WIFI

Book **Beginner's guide to wi-fi wireless networking**

Link :
http://etutorials.org/Networking/beginners+guide+to+wi-fi+wireless+networking/

By Harold Davis

WI FI

- **Wi-Fi**, also spelled **Wifi** or **WiFi**, is a local area wireless technology that allows an electronic device to exchange data or connect to the internet using 2.4 GHz UHF and 5 GHz SHF radio waves.
- The Wi-Fi Alliance defines Wi-Fi as any "wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards".
- However, since most modern WLANs are based on these standards, the term "Wi-Fi" is used in general English as a synonym for "WLAN".
- Only Wi-Fi products that complete Wi-Fi Alliance interoperability certification testing successfully may use the "Wi-Fi CERTIFIED" trademark.

Wi-Fi Alliance

Formation	1999; 22 years ago
Headquarters	Austin, Texas, United States
Website	www.wi-fi.org
Formerly called	Wireless Ethernet Compatibility Alliance

- The Wi-Fi Alliance is a not-for-profit organization
- Certifies the interoperability of wireless devices built around the 802.11 standard.
- Goals: to promote interoperability of devices based on 802.11, and, presumably, to promote and enhance the standard.
- For better or worse, this is no neutral organization.
- The members of the Wi-Fi Alliance are manufacturers that build 802.11 devices.

Wi-Fi Alliance® surpasses 50,000 Wi-Fi CERTIFIED™ products

Wi-Fi CERTIFIED ensures consumer satisfaction with Wi-Fi®

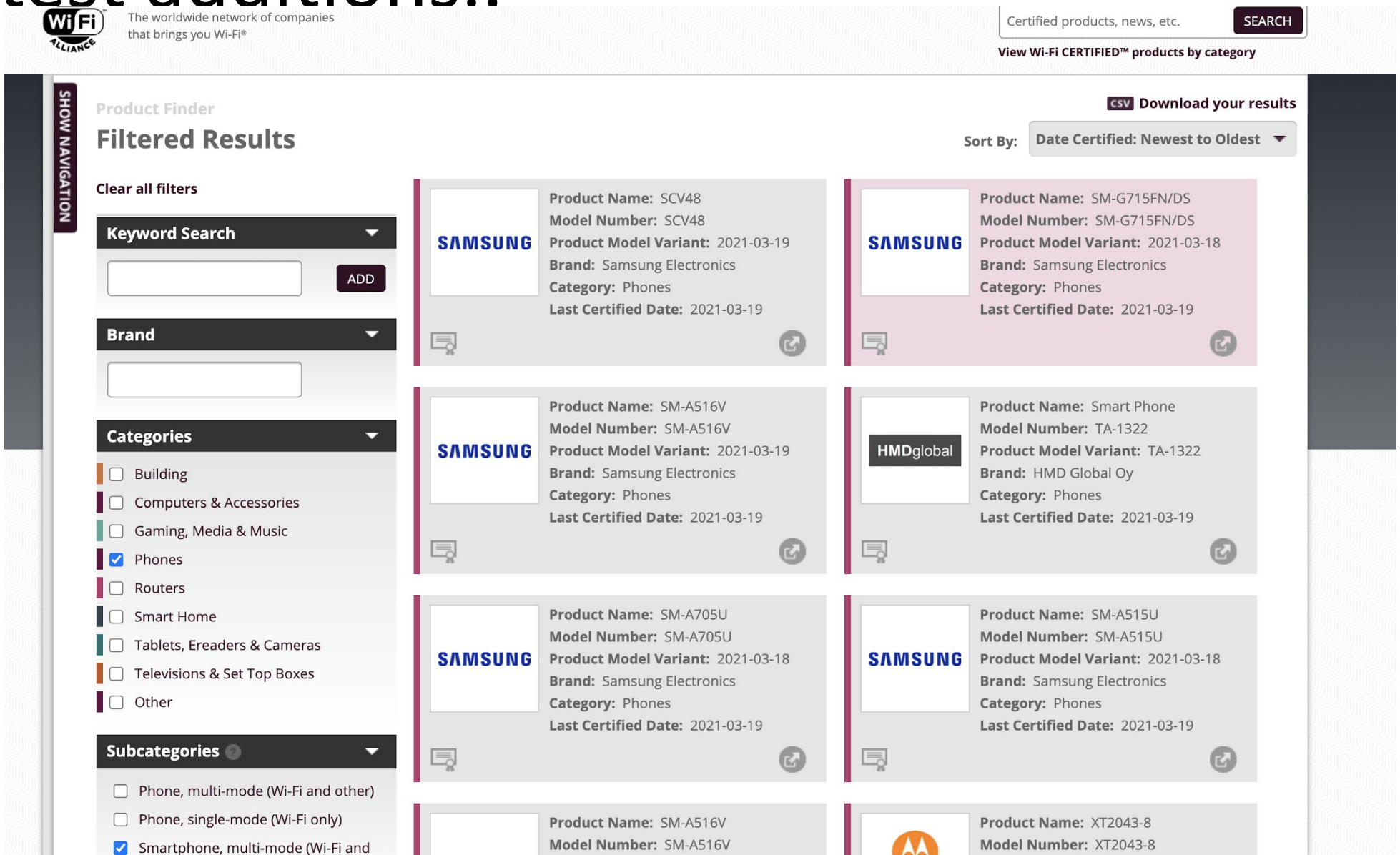
January 13, 2020 [illegible] ET | Source: Wi-Fi Alliance

- As of this writing, there are 850 companies that belong to the Wi-Fi Alliance and more than 50000 products that have been certified as Wi-Fi interoperable.

  The promise that the Wi-Fi Alliance makes is that if you buy an 802.11 device with the Wi-Fi seal of certification, the device will work seamlessly with any other Wi-Fi certified device.

- You can find more information about the Wi-Fi Alliance at the Alliance's Web site, www.wi-fi.org.

Latest additions..



Wireless Spectrums

- Unlike many other wireless standards, 802.11 runs on "free" portions of the radio spectrum.
- This means that (unlike cell telephone communications) no license is required to broadcast or communicate using 802.11 (or Wi-Fi).
- The free portions of the radio spectrum used by 802.11 (Wi-Fi) are the 2.4GHz band, and the 5GHz band.

Many household appliances such as microwave ovens and (most significantly) wireless telephone handsets also use these free spectrums 2.4 GHz.

- The 802.11 (and Wi-Fi) standard includes what is called a physical layer. This physical layer uses something known as Direct Sequence Spread Spectrum technology (DSSS) to prevent collisions and avoid interference between devices operating on the same spectrum.
- You'll find much the same kind of technology in your wireless telephone handset. The idea here is that you don't want the signal coming out of your microwave unit to interfere with your email (or vice versa).
- In addition to its physical layer, each 802.11 Wi-Fi device has an access control layer. The access control layer specifies how a Wi-Fi device, such as a mobile computer, communicates with another Wi-Fi device, such as a wireless access point.

TIP

- If you find that your Wi-Fi device is getting interference from some other appliance such as a microwave or wireless telephone, one of the first things to try is moving either your Wi-Fi device, or the other device, to a new physical location.

Understanding WIFI-**The Free Spectrums**

- As you probably know, any signal that is sent without wires is called a radio transmission. A common example is that the radio in your car receives transmissions. Similarly, a standard cell phone works by receiving and transmitting radio signals.
- Every device that broadcasts a radio transmission does so at a particular *frequency.* The entire set of radio frequencies is known as the radio spectrum.
- **FM radio**, always remains at constant amplitude, so signal strength does not change. **FM** uses a higher frequency range and a bigger bandwidth **than AM**. This means that an **FM station** can transmit 15 times as much information as an **AM station** and explains why music sounds so much **better** on **FM.**

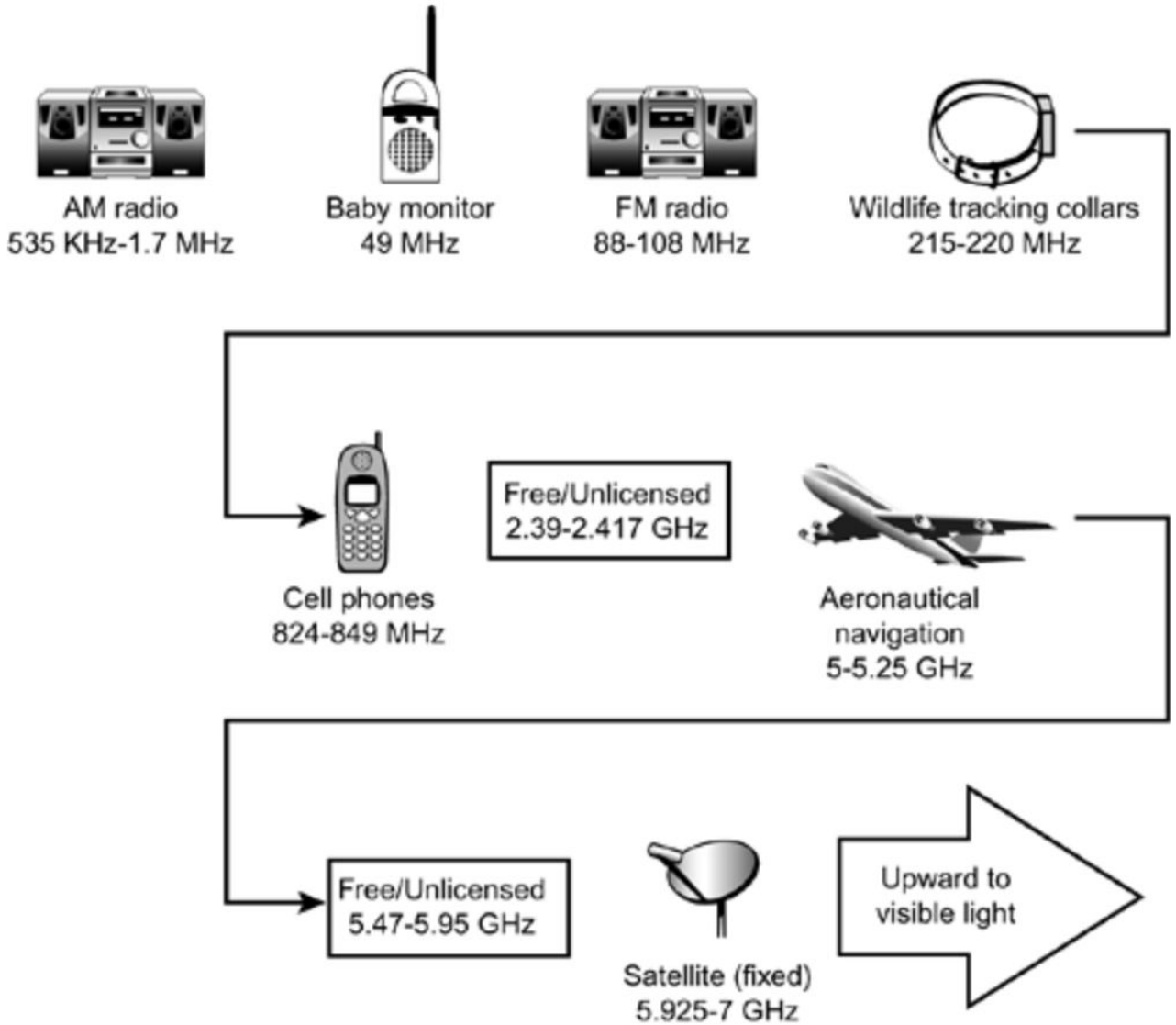
- Radio frequencies describe the oscillations of a radio wave. For example, if you are tuned to an FM radio station at 92.5, it means that the radio transmission is oscillating at 92.5 megahertz per second. 92.5 megahertz (pronounced "may-ga-hurts" and abbreviated MHz) means that the radio transmission wave oscillates, or moves from its valley to its peak, at a rate of 92,500,000 times per second.
- One thousand megahertz is equal to one gigahertz (pronounced "gig-a-hurts" and abbreviated GHz). So when you refer to the 2.4GHz frequency, you are actually talking about 2,400,000,000 (2.4 billion) oscillations per second.

- Although it is commonly referred to as the 2.4GHz band, the actual spectrum is 2.39GHz to 2.417GHz. In the case of the 5GHz spectrum band, the band actually runs from 5.47GHz to 5.725GHz.
- As a partial answer to frequency conflicts, the government has regulated the usage of most of these frequencies. In the United States, government regulation of radio frequencies is controlled by the Federal Communications Commission (FCC).

- Some frequencies are reserved for particular usages, such as the military.
- Others, such as the AM and FM bands, are licensed.
- This means that only the licensees can use the frequency for the purpose it was licensed.
- In addition, some areas of the spectrum have been set aside for unlicensed uses. These set-aside areas include the 2.4GHz and 5GHz spectrums, which is what Wi-Fi uses.

Figure 2.1. Selected uses for the radio spectrum.

[View full size image]



- The fact that the 2.4GHz and 5GHz frequencies have been set aside for unlicensed usages does have an extremely important implication: They are cheap to use.
- But there are some legal restrictions on what you can do within the free spectrums
- There are conflicts within the 5GHz band as well as the 2.4GHz band, but 5GHz band conflicts primarily concern competing usages such as radar and satellite radio, which are being ironed out by the FCC.
- Also, the 2.4GHz spectrum has become like a shanty town in which it is cheap to live. All kinds of transmission devices have crowded into the neighbourhood, from microwaves to cordless telephones. These devices can interfere with your Wi-Fi transmissions and reception.

The 802.11 Standard and Its Variations: 802.11b Standard

- When you say "Wi-Fi" today, you probably mean 802.11b, which is a subset of the general 802.11 standard. Most Wi-Fi devices that are currently in operation are using 802.11b. However, technology moves quickly, and 802.11g is gaining momentum fast.
- The full 802.11b specification document is more than 500 pages long, but here are the key things to know about 802.11b:
- The 802.11b standard uses the 2.4GHz spectrum.
- The 802.11b standard uses a technology called Direct Sequence Spread Spectrum (DSSS) to minimize interference with other devices transmitting on the 2.4GHz spectrum.

- The 802.11b standard has a theoretical throughput speed of 11 megabytes per second (Mbps).
- The **factor that slows down 802.11b Wi-Fi is that transmissions are in duplex mode**, which means that communication consists of a **query and a response** (rather than simultaneous communication). This slows down speeds noticeably.

The 802.11a and 802.11g Standards

- The 802.11a and 802.11g standards are different variants of 802.11 that can be thought of as 802.11b's smarter, younger brothers. The 802.11a standard uses the 5GHz band for transmission, which minimizes the possibility of interference with the plethora of 2.4GHz devices out there (think microwaves, garage door openers, and so on) and promises a theoretic throughput of 24Mbps.
- Still newer than 802.11a, 802.11g operates on the 2.4GHz spectrum and boasts throughput as fast as 54Mbps.
- In other words, **both 802.11a and 802.11g show the promise of being considerably faster than 802.11b**.

- The 802.11a standard poses some compatibility issues with 802.11b. But at least one vendor, Atheros Communications, makes 802.11a equipment that is backward- compatible with 802.11b. (Atheros also makes a "tri-mode" chipset that uses 802.11a, 802.11b, and 802.11g.) The chief advantage of 802.11a is that it will run into less interruption from other devices because it does not use the crowded 2.4GHz band.

- Moving to 802.11a has some pluses and minuses, but moving to 802.11g is a no-brainer, because 802.11g systems are backward-compatible with 802.11b, and faster. This backward compatibility of 802.11g devices is a requirement for Wi-Fi certification.
- In fact, the 802.11g standard is replacing 802.11b as the standard for new equipment (it is preferred to 802.11a because of its backward compatibility).
- 802.11g will be the de facto Wi-Fi standard that is at the "sweet" price point, and other, faster Wi-Fi standards such as 802.11n will be the new contender knocking at the door.

802.11n

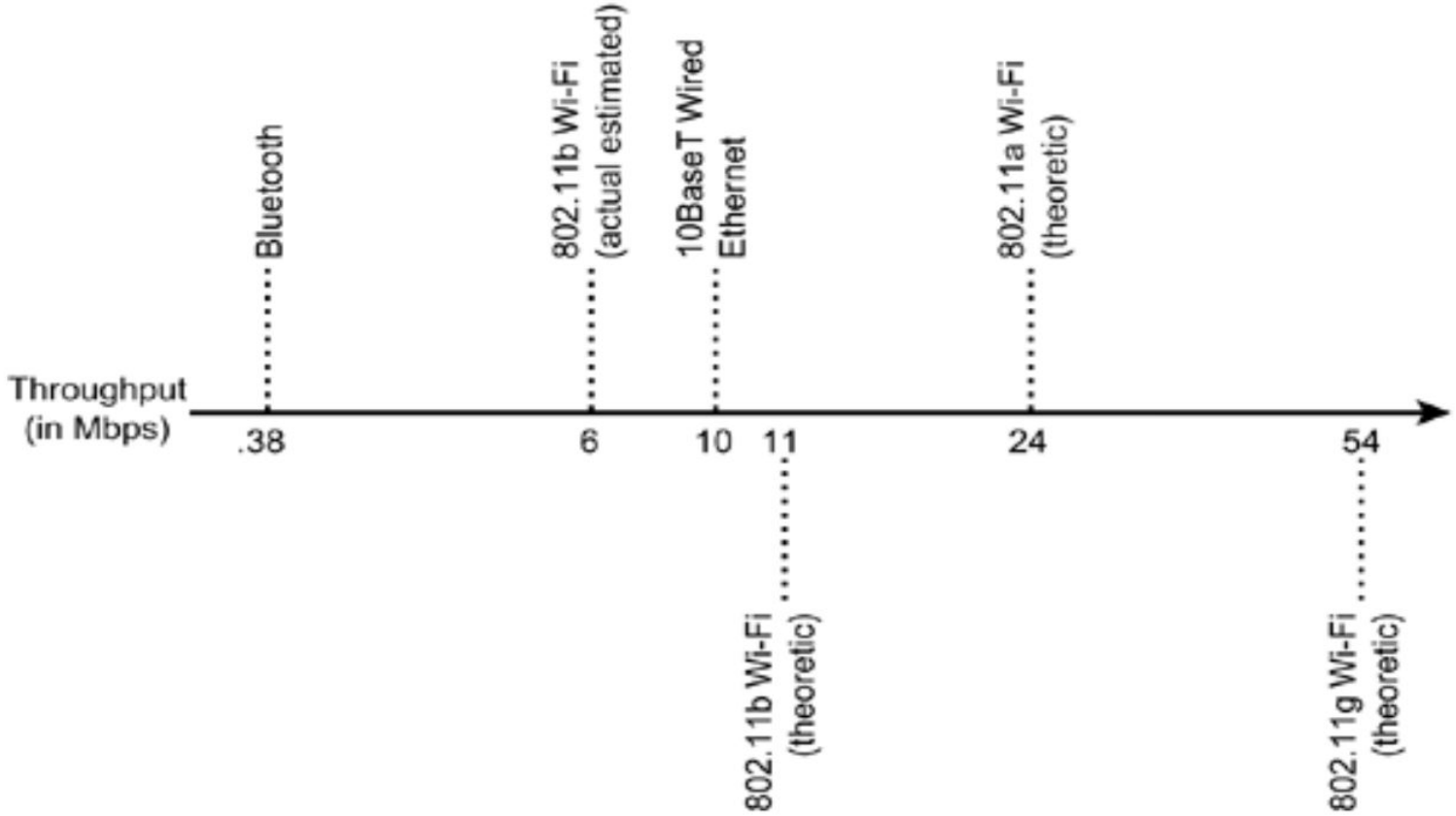
- IEEE 802.11n-2009 or 802.11n is a wireless-networking standard that uses multiple antennas to increase data rates.
- The Wi-Fi Alliance has also labelled the technology for the standard as Wi-Fi 4.
- It standardized support for multiple-input multiple-output, frame aggregation, and security improvements, among other features, and can be used in the 2.4 GHz or 5 GHz frequency bands.
- 802.11n uses multiple input / multiple output (MIMO) technology and a wider radio frequency channel. It also provides a mechanism called ***frame aggrega****tion* to decrease time between transmissions.
- Current WLAN technologies require that the sending station request the channel, send one packet, release the channel, and then request again in order to send the next packet. With frame aggregation, once a station requests the channel and has the authority to transmit, it can transmit a series of frames without having to release the channel and regain authority for each frame. With 802.11n, raw data throughput is expected to reach as much as 600 Mbps -- that's more than 10 times the throughput of 802.11g.

The 802.11i Standard

- The IEEE is in the process of developing a new security standard for 802.11 that is named 802.11i. The Wi-Fi Alliance has released a subset of the 802.11i standard that the Alliance has developed called "Wi-Fi Protected Access."
- Products that successfully complete the Wi-Fi Alliance testing required for meeting its version of the 802.11i standard will be called "Wi-Fi Protected Access" certified.
- Wi-Fi Protected Access provides a stronger level of encryption and authentication. This means that Wi-Fi networks will be better protected from unauthorized access and other security problems. Wi-Fi Protected Access is intended to replace WEP encryption built into Wi-Fi.

WEP=Wired Equivalent Privacy is a security algorithm for IEEE 802.11 wireless networks. Introduced as part of the original 802.11 standard ratified in 1997, its intention was to provide data confidentiality comparable to that of a traditional wired network.

Figure 2.2 shows some comparative throughput speeds for most of the wireless standards I've discussed in this chapter.



- In order to keep the comparison real-world, I've included estimated actual throughput for 802.11b as well as its theoretical maximum.
- For purposes of reference, and to help you see that Wi-Fi is unlikely to slow you down much, I've included the throughput you can expect from a 10BASE-T Ethernet network in the figure (this is the kind of wired network you are most likely to find in your home or office, although many wired networks are based on the faster 100BASE-T standard).
- You should take away these points from Figure 2.2:
- 802.11b Wi-Fi is a little slower in the real world than a wired network, but more than adequate for small office and home networks.
- Wi-Fi is getting faster and better all the time.

There are 2 more: Home work

- 802.11ac (Wi-Fi 5)
- 802.11ax (Wi-Fi 6)

The Future of Wi-Fi

- Wi-Fi is a disruptive technology that came unexpectedly and has been growing by leaps and bounds, mainly because it is inexpensive and fills a need.
- Originally, Wi-Fi was just a hack so that people could connect a notebook to a network via wireless using a spectrum that didn't have to be paid for.
- No one expected it to grow so fast, and to become used so widely. The fact that it has spread like wildfire has caused many kinds of technology companies, from wireless cell phone providers to network hardware manufacturers, to rethink their businesses.

5GHz vs 2.4GHz – How to choose the right WiFi frequency for your business?

Coverage area vs. data rate

- The 2.4GHz frequency band covers a larger area and provides a more extended range than the 5GHz band, but with lower data rates. Instead, the 5GHz band provides a smaller coverage area than the 2.4 GHz band but with a higher data rate.

Speed

- The GHz range that a wireless device uses does not necessarily determine the maximum speed of the WiFi. The environment in which the network will be set up is what really should be considered.
- For instance, the 2.4GHz band usually supports up to 450 Mbps or 600 Mbps, depending on the device type, however as so many devices use the 2.4GHz band, the resulting congestion can cause discontinued connections and slower speeds.

- Instead, the 5GHz band can bear up to 1300 Mbps. It tends to be less overcrowded than the 2.4GHz band because fewer devices use it and because it has more channels for devices to use than the 2.4GHz. The maximum speed would depend on the wireless standard the access point supports, i.e., 802.11b, 802.11g, 802.11n, or 802.11ac.
- When comparing the 2.4GHz band with the 5GHz, the latter provides a lower coverage. Thus, when the frequency increases, its ability to penetrate solid objects (like walls) decreases, *reason why the 5GHz band was used mostly in outdoor deployments at the beginning*.
- But at the same time, the higher the frequency, the faster the data is transmitted. Therefore, the 5GHz band carries more data and sends it faster. Then, if your priority is to provide an excellent WiFi speed performance, your choice should lean to the 5GHz band, instead.

- **Interference**
- The other thing to check for is potential interference with the WiFi network's frequency range. Interference can slow down a network significantly and reduce its scope as well. For instance, for the 2.4GHz band, the two most obvious sources of wireless network interference are wireless telephones and microwave ovens. Instead, for the 5GHz band, cordless phones, radars, digital satellite and perimeter sensors are the most common sources of interference.

Some cordless phones formerly advertised as 5.8 GHz actually transmit from base to phone on 5.8 GHz and transmit from phone to base on 2.4 GHz or 900 MHz, to conserve battery life.

- **Congestion**
- When multiple devices attempt to use the same radio space, overcrowding happens. A negative connotation of the 2.4GHz band is its significant congestion driven by the high use of this band not only for WiFi but also for other devices, like garage door openers, microwave ovens, cordless phones, and Bluetooth devices.
- On the other hand, the 5GHz band is not so overcrowded, and it has more free radio air and channels, i.e., 23 working channels vs. 11 in the 2.4GHz band. Consider that channel availability depends on the country in which the deployment is located, which results in higher stability and connection speed.
- **Cost**
- Finally, you should be aware that the cost of access points supporting 5GHz is higher than supporting 2.4GHz. This is because 5GHz is newer in the market. Furthermore, many 5GHz devices also support 2.4GHz radios.

Related Wireless Standards

- You might also hear about some other wireless standards, and wonder how they are related to Wi-Fi. The two other wireless standards you are most likely to hear about are *Bluetooth* and *NFC*.
- Bluetooth is a short-range connectivity solution designed for data exchange between devices such as printers, cell phones etc.
- Like 802.11b, it uses the 2.4GHz spectrum. Although Bluetooth is built into a great many devices, it is a standard with some severe disadvantages, mainly that it is far slower than 802.11b (with nominal throughput of up to 721 Kilobytes per second) and with a maximum range of about 30 feet (compared to Wi-Fi's unamplified range of several hundred feet).
- Bluetooth's main claim to fame is that it is inexpensive, which is why it has been added to so many devices.

BLUETOOTH

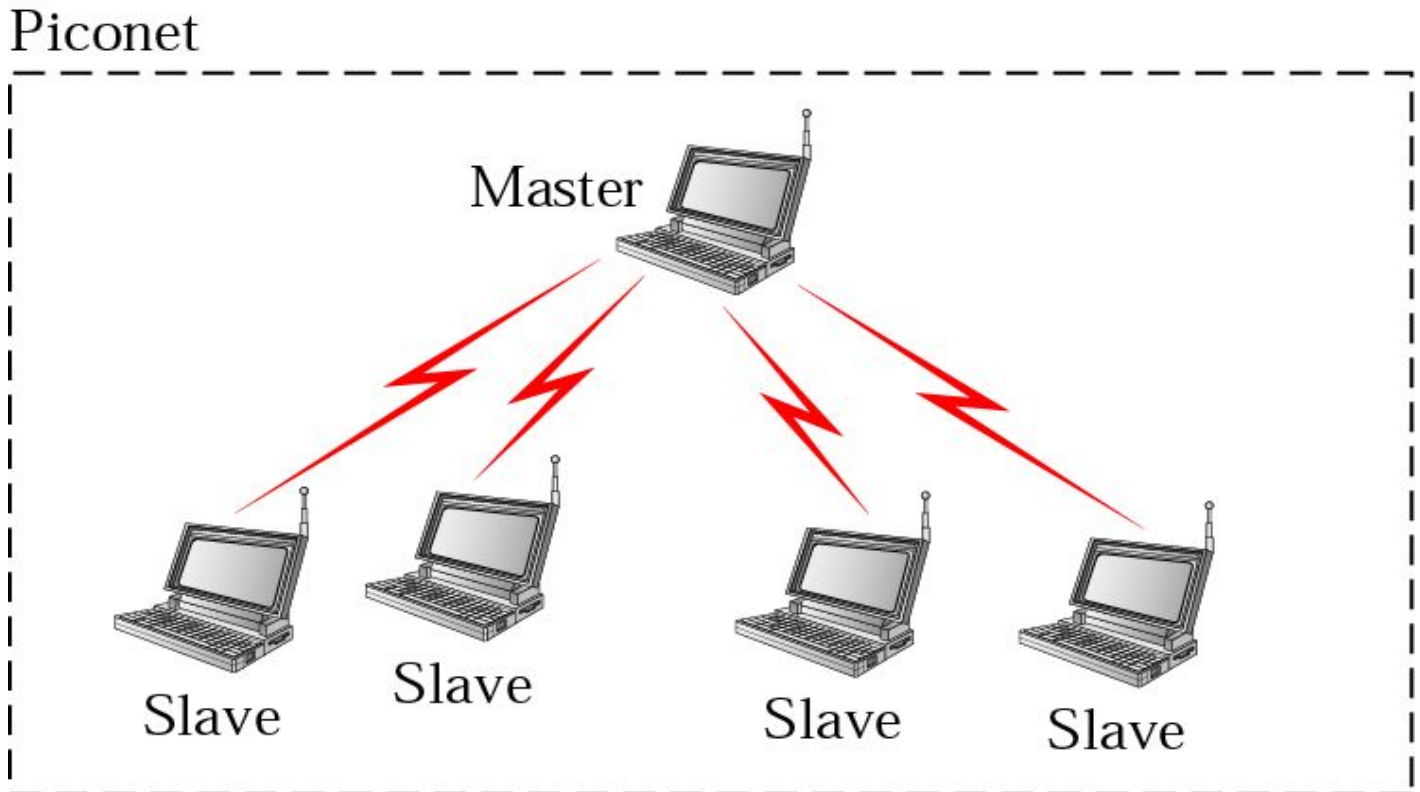
- A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously; the devices, sometimes called gadgets, find each other and make a network called a piconet.
- A Bluetooth LAN can even be connected to the Internet if one of the gadgets has this capability.
- A Bluetooth LAN, by nature, cannot be large. If there are many gadgets that try to connect, there is chaos.
- Bluetooth technology has several applications. Peripheral devices such as a wireless mouse or keyboard can communicate with the computer through this technology.

- Bluetooth was originally started as a project by the Ericsson Company.
- It is named for Harald Blaatand, the king of Denmark (940-981) who united Denmark and Norway.
- *Blaatand translates to Bluetooth in English.*
- Today, Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard.
- The standard defines a wireless personal-area network (PAN) operable in an area the size of a room or a hall.

Architecture

Bluetooth defines two types of networks: piconet and scatternet.

- ***Piconets:***
- A Bluetooth network is called a piconet, or a small net.
- A piconet can have up to eight stations, one of which is called the primary; the rest are called secondaries.
- All the secondary stations synchronize their clocks and hopping sequence with the primary.
- Note that a piconet can have only one primary station.
- The communication between the primary and the secondary can be one-to-one or one-to-many.

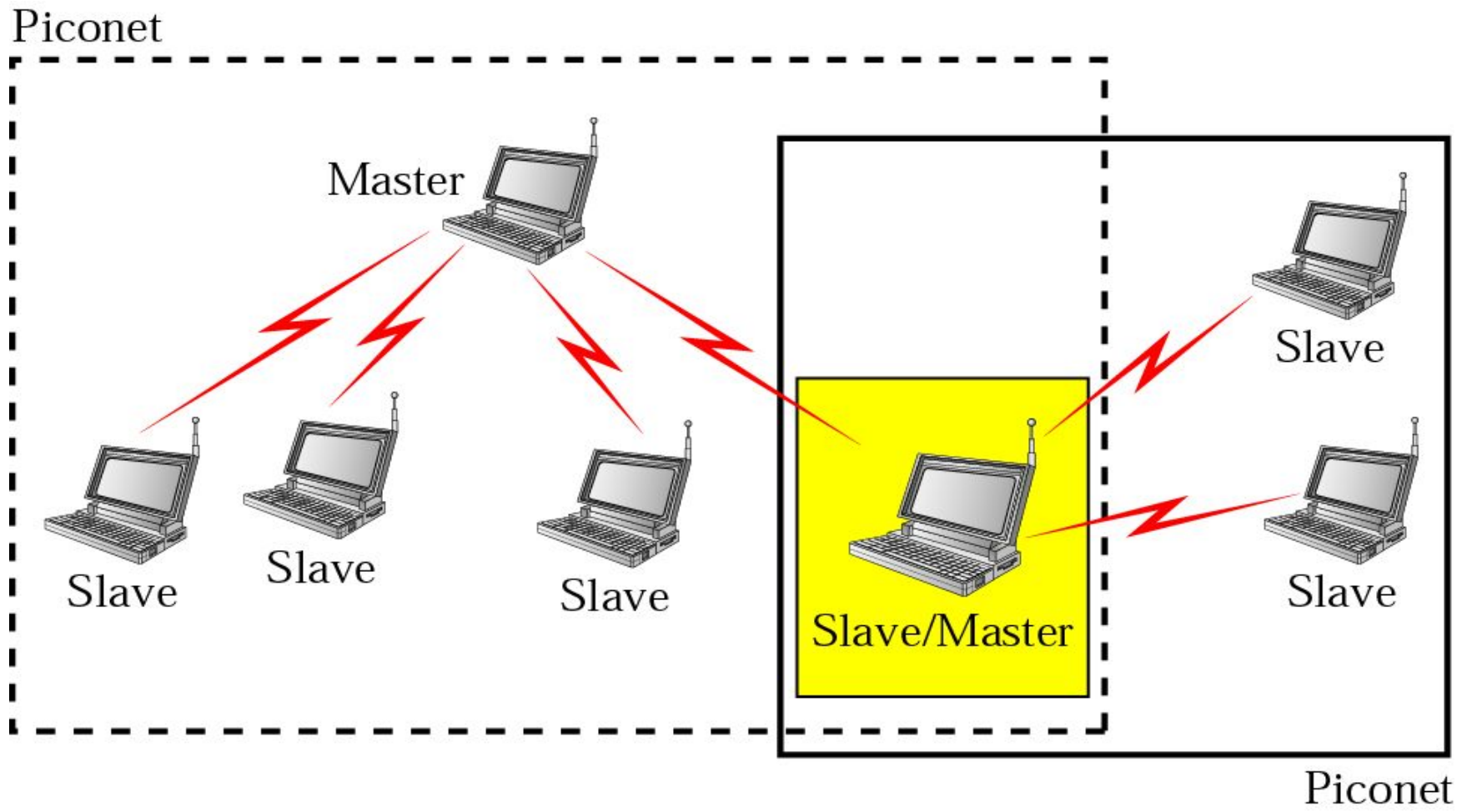

Piconet
Master
Slave
Slave
Slave
Slave

- Although a piconet can have a maximum of seven secondaries, an additional eight secondaries can be in the *parked state*.
- *A secondary in a parked state is synchronized* with the primary, but cannot take part in communication until it is moved from the parked state.
- Because only eight stations can be active in a piconet, activating a station from the parked state means that an active station must go to the parked state.

Scatternet

- Piconets can be combined to form what is called a scatternet.
- A secondary station in one piconet can be the primary in another piconet. This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet.
- A station can be a member of two piconets.

Scatternet


Piconet
Master
Slave
Slave
Slave
Slave/Master
Slave
Slave
Piconet

NFC

- **Near field communication** (**NFC**) is a set of standards for smart phones and similar devices to establish radio communication with each other by touching them together or bringing them into proximity, usually no more than a few inches.
- Present and anticipated applications include contactless transactions, data exchange, and simplified setup of more complex communications such as Wi-Fi. Communication is also possible between a NFC device and an unpowered NFC chip, called a "tag".

- NFC builds upon RFID systems by allowing two-way communication between endpoints, where earlier systems such as contactless smart cards were one-way only.
- It has been used in devices such as Google Nexus, running Android 4.0 Ice Cream Sandwich, named with a feature called "Android Beam" which was first introduced in Google Nexus.
- Android Beam uses NFC to enable Bluetooth on both devices, instantly pair them, and disable Bluetooth automatically on both devices once the desired task has completed. This only works between Android devices version Jelly Bean and above.

- It has also been used in Samsung Galaxy devices. with the feature named as S-Beam.
- It is an extension of Android Beam, it uses the power of NFC (to share MAC Address and IP addresses) and then uses Wi-Fi Direct to share files and documents.
- The advantage of using WiFi Direct over Bluetooth is that it is much faster than Bluetooth, having a speed of **300Mbit/s** for sharing large files.

- NFC devices can be used in contactless payment systems, similar to those currently used in credit cards and electronic ticket smartcards, and allow mobile payment to replace or supplement these systems.
- For example, Google Wallet allows consumers to store credit card and store loyalty card information in a virtual wallet and then use an NFC-enabled device at terminals that also accept MasterCard PayPass transactions.[
- Germany, Austria, Finland, New Zealand, Italy, Iran,and Turkey have trialled NFC ticketing systems for public transport. Vilnius fully replaced paper tickets for public transportation with ISO/IEC 14443 Type A cards on July 1, 2013.

- NFC stickers based payments in Australia’s Bankmecu and card issuer Cuscal have completed an NFC payment sticker trial, enabling consumers to make contactless payments at Visa payWave terminals using a smart sticker stuck to their phone.
- India is implementing NFC based transactions in box offices for ticketing purposes.

- NFC and Bluetooth are both short-range communication technologies that are integrated into mobile phones.
- NFC operates at slower speeds than Bluetooth, but consumes far less power and doesn't require pairing.
- NFC sets up more quickly than standard Bluetooth, but has a lower transfer rate than Bluetooth.
- With NFC, instead of performing manual configurations to identify devices, the connection between two NFC devices is automatically established quickly: in less than a tenth of a second.
- The maximum data transfer rate of NFC (424 kbit/s) is slower than that of Bluetooth V2.1 (2.1 Mbit/s).

NFC VS BLUETOOTH

Aspect	NFC	Bluetooth	Bluetooth Low Energy
Network Standard	ISO 13157 etc.	IEEE 802.15.1	IEEE 802.15.1
Network Type	Point-to-point	WPAN	WPAN
Cryptography	not with RFID	available	available
Range	< 0.2 m	~100 m (class 1)	~50 m
Frequency	13.56 MHz	2.4–2.5 GHz	2.4–2.5 GHz
Bit rate	424 kbit/s	2.1 Mbit/s	1 Mbit/s
Set-up time	< 0.1 s	< 6 s	< 0.006 s
Power consumption	< 15mA (read)	varies with class	< 15 mA (read and transmit)

Thank you