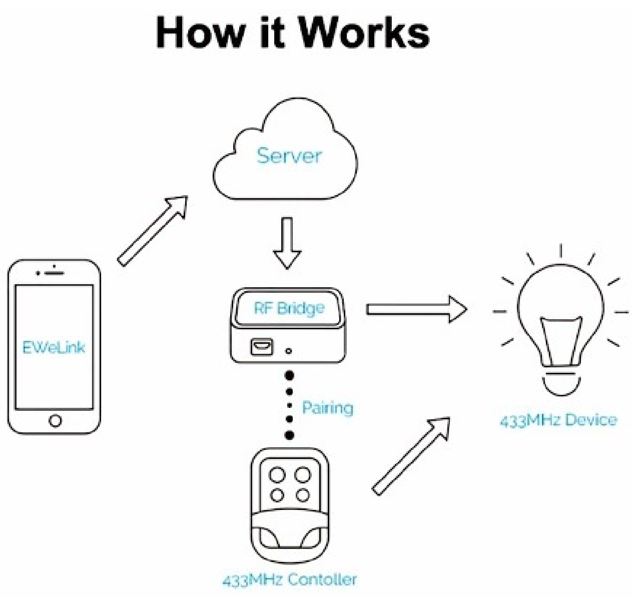
Z-Wave versus *ZigBee* versus *Wi-Fi*
Smart home basics: how to pick the right protocol [1]

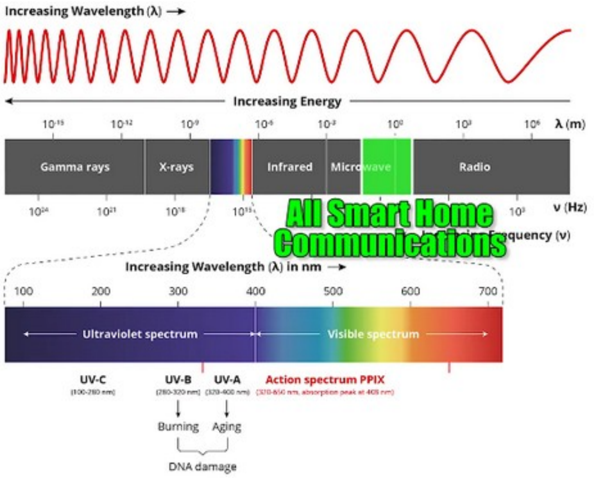
1. Today on *The Hook Up*, I'm going to tell you more than you ever wanted to know about the three most common ***home automation communication protocols***: *ZigBee*, *Z-Wave*, and *Wi-Fi*.

Here's a short list of the most popular communication protocols in the smart home industry. As a new buyer, picking which technology to use can be daunting, and it may affect your perception of smart home products forever. This video is going to focus primarily on the three main consumer smart home technologies: that's *ZigBee*, *Z-Wave*, and *Wi-Fi*. And to truly understand these technologies and their individual advantages, I'm gonna divide up this video and look at these protocols through ***three different lenses***: science, technology, and business.

2. Let's start by learning a little bit about the ***science***. Even though there's a protocol that we specifically call *Radio Frequency*, or *RF433*, all smart-home communication protocols actually use radio frequencies. Radio frequencies are a type of electromagnetic radiation that sets the lowest energy side of the electromagnetic spectrum. Everything on this spectrum has two important attributes: ***wavelength*** and ***frequency***. And multiplying the wavelength times the frequency gives you the speed at which the waves travel, which is constant at the speed of light for everything on the electromagnetic spectrum. Since the speed is constant, that means that if the wavelength is short, the frequency then needs to be high; and conversely, if the wavelength is long, it means that the frequency is low.

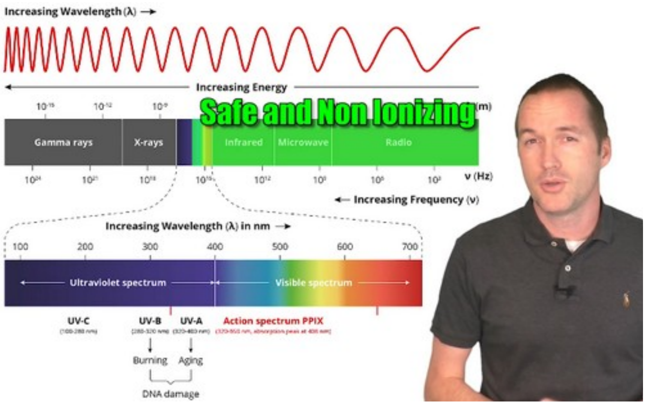


3. Knowing the frequency of a wave matters for two reasons. First, frequency is directly related to the ***energy*** of the wave: higher frequencies are higher energy. Frequency is measured in something that's called *Hertz*, or cycles per second, and in order to be able to more effectively compare the differences in frequency in this video, I'm gonna express all of them in *Gigahertz.*

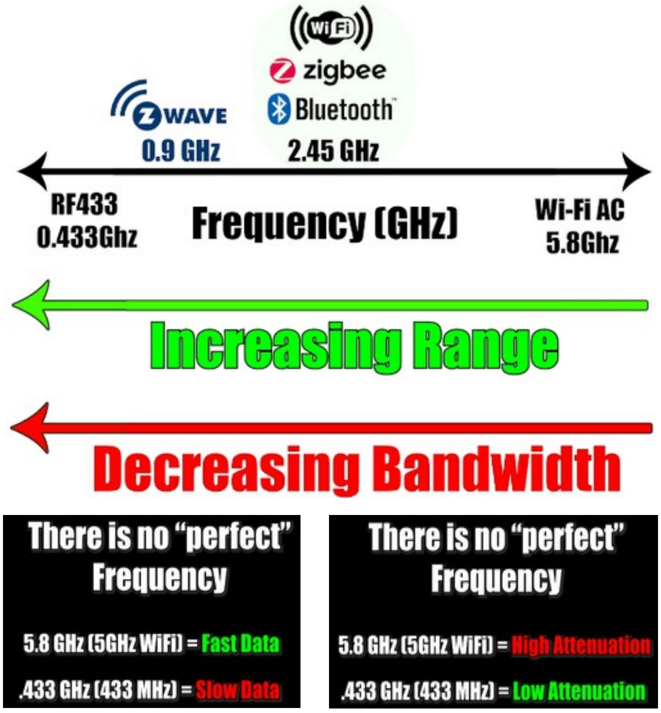


The term "electromagnetic radiation" may sound scary and it might cause some people to worry, but most of the ***radiation*** that we're exposed to on a daily basis is completely harmless.

[1] https://www.youtube.com/watch?v=v8-VNIQQiQE

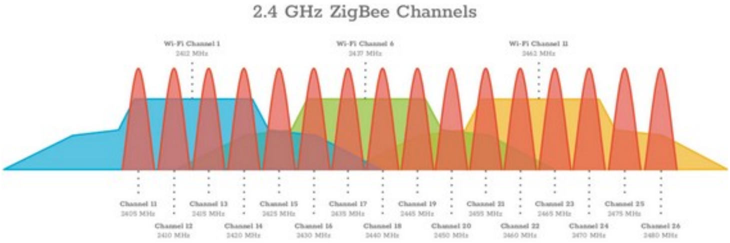


4. Radiation that we do need to be concerned about are the waves that are high enough energy to displace electrons in chemical bonds, because this can cause both cell damage and mutations in DNA. This dangerous radiation is called *ionizing radiation*, and it starts in a part of the spectrum above visible light called *ultraviolet*. The technologies we're going to talk about today are relatively ***low energy*** and have frequencies that range from about 0.433 GHz to 2.4 GHz. And, for reference, ionizing radiation – specifically far ultraviolet – begins at around 2.4 million GHz. So arguments that these radio frequencies are gonna scramble our brains or give us cancer are unfounded and not backed by scientific research.


Wi Fi
zigbee
Bluetooth
Z WAVE
0.9 GHz
2.45 GHz
RF433
0.433Ghz
Frequency (GHz)
Wi-Fi AC
5.8Ghz
Increasing Range
Decreasing Bandwidth
There is no "perfect" Frequency
5.8 GHz (5GHz WiFi) = Fast Data
.433 GHz (433 MHz) = Slow Data
There is no "perfect" Frequency
5.8 GHz (5GHz WiFi) = High Attenuation
.433 GHz (433 MHz) = Low Attenuation

5. The second reason frequency is important is that it affects the ***ability to transmit data***. Higher frequency means higher bandwidth, or the ability to transfer more data in a shorter period of time. But lower frequencies have lower attenuation when traveling through solids, meaning they can pass through obstacles like walls without being blocked or losing their energy. *ZigBee*, *Wi-Fi* and *Bluetooth* all used the 2.45 GHz band, where a *Z-Wave* uses the 0.9 GHz band. This means that, all things considered, *Z-Wave* will have the greatest non-line-of-sight range between devices due to its lower frequency, but it will sacrifice some bandwidth in order to do so. Currently, the slower data transmission isn't that huge of a deal because messages being sent by these devices are relatively small. But as these technologies make it into more high resolution sensors, we may reach the limit of what *Z-Wave* frequency is capable of transmitting.

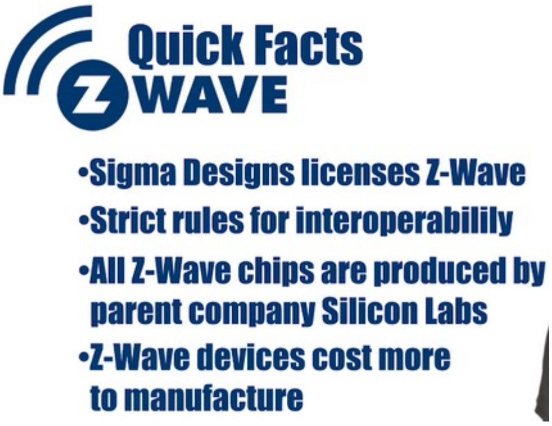
6. The last thing to talk about in this science section is frequency congestion, sometimes referred to as ***interference***. When many devices are trying to communicate on the exact same frequency, the data can get messy and the messages can get lost, similarly to trying to have a conversation with somebody in a crowded restaurant. *ZigBee*, *Wi-Fi* and *Bluetooth* all communicate on the 2.45 GHz band, meaning that the potential for interference is high.



But in actuality, they're able to tune to slightly different frequencies within that band called ***channels*** in order to reduce interference. Still, even with different channels, having too many devices constantly broadcasting on the same channel can lead to faults and drop messages, which leads me into my next section about protocols and the technologies associated with each of these standards.

7. ***Protocols*** are a defined set of rules for how devices communicate. Sometimes we refer to these protocols using terms like “light weight” or error-tolerant”, based on their specific rule set. An example of a human protocol is when you order something at a drive-thru and the cashier repeats your entire order to you at the end. This would be an example of a fault-tolerant protocol, because you confirm that your entire order was received and no parts of the message were lost. But this protocol not only takes more time, but it would also break down if I spoke a different language than the cashier, and we only knew the names of the foods in our own languages. So how does this apply to smart home devices?

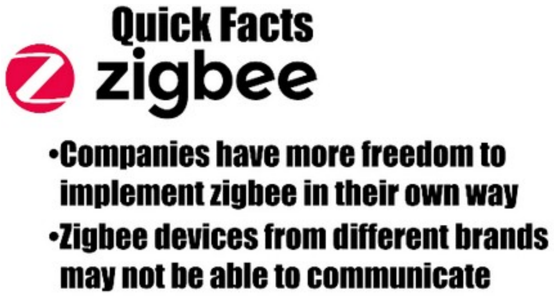
8. ***Z-Wave*** is a proprietary technology run by a company called *Sigma Designs*. If your device says “*Z-Wave*” on it, it means that it's licensed by *Sigma designs*, and the manufacturer had to adhere to strict rules about the protocol and language to ensure maximum compatibility between devices. *Sigma* even exercises control over who can produce *Z-Wave* chips, which are all produced by *Silicon Labs*. The upside to this total control is that the protocol is extremely standardized and you can always be sure that your *Z-Wave* devices will be able to communicate with your *Z-Wave* hub, regardless of the brand. But the downside is that *Sigma Designs* is able to charge more for these chips and for the licensing, which results in a higher cost per device.



Quick Facts Z WAVE

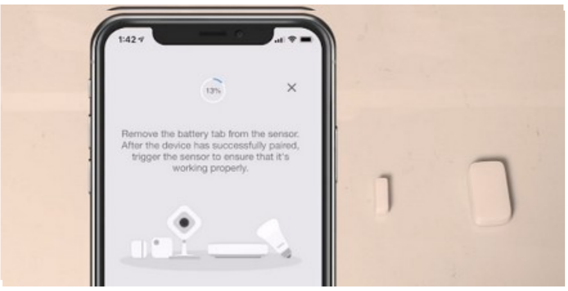
- Sigma Designs licenses Z-Wave
- Strict rules for interoperabilily
- All Z-Wave chips are produced by parent company Silicon Labs
- Z-Wave devices cost more to manufacture

9. ***ZigBee*** on the other hand is an open wireless standard, meaning individual companies can implement their own products without the strict set of rules like those enforced by *Z-Wave*. As a result, just like ordering from a drive-thru in a different language, even though every *ZigBee* hub will be able to hear every *ZigBee* device, it might not be able to understand what that device is saying. For example, I have these *Tuya ZigBee* sensors that are designed to be used with the *Tuya ZigBee* hub. A *Samsung SmartThings* hub can easily discover these *ZigBee* devices, but since the protocol is not standardized, the hub has no idea what type of device they are or what information they're trying to convey. These slight differences in implementation of *ZigBee* devices can cause even larger issues due to the way that they form the communication network.



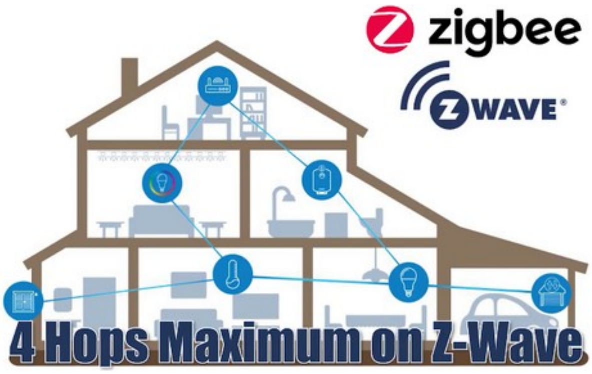
Quick Facts zigbee

- Companies have more freedom to implement zigbee in their own way
- Zigbee devices from different brands may not be able to communicate



Remove the battery tab from the sensor. After the device has successfully paired, trigger the sensor to ensure that it's working properly.

10. Both *ZigBee* and *Z-Wave* forms something that's called a ***mesh network***, where they can extend the range of the signal by relaying information from one device to the next in order to make it back to the hub. Best-case scenario is that this relay process extends the devices range while only introducing a minor delay or latency. But as the number of relays or hops increases, the delay can become very noticeable. In an effort to reduce this latency and increase customer satisfaction, *Z-Wave* limits devices to a maximum of four hops, while *ZigBee* hasn't implemented any limit.



11. Because of the need to relay messages to the hub, you may also need to intentionally place *ZigBee* or *Z-Wave* devices in intermediate locations in order to extend the range of your mesh. And it's also important to understand that these mesh devices must have ***constant power***. So we're talking about things like light bulbs, plugs and switches, that will act as nodes and not battery-powered sensors.

    Further complicating things, if you have *ZigBee* devices from multiple manufacturers in your smart home, they might not be able to communicate with each other, meaning they might need to form separate mesh networks which can actually end up interfering with each other, causing dropped or lost signals.

zigbee
ZWAVE

Mesh nodes must be powered
- Switches/Bulbs
- Plugs/Outlets
- Thermostats

12. ***Reliability*** and ***fault tolerance*** are also worth discussing when considering these different technologies. Like I said before, as radio frequency bands become more congested, the likelihood of data loss increases dramatically. *ZigBee* and *Z-Wave* are relatively lightweight protocols when compared to *Wi-Fi*, meaning there's less handshaking, data redundancy, and confirmation in their communication. Most of the time, this lightweight protocol represents a huge benefit, since battery-powered *ZigBee* or *Z-Wave* devices will transmit significantly less data than a *Wi-Fi* device and will therefore have a much longer battery life. But in terms of fault tolerance, they are unquestionably worse. It's unlikely that a purely *Z-Wave* network would ever have enough traffic to cause issues, but if there were another device communicating or emitting a signal around that 0.9 GHz band, there could theoretically be a whole network breakdown.

Fault Tolerance:
The ability for a device to continue normal operation in the event of a [data] transmission failure.

13. ***Wi-Fi*** is a completely different animal when compared to *ZigBee* and *Z-Wave.* The *Wireless 802.11n* standard that most smart devices use is an open protocol that any device maker can implement, and it's got a strict set of rules for how your device needs to communicate with your network. Unlike the mesh networks of *ZigBee* and *Z-Wave*, *Wi-Fi* devices communicate directly with the closest access point, and will not relay information between devices.

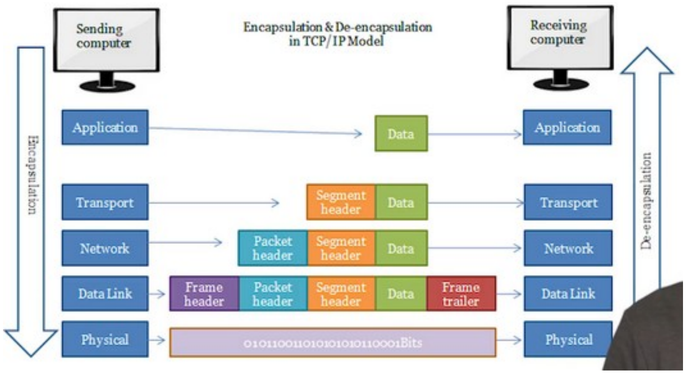
    The reason *Wi-Fi* can get away with this connection method is because you ostensibly already have or at least want to have ***a good Wi-Fi connection*** everywhere in your house. If you're thinking about starting a smart home and you have a spotty *Wi-Fi* coverage in your house, I'd recommend tackling that issue first before jumping into home automation. It's going to save you a lot of headaches later. Even with dozens of devices communicating with a centralized access point, your *Wi-Fi* network is actually extremely orderly, and your access points do an amazing job telling each device to wait their turn in order to reduce signal noise.

Quick Facts

Wi Fi

- Most smart home devices still use 802.11N
- No such thing as incompatible Wi-Fi
- Wi-Fi communicates with an access point
- Add devices to your existing Wi-Fi network
- Wi-Fi is designed with high network capacity in mind.

14. In addition, *Wi-Fi* devices communicate on your network using the TCP/IP protocol which is designed with fault tolerance in mind. Each TCP/IP communication employs a specific handshake and data validation in order to ensure that no parts of the transmission are lost. The downside of fault tolerance is that it requires significantly more data transmission, which requires ***more power***. A battery-powered *Wi-Fi* censor will drain its battery significantly faster than a comparable *ZigBee* or *Z-Wave* sensor.

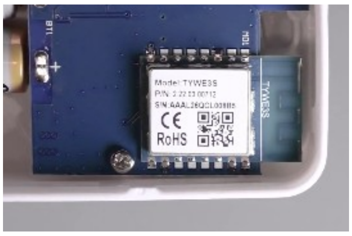


15. And the last difference in technology that I want to talk about is how these devices are ultimately controlled. Let's compare the ***communication methods*** of a *Wi-Fi* door sensor versus a *ZigBee* or *Z-Wave* door sensor. In this example, let's say that I want to be notified on my phone whenever a door opens.

- For a *ZigBee* or a *Z-Wave* system, the contact sensor pulls apart, the device then wakes up and begins its transmission. If the device is too far away from the hub to communicate directly with it, it will contact its closest powered neighbor and send the state of the door. That device will then relay that information through the mesh until it arrives at the hub. Let's say in this case that the hub is a *Samsung SmartThings* hub. That hub will then send the information over the Internet to the *Samsung SmartThings* cloud server and that server – which is connected to the *Samsung* app on my phone – will then send a message to my phone via a push notification.

- In the *Wi-Fi* device like this *Tuya* door sensor, the device will send its message directly to the wireless access point, which will then be routed to the *Tuya* cloud server – which is connected to my *Tuya* app – causing a push notification to be sent to my phone. This *Wi-Fi* communication sounds much more efficient.

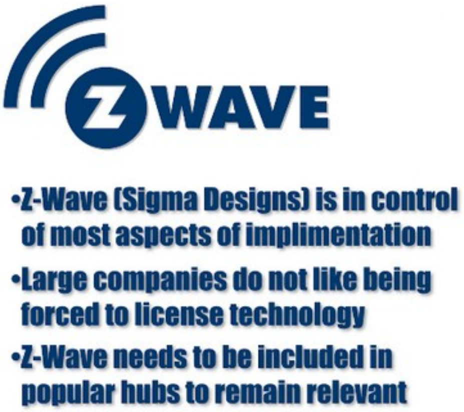
16. But, in my opinion, it's where I think *ZigBee* and *Z-Wave* devices actually have the greatest advantage over *Wi-Fi.* It's true that *Wi-Fi* devices that use the popular *ESP8266* chip are able to be flashed with custom firmware to keep their traffic local. But this method is not something that the typical user is going to be comfortable with, and it's not something that would be applicable to every device type. But, since *ZigBee* and *Z-Wave* sensors communicate directly with a hub, the user can decide which hub they want to utilize in order to control their smart home. In my example, I showed the *SmartThings* hub because it's the most popular entry-level hub on the market, but since it's a cloud-based system, it doesn't represent any increase in reliability or privacy over a *Wi-Fi* sensor.



However, locally controlled in process hubs like the *Hubitat Elevation* are available or, even better, home assistant can add *ZigBee* or *Z-Wave* compatibility with a USB dongle. In these instances, cloud services can be cut completely out of the picture, which will increase reliability and privacy, while decreasing security risks significantly.

17. The last consideration for these standards is a topic that I'm significantly less familiar with, and that's ***business contracts*** and ***economics***.

    Z-Wave is a completely proprietary system, and as I understand it, there's not a whole lot of development being done by other companies. If you're a manufacturer and you want your device to speak *Z-Wave*, you pay them a fee, you get a module and you plug it into your device. The *Z-Wave Alliance* then tests out your device to make sure it adheres to the strict *Z-Wave* standard and allows you to print the *Z-Wave* certified logo on your packaging. As a result, *Z-Wave* devices tend to be more expensive than comparable *ZigBee* or *Wi-Fi* devices, and even though their compatibility with the *Z-Wave* hub is guaranteed, I'm not sure what business decisions are being made to ensure that *Z-Wave* radios will be included in the next generation of hubs, as new technologies emerge.



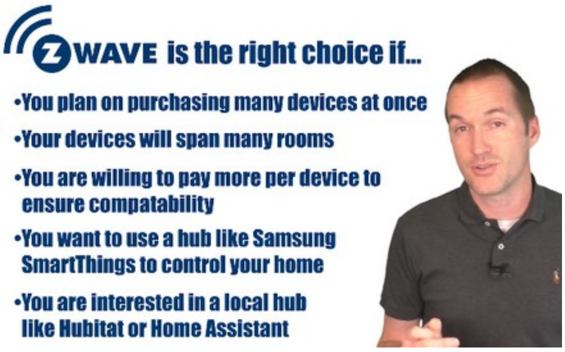
WAVE

- Z-Wave (Sigma Designs) is in control of most aspects of implimentation
- Large companies do not like being forced to license technology
- Z-Wave needs to be included in popular hubs to remain relevant

    For instance, in 2019, *Apple*, *Google*, *Amazon*, and the *ZigBee Alliance* among others, joined forces on a project that they're calling "***connected home over*** IP", which will undoubtedly shape the future of smart home devices. *Z-Wave* was notably not listed in this huge collaboration of companies, which could possibly be disastrous for them in the future. The good news is that your *Z-Wave* devices aren't likely to just stop working all the sudden. But there could come a time in the not-too-distant future when companies move away from the *Z-Wave* standard, which could in turn affect the range and reliability of your existing *Z-Wave* mesh network as you upgrade your new devices to this chip standard.

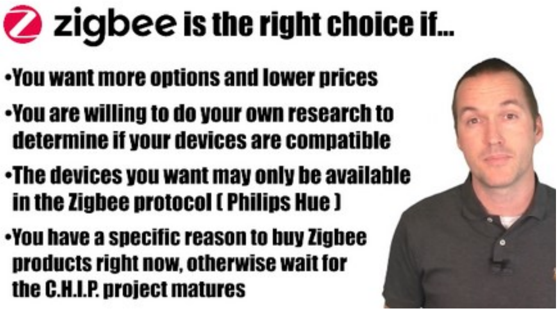
18. If you watch this video thinking it would help you decide on a technology and use in your smart home but ended up more indecisive than ever, here's the most ***condensed advice*** that I can offer:

    - Choose ***Z-Wave*** if you're going to buy a lot of products at once, put them all over your house, and you don't mind spending a little bit more on each device. The more *Z-Wave* products you have, the better your mesh will be, and the more reliable your network becomes. If you're just getting started, the *Samsung SmartThings* hub is easy to use and has a lot of information about how to get set up. But if you value your privacy, it is absolutely worth looking into a local solution like *Hubitat* or *Home assistant* to act as your *Z- Wave* hub.
    - ***ZigBee*** does sound good in theory, because the products are cheap and diverse, but you should be aware that not all *ZigBee* devices can communicate with each other, and some proprietary *ZigBee* networks like *Philips Hue* for example will form separate meshes that could end up interfering with your main *ZigBee* mesh. In my personal opinion, unless you have a specific reason to buy *ZigBee* right now, it's probably best to go a different way until the connected over IP product reaches maturity.



WAVE is the right choice if...

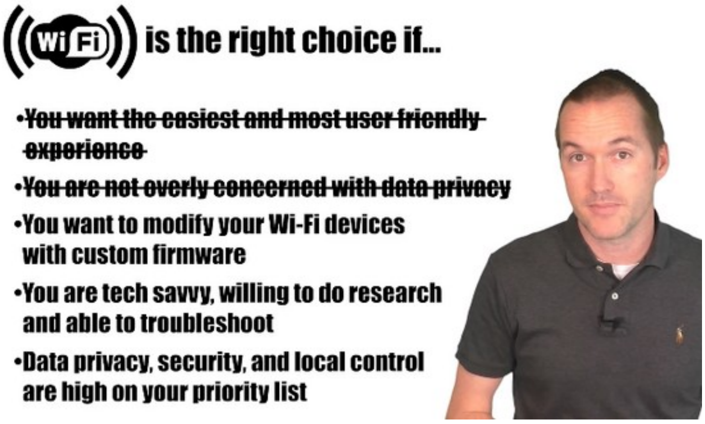
- You plan on purchasing many devices at once
- Your devices will span many rooms
- You are willing to pay more per device to ensure compatability
- You want to use a hub like Samsung SmartThings to control your home
- You are interested in a local hub like Hubitat or Home Assistant



zigbee is the right choice if...

- You want more options and lower prices
- You are willing to do your own research to determine if your devices are compatible
- The devices you want may only be available in the Zigbee protocol (Philips Hue)
- You have a specific reason to buy Zigbee products right now, otherwise wait for the C.H.I.P. project matures

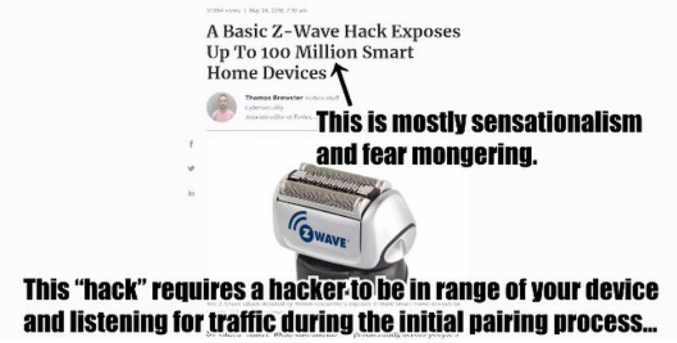
19. • ***Wi-Fi*** devices can be utilized in two very different ways:
    - You can buy *Wi-Fi* products and use them right out of the box with no hub to connect to your *Google Home* or *Amazon Echo*. This is by far the easiest and most user-friendly implementation of smart home products, but it's also the least secure. And that's not to say that there is an eminent risk, just that it's the most exposed way of adding a smart device to your home network, since each device is going to be communicating directly with the cloud service.
    - The second and best way to use *Wi-Fi* devices is in a local communication only setup. As I mentioned earlier, many of the *Wi-Fi* devices on the market today utilize the *ESP8266* chip, which allows more advanced users to replace the factory cloud firmware with custom firmware that uses local communication in processing like MQTT and *Home Assistant*. For devices where custom firmware is possible, local *Wi-Fi* setups are the most fault tolerant, reliable and responsive solution – given the right networking equipment.



Wi Fi is the right choice if...

- ~~You want the easiest and most user friendly experience~~
- ~~You are not overly concerned with data privacy~~
- You want to modify your Wi-Fi devices with custom firmware
- You are tech savvy, willing to do research and able to troubleshoot
- Data privacy, security, and local control are high on your priority list

20. I purposely didn't address some of the ***possible hacks*** on *ZigBee* and *Z-Wave* systems because I think the likelihood of them occurring would be similar to you being eaten by a circus lion. But I am going to talk about them in an upcoming video about smart door locks anyway.



A Basic Z-Wave Hack Exposes Up To 100 Million Smart Home Devices

This is mostly sensationalism and fear mongering.

This "hack" requires a hacker to be in range of your device and listening for traffic during the initial pairing process...

Thank you so much to my awesome patrons over *Patreon* for continuing to support my channel. If you're interested in supporting my channel, please check out the links down in the description. If you enjoyed this video, please hit that *like* button and consider subscribing.