting
- How does Wi-Fi encryption work – More Detail
- How to break that encryption
- More industrial and enterprise versions and applications of Wi-Fi

Wi-Fi Application Spectrum Analyzer - Windows



https://www.techspot.com/downloads/5936-inssider.html

SECURESETACADEMY.COM

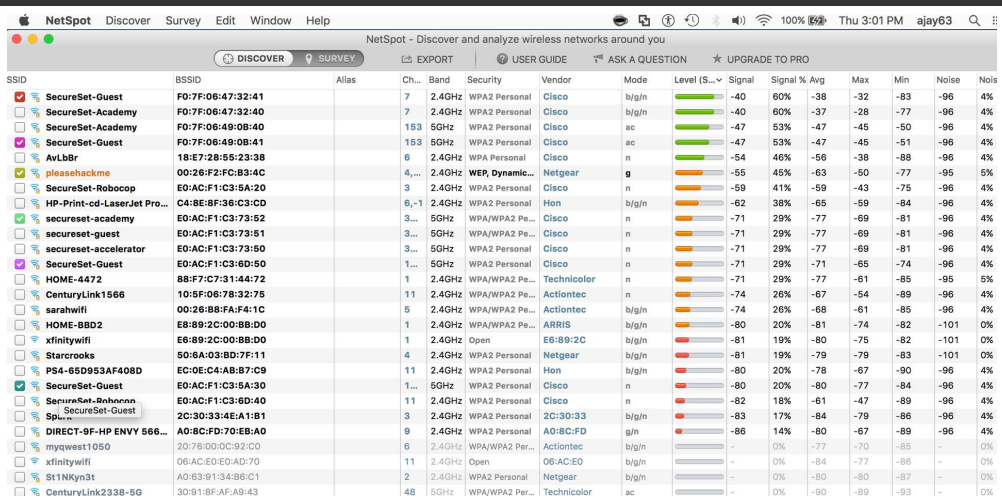
©2017 SecureSet Academy, Inc. | All Rights Reserved

inSSIDer 3.1.2.1 is the last “FREE” version of their product.

This Wi-Fi network discovery tool displays every wireless hotspot’s MAC address, encryption, signal strength and channel, and is the standard troubleshooting tool for millions of Wi-Fi users throughout the world.

https://www.techspot.com/downloads/5936-inssider.html

Wi-Fi Application Spectrum Analyzer – OSx and Windows



https://www.netspotapp.com/download-other.html

©2017 SecureSet Academy, Inc. | All Rights Reserved

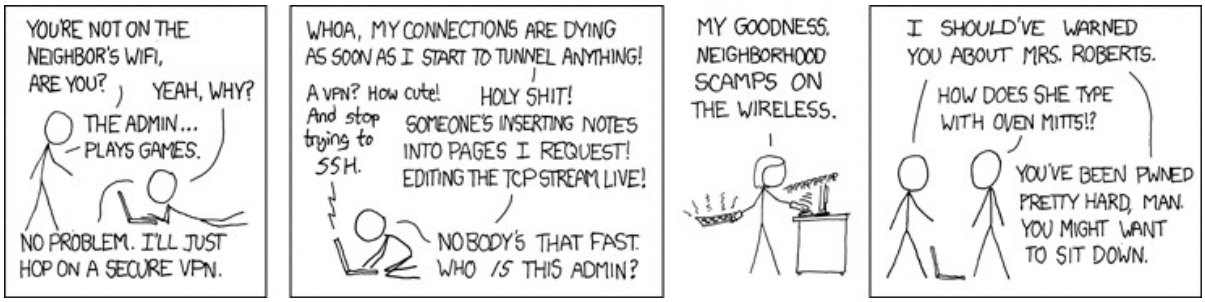
https://www.netspotapp.com/download-other.html

Wi-Fi surveys are the key feature of **NetSpot**.

You run a survey by walking, marking your position on the map, giving NetSpot a few seconds to collect data samples, watching Wi-Fi networks being detected and visualized.

15+ heatmap coverage graphs are available with powerful customizable reports.

Wi-Fi 101



PLEASE BROWSE TO:

HTTPS://GITHUB.COM/AJAY63/WI-FI-101

©2017 SecureSet Academy, Inc. | All Rights Reserved

Wi-Fi – Hacking 101 Labs

The labs for this WIFI Hacking 101 are pretty benign and are meant as take home.

Using one of the previously shown Wi-Fi Analyzers

1. Analyze multiple Wi-Fi networks in different locations
2. Are you able to find unsecured networks?
3. Are you able to identify multiple access points using the same frequency?
4. Are you able to identify interreference?
5. Are you able to identify printers and other IoT devices creating ad-hoc Wi-Fi?
6. Are you able to identify access points that might be transmitting intermittently?

©2017 SecureSet Academy, Inc. | All Rights Reserved