



SMART HOMES

INSPECTION CERTIFICATION ASSOCIATES

Topics Discussed

- ▶ Why it is important to know about Smart Homes?
- ▶ Definitions of common Smart Home Terminology
- ▶ User Interfaces
- ▶ Digital interfaces
- ▶ Smart Home Automation
- ▶ Smart Home Hubs
- ▶ Smart Devices
- ▶ Smart Home and Information Protection
- ▶ How to inspect Smart Homes, what to look for, what to include in your report



Module 1

INSPECTION CERTIFICATION ASSOCIATES

What is a smart home?



A smart home is a home with appliances or components installed that are interconnected. They can be controlled either by a device, voice, or other communication means.

Smart Devices

A smart device is an electronic device generally connected to other devices or networks via different wireless and wired protocols.





Wi-Fi Necessity

Why make a home into a smart home?



Convenience



Flexibility



Security



Remote Control



Increased Energy Efficiency



Improved Appliance Functionality



Home Management Insights

Why is knowing about Smart Homes important?

- ▶ Older home integration
- ▶ Built into new home construction
- ▶ Becoming apart of the essential function of the home

Home Inspector Testing

Testing standards such as the NHIE are now including questions about Smart Homes in their test question bank. Again, this is because Smart Homes are becoming a real thing in residential setting and apart of their over function.



National
Home Inspector
Examination[®]

Standards of Practice

Although not many if not all parts of Smart Homes are excluded from all Standards of Practices such as ASHI's and InterNACHI's, it is prudent to have at least a basic knowledge of these devices and systems. As Home Inspectors, we are essentially consultants to provide information to your client.



Common Real Estate Law

Fixture Definition:

A “fixture” is personal property that, by means of permanent physical attachment to the land or structure, such as with bolts, nails, screws, cement, glue or other attachment method, is converted to real property.

If the “fixture” is not included on the sale of the home, it should be specified in the initial offer contract.



Consistency

You should treat every home the same and if it is there, it should be inspected or documented if:

- ▶ Directly attached to the home
- ▶ If it is essential for the function of the home



CONSIST
ENCY

Providing Added Information

Ultimately, the information you provide, whether it falls under your Standards of Practice or not, should meet following:

- ▶ Not increase liability
- ▶ Decrease liability
- ▶ Provide more information = better customer service
- ▶ Limit potential question = providing more answers than questions

Reported Information

Your report and the information provided is used by your client to make very real and important decisions. Your report gives your client the information to way out assets vs liabilities to make a truly informed decision.



Reduction in Liability

The first step in reducing liability is knowing and understanding the information you are providing.



What is
needed for a
Smart Home?

USER



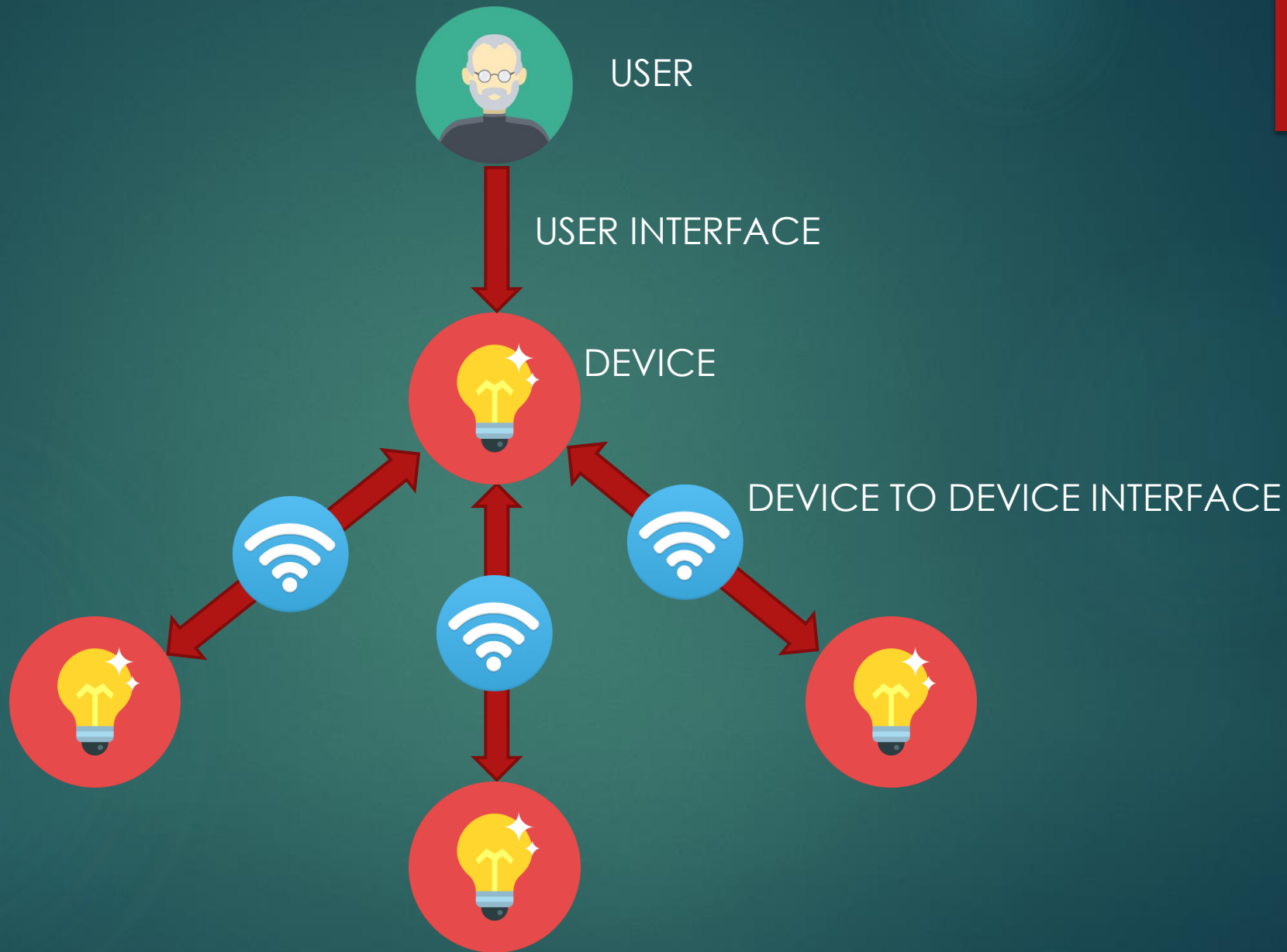
SMART
DEVICE



Two Types of Interfacing

- ▶ Between a person and a device
- ▶ Between a device and other devices





Device to Device Interface

Device to device interfaces are a protocol systems that enable the communication and transportation of data over a network.



Internet

Although not necessary, internet allows Smart Devices to:

- ▶ Allow the user to control them remotely
- ▶ Create a mesh network which allows for better coverage in a home
- ▶ Allows for firmware updates that improves to function of the devices



Types of Interface

- ▶ Smart Phone
- ▶ Tablet
- ▶ Computer
- ▶ Location Based
- ▶ Biometric
- ▶ Voice
- ▶ Gesture
- ▶ Biomechanical

Smart Phone, Tablet and Computer

These are device-based interfaces and depending on the device, and whether it is connected to a hub, will depend on the application used for this interface.



Location Based

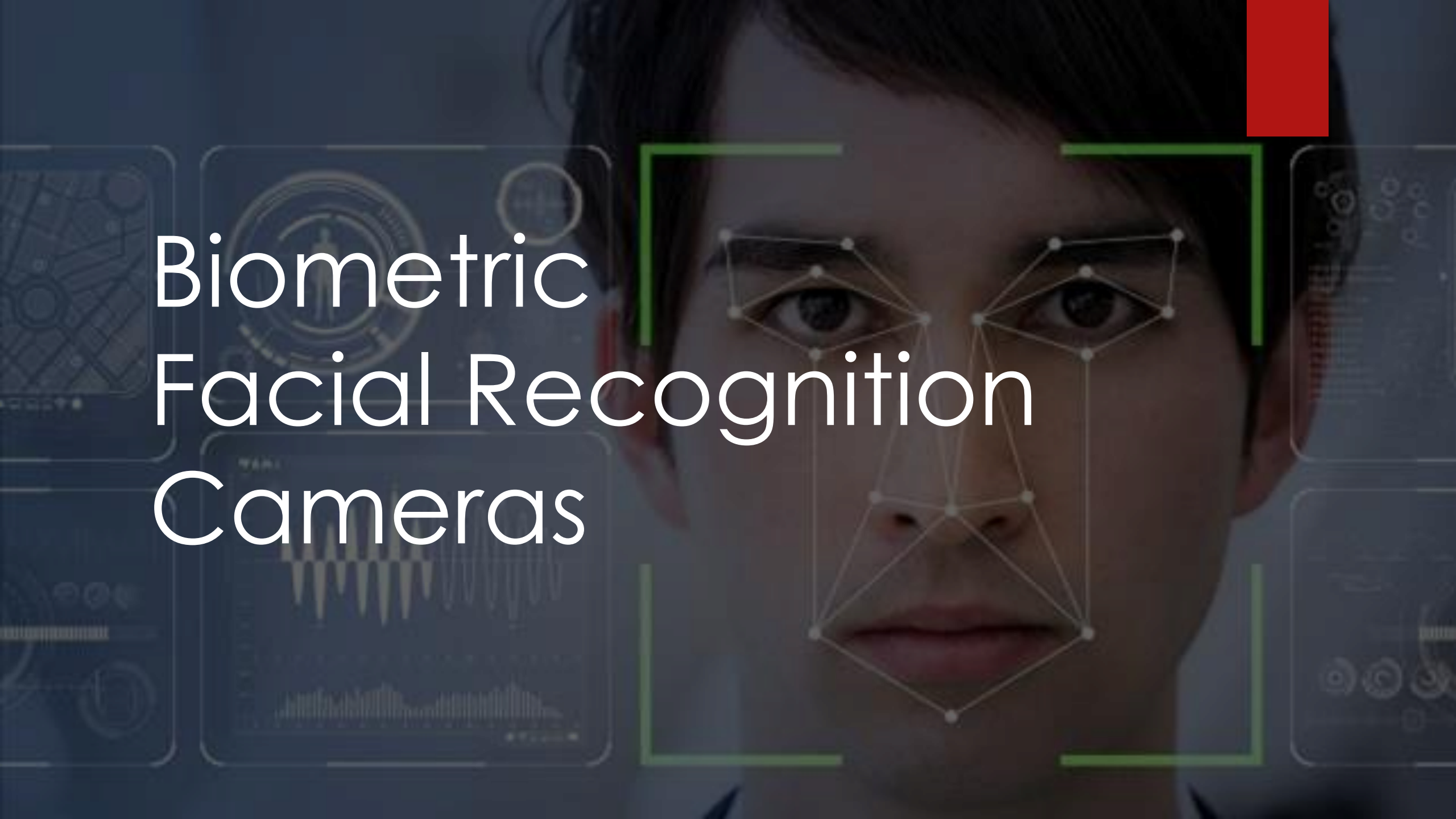
Typically called Geofencing, Geofencing is the practice of using global positioning (GPS) or radio frequency identification (RFID) to define a geographic boundary. Then, once this “virtual barrier” is established, the administrator can set up triggers that send a text message, email alert, or app notification when a mobile device enters (or exits) the specified area.





Biometric Fingerprint Door Locks

Biometric Facial Recognition Cameras





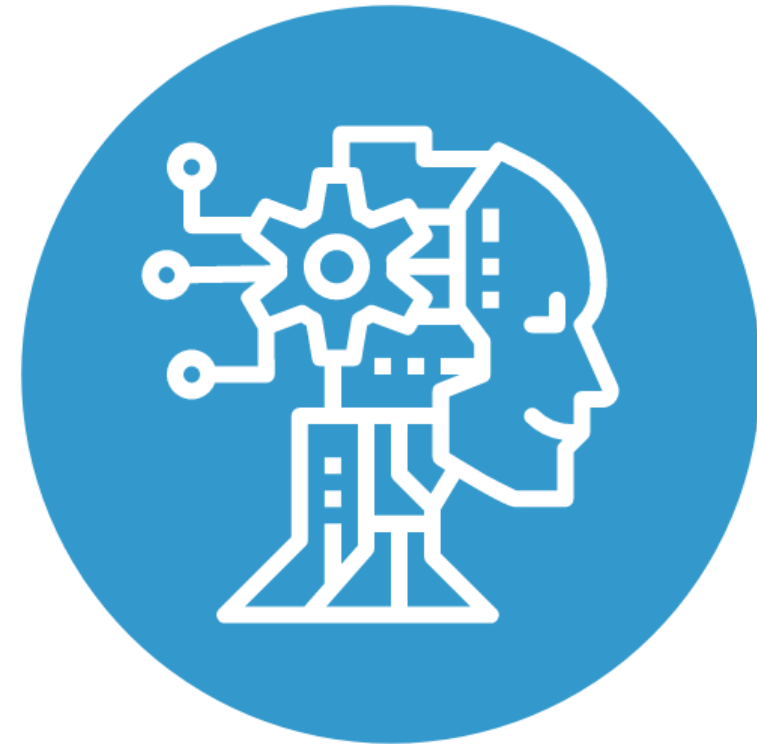
Voice Recognition

AI Based Interfaces

Artificial intelligence (AI), also becoming a powerful presence in technology, has been swiftly dominating the home automation market. AI allows us to integrate smart solutions into our everyday tasks. Not only is AI creating solutions to common everyday problems, but it also making life simpler for everyone. Its presence in home automation allows us to control our appliances, secure our homes, and even limit our expenses. The ultimate goal of home automation is to limit the need for human involvement.

Type of AI in Smart Homes

Smart Home artificial intelligence is a very basic form of AI and is more machine learning. Its programmed goal is to learn from consistent behavior and events to increase efficiency and reduce total work in a home.



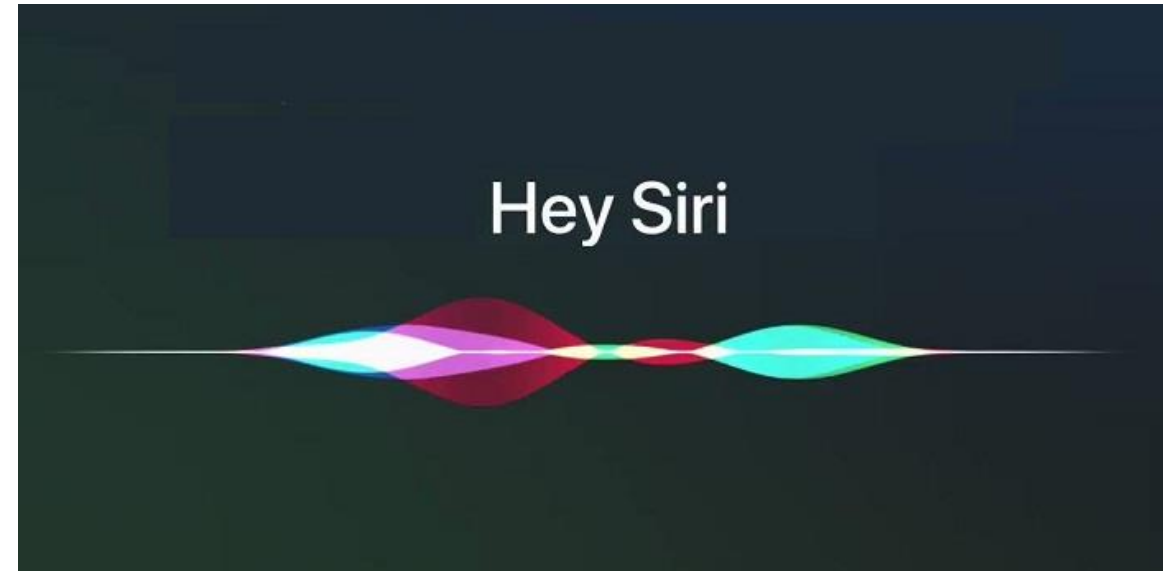
Big 3 Smart Home AI

- ▶ Apples Siri
- ▶ Google Assistant
- ▶ Amazon Alexa



Apple Siri

- ▶ User interface is limited to Apple products
- ▶ It does have a multitude of language settings
- ▶ Internet connection is necessary



Google Assistant

- ▶ Can handle up to 3 tasks at once
- ▶ Can translate in real-time
- ▶ It does not require internet as long as the tasks are local
- ▶ Integrates with more devices



Amazon Alexa

- ▶ Requires internet connection
- ▶ Highest 3rd party skills
- ▶ Access to Amazon Prime



amazon alexa

A hand is shown on the right side of the image, palm facing left, with fingers slightly spread. In the center-left, there is a dark, circular device with a glowing blue and green light inside. From this device, several thin, wavy lines of light extend outwards, creating a sense of motion or interaction. The background is dark and slightly blurred, showing some faint text from a screen. A solid red rectangle is located in the top right corner.

Gesture Control

Spotify Free

Of The Moment!

Qeios • 40 songs, 2 hr 19 min



- Heart rate
- Blood oxygen levels
- Breathing rate
- Muscle electrical activity
- Stress/emotion
- Cognitive function
- Movement patterns
- Sweat analysis
- Sleep

Biomechanical Control

Near Future Interfacing Emotion Based

The next AI-driven UI for the smart home could be emotion analysis, based on facial recognition, speech, voice tone, and biometrics. Innovators such as Beyond Verbal, which envisions a VDA who listens to your conversations and, based on tone and content, interprets your emotional state and acts as your health coach, or the Massachusetts Institute of Technology's (MIT) EQ-Radio, which "can infer a person's emotions using wireless signals. It transmits an RF signal and analyzes its reflections off a person's body to recognize his emotional state (happy, sad, etc.).

IOT

- ▶ The Internet of Things or IOT are all the devices that are connected and can be accessed through the internet.

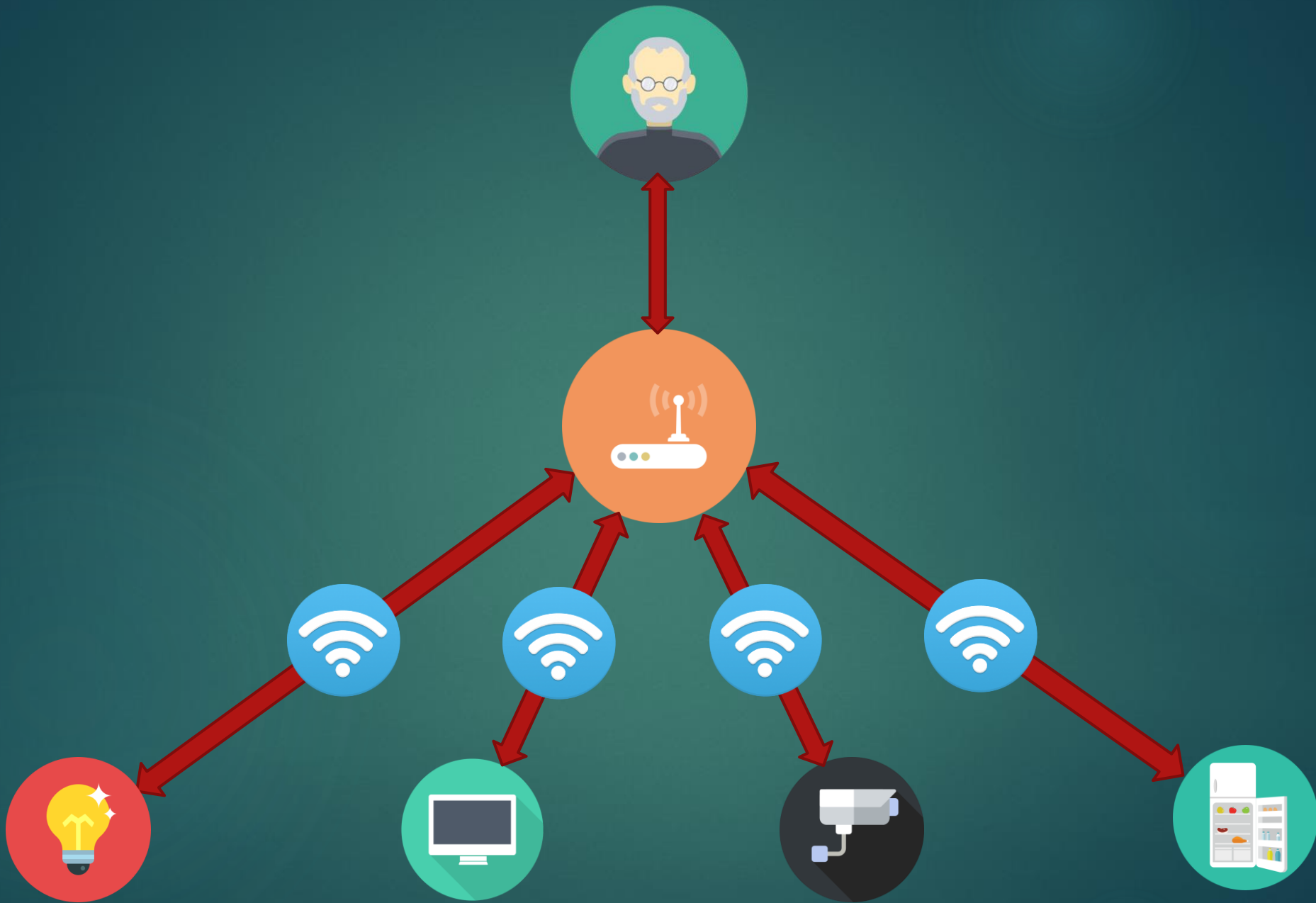


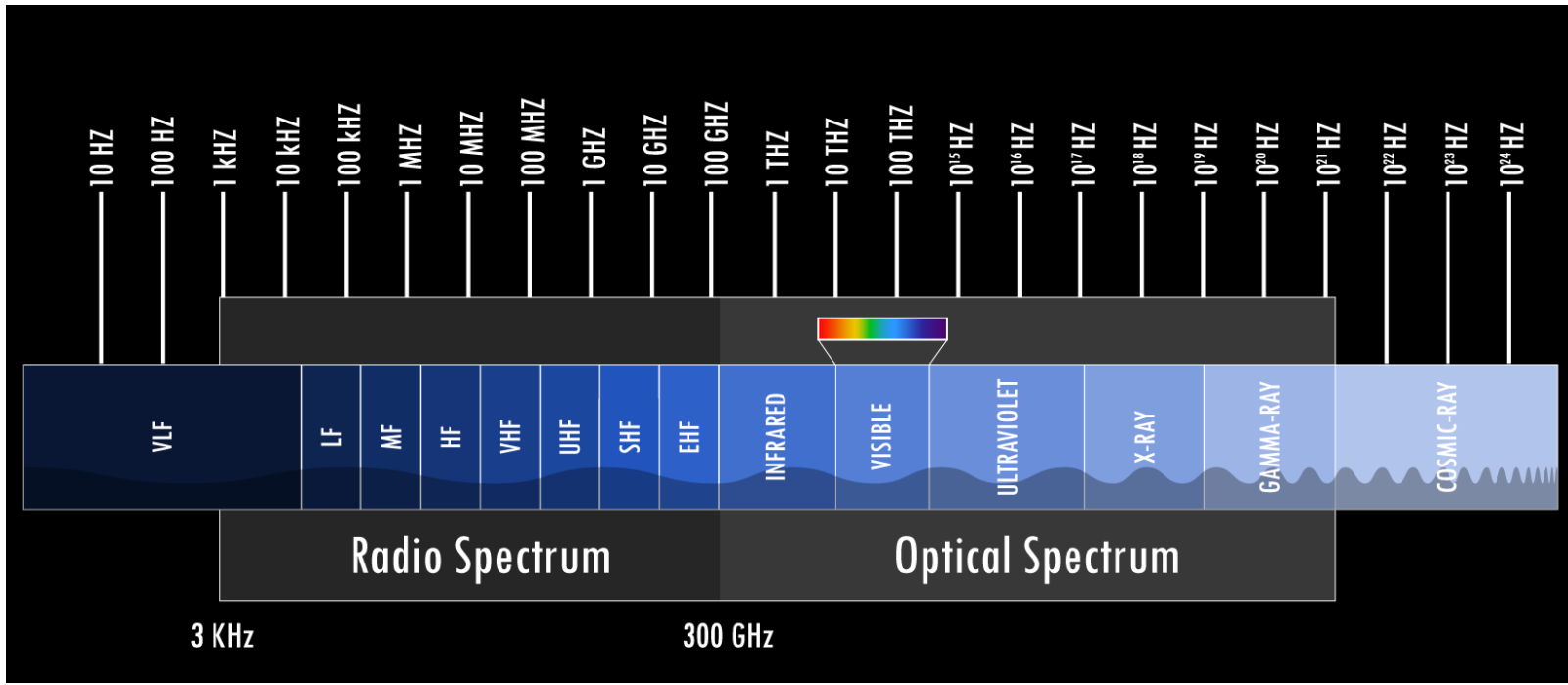


Module 2

Digital Interfacing

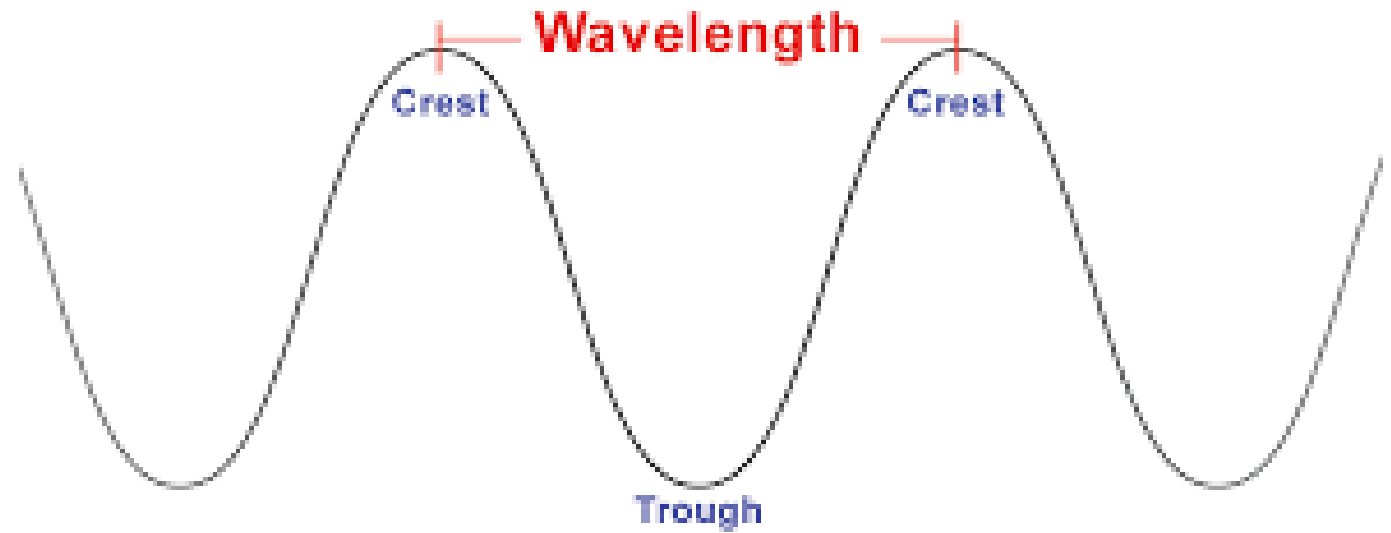
INSPECTION CERTIFICATION ASSOCIATES





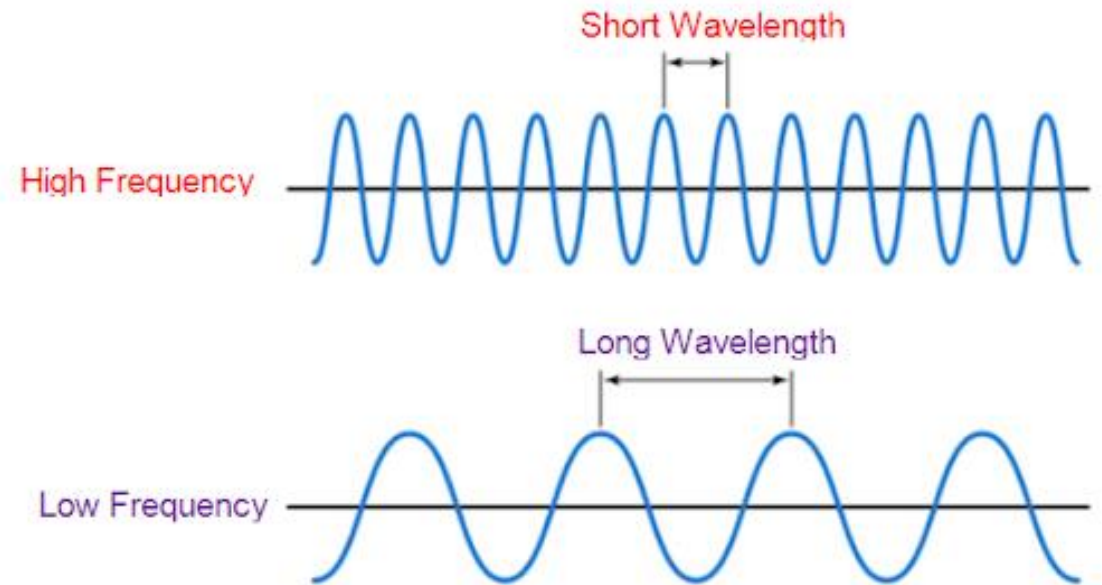
Radio Frequencies

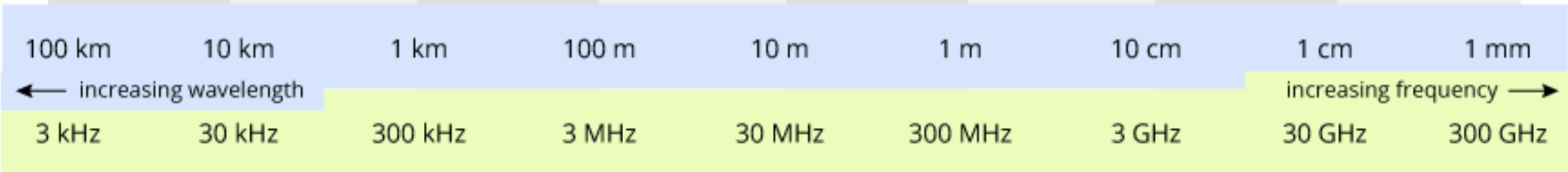
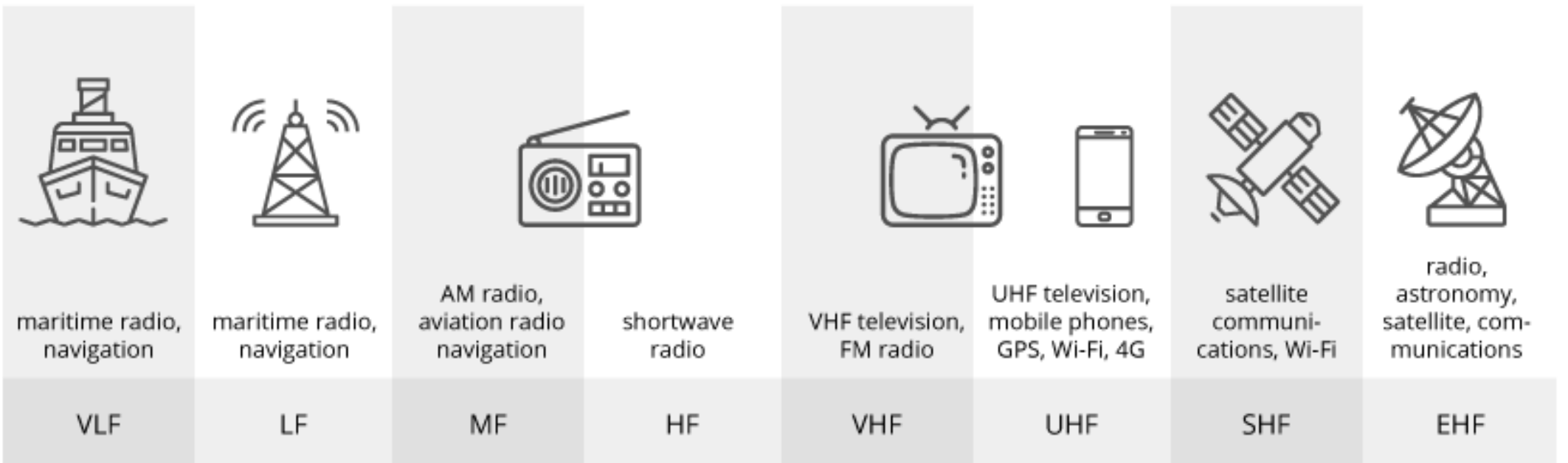
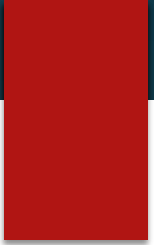
What is a wavelength?



What is a Hz?

- ▶ A Hertz is the amount of each full wavelength in a second. So 20 KHz is 20,000 wavelengths in a second and 300 GHz is 300,000,000,000 wavelengths in a second.





What is Wi-Fi?

Wi-Fi is a wireless networking protocol that allows devices to communicate without direct cable connections. It's technically an industrial term that represents a type of wireless local area network protocol based on the 802.11 IEEE network standard.



What is 802.11 IEEE network standard?

The 802 series is a list of protocols put for by the IEEE (Institute for Electrical and Electronic Engineers) that for the implementation of WLAN (Wireless Local Area Networks) for various frequencies, including but not limited to 2.4 GHz, 5 GHz, and 60 GHz frequency bands



IEEE

Wi-Fi Alliance

Wi-Fi is the most popular means of communicating data wirelessly, within a fixed location. It's a trademark of the Wi-Fi Alliance, an international association of companies involved with WLAN and products.



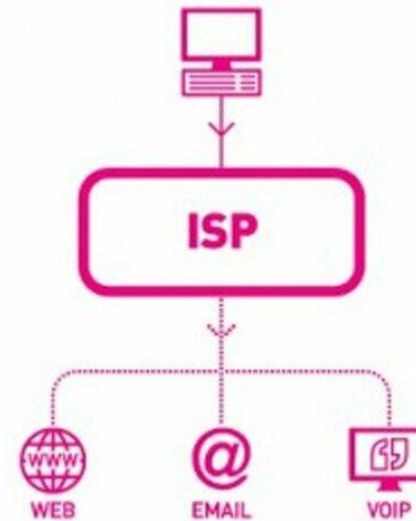
Understanding Wi-Fi

The easiest way to understand Wi-Fi is to consider an average home or business. The main requirement for Wi-Fi is that there's a device that can transmit and receive the wireless signal such as a wireless router.



Internet Service Provider

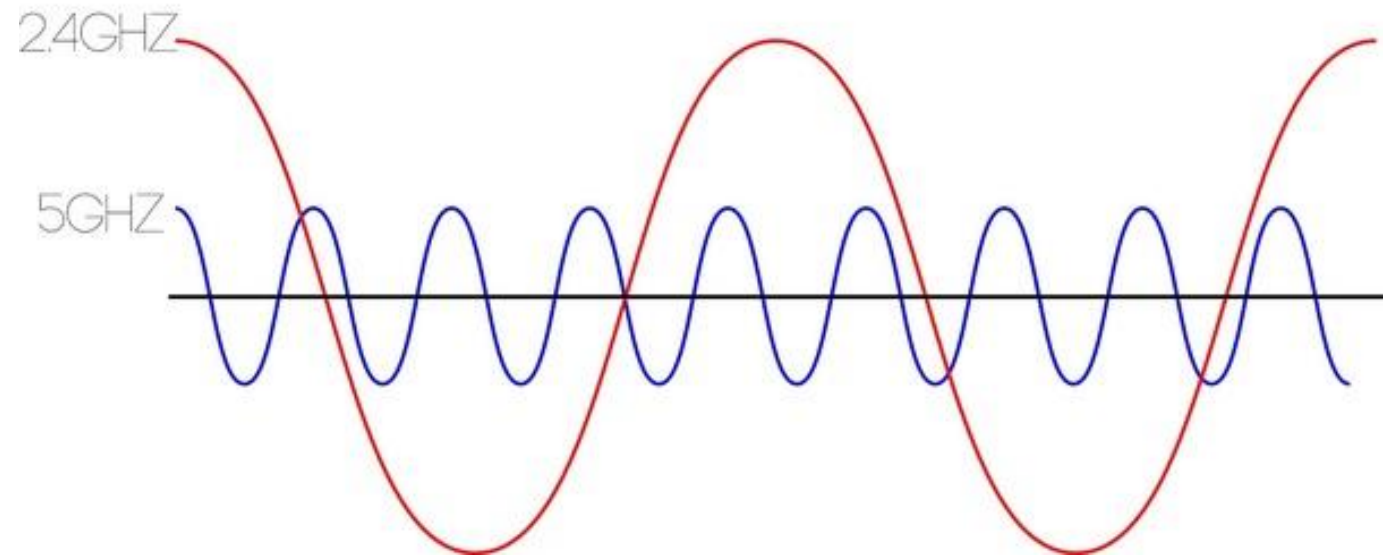
In a typical home, a router transmits an internet connection coming from outside the network, like an ISP (Internet Service Provider), and delivers that service to nearby devices that can reach the wireless signal.



What are the two main frequency bands?

- ▶ 2.4 GHz
- ▶ 5 GHz

2.4GHZ AND 5GHZ WAVELENGTHS



There are four main differences between the 2.4 GHz Wi-Fi band and the 5 GHz Wi-Fi band:



Coverage



Speed



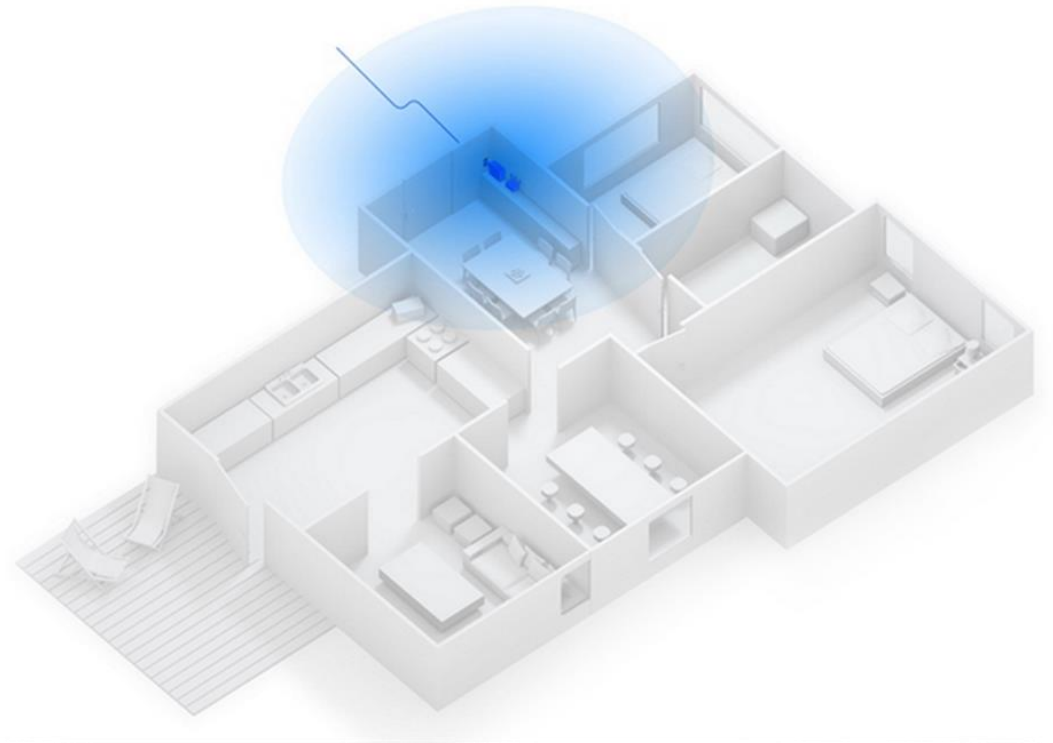
Interference



Compatibility

Coverage

- ▶ When it comes to Wi-Fi coverage, 2.4 GHz outshines 5 GHz. In the 2.4 GHz band, the lower frequencies that are transmitted here can more easily penetrate solid objects, meaning the signal can be better carried out throughout your home.



Speed

- ▶ The higher frequency 5 GHz band makes up for its shorter range with much faster Wi-Fi speeds than the 2.4 GHz band. To compare, the 2.4 GHz band will support speeds between 450 Mbps and 600 Mbps, while 5 GHz will support speeds of up to 1300 Mbps. (Of course, the kind of router you have will better dictate the Wi-Fi speed you can achieve.)



Interference

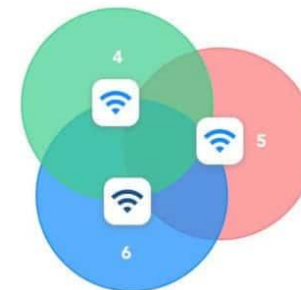
In the 2.4 GHz band, you have the option to choose from 11 Wi-Fi channels, where 3 of which are non-overlapping. In the 5 GHz band, you have the option to choose from 45 Wi-Fi channels, where 24 of which are non-overlapping. Overlapping channels are what lead to network interference, so comparing the two Wi-Fi frequency bands, we can easily see that 5 GHz provides less room for co-channel interference. It's also important to note that in the 2.4 GHz band, you aren't just receiving interference from other Wi-Fi networks.

Co-Channel



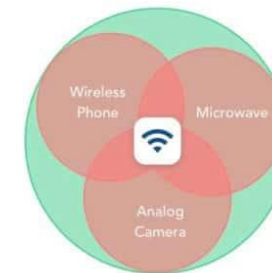
Every client and access point on the same channel competes for time to talk.

Adjacent-Channel



Every client and access point on overlapping channels talk over each other

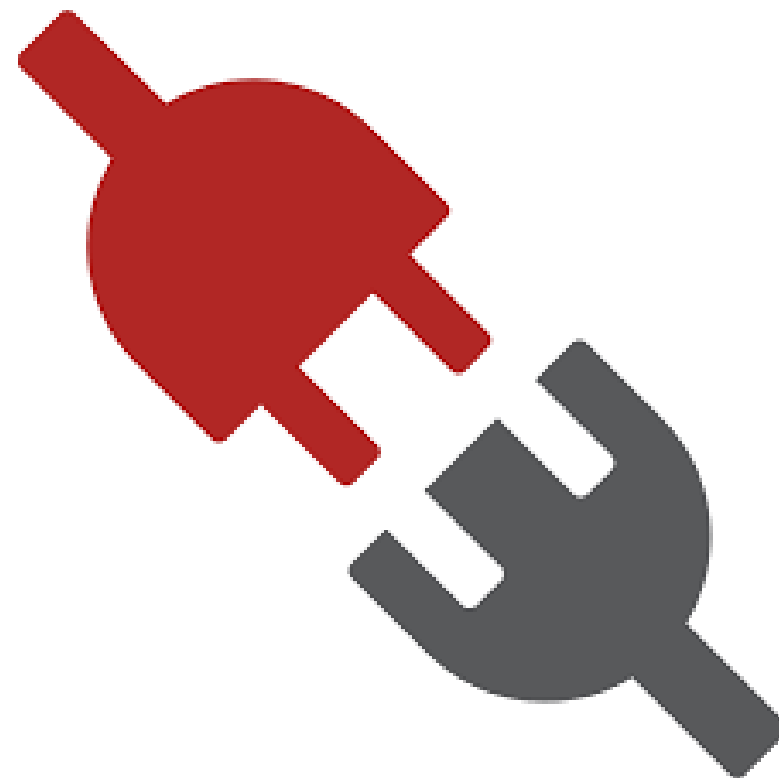
Non-Wi-Fi



Non-802.11 devices compete for medium access

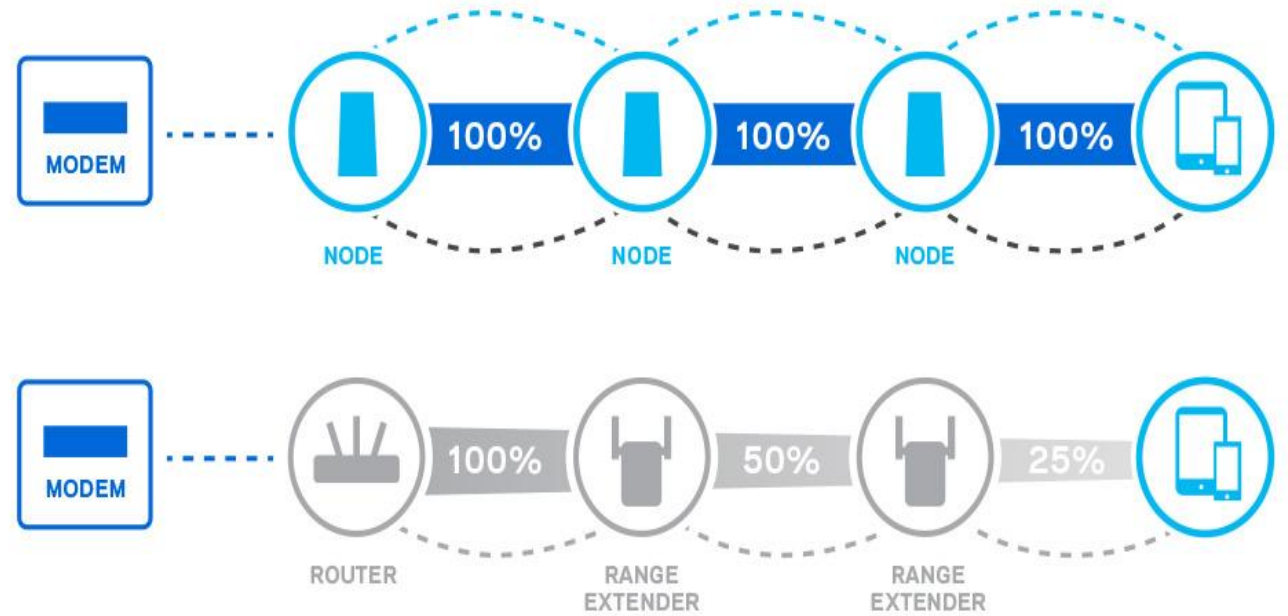
Compatibility

Considering the fact that Wi-Fi standard 802.11n (Wi-Fi 4) has been around for nearly a decade now, the majority of our wireless technologies have been built to support both the 2.4 GHz and 5 GHz bands. But, if you have any old networking equipment or devices from pre-2009, there's a chance they may only be compatible with the 2.4 GHz band.



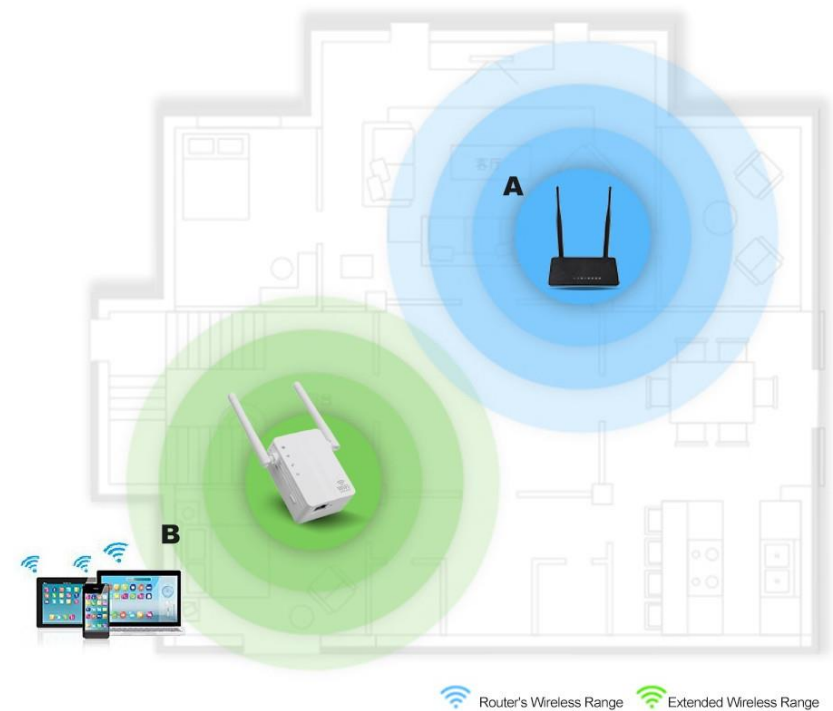
Three ways of extending Wi-Fi:

- ▶ Extender
- ▶ Repeater
- ▶ Mesh Network



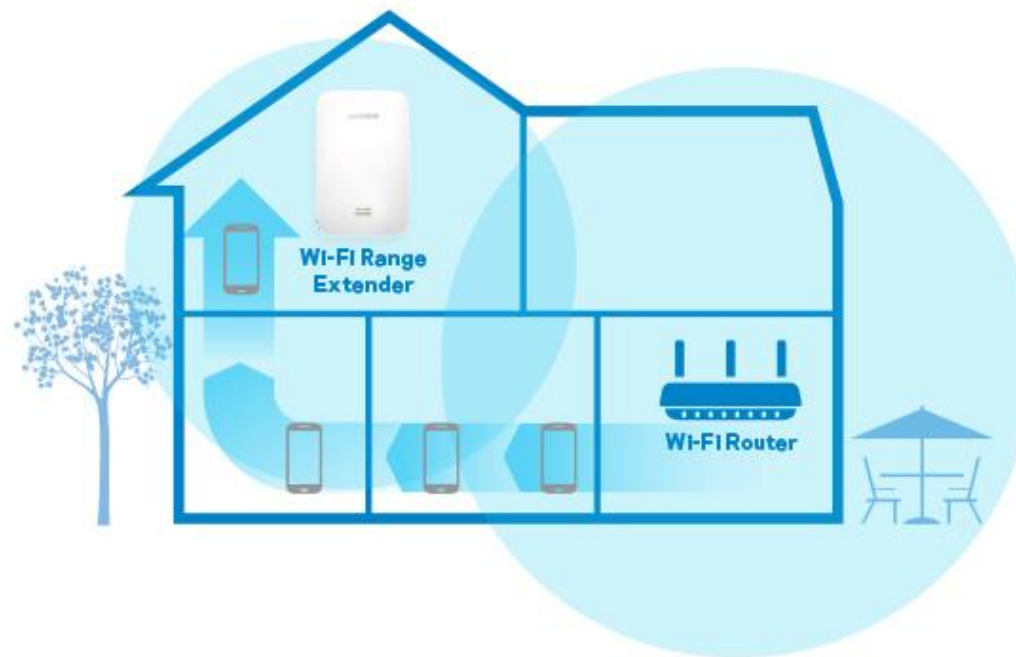
Wi-Fi Repeater

- ▶ A Wi-Fi Repeater is a plug in appliance that extends the range of the network. These devices create an additional network that must be logged into to access. Because of the design, they do have reduced data rates.



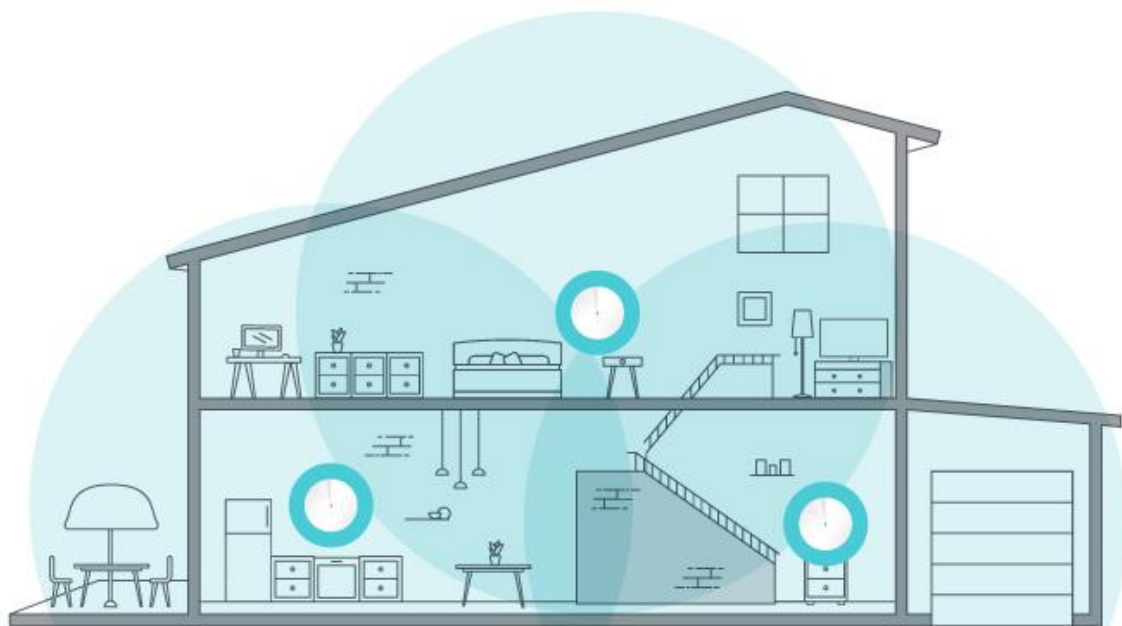
Wi-Fi Extender

- ▶ A Wi-Fi Extender aka a signal booster is a hard wired device to extend Wi-Fi throughout the home. An extender does not create another network unlike a Wi-Fi Repeater.



Wi-Fi Mesh Networks

- ▶ Unlike an extender or a repeater, which you can add to an existing Wi-Fi network, mesh systems are typically complete replacements for your home Wi-Fi.



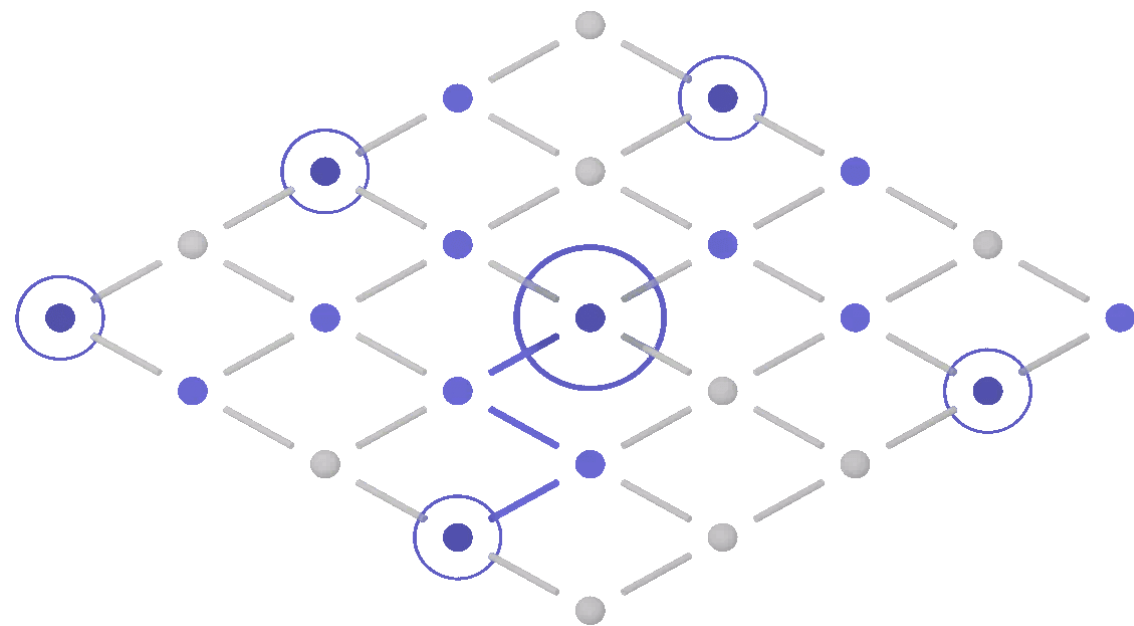
How do Mesh Networks Work?

- ▶ Mesh Wi-Fi or Whole Home Wi-Fi systems consists of a main router that connects directly to your modem, and a series of satellite modules, or nodes, placed around your house for full Wi-Fi coverage. They are all part of a single wireless network and share the same SSID and password, unlike traditional Wi-Fi routers.



Wi-Fi Mesh Networks

Because they're designed to be used in tandem, they have some advantages over traditional extenders. They don't create a separate network, so wherever you go in your house, you'll always be connected to the nearest node automatically.



Change the default name of the home Wi-Fi

The first step towards a safer home Wi-Fi is to change the SSID (service set identifier). SSID is the network's name. Many manufacturers give all their wireless routers a default SSID. In most cases it is the company's name. When a computer with a wireless connection searches for and displays the wireless networks nearby, it lists each network that publicly broadcasts its SSID. This gives a hacker a better chance of breaking into your network. It is better to change the network's SSID to something that does not disclose any personal information thereby throwing hackers off their mission.

Make the wireless network password unique and strong

Most wireless routers come pre-set with a default password. This default password is easy to guess by hackers, especially if they know the router manufacturer. When selecting a good password for the wireless network, make sure it is at least 20 characters long and includes numbers, letters, and various symbols. This setting will make it difficult for hackers to access the network.

Enabling network encryption

Almost all wireless routers come with an encryption feature. By default it is turned off. Turning on the wireless router's encryption setting can help secure your network. Make sure you turn it on immediately after your broadband provider installs the router. Of the many types of encryption available, the most recent and effective is "WPA2."

Turn off network name broadcasting

When using a wireless router at home, it is highly recommended that you disable network name broadcasting to the general public. This feature is often useful for businesses, libraries, hotels and restaurants that want to offer wireless Internet access to customers, but it is usually unnecessary for a private wireless network.

Keep the router's software up to date

Sometimes router's firmware, like any other software, contains flaws that can become major vulnerabilities unless they are quickly fixed by firmware releases from the manufacturer. Always install the latest software available on the system and download the latest security patches to ensure no security hole or breach is left open to online predators.

Make sure to have a good firewall

- ▶ A “firewall” is designed to protect computers from harmful intrusions. Wireless routers generally contain built-in firewalls but are sometimes shipped with the firewall turned off. Be sure to check that the wireless router’s firewall is turned on. In case the router doesn’t have such a firewall, make sure to install a good firewall solution on the system to watch for malicious access attempts to the wireless network.

Use VPNs to access the network

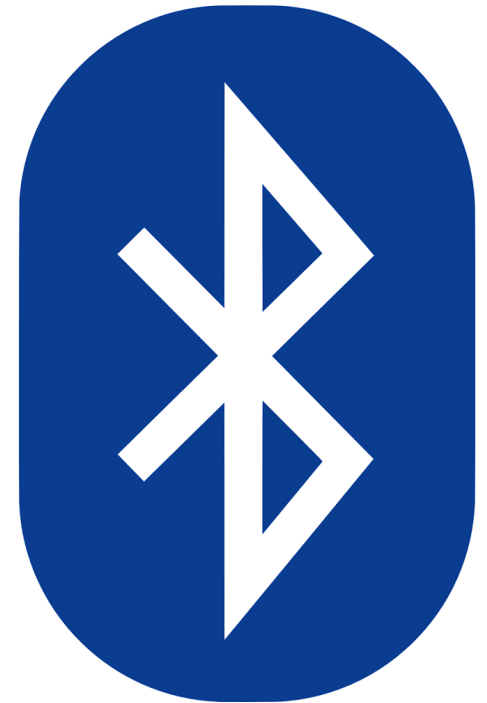
A virtual private network, or VPN, is a group of computers or networks that work together over the Internet. Individuals can use VPNs, like Norton Secure VPN as a method to secure and encrypt their communications. When you connect to a VPN, a VPN client is launched on your computer. When you log in with your credentials your computer exchanges keys with another server. Once both computers have verified each other as authentic, all your Internet communication is encrypted and secured from outside prying.

Types of Device to Device Interfaces

- ▶ X10
- ▶ Bluetooth
- ▶ Zigbee
- ▶ Z-Wave
- ▶ Insteon
- ▶ Lutron's Clear Connect
- ▶ Google's Thread
- ▶ Rubee

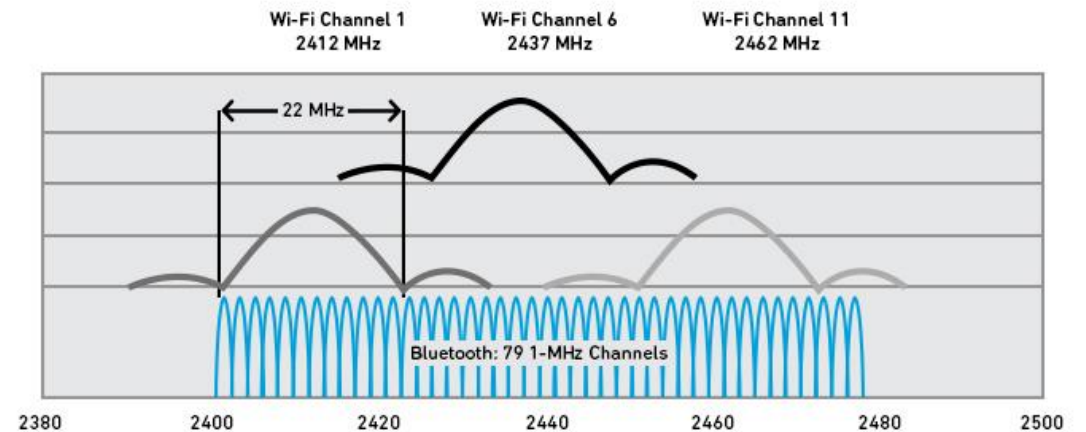
What is Bluetooth?

Bluetooth is a short-range wireless communication technology that uses radio waves to transmit information, much like Wi-Fi. But where that wireless standard operates semi-permanent networks and can do so over a vast distance.



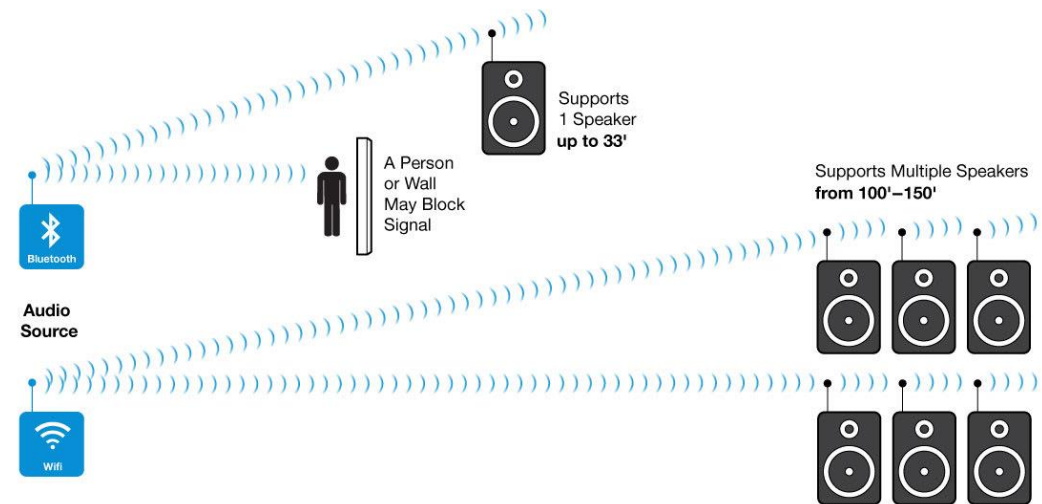
How does Bluetooth work?

Bluetooth works by sending information over ultra-high-frequency radio waves and operates within the industrial, scientific and medical (ISM) radio bands. It works between the 2.4 and 2.485 GHz frequencies, much like many Wi-Fi devices do, which can create problems with interference when both technologies are running simultaneously or if multiple devices are operating within the same area.



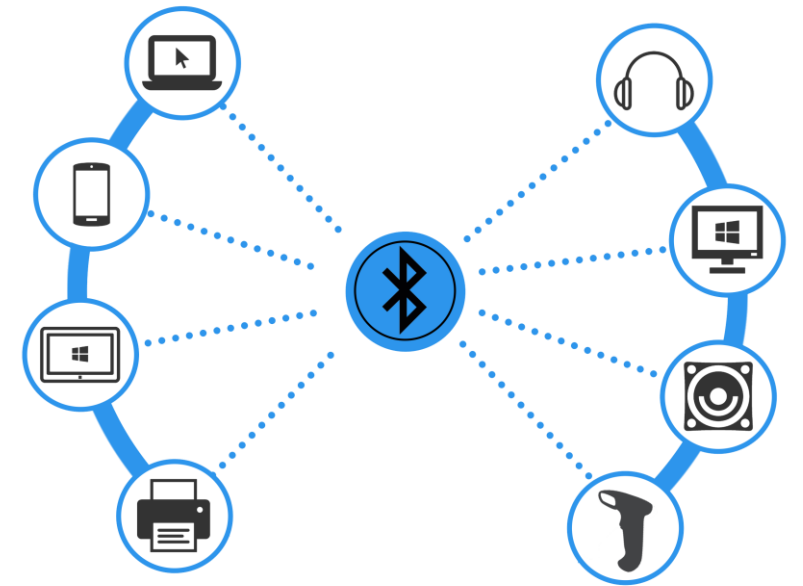
Range of Bluetooth vs Wi-Fi

Ranges are much shorter for Bluetooth at around 33' vs Wi-Fi that can have 100' to 150' ranges.



Differences with Bluetooth

Where Wi-Fi operates asymmetrically (with a singular access point and multiple devices) Bluetooth typically works symmetrically, with one Bluetooth device connecting to another. Although up to eight devices can be connected on a single personal area network (PAN), in the case of smartphones, it typically means connecting two handsets together for file transfers, or one smartphone and a Bluetooth speaker.

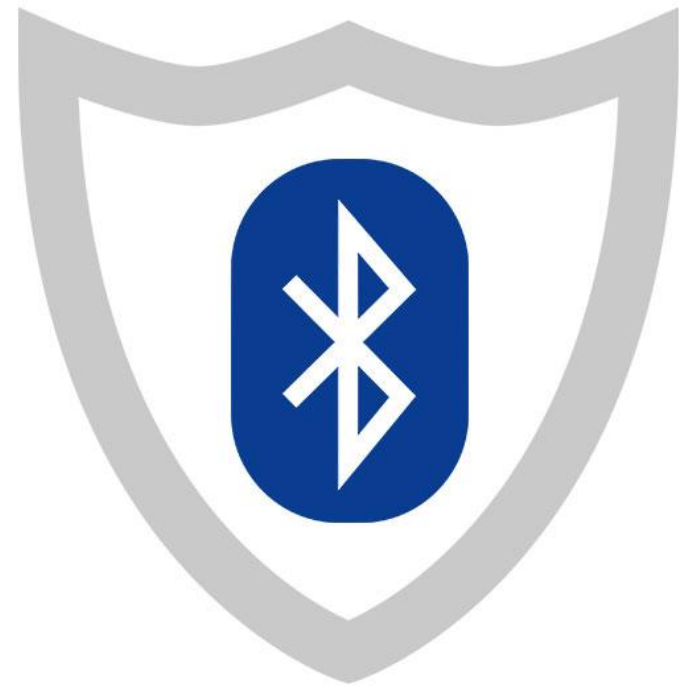


Versions of Bluetooth

Bluetooth Versions	Specification
Bluetooth v1.0 to v1.08	Mandatory Bluetooth hardware device and address
Bluetooth v1.1	IEEE standard 802.15.1-2002
Bluetooth v1.2	Faster connection
Bluetooth v2.0+EDR	Enhanced data rate
Bluetooth v2.1	Secure simple pairing
Bluetooth v3.0	High-speed data transfer
Bluetooth v4.0	Low energy consumption recently used in apple I – phone 4s

Bluetooth Security

To make snooping on its radio transmissions more difficult, Bluetooth utilizes adaptive frequency-hopping spread spectrum which automatically changes the radio frequency as many as 1,600 times per second. Data transmitted is split into packets and then transmitted across the randomly selected channels, avoiding any that are particularly busy. This is just one area that has been improved through successive generations of Bluetooth technology.



What is Zigbee?

- ▶ Zigbee is based on the IEEE's 802.15.4 personal-area network standard. All you need to know is that Zigbee is a specification that's been around for more than a decade, and it's widely considered an alternative to Wi-Fi and Bluetooth for some applications including low-powered devices that don't require a lot of bandwidth - like your smart home sensors.



Zigbee

The Zigbee technology is designed to carry small amounts of data over a short distance while consuming very little power. As opposed to Wi-Fi, it's a mesh networking standard, meaning each node in the network is connected to each other. This means you don't have to rely solely on the router and the endpoint.



Zigbee

A typical example is when you have a Zigbee-enabled light bulb and a Zigbee-enabled light switch and you want the light switch to control the light bulb. With Zigbee, the two devices - even if they're from different manufacturers - speak a common language, so there's no barrier to communication.



What devices use Zigbee?

- ▶ Amazon
- ▶ Comcast
- ▶ Honeywell
- ▶ Huawei
- ▶ Philips
- ▶ SmartThings
- ▶ Texas Instruments
- ▶ Belkin
- ▶ Ikea
- ▶ Lutron
- ▶ Nokia
- ▶ Osram
- ▶ Bosch
- ▶ Indesit
- ▶ Samsung
- ▶ Velux
- ▶ Humax
- ▶ Panasonic
- ▶ Miele

What is Z-wave?

Z-Wave is a wireless protocol harnessing low-energy radio waves to help smart devices or appliances communicate successfully with one another.



Z-Wave vs Zigbee

The stated goal was to create a cost-effective Zigbee alternative enabling devices from different brands to communicate in harmony.



Z-Wave

Z-Wave operates using very little power. By using frequencies of 908.42 MHz in the US and 868.42 MHz throughout Europe, Z-Wave suffers from very little interference as the 800 to 900 band is well clear of the 2.4GHz and 5GHz used by Wi-Fi and other devices, appliances, and protocols.



Advantages of Z-Wave

- ▶ Compatibility
- ▶ Wireless communication of 50 – 100 ft
- ▶ Low interference from other devices
- ▶ Secure- It uses AES-128 encryption to provide a secure network to users
- ▶ Range is increased with more devices as they act as a mesh network.
- ▶ High transmission speed



Cons to Z-Wave

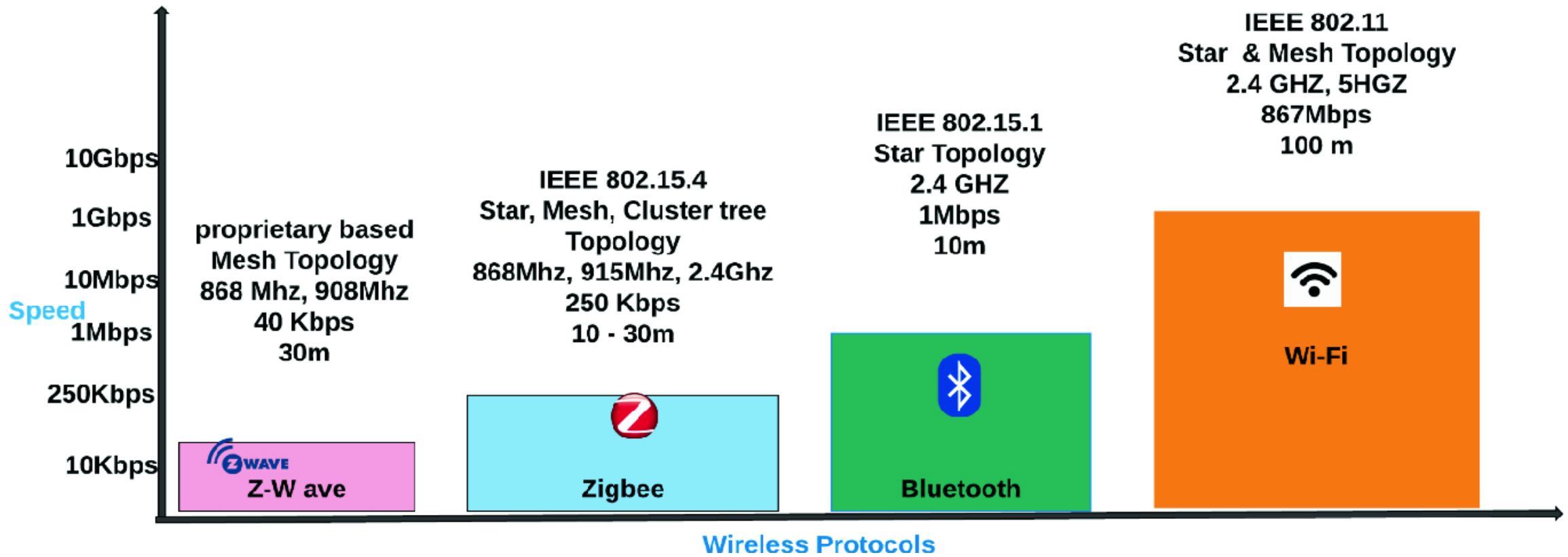
- ▶ It uses more power than others
- ▶ Although encrypted, because it is over normal radio frequencies, it is open to hacking.
- ▶ Low data rates of transmission
- ▶ A hub is required for operation
- ▶ Limitation of coverage




Devices that Use Z-Wave

- ▶ Fibaro Flood Sensor
- ▶ Kwikset Obsidian Smart Lock
- ▶ Ring Door/Window Sensor
- ▶ Oomi Dual In-Wall Switch
- ▶ Logitech Home Harmony Hub Extender
- ▶ August Smart Lock
- ▶ Zipato Bulb 2
- ▶ Abode Gateway
- ▶ Yale Keyfree Connected
- ▶ D-Link mydlink sensors
- ▶ Somfy ILT Series blinds
- ▶ ADT Security Hub
- ▶ GE Lighting Control

Smart Home Standard	Range	Data rate	Max no. of devices	Hub needed?
 Z-WAVE [®]	30 m (100 ft)	9.6 - 100 kbps	232	Yes
 ZigBee [®]	10 m (35 ft)	20 - 250 kbps	65,000	Yes



 **Z-W ave**

 **Zigbee**

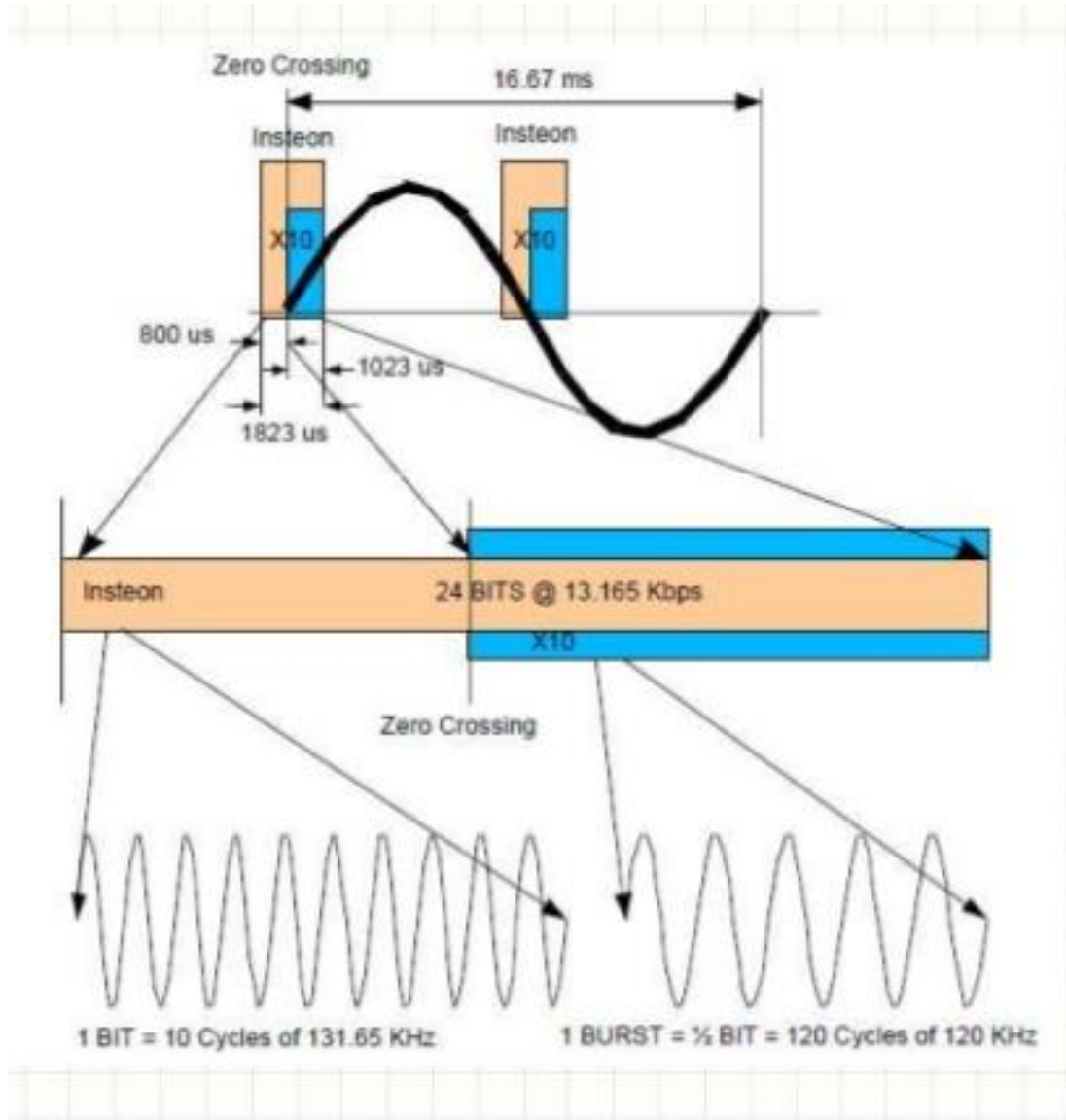
 **Bluetooth**

 **Wi-Fi**

Insteon

Insteon device to device interface is quite a bit different than other interfaces. It offers dual connectivity using the normal Wi-Fi network and the electrical powerlines that run to the devices. This creates a dual mesh network. Every device transmits, receives, and repeats messages. Any time a message is received, it is checked for errors and corrects it prior to transmission.

I N S T E  N[®]



Insteon Data Over Powerlines

HIDING DATA INSIDE OF THE
ALTERNATING CURRENT
WAVE

C-Bus

C-Bus is a Smart relay bus bar that allows the user to turn power sources on or off, or to dim them. Unlike X10 or UPB, C-Bus uses low voltage Cat5e cable to activate or deactivate a relay. The low voltage Cat5e is run to the C-Bus controller where it integrates into the rest of the Smart Home system for more user interface.



X10

X10 which is similar to Insteon, carries a signal over the mains power wiring in your home so you can control light switches, lamp holders or mains outlets. X10 allows you to control these locally or by remote control.



X10

X10 has been around for over 40 years, and even though there are now alternatives available without some of the shortcomings of X10 along with more bandwidth and functionality, X10 still occupies a pivotal role in home automation for millions of global users.



UPB

Universal powerline bus (or UPB) is a protocol for communication among devices used for home automation. It uses power line wiring for signaling and control.

UPB was developed by Powerline Control Systems (PCS) of Northridge, California and released in 1999. Based on the concept of the ubiquitous X10 standard, UPB has an improved transmission rate and higher reliability.



Lutron's Clear Connect

Lutron's patented Clear Connect RF technology minimizes interference from other "smart" devices in the home using a low-frequency 433MHz band.



Clear Connect

Lutron has solved a problem in home wiring in that it is now possible to not have to wire switches to allow them to control a light. This includes 3-ways and 4-ways. The cost benefit on the reduction in labor and material cost enables Clear Connect to be a more viable option than traditional wiring methods.



Google Thread

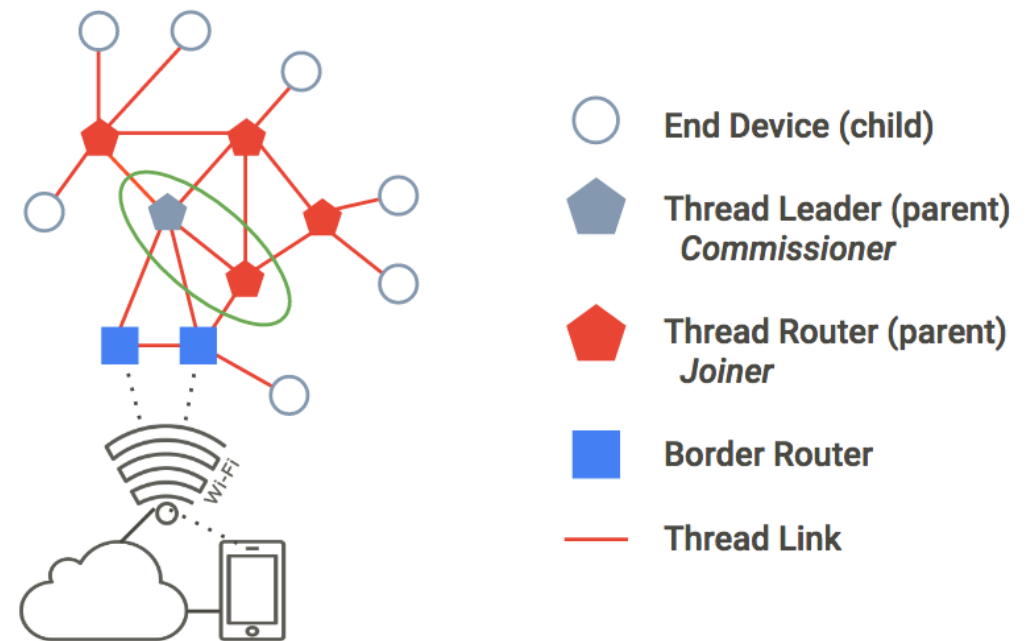
- ▶ Thread is a low-power wireless mesh networking protocol, based on the universally-supported Internet Protocol (IP), and built using open and proven standards.
- ▶ Thread is based on the broadly supported IEEE 802.15.4 radio standard, which is designed from the ground up for extremely low power consumption and low latency.



**BUILT ON
THREAD**

Google Thread Mesh

- ▶ Thread enables device-to-device and device-to-cloud communications and reliably connects hundreds (or thousands) of products and includes mandatory security features.
- ▶ Thread networks have no single point of failure, can self-heal and reconfigure when a device is added or removed.



RuBee

RuBee utilizes the IEEE 1901.2 protocol which is a long wave radio frequency. This means that it is limited on data transmission but is very low power consumption.

RuBee®

RuBee

RuBee tags are often confused with RFID tags. RFID tags do not transmit or receive but only reflect information from other transmitted sources. RuBee tags operate very much like Zigbee and Z-Wave in that they actively communicate between devices over a wireless protocol system.



RuBee Protocol

RuBee protocols are mainly used in security sensors and any other remote sensors that may not have the ability of a constant power source and transmit basic information such as activated or not activated.



Smart Home Automation

Smart Home Automation is helpful to reduce the total user input in the function of Smart Home. If there is a sequence of tasks that needs to be performed by an interface, automation allows these be performed seamlessly.



IFTTT

- ▶ While many smart home devices have built-in apps that allow for minute levels of customization and control, IFTTT makes it possible for different devices to trigger one another. For example, if something triggers your motion sensor, you can have an IFTTT recipe that in turn triggers your smart lights to flash.

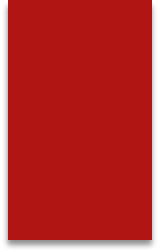


IFTTT Recipes

Creating a chain of actions that is triggered by a user interface is called a recipe.

Example:

- ▶ A geofence 150' around the home is triggered the Smart garage door opener opens the door.
- ▶ 2 minutes later, the Smart door lock unlocks the door leading from the garage to the home.
- ▶ If, geofence is activated during low light conditions, lights are illuminated down the driveway, garage and interior.
- ▶ Interior lighting is adjusted to warm hue in evening and cool hue in morning when activated.



Yonomi Smart Home Automation

The free Yonomi app is one the best way to create automated routines for all the smart home devices and bring the home to life. Yonomi makes it simple to discover, connect, and automate the most popular smart home devices using a single app.



Yonomi vs IFTTT

Yonomi (pronounced You Know Me) starts very similar to IFTTT. You connect devices, services, and accounts for the app to access. And then you set up automation (called routines here) in a “when this happens, run that action” manner.

Where Yonomi differs from IFTTT is that you can have multiple “when” triggers and Yonomi adds a “but only when” clause.

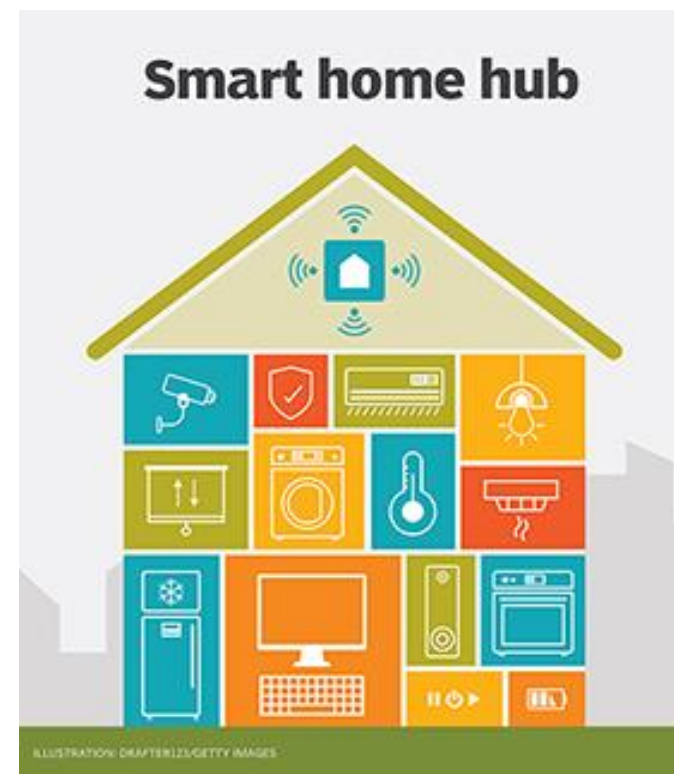


Module 3

INSPECTION CERTIFICATION ASSOCIATES

What is a Smart Home Hub?

- ▶ A hub is a device that serves as the nerve center of the home automation system and ties all of the devices together. Whether you need one or not depends on the type of components that are in need tying together.



What does a Smart Home Hub do?

If there are multiple smart home gadgets in the house from a variety of different manufacturers to make them work together may require a smart home hub.



Why have a Smart Home Hub?

To control many smart home devices such as the Ecobee, Ring doorbell, Arlo, it often requires individual apps for each access and control. A smart home hub gives you the ability to control many devices using only one access point or app.



Smart Home Hubs

- ▶ Wink Hub
- ▶ Wink Hub 2
- ▶ Echo by Amazon
- ▶ Google Home
- ▶ Samsung SmartThings
- ▶ Hubitat Elevation
- ▶ HomeKit by Apple
- ▶ Control 4
- ▶ Essentials Gateway
- ▶ Yonomi

Wink and Wink 2 Hub Supported Protocols

Bluetooth
Kidde
Clear Connect
Z-Wave
ZigBee



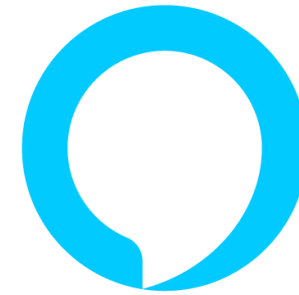
Amazon Echo Supported Protocols

- ▶ Zigbee
- ▶ Wi-Fi
- ▶ Bluetooth



Amazon Echo Show AI

The Echo Show Allows for the
integration of the AI Alexa.



amazon alexa

Google Nest Supported Protocols

- ▶ Wi-Fi
- ▶ Zigbee
- ▶ Z-wave
- ▶ Bluetooth



Google's Nest AI

Google's Nest AI Google Assistant
integrated



Samsung SmartThings Protocols

Z-Wave

Zigbee

Bluetooth

Wi-Fi



Samsung's Connect Home

The Connect Home box - essentially the Samsung SmartThings Hub - offers a hub/mesh-router combo that helps cut down on white box clutter and integrate everything more tightly.



SmartThings AI Integration

A big plus for SmartThings is the versatility of its AI integration. It is both compatible with both Alexa and Google Assistant.



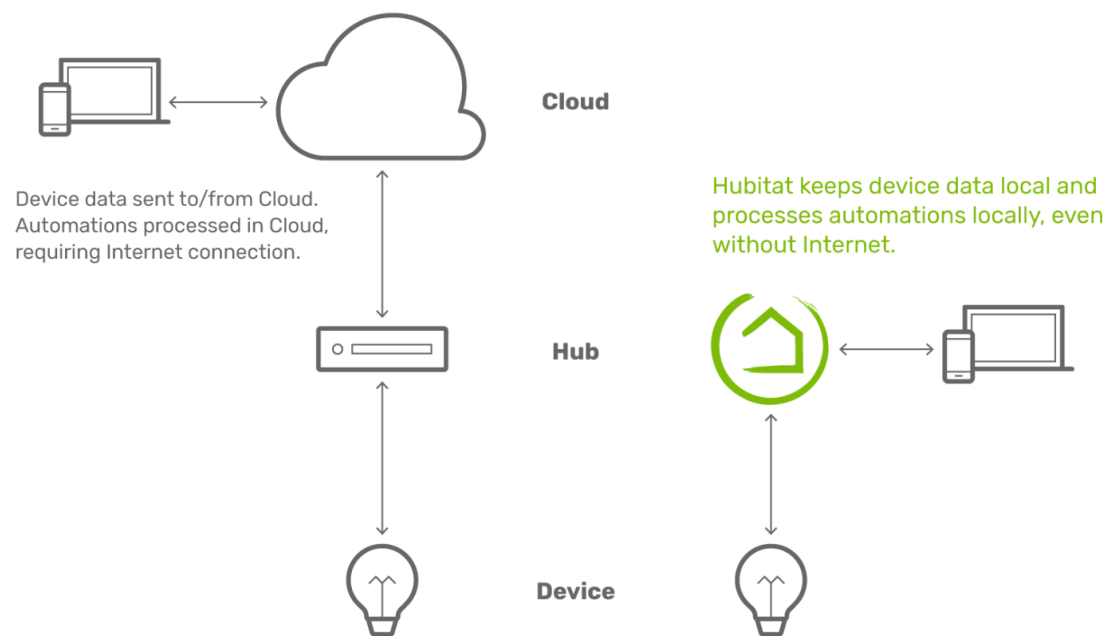
Hubitat Elevation

Hubitat works with a sizable number of products, primarily anything in the Z-Wave and ZigBee universes. It also has hooks for Lutron (including that company's RadioRA2, Serena, and Sivoia platforms) and a few other devices.



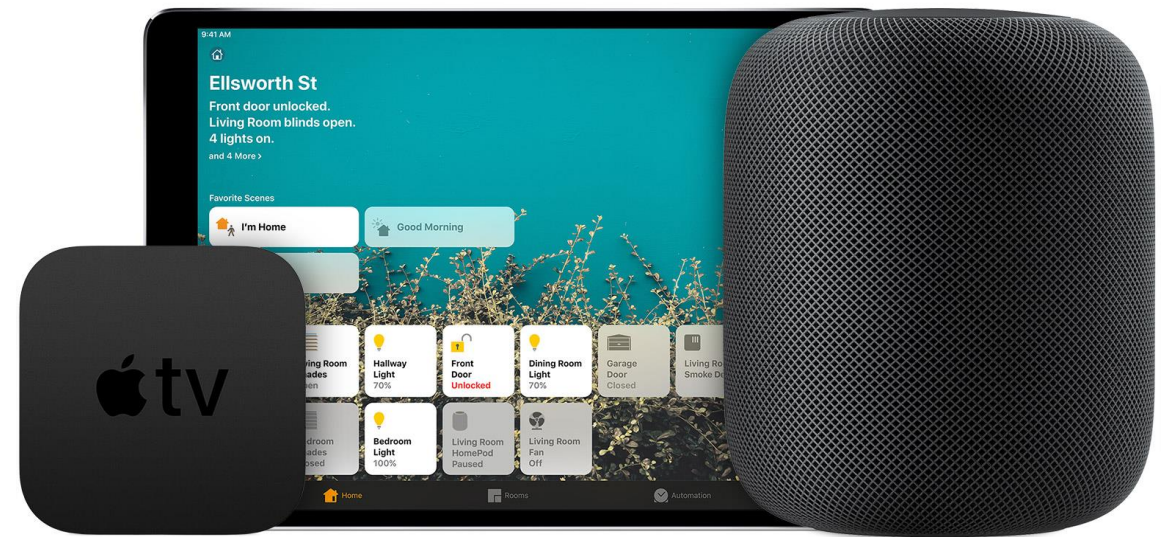
Habitat Elevation Security

Habitat boasts that because the system is entirely local and not cloud based on many of the other Smart Home Hubs, it is less prone to infiltration. All data is also stored locally which means backups are always recommended.



Homekit by Apple

There are many limitations to Homekit as it is more for connecting and streaming entertainment than other devices. Its digital interface types are limited to just Wi-Fi or Bluetooth and is not equipped with at the very least with Z-Wave or Zigbee.



HomeKit AI Compatibility

Because HomeKit is through Apple, it is limited to the use of Siri for AI integration into the Smart Home System.



Hey Siri

Control4

Control4 takes IFTTT to the next level and gives the user more control over the automation of the home by adding layers of integration. What is required is a Control4 control, what would be normally a Smart Home Hub.



Control4

Control4 user interface is done using remotes with various looks and abilities.



Control4 Protocol

Control4 uses:

- ▶ Wi-Fi
- ▶ Bluetooth
- ▶ Zigbee
- ▶ Z-Wave



Smart Home AI Interface Integration

If the hub does not have the ability for access to Siri, Alexa, or Google Assistant, integration with a device into the Smart Home System will often give the ability of the voice recognition AI interface.



Types of Smart Home Devices

- ▶ Entertainment
- ▶ Security, Safety, and damage control
- ▶ Lighting and Power
- ▶ Appliances
- ▶ HVAC

Entertainment

The majority of all entertainment or audio visual devices sold now are either Smart capable, or require connection to other Smart devices for them to function.



TV's and Projectors

With the rise of streaming news and entertainment and slow death of cable and satellite TV, Smart TV's and Projectors are becoming commonplace in the home. This means that the home needs good coverage of Wi-Fi for proper coverage.



Smart Speakers

Smart Speakers such as Sonos, Bose, and Echo can work without any other device but can access points for AI voice recognition interface but require connection to Wi-Fi and/or Bluetooth and then connected to the internet. Many times, these are not directly attached to the house.



Security Systems

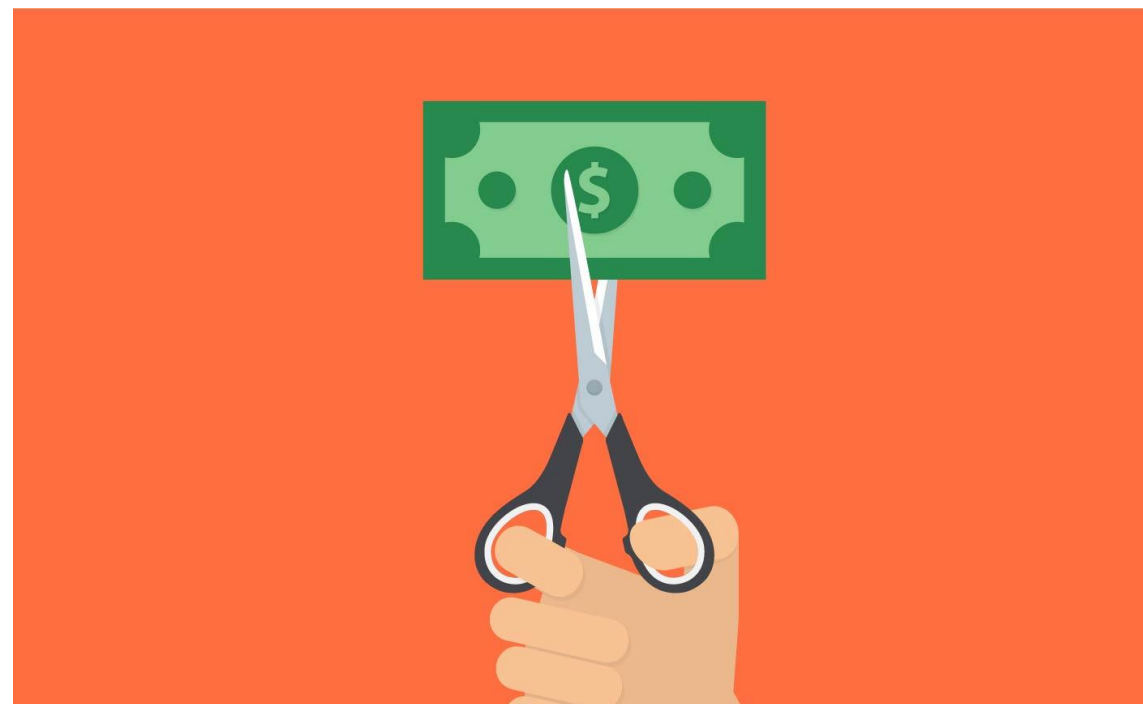
Security systems fall into two general categories:

- ▶ Monitored or the ability to be monitored
- ▶ Unmonitored



Advantage of Monitored

Typical insurance underwriters offer sometimes as much as 20% reduction on the homeowner's premium.



Popular Smart Security Systems

- ▶ ADT Pulse
- ▶ Ring
- ▶ Vivint
- ▶ Zegool
- ▶ Simplisafe

Components to a Smart Home Security System

- ▶ Hub
- ▶ Access Point
- ▶ Door and Window Sensors
- ▶ Motion Sensors
- ▶ Glass Break Sensors
- ▶ Cameras
- ▶ Smoke and Carbon Dioxide Detectors



Smart Security Interface Protocols

Wired

- ▶ X10
- ▶ UPB

Wireless

- ▶ Zigbee
- ▶ Z-wave

Hybrid

- ▶ Insteon
- ▶ RuBee

Smart Home Surveillance Systems

- ▶ Ring Cameras
- ▶ Google Nest Cameras
- ▶ Arlo
- ▶ Blink
- ▶ Zmodo

Types of Cameras

- ▶ Door
- ▶ Dome
- ▶ PTZ (Pan, Tilt, and Zoom)
- ▶ Bullet
- ▶ Hidden

Smart Home Security Camera Interface Protocols

Most Smart Home Security Cameras are now wireless IP (Internet Protocol) capable. Because of the potential distance to the cameras and high amounts of data, there are only a few options for protocols to use:

- ▶ Wi-Fi
- ▶ Zigbee
- ▶ Z-Wave

Door Cameras

Probably the most common for ease of installation and function



Dome Cameras

LIMITED TO CEILING
INSTALLATIONS





PTZ (Pan, Tilt, and Zoom) Cameras



Bullet Cameras



Hidden Cameras



Smart Door Locks

Smart Water Shut Off

- ▶ Moen
- ▶ Stream Labs
- ▶ Guardian
- ▶ Alexa



Smart Water Shut Off Capabilities

- ▶ Track water usage
- ▶ Remotely turn on or off
- ▶ Leak detection and automated shut off



Smart Lighting Systems

- ▶ Wyze
- ▶ Phillips Hue
- ▶ Lixt
- ▶ GE
- ▶ Sylvania
- ▶ Lutron



Smart Lighting Capabilities

- ▶ Dimmability
- ▶ Change of hue
- ▶ Automation
- ▶ Motion sensing

Smart Outlets and Switches

- ▶ Eaton
- ▶ Honeywell
- ▶ Leviton





Smart Circuit Breakers

Smart Home Appliances

- ▶ Refrigerators
- ▶ Washers and Dryers
- ▶ Stoves and Ovens
- ▶ Thermostats
- ▶ Garage Door Openers
- ▶ Gate Openers



Smart Refrigerator Capabilities

- ▶ Streaming music
- ▶ Automatically raising or lowering temperature for efficiency
- ▶ Looking inside without opening the door
- ▶ Creating an automated shopping list
- ▶ Ordering food based on usage



Smart Washers and Dryers Capabilities

- ▶ Ability to remotely control
- ▶ Automatically turning on or off for efficiency due to peak power usage of the day



Smart Home Ovens

- ▶ Remotely control
- ▶ Remote viewing





Smart Garage Door Openers





Smart Gate Openers

Smart Thermostats



- ▶ Ecobee
- ▶ Nest
- ▶ Honeywell Lyric
- ▶ Lux
- ▶ Idevices
- ▶ Hive

Smart Thermostats Capabilities

- ▶ Remotely controlled
- ▶ Change function based on what is necessary
- ▶ Track temperature and humidity inside and out
- ▶ Learn your habits to increase efficiency



Communicating vs Smart Thermostats

If an AC/furnace has any part of its system variable speed, the thermostat must be a “Communicating” thermostat. This means that the thermostat communicates directly with the components to determine capability.

Communicating Smart Thermostat

A thermostat can be both
“Communicating” and “Smart”

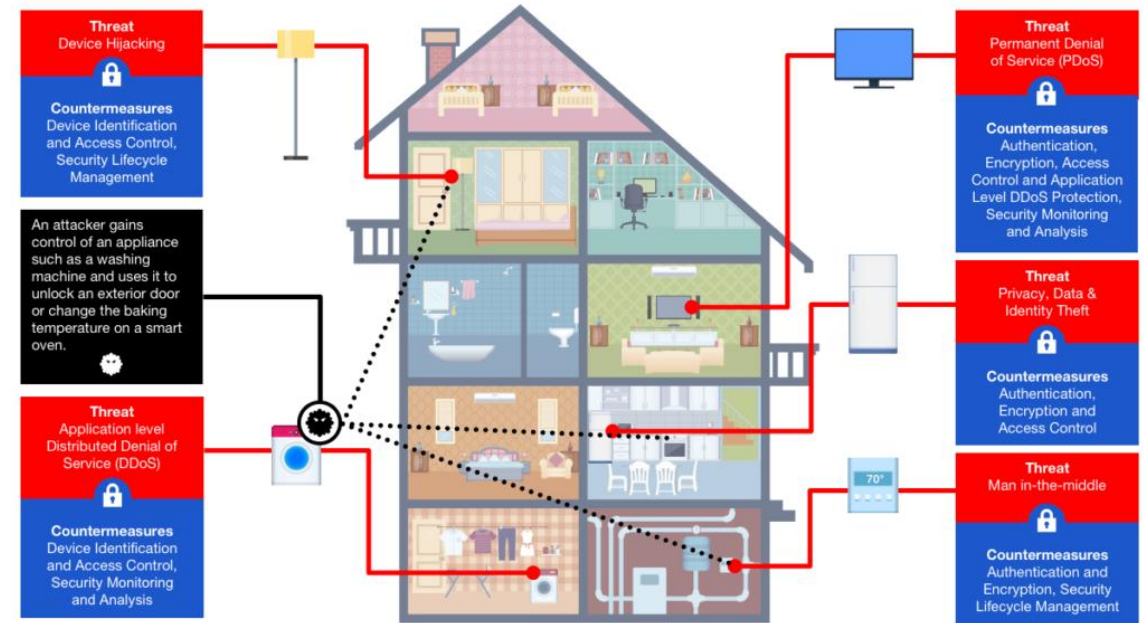


Module 4

INSPECTION CERTIFICATION ASSOCIATES

Smart Home System Vulnerabilities

An estimated 80% of Smart Home Devices are vulnerable to a wide range of attacks.

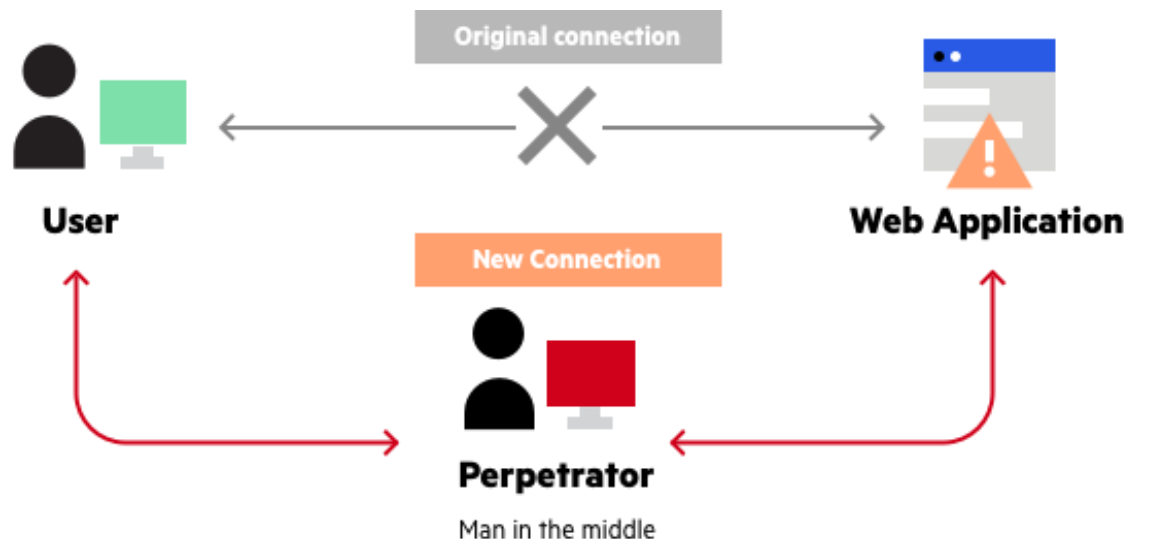


Common Attacks and Threats

- ▶ Man-in-the-middle
- ▶ Data and identity theft
- ▶ Device hijacking
- ▶ Distributed denial of service
- ▶ Permanent denial of service

Man-in-the-middle

A Man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other. One example of a MITM attack is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones.



Data and Identity Theft

Smart Home devices and systems are prone to data breaches either through a particular device or through the systems connection to the internet.



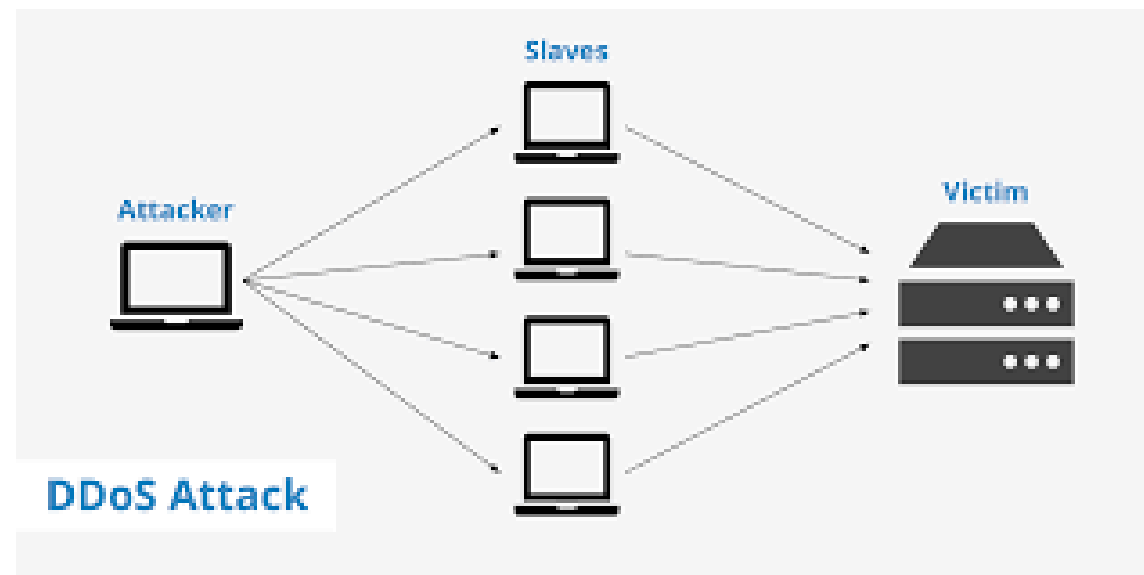
Device Hijacking

The attacker hijacks and effectively assumes control of a device. These attacks are quite difficult to detect because the attacker does not change the basic functionality of the device. Moreover, it only takes one device to potentially re-infect all smart devices in the home. For example, an attacker who initially compromises a thermostat can theoretically gain access to an entire network and remotely unlock a door or change the keypad PIN code to restrict entry



Distributed Denial of Services

A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network. A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users.



Permanent Denial of Service

Permanent denial-of-service attacks (PDoS), also known as phlashing, is an attack that damages the device so badly that it requires replacement or reinstallation of hardware. BrickerBot, coded to exploit hard-coded passwords in IoT devices and cause permanent denial of service, is one such example. Another example could see fake data fed to thermostats in an attempt to cause irreparable damage via extreme overheating.



Keeping a Smart Home Secure

- ▶ Rename the router
- ▶ Use strong encryption for the Wi-Fi
- ▶ Setup a guest network
- ▶ Change default user names and passwords
- ▶ Use strong unique passwords and device accounts
- ▶ Checking the smart device settings
- ▶ Disable unused features on the devices
- ▶ Keep the software up to date
- ▶ Audit older devices
- ▶ Two factor authentication
- ▶ Avoid public Wi-Fi networks
- ▶ Usage of VPN's
- ▶ Setup a firewall

Rename the Router

Renaming the router name away from the default preprogrammed name is important. Names should be somewhat obscure and not include any personal or address identifiers.



Hello
my name is

Encrypting Wi-Fi

- ▶ WEP
- ▶ WAP & WAP2
- ▶ WPS



Wired Equivalent Privacy Encryption

WEP stands for Wired Equivalent Privacy, a Wi-Fi wireless network security standard. A WEP key is a security passcode for Wi-Fi devices. WEP keys enable devices on a local network to exchange encrypted (mathematically encoded) messages with each other while hiding the contents of the messages from easy viewing by outsiders. WEP is less secure than other measures is more prone to hacking.

Wireless Protected Access 1,2,3

Wi-Fi Protected Access (WPA) was the Wi-Fi Alliance's direct response and replacement to the increasingly apparent vulnerabilities of the WEP standard. WPA was formally adopted in 2003, a year before WEP was officially retired. The most common WPA configuration is WPA-PSK (Pre-Shared Key). The keys used by WPA are 256-bit, a significant increase over the 64-bit and 128-bit keys used in the WEP system.

WPS

WPS stands for Wi-Fi Protected Setup. It is a wireless network security standard that tries to make connections between a router and wireless devices faster and easier. WPS works only for wireless networks that use a password that is encrypted with the WPA Personal or WPA2 Personal security protocols.

Setup a Guest Network

Keep your Wi-Fi account private. Visitors, friends and relatives can log into a separate network that doesn't tie into your IoT devices.



Change Default Names and Passwords

Cybercriminals probably already know the default passwords that come with many IoT products. That makes it easy for them to access your IoT devices and, potentially, the information on them.

Using Strong Unique Passwords and Device Accounts

Avoid common words or passwords that are easy to guess, such as “password” or “123456.” Instead, use unique, complex passwords made up of letters, numbers, and symbols. You might also consider a password manager to up your security game.

Checking Device Settings

Smart Home devices might come with default privacy and security settings. You might want to consider changing them, as some default settings could benefit the manufacturer more than they benefit you.

Device Features

Smart Home devices come with a variety of services such as remote access, often enabled by default. If there are settings on devices that are not being utilized or are not 100% necessary, disable the feature to limit potential vulnerabilities.

Updating Software

When your smart phone manufacturer sends you a software update, don't put off installing it. It might be a patch for a security flaw. Mobile security is important, since you may connect to your smart home through mobile devices. Your IoT device makers also may send you updates — or you might have to visit their websites to check for them. Be sure to download updates and apply them to your device to help stay safe.

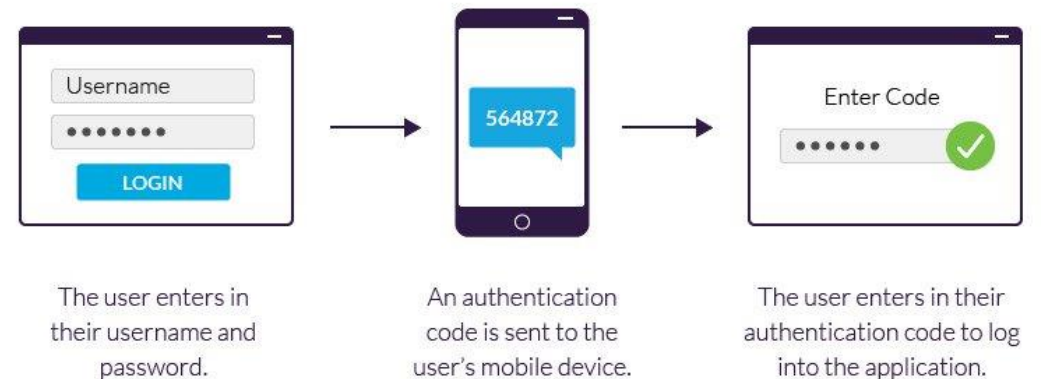
Audit Older Devices

Older devices may have design flaws that may allow access to the entire system.



Two-factor Authentication

Two-factor authentication (2FA), a type of multi-factor authentication (MFA), is a security process that cross-verifies users with two different forms of identification, most commonly knowledge of an email address and proof of ownership of a mobile phone.



Two-factor Authentication

Used on top of the regular username/password verification, 2FA bolsters security by making it more difficult for intruders to gain unauthorized access, even if a perpetrator gets past the first authentication step (e.g., brute forces a username and password).

Multi-factor Authentication Methods

MFA identification can be categorized into three types:

- ▶ Knowledge factors (something the user knows) – Common examples are email addresses, username-password combinations, answers to security questions, and the CVV on the back of a credit card.
- ▶ Possession factors (something the user owns) – Examples of this authentication type include a mobile phone, USB token and a card reader.
- ▶ Inherence factors (something the user is/has) – This authentication type pertains to unique physical attributes that are inherent to a single person, such as fingerprint readers, retinal scans and voice recognition.

Public Wi-Fi

Managing smart home devices through a mobile device in a coffee shop across town can allow others on the network potential access for a host of attacks and access to the smart home system.



VPN

A virtual private network (VPN) gives you online privacy and anonymity by creating a private network from a public internet connection. VPNs mask your internet protocol (IP) address so your online actions are virtually untraceable. Most important, VPN services establish secure and encrypted connections to provide greater privacy than even a secured Wi-Fi hotspot.



What are Firewalls?

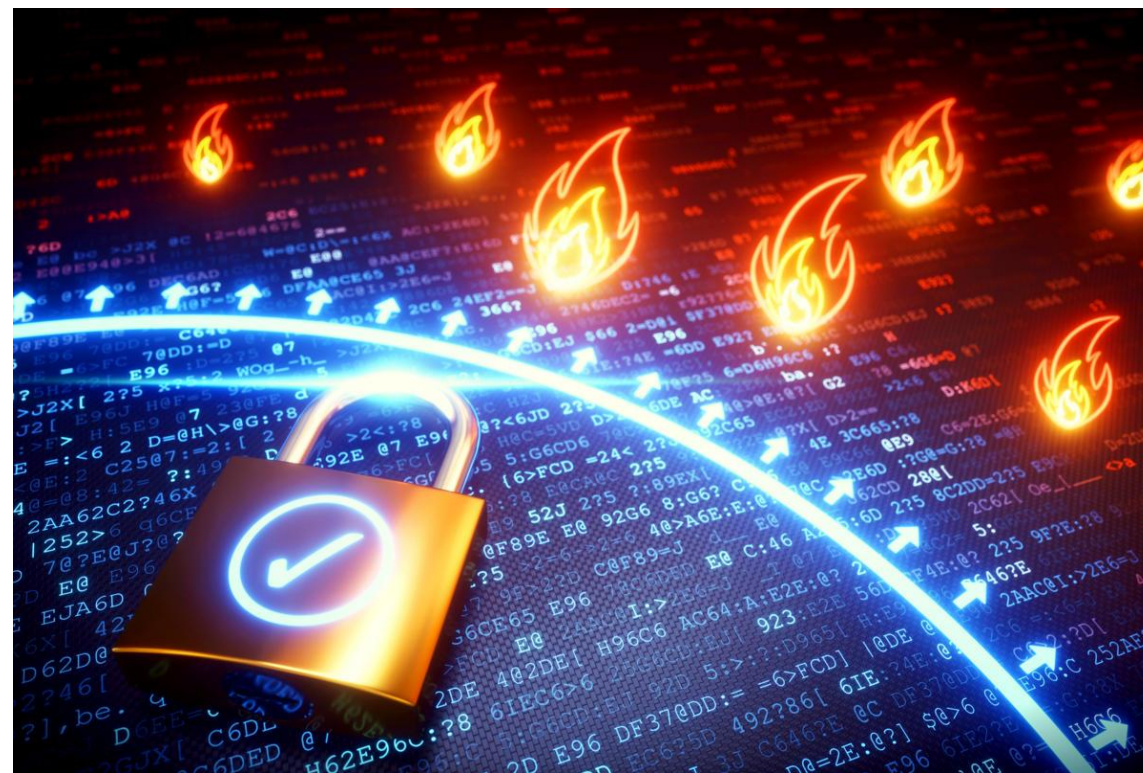
Firewalls carefully analyze incoming traffic based on pre-established rules and filter traffic coming from unsecured or suspicious sources to prevent attacks. Firewalls guard traffic at a computer's entry point, called ports, which is where information is exchanged with external devices. For example, "Source address 172.18.1.1 is allowed to reach destination 172.18.2.1 over port 22."

Firewalls

Think of IP addresses as houses, and port numbers as rooms within the house. Only trusted people (source addresses) are allowed to enter the house (destination address) at all—then it's further filtered so that people within the house are only allowed to access certain rooms (destination ports), depending on if they're the owner, a child, or a guest. The owner is allowed to any room (any port), while children and guests are allowed into a certain set of rooms (specific ports).

Firewalls

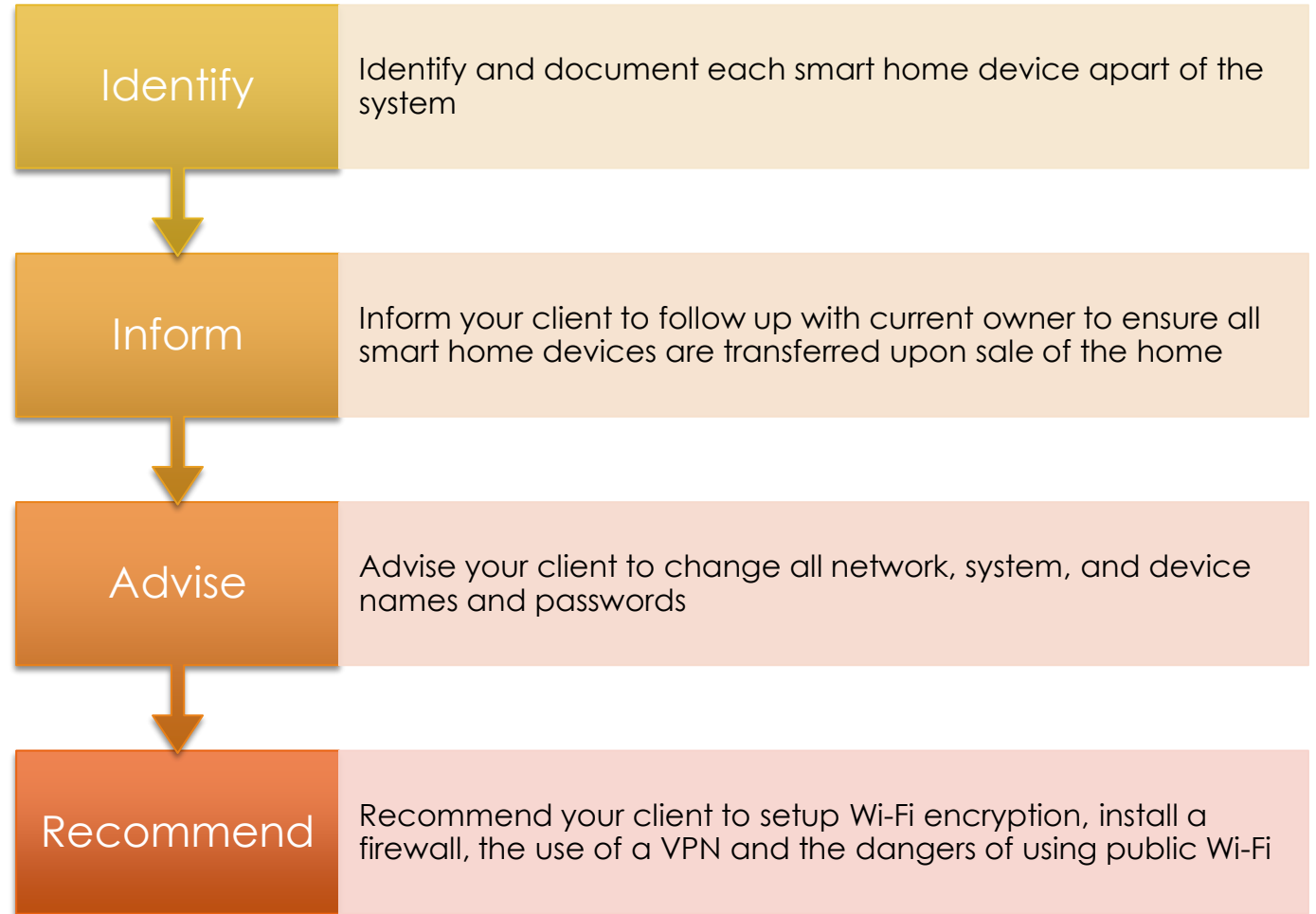
Many routers have a firewall you can turn on, but if you really want to be safe, you can purchase hardware options that can be placed between your modem and your Wi-Fi access point.



Summary

- ▶ Know how to spot smart home devices
- ▶ Know what to advise your client about the existing smart home devices
- ▶ Inform your client of steps to take to protect the smart home system

Your Client





End of Course

INSPECTION CERTIFICATION ASSOCIATES