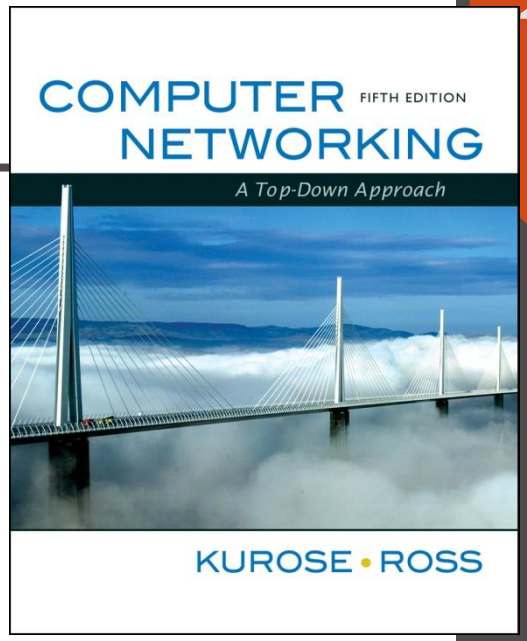
U.PORTO

U.PORTO
FCUP FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

[dcc]

Wireless Networks

Tópicos Avançados em Redes
2023/2024



A note on the use of these ppt slides:

We're making these slides freely available to all (faculty, students, readers). They're in PowerPoint form so you can add, modify, and delete slides (including this one) and slide content to suit your needs. They obviously represent a *lot* of work on our part. In return for use, we only ask the following:

- If you use these slides (e.g., in a class) in substantially unaltered form, that you mention their source (after all, we'd like people to use our book!)
- If you post any slides in substantially unaltered form on a www site, that you note that they are adapted from (or perhaps identical to) our slides, and note our copyright of this material.

Thanks and enjoy! JFK / KWR

Computer Networking: A Top Down Approach
5th edition.
Jim Kurose, Keith Ross
Addison-Wesley, April 2009.

With changes by pbrandao

Outline

Introduction

Wireless

- Wireless links, characteristics
  - CDMA
- IEEE 802.11 wireless LANs (“wi-fi”)

Recap on Link Layer

Link Layer Services

- *framing, link access:*
  - encapsulate datagram into frame, adding header, trailer
  - channel access if shared medium
  - "MAC" addresses used in frame headers to identify source, dest
    - different from IP address!
- *reliable delivery between adjacent nodes*
  - seldom used on low bit-error link (fibre, some twisted pair)
  - wireless links: high error rates
    - Q: why both link-level and end-end reliability?

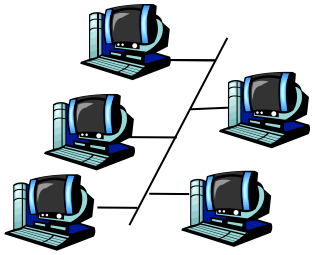
Link Layer Services (more)

- *error detection:*
  - errors caused by signal attenuation, noise
  - receiver detects presence of errors:
    - signals sender for retransmission or drops frame
- error correction:
  - receiver identifies *and corrects* bit error(s) without resorting to retransmission
- *flow control:*
  - pacing between adjacent sending and receiving nodes
- *half-duplex or full-duplex*
  - with half duplex, nodes at both ends of link can transmit, but not at same time

Multiple Access Links and Protocols

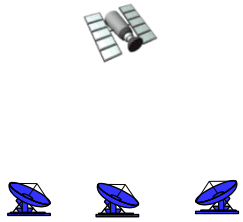
Two types of links:

- point-to-point
  - leased line connecting two routers via synchronous serial ports
  - full duplex Ethernet link between switch and host
- broadcast (shared medium)
  - old-fashioned Ethernet
  - upstream HFC (cable)
  - 802.11 wireless LAN



shared wire (e.g., cabled Ethernet)

shared RF (e.g., 802.11 WiFi)



shared RF (satellite)

humans at a cocktail party (shared air, acoustical)

Multiple Access protocols

- single shared broadcast channel
- two or more simultaneous transmissions by nodes: collision
  - if node receives two or more signals at the same time, they interfere with each other and none is received correctly

multiple access protocol

- distributed algorithm that determines how nodes share channel, i.e., determine when node can transmit
- communication about channel sharing must use channel itself
  - no out-of-band channel for coordination!

Ideal Multiple Access Protocol

Ideally, in a broadcast channel of capacity R bps

1. when one node wants to transmit, it can send at rate R
2. when M nodes want to transmit, each can send at average rate R/M
   - efficient use of channel capacity
   - fair distribution of channel capacity
3. fully decentralized
   - no special node to coordinate transmissions
   - no synchronization of clocks, slots
4. simple

MAC Protocols: a taxonomy

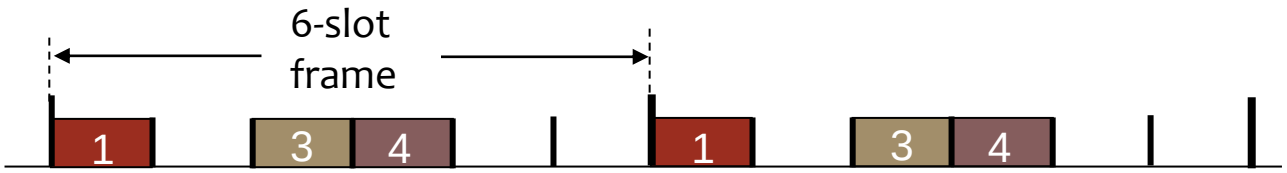
Three broad classes:

- Channel Partitioning
  - divide channel into smaller "pieces" (time slots, frequency, code)
  - assign pieces to nodes for exclusive use
- Random Access
  - channel not divided, allow collisions
  - "recover" from collisions
- "Taking turns"
  - nodes take turns, but nodes with more to send can take longer turns

Channel Partitioning MAC protocols: TDMA

TDMA: time division multiple access

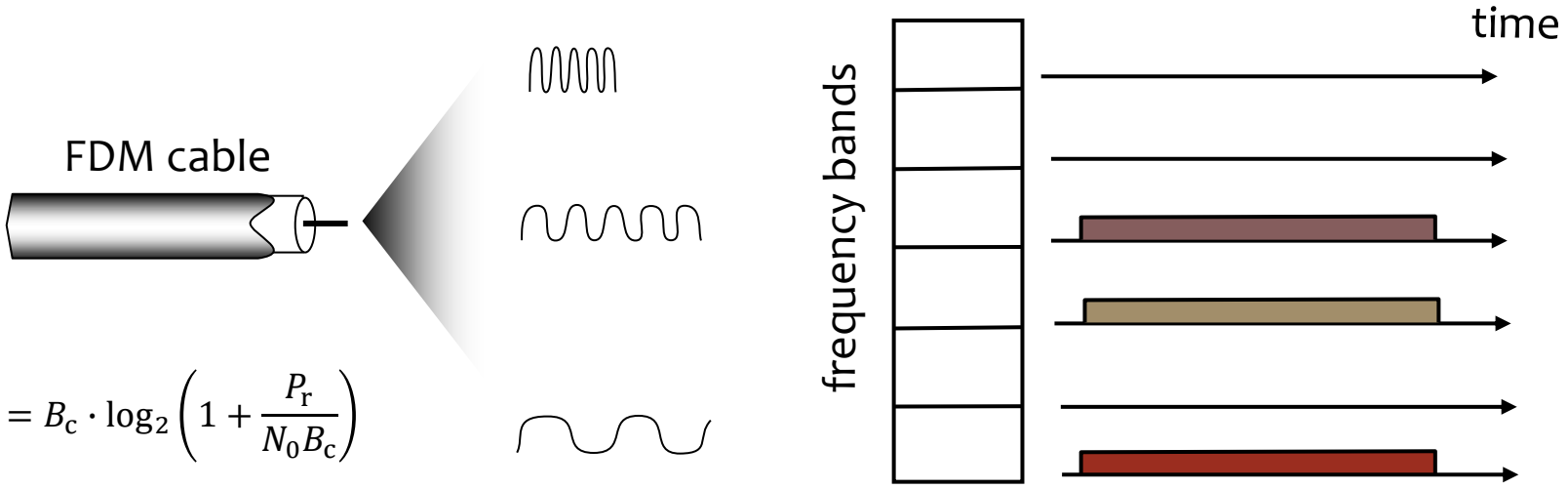
- access to channel in "rounds"
- each station gets fixed length slot (length = pkt tx time) in each round
- unused slots go idle
- example: 6-station LAN, 1,3,4 have pkt, slots 2,5,6 idle



Channel Partitioning MAC protocols: FDMA

FDMA: frequency division multiple access

- channel spectrum divided into frequency bands
- each station assigned fixed frequency band
- unused transmission time in frequency bands go idle
- ex.: 6-station LAN; stations 1,3,4 have pkts; freq. bands 2,5,6 idle

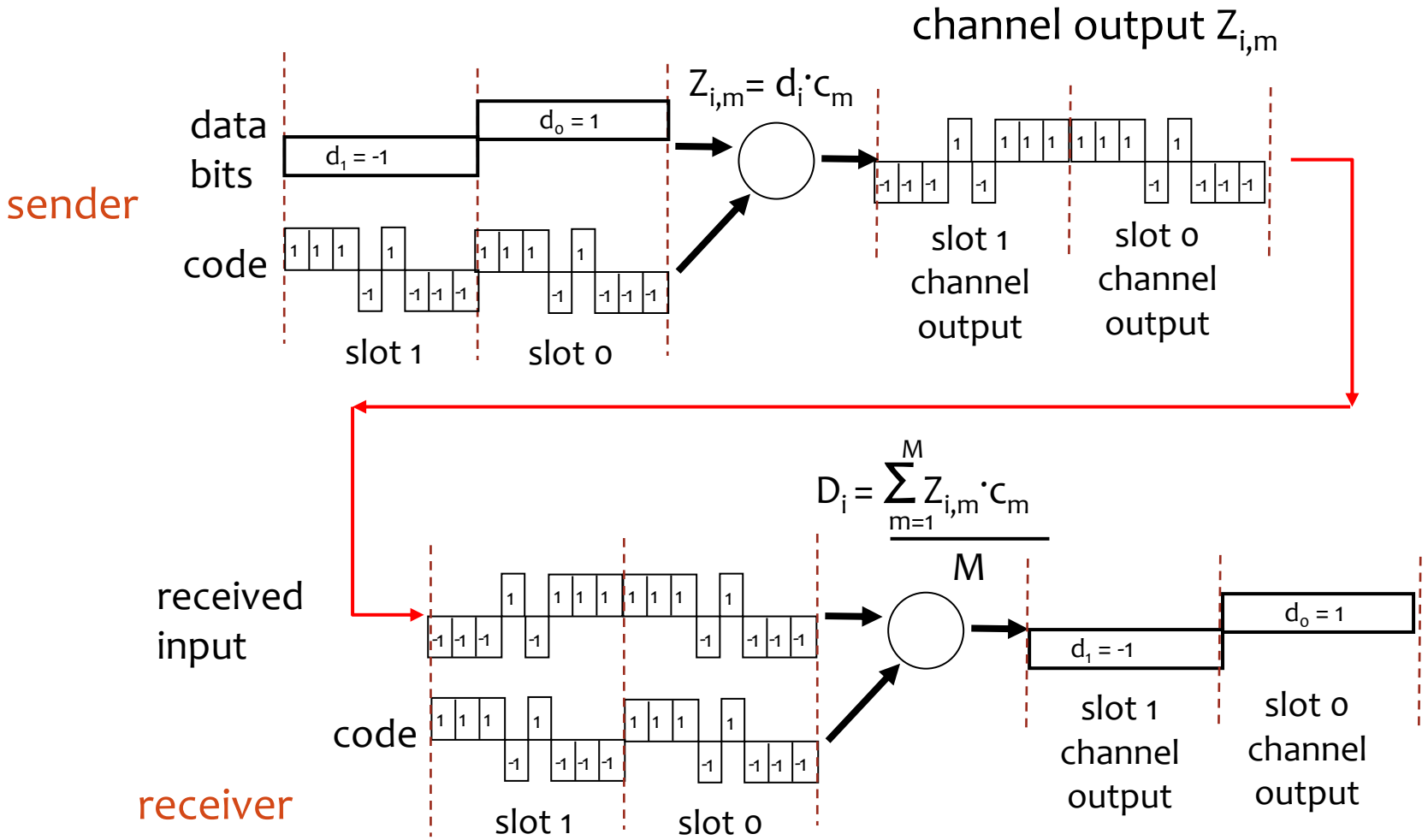


$$C = B_c \cdot \log_2\left(1 + \frac{P_r}{N_0 B_c}\right)$$

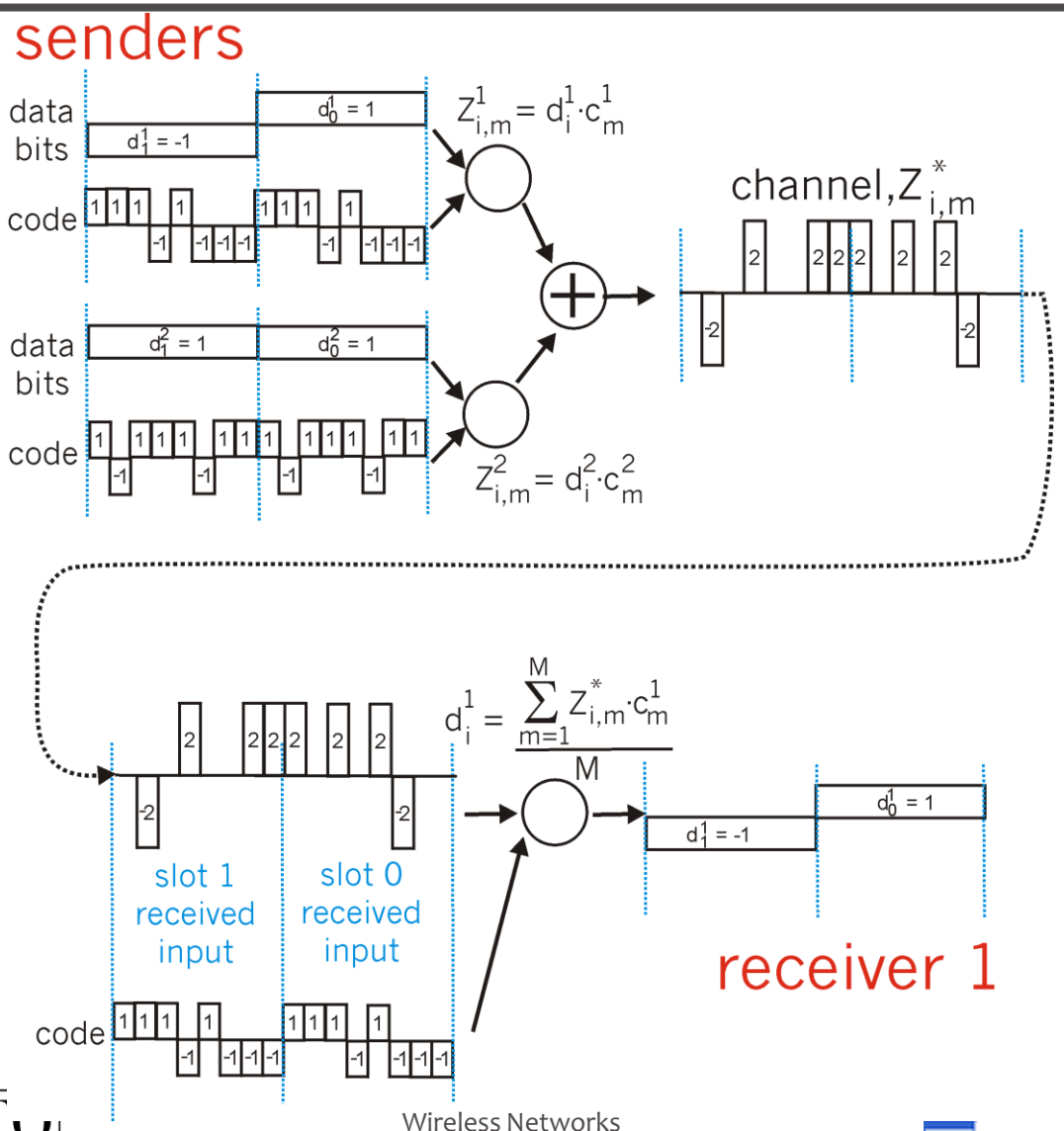
Code Division Multiple Access (CDMA)

- used in several wireless broadcast channels standards (cellular, satellite, etc.)
- unique "code" assigned to each user ➔ code set partitioning
- all users share same frequency, but each user has own "chipping" sequence (code) to encode data
- encoded signal = (original data) × (chipping sequence)
- decoding: inner-product of encoded signal and chipping sequence
- allows multiple users to "coexist" and transmit simultaneously with minimal interference
  - provided codes are "orthogonal"…

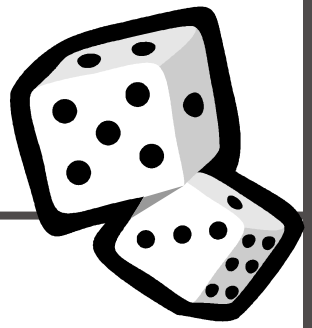
CDMA Encode/Decode



CDMA: two-sender interference



Random Access Protocols



- When node has packet to send
  - transmit at full channel data rate R.
  - no *a priori* coordination among nodes
- Two or more transmitting nodes ➜ "collision"
- A random access MAC protocol specifies:
  - how to detect collisions
  - how to recover from collisions (e.g., via delayed retransmissions)
- Examples of random access MAC protocols:
  - ALOHA
  - slotted ALOHA
  - CSMA, CSMA/CD, CSMA/CA

Slotted ALOHA

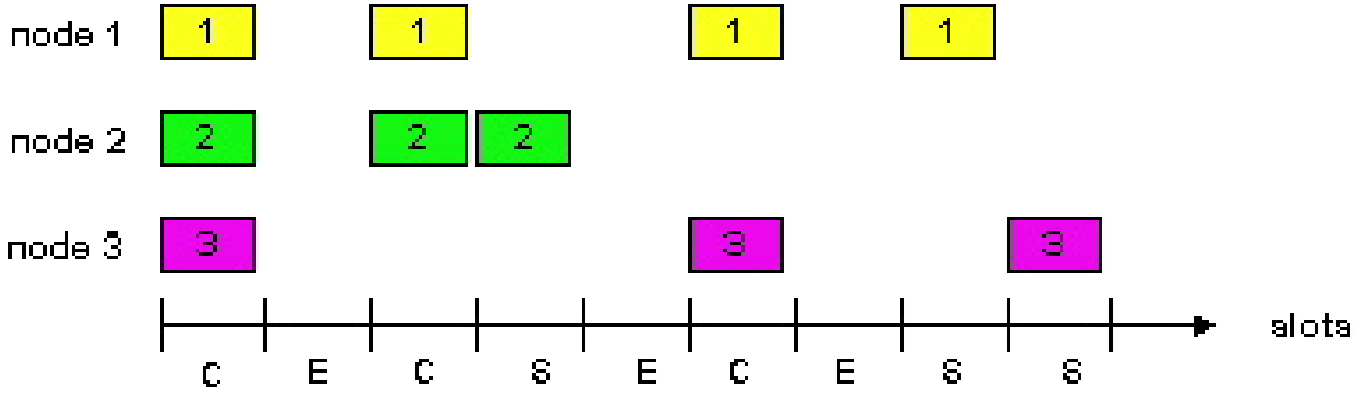
Assumptions:

- all frames have same size
- time divided into equal size slots (time to transmit 1 frame)
- nodes start to transmit only at slot beginning
- nodes are synchronized
- if 2 or more nodes transmit in slot, all nodes detect collision

Operation:

- when node obtains fresh frame, transmits in next slot
  - *if no collision:* node can send new frame in next slot
  - *if collision:* node retransmits frame in each subsequent slot with prob. *p* until success

Slotted ALOHA



Pros

- single active node can continuously transmit at full rate of channel
- highly decentralized: only slots in nodes need to be in sync
- conceptually simple

Cons

- collisions, wasting slots
- idle slots
- nodes may be able to detect collision in less time than to transmit packet
- needs clock synchronization

Slotted Aloha efficiency

- prob that given node has success in a slot
  $= p(1-p)^{N-1}$
- prob that *any* node has a success
  $= Np(1-p)^{N-1}$

- max efficiency: find p* that maximizes
  $Np(1-p)^{N-1}$
- for many nodes, take limit of
  $Np^*(1-p^*)^{N-1}$ as $N \rightarrow \infty$
- substitute p* for p in efficiency formula to get:

Max efficiency
$= 1/e = 0.37$

At best: channel used for useful transmissions only 37% of the time!

!

Pure ALOHA

- Aloha: simple, no synchronization needed
- when frame first arrives
  - transmit immediately
- collision probability increases:
  - frame sent at t_0 collides with other frames sent in $[t_0-1, t_0+1]$

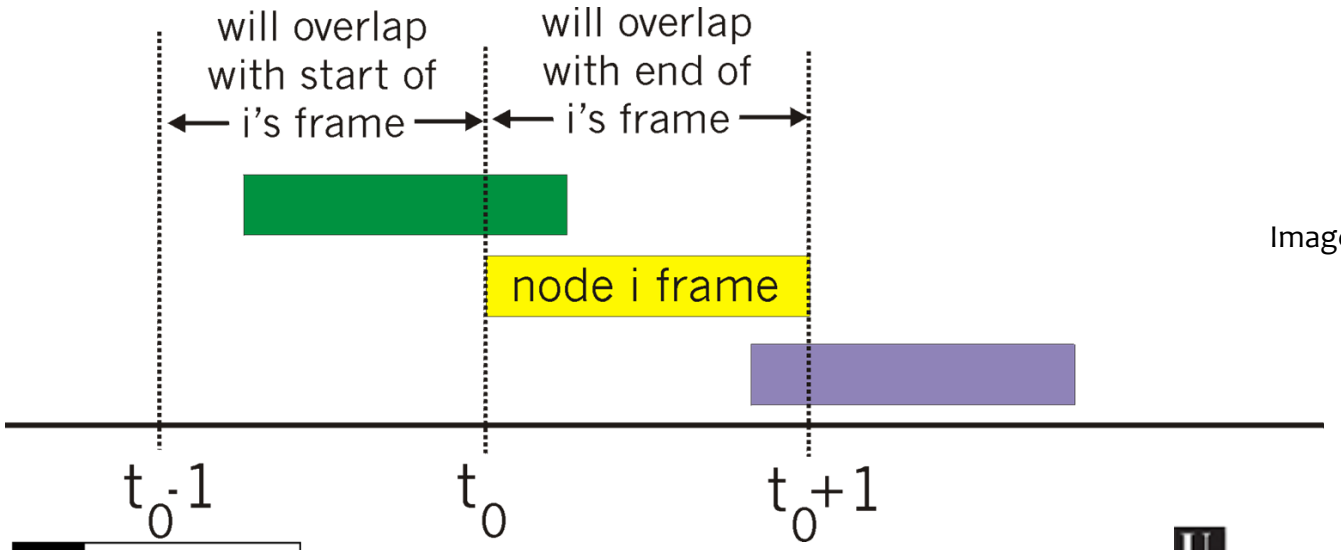


Image from Wikipedia

Aloha efficiency

Efficiency : long-run fraction of successful slots (many nodes, all with many frames to send)

- *suppose:* N nodes with many frames to send, each transmits in slot with probability *p*

P(success by any node)
= $N \cdot p \cdot (1-p)^{2(N-1)}$

choosing optimum p and then letting N → ∞...

= 1/(2e) = 0.18

P(success by given node) =
P(node transmits) x
P(no other node transmits in $[p_o\text{-}1, p_o]$) x
P(no other node transmits in $[p_o, p_{o+1}]$)
= $p \cdot (1-p)^{N-1} \cdot (1-p)^{N-1}$
= $p \cdot (1-p)^{2(N-1)}$

At best: channel used for useful Transmissions only 18% of the time!

!

Pure vs Slotted Aloha

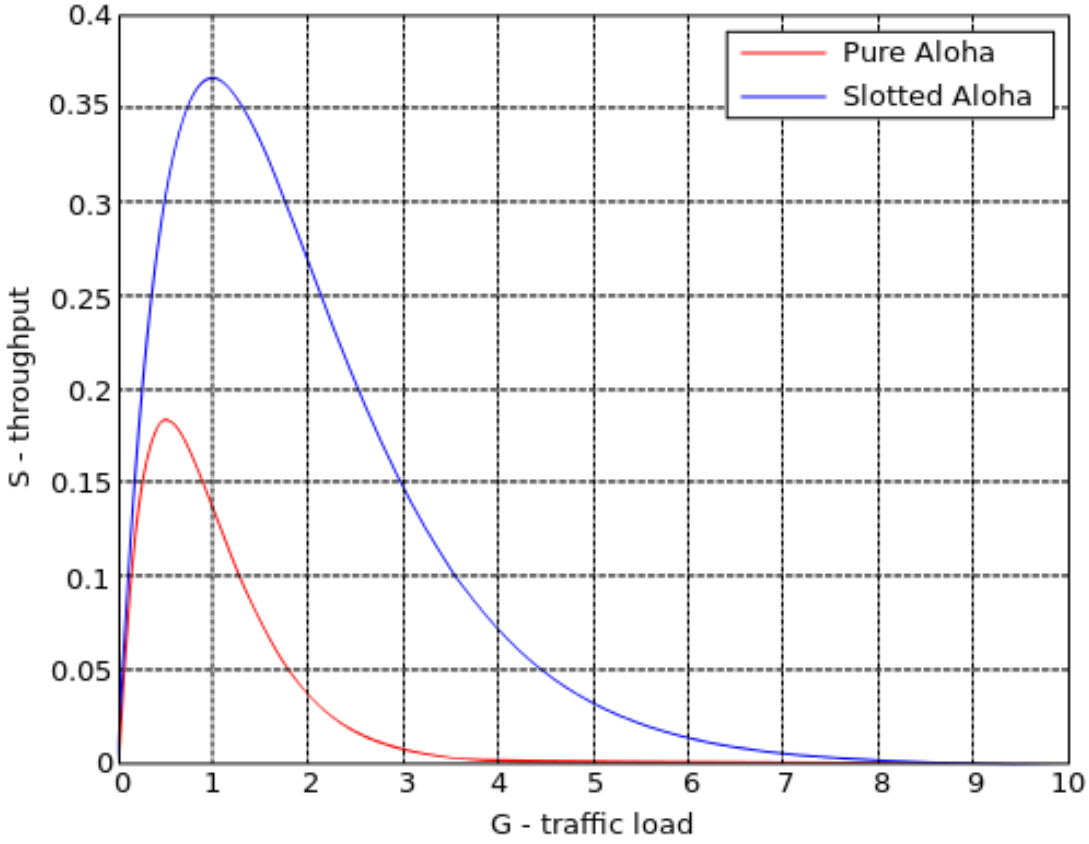


Image from Wikipedia

CSMA (Carrier Sense Multiple Access)

CSMA: listen before transmit:

- If channel sensed idle: transmit entire frame
- If channel sensed busy, defer transmission

- human analogy: don't interrupt others!

CSMA collisions

- collisions can still occur:

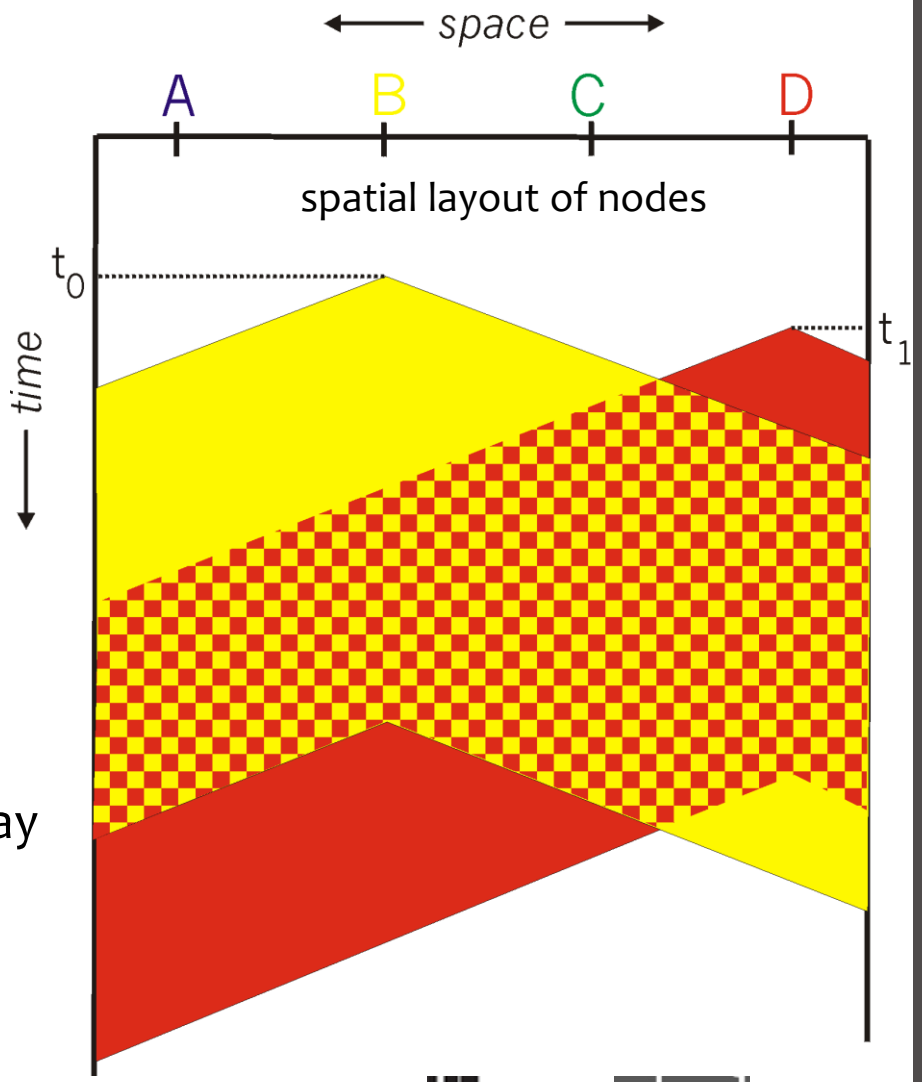
propagation delay means two nodes may not hear each other's transmission

- collision:

entire packet transmission time wasted

- note:

role of distance & propagation delay in determining collision probability



CSMA/CD (Collision Detection)

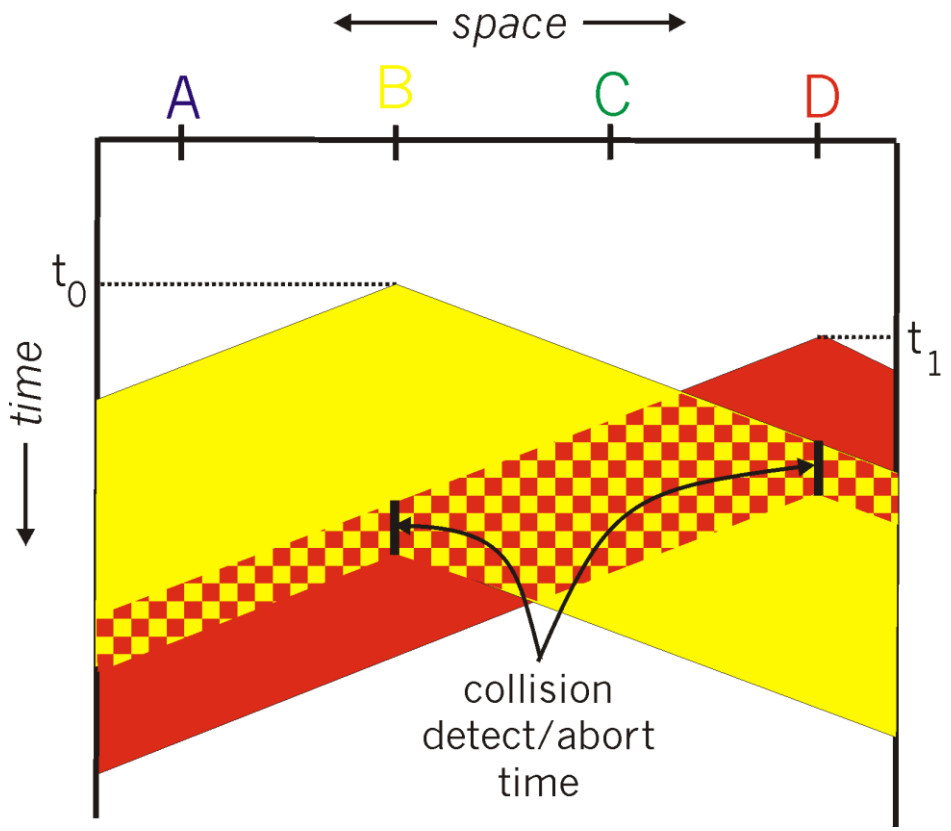
CSMA/CD: carrier sensing, deferral as in CSMA

- collisions *detected* within short time
- colliding transmissions aborted, reducing channel wastage

- collision detection:
  - easy in wired LANs: measure signal strengths, compare transmitted, received signals
  - difficult in wireless LANs: received signal strength overwhelmed by local transmission strength

- human analogy: the polite conversationalist

CSMA/CD collision detection



"Taking Turns" MAC protocols

channel partitioning MAC protocols:

- share channel *efficiently* and *fairly* at high load
- inefficient at low load: delay in channel access, 1/N bandwidth allocated even if only 1 active node!

Random access MAC protocols

- efficient at low load: single node can fully utilize channel
- high load: collision overhead

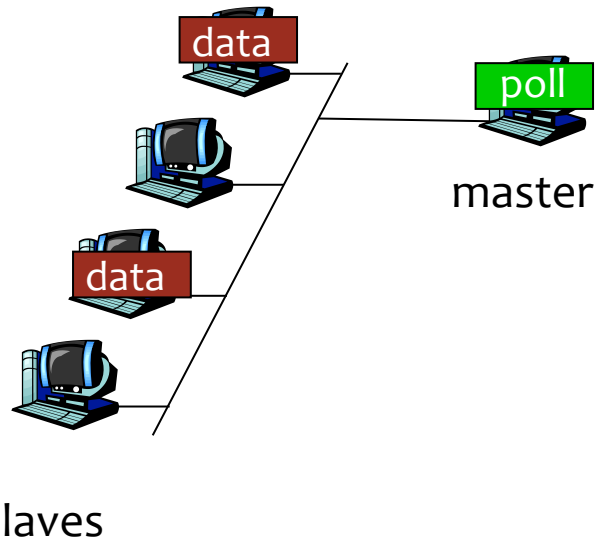
"taking turns" protocols

look for best of both worlds!

"Taking Turns" MAC protocols

Polling:

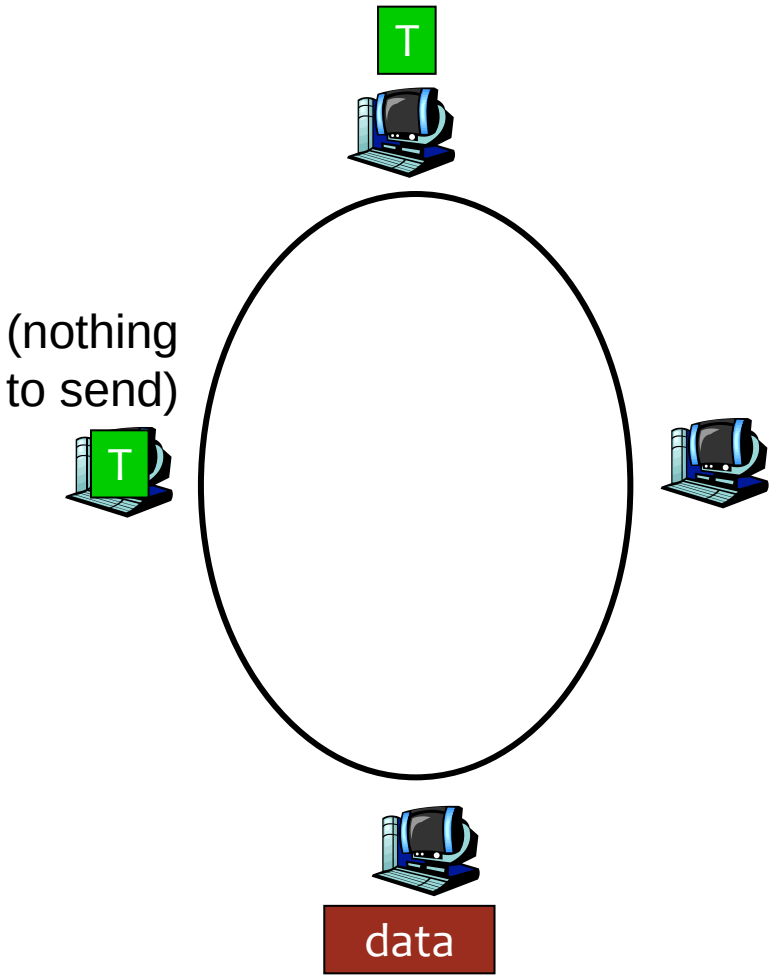
- master node "invites" slave nodes to transmit in turn
- typically used with "dumb" slave devices
- concerns:
  - polling overhead
  - latency
  - single point of failure (master)



"Taking Turns" MAC protocols

Token passing:

- control **token** passed from one node to next sequentially.
- token message
- concerns:
  - token overhead
  - latency
  - single point of failure (token)

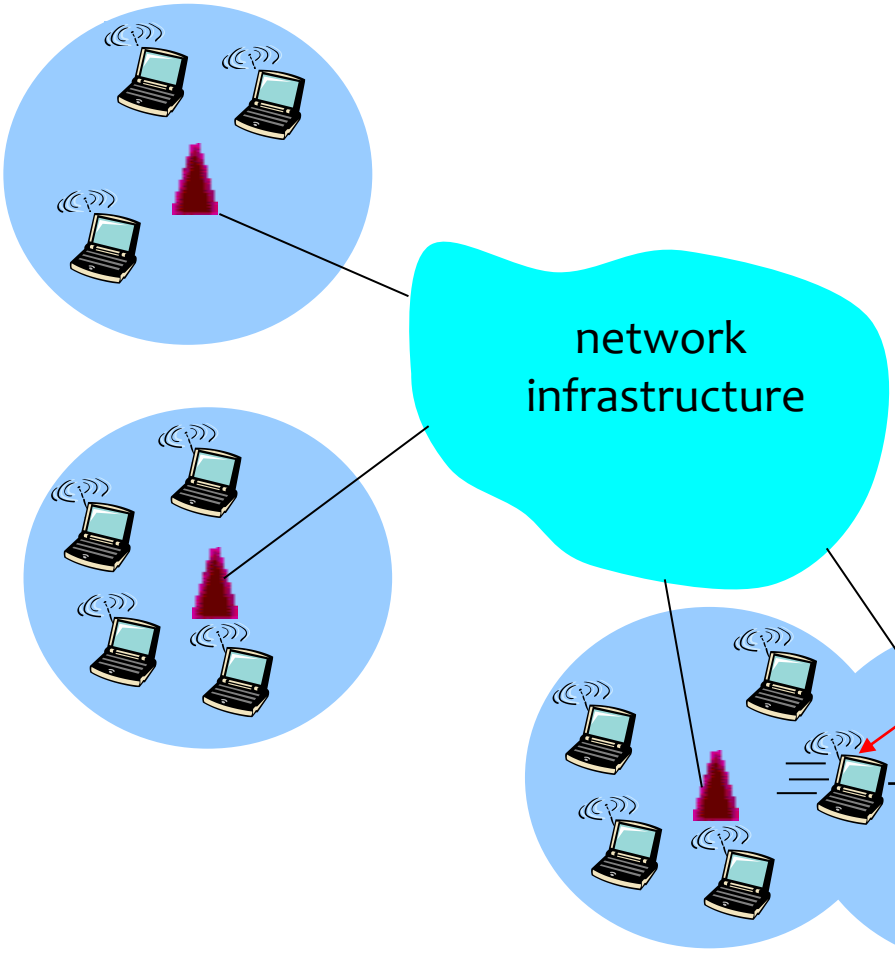


Summary of MAC protocols

- *channel partitioning,* by time, frequency or code
  - Time Division, Frequency Division
- *random access* (dynamic),
  - ALOHA, S-ALOHA, CSMA, CSMA/CD
  - carrier sensing: easy in some technologies (wire), hard in others (wireless)
  - CSMA/CD used in Ethernet
  - CSMA/CA used in 802.11
- *taking turns*
  - polling from central site, token passing
  - Bluetooth, FDDI, IBM Token Ring

Wireless

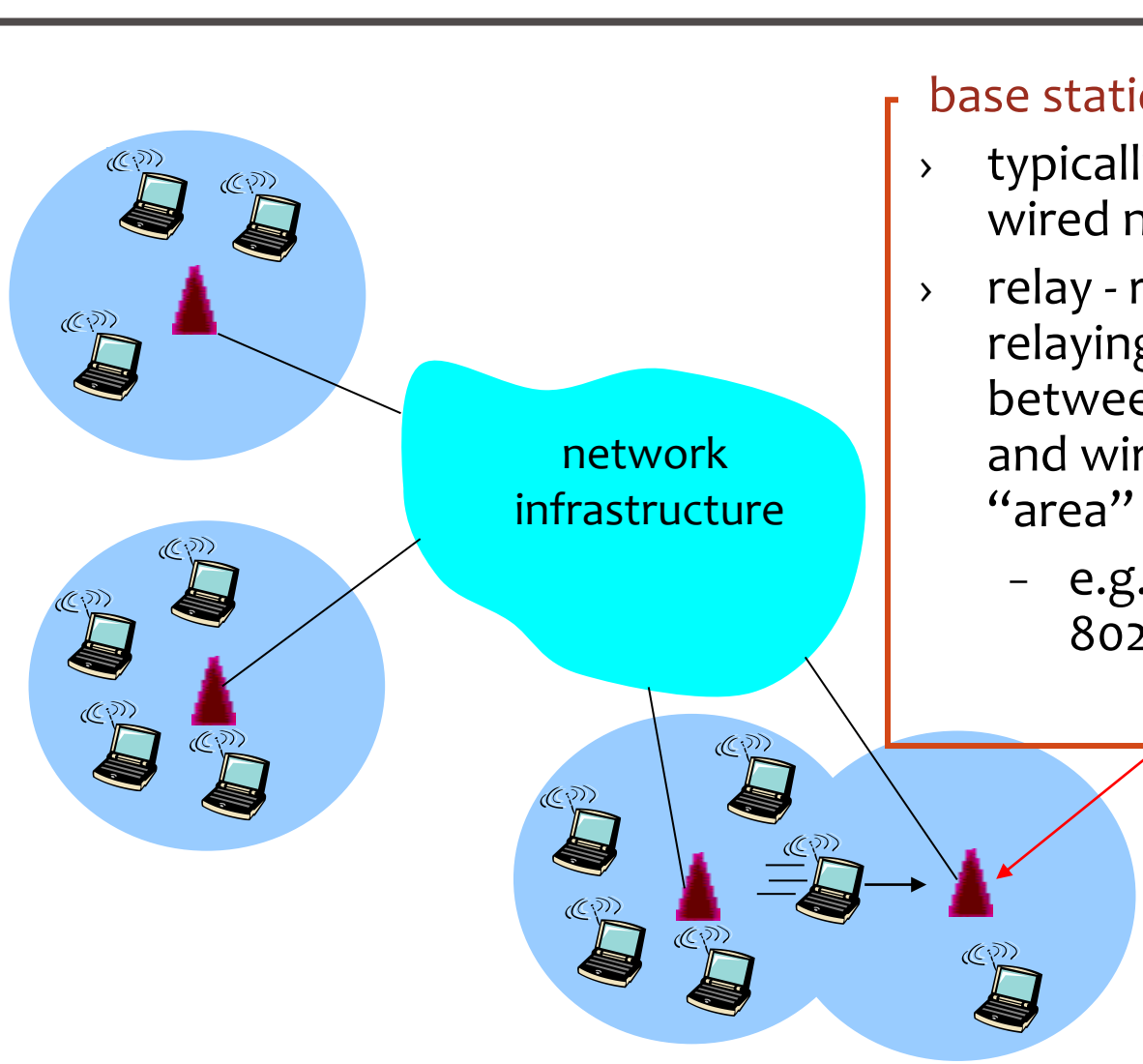
Elements of a wireless network



wireless hosts

- laptop, smartphone, …
- run applications
- may be stationary or mobile
  - wireless does *not* always mean mobility

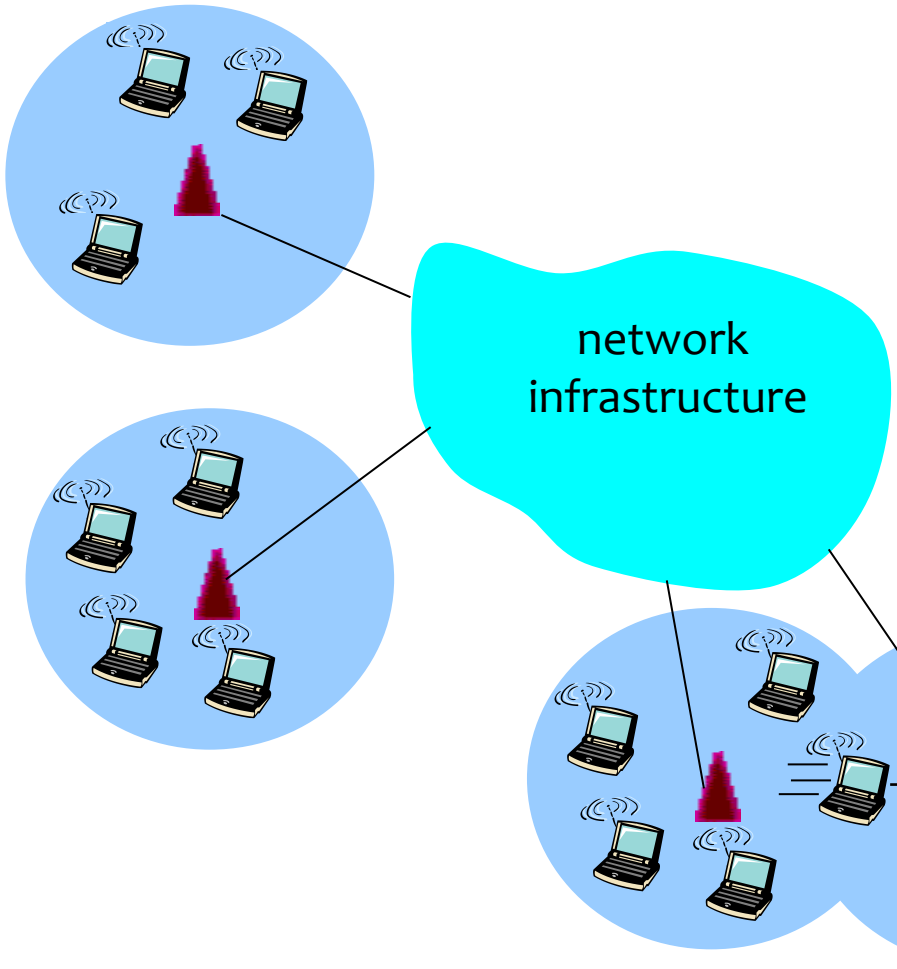
Elements of a wireless network



base station

- typically connected to wired network
- relay - responsible for relaying packets between wired network and wireless host(s) in its "area"
  - e.g., cell towers, 802.11 access points

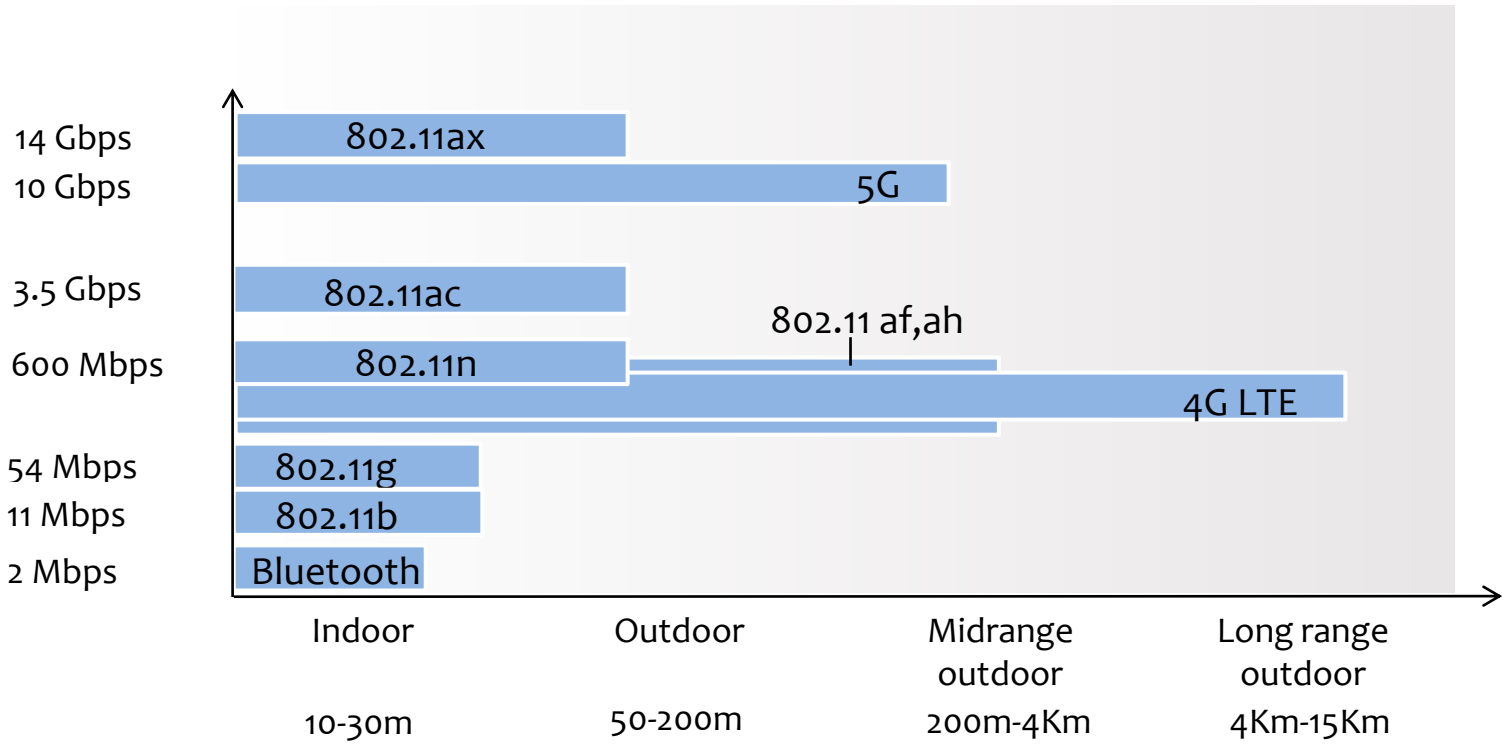
Elements of a wireless network



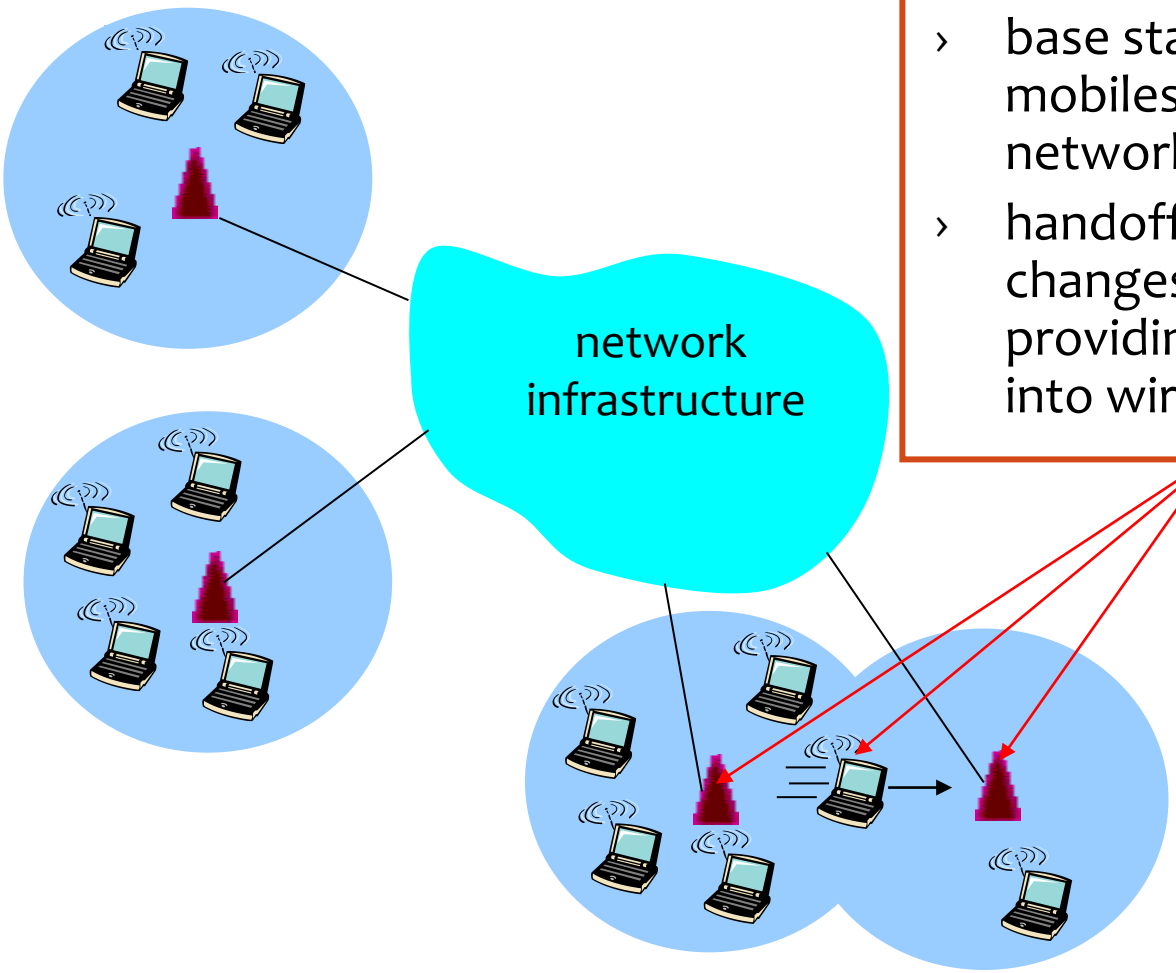
wireless link

- typically used to connect mobile(s) to base station
- also used as backbone link
- link access coordinated by a multiple access protocol
- various data rates, transmission distance

Characteristics of selected wireless link standards



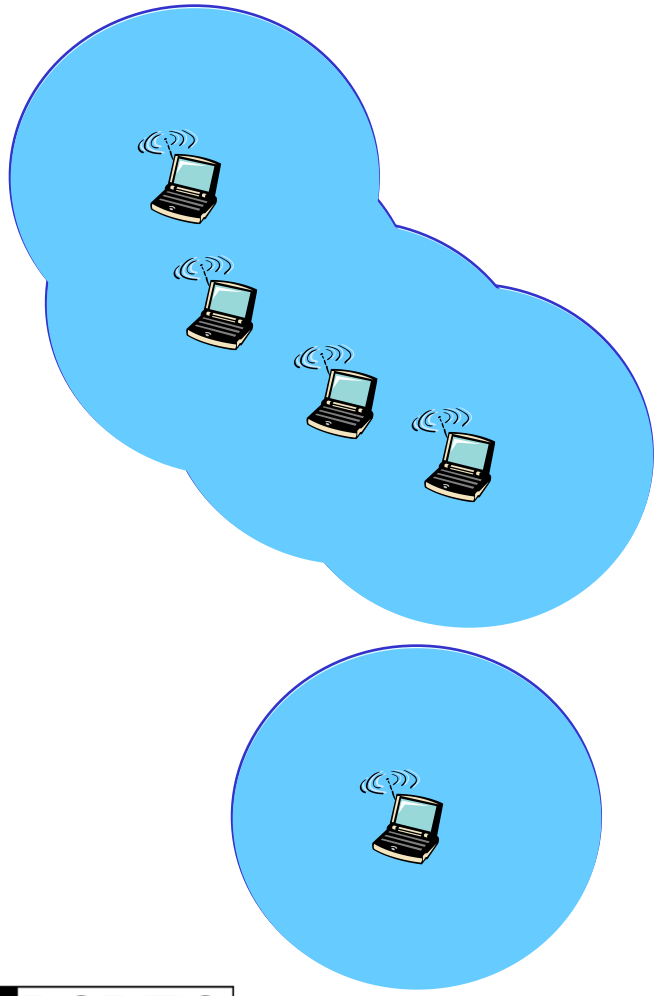
Modes of operation



infrastructure mode

- base station connects mobiles into wired network
- handoff: mobile changes base station providing connection into wired network

Modes of operation



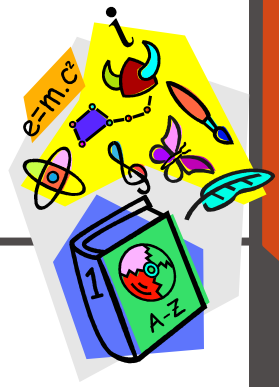
ad hoc mode

- no base stations
- nodes can only transmit to other nodes within link coverage
- nodes organize themselves into a network: route among themselves
- requires all nodes in range of each other or an ad hoc routing protocol

Wireless network taxonomy

	single hop	multiple hops
infrastructure (e.g., APs)	host connects to base station (WiFi, WiMAX, cellular), which connects to larger Internet	host may have to relay through several wireless nodes to connect to larger Internet: *mesh network*
no infrastructure	no base station, no connection to larger Internet (Bluetooth, ad hoc nets)	no base station, no connection to larger Internet. May have to relay to reach other wireless nodes MANET, VANET, …

802.11 Concepts & Terminology

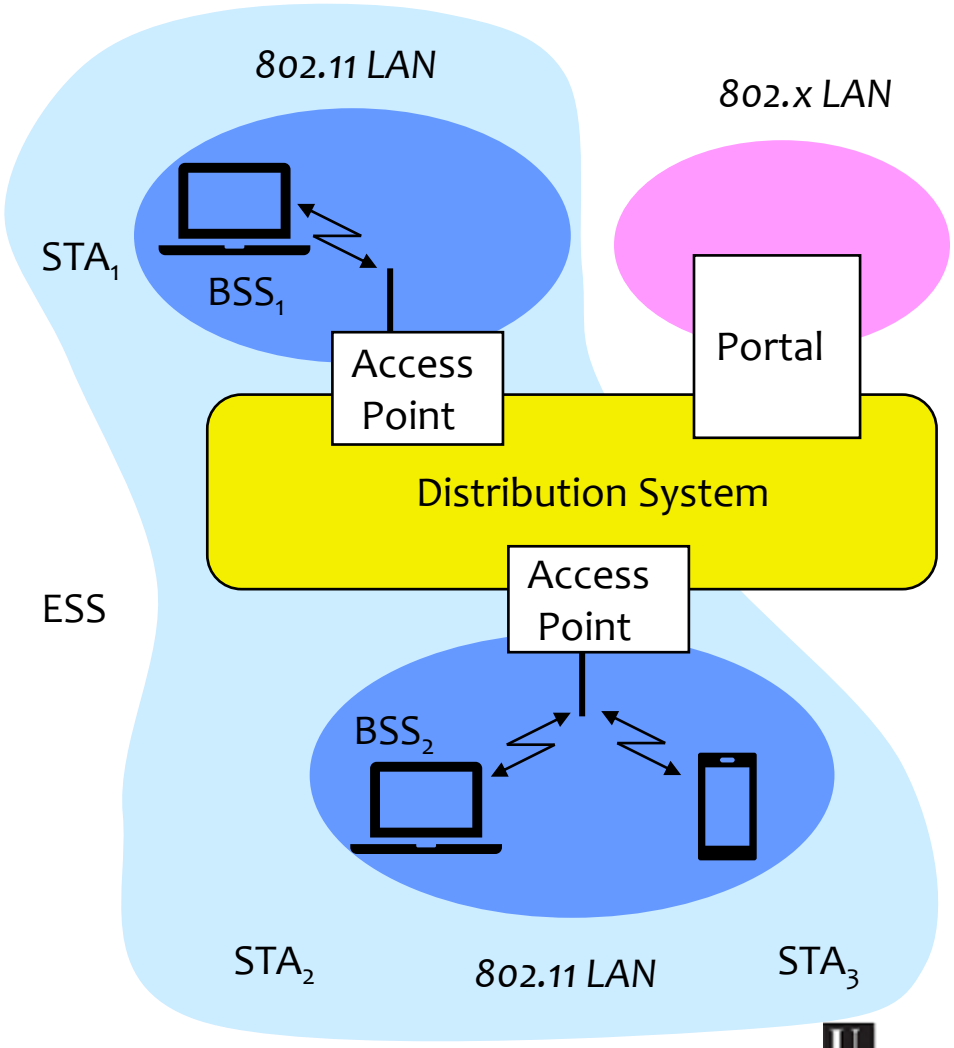


- Station (STA)
  - The mobile terminal
- Access Point (AP)
  - STAs connect to APs on infrastructure networks
- Basic Service Set (BSS)
  - STAs and AP on the same covered cell, using the same frequency
  - If no distribution system exists, then it is independent (IBSS)
- Extended Service Set
  - BSSs with APs interconnected through a distribution system

802.11 Concepts & Terminology

- Distribution system
  - Interconnection of several BSSs to form an ESS
- Portal
  - Bridge to access other networks (e.g., *ethernet*)
- Service Set Identifier (SSID)
  - Network name (32 bytes)
  - One per ESS (or IBSS)
- Basic Service Set Identifier (BSSID)
  - Cell identifiers (6 bytes)
  - MAC address of AP

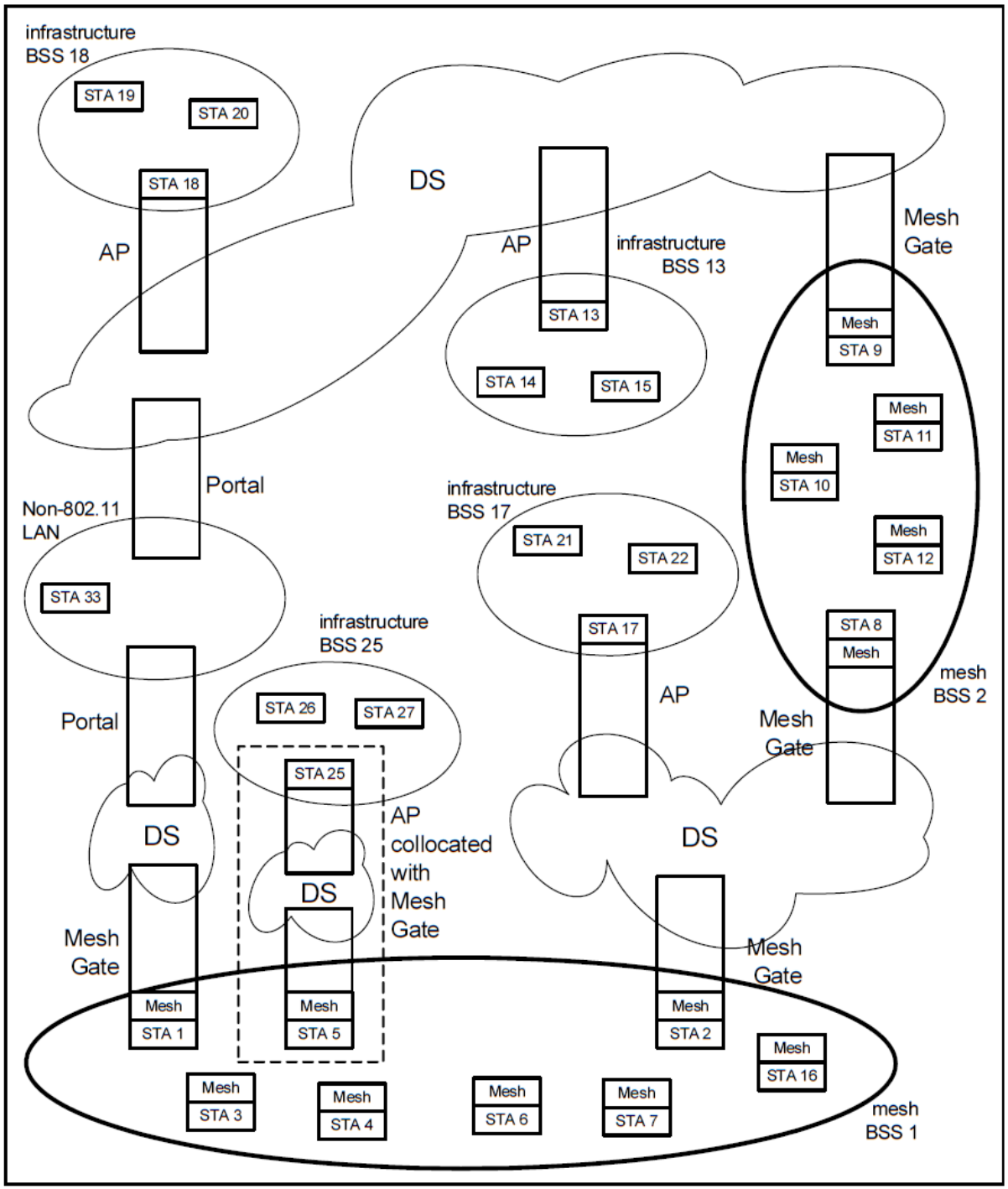
Infrastructure– Components



Adapted from:
IEEE 802.11 MAC,
Sridhar Iyer

Example MBSS containing mesh STAs, mesh gates, APs, and portals

From IEEE 802.11-2012, page 63



U.PORTO

Digital Modulation

- Data transmission over radio waves requires *modulating* (changing properties of) a wave
  - Amplitude
  - Frequency
  - Phase

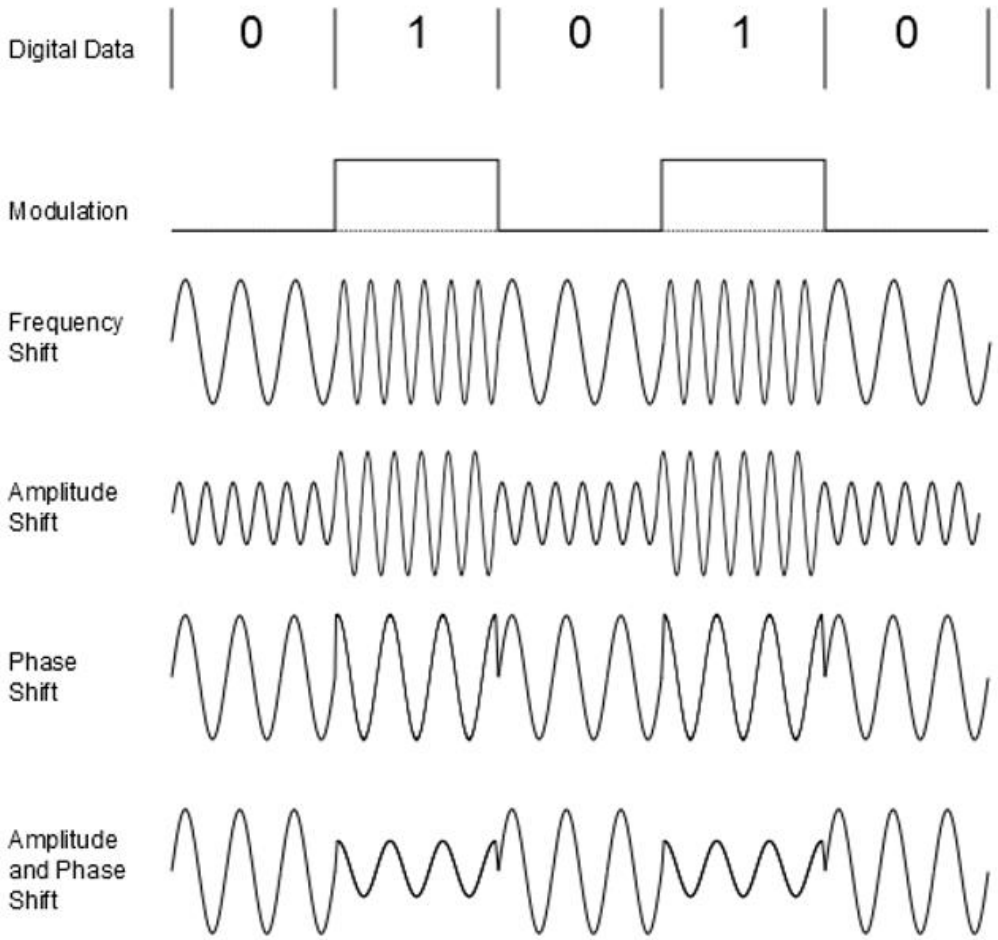
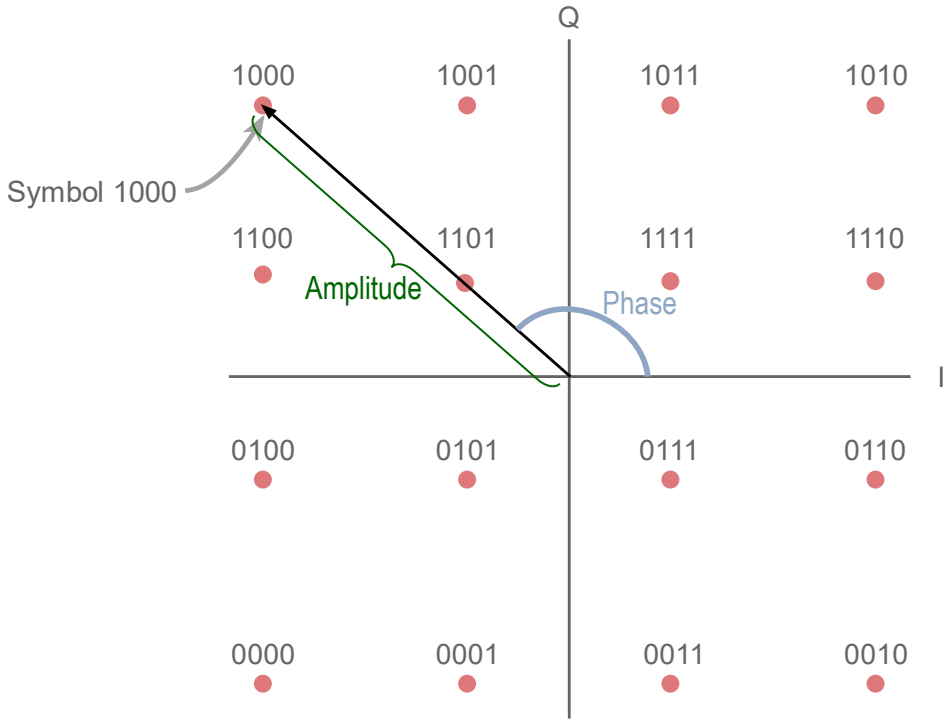


Image from:
Spectrum and Network Measurements (2nd Ed.), Robert A. Witte, Chap. 6, SciTech Publishing, 2014.

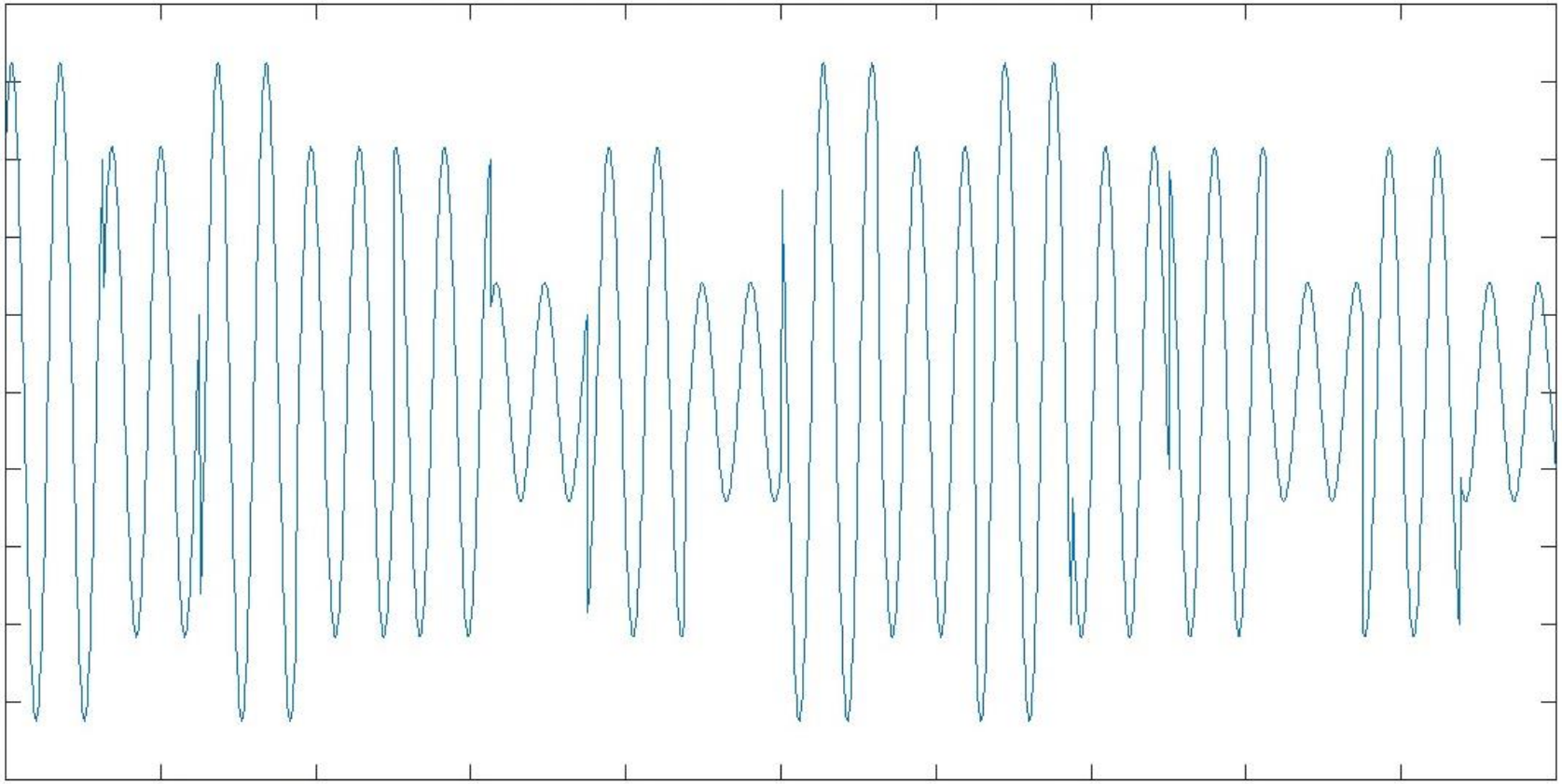
Quadrature Amplitude Modulation

- Change amplitude and phase to send a symbol
- Multiple bits per transmitted symbol
  - $\log_2(n)$ bits per symbol with a constellation of size n



Example: QAM16

Example 16-QAM signal



Wireless Link Characteristics (1)

Differences from wired link ….

- decreased signal strength: radio signal attenuates as it propagates (path loss)
  - even in free space, decreases with the distance squared
- interference from other sources: standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well
- multipath propagation: radio signal reflects off objects, ground, arriving at destination at slightly different times

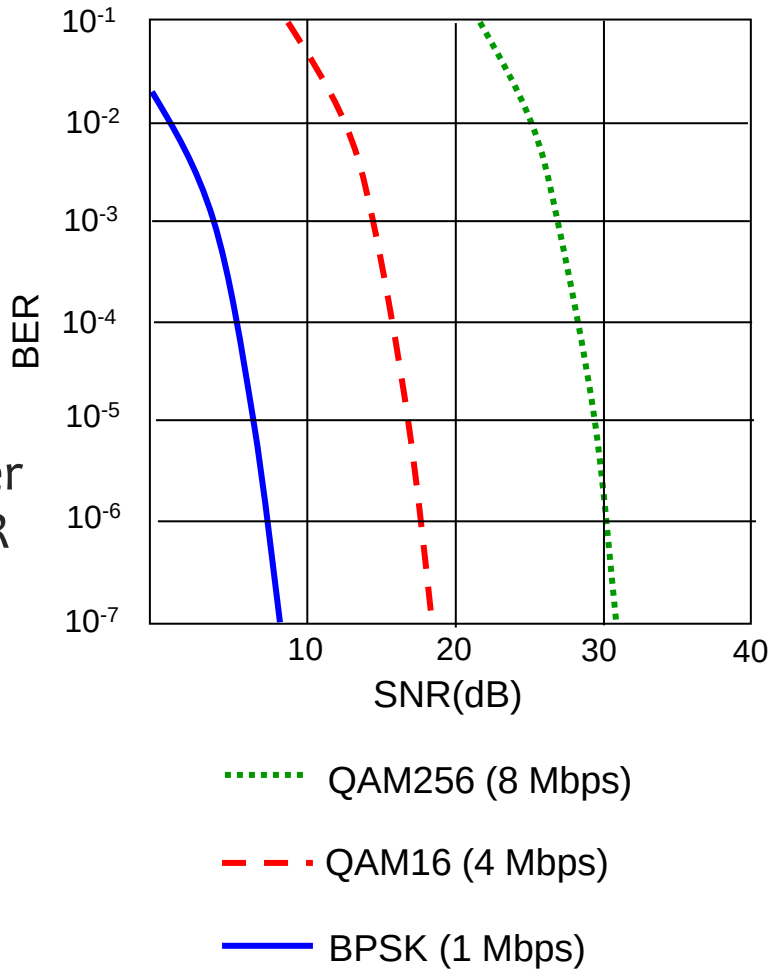
…. make communication (even point-to-point) across wireless links much more "difficult"

Wireless Link Characteristics (2)

- Max. theoretical capacity

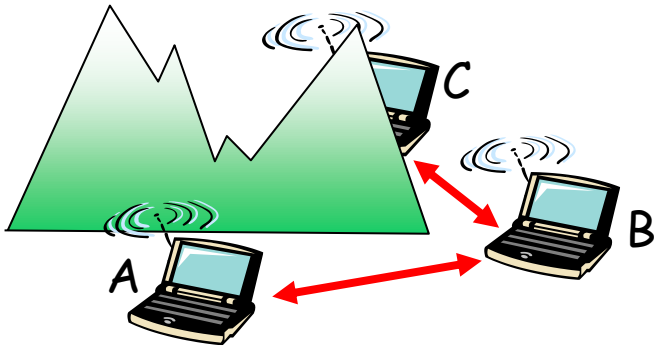
$$C = B_c \cdot \log_2\left(1 + \frac{P_r}{N}\right)$$

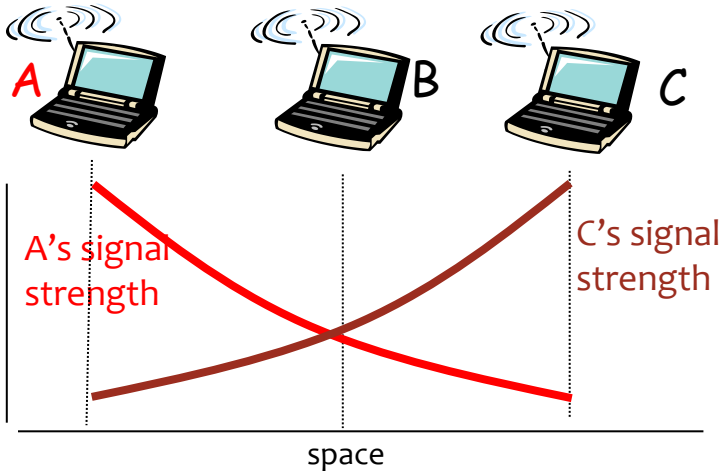
- SNR: signal-to-noise ratio
  - larger SNR – easier to extract signal from noise (good)
- *SNR versus BER tradeoffs*
  - *given modulation:* increase power → increase SNR → decrease BER (bit error rate)
  - *given SNR:* choose modulation that meets BER requirement, giving highest throughput
    - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)



Wireless network characteristics

Multiple wireless senders and receivers create additional problems (beyond multiple access):





Hidden terminal problem

- B, A hear each other
- B, C hear each other
- A, C can not hear each other

means A, C unaware of their interference at B

Signal attenuation:

- B, A hear each other
- B, C hear each other
- A, C can not hear each other interfering at B

Outline

Introduction

Wireless

- Wireless links, characteristics
  - CDMA
- IEEE 802.11 wireless LANs (“wi-fi”)

IEEE 802.11 Wireless LAN

802.11b
- 2.4 GHz
- up to 11 Mbps
- DSSS in physical layer

802.11a
- 5 GHz
- up to 54 Mbps
- OFDM in physical layer

802.11g
- 2.4 GHz
- up to 54 Mbps

802.11n (Wi-Fi 4)
- 2.4 GHz
- MIMO (multiple antennae)
- up to 600 Mbps

802.11ac (Wi-Fi 5)
- 5 GHz
- up to 7 Gbps
- MU-MIMO (downlink only)

802.11ax (Wi-Fi 6/6E)
- 2.4, 5, 6 GHz
- up to 9.6 Gbps
- MU-MIMO
- OFDMA (optional)

upcoming: 802.11be (Wi-Fi 7)
- 2.4, 5, 6 GHz
- up to 46 Gbps
- MLO
- Preamble puncturing

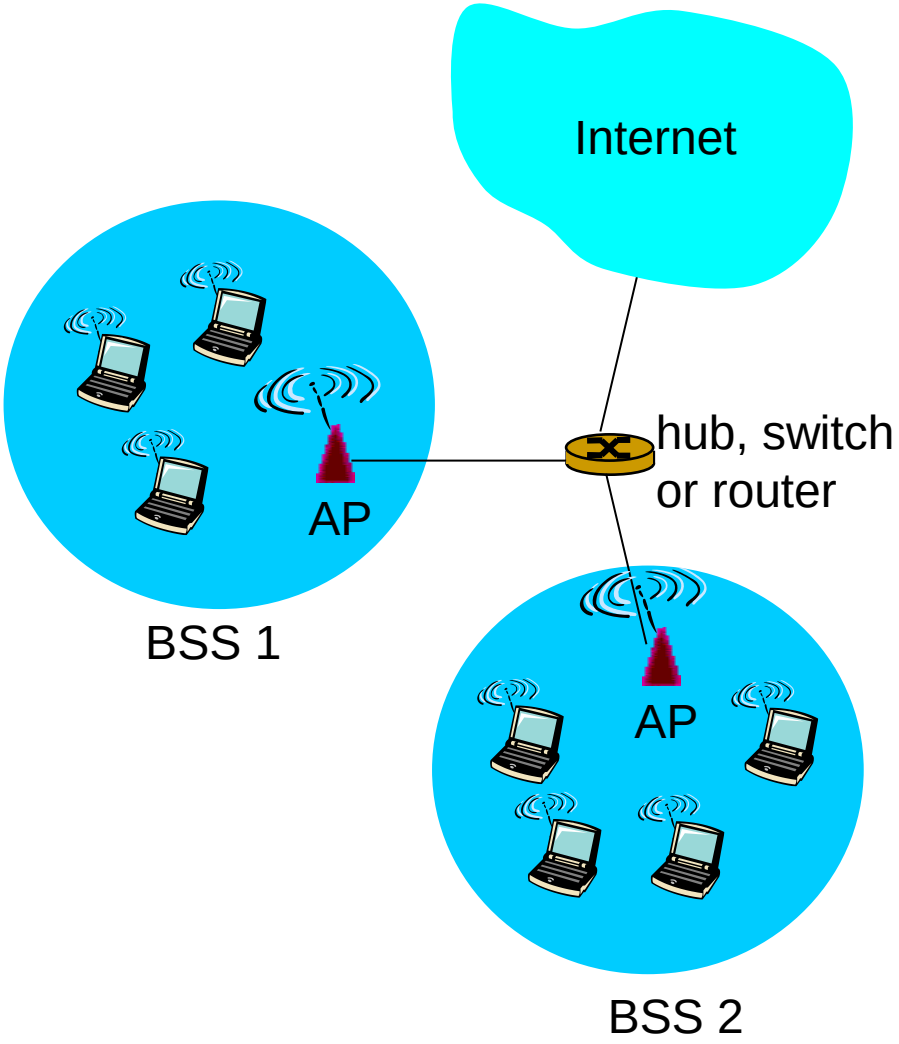
- different physical layers
- all use CSMA/CA for multiple access
- all have infrastructure and ad-hoc network versions

IEEE 802.11 Wireless LAN (others)

- 802.11s
  - Mesh networks
- 802.11p
  - wireless access in vehicular environments (WAVE)
- 802.11e
  - Medium Access Control (MAC) Quality of Service Enhancements
- 802.11r
  - Fast Basic Service Set (BSS) Transition (handoff)
- 802.11i and 802.11w
  - Security enhancements

All incorporated in 802.11-2012

802.11 LAN architecture

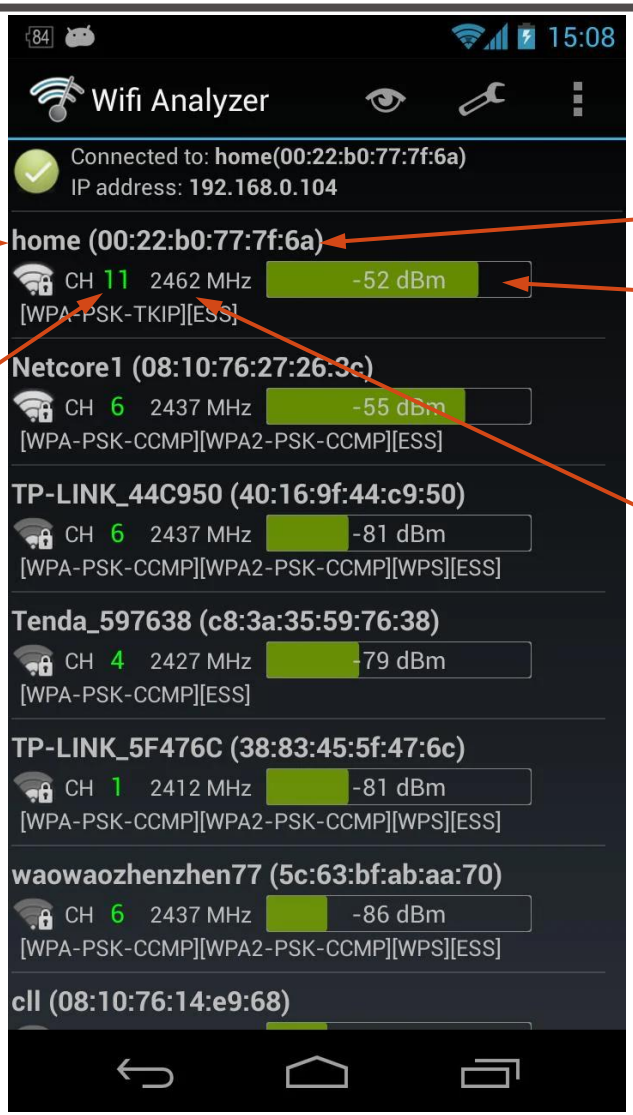


- wireless hosts communicate through an access point (AP)
  - access point = base station
- Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc (IBSS) mode: hosts only

802.11: Channels, association

- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 to 14 channels at different frequencies
  - AP admin chooses frequency for AP
  - interference possible if channel is the same as that chosen by neighboring AP!
- station (host): must *associate* with an AP
  - scans channels, listening for *beacon frames* containing network name (SSID) and AP MAC address
  - selects AP to associate with
  - may perform authentication
  - will typically run DHCP to get IP address in AP's subnet

802.11 Channels, association



(E)SSID (network name)

BSSID (AP's MAC address)

RSSI (Received Signal Strength Indicator)

Channel

Channel frequency

Image source: Google Play store

802.11 b Channels

- Some countries restrict use of some channels; others (Japan) added another channel
  - Defined "regulatory domain" used to limit available channels

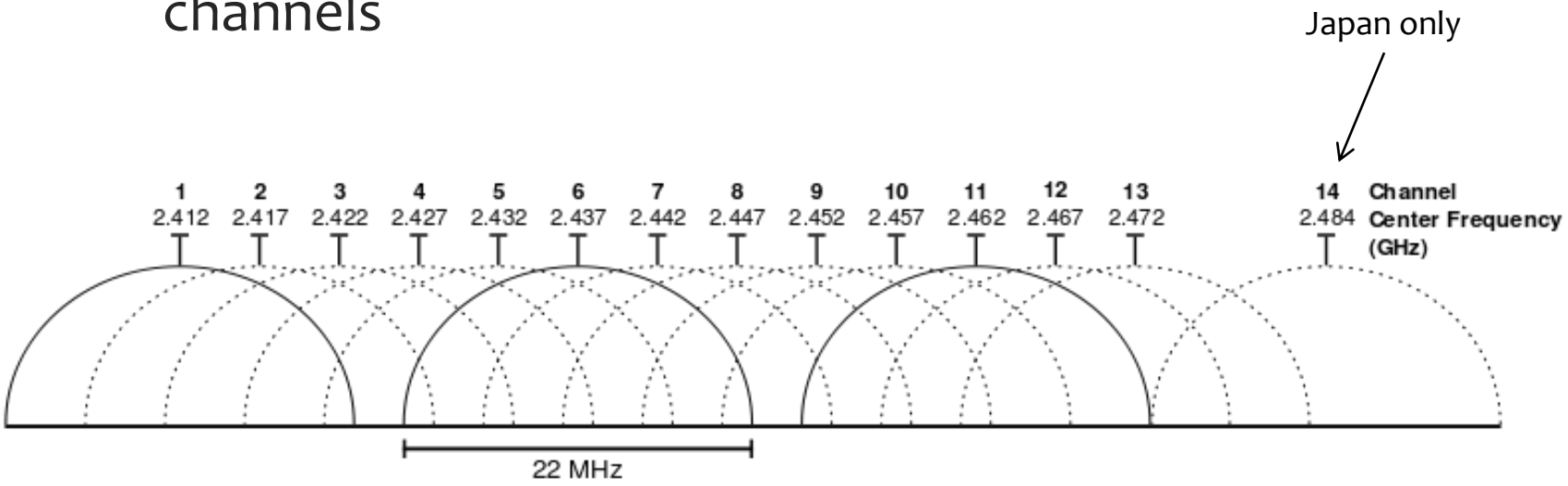
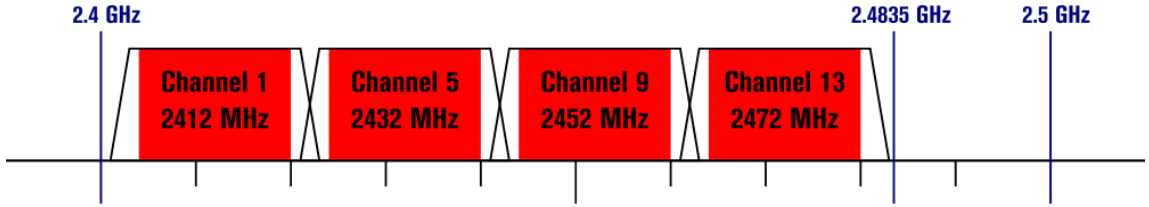


Image from Wikipedia

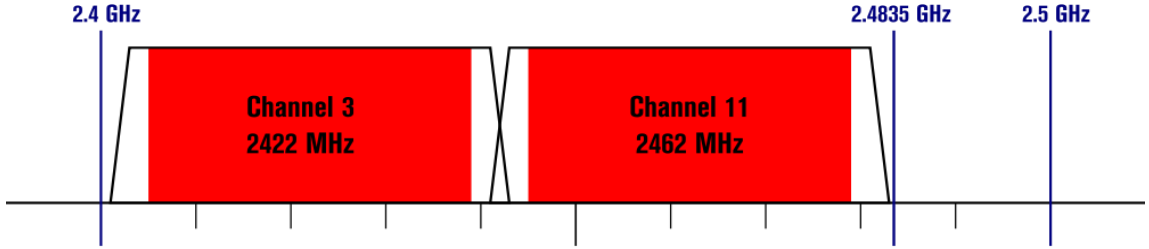
802.11 g/n/ac Channels

802.11g/n (OFDM) 20 MHz ch. width – 16.25 MHz used by sub-carriers

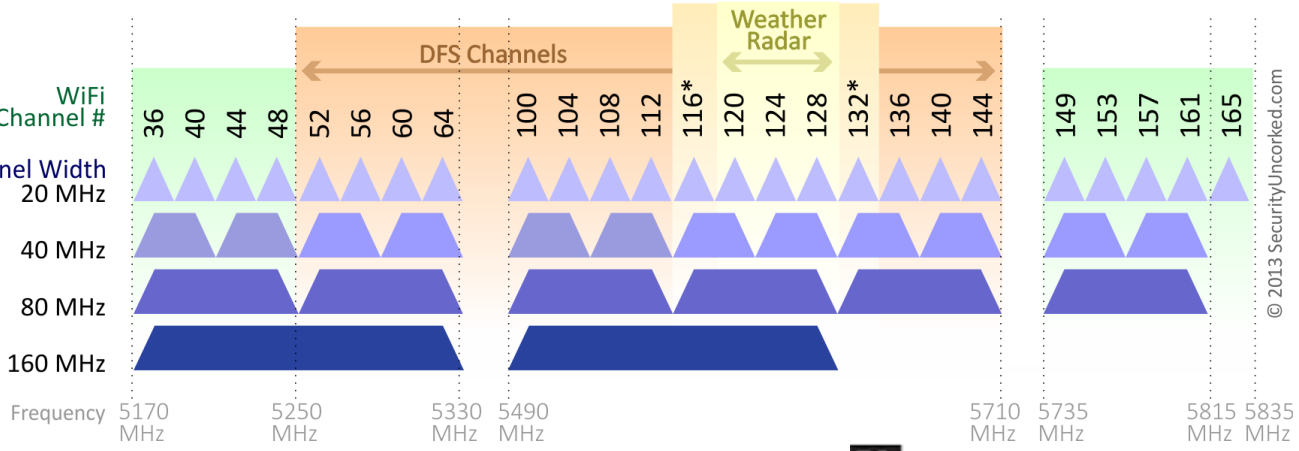
Wikipedia



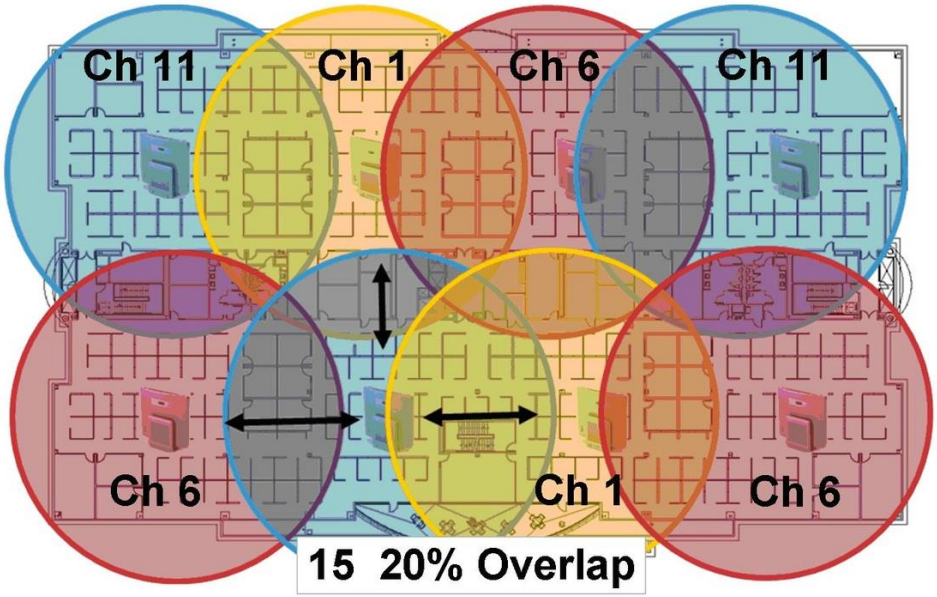
802.11n (OFDM) 40 MHz ch. width – 33.75 MHz used by sub-carriers



802.11ac (5GHz)

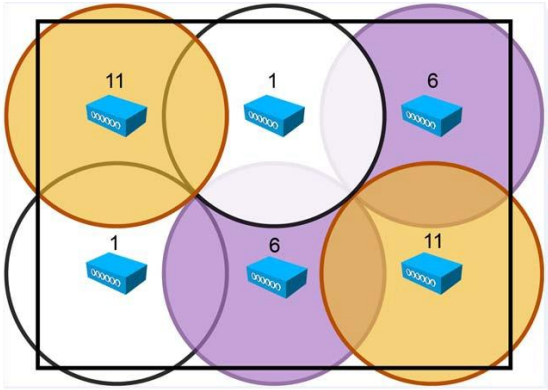


Channel planning

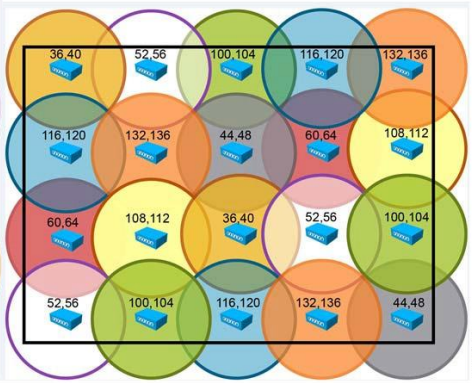


Placing access points and assigning channels so that coverage is maximized and interference minimized

Easier in the 5GHz band where range is shorter and more channels are available

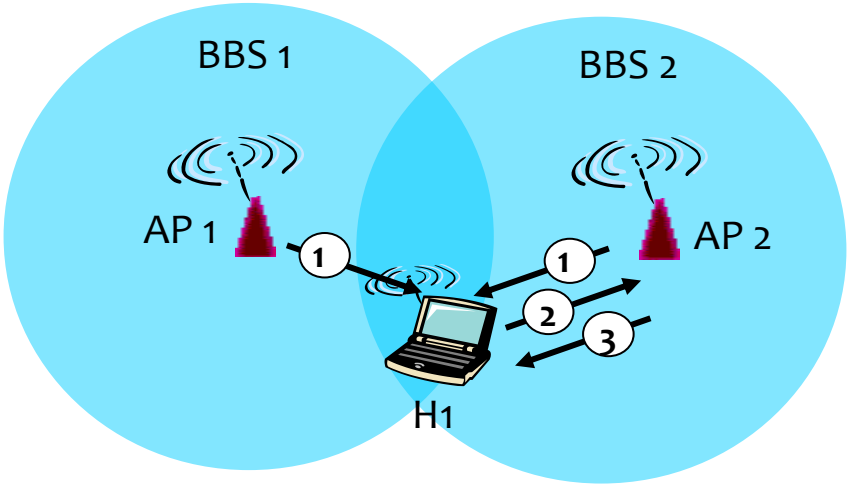


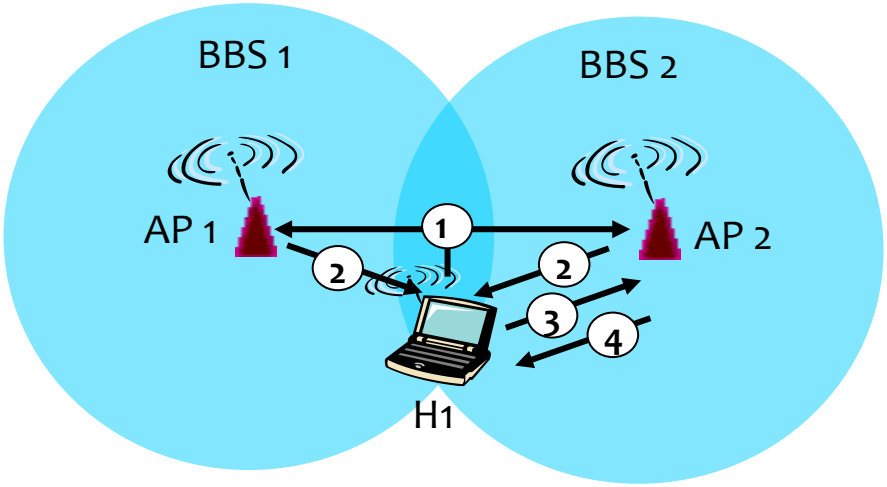
2.4GHz



5GHz

802.11: passive/active scanning





Passive Scanning:

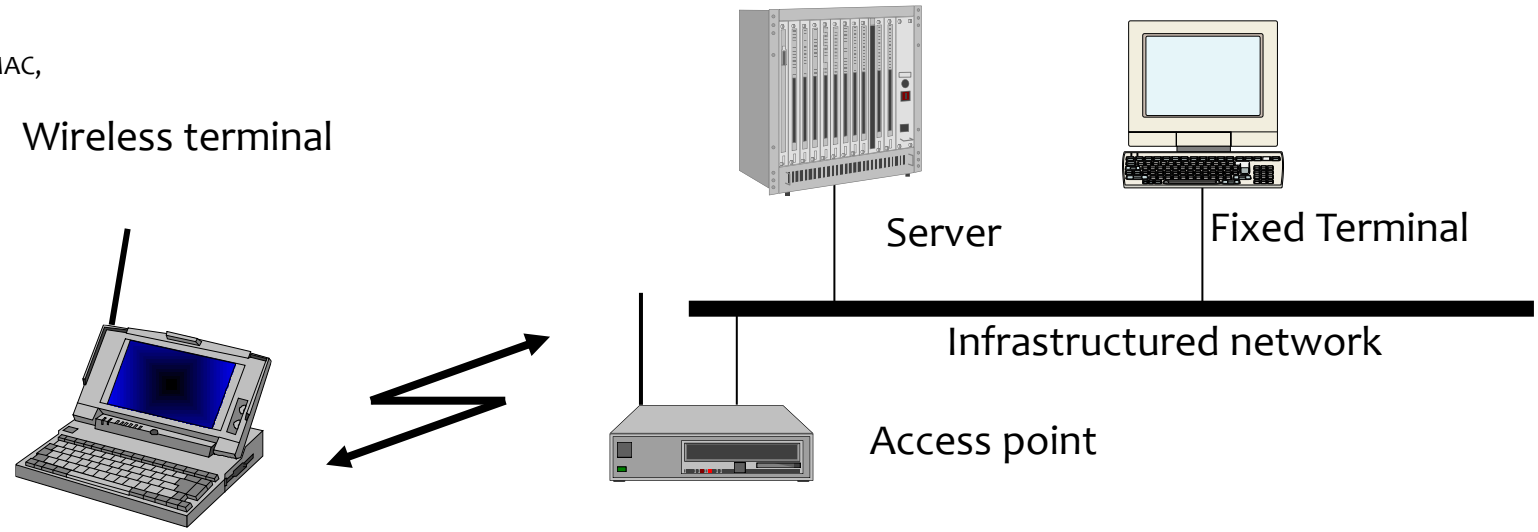
(1) beacon frames sent from APs
(2) association Request frame sent: H1 to selected AP
(3) association Response frame sent: selected AP to H1

Active Scanning:

(1) Probe Request frame broadcast from H1
(2) Probe response frames sent from APs
(3) Association Request frame sent: H1 to selected AP
(4) Association Response frame sent: selected AP to H1

802.11 and TCP/IP stack

Source:
IEEE 802.11 MAC,
Sridhar Iyer

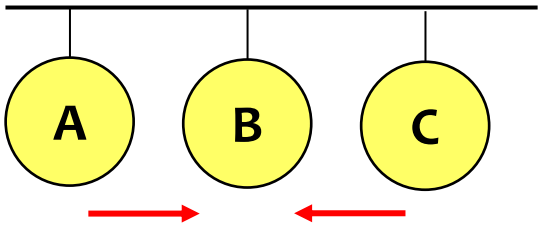


	Application		Application
	TCP		TCP
	IP		IP
Link Layer	802.2 LLC	LLC	LLC
	802.11 MAC	802.11 MAC / 802.3 MAC	802.3 MAC
	802.11 PHY	802.11 PHY / 802.3 PHY	802.3 PHY

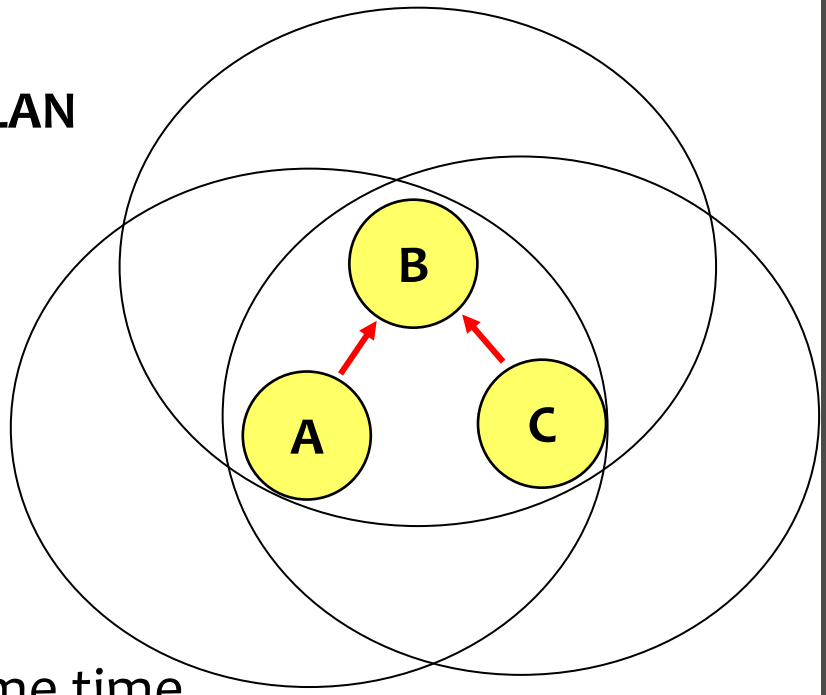
Ethernet vs. Wireless

Source:
IEEE 802.11 MAC,
Sridhar Iyer

Ethernet LAN



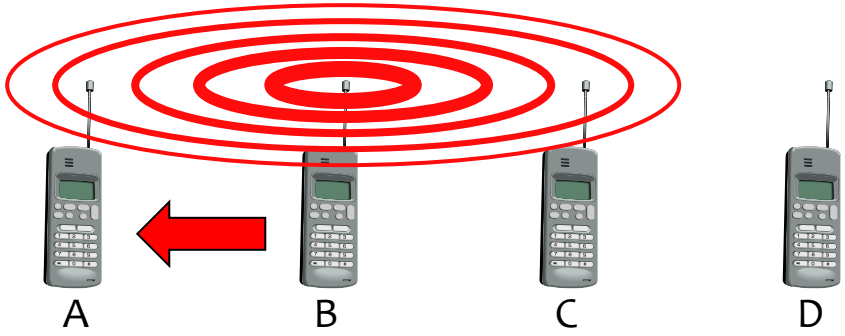
Wireless LAN



- A and C see free channel at same time
  - Transmit at the same time
- Ethernet: source can detect collision
- Wireless: half-duplex radios can't detect collision
  - Besides the hidden terminal problem

Exposed node problem

Source:
Wireless LAN – IEEE 802.11



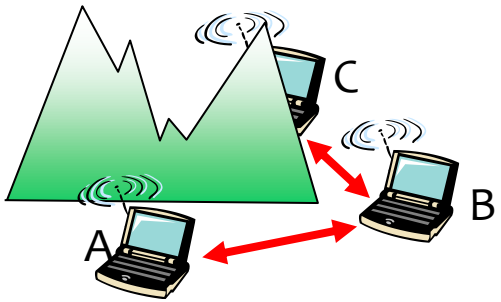
- B transmits to A
- C wants to transmit to D
- D is out of reach of B and A is out of reach of C
  - The transmission could be simultaneous
- But C senses medium busy
  - Does not transmit

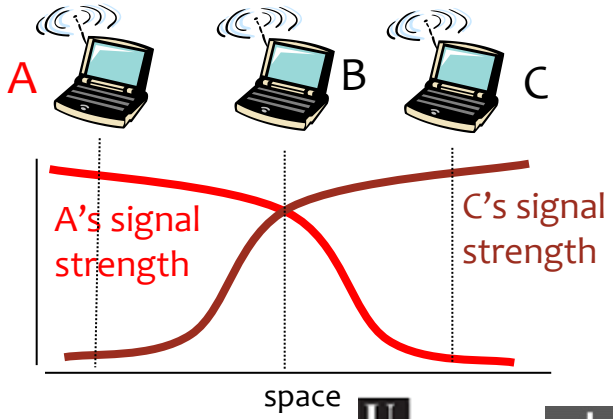
The need for a wireless MAC

- Shared medium cabled nets
  - Typically CSMA/CD
    - Free medium → STA transmits
    - Continue listening to detect collisions
- Wireless nets
  - Power diminishes with the square of the distance
  - Even if senders could use CD, collisions occur at receivers
    - Source may not "hear" collision (CD won't work)
    - CS may not work (hidden node problem)
    - CS may work "too much" (exposed node problem)

IEEE 802.11: multiple access

- avoid collisions (2+ nodes transmitting at same time)
- CSMA - sense medium before transmitting
  - don't collide with ongoing transmission by other node
- *no* collision detection!
  - extremely difficult to receive (sense collisions) when transmitting due to weak received signals
  - can't sense all collisions in any case: hidden terminal, fading
  - goal: *avoid collisions:* CSMA/C(ollision)A(voidance)



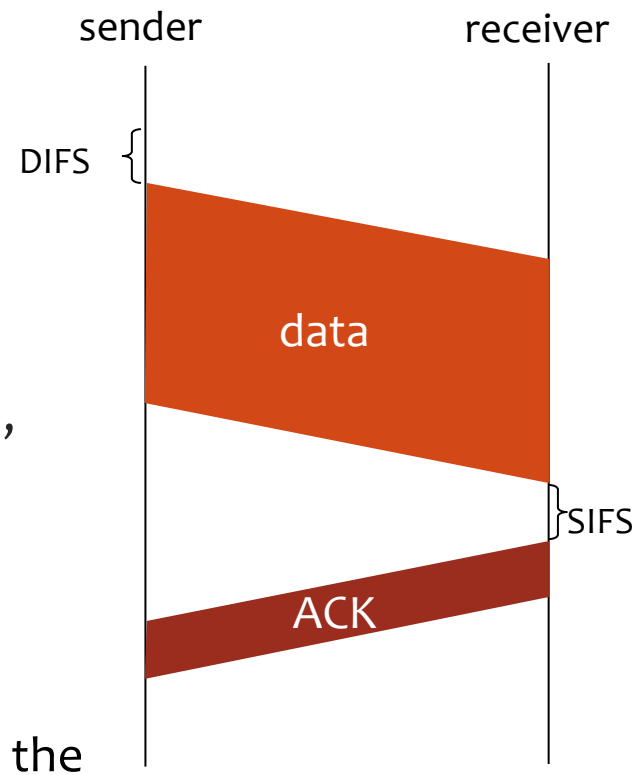


IEEE 802.11 MAC Protocol: CSMA/CA

802.11 sender

1) if sense channel idle for **DIFS** then
   transmit entire frame (no CD)

2) if sense channel busy then
   start random backoff time
   timer counts down while channel idle
   transmit when timer expires
   if no ACK, increase random back off interval, repeat 2



802.11 receiver

- if frame received OK

return ACK after **SIFS** (ACK necessary due to the hidden terminal problem)

Avoiding collisions (enhancement)

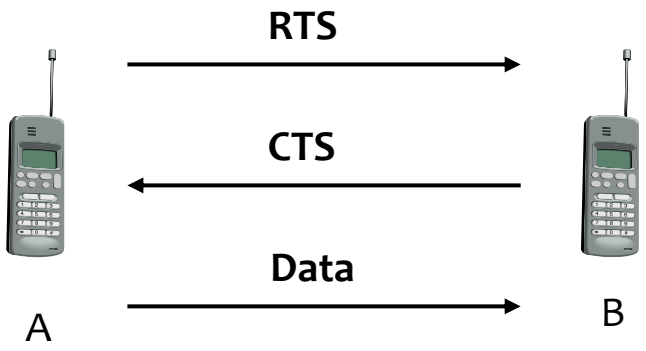
- idea: allow sender to "reserve" channel, rather than random access of data frames
  - avoid collisions of long data frames
- sender first transmits small request-to-send (RTS) packets to AP using CSMA
  - RTSs may still collide with each other, but they're short
- AP broadcasts clear-to-send (CTS) in response to RTS
- CTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions

avoid data frame collisions completely
using small reservation packets!

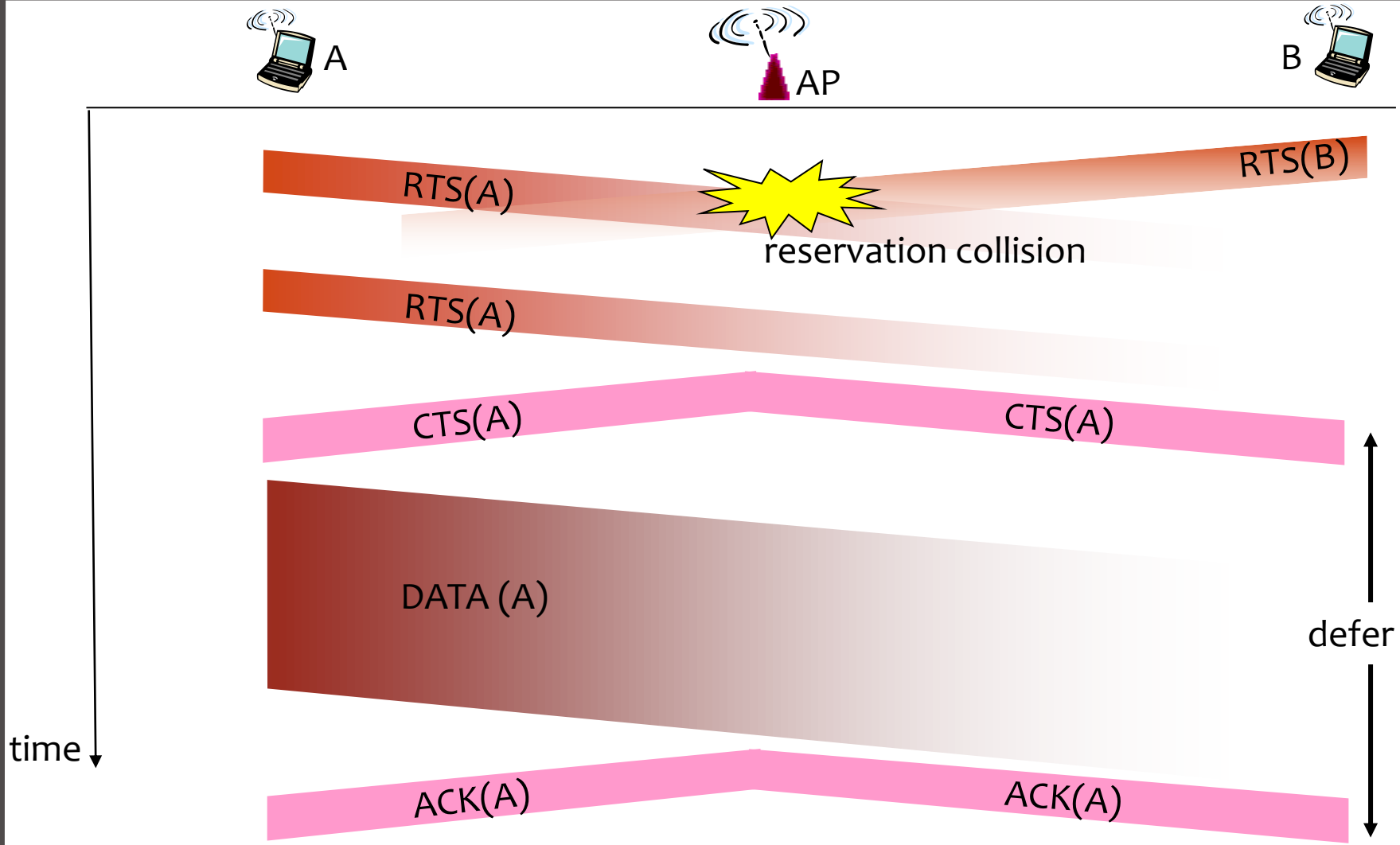
Multiple Access with Collision Avoidance (MACA)

- Prevents collisions using signaling packets before data
  - RTS (Request To Send)
  - CTS (Clear To Send)
- Signaling Packets contain:
  - Source address
  - Destination address
  - Estimated duration of transmission

Source:
Wireless LAN – IEEE 802.11

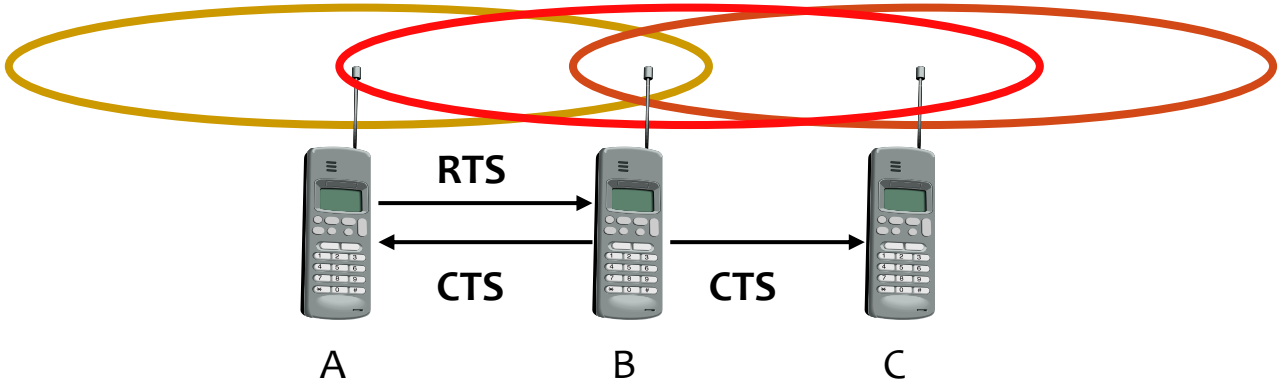


Collision Avoidance: RTS-CTS exchange



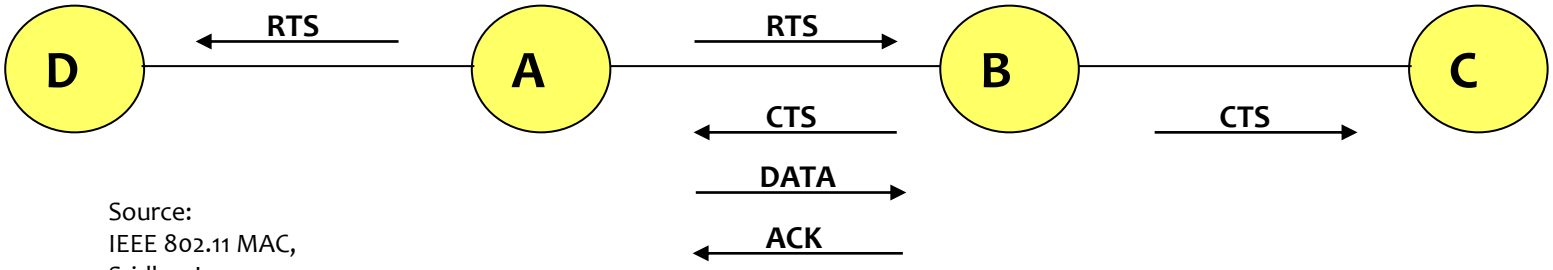
MACA solves hidden node problem

- A and C want to transmit to B
- A sends RTS first
- C hears CTS and waits



MAC: Reliability

- Wireless prone to errors
- Solution: use ACKs
  - B receives data from A and sends ACK
  - If A does not receive ACK, retransmits
  - C does not transmit until end of ACK
  - RTS and CTS have estimated duration of transmission (including ACK)



Source:
IEEE 802.11 MAC,
Sridhar Iyer

MAC: Avoiding collisions

- Half-duplex radios cannot detect collisions
  - Even if they could, collisions occur at receiver
- "Collision avoidance"
  - If channel is free, wait random time before trying to reserve it with RTS (or grabbing it with a data frame transmission)
- Distributed Coordination Function (DCF)
  - Before transmission, pick wait time [0,CW]
  - Free medium: count wait time
  - Busy medium: suspend counting
  - When count reaches 0, transmit RTS (or data frame)
- Contention window size tradeoff
  - Big CW → wait more before transmitting
  - Small CW → more collisions

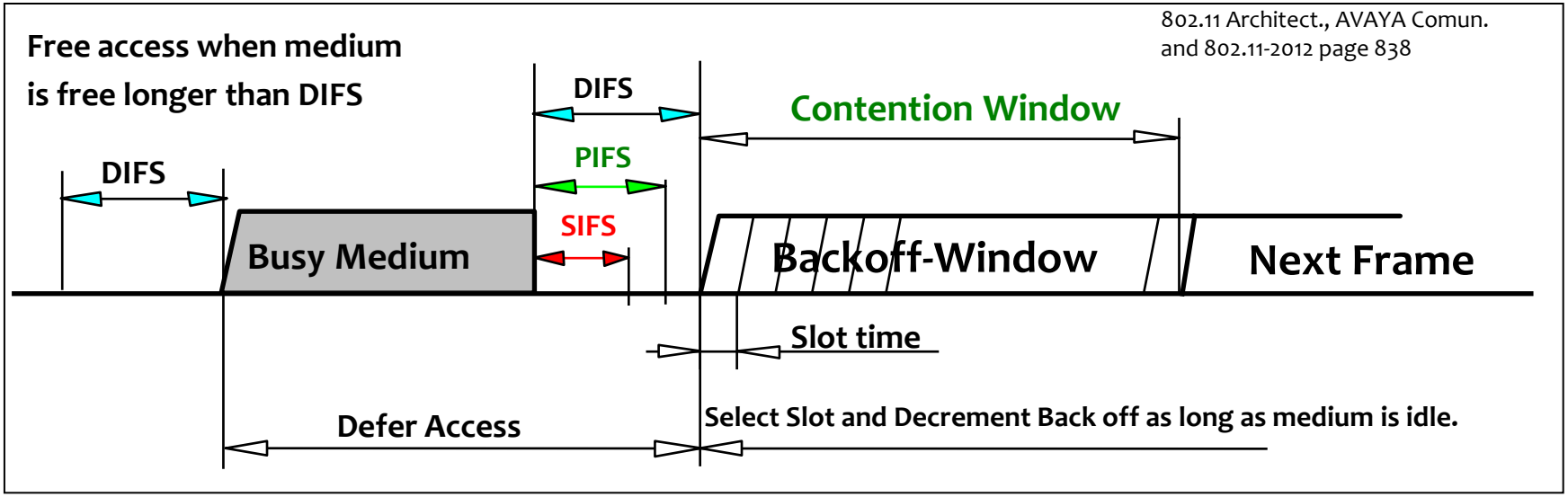
MAC: Congestion control

- Congestion varies with # of nodes and information to send
- DCF: congestion control varying CW
- Binary Exponential Backoff
  - If CTS fails after RTS (or ACK fails after data packet), the CW doubles (till CWmax)
  - After successful transmission, CW=CWmin
- Broadcast & multicast frames are not ACKed
  - No backoff!
  - Excessive broadcast /multicast traffic can lead to lots of collisions

Mechanisms for Medium Access Control

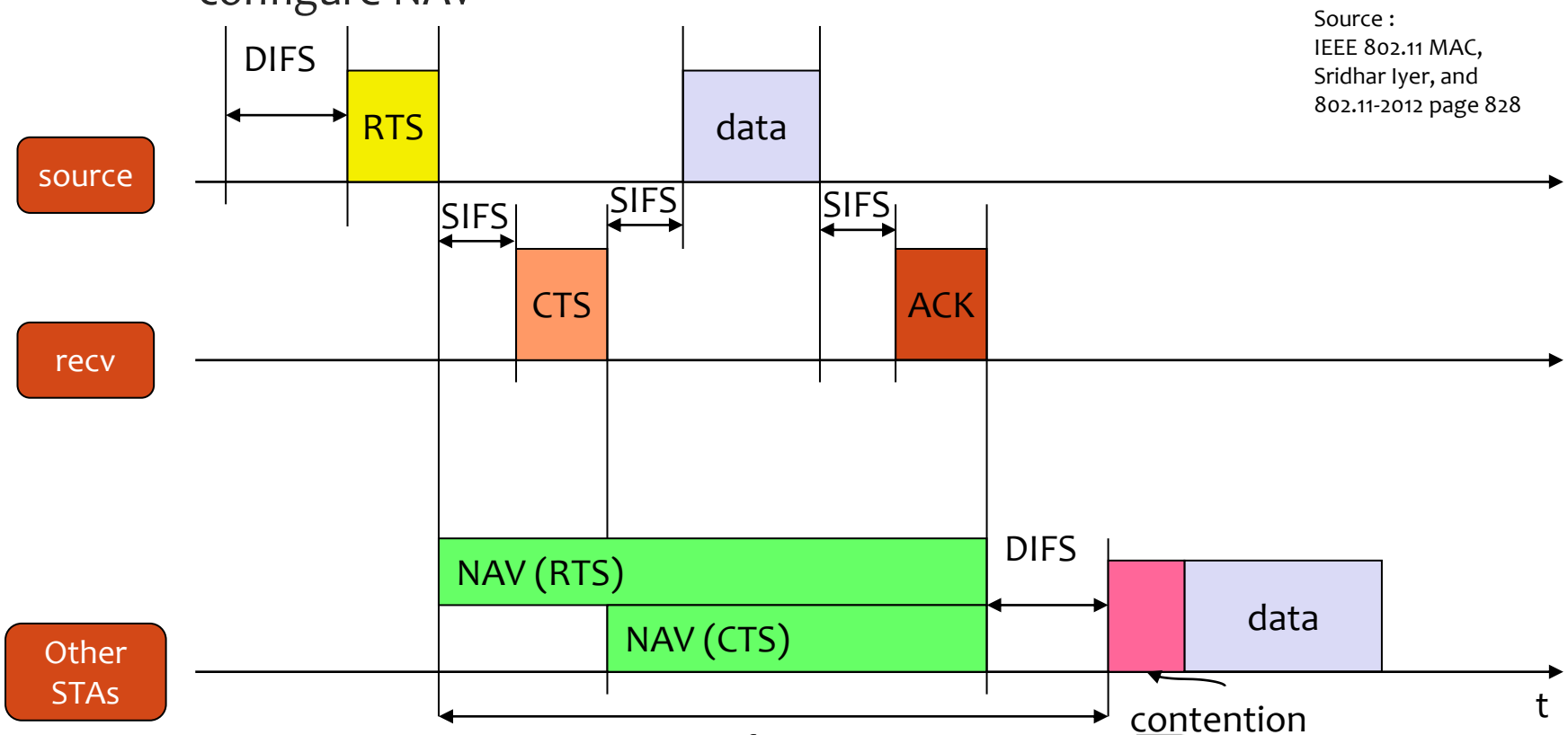
- Distributed Coordination Function (DCF)
  - Asynchronous data service
  - CSMA/CA
  - optionally with RTS/CTS
- Point Coordination Function (PCF)
  - Real-time data service
  - AP polls STAs
  - Only in infrastructure mode
- SIFS (Short Inter Frame Spacing)
  - Higher priority, for ACK, CTS, and answer to polling
- PIFS (PCF IFS)
  - Medium priority, for real-time service with PCF
- DIFS (DCF IFS)
  - Lower priority, for normal data service

Source:
802.11 Architect., AVAYA Comun. and 802.11-2012 page 838



Virtual Carrier Sensing

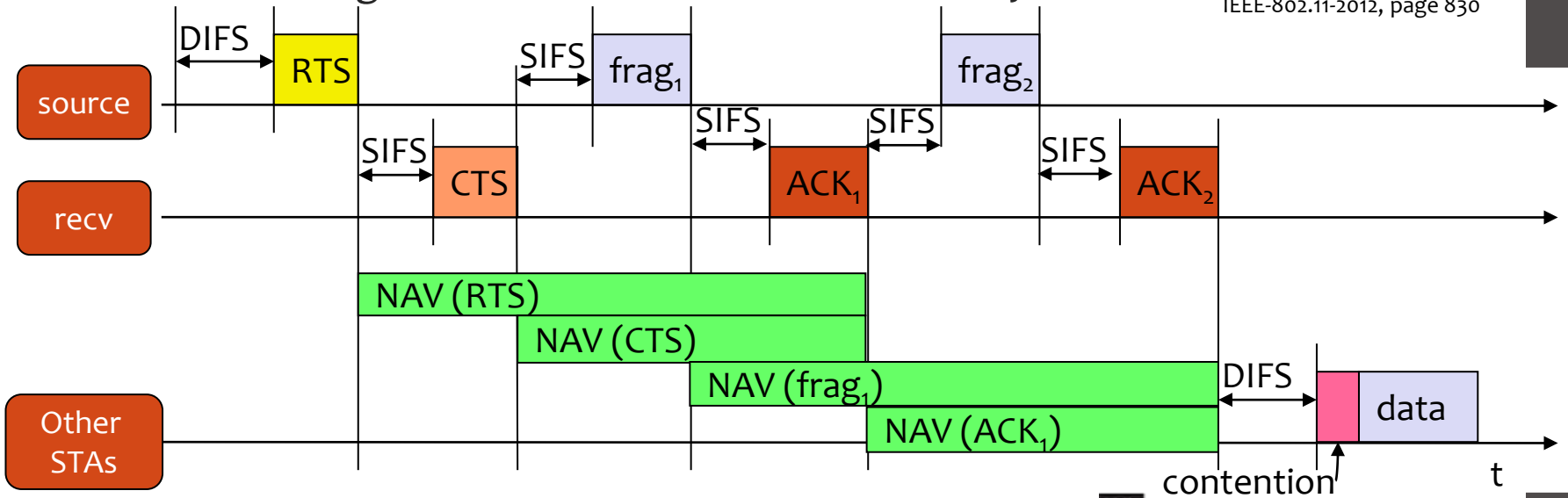
- NAV – Network Allocation Vector
  - Indicate medium usage (estimated)
  - RTS and CTS contain data packet duration; allows other STA to configure NAV



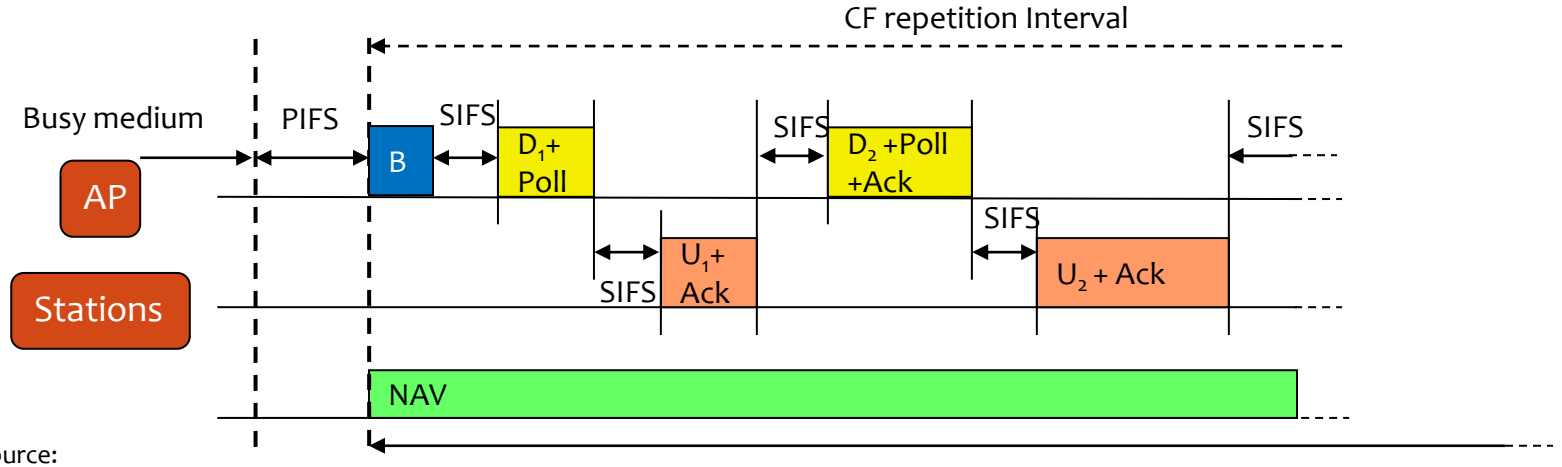
Fragmentation

- Wireless → high error rates
- Without fragmentation: the full frame is retransmitted in case of error
- With fragmentation only the fragment with error is retransmitted
  - Big fragments → more collisions
  - Small fragments → more overhead/latency

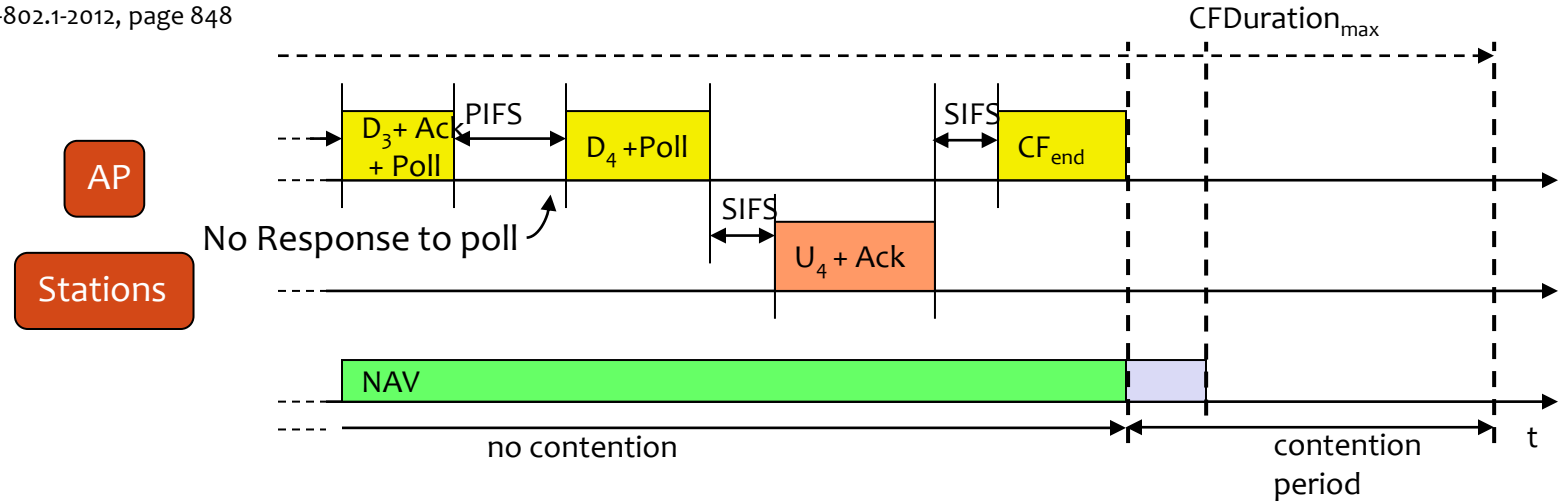
Source :
IEEE 802.11 MAC,
Sridhar Iyer and
IEEE-802.11-2012, page 830



PCF with polling



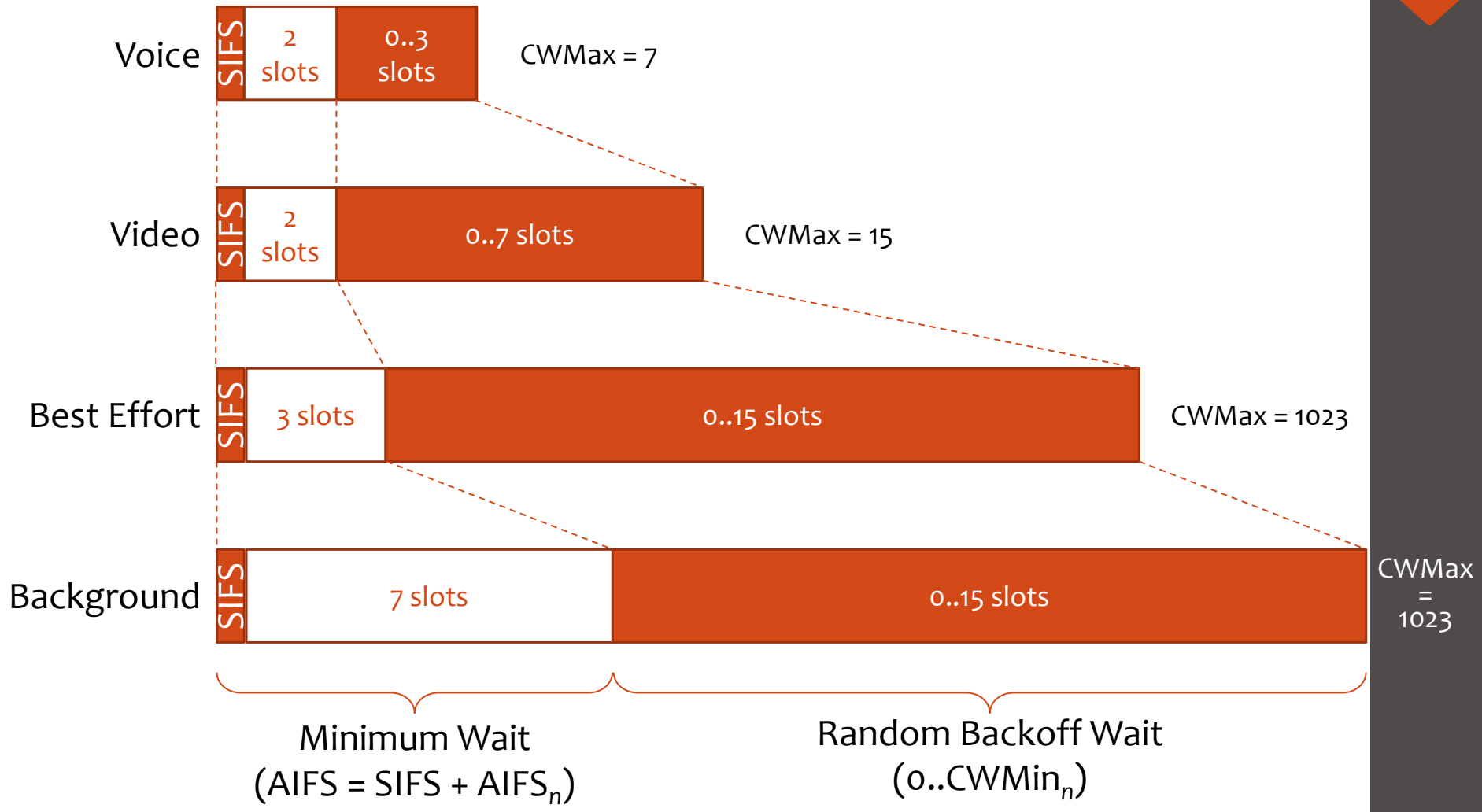
Source:
IEEE 802.11 MAC, Sridhar Iyer, and IEEE-802.1-2012, page 848



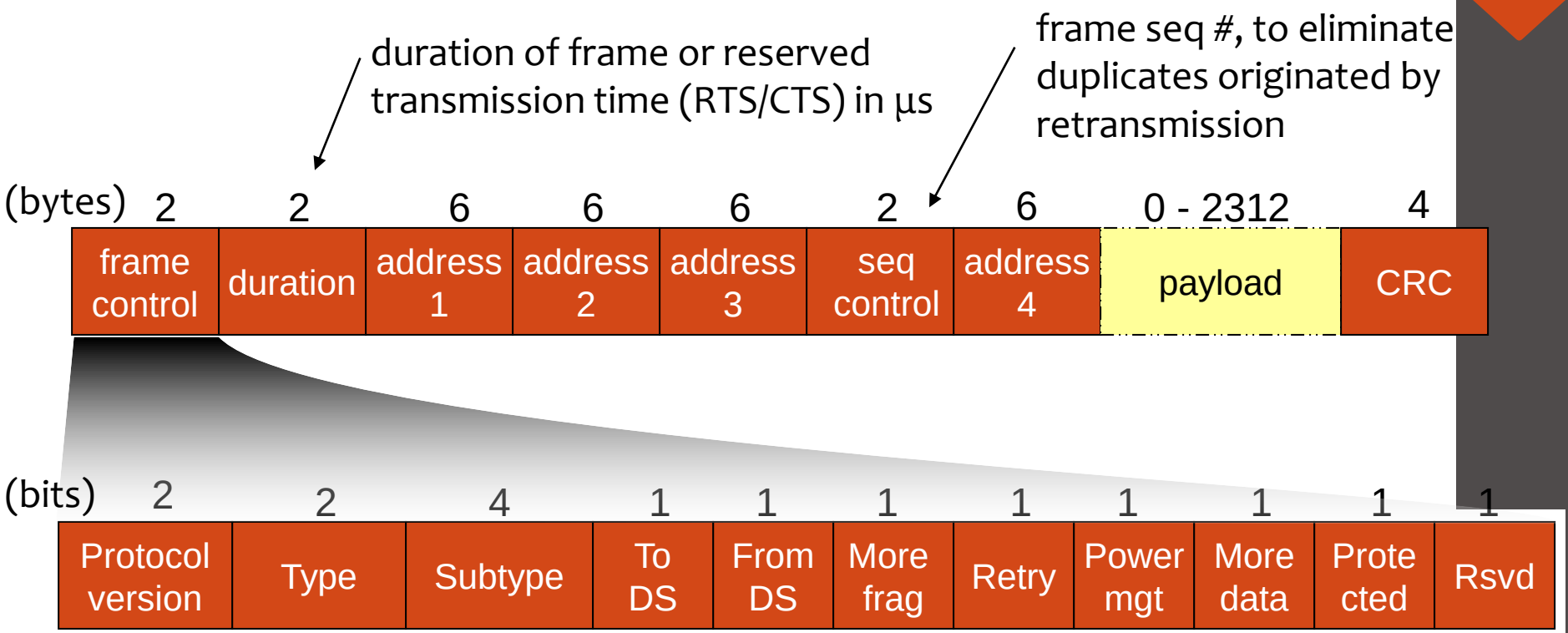
802.11e — WiFi Multimedia (WMM)

- New access control mechanism: Hybrid Coordination Function (HCF)
  - Enhanced distributed channel access (EDCA)
    - Like DCF, but supporting different access categories
    - Arbitration Inter-Frame Spacing ($AIFS_n$) instead of DIFS
    - Frames of higher priority categories use shorter AIFS and shorter contention windows
    - Possibility of per-AC admission control at the AP
      - TSpec for uplink, downlink or both
  - HCF Controlled Channel Access (HCCA)
    - Improved PCF
    - Controlled Access Phase (CAP) like CFP, but can be initiated at any time
    - Optional, not implemented in commercial hardware

Access Categories in EDCA



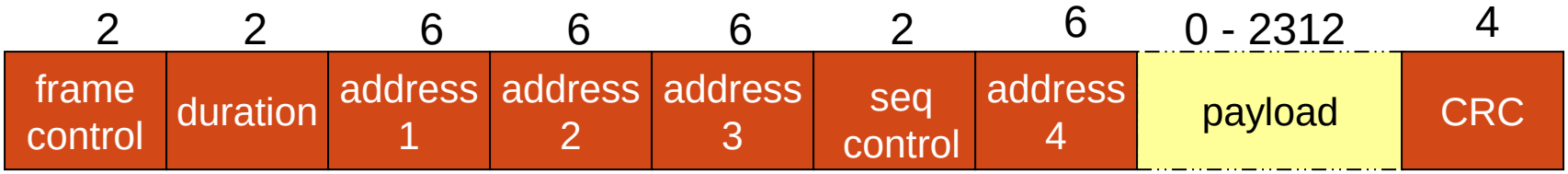
802.11 frame



frame type (management, control, data)

Ex.:
Type: 01 → control frame
SubType: 1011 → RTS

802.11 frame: addressing



Receiver address: MAC address of wireless host or AP which is the immediate receiver of this frame (not necessarily the final receiver)

Transmitter address : MAC address of wireless host or AP transmitting this frame (not necessarily its originator)

Address 3: varies…

Address 4: used only in wireless bridging

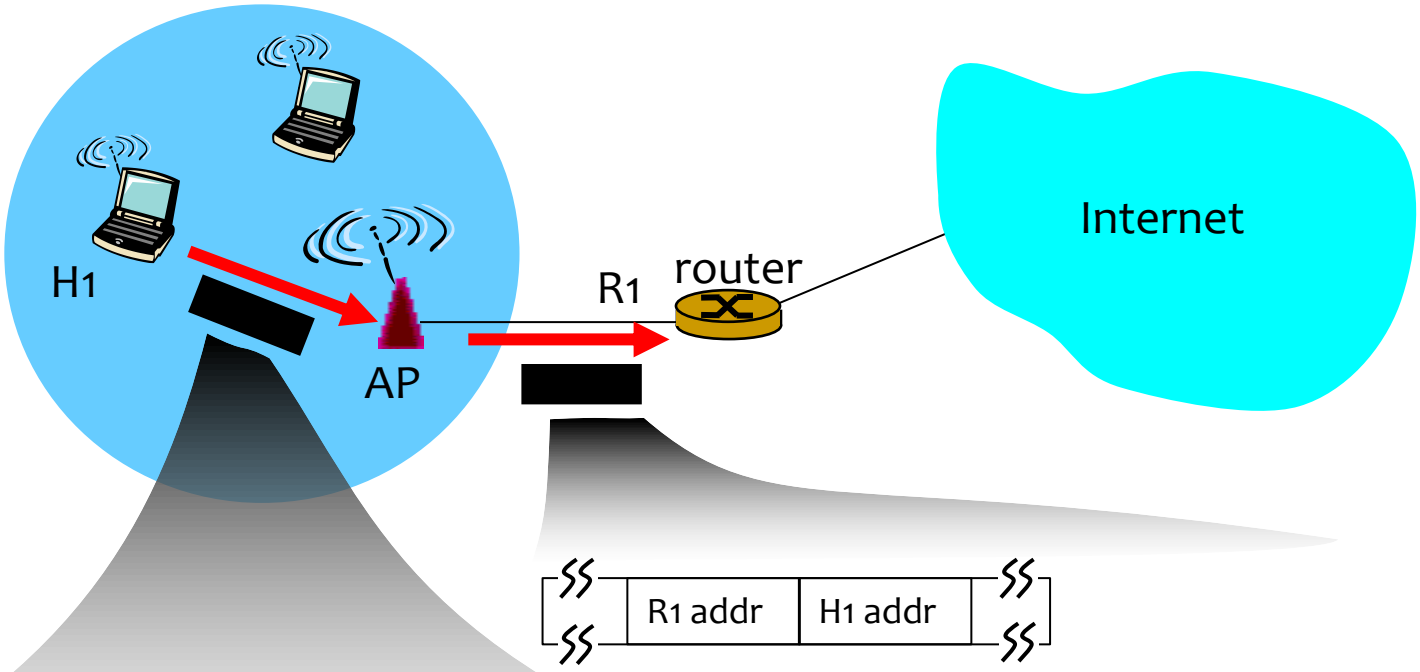
Addresses

Scenario	To DS	From DS	Addr 1	Addr 2	Addr 3	Addr 4
Ad-hoc (IBSS)	0	0	DA	SA	BSSID	-
From AP (infrastructure)	0	1	DA	BSSID	SA	-
To AP (infrastructure)	1	0	BSSID	SA	DA	-
WDS (bridge)	1	1	RA	TA	DA	SA

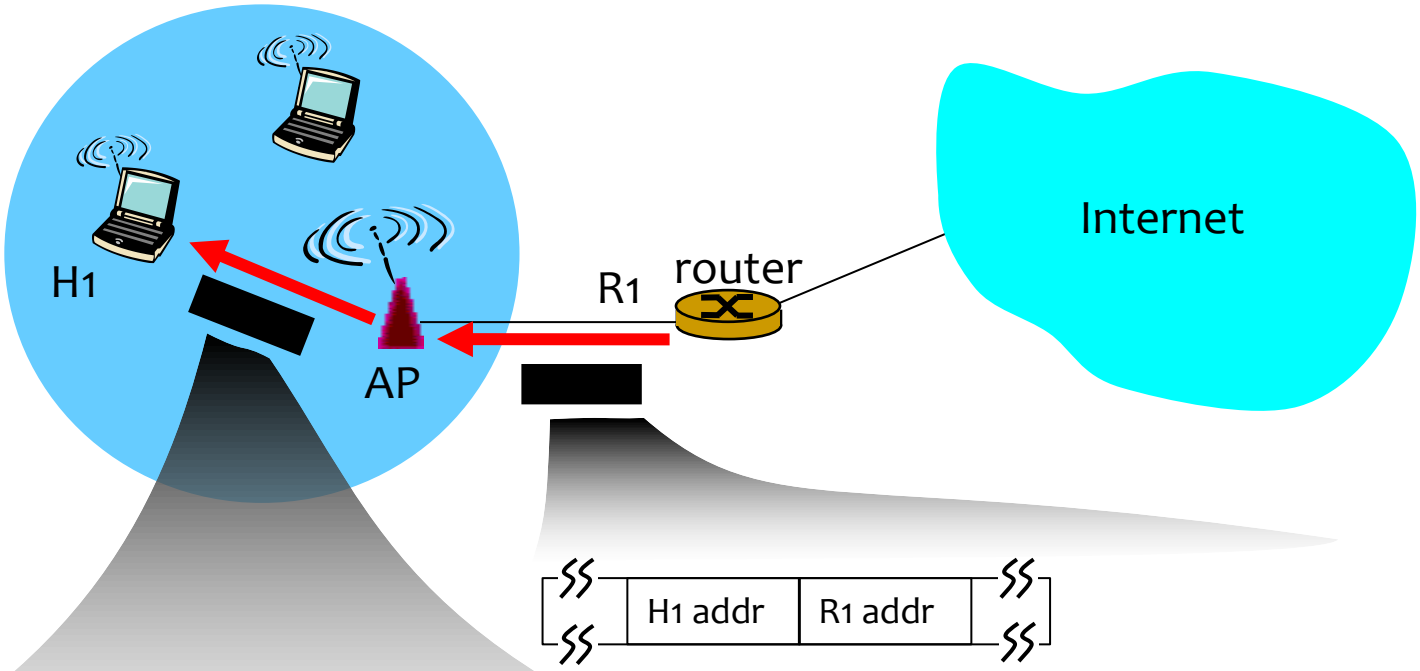
Source:
[802.11Guide]

DS: Distribution System
AP: Access Point
DA: Destination Address
SA: Source Address
BSSID: Basic Service Set Identifier
RA: Receiver Address
TA: Transmitter Address

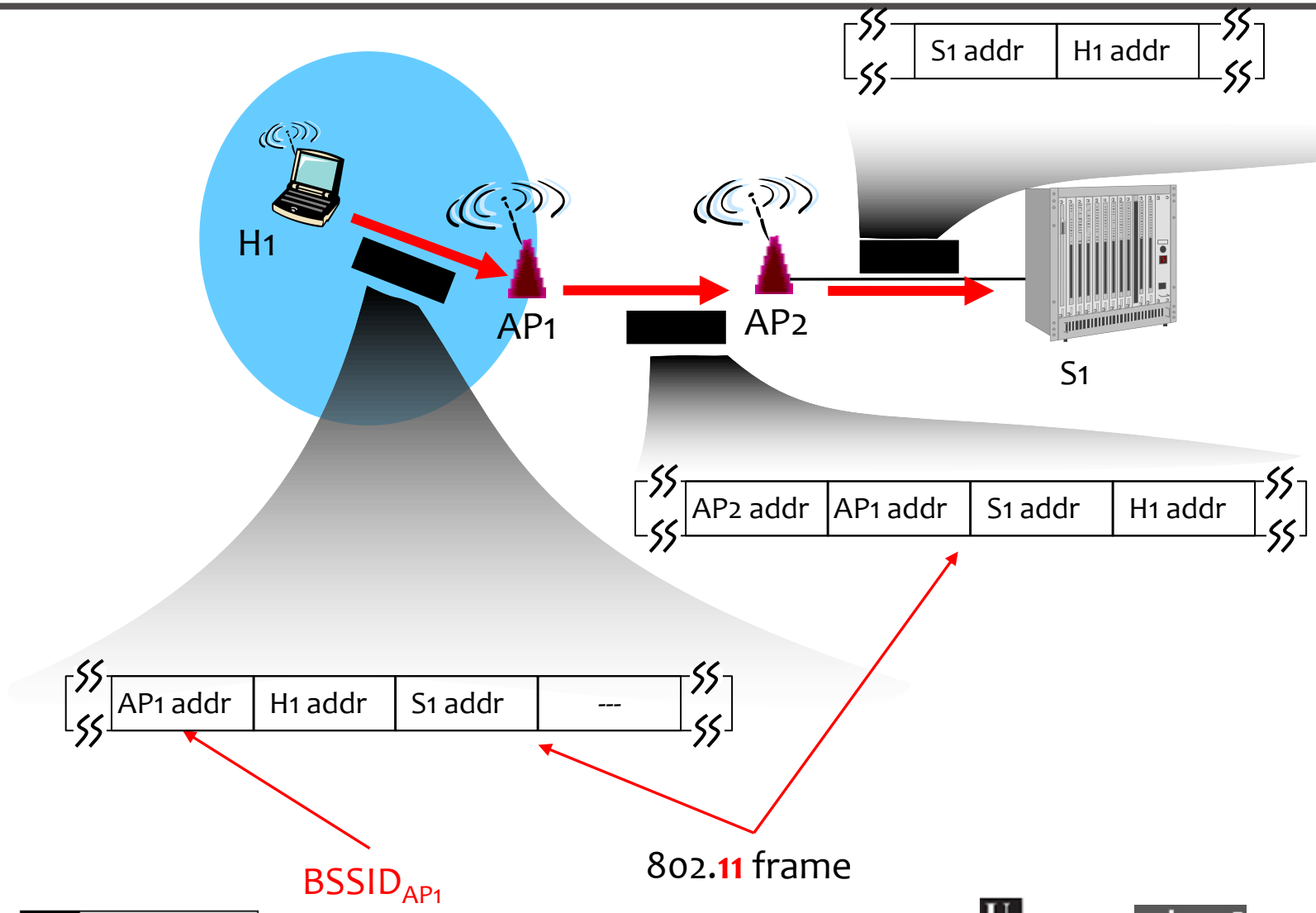
802.11 frame: addressing



802.11 frame: addressing

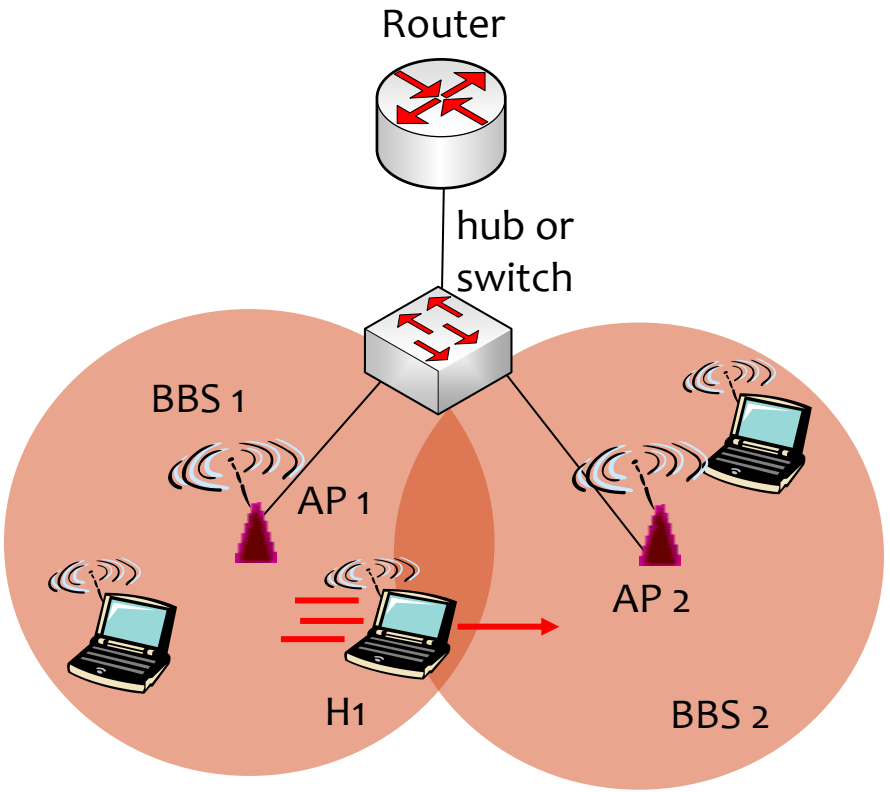


802.11 frame: addressing



802.11: L2 mobility (within same subnet)

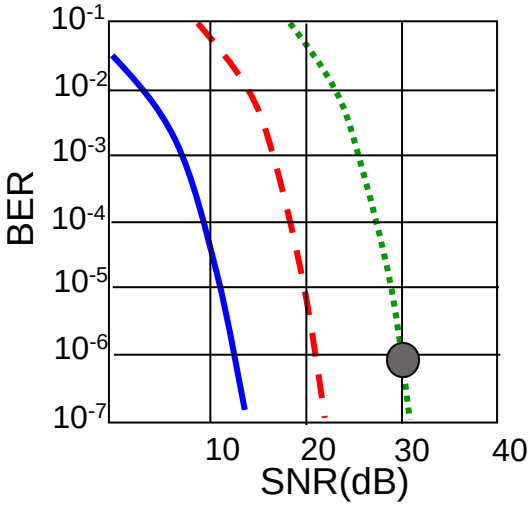
- H1 remains in same IP subnet: IP address can remain the same
- How does the switch know which AP is associated with H1?
  - self-learning: switch will see frame from H1 and "remember" which switch port can be used to reach H1
  - No L3 mobility

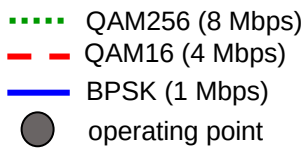


802.11: Rate Adaptation

Rate Adaptation

- base station, mobile dynamically change transmission rate (physical layer modulation technique) as SNR changes

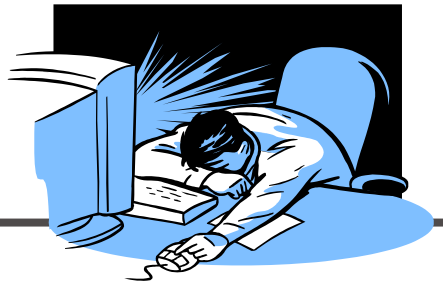




1. SNR decreases, BER increase as node moves away from base station

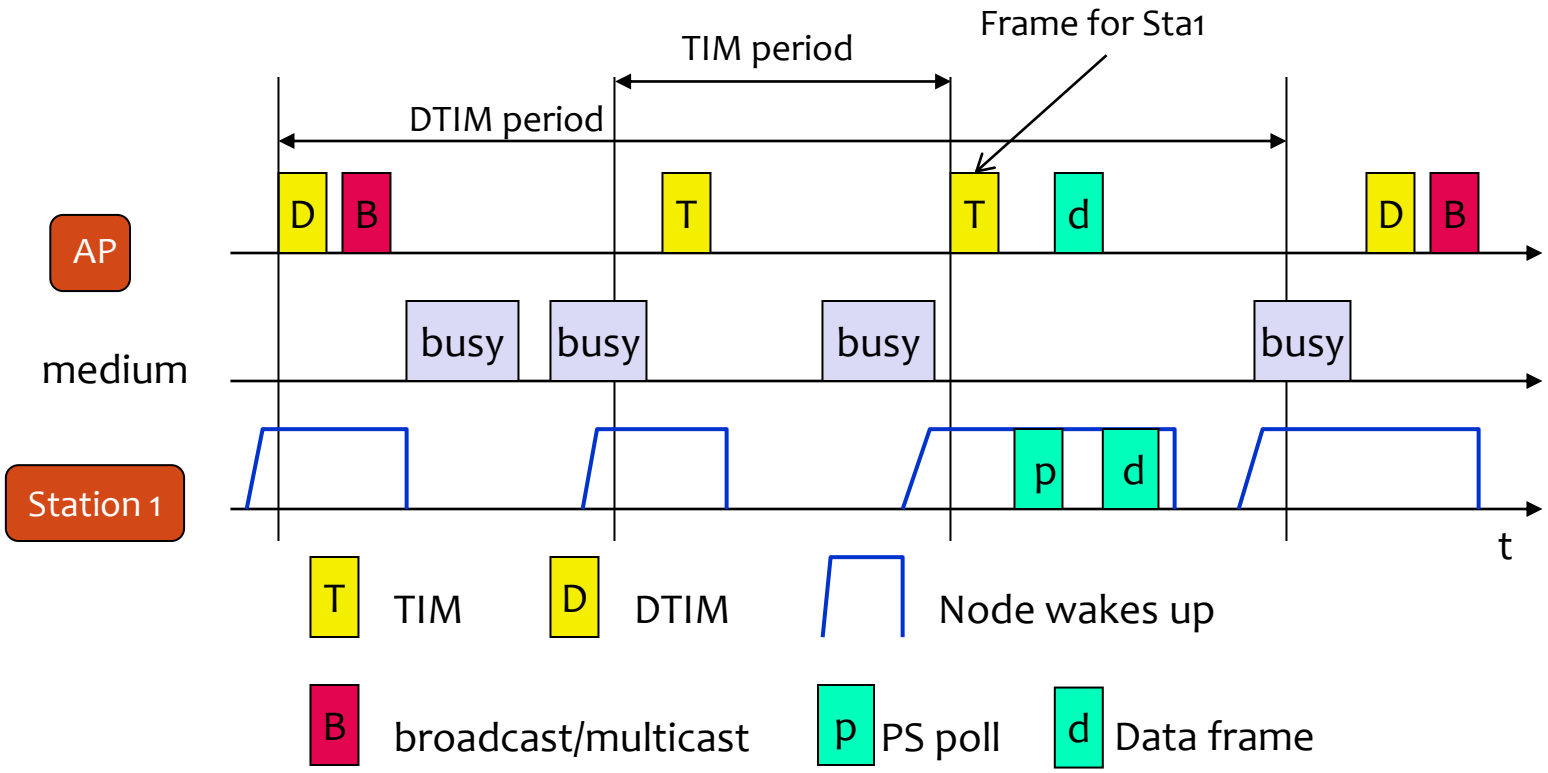
2. When BER becomes too high, switch to lower transmission rate but with lower BER

Power Saving



- Disconnect radio when not needed
- Saving in infrastructure mode
  - APs send Beacons
    - Beacons indicate nodes that have packets waiting
  - STA in saving mode wakes up to receive beacons
  - AP knows the status of each STA
- APs buffer data packets to sleeping STAs
  - APs announce buffered frames in beacon
  - Traffic Indication Map (TIM)
  - Common Period for multicast and broadcast frames (DTIM)
- STA wake periodically
  - If it has packets waiting sends PS-Poll
    - It knows from the TIM frame
  - AP answers with data

Power Saving

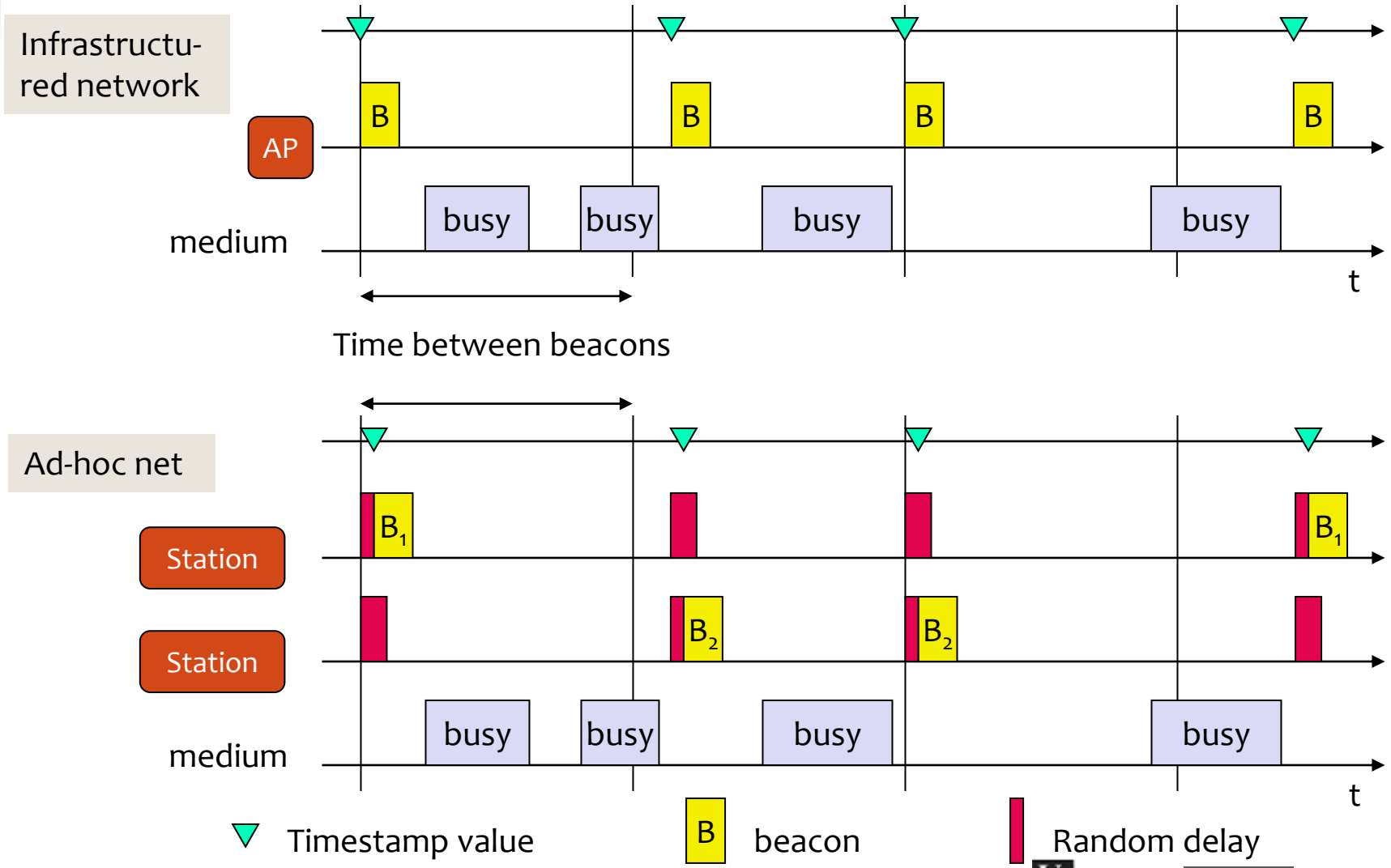


NOTE: This figure illustrates legacy power saving. 802.11 provides several additional power saving features.

Synchronization

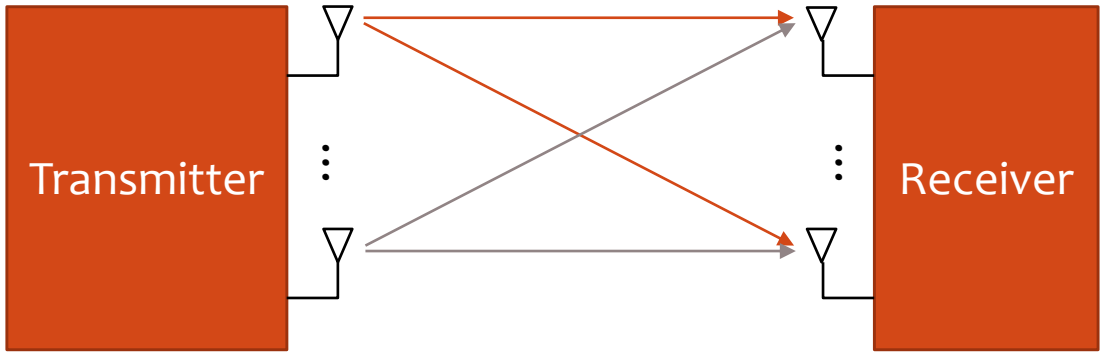
- Timing Synchronization Function (TSF)
  - Beacons from the AP are sent at defined times
  - Have the exact instant they were sent to the network
- Used for power management
  - Clocks for all STAs in the BSS are synchronized
- In ad-hoc mode (IBSS) every STA sends beacons
  - After a random delay to avoid collisions
  - After hearing a beacon from other STA, a STA does not send a beacon itself in this period

Synchronization



MIMO — Multiple Input, Multiple Output

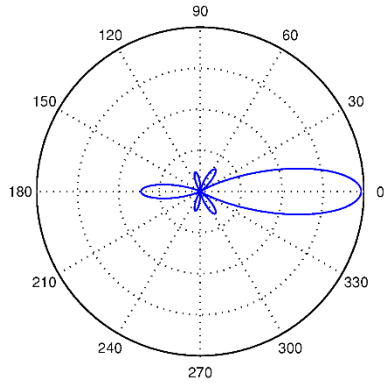
- 802.11n, ac and ax take advantage of multiple antennas at the transmitter and the receiver
- Gains from spatial diversity and beamforming (Tx & Rx)



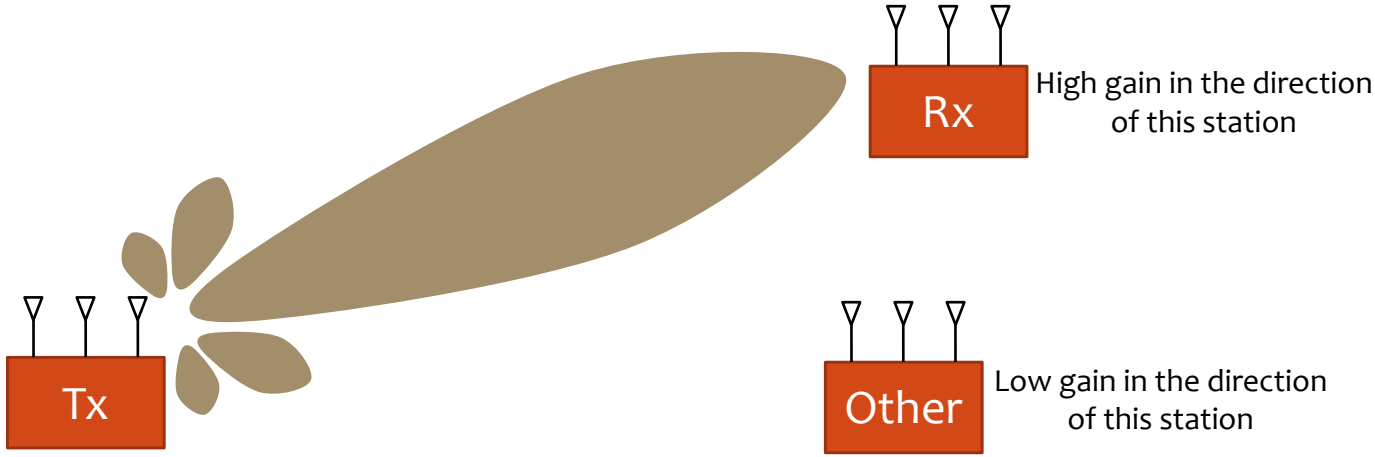
Spatial multiplexing

MIMO — Beamforming

- Multiple antennas may use constructive / destructive interference to
  - Increase gain in some directions
  - Decrease it in others
- Beamforming may be used in
  - Transmission: transmit a directed beam
  - Reception: listen selectively in some directions



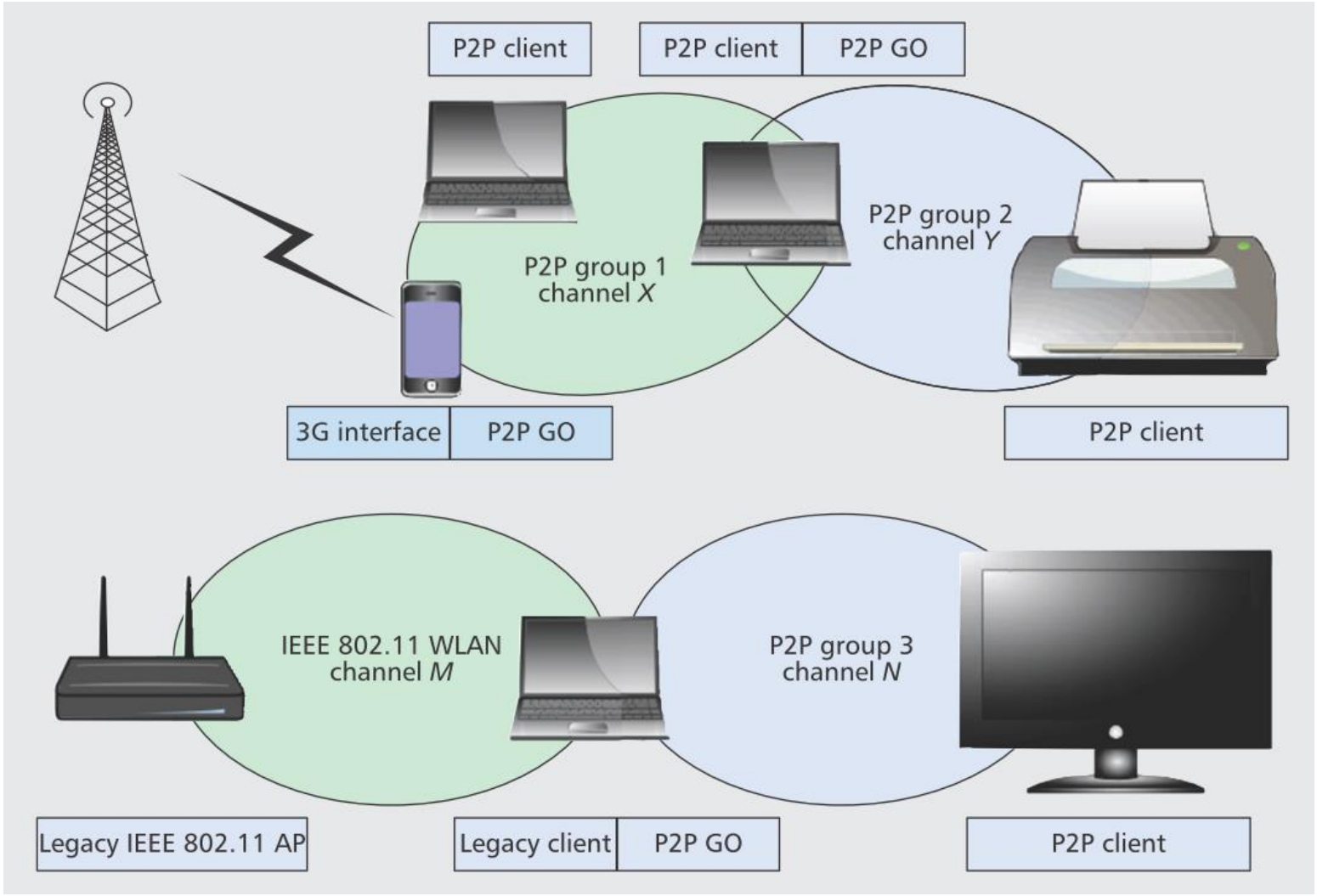
Example radiation pattern



WiFi Direct (P2P)

- Device-to-device connectivity without infrastructure (AP) is useful in many scenarios
- But ad-hoc mode of 802.11 is has several drawbacks
  - Difficult to configure
  - All nodes use the same channel
  - Inefficient power management
- WiFi Peer-to-Peer allows ad-hoc formation of groups where one device, the Group Owner (GO), plays the role of an AP
  - Security built into the protocol
  - Provides device and service discovery
  - More efficient power saving
  - Extended QoS capabilities
  - Devices can belong to a group and be connected to the Internet simultaneously

WiFi Direct: Topologies & Use Cases

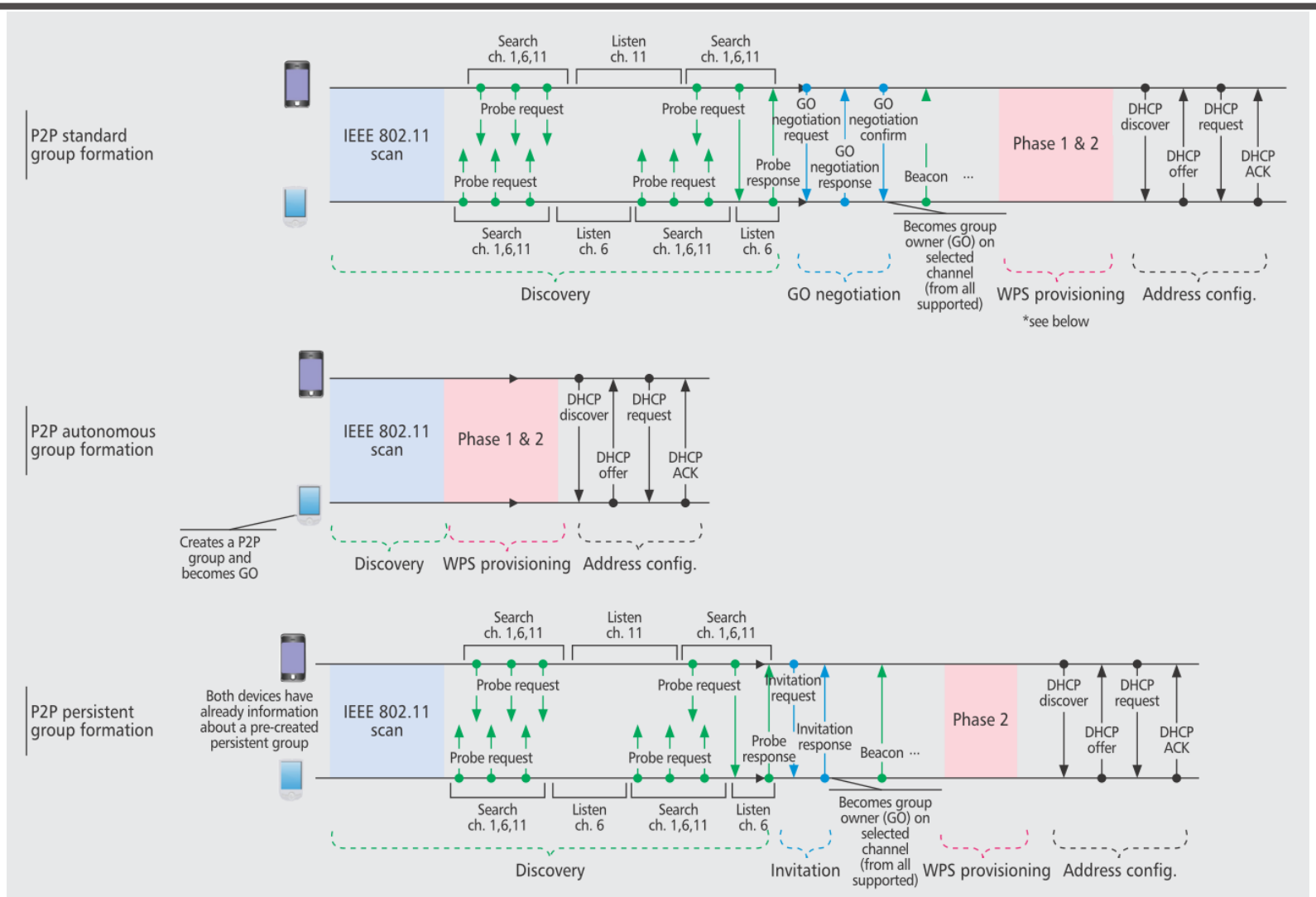


Source: D. Camps-Mur, A. Garcia-Saavedra and P. Serrano, "Device-to-device communications with Wi-Fi Direct: overview and experimentation," in IEEE Wireless Communications, vol. 20, no. 3, pp. 96-104, June 2013.

WiFi Direct

- The role of GO can be
  - negotiated between the devices
  - or directly assumed by one of the devices
- IP configuration is easy
  - GO acts as DHCP server for other devices
- GO may provide routing to external networks
  - typically, through NAT
  - bridging is not allowed
- The role of GO is not transferrable
  - if the GO leaves, a new group must be formed
- WiFi Direct mandates support of WiFi Protected Setup (WPS)
  - easy security configuration using a PIN or push-button

WiFi Direct: Group Formation

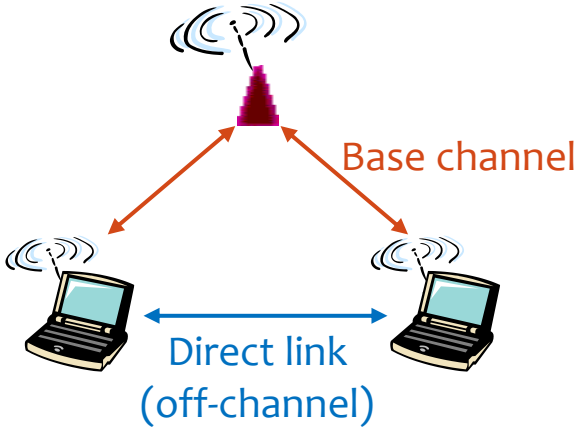


Source: D. Camps-Mur, A. Garcia-Saavedra and P. Serrano, "Device-to-device communications with Wi-Fi Direct: overview and experimentation," in IEEE Wireless Communications, vol. 20, no. 3, pp. 96-104, June 2013.

TDLS — 802.11z

- In infrastructure mode, nodes communicate through the AP
  - Similarly in WiFi Direct through the GO
- Frames are transmitted twice even if stations can hear each other
  - From source station to AP
  - From AP to destination station
- Inefficient use of capacity
  - More transmissions than necessary
  - More collisions…
- Tunneled Direct Link Setup (TDLS) allows the negotiation of a different channel for direct communication
  - AP needs not be aware of negotiation ➔ works through any AP
  - AP may explicitly forbid it, though (in the beacons)

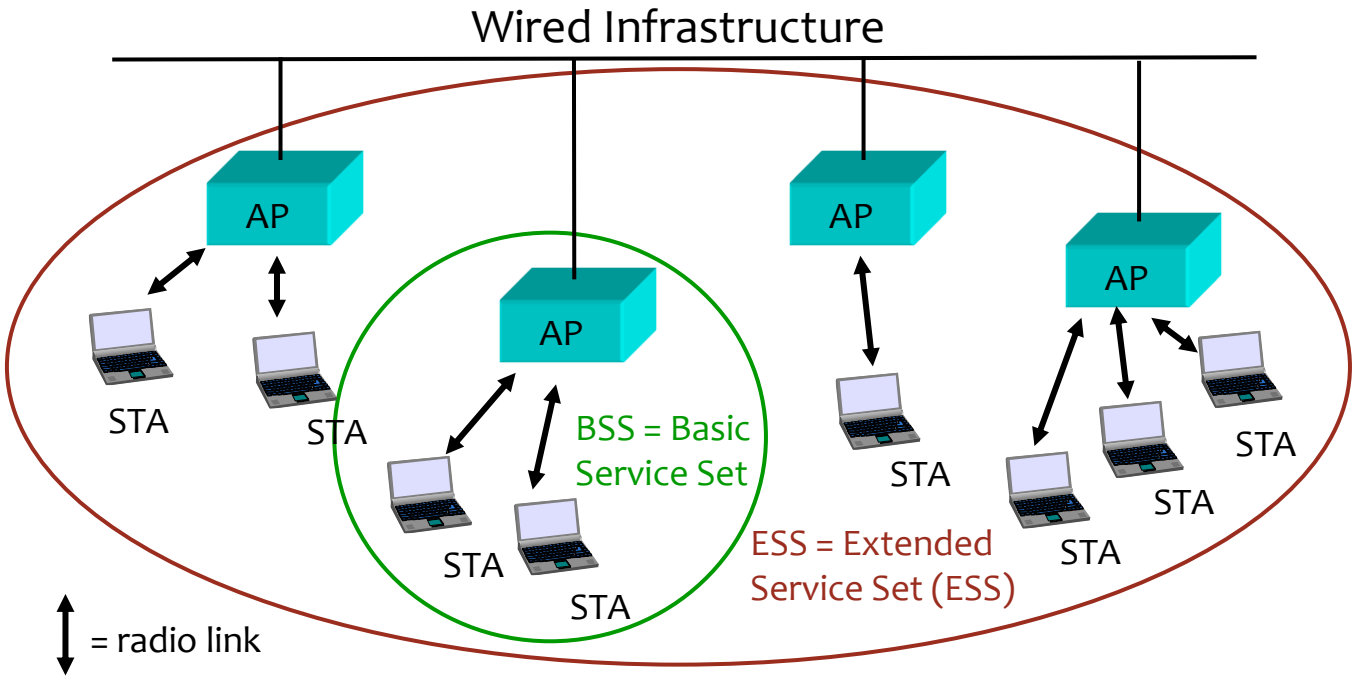
TDLS — 802.11z



Example:
2.4GHz 802.11g
5GHz 802.11ac

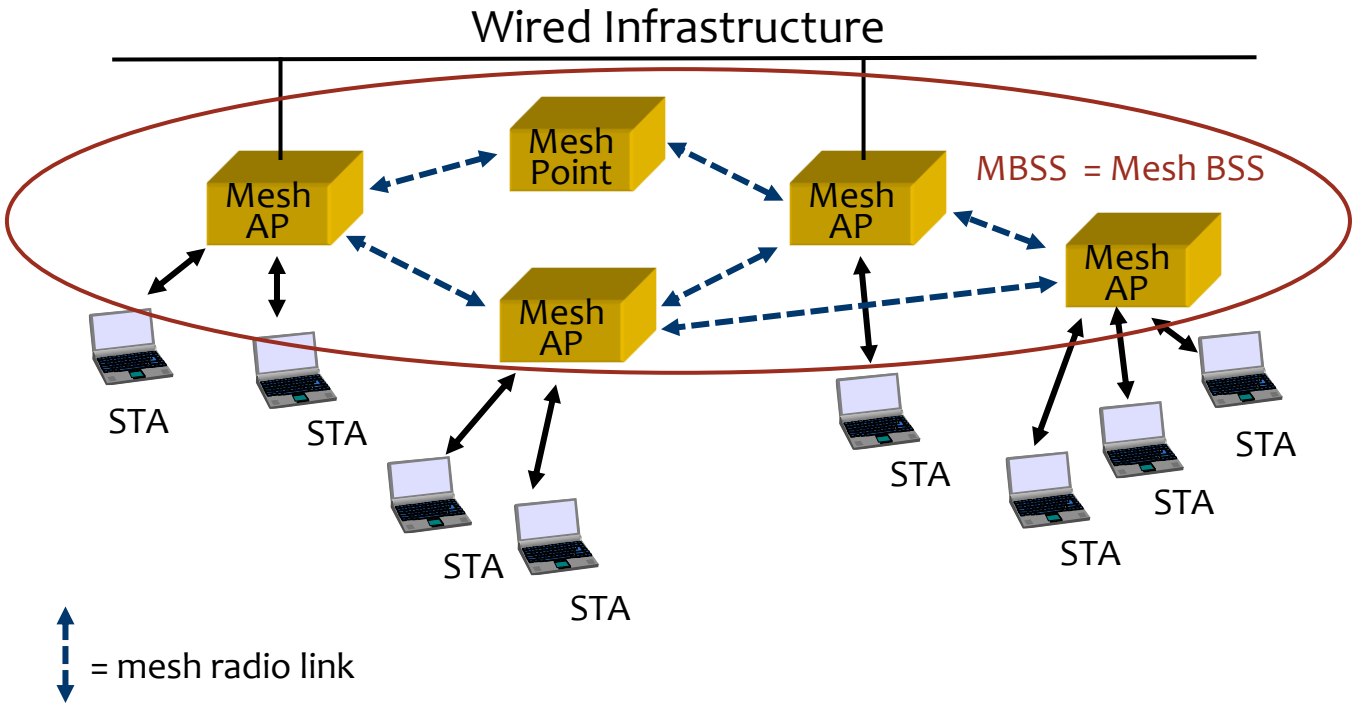
- Direct link may
  - be in different frequency band
  - use different PHY
  - ➔ useful even with old APs
- TDLS initiator and responder remain connected to the AP
- Single radio nodes periodically switch to base channel, with or without band steering
  - Listen to AP beacons
  - Communicate in the BSS

Mesh Networking: Why?



- Paradox: WLAN APs are typically wired!
- Wireless Distribution System
  - Standard defines frame format, but not how such frames should be used ➔ incompatible implementations

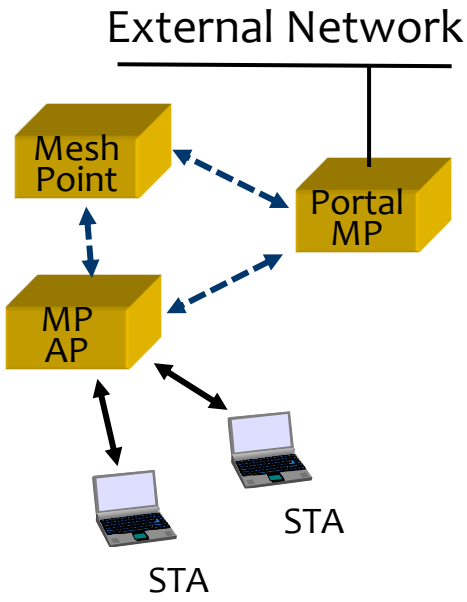
Mesh Networking: 802.11s



- 802.11s added mesh networking capabilities to 802.11 WLANs
- Benefits: flexible, self-forming, self-healing wireless backhaul

802.11s: Device Classes

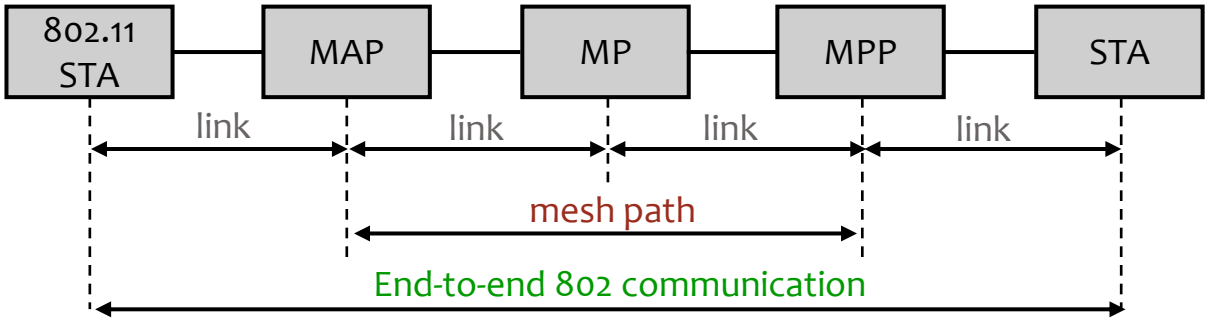
- Mesh Point (MP): establishes peer links with MP neighbors, full participant in WLAN Mesh services
- Mesh AP (MAP): functionality of a MP collocated with AP which provides BSS services to support communication with STAs
- Mesh Portal (MPP): point at which frames exit and enter a WLAN Mesh (relies on higher layer bridging functions)
- Station (STA): outside of the WLAN Mesh, connected via Mesh AP



802.11s: Addressing

- Two additional addresses in mesh frames
  - Need to identify mesh entry and exit points

Scenario	To DS	From DS	AE Flag	Addr 1	Addr 2	Addr 3	Addr 4	Addr 5	Addr 6
Ad-hoc (IBSS)	0	0	0	DA	SA	BSSID	-	-	-
From AP	0	1	0	DA	BSSID	SA	-	-	-
To AP	1	0	0	BSSID	SA	DA	-	-	-
WDS	1	1	0	RA	TA	DA	SA	-	-
Mesh	1	1	1	RA	TA	Mesh DA	Mesh SA	DA	SA



802.11s: Path Discovery & Selection

- "Routing", but at link layer
  - Using MAC (instead of IP) addresses
  - Full addresses (not prefixes), since MAC addressing is flat
- Hybrid Wireless Mesh Protocol (HWMP)
  - Reactive (on-demand) path descovery
    - Based on AODV
  - Proactive path discovery to mesh portals
    - Tree-based
  - Uses airtime as metric
    - Minimize total consumption of time for transmissions
- Other protocols and metrics may be used
  - But support for HWMP using airtime metric is mandatory

The end

References

- [802.11Guide] Matthew S. Gast, "802.11 Wireless Networks: The definitive guide" 2nd Edition, O'Reilly, 2005
- [Sridhar] Slides from Dr. Sridhar Iyer for cs716 at IIT Bombay

Acronyms – 802.11

- AP – Access Point
- ATIM - Announcement Traffic Indication Messages
- BER - Bit Error Rate
- BPSK - Binary Phase Shift Keying
- BSS – Basic Service Set
- BSSID – Basic SSID
- CSMA - Carrier Sense Multiple Access
- CSMA/CA - CSMA/Collision Avoidance
- CSMA/CD – CSMA with Collision Detection
- CTS – Clear To Send
- CW – Contention Window
- DCF – Distributed Coordination Function
- DIFS – DCF Interframe Space
- DS – Distribution System
- DTIM - Delivery TIM
- ESS – Extended Service Set
- ESSID – Extended SSID
- IBSS – Independent BSS
- LLC - Logical Link Control
- MACA – Multiple Access with Collision Avoidance
- MLME – MAC Layer Management Entity
- MSC - Mobile Switch Center
- NAV – Net Allocation Vector
- PCF - Point Coordination Function
- PIFS – PCF Interframe Space
- QAM - Quadrature Amplitude Modulation
- RTS - Request To Send
- SIFS – Short Interframe Space
- SNR - Signal to Noise Ratio
- SSID – Service Set Identifier
- STA – STAtion
- TFT – Timing Synchronization Function
- TIM – Traffic Information Map
- WDS – Wireless Distribution System