Wi-Fi Client Technologies

Crowley

Chapter 5

Topics

- Wireless network attributes
- Wireless network standards & related organizations
- Wireless technologies
- Wireless security briefly
- Site surveys

Wi-Fi Includes

- Frequency bands for wireless networks
  - Designated by Federal Communications Commission (FCC) or similar
- Standards issued by the Institute of Electrical and Electronics Engineers (IEEE)
- Certifications issued by the Wi-Fi Alliance

Wireless Networking

- Can be viewed as starting with the 802.11 standards.
- Cable and phone companies began to offer higher speed connections in the form of cable modems and Digital Subscriber Line (DSL) connections.
- In addition, satellite-based Internet services were offered to those beyond the reach of cable company or beyond the distance required for DSL connections.
- More recently, Wi-Fi Alliance reports that 2 billion Wi-Fi devices were sold in 2013.

Bandwidth and Speed

- As higher bandwidth and speed was introduced, devices became more affordable, people added more devices.
  - As the number of computers and Internet-connected devices increased, the need for wireless technologies increased.
- Wireless device manufacturers saw need produced devices that used newer wireless technologies, offered faster connections, and supported multiple devices.

Client

- Device that connects to a wireless network.
- Laptop, desktop, tablet, smartphone, network server, or other…
  - Note that the term station (or STA) may also refer to a wireless client.
- Wireless clients have a wireless interfac.
- Some commercial and industry devices come with embedded (chip-based) OSes for specialized use.
  - Have limited configuration options to connect to wireless networks.

Client Interface

- Clients can have wireless network cards that:
- Fit into a slot on the motherboard (as in the case of desktop clients)
- Use Personal Computer Memory Card International Association (PCMCIA) card slots
- Connect via USB
- Integrated into the motherboard.

- A variety of both legacy and newer wireless adapters for clients.

Access Points

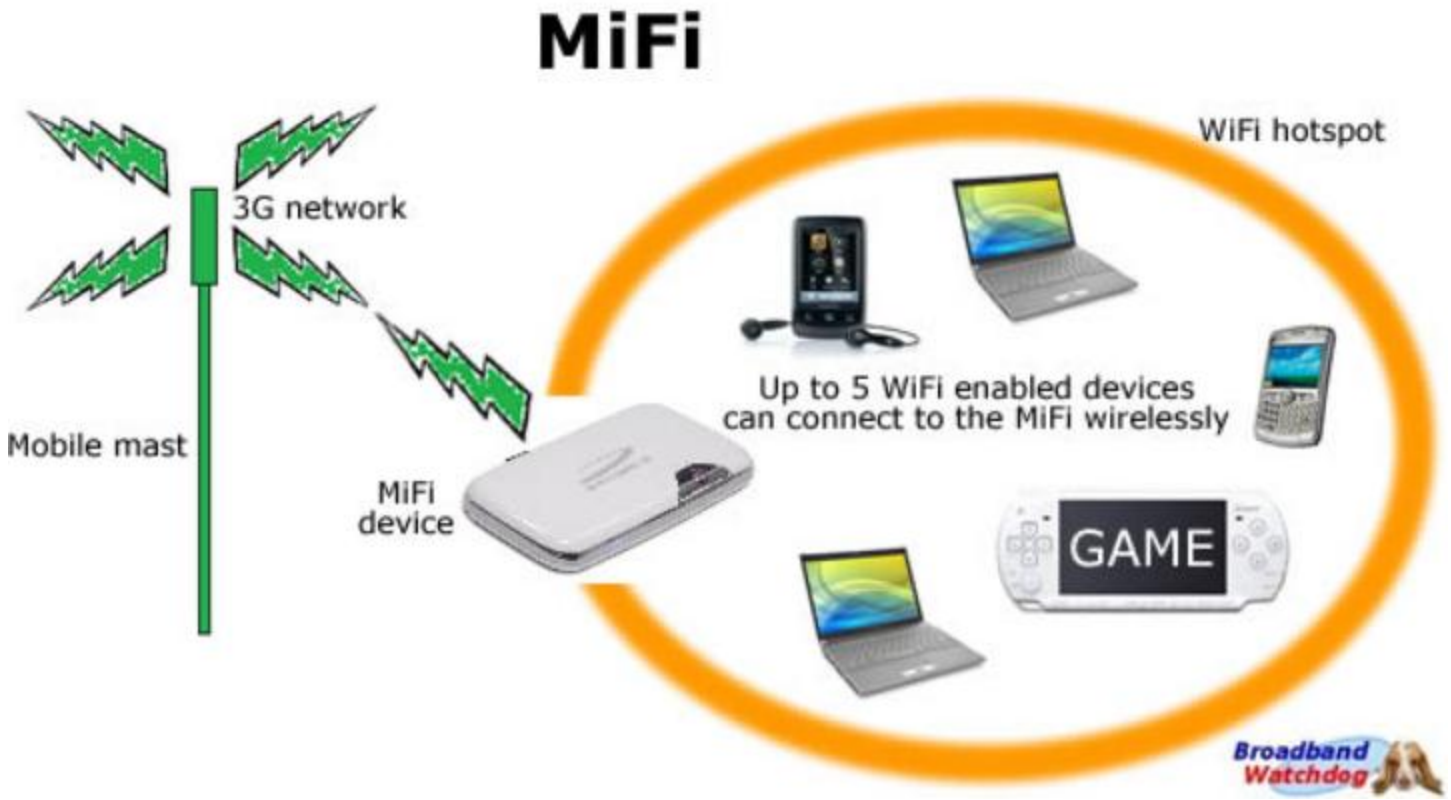
- An access point can be a small home use device, a simple SOHO (Small Office Home Office) device, or an enterprise-level device with several features that control access to multiple networks, including wired networks.
- Can offer security features, accounting features, and control access to both networks and data by specific users.
- Common access points shown.

Portable Hotspots

- Typically a small device with access to cellular technologies that provides access to these networks for Wi-Fi devices.
  - Can be purchased from wireless providers such as Verizon, Sprint, AT&T, T-Mobile, or other carriers.
  - Usually specific to their type of broadband network.
  - Provide wireless access for up to five or ten devices.
- Basically wireless routers that route traffic between Wi-Fi devices and broadband technologies.
- Depending upon the carrier, some cellular phones, as well as some tablets, can act as portable hotspots.

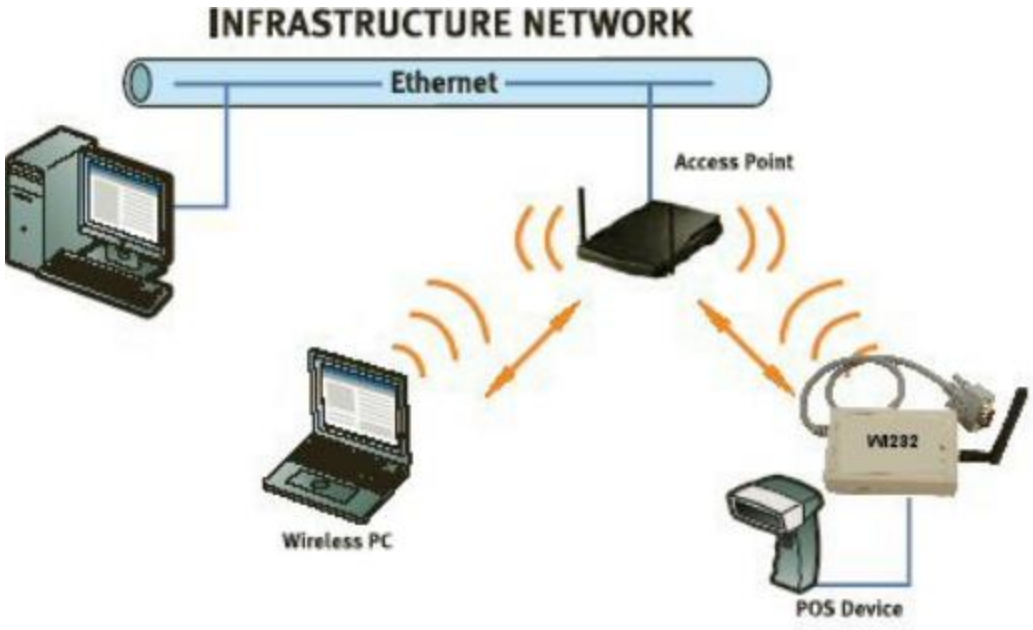
MiFi

- The popular term used for portable hotspots, as well as devices like cellular phones that also provide hotspot service, is MiFi (My Wi-Fi).
- Novatel Wireless actually owns the trademark, but it has become common to refer to most of these devices as MiFi-capable.
- Screenshot shows an Android phone acting as a portable hotspot.


MiFi
WiFi hotspot
3G network
Mobile mast
MiFi
device
Up to 5 WiFi enabled devices
can connect to the MiFi wirelessly
GAME
Broadband
Watchdog

Ad-hoc and Infrastructure Modes of Operation.

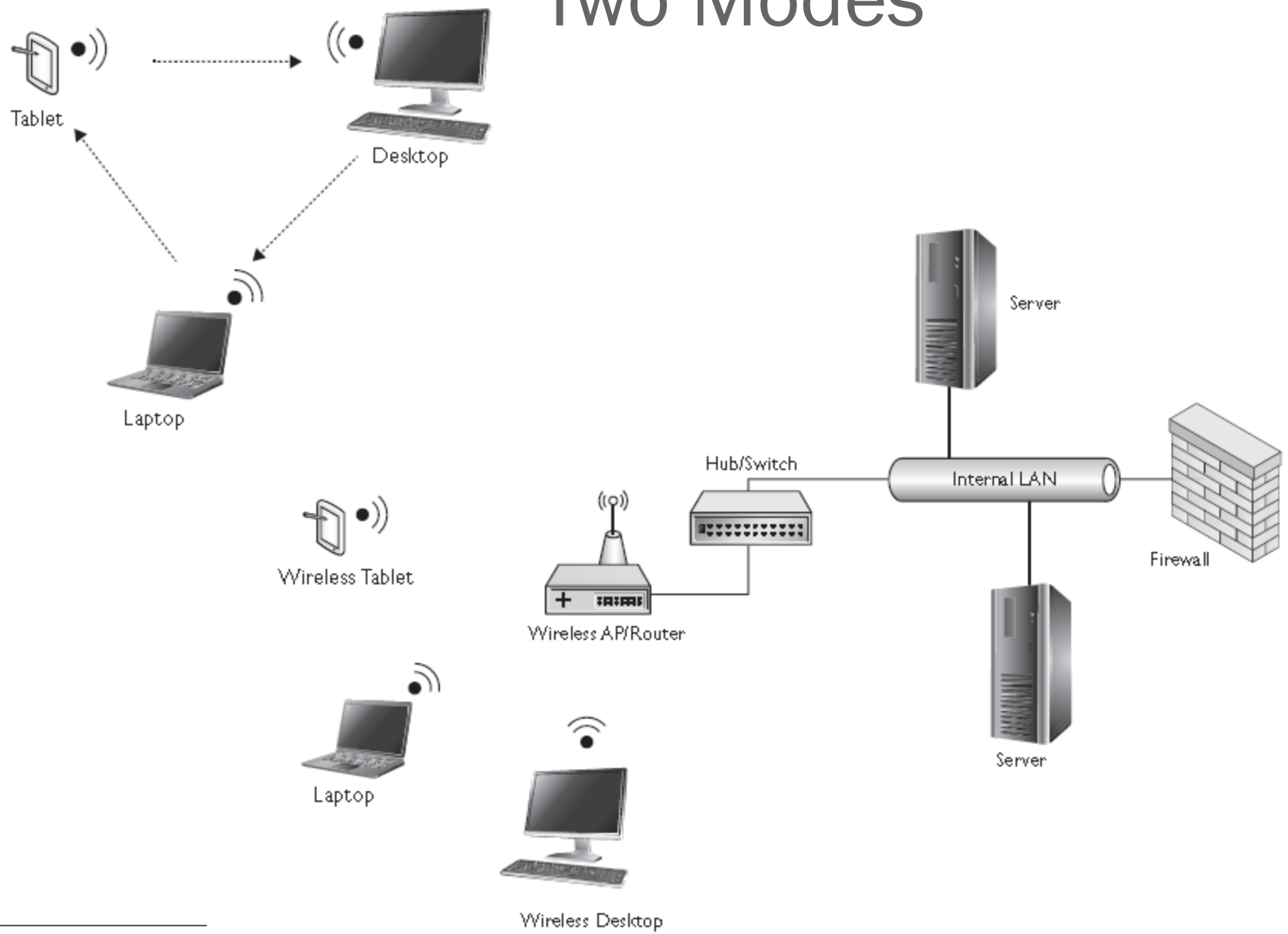
- Depends upon whether the wireless network is centrally managed or is a simple peer- to-peer network.
- Ad hoc network, peer to peer, usually consists of just a few devices connected together for the purposes of sharing files, gaming, or Internet connection sharing.
- Typically characterized by low security settings, and devices that are relatively close to each other.
- For these networks to work, each client device has to be configured with identical configuration settings, including network name; security settings, such as authentication and encryption; and any passwords or shared keys used to connect to each other.



Infrastructure Mode

- Characterized by several client devices that connect to a central access point, usually a wireless access point (WAP) or, in larger organizations, a wireless LAN controller.
- WAP enables clients to connect to one another and to another network, such as a wired network,.
- Most of the wireless networks are infrastructure mode networks.

Two Modes

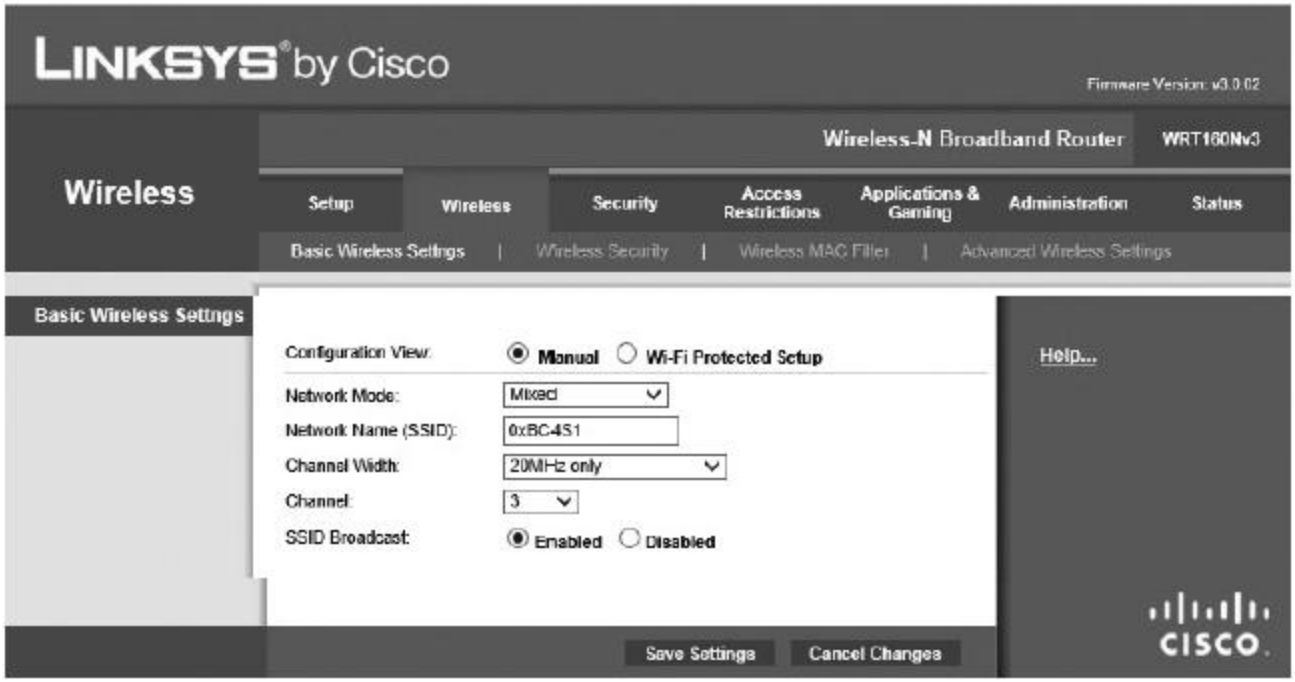

Tablet
Desktop
Laptop
Server
Hub/Switch
Internal LAN
Firewall
Wireless Tablet
Wireless AP/Router
Laptop
Server
Wireless Desktop

SSID Service Set Identifier

- Refers to unique wireless network name.
- A wireless client can detect net-works on a range of channels and frequencies, and lists those wireless network names it has detected for the user to choose from and connect to.
- Typically, the wireless access point "broadcasts" SSID.
- Many access points, when they are first powered up, broadcast a default SSID, which can (and should) be changed.

Change Default SSID

- SSIDs should be changed from their device defaults to a network name consistent with an organization's naming conventions.
  - SSID can be composed of both uppercase and lowercase letters, numerals, and special characters.
  - Can be up to 32 characters in length
  - Is case sensitive.
- Name should not delineates a purpose or target a particular client audience, such as marketing or accounting.
  - Though, could use a code that would.
- May also be used to separate groups of users and their allowed access.



- One frequent recommendation was to turn SSID broadcasting off.
- Supposedly keeps unwanted clients from connecting to the wireless network.
- SSID hiding is another example of 'security through obscurity' which has been repeatedly proven to not work.

IBSS Independent Basic Service Set

- Describes network in use in an ad-hoc mode network.
- This network, as described earlier, is basically a device-to-device type of network that is set up by users to transfer files, play games, and so forth on the fly.
- It's also used when there's no real need for an intermediary device, such as a wireless router, to control the connections.

ESSID Extended Service Set ID

- Network name of a larger infrastructure mode network that has multiple access points, and at some point, connects to a larger wired network.
- Usually a corporate network infrastructure, which provides wireless coverage for a large organization, with multiple devices, locations, and user and device characteristics.

BSSID Basic Service Set ID

- Describes the basic plain infrastructure-type of network, typically associated with one wireless access point.
- When referencing a network by BSSID, it is usually the hardware or MAC address of the wireless access point.
- So, where an SSID and ESSID are referenced as network names, the BSSID is usually the hardware address of a given WAP.

Wi-Fi Organizations: FCC

- In the United States, the Federal Communications Commission (FCC) is regulatory authority for the use of radio frequencies and technologies.
- Allows private and commercial wireless networks to operate on four separate frequency bands.

1. 2.4 GHz Industrial, Scientific, and Medical (ISM) band
2. 3.6 GHz band
3. 5 GHz Unlicensed National Information Infrastructure (U-NII) band
4. 60 GHz band.

- Most of the wireless specifications that we are concerned with operate in the 2.4 and 5 GHz bands.

Institute of Electrical and Electronics Engineers

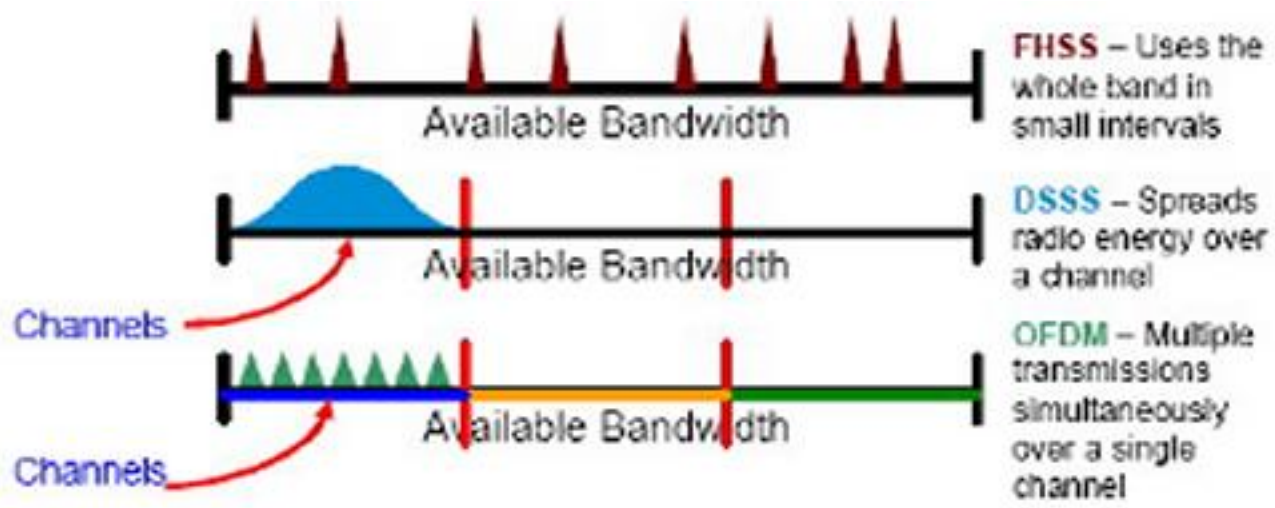
- IEEE 802 committee responsible for developing the LAN, MAN, and wireless LAN (WLAN) standards.
- 802.11 standards dictate signaling, power, security technologies, and other factors used to develop and field a standards-compliant wireless network that is interoperable, regardless of manufacturer and equipment.
- 802.16 WiMax

Wi-Fi Alliance

- Group of manufacturers and other interested parties that formed a trade association of sorts to jointly produce interoperable equipment and technologies.
  - Members currently include Cisco, Microsoft, Nokia, Samsung, Dell, Apple, Sony, and others.
- Sponsors a Wi-Fi Certification program that certifies technologies and devices as being interoperable and compliant with standards, enabling a manufacturer's devices to be branded with the Wi-Fi Alliance logo if it is submitted for certification and meets requirements.
  - Serves to advise organizations, like the IEEE, on potential new technology standards.

802.11 Standards

- The IEEE 802.11 standards are a set of physical layer signaling and technology standards for implementing WLANs in the 2.4, 3.6, 5, and 60 GHz frequency bands.
  - Actually a family of standards, including the a, b, g, i, k, n, and others.
- Original 802.11 (with no suffix) was released in 1997.
- Data rates of the standard were extremely slow.
  - Specified two net bit rates of 1 or 2 megabits per second (Mbps).
  - Never really widely implemented.
- Quickly supplanted by the faster: 802.11a and b..



- 802.11 standard operated in the 2.4 GHz ISM band and originally provided for both:
  - Frequency hopping spread spectrum (FHSS)
  - Direct sequence spread spectrum (DSSS).
- A third signaling technology, called orthogonal frequency division multiplexing (OFDM), was introduced later…

802.11a

- One of the first wireless standards to come out.
  - About the same time as the wireless "b" standard (802.11b) in 1999.
- 54 megabits per second (Mbps) throughput.
- Operates in the 5 GHz range.
- Using this frequency range can mean less interference from other wireless devices.

802.11a

- Uses a orthogonal frequency division multiplexing, or OFDM.
  - Rather than using just one frequency, it uses several adjacent ones to carry data.
  - "A" standard not widely adopted when it was first introduced.
  - While this range falls within the unregulated bands in the United States, in Europe the 5 GHz range was still subject to heavier regulation.
- Since 2003, 802.11a wireless has become more widely implemented worldwide.
- Wireless "b" standard, which also came out about the same time in 1999, was more widely used.

802.11b

- More readily adopted and accepted in the consumer market space.
  - Due primarily to the high proliferation and avail-ability of equipment (access points and network cards).
- Operates in the unlicensed 2.4 GHz Industrial, Scientific, and Medical (ISM) range
- Throughput of about 11 Mbps.
- Uses a physical layer signaling technology known as direct sequence spread spectrum (DSSS).
  - DSSS basically means that the wireless signal is spread over the full bandwidth of a frequency or channel.

802.11b and WEP

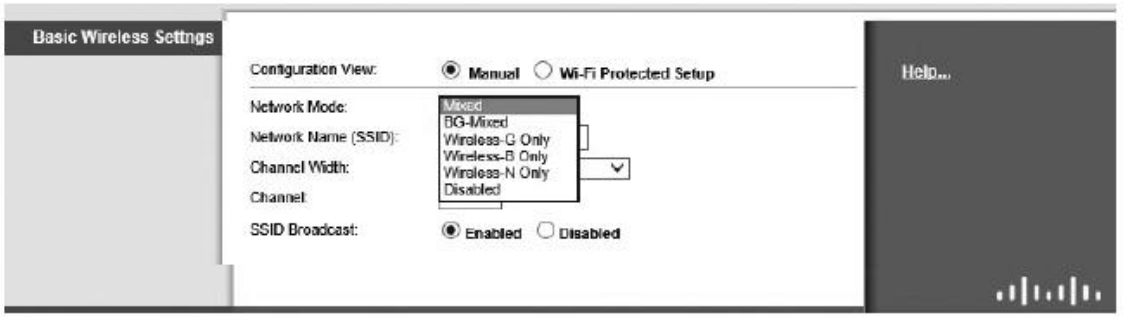
- Although now considered insecure, 802.11b networks introduced the first wireless security standard, known as Wired Equivalent Privacy, or WEP.
  - 802.11b networks are not often seen any longer, due to the heavy proliferation of improved wireless technologies and standards.

802.11g

- Once, most commonly used 802.11 standards.
  - Rapidly been replaced by 802.11n.
  - Introduced in 2003
  - Backwards compatible with 802.11b
- Operate in the same 2.4 GHz ISM band that "b" networks operate in, and use OFDM.
- Backwards compatible with 802.11b.
  - Incurs performance degradation on the 802.11g devices when backwards compatibility is used.

Mixed Mode

- Can be changed on the wireless access point to reflect mixed "b" and "g" modes, or set to allow for wireless "g" only.
  - 802.11g supports data rates of up to 54 Mbps, with legacy equipment running at lower supported rates.
- Some newer devices have dropped support for the legacy 802.11b networks, as this equipment is phased out and no longer made or sold by the mainstream retailers.
- Example of mixed-mode settings.



Draft 802.11n Devices

- Over the years moving faster in implementation than the formal adoption of the standards by the IEEE, manufacturers produced "draft" standards devices.
  - Understanding that these devices will be fully (for the most part) compatible with the formal standards.
  - For example, the 802.11n standard, approved as final in 2009.
  - Standard was in draft for many years, but there were devices that were produced and sold as "compatible" with the draft standard long before it was approved.
- Devices were marketed and sold as "draft-N compatible."

802.11n

- Increased data rates significantly,.
  - From 54 Mbps in 802.11g to a theoretical 600 Mbps.
- Uses multiple-input multiple-output (MIMO) streams.
  - Supports up to four separate streams of 40 MHz each, effectively doubling the channel width of previous technologies from 20 MHz.
- Multiple antennas to separate the spatial streams, and uses a signaling technology called spatial division multiplexing, or SDM.
  - Significant security improvements.
- Can operate in both the 2.4 GHz and 5.0 GHz frequency ranges.
- Current standard for higher-speed wireless.
- About to be replaced by newer 802.11ac standard.

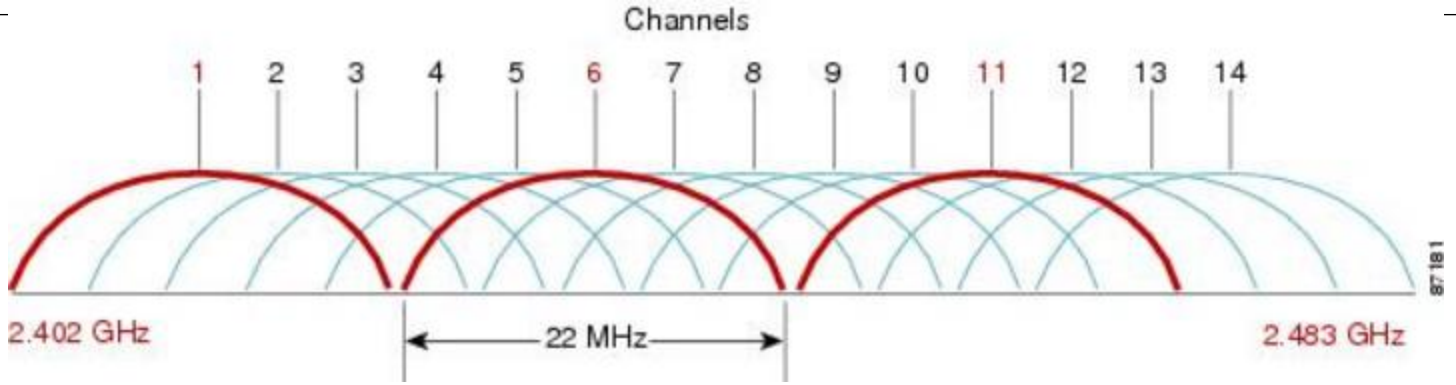
January 2014 802.11ac Approved

- For high bandwidth application (think HD video streaming).
  - Widens RF bandwidth to 160 MHz.
  - Extends and improves the MIMO technology, allowing up to eight separate multiuser MIMO spatial streams.
- Speeds up to 1 Gbps (for multi-station WLANs), and 500 Mbps for single station links.
- Operates only in the 5 GHz range.
  - Won't necessarily replace 802.11n.

802.11 Standard	Data Rates	PHY Signaling Technology	Band	Frequency Range
802.11	1 to 2 Mbps	FHSS/DSSS	ISM, 2.4 GHz	2.4 GHz
802.11a	6–54 Mbps	OFDM	UNII, 5 GHz	5.150–5.250 GHz UNII-1 5.250–5.350 GHz UNII-2 5.725–5.825 GHz UNII-3
802.11b	5.5 and 11 Mbps	DSSS	ISM, 2.4 GHz	2.4–2.4835 GHz
802.11g	Up to 54 Mbps (when used in mixed mode, data rates match legacy devices)	OFDM (but backwards compatible with 802.11b using DSSS and HR/DSSS)	ISM, 2.4 GHz	2.4–2.4835 GHz
802.11n	Up to 600 Mbps (when used in mixed mode, data rates match legacy devices)	HT-OFDM	ISM, 2.4 GHz UNII, 5 GHz	Same as 802.11a/b/g
802.11ac	Up to 1 Gbps	HT-OFDM	UNII, 5 GHz	Same as 802.11a/n

Wireless Channels and Frequencies

- Channels and frequency ranges dependent upon the region in which they're used.
  - Some channels used in Europe, other channels used in North America, Japan, and other countries.
  - Some countries restrict which channels can be used indoors and which can be used outdoors.
- For example, there are 14 available channels in the 2.4 GHz ISM band, which is used by DSSS and HR/DSSS PHY technologies.
  - In the Americas, channels 1 through 11 are used, and in Europe 1 through 13.
  - Japan uses all 14 channels.



- DSSS channels 22 MHz wide.
- Each channel separated by 5 MHz.
- Three adjacent non-overlapping channels.
  - Channels 1, 6, and 11.
- Theoretically allows three separate wireless access points in the same area without overlapping channel interference.
- As you will see in site survey discussion, this is important because you want to minimize Wi-Fi interference from other devices as much as possible.

Frequency (GHz)	Channel	Notes
2.412	1	Used by all countries
2.417	2	Used by all countries
2.422	3	Used by all countries
2.427	4	Used by all countries
2.432	5	Used by all countries
2.437	6	Used by all countries
2.442	7	Used by all countries
2.447	8	Used by all countries
2.452	9	Used by all countries
2.457	10	Used by all countries
2.462	11	Used by all countries
2.467	12	Used by Europe, Israel, Japan, and other countries
2.472	13	UsedUsed by Europe, Israel, Japan, and other countries
2.484	14	Only used by Japan per IEEE 802.11-2012 standard

Table 5-2 2.4 GHz ISM Band Frequencies and Channels

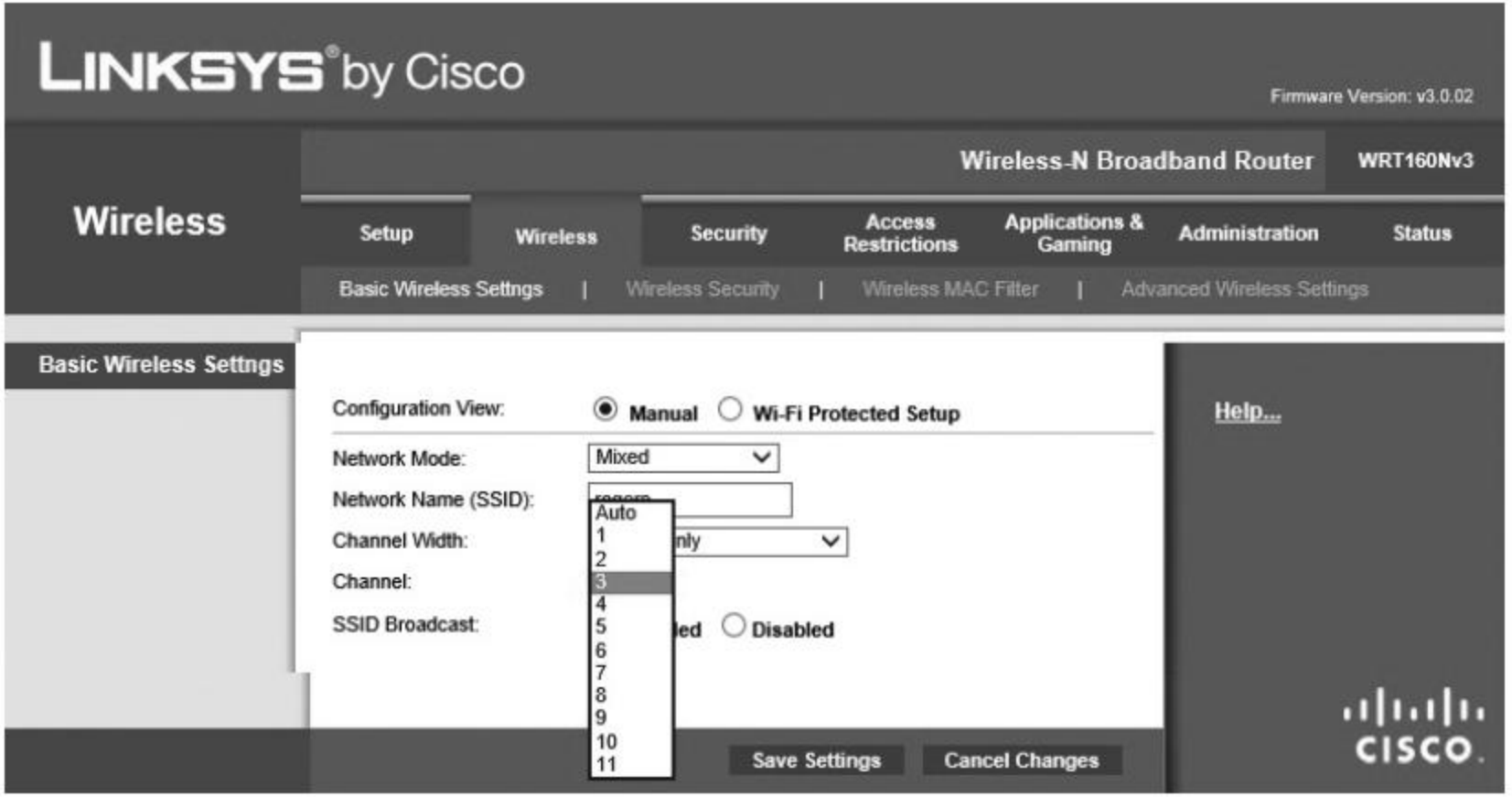
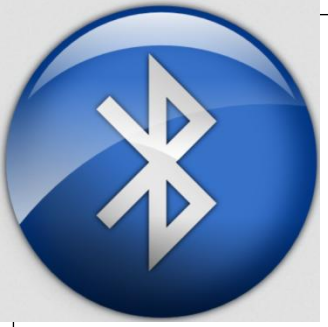


Figure 5-10 Changing the channels on a Linksys wireless AP



Bluetooth

- Wireless technology standard for exchanging data over short distances.
  - Uses ISM Band from 2.4 to 2.485 GHz.
  - Originally conceived as a wireless substitute for RS-232 serial interfaces.
- Can connect small devices, such as headsets to cell phones and other portable media devices.
- Originally 802.15.1 but now managed by Bluetooth Special Interest Group (SIG).
  - Promotes Bluetooth technologies pretty much the same way the Wi-Fi Alliance does for 802.11 technologies.

802.15 Bluetooth

- Open standard for short-range radio frequency (RF) communication.
- Used mainly to establish ad-hoc wireless personal area networks (WPANs) between devices such as cell phones, laptops, automobiles, medical devices, printers, keyboards, mice, and headsets.
- Allows easy file sharing, elimination of cables as well as Internet connectivity sharing between devices.
- Uses Frequency Hopping Spread Spectrum (FHSS) signaling technology.

Bluetooth Devices Classes

- A Class 1 device (high power) can communicate with another device up to 100 meters (328 feet) away,
- A Class 2 device (medium power) has a range of up to 10 meters (33 feet)
- A Class 3 device (low power) has a range of about 1 meter (3 feet).

Table 5-3 Bluetooth Specifications, Data Rates, and Ranges

Bluetooth Specification	Data Rate
1.x	Up to 1 Mbps (Basic Rate)
2.0	Up to 3 Mbps (Enhanced Data Rate)
3.0	Up to 24 Mbps (High Speed)
4.0	Up to 24 Mbps (High Speed)

Personal Area Network (PAN)

- Created when two or more Bluetooth devices are connected in exchange data.
- Could consist of a cellular phone and Bluetooth headset, or two cellular phones connected together, or even to laptops or tablets that are connected in exchange information.
- A Bluetooth PAN can also be called a piconet.
- Has a typical range of no more than about 30 feet, given current Bluetooth capabilities.
  - PAN consists of devices that are very close to each other.

Near Field Communications (NFC)

- Technology that enables smartphones to establish radio communication with each other by touching them together or bringing them into proximity.
  - Often cloud connected devices.
- Uses chips embedded in mobile devices that create electromagnetic fields when these devices are close to each other.
  - Typical range for NFC communications is 10 cm or less..
- Uses electromagnetic induction between two loop antennas located within each other's near fields.
- Operates on globally available and unlicensed ISM band of 13.56 MHz…
- Involves initiator and target.

WiMAX Worldwide Interoperability for Microwave Access IEEE 802.16

- Used for middle-haul or back-haul communications across larger areas, such as metropolitan areas or areas where customers can't get DSL, cable modem, or other broadband access from a typical provider.
- Based upon microwave technologies and enables wireless clients (with a special wireless network card or adapter) to access high-speed mobile broadband from greater distances, without the aid of a portable hotspot connecting them to 3G or 4G cellular technologies.

Authentication and Encryption

- In wired networks, some protection is offered by physical security.
  - Wireless networks lack this.
- All wireless data is sent via radio waves.
  - If the is not otherwise protected, data is subject to interception and disclosure.
- Two critical areas of mobile security in general, and 802.11 wireless technologies in particular, are authentication and encryption.

Authentication

- Overall process involved with identifying a user, program, process, or device, and then confirming (or authenticating) their identity.
- Authentication technologies usually involve some method for passing encrypted credentials across the network to an authentication device or server, which has a database of user credentials.
- Either (or both) devices and users can be authenticated.

Wireless Authentication

- This first, and least secure, involves supplying a preshared key (or passphrase) to a device (typically a client), which is encrypted.
  - Encrypted hash usually sent to the authenticating device (wireless access point), which verifies the encrypted hash as having been generated only from the pre-shared key.
- The second method involves the use of public/private key pairs, using an existing Public Key Infrastructure (PKI).

802.11 Shared Key

- 802.11 wireless networks employ several different types of authentication.
- For example, open authentication is the very basic type of authentication used by wireless networks.
  - But it's really no authentication all, as any client can connect to any access point as long as they have the password or key.
- Shared key authentication, on the other hand, is used by WEP.
- PSK-Personal and PSK-Enterprise are used by WPA.

Encryption

- Process of encoding information in such a way that only authorized parties can read it.
  - In the context of wireless technologies, this key is often called a pre-shared key, or pass- phrase, or a password.
- Together, key and algorithm provide a secure way to send data from one user or device to another user or device, with confidence that the data sent will not be compromised.

Types of Encryption

DES
TripleDES
AES
RC5

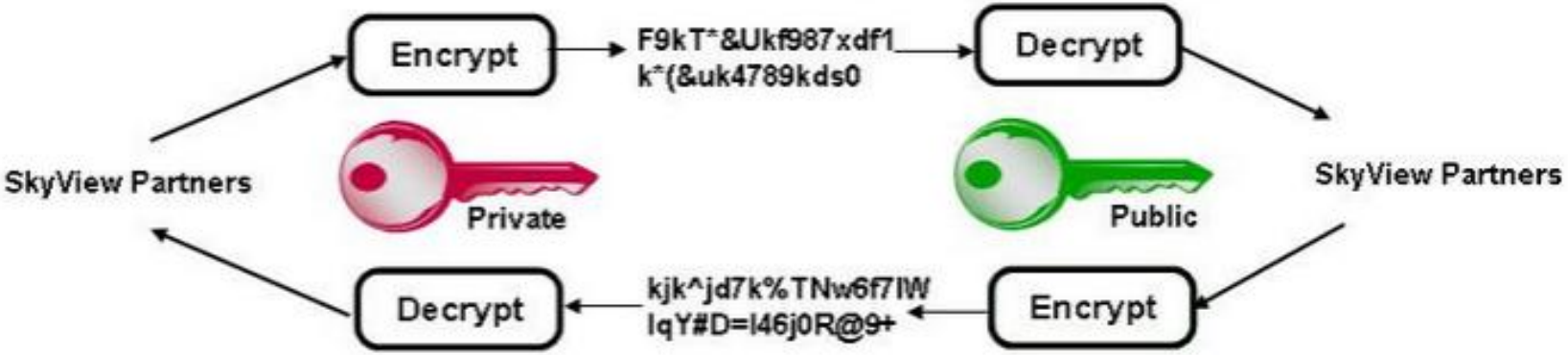
Symmetric Keys

- Encryption and decryption use the **same key**.

RSA
Elliptic Curve

Asymmetric keys

- Encryption and decryption use different keys, a **public key** and a **private key**.



WEP Wired Equivalent Privacy

- Introduced in 802.11b.
  - 802.11b standard requires only a 64-bit key.
- WEP uses shared key authentication.
  - Employs the same key for authentication and for data encryption.
- WEP uses small key sizes, which come in two variations.
- Keys are static
  - They do not change once they are entered into the device.
- All devices must be configured with same key.
  - If key is changed, it has to be changed on all of the devices that communicate over the network.

Initialization Vector

- WEP uses a 24-bit initialization vector (IV), which serves as a random "seed" to generate the authentication and encryption key.
- Two key sizes
  - 64-bit key consisting of a 40-bit key and a 24-bit IV.
  - 128-bit keys consisting of a 104- bit key and a 24-bit IV.
- WEP uses a flawed RC4 implementation .
- WEP shouldn't be used.

Don’t use WEP!

- Unless, you have too…
- Some legacy devices, particularly the older 802.11b devices, cannot use stronger, more modern authentication and encryption methods.
- For these devices, other compensating methods may be used, such as host-based data encryption or RAS with an EAP implementation.

WPA, Wi-Fi protected access

- Developed primarily by the Wi-Fi Alliance and other interested parties as a stop-gap to secure wireless networks while the IEEE worked on a standardized improvement to security.
- Uses passphrases to allow users to create longer, stronger pre-shared keys.
  - A WPA passphrase can be from 8 to 63 ASCII characters (which are case-sensitive), or 64 hexadecimal characters.
  - The actual passphrase is not the key; rather, it is used by the system to generate the 256-bit pre-shared key.
  - This is unlike WEP, which allows only 6 or 10 character passwords (depending upon the key size of 64 or 128 bits, respectively).

TKIP

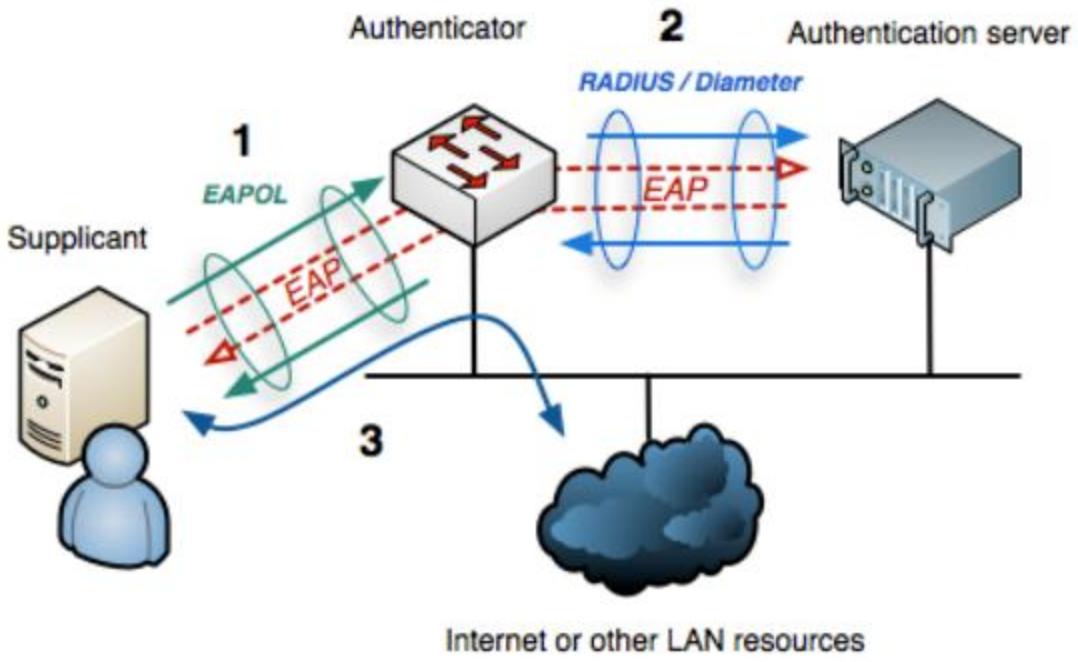
- WPA uses the Temporal Key Integrity Protocol (TKIP) to dynamically generate 128-bit keys on a per packet basis.
- In other words, every packet that is transmitted has a new 128-bit key.
- As implemented in WPA, TKIP uses a 48-bit initialization vector and an improved implementation of the RC4 stream cipher for backwards compatibility with WEP.

802.11i

- IEEE ratified the 802.11i standard in 2004, which is a formalized version of WPA and is called WPA2.
- WPA2 offers TKIP for backwards compatibility with WPA devices, but prefers AES (Advanced Encryption Standard) encryption as its default.
- WPA and WPA2 differ in encryption methods.
- WPA2 uses AES to implement the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) required as part of the 802.11i standard.
- WPA2 also uses TKIP for backwards compatibility with WPA and legacy devices that don't support AES.
- Other form of WPA is called WPA2-Enterprise allows authentication of both the user and the device or client they are communicating from.
  - Requires a specialized infrastructure.

802.1X

- EAP over LAN.
- Defines the encapsulation of the Extensible Authentication Protocol (EAP) over IEEE 802.



802.1X Terms

- Supplicant another name for a wireless client device.
- An authenticator is simply the wireless access point or wireless LAN controller itself.
- The third term is authentication server
  - Uses a remote access authentication protocol such as Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access-Control System (TACACS), or its Cisco-developed successor, TACACS+ to provide authentication and accounting services using an enterprise-level user database, such as Microsoft's Active Directory.

EAP

- While 802.1X is really a port-based protocol, it also serves as an authentication framework that allows other authentication protocols to be used in conjunction with it.
- Most common one is Extensible Authentication Protocol (EAP).
- EAP is the primary authentication protocol used with 802.1X networks.
  - Several EAP variations including EAP-TLS, Protected EAP (PEAP), EAP-MD5, EAP MS-CHAPv2, and others.
- Because EAP is extensible, it allows a wide variety of authentication methods, including username and password combinations or certificate-based (PKI) authentication.

Summary of wireless security technologies.

Wireless Security Technology	Protocols	Notes
WEP	RC4 streaming protocol	24-bit IVs, static keys that repeat. Easily broken.
WPA	TKIP	48-bit IVs, dynamic keys.
WPA2	AES-CCMP/TKIP	802.11i standard, backwards compatible with WPA.
802.1X	EAP	Port-based authentication framework; used for WPA/WPA2-Enterprise.

Table 5-4 Summary of Wireless Security Technologies

Site Survey

- Effort to understand the environment for purposes of determining capacity, coverage, and growth of the network, while also determining any factors that may interfere with the effective network operation, such as radio interference and other environmental factors.
- Typically performed before implementation.
  - Also useful to monitor the growth and performance of network.
  - Ensure that the installation stays optimized.
- Elements to be considered:
  - Location
  - environment and physical considerations
  - interference from other devices
  - Numbers of users and devices, bandwidth
  - Other factors.

Preparation: Key to successful survey.

- Gathering information including:
  - business model of the organization
  - details of the site and environment
  - security documentation
  - how it will integrate into an existing network, and so forth.
- Why the customer wants the network?
  - For example, a business that is devoted to manufacturing will have different needs than one specializing in storing inventory in a warehouse.
  - A coffee shop or bookstore will have different needs than a medical clinic.

Gathering Information

- You may have to interview the customers and also request documentation artifacts from them, such as blueprints or floor plans, business plans, security plans and procedures, and so on.
- You also may have to look at public sources of information, such as weather patterns and utilities usage.
- In addition to experts on wireless technologies, you also may have to include people knowledgeable with building codes and construction, electricity and electrical systems, security, and network systems on the survey team.

Capacity Considerations

- Refers to the ability of the wireless network to handle increasing numbers of users and devices as well as the workload put on the wireless network.
  - How many users?
  - How many devices?
- What kind of technologies each device incorporates, such as 802.11a/b/g or n.
- Number of users and devices expected to grow over the next year or two?

Capacity: Applications

- emailing and web surfing?
- Any business-unique applications that must send data across the network?
  - Inventory or job scheduling information?
- How much bandwidth does data consume?
- Will users be transferring or sharing large files?
- Performance requirements?

Coverage Factors

- Typically addresses specific areas within the facility or organization.
  - Distances between the access points and the clients;
  - Signal strength and quality between those clients and access points
  - Transmit and receive power
  - Bandwidth.
- For example, in a warehouse, wireless devices such as barcode readers may require coverage from one end of the warehouse to another.
- Wireless lap-tops and tablets in the office areas require coverage as well, but this could be from a different access point that operates on an different network segment.

Coverage Factors

- Distance between devices
- Objects such as walls, machinery, furniture, and other items that may block RF signals.
- Placement of wireless access points.
- Electrical interference and other environmental factors.
- Amount of power that an access point and device transmit with can affect coverage area as well.
- Saturation of users and devices within the coverage area.
  - If the capacity of a given coverage area is exceeded, users may experience slow response times and inadequate signal strength.

Access Point Placement

- Consider multiple access points, especially in larger facilities.
- Consider power levels on the access points.
- Higher power levels may mean greater coverage, but this has to be balanced with security as well because higher power outputs mean that the wireless signal may be more easily intercepted.
- Access point placement should be carefully considered to optimize coverage, as well as provide security for these devices.

Access Points

- An access point shouldn't necessarily be placed near an outer wall, as this affects both coverage (distance to the opposite side of the facility) and security (eavesdroppers may be able to pick up the wireless signal outside of the facility).
  - Access points may need to be placed more centrally within the facility at designated areas and within certain distances of each other.
- Should be placed away from potential interference sources such as break rooms (potential interference from microwave ovens), electrical devices and outlets, machinery and manufacturing equipment, and other high interference areas.
- Should also be placed so they are not easily accessible by unauthorized personnel.

Testing

- To check and verify RF coverage, you should test RF reception in several different areas of the facility.
- For example, you may want to check coverage in different office areas, the warehouse, production areas, within secure areas, and even outside the building to see how much wireless signal leakage there is beyond the walls of the facility.
- When you test coverage in these various areas, try to test the RF transmission and reception under heavy load conditions.
  - Use typical applications that the organization and its users may use, especially ones that require large amounts of bandwidth, such as file sharing and streaming.
- Test load in different locations from multiple devices and users.
- Test signal strength.
- Record each items as well within each coverage area you test.

Signal Strength

- Refers to the strength of the transmission power from the transmitting device.
- Various factors affect signal strength.
- Transmit power, however, is one consistent way of discussing signal strength with wireless devices.
- On some devices, the transmit power can be set in its configuration utility, but this can be limited due to restrictions placed on the device by the manufacturer, or even restrictions imposed by local laws.
- Another factor affecting signal strength is the type of antenna used.
- Signal strength is typically measured by the distance from the transmitter, and can be viewed in most devices in terms of dB-millivolts or dB-microvolts per meter.

Receive Signal Strength

- Refers to the amount of power received from a wireless transmission.
  - Influenced by the power of the transmitter, obviously, but also by radio frequency noise in the area.
  - RF noise could be from other transmitters, electrical interference, blockage by solid objects…
- Signal-to-noise ratio (or SNR) describes the difference between the received signal and the noise level.
  - Measured in dB
  - Can be calculated by subtracting the received signal (in dBm) from the noise (also in dBm).
  - For example, if the received signal is –70 dBm, and the noise is –90 dBm, then the SNR value is 20 dB.
  - Typical SNR ratios for wireless networks are from around 20 to 25 dB.
- Some wireless devices have what's called a received signal strength indicator (RSSI) that shows a value for the receive signal strength.
  - Sometimes this is an arbitrary value assigned by the device itself.

Interference

- Can come from devices that may use frequencies near the wireless network.
  - May include cordless telephones, Bluetooth devices, industrial equipment such as manufacturing machinery, radar systems, and microwave ovens.
  - Machinery or powered equipment can also generate non-wireless interference.
- Methods are used to find interference include spectrum analyzers.

Wireless interference

- Can come from other 802.11 wireless networks and devices that operate in either the ISM or UNII frequency bands.
- One type of interference is called co-channel interference.
  - Usually results from other devices that occupy and use the same channel.
- Other type of interference is called adjacent channel interference.
  - Refers to other devices on overlapping channels.
- Spectrum analyzer can help determine source of RF interference.

Spectrum Analysis

- Term that is used to describe examining different RF characteristics to determine signal strength, interference and noise, signal-to-noise ratio, frequency usage, and other factors.
- A spectrum analyzer is a device, or software used with a device, that can show the various RF characteristics for given frequencies and channels.
  - From a technical perspective, the spectrum analyzer measures the magnitude of an input signal versus its frequency.
  - The spectrum analyzer can give you a visual representation of how the physical radio frequency usage appears.
- Spectrum analyzers can be dedicated devices, or they can be a software package.
- Several popular spectrum analyzers available, with some of the dedicated devices and enterprise-level software packages coming from vendors such as Cisco, Fluke Networks, SolarWinds.
- There are also open source or freeware analyzers available.

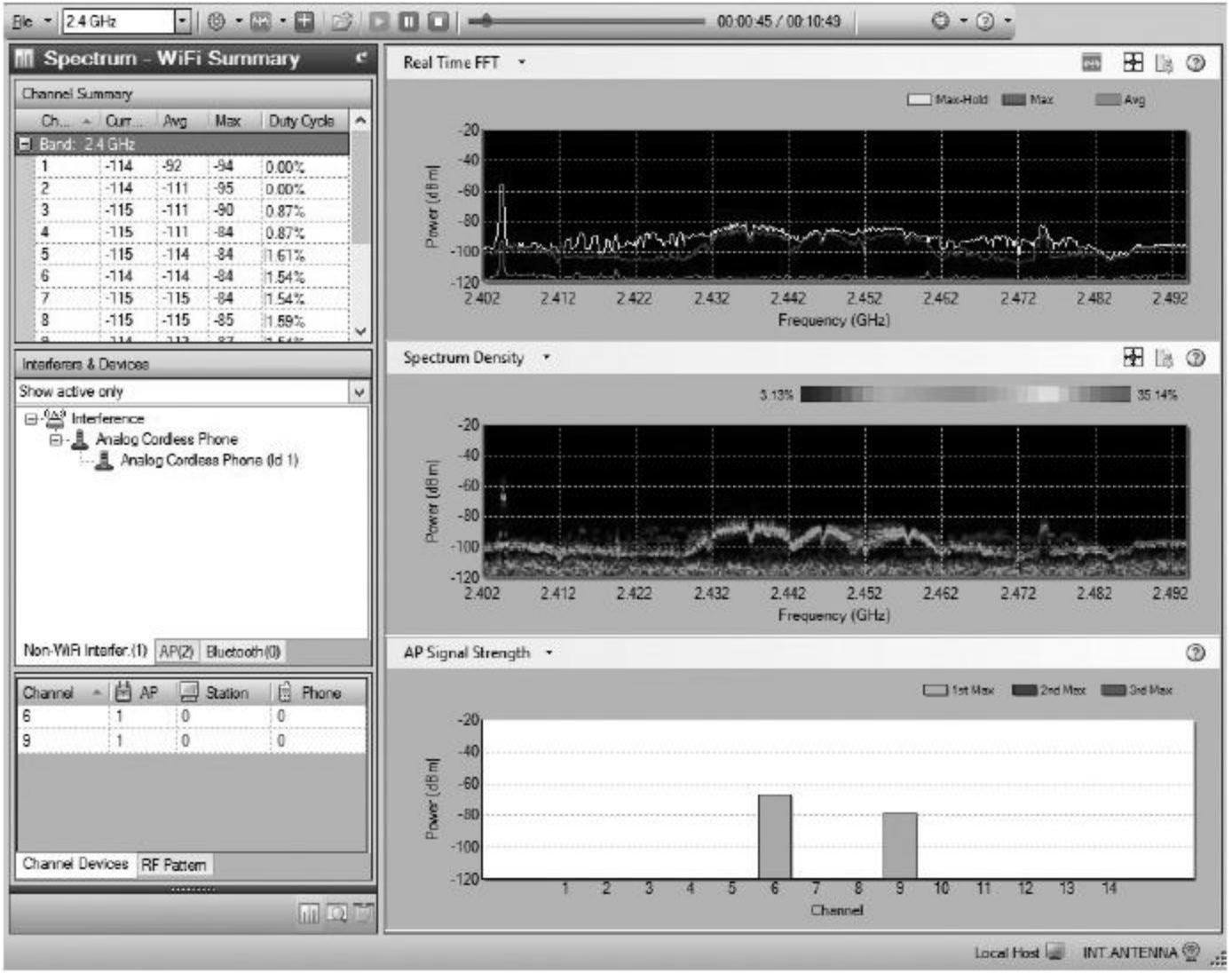


Figure 5-15 A software spectrum analyzer from Fluke Networks

Site Survey Report

- Includes analysis of the wireless capacity, coverage, interference, signal strengths at various locations within the facility, and environmental factors (obstacles, machinery, and so on) that could affect the network.
- Should also offer a solution for the network, in the form of network and facility diagrams laying out the proposed placement of access points, power settings, and even the recommended vendors and models for the equipment.
- Security recommendations, in concert with the organizations existing security policies, procedures, and infrastructure, should also be presented.
- Usually a site survey is performed by several experienced individuals who have both the broad-based knowledge of wireless networks, RF principles, and general networking, as well as the specialized training on the possible solutions that may be required.

Post Site Survey

- After the site survey is accomplished, the solution is developed, refined, and eventually implemented.
  - Important that the documentation for the network be maintained in as current a state as possible.
- The site survey documentation and site map should be updated to reflect how the solution was actually implemented.
  - Over time the network may need to change and grow.
- Site survey documentation/site map will be invaluable when that happens because surveys may be conducted again to accommodate this new growth.
- Additionally, architecture documentation, equipment inventory information, application, security, and performance information all need to be collected, maintained, and updated as the network changes.

Questions???