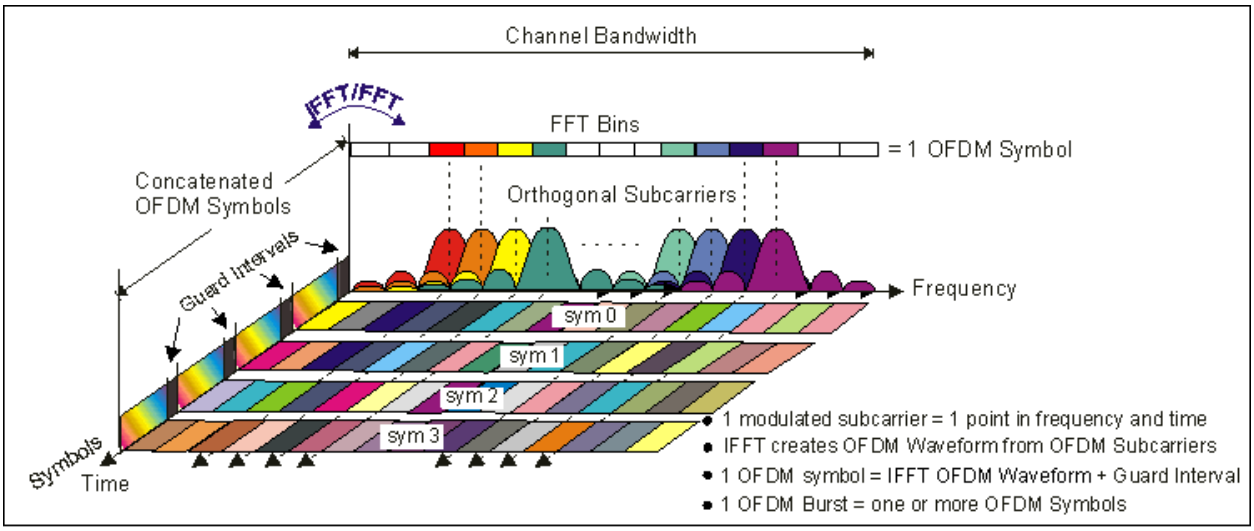
Wireless Network Defense

Wireless Terminologies

Orthogonal Frequency-Division Multiplexing (OFDM)

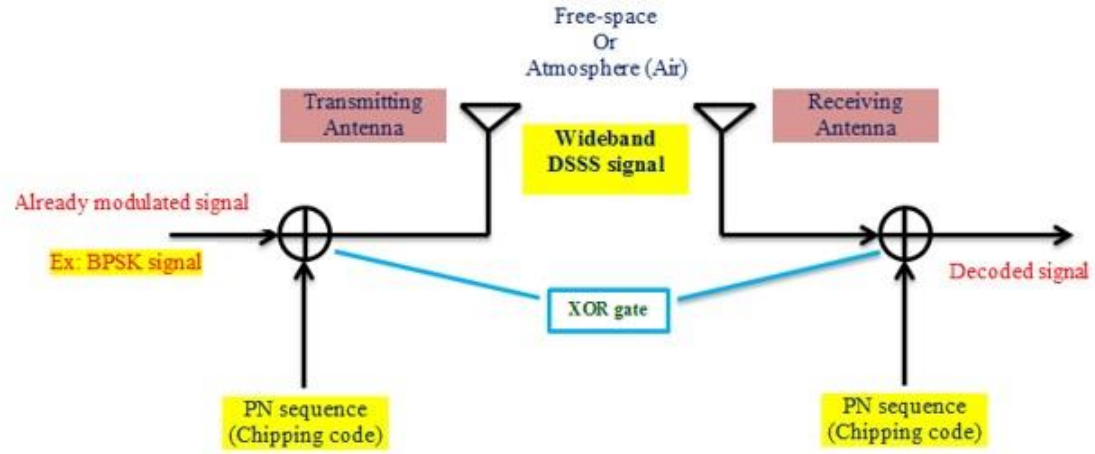
OFDM is a system modulation format that encodes digital data to multiple channels distributed across the frequency band. OFDM minimizes the attenuation in transmission, resulting in high throughput. It is used by 802.11 a, g, n, and ac wireless standards.



Frequency-Time Representative of an OFDM signal

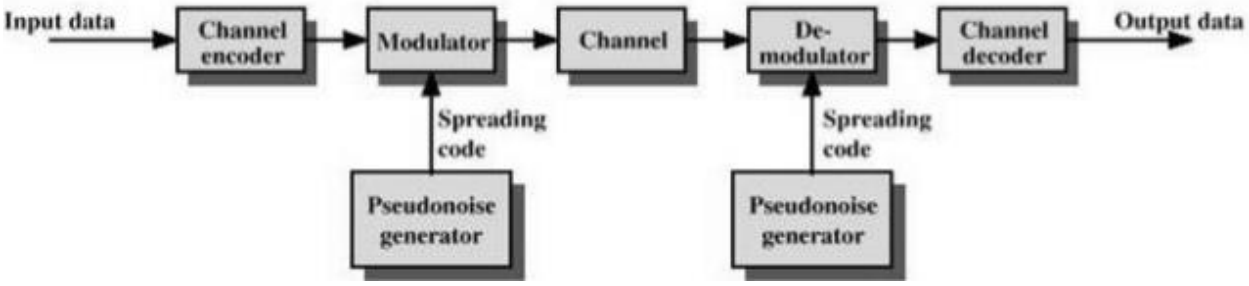
Direct-Sequence Spread Spectrum (DSSS)

DSSS is a modulation technique that transmits digital signals over airwaves. This transmission process needs spread spectrum modulation. 802.11b network works on the DSSS technique. DSSS requires more bandwidth, as it allows channel sharing.



Frequency-hopping Spread Spectrum (FHSS)

Local-Area Wireless Network (LAWN) uses the FHSS modulation technique. The transmission hop in FHSS occurs several times per second, allowing devices in a short range to work well. Large systems using the same frequency do not affect how small devices work.



Multiple-input, Multiple Output-Orthogonal Frequency Division Multiplexing (MIMO-OFDM)

MIMO-OFDM influences the spectral efficiency of 4G and 5G wireless communication services. Adopting the MIMO-OFDM technique reduces the interference and increases the robustness of the channel.

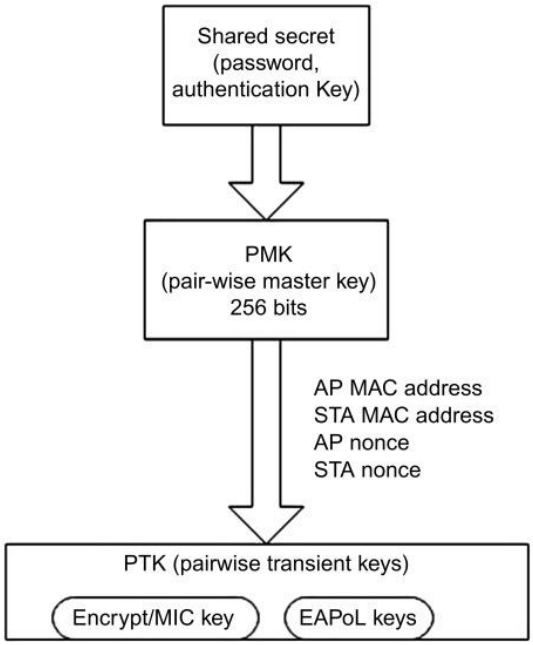
Service Set Identifier (SSID)

SSID is a 32-character alphanumeric sequence that acts as a wireless identifier on the network.

The SSID permits connections to the required network among an available independent network. Devices connecting to the same WLAN should use the same SSID to establish the connection.

Temporal Key Integrity Protocol (TKIP)

A TKIP is an encryption protocol that is a part of a WLAN. It encrypts each data packet with a unique encryption key. A TKIP is a set of algorithms and is more secure than WEP.



Lightweight Extensible Authentication Protocol (LEAP)

LEAP is a proprietary CISCO authentication version protocol that is used in wireless networks and point-to-point connections. The authentication protocol depends on WEP keys that change with the frequent authentication process between a client and a server.

Extensible Authentication Protocol (EAP)

The EAP authentication protocol is used by the point-to-point protocol (PPP). It supports multiple authentication types such as smart cards, token cards, public key encryption, etc. EAP has several authentication methods including EAP-TLS, EAP-SIM, EAP-AKA, and EAP-TTLS.

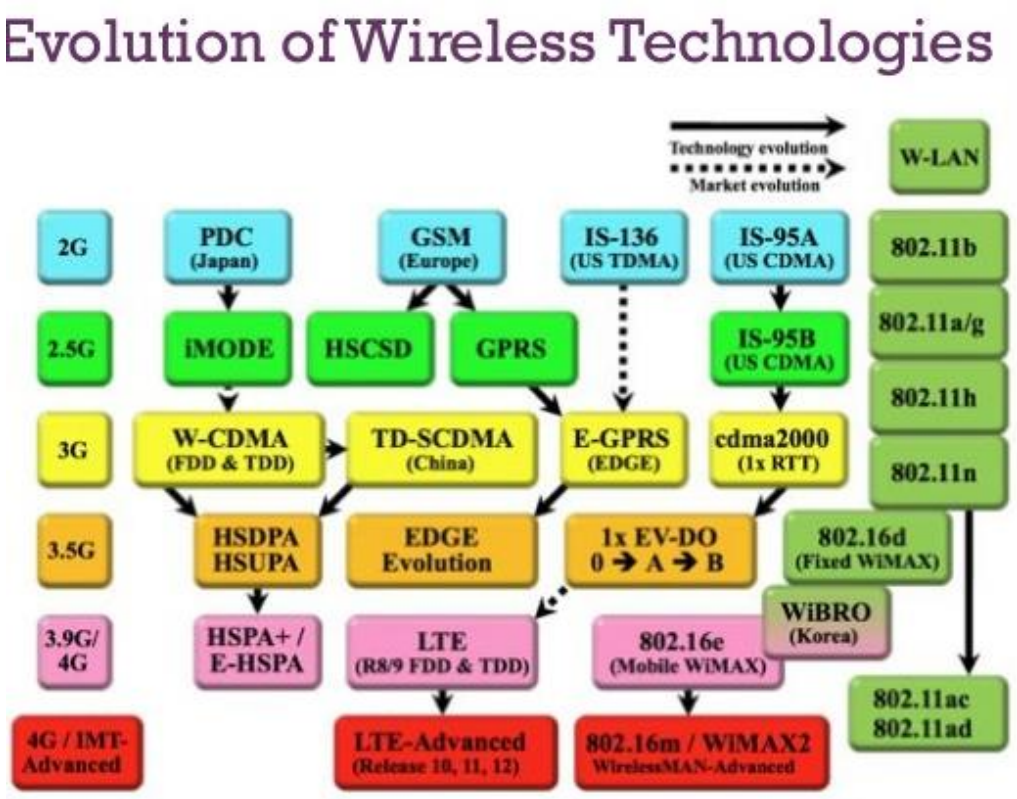
Wireless Networks

The computer world is heading toward a new era of technological evolution through the use wireless technologies. Wireless networking is revolutionizing the way people work and play. By removing the physical connection or cable, individuals are able to use networks in newer ways to make data portable, mobile, and accessible.

A wireless environment opens up so many new expansions and workflow possibilities. With wireless, there is no need to worry if a user wants to move the PC from one office to the next—or if they want to work in a location that does not have an Ethernet port. Wireless networking is very useful in public places including libraries, coffee shops, hotels, airports, and other establishments that offer wireless local-area network (LAN) connections. The most important thing for wireless networking is an access point where the user can communicate with other mobile devices or a fixed host. An access point is a device that contains a radio transceiver (send and receive signals) along with a RJ-45 wired network interface, which allows a user to connect to a standard wired network using a cable.

Wireless Technologies

In a wireless network, data transmits by means of electromagnetic waves to carry signals over the communication path.



Types of wireless technologies:

Wi-Fi

Wi-Fi is a part of the IEEE 802.11 family of wireless networking standards. This technology uses radio waves or microwaves to allow electronic devices to exchange the data or connect to the Internet. Many devices such as personal computers, laptops, digital cameras, and smartphones support Wi-Fi. Wi-Fi operates in the frequency band between 2.4 GHz to 5GHz. A Wi-Fi network uses radio waves to transmit the signals across the network. For this purpose, the computer should have a wireless adapter to translate data into radio signals and then pass them through the antenna and router. This is where the message is decoded and then the data is sent to the Internet or through another network. Hotspots refer to areas with Wi-Fi availability, where users can enable Wi-Fi on their devices and connect to the Internet through a hotspot.

Bluetooth

With Bluetooth technology data is transmitted between cellphones, computers, and other networking devices over short distances. Signals transmitting from Bluetooth cover short distances compared to other modes of wireless communication (i.e. up to 10 meters). Bluetooth transfers the data at less than 1Mbps and operates in the frequency range of 2.4 GHz. This technology comes under IEEE 802.15 and uses a radio technology called frequency-hopping spread spectrum to transfer data to other Bluetooth-enabled devices.

RFID

RFID stands for Radio-Frequency Identification. This technology uses radio-frequency electromagnetic waves to transfer data for automatic identification and tracking tags attached to objects. RFID devices work within a small range (i.e. up to 20 feet).

WiMax

This technology uses long-distance wireless networking and high-speed Internet. It stands for Worldwide Interoperability for Microwave Access and belongs to the IEEE 802.16 family of wireless networking standards. WiMAX signals can function over a distance of several miles with data rates reaching up to 75 Mbps. It uses a fixed wireless application and mobile stations to provide high-speed data, voice, video calls, and Internet connectivity to users. The WiMax forum developed WiMax and reports that nearly 135 countries have deployed over 455 WiMax networks

Wired vs. Wireless Networks

The differences between a wired and a wireless network are shown below:

Wired Network	**Wireless Network**
Low error rates	High error rates
Connected operation	Disconnected operation
High bandwidth	Low bandwidth
Low bandwidth variation	High bandwidth variation
More secure	Less secure
Less equipment dependent	More equipment dependent
Symmetric connectivity	Possible asymmetric connectivity
Low delay	Higher delay

Wireless network advantages:

- **Accessibility**: Devices connected to a wireless network can be accessed from any location within the coverage area.
- **Flexibility**: Devices may be carried from one location to another within the coverage area. This helps people access the Internet from any location.
- **Efficiency**: A wireless network improves the efficiency of employees in an organization, as they are able to access the Internet and perform suitable actions in order to complete the work within the stipulated time. They can work on the go and do not require an office.
- **Easy to Set-up:** Low cost and less time to set up makes a wireless network easier to use than a wired network.
- **Security**: Advanced security features have been employed for the security of the wireless network.
- **Expandable**: Easy to expand the coverage area for a particular location. Installation is easy and eliminates wiring

Wireless network disadvantages:

There are disadvantages for wireless networks when compared to the wired networks. The disadvantages include:

- Electromagnetic interference caused by another network or other devices may interrupt the network, leading to system failure and slow/lost signals.
- Some locations are not suitable for wireless networking. The areas where no signals are available are called black spots.
- Wi-Fi security may not meet expectations.
- The bandwidth suffers with the number of users on the network.
- Wi-Fi standard changes may require replacing wireless components.
- Some electronic equipment can interfere with the Wi-Fi network.

Wireless Standards IEEE standards

These standards are wireless networking transmission methods.

Standard	Freq Band	Bandwidth	Modulation	Max Data Rate
802.11	2.4 GHz	20 MHz	DSSS,FHSS	2 Mbs
802.11b	2.4 GHz	20 MHz	DSSS	11 Mbs
802.11a	5.0 GHz	20 MHz	OFDM	55 Mbs
802.11g	2.4 GHz	20 MHz	DSSS,OFDM	55 Mbs
802.11n	2.4 GHz, 5.0 GHz	20 MHz,40 MHz	OFDM	600 Mbs
802.11ac	5.0 GHz	20 MHz,40 MHz, 80 MHz,160 MHz	OFDM	6.93 Gbs

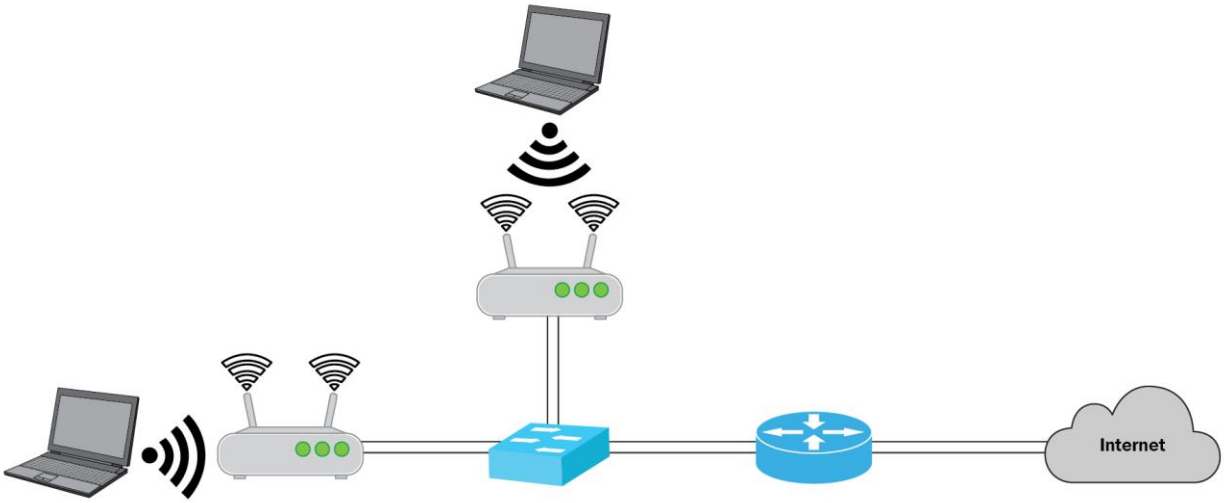
The following are the IEEE standards:

- **8021.11 (Wi-Fi):** It applies to wireless LANs and uses FHSS or DSSS as the frequency-hopping spectrum. It allows the electronic device to connect using a wireless connection that is established in any network.
- **802.11a**: It is the second extension to the original 802.11 and it operates in the 5GHz frequency band. It supports bandwidth up to 54 Mbps by using Orthogonal Frequency-Division Multiplexing. It has a fast maximum speed, but is more sensitive to walls and other obstacles.
- **802.11b:** IEEE expanded the 802.11 by creating 802.11b specifications in 1999. This standard operates in the 2.4 GHz ISM band and it supports bandwidth up to 11 Mbps by using direct-sequence spread spectrum modulation.
- **802.11d**: It is an enhanced version of 802.11a and 802.11b. The standard supports regulatory domains. The particulars of this standard can be set at the media access control (MAC) layer.
- **802.11e**: It defines the Quality of Service (QoS) for wireless applications. The enhanced service is modified through the MAC layer. The standard maintains the quality of video and audio streaming, real-time online applications, VoIP, etc.
- **802.11g:** It is an extension of 802.11 and supports a maximum bandwidth of 54Mbps using the Orthogonal Frequency-Division Multiplexing (OFDM) technology. It uses the same 2.4 GHz band as 802.11b. It is compatible with the 802.11b standard, which means 802.11b devices can work directly with an 802.11g access point.

- **802.11i:** It is used as a standard for WLANs and provides improved encryption for networks. 802.11i requires new protocols such as TKIP and AES.
- **802.11n:** Developed in 2009. This standard aims to improve the 802.11g standard in terms of bandwidth amount. It operates on both the 2.4 and 5 GHz bands and supports a maximum data rate up to 300Mbps. It uses multiple transmitters and receiver antennas (MIMO) to allow a maximum data rate—along with security improvements.
- **802.11ac:** It provides a high throughput network at the frequency of 5GHz. It is faster and more reliable than the 802.11n version. The standard involves Gigabit networking that provides an instantaneous data transfer experience.
- **802.11ad**: 802.11ad involves the inclusion of a new physical layer for 802.11 networks. The standard works on the 60GHz spectrum. The data propagation speed in this standard is a lot different from bands operating on 2.4GHz and 5GHz. With a very high frequency spectrum, the transfer speed is much higher than that of 802.11n.
- **802.12**: This standard dominates media utilization by working on the demand-priority protocol. Based on this standard, the Ethernet speed increases to 100Mbps. It is compatible with 802.3 and 802.5 standards. Users currently on those standards can directly upgrade to the 802.12 standard.
- **802.15:** It defines the standards for a wireless personal area network (WPAN). It describes the specification for wireless connectivity with fixed or portable devices.
- **802.15.1 (Bluetooth):** Bluetooth is mainly used for exchanging data over short distances for fixed and mobile devices.
- **802.15.4 (ZigBee):** The 802.15.4 has a low data rate and complexity. ZigBee is the specification used in the 802.15.4 standard. ZigBee transmits long-distance data through a mesh network. The specification handles applications with a low data rate, but longer battery life. Its data rate is 250kbits/s.
- **802.15.5**: The standard deploys itself on a full mesh or a half-mesh topology. It includes network initialization, addressing, and unicasting.
- **IEEE 802.16:** It is also known as WiMax. This standard is a specification for fixed broadband wireless metropolitan access networks (MANs) that use a point-to-multipoint architecture

Wireless Topologies

To plan and install a wireless network, first determine the type of architecture suited for the network environment.



There are two types of wireless topologies:

Standalone Architecture (Ad-Hoc mode)

Ad-Hoc mode is also called an IBSS (Independent Basic Service Set) mode. Devices connected over the wireless network communicate with each other directly (as in the peer-to-peer communication mode). The Ad-Hoc mode does not use wireless components such as routers and switches for communication between devices. Configure the wireless adaptors on each device on Ad-Hoc mode rather than on infrastructure mode. Adaptors for all the devices must use the same channel name and SSID to establish the connections successfully.

This mode works effectively for a small group of devices and it is necessary to connect all the devices with each other in close proximity. Performance degrades as the number of devices increases. It becomes cumbersome for a network administrator to manage the network in this mode because devices connect and disconnect regularly. It is not possible to bridge this mode with a traditional wired network and it does not allow Internet access until a special gateway is present.

The key characteristics of infrastructure mode include:

- Increases or decreases the wireless network range by adding and removing access points.
- The controller reconfigures the network according to the changes in the RF footprint.
- The controller regularly monitors and controls the activities on the wireless network by reconfiguring the access point elements to maintain and protect the network.
- The wireless centralized controller manages all the access-point tasks.
- The wireless network controller performs various crucial tasks such as user authentication, policy creation and enforcement, fault tolerances, network expansion, configuration control, etc.

- Maintains backups of other access points in another location and is used when the access point malfunctions.

Typical Uses of a Wireless Networks

Wireless networks are classified based on the connection used and the geographical area. Using a wireless network based on the connection:

Extension to a Wired Network

Extension to a wired network can be obtained by placing access points between the wired network and the wireless devices. In this network, the access point acts like a hub providing connectivity for wireless computers. It can also connect a wireless LAN to a wired LAN, which allows wireless computers access to LAN resources (such as file servers or existing Internet connectivity).

The two types of access points used in this wireless network are:

1. Software access points can be connected to a wired network and run on a computer with a wireless network interface card.

2. Hardware access points (HAP) provide comprehensive support of most wireless features. With suitable networking software support, users on the wireless LAN can share files and printers situated on the wired LAN (and vice versa).

The network may be further extended in accordance with the size of the location and interference from other devices. This enables the wired/wireless connection across the location for multiple users.

Multiple Access Points

Wireless computers connect using multiple access points. If a single large area is not covered by a single access point, then use multiple access points (or extension points). Extension points are not defined in the wireless standard. While using multiple access points, each access point must cover its neighbors. This allows users to move around seamlessly using a feature called roaming. Some manufacturers develop extension points, which act as wireless relays—extending the range of a single access point. Multiple extension points can be strung together to give wireless access to distant locations from the central access point.

LAN-to-LAN wireless networks

Access points provide wireless connectivity to local computers and computers on a different network. All hardware access points have the capability to directly connect to another hardware access point. Interconnecting LANs by using wireless connections is large and complex. Several LAN-enabled PCs can be connected to the access point for wireless communication.

3G Hotspot

A hotspot provides Internet access over a WLAN with the help of a router connected to the ISP. Many devices may be connected at the same time using a Wi-Fi network

adapter. 3G networks provide 300Kbits per second. Hotspots use the service from cellular providers for 3G Internet access. Computers generally scan for hotspots, thereby identifying the SSID (network name) of the wireless network.

Using a wireless network based on the Geographic Area:

Wireless networks are classified into WLAN, WWAN, WPAN, and WMAN based on the area they cover geographically. WLAN (Wireless Local-Area Network) A WLAN is a Wireless Local-Area Network that connects users in a local area with a network. The area may range from a single room to an entire campus.

- It connects wireless users and the wired network.
- It uses high-frequency radio waves.
- WLAN is also known as a LAWN (Local-Area Wireless Network).
- In 1990, IEEE (Institute of Electrical and Electronic Engineers) created a group to develop a standard for wireless equipment.
- In the peer-to-peer mode, wireless devices within range of each other communicate directly without using a central access point.
- While in infrastructure mode, the access point is wired to the Internet with wireless users. An access point functions as a mediator between the wired and wireless networks.

WWAN (Wireless Wide-Area Network)

The WWAN is a Wireless Wide-Area Network. It covers an area larger than the WLAN.

- It handles cellular network technology such as CDMA, GSM, GPRS, and CDPD for data transmission.
- This technology may cover a particular region, nation, or even the entire globe.
- The system has a built-in cellular radio (GSM/CDMA), which helps users send or receive data.
- In WWAN, the wireless data consists of fixed microwave links, digital dispatch networks, wireless LANs, data over cellular networks, wireless WANs, satellite links, one-way and two-way paging networks, laser-based communications, diffuse infrared, keyless car entry, the global positioning system, and more.

WPAN (Wireless Personal-Area Network)

WPAN is a Wireless Personal-Area Network. It interconnects devices positioned around an individual, in which the connections are wireless.

- PAN has a very short range. It can communicate within a range of 10 meters—for example, Bluetooth.
- A WPAN interconnects the mobile network devices that people carry with them or have on their desk.
- A main concept in WPAN technology is plugging in.
- When any two WPAN devices come within the range of a few meters to the central server, they communicate with each other—like a wired network.

- Another characteristic of a WPAN is the ability to lock out other devices and prevent interference.
- Every device in a WPAN can connect to any other device in the same WPAN, but they should be within physical range of each another. Bluetooth is the best example of WPAN.

WMAN (Wireless Metropolitan-Area Network)

WMAN covers a metropolitan area such as an entire city or suburb.

- It accesses broadband area networks by using an exterior antenna.
- It is a good option for a fixed-line network. It is simple to build and is inexpensive.
- In a WMAN, the subscriber stations communicate with the base station that is connected to a central network or hub.
- A WMAN uses a wireless infrastructure or optical fiber connections to link the sites.
- A WMAN links between the WLANs. Distributed Queue Dual Bus (DQDB) is the MAN standard for data communications, specified by the IEEE 802.6 standards. With the DQDB, the network can be established over 30 miles with a speed of 34 to 154 Mbits/s.

Components of a Wireless Network

Typical wireless components are devices that connect to the network.

The key components of a Wireless Network include:

Wireless Access point (WAP): A WAP is a hardware device that uses the wireless infrastructure network mode to connect wireless components to a wired network for data transmission. It serves as a switch or hub between the wired LAN and wireless network. It has a built-in transmitter, receiver, and antenna. The additional ports in the WAP help to expand the network range and provide access to additional clients. The number of APs depends on the network size. However, multiple APs provide access to more wireless clients and, in turn, expand the wireless network range. The transmission range and distance a client has to be from the wireless access point is a maximum default value; access points transmit usable signals well beyond the default range. The distance a wireless access point signal is transmitted depends on the wireless standards, obstructions, and environmental conditions between the clients and the access points. The transmission range and number of devices that a WAP can connect depends on the wireless standard used and the signal interference between the devices. In the wireless infrastructure network design, multiple access points can be used to cover an extensive area or a single access point can be used to cover a small geographical area (such as buildings, homes, etc.).

Wireless Network Cards:

Wireless network cards or Wireless network adapters (wireless NICs) are cards that locate and communicate to an access point with a powerful signal, giving users network access. It is required of each device to connect to the wireless network. Laptops or desktop computers generally have built-in wireless NICs or have slots to attach them.

These include two types of plug-in cards; one is called a PCMCIA and the other is a PCI. Laptops have slots to insert the PCMCIA plug-in cards, whereas desktop computers have internal slots to add PCI cards. The functionality of a wired network card and a wireless network card is similar to each other.

Wireless Modem: A wireless modem is a device that allows PCs to connect to a wireless network and access the

Internet connection directly with the help of an Internet Service Provider (ISP). They receive and transmit network signals to other units without a physical cable. Wi-Fi routers have the capacity to transmit an Internet service up to a confined range; whereas, wireless modems can be used in almost any place where a mobile phone is present. Portable devices (such as laptops, mobile phones, PDAs etc.) use wireless modems to receive signals over the air like a cellular network. There are various types of wireless modems. Users can choose a wireless modem based on their needs. Common types of wireless modems include:

Cards: Oldest form of wireless connection. Two types of cards are data cards and connect cards, which are available from mobile providers and used by laptops, PCs, and routers. They are small and easy to use.

USB Sticks: Quickly connects to the Internet with a wireless modem. They resemble a USB flash drive and fit easily into the USB port of a laptop. Computers require installation of special drivers and software to use them. They are portable.

- Mobile Hotspots
- Wireless Routers

The following features should be used for deciding on a wireless modem:

- Speed of the modem
- Protocols it can support such as Ethernet, GPRS, ISDN, EVDO, Wi-Fi, CPCD, etc.
- Frequency band: 900 MHz, 2.4 GHz, 23 GHz, 5 Hz, etc.
- Radio technique such as direct-sequence spread spectrum or frequency hopping
- Total number of channels for transmitting and receiving
- Maximum signal strength
- Full duplex or half-duplex capability

Wireless Bridge:

A wireless bridge connects multiple LANs at the MAC layer. These bridges separate networks either logically or physically. They cover longer distances than APs. Few wireless bridges support point-to-point connections to another AP and some support point-to-multipoint connections to several other APs. Wireless bridging helps connect two LAN segments through a wireless link. Two segments reside on the same subnet and look like two Ethernet switches connected with a cable to all computers within the subnet. Broadcasts reach all the machines on that subnet, allowing DHCP clients in one segment to obtain respective addresses from a DHCP server from a different

segment. A wireless bridge can be used to connect computers in one room to computers in another room without a cable.

Wireless Repeater (Range Expanders):

This device retransmits the existing signal captured from the wireless router or access point to create a new network. It works as an access point and station simultaneously. The clients who are too far away from the router or access point can integrate with the same wireless local-area network via a repeater. It means that it extends the signal by taking it from a wireless access point and transmits it to the uncovered area. These repeaters require an omni-directional antenna. It captures, boosts, and retransmits the signals.

Wireless Router:

A wireless router is a device in a wireless local-area network (WLAN) that interconnects two types of networks through radio waves to the wireless-enabled devices like computers, laptops, and tablets. It functions as a router in the LAN, but also provides mobility to users. Wireless routers have the ability to filter the network traffic based on the sender and receiver's IP address. A wireless router provides strong encryption, filters MAC addresses, and controls SSID authentication.

Wireless Gateways:

A wireless gateway is the key component of a wireless network. It is a device that allows Internet-enabled devices to access the connection. It combines the functions of wireless access points and routers. Wireless gateways have a feature like NAT, which translates the public IP into a private IP and DHCP.

Wireless USB Adapter:

A wireless USB adapter enables Internet access through a USB port on a computer. It also supports communication links and syncs between two or more devices. There are three main varieties of a wireless adapter:

- Cellular
- Bluetooth
- Wi-Fi

Antenna

An antenna is a device that is designed to transmit and receive electromagnetic waves that are called radio waves. An antenna is a collection of metal rods and wires that capture radio waves and translate them into electrical current. The size and shape of an antenna is designed according to the frequency of the signal they are designed to receive.

An antenna that gains high frequency is highly focused, while a low-gain antenna receives or transmits over a large angle.

A transducer translates radio frequency fields into AC current (and vice-versa).

Antennas Functions The antenna functions are:

Transmission line:

Antennas transmit or receive radio waves from one point to another. This power transmission takes place in free space through the natural media like air, water, and earth. Antennas avoid power that is transmitted through other means.

Radiator:

It radiates the energy powerfully. This radiated energy is transmitted through the medium. A radiator is always the size of half a wavelength.

Resonator:

The use of the resonator is necessary in broadband applications. Resonances that occur must be attenuated.

Antenna Characteristics

The characteristics of an antenna are:

- **Operating frequency band**: Antennas operate at a frequency band between 960 MHz and 1215 MHz.
- **Transmit power**: Antennas transmit power at a 1200-watt peak and a 140-watt average.
- **Typical gain**: Gain is the ratio of power input to the antenna to the power output from the antenna. It is measured in decibels (dBi). Gain is 3.0dBi.
- **Radiation pattern**: The radiation pattern of an antenna is in a 3-D plot. This pattern generally takes two forms of patterns: elevation and azimuth.
- **Directivity**: The directivity gain of an antenna is the calculation of radiated power in a particular direction. It is generally the ratio of radiation intensity in a given direction to the average radiation intensity.
- **Polarization**: It is the orientation of electromagnetic waves from the source. There are a number of polarizations like linear, vertical, horizontal, circular, Circular Left Hand (LHCP), and Circular Right Hand (RHCP).

There are five types of wireless antennas:

Directional Antenna: A directional antenna can broadcast and receive radio waves from a single direction. In order to improve the transmission and reception, the directional antenna is designed to work effectively in a specified direction. This also helps in reducing interference.

Omni-directional Antenna:

Omni-directional antennas radiate electromagnetic energy in all directions. They usually radiate strong waves uniformly in two dimensions, but not as strongly in the third. These antennas are efficient in areas where wireless stations use time-division multiple access technology. A good example of an omni-directional antenna is the one used by radio stations. These antennas are effective for radio signal transmissions because the

receiver may not be stationary. Therefore, a radio can receive a signal regardless of where it is.

Advantages:

Omni-directional can deal with signals from any direction.

Disadvantages:

The distance covered by omni-directional antennas may be wasted because of the interference of walls and other obstacles. It is difficult for an omni-directional antenna to work in an internal environment.

Parabolic Grid Antenna:

A parabolic grid antenna relies on the principle of a satellite dish, but it does not have a solid backing. Instead of a solid backing, this kind of antenna has a semi-dish formed by a grid made of aluminum wire. These grid parabolic antennas can achieve long-distance Wi-Fi transmissions by making use of the principle of a highly focused radio beam. This type of antenna can transmit weak radio signals millions of miles back to earth.

Advantages:

The parabolic grid antenna is wind resistant.

Disadvantages:

A parabolic grid antenna is expensive, as it requires a feed system for reflecting the radio signals.

Along with the feed system, the antenna requires a reflector as well. The assembling of these components makes the installation time consuming.

Yagi Antenna:

A Yagi antenna is a uni-directional antenna commonly used in communications for a frequency band of 10 MHz to VHF and UHF. The main objectives of this antenna is to improve the gain of the antenna and reduce the noise level of a radio signal. It not only has an uni-directional radiation and response pattern, but also concentrates the radiation end-fire radiation pattern. The other name for a Yagi antenna is a Yagi Uda antenna.

Advantages:

A Yagi antenna includes good range and ease of aiming the antenna.

The Yagi antenna is directional, focusing the entire signal in a cardinal direction. This results in high throughput.

The installation and assembly of the antenna is easy and less time consuming compared with other antennas.

Disadvantages:

The antenna is very large, especially for high gain levels.

Dipole Antenna:

A dipole is a straight electrical conductor measuring half a wavelength from end to end and connected to the RF feed line's center. The other name for a dipole antenna is a "doublet." It is bilaterally symmetrical, so it is inherently a balanced antenna. Usually, a balanced parallel-wire RF transmission line serves this kind of antenna.

Advantages:

A dipole antenna offers balanced signals. With the two-pole design, the device receives signals from a variety of frequencies.

Disadvantages:

Although the indoor dipole antenna might be small, the outdoor dipole can be much larger, making it difficult to manage.

To get the perfect frequency, antennas are required to undergo multiple combinations. This can be a hassle, especially in the case of outdoor antennas.

Reflector Antennas:

Reflector antennas are used to concentrate EM energy that is radiated or received at a focal point. These reflectors are generally parabolic.

Advantages:

If the surface of the parabolic antenna is within the tolerance limit, it can be used as a primary mirror for all the frequencies. This can prevent interference while communicating with other satellites.

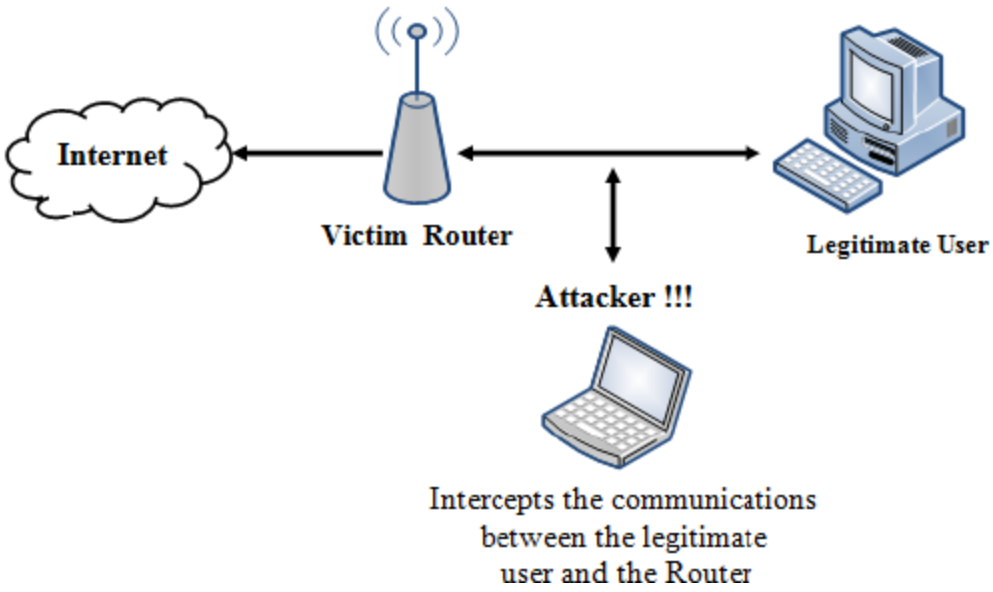
The larger the antenna reflector in terms of wavelengths, the higher the gain.

Disadvantage:

Reflector antennas reflect radio signals; the manufacturing cost of the antenna is high.

WEP (Wired Equivalent Privacy) Encryption

The 802.11 MAC implementation specifies a protocol called Wired Equivalent Privacy (WEP). The objective of WEP is to make WLAN communication as trustworthy as a wired LAN communication. WEP presents two vital segments to the architecture of wireless security. They are the validation of data and the secrecy of the data. WEP uses a mechanism in which a key is used in common with a cipher that is symmetric (called RC4).



A 24-bit arbitrary number known as the Initialization Vector (IV) is added to the WEP key. The WEP key and the IV together are called a WEP seed. The 64, 128, and 256-bit WEP versions use 40, 104, and 232-bit keys, respectively. The WEP seed is used as the input for the RC4 algorithm to generate a keystream (the keystream is bit-wise XORed with the combination of data and ICV to produce the encrypted data). The CRC-32 checksum is used to calculate a 32-bit Integrity Check Value (ICV) for the data, which, in turn, is added to the data frame. The IV field (IV+PAD+KID) is added to the cipher-text to generate a MAC frame.

A standard 64-bit WEP is used as a string of 10 Hexadecimal (Base 16) characters (0-9) (A-F). Each character has 4 bits; 10 digits of 4 bits is 10 * 4, which is 40 bits (WEP-40). Now the 40-bit keys are attached to another 24-bit Initialization Vector (IV), which completes the 64-bit WEP (4 * 10 = 40 bits + 24-bit IV = 64 bits) key.

Another WEP standard used is the 128-bit WEP that uses a 104-bit key. The 128-bit key is entered as a 26 Hexadecimal character. Here, 26 digits * 4 bits = a 104-bit key. Again, adding a 24-bit IV gives 104 bits + 24 bits = a 128-bit WEP key. Similarly, 152-bit and 256-bit WEP is available that uses a 128-bit and a 232-bit key, respectively. Now, adding the 24-bit IV to 128-bit key and 232-bit key provides the 152-bit and 256-bit WEP. How WEP works when using RC4:

- Packets to be transmitted are passed through an integrity check algorithm in order to generate a checksum (checksums avoid changing the message).
- The 24-bit Initialization Vector (IV) together with a 40-bit WEP key produces the 64-bit key.
- RC4 uses this key to generate the keystream. The keystream should have the same length as the plain-text or original message with the checksum included.
- The keystream is XORed with the original message or the plain-text along with a checksum. This generates a cipher-text or an encrypted packet.

- The client, on the other hand, receives the encrypted text and XORes it with the same keystream to generate the plain-text or original message. The client validates the checksum in order to authenticate the message

WEP Issues

WEP has the following issues:

1. CRC32 is not sufficient to ensure complete cryptographic integrity of a packet:

By capturing two packets, an attacker can reliably flip a bit in the encrypted stream and modify the checksum so that the packet is accepted.

2. IVs are 24 bits:

An AP broadcasting 1500-byte packets at 11 Mb/s would exhaust the entire IV space in five hours.

3. Known plain-text attacks:

When there is an IV collision, it becomes possible to reconstruct the RC4 keystream based on the IV and the decrypted payload of the packet.

4. Dictionary attacks:

WEP is based on a password.

The small space of the initialization vector allows the attacker to create a decryption table, which is a dictionary attack.

5. Denial of service:

Associate and disassociate messages are not authenticated.

6. Eventually, an attacker can construct a decryption table of reconstructed keystreams:

With about 24 GB of space, an attacker can use this table to decrypt WEP packets in real time.

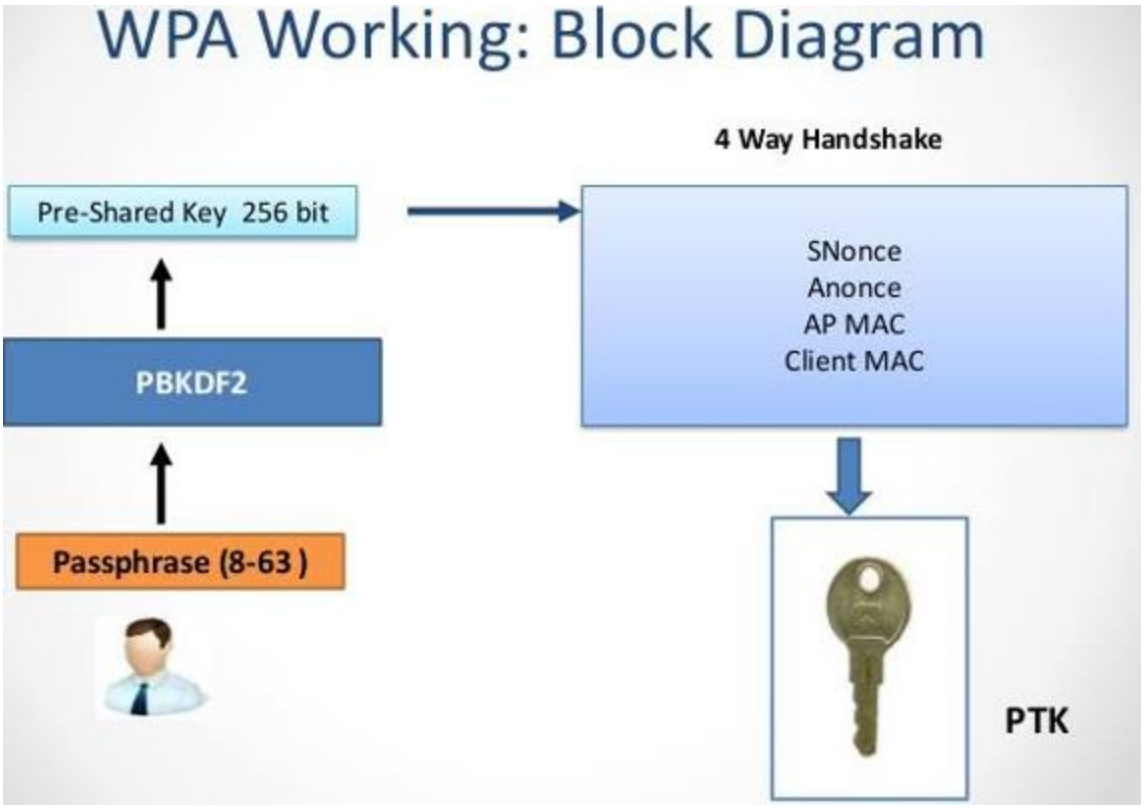
7. A lack of centralized key management makes it difficult to change WEP keys with any regularity.

8. IV is a value that is used to randomize the keystream value and each packet has an IV value:

The standard allows only 24 bits, which can be used within hours at a busy AP.

WPA (Wi-Fi Protected Access) Encryption

Wi-Fi Protected Access (WPA) is used as a security standard for Wi-Fi connections. WPA provides refined data encryption and user authentication techniques. WPA uses TKIP for data encryption and TKIP eliminates the weaknesses of WEP by including per-packet mixing functions, message integrity checks, extended initialization vectors, and re-keying mechanisms.



WEP normally uses a 40-bit or a 140-bit encryption key, whereas TKIP uses 128-bit keys for each packet. The message integrity check for WPA avoids the chances of the attacker changing or resending the packets. TKIP uses a Michael Integrity-Check algorithm with a message-integrity check key to generate the MIC value. The temporal encryption key, transmit address, and TKIP sequence counter (TSC) are used as inputs for the RC4 algorithm to generate a keystream. A MAC Service Data Unit (MSDU) and message integrity check (MIC) are combined using the Michael algorithm. The combination of the MSDU and the MIC is fragmented to generate the MAC Protocol Data Unit (MPDU). A 32-bit ICV is calculated for the MPDU; the combination of the MPDU and the ICV is then bitwise XORed with the keystream to produce the encrypted data. The IV is added to the encrypted data to generate the MAC frame. WPA requires 802.1X authentication and changes the unicast and global encryption keys. TKIP is used in an unicast encryption key, which changes the key for every packet—thereby enhancing the security. This change in the key for each packet is coordinated between the client and the access point. In a global encryption key, the access points advertise the change in the key to the connected wireless clients.

Temporal Key Integrity Protocol (TKIP)

TKIP is comprised of three main elements that increase encryption:

- A key integration function for individual packets.
- An enhanced Message Integrity Code (MIC) function named Michael.
- An improved IV, including sequencing guidelines.

TKIP is a short-term fix for WEP, organized as a simple software/firmware upgrade. A number of design weaknesses are made in order to sustain reverse compliance with the large number of existing hardware in the field. TKIP detects all of the identified weaknesses linked with WEP.

Types of WPA

1. **WPA-Personal**: This version makes the use of setup passwords and protects unauthorized network access.

2. **WPA-Enterprise**: It confirms the network user through a server. Features of WPA

WPA Authentication: WPA needs 802.1X authentications. WPA makes the use of a pre-shared key for the environment without the Remote Authentication Dial-In Use Service (RADIUS) infrastructure and uses the Extensible Authentication Protocol (EAP) and RADIUS for environments with a RADIUS infrastructure.

WPA Key Management: It is necessary to change both the unicast and global encryption keys while using WPA. The temporal key integrity protocol (TKIP) keeps changing the key for every frame when using an unicast key. In the case of a global key, WPA enforces the wireless access point to report the changed key to the connected wireless clients.

WPA2 Encryption

WPA2 depends on IEE 802.11i standards for data encryption and has replaced WPA technology in 2006. This protocol provides greater protection compared to WPA and WEP. It uses Advanced Encryption Standard (AES) to encrypt the data over wireless networks and supports for the CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) encryption mechanism. There are two modes of authentication in WPA2:

WPA2-Personal: Mostly used in home networks. It supports homes or locations where authentication servers are not used. Each wireless device uses the same 256-bit key generated from a password to authenticate with the AP. The router uses the combination of a passphrase, a network SSID, and a TKIP to generate a unique encryption key for each wireless client. These encryption keys keep changing constantly.

WPA2-Enterprise: Mostly used for securing wireless networks in organizations. It supports networks that include authentication servers. It uses EAP or RADIUS for centralized client authentication using multiple authentication methods—such as token cards, Kerberos, certificates, etc. WPA-Enterprise assigns a unique ciphered key to every system and hides it from the user in order to provide additional security and to prevent the sharing of keys.

How WPA2 Works

During a CCMP implementation, additional authentication data (AAD) is generated using a MAC header and is included in the encryption process that uses both AES and CCMP encryptions. Because of this, it protects the non-encrypted portion of the frame from alteration or distortion. The protocol uses a sequenced packet number (PN) and a

portion of the MAC header to generate a nonce that it used in the encryption process. The protocol provides plain-text data, temporal keys, AAD, and nonces as input to the encryption process that uses both AES and CCMP algorithms. A PN is included in the CCMP header to protect against replay attacks. The results from the AES and the CCMP algorithms produce encrypted text and an encrypted MIC value. Finally, the assembled MAC header, CCMP header, encrypted data, and encrypted MIC forms the WPA2 MAC frame. The following diagram depicts the functions of WPA2.

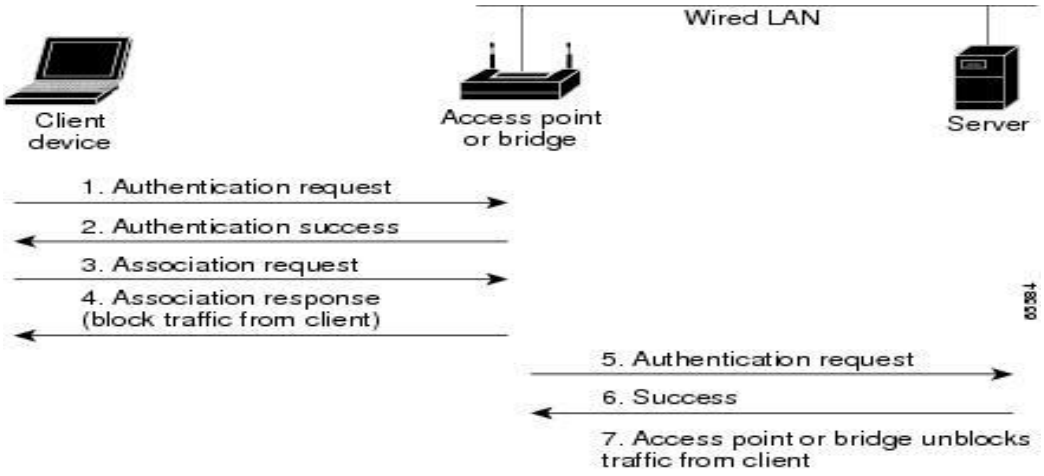
WEP vs. WPA vs. WPA2

WEP initially provided data confidentiality on wireless networks, but it was weak and failed to meet any of its security goals. WPA fixes most of WEP's problems. WPA2 makes wireless networks almost as secure as wired networks. WPA2 supports authentication, so that only authorized users can access the network. WEP should be replaced with either WPA or WPA2 in order to secure a Wi-Fi network.

	WEP	WPA	WPA2	WPA3
Brief description	Ensure wired-like privacy in wireless	Based on 802.11i without requirement for new hardware	All mandatory 802.11i features and a new hardware	Announced by Wi-Fi Alliance
Encryption	RC4	TKIP + RC4	CCMP/AES	GCMP-256
Authentication	WEP-Open WEP-Shared	WPA-PSK WPA-Enterprise	WPA2-Personal WPA2-Enterprise	WPA3-Personal WPA3-Enterprise
Data integrity	CRC-32	MIC algorithm	Cipher Block Chaining Message Authentication Code (based on AES)	256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)
Key management	none	4-way handshake	4-way handshake	Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA)

Both WPA and WPA2 incorporate protections against forgery and replay attacks. The previous page provides a comparison between WEP, WPA, and WPA2 with respect to the encryption algorithm used, size of the encryption key, and the initialization vector (IV) it produces.

Wi-Fi Authentication Methods



Open System Authentication

In the open-system authentication process, any wireless client that wants to access a Wi-Fi network sends a request to the wireless AP for authentication. In this process, the station sends an authentication management frame containing the identity of the sending station for authentication and connection with the other wireless stations. The AP then returns an authentication frame to confirm access to the requested station and completes the authentication process.

Open system authentication is a null authentication algorithm that does not verify whether it is a user or a machine. It uses clear-text transmission to allow the device to associate with an AP. In the absence of encryption, the device can use the SSID of an available WLAN to gain access to the wireless network. The enabled WEP key on the access point acts as an access control to enter the network. Any user entering the wrong WEP key cannot transmit messages via the AP even though the authentication is successful. The device can only transmit the messages when its WEP key matches with the WEP key of the access point. This authentication mechanism does not depend on a RADIUS server on the network.

Shared Key Authentication

In this process, each wireless station receives a shared secret key over a secure channel that is distinct from the 802.11 wireless network communication channels. The following steps illustrate the establishment of a connection in the shared-key authentication process:

- The station sends an authentication frame to the AP. The AP sends the challenge text to the station.
- The station encrypts the challenge text by making use of its configured 64-bit or 128-bit key and it sends the encrypted text to the AP.
- The AP uses its configured WEP key to decrypt the encrypted text. The AP compares the decrypted text with the original challenge text. If the decrypted text matches the original challenge text, the AP authenticates the station.
- The station connects to the network.

The AP can reject the station if the decrypted text does not match the original challenge text, and then the station will be unable to communicate with either the Ethernet network or 802.11 network.

Wi-Fi Authentication Process Using a Centralized Authentication Server

The 802.1X standard provides centralized authentication. For 802.1X authentication to work on a wireless network, the AP must be able to securely identify the traffic from a specific wireless client. In this Wi-Fi authentication process, a centralized authentication server known as Remote Authentication Dial in User Service (RADIUS) sends authentication keys to both the AP and the clients that want to authenticate with the AP. This key enables the AP to identify a particular wireless client.

Wireless Network Threats

Wireless proves to be an advanced networking option for Internet users. However, wireless networks may pose various security risks that can affect the function of the entire network. The wireless network can be at risk to various types of attacks, including access control attacks, integrity attacks, confidentiality attacks, availability attacks, authentication attacks, etc.

Wardriving

In a wardriving attack, wireless LANS are detected either by sending probe requests over a connection or by listening to web beacons. An attacker who discovers a penetration point can launch further attacks on the LAN. Some of the tools that the attacker may use to perform wardriving attacks are KisMAC, NetStumbler, and WaveStumber.

Rogue Access Point Attack

In order to create a backdoor into a trusted network, an attacker may install an insecure AP or fake AP inside a firewall. The attacker may also use a software or hardware AP to perform this kind of attack. A wireless access point is called a rogue access point when it is installed on a trusted network without authorization. An inside or outside attacker can install rogue access points on your trusted network for malicious intention.

Types of Rogue Access Points:

1. Wireless router connected via the “trusted” interface
2. Wireless router connected via the “untrusted” interface
3. Installing a wireless card into a device already on the trusted LAN
4. Enabling wireless on a device already on the trusted LAN

Misconfigured Access Point Attack

This is an internal threat that arises when a networking device is misconfigured. A misconfigured networking device acts as an open gateway for data theft. If users improperly configure any of the critical security settings at any of the APs, the entire

network could be open to attack. If the networking devices are managed centrally, it could go unnoticed.

Ad-Hoc Connection Attack

An attacker may carry out this kind of attack by using any USB adapter or wireless card. The attacker connects the host to an unsecure client to attack a specific client or to avoid AP security.

AP MAC Spoofing

Using the MAC spoofing technique, an attacker can reconfigure a MAC address to appear as an authorized AP to a host on a trusted network. Tools for carrying out this kind of attack include changemac.sh, SMAC, and Wicontrol.

Denial of Service (DoS)

In a DoS attack, an attacker floods a victim system with non-legitimate service requests or traffic to overload its resources.

WEP Cracking

It involves capturing data to recover a WEP key using a brute-force attack or Fluhrer-Mantin-Shamir (FMS) cryptanalysis.

WPA-PSK Cracking

Attackers use various sniffing tools like packet analyzers to sniff for authentication packets in the network. With the brute-force method, the attacker can crack the WPA-PSK key.

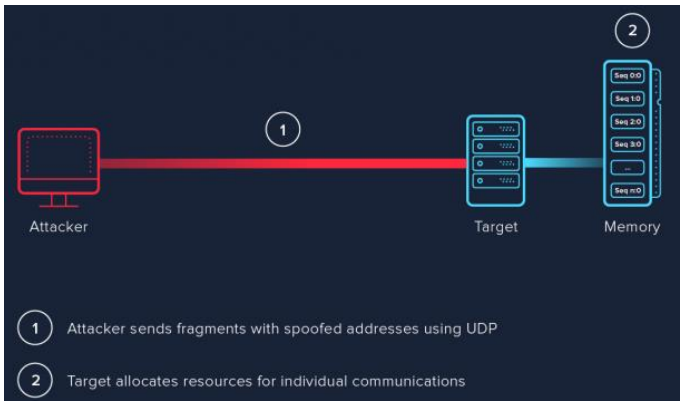
Man-in-the-Middle Attack

In a MITM attack, the attacker runs traditional MITM attack tools on an evil twin AP to intercept TCP sessions or SSL/SSH tunnels.

RADIUS Replay

It involves capturing RADIUS Access-Accept or Reject messages for later replay. In this type of attack, the attacker maliciously repeats the valid data.

Fragmentation Attack



A fragmentation attack is the process of breaking up a single packet into multiple packets of a much smaller size. Fragmentation attacks can be performed through:

1. **Ping of Death**: It is a denial-of-service attack that utilizes the ping utility for creating an IP packet. It uses fragmented ICMP packets that upon reaching the destination exceed the allowable size of an IP datagram.

2. **Tiny Fragment Attack**: Small fragments are used to gather the TCP header information. This attack targets the filtering rules set on the networking device.

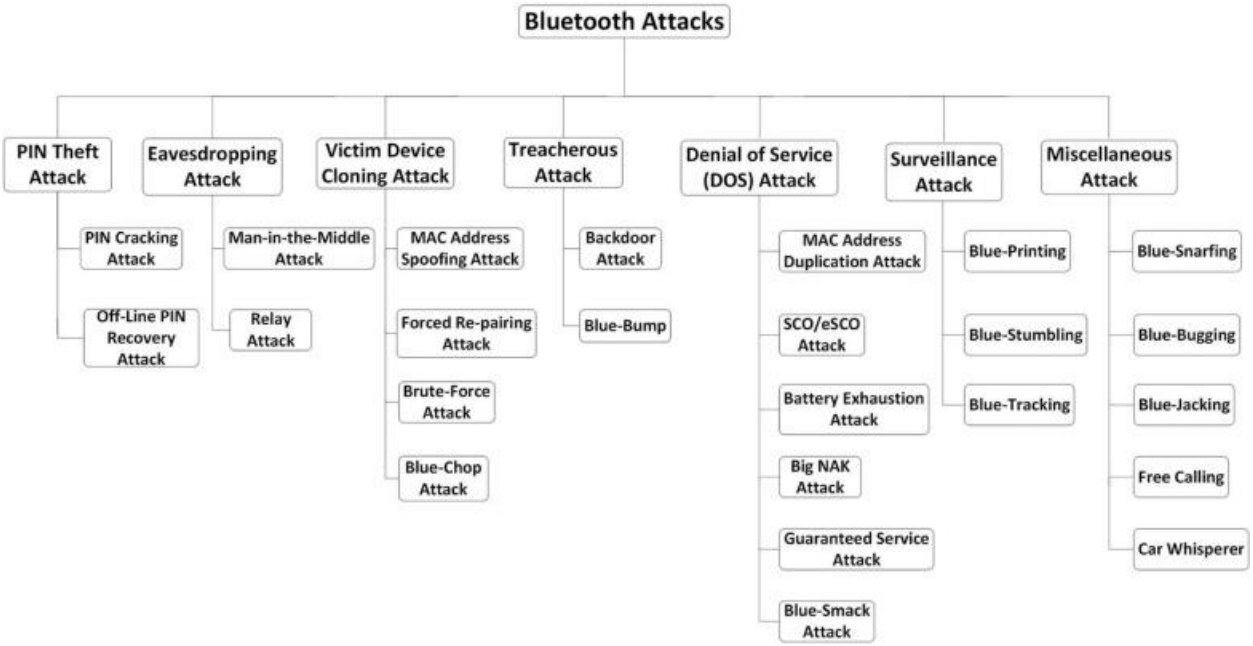
3. **Teardrop Attack**: It causes the target machine to reboot or shutdown. The attack occurs on the IP protocol, which utilizes the offset fields of a UDP packet.

ARP Poisoning Attack

In this spoofing attack, the attacker first spoofs the MAC address of the victim's wireless laptop and attempts to authenticate to AP1 using the Cain & Abel ARP poisoning tool, which is a password-recovery tool for Windows. AP1 sends the updated MAC address information to the network routers and switches, which, in turn, updates their routing and switching tables. The system does not send traffic now destined from the network backbone to the victim's system to AP2, but instead sends it to AP1.

Bluetooth Threats

Similar to wireless networks, Bluetooth devices are also at risk of compromise from various threats. Attackers target the vulnerabilities in security configurations of Bluetooth devices to gain access to confidential information and the network to which they are connected.



Here are a few of the common threats to Bluetooth:

1. **Leaking Calendars and Address Books**: Once the attacker gets access to information such as the user's address book, calendars, photos, or personal messages, it can be stolen, changed, and used in malicious way.

2. **Remote Control**: Attackers can gain access to the target phone and make changes to the settings. The affected device can be used to send bulk random messages or make phone calls.

3. **Bugging Device:** Attackers can program the device to perform random activities without the user's consent. An attacker can eavesdrop on the user's conversation, converting the user's device into a bugging device.

4. **Social Engineering**: Attackers can perform social engineering through the user's phone to steal sensitive information from the intended victim.

5. **Sending SMS Messages**: Attackers can send messages with false bomb threats through a user's mobile phone.

6. **Malicious Code**: An attacker can use Bluetooth-specific malicious code to infect a user's device or gain access to the user's phone.

7. **Causing Financial Losses**: With the user's phone, an attacker can send a large number of MMS messages, which is expensive for large files (especially for international communication).

8. **Protocol Vulnerabilities**: Attackers can exploit vulnerabilities that already exist in the core Bluetooth protocol of the devices, making it vulnerable to various types of attacks.

Wireless Network Security

An attacker can easily compromise a wireless network if proper security measures are not applied or if there is not an appropriate network configuration. Lack of adequate knowledge and skills can pose a large risk to the wireless network.

Besides wireless network policies, administrators need to apply various security measures and tricks to ensure the security of their wireless network from various types of attacks. The administrator needs to focus on an appropriate use of security controls and their effective configuration to defend their networks.

The following points should be clearly stated in the organization's wireless security policy.

- Identify the users who are using the network.
- Determine whether the user is allowed to access it or not.
- Clearly define who can and cannot install the access points and other wireless devices in the enterprise.
- Describe the information type that users are allowed to communicate over the wireless link.
- Provide limitations on access points (such as location, cell size, frequency, etc.) in order to overcome wireless security risks.
- Clearly define the standard security setting for wireless components.
- Describe conditions where wireless devices are allowed to use the network.

Furthermore, a successful and effective wireless security implementation should involve the following:

- Centralized implementation of security measures for all wireless technology.
- Security awareness and training programs for all employees.
- Standardized configurations to reflect security policies and procedures.
- Configuration management and control to make sure the latest security patches and features are available on wireless devices.

The following activities help administrators defend and maintain the security of the wireless network.

- Creating an inventory of the wireless devices
- Placement of the wireless AP and antenna
- Disable SSID broadcasting
- Selecting a stronger wireless encryption mode
- Implementing MAC address filtering
- Monitoring wireless network traffic
- Defending against WPA cracking
- Detecting rogue access points
- Locating rogue access points
- Protecting from denial-of-service attacks
- Assessing the wireless network security
- Deploying Wireless IDS (WIDS) and Wireless IPS (WIPS)
- Configuring security on wireless routers

Creating an Inventory of the Wireless Devices

Use of wireless devices in organizations continues to grow. Therefore, it becomes increasingly important for organizations to track and manage their wireless assets for security purposes. Maintaining an accurate and up-to-date inventory of wireless devices is required for proper security. Network device inventory helps administrators consolidate all the updated network data and devices. The inventory can help administrators quickly identify any non-functioning devices, as well as any rogue network devices that are present on the network. A list of those devices that are not connected to the network should also be added to the list. This helps detect unknown devices in the network. Regular scanning of the inventory is important. Through scanning, administrators can determine the rogue network devices, problem devices, potential vulnerabilities, and which devices need a patch/update in the network. A network is only as secure as its weakest link. Administrators should maintain information about all the devices regardless of their configuration settings or the vendor. An administrator should maintain the inventory either manually or with the help of an effective inventory tracking solution. At times, an inventory tool may not auto-update the network device. In such scenarios, administrators are required to add the device in the inventory list.

Placement of a Wireless AP and Antenna

The appropriate location of APs is important, as it plays a vital role in achieving a high network performance, coverage, and speed. Many organizations have their APs placed across their interior spaces. Every AP requires installation at a specific location and

angle. Installation of APs at random locations will restrict the network performance. Plan the coverage area wisely. Overlap is good. Be careful to not create dead zones.

Placement of a Wireless Antenna: Placement of an antenna depends on the type, angle, location of the AP, and the coverage required.

Guidelines for the placement of a wireless antenna:

- A wireless device should be placed in the center of a room with proper positioning of the antennas. The antennas should be positioned vertically, especially in a spacious interior.
- Use third-party applications to help find the best location for placing the device. Applications like HeatMapper build a map of the interior and according to the map designed, it provides a guide that helps place the device in the best location.
- Choose an appropriate band and channel for the wireless antenna to work on. A reliable frequency starts from 2.4 GHz. Establish a frequency that is compatible with the wireless device and can travel through walls. To analyze an appropriate channel use applications like Wi-Fi Analyzer.
- Replace the wireless antenna to get better networking results. Set up omni-directional antennas that will help improve the range of the wireless environment.

Disable SSID Broadcasting

The SSID is the character sequence or code that is attached to each packet in a wireless network. This is used to identify the packet that is covered in a particular network when there are a number of networks present. The code can contain a maximum of 32 alphanumeric characters. All wireless devices that communicate with each other have the same SSID. A SSID is used to uniquely identify a set of wireless network devices that work in the given service set. A wireless network SSID can be either broadcast or hidden. By broadcasting a SSID, anyone can find it and access it. If the SSID is hidden, the user has to know the exact SSID in order to connect to the wireless network. Network administrators should always disable SSID broadcasting on their devices.

SSID broadcast, if enabled

By enabling the SSID broadcast, the wireless router will broadcast its presence and its name. When scanning for available wireless connections, if the SSID is broadcast, the network name and presence will be identified. It may be locked with a password, but anyone will be able to see it.

SSID broadcast, if disabled

If the SSID broadcast is disabled, then the wireless router will broadcast its presence, but will not display the name. It displays as an “unnamed network” connection present within your range. The user can connect to the wireless setup after naming it and providing it with the correct authentication credentials.

Selecting a Stronger Wireless Encryption Mode

Administrators should use a strong wireless encryption mode to keep their wireless network safe from various types of attacks. Various encryption modes can be used for the organization's wireless network. Order of preference for choosing encryption modes:

1. WPA2-Enterprise with RADIUS
2. WPA2-Enterprise
3. WPA2-PSK
4. WPA-Enterprise
5. WPA
6. WEP

Order of preference for choosing Wi-Fi security methods:

1. WPA2 + AES
2. WPA + AES
3. WPA + TKIP/AES
4. WPA + TKIP
5. WEP
6. Open Network (no security at all)

Monitoring Wireless Network Traffic

Wireless network traffic analysis helps identify intrusion attempts on the wireless network. Administrators are required to monitor the traffic of a wireless network in order to find any abnormalities or signs of an attack. Just like a wired network, the network traffic on a wireless network can be monitored using packet-sniffing utilities such as Wireshark. Select the wireless network interface corresponding to the wireless router and start sniffing the traffic on it. Look for the traffic based on 802.11 standard wireless protocols denoting wireless network traffic. Apply various filters to filter out the traffic, which is required for a particular analysis.

Defending Against WPA Cracking

Passphrases:

The only way to crack WPA is to sniff the password PMK associated with the "handshake" authentication process; and if this password is extremely complicated, it might be almost impossible to crack

Passphrase Complexity:

Select a random passphrase that is not made up of dictionary words

Select a complex passphrase that contains a minimum of 20 characters and change the passphrase at regular intervals

Client Settings:

Use WPA2 with AES/CCMP encryption only

Properly set the client settings (e.g., validate the server, specify server address, don't prompt for new servers, etc.)

Additional Controls:

Use a virtual private network (VPN) such as a remote access VPN, Extranet VPN, Intranet VPN, etc.

Implement a Network Access Control (NAC) or Network Access Protection (NAP) solution for additional control over end-user connectivity

WPA-cracking defense recommendations:

- Construct a strong WPA password/key
- Do not use words from the dictionary
- Do not use words with numbers appended at the end
- Do not use double words or simple letter substitution (such as p@55w0rd)
- Do not use common sequences from your keyboard (such as qwerty)
- Do not use common numerical sequences
- Avoid using personal information in the key/password

WPA password should be constructed according to the following rules:

- Random
- At least 12 characters in length
- Contains at least one uppercase letter
- Contains at least one lowercase letter
- Contains at least one special character, such as @ or !
- Contains at least one number

Detecting Rogue Access Points

A wireless access point becomes a rogue access point when it is installed on a trusted network without authorization. An inside or outside attacker can install rogue access points on a trusted network with malicious intent.

Types of Rogue Access Points:

1. Wireless router connected via the "trusted" interface

2. Wireless router connected via the "untrusted" interface

3. Installing a wireless card into a device already on the trusted LAN

4. Enabling wireless on a device already on the trusted LAN

Use following methods to detect wireless networks in the vicinity of the network and compare the detected wireless access points with the wireless device inventory for the

environment. If an access point is found that is not listed in the inventory, it can generally be considered a rogue access point.

Wireless Scanning:

- Perform active wireless network scanning to detect the presence of wireless access points in the vicinity.
- It will help detect unauthorized or hidden wireless access points that can be malicious.
- Use wireless discovery tools such as inSSIDer, NetSurveyor, NetStumbler, Vistumbler, and Kismet to detect wireless networks.

Wired Network Scanning:

Use wired network scanners such as Nmap to identify a large number of devices on a network by sending specially crafted TCP packets to the device (Nmap-TCP fingerprinting).

It will help locate rogue access points attached to the wired network.

SNMP Polling:

Use Simple Network Management Protocol (SNMP) polling to identify IP devices attached to the wired network.

Use SNScan SNMP Detection Utility to identify SNMP-enabled devices on the network.

Wi-Fi Discovery Tools

Administrators can use the following Wi-Fi discovery tools for their wireless network scanning activity.

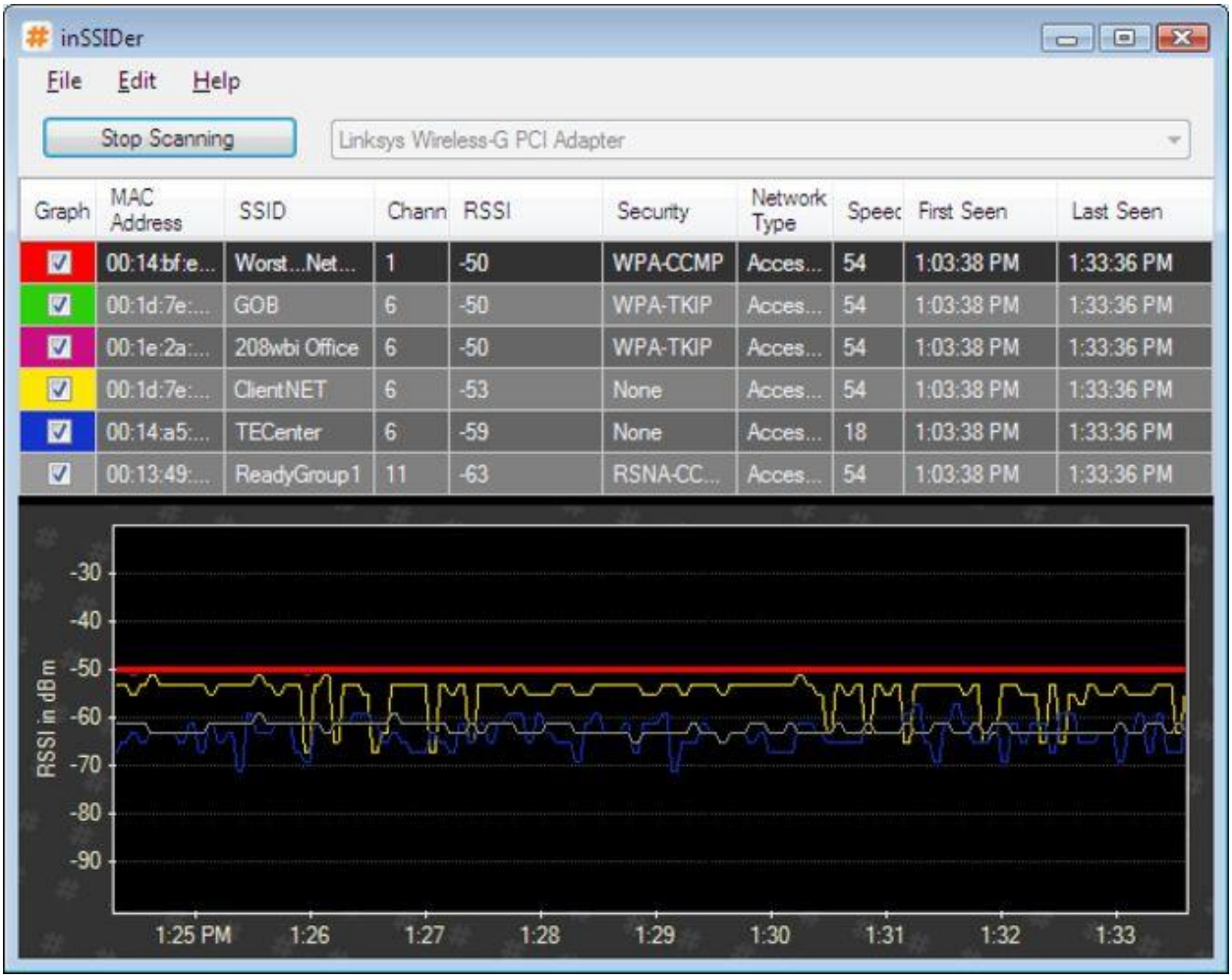
NetSurveyor

NetSurveyor is an 802.11 (Wi-Fi) network discovery tool that gathers information about nearby wireless APs in real time and displays it in useful ways. It displays the data using a variety of different diagnostic views and charts. It records and plays back the data. Features: Provides six graphical diagnostic views, generates reports in Adobe PDF format that include the list of APs and their properties along with images, and supports most wireless adapters installed with a NDIS 5.x driver or later.

InSSIDer

InSSIDer is an open-source, multi-platform Wi-Fi scanner software. It provides the user with information about the proper channeling of a wireless network, while offering the ability to check co-channel effects and overlapping networks. The application uses a native Wi-Fi API and the user's NIC and sorts the results by MAC address, SSID, channel, RSSI, MAC, vendor, data rate, signal strength and Time Last Seen. Features: Inspect WLAN and surrounding networks to troubleshoot competing APs, track the strength of the received signal in dBm over time, filter APs, highlight APs for areas with high Wi-Fi concentration, export Wi-Fi and GPS data to a KML file to view in Google

Earth, and shows which Wi-Fi network channels overlap and are compatible with GPS devices.



Vistumbler:

Vistumbler Features:

- Finds wireless access points
- Uses the Vista command “netsh wlan show networks mode=bssid” to get wireless information
- It supports GPS and live Google Earth tracking
- Export/import APs from Vistumbler TXT/VS1/VSZ or Netstumbler TXT/Text NS1
- Export AP GPS locations to a Google earth kml file or GPX (GPS eXchange format)
- Live Google Earth Tracking: auto KML shows APs in Google Earth
- Displays signal strength using sound files, Windows sound API, or MIDI

NetStumbler:

Facilitates detection of Wireless LANs using the 802.11b, 802.11a, and 802.11g WLAN standards. It is commonly used for wardriving, verifying network configurations, and finding locations with poor coverage in a WLAN.

NetStumbler uses:

- Wardriving
- Verifying network configurations
- Finding locations with poor coverage in a WLAN
- Detects causes of wireless interference
- Detects unauthorized (rogue) APs
- Aiming directional antennas for long-haul WLAN links

WirelessMon:

WirelessMon is a software tool that allows users to monitor the status of wireless Wi-Fi adapter(s) and gather information about nearby wireless APs and hot spots in real time. It can log the information it collects, while also providing comprehensive graphing of signal level and real-time IP and 802.11 Wi-Fi statistics.

Kismet:

Kismet is an 802.11 layer 2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless NIC that supports raw monitoring (rfmon) mode; it can sniff (with appropriate hardware) 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet also supports plug-ins, which allow sniffing other media such as DECT.

Wi-Fi Hopper:

Wi-Fi Hopper is a WLAN utility that performs Network Discovery and Site Survey. It includes a collection of network details, filters, RSSI graphing, as well as built-in GPS support for identification and advanced characterization of neighboring wireless devices. Wi-Fi Hopper can connect to unsecured, WEP, WPA-PSK, and WPA2-PSK networks directly from within the application.

Locating Rogue Access Points

Once a rogue access point is detected in the network, the next step is to trace its location in the organization. This can be done with AirCheck Wi-Fi Tester. It helps find the exact location of any wireless access point. It is a handheld wireless tester. The AirCheck Wi-Fi Tester must be carried to track the rogue access point. It detects the access point based on the signal strength.

AirCheck Wi-Fi Tester

Track down rogue and other APs by graphing the signal strength over time or by using an audible indication, which can be muted.

Protecting from Denial-of-Service Attacks: Interference Wireless networks are often susceptible to denial-of-service (DoS) attacks; as wireless networks have a shared medium of transmission. DoS attacks may be carried out in the various levels of the OSI

network layer. The DoS attack in the physical layer is carried out through signal jamming or intentional interference. Wireless networks use radio frequencies for communication; RF-spectrum analyzing tools can be helpful in detecting the radio frequency interference. They provide notification about excessive RF interference on the wireless network. There are various RF spectrum analyzers available:

AirMagnet Spectrum XT

AirMagnet Spectrum identifies the radio frequency interference affecting a wireless network's performance

Wi-Fi Surveyor

Wi-Fi Surveyor provides the following services:

- Displays the RF environment
- Monitors RF signals
- Troubleshoots RF issues
- Detects sources of RF interference

Wi-Fi surveyor helps detect the wireless devices and RF interference in the network that may affect the network's performance.

Ekahau Spectrum Analyzer

Ekahau is a device that assists in determining the devices causing the interference.

Accessing the Security of a Wireless Network

A wireless network should be regularly checked for possible vulnerabilities. Parameters such as security, performance, and speed should be considered while performing the assessment. This helps to ensure that the wireless network is adequately protected from attacks. Use various security assessment and vulnerability scanning tools to find the potential vulnerabilities.

Wi-Fi Security Auditing Tools: AirMagnet

Wi-Fi Analyzer AirMagnet Wi-Fi analyzer offers continuous evaluation of the wireless channels, devices, speeds, interference issues, and RF spectrum. It helps automatically detect security threats and wireless network vulnerabilities, common wireless performance issues including throughput issues, connectivity issues, device conflicts, and signal multi-path problems.

AirMagnet Wi-Fi Analyzer can detect Wi-Fi attacks such as DoS attacks, authentication/encryptions attacks, network penetration attacks, etc. It can easily locate unauthorized (rogue) devices or any policy violator. The tool examines 802.11a\b\g\n and 5GHz channels for interference and can be installed in PCs, laptops, or tablets in order to assess for interference issue

WPA Security Assessment Tool: Elcomsoft Wireless Security Auditor

Elcomsoft Wireless Security Auditor allows you to verify the security of a company's wireless network by executing an audit of accessible wireless networks. It comes with a built-in wireless network sniffer (with AirPcap adapters). It attempts to recover the original WPA/WPA2-PSK text passwords in order to test how secure the wireless environment is.

WPA Security Assessment Tools

WepAttack

WepAttack is a WLAN open-source Linux tool for breaking 802.11 WEP keys. This tool is based on an active dictionary attack that tests millions of words to find the right key.

Wesside-ng

Wesside-ng incorporates a number of techniques to seamlessly obtain a WEP key in minutes. It first identifies a network, and then proceeds to associate with it, obtain PRGA (pseudo random generation algorithm) XOR data, determine the network IP scheme, reinject ARP requests, and finally determine the WEP key.

Aircrack-ng

Aircrack-ng is a complete suite of tools to assess Wi-Fi network security. It focuses on different areas of Wi-Fi security:

Monitoring: Packet capture and export of data to text files for further processing by third-party tools.

Attacking: Replay attacks, de-authentication, fake access points, and others via packet injection.

Testing: Checking Wi-Fi cards and driver capabilities (capture and injection).

Cracking: WEP and WPA PSK (WPA 1 and 2).

WEPCrack

WEPCrack is an open-source tool for breaking 802.11 WEP secret keys. It cracks 802.11 WEP encryption keys using the latest discovered weakness of RC4 key scheduling.

WepDecrypt

WepDecrypt guesses WEP Keys based on an active dictionary attack, key generator, distributed network attack, and some other methods.

Portable Penetrator

With Portable Penetrator, you can recover Wi-Fi passwords in WEP, WPA, WPA2, and WPS PINs. It can reveal Wi-Fi passwords from access points for WEP, WPA, WPA2, and WPS encryption.

CloudCracker

It is an online password-cracking service that will help you in checking the security of WPA protected wireless networks, crack password hashes, or break document encryption.

Wi-Fi Vulnerability Scanning Tools

Wi-Fi vulnerability scanning tools determine the weaknesses in wireless networks and secures them before attackers actually attack. Wi-Fi vulnerability scanning tools include:

Zenmap

Zenmap is a multi-platform GUI for the Nmap Security Scanner, which is useful for scanning vulnerabilities on wireless networks. This tool saves the vulnerability scans as profiles to make them run repeatedly. The results of recent scans are stored in a searchable database.

Nessus

Nessus is a vulnerability, configuration, and compliance scanner. It features high-speed discovery, configuration auditing, asset profiling, malware detection, sensitive data discovery, patch management integration, and vulnerability analysis of a wireless network.

OSWA-Assistant

The Organizational Systems Wireless Auditor Assistant (OSWA-Assistant) is a wireless auditing toolkit. This toolkit can be used for wireless security/auditing to execute technical wireless security testing against a wireless infrastructure and clients.

WiFizoo

WiFizoo tool is intended to get all the possible info from open Wi-Fi networks (and possibly encrypted networks, at least with WEP) without joining any network and covering all Wi-Fi channels.

Network Security Toolkit

Network Security Toolkit (NST) is a Fedora-based application that provides easy access to open-source network security applications. The toolkit includes an advanced user interface for system/network administration, navigation, automation, network monitoring, host geolocation, network analysis, and configuration of many network and security applications found within the NST distribution.

Nexpose Community Edition

Nexpose is a vulnerability management application that analyzes vulnerabilities, controls, and configurations to find security risks. It uses RealContext, RealRisk, and the attacker's mindset to prioritize and drive risk reduction. This tool helps a user to understand the network, prioritize, and manage risks effectively.

Deploying a Wireless IDS (WIDS) and a Wireless IPS (WIPS)

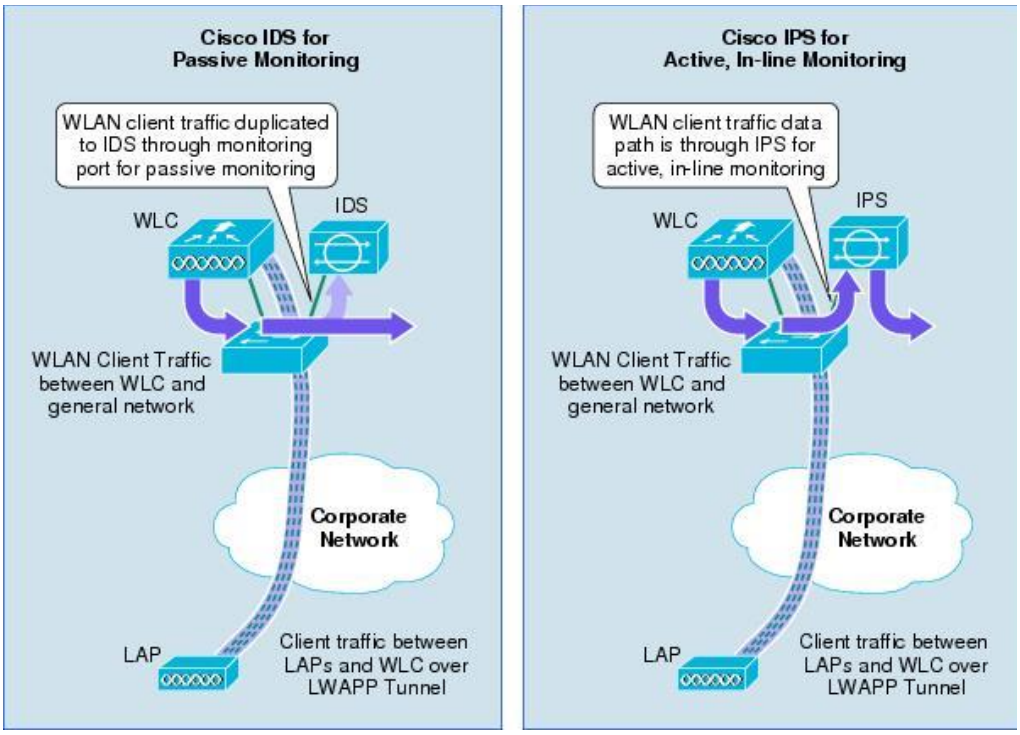
Wireless Intrusion Prevention System (WIPS)

A wireless intrusion prevention system (WIPS) is a network device that monitors the radio spectrum to detect access points (intrusion detection) without the host's permission in nearby locations. It can also implement countermeasures automatically. Wireless intrusion prevention systems protect networks against wireless threats and provide administrators with the ability to detect and prevent various network attacks.

Wireless Intrusion Detection System (WIDS)

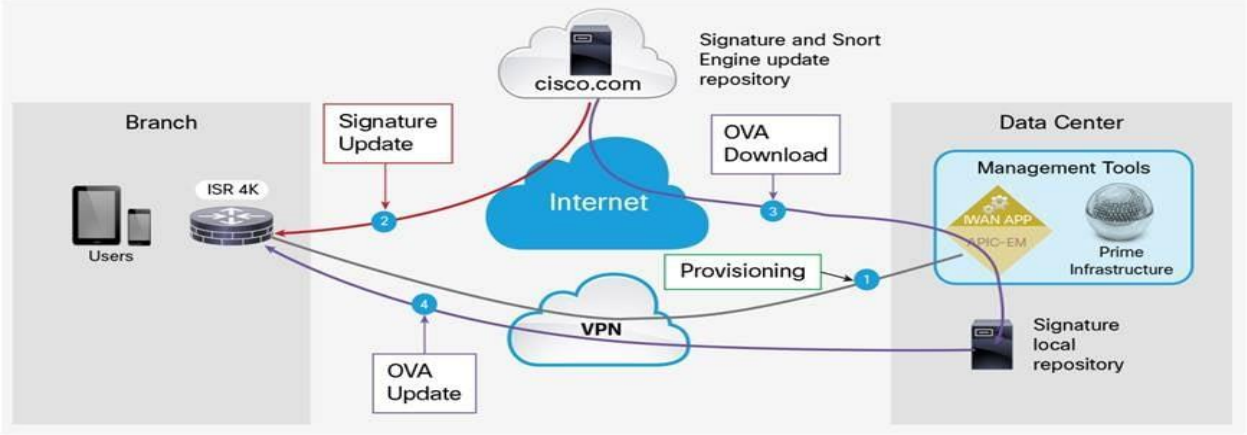
A wireless intrusion detection system (WIDS) is a tool that collects data about user activity. It monitors unauthorized network activity, policy violations, and known patterns of recognized wireless threats. It alerts the system administrator if it finds any anomalies in the network, rogue wireless APs, unencrypted traffic, etc. Wireless intrusion prevention systems (WIPS) provide additional features beyond a WIDS to prevent wireless threats. Consists of three components:

1. **Sensors**: Antennas or radios deployed to scan and capture packets.
2. **Servers**: Analyzes the captured packets.
3. **Console**: User interface for system admin to manage and report.



Typical Wireless IDS/IPS Deployment

A WIPS consists of a number of components working together to provide a unified security monitoring solution.



Component functions in a Cisco Wireless IPS deployment:

- **Access Points in Monitor Mode**: Provides constant channel scanning with attack detection and packet-capture capabilities.
- **Mobility Services Engine (running wireless IPS service)**: The central point of alarm aggregation from all controllers and their respective wireless IPS Monitor Mode access points. Alarm information and forensic files are stored on the system for archival purposes.
- **Local Mode Access Point(s):** Provides wireless service to clients in addition to time-sliced rogue and location scanning.
- **Wireless LAN Controller(s):** Forwards attack information from wireless IPS Monitor Mode access points to the MSE and distributes configuration parameters to APs.
- **Wireless Control System**: Provides the administrator with the means to configure the wireless IPS service on the MSE, push wireless IPS configurations to the controller, and set APs in wireless IPS Monitor Mode. It also allows the user to view wireless IPS alarms, forensics, reporting, and access the threat encyclopedia.

Configuring Security on Wireless Routers

To harden the wireless router, apply all the recommended security configurations on the wireless router. These security configuration settings will help minimize any wireless attacks and will provide the best performance, security, and reliability when using Wi-Fi. It should include:

1. Changing the default password of the wireless router.
2. Assigning a strong and complex password to the router
3. Choosing HTTPS for secure communication.
4. Disabling remote router access.
5. Enabling the firewall to block certain WAN requests.

6. Configuring an Internet Access policy.

7. Specifying the blocked services, URL, keywords, etc.

8. Disabling the DMZ option.

9. Configuring the Quality of Service (QoS) settings.

10. Avoid using the default IP ranges.

11. Keep the router firmware up to date.

Configuring Security on Wireless Routers

The following list contains the security measures and configurations an administrator should use for Wi-Fi security:

- Set the router access password and enable firewall protection.
- Do not use the SSID, company name, network name, or any easy-to-guess string in passphrases.
- Place a firewall or packet filter in between the AP and the corporate intranet.
- Limit the strength of the wireless network so that it cannot be detected outside the organization.
- Regularly check the wireless devices for configuration or setup problems.
- Implement a different technique for encrypting traffic, such as IPSEC over wireless.
- Disable the remote router login and administration.
- Regularly change the passphrases.
- Choose Wi-Fi Protected Access (WPA) instead of WEP.
- Implement WPA2-Enterprise wherever possible.
- Disable the network when not required.
- Log out of the router's web interface when not in use.
- Everything should be password-protected in order to avoid unauthorized access of the content in the system.
- The WEP keys should be changed often. It is recommended to use a very difficult key to avoid unauthorized access.
- The wireless access point should be password-protected.
- The MAC address-filtering technique should be used in a smaller network.
- Change the SSID value so only the user understands it.
- The access points should be kept in the middle of the building in order to avoid wardriving.
- Avoid the broadcasting of SSIDs, as they can become easy targets for the intruder to enter the network.
- Identify the physical location of the WLAN threat.
- Gather information about the source, destination IP address, ports, MAC address, login names/IDs, duration, and timestamps for analysis and investigation.

- Collect the connection logs can help to determine the unnecessary utilization of a wireless network in the organization.
- Monitor using WIDPS sensors and WLAN scanners to detect a rogue WLAN connection.
- Scan the locations within a close proximity to the organization.
- Monitor the security of the link passing information among the components in the network.
- Detect the laptops that are being illegitimately used as access points