Topic 9: Wireless Technologies

Wireless Technology

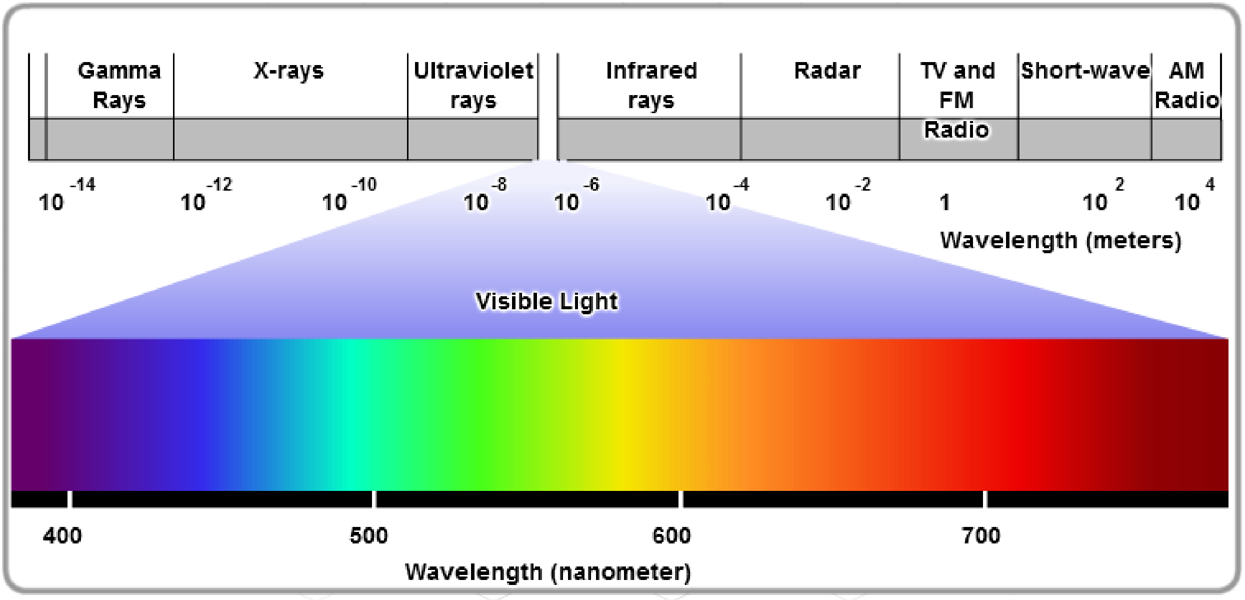
Wireless Technologies and Devices

In addition to the wired network, various technologies exist that allow the transmission of information between hosts without cables. These are known as wireless technologies.

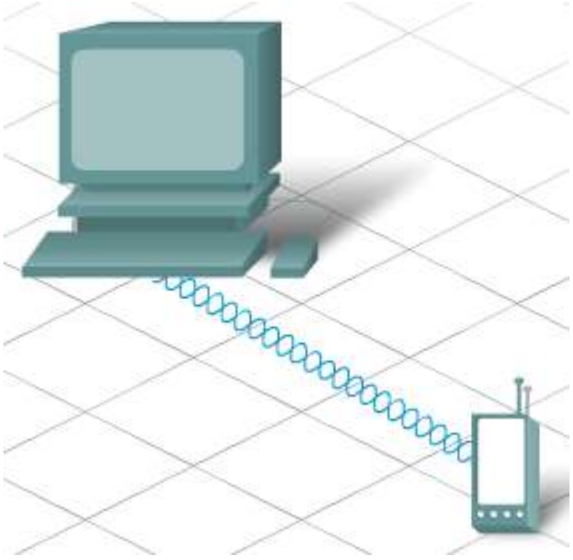
Wireless technologies use electromagnetic waves to carry information between devices. An electromagnetic wave is the same medium that carries radio signals through the air.

The electromagnetic spectrum includes such things as radio and television broadcast bands, visible light, x-rays and gamma-rays. Each of these has a specific range of wavelengths and associated energies as shown in the diagram.

Some types of electromagnetic waves are not suitable for carrying data. Other parts of the spectrum are regulated by governments and licensed to various organizations for specific applications. Certain areas of the spectrum have been set aside to allow public use without the restriction of having to apply for special permits. The most common wavelengths used for public wireless communications include the Infrared and part of the Radio Frequency (RF) band.



Infrared

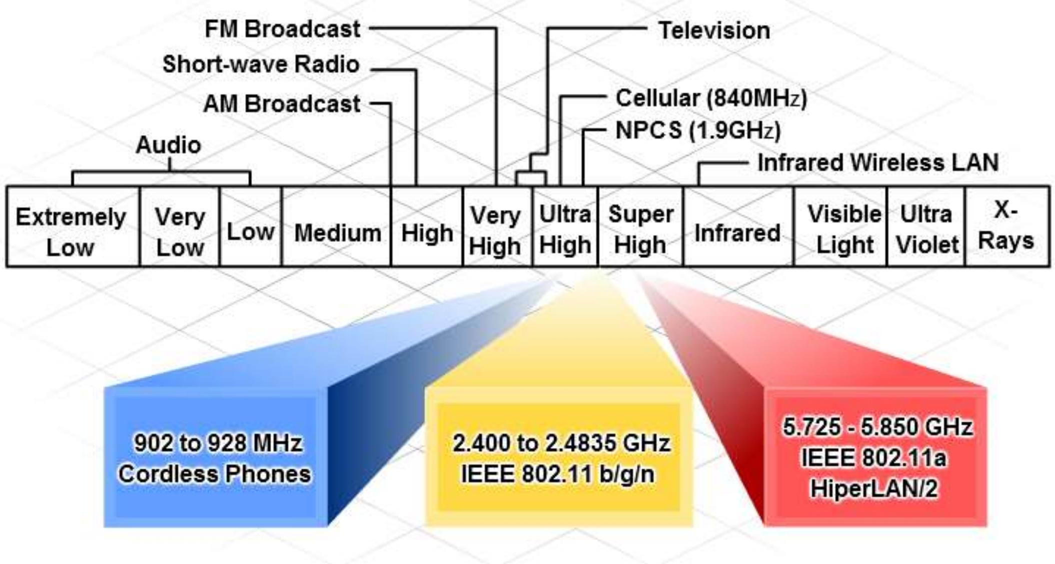


Infrared (IR) is relatively low energy and cannot penetrate through walls or other obstacles. However, It is commonly used to connect and move data between devices such as Personal Digital Assistants (PDAs) and PCs. A specialized communication port known as an Infrared Direct Access (IrDA) port uses IR to exchange information between devices. IR only allows a one-to-one type of connection.

IR is also used for remote control devices, wireless mice, and wireless keyboards. It is generally used for short-range, line-of-sight, communications. However, it is possible to reflect the IR signal off objects to extend the range. For greater ranges, higher frequencies of electromagnetic waves are required.

Radio Frequency (RF)
RF waves can penetrate through walls and other obstacles, allowing a much greater range than IR.

Certain areas of the RF bands have been set aside for use by unlicensed devices such as wireless LANs, cordless phones and computer peripherals. This includes the 900 MHz, 2.4 GHz and the 5 GHz frequency ranges. These ranges are known as the Industrial Scientific and Medical (ISM) bands and can be used with very few restrictions.

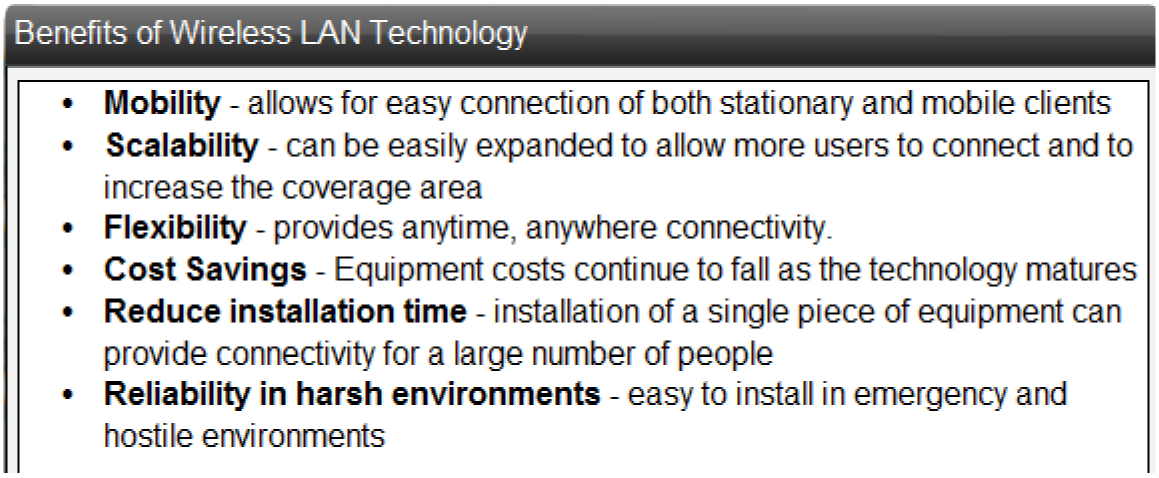


Bluetooth is a technology that makes use of the 2.4 GHz band. It is limited to low-speed, short-range communications, but has the advantage of communicating with many devices at the same time. This one-to-many communications has made Bluetooth technology the preferred method over IR for connecting computer peripherals such as mice, keyboards and printers.

Other technologies that make use of the 2.4 GHz and 5GHz bands are the modern wireless LAN technologies that conform to the various IEEE 802.11 standards. They are unlike Bluetooth technology in that they transmit at a much higher power level, which gives them a greater range.

Benefits and Limitations of Wireless Technology
Wireless technology offers many advantages compared to traditional wired networks.

One of the main advantages is the ability to provide anytime, anywhere connectivity. The widespread implementation of wireless in public locations, known as hotspots, allows people to easily connect to the Internet to download information and exchange emails and files.

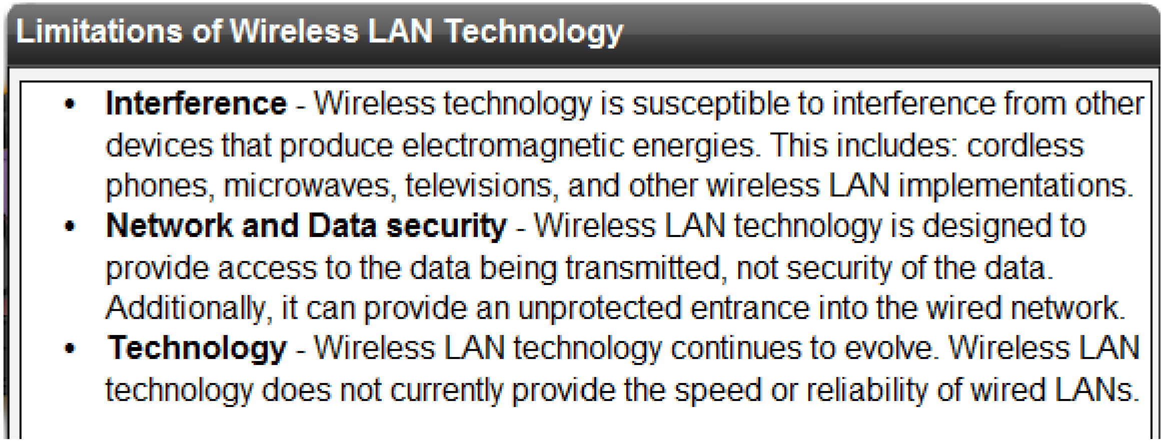

Benefits of Wireless LAN Technology

- **Mobility** - allows for easy connection of both stationary and mobile clients
- **Scalability** - can be easily expanded to allow more users to connect and to increase the coverage area
- **Flexibility** - provides anytime, anywhere connectivity.
- **Cost Savings** - Equipment costs continue to fall as the technology matures
- **Reduce installation time** - installation of a single piece of equipment can provide connectivity for a large number of people
- **Reliability in harsh environments** - easy to install in emergency and hostile environments

Wireless technology is fairly easy and inexpensive to install. The cost of home and business wireless devices continues to decrease. Yet, despite the decrease in cost, the data rate and capabilities of these devices have increased, allowing faster, more reliable wireless connections.

Wireless technology enables networks to be easily expanded, without the limitations of cabled connections. New and visiting users can join the network quickly and easily.

Despite the flexibility and benefits of wireless, there are some limitations and risks.



Limitations of Wireless LAN Technology

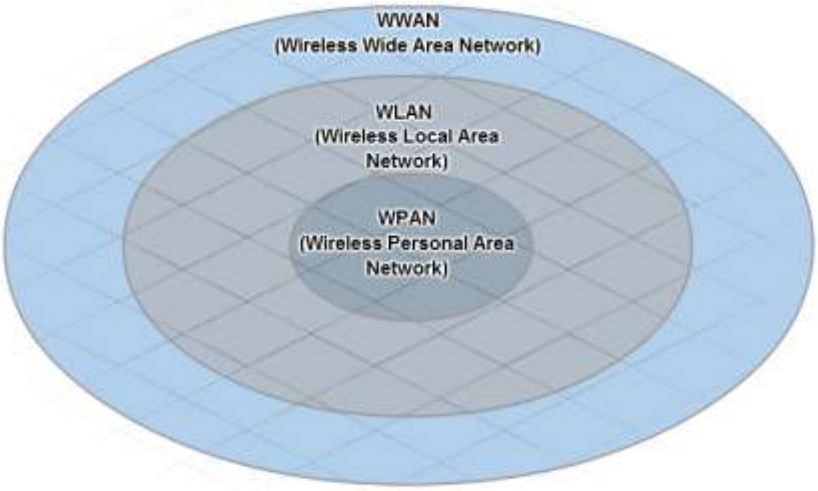
- **Interference** - Wireless technology is susceptible to interference from other devices that produce electromagnetic energies. This includes: cordless phones, microwaves, televisions, and other wireless LAN implementations.
- **Network and Data security** - Wireless LAN technology is designed to provide access to the data being transmitted, not security of the data. Additionally, it can provide an unprotected entrance into the wired network.
- **Technology** - Wireless LAN technology continues to evolve. Wireless LAN technology does not currently provide the speed or reliability of wired LANs.

First, Wireless LAN (WLAN) technologies make use of the unlicensed regions of the RF spectrum. Since these regions are unregulated, many different devices make use of them. As a result, these regions are congested and signals from different devices often interfere with each other. In addition, many devices such as microwave ovens and cordless phones use these frequencies and can interfere with WLAN communications.

Second, a major concern with wireless is security. Wireless provides ease of access. It does this by broadcasting data in a manner that allows anyone the ability to access it. However, this same feature also limits the amount of protection wireless can provide for the data. It allows anyone to intercept the communication stream, even unintended recipients. To address these security concerns, techniques have been developed to help secure wireless transmissions including encryption and authentication.

Types of Wireless Networks and Their Boundaries

Wireless networks are grouped into three major categories: Wireless Personal Area networks (WPAN), Wireless Local Area networks (WLAN), and Wireless Wide Area networks (WWAN).

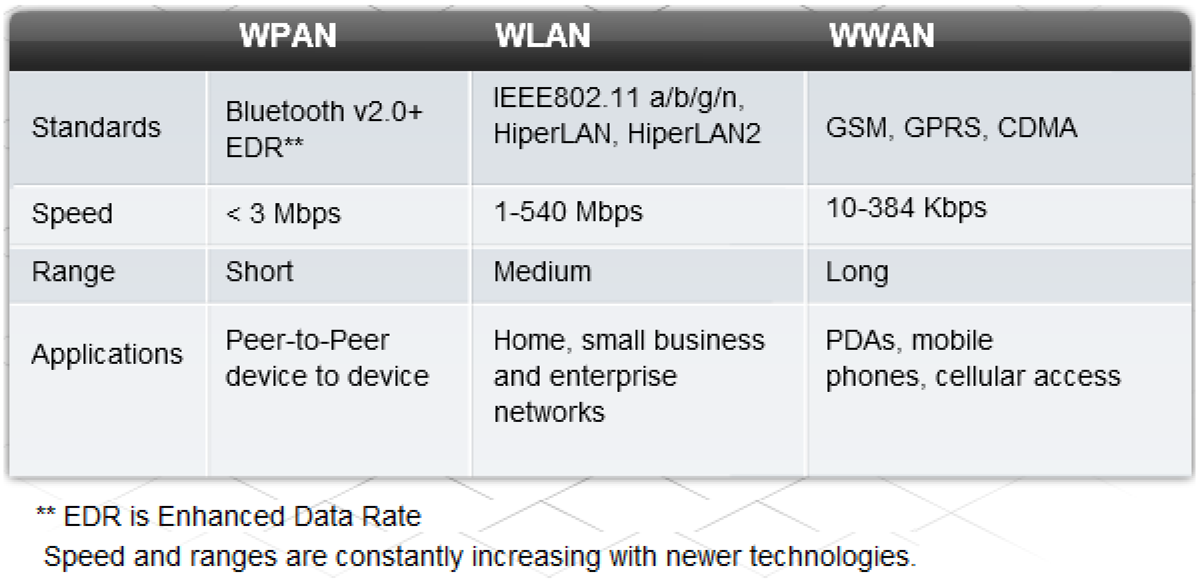

WWAN
(Wireless Wide Area Network)
WLAN
(Wireless Local Area Network)
WPAN
(Wireless Personal Area Network)

Despite these distinct categories, it is difficult to place boundary limitations on a wireless implementation. This is because, unlike a wired network, wireless networks do not have precisely defined boundaries. The range of wireless transmissions can vary due to many factors. Wireless networks are susceptible to outside sources of interference, both natural and man-made. Fluctuations in temperature and humidity can greatly alter the coverage of wireless networks. Obstacles within the wireless environment can also affect the range.

WPAN
This is the smallest wireless network used to connect various peripheral devices such as mice, keyboards and PDAs to a computer. All of these devices are dedicated to a single host with usually use IR or Bluetooth technology.

WLAN
WLAN is typically used to extend the boundaries of the local wired network (LAN). WLANs use RF technology and conform to the IEEE 802.11 standards. They allow many users to connect to a wired network through a device known as an Access Point (AP). An Access Point provides a connection between wireless hosts and hosts on an Ethernet wired network.

WWAN
WWAN networks provide coverage over extremely large areas. A good example of a WWAN is the cell phone network. These networks use technologies such as Code Division Multiple Access (CDMA) or Global System for Mobile Communication (GSM) and are often regulated by government agencies.



	WPAN	WLAN	WWAN
Standards	Bluetooth v2.0+ EDR**	IEEE802.11 a/b/g/n, HiperLAN, HiperLAN2	GSM, GPRS, CDMA
Speed	< 3 Mbps	1-540 Mbps	10-384 Kbps
Range	Short	Medium	Long
Applications	Peer-to-Peer device to device	Home, small business and enterprise networks	PDAs, mobile phones, cellular access

** EDR is Enhanced Data Rate
Speed and ranges are constantly increasing with newer technologies.

Wireless LANs

Wireless LAN Standards
A number of standards have been developed to ensure that wireless devices can communicate. They specify the RF spectrum used, data rates, how the information is transmitted, and more. The main organization responsible for the creation of wireless technical standards is the IEEE.

The IEEE 802.11 standard governs the WLAN environment. There are four amendments to the IEEE 802.11 standard that describe different characteristics for wireless communications. The currently available amendments are 802.11a, 802.11b, 802.11g and 802.11n. (802.11n is not ratified at the time of this writing.) Collectively these technologies are referred to as Wi-Fi, Wireless Fidelity.

Another organization, known as the Wi-Fi Alliance, is responsible for testing wireless LAN devices from different manufacturers. The Wi-Fi logo on a device means that this equipment meets standards and should interoperate with other devices of the same standard.

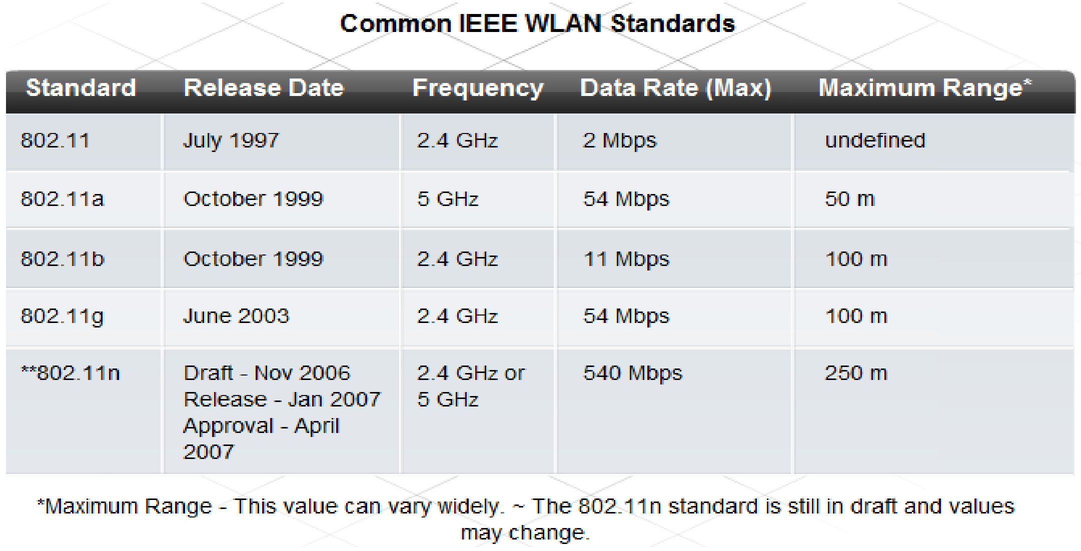
802.11a:
Uses 5 GHz RF spectrum
Not compatible with 2.4 GHz spectrum, i.e. 802.11b/g/n devices

Range is approximately 33% that of the 802.11 b/g
Relatively expensive to implement compared to other technologies.
Increasingly difficult to find 802.11a compliant equipment

802.11b:
First of the 2.4 GHz technologies
Maximum data-rate of 11 Mbps
Range of approximately 46 m (150 ft) indoors/96 m (300 ft.) outdoors

802.11g:
2.4 GHz technologies
Maximum data-rate increase to 54 Mbps
Same range as the 802.11b
Backwards compatible with 802.11b

802.11n:
Newest standard in development
2.4 GHz technologies (draft standard specifies support for 5 GHz)
Extends the range and data throughput
Backwards compatible with existing 802.11g and 802.11b equipment (draft standard specifies 802.11a support)



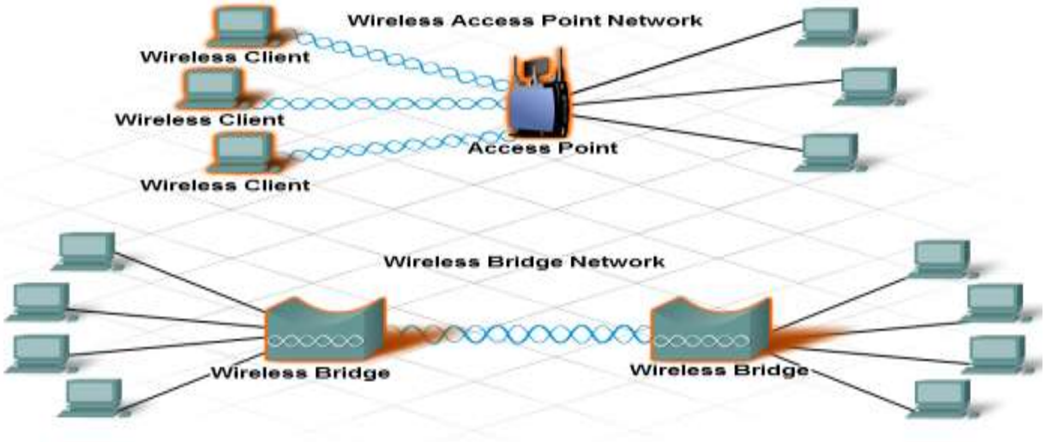
Common IEEE WLAN Standards

Standard	Release Date	Frequency	Data Rate (Max)	Maximum Range*
802.11	July 1997	2.4 GHz	2 Mbps	undefined
802.11a	October 1999	5 GHz	54 Mbps	50 m
802.11b	October 1999	2.4 GHz	11 Mbps	100 m
802.11g	June 2003	2.4 GHz	54 Mbps	100 m
**802.11n	Draft - Nov 2006 Release - Jan 2007 Approval - April 2007	2.4 GHz or 5 GHz	540 Mbps	250 m

*Maximum Range - This value can vary widely. ~ The 802.11n standard is still in draft and values may change.

Wireless LAN Components

Once a standard is adopted, it is important that all components within the WLAN adhere to the standard, or are at least compatible with the standard. There are various components that must be considered in a WLAN including: a wireless client or STA, an Access Point, a Wireless Bridge and an antenna.



Access Point:

- Controls access between a wired and a wireless network. I.E. allows wireless clients to gain access to a wired network and vice versa.
- Acts as a media converter accepting the Ethernet frames from the wired network and converting them to 802.11 compliant frames before transmitting them on the WLAN.
- Accepts 802.11 frames from the WLAN and converts them into Ethernet frames before placing them onto the wired network.
- APs support wireless connections within a limited area, known as a cell or Basic Service Set (BSS)

Wireless Client:

- Any host device that can participate in a wireless network. Most devices that can be connected to a traditional wired network can be connected to a WLAN if equipped with the proper wireless NIC and software.
- Can either be stationary or mobile.
- Commonly referred to as a STA, short for station.
- Examples include: laptops, PDAs, printers, projectors and storage devices.

Wireless Bridge:

- Used to connect two wired networks through a wireless link
- Allows long range point-to-point connections between networks
- Using the unlicensed RF frequencies, networks 40 km (25 miles) or more can be connected without the use of wires

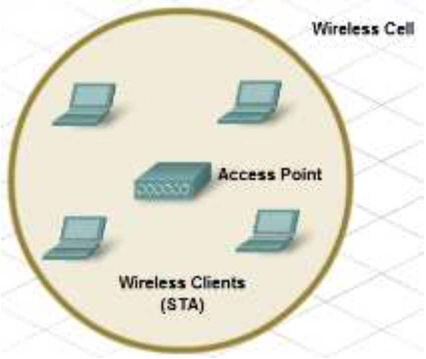
Antennas:

Used on APs and Wireless bridges
Increases the output signal strength from a wireless device
Receives wireless signals from other devices such as STAs
Increase in signal strength from an antenna is known as the gain
Higher gains usually translate into increased transmission distances

Antennas are classified according to the way they radiate the signal. Directional antennas concentrate the signal strength into one direction. Omni-directional antennas are designed to emit equally in all directions.

By concentrating all of the signal into one direction, directional antennas can achieve great transmission distances. Directional antennas are normally used in bridging applications while omni-directional antennas are found on APs.

WLAN and the SSID



When building a wireless network, it is important that the wireless components connect to the appropriate WLAN. This is done using a Service Set Identifier (SSID).

The SSID is a case-sensitive, alpha-numeric string that is up to 32-characters. It is sent in the header of all frames transmitted over the WLAN. The SSID is used to tell wireless devices which WLAN they belong to and with which other devices they can communicate.

Regardless of the type of WLAN installation, all wireless devices in a WLAN must be configured with the same SSID in order to communicate.

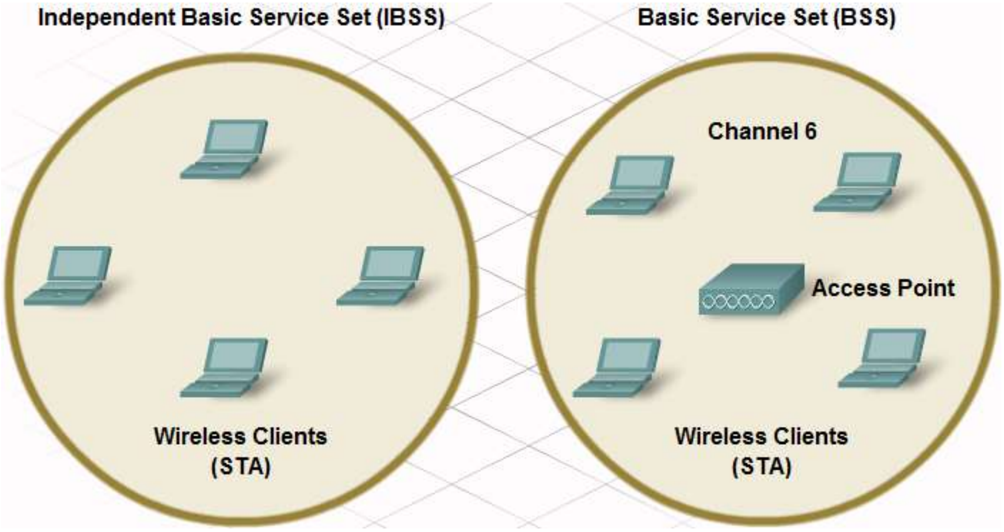
There are two basic forms of WLAN installations: Ad-hoc and infrastructure mode.

Ad-hoc

The simplest form of a wireless network is created by connecting two or more wireless clients together in a peer-to-peer network. A wireless network established in this manner is known as an ad-hoc network and does not include an AP. All clients within an ad-hoc network are equal. The area covered by this network is known as an Independent Basic Service Set (IBSS). A simple ad-hoc network can be used to exchange files and information between devices without the expense and complexity of purchasing and configuring an AP.

Infrastructure Mode

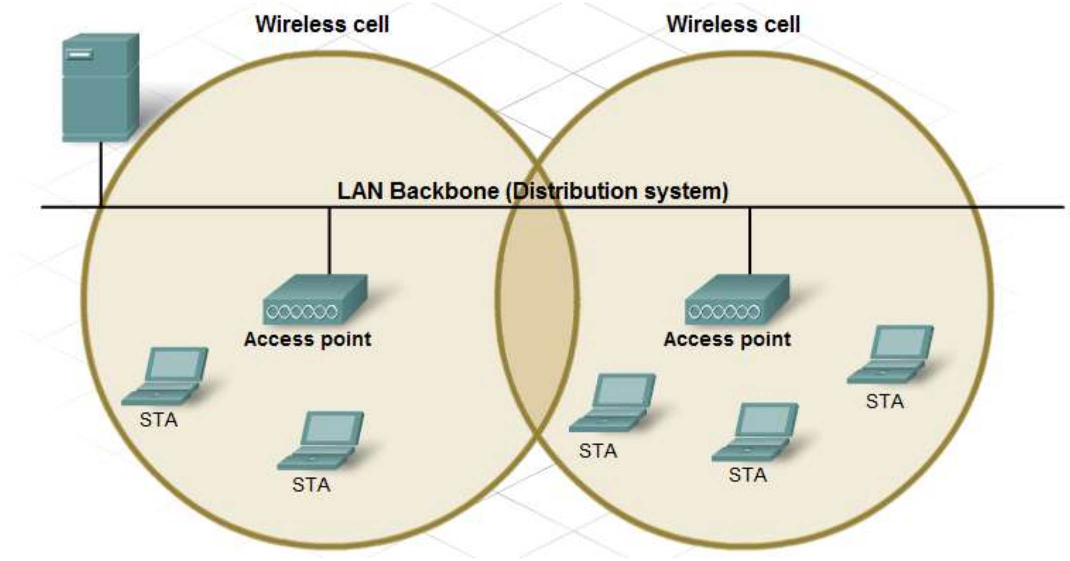
Although an ad-hoc arrangement may be good for small networks, larger networks require a single device that controls communications in the wireless cell. If present, an AP will take over this role and control who can talk and when. This is known as infrastructure mode and is the mode of wireless communication most often used in the home and business environment. In this form of WLAN, individual STAs can not communicate directly with each other. To communicate, each device must obtain permission from the AP. The AP controls all communications and ensures that all STAs have equal access to the medium. The area covered by a single AP is known as a Basic Service Set (BSS) or cell.



The Basic Service Set (BSS) is the smallest building block of a WLAN. The area of coverage of a single AP is limited. To expand the coverage area, it is possible to connect multiple BSSs through a Distribution System (DS). This forms an Extended Service Set (ESS). An ESS uses multiple APs. Each AP is in a separate BSS.

In order to allow movement between the cells without the loss of signal, BSSs must overlap by approximately 10%. This allows the client to connect to the second AP before disconnecting from the first AP.

Most home and small business environments consist of a single BSS. However, as the required coverage area and number hosts needing to connect increases it becomes necessary to create an ESS.



Wireless Channels

Regardless if the wireless clients are communicating within an IBSS, BSS or ESS the conversation between sender and receiver must be controlled. One way this is accomplished is through the use of Channels.

Channels are created by dividing up the available RF spectrum. Each channel is capable of carrying a different conversation. This is similar to the way that multiple television channels are transmitted across a single medium. Multiple APs can function in close proximity to one another as long as they use different channels for communication.

Unfortunately it is possible for the frequencies used by some channels to overlap with those used by others. Different conversations must be carried on non-overlapping channels. The number and distribution of channels vary by region and technology. The selection of channel used for a specific conversation can be set manually or automatically, based on factors such as current usage and available throughput.

Normally each wireless conversation makes use of a separate channel. Some of the newer technologies combine the channels to create a single wide channel, which provides more bandwidth and increases the data rate.

Within a WLAN, the lack of well-defined boundaries makes it impossible to detect if collisions occur during transmission. Therefore, it is necessary to use an access method on a wireless network that ensures collisions do not occur.

Wireless technology uses an access method called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). CSMA/CA creates a reservation on the channel for use by a specific conversation. While a reservation is in place, no other device may transmit on the channel thus possible collisions are avoided.

How does this reservation process work? If a device requires use of a specific communication channel in a BSS, it must ask permission from the AP. This is known as a Request to Send (RTS). If the channel is available, the AP will respond to the device with a Clear to Send (CTS) message indicating that the device may transmit on the channel. A CTS is broadcast to all devices within the BSS. Therefore, all devices in the BSS know that the requested channel is now in use.

Once the conversation is complete, the device that requested the channel sends another message to the AP known as an Acknowledgement (ACK). The ACK indicates to the AP that the channel can be released. This message is also broadcast to all devices on the WLAN. All devices within the BSS receive the ACK and know that the channel is once again available.

Configuring the Wireless Client

A wireless host, or STA, is defined as any device that contains a wireless NIC and wireless client software. This client software allows the hardware to participate in the WLAN. Devices that are STAs include: PDAs, laptops, desktop PCs, printers, projectors and Wi-Fi phones.

In order for a STA to connect to the WLAN, the client configuration must match that of the AP. This includes the SSID, security settings, and channel information if the channel was manually set on the AP. These settings are specified in the client software that manages the client connection.

The wireless client software used can be software integrated into the device operating system, or can be a stand-alone, downloadable, wireless utility software specifically designed to interact with the wireless NIC.

Integrated Wireless Utility Software

The Windows XP wireless client software is an example of a popular wireless client utility that is included as part of the device OS. This client software is basic management software that can control most wireless client configurations. It is user friendly and offers a simple connection process.

Stand-alone Wireless Utility Software

Wireless utility software, such as that supplied with the wireless NIC, is designed to work with that specific NIC. It usually offers enhanced functionality over Windows XP wireless utility software including feature such as:

- Link Information - displays the current strength and quality of a wireless single
- Profiles - allows configuration options such as channel and SSID to be specified for each wireless network
- Site Survey - enables the detection of all wireless networks in the vicinity

It is not possible to allow both the wireless utility software and Windows XP client software to manage the wireless connection at the same time. For most situations Windows XP is sufficient. However, if multiple profiles must be created for each wireless network or advanced configurations settings are necessary, it is better to use the utility supplied with the NIC.

Once the client software is configured, verify the link between the client and the AP.

Open the wireless link information screen to display information such as the connection data rate, connection status, and wireless channel used. The Link Information feature, if available, displays the current signal strength and quality of the wireless signal.

In addition to verifying the wireless connection status, verify that data can actually be transmitted. One of the most common tests for verifying successful data transmission is the Ping test. If the ping is successful, data transmission is possible.

If the ping is unsuccessful from source to destination, then ping the AP from the wireless client to ensure that wireless connectivity is available. If this fails as well, the issue is between the wireless client and the AP. Check the setting information and try to reestablish connectivity.

If the wireless client can successfully connect to the AP, then check the connectivity from the AP to the next hop on the path to the destination. If this is successful, then the problem is most likely not with the AP configuration, but may be an issue with another device on the path to the destination or the destination device itself.

Security Consideration on a Wireless LAN

Why People Attack WLANs

One of the primary benefits of wireless networking is ease and convenience of connecting devices. Unfortunately that ease of connectivity and the fact that the information is transmitted through the air also makes your network vulnerable to interception and attacks.

With wireless connectivity, the attacker does not need a physical connection to your computer or any of your devices to access your network. It is possible for an attacker to tune into signals from your wireless network, much like tuning into a radio station.

The attacker can access your network from any location your wireless signal reaches. Once they have access to your network, they can use your Internet services for free, as well as access computers on the network to damage files, or steal personal and private information.

These vulnerabilities in wireless networking require special security features and implementation methods to help protect your WLAN from attacks. These include simple steps performed during initial setup of the wireless device, as well as more advanced security configurations.

One easy way to gain entry to a wireless network is through the network name, or SSID.

All computers connecting to the wireless network must know the SSID. By default, wireless routers and access points broadcast SSIDs to all computers within the wireless range. With SSID broadcast activated, any wireless client can detect the network and connect to it, if no other security features are in place.

The SSID broadcast feature can be turned off. When it is turned off, the fact that the network is there is no longer made public. Any computer trying to connect to the network must already know the SSID.

Additionally, it is important to change the default setting. Wireless devices are shipped preconfigured with settings such as SSIDs, passwords, and IP addresses in place. These defaults make it easy for an attacker to identify and infiltrate a network.

Even with SSID broadcasting disabled, it is possible for someone to get into your network using the well-known default SSID. Additionally, if other default settings, such as passwords and IP addresses are not changed, attackers can access an AP and make changes themselves. Default information should be changed to something more secure and unique.

These changes, by themselves, will not protect your network. For example, SSIDs are transmitted in clear text. There are devices that will intercept wireless signals and read clear text messages. Even with SSID broadcast turned off and default values changed, attackers can learn the name of a wireless network through the use of these devices that intercept wireless signals. This information will be used to connect to the network. It takes a combination of several methods to protect your WLAN.

Limiting Access to a WLAN

One way to limit access to your wireless network is to control exactly which devices can gain access to your network. This can be accomplished through filtering of the MAC address.

MAC Address Filtering

MAC address filtering uses the MAC address to identify which devices are allowed to connect to the wireless network. When a wireless client attempts to connect, or associate, with an AP it will send MAC address information. If MAC filtering is enabled, the wireless router or AP will look up its MAC address a preconfigured list. Only devices whose MAC addresses have been prerecorded in the router's database will be allowed to connect.

If the MAC address is not located in the database, the device will not be allowed to connect to or communicate across the wireless network.

There are some issues with this type of security. For example, it requires the MAC addresses of all devices that should have access to the network be included in the database before connection attempts occur. A device that is not identified in the database will not be able to connect. Additionally, it is possible for an attacker's device to clone the MAC address of another device that has access.

Authentication on a WLAN

Another way to control who can connect is to implement authentication. Authentication is the process of permitting entry to a network based on a set of credentials. It is used to verify that the device attempting to connect to the network is trusted.

The use of a username and password is a most common form of authentication. In a wireless environment, authentication still ensures that the connected host is verified, but handles the verification process in a slightly different manner. Authentication, if enabled, must occur before the client is allowed to connect to the WLAN. There are three types of wireless authentication methods: open authentication, PSK and EAP.

Open Authentication

By default, wireless devices do not require authentication. Any and all clients are able to associate regardless of who they are. This is referred to as open authentication. Open authentication should only be used on public wireless networks such as those found in many schools and restaurants. It can also be used on networks where authentication will be done by other means once connected to the network.

Pre-shared keys (PSK)

With PSK both the AP and client must be configured with the same key or secret word. The AP sends a random string of bytes to the client. The client accepts the string, encrypts it (or scrambles it) based on the key, and sends it back to the AP. The AP gets the encrypted string and uses its key to decrypt (or unscramble) it. If the decrypted string received from the client matches the original string sent to the client, the client is allowed to connect.

PSK performs one-way authentication, that is, the host authenticates to the AP. PSK does not authenticate the AP to the host, nor does it authenticate the actual user of the host.

Extensible Authentication Protocol (EAP)

EAP provides mutual, or two-way, authentication as well as user authentication. When EAP software is installed on the client, the client communicates with a backend authentication server such as Remote Authentication Dial-in User Service (RADIUS). This backend server functions separately from the AP and maintains a database of valid users that can access the network. When using EAP, the user, not just the host, must provide a username and password which is checked against the RADIUS database for validity. If valid, the user is authenticated.

Once authentication is enabled, regardless of the method used, the client must successfully pass authentication before it can associate with the AP. If both authentication and MAC address filtering are enabled, authentication occurs first.

Once authentication is successful, the AP will then check the MAC address against the MAC address table. Once verified, the AP adds the host MAC address into its host table. The client is then said to be associated with the AP and can connect to the network.

Encryption on a WLAN

Authentication and MAC filtering may stop an attacker from connecting to a wireless network but it will not prevent them from being able to intercept transmitted data. Since there are no distinct boundaries on a wireless network, and all traffic is transmitted through the air, it is easy for an attacker to intercept, or sniff the wireless frames. Encryption is the process of transforming data so that even if it is intercepted it is unusable.

Wired Equivalency Protocol (WEP)

Wired Equivalency Protocol (WEP) is an advanced security feature that encrypts network traffic as it travels through the air. WEP uses pre-configured keys to encrypt and decrypt data.

A WEP key is entered as a string of numbers and letters and is generally 64 bits or 128 bits long. In some cases, WEP supports 256 bit keys as well. To simplify creating and entering these keys, many devices include a Passphrase option. The passphrase is an easy way to remember the word or phrase used to automatically generate a key.

In order for WEP to function, the AP, as well as every wireless device allowed to access the network must have the same WEP key entered. Without this key, devices will not be able to understand the wireless transmissions.

WEP is a great way to prevent attackers from intercepting data. However, there are weaknesses within WEP, including the use of a static key on all WEP enabled devices. There are applications available to attackers that can be used to discover the WEP key. These applications are readily available on the Internet. Once the attacker has extracted the key, they have complete access to all transmitted information.

One way to overcome this vulnerability is to change the key frequently. Another way is to use a more advanced and secure form of encryption known as Wi-Fi Protected Access (WPA).

Wi-Fi Protected Access (WPA)

WPA also uses encryption keys from 64 bits up to 256 bits. However, WPA, unlike WEP, generates new, dynamic keys each time a client establishes a connection with the AP. For this reason, WPA is considered more secure than WEP because it is significantly more difficult to crack.

Traffic Filtering on a WLAN

In addition to controlling who can gain access to the WLAN and who can make use of transmitted data, it is also worthwhile to control the types of traffic transmitted across a WLAN. This is accomplished using traffic filtering.

Traffic filtering blocks undesirable traffic from entering or leaving the wireless network. Filtering is done by the AP as traffic passes through it. It can be used to remove traffic from, or destined to, a specific MAC or IP address. It can also block certain applications by port numbers. By removing unwanted, undesirable and suspicious traffic from the network, more bandwidth is devoted to the movement of important traffic and improves the performance of the WLAN. For example, traffic filtering can be used to block all telnet traffic destined for a specific machine, such as an authentication server. Any attempts to telnet into the authentication server would be considered suspicious and blocked.

Configuring an Integrated AP and Wireless Client

Planning the WLAN

When implementing a wireless network solution, it is important to plan before performing any installation. This includes:

- Determining the type of wireless standard to use
- Determining the most efficient layout of devices
- An installation and security plan
- A strategy for backing up and updating the firmware of the wireless devices.

Wireless Standard

It is necessary to consider several factors when determining which WLAN standard to use. The most common factors include: bandwidth requirements, coverage areas, existing implementations, and cost. This information is gathered by determining end-user requirements.

The best way to learn end-user requirements is to ask questions.

- What throughput is actually required by the applications running on the network?
- How many users will access the WLAN?
- What is the necessary coverage area?
- What is the existing network structure?
- What is the budget?

The bandwidth available in a BSS must be shared between all the users in that BSS. Even if the applications do not require a high-speed connection, one of the higher-speed technologies may be necessary if multiple users are connecting at the same time.

Different standards support different coverage areas. The 2.4 GHz signal, used in 802.11 b/g/n technologies, travels a greater distance than does the 5 GHz signal, used in 802.11a technologies. Thus 802.11 b/g/n supports a larger BSS. This translates into less equipment and a lower cost of implementation.

The existing network also affects new implementation of WLAN standards. For example, the 802.11n standard is backward compatible with 802.11g and 802.11b but not with 802.11a. If the existing network infrastructure and equipment support 802.11a, new implementations must also support the same standard.

Cost is also a factor. When considering cost, consider Total Cost of Ownership (TCO) which includes the purchase of the equipment as well as installation and support costs. In a medium to large business environment, TCO has a greater impact on the WLAN standard chosen than in the home or small business environment. This is because in the medium to large business, more equipment is necessary and installation plans are required, increasing cost.

Installation of Wireless Devices

For home or small business environments, the installation usually consists of a limited amount of equipment which can be easily relocated to provide optimum coverage and throughput.

In the enterprise environment, equipment cannot be easily relocated and coverage must be complete. It is important to determine the optimum number and location of APs to provide this coverage at the least amount of cost.

In order to accomplish this, a site survey is usually conducted. The person responsible for the site survey must be knowledgeable in WLAN design and equipped with sophisticated equipment for measuring signal strengths and interference. Depending on the size of the WLAN implementation, this can be a very expensive process. For small installations a simple site survey is usually conducted by simply using wireless STAs and the utility programs packaged with most wireless NICs.

In all cases, it is necessary to consider known sources of interference such as high-voltage wires, motors, and other wireless devices when determining the placement of WLAN equipment.

Installing and Securing the AP

Once the best technology and placement of the AP is determined, install the WLAN device and configure the AP with security measure. Security measures should be planned and configured before connecting the AP to the network or ISP.

Some of the more basic security measures include:

- Change default values for the SSID, usernames and passwords.
- Disable broadcast SSID
- Configure MAC Address Filtering

Some of the more advanced security measures include:

- Configure encryption using WEP or WPA
- Configure authentication
- Configure traffic filtering

Keep in mind that no single security measure will keep your wireless network completely secure. Combining multiple techniques will strengthen the integrity of your security plan.

When configuring the clients, it is essential that the SSID matches the SSID configured on the AP. Additionally, encryption keys and authentication keys must also match.

Backing-up and Restoring Configuration Files

Configuration Backups

Once the wireless network is properly configured and traffic is moving, a full configuration backup should be performed on wireless devices. This is especially important if a great deal of customization is done to the configuration.

With most integrated routers designed for the home and small business markets, this is simply a matter of selecting the Backup Configurations option from the appropriate menu and specifying the location where the file should be saved. The integrated router provides a default name for the configuration file. This file name can be changed.

The restore process is just as simple. Select the Restore Configurations option. Then, simply browse to the location where the configuration file was previously saved and select the file. Once the file is selected, click Start to Restore to load the configuration file.

Sometimes it may be necessary to return the setting to the factory default conditions. To accomplish this select either the Restore Factory Defaults option from the appropriate menu or press and hold the RESET button located for 30 seconds. The latter technique is especially useful if you are unable to connect to the AP of the integrated router through the network but have physical access to the device.

Updating the Firmware

The operating system on most integrated routers is stored in firmware. As new features are developed or problems with the existing firmware are discovered, it may become necessary to update the firmware on the device.

The process for updating firmware on an integrated router, such as the Linksys wireless router, is simple. However, it is important that once the process is started, it is not interrupted. If the update process is interrupted before completion, the device may be rendered non-operable.

Determine the version of the firmware currently installed on the device. This information is usually displayed on the configuration screen or the connection status screen. Next, search the manufacturer's web site and related news groups on the Internet to discover the firmware feature set, issues that may warrant an upgrade, and whether updates are available.

Download the updated version of the firmware and store it on the hard drive of a device that can be directly connected to the integrated router. It is better if the machine is directly connected to the integrated router with a cable to prevent any interruption in the update process caused by a wireless connection.

Select the Firmware Upgrade feature in the GUI. Browse to the appropriate file on the directly connected device and start the upgrade.

Adapted and Compiled from:

CCNA IT Essential, “PC Hardware and Software” version 4.0, Cisco Networking Academy
CCNA Discovery 1, “Networking for Home and Small Businesses”, Cisco Networking Academy
CCNA Discovery 2, “Working at a Small-to-Medium Business of ISP”, Cisco Networking Academy
CCNA Exploration 1, “Network Fundamentals”, Cisco Networking Academy
Cisco Networking Academy Program, CCNA 1 and 2 Companion Guide, Cisco Press