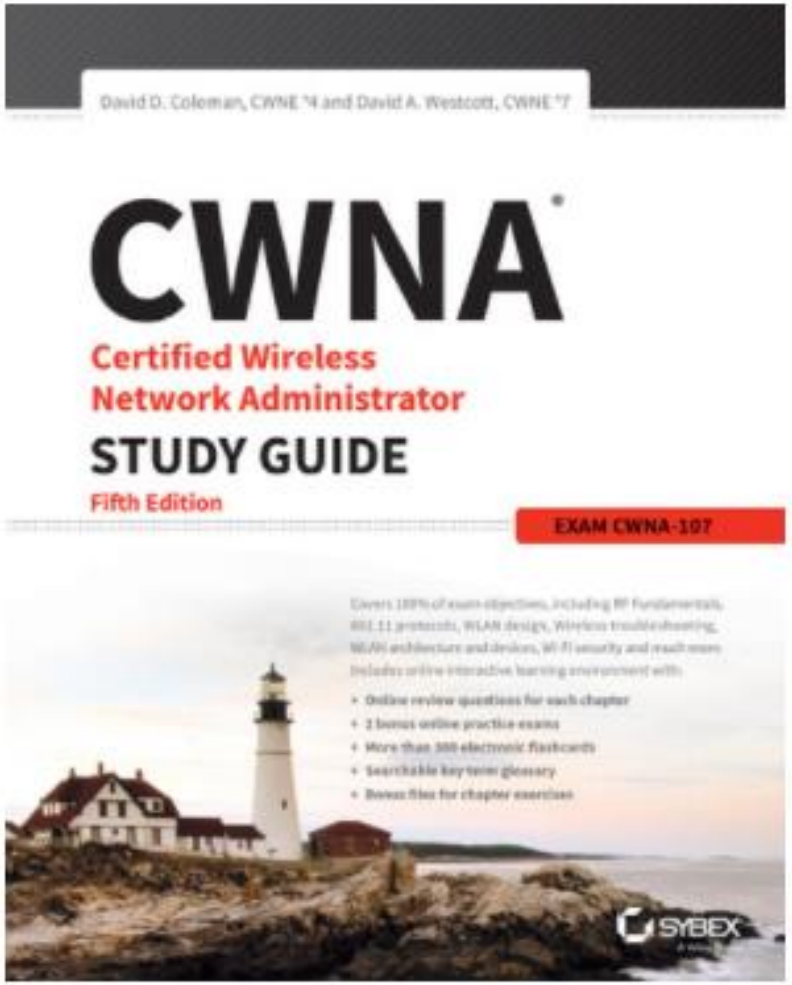
ICA0008
Fundamentals of Wireless LANS

Tauseef Ahmed, PhD

Introduction

- Assessment: Pass/Fail
- ECTS Credits: 3.0
- Book: CWNA® Certified Wireless Network Administrator Official Study Guide, 5e
- Course page: Moodle
- Enrollment Key: **2021ica0008fall**
- Friday:
  - Lectures + practice (total 4)
    - 12:00-15:15
    - practices (total 4)
    - 10:00 – 13:30

Course Book


David D. Coleman, CWNE #4 and David A. Westcott, CWNE #7
CWNA
Certified Wireless
Network Administrator
STUDY GUIDE
Fifth Edition
EXAM CWNA-107
SYBEX

Assessment criteria

- Practice Exercises (labs) = 50%
  - Minimum 2 labs are mandatory to eligible for final theory exam.
  - Every lab must be completed within schedule time.
- Final Exam (Theory) = Total 50 %
- If points_achived ≥ 51:

  Pass
- Else

  Fail

Lecture 1

- Introduction to WLANs
- Wireless standards, organizations, applications
- IEEE 802.11
- 802.11 Medium Access
- 802.11 MAC
- Wireless LAN Topologies
- Wireless LAN Architecture

Over 10 years ago

Wi-Fi laptop

I can use Wi-Fi in the meeting room, but I lose signal if I move away

Everything else is wired

Wired Phone

I heard that some phones have Wi-Fi capabilities, but where would I use them?

Then…

I get Wi-Fi from home, the office, most public places, some streets

Multi Wi-Fi

Like most people, have 2 or 3 Wi-Fi devices

More Applications

I rely on Wi-Fi for critical applications… and do not see why video is so slow…

Now…

802.11ac
802.11n
Everything uses Wi-Fi…
Everything?

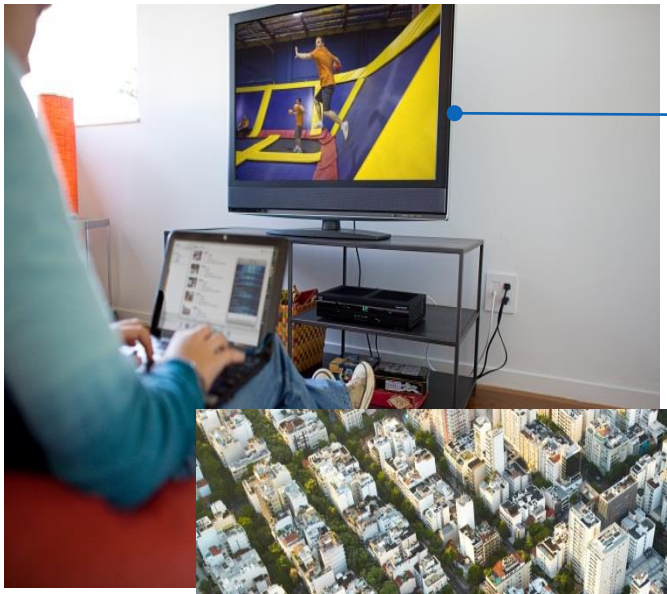
Far Reaching Wi-Fi

I get Wi-Fi from
almost everywhere

More Applications

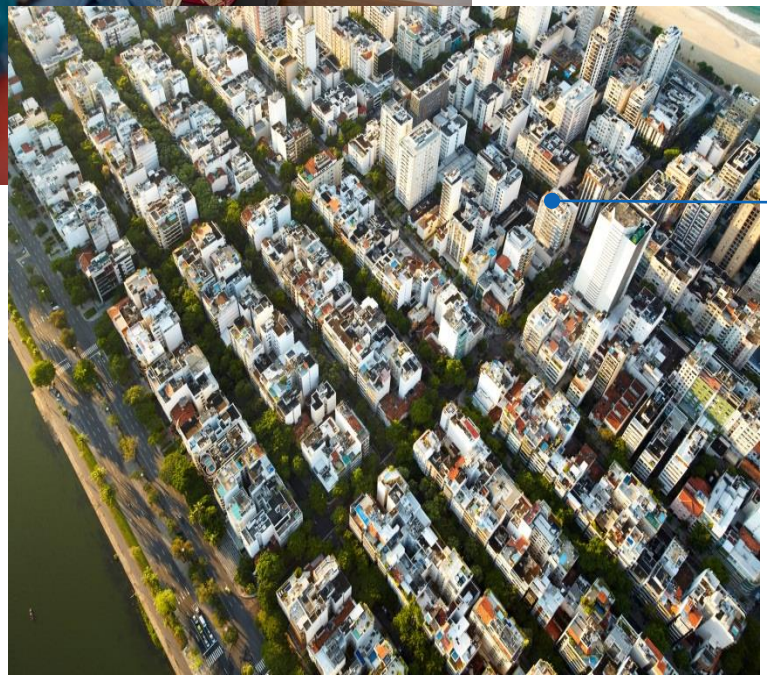
Everyone uses Wi-Fi…
for almost everything

....



802.11ac -> 802.11ad

Your media server can stream to your TV, your laptop, your phone, your tablet… multiple streams everywhere in the house



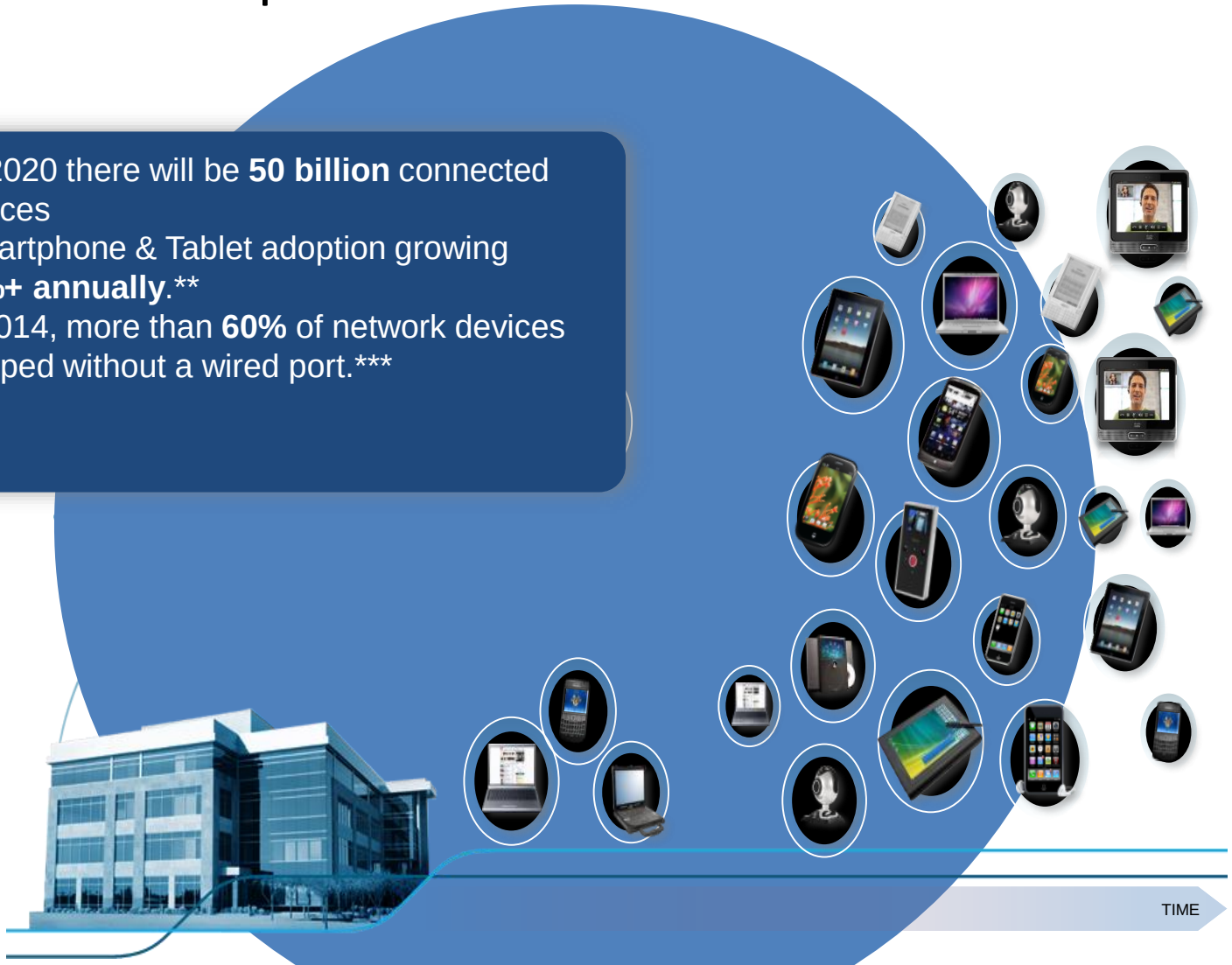
802.11ah – Wireless for IoT

Wi-Fi is used to monitor your electricity, gas meters, industrial sensors (wind-mills etc.), hospital remote patients vitals, etc.

9

Explosive Mobile Device Growth

- In 2020 there will be **50 billion** connected devices
- Smartphone & Tablet adoption growing **70%+ annually**.**
- In 2014, more than **60%** of network devices shipped without a wired port.***

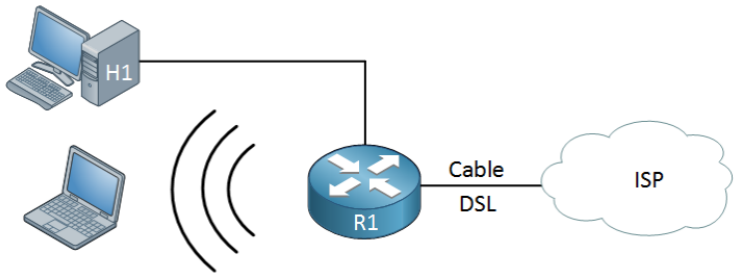


Source: *ABI Research, **IDC, *** Morgan Stanley Market Trends

Wireless Local Area Network (WLAN)

- A wireless local area network (WLAN) is a local area network (LAN) that does not rely on wired **Ethernet** connections. A **WLAN** can be either an extension to a current wired network or an alternative to it.
- WLANs have data transfer speeds ranging from 1 to 54Mbps, with some manufacturers offering proprietary 108Mbps solutions
- The wireless signal is broadcast so everybody nearby can share it
- Several security precautions are necessary to ensure only authorized users can access designated WLAN
- A WLAN signal can be broadcast to cover an area ranging in size from a small office to a large campus, commonly, a WLAN access point provides access within a radius of 65 to 300 feet (~20 to 90 meters)

- WLANs redefine the way the industry views LANs.
- Connectivity no longer implies attachment.
- Wireless networking provides all the features and benefits of traditional LAN technologies without the limitations of wires or cables.
- The freedom to roam while still maintaining connectivity has helped launch wireless networking to new heights.



Organizations that Set or Influence WLAN Standards

- ITU-R
  - Worldwide standardization of communications that use radiated energy, particularly managing the assignment of frequencies
- IEEE
  - IEEE-SA - Working Group
    - Standardization of wireless LANs (802.11)
- Wi-Fi Alliance
  - An industry consortium that encourages interoperability of products that implement WLAN standards through their Wi-Fi certified program
- Federal Communications Commission (FCC)
  - The U.S. government agency with that regulates the usage of various communications frequencies in the U.S.

Wireless Technologies

- PAN/WPAN (Personal Area Network)
  - Bluetooth, IEEE 802.15.4
- LAN (Local Area Network)
  - IEEE 802.11
- MAN (Metropolitan Area Network)
  - IEEE 802.11, IEEE 802.16, IEEE 802.20
- WAN (Wide Area Network)
  - GSM, CDMA, Satelite

http://www.ieee.org/index.html

Wireless Personal Area Network (WPAN)

- Networks with feet (meters) of coverage
  - Between Laptops
  - Between PDAs
  - Between wireless phones
  - Headsets
- Technologies used
  - Bluetooth
  - Infrared
  - ZigBee
  - Radio
  - FHSS

Wireless Metropolitan Area Network (WMAN)

- Networks with miles of coverage
- Networks for metropolitan areas
  - Around Washington DC
  - Around Boston
  - DC government network
- WMAN technologies
  - IEEE 802.16
  - WiMAX
- Can provide “the last mile” coverage

Wireless Wide Area Networks (WWAN)

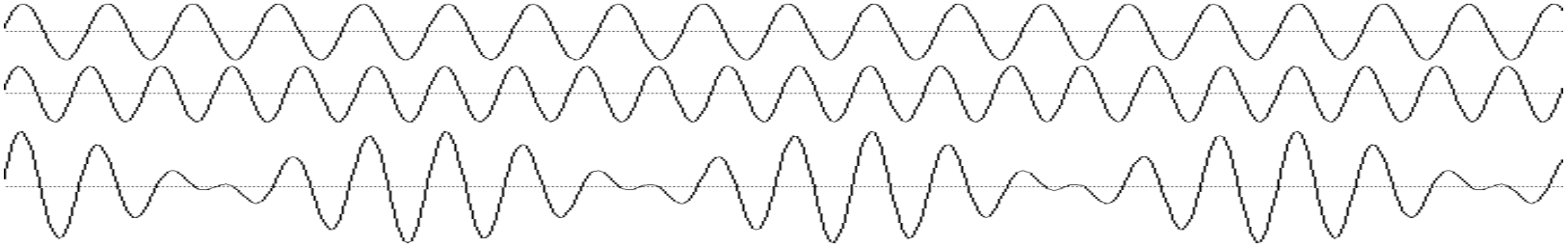
- Networks with ten's of miles of coverage
- Wireline WANs
  - T1, Frame Relay, ATM, MPLS
- WLANs
  - Cellular, T-Mobile, Verizon
  - GPRS, CDMA, TDMA, GSM technologies
- Wireless point-to-point networks
- IEEE 802.11 was not designed for WWAN

Wireless Local Area Network (WLAN)

- Networks with hundred's of feet of coverage
- Provides end user access to LANs
- Coverage for buildings and campuses
- Great fit for 802.11 technology
- 802.11 WLAN provides balance of:
  - Performance
  - Cost
  - Availability
  - Technology evolution

Electromagnetic waves

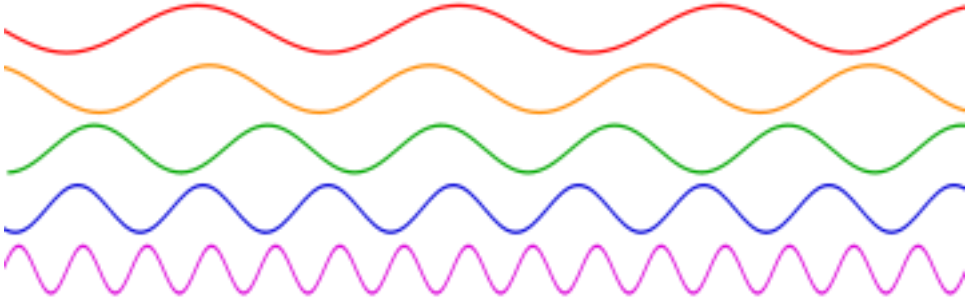
- Wireless technologies use electromagnetic waves



- What types of communication mediums do we have in wired networks?
  - Coper, Fiber
- What communication medium do we have in wireless?
  - The Earth's Athmosphere

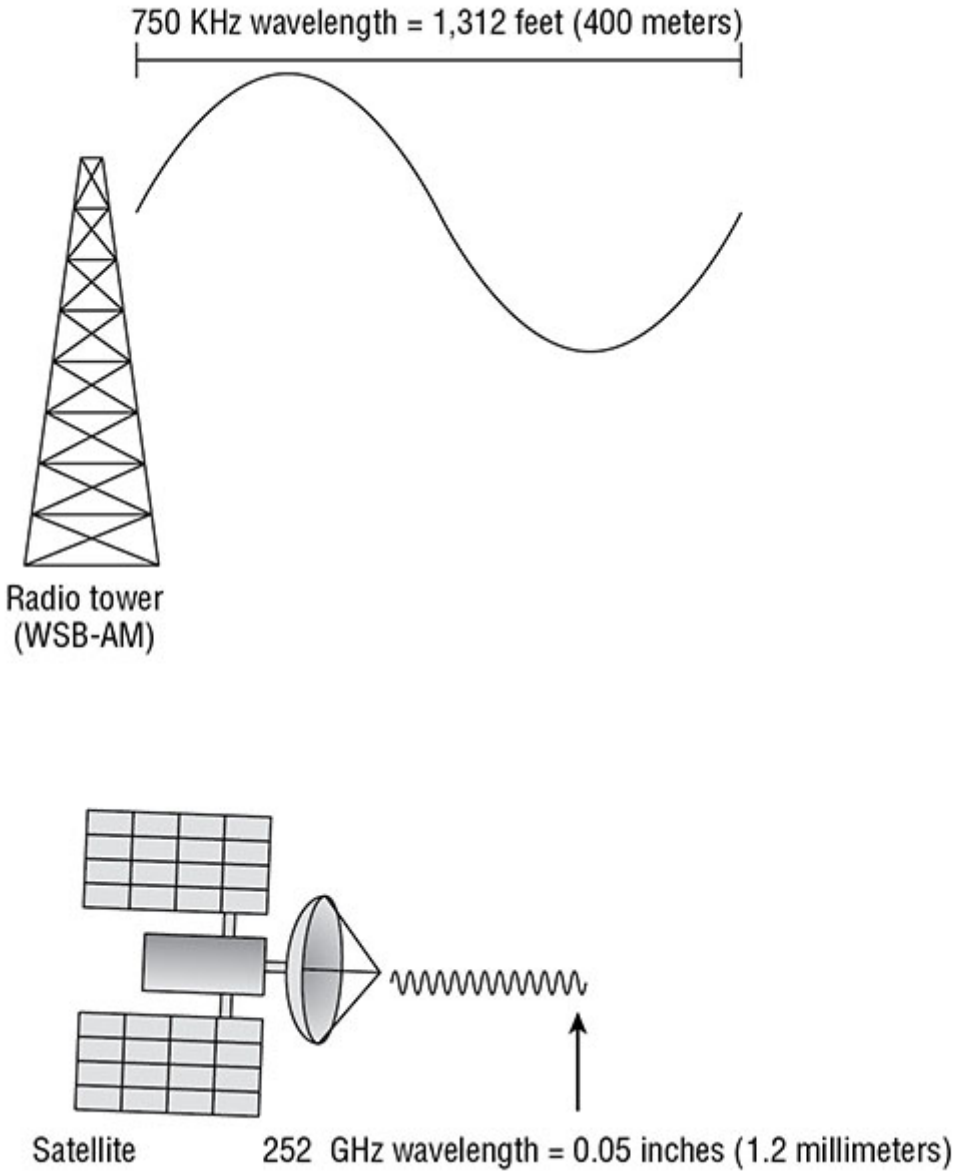
Where it starts

- Frequency (f - Hz)
  - **Frequency** is the number of occurrences of a repeating event per unit time.

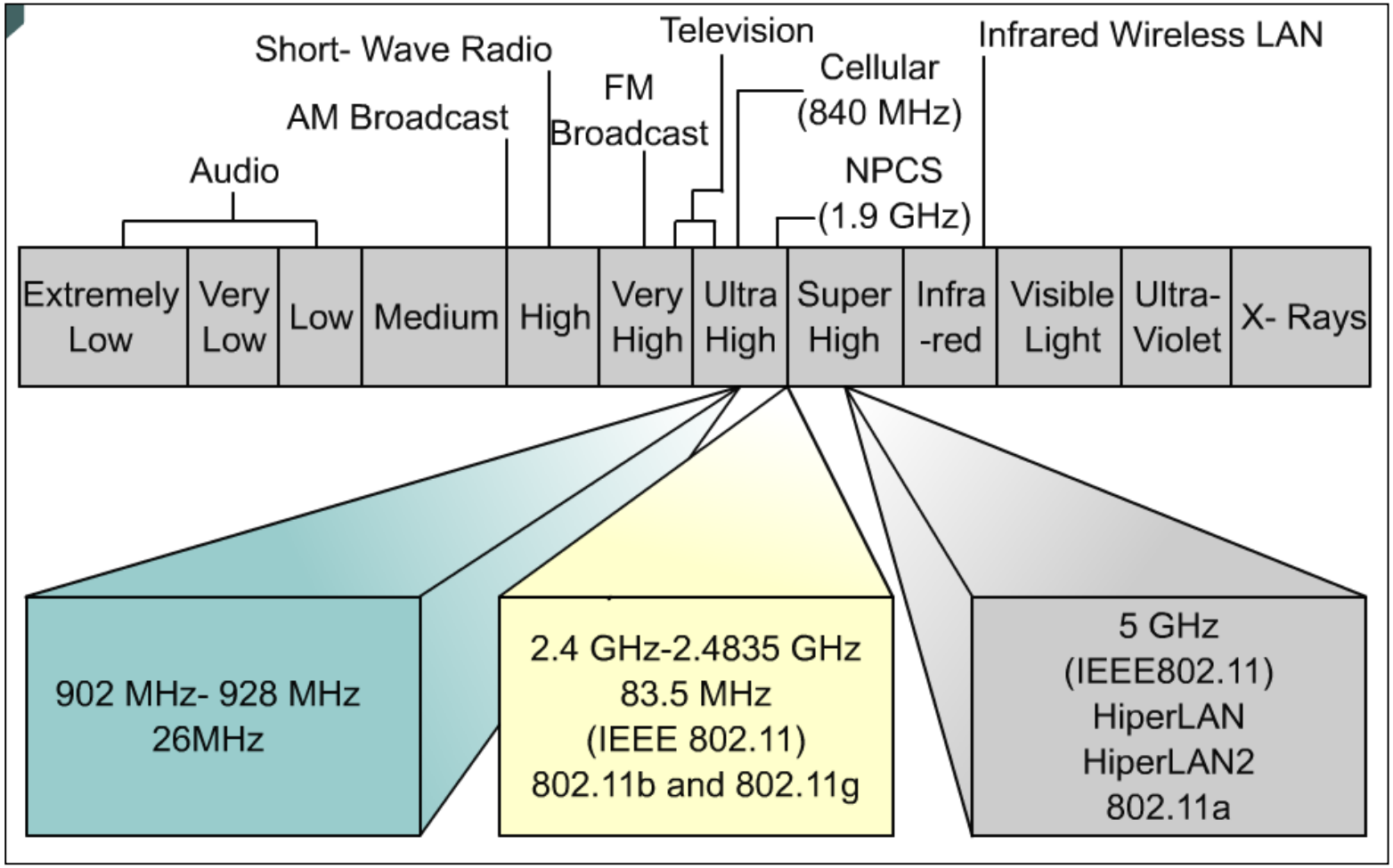


- Higher frequency:
  - Greater speed
  - Shorter range
  - High reflection rate
  - Higher absorption in the Earth's atmosphere
  - Higher costs

Example:

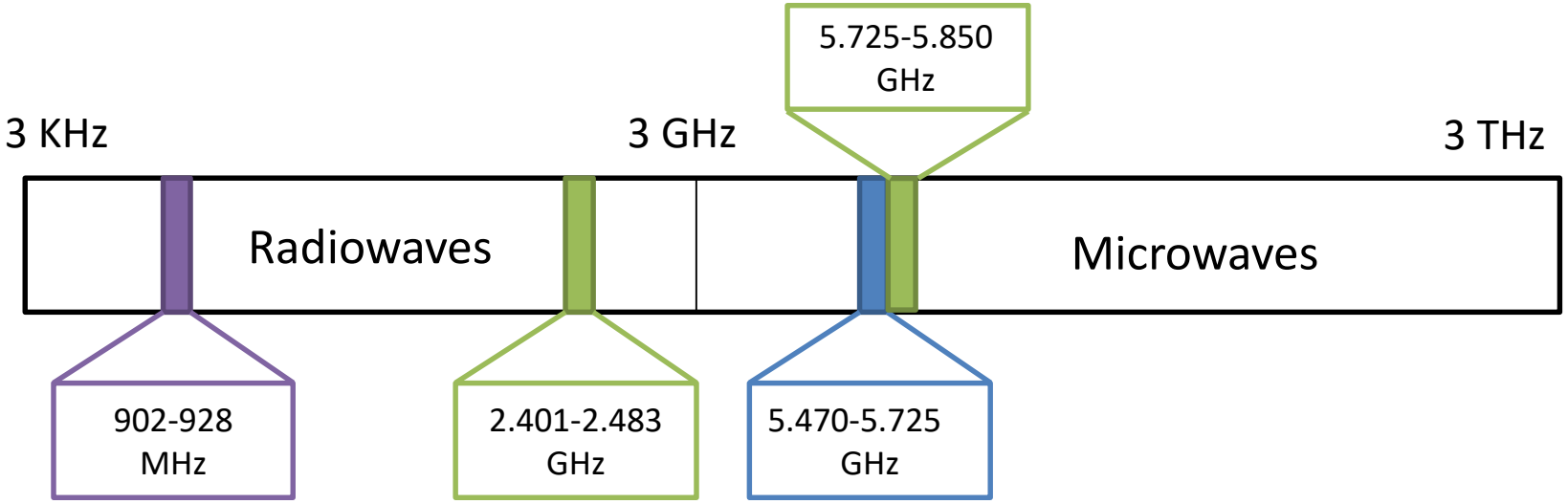

750 KHz wavelength = 1,312 feet (400 meters)
Radio tower
(WSB-AM)
Satellite
252 GHz wavelength = 0.05 inches (1.2 millimeters)

Frequency Bands



Frequency in LAN?

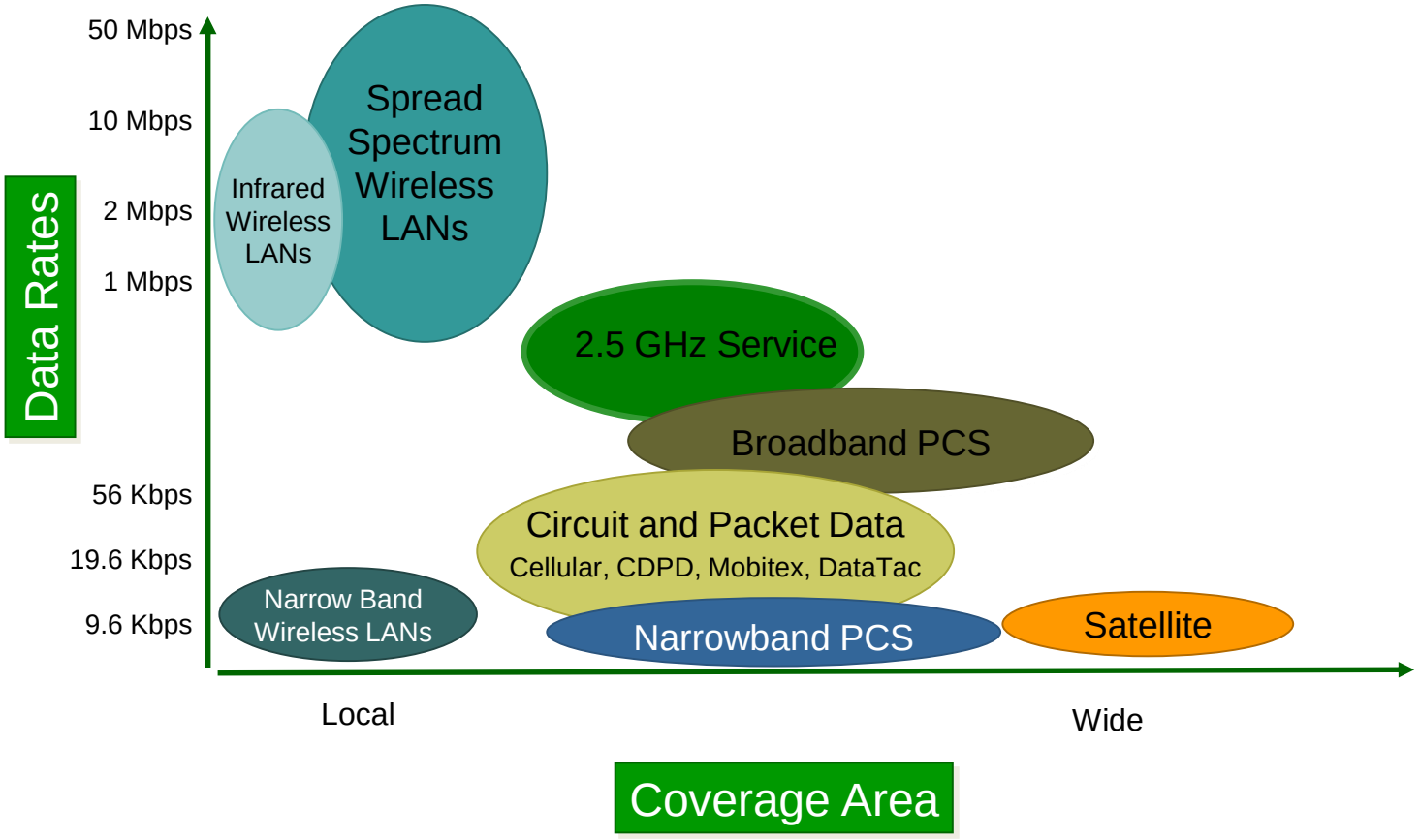
- ISM – Industrial Scientific Medical
  - Free to transmit
  - http://en.wikipedia.org/wiki/ISM_band
- 2,4 and 5 GHz bands
- Disadvantage:
  - They are very occupied
  - The frequencies are high



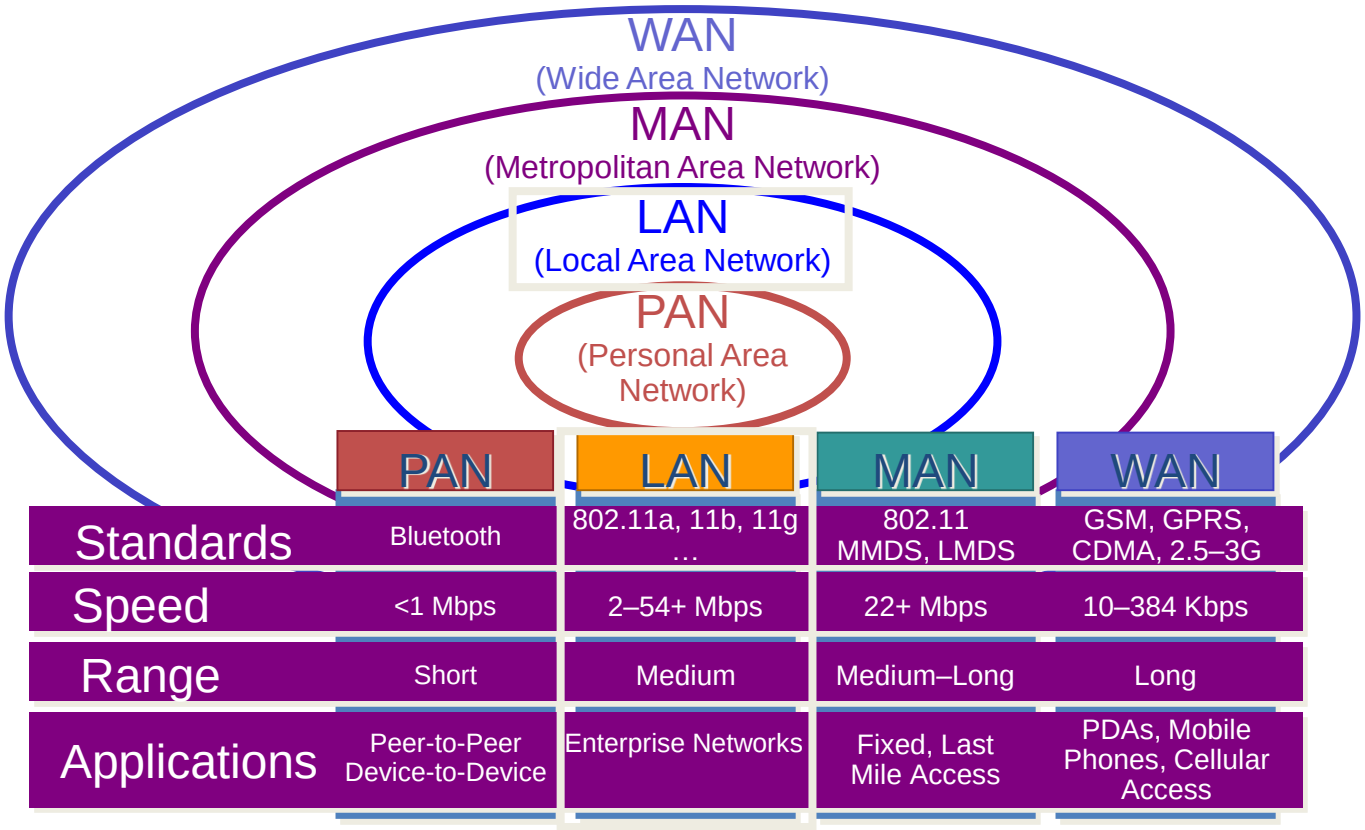
Modulation and Multiplexing

- Encoding digital data into wireless signals (OFDM)
- Higher bandwidth requires higher modulation techniques
- Analog modulation: AM, FM, PM etc
- Digital modulation: ASK, APSK, QAM-64 etc
- Spread Spectrum: DSSS, FHSS, OFDM

Wireless Data Networks



Wireless Technologies

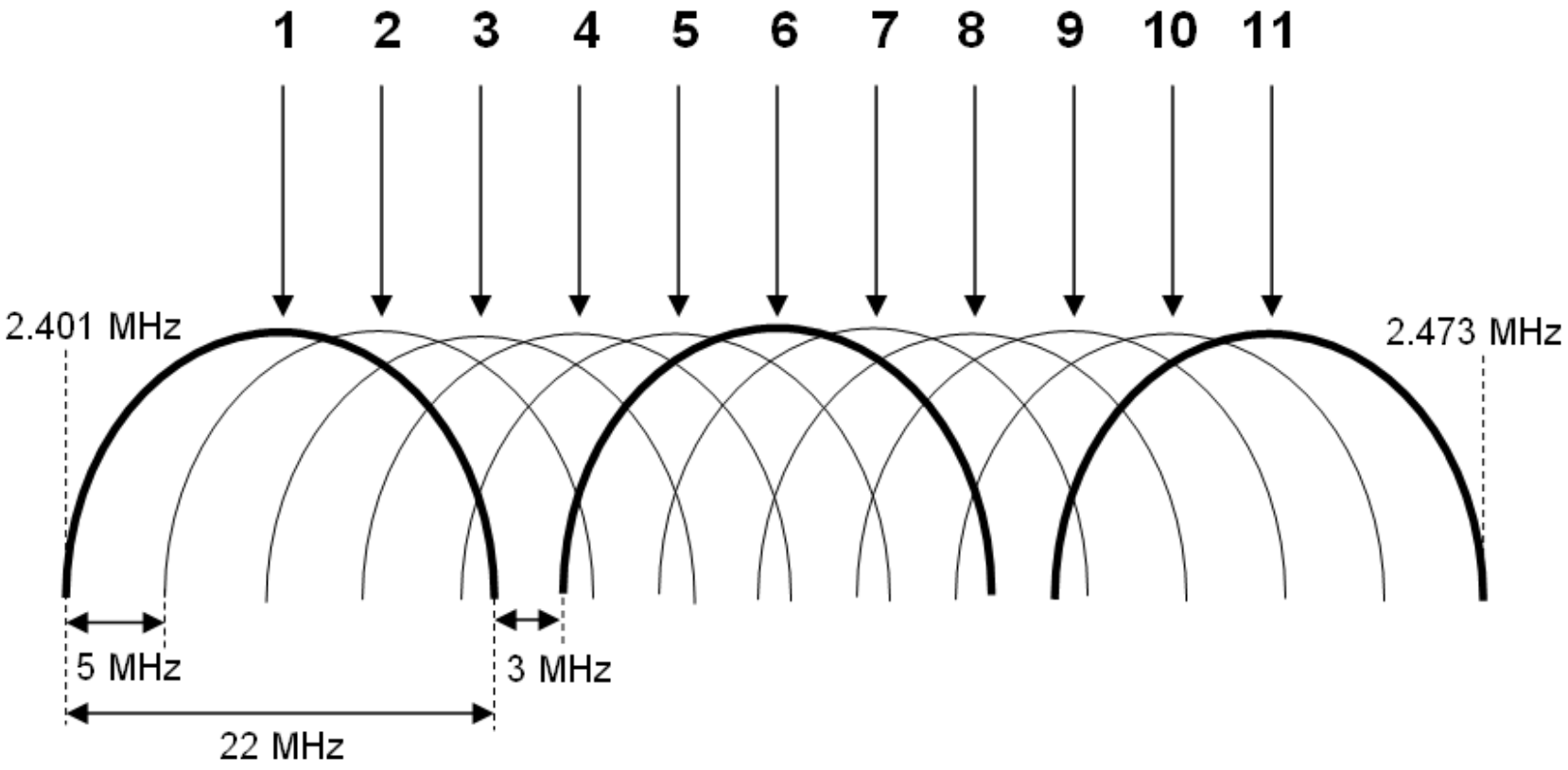


	PAN	LAN	MAN	WAN
Standards	Bluetooth	802.11a, 11b, 11g …	802.11 MMDS, LMDS	GSM, GPRS, CDMA, 2.5–3G
Speed	<1 Mbps	2–54+ Mbps	22+ Mbps	10–384 Kbps
Range	Short	Medium	Medium–Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise Networks	Fixed, Last Mile Access	PDAs, Mobile Phones, Cellular Access

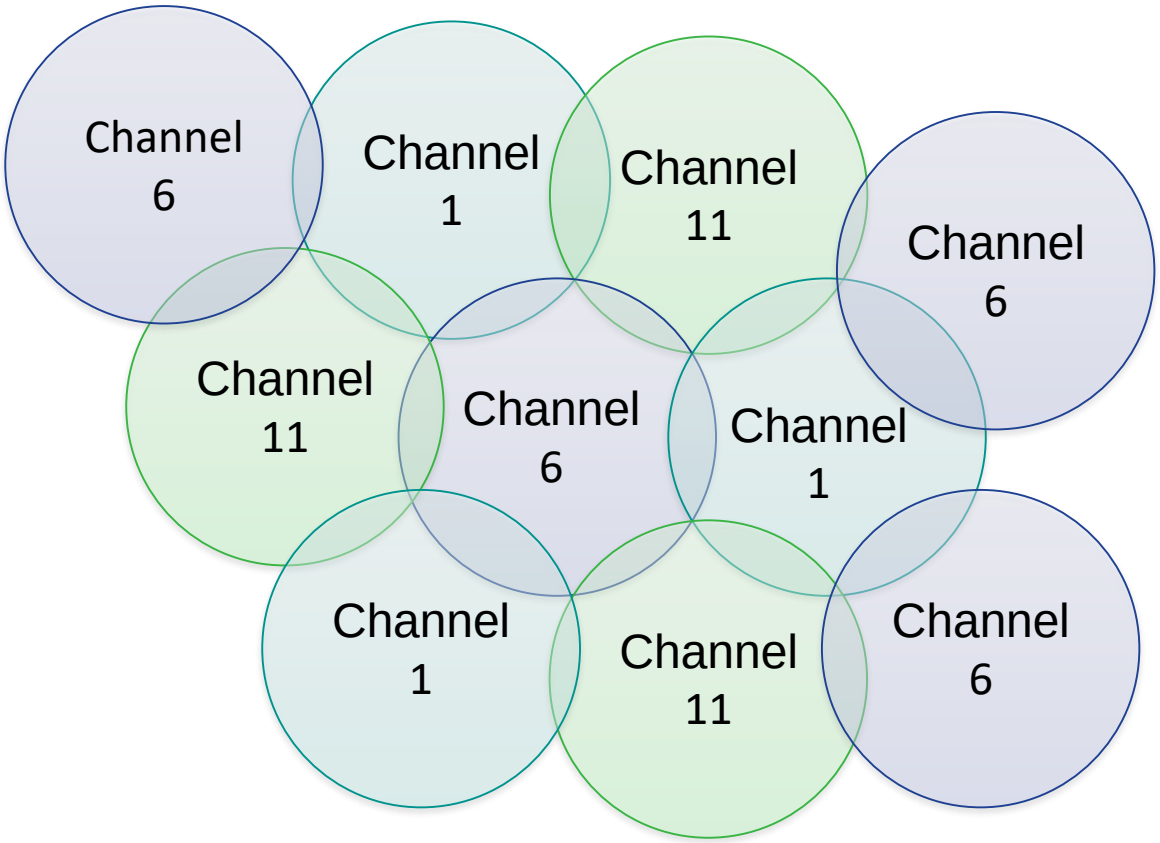
Communication channel

- The wireless transmition medium is shared
- It is not possible to transmit in the exact same frequency without collisions
- How many Hz do we need to transmit 54 Mbps in 802.11g?
  - Answer: **22 Mhz**
- Solution: we could split the ISM band into channels and map each WLAN/SSID on a single channel, thus having multiple networks in the same band

Multiple channels



Multiple Channels



It is possible to cover any surface using just 3 channels

Wi-Fi™

- Wi-Fi™ Alliance
  - Wireless Fidelity Alliance
  - 170+ members
  - Over 350 products certified
- Wi-Fi's™ Mission
  - Certify interoperability of WLAN products (802.11)
  - Wi-Fi™ is the "stamp of approval"
  - Promote Wi-Fi™ as the global standard

WLAN Standards

- 1997
  - 802.11
- 1999
  - 802.11 b
  - 802.11 a (mid 802.11 a cleared for use in Europe)
- 2003
  - 802.11 g
- 2009
  - 802.11 n
- 2014
  - 802.11 ac

802.11

- Legacy – released in 1997
- Specified in infrared and wireless
- Spread Spectrum – FHSS/DSSS
- Speed: 1-2 Mbps
- Frequency: 2.4 Ghz and 900 Mhz

802.11 a and b

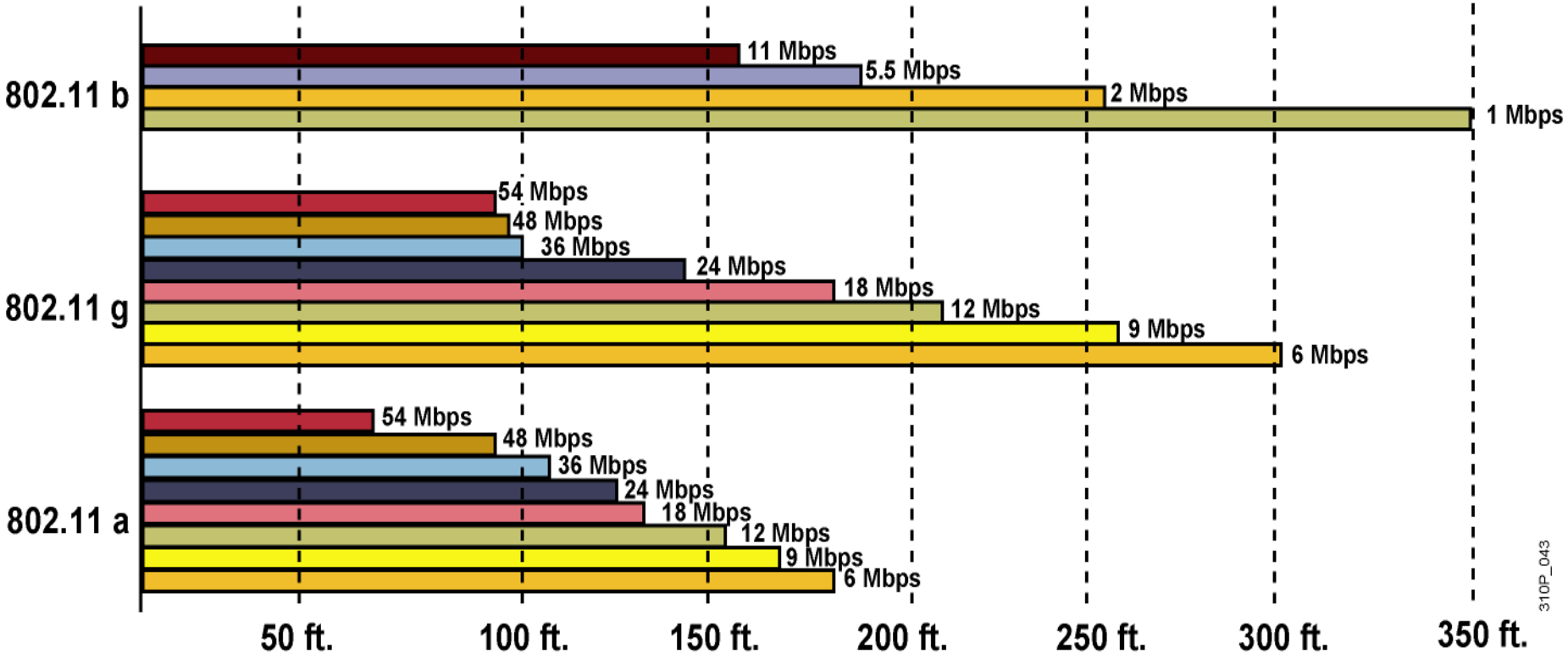
- Both standards appeared about the same time - 1999
- 802.11a
  - Introduces OFDM and takes speed up to 54 Mbps
  - Frequency band: 5 GHz
  - Distance to transmit signal: 25m
- 802.11b
  - Bandwidth: 11 Mbps
  - Frequency band: 2.4 GHz
  - Became very popular – called WiFi

802.11g

- Standardized in 2003
- Best of both worlds (a & b)
- Frequency band: 2.4 GHz
- Bandwidth: 54 Mbps
- Modulation: OFDM
- Used for a long time and can still be found in networks

802.11a/b/g – Area coverage

The measurement was made in indoor office spaces

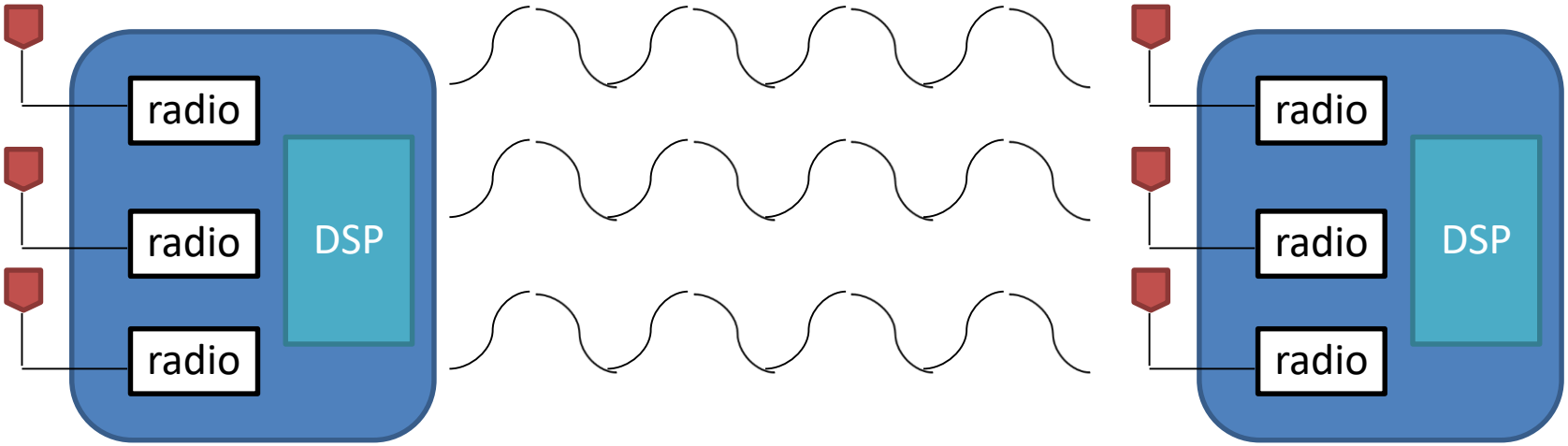


802.11n

- 802.11n – standardized 29 October 2009
- Far greater speeds: theoretical maximum 600 Mbps
- Better coverage and density of the signal
- Backwards compatible with 802.11 a/b/g
- Uses multiple antenaes and MIMO technology
- Increased channel width to 40 Mhz
- Improved imunity to noise using complex modulation techniques
- Support packet aggregation (one header for multiple data packets)

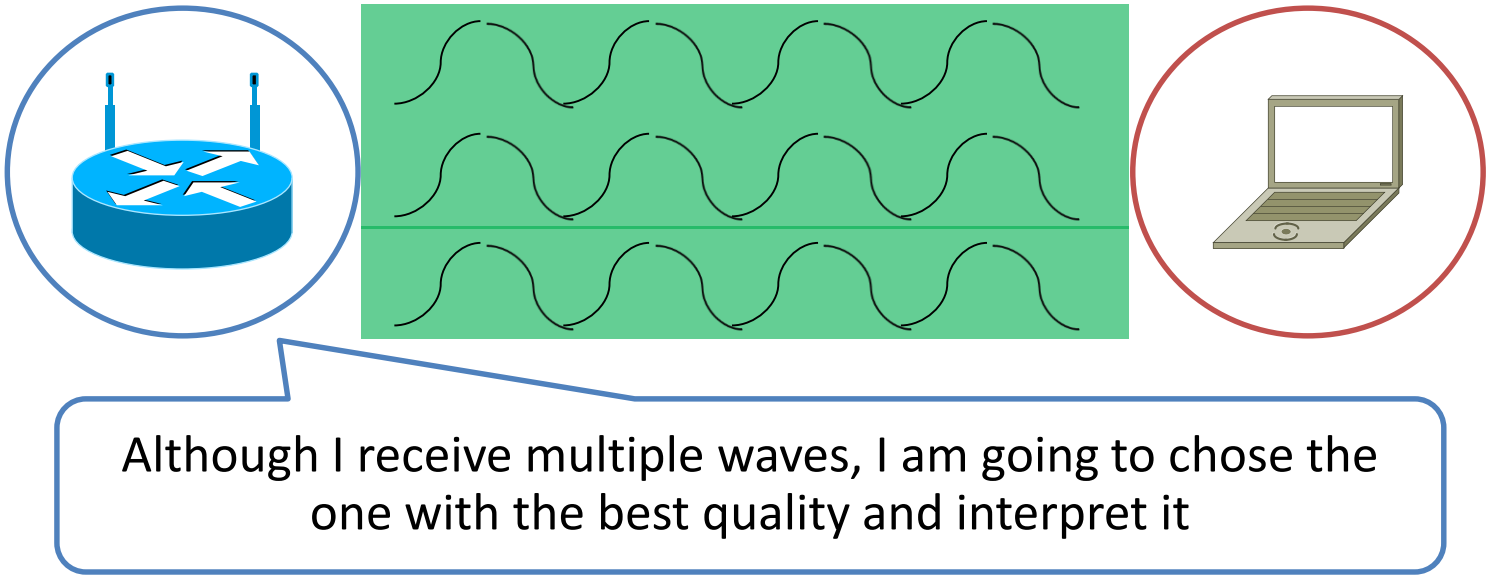
802.11n - MIMO

- **M**ultiple **I**nput **M**ultiple **O**utput uses DSP processors to multiplex and demultiplex the signal



802.11n – Maximum Ratio Combining (MRC)

- The multipath effect = the process in which many waves carrying the same information are reflected differently from surfaces and with varying clarity
- In 802.11g, the DSP chose the wave with the best signal to noise ratio



802.11n – Maximum Ratio Combining (MRC)

- Problem description: some weaker SNR waves are ignored even if there is the possibility that they contain relevant information
- In 802.11n, MRC is implemented in the NIC's DSP so that it takes all the waves and composes just one high-quality wave, thus increasing throughput
- Concluding:
  - MRC is a client-side technology
  - If you have an 802.11n board in a 802.11g network, you will have higher-than-ordinary throughput
  - It is like having a cat with multiple ears

802.11ac

- 802.11ac – standardized 2013
- Far greater speeds, defines very high throughput (VHT)
- Operates only in 5 GHz which provide greater spectrum space
- maximum data rate of 6933.3 Mbps .
- 802.11ac provides gigabit speeds using the following four major enhancements:
  - Wider channel: 802.11ac supports channel widths of 20 MHz, 40 MHz, 80 MHz, and 160 MHz channels
  - New Modulation: 802.11ac provides the capability to use 256-QAM modulation, which can provide at least a 30 percent increase in speed over previous modulation methods. 256-QAM modulation requires a veryhigh signal-to-noise (SNR) ratio to be effective.
  - More Spatial Streams
  - Improved MIMO and Beamforming

General comparison of standards

Standard	802.11a	802.11b	802.11g	802.11n
Published	1999	1999	2003	2009
Frequency	5GHz	2.4GHz	2.4GHz	2.4GHz / 5GHz
Bandwidth	54Mbps	11Mbps	54Mbps	160-600 Mbps
Modulation	OFDM	DSSS	OFDM, DSSS	OFDM
Coverage: Interior Exterior	 35m 120m	 38m 140m	 38m 140m	 70m 250m
Advantages	Strong signal in a small office	Low price	Good speed and good coverage	Very big speed Very big coverage
Disatvantages	Incompatible with g and b	Interference	Interference	More expensive

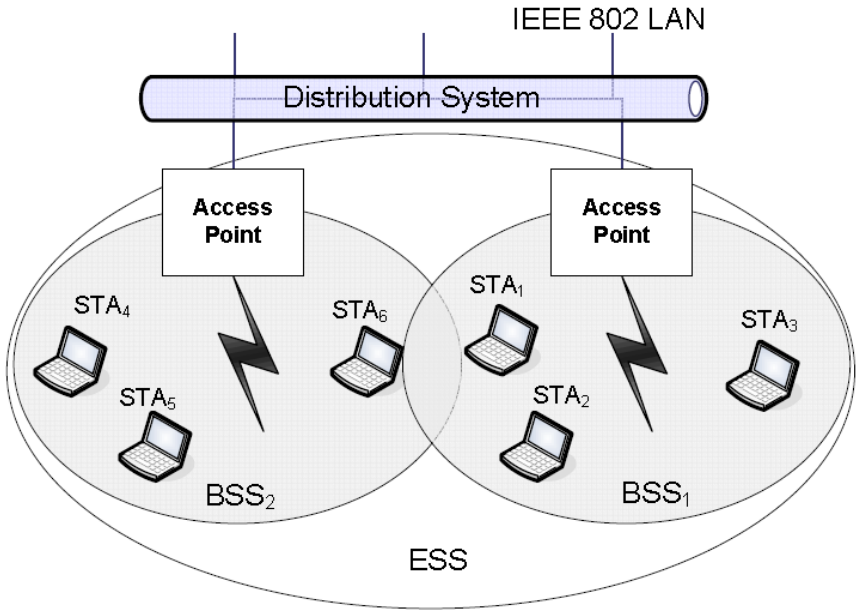
WLAN Topologies

- WLANs can use one of two modes — ad hoc mode or infrastructure mode.
- In ad hoc mode there is no central authority and a wireless devices connects to other devices directly. In infrastructure mode, there is a central device (called access point, i.e. AP) and devices communicate through that device.
- Three main topologies:
  1. Independent Basic Service Set (IBSS)*
  2. Basic Service Set (BSS)
  3. Extended Service Set (ESS)

*Service Set: a logical group of devices

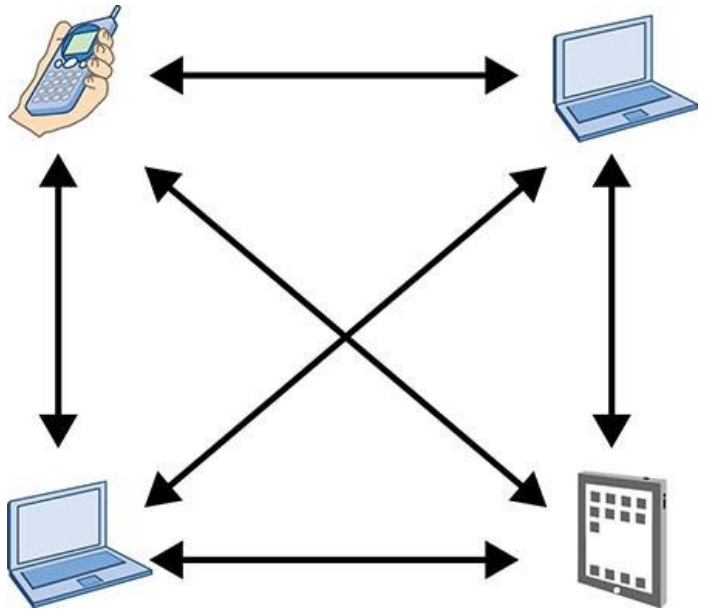
802.11 WLAN Terms

- Station (STA)
- Access Point (AP)
- Basic Service Set (BSS)
- Basic Service Area (BSA)
- Extended Service Set (ESS)
- Distribution System (DS)



Independent Basic Service Set (IBSS)

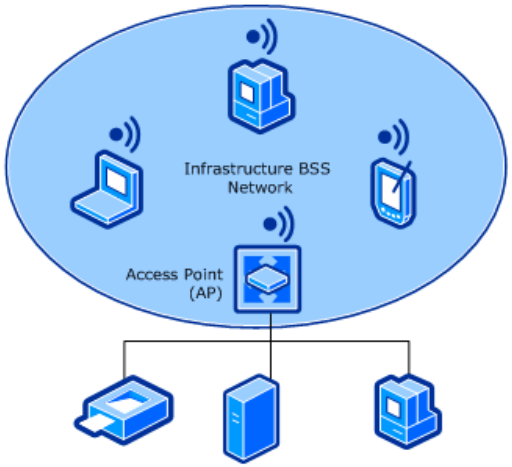
- ad hoc wireless network
- IBSS is a collection of STAs* that are communicating with each other directly without the use of an AP
- In order for a STA to be able to communicate with another STA, they must be within RF range of each other.
- There is no relaying of signals from one STA to another through the various STAs in the IBSS.
- Short period of time
- Problems: STAs cannot retransmit.



*STA: stations

Basic Service Set (BSS)

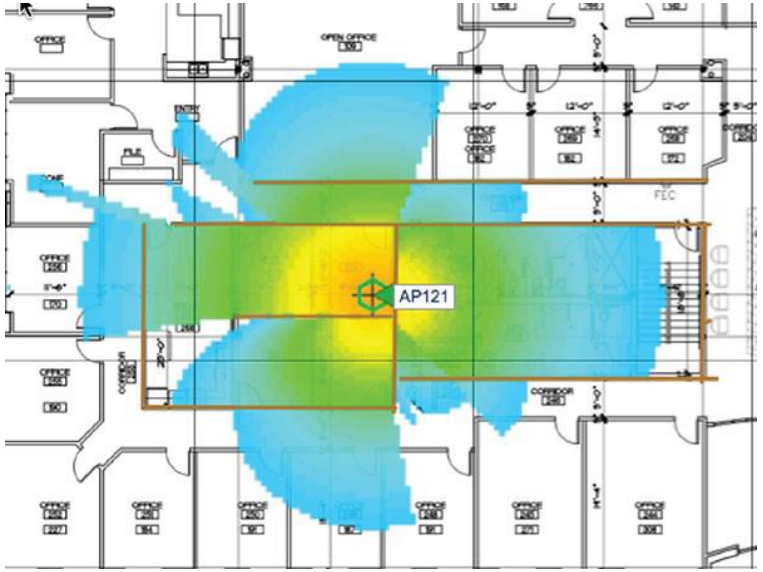
- BSS is infrastructure based, often referred as infrastructure BSS network.
- All STAs within the BSS communicate with each other through an AP.
- Each AP within the BSS network provides 802.11 authentication and authorization services for access to the BSS network, as well as privacy services for the encryption of data sent through the BSS network.
- Each AP can act as a bridge between the wireless and wired LANs, allowing stations on either LAN to communicate with each other.



Basic Service Area (BSA)

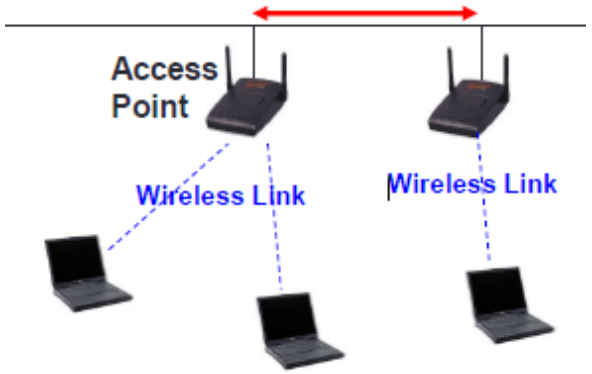
- The physical area of coverage provided by an access point in a BSS is known as the basic service area (BSA).
- Client stations can move throughout the coverage area and maintain communications with the AP as long as the received signal between the radios remains above received signal strength indicator (RSSI) thresholds.

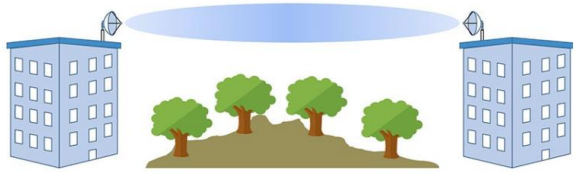
- The size and shape of a BSA depends on many variables, including AP transmit power, antenna gain, receive sensitivity, and physical surroundings.
- It is common to draw a circle around the AP to illustrate the theoretical coverage area



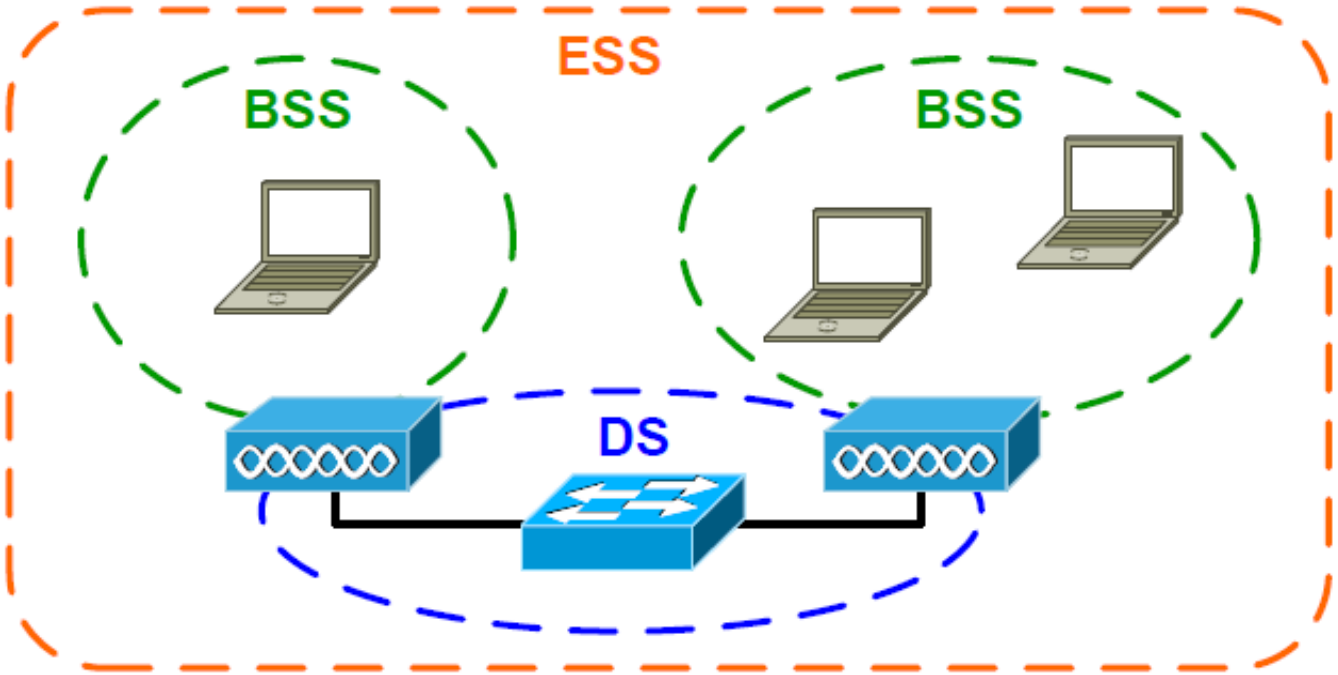
Extended service set (ESS)

- Multiple BSSs can be connected together with the help of a backbone network (layer 2) to form a ESS network.
- 802.11 standard does not define any backbone.
- Backbone network is called Distribution System (DS) and can be wired/wireless
- STAs are associated with one AP at any particular time.
- The SSID is same for all BSS areas in the ESS (unless multiple BSS have been created, e.g. TTU, TTU Campus)





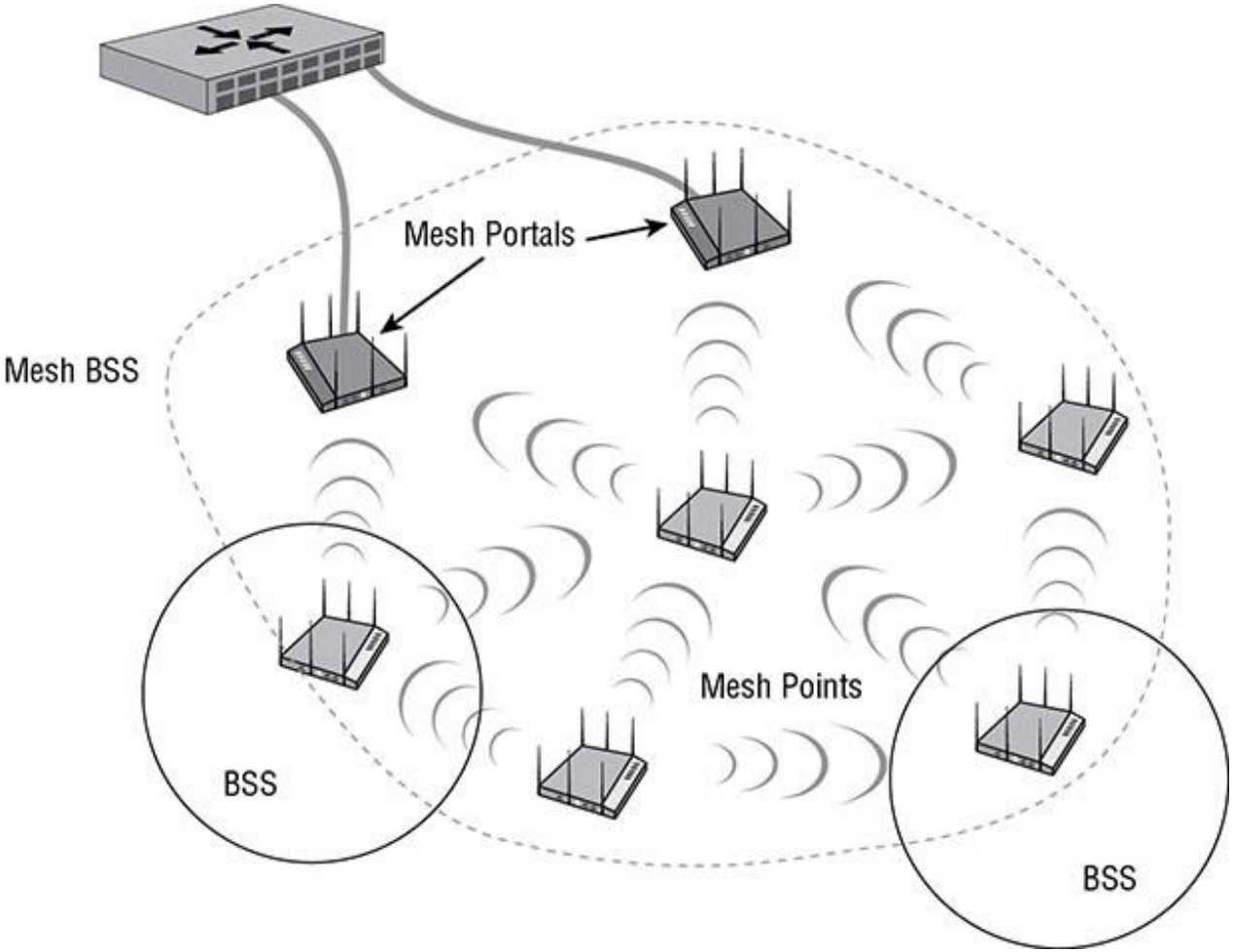
Overview of WLAN Topologies



Mesh Basic Service Set (MBSS)

- The 802.11-2016 standard also defines a service set for an 802.11 mesh
- When access points support mesh functions, they may be deployed where wired network access is not possible.
- The mesh functions are used to provide wireless distribution of network traffic, and the set of APs that provide mesh distribution form a mesh basic service set (MBSS)
- An MBSS requires features that are not necessary in a BSS, ESS, or IBSS because the purpose of an MBSS is different from the other topologies.
- The backhaul connection between a mesh point and a mesh portal is considered to be a wireless distribution system (WDS).
- Client stations that are associated to the mesh points have their traffic forwarded through the wireless backhaul.
- Usually the MBSS uses the 5 GHz radios for backhaul communications.

Mesh Basic Service Set (MBSS)

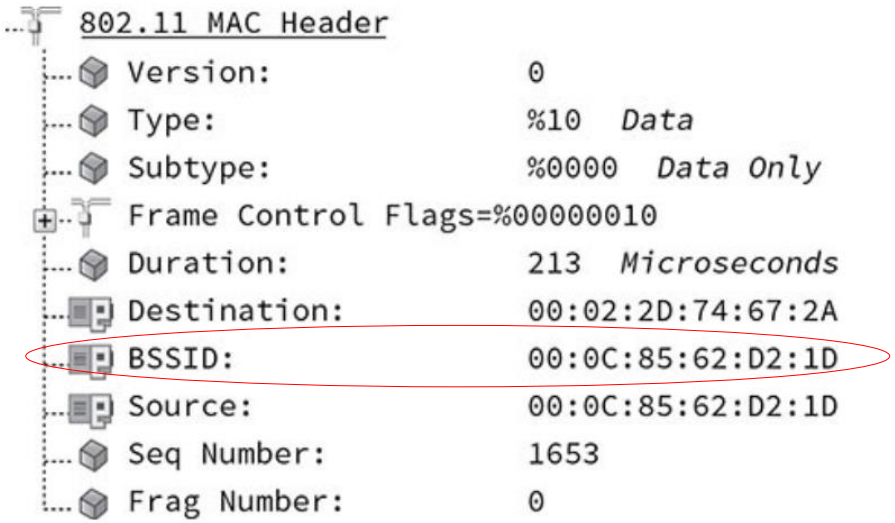


Service Set Identifier (SSID)

- WLANs provide network access by broadcasting a signal across a wireless radio frequency
- Transmitter prefaces its transmission with a Service Set Identifier (SSID). It is the identity of an IBSS, BSS or ESS
- STA may receive transmission from transmitters with same or different SSIDs
- As SSID is between 2 to 32 alphanumberic charachters
- A STA seeking to join a WLAN may send probe request frames including the SSID of the desired WLAN
- If an AP “hears” the probe request frame and it uses the same SSID, it will respond with a probe response frame.
- The STA that transmitted the original probe request frame may now authenticate and, if successful, associate with the BSS.

Basic Service Set Identifier (BSSID)

- The basic service set identifier (BSSID) should not be confused with the SSID.
- The BSSID is a 48-bit identifier that is used to uniquely identify each service set, i.e. the MAC address of the radio network interface in an access point.
- However, the proper definition is that the BSSID address is the layer 2 identifier of each individual BSS



Distribution System (DS)

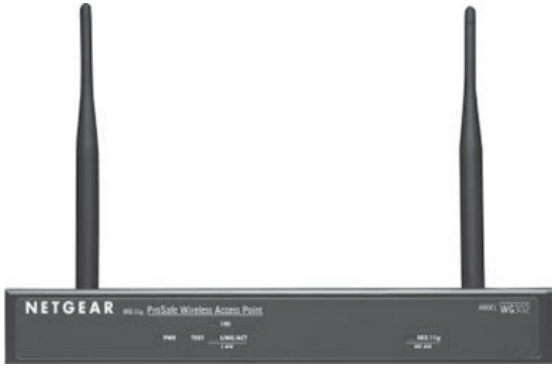
- The distribution system (DS) is defined as a system used to interconnect a set of BSSs and an integrated LAN to form an ESS.
- The DS is used for the transfer of communications between the APs in the ESS.
- Every AP has a DS within it, regardless of whether it is connected to other APs across some other shared system such as Ethernet.
- The DS is composed of two parts:
  - Distribution System Medium: Ethernet, WLAN bridge backhaul, Token ring, etc.
  - Distribution System Services: services that provide the delivery of frame payloads between stations

Access points (APs)

- Access points (APs) are the most frequently installed infrastructure (non-client) devices.
- They provide access to the WLAN and may bridge to a wired LAN
- APs provide a point of access to the WLAN and derive their name from this functionality
- AP will provide connectivity to a wired LAN or WAN for wireless client STAs, however, this does not have to be the case.
- APs are often used at construction sites to form controlled and secure networks that are entirely wireless (with the exception of the power cords connected to the APs) as just one example of the use of APs where access to wired networks is not the intent.

- **Autonomous access points** are APs that contain the software for complete management of the WLAN processes within themselves. These were the only kind of APs in early WLANs until the lightweight AP was later developed.
- **Lightweight access points** are APs that contain limited software and depend on centralized WLAN switches or controllers to provide the remaining functionality.
- Autonomous APs are sometimes called fat or thick APs, whereas lightweight APs are also called access ports or thin APs.
- Some APs can act as either an autonomous or lightweight AP, depending on the configuration determined by the WLAN administrator.
- When used as an autonomous AP, all the AP software features are enabled.
- When used as a lightweight AP (or access port), many of the AP software features are disabled or are simply controlled by the centralized WLAN switch or controller.

APs



WLAN Models

- There are two primary implementation methodologies:
  1. single MAC model: is also known as an *edge* or *intelligent edge* model
  2. split MAC model: is also known as a *centralized* model

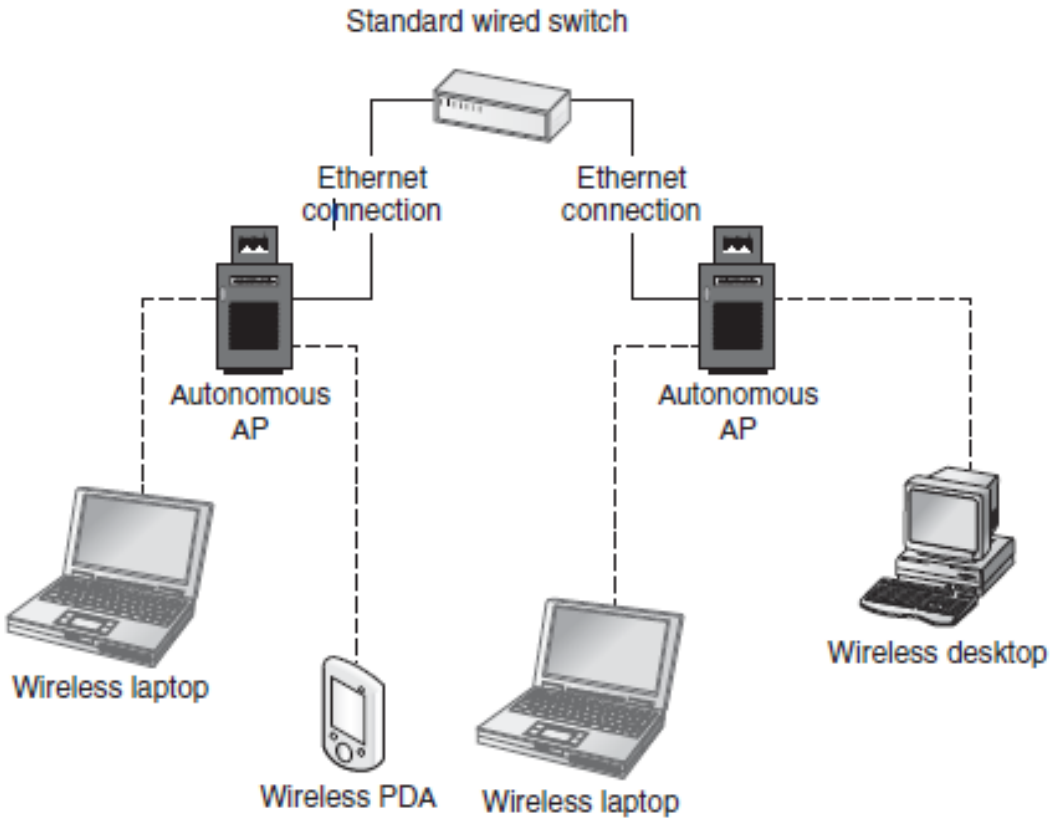
Single MAC Model (Edge, Autonomous, or Stand-Alone)

- When a single MAC model is used, it means that the APs contain all of the logic within them to perform MAC-layer operations (all IEEE 802.11 services reside within the AP)
- The single MAC model is the oldest and is still very popular in small- and medium-sized WLANs.
- Advantages:
  - No single point of failure. If one AP goes down, the others continue to function.
  - Less wired network traffic is required to manage the wireless stations.
  - More features are available within the APs themselves
- Disadvantages:
  - Decentralized administration may require more ongoing support effort.
  - APs may be more expensive, since they have more powerful hardware.
  - Each AP may be able to handle fewer client stations.

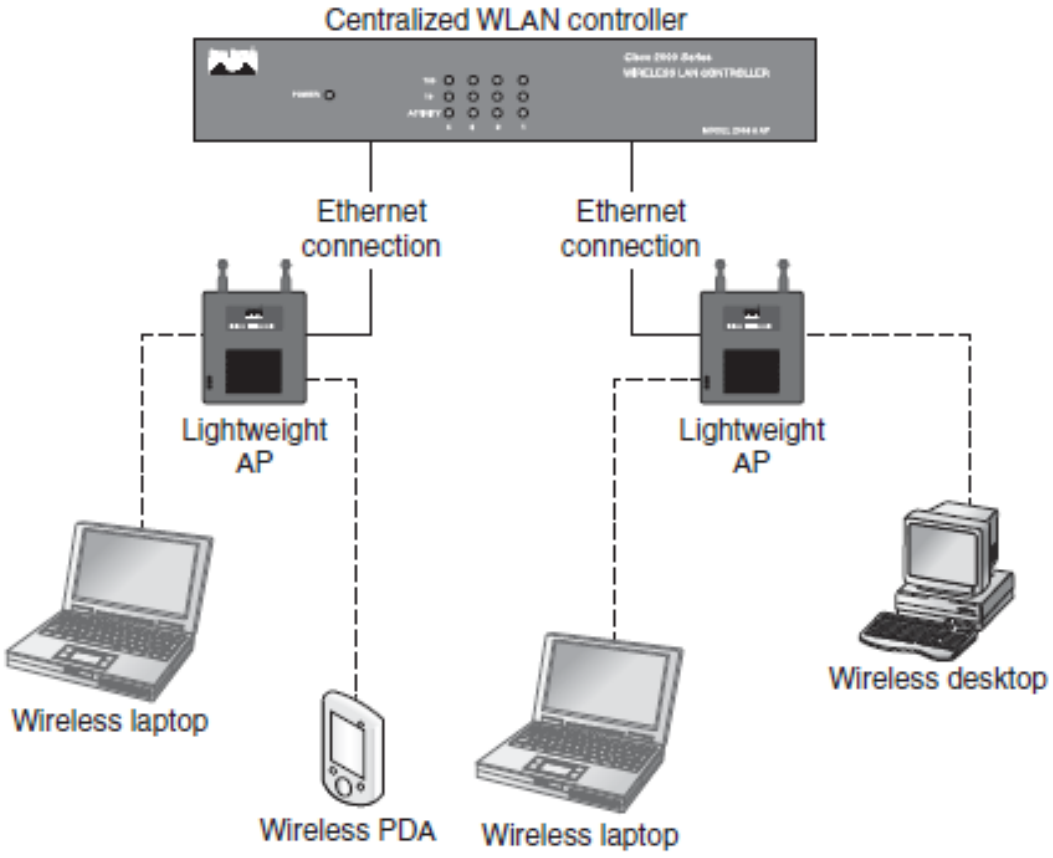
Split MAC Model (Centralized)

- Portions of the MAC-layer operations are offset to centralized controllers and other portions remain in the AP.
- The split MAC model is very popular in large networks today and is becoming more popular in smaller networks as well.
- Advantages:
  - Centralized administration may reduce ongoing support efforts.
  - APs may (or may not) be less expensive, since they can have less memory and processing power.
  - Each AP may be able to handle more client stations, since the AP does not have to handle management processing overhead
- Disadvantages:
  - A possible single point of failure occurs at the WLAN controller.
  - Increased wired network traffic is required to manage the wireless stations.
  - There are fewer features within the APs themselves when using truly thin APs.

Autonomous AP implementation (Single MAC Model)

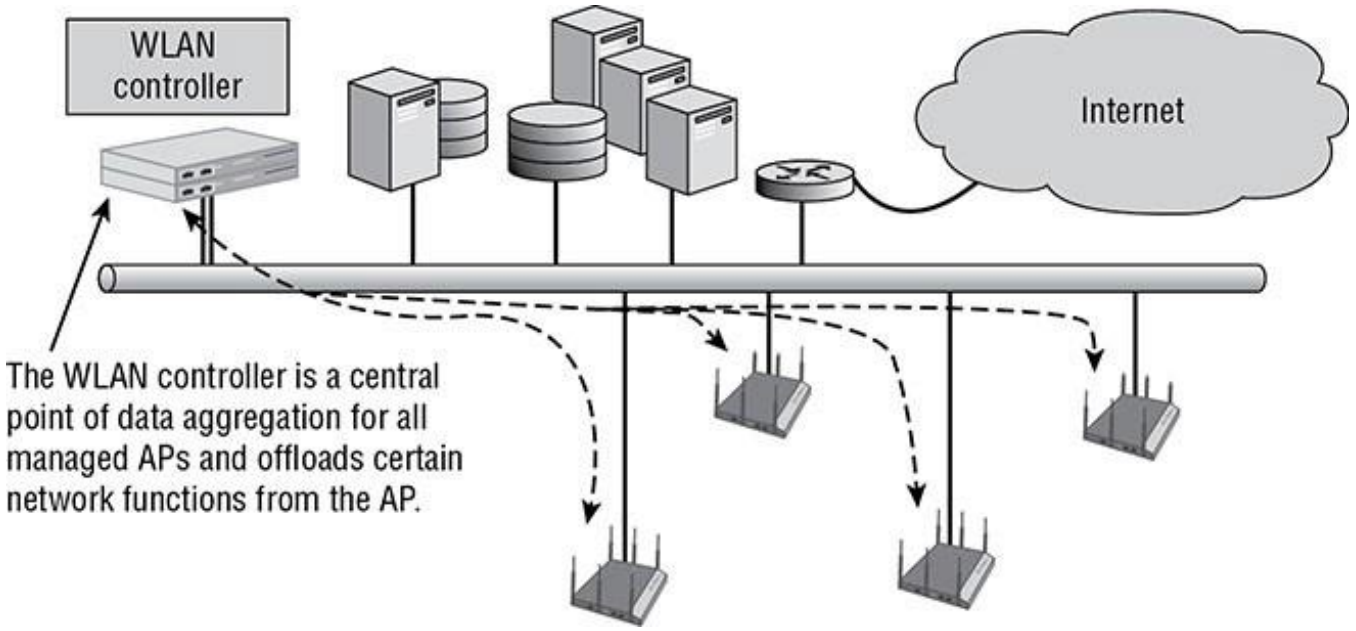


Lightweight AP implementation (Split MAC Model)

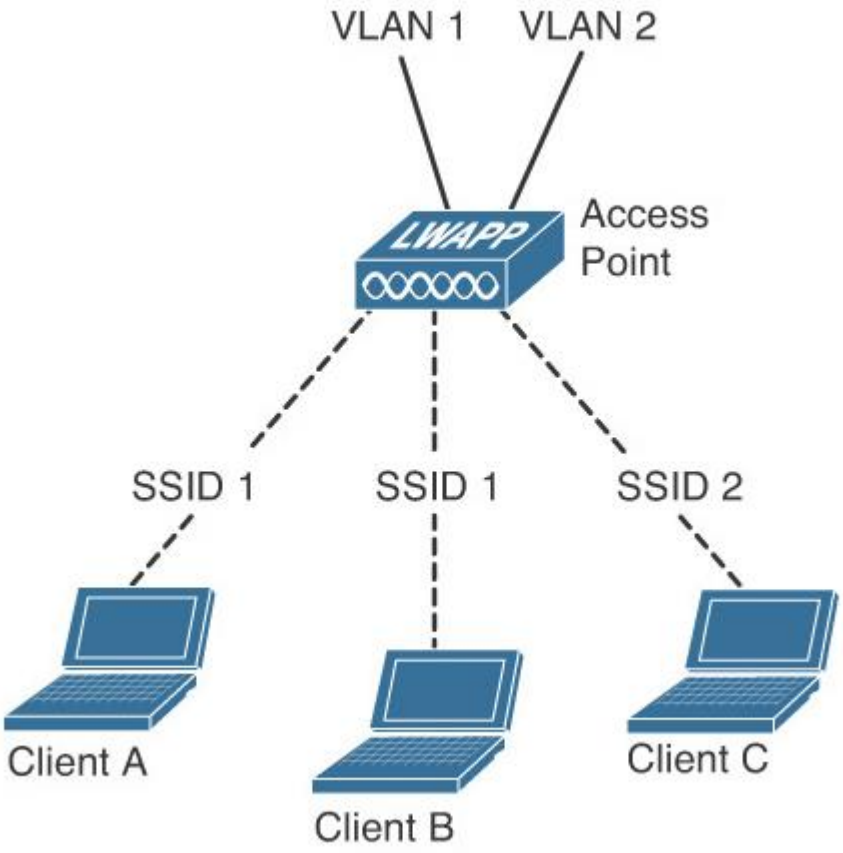


Controller-Based Access Point Architecture

- The lightweight access points connect to a WLAN controller, which provides centralized management, security, and performance functions (power, data rate, etc).
- **L**ightweight **A**ccess **P**oint **P**rotocol (**LWAPP**), supports access point discovery and configuration (Cisco Propriety)
- **C**ontrol **a**nd **P**rovisioning of **W**ireless **A**ccess **P**oints (**CAPWAP**) protocol for managing and monitoring access points. (IETF)
- The network infrastructure must support layer 3 functionality because the discovery process uses IP addresses, not MAC addresses.
- Recommended to use controller if deploying more than 10 access points


WLAN
controller
Internet
The WLAN controller is a central point of data aggregation for all managed APs and offloads certain network functions from the AP.

virtual WLANs

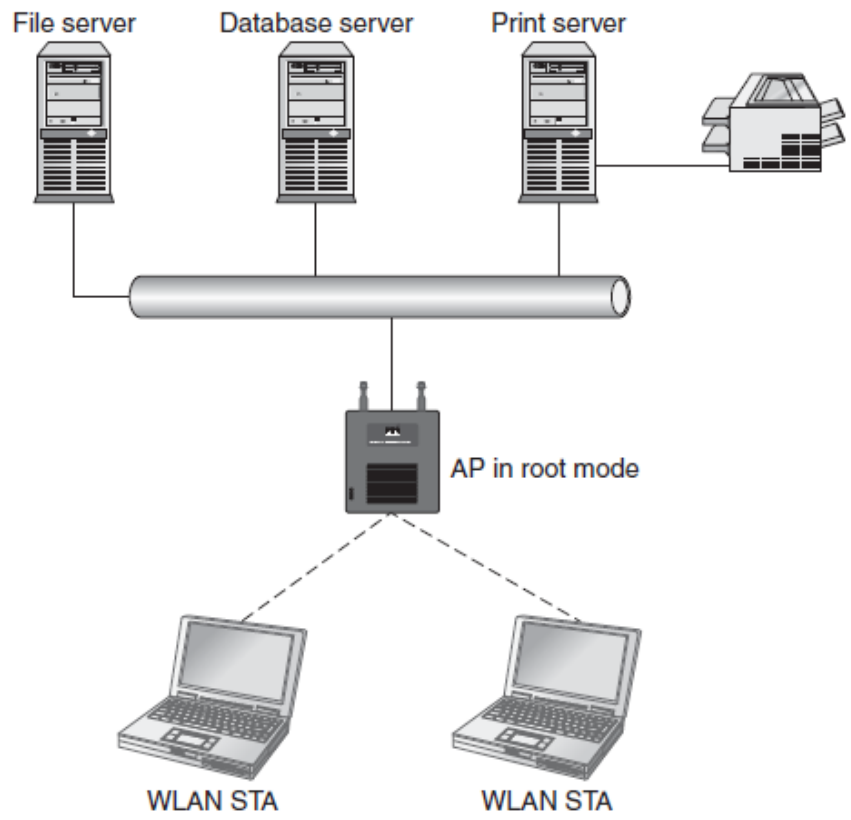


AP: Operational Modes

- The IEEE 802.11 standard defines an AP only as a STA that provides access to the distribution services via the wireless medium for associated STAs.
- APs have three operational modes are available.
  1. Root mode
  2. Bridge mode
  3. Repeater mode

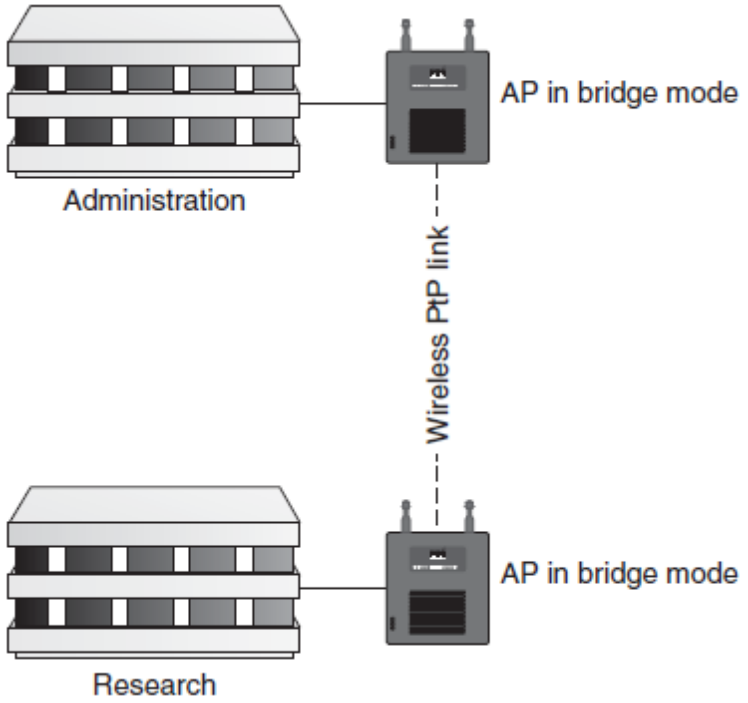
root mode

- An AP operating in root mode is providing wireless clients with access to the WLAN and possibly a wired network. Root mode is the default mode of operation for all WLAN devices sold as APs.



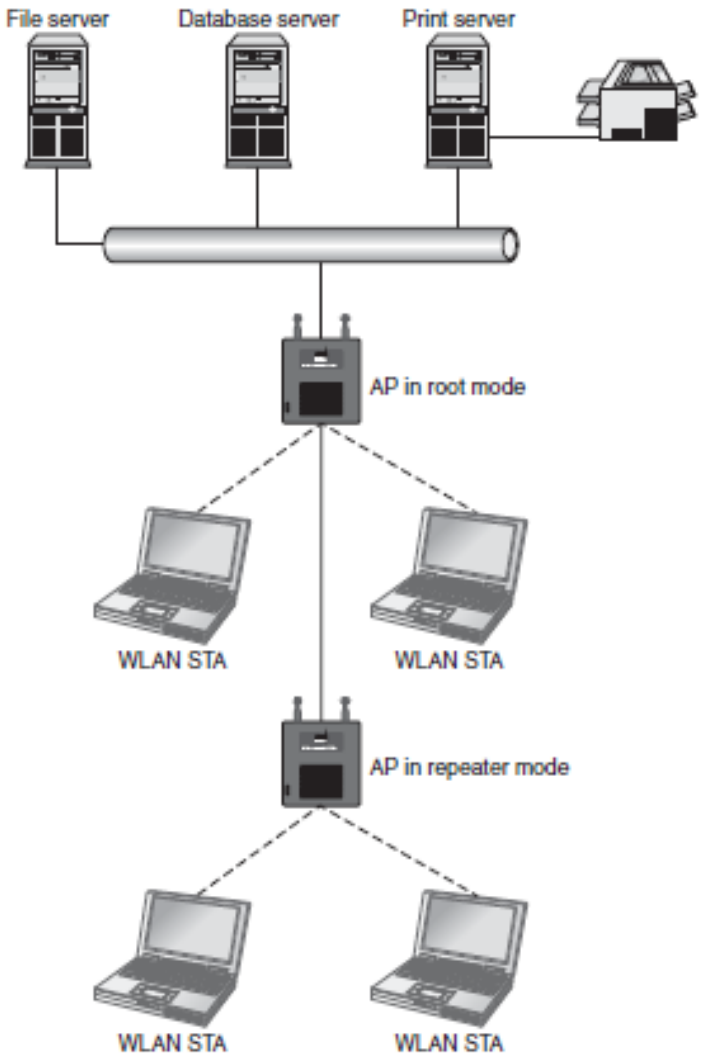
bridge mode

- Bridge mode is used to create a link between two or more APs. When only two APs are used, a point-to-point link is created. When more than two APs are involved, a set of point-to-multipoint links are created.



repeater mode

- to extend the range of a WLAN beyond its normal usable boundaries.
- The repeater AP acts as the AP for clients that would otherwise be out of range of the distant AP operating in root mode.
- Where a root AP is the connection point for many clients and is a client to no other APs, the AP in repeater mode is a client to the AP in root mode while also accepting connections from client stations itself
- Mesh mode is sometimes also referred to as repeater mode



sensor mode

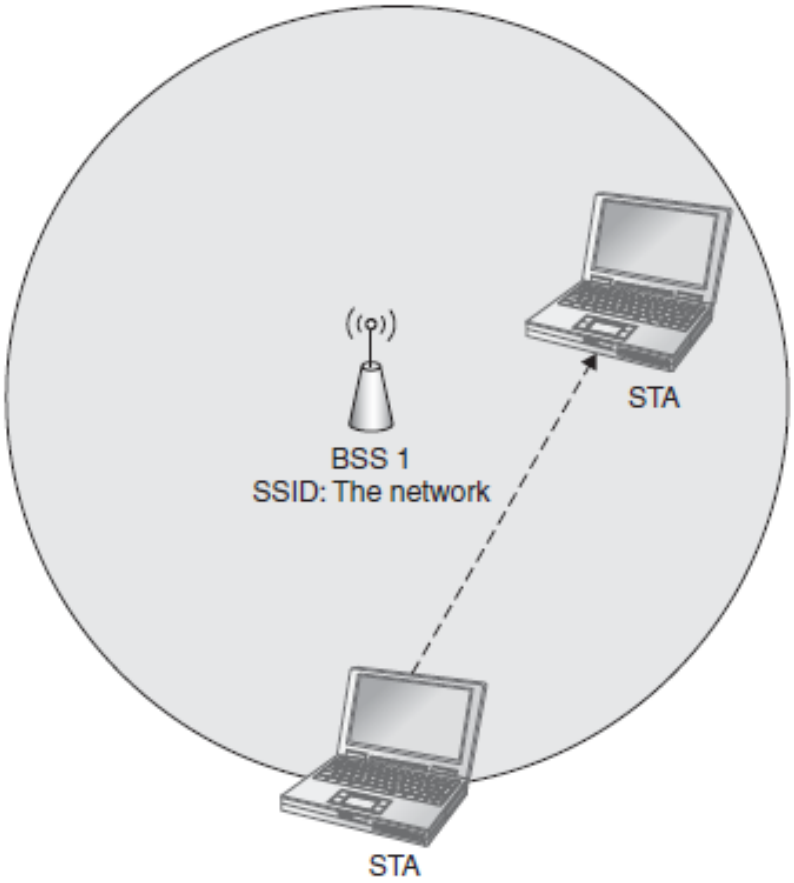
- The AP radio is converted into a sensor radio, allowing the AP to integrate into a wireless intrusion detection system (WIDS) architecture.
- An AP in sensor mode is in a continuous listening state while scanning between multiple channels.
- Sensor mode is also often referred to as **monitor** mode or **scanner**

roaming

- When a station associates with an AP in a BSS, it is joining a potentially larger network (the ESS). If the station moves out of the range of the initial AP, it may disassociate and reassociate with another AP that is participating in the same ESS. This process of reassociation is known as roaming.
- Roaming provides mobility, there are three basic types of mobility that can occur in an IEEE 802.11 WLAN
  1. No-Transition Static or local movement.
  2. BSS-Transition Moving around to different BSSs within an ESS.
  3. ESS-Transition Moving from a BSS in one ESS to a BSS in another. The IEEE states that upper-layer connections are not guaranteed and are likely to be lost.

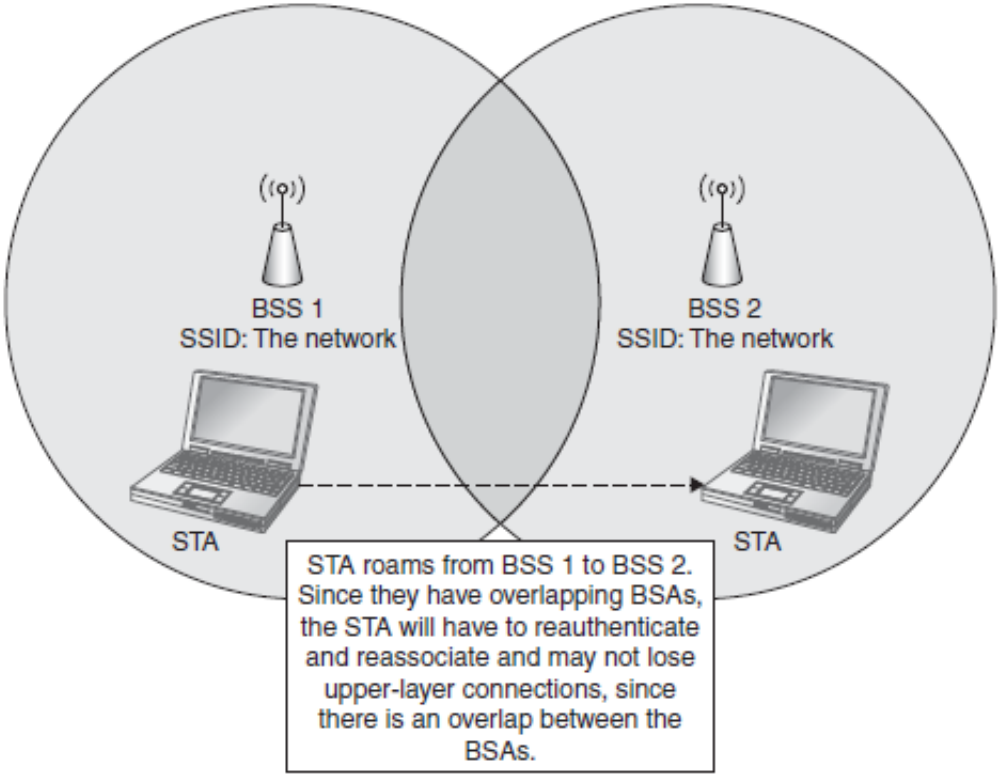
- There are two types of roaming: seamless and reconnecting.
- **Seamless** roaming would be roaming that allows a station to move its association from one BSS to another without losing upper-layer connections. Seamless roaming is usually an implementation of BSS-transition mobility.
- **Reconnecting** roaming would require a new connection. BSS-transition mobility may fall into this category if there is no association handoff operation that can be performed between the two BSSs even though they are in the same ESS.

No-transition mobility



STA moves around within range of its BSS. No roaming occurs and the connection is not lost. This is no-transition mobility.

Seamless roaming
(BSS-transition mobility)

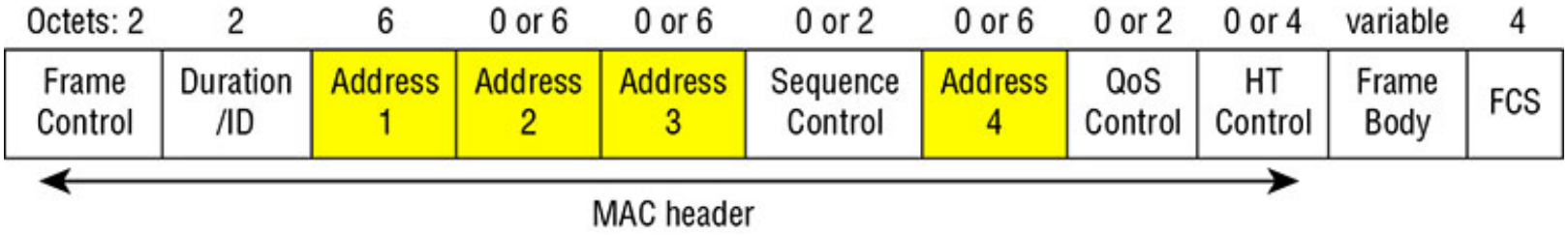


Bits, Bytes, Octets, Frames, Packets

- Bits =1 or 0
- Bytes = 8 bits
- Octets = 8 bits = Byte
  - Octet is used by telecommunication people
  - Byte is used by IT people
- Frames = grouping of bits at layer-2
- Packets = grouping of bits at layer-3
- Datagrams = another term for packets

Frame Categories / Types

- Management Frames: Used to discover APs and to join a BSS
  - Beacon Frame
  - Probe Frames
  - Association Frames… more
- Control Frames: Used to acknowledge successful transmissions and reserve the wireless medium
  - RTS and CTS Frames
  - ACK – Acknowledgement Frames… more
- Data Frames
  - Data Payload Frames (0 – 2304 bytes)
- Extension
  - A new, flexible frame format, currently used only with 802.11ad



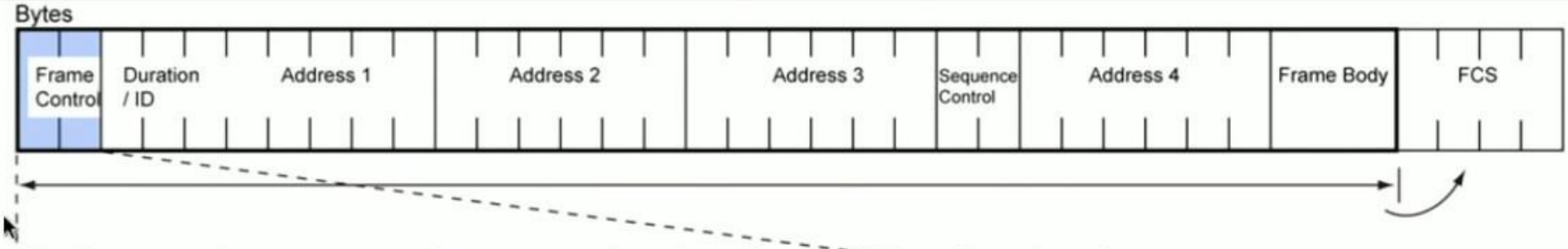
802.11 Frame

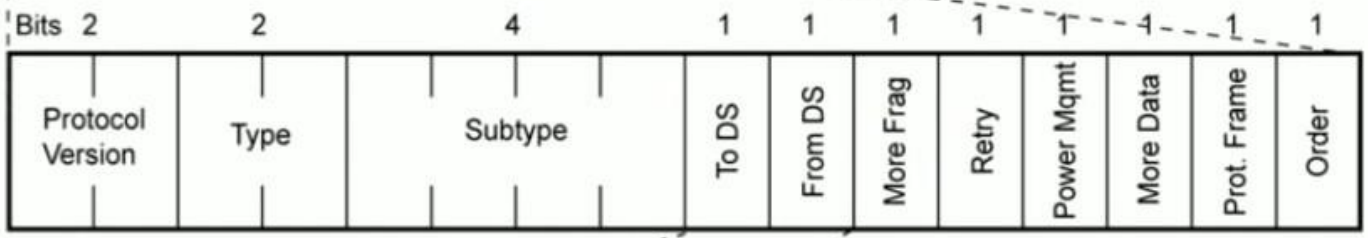
- 802.11 headers are much longer than Ethernet header
- Start with preamble (72 bits or 144 bits) followed by:
- Frame control (2 bytes)
- Duration field: states how long the medium is reserved for (2 bytes)
- Three MAC address (18 bytes)
- Fourth MAC address which is optional (6 bytes)
- Frame body (2304 bytes)
- Frame Check Sequence (4 bytes)
- Total Length of the frame is 2346 bytes maximum

- Used for all data and control frames, but not all fields are used in all contexts. The fields are:
- **Frame Control**:
  - Indicates the type of frame (control, management, or data) and provides control information. Control information includes whether the frame is to or from a DS, fragmentation information, and privacy information.
- **Duration/Connection ID**:
  - If used as a duration field, indicates the time (in microseconds) the channel will be allocated for successful transmission of a MAC frame. In some control frames, this field contains an association, or connection, identifier.

- Addresses:
  - The number and meaning of the 48-bit address fields depend on context. The transmitter address and receiver address are the MAC addresses of stations joined to the BSS that are transmitting and receiving frames over the wireless LAN. The service set ID (SSID) identifies the wireless LAN over which a frame is transmitted.
- Sequence Control:
  - Contains a 4-bit fragment number subfield, used for fragmentation and reassembly, and a 12-bit sequence number used to number frames sent between a given transmitter and receiver.
- Frame Body:
  - Contains an MSDU or a fragment of an MSDU. The MSDU is a LLC protocol data unit or MAC control information.
- Frame Check Sequence:
  - A 32-bit cyclic redundancy check.

Frame Control Field

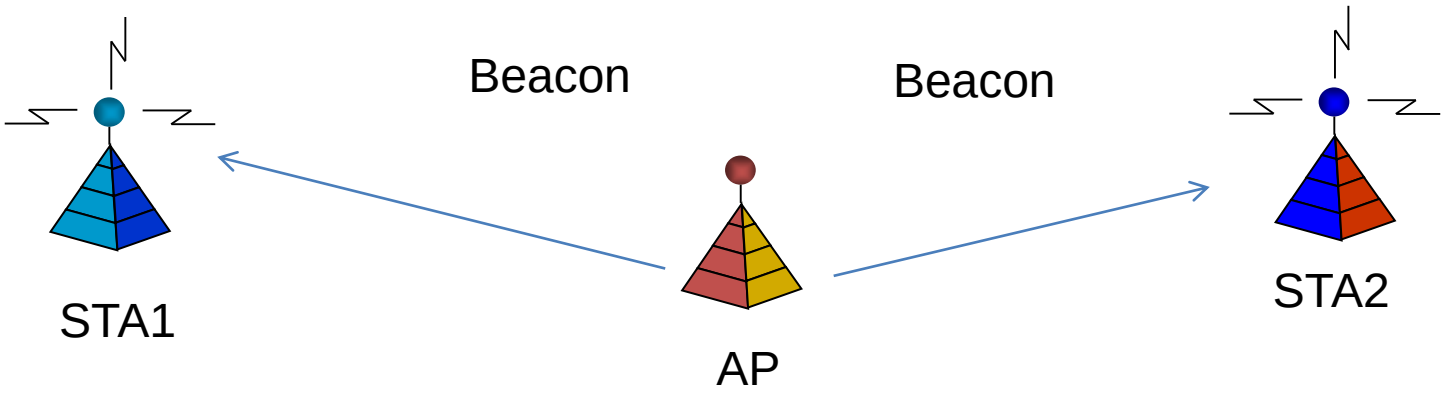




To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	RA/DA	TA/SA	BSSID	n/a
0	1	RA/DA	TA/BSSID	SA	n/a
1	0	RA/BSSID	TA/SA	DA	n/a
1	1	RA	TA	DA	SA

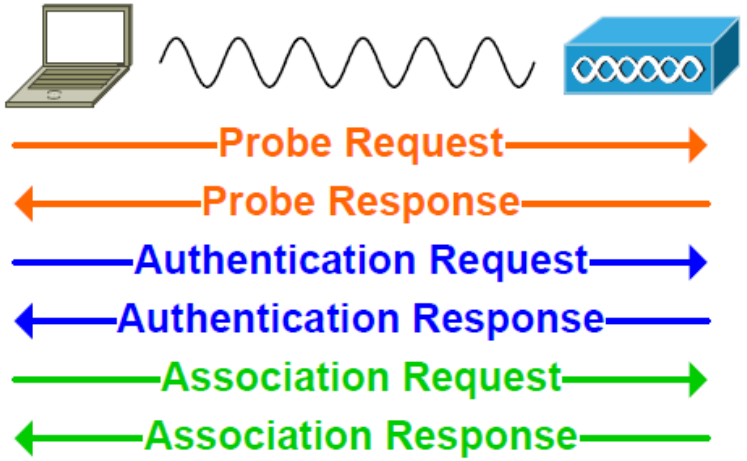
Beacon Management Frame (Beacon)

- Beacon frame is one of the management frames that contains all the information about the network.
- Beacon frames are transmitted periodically, they serve to announce the presence of a wireless LAN and to synchronize the members of the service set.
- Beacon frames are transmitted by the access point (AP) in an infrastructure basic service set (BSS).
- In an ad hoc (IBSS) wireless network all stations take turns broadcasting the beacon frame

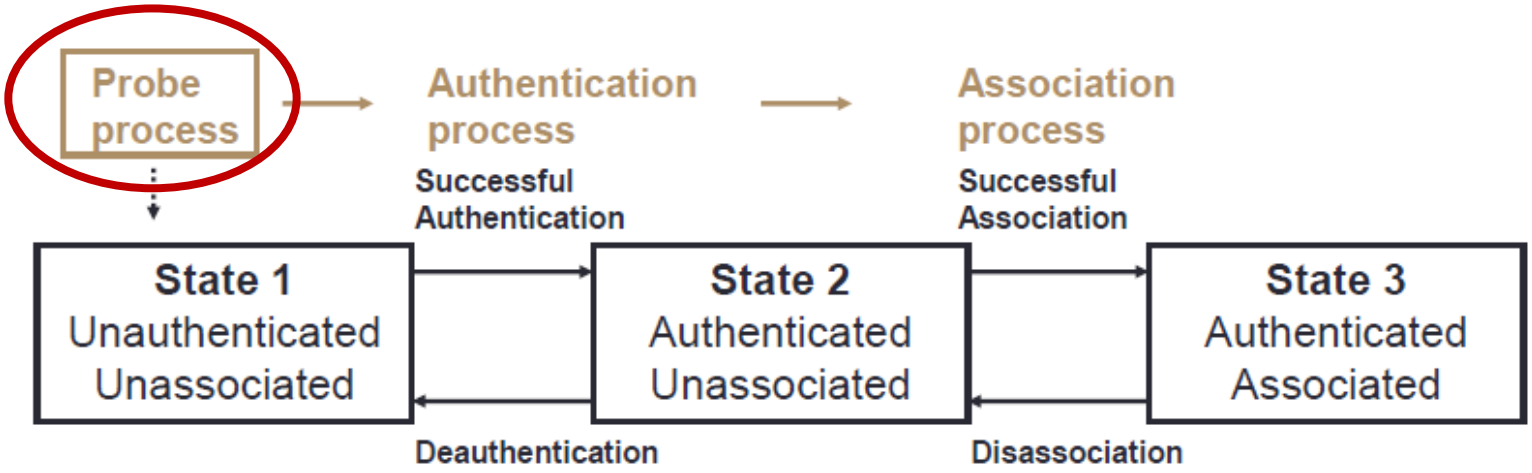


Wireless Connection Process

- The entire process can be broken down into three phases;
  - probe phase,
  - authentication phase
  - association phase.
- Moreover, if the station is in motion it might be necessary to perform a reassociation procedure from time to time.



Station Connectivity process

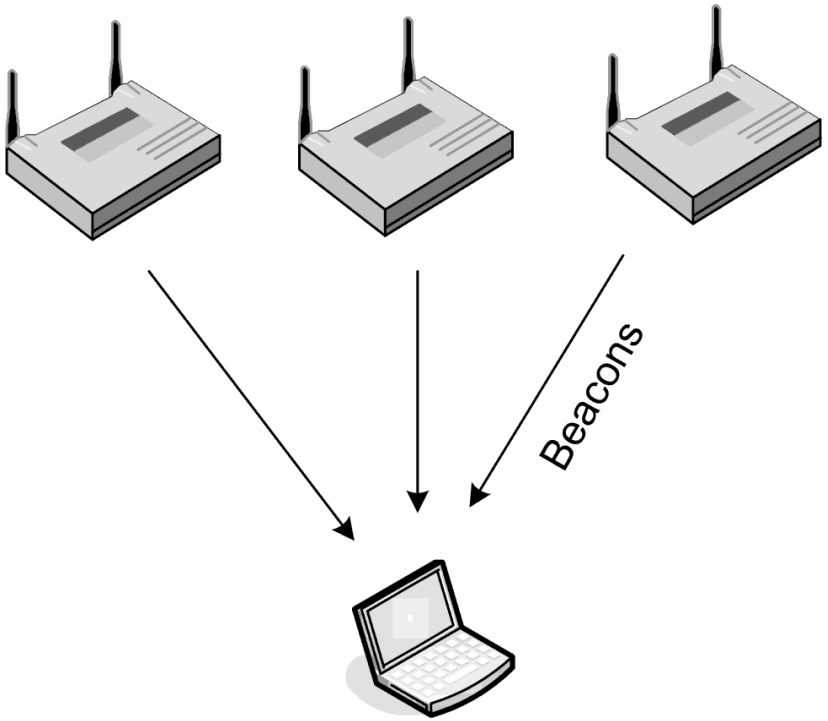


Probe process (scanning)

- Each 802.11 station periodically scans each RF channel in order to find a BSS to join. The process of scanning is critical when a station is first activated.
- After powering up, the station will initiate scanning to find an initial BSS to join.
- As RF conditions change, the station will periodically scan and possibly reassociate with another BSS.
- There are two forms of scanning: passive scanning and active scanning.

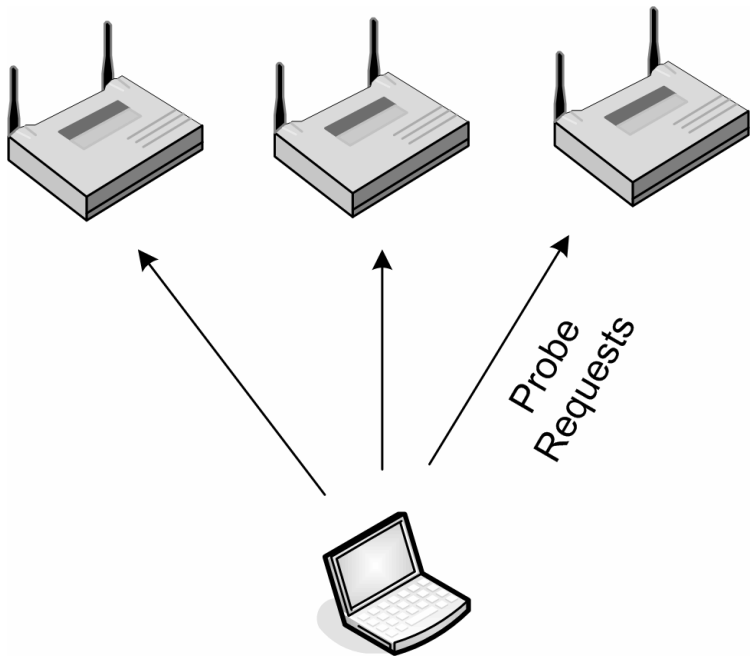
Passive scanning

- Passive scanning is the process through which a STA listens to each channel (or set of channels) for a specific period of time.
- The STA waits for the transmission of beacon management frames (a.k.a. beacons) having the SSID of the network that the station is configured to join.
- Beacons contain fixed fields and information elements that hold information about the BSS which are used by stations to determine whether or not the STA may associate.
- Once the STA detects beacons from one or more APs, it will decide which AP with which to associate
- STA will negotiate a connection on the applicable channel by proceeding with authentication and association processes.



Active scanning

- An STA broadcast probe request frames indicating the SSID of the network that the STA is configured to join.
- The STA that sends the ***probe request*** frames will receive ***probe response*** frames from APs within range and having the specified SSID.
- This process, like that of passive scanning, provides information that the STA can use to determine the AP with which to associate.
- Alternately, an STA can send probes containing a broadcast SSID (a null value) that causes all APs within reach to respond.
- An AP must reply to all probes that contain the broadcast SSID or an SSID that matches its own.



Passive vs Active

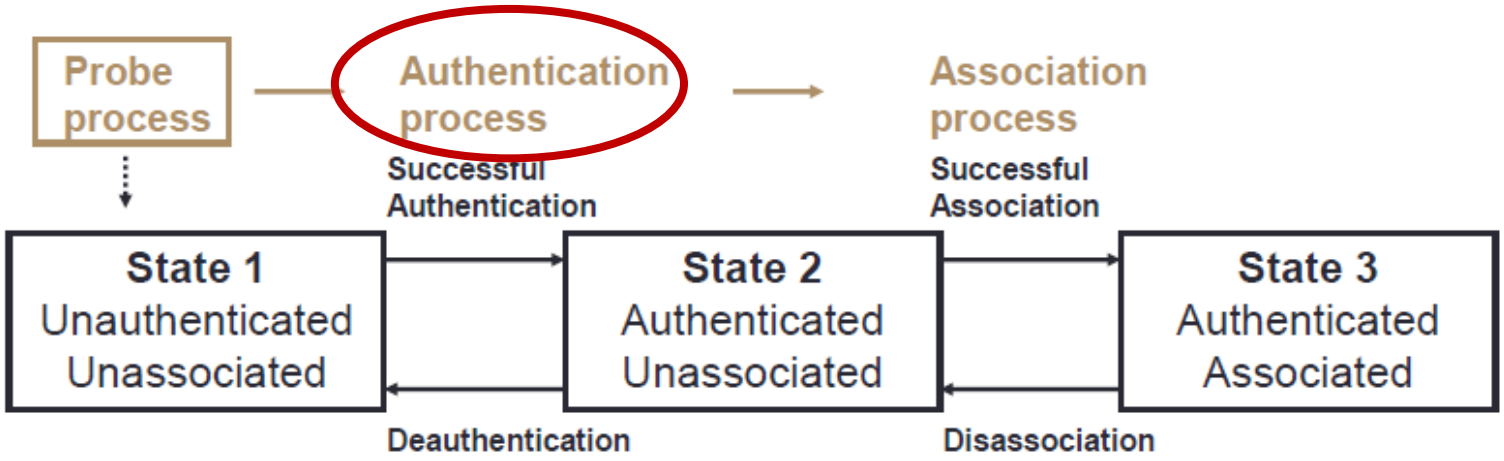
Passive scanning

- The advantage of passive scanning is that;
- it does not require the transmission of any additional frames, which reduces overhead traffic on the wireless medium and improves overall network throughput.

Active scanning

- The advantage of active scanning is that;
- it identifies potential APs faster, which may be necessary if the client STA is experiencing a rapid decrease in received signal strength from frames.

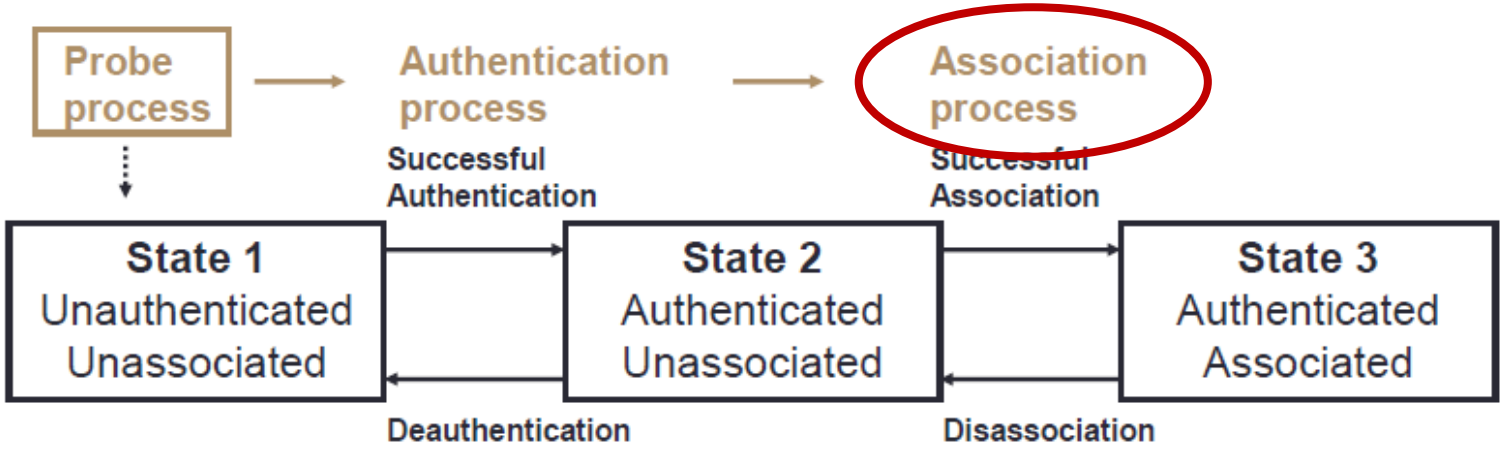
Station Connectivity process



Authentication process

- Authentication is the process by which two stations that wish to communicate, establish their identity to a mutually acceptable level
- Open System Authentication
  - is essentially a null algorithm.
  - all request are accepted – in other words no true authentication (verification of identity) occurs)
- Shared Key Authentication
  - utilizes the wired equivalent privacy (WEP) key for authentication.
  - due to the weaknesses discovered in the WEP algorithm, very few networks should implement and use Shared Key authentication or WEP encryption today

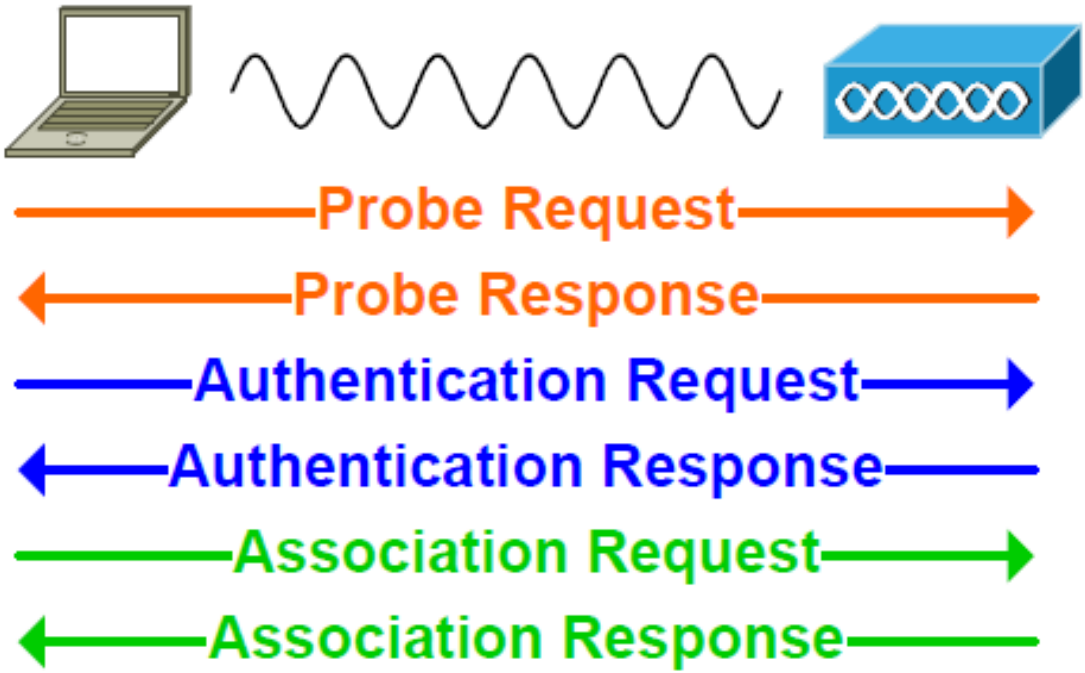
Station Connectivity process



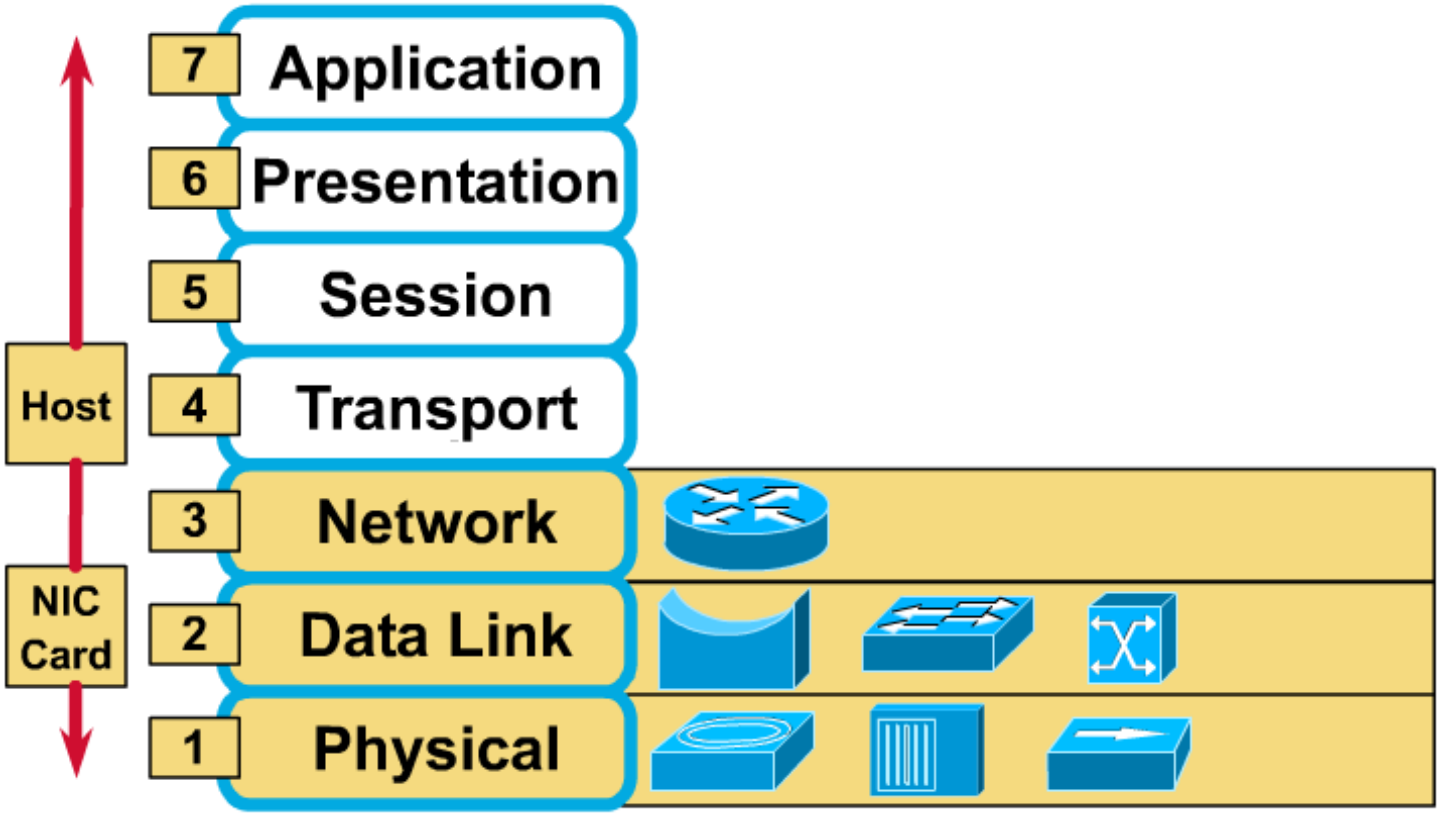
Association process

- Association provides mapping between the STA and AP that allows messages within DS to reach the AP with which STA is associated and ultimately to the STA itself
- Reassociation:
  - when the STA moves from one AP to another with the same ESS (roaming).
  - Keeps the DS informed about current mapping between STAs and APs.
- Disassociation:
  - terminates the existing association
- The STA can associate with only one AP at a time.

Establishing connection

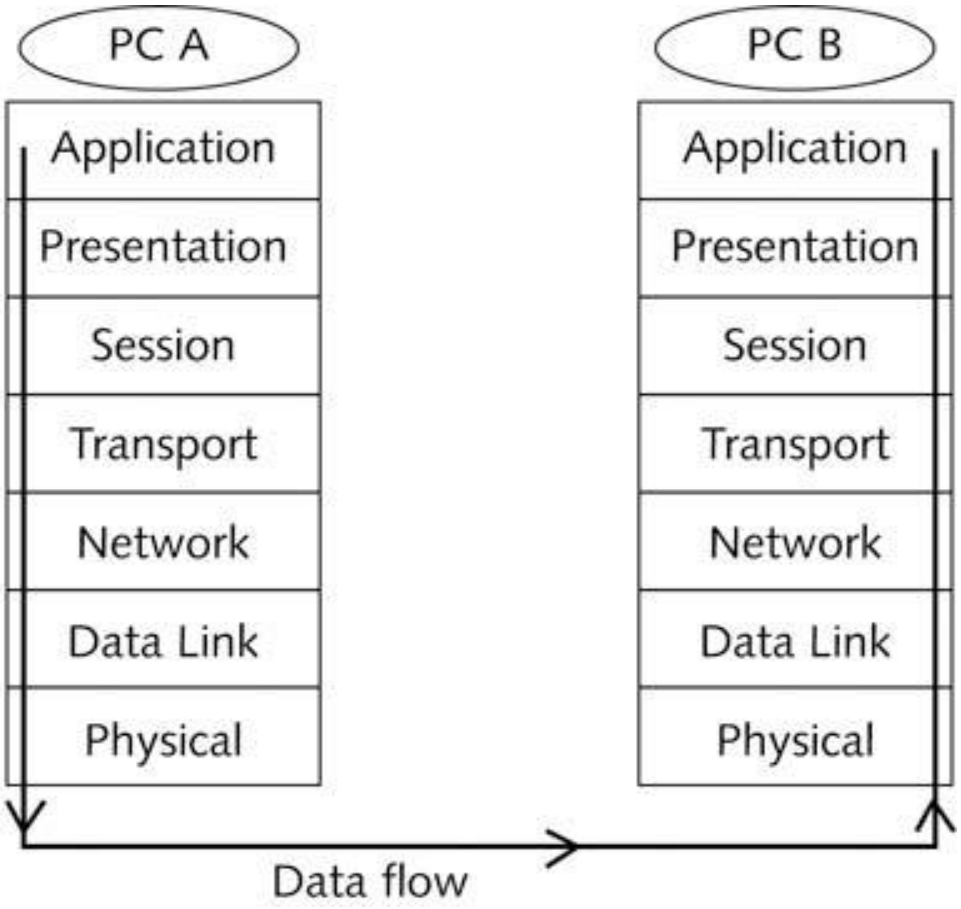


OSI Model

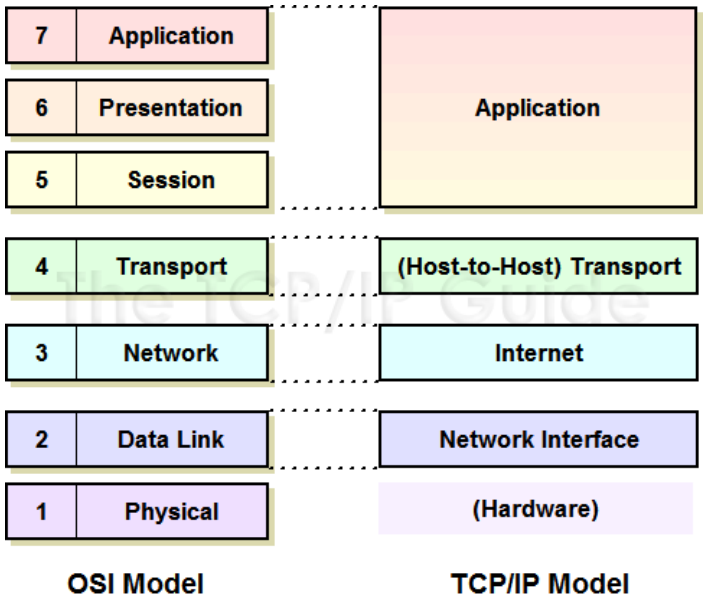


Hosts and servers operate at Layers 2-7; they perform the encapsulation process.
Routers: Layers 1 through 3, make decisions at layer 3
Switches and NICs: Layers 1 and 2, make decisions at layer 2
Hubs and transceivers: Layer 1, no decisions to make

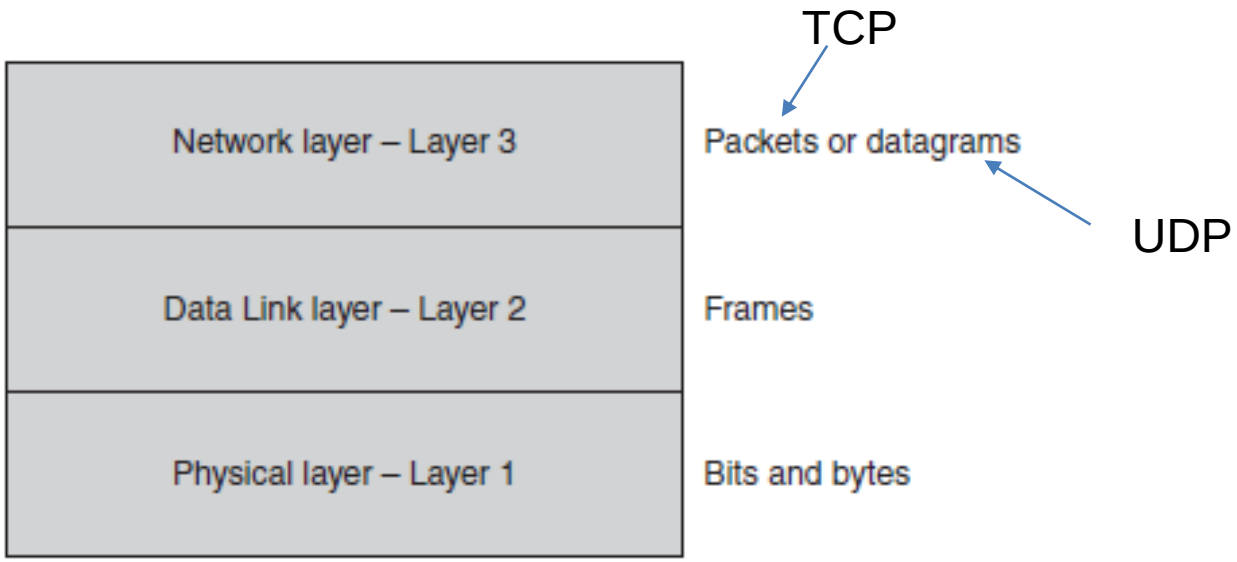
OSI data flow



TCP/IP – OSI model

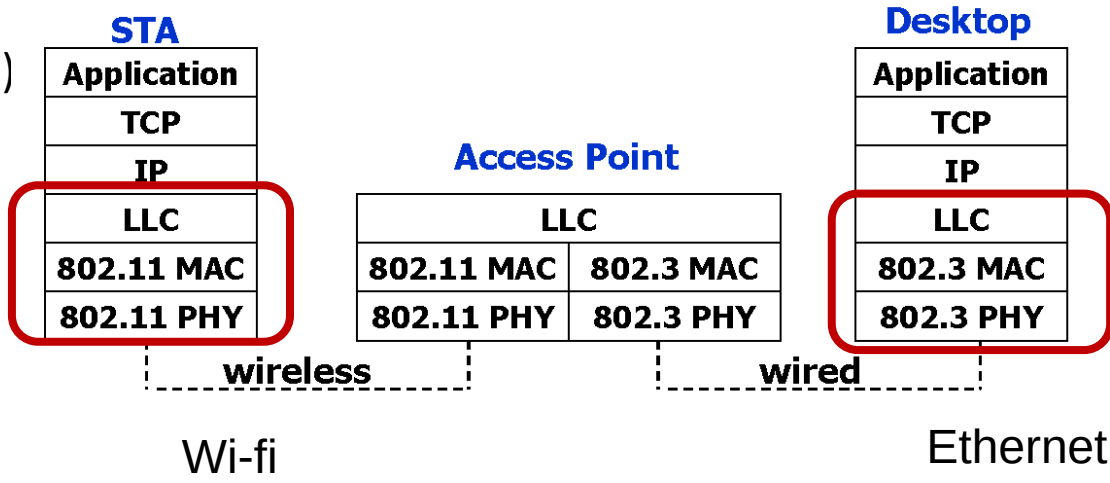


Frames, Packets, and Datagrams

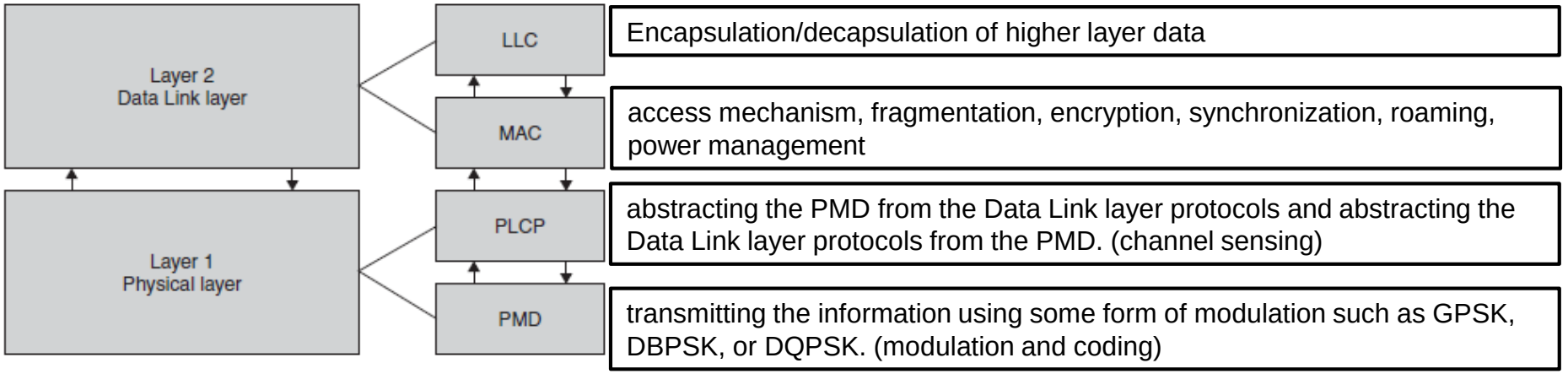


IEEE 802.11 Layers

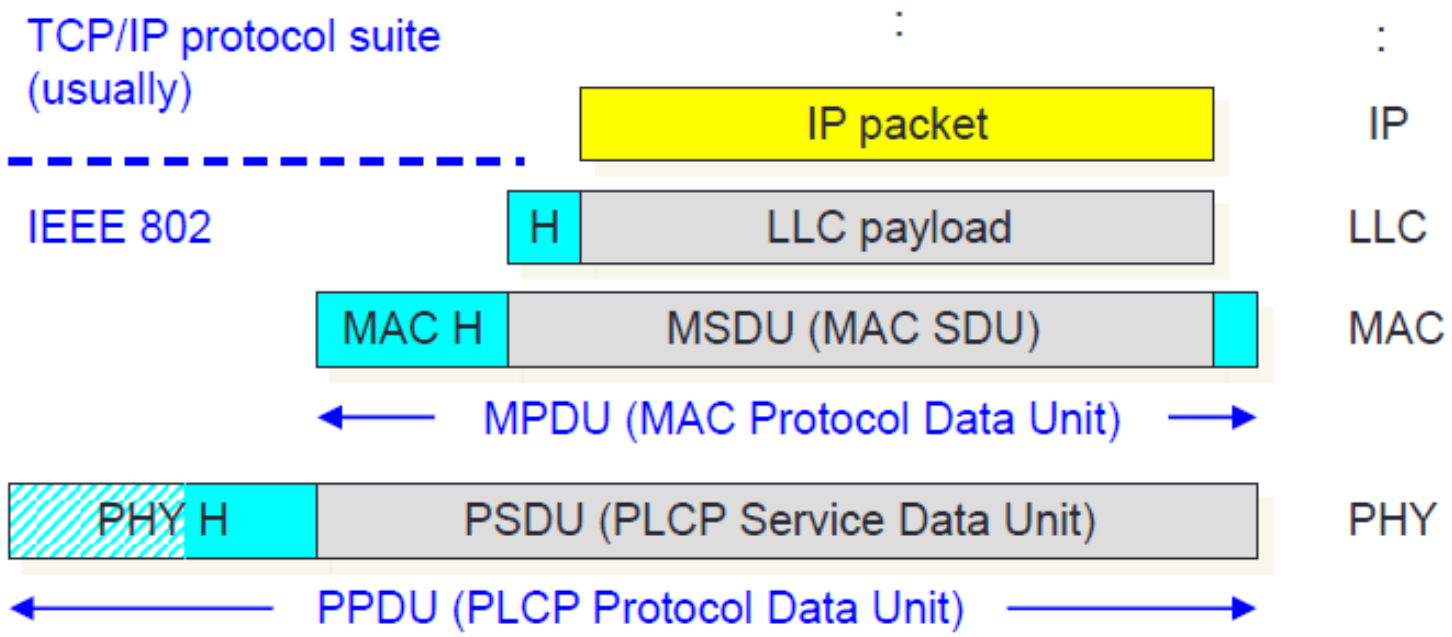
- Data link layer
  - Logical Link Control (LLC)
  - Medium Access Control (MAC)
- Physical (PHY) layer
  - Physical Medium Dependent (PMD)
  - Physical Layer Convergence Protocol (PLCP)



IEEE 802.11 layers and functions



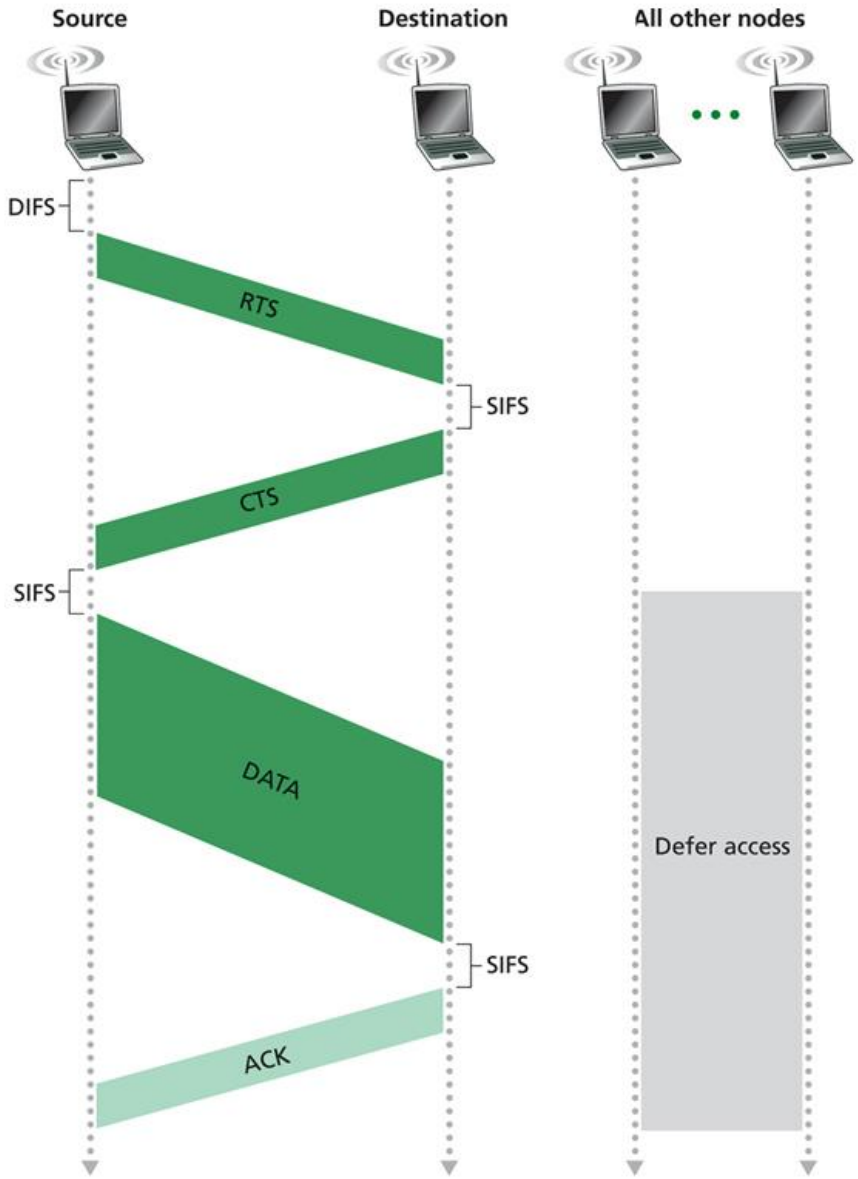
IEEE 802.11 frame structure



IEEE 802.11 Medium Access Control (MAC) Functions

- Scanning- discover AP or BSS
- Synchronization- all stations have the same clock
- Frame Transmission- rules for frame transfer
- Authentication-allow device in network
- Association-after authentication associate with AP
- Reassociation-roaming and association with new AP
- Data Protection-data encryption protects data
- Power Management-save power by sleeping transceiver
- Fragmentation-breakup frame for efficiency and interfere.
- RTS/CTS- solution to hidden node problem

Access control

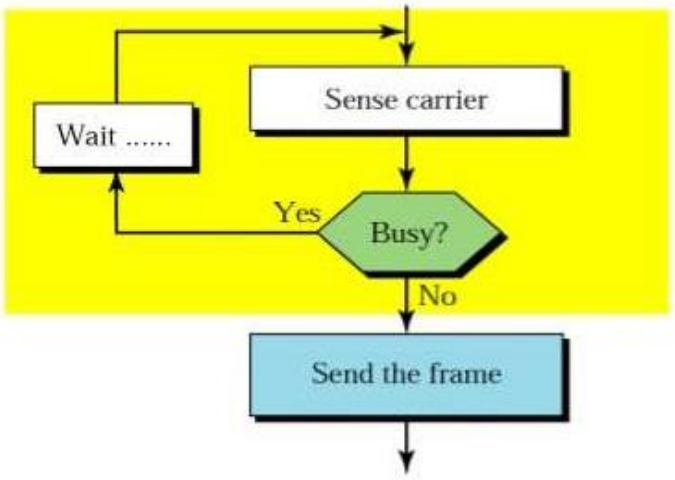


CSMA/CA

Carrier-Sense Multiple Access with Collision Avoidance

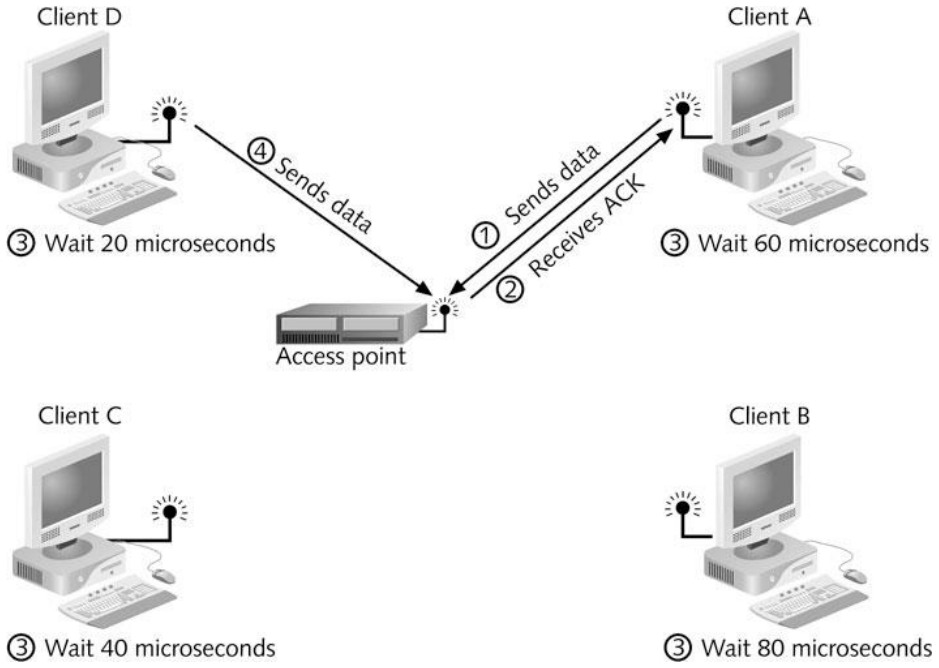
IEEE 802.11 CSMA/CA

- Carrier Sense Multiple Access/Collision Avoidance or CSMA/CA
- Carrier sense is the process of checking to see if the medium is in use or busy.
- Collision avoidance is achieved by signaling to the other devices that one device is about to communicate.
- In IEEE 802.11 WLANs, there are two kinds of carrier sense that are performed:
  1. Virtual carrier sense
  2. Physical carrier sense.



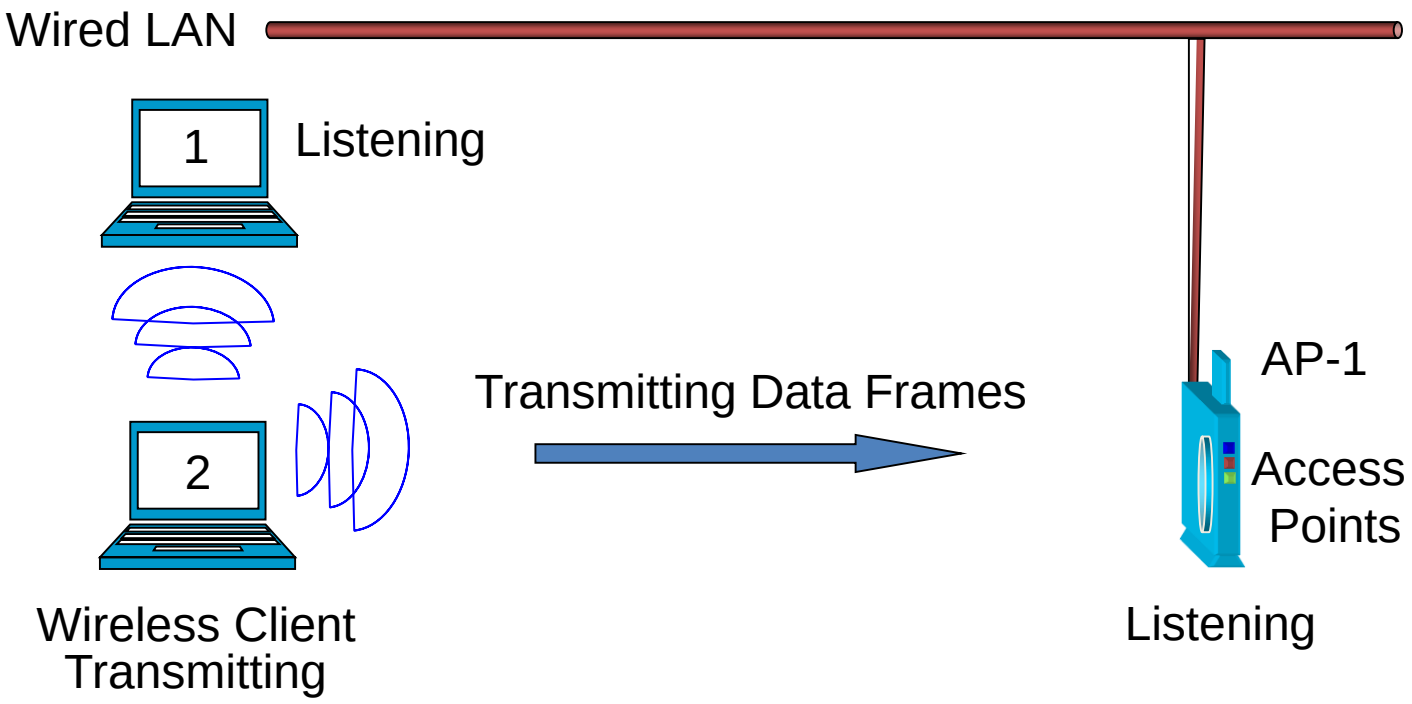
CSMA/CA and ACK

- CSMA/CA also reduces collisions via explicit **frame acknowledgment**
- **Acknowledgment frame (ACK):** Sent by receiving device to sending device to confirm data frame arrived intact
- If ACK not returned, transmission error assumed
- CSMA/CA does not eliminate collisions and does not solve hidden node problem



CSMA/CA Collision Handling

- 802.11 standard employs half-duplex radios-radios capable of transmission or reception-but not both simultaneously



- **Physical carrier sense** uses clear channel assessment (CCA) to determine if the physical medium is in use. CCA is accomplished by monitoring the medium to determine if the amount of RF energy detected exceeds a particular threshold.
- *A STA may be able to hear the AP and the AP may be able to hear the other STA, but the two STAs may not be able to hear each other. This results in what is commonly known as the* ***Hidden Node Problem****. For this reason, wireless networks must use other forms of carrier sense to deal with medium access control.*
- **Virtual carrier sense** uses a *network allocation vector* (NAV). The NAV is a timer in each STA that is used to determine if the STA can utilize the medium. If the NAV has a value of 0, the STA may contend for the medium. If the NAV has a value greater than 0, the STA must wait until the timer counts down to 0 to contend for the medium. STAs configure their NAV timers according to *Duration Fields* in other frames using the medium.

Interframe Spacing

- After the station has determined that the medium is available, using carrier sensing techniques, it must observe interframe spacing (IFS) policies
- IFS is a time interval in which frames cannot be transmitted by stations within a BSS.
- The time interval differs, depending on the frame type and the applicable IFS type for that frame.
- The IFS include the following types;
  - Short interframe spacing (SIFS)
  - Point (coordination function) interframe spacing (PIFS)
  - Distributed (coordination function) interframe spacing (DIFS)
  - Extended interframe spacing (EIFS)

Contention Window

- The IFS delay interval is not the end of the wait for devices that are seeking time on the wireless media. After the IFS delay interval has passed, the device must then initiate a random backoff algorithm and then contend for the wireless media if the Distributed Coordination Function is in effect. This random backoff algorithm is processed and applied using the contention window.

Collision Avoidance

- Ultimately, the carrier sense, IFS, and random backoff times are used in order to decrease the likelihood that any two stations will try to transmit at the same time on the Wireless Media.
- The IFS parameters are also used in order to provide priority to the more time-sensitive frames such as ACK frames and CTS frames.
- The CCA (PHY and MAC), IFS, variable contention window, and random backoff times, together, form the core of the Distributed Coordination Function.

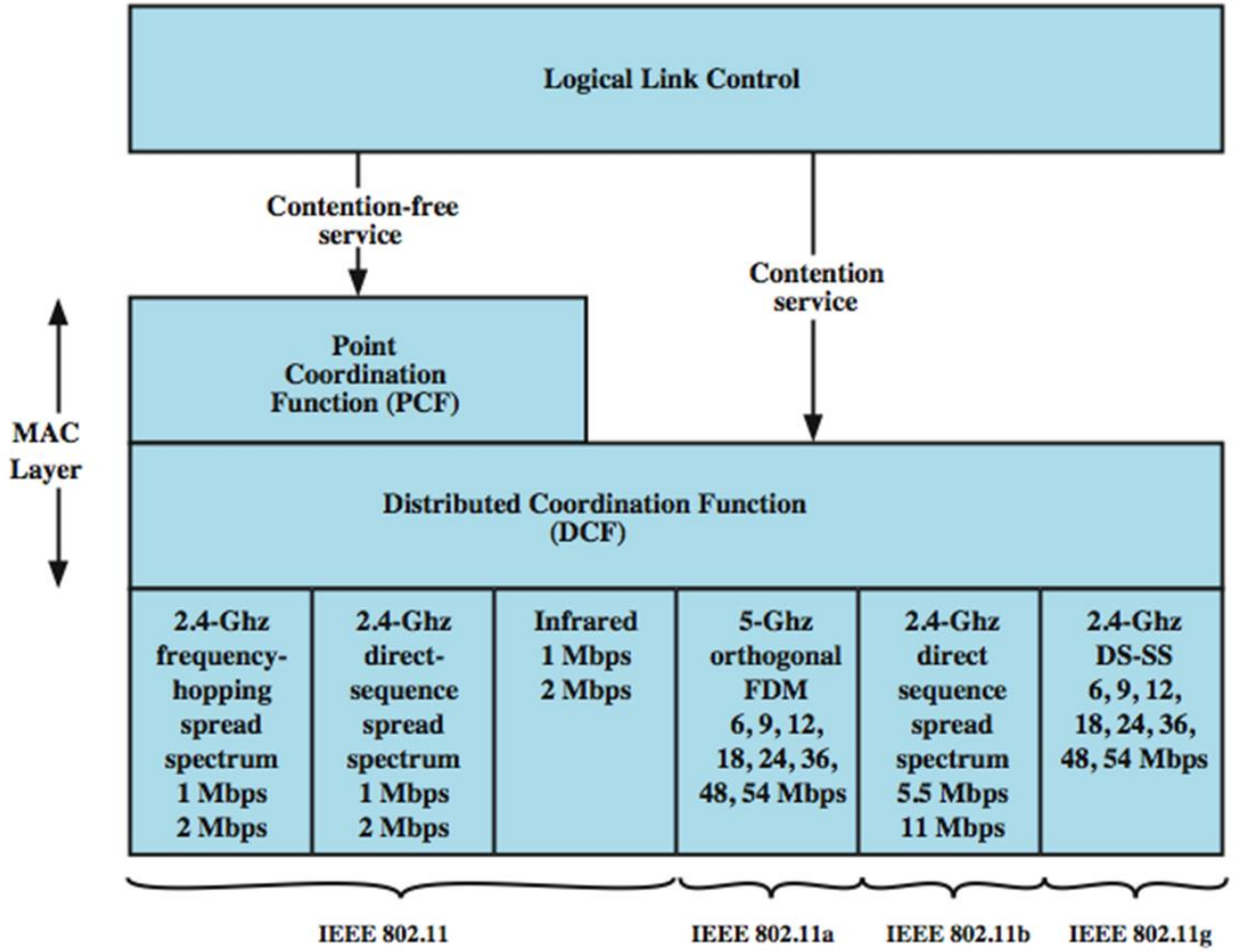
Contention Window and Backoff Time

- Contention Window is a range of integers (0 – 31), which is chosen at random to become the backoff time
- Backoff time is a random time used to establish a frame-to-transmit
  - Random Backoff Time = Random Integer x Slot Time
  - Slot time varies for PHY modulation (number of slots is announced by the STA for the data to be sent)
    - FHSS-50us, DHSS-20us, OFDM-9us, HR/DSS-20us, ERP Long Slot-20us, ERP Short Slot-9us, 802.1n-9us

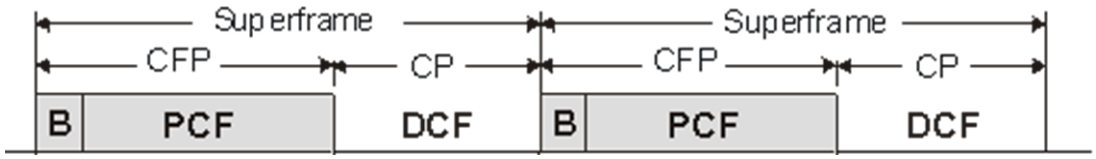
Transmitting on the WLAN: Fragmentation

- **Fragmentation:** Divide data to be transmitted from one large frame into several smaller ones
  - Reduces probability of collisions
  - Reduces amount of time medium is in use
- If data frame length exceeds specific value, MAC layer fragments it
  - Receiving station reassembles fragments
- Alternative to RTS/CTS
  - High overhead
    - ACKs and additional SIFS time gaps

802.11 Medium Access Methods



- PCF and DCF operate concurrently within the same BSS.
- The two access methods alternate, with a contention-free period (CFP) followed by a contention period (CP).



- DCF: fundamental access method of IEEE 802.11 MAC, implemented in all STAs.
  - known as CSMA/CA

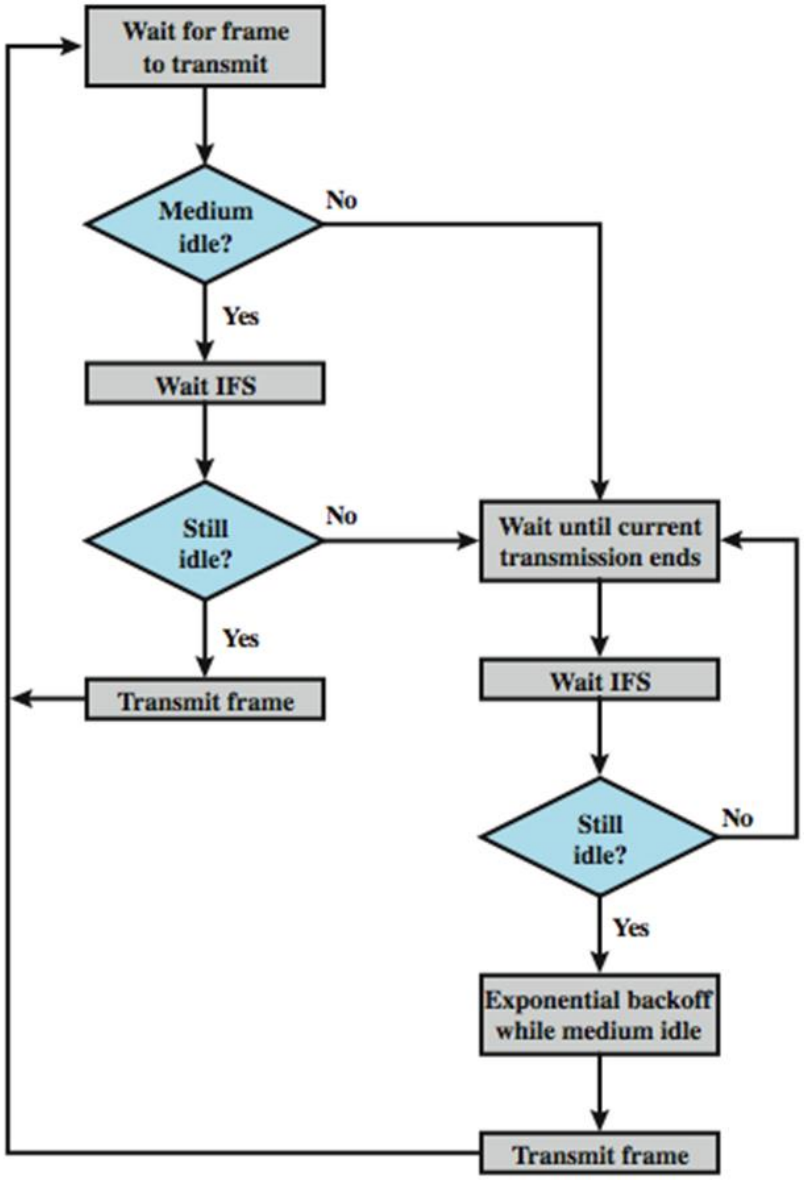
Point Coordination Function

- Supports time-bounded services.
- Lets STAs to have priority access to the wireless medium.
- Polling STAs one by one (centralized operation)
- Coordinated by Point Coordinator (PC), typically collocated with the AP.
- PCF has higher priority than the DCF.
- Beacon frame is a management frame that maintains the synchronization of the timers in the STAs and delivers protocol related parameters.

Distributed Coordination Function (DCF)

- To avoid interference among simultaneous transmissions
  - But enable as many non-interfering transmission as possible
  - Maintain fairness among transmissions
- No centralized coordinators: fully distributed operations
- No clock synchronization: asynchronous operations
- Physical and virtual carrier sense (NAV) is used
- uses CSMA/CA
- Backoff is used
- Medium reservation with RTS/CTS

IEEE 802.11 Medium Access Control Logic



Summary

Overview of Wireless Standards, Organizations, and Fundamentals (1)
IEEE 802.11 Standard and Amendments (2)
Wireless LAN Topologies (7)
802.11 Medium Access (8)
802.11 MAC (9)
WLAN Architecture (11)

THANK YOU