Post 1

Thursday, January 24, 2019 11:40 PM

WLAN – NETWORK TYPES: REVIEW

Common networking types in use today:

LAN	Local Area Networks
WAN	Wide Area Networks
MAN	Metropolitan Area Networks
CAN	Campus Area Networks
PAN	Personal Area Networks

LAN: Local Area Network: A group of computers connected by a physical medium in a specific arrangement

Common topologies:

Bus	**Ring**	**Star**	**Mesh**

Common uses of early LAN's:

- File/Print services (shared printers): Stored data securely
- Centralized location of data for accessibility
- Ability to back up/archive saved data (disaster recovery)

WAN: Wide Area Network: Mostly point-to-point or point-to-multipoint connections between 2/more LAN's

- Large geographic areas: Can use leased lines from telecommunications providers (telcos), fiber/wireless
- Wireless for bridging LAN's growing b/c cost-effective

Point-to-Point Connections	▪ When at least 2 LAN's are connected together | Wired/wireless ▪ Includes: Bridges/wireless AP's/routers WLAN point-to-point: Links can extend very long distances Wired point-to-point: Fiber-optic connections/leased lines from local telco providers Wireless point-to-point: ▪ Typically semi-directional/highly directional antennas ▪ Directional antennas/encryption to protect wireless data as it propagates through air Point-to-multipoint link: ○ *Regulatory domains:* FCC (Federal Communications Commission) ○ When omnidirectional antenna used in this config: Considered special case
Point-to-Multipoint Connections	○ Infrastructure connecting more than 2 LAN's together ○ When used w/wireless: 1 omnidirectional/multiple semi-directional/highly directional antennas ○ Often used in campus-style deployments: Connections to multiple buildings/locations ○ Often called "clouds" ○ Like point-to-point: Can use either direct wired connections (fiber/leased line from telco's)

MAN: Metropolitan Area Network: Networks that can span entire cities

- Interconnects devices for access to computer resources in an area larger then LAN's | smaller than WAN's
- Fast connectivity between local networks (may include fiber/wired): Capable of longer distances/higher capacity than LAN
- Connections to outside larger networks such as Internet: Services like: Cable TV/streaming video/phone

- May be owned by town/county

CAN: Campus Area Networks: A set of interconnected LAN's: Smaller version of WAN w/in office/campus

- Limited geographical area
- Each building of campus | Separate LAN: Often connected using fiber (bigger distance than copper using IEEE 802.3 Ethernet)
- Common way to connect individual LAN's: Cost effective
- May link many buildings (School of Business/Law/Engineering/Library/etc..)
- Number of wireless AP's/capacity of each need to be considered

PAN: Personal Area Networks: Connects devices w/in immediate area of individuals | Wired/Wireless/both

- Wired: Includes USB devices (printers/keyboards/mice)
- Wireless: Short-range networks/Bluetooth (IEEE 802.15)
- Commonly used in for personal accessories (phones/headsets/tablets/etc)

Network Topologies: Topology: Layout/physical design of a network: Includes cabling/devices part

Bus: Multiple devices connected along single shared medium w/2 defined endpoints | LEGACY

- AKA High-speed linear bus | Single broadcast domain | All devices receive all msgs
- Both endpoints have a 50 ohm termination device
- Usually **Bayonet Neill-Concelman (BNC)** connector w/50 ohm resistor

Disadvantages:

- Any point along cable damaged? Entire LAN goes down
- Troubleshooting: Half-split method | Engineer "breaks"/separates link at about halfway point
- Measures resistance on both ends: If segment @50 ohms: Good chance that side of LAN functions
- If not: Signals problem w/that part LAN segment: Rinse & repeat till exact location found

Ring: Each device connects to 2 other devices: Forms a ring

- Rarely used w/LAN's: Still used by ISP's for high-speed resilient backhaul connections over fiber
- May use token-passing access method: Data travels around ring in 1 direction
- Only 1 device at time transmits data: No collision detection
- Commonly outperforms bus: Higher data rates than possible using collision detection access method
- Each machine on ring can act as repeater (allows for stronger signal)

Star: Multiple devices connected by central connection device

- Most commonly used method today
- Common central connection devices (switches/wireless AP's): Single broadcast similar to bus
- Switch/wireless AP have intelligence: Ability to decide which port specific network traffic can be sent to

Advantage over bus/ring:

- If connection breaks: Entire network not down: Only device affected
- Central connection device can be considered potential point of failure

Mesh: Each device has 1/more connections to other devices part of mesh

- Network resilience in case of link/device failure | Cost savings | Wired/wireless
- Amendment to IEE 802.11 standard for mesh is 802.11s
- Ratified in 2011 | Now IEEE 802.11-2012 standard
- Proprietary L2 routing protocols | Form self-healing wireless infrastructure

OSI Model: The Open Systems Interconnection Model: Basic concept of communications in networks

All	**Application**	Layer 7
People	**Presentation**	Layer 6
Seem	**Session**	Layer 5
To	**Transport**	Layer 4
Need	**Network**	Layer 3
Data	**Data Link**	Layer 2
Processing	**Physical**	Layer 1

Layer 1 -Physical	▪ Bit-level data streams/HW connecting devices together Includes: NIC's/cables/switches/wireless AP's/bridges **Wireless networking:**

	▪ RF: Radio frequency uses air as medium for wireless **2 sublayers**: • **Physical Layer Convergence Protocol (PLCP):** Higher of 2 layers: Int bet PMD/MAC sublayer • **Physical Medium Dependent (PMD):** Lower sublayer at bottom of protocol stack ○ Responsible for transmitting data onto wireless medium
Layer 2 – Data Link	▪ Organizes bit-level data for communication between devices on network ▪ Detects/corrects Physical layer errors Consists of 2 sublayers: • **Logical Link Control (LLC)** • **Media Access Control (MAC):** Bit-level communication accomplished though MAC addressing ○ A unique ID/logical address assigned to network device [physical address]
Layer 3 – Network	Where IP resides: Addressing/routing data IP is defined as a numerical ID/logical address assigned to a network device
Layer 4 – Transport	**Transmission Control Protocol (TCP)**: • Connection-oriented for communications requiring reliability **User Datagram Protocol (UDP):** • Connectionless for simple communications requiring efficiency
Layer 5 – Session	Opens/closes/manages sessions between end-user application processes
Later 6 – Presentation	Provides delivery/formatting of info for processing/display
Layer 7 – Application	File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), Post Office Protocol v3 (POP3), etc…

Wired: Cables/repeaters/bridges/L2 switches
Wireless: Access points/bridges/repeaters/radio frequency/open air
Peer Communication: Peer layers communicate w/other peer layers & layers underneath are support systems

- Horizontal link between devices on network

Device Addressing: Every device requires unique ID: Can be done one of 2 ways:

1. **Physical addresses:** MAC address
2. **Logical addresses:** IP address

Post 2

Thursday, January 24, 2019 11:41 PM

WIRELESS LAN NETWORKS (CH.2)

Wireless networks: Types of topologies:
WPAN: Wireless Personal Area Network
WLAN: Wireless Local Area Network
WMAN: Wireless Metropolitan Area Network
WWAN: Wireless Wide Area Network

WPAN	**PAN:** Connects devices w/in immediate area of individuals • Users connect various devices wirelessly to their PAN Example: Keyboards/mice/headsets **Bluetooth**: Most popular type of WPAN • **FHSS: Frequency Hopping Spread Spectrum** used • Under IEEE 802.15 standard (specifies WPAN) • **2.4 GHz ISM: Industrial Scientific/Medical** band **WPANs: May use infrared:** • Near visible light in 850nm-950nm range for communication • Specified: Original 802.11 standard (obsolete)
WLAN	**LAN:** A group of computers connected by a physical medium: WLAN: Same description (no wire) • Same physical area: Bound by building perimeters: Long existence • Either licensed/unlicensed RF: Radio Frequency spectrum Common frequency spectra: • **Unlicensed 2.4GHz ISM band** • **Unlicensed 5GHz UNII band** ○ **UNII:** Unlicensed National Information Infrastructure
WMAN	**MAN:** Consists of networks that may span entire cities/interconnects them for resources • Larger than LAN's || Smaller than WAN's • IEEE 802.16 standard: Developed to address this type of network • May fall under WiMAX category/addresses diff tech ○ **WiMAX: Worldwide Interoperability for Microwave Access**
WWAN	**WAN:** Consists of point-to-point/point-to-multipoint connections bet 2/more LAN's • Can extend very long distances through use of fiber/leased lines from telcos • Extend beyond the point of connecting LANs together • Encompasses very large geographical areas • May include different wireless tech (like cellular)

Common WLAN Deployment Scenarios

- SOHO: Small Office |Home Office
- Enterprise: Corporate data access/end-user mobility
- Extension of existing networks to remote locations
- Public wireless hotspots
- Carpeted office
- Industrial
- Healthcare
- Last-Mile data delivery: Wireless ISP
- High-density: Municipal/law enforcement/transportation

Site survey: Helps determine areas of RF coverage, interference, number and placement of AP's.

SOHO	Many same needs as larger businesses: Remoting in **Good to do a site survey:** • Helps know other wireless networks/devices in area • Anything that may cause RF interference
Enterprise	Used in wired LAN's for decades: Interoperability/security • Extensions w/wired wasn't always feasible (too costly)

	• New advancements: Deployments growing fast • Workstations/printers/barcode scanners/voice headsets/location services • Cost decreased: Speed/sec/performance increased • Cost savings over Ethernet enormous Only option in some cases
Extensions	Early days: Wireless deployed as extension of wired • Some users needed access farther than 100 meter limit of IEEE 802.3 (Ethernet) • Fiber/leased lines not always logical • This became an alternative
Hotspots	Provides portability/mobility: Major benefits **Wireless hotspot**: Location that offers wireless for free/for-profit public • Allows variety of mobile devices to connect/access public/private Internet/network **Captive portal**: Page that lists terms/conditions usr has to agree to prior to accessing Internet on hot spot Can raise security concerns for user: • All info passed in clear txt through air via RF • Could allow attackers to capture usrnames/passwds/CC #'s/other info • Most hotspots don't have capability to provide secure wireless from user's device Extra measures should be implemented by users **VPN: Virtual Private Network:** Allows secure encrypted connection for user from hotspot to network • Creates secure tunnel between user/hotspot
Carpeted Office	Upgrading copper wiring/installing new wired drops can cost a lot • Common to connect 20-25 usrs/devices to single AP • Max size depends on SW apps/# of devices connected Benefit to 802.11: AP will require only single Ethernet drop to support all devices/usrs Access Point: A shared medium for everything that connects wirelessly • Performance/throughput can be issue if proper design isn't used
Educational	School buildings may pose concerns w/wireless deployments • Brick/concrete walls • Lath/plaster walls • Inconsistent material (from building additions) • RF may not propagate well depending on density/composition of building materials • Potentially adding AP's/extra design considerations Location/distance from main building should be taken into consideration: • Point-to-multipoint connection/line of sight Some institutions have a "one-to-one" initiative: • 1 Internet-accessible device for every 1 student • Possible density concerns b/c of high # of students in classroom
Industrial	Been using WLAN for years before IEEE 802.11 • Barcode/scanning solutions for manufacturing • Warehousing/inventory/retail Many businesses have the following characteristics: • High ceilings • Tall storage racks • Large inventory of product • Forklifts Can cause issues w/wireless b/c of the way RF propagates • High ceilings: Various antennas need to be tested/coverage verified throughout facility • Tall storage racks: May have varying levels of inventory/product: Poor propagation Depends on what products made of: Direct RF behavior impact • High density of water/paper products will absorb RF Forklifts need to be outfitted w/wireless barcode scanners/mobile devices in many cases RF site survey highly recommended to ensure proper coverage
Healthcare	One of the fastest growing sectors today in the US • Poses many challenges for design/deployment/support for wireless

	• Hospitals run 24/7/365 WLANs have numerous apps including: • Patient registration/charting • Prescription automation • Treatment verification • Inventory tracking • Electronic medical records • Location services • Electronic imaging Hospitals use many devices that operate in unlicensed ISM RF band • Can create challenges for design/reliability Other potential issues: • Building materials that hinder RF propagation • Lead-lined walls used in radiology (protects people from X-Rays) • Identical floor layouts above/below: Leads to stacking AP issues • Limited accessibility to areas such as surgery/patient care rooms • Aesthetics of installed equipment Compliance w/HIPAA (Health Insurance Portability/Accountability) Act of 1996: • Needs to be taken into consideration
Last-Mile Data	**Last-mile data delivery:** Telco term: Used to describe connection from provider to endpoint • Example: Home/business (not necessarily mile in distance) Can be costly solution in many apps: • Each endpoint needs separate physical connection • Wireless provides more cost-effective solutions for last-mile data delivery Some communication tech (DSL): • Physical limitations that prohibit connections in some cases May not be cost effective in some rural areas: • WLANs can service areas that may not be part of a last-mile run Things to consider: • Feasibility • Line of sight/obstacles • RF interference
High-Density	**"High-density WiFi deployment" means?** • Differing opinions (subjective) • Some claim in next few years # of installed devices will exceed # of installed wired devices • Average person: May have 1-5 separate wireless devices Issues to consider: • Frequency band to use • Co-channel interference • Cell-sizing • AP capacity
Municipal	Valuable tech in industrial/municipal/law enforcement/transportation networks Federal/local law enforcement agencies frequently maintain state-of-the-art-tech • Utilizing forensics/WLAN • Tech that uses 19.2 Kbps becoming obsolete b/c of slower rates • Police/fire/utilities/city/services often all connected to common WLAN Transportation networks: No exception: • WLAN installs becoming common in buses/trains/airplanes/cars • Users can connect free/pay a fee

Building-to-Building Connectivity Using WLAN Tech:

- **WLAN:** Often used as alternative to copper/fiber/leased lines between buildings
- Antenna selection: Important role

Wireless Point-to-Point

Point-to-point: Connecting at least 2 wired LAN's together

Wireless point-to-point: Can provide long-range coverage depending on terrain/local conditions

- Semidirectional/highly directional antennas
- **Special case:** Omnidirectional antenna used in this config (point-to-multipoint connection)

- Correct antenna selection is impt

Point-to-Multipoint: Connects 2/more LAN's together

Wireless: Config usually consists of 1 omnidirectional and multiple semi/highly directional antennas

- Often campus-style deployments
- Becoming more common b/c low cost of equipment/ease of install: Can be a few hours

RF Regulatory Domain Governing Bodies/Local Regulatory Authorities

Wireless networks use RF to communicate

- RF spectrum needs to be regulated to ensure correct use of frequency bands

Global: The ITU-R: International Telecommunication Union-Radiocommunication Sector

- Responsible for global management of RF spectrum in addition to orbits
- Currently: 191 member states || Over 700 sector members

Manages 5 regions:

- Region A: (North/South America/Inter-American Telecommunication Commission [CITEL])

ITU-R Regions:

Region	Location	URL
Region A	America	citel.oas.org
Region B	Western Europe	cept.org
Region C	Eastern Europe/Northern Asia	en.rcc.org.ru
Region D	Africa	atu-uat.org
Region E	Asia/Australia	aptsec.org

FCC: Federal Communications Commission

Local regulatory authority: US: FCC: Founded 1934

- Responsible for regulating licensed/unlicensed RF spectrum
- IEEE 802.11 may use licensed/unlicensed frequencies for communication between devices

Benefit of unlicensed radio spectrum? No cost to the end user

IEEE commonly uses 2 of 3 unlicensed RF bands allowed by the FCC:

- **2.4 GHz ISM**
- 5 GHz UNII

Licensed RF Bands used w/IEEE 802.11: 2 additional licensed bands can be used:

- **3.650 – 3.700 GHz band**
- 4.940 – 4.990 GHz public safety band

2008: IEEE ratified 802.11y standard: Allows use of high-powered WLAN equipment to operate in 3.650-3.700 GHz band

- W/in US this licensed band requires user to pay some type of licensing fee

IEEE 802.11-2012 standard specifies use of 4.940-4.990 GHz public safety band in US:

- Consists of 5 MHz, 10 MHz, 20 MHz wide channels w/both high/low power limits

Europe: ETSI: European Telecommunications Standards Institute: Produces standards for info/comm tech

Includes: Mobile/radio/converged/broadcast/Internet tech

- Created by EU **CEPT: Conference of Postal and Telecommunications Administrations**: 1988

IEEE/WLAN Standards

IEEE: Institute of Electrical and Electronics Engineers: Eye triple E: Non-profit org

- Generates a variety of standards: Largest tech pro society
- Since 1997: Has released series of standards related to WLAN

802.11	**Released: 1997: Initially defined WLAN comm standards** • Data rate in original slow today (1/2 Mbps) • **2.4 GHz ISM band** • **FHSS: Frequency hopping spread spectrum** • **IR:** Infrared • 1 and 2 Mbps FHSS: Considered legacy: Used in other tech like:

	• 802.15 Bluetooth • **PSTN:** Wireless cordless public switched telephones/network telephones
802.11a	**Rates: Up to 54 Mbps using OFDM** • **5 GHz UNII band** • **5.150 – 5.250 GHz UNII-1** • **5.250 – 5.350 GHz UNII-2** • **5.725 – 5.825 GHz UNII-3** • **OFDM: Orthogonal Frequency Division Multiplexing** • **6/12/24 Mbps OFDM** required data rates • **9/18/36/48/54 Mbps OFDM** rates supported/not required ○ Benefits: Less interference with UNII band (not all devices support it)
802.11b	**Backwards compatible to 802.11 DSSS for 1/2 Mbps** • **2.4 GHz ISM band** • **2.4 GHz – 2.4835 GHz** North America/China/Europe (NOT Spain/France) • **DSSS: Direct Sequence Spread Spectrum** • **HR/DSSS: High Rate-Direct Sequence Spread Spectrum** • **5.5** and **11** Mbps
802.11g	**Addresses extended data rates w/OFDM tech** **Backwards compatible 802.11/802.11b** • **2.4 GHz ISM band** • **2.4 GHz – 2.4835 GHz** North America/China/Europe (NOT Spain/France) • **DSSS** • **HR/DSSS** • **ERP-OFDM: Extended rate physical**-Orthogonal Frequency Division Multiplexing • **PBCC: Packet Binary Convolutional Code:** Optional • **1 and 2 Mbps** (compatible w/DSSS) • **5.5 and 11 Mbps CCK: Complementary Code Keying** (compatible w/HR/DSSS) • **6/12/24 Mbps OFDM required data rates** • **9/18/36/48/54 Mbps OFDM data rates supported but not required**
802.11n	**Amendment approved: 2009** • Allowed opportunity to move forward w/new LAN equipment/tech • Better throughput/performance WiFi certified devices draft 2.0: Avail for 7 years prior to ratification • **2.4 GHz ISM band** • **5 GHz UNII band** • **MIMO: Multiple-input multiple-output technology** • **PHY:** Physical layer enhancements • **MAC:** Data Link Layer enhancements • **Data rates up to 600 Mbps** **MIMO: BIG part of why standard is great** Prior to n: a/b/g devices used single radio to transmit/receive signals • **SISO: Single-Input Single-Output** **MMO: Multiple radios or "radio chains" to transmit/receive radio signals** • SISO systems were subject to **multipath** **Multipath:** • Several wave fronts of signal would be received out of phase because of reflections **MIMO uses reflections to enhance performance/throughput w/several radio chains in n** Consists of 7 types of new tech like: • **TxBF:** Transmit beamforming • **MRC:** Maximal Ratio Combining • **SM:** Spatial Multiplexing • **STBC:** Space Time Block Coding **Enhancements to physical layer include:** • 40 MHz channels through channel bonding • More subcarriers for higher rates • Optional short guard intervals to provide more potential throughput • Varying modulation types for rates of up to 600 Mbps

	MAC sublayer of Data Link also provides enhancements that include: • Frame aggregation for less 802.11 overhead • Block Acknowledgements (block ACKs) • **RIFS:** Reduced InterFrame Spacing • **SMPS**: Spatial Multiplexing Power Save to help conserve battery life • **PSMP:** Power Save Multi-Poll for devices enabled for QoS

Summary of 802.11 communication standards/amendments

Details	**802.11**	**802.11a**	**802.11b**	**802.11g**	**802.11n**
2.4 GHz ISM band	**Yes**		**Yes**	**Yes**	**Yes**
5 GHz UNII bands		**Yes**			**Yes**
FHSS	**Yes**				
DSSS	**Yes**		**Yes**	**Yes**	**Yes**
HR/DSSS			**Yes**	**Yes**	**Yes**
OFDM		**Yes**			**Yes**
ERP-OFDM				**Yes**	**Yes**
HT-OFDM					**Yes**
1/2 Mbps	**Yes**		**Yes**	**Yes**	**Yes**
5.5 and **11** Mbps			**Yes**	**Yes**	**Yes**
6/9/12/18/24/36/48/54 Mbps		**Yes**		**Yes**	**Yes**
Up to **600** Mbps					**Yes**

Post 3

Thursday, January 24, 2019 11:41 PM

WIRELESS LAN INFRASTRUCTURE DEVICES (CH.3)

Wireless Access Point: AP: Allows variety of devices to access any network resources the device/user has perms for
3 Common types:

1. **Autonomous:** Self-contained units: Function as independent network infrastructure devices
2. **Controller-based**: Function in conjunction w/WLAN controller
3. **Cooperative:** Provides wireless infrastructure w/out use of a HW controller

AP provides: PC's/Wi-Fi phones/tablets/Devices access to LAN using RF comm mechanism through free space (air) as medium

Infrastructure mode	**When wireless device is connected to AP** • All data is passed through the AP to intended destination • Can act as standalone device: Config independently to allow devices to connect • Can act as part of larger wireless network: Shares some of same configs like SSID **SSID: Service Set Identifier:** Logical name/identifier all devices connected to AP share
Access Points	**Half duplex**: 2-way comm only happens in 1 direction at time • Less throughput for connected device A device that can connect to a **DS: Distribution System** • Ethernet segment/cable: Allows wireless usrs to access network Considered stations (STA)

Autonomous AP:
Self-contained unit w/intelligence to provide devices w/wireless access to wired network devices w/perms to use them
2 Types of autonomous AP's:

1. SOHO
2. Enterprise

SOHO AP: Small Office/Home Access Point

SOHO AP	Less extensive feature set than enterprise-grade • Now supports highest standards-sec options (WPA 2.0) • Limited # of connections for PC's/devices **Features:** • IEEE 802.11 standards support • Wi-Fi Alliance certifications • Removable antennas • Static output transmit power • Advanced sec options • Wireless bridge functionality • Wireless repeater functionality • DHCP server • Config/settings options **802.11 Standards Support** • Most later-model's support 802.11: Others need firmware updates • Support will vary on factors (cost/complexity) • Common: Support **802.1b/g/n** • Dual-band AP: Both **802.11a/n** and **802.11b/g/n** NOT as common • Cost higher than single-band 802.11b/g/n **Wi-Fi Alliance Certifications: Common:** WPA/WPA2.0/WPS **||** WMM/WMM-PS for QoS **Removable Antennas:** • Some equipped w/removable antennas • Allows end user to change to larger/higher-gain antenna: Allowing RF to cover wider area • Connecting smaller/lower-gain antenna will decrease coverage

	Static Output Transmit Power • Occasionally: The ability to adjust transmit output power in SOHO AP • If available: Settings are basic (low/medium/high) • **Enterprise AP**: Can change the power in increments of mW or dBm **Cell:** Transmit output power that determines the area of RF coverage • Typical output power of SOHO is 15dBm or 32 mW (varies) • Models w/static output power can't be adjusted: Limits ability to decrease/increase size of RF cell • Only way to change cell size is to change gain of antenna in removable antenna models Replacing antenna changes vertical/horizontal beamwidths/radiation pattern that propagates away from it **Advanced Security options:** Provides more features: 802.1X/EAP || VPN pass-through **Wireless Bridge Functionality:** Occasionally config'd in wireless bridge mode • Point-to-point/point-to-multipoint settings available • Enables admins to connect 2/more wired LANs together wirelessly **Wireless Repeater Functionality:** • Some can be config'd to function as wireless repeaters • Enables admins to extend size of RF cell: Devices not in hearing range of AP can connect to wireless • Reduced throughput for other devices accessing network through a repeater **Config/Setting Options:** • Config via web browser (HTTP/HTTPS) • Rarely offers CLI • Best to config from wired side of network whenever possible
Enterprise AP	Much more extensive features **Features:** • IEEE 802.11 standards support • Wi-Fi Alliance certifications • Removable/expandable antennas • Adjustable output transmit power • Advanced sec options • Multiple operation modes: Root AP/wireless bridge/wireless repeater capabilities • GUI/CLI config • Outdoor use • Plenum/industrial environment ratings • More memory/faster processors **802.11 Standards Support** • Supports all communication standards by utilizing **802.11a/n** and **802.11b/g/n** dual-band radios • Can include support for amendments not supported by SOHO Example: 802.11e QoS, Wi-Fi multimedia, 802.11r fast BSS transition (FT) Example: 802.11w security of management frames **Removable/Expandable Antennas:** Removable/expandable antenna capabilities • Omnidirectional/Semidirectional/highly directional antennas common • Some use internal antennas: Offers options for connecting externals if needed **Adjustable Output Transmit Power:** Ability to adjust output transmit power/Can adapt to environment **Advanced Security options:** 802.11i WPA/WPA 2.0, passphrase, 802.1X • **RADIUS: Remote Auth Dial-In User Service** authentication included ○ Allows small/medium businesses to provide own advanced auth features ○ W/out need of external RADIUS authentication services ○ Reduces cost/lowers overhead • **WIPS: Wireless Intrusion Prevention System** ○ Helps determine/has potential to mitigate certain lvls of wireless attacks on network Example: Detection of rogue AP **Multiple Operation Modes:** Enterprise typically have 7 operation modes

Root AP Mode	Wireless Bride Mode	Wireless Repeater Mode

Root AP mode: AKA: Default operation mode

- Connecting AP to a **DS: Distribution System:** Like an Ethernet segment
- **WDS: Wireless distribution system**
- Allows devices to connect to AP/use network based on assigned perms of user/device

Wireless Bridge Mode: Connecting LANs together

- Allows AP to be set in bridge mode for wireless point-to-point/point-to-multipoint configs
- Connects 2/more LANs together
- Benefits: Cheaper/high data transfer rates compared to other options

Wireless Repeater Mode: Extends RF cell

- Allows devices outside of radio hearing range to connect to network via wireless repeater

AP config methods: Can be config or "staged" 2 ways:

1. GUI: Web browser (HTTP/HTTPS)
2. CLI: More extensive/detailed config options: May perform tasks GUI won't

Controller-Based AP: Differ from autonomous AP's: Used w/WLAN controllers NOT as standalone devices

- Shifts most intelligence to wireless LAN controller
- Lower intelligence == Lower cost
- Centrally managed from WLAN controller
- Layer 3 VPN connectivity

Cooperative AP: AKA "Controller-less architecture" Provides alt for deploying WLAN infrastructures

- Intelligence pushed back out/distributed to AP edge
- Similar to autonomous AP but much more intelligence/capabilities
- Managed through "cloud" software config tool: Eliminates need for HW controller
- Can be accessed from any computer

Benefits: Reliance on cloud server | No need for expense of HW controller

- Scalable/Performs well w/out relying on tunnel to be built from AP to a controller
- Distributed intelligence: Allows cooperative AP to make decisions about how frames traverse both wired/wireless network
- Some manufacturers provide variant of cooperative tech:
  - □ They allow autonomous AP's to be "adoptable" by a controller

Site survivable: AKA adaptive AP: Will still be able to function standalone should connectivity w/controller is lost

Wireless Mesh: All nodes connect together w/at least 2 paths for every node

- Allows for reliable comm in event of device/path failure | Popular in outdoor market
- Most outdoor mesh devices provide high lvls of sec | Inside enclosure to protect them

Examples where wireless mesh networks are utilized:

- Metropolitan
- University campuses
- Public Safety
- Transportation
- Government
- Amphitheaters

Indoor deployments still in testing phase:

- Use both unlicensed bands for mesh operation
- Use 2.4 GHz ISM band for device access and 5 GHz UNII band for mesh device connectivity
- Use of 3rd radio may be an option | Can be used in event of Ethernet loss to AP
- Some cooperative AP's auto mesh when they suffer an Ethernet loss

Wireless LAN Router

Wireless Residential Gateway: SOHO broadband routers usually have w/internet port/several ports for eth0 switches/wireless AP

- Config'd through web browser | Simple | Many same features as SOHO AP
- Most cases: Broadband router connects to ISP: Able to accept wired/wireless connections for PC's/devices

Features	NAT: Network Address Translation	DHCP Server	IP routing	DNS services	Firewall

Wireless Branch Router Can be used to extend corporate network to remote location using WAN/Internet

Typically 3 interfaces available:

1. Eth0 ports to connect to LAN
2. Internet port to connect to WAN or Internet

3. Wireless port to allow 802.11 devices to connect to network through wireless

More extensive features:

- Layer 3 VPN tunnels between devices | Router on each side acts as VPN endpoint/pass-through
- PPTP: Point-to-Point Tunneling Protocol
- L2TP/IPSec: Layer 2 Tunneling Protocol/Internet Protocol Security
- SSH2
- Advanced IP networking services
- Edge router capability

Wireless Bridges Connect 2/more wired LAN's together

2 configs: Point-to-point/point-to-multipoint

- Dedicated device: Functions like AP in bridge mode
- Many same features as enterprise AP's
- Removable antennas | Selectable power levels

Benefits:

- Fast installation/Cost savings/Can span long distances
- High data transfer rates
- Can work in either 2.4 GHz ISM or 5 GHz UNII band

Wireless Repeaters: AKA Wireless Range Extender Used to extend RF cell

- Wired network: Repeaters function at L1 to extend eth0 segment
- Lacks intelligence: Can't determine data traffic types/simply passes data across device
- Distance depends on factors (transmit power to AP/gain of antenna)
- Allow devices to connect to WLAN even when outside normal hearing range of AP connected to network
- Will allow this comm to occur in case where wireless client is outside RF cell or **BSA: Basic Service Area** of AP
- Client: Sends info/frames to repeater: Repeater fwds them to AP
- Config reduces overall throughput

Wireless LAN controllers Benefits:

Centralized administration	Gives admin complete control over wireless network from single location • One-stop shop for config/management **WNMS: Wireless Network Management System** • Used as centralized tool to manage autonomous AP's • Used to help scale autonomous AP architecture: Not required
Controller-based AP	Similar to autonomous AP benefit wise • RF management/security/QoS • Cost less than autonomous AP's • Little/no info contained w/in devices • PoE-capable for ease of deployment • Mid-sized/large orgs
VLAN	802.1Q • Define broadcast domains in L2 network by inserting VLAN info into eth0 frames
PoE	Power over Ethernet capabilities
Improved device roaming	**L2/L3 roaming between AP's** • Connection while physically moving throughout network • 802.11r specifies FT: Fast Transition • Exists in very few SOHO deployments
Wireless profiles	**Ability to create profiles** • In conjunction w/VLANs to allow/deny access • Can be config'd for various situations • Diff SSID's: Guest/corporate/voice/sec/QoS • Can also be accomplished w/WNMS for controllerless/cooperative deployments
Advanced sec features	802.11i WPA/WPA 2.0 with both passphrase/enterprise config capabilities
Captive portal	**Intercepts attempts to access network by redirecting traffic to page** • May request credentials/payment/agreement to TOS Example: Wireless hotspot

Built-in RADIUS services	**Services for 802.1X/EAP auth: Supported by WPA/WPA 2.0** • Limited # of usrs • Good for SMB/remote office (not large orgs) • Larger networks: External RADIUS
Site survey tools	**Predictive tools assist in placement of AP's/devices** • Sometimes feature WLAN controller
RF spectrum management	Adjust RF params like channel frequency/RF transit power after deployment • Allows network to adapt to changes
Firewall/QoS/Redundancy	**Stateful firewalls:** Keep records of all connections • Protects against broadcast storms/rogue DHCP server attacks/ARP poisoning **Redundancy:** Allows fault-tolerant deployments/provides uninterrupted access in event of failure
WIPS	Wireless intrusion prevention system
Direct/distributed AP connectivity	**Distributed:** • Connecting AP's that are not directly plugged into port on WLAN controller • Beneficial in large scale deployments **Direct:** Direct connection to ports on switch
L2/L3 AP connectivity	**L2 roaming:** • When a PC/other device moves out of radio cell of currently connected AP ○ Connects to a diff AP maintaining L2 connectivity **L3 roaming:** • When a client moves to an AP that covers a different subnet. • After roaming: Client will no longer have valid IP from original subnet • Device will be issued IP from new subnet while maintaining L3 connectivity

Distributed/Centralized Data Fwding
WLAN controller solutions consist of 2 types of architecture:

- **Centralized: AKA: Split-MAC architecture**
- Distributed

Centralized: Separated intelligence from AP/placed into wireless controller to allow for centralized management of network

- ▪ AP was mostly a radio/antenna: Traffic decisions were sent to controller through eth0 cable
- ▪ Could cause bottlenecks/overloads/issues

Distributed: Reduces amt of traffic b/c controller-based AP able to make more decisions: Takes load away from controller

- ▪ Moving some intelligence back to edge (wireless AP) min. bottlenecks/other issues like latency
- ▪ Also true in cooperative/controllerless architecture
- ▪ Eliminates need for data to be sent to controller for handling

Power over Ethernet Sends DC voltage/data over same Eth0 cable: Enables device to receive DC power/data simultaneously

- ▪ Eliminates need for external AC power source

Consists of 2 ratified amendments:

• **802.3af**	• **802.3at** (**PoE+**)

Amendments define specifications for devices used in wired/wireless networking to receive DC power from eth0 connection

Allowed power to be supplied 1 of 2 ways:

1. Over same wired pairs that carry data
2. Over pairs that don't carry data
    - □ 10BASE-T/100BASE-T (Gigabit) may use all 4 pairs (8 wires) to carry data
    - □ Standard defines which wire pairs allowed to carry based on whether 10BASE-T/100BASE-T/1000BASE-T
    - □ Whether power is sourced from endpoint/mid-span injector

PSE: Power Sourcing Equipment: Device that supplies DC voltage to end devices that receive it
Delivered 1 of 2 ways:

1. Endpoint device: (WLAN controller/switch): Delivers DC directly over same wire pairs that carry data over unused wire pairs
2. Midspan device: (Single port/multiple port injector): Injects DC power into eth0 cable over unused wire pairs/data pairs

Powered Device: Device receiving DC such as AP/bridge/IP camera/IP phone/etc..

- Defines max cable length of eth0 cable to be 328′ or 100 m
- Because of line loss table shows less then max power

Specification	802.3-2005 Clause 33	802.3at
PSE Power Max	15.4 W	25.5 W
PD Power Max	12.95 W	24.0 W

Powered Device Classification: Manufacturers have option of defining classification signature

- Determines max amt of power device requires
- Allows PSE to better manage amt of power delivered to specific port

Class	Use	PSE Power output in watts	PD max levels in watts
0	Default	15.4 W	0.44 W to 12.95 W
1	Optional	4.0 W	0.44 W to 3.84 W
2	Optional	7.0 W	3.84 W to 6.49 W
3	Optional	15.4 W	6.49 W to 12.95 W

Post 4

Thursday, January 24, 2019 11:41 PM

WLAN – CHAPTER 4 NOTES

Wireless LAN adapters: Avail in various types: External/internal
External adapters: Will connect to avail int in device

Examples	PCMCIA	ExpressCard	USB	Compact Flash (CF)

Internal adapters May require some lvl of disassembly/removal

Examples	PCI	Mini-PCI	Full Mini-PCIe	Half Mini PCIe

Wireless differ from Eth0 adapters: They use radio HW/RF to send data over air
Radio HW Used w/Wireless LAN Technology: 802.11: Every addressable unit used in WLAN is considered STA (station)

- Both clients that connect to network: Wireless AP's that allow device to connect
- 802.11n: Client device selection to be carefully considered
- Ideal to use 802.11n devices w/802.11n MIMO AP's (multiple-input-multiple-output)
- 802.11a/b/g may benefit from MIMO also

BYOD: Bring **Y**our **O**wn **D**evice
PCMCIA: Personal Computer Memory Card International Association: Early 1990's

- Portable industry needed smaller/lighter/more mobile tech
- Was common for notebooks: Had int slot: Allowed PCMCIA adapter
- *Devices now:* Either built-in wireless adapter/USB one

PCMCIA standard addressed 3 types of cards:

Type I	Type II	Type III

Only diff was thickness: Had same width/length/68-pin connector: 5 vers of PCMCIA standard

- **Release numbers:** 1/2/2.1/5/8
- Releases 1 – 2.1: Support 16-bit apps
- Releases 5+: Address 32-bit ints

Card Type	Thickness	Common Use
Type I	3.3 mm	RAM, flash OTP, SRAM mem cards
Type II	5 mm	LANs, data/fax modems, mass storage I/O devices
Type III	10.5 mm	Rotating mass storage devices

Install/Config PCMCIA Cards: Verify physical chars of card (type)/device to be used in

- Card/host device must be physically compatible

Device driver: SW required for component to communicate w/computer/device OS
ExpressCard: Newer gen PC Card tech:

- More narrow than predecessor (PCMCIA)/avail for newer WLAN tech
- Used on many notebooks/some WLAN controllers/wireless AP's

EVDO: Evolution-Data Optimized card: Provides backhaul for emergency use in high-avail roles

- Lower cost/smaller size/higher performance

Features: Built on 16/32bit PC Card standards

Modules avail in 4 types:

34 mm	34 mm extended	54 mm	54mm extended

Extended modules: Can be used for external connectors (TV tuners/wireless broadband)

Hot-plug: Can install/remove w/out having to power down machine

USB 1/1.1/2/3

USB: Universal Serial Bus: 1.0: Introduced in 1995: Designed to replace legacy serial/parallel connections

Serial communication: Process of transmitting 1 data bit at a time

Parallel communication: Capability of transmitting 7 data bits at a time

Devices replaced include:

- Keyboard
- Mouse
- Digital camera
- Printer
- Computer networking adapter

USB 1.0	Released 1995: Replaced by 1.1: 1998 • **Data rates:** 1.5 Mbps – 12 Mbps
USB 2.0	Released April, 2000: 1st revision: December, 2000 Revised 7 times since: 7 changes/Including connector types • **Data rates:** Max speed of up to 480 Mbps
USB 3.0	Released early 2010: Faster rates/Wider BW • Multiple logical streams • Improved bus use | Asynchronous readiness notification w/out polling Greatly increases transmission speed • **Data rates:** Up to 4.8 Gbps: AKA: SuperSpeed • Specification address improvements Includes: • BW by using bidirectional data paths/power mgmt/improved bus utilization

USB standards: Implemented USB-IF: USB Implementers Forum:

- Org consists of companies from comp/electronics industries (Intel/MS/NEC/HP)

Features of USB:

- Standard connector that replaces 9-pin serial/25-pin parallel/other connector types
- External config allows user to plug in device/power it w/single port
- Supports hot-swapping devices

PCI: Peripheral Component Interconnect Standard for comp int cards developed by Intel

- Card inserted into slot on MB: Allows for attachment of peripheral devices

Features: Connects to data bus in desktop

Data bus: Allows connection of devices to comp's processor

- Early days: Many devices used data bus

Devices included:

- Video
- HDD
- Serial ports
- Eth0 adapters
- Parallel ports for printers

They connected to ISA bus (Industry Standard Architecture)

Modern computers have integrated many of these ints directly into MB: Data bus arch evolved

- Went from 32-bit to 64-bit bus

1995: MS introduced Plug and Play: Accelerated interest in PCI

- PnP made installing card easy: All required: Plug card into MB | Recognized auto to work w/OS

Mini-PCI, Mini-PCIe, and Half Mini-PCIe

Mini-PCI	Variation of PCI standard: Designed for laptops/other small sys Example: 802.11 Mini-PCI adapter Common in many devices: Fast Eth0 networks/Bluetooth/modems/HDD controllers/WLANs • Used in AP's/client devices (laptops) **Mini-PCI Express (Mini-PCIe):** Cards replacement for Mini-PCI card based on PCI Express

Features: Mini-PCI cards avail in 3 types:

Type I	100-pin stacking connector
Type II	100-pin stacking connector • RJ11/RJ45: Commonly located at edge of comp/docking station • So connectors can be mounted for external access • Such as a modem/comp network
Type III	124-pin edge connector

Cards: 30 mm x 56 mm | 52-pin edge connector | Consists of 2 staggered rows on a .08 mm pitch

- Cards are 1 mm thick excluding components

Half Mini-PCIe cards: 30 mm x 31.90 mm

- Main diff bet this card/Mini-PCIe: Length: Length of new form factor is 1/2 of Mini-PCIe card

Card Type	**Connectors**	**Size**
Mini-PCI Type IA	100-pin stacking	7.5 mm x 70 mm x 45 mm
Mini-PCI Type IB	100-pin stacking	5.5 mm x 70 mm x 45 mm
Mini-PCI Type IIA	100-pin stacking, RJ11, RJ45	17.44 mm x 70 mm x 45 mm
Mini-PCI Type IIB	100-pin stacking, RJ11, RJ45	5.5 mm x 78 mm x 45 mm
Mini-PCI Type IIIA	124-pin edge	5 mm x 59.75 mm x 50.95 mm
Mini-PCI Type	124-pin edge	5 mm x 59.75 mm x 44.6 mm

IIIB		
Full Mini-PCIe	52-pin edge, 2 staggered rows on 0.8 mm pitch	30 mm x 31.90 mm x 1 mm (excluding components)
Half Mini-PCIe	2-pin edge, 2 staggered rows on 0.8 mm pitch	30 mm x 56 mm x 1 mm (excluding components)

Additional Adapter Types

- **CF: CompactFlash Devices**
- **SD: Secure Digital**

CompactFlash Devices: Designed as mass storage device fmt used in portable electronic devices

SanDisk: Introduced fmt: 1994: Now used for variety of devices/tech Including: Eth0 networks/Bluetooth/digital cameras/RFID/WLANs

Features: Available in 2 types: Type I | Type II

- Both types have same length/width: 36 mm x 43 mm
- Only diff: Thickness

Card Type	Thickness	Common Use
Type I	3.3 mm	RAM, flash mem cards
Type II	5 mm	WLANs, Microdrives

Install/config: Diff from previous examples:

- May need to connect handheld personal comp running MS OS (Pocket PC)
- Or **PDA (Personal Digital Assistant)** to another comp in order to complete install process

Secure Digital: SD designed as flash mem storage device w/storage capacities from 8 MB – 4 GB

- 1999: SanDisk/Toshiba/Panasonic
- Even though SD was designed to provide flash mem: Slot allows for connection of other devices

Examples:

- Cameras
- GPS: Global Positioning System units
- FM radios
- TV tuners
- Eth0 networks
- WLANs

In this fmt SD card AKA: **SDIO: Secure Digital Input Output**

- Card designed to provide high-speed data I/O w/low power consumption for mobile devices

Features of SDIO cards: Avail in 2 sizes:

Full-size SDIO	24 mm x 32 mm x 2.1 mm	Size of postage stamp: Intended for portable stationary apps
Mini-SDIO	27 mm x 20 mm x 1.4 mm	Used w/WLANs/Bluetooth adapters

Install:

1. Connect Pocket PC/PDA to host PC running ActiveSync
2. Install SW using host PC
3. Insert SDIO WLAN card

4. Start program on Pocket PC/PDA
5. Find WLAN to connect/create profile
6. Connect to WLAN

Wireless Workgroup Bridges: A wireless device acting as a client that will allow up to 7 eth0 devices on an eth0 segment

- Devices connected to a common physical layer boundary: They connect to an infrastructure through a wireless AP
- Accomplished w/out need to upgrade each wired device on eth0 segment to wireless

WWB: Wireless Workgroup Bridge: AKA: Wireless client bridge:

- Can be used in business/SOHO apps

Including: Enterprise/medical/retail/education/warehouse

Supported devices:

- Computers
- Printers
- Scales
- Medical equipment
- Barcode readers
- POS machines (cash registers)

Although workgroup/bridge may have features of infrastructure device: Considered client device

- A workgroup bridge will allow for a limited # of wired client devices to connect to/use network resources
- Wireless AP sees wireless workgroup bridge as single station: Even if 7 wired stations connected
  - B/C bridge multiplexes signal to single wireless connection
  - Basically a multiplex device

May include these features:

- Fixed/detached antennas
- Sec: WEP/WPA/WPA2.0
- Web browser/CLI
- MAC filtering
- Multiple connectivity modes
- PoE
- Support for connection of limited # of client devices

Install/Config

1. Connect workgroup/client bridge to eth0 segment that needs to have wireless
2. If PoE not feature of device: Connect bridge power adapter to wall jack
3. Using browser: Connect to IP: Some cases: May need to assign IP to workgroup/client bridge from CLI prior to config/bridge
4. From web mgmt int: Assign correct SSID/RF chan in order to associate to correct AP
5. Config correct sec settings: Either WPA/Personal/Enterprise
6. Verify association of workgroup/client bridge to desired AP

Another form of wireless client bridge is 1 designed to allow variety of single eth0 devices:

- Not just computers to connect to/use wireless networks

These devices: Have eth0 port: Not wireless-capable

- This client bridge also has chars similar to some infrastructure devices (wireless AP’s)
- In most cases no SW required

Devices that can benefit from this type of client bridge are:

- DVD
- Media players
- Game consoles

Client Device Drivers: All devices connected to comp require drivers

Devices include: Keyboards/mice/video cards/USB ports/printers/NICs/WLAN cards/etc…

Device driver: SW that allows installed device to comm/take instructions from OS in order to function

- Impt to verify latest drivers

Client Utility SW: ALL 802.11 WLAN cards require config in order to connect to a wireless network

- Config capabilities of device drivers usually limited
- Usr needs additional config SW

Supplicant: Client device when 802.1X port-based auth used

- Supplicant will provide auth credentials to authenticator which is the AP

Manufacturer-Specific Client Utilities: Features depend on whether client is SOHO/enterprise

- **SOHO grade client utilities:** Basic connection/sec params
- SW install usually part of adapter install process
- **Enterprise-grade:** More advanced features: Connection stats/site survey
- User can install driver/client simultaneously

Third-Party Client Utilities: Another option for WLAN adapter client utility: Built into OS

Windows XP/Vista/7: Client utility built-in/running as service

Windows XP: Available from **Wireless Zero Config service (WZC)**

Later ver of Win7: Service called WLAN AutoConfig

After adapter installed: Usr may select network to connect to

Post 5

Thursday, January 24, 2019 11:42 PM

PHYSICAL LAYER ACCESS/SPREAD-SPECTRUM TECHNOLOGY

Wired/wireless networks: Access method is used to transfer electronic info.
2 common access methods:

- **CSMA/CD**
- CSMA/CA

Type of medium used determines which of the 2 methods used
802.11-2012: Part of 802.11-2007: Includes a/b/g/n
Network Access Methods: Allows devices connected to common infrastructure to comm/transmit data across a medium

- **CSMA/CD: Carrier Sense Multiple Access/Collision Detection**
- CSMA/CA: Carrier Sense Multiple Access/Collision Avoidance

Eth0 networks: Ability to detect collisions: Uses CSMA/CD access method
WLAN: No detect collisions: Uses CSMA/CA for access method
Detecting Network Traffic Collisions: CSMA/CD: 802.3: Uses CSMA/CD

Carrier Sense	Devices sense medium to see if it's clear (no data being transmitted) • Medium: eth0 cable
Multiple Access	Lots of devices accessing medium at same time
Collision Detection	Collisions that occur on medium during data transmission

Contention-based media access control method

- Allows only 1 device to transmit at a time

Contention: Multiple devices competing for a shot to send data: 1 reason for decreased throughput of transmission
How it works:

1. Device w/data to transmit checks if anything is being transmitted on eth0 cable (sensing)
2. If clear/no data being transmitted: Transmits its own data
3. If more than 1 device transmits at same time: *Collision*: Data lost: Devices detect collision: Back off for random amt of time
4. After time expires: Devices check cable: Attempt to send data again

Avoiding Network Traffic Collisions: CSMA/CA WLANS: Main diff: Collision avoidance

Carrier Sense	Senses medium: Air
Multiple access	Lots of devices accessing medium at same time
Collision Avoidance	Avoids collisions that may occur on medium during transmission

WLANs have no way to detect collisions so CD isn't adequate

- If CD was used: Collisions at wireless AP: Data would be lost
    - Device wouldn't know where to retransmit: Receiving device would be unaware of collision: Bad performance

CSMA/CA: Uses mechanisms that attempt to avoid collisions
Some overhead: Benefit is greater however w/better throughput B/C collisions minimized
Why overhead occurs: Devices use "countdown timers": Requires them to wait before they can transmit again
Reserving Time for Data Transmission Using DCF: Distributed Coordination Function
DCF: Distributed Coordination Function: One access method WLANs use to comm

- Employs contention period for devices competing to send data

Collision avoidance: Requiring criteria be met for frame to be transmitted across medium (L2 digital transmission unit)

- **WLAN:** Medium: Air using RF

To avoid collisions: Devices required to:

1. **CCA: Clear Channel Assessment:** Technique to detect RF energy of other devices transmitting

    - ○ Announces how much time required for frame exchange to occur
    - ○ Allows other stations read duration field: Set **NAV: Network Allocation Vector**

2. **InterFrame Spacing:** Waits for predetermined time bet frames
3. **Random back off timer via contention window**: Backs off/retries if medium busy
4. Devices reserve medium so transmissions can take place **|** Avoid collisions

802.11: 2 other access methods used in wireless networking:

PCF: Point Coordination Function	**Contention-free mode** • Works by polling stations/giving them opportunity to send info • W/out contending w/other devices
HCF: Hybrid Coordination Function	**QoS** technology

Effects of Half Duplex on Wireless Throughput

Half-duplex: Comm that occurs in 1 direction at time: Less data throughput for connected devices

- Part of reason why amt of data being transferred can be less than 1/2 of advertised rate
- Collisions/additional overhead other factors

Narrowband vs. Spread-Spectrum Communication

2 examples of how devices comm using RF

Example of narrowband: Radio station: Licensed frequency ranges in the FM band

Spread-Spectrum Technology: Uses low power over wider range of frequency

2 types of spread-spectrum: 802.11:

- **FHSS: Frequency-hopping spread spectrum**
- DSSS: Direct-sequence spread spectrum

    - ○ Both comm in 2.4 GHz range

Spread-Spectrum	Takes digital info generated by computer (1's/0's) • Through modulation: Sends it across air bet devices using RF In order for devices to comm effectively/understand 1/another: • Must be using same spread-spectrum/modulation ○ Example: 2 people don't know same lang? No convo

FHSS: Frequency-Hopping Spread Spectrum: Original 802.11: Legacy

- Used by many early adopters of wireless (comp/barcode scanners/handheld devices)
- Still common in many devices:
    - ○ Cordless phones/WPANs/Bluetooth mice/cameras/phones/wireless headsets/older WLAN devices
- Bluetooth slower than newer wireless comms

FHSS	**Sends small amts of info across entire 2.4 Ghz ISM band** • Changes frequency (hops) constantly: Specific pattern • **Dwell time:** Remains on frequency for specified amt of time ○ Dwell time value depends on local regulatory domain where device used ○ US: FCC: Max dwell time: 400 milliseconds Transmitter/receiver sync'd w/same hopping sequence: Allows devices to comm **Data rate**: 1-2 Mbps

DSSS: Direct-Sequence Spread Spectrum: Original 802.11

Data rates of 1-2 Mbps: Special techniques to transmit data across air using RF

Modulates/modifies RF chars such as:

- Phase
- Amplitude
- Frequency

Spreading code: Tech that provides redundancy of data as it traverses through air

- Spreading code transmission: Info on multiple subcarriers
    - ○ Redundancy helps receiver detect errors from interference
- **Spreads info across 22 MHz wide channel:**
    - ○ Helps make DSSS resilient to interference
- Allows receiver to determine if single bit of data received is 0/1

Depending on data rate:

- Transmitter/receiver understand spreading code in use: Are able to comm
    - ○ Example: Barker code: Spreading code for DSSS
    - ○ 802.11 WLANs: Can use 11 "chip" spreading code for comms

    - Each bit combined w/set Barker code through exclusive OR (XOR) process

XOR: Way of combining binary data bits: Result: Spreads binary 0 or 1

- Both transmitter/receiver understand code: Can determine info sent across air

Channel: Operates w/in range of RF frequency defined by its center frequency
Channel 1: 2.412 GHz on center
Channel 2: 2.416 GHz on center
Separated by 5 MHz on center

Unlike narrowband which operates on single narrow frequency:

- DSSS channel: 22 MHz wide: 1 of 14 channels in 2.4-2.5 GHz ISM band
- Country/location of device determines which of 14 channels available for use

FHSS/DSSS both operate in same frequency range

- If devices use both techs are occupying same physical area: May have some interference

802.11b HR/DSSS: High Rate/Direct-Sequence Spread Spectrum: 802.11b

Introduced higher data rates of 5.5/11 Mbps

- Like DSSS: HR/DSSS uses 1 of 14, 22 MHz wide channels to transmit/receive data
- Supports higher data rates: Uses diff spreading code/encoding technique then DSSS
- Uses **CCK: Complementary Code Keying** for transmitting data at 5.5/11 Mbps

802.11 DSSS and HR/DSSS Channels

- Operate in 2.4 GHz ISM license free band
- Band has 14 channels

Channel	Frequency (GHz)	Americas	EMEA	Israel	China	Japan
1	2.412	**X**	**X**	**X**	**X**	**X**
2	2.417	**X**	**X**	**X**	**X**	**X**
3	2.422	**X**	**X**	**X**	**X**	**X**
4	2.427	**X**	**X**	**X**	**X**	**X**
5	2.432	**X**	**X**	**X**	**X**	**X**
6	2.437	**X**	**X**	**X**	**X**	**X**
7	2.442	**X**	**X**	**X**	**X**	**X**
8	2.447	**X**	**X**	**X**	**X**	**X**
9	2.452	**X**	**X**	**X**	**X**	**X**
10	2.457	**X**	**X**	**X**	**X**	**X**
11	2.462	**X**	**X**	**X**	**X**	**X**
12	2.467		**X**	**X**		**X**
13	2.472		**X**	**X**		**X**
14	2.484					**X**

Of 14 channels:

- Mathematically only 3 adjacent non-overlapping ones: Except channel 14

Channel 14:

- Specifically for operation in Japan
- Separated by 12 MHz on center from Channel 13

Channels 1-13:

- Separated by 5 MHz on center of each channel

There are 3 MHz of separation where RF of 1 channel ends: Next adjacent non-overlapping channel begins

- Means: 3 AP's can be co-located in same phys space w/out overlapping channel interference
    - Still theoretically small amt of overlapping RF/Harmonics bet the 2 channels
    - Small overlap: NOT large enough to cause real interference

Each DSSS channel: 22 MHz wide: Uses spread-spectrum technology:

- Channel size helps add resiliency to interference for transmissions
- Gives capability to move large amts of data w/small amt of power

802.11g ERP: Extended Rate Physical

- Amendment released 2003: Introduced tech that allowed for higher data rates for devices
- Operation in 2.4 GHz ISM band

Objective of amendment: Allow higher data rates (up to 54 Mbps) using **OFDM: Orthogonal**

Frequency Division Multiplexing

- To maintain backward compatibility w/existing 802.11b tech/devices

Builds on data rates of 1, 2 Mbps DSSS (802.11) | 5.5, 11 Mbps HR/DSSS
Addresses 7 compatibility operation modes:

- **ERP-DSSS/CCK**
- ERP-OFDM
- ERP PBCC (optional)
- DSSS-OFDM (optional)

802.11g required support for ERP-DSSS/ERP-OFDM

- Allowed both 802.11b data rates of 1, 2, 5.5, 11 Mbps/new OFDM data rates of 6, 9, 12, 18, 24, 36, 48, 54 Mbps

Manufacturers implement in various ways

- GUI: May be drop-down that allows specific operation mode (mixed/b/g mode/b-only)
- Can select individual rates using radio buttons
- CLI

802.11n High Throughput: Amendment ratified: September 2009
HT: High Throughput PHY: Physical layer tech based on OFDM (PHY)

- HT allows extensibility of up to 4 spatial streams: Using channel width of 20 MHz
- Transmission of 1-4 spatial streams defined for operation in 20/40 MHz channel width mode
- Capable of supporting data rates up to 600 Mbps using 4 spatial streams w/20/40 MHz channel
- Provides features that can support throughput 100 Mbps+

Optional features on both transmit/receive sides:

- **HT-greenfield format**
- Short guard interval (GI), 400 ns
- TxBF: Transmit Beam Forming
- STBC: Space-Time Block Coding

Allows for operation in both 2.4 GHz ISM/5 GHz UNII bands w/either 20/40 MHz wide channels
Data rates: What a station is capable of exchanging info
Throughput: The rate at which info is actually moving
802.11a, 802.11g and 802.11n OFDM: Orthogonal Frequency Division Multiplexing
OFDM: 802.11a
ERP-OFDM: 802.11n
HT-OFM: 802.11
OFDM: Allows for much higher data rate transfers than DSSS and HR/DSSS

- Up to 54 Mbps for a/g: Potentially up to 600 Mbps for n

OFDM: Orthogonal Frequency Division Multiplexing:

- Designed to transmit as many signals simultaneously over 1 transmission path in shared medium
- Every signal travels w/in its own unique frequency subcarrier (separate signal carried on main RF transmission)

802.11a/g OFDM: 52 subcarriers: 4 of 52 subcarriers don't carry data/used as pilot channels
802.11n: 56 subcarriers: 52 usable: 20 MHz wide channel

- 114 subcarriers: 108 usable: 40 MHz wide channel

802.11n devices (HT-OFDM):

- May use MIMO SM: Spatial Multiplexing
- Uses 7 radio chains to transmit diff pieces of same info simultaneously
- Greatly increases throughput

OFDM helps provide resiliency to interference from other wireless devices
802.11a/g/n OFDM Channels
Functions in either 2.4 GHz ISM/5 GHz UNII bands:

- Channel width smaller than DSSS/HR-DSSS
- Only 20 MHz compared to 22MHz for DSSS

Like DSSS: When OFDM used in 2.4 GHz ISM: Only 3 non-overlapping adjacent channels for use

- Limits the use of bonded channels (20/40 MHz wide) in 802.11n

5GHz UNII: Channel spacing: No overlap

- Frequency range used: Determines how many non-overlapping channels available

Lower/upper UNII: 4 non-overlapping channels
Middle UNII: 15 non-overlapping channels

- **All UNII channels: 20 MHz wide**
- **Separated by 20 MHz from center frequencies**
- Certain regulatory domains: US FCC/EU ETSI require use of DFS: Dynamic frequency Selection support
- For AP's that operate in middle 5 GHz (5.250-5.75 GHz) UNII band

DFS: Allows AP to change RF channel operating on to avoid interfering w/certain type of radar sys

Regulatory Domain	Frequency Band (GHz)	Frequency Center (GHz)	Channel Number
Americas/EMEA 4 channels	**5.150-5.250**	5.180	36
		5.200	40
		5.220	44
		5.240	48
Americas/EMEA 4 channels	**5.250-5.350**	5.260	52
		5.280	56
		5.300	60
		5.320	64
Americas/EMEA 11 channels	**5.470-5.725**	5.500	100
		5.520	104
		5.540	108
		5.560	112
		5.580	116
		5.600	120
		5.620	124
		5.640	128
		5.660	132
		5.680	136
		5.700	140
Americas/EMEA 4 channels	**5.725-5.825**	5.745	149
		5.765	153
		5.785	157
		5.805	161
ISM	**5.725-5.850**	5.825	165

802.11n: MIMO: Multiple Input/Multiple Output Technology

MIMO: Used by 802.11n devices:

- Potential data rates: Up to 600 Mbps
- Devices using MIMO capable of rates 300-450 Mbps
- Provides users w/better experience for data/voice/video comms
- Throughput up to 5x more than current 802.11a/g SISO networks

SISO: Single Input/Single Output: Most basic wireless antenna tech used in WLAN sys

1 antenna: Used to transmit data | 1 antenna used to receive data

Diversity: Some SISO sys support: 2 antennas w/single radio

- Will help lessen effects of multipath: Caused by reflections
- Coverage more consistent w/MIMO b/c devices using it: Able to utilize reflected signals

MIMO: Also allows 802.11n networks better throughput than DSSS/OFDM at same distance

- Backward compatibility with a/b/g in both 2.4 GHz ISM/5GHz UNII
- Allows for deployments to continue using existing HW

Benefits of 802.11n MIMO networks: Throughput/reliability/predictability

- 5x more throughput: Enhanced file transfer/DL speeds
- 2x as reliable: Lower latency for mobile comm
- 2x as predictable: More consistent coverage/throughput for mobile apps

Unlike 802.11b (HR/DSSS)/802.11a/g (OFDM) AP's:

- **MIMO AP's use multiple radios w/multiple antennas**
- Multiple radio chains/additional intelligence give MIMO 802.11n AP's capability to process reflected signals

Dual-band 802.11n MIMO AP will have up to 6 radio chains

- 3 for 2.4GHz
- 3 for 5 GHz
- 6 antennas (1 for each radio)
- Data rates of up to 450 Mbps

Techniques:

- **MRC: Maximal Ratio Combining**
- TxBF: Transmit Beam Forming
- SM: Spatial Multiplexing

802.11a/b/g networks: Known as SISO Systems

- Performance can degrade from multipath/poor reception/obstacles/RF interference

MIMO 802.11n: Takes advantage of multipath to help increase throughput at given range

Co-location of 802.11b HR/DSSS and 802.11a/g/n Systems:

Co-located: They can function in same RF space

HR/DSSS and ERP-OFDM networks operate in 2.4 GHz ISM: Backward compatible at a price

- Reduced throughput B/C of protection mechanisms

HR/DSSS and ERP-OFDM common features:

1. Both operate at 2.4 GHz ISM
2. Both have 3 non-overlapping channels
3. Both subject to interference from devices operating in same frequency range

Ripple effect: When 1 802.11g AP can "hear another 802.11g AP on same radio frequency chan in ERP protection mode

802.11a OFDM/802.11n HT-OFDM 7 common features:

1. Both operate in 5 GHz UNII
2. Both have up to 23 non-overlapping channels
3. Both subject to interference from other devices operating in same frequency range

MCS: Modulation and Coding Scheme: Diff way to represent data rates available w/802.11n tech

Adjacent-Channel and Co-channel Interference:

- 2/more RF signals interacting w/each other
- Causes degradation of performance
- AKA ***co-channel cooperation***

Why? B/C wireless devices contending to use medium rather than being seen as RF noise to each other

Channel planning: Designing wireless networks so that overlapping RF cells are on diff non-overlapping channels

WLAN/WPAN Coexistence

WPANs: Typically consist of portable devices (PDA's/cell phones/headsets/keyboards/mice/tablets)

Can be affected when co-located w/WPAN devices

- Early Bluetooth tech could cause significant interference
- Newer versions of Bluetooth: Use AFH: Adaptive Frequency Hopping: Less likely to interfere

Post 6

Thursday, January 24, 2019 11:42 PM

UNDERSTANDING RADIO FREQUENCY

RF: Radio Frequency: Waves used in variety of communications: Radio/TV/Cordless phones/WLAN’s/Satellite

Consists of: High-frequency AC (alternating current) signals passed over copper connected to antenna

- Antenna transforms received signal into radio waves: Air
- AC signal: Sine wave: Result: Electrical current varying in voltage over time
  - Cycle will repeat specific # of times/cycles over 1 second

Frequency: # of cycles per second

Radio transmissions: 2 components work together:

1. Transmitter
2. Receiver

Transceiver: Wireless station can transmit/receive together || Forms AC signals

- Antenna: Transforms signals into waves through air: Carries info from transmitter to receiver

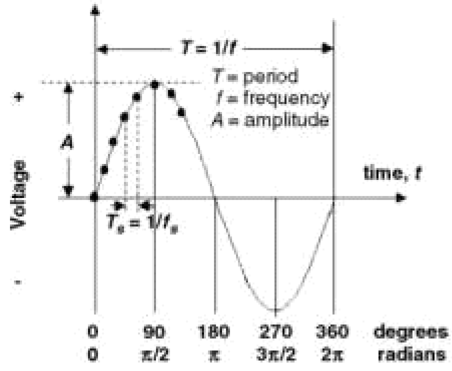
Includes:

- Wavelength
- Frequency
- Amplitude
- Phase

Wavelength: Distance of 1 complete cycle of 1 oscillation of AC signal (Greek lambda λ) || Measured in cm/in

Radio transmission wavelengths for WLANs

RF Channel	Frequency (GHz)	Length (in)	Length (cm)
6	2.437	4.85	12.31
40	5.200	2.27	5.77
153	5.765	2.05	5.20



Oscillating sine wave showing relationship between frequency vs Phase

Frequency: # of complete cycles in 1 second

Low frequencies = Long wave	**High frequencies = Short waves** (range)

Amplitude: Strength/amt of power of an RF signal

- Calc from height on Y axis of sine wave: Representing voltage
- Sine wave: Change in voltage over time
- Voltage: At peak of signal: Can be used to calc RF power

Increase in amplitude = Increase in RF power

Gain: Increase in power	**Loss:** Decrease in power

- As signal travels through RF cable: Loss: Attenuation
- Less amplitude at end: Cable loss value

Phase: Diff in degrees at particular point in time of cycle: Measured from 0/expressed as angle

Example: 2nd sine wave starts 1/4 of length after 1st wave: Considered 90° out of phase w/1st wave

Phase difference: 2 waves have same frequency, but start at diff times: Considered out of phase w/1 another

- Typically measured in degrees from 0-360°

Multipath: When waves arrive at receiver out of phase/exp distortion: Causes corruption

Delay spread: Diff in time of arrival of main signal/reflected signal that causes multipath problems

- 2 waves arrive at receiver 180° out of phase: Cancellation effect: Nullifies 2 signals

Upfade: 2 waves arrive in phase are **additive**: Increase in signal strength

- Amplitude of waves that exp upfade effect will never be higher than wave transmitted

Radio Frequency

Location	Regulation
Canada	ISC RSS-210
China	RRL/MIC Notice 2003-13
Europe (ETSII)	ETS 300.328ETS 301.893
Israel	MOC
Japan (MKK)	TELEC 33BTELEC ARIB STD-T71
Singapore	IDA/TS SSS Issue 1
Taiwan	PDT
US	FCC (47 CFR) Part 15C, Section 15.247FCC (47 CFR) Part 15C, Section 15.407

US FCC: Unlicensed Frequency Bands

FCC: Local regulatory agency: Regulates licensed/unlicensed radio spectrum

Unlicensed RF bands avail for use w/wireless comm:

- **ISM: Industrial, Scientific, Medical**
- 902 – 928 MHz (not specified for use w/standards-based 802.11)
- 2.4 – 2.4835 GHz
- 5.725 – 5.875 GHz

UNII: Unlicensed National Information Infrastructure:

- 5.15 – 5.25 GHz: **UNII-1**, lower
- 5.25 – 5.35 GHz: **UNII-2**, lower middle
- 5.470 – 5.725 GHz: **UNII-2e**, upper middle
- 5.725 – 5.825 GHz: **UNII-3**, upper

802.11 standard addresses 2.4 GHZ ISM band and 5 GHz UNII bands

- 2.4 GHz ISM allows 11 of 14 total channels to be used w/wireless
- 5 GHz UNII consists of 4 bands using 4 frequency ranges: UNII-1, UNII-2, UNII-2e, UNII-3

802.11 frequency/channel allocations

Band	Frequency	# of channels
ISM	2.400-2.4835 GHz	14
UNII-1	5.150-5.250 GHz	4
UNII-2	5.250-5.350 GHz	4
UNII-2e	5.470-5.725 GHz	11
UNII-3	5.725-5.825 GHz	4
ISM	5.725-5.8750 GHz	1

RF Channels: RF divided into bands: Further divided into channels

Channel: Smaller allocation of RF band | Example: TV

- Certain unlicensed freq ranges allocated for wireless networking/subdivided into channels
- In order for transmitter/receiver to comm w/1 another: Must be on same channel

Range: WLANs: Based on wavelength/distance of single cycle

Higher freq = Shorter range of signal

Lower freq = Longer range of signal

At same power lvl: 2.4 GHz signal will travel almost 2x as far as 5 GHz signal

- If network is planning to use dual-band AP's: Range needs to be considered

Coverage/Capacity

Capacity: # of devices that can connect to an AP (more devices = lower performance)

Coverage: Determined by RF cell size

Cell: Area of RF coverage of transmitter: Usually AP

Farther away from AP = Less throughput device/usr will exp

Depends on factors	• Physical size of area • BW-intensive SW/HW in use (may negatively impact performance) • Smaller RF cells needed • Obstacles: Building materials/propagation (way waves spread through area) • Range • WLAN HW in use (Higher freqs don't travel as far) • Transmitter output power • WLAN HW output power: Antenna type/orientation/gain *Higher gain antenna?* Greater coverage area *Lower gain antenna?* Smaller coverage • Polarization of antenna (horizontal/vertical)

Capacity: Max amt that can be received/contained

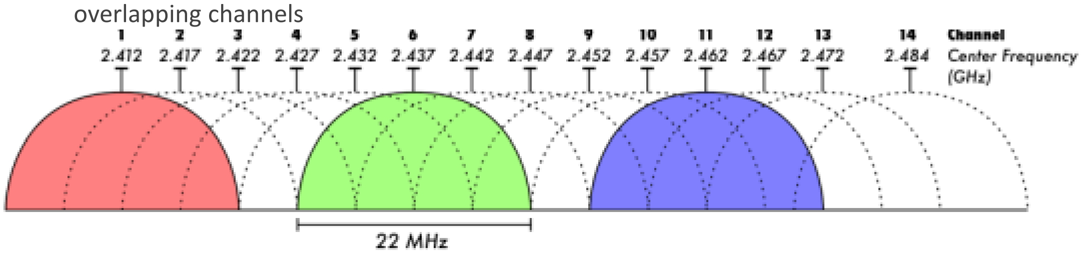
Depends on factors	• SW/HW apps in use • Desired throughput/performance • # of devices/usrs

RF Channel Reuse/Device Co-location

2.4 GHz ISM band: 3 non-overlapping channels (US FCC: 1/6/11)

Non-overlapping channel: Must be separation of 5 chans in order to be considered (5 MHz on center)

- Chans must be separated by 25 MHz/more to be nonoverlapping
- Calc from 5 chans of separation x by 5MHz on center (5×5=25)
- **Channel plan:** Will min chance of interference caused by 2 transmitters (AP's) set to same adjacent overlapping channels


1 2 3 4 5 6 7 8 9 10 11 12 13 14 Channel
2.412 2.417 2.422 2.427 2.432 2.437 2.442 2.447 2.452 2.457 2.462 2.467 2.472 2.484 Center Frequency (GHz)
22 MHz

RF Range/Speed

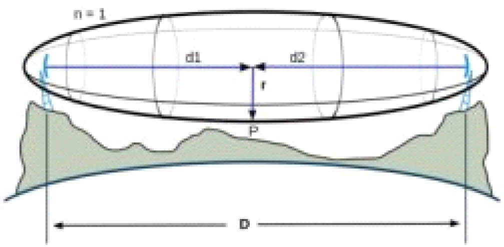
Line of Sight: Wireless Networking: RF comm bet devices in 802.11 networking uses diff types of line of sight

2 types:

Visual line of sight	Direct link RF line of sight

Visual line of sight: When transmitter/receiver "see" each other

- Clear unobstructed view bet transmitter/receiver || Few/no obstacles blocking RF signal bet devices

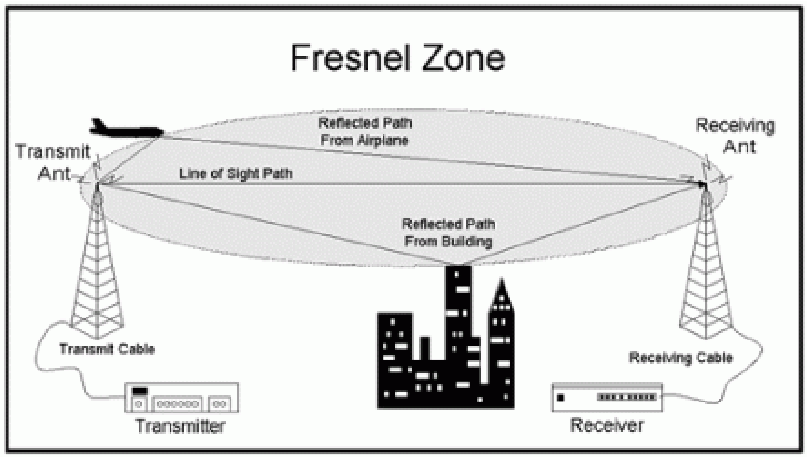


RF line of sight: Unobstructed line bet radio transmitter/receiver

- Surrounded by area of RF transmissions known as **Fresnel zone**

Fresnel zone: Concentric ellipsoidal volumes that surround direct RF line of sight bet 2 points

Example: RF transmitter/receiver of 2 wireless bridges)



Outdoor wireless install: RF line of sight could be **affected in total area if Fresnel zone blocked by more than 40%**

Blockage can come from many sources:Trees/buildings/terrain/curvature of Earth (7 miles +)

Wi-Fi/Non Wi-Fi Interference

Interference: From RF POV: Occurs when receiver hears 2 diff signals on same/close frequency

- Causes received RF signals to be distorted | Impacts quality of signal received | Less throughput

2.4 GHz ISM band is used for many devices including:

Cordless phones	Microwaves	Medical devices	Industrial devices	Baby monitors	Wireless networks 802.11

Co-channel/Adjacent Channel Interference: Occurs when 2 devices in same physical area tuned to close RF/same chans

Example: AP Channel 1/AP Channel 2: In close/hearing range: May exp adjacent channel interference

- Reduced throughput | Equivalent collisions causing data retransmissions

Overlapping interference:

- 2 devices (AP's): Same frequency overlapping 1 another

Example: 2 AP's in close proximity: One on Chan 1/Other on Chan 3: Might interfere w/each other

- Poor throughput | Properly designed WLAN have overlapping RF cells

Overlapping cells: Provide continuous coverage for entire area where AP's placed

- Allow devices to move from 1 AP to another/maintain constant connection
- 20-30% overlap to encourage better roaming
- Wireless repeaters require 50% overlap
- Frequency in use determined by how many nonoverlapping channels avail in band

WLAN/WPAN Interference

Bluetooth = Example of WPAN (Wireless Personal Area Network)

- Can be affected when co-located w/802.15 WPAN
- 2.4 GHz frequency range/use of **FHSS (Frequency Hopping Spread Spectrum)**
- Older Bluetooth devices potentially interfere w/802.11
- Newer vers use **AFH (Adaptive Frequency Hopping**)
  - Less chance of interference w/wireless

  AFH: Adaptive Frequency Hopping: Devices adapt to RF env by seeking areas of interference/not operating in those ranges
- Lessens chances of 802.15 WPAN devices interfering w/802.11 WLAN devices
- Devices can coexist in same physical radio chipset

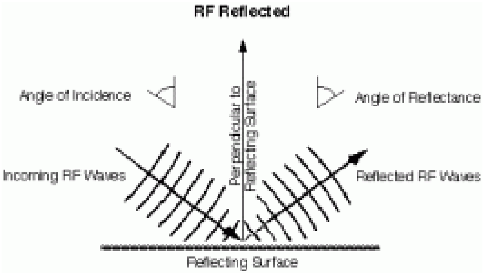
Environment: RF Behavior: Interaction bet RF/env can affect performance of 802.11 networks

RF behavior result of env conditions including:

Reflection	**Refraction**	**Diffraction**	**Scattering**	**Absorption**	**Diffusion**

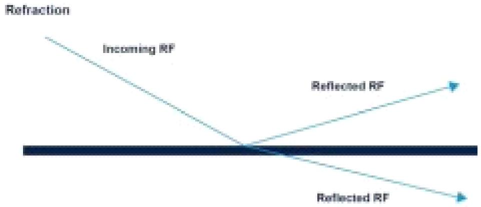
Reflection: **RF signals bounce off a smooth, non-absorptive surface (e.g. tabletop): Changes direction**

- Can affect indoor WLAN's | Type of walls/floors/furnishings
- Could decrease throughput



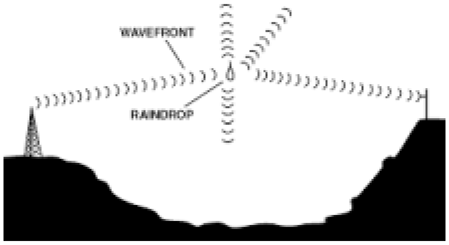
Refraction: **RF signal passes bet mediums of diff densities: May change speeds/bends (e.g. glass)**

- RF signals come in contact w/obstacle: Signal is refracted (bent) as passes through
- Some signal lost/Amt of loss depends on type of glass/thickness/properties



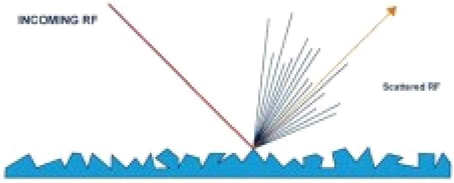
Diffraction: **RF signal passes obstacle, wave changes direction by bending around it (e.g. tall building/pond)**

- When bending around object, signal weakens/some loss



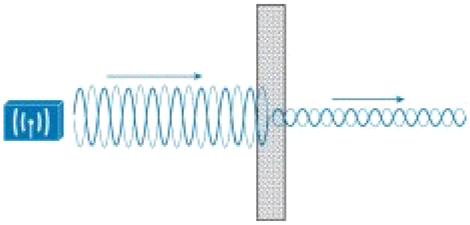
Scattering: **RF signal strikes uneven surface: Wave fronts of signal reflect off uneven surface in several directions**

- Loss/signal degradation



Absorption: Material absorbs signal: No signal penetrates through (e.g. Human body b/c of high water content)

- Becomes problem in certain envs (conference hall/airport/high pop. density)



Diffusion: **RF signal naturally widens as it leaves antenna element**

FSPL: Free Space Path Loss: Transmitted signals decrease in amplitude/less powerful of any distance from antenna

- Greatest form of loss factor in RF link
- Calc using freq/distance as vars entered into formula

- Receiving antenna only able to receive small amt of transmitted signal b/c of widening effect of diffused signal
- Any signal not received by intended device considered loss

Basic Units of RF Measurement:

Basic unit of measure for RF is watt || 1 milliwatt = 1/1000th of a watt

- Currency (dollars/cents denominations of money): Watts/milliwatts measurements of RF power

Other units of measurement for RF:

dB	**dBi**	**dBd**	**dBm**

Absolute Measurements of RF Power = Amt of power leaving wireless AP (ex)

- Measurable amt of power that can be determined w/proper instruments (watt meter)
- Typical max amt of output power from AP 100mW

Measure of AC power can be calc:

P = E x I

Power (P) = Voltage (E) x Current (I)

Example: Calc power from 1 volt and 1 amp:
P = 1 volt x 1 amp || Answer = 1 watt

Watt (W): Basic unit of power measurement: Absolute/measurable value

- Most wireless networks function in milliwatt range
- Common in point-to-point/point-to-multipoint

Milliwatt (mW): 1/1000th of watt | Absolute unit of power measurement

- Common value in RF work/WLANs
- Output power of AP typically ranges from 1mW-100mW

Enterprise-grade AP's: Allow output change

SOHO-grade AP's: Fixed output power (typically 30mW)

Decibel Relative to Milliwatt (dBm): Absolute unit of power measurement

dBm: Power lvl compared to 1 milliwatt: Based on logarithmic function

0 dBm = 1 mW (value is considered absolute 0)

Relative Measurements of RF Power: Relative: Changes in RF power

dB/dBi: Relative measurements of power (example: RF amplifier)

- If input to amplifier is 10mW and output is 100mW: Gain of amplifier is 10dB (change in power)
- If input to antenna is 100mW and output is 200mW: Gain of antenna is 3dBi (change in power)

Decibel (dB): dB: Ratio of 2 diff power lvls caused by change in power

0 dBm = 1 mW

3's or 10's rule:

Increase +3dBm || Power in mW x2
Decrease -3dBm || Power in mW /2
Increase +10dBm || Power in mW x10
Decrease -10dBm || Power in mW /10

Decibel Isotropic (dBi): Unit represents gain/increase in signal strength of antenna

Isotropic: RF: Energy broadcast equally in all directions in spherical fashion

Isotropic radiator: Imaginary, perfect antenna || Theoretical/used as reference in calcs

Absolute/Relative Measures of Power

Absolute Power	Relative Power
Watt	dB
Milliwatt	dBi
dBm	dBd

Relative values: Changes in power from 1 value to another value

Decibel Dipole (dBd): Gain of some antennas measured in dBd: Antenna gain w/respect to reference dipole antenna

- Most antennas in WLAN's measured in dBi; however some reference dBd

Derive dBi value from dBd value:

dBi = dBd + 2.14

Convert dBi to dBd

dBd = dBi = 2.14

RF Signal Measurements: Tools like wireless adapter client utilities/spectrum analyzers allow viewing of diff statistics for WLAN's

Some statistics:

- Receive sensitivity
- RF noise
- RSSI: Received Signal Strength Indicator
- SNR: Signal-to-Noise ratio

Receive Sensitivity: Measurable amt of RF signal usable by receiver || Determined by how much RF noise in area of receiver

Radio Frequency Noise: RF signals from sources other than transmitter/receiver in comm

- Crowded open space restaurant: Unrelated conversations occurring through it
- If paused convo, you'd hear it

RSSI: Received Signal Strength Indicator: Arbitrary # assigned by radio chipset/device manufacturer

- No standard for this value; Won't be comparable bet devices
- Calculation done in proprietary manner
- How "well" WLAN device will perform

SNR: Signal-to-Noise Ratio: Diff bet the amt of received signal/noise floor

- Restaurant: If everyone speaks at high volume you may not be able to hear partner

Example: Device receives signal of -85 dBm and noise floor is -95: SNR would be 10dB

-85 dBm -(-95dBm) = 10dB (Not good SNR)

Example II: Received signal is -65dBm and noise floor is -95dBm: DNR would be 30dB

-65dBm -(-95dBm) = 30dB (Excellent SNR)

Post 7

Thursday, January 24, 2019 11:42 PM

BASIC ANTENNA CONCEPTS CH.7

Transmitter perspective: Antenna takes energy from transmission system: Transforms into radio waves: Propagates through free air

Receiver perspective: Antenna receives radio waves: Transforms it back to AC signals: Sends info to PC/devices

Factors: Antenna to use:

Indoor/Outdoor install	Distance transmitter/receiver	Frequency	Horizontal/vertical orientation/polarization
Aesthetics	Cost	Manufacturer	Use
Mounting brackets	Electrical characteristics	Height	Location
Ordinances			

Characteristics of Antennas:

RF lobes: Shape of radiation patterns

Beamwidth: Horizontal/vertical angles

Antenna charts: Azimuth/elevation

Gain: Changing RF coverage pattern (beamwidths)

Polarization: Horizontal/vertical orientation

RF Lobes: Used to define projecting part: Shape of RF energy emitted from antenna element

Determined by physical antenna design:

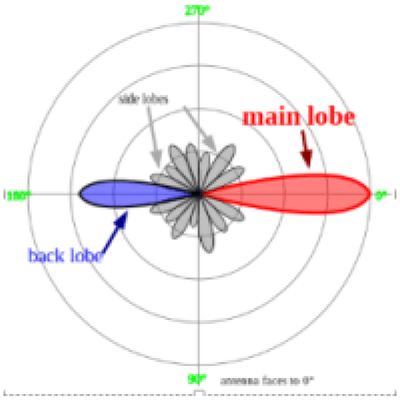
- How lobes project from antenna element
- Choosing right antenna? Critical in design
- May project many lobes of RF signal (some not usable areas)

Lobes not part of main/intended coverage? Rear/side lobes

- Usable RF: Not used for WLAN cell though

Type of antenna: Omni/semi/highly-directional: Determines usable lobes

Main signal: Lobe intended for use



Antenna Beamwidth: Design determines how RF propagates/specific patterns of energy propagated from an element

Lobes: Energy emitted from antenna

Beamwidth: Angle of measurement of main RF lobe: **Half-power** or **-3dB** point

- Measured in degrees: Both horizontally/vertically
- Antennas: Shape RF coverage/isotropic energy that radiates from element

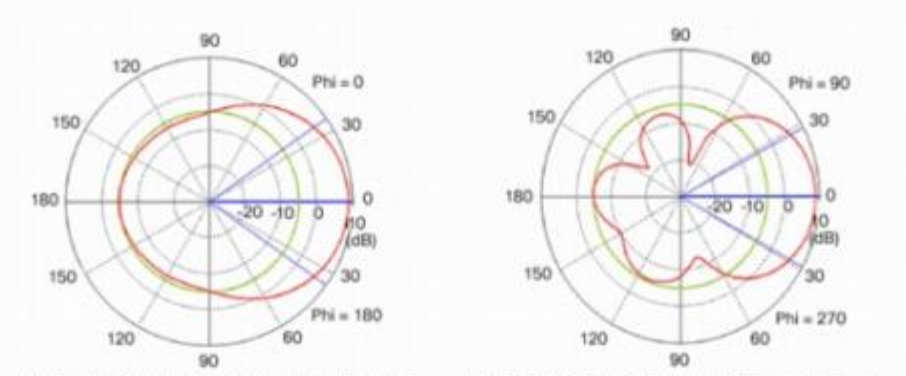
Azimuth: Horizontal RF coverage pattern

- *View from above* || *Bird's eye view* of RF pattern
- Some cases: 360°

Elevation: Vertical RF coverage pattern

- Like side view: If looking at mountain from side: Certain height/elevation

Azimuth/Elevation Charts:



(c) Patch Antenna Azimuth Plane Pattern (d) Patch Antenna Elevation Plane Pattern

Circular pattern: Readings from 0°- 360°: Many rings w/in charts

Outermost ring: Strongest signal from testing process of antenna

Inner rings: Measurements/dB ratings less than strongest measured signal from outside ring

Antenna Gain: Provides change in coverage: Result of antenna focusing area of RF propagation: From physical design

Amplitude: Height (voltage lvl/amt of power of sine wave)

- Created by varying voltage over period of time
- Measured: Peaks of signal from top to bottom

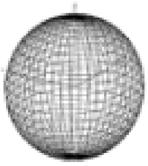
Amplification of an RF signal = Gain

Antenna: Device can change coverage area: Propagates RF signal further

Measured: dBi (decibels isotropic): Change in power result of increasing isotropic energy

Isotropic energy: Energy emitted equally in all directions

Example: Sun



Passive Gain: Change in coverage w/out use of external power source

Antennas: Focus isotropic energy into specific radiation pattern: Increases coverage in a direction

Example: Magnifying glass (convex shape of glass focuses sun energy into 1 area when aligned)

Functions same way by focusing energy received from signal source into specific RF radiation pattern

As gain of antenna increases: Both horizontal/vertical radiation patterns (beamwidths) decrease

- Create narrower beamwidths

As gain of antenna decreases: Beamwidths increase making larger radiation pattern

Exception: Omnidirectional antenna: Horizontal beamwidth of 360°

- Size of coverage area will increase/decrease depending on change in gain

  Example: Passive gain: Cone shaped paper/volume

Active Gain: Provides increased signal strength: Accomplished by providing external power source to installed device

Example: Amplifier

Antenna Polarization: **Polarization:** How wave emitted from antenna: Orientation of electrical component/field of waveform

To max signals: Transmitting/receiving antennas: Polarized in same direction/closely as possible

Polarization of transmitter/receiver diff? Power of signal will decrease depending how diff polarization is

- Site surveys show signal strength based on factors (including polarization of AP antennas)

WLAN Antenna Types: Wrong types of antennas can cause problems:

- Interference: Neighboring sys
- Poor signal strength
- Incorrect coverage pattern for design

3 common types antennas use w/WLANs:

1. **Omnidirectional/dipole antennas**

2. **Semidirectional antennas**
3. **Highly directional antennas**

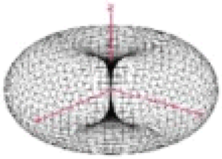
Omnidirectional Antennas

Common on AP's of SOHO/Enterprise

- Horizontal beamwidth (azimuth) of 360°
- Antenna vertically polarized (perpendicular to earth surface): Horizontal radiation pattern 360°
- Will propagate RF energy in every direction horizontally
- Vertical beamwidth (elevation) will vary depending on antenna gain

Gain of antenna increases = Horizontal radiation pattern increases: More horizontal coverage

Torus: Shape of radiation pattern: Looks like donut



Common type of antenna for indoor deployments

- Most AP's use: Enterprise-grade AP's: Removable antennas sold separately

Rubber duck antenna: Common type of omnidirectional antenna: Can be used indoors

- Low gain of 2dBi – 3dBi: Connects directly to AP
- Pivot point
- Polarization can be adjusted vertically/horizontally regardless of how AP mounted

Omnidirectional Specs: In addition to beamwidth/gain:

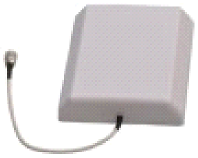
- Frequency range
- **VSWR: Voltage Standing Wave Ratio**
- Polarization
- Attached cable length
- Dimensions
- Mounting reqs

Semidirectional Antennas: Take RF power from transmitting sys/focus into more specific pattern than omni

Various types: Patch/Panel/Sector/Yagi

- Indoor/outdoor use
- More specific coverage: Focuses horizontal radiation patterns to value less than 360°
- Rooms/areas omnidirectional isn't good: (rectangular rooms/offices/hallways/corridors)
- Outdoor deployments: Point-to-point | Point-to-multipoint bridging installs

Patch/Panel Antennas: Requires knowing dimensions of physical area covered/amt of gain req



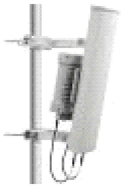
- Horizontal beamwidth as high as 180°
- Bet 35°-60°
- Vertical beamwidths bet 30°-80°
- Indoors/outdoors

Radome: Protective antenna cover: Keeps safe from elements

- Attenuation from materials that radome constructed from minimal

Sector Antenna: Can be used to create omnidirectional radiation patterns using semidirectional antennas

- Often base station connectivity for point-to-multipoint connectivity



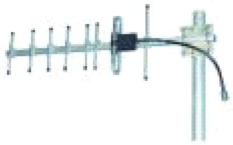
Sector Specs:

- Azimuth varies from 90°-180°
- Config to offer total azimuth of 360°
  Example: Antennas w/azimuth of 120° each would require 3 antennas to get omnidirectional 360° coverage

Common config: Array to allow semidirectional antennas to provide omnidirectional coverage

- Campus envs/community arrangements
- Wide horizontal beamwidth (azimuth): Narrow vertical beamwidth (elevation)

Yagi Antennas: Indoors (long hallways/corridors) | Outdoors (short-range bridging less than 2 miles)



- Vertical/Horizontal beamwidths ranging from 25°-65°
- Radiation patterns: Like a funnel/cone

Signal propagates away from antenna: Coverage naturally widens (diffusion)

- Aperture of receiving antenna: More narrow than signal by then
- Result of diffusion: Biggest form of loss in RF link

Highly Directional Antennas: Parabolic dish antennas: Long-range point-to-point bridge connections

- Available w/solid reflector or grid: Appearance of funnel
- Parabolic dish antennas: Very narrow horizontal/vertical beamwidths
- Beamwidth can range from 3°-15° w/radiation pattern similar to yagis
  - Starts very narrow at antenna element/naturally widens B/C diffusion

Designed for outdoor use: Must withstand environmental conditions

- Wind rating/mounting
- Grid antenna: Can provide similar coverage/less susceptible to wind loading '

RF Frequency Cables/Connectors: Plays role in various deployments:

- May be used to connect AP's/devices to antennas/to connect other devices

Things to consider:

Type of cable	Length of cable	Cost of cable	Impedance rating

- Right cable helps ensure signal loss (decrease in strength) is min/performance maximized

RF Cable Types: Cables vary in diameter/application/determine type of cable

- Thick, rigid cables best for longer runs
- WLANS: 50 ohm cables: TV (satellite): 75 ohm cables
- Correct ratings will min VSWR: Voltage Standing Wave Ratios

RF Cable Length: Short length will have some attenuation/loss

Loss: Decrease in signal strength: Less performance/throughput for usrs

- Correct lengths min issues

Pigtail: Short length of cable: Used to connect standard cable to proprietary cable

- If RF cable used/extended: Attenuation introduced can be offset w/use of amplifier
- Provides active gain/antenna provides passive gain
- Incorrect amplifier: May void sys cert/using higher-gain antenna: May exceed rules set by local regulatory agencies

Impedance/VSWR:

Impedance: Measurement of AC: Alternating Current resistance

- Normal to have some lvl of impedance mismatch in WLAN
- Impedances of all components should be matched as closely as possible
- Can result in **VSWR: Voltage Standing Wave Ratio**
    - Will have impact on WLAN & transmitted/received signal
    - Electrical resistance measured in ohms: Impedance: 50 ohms

RF Connectors: Also cause impedance mismatch/increase lvl of VSWR

- To min effects of VSWR: Keep use of connectors to min
- Using connectors: Can also result in insertion loss

Insertion loss: Can contribute to overall loss: Less RF signal/throughput

Proprietary Connecters

MC	Dell, Buffalo, IBM, Toshiba, Proxim-ORRiNOCO
MMCX	3Com, Cisco, Proxim, Samsung, Symbol, and Motorola
MCX	Apple, SMC devices
RP-MMCX	Used by SMC devices

Factors: Antenna Install

Earth Curvature: Beyond 7 miles: Impact on point-to-point/point-to-multipoint WLANS

Earth bulge: Adding height to antenna

Antenna Placement: Install/loc/placement depend on type of antenna/application

- Outdoor antennas: Lightning arrestors, grounding/adherence to codes

Omnidirectional Antenna Placement: Depends on use

- Some can be connected directly to an AP/be integrated with
- Usually placed in the center of the intended coverage area
- High-gain omnidirectional antennas are typically used in outdoor installations for point-to-multipoint configs

Semidirectional Antenna Placement

- Indoor/outdoor installations
- Mounted indoors: Patch/panel will be mounted flat on wall w/connector upward for connections to cable/directly to AP

Yagi: Indoor/outdoor

- Outdoors: Short-range point-to-point/point-to-multipoint bridging solutions
- Needs mounting bracket such as tilt/swivel for wall mounting | U-bolts/plate for mast/pole mounting

Highly Directional Antenna Placement: Antennas such as parabolic dish: Almost always exclusive in outdoor installs

- Long-range point-to-point bridging links/Install on building rooftops/antenna towers
- Alignment for long-range links: Critical for reliable comm

Minimizing Effects of Multipath Using Antenna Diversity

Reflection: Caused by RF signal bouncing off smooth, non-absorptive surface/changing direction

- Indoor envs prone to reflections

Multipath: Result of 7 wave fronts of receiver being confused about signals: Corrupted signal: Less throughput

Antenna diversity: Reduce effects of multipath

- Tech used where station (AP/client device) will utilize 2 antennas combined w/1 radio
- Multiple antennas/some additional intelligence: Receiver will determine which antenna will receive/send best signal

Diversity systems: 2 antennas spaced at least 1 wavelength apart

- Allows receiver to use antenna w/best signal to transmit/receive

- Antennas required to be same design/freq/gain/orientation

Effects of Wind/Lightning:

Wind: Most outdoor antennas can be affected by wind

- Will have wind-loading data in spec sheet

Wind-loading: Result of wind blowing at high speeds/causing antenna to move

Lightning: Can destroy components if takes direct/indirect strike

- Properly grounded arrestor will help with this

Lightning Arrestors: Transient/induced electrical currents are the result of an indirect lightning strike in WLAN antenna systems

Lightning arrestors: In-series device installed after antenna/prior to transmitter/receiver

- Protection from indirect lightning strikes | No protection from direct strikes
- Electrical currents from lightning strike travel to antenna
- Arrestor will shunt excess current to ground

Grounding Rods: Metal shaft used for grounding device (like an antenna)

- At least 8' deep: Resistance bet 5-25 ohms
- Various types of steel (stainless/galvanized/copper clad)
- Various diameters/lengths
- Don't share grounding rods w/other equipment

Precautions to consider:

- Read installation manual
- Avoid power lines: Can kill
- Use correct safety equip
- Install/use grounding rods when appropriate
- Comply w/regulations for use in area/use of towers

Antenna Mounting: Indoors/outdoors, device/client access, bridging solutions (point-to-point/point-to-multipoint)

Mounting types:

Internal/external (to AP)	Pole/mast	Ceiling	Wall

Internal/External Antennas: Some AP's allow use of integrated/external antennas

Controller-based/cooperative AP's: Integrated antennas

- Some have connectors: Allow for external use

Integrated: Mostly aesthetics (less noticeable)

Disadvantage:

AP w/integrated antennas: Antennas can't be changed to any other type

- Stuck using antenna part of AP
- Unable to add antenna w/higher gain/diff radiation pattern

External w/AP's: External antenna connectors to allow diff antennas

- Allow for higher gain/diff radiation pattern
- Requires SW config that will disable integrated antenna when external antennas install

Pole/Mast Mount: Typically consists of mounting bracket/U-bolt mounting HW (L-shaped)

Wall Mount: Consider polarization of antenna

- Some designed to be mounted on ceiling: Don't mount on wall (especially for AP's w/integrated antennas)
- Match polarization of AP's/devices
- If vertically polarized: Client devices should be polarized in same way

Maintaining Better Communications: Factors affect if 2 devices comm w/each other

- Line of sight (visual/RF)
- Fresnel zone
- Indoor WLAN's: Use low amt of RF transmit power: 30mW-50mW
- Will be able to comm even if device doesn't have LoS to AP
  - RF able to penetrate walls/windows/door
- Outdoor installs use much higher output transmit power
  - Will require RF LoS for effective comm

Visual Line of Sight: 2 points have unobstructed view of one another

RF LoS: 2 devices successfully comm at distance via RF (point-to-point/point-to-multipoint)

- Clear path for RF energy to travel bet 2 points necessary (called RF LoS: Basis of Fresnel zone)

Fresnel Zone: Area of RF coverage surrounding visual LoS.

- Outdoor point-to-point/point-to-multipoint install: Impt Fresnel zone clear of obstructions for transmitter/receiver comm
- 60% for Fresnel zone obstruction-free clearance
- Diff to maintain as distance increases

Obstructions: Trees	Buildings/other structures	Earth curvature	Natural (hills/mountains)

Post 8

Thursday, January 24, 2019 11:42 PM

WLAN TERMINOLOGY/TECH CH.8

WLAN Modes of Operation: Config to op in diff modes for device/usr access
2 modes for access:

- **Ad hoc**
- Infrastructure

Broken down into 3 configs:

- **IBSS: Independent Basic Service Set**
- BSS: Basic Service Set
- ESS: Extended Service Set

IBSS: Independent Basic Services Set: No AP's: Only devices/client machines: Only devices part of same IBSS

- No Centralized control **|** Manageable sec **|** Accounting features
- Certain params must be set on devices: Must be same on all devices

3 common params set on devices:

1. SSID: Service Set Identifier
2. RF channel
3. Security config

SSID	**Service Set Identifier:** Common param: Name used to ID network • Done through discovery phase • Passive/active scanning • Infrastructure: Manually set on AP **Client side:** Usr param set manually in SW: Receives networks that broadcast info • Be unique • Don't divulge who you are/loc of devices (unless public/accessible to all) • Max 32 chars/32 octets
SSID Hiding	Hidden from view for devices attempting to locate • Not effective security/shouldn't be used for it **Disadvantages:** • Increase in roaming times in enterprise deployment • Neighbors may deploy on same chan you're using
RF Channel	

IBSS: Requires usr to set specific RF chan to use on all devices part of same IBSS network

- In client utility SW for network adapter (advanced properties)
- All devices in IBSS must be comm on same chan
- Additional devices wishing to join must do so by scanning passively/actively

IBSS Sec: No centralized control/no sec mgmt features

- Up to individual usr/device
- If usr shares resource: Could expose sensitive info
- Against corporate policy in many orgs

Usually ID by 1 of 3 terms:

1. IBSS: Independent Basic Services Set
2. Ad hoc
3. Peer-to-peer

Comes down to devices connecting to each other w/out use of AP/infrastructure device

- All work independently of 1 another
- Useful in homes/small offices for ease of install

Advantages/Disadvantages: Vary depending on application

Advantages	**Easy config:** Usr specifies SSID, sets RF chan, enables sec setting **No AP HW:** 802.11 adapter built in: No device like AP required

Disadvantages	**Limited RF Range:** Radio comms 2-way: All devices need mutual comm range of 1/another to work well **No Centralized Admin:** Many against sec policy B/C impossible to manage centrally **Not Scalable:** No set max # of devices can be part of IBSS: Capacity low **Diff to Secure:** Usrs may share sensitive info: Provides bridge to company infrastructure

BSS: Basic Service Set: Foundation of WLAN: AP connected to network infrastructure/associated devices

- Foundation b/c may be 1 of many AP's that form WLAN

DS: Distribution System: Each AP connected to network infrastructure

- Allows connected devices to access network resources based on perms

RF area of coverage depends on factors like: Antenna gain, RF output power settings

BSA: Basic Service Area: Area of coverage listed above

- Any 802.11 device on radio range/part of BSA w/config params (SSID/Sec) able to successfully connect to AP
- BSS consisting of 1 AP common in SOHO's/SMB's (small-to-medium businesses)

Decision to use 1 AP depends on things like size of loc/WLAN used/how many devices…

Params to config for BSS:

- SSID
- RF chan
- Sec params

AP will broadcast params about WLAN to devices that want to connect to BSS (min config on client)

- **Unlike IBSS:** RF chan set on AP/not wireless client/device

Advantages/Disadvantages:

Advantages	**Intelligent devices:** Provide usrs w/consistent/reliable/secure comms to WLAN **Useful:** Variety of situations: Homes/SOHO/Small to large businesses **Scalable:** Can increase coverage/capacity by adding more AP's **Centralized admin control:** Params/specific access set centrally
Disadvantages	**Additional HW costs:** Site survey to determine RF coverage/capacity reqs **Must be connected to infrastructure:** Distribution system: Wireless/wired **Additional knowledge**

ESS: Extended Service Set: 1/more interconnected basic service sets (BSS's) that appear as single BSS to LLC (Logical Link Controller) layer at any station (STA) associated w/one of them

1/more AP's connected to common wired/wireless distribution system: Common in WLAN's for small/medium/large enterprises

- Provide consistent/complete coverage across entire org
- Must have matching params: SSID/sec settings
- If SSID's of 2 AP's no match: Considered separate basic service sets: Even if connected by common network infrastructure

Distribution Systems connecting these together/common SSID what make ESS

- BSS basic service area overlaps to allow roaming from 1 BSS to another
- Roaming bet AP's critical of WLAN tech in most modern deployments: WLAN major part of every corporate network

BSA: Basic Service Area: Area of RF coverage/cell that encompasses wireless AP/associated stations

- Device will be contained in BSA as long as required receive signal strength to maintain association state w/AP

SSID/ESSID/BSSID

SSID	**Service Set Identifier:** Network name • Provides segmentation of wireless network
ESSID	**Extended Service Set Identifier:** Term some manufacturers use in place of SSID (synonymous with) • Segmentation of wireless network • Term varies among manufacturers (not defined by 802.11 standards) • More than 1 AP using same SSID/sec settings connected to common DS: Distribution sys
BSSID	**Basic Service Set Identifier:** Unique identifier: MAC address of basic service set (Media Access Control) • Some manufacturers: May allow many BSSID's to be connected to single AP radio ○ Or for a single common BSSID to be shared among many AP's **MAC**: Unique identifier of network adapter/HW address of: 48-bit

	Radio: An AP/network adapter: Used for L1 comms **Ad hoc/IBSS network:** No AP for centralized comm • Devices comm directly w/each other • No config: BSSID randomly generated #: Has same fmt as MAC • Generated by 1st ad hoc device at startup

Connecting to 802.11: In order for device to connect to wireless network: Diff frame exchanges take place

Authentication/Association	Reserving medium	Exchanging data	Power/save functions

Frame Types: Devices comm by sending RF waves to each other through air: Carry data from 1 device to other

- Org into frames: Types play roles depending on info

WLAN's use 3 diff frame types

- **Management Frames**
- Control Frames
- Data Frames

Mgmt	**Manage network:** Assist devices in finding/connecting to wireless network **Includes:** • Advertising capabilities of WLAN • Allowing connections by authentication/association Exchanged only bet immediate devices: AP/client: • Never crosses DLL (Data Link: L2) • Always transmitted at lowest mandatory data rate of service set ○ All stations on same RF chan in basic service area can understand them **Examples:** • Beacon • Probe request • Probe response • Authentication • Association request • Association response
Control	**Control access to wireless medium:** Allows devices to reserve medium/acknowledge data • Sometimes used to request data from AP after returning from power save • Protection mechanisms allow device coexistence **Examples:** • RTS • CTS • CTS to Self • PS-Poll • ACK
Data	**Carry data payload/L3 info bet wireless devices** **Null data/Null function frame:** Helps implement power save features/not carry data payload **QoS null frame:** Variant of null frame: QoS functions **Examples:** • Data • QoS data • Null data

Network Discovery: Process of client device looking for networks/ID'ing params of network

SSID	Supported data rates	Sec settings

Passive Scanning: 1st part of discovery phase

Allows devices to "listen" for info about networks in radio receiving area of network/basic service area

- During process: Devices listen for specific info to make them aware of networks in area
- Mgmt frames assist WLAN devices in finding/connecting to wireless network

Example: Beacon frame:

- Frame advertisement of network

- Carries specific info about AP/basic service set [SSID, RF chan/avail data rates config, sec params etc..]

During phase: Devices listen for beacons advertising details about networks in area/radio range of device

- Devices constantly listen for beacon frames

Beacons:	**Broadcast:** 10x second **Value:** 1024 microseconds **TBTT: Target Beacon Transmission Time** • Interval can be changed/only if recommended

Active Scanning: 2nd part of discovery phase

Devices wishing to connect to network send out mgmt frame known as probe request

- Finds specific AP to connect w/
- Depends on SW used: If SSID specified in active profile: Device will join network w/matching SSID
    - **Exception**: **Wildcard/Null SSID:** Type of probe request
- **802.11:** Requires all AP's to respond to null/broadcast probe requests
- Probe request frame won't specify SSID value/rely on AP's to provide SSID in probe response frame

AP's constantly listen for probe request frames

- Any AP w/in hearing range of device/having matching SSID sends out probe response frame to device
- If more than 1 AP responds: Device selects best AP to connect w/based on certain factors (signal str/quality)

Frames used for active scanning:

During active scanning: 2 frames exchanged bet device/AP

1. Device sends broadcast probe request frame to all devices (including AP's in radio range)
2. AP's send probe response frame to device so it can ID params of network before joining

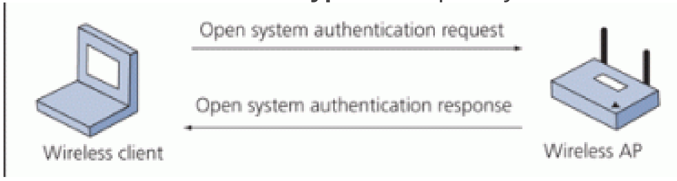
802.11 Authentication: Authentication: Verifying/confirming identity: We use it all the time:

- Logging onto computers/networks
- Accessing secure websites
- ATM's
- Using badges at a job

Different than regular authentication methods:

– Providing credentials (usr/pass) is used to gain access to network/participate in data frame exchanges

Authentication method types: 1. Open system 2. Shared key


Open system authentication request
Open system authentication response
Wireless client
Wireless AP

Open System Authentication: A null authentication algorithm: 2 step process

2 mgmt frames are exchanged bet the wireless device/AP

- 2-way frame exchange b/c 2 authentication frames sent during process
- **Not request/response: Authentication/success**

Can't really fail unless other security measures (MAC filtering) are put in place

- Will prevent the device from accessing networks

Always exists: Used to allow wireless stations to connect to AP's

After association: Open system uses additional credentials (usr/pass pair) for authentication

- If wireless station didn't perform open sys auth/association 1st: No way to use added sec mechanisms

RSN: Robust Security Network: A protocol for establishing secure communications over 802.11 wireless networks

- Part of the 802.11i
- Only valid authentication process allowed w/newer WLAN sec amendments to be considered for an RSN

LAN device to AP: *"Can I be part of network?"*

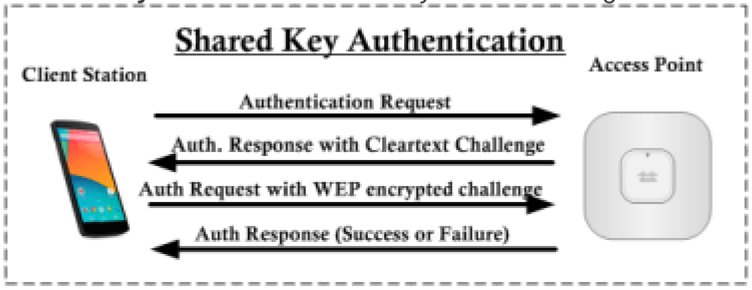
AP responds: *"Sure"*

Process: 1 mgmt frame sent at each step

1. WLAN device wanting to auth sends auth frame to AP: Frame acknowledged by AP

2. AP accepting auth sends successful auth frame to device: Frame acknowledged by auth device

Shared-Key Authentication: 4-way frame exchange


Shared Key Authentication
Client Station
Access Point
Authentication Request
Auth. Response with Cleartext Challenge
Auth Request with WEP encrypted challenge
Auth Response (Success or Failure)

- mgmt frames sent between device wanting to join/wireless network/AP

Differs from open system:

- Shared-key used for **both** 802.11 authentication **AND** data encryption

Flaws: Authentication key and encryption (WEP key) can be captured

- If someone captures the 4 frames used in process: The WEP key could be extracted
- Requires use of WEP for both wireless device auth/data encryption: WEP is mandatory

Should be avoided: Not allowed with 802.11i/WPA/WPA2: Open system considered more secure

Process:

1. WLAN device wanting to auth sends auth frame to AP: Frame acknowledged by AP
2. AP sends frame back to device that contains a challenge text. Frame acknowledged by device
3. Device sends a frame back to AP containing encrypted response to challenge text:
    - Response encrypted using device's WEP key. Frame acknowledged by AP

1. After verifying response: AP accepts auth/sends "*successful auth*" frame back to device:
    - Final frame acknowledged by device

Association: Takes place after device has been successfully authenticated by open system/shared-key

Association state: Auth device can pass traffic across AP to network/devices: Allows access to resources device/usr has perms to

After device auth/associated: Considered part of basic service set

- Device must be authenticated before it can be associated
- After association: Auth/association complete: More sophisticated auth mechanisms (802.1X/EAP/pre-shared key) can be used

Frames used for 802.11 Association

After authentication: Association begins: Allows a wireless device to send info across AP to network infrastructure:

1. WLAN device sends association request frame to AP: Frame acknowledged by AP
2. AP sends association response frame to device: Frame acknowledged by associating device

Deauthentication/Disassociation: Opposite of authentication/association can also happen

Deauthentication: When existing auth no longer valid (can be WLAN device logging off/roaming to diff BSS)

Disassociation: When association to AP terminated (may occur when associated device roams from 1 BSS to another)

Both are notifications: NOT requests

Since neither can be refused by either side: Both considered auto successful from sender's perspective

Unless 802.11w implemented: Deauthentication can be considered sec issue

- Frames can be used for DoS attacks/to hijack device
- Both frames management frames

The Distribution System: Common network infrastructure to which AP's are connected: Can be wired/wireless

- AP acts like L2 translational bridge

Translational bridge: Device used to connect 2/more dissimilar types of LAN's together (802.11/eth0 802.3)

Receivers perspective:

- Allows AP to take info from air/make decision either to send back out to same wireless radio/fwd it across to DS
- AP's have enough intel to determine if data frame destined to be sent to DS/if it should stay on wireless side of network
- AP knows whether device is part of WLAN side through auth/association methods

DS: Network segment that consists of 1/more connected basic service sets

ESS: Extended Service Set: 1/more interconnected basic service sets

- DS allows WLAN devices to comm w/resources on wired network infrastructure
    - Or comm w/each other through wireless medium
- ALL wireless frame transmissions traverse through AP

WDS: Wireless Distribution System: Connects basic service sets together using WLAN tech

- May be feasible/justified to use WDS
- Best way to use WDS: Use 2 diff radio tech in same AP's

Example: 2.4GHz band for wireless device access/5GHz band for DS:

- Will limit contention/provide associated devices better exp b/c 1 radio used for devices/other the WDS

Data Rates: Speed wireless devices are designed to exchange info at

- Differs depending on standard/amendment/spectrum type/Physical Layer tech in use
- Don't accurately present amt of info actually transferred bet devices/wireless network

Data rates based on spread spectrum type

Standard	Tech	Data Rates
802.11	FHSS	1/2 Mbps
802.11	DSSS	1/2 Mbps
802.11b	HR/DSSS	5.5/11Mbps | 1/2 Mbps from DSSS
802.11a	OFDM	6/9/12/18/24/36/48 Mbps
802.11g	ERP-OFDM	6/9/12/18/24/36/48 Mbps
802.11n	HT-OFDM	Up to 300 Mbps

Throughput: Amt of info actually being correctly received/transmitted
Unlike data rate (max amt of info theoretically capable of being sent)

Variables affect throughput of info sent:

- Spread spectrum/Physical Layer tech in use
- RF interference
- #r of devices connected to AP

DRS: Dynamic Rate Switching: When device moves through BSA (basic service area)

- Distance from AP increases: Data rate decreases
- Device moves closer to AP: Data rate increases

DRS: Dynamic Rate Switching: AKA Dynamic shifting/dynamic rate selection:
Allows associated device to adapt to RF in particular location of BSA

- Accomplished through proprietary mechanisms by manufacturer
- Main goal: To improve performance for devices connected to AP
- **As device moves away from AP:** Received signal decreases b/c of **FSPL: Free Space Path Loss**
    - When occurs: Modulation type will change b/c RF signal quality less
    - Using less complex modulation type at lower data rate: Provides better performance as station moves away from AP

WLAN Roaming/Transition

Roaming: When device moves from 1 basic service set/AP to another

- Not addressed in original 802.11 standard
- When device moves through BSA/receives signal from another AP: Needs to make decision whether to stay associated
    - Or to re-associate w/new AP
- Decision completely proprietary

Some criteria manufacturers use:

- Signal strength
- Signal-to-noise ratio
- Error rate
- # of currently associated devices

When device chooses to re-associate to new AP: Original AP hands off association to new AP as requested from it

- Move done over wired network/DS based on how manufacturer implemented roaming criteria

Frames Used for Reassociation: When device move/roams to new AP: Needs to associate to new AP
B/c device is already associated: Must complete reassociation process:

1. WLAN device sends reassociation request frame to new AP: Frame is acknowledged by new

AP

2. New AP sends reassociation response frame to device after handoff across DS from original AP: Frame acknowledged by reassociating device

Power Save Operations: Designed to allow device to enter dozing state in order to conserve DC power/extend battery life

- Many devices portable/use DC power
- Especially true w/newer 802.11n adapters that support MIMO
- If devices plugged in: No need to use

2 diff power save modes

- **AM: Active Mode**
- PS: Power Save mode

PS mode: Considered legacy: Still used for lots of devices

- 802.11e for QoS addresses more efficient power save mechanisms
- Null function frame used w/power mgmt/doesn't carry any data: Used to inform AP of change in power state

Active Mode: When device/station (STA) may receive frames at any time/always in "awake" state

- Not relying on battery power
- Some manufacturers refer to as **CAM: Continuous Aware Mode**

Power Save Mode: In PS mode: Device/STA will doze/enter low power state for short periods of time At specific intervals: Device will "listen" for selected beacons/determine if data is waiting for it (buffered) at AP

- Beacon frame contains info for associated devices regarding power save
- When device associates to AP: Device receives **Association ID (AID)**
- AID is value that represents device in various functions (including PS mode)

Beacon frame contains indicator for each AID device to let them know whether they have data waiting/buffered at AP

- If determined that AP has data buffered for specific device:
- Device will send control frame msg (PS-Poll frame) to AP to request the buffered data

APSD: Automatic Power Save Delivery: Differs from original PS mode: Trigger frame will wake device in order to receive data

- More efficient power save functions
- Works well w/time-bound apps subject to latency (voice/video)

Protection Mechanisms: Backwards compatibility designed to allow diff tech to coexist in same RF space

2 broad categories of protection mechanism:

1. **ERP: Extended Rate Physical** protection mechanism 802.11g networks
2. **HT: High-throughput** protection mechanism for 802.11n networks

Each category includes modes for specific situations:

802.11g ERP Mechanisms	**To coexist w/802.11b devices in same BSS area: AP must have ERP protection** • Most WLAN equip will provide options for coexistence **1 of 3 modes:** • **802.11b Only: DSSS | HR/DSSS** • **802.11g Only: ERP-OFDM** • **802.11b/g mixed: DSSS | HR/DSSS | ERP-OFDM**
802.11b-Only	**Disables all 802.11g ERP-OFDM data rates of 6/9/12/18/24/36/48/54 Mbps** • Allows only DSSS rates of 1/2 Mbps and HR/DSSS rates of 5.5/11 Mbps • Limits max data rate to 11 Mbps • Limited apps such as using legacy 802.11b only capable devices
802.11g-Only	**Opposite of 802.11b only mode** • Disables all 802.11b DSSS | HR/DSSS data rates of 1/2/5.5/11 Mbps • Allows 802.11g ERP-OFDM rates of 6/9/12/18/24/36/48/54 Mbps • Useful in env where backward compatibility to 802.11b not required • Throughput needs to be max
802.11b/gMixed	**Allows devices that support g/b devices to operate together in same BSA/associated to same AP** • Uses control frames to reserve wireless medium **2 options:**

	1. **RTS/CTS: Request to Send/Clear to Send:** Control frames as protection mech to reserve RF medium 2. **CTS to self:** Single frame used as protection mech. Common implementation by WLAN equip **Benefit:** Less overhead than RTS/CTS **RTS/CTS-to-Self-control frames:** Devices using diff Physical Layer tech to share medium/avoid collisions • Control frames say time needed for frame exchange bet transmitter/receiver to complete • Time value processed by all devices in BSA not part of frame exchange • Once time expired: Medium considered clear

802.11n High-Throughput Protection Mechanisms: Operate in 2.4GHz/5GHz

- Backward compatibility for 802.11a/b/g devices need to be taken into consideration
- Modes for HT protection mechanisms

Mechanisms known as HT protection modes: Set of rules devices/AP's use for compatibility:

- **Mode 0 – Greenfield mode**
- Mode 1 – HT nonmember protection mode
- Mode 2 – HT 20 MHz protection mode
- Mode 3 – HT Mixed mode

Mode 0 – Greenfield	**Allows HT (high-throughput) devices only** **HT devices must also share op functionality/must match:** Example: Must all support 20MHz or 20/40MHz chans only If 802.11n HT AP set to 20/40MHz chan width/client capable of only 20 MHz wide chan associates: *Connection isn't considered Greenfield* • Doesn't allow 802.11a/b/g devices using same RF chan • Not able to comm w/AP in Greenfield mode • Transmissions from devices cause collisions at AP: Degradation: Seen by HT sys as RF interference
Mode 1 – HT Nonmember	**All devices must be HT-capable** • When non-HT device (a/b/g) AP/client device w/in hearing range of HT AP ○ and on same 20 MHz chan/1 of 20/40 MHz wide chans: Protection mode activated
Mode 2 – HT 20 MHz	**All devices must be HT-capable** • Based on 802.11n devices can use 20 MHz or 20/40 MHz wide chans • 1 20 MHz HT STA associated w/HT 20/40 MHz AP: AP provides compatibility for 20 MHz devices
Mode 3 – HT Mixed	1/more non-HT stations associated in BSS • Mode allows backward compatibility w/non-802.11n or a/b/g devices • Most common mode for 802.11n HT networks • B/c of need for backward compatibility/legacy devices still in use
Additional HT	**2 other HT protection modes also available:** 1. **Dual CTS:** L2 protection mech used for backward compatibility bet 802.11n HT/a/b/g devices 2. **PCO: Phased Coexistence Operation:** Optional BSS mode w/alternating 20 MHz/20/40 MHz phases controlled by PCO-capable AP

Post 9

Thursday, January 24, 2019 11:43 PM

WLAN SECURITY BASICS CH 9

Concerns of threats:

Eavesdropping	RF DoS	MAC address spoofing
Hijacking	MITM	Peer-to-peer attacks
Encryption cracking		

802.11 original standard addressed 2 areas of sec:

1. Authentication
2. Data privacy

Authentication: Confirming identity: You are who you say you are
Data privacy: Ensuring data is understandable only by who it's intended for
Types of authentication: Diff: Performed by WLAN protocol/except for shared-key doesn't need usr intervention

1. Open system
2. Shared-key

Open System Authentication: 2-step process: 2-frame exchange: **Null authentication**
Shared-Key Authentication: 4-step process: Don't confuse w/WPA/WPA2 personal (uses pre-shared key)

- WEP mandatory to function: Both authentication/data encryption
- **WEP insecure: Shared-key insecure**
- Intended to protect usrs against casual eavesdrops

Early WLAN Sec Tech: Looked good on paper: Bad in practice
Common WLAN Legacy sec solutions:

- SSID hiding
- MAC filtering
- WEP

Early adopters had no choice but to use these
SSID: Name for wireless network: Device segmentation

- Devices ID/connect to WLAN using discovery phase
- Includes passive/active scanning

Passive scanning: Client device listens for beacon frames

- SSID specified in beacon frame in info element: Advertise network
- Default: Broadcast 10x second

Specify SSID to be joined: Probe request frames w/intent of joining

- 802.11 standard requires AP to respond to all probes that have matching SSID: AKA **wildcard SSID**

Wildcard SSID: Value of 0: **AKA null SSID:** When client doesn't specify SSID
SSID Hiding: Disables SSID broadcasting: Would normally appear in broadcast beacon frames
If isn't broadcast: Network may not be seen by devices that don't know it

- No broadcast in beacon frames? Can still ID in other frames: Probe responses
- Anyone w/packet analyzer: Can determine SSID by monitoring frames sent through air
- Shouldn't be used for sec: Sometimes to prevent usrs from trying to connect to wrong network

Media Access Control Address: Unique HW identifier of network device: 6-byte address: L2: Allows frames sent/received

- No 2 devices should have same L2 MAC
- Easily visible to anyone using packet analyzer
- Req for network to send/receive info: Can't be encrypted

MAC Address Filtering: Physical/DLL: Allow/disallow access by restricting which MAC's authenticate/associate

- Weak/easy compromise
- Wireless uses air as medium: RF exchanges info bet devices

MAC Address Spoofing: Tricking device into thinking MAC is something other than what's on card
7 ways for an intruder to accomplish:

- Utilities like SMAC
- W/in OS

- MS Win registry
  - May enter new MAC value in driver config: Considered modifiable address
  - May be stored in config file/nonvolatile mem
  - Only changes SW reference OS sees/uses
  - Doesn't change BIA (Burned-In Address)/hard-coded address: Unmodifiable

WEP: Wired Equivalent Privacy:

- All info including data payload, travels through air from 1 device to another
- Open system all info broadcast through air in plain text
- Simple to implement: Requires all devices have same WEP key
- Key can be 64/128 bit: Standard only required 64

Disadvantages:

- Uses static keys: All devices/AP's/bridges/stations must have same key/must be manually entered
- No matter which used (64/128bit), still only using 24-bit IV: Both vuln to same attacks
- Keys cracked easily/Insecure/Easy to capture data using packet analyzer

SOHO/Enterprise Sec Tech: 802.11i improvements in sec: Amendment introduced **RSN: Robust Secure Network**

- In order to create RSN: Must be RSN capable/802.11i compliant
- Optionally supports **TKIP (Temporal Key Integrity Protocol)**
- Must support **CCMP (Counter Mode w/Cipher-Block Chaining Message Auth Code Protocol)**
- SOHO/Enterprise: WPA/WPA2 **|** Home: WPS

Wi-Fi Protected Setup: PIN-Based/Push-Button Config: Simplified process of securing network for SOHO/home usrs

WPS: Wi-Fi Protected Setup: Cert addresses both solutions

PIN-Based Sec: PIN: Personal ID #: Required for device to be WPS (Wi-Fi Protected Setup) certified

- PIN to be entered on all devices part of same network
- Fixed label/sticker on device/dynamically generated
- Diff bet PIN/pass: PIN numerical
- AP detects when new device that supports WPS in radio range
- When tries to join network: Prompts usr to enter PIN: Once entered auth device/encrypts data sent to/from it

PBC: Push-Button Config Security: Usrs config WLAN w/"push of button": 1 step process

- Usr pushes HW button on gateway/clicks SW button: Creates connection bet devices
- It configs network's SSID/turns on sec

SES: SecureEasySetup: Linksys ver of push-button: All devices must support feature: 1st button pushed on HW then SW

- Devices w/in RF hearing range participating become part of network
- Support for both PIN/PBC configs required for AP's
- Client devices: Min must support PIN

NFC: Near Field Communication: 3rd option: Tokens: USB may be used to store/transfer creds

Many SOHO equip manufacturers have WPS

Some include:

Belkin	Broadcom	D-Link	Linksys	Netgear	TRENDnet	ZyXEL

Wi-Fi Protected Access/WPA2 Personal Sec: Passphrase-based sec: SOHO/home usr: Usr can create sec w/out exp/knowledge

- All devices part of same network must have same 256-bit pre-shared key (PSK)
- Usr enters strong passwd on all devices part of same WLAN

Passwd Chars	○ 8-63 ASCII (case sensitive)/64 hex chars ○ Creates 256-bit pre-shared key ○ Longer/more random: More sec ○ Weak passwds compromised

WPA/WPA2 Enterprise Security: L2: IEEE standard: Advanced enterprise solution 802.1X: AKA user-based sec

User-based security:

- Admin can restrict access to resources by creating usrs in centralized DB
- Anyone joining: Required to auth by valid usr/pass
- Successful auth? Gain access w/perms

802.1X/EAP: 2 diff components used together to form enterprise sec solution

802.1X: Port-based access control method: Designed to work w/802.3 eth networks: Adapted into wireless as alt

- Devices that use 802.1X ID’d using diff terminology

Terminology as follows:

- **Supplicant** (client device)
- **Authenticator** (AP)
- **Authentication server RADIUS/AAA auth server**

Supplicant	**Another name? Client device attempting to connect** • SW sec component of client
Authenticator	**Wireless AP/WLAN controller** • Middleman bet supplicant/auth server • Supplicant requests join: Authenticator passes auth info bet 2 devices
Auth Server	**ID server will auth wireless supplicant** • Receives all info from authenticator • Server may be AAA/RADIUS

EAP: Extensible Authentication Protocol: Allows for auth process: 802.1X will employ some EAP to complete

- Diff types EAP avail: Can be used w/802.11
- Vary from proprietary solutions to very sec standard solutions

Examples of EAP types:

EAP-TLS |	**TTLS (EAP-MSCHAPv2) |**	**PEAP (EAP-MSCHAPv2) |**	**EAP-FAST**

RADIUS: Remote Authentication Dial-In User Service: Networking service: Centralized auth/admin of usrs

- Started as way to auth/authorize dial-up networking usrs
- User dial up using **PTSN (Public switched telephone network)**/modem
- Usr prompted by remote access server to enter usr/pass to auth
- Once creds valid: Access to resources

Took decentralized remote access service DB’s/combined them in 1 central location

- Centralized usr mgmt
- AP can act as RADIUS client: Capability to accept requests from client devices/fwd them to RADIUS server for auth
- Client device is auth as usr in DB of RADIUS server
- Server authenticating server/DB
- May also be AAA: Auth/Authorization/Accounting server
  - In this config: Will auth usrs/provide access to resources they have perms to
  - Keeps track of all transactions by accounting

AAA: Auth/Authorization/Accounting: Protocol provides framework 4 sec access/authorization/keeps track of usr activity

3 components of AAA protocol:

1. Authentication
2. Authorization
3. Accounting

Authentication	**Validating identity** • 802.1X/EAP/usr-based auth common • Addition to usr/pass networks: Other auth methods like digital certs/smart cards
Authorization	**Access to resources a device/usr has perms to** (tied to usr/group/object) • After auth: Protocol allows authorization • Functionality: BW controls/time restrictions/controls/QoS policies
Accounting	**Keeps track of every place usr visits/everything done** • Monitors network activity • Can track resource usage for SW/HW/budgeting purposes • Can determine what tech diff areas using/how they contribute to cost

Encryption Methods

3 diff encryption mechanisms used:

- **WEP: Wired Equivalent Privacy: Mentioned earlier/insecure**
- TKIP: Temporal Key Integrity Protocol

- CCMP: Counter Mode w/Cipher Block Chaining Message Authentication Code Protocol

TKIP: Temporal Key Integrity Protocol: Designed as firmware upgrade to WEP: Added 7 enhancements to WEP alg

- Foundation for Wi-Fi Protected Access cert (WPA)

Enhancements include:

- Per-packet key mixing of IV to separate from weak keys
- Dynamic keyring mechanism to change encryption/integrity keys
- 48-bit IV/sequence counter: Prevent replay attacks
- MIC: Message Integrity Check: Prevent forgery attacks
- RC4 stream cipher: Backward compatibility w/WEP

Config network to use TKIP: w/web or CLI

CCMP: Counter Mode w/Cipher Block Chaining Message Authentication Code Protocol:

- Mandatory part 802.11i amendment/802.11-2012 standard/WPA2 cert
- AES: Advanced Encryption Standard alg block cipher
- Mandatory for RSN compliance
- Intended as replacement to TKIP
- Strong encryption may require replacement of legacy HW
- May use separate chip to perform computation-intensive AES ciphering
- Similar to TKIP: Diff: Older HW may not support

Wi-Fi Alliance sec method	Authentication method	Encryption/cipher method
WPA – Personal	Passphrase	TKIP/RC4
WPA – Enterprise	IEEE 802.1X/EAP	TKIP/RC4
WPA2 – Personal	Passphrase	CCMP/AES or TKIP/RC4 (optional)
WPA2 – Enterprise	IEEE 802.1X/EAP	CCMP/AES or TKIP/RC4 (optional)

Role-Based Access Control: RBAC: Way of restricting access to authorized usrs

- Access from auth: Based on specific roles rather than usr ID's
- May fit will w/AAA b/c of similarities
- Usrs/groups
- Various activities: Amt of throughput/enforcing time restrictions/controlling access to specific resources

VPN: Virtual Private Networking: Create private coms over public network infrastructure

- Protocol based: L3 (Network): Some work at L2

2 parts:

1. Tunneling
2. Encryption

Standalone VPN tunnel: No data encryption: VPN tunnels created across IP networks

- Use encapsulation methods: 1 IP frame encapsulated w/in 2nd IP frame
- Encryption performed as separate function

2 common VPN protocols:

- **PPTP: Point-to-Point Tunneling Protocol**
- L2TP: Layer 2 Tunneling Protocol

PPTP: Point-to-Point Tunneling Protocol: Vendor consortium that included MS

- Popular b/c of ease of config/included w/Win since 95
- MS Point-to-Point Encryption (MPPE-128) Protocol for encryption
- Both tunneling/encryption for usr data

L2TP: Layer 2 Tunneling Protocol: Combo of 2 diff tunneling protocols

- **Cisco's L2 Fwding (L2F)**
- MS's PPTP

Defines tunneling process which requires some lvl of encryption in order to function

- Popular to use IPSec for encryption
- L2TP: 1999: Proposed standard
- More secure than PPTP

3 Components VPN Solution:

1. **Client side** (endpoint)
2. **Network infrastructure** (public/private)
3. **Server side** (endpoint)

WIPS: Wireless Intrusion Prevention System: SW/HW monitors radio waves/using sensor: Captures info recorded in DB

- Takes appropriate countermeasures
- Countermeasures based on ID'ing intrusion: Compares captured info to intrusion sig DB w/in WIPS server

Advantages:

- Captures info: 24/7 monitoring
- Detects threats such as DoS/rogue AP's
- Notifies about threats through variety of mechanisms
- Integrated spectrum analysis
- Elaborate reporting sys
- Ensures compliance w/corporate sec policy/legislative
- Retains data for forensic investigation
- Uses HW sensors for monitoring

24/7 Monitoring	**ID's potential attacks 24/7** • Includes: DoS on L1 RF/L2 SW: Deauthentication storm • Finds rogue AP's/misconfig devices
Detection/Mitigation	**Unlike WIDS: WIPS has capability to detect/react** • Solutions auto respond to threats by stopping device/process that contains threat • Before it has chance to cause damage
Threat Notification	**Notifications based on potential threats encountered during monitoring** • Variety of ways: Such as email/pager
Integrated Spectrum Analysis	**Admin can view remote radio env at branch office/remote location** • Accurate diagnosis of spectrum problems: Including L1 DoS
Reporting System	**Admins create customized reports in short time period** • Enables org to meet specific reqs of audit groups (internal/external)
Regulatory Policy Compliance	**Helps ensure org maintains necessary legislative compliance** • Reqs include HIPAA/PCI: Payment Card Industry
Retains Data for Forensics	**May be used in investigations** • Provides proof org may need to take action on events recorded • Fine-tuning to eliminate misrepresentation of threat sigs sys detects • Baseline of env: Admins gauge lvls of detection/reaction
HW Sensors	Either dedicated HW sensors/share sensor functionality w/AP's • Will collect data by monitoring air 24/7/allowing info to be reported to DB

Overlay/Integrated WIPS Tech: HW sensors for monitoring/sending data to server: Dedicated devices/share functionality w/AP

Terminology:

1. Overlay WIPS sensors
2. Integrated WIPS sensors

Overlay WIPS Sensors: Dedicated devices: Physical chars similar to AP's: Only used for scanning air/sending data to WIPS server

- Passive/will not interfere w/other devices
- Don't need 1 WIPS sensor w/every AP
- Commonly 1:3/1:4 ratio

Disadvantage: Extra cost for dedicated sensors

- Some AP can run as a dedicated sensor: Cost would be same as AP

Integrated WIPS Sensors: Part of AP function: Maybe dedicated radio for FT WIPS monitoring

- May share radio w/AP for PT WIPS monitoring
- Dedicated WIPS radio built into AP will monitor air/send data directly to server FT

Advantage: Cost less than overlay (no separate sensors)

- Other type of integrated WIPS sensor shares radio w/AP

Disadvantage: WIPS monitoring will only be PT/won't capture everything
Captive Portal: Redirects usr to auth source of some kind before they access WLAN: Usually webpage
May include:

- Enter creds
- Input payment info
- Agree to terms/conditions

WNMS: Wireless Network Mgmt/Monitoring Sys: Centralized SW run on server/HW as standalone appliance

- Manage/control entire WLAN centrally
- Can also incorporate WIPS tech for complete mgmt/monitoring/sec solution

WNMS solutions from various manufacturers:

Manufacturer	Solution	Description
Aerohive	HiveManager NMS	Cloud-based, public/private cloud using VM
Aruba Networks	AirWave	Also vendor-neutral/multi-vendor
Cisco	Cisco Wireless Control System (WCS)	
HP	HP Intelligent Mgmt Center (IMC)	
Meraki		Cloud-based
Motorola	AirDefense Services Platform (ADSP)	HW appliance/VM
Xirrus	Xirrus Mgmt System (XMS)	SW, App, Cloud-based

Physical Layer Monitoring: Allows engineer to see what's happening in air as it relates to RF

- Use of spectrum analyzer
- Interference from WLAN/other devices such as 2-way radio/microwaves visible w/spectrum analyzer
- Detects L1 sec issues such as narrow-band/wide-band RF DoS

Manufacturers of WLAN spectrum analyzers:

Manufacturer	Solution	Comments
AirMagnet/Fluke Networks	Spectrum XT	
Cisco	Cisco Spectrum Expert	Formerly Cognio
Fluke Networks	AirCheck Wi-Fi Tester	Handheld device
MetaGeek	Chanalyzer	

Data Link Layer Monitoring: Looks at L2 info: Engineer views WLAN frames that traverse air/potential performance/sec issues

- Protocol analysis tools: Viewing both frame exchanges/frame decoding by expanding on captured frames
- Some can capture/reconstruct TCP/IP frames/reconstruct session/allow pages to be seen/email read from captures

Common protocol analyzers:

Manufacturer	Solution	Comments
AirMagnet/Fluke Networks	WiFi Analyzer	
MetaGeek	Eye P.A.	
Tamosoft	Commview for WiFi	
Wildpackets	OmniPeek Network Analyzer	
Wireshark		Formerly Ethereal

PCI Compliance: Payment Card Industry: Regulation requires companies to adhere to sec standards created to protect card info
Must meet following 6 criteria:

1. Build/maintain sec network
2. Protect cardholder data
3. Maintain vuln mgmt program

4. Implement strong access control measures
5. Regularly monitor/test networks
6. Maintain info sec policy

HIPAA Compliance: US Health Insurance Portability and Accountability Act of 1996:
Standardized mechanisms for data exchange/sec/confidentiality of all healthcare-related computer info/data

2 parts:

1. HIPAA, Title I
2. HIPAA, Title II

- Someone loses job? Title I protects health insurance
- Title II: Mandatory regulations require extensive changes to way healthcare providers conduct business by securing computer info/data