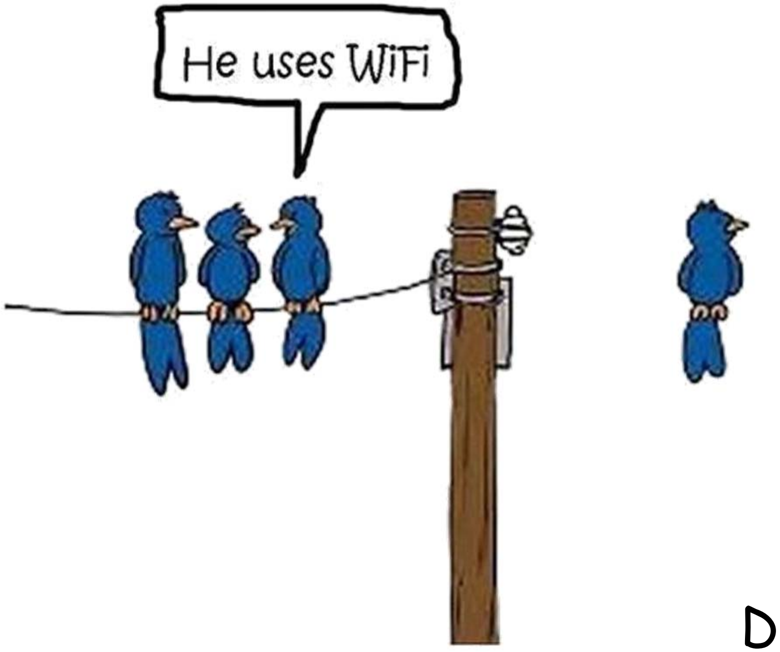


CSCE 560 Introduction to Computer Networking

Dr. Barry Mullins
AFIT/ENG
Bldg 642, Room 209
255-3636 x7979

Chapter 7 Outline

7.1 Introduction

Wireless

7.2 Wireless links, characteristics
  - CDMA

7.3 IEEE 802.11 wireless LANs ("Wi-Fi")

7.4 Cellular Internet Access
  - Architecture
  - Standards (e.g., GSM)

CSCE 660

Mobility

7.5 Principles: addressing and routing to mobile users

7.6 Mobile IP

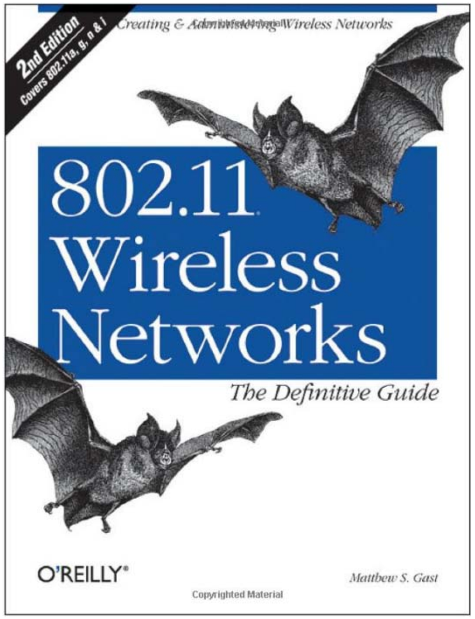
7.7 Managing mobility in cellular networks

7.8 Wireless and Mobility: Impact on higher-layer protocols

CSCE 660

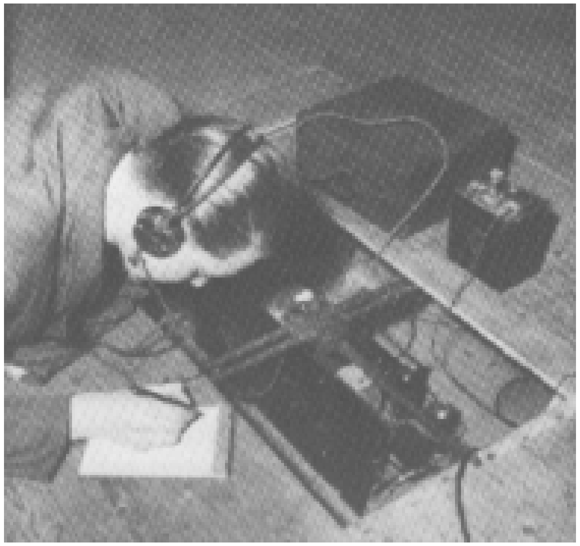
Another great source:

802.11 Wireless Networks - The Definitive Guide by Matthew Gast

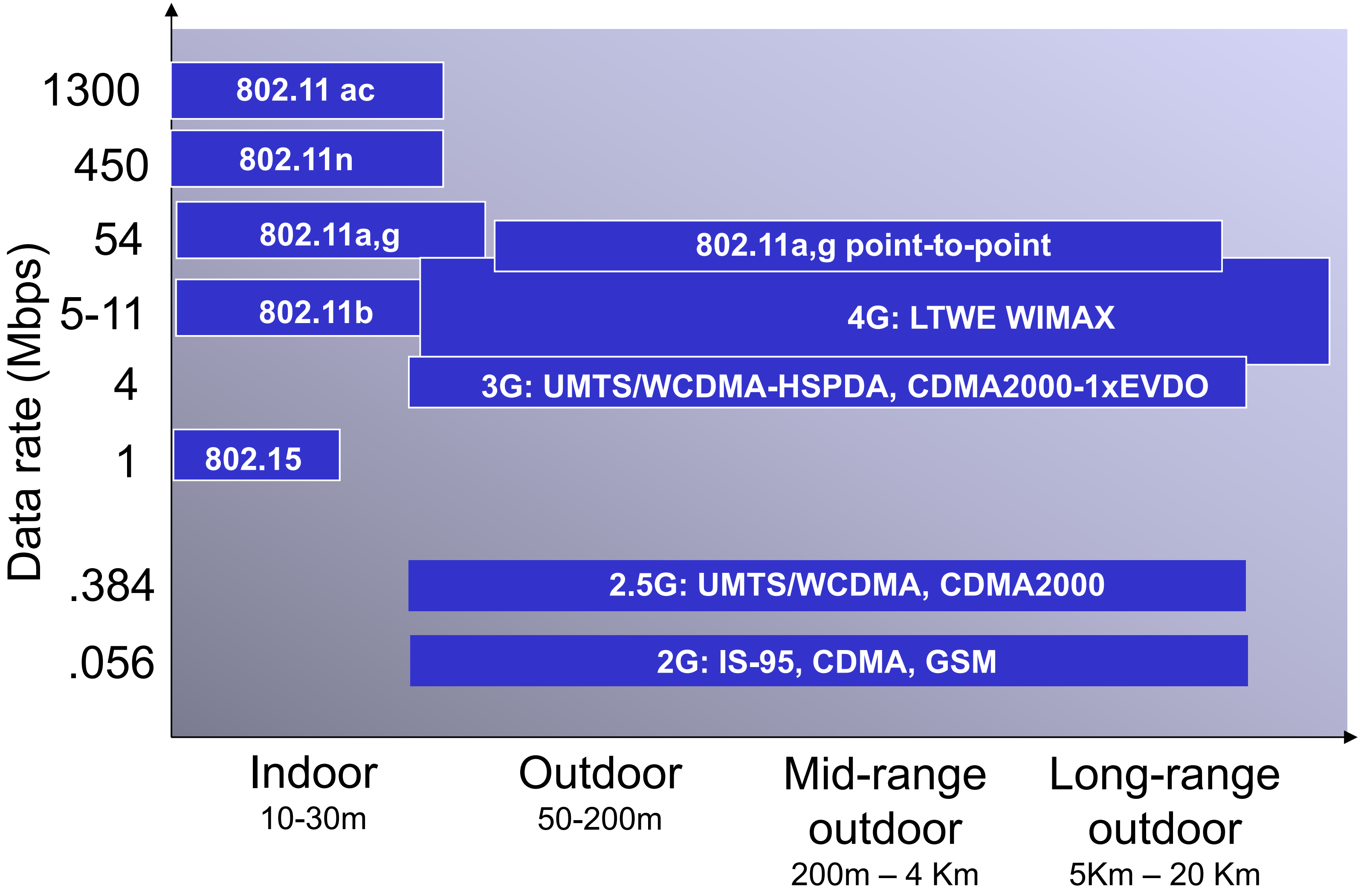


Abridged Wireless History

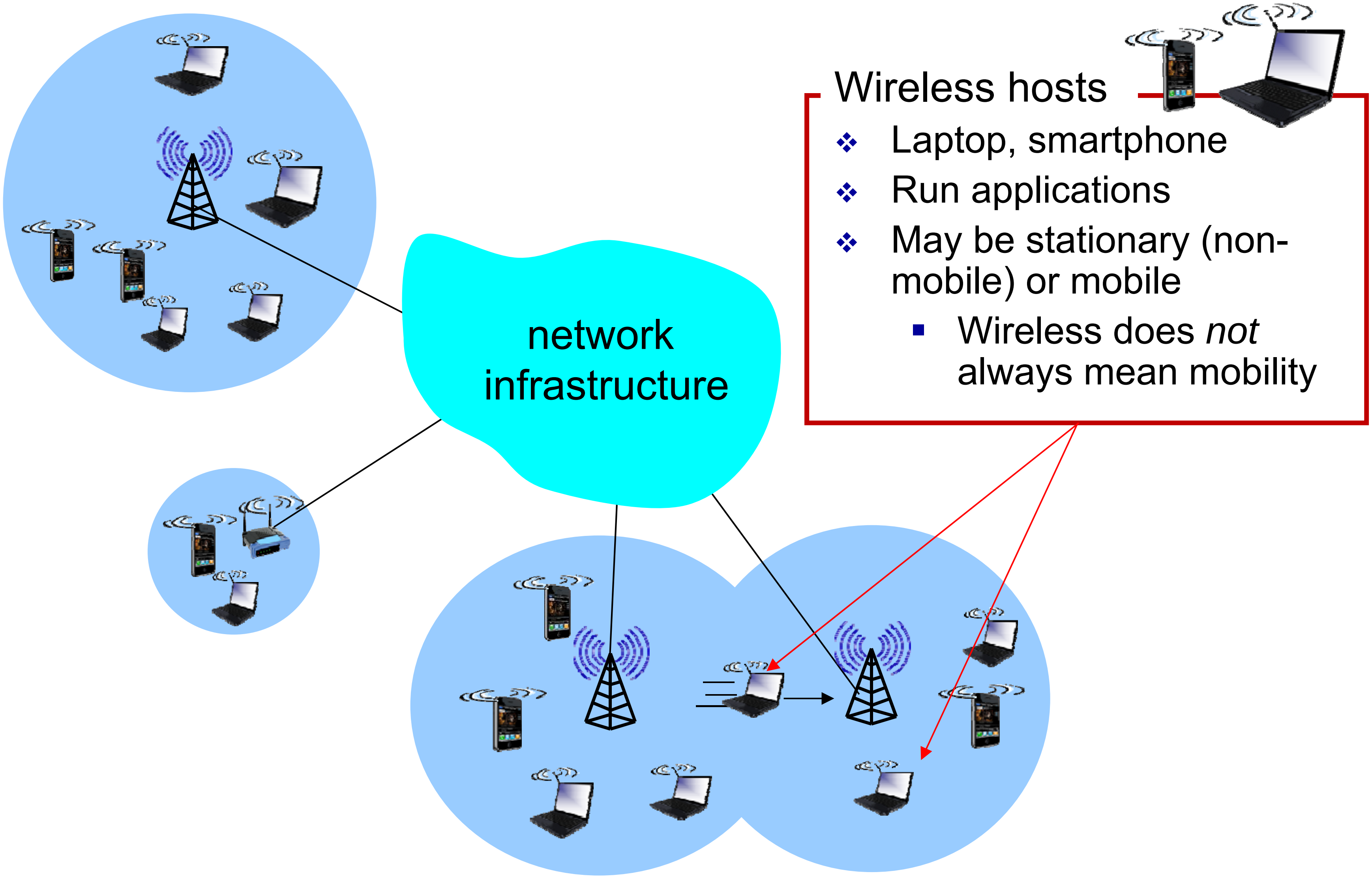
- 1867 - Maxwell predicts existence of electromagnetic (EM) waves
- 1887 - Hertz proves existence of EM waves
  - First spark transmitter generates a spark in a receiver several meters away
- 1896 - Marconi demos wireless telegraph to English telegraph office
- 1898 - First commercial radio data service
- 1914 - First voice over radio transmission
- 1920s - Mobile receivers installed in police cars in Detroit
- 1946 - First interconnection of mobile users to public switched telephone
  - St. Louis using Push-to-talk
- 1962 – First communication satellite, Telstar, launched into orbit
- 1970 - First Cellular Phone Service:
  - Chicago using cells, handoff, and roaming
- 1971 - First Wireless Data Network:
  - Aloha at University of Hawaii
- 1990 - First Commercial Wireless LAN Product
  - AT&T WaveLAN
- 1997 - First Wireless LAN Standard - IEEE 802.11
  - 2 Mbps
- 2016 - about 15 billion Wi-Fi devices sold
- 2018 – More than half the Internet traffic traverses Wi-Fi networks



Characteristics of Selected Wireless Links



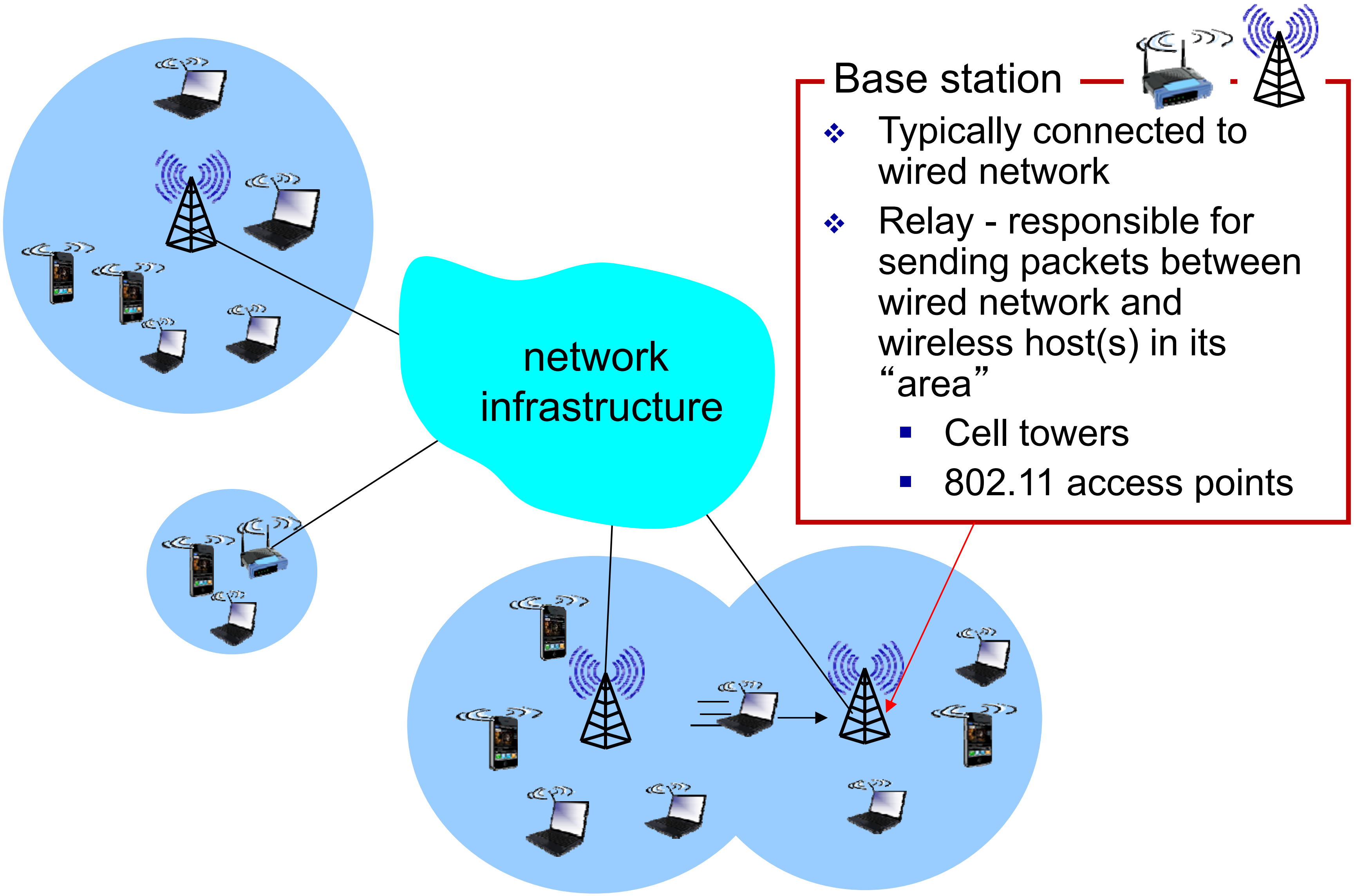
Wireless Hosts



Wireless hosts

- Laptop, smartphone
- Run applications
- May be stationary (non-mobile) or mobile
  - Wireless does *not* always mean mobility

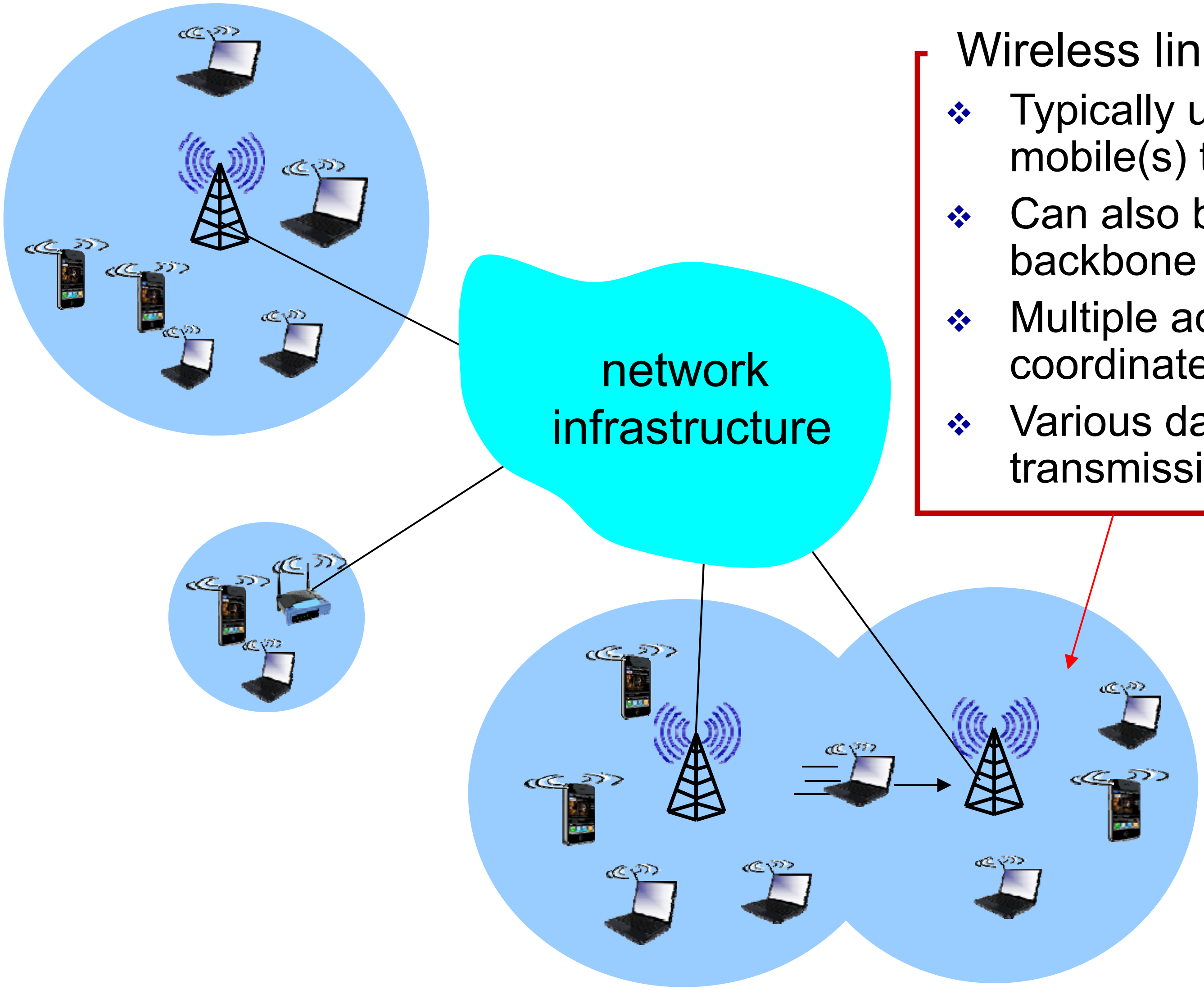
Base Station



Base station

- Typically connected to wired network
- Relay - responsible for sending packets between wired network and wireless host(s) in its “area”
  - Cell towers
  - 802.11 access points

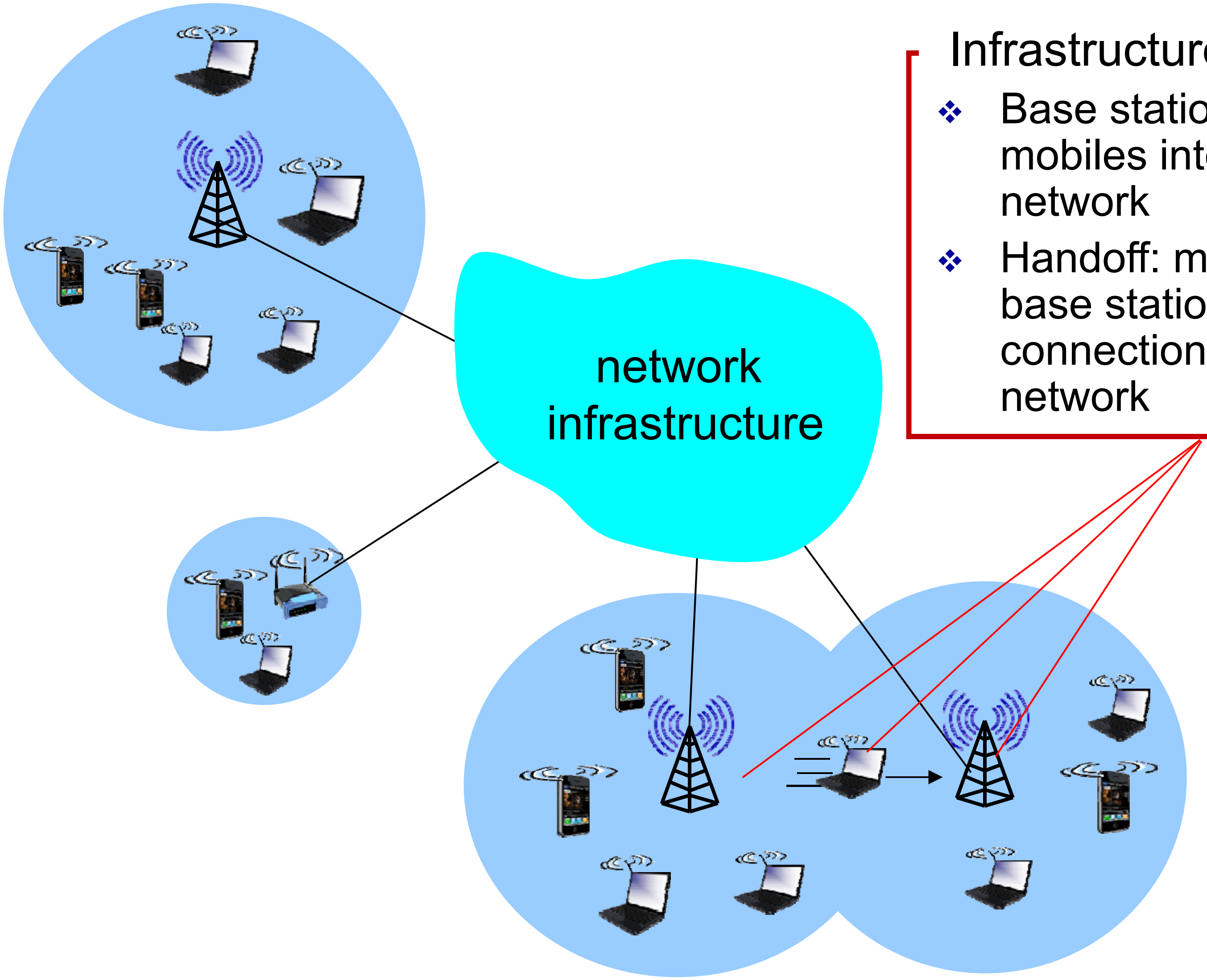
Wireless Link



Wireless link

- Typically used to connect mobile(s) to base station
- Can also be used as backbone link
- Multiple access protocol coordinates link access
- Various data rates, transmission distance

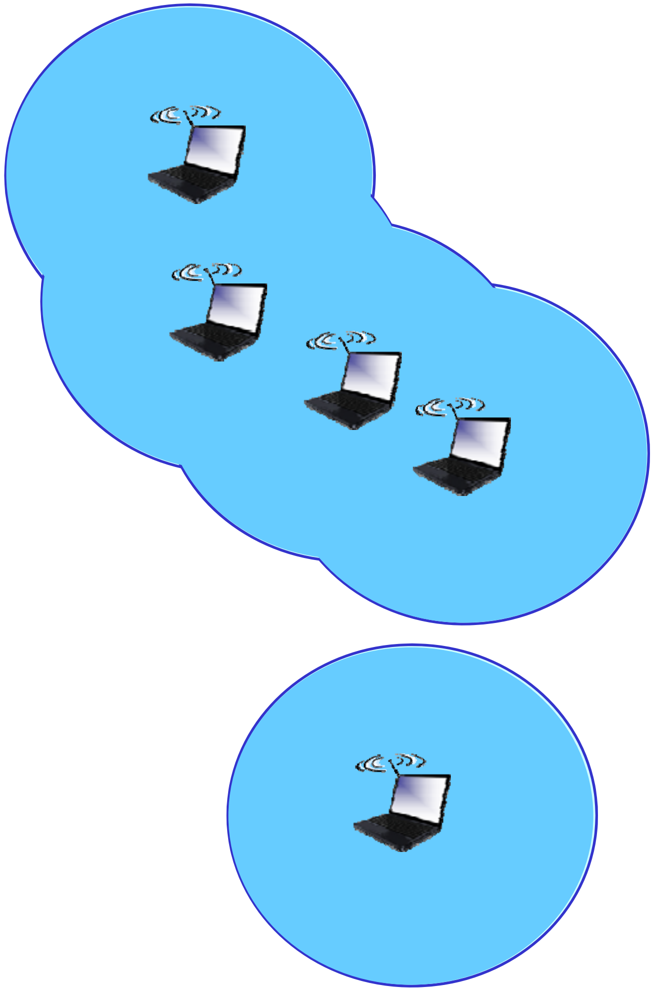
Infrastructure Mode



Infrastructure mode

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

Ad Hoc Mode



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

Chapter 7 Outline

7.1 Introduction

Wireless

7.2 Wireless links, characteristics
  - CDMA

7.3 IEEE 802.11 wireless LANs ("Wi-Fi")

7.4 Cellular Internet Access
  - Architecture
  - Standards (e.g., GSM)

Mobility

7.5 Principles: addressing and routing to mobile users

7.6 Mobile IP

7.7 Managing mobility in cellular networks

7.8 Wireless and Mobility: Impact on higher-layer protocols

Wireless Link Characteristics

Differences from wired link …

- Decreased signal strength: radio signal attenuates significantly as it propagates (path loss)
- Interference from other sources: standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., cordless phones); devices (motors) generate EM noise
- Multipath propagation: radio signal reflects off objects, ground arriving at destination at slightly different times

… make communication across (even a point to point) wireless link much more “difficult” and …

… increases the bit error rate forcing the use of link-level ARQ protocols

Signal Loss

- Even when line-of-sight exists, signal attenuates with distance

- Path loss: attenuation undergone by electromagnetic wave in transit between transmitter and receiver

- Roughly proportional to $1/d^2$

Loss at 2.45 GHz

Distance (m)	Loss (dB)
100	80.2
200	86.2
500	94.2
1000	100.2

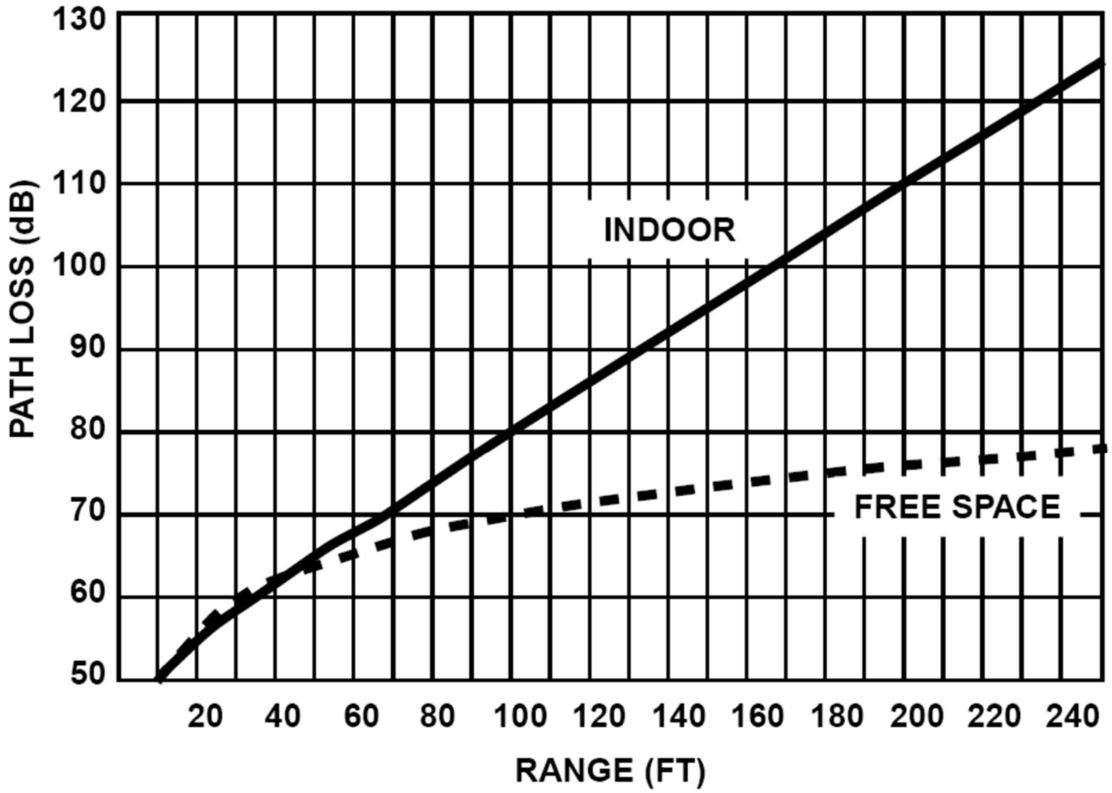
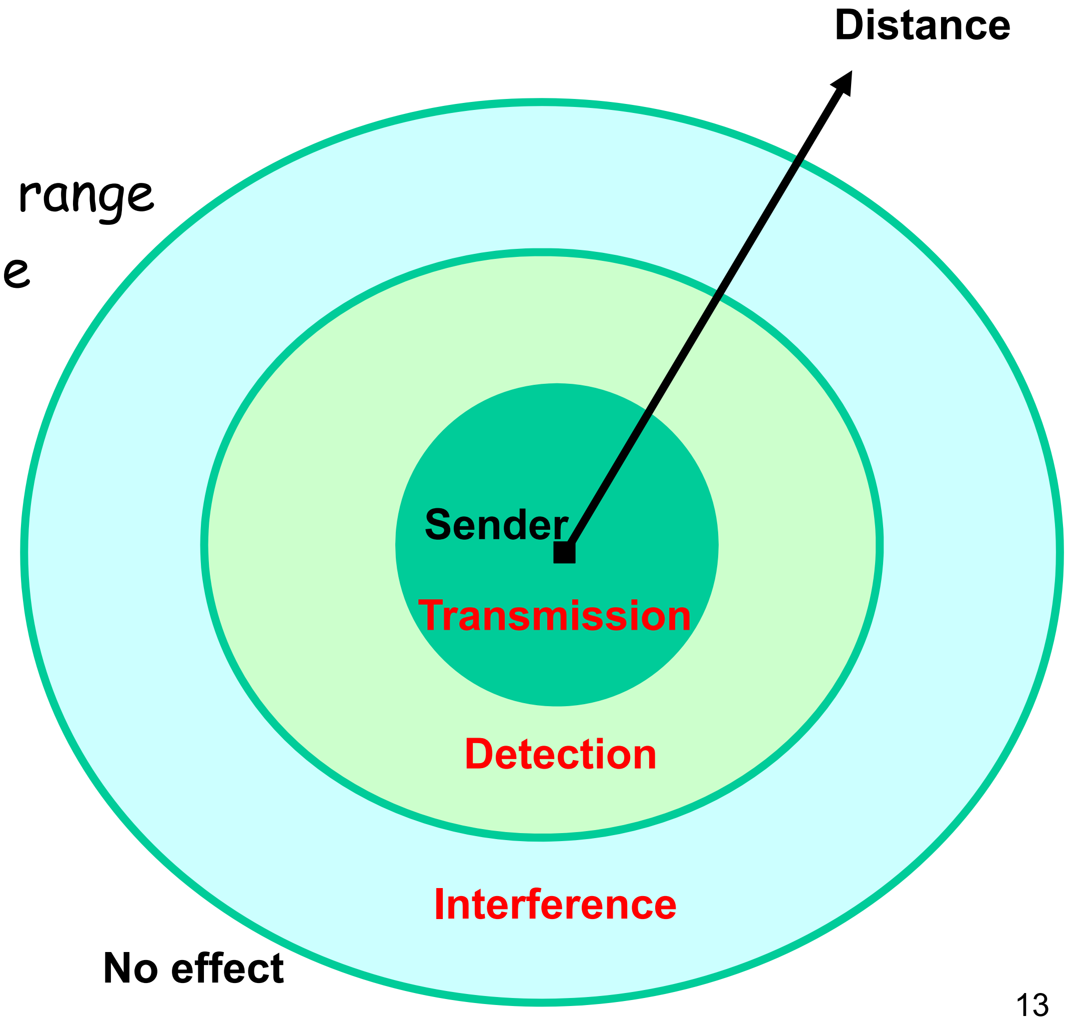


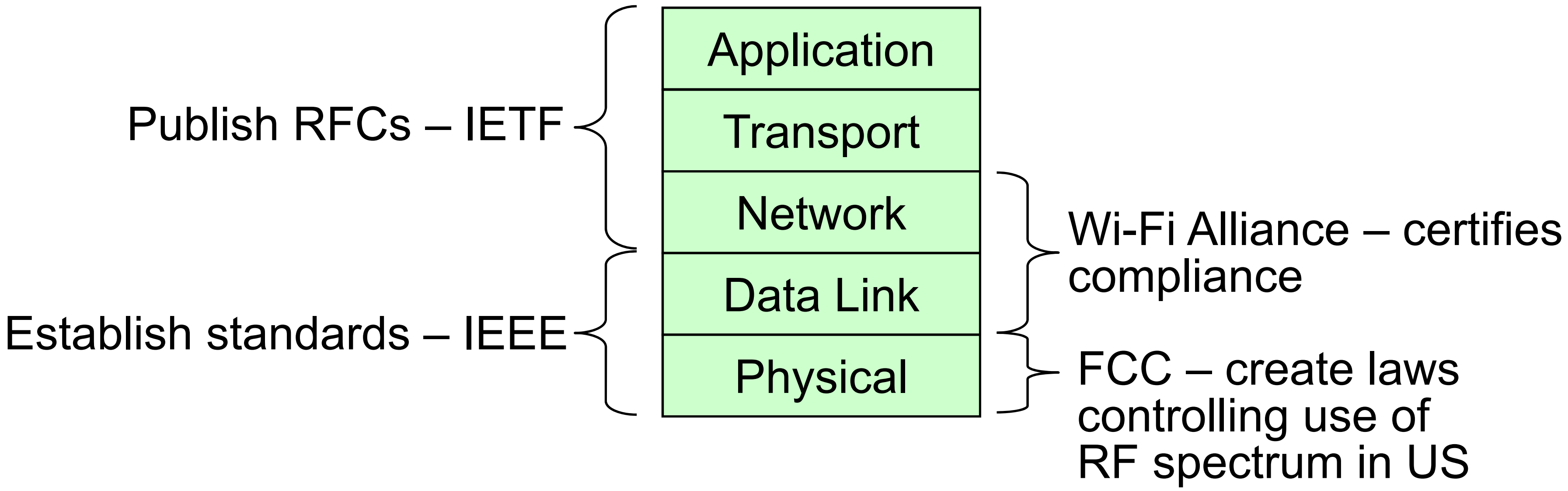
FIGURE 1. ESTIMATED INDOOR PROPAGATION LOSSES AT 2.4GHz

Interference from Other Sources

- Generally nodes use the same frequency
- Transmission range
  - Communication possible
  - Low error rate
- Detection (carrier sensing) range
  - Signal detection possible
  - No comm possible
  - Triggers carrier sense detection at receiver
- Interference range
  - Signal may not be detected
  - Signal adds to background noise



Standards Bodies Responsibilities



Application

Transport

Network

Data Link

Physical

Publish RFCs – IETF

Establish standards – IEEE

Wi-Fi Alliance – certifies compliance

FCC – create laws controlling use of RF spectrum in US

IETF – Internet Engineering Task Force
IEEE – Institute of Electrical and Electronics Engineers
FCC – Federal Communications Commission

Wi-Fi Alliance

- Wi-Fi → Wireless Fidelity

- Certifies interoperability of 802.11-based products
    - Non-profit organization founded in 1999
    - Over 600 member organizations
    - Develop universal specifications and follow through with rigorous testing and Wi-Fi certification of wireless devices
    - Certified the interoperability of more than 40,000 products

FCC Rules

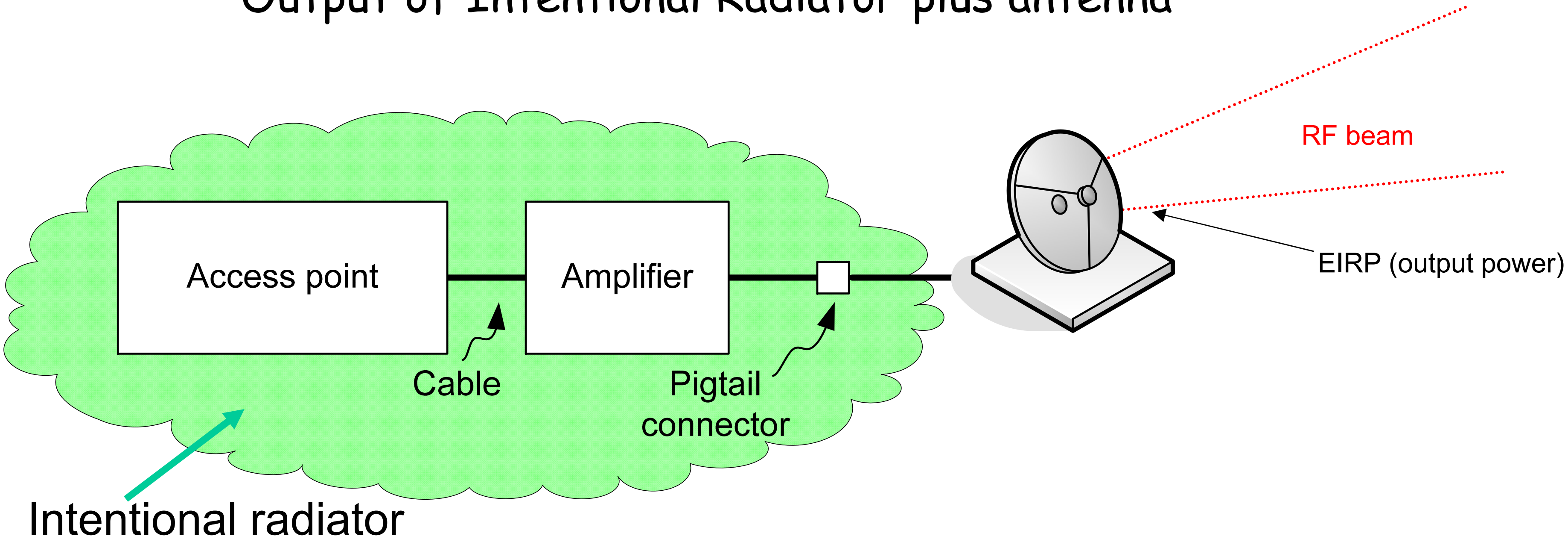
- Although the FCC does not require a license to operate in the ISM bands, you must still abide by certain limitations
  - Part 47 Code of Federal Regulations (CFR), Chapter 1, Section 15.247
    - TITLE 47—TELECOMMUNICATION
    - CHAPTER I--FEDERAL COMMUNICATIONS COMMISSION
    - PART 15--RADIO FREQUENCY DEVICES--Table of Contents
    - Subpart C--Intentional Radiators
    - Sec. 15.247 Operation within the bands
      - 902-928 MHz,
      - 2400-2483.5 MHz
      - 5725-5850 MHz

- Point-to-Multipoint (PtMP) communications (primarily indoor)
  - Maximum EIRP for indoor applications < 1 watt (30 dBm)

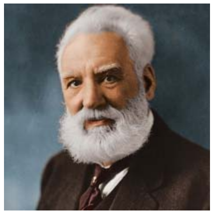
- Point-to-Point (PtP) systems (primarily outdoor)
  - Maximum EIRP for outdoor applications < 4 watts (36 dBm)

Intentional Radiator and EIRP

- Intentional Radiator
  - Device that intentionally generates and emits RF energy
  - Includes radio, cables, and connectors
  - Does not include antenna
- Equivalent Isotropically Radiated Power (EIRP)
  - Power that is radiated into free space
    - Output of Intentional Radiator plus antenna



dB (One Tenth of a Bel)



- decibels (dB) are measured as the ratio of two power levels
  - Based on a logarithmic scale

$$N_{dB} = 10 \log_{10} \frac{P_1}{P_2}$$

- Power and gain are measured in dB
- Units of measure for wireless systems
  - Watts – basic unit of power
  - Milliwatt (mW) – absolute standard of measurement
  - dBm – decibel milliwatt
    - Power relative to 1 milliwatt (i.e., 0 dBm = 1 mW)
- dBi – decibel isotropic
  - Used for antennas
  - Power relative to an isotropic radiator (gain = 1)

dB Math

$$N_{dB} = 10 \log_{10} \frac{Pout}{Pin}$$

- -3 dB = half power

$$10 \log_{10} \frac{50\,mW}{100\,mW} = 10 \log_{10} 0.5 = 10 * (-0.301) = -3\,dB$$

- +3 dB = double power

$$10 \log_{10} \frac{100\,mW}{50\,mW} = 10 \log_{10} 2 = 10 * (0.301) = 3\,dB$$

- -10 dB = one tenth power

$$10 \log_{10} \frac{10\,mW}{100\,mW} = 10 \log_{10} 0.1 = 10 * (-1) = -10\,dB$$

- +10 dB = ten times power

$$10 \log_{10} \frac{100\,mW}{10\,mW} = 10 \log_{10} 10 = 10 * (1) = 10\,dB$$

dB Math

$$N_{dB} = 10 \log_{10} \frac{Pout}{Pin}$$

dBm	**mW**	**dBm**	**mW**
0 dBm	1 mW	0 dBm	1 mW
1 dBm	1.25 mW	-1 dBm	0.8 mW
3 dBm	2 mW	-3 dBm	0.5 mW
6 dBm	4 mW	-6 dBm	0.25 mW
7 dBm	5 mW	-7 dBm	0.20 mW
10 dBm	10 mW	-10 dBm	0.10 mW
12 dBm	16 mW	-12 dBm	0.06 mW
13 dBm	20 mW	-13 dBm	0.05 mW
15 dBm	32 mW	-15 dBm	0.03 mW
17 dBm	50 mW	-17 dBm	0.02 mW
20 dBm	100 mW	-20 dBm	0.01 mW
30 dBm	1000 mW (1 W)	-30 dBm	0.001 mW
40 dBm	10,000 mW (10 W)	-40 dBm	0.0001 mW

Increase	Factor	Decrease	Factor
0 dB	1 x (same)	0 dB	1 x (same)
1 dB	1.25 x	-1 dB	0.8 x
3 dB	2 x	-3 dB	0.5 x
6 dB	4 x	-6 dB	0.25 x
10 dB	10 x	-10 dB	0.10 x
12 dB	16 x	-12 dB	0.06 x
20 dB	100 x	-20 dB	0.01 x
30 dB	1000 x	-30 dB	0.001 x
40 dB	10,000 x	-40 dB	0.0001 x

$$10^{\frac{dB}{10}} = mW$$

$$10^{\frac{dB}{10}} = factor$$

dB Math Examples

$$N_{dB} = 10 \log_{10} \frac{Pout}{Pin}$$

- We will transmit the following power from an intentional radiator through an antenna or cable
  - Calculate the EIRP

- 20 mW thru a -3 dB cable
  - 20 mW * 0.5 = 10 mW

- 20 mW thru a +3 dBi antenna
  - 20 mW * 2 = 40 mW

- 13 dBm thru a -10 dB cable
  - 20 mW * 0.1 = 2 mW OR 13 dBm – 10 dB = 3 dBm = 2 mW

- 13 dBm thru a +10 dBi antenna
  - 20 mW * 10 = 200 mW OR 13 dBm + 10 dB = 23 dBm = 200 mW

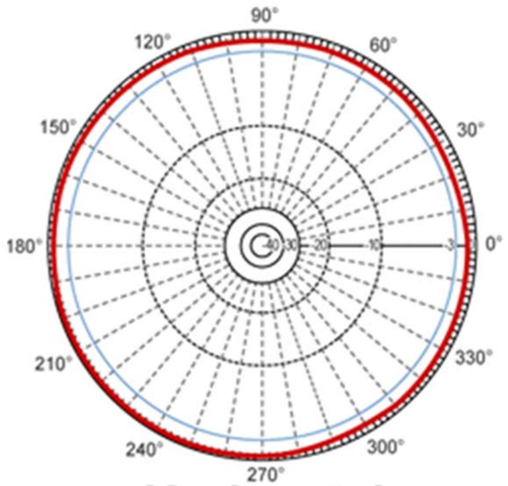
dB Math - You Try

$$N_{dB} = 10 \log_{10} \frac{Pout}{Pin}$$

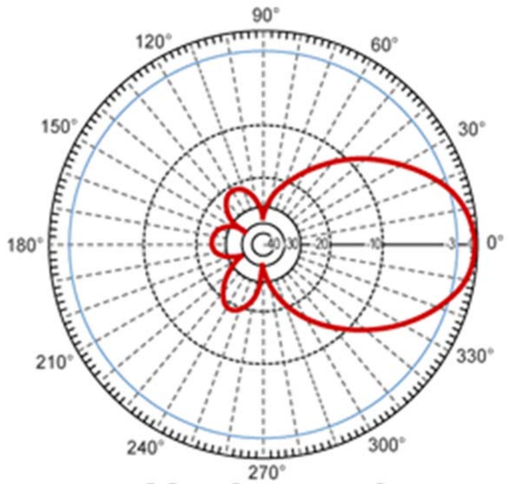
- 20 dBm radio + 3 dBi antenna
- 16 dBm radio + 9 dBi antenna
- 16 dBm radio + 8 dBi antenna + 2 cable connectors
  - Each connector experiences 1 dB loss
- 300 mW radio + 10 dBi antenna
- 20 dBm radio + 23 dBi antenna

Antennas

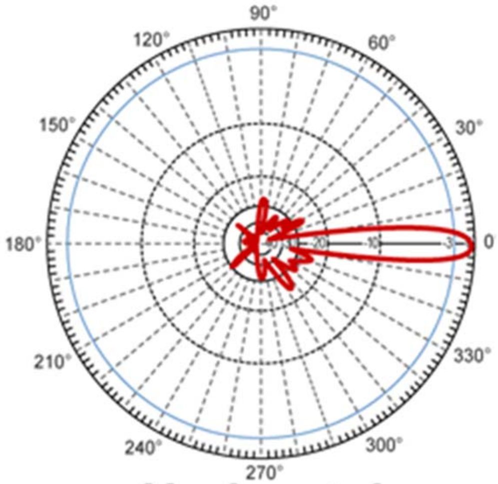
- An antenna is a passive device that focuses radiation energy by virtue of its shape
  - Antenna does not condition or amplify the signal
  - It simply redistributes energy in some directions better than others
- Amount of gain depends on type of antenna



Horizontal



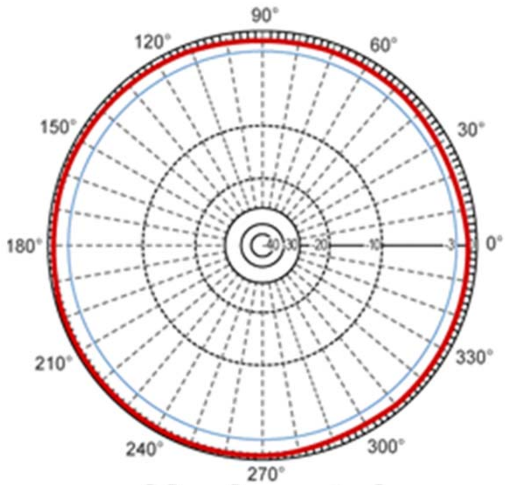
Horizontal



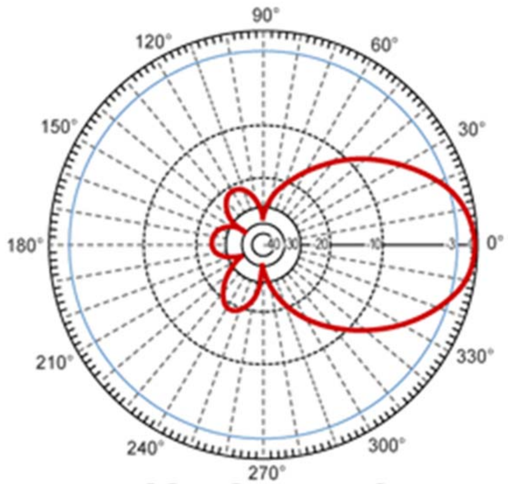
Horizontal

Antennas

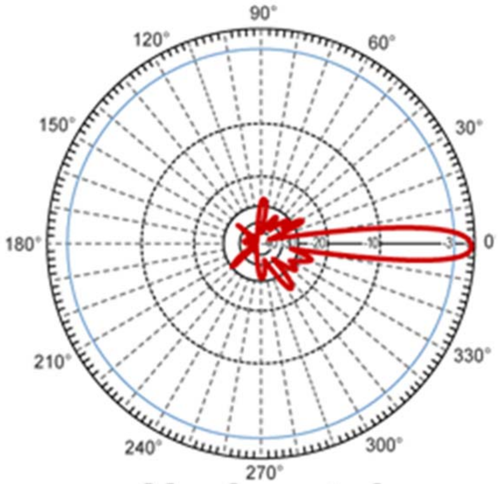
- ❑ Think of an adjustable flashlight
  - ❖ A wider beam does not project as much light at a distance as does a narrow, focused beam
- ❑ Beamwidth is the measure of beam focus
  - ❖ Omni-directional antenna = 360 degrees
    - Antenna on the left is an example
  - ❖ Antenna to the right is highly focused



Horizontal



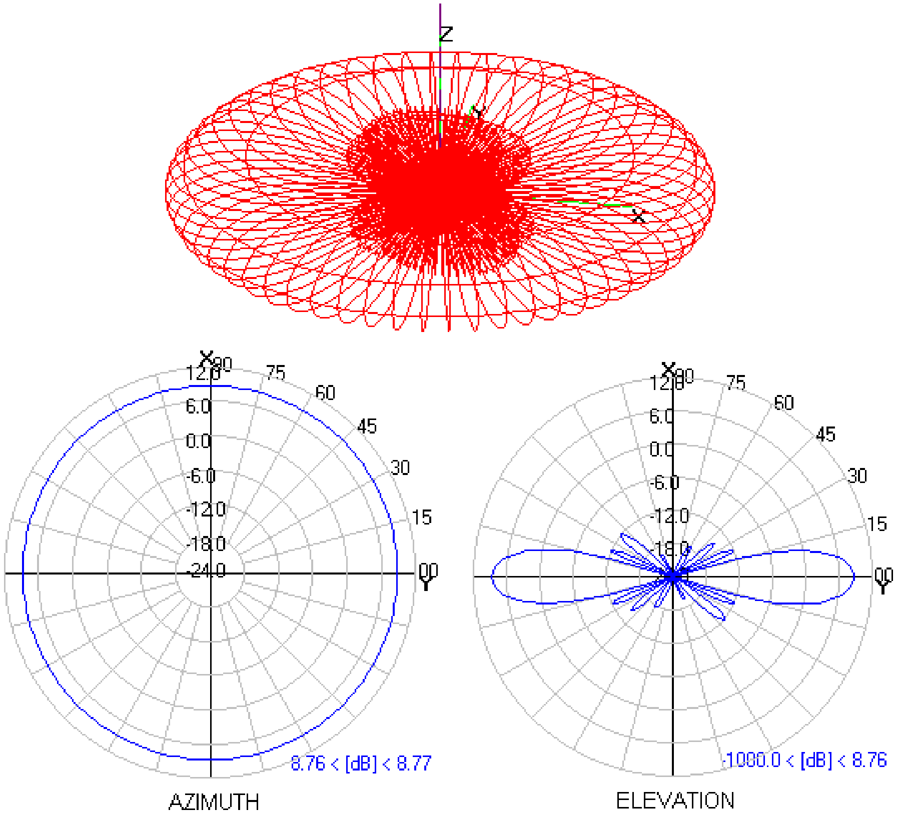
Horizontal



Horizontal

Omni-directional Antennas (Dipole)

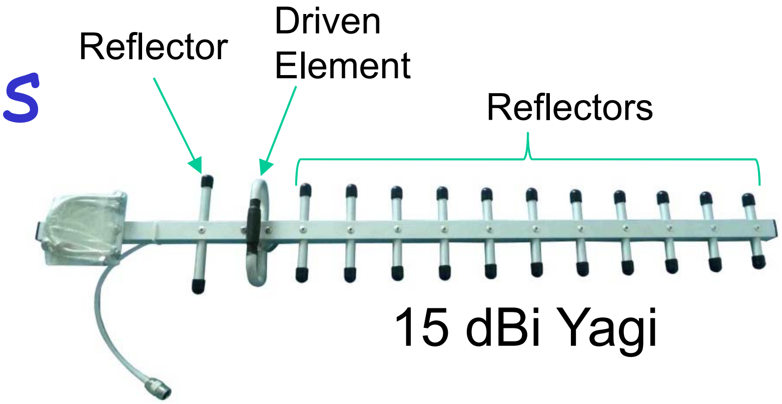
- Most common type of WLAN antenna
- Radiates equally well in all directions horizontally
- Useful for large coverage areas



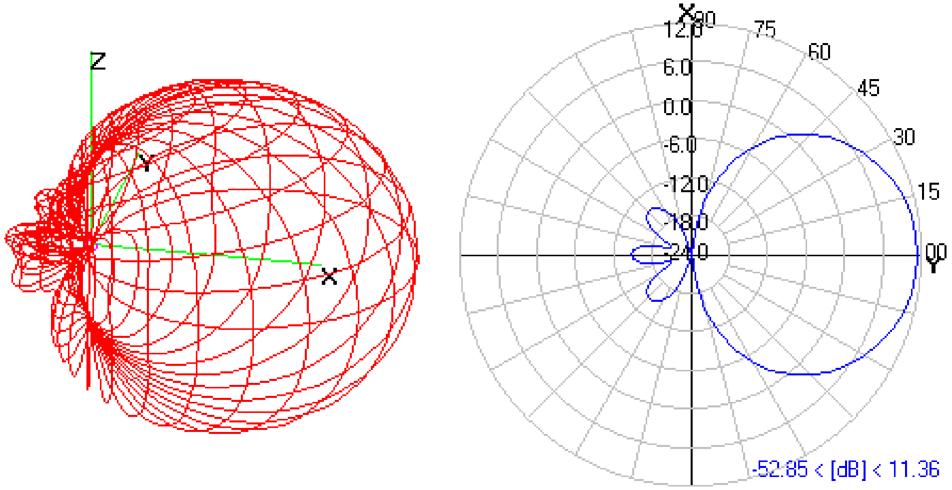
9 dBi Omni

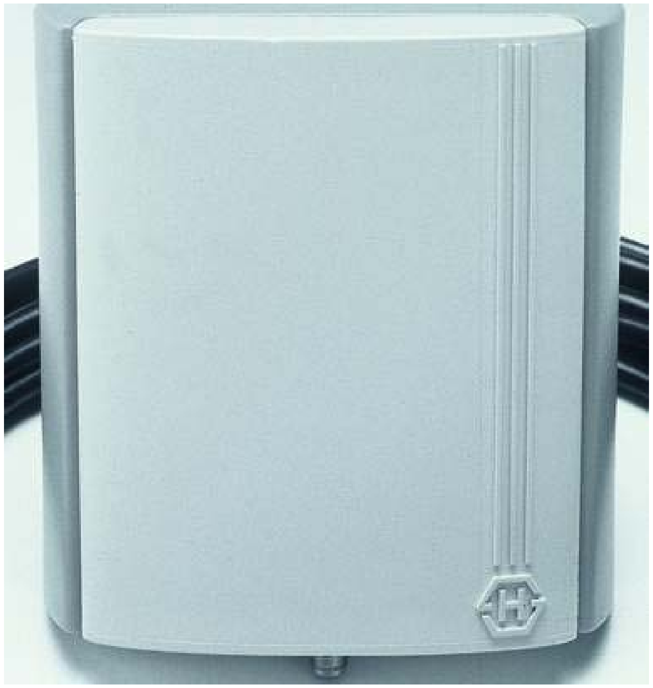
Semi-directional Antennas

- Concentrate energy in one direction
- Yagi, Panel
- Useful for point-to-point connections



15 dBi Yagi



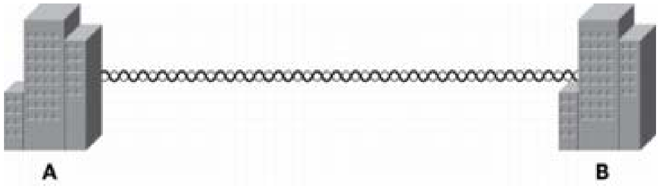


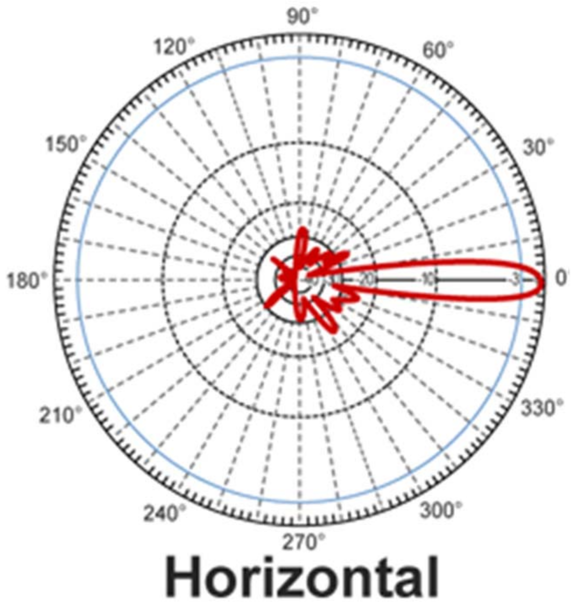
8 dBi Uni (Panel)

Highly-directional Antennas

21 dBi antenna

- Useful for point-to-point communication over long distances

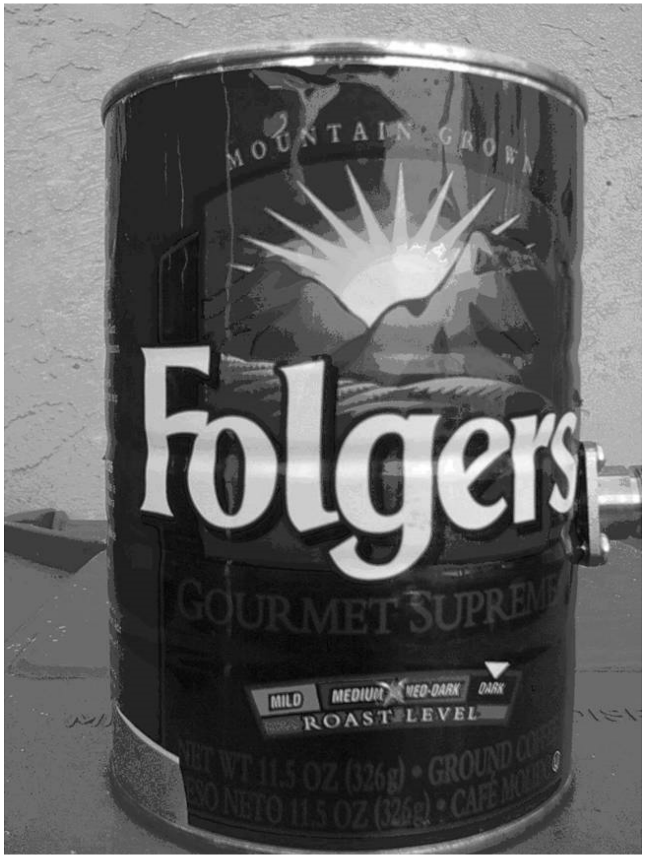




24″ x 36″ Mesh Grid Antenna (21 dBi)

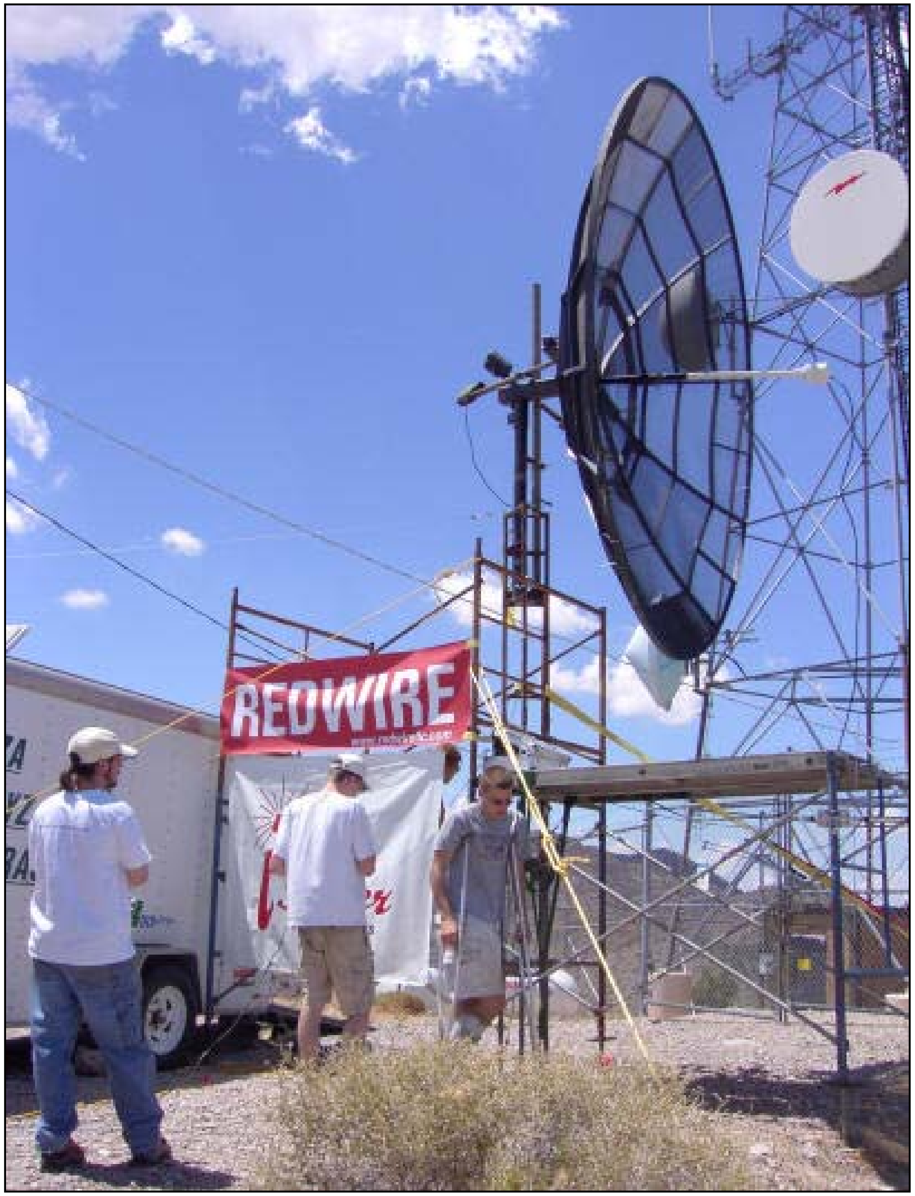
Other Antennas

- Cantennas



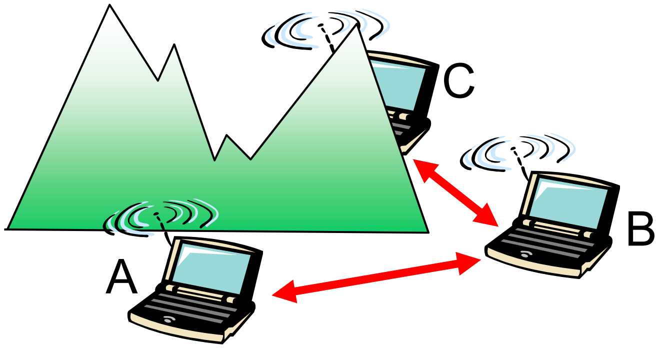
DEFCON WiFi Shootout 2005

- Team iFiber Redwire established an unamplified 802.11b link at 124.9 miles for 3 hours!
  - Used 12′ dish on Mt. Potosi near Las Vegas and a 10′ dish on a mountain near St. George Utah.
  - Used 300 mW PCMCIA cards
  - All team members were licensed amateur radio operators
    - Allowed higher power
  - Made 11,000 pings and set up a VNC connection



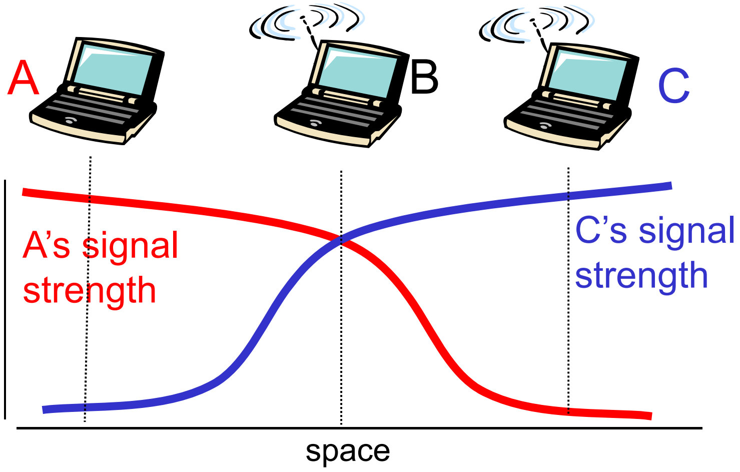
Wireless Network Characteristics

- 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 cannot hear each other means A, C unaware of their interference at B



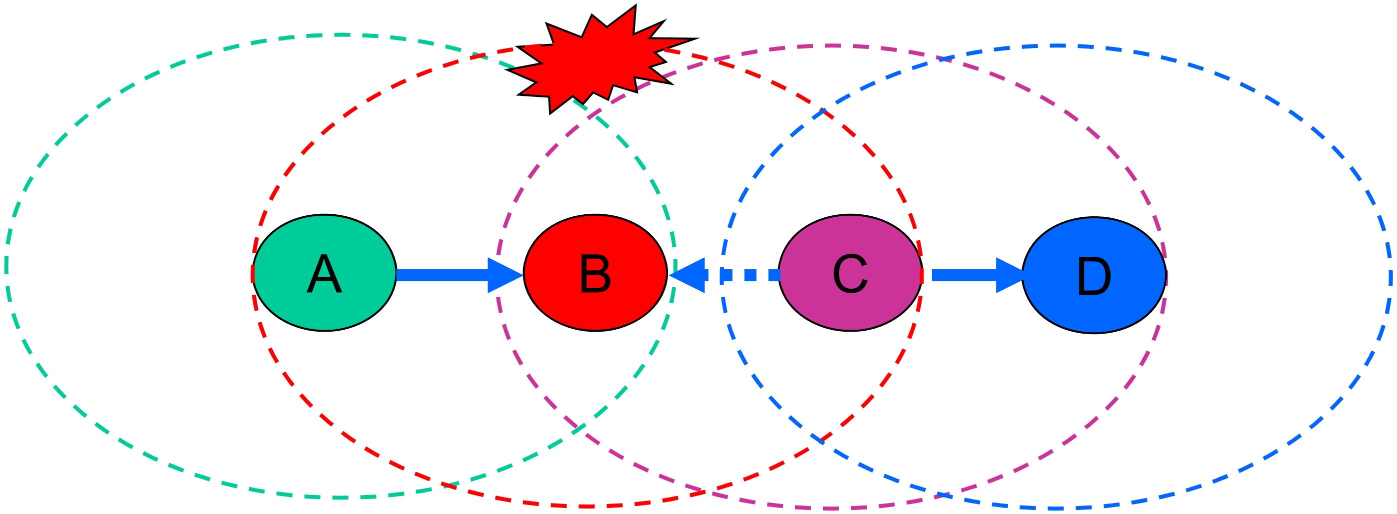
Signal attenuation:

- B, A hear each other
- B, C hear each other
- A, C cannot hear each other interfering at B

Unlike wired networks, wireless network nodes do not hear all transmissions

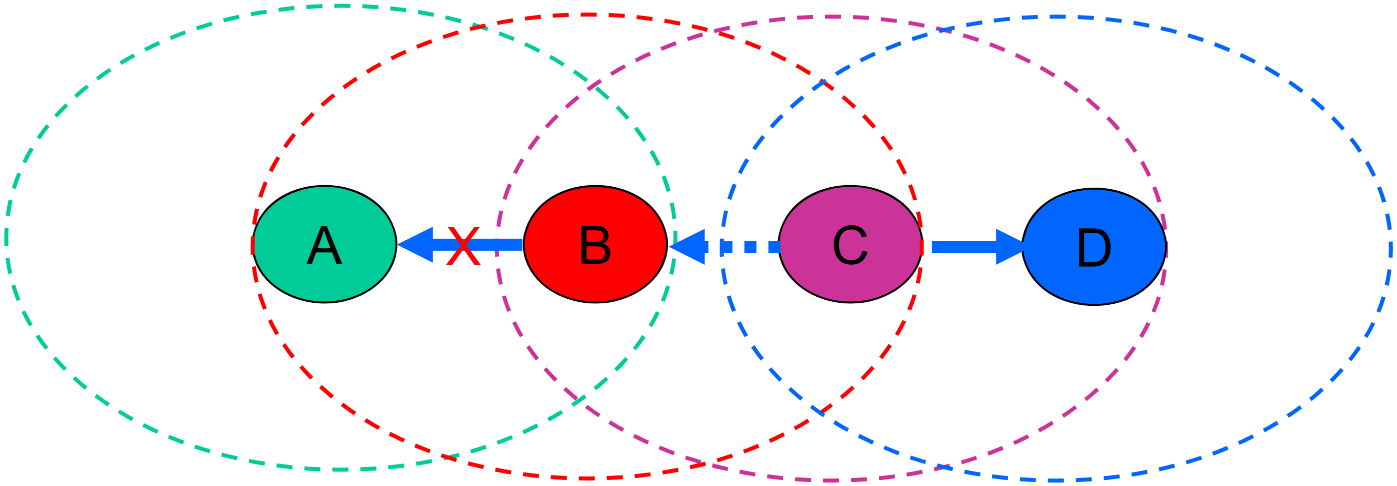
Hidden Terminal Problem

- Interference manifests itself at the receiver!!
- Node B can communicate with A and C
- A and C cannot hear each other
- When A transmits to B, C cannot detect the transmission using the carrier sense mechanism
- If C transmits to D, collision will occur at B

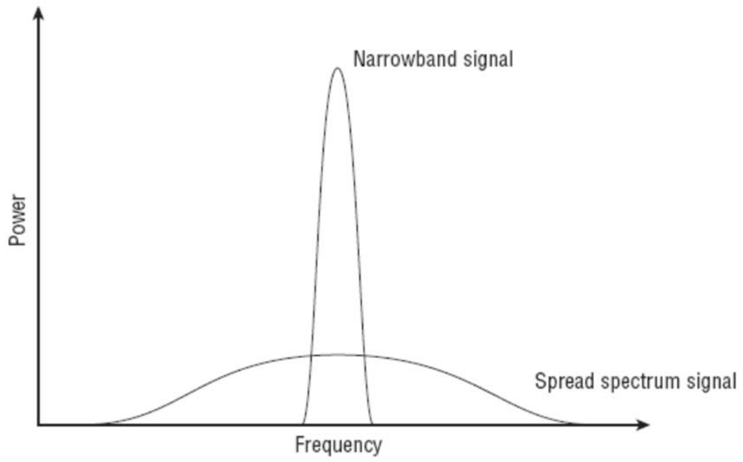


Exposed Terminal Problem

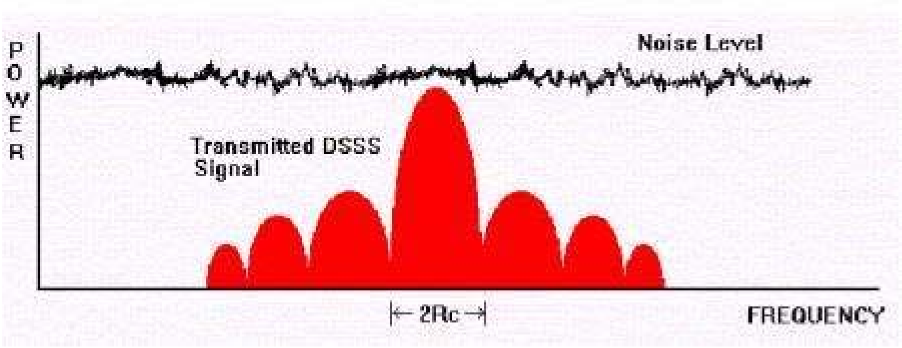
- Once again, can only hear nearest neighbor
  - Node C can communicate with B and D
  - Node B can communicate with A and C
  - Node A cannot hear C
  - Node D cannot hear B
- When C transmits to D, B detects the transmission using the carrier sense mechanism and does not transmit to A, even though the transmission will not cause collision



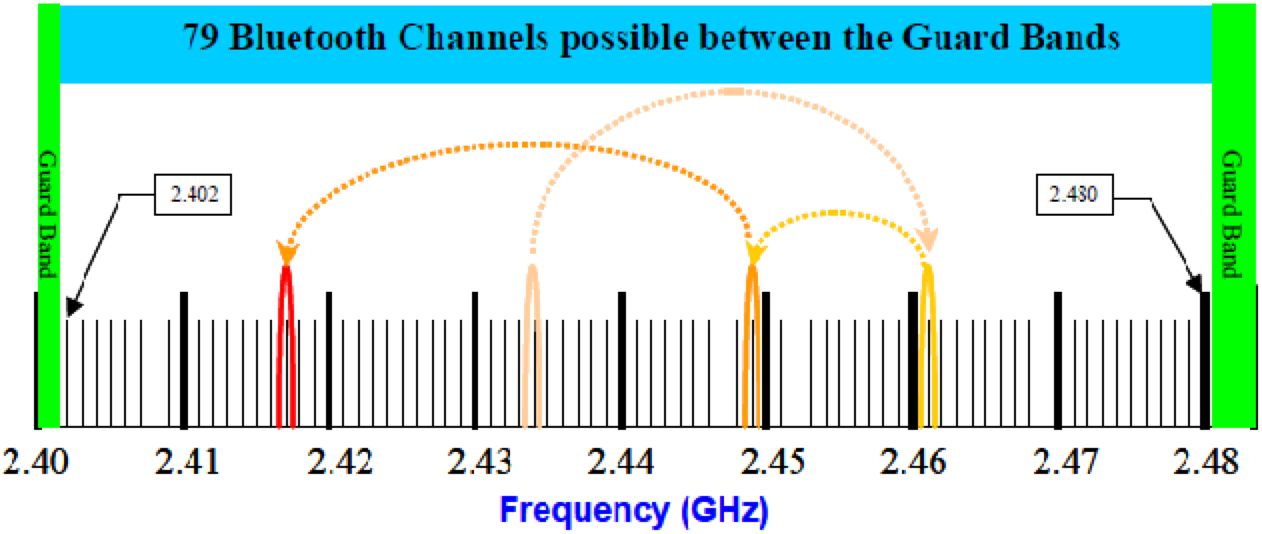
Spread Spectrum



- Spread spectrum signals are distributed over a wide range of frequencies and then collected back at the receiver
  - These wideband signals are noise-like and hence difficult to detect or interfere with
- Initially adopted in military applications
  - Resistance to jamming
  - Difficulty of interception
- More recently adopted in commercial wireless communications
- Two types
  - Frequency hopping (FHSS)
  - Direct sequence (DSSS)



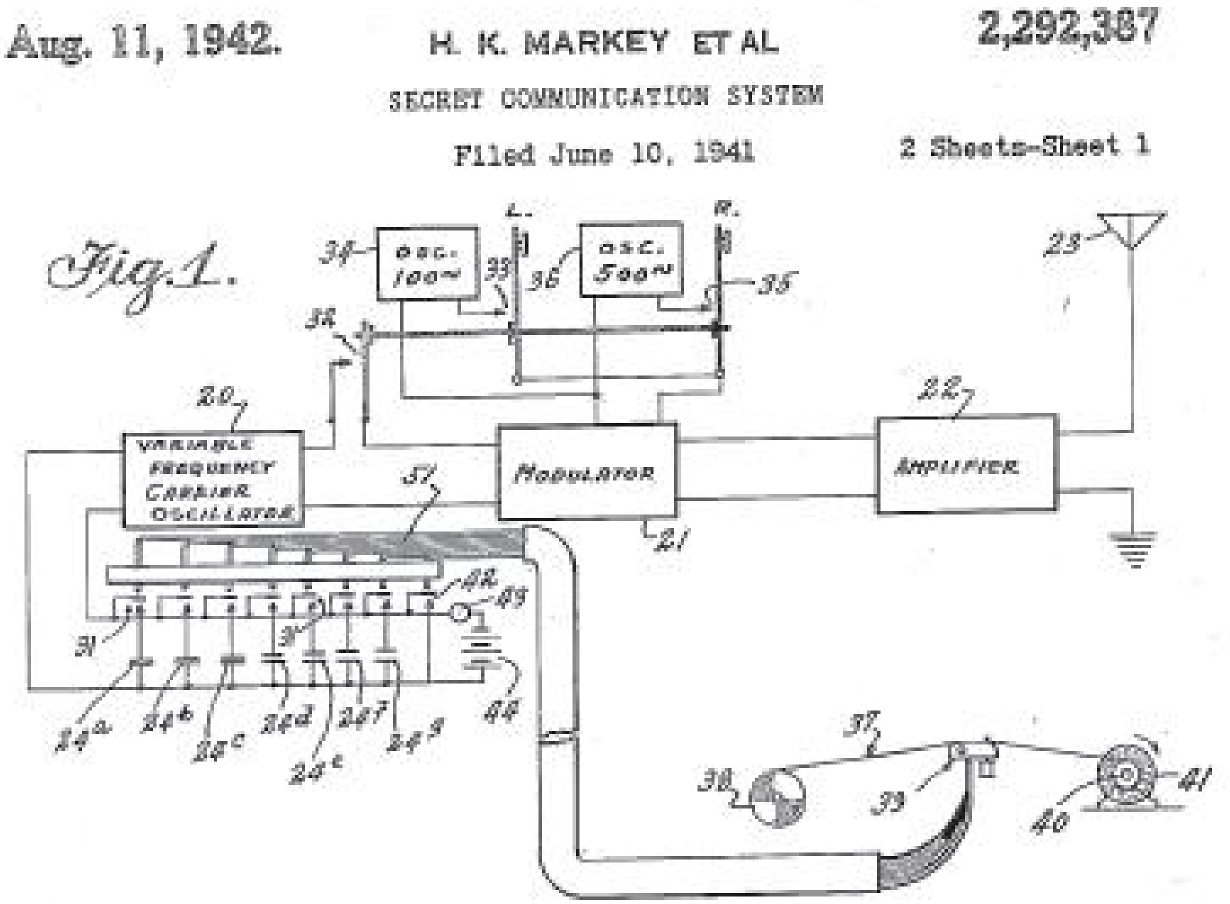
Frequency Hopping



- Transmitter and receiver "hop" among different frequency channels according to a pre-established hopping sequence
  - Time at each channel is the dwell time, t_D
- Total available bandwidth divided into smaller bandwidth channels (plus guard bands)
- Examples:
  - GSM (**G**lobal **S**ystem for **M**obile Communications)
  - Bluetooth
  - 802.11 Frequency Hopping PHY uses 79 non-overlapping frequency channels with 1 MHz channel spacing with hop times ~ 400 ms

Frequency Hopping Genesis

- Australian actress Hedy Lamarr (born Hedwig Eva Maria Kiesler and aka H. K. Markey) holds a patent for Frequency Hopping along with composer George Antheil



Aug. 11, 1942. H. K. MARKEY ET AL 2,292,387

SECRET COMMUNICATION SYSTEM

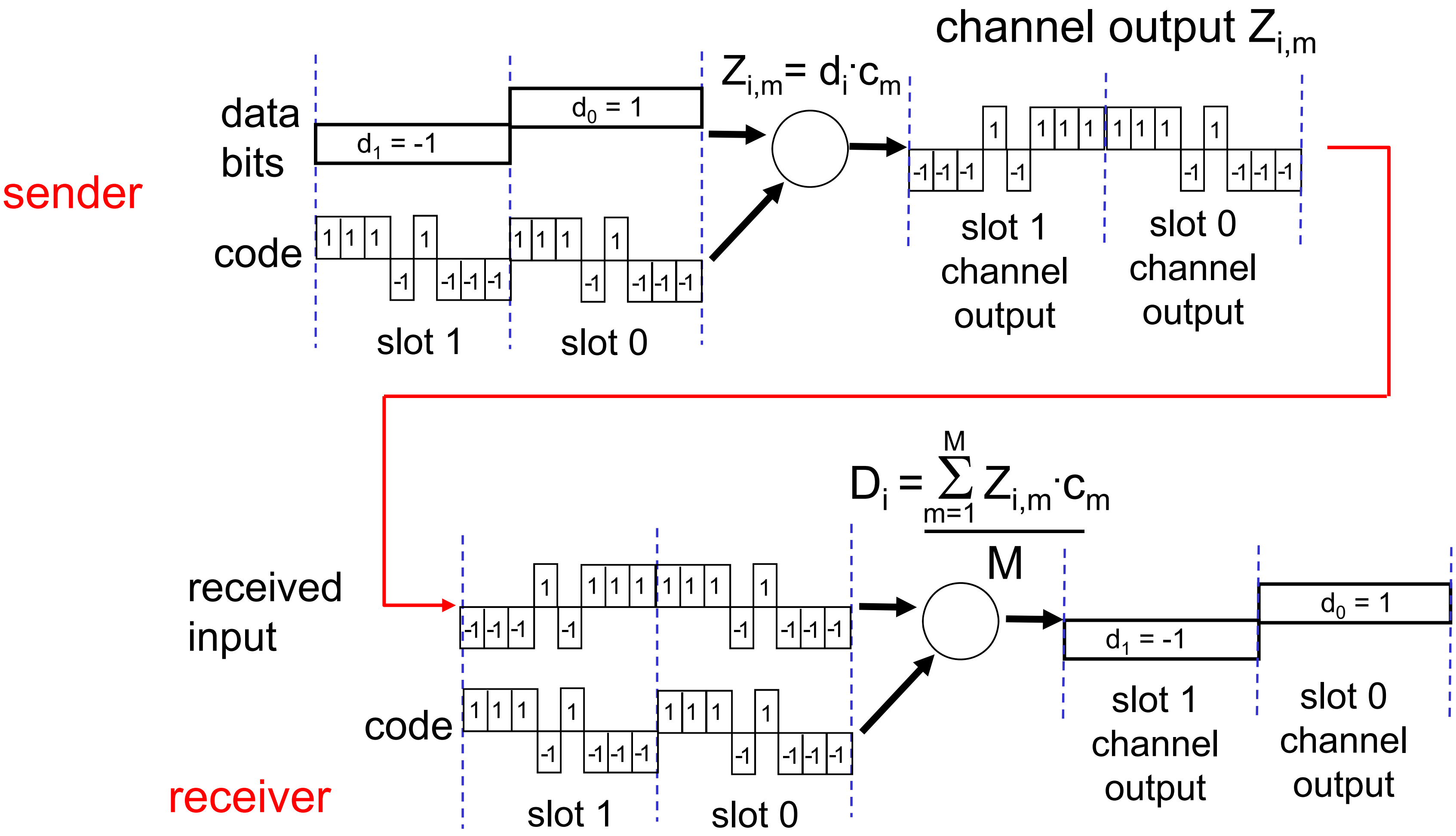
Filed June 10, 1941 2 Sheets-Sheet 1

Direct Sequence
Code Division Multiple Access (CDMA)

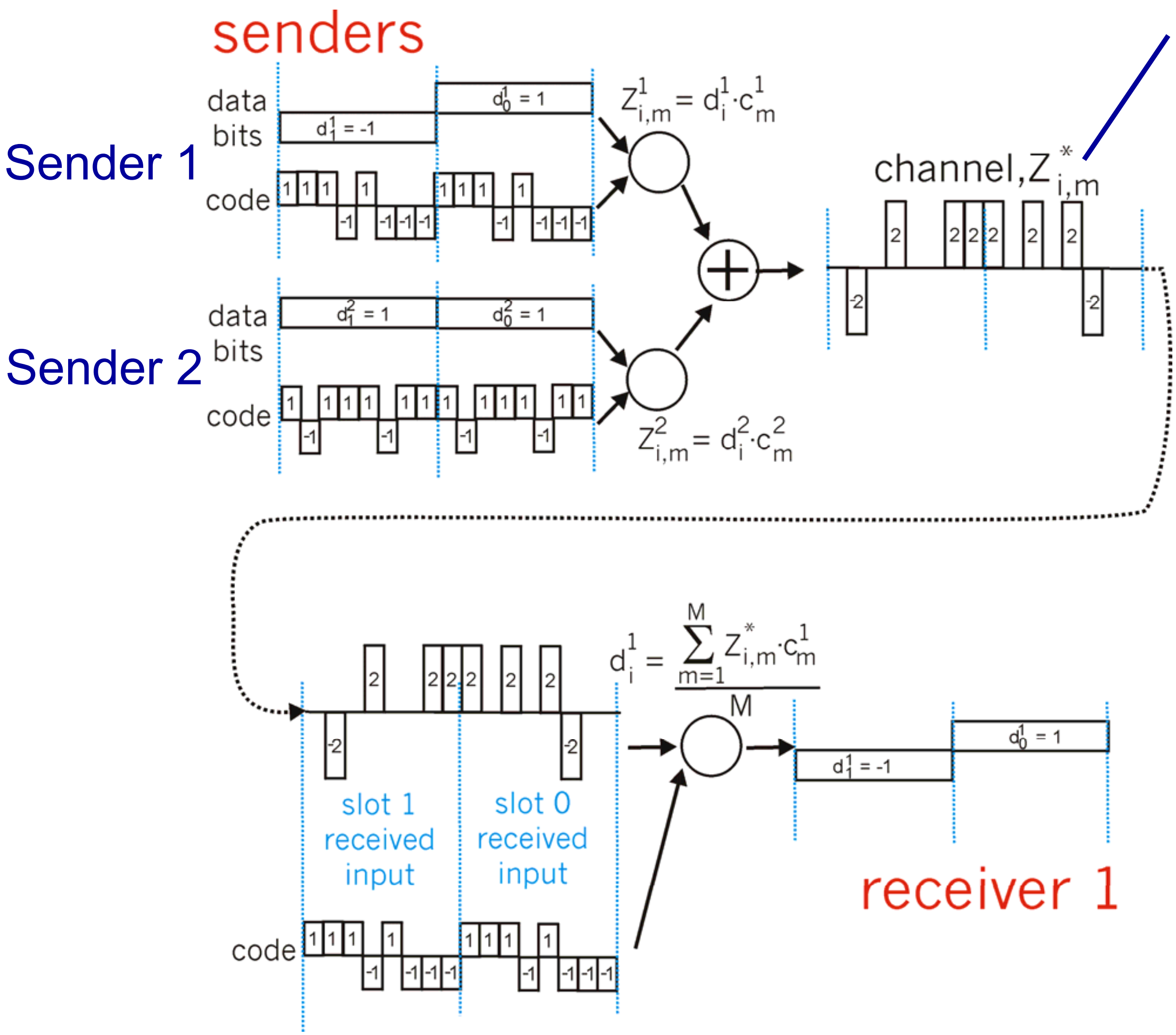
- Used in several wireless broadcast channel standards
  - Cellular, satellite, WLAN
- Unique "code" assigned to each set of users → code set partitioning
  - Code is a pseudo-random sequence of 1 and –1 values
    - Code resembles white noise → pseudo-noise (PN) code
  - All users share same frequency, but each user set has own "chipping" sequence (i.e., code) to encode data
  - Allows multiple user sets to "coexist" and transmit simultaneously with minimal interference (if codes are "orthogonal")
- Examples
  - GPS
  - IEEE 802.11b – but only uses one pre-defined PN code
  - Cordless phones
  - Radio-controlled models

CDMA Encode/Decode

- These two slides demonstrate basic operation
- Actual implementation is slightly different than shown



CDMA: Two-sender Interference



Channel (free space) “sums” together transmissions by sender 1 and 2

Using same code as sender 1, receiver 1 recovers sender 1’s original data from summed channel data!

Direct Sequence Spread Spectrum (DSSS)

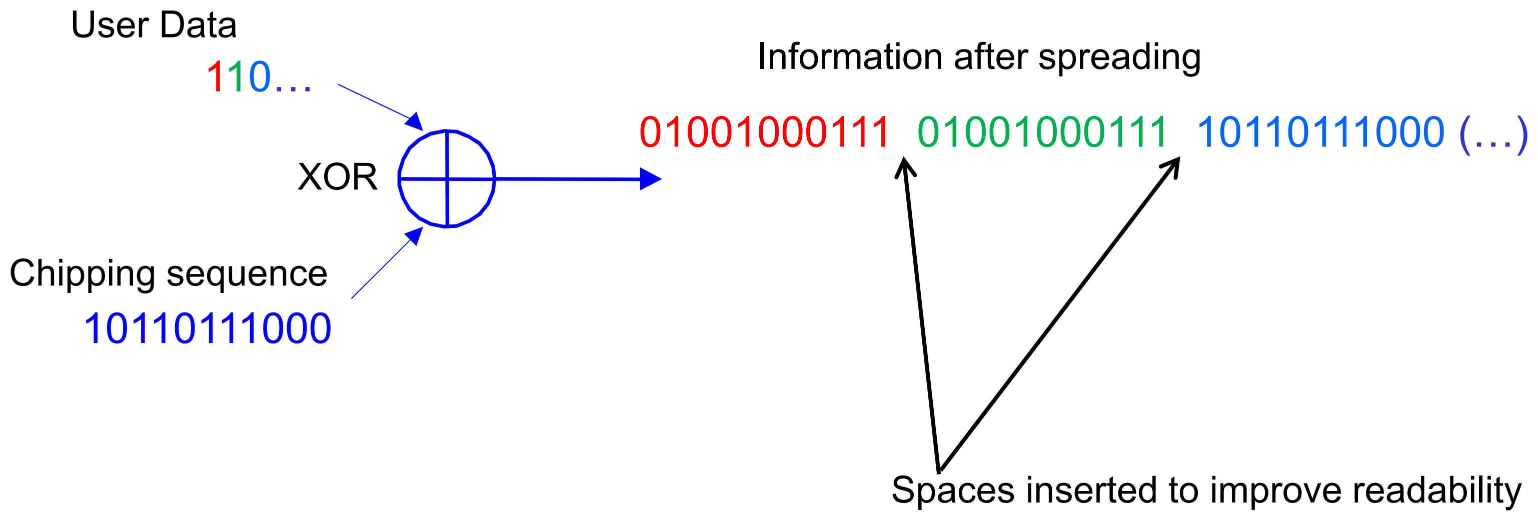
- ❑ Actual implementation uses XOR operation instead of multiplication
- ❑ User bit stream is XORed with a chipping sequence

Spreading factor

$$s = \frac{t_b}{t_c}$$

Bit period

Chip period



User Data

110…

XOR

Chipping sequence

10110111000

Information after spreading

01001000111 01001000111 10110111000 (…)

Spaces inserted to improve readability

DSSS Spreading Factor

- Spreading factor determines the bandwidth of the signal to be transmitted
  - Order of 10 to 100 for commercial applications
  - Up to 10,000 for military applications

- IEEE 802.11 uses 11 chip Barker code
  - 10110111000

DSSS versus FHSS

- Frequency hopping spread spectrum
  - Use only a portion of the bandwidth at any given time
  - Implementation of FHSS is simpler than DSSS

- Direct sequence spread spectrum
  - More resistant to fading (attenuation) and multipath
  - Harder to detect and intercept than FHSS
  - Opportunities for CDMA and adaptive communication schemes

Chapter 7 Outline

7.1 Introduction

Wireless

7.2 Wireless links, characteristics
- CDMA

7.3 IEEE 802.11 wireless LANs ("Wi-Fi")

7.4 Cellular Internet Access
- Architecture
- Standards (e.g., GSM)

Mobility

7.5 Principles: addressing and routing to mobile users

7.6 Mobile IP

7.7 Managing mobility in cellular networks

7.8 Wireless and Mobility: Impact on higher-layer protocols

IEEE 802.11 Wireless LAN

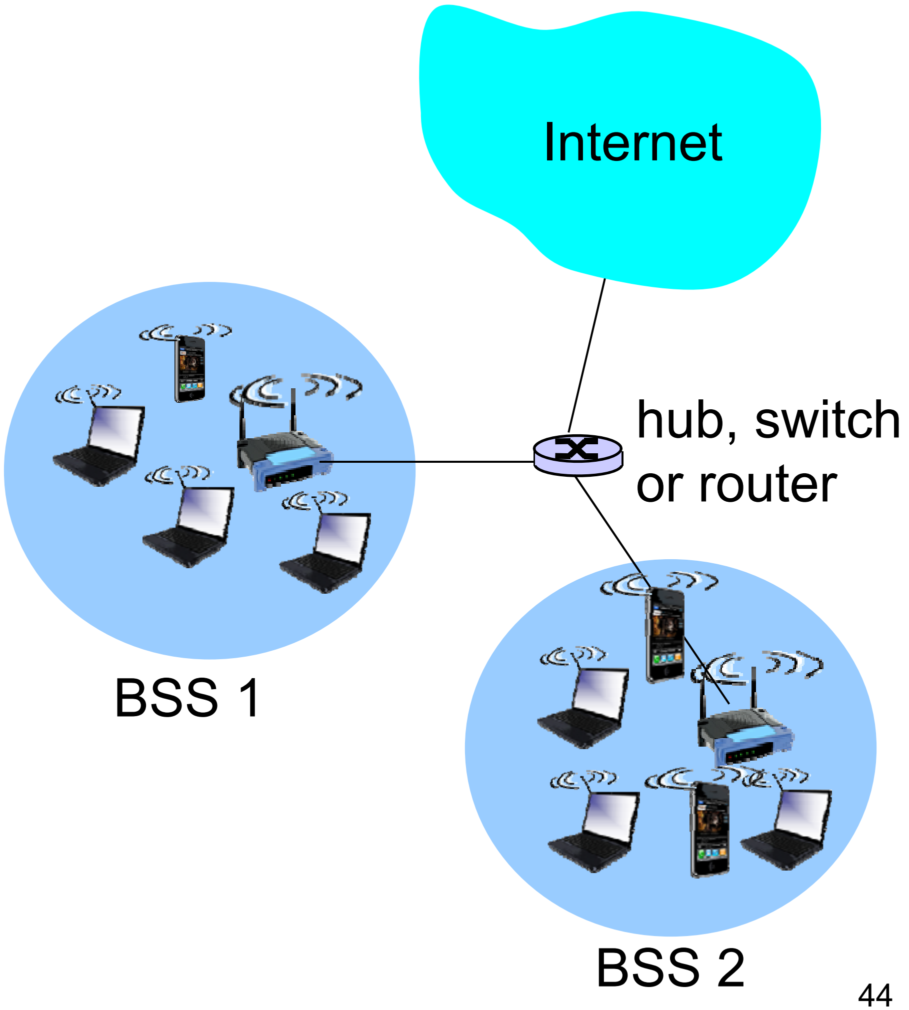
- 802.11b (1999 - DSSS)
  - 2.4 or 5 GHz
  - Up to 11 Mbps
- 802.11a (1999 - OFDM)
  - 5 GHz
  - Up to 54 Mbps
- 802.11g (2003 - OFDM)
  - 2.4 or 5 GHz
  - Up to 54 Mbps
- 802.11n (2009 - OFDM)
  - MIMO – 4 data streams
  - 2.4 or 5 GHz
  - Up to 200 Mbps
- 802.11ac (2013 - OFDM)
  - MIMO – 8 data streams
  - 5 GHz
  - Up to 866 Mbps

- IEEE Std 802.11™-2012 → 2,793 pages ☺
- All use CSMA/CA for multiple access
- All have base-station and ad-hoc network versions

OFDM - Orthogonal frequency-division multiplexing
MIMO - Multiple-Input and Multiple-Output

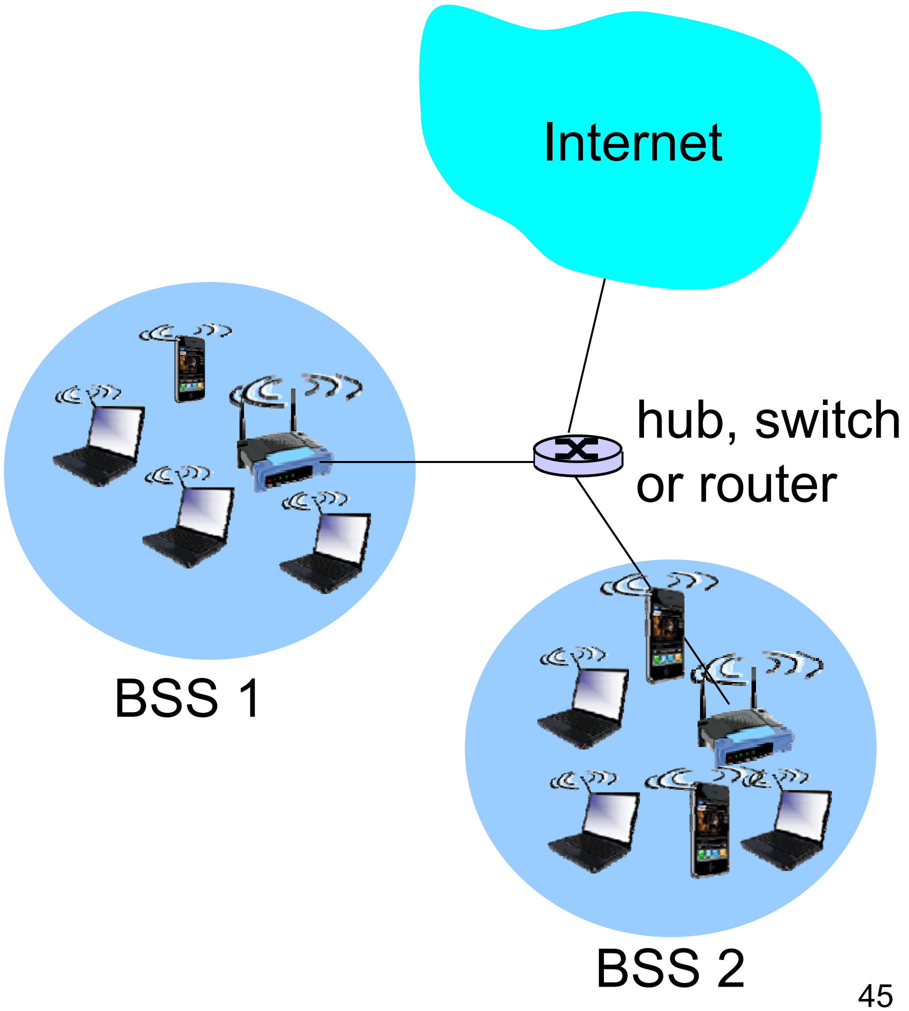
IEEE 802.11 Architecture

- 802.11 networks consist of four major physical components
  - Access Points
  - Wireless Medium
  - Stations
  - Distribution System



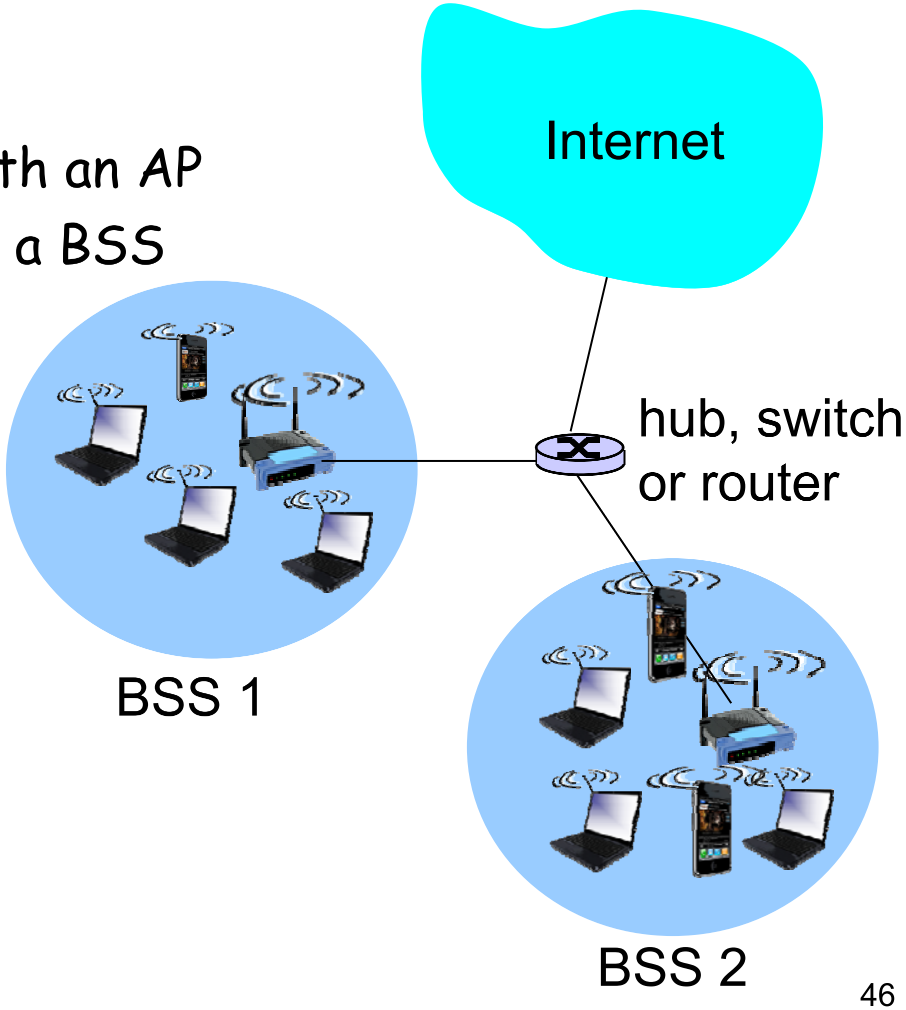
Distribution System (DS)

- Logical component of 802.11 used to forward frames to destination
  - Combination of bridging engine and DS medium (e.g., backbone network)
- 802.11 does not specify a particular technology for DS
  - Typically Ethernet
  - Could also let APs communicate wirelessly to form a DS
    - Wireless DS (WDS)



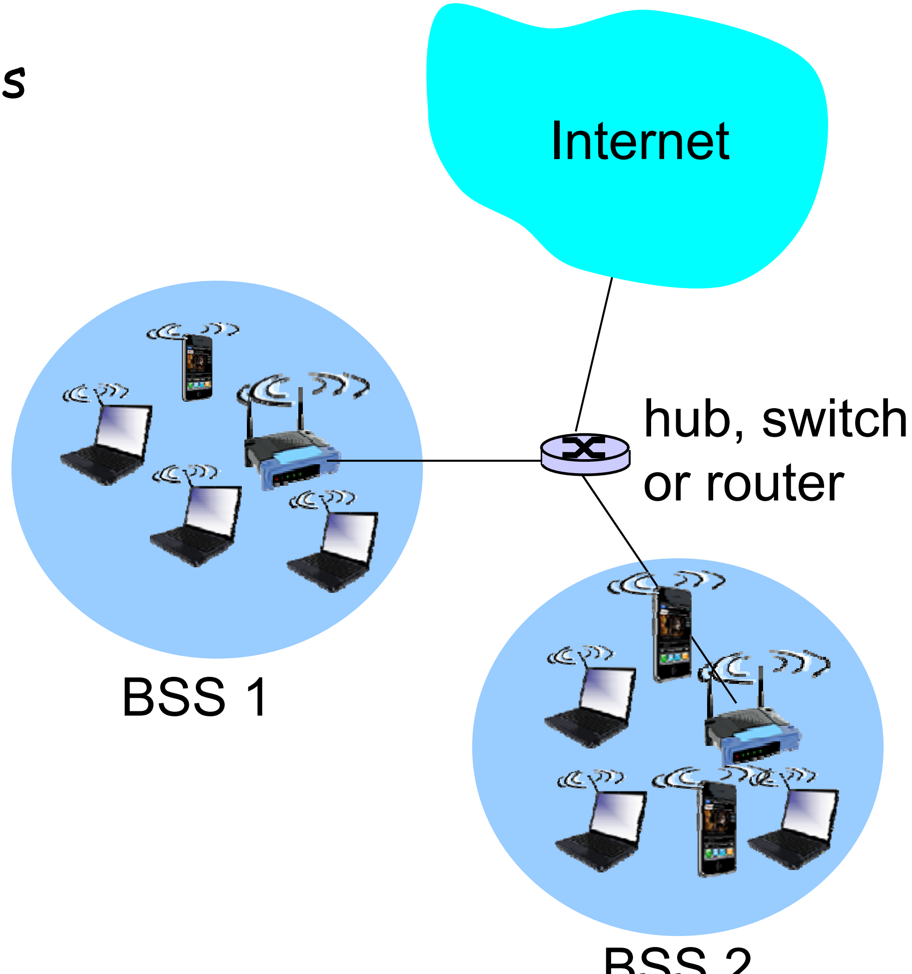
Basic Service Set (BSS)

- Basic building block of 802.11 network
  - Each AP has a service set identifier (BSSID)
    - Typically MAC address of AP's wireless interface
- Stations associate themselves with an AP
  - AP + associated stations form a BSS
- BSSs come in two flavors
  - Infrastructure BSS
    - Wireless hosts communicate only with AP
  - Independent BSS (IBSS)
    - Ad hoc mode: hosts only



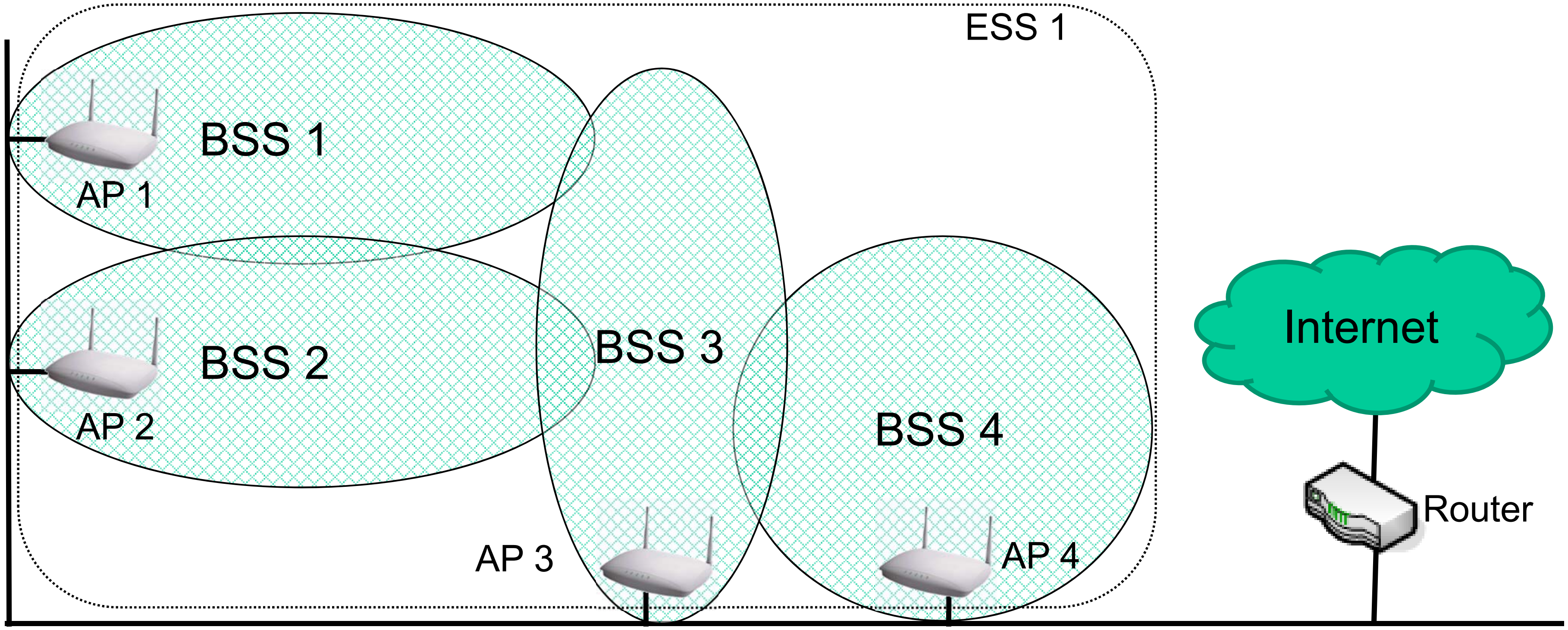
Infrastructure Mode

- Requires some infrastructure (access points)
- Access point is responsible for forwarding messages, control and management functions
- Access point acts as a bridge between wireline and wireless networks
- No direct communication between hosts
- Applications
  - Office-wide WLANs
  - Hotspots



Extended Service Set (ESS)

- Created by chaining several BSSs together with a backbone network (distribution system)
- ESSs are highest-level abstraction supported by 802.11 networks

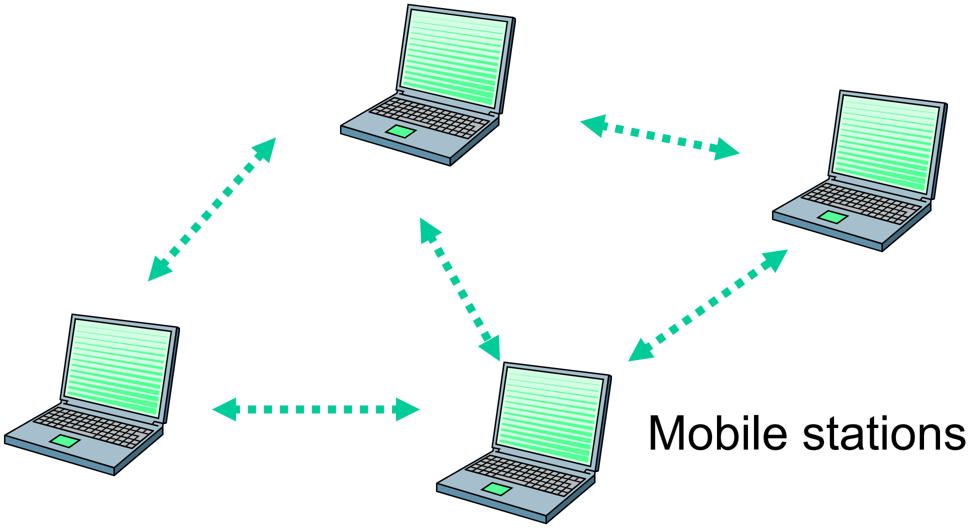


ESS and Distribution Systems

- ESS has its own identifier → SSID: Service Set ID
  - Commonly known as the network name—human-readable name
  - "ESSID" is sometimes used to refer to the SSID used in the context of an ESS
  - Transparent to the end user
    - Traffic in ESS may use several different BSSIDs (APs)

- DSs enable mobile device support
  - Address-to-destination mapping
  - Seamless integration of several BSSs
  - In practice, an access point implements DS services

Independent Basic Service Set



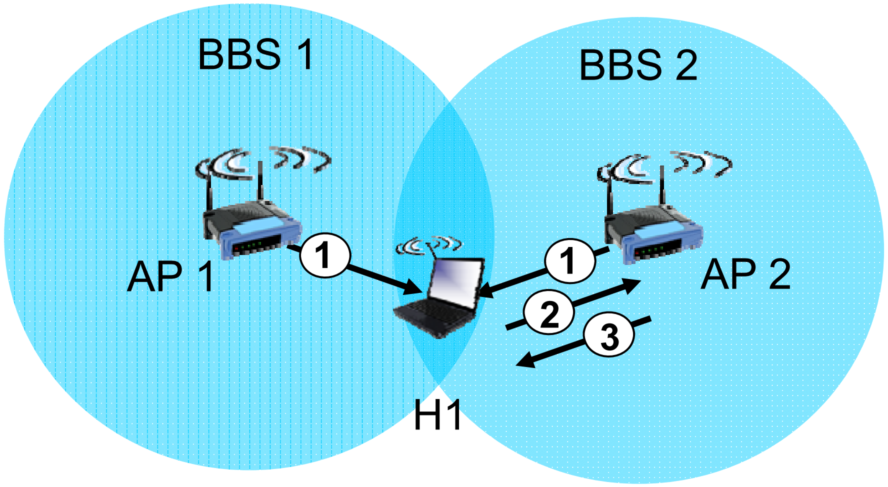
- Also known as ad hoc or peer-to-peer
- IBSSs are formed by stations communicating directly with one another (no AP)
- Multiple IBSSs can coexist in same geographic area by operating on different frequencies
- Ad hoc networks can coexist with infrastructure-based networks
- Stations use a random number as BSSID
  - First station selects BSSID and the others use it

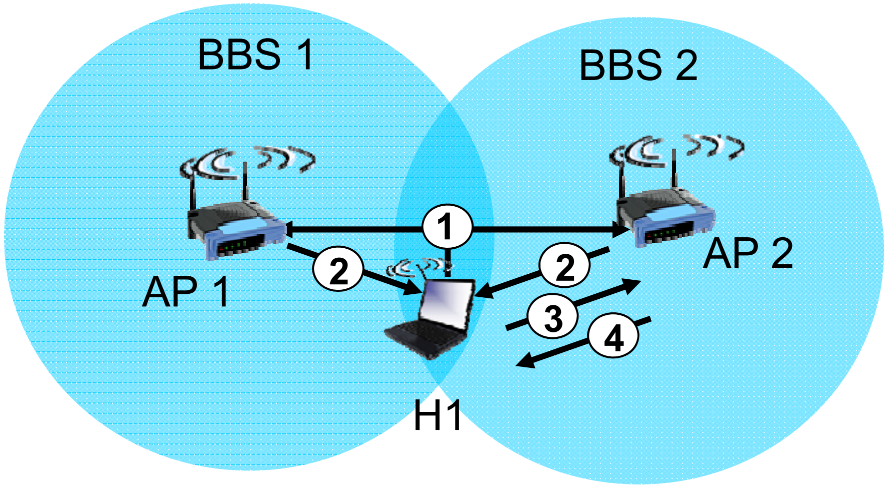
802.11 Authentication and Association

- Host must associate with an AP before data can be sent / received

- Host
  1. Scans channels listening for *beacon frames* containing AP's name – Service Set ID (SSID) and MAC address
  2. Selects an AP
  3. If required, perform authentication
     - Client proves knowledge of a given password
  4. Performs association
     - Exchange info about stations and BSS capabilities
     - Creates a virtual wire between station and AP

802.11 Passive/Active Scanning





Passive Scanning:

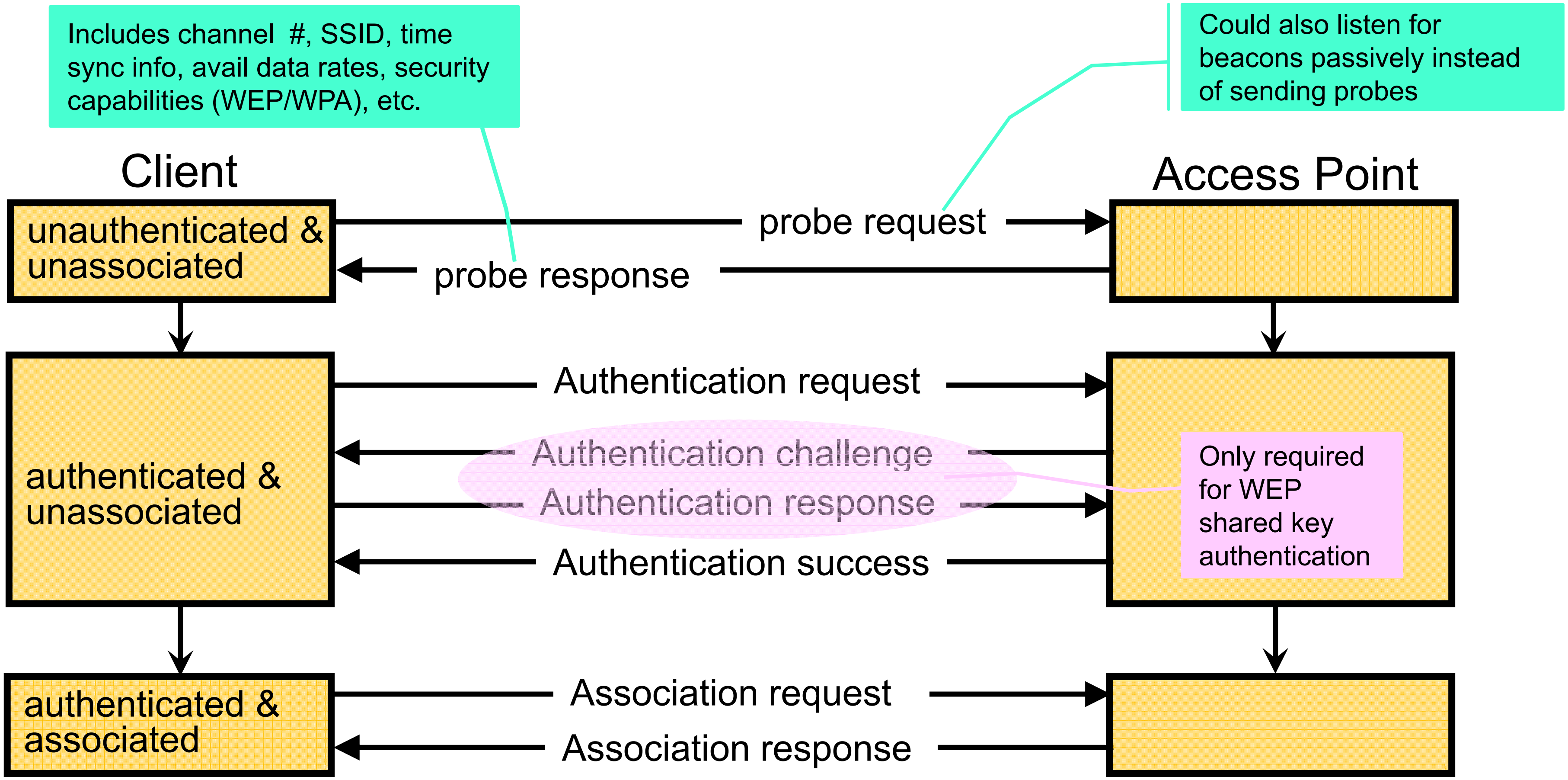
1. APs send beacon frames
2. Association Request frame sent: H1 to selected AP
3. Association Response frame sent: AP to H1

Active Scanning:

1. Probe Request frame broadcast from H1
2. Probe Response frames sent from APs
    - H1 selects strongest AP
3. Association Request frame sent from H1 to selected AP
4. Association Response frame sent from AP to H1

802.11 Authentication and Association

- Prior to communicating data, access point requires client to authenticate and associate



Includes channel #, SSID, time sync info, avail data rates, security capabilities (WEP/WPA), etc.

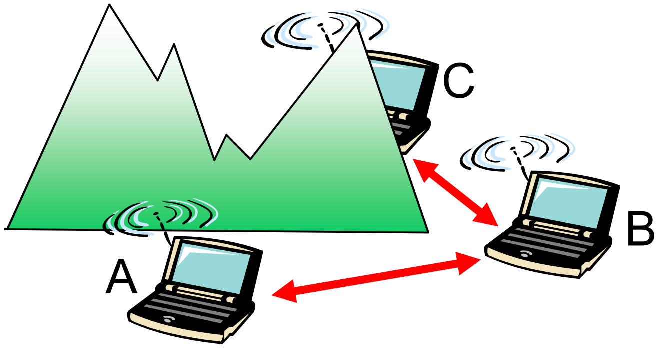
Could also listen for beacons passively instead of sending probes

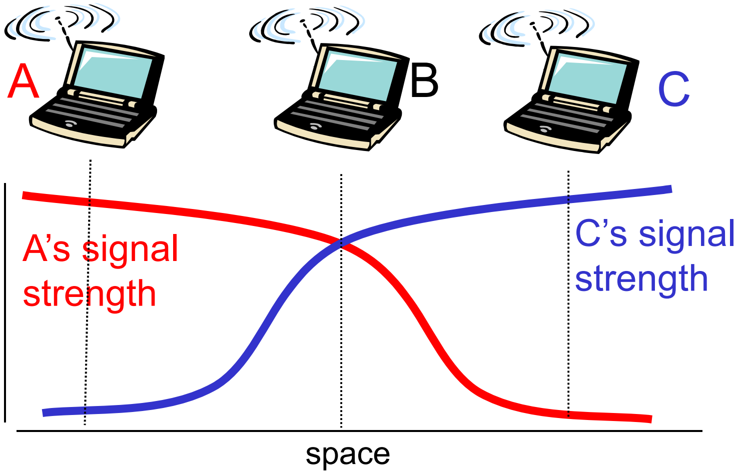
Only required for WEP shared key authentication

Association enables data transfer between STA and AP

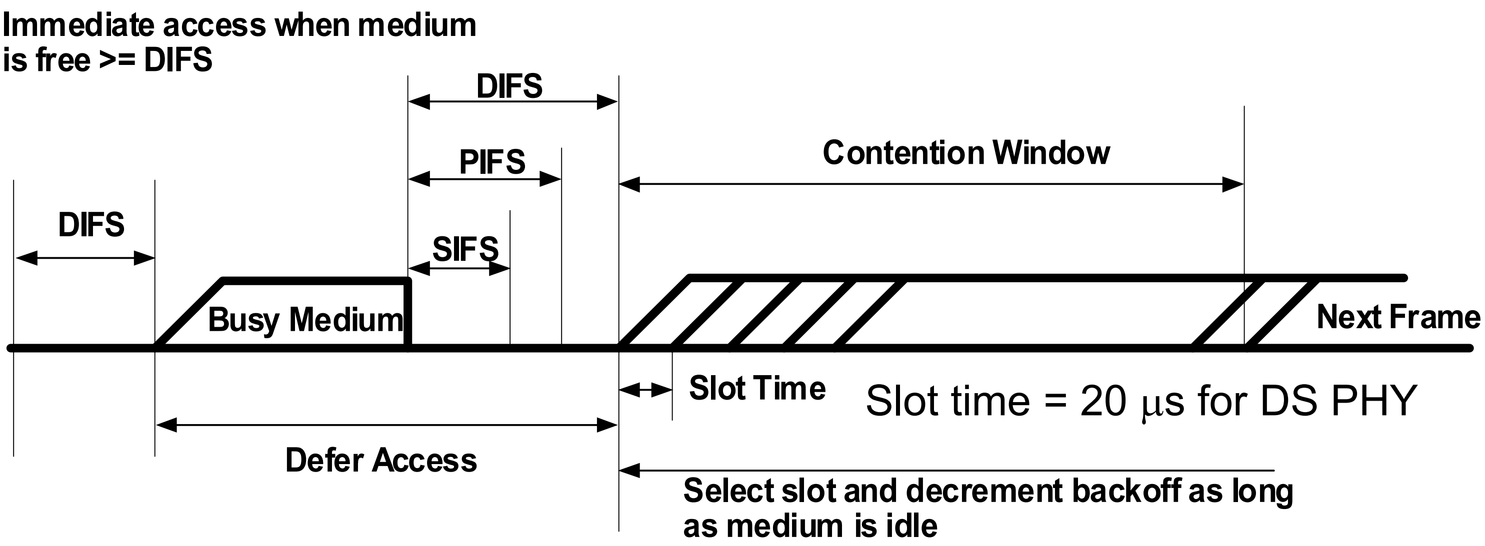
802.11 Multiple Access – CSMA/CA

- Avoid collisions: 2^+ nodes transmitting at same time
- 802.11: CSMA - sense before transmitting
  - Don't collide with ongoing transmission by other node
- 802.11: *no* collision detection!
  - Difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
  - Can't sense all collisions in any case: hidden terminal, fading
  - Goal: *avoid collisions:* CSMA/C(ollision)A(voidance)



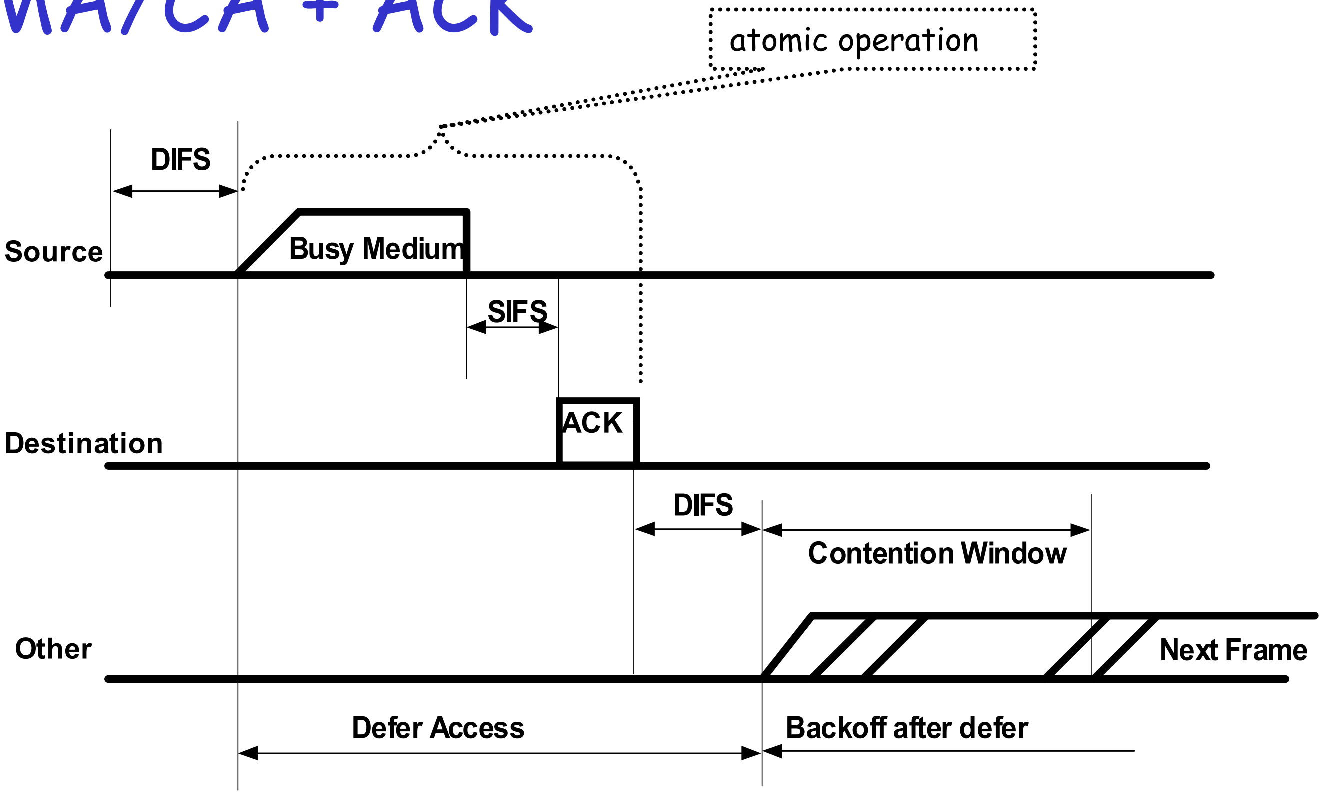


Inter-frame Spacing



- Implement 3 levels of priority using Inter-frame Space (IFS)
  - DIFS (DCF IFS) - Used for asynchronous data service
  - PIFS (PCF IFS) - Used during the contention free period—time-bounded service
  - SIFS (Short IFS) - Used to send ACK, RTS/CTS, and other management frames → 10 μs for DS PHY
- There are actually 6 IFSs!

CSMA/CA + ACK

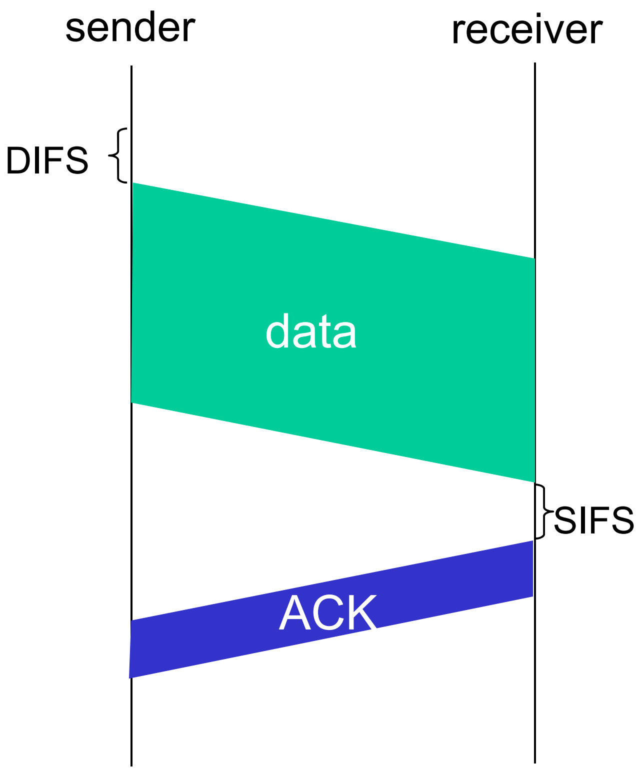


- Destination returns ACK to indicate successful (correct CRC) reception of data
- If ACK never arrives, the source retransmits the frame after backoff time

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 only counts down while channel idle
3. Transmit when timer expires and wait for ACK
4. If ACK received and more frames to send – goto 2 (backoff)
   If no ACK, increase random backoff interval and goto step 2



802.11 receiver

If frame received OK

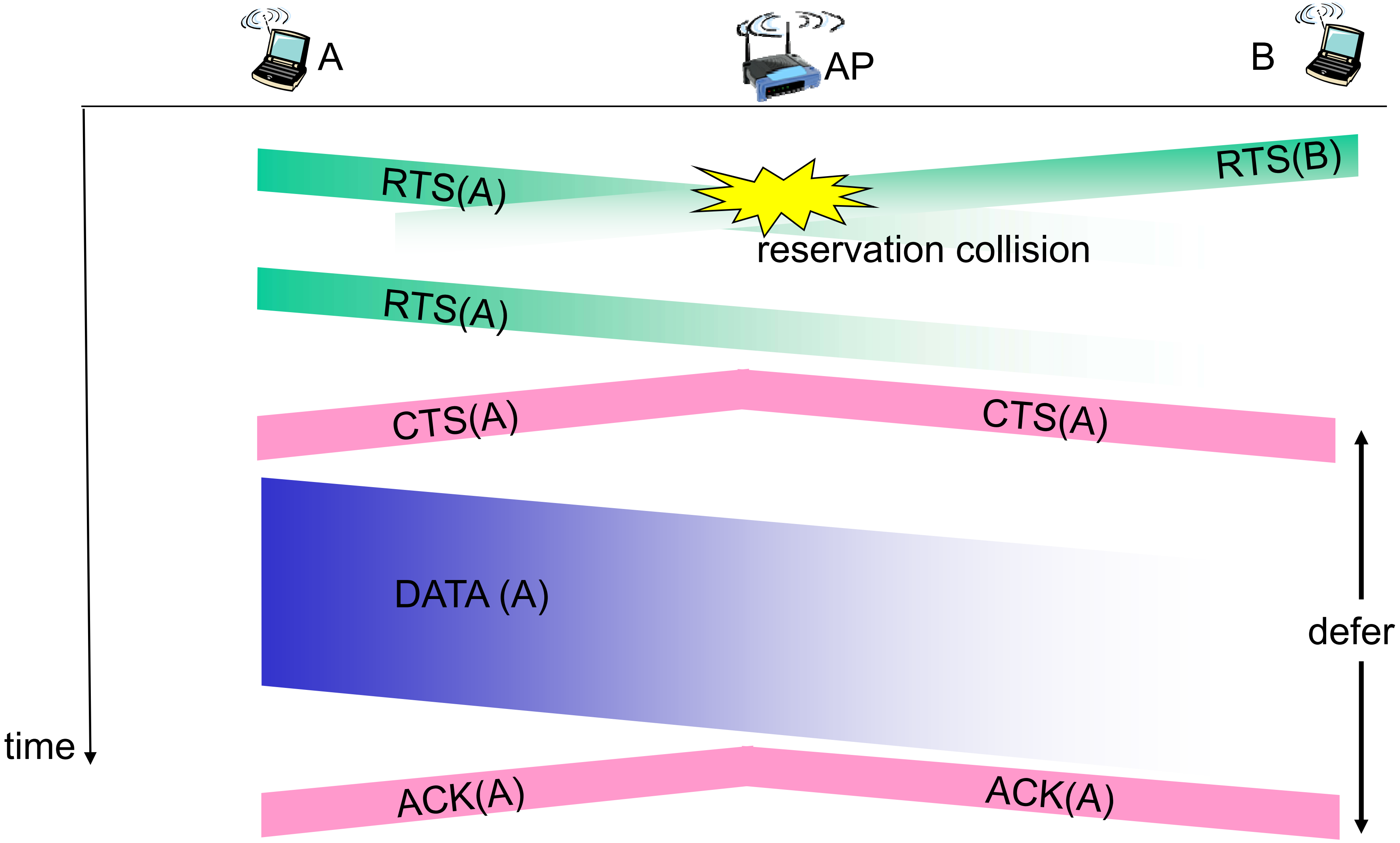
return ACK after **SIFS** (ACK needed due to hidden terminal problem)

Collision Avoidance (CA)

- Idea: Allow sender to "reserve" channel rather than random access of data frames: avoid collisions of long data frames

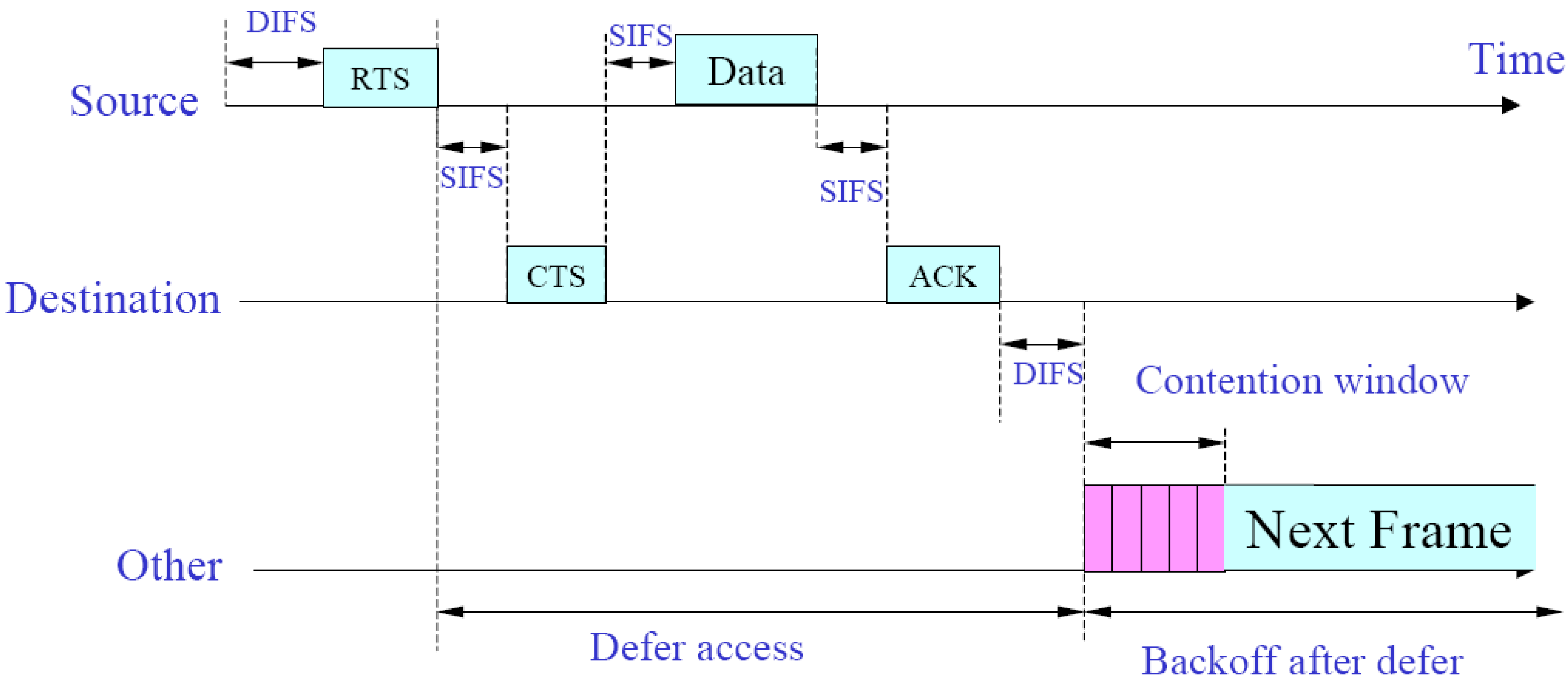
- Sender first transmits a small request-to-send (RTS) packet to AP using CSMA
  - RTSs contain the amount of time required by the station
  - RTSs may still collide with each other (but they're short)
- AP broadcasts clear-to-send (CTS) in response to RTS
- CTS heard by all associated nodes
  - Sender transmits data frame
  - Other stations defer transmissions

Collision Avoidance: RTS-CTS Exchange



See this applet: http://media.pearsoncmg.com/aw/aw_kurose_network_2/applets/csma-ca/withhidden.html

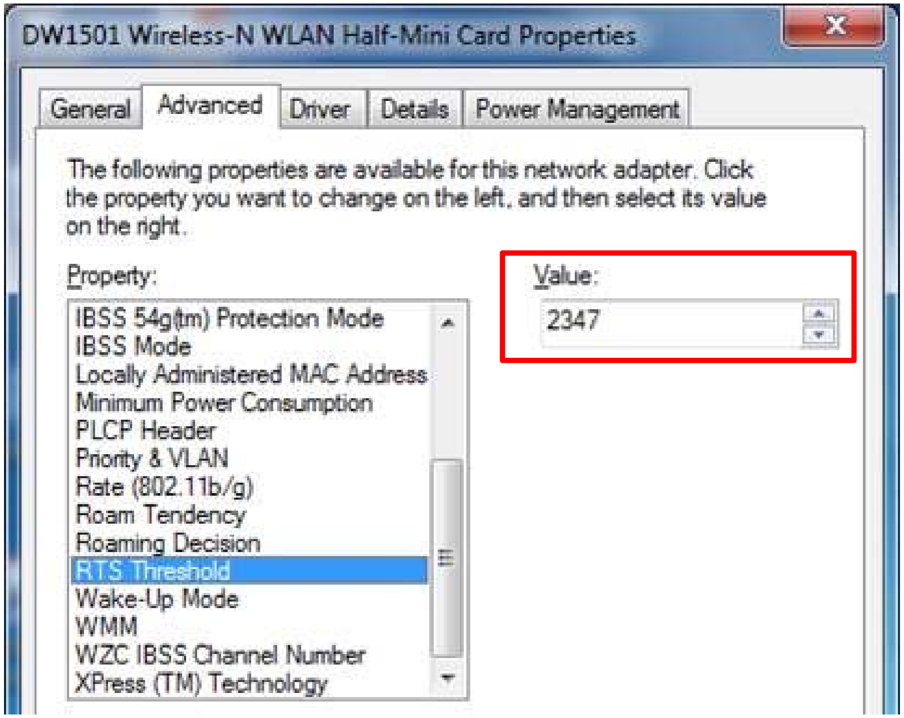
Collision Avoidance: RTS-CTS Exchange



Collision Avoidance (CA)

- RTS/CTS optional and is set by RTS threshold in sender
- Source can be Station or Access Point
  - Range = 0 – 2347
  - Most vendors recommend using a threshold of around 500
  - Threshold of 2347 bytes effectively disables RTS/CTS

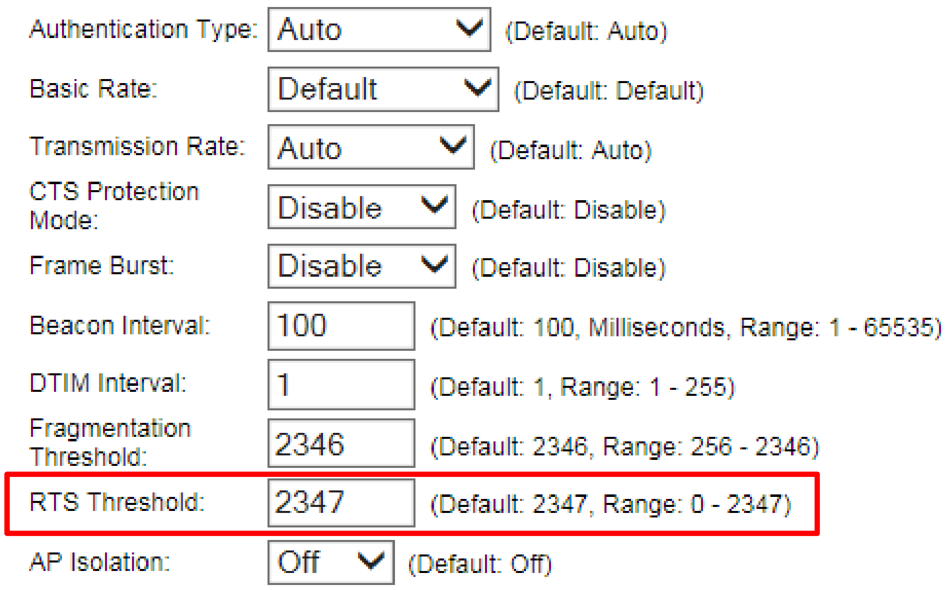
Client



The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

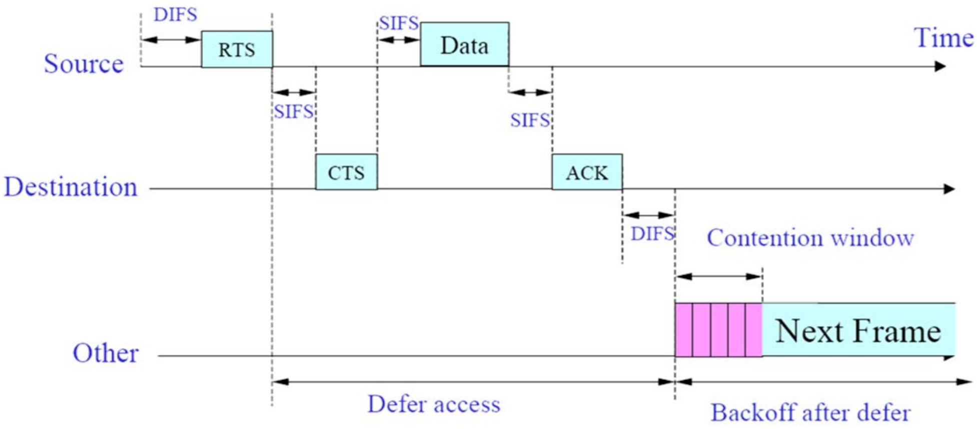
Value: 2347

Access Point



Authentication Type:	Auto	(Default: Auto)
Basic Rate:	Default	(Default: Default)
Transmission Rate:	Auto	(Default: Auto)
CTS Protection Mode:	Disable	(Default: Disable)
Frame Burst:	Disable	(Default: Disable)
Beacon Interval:	100	(Default: 100, Milliseconds, Range: 1 - 65535)
DTIM Interval:	1	(Default: 1, Range: 1 - 255)
Fragmentation Threshold:	2346	(Default: 2346, Range: 256 - 2346)
RTS Threshold:	2347	(Default: 2347, Range: 0 - 2347)
AP Isolation:	Off	(Default: Off)

Control Frames



Equal to 0 for final fragment or lone data frame

	bytes 2	2	6	4
ACK	frame control	duration	receiver address	CRC

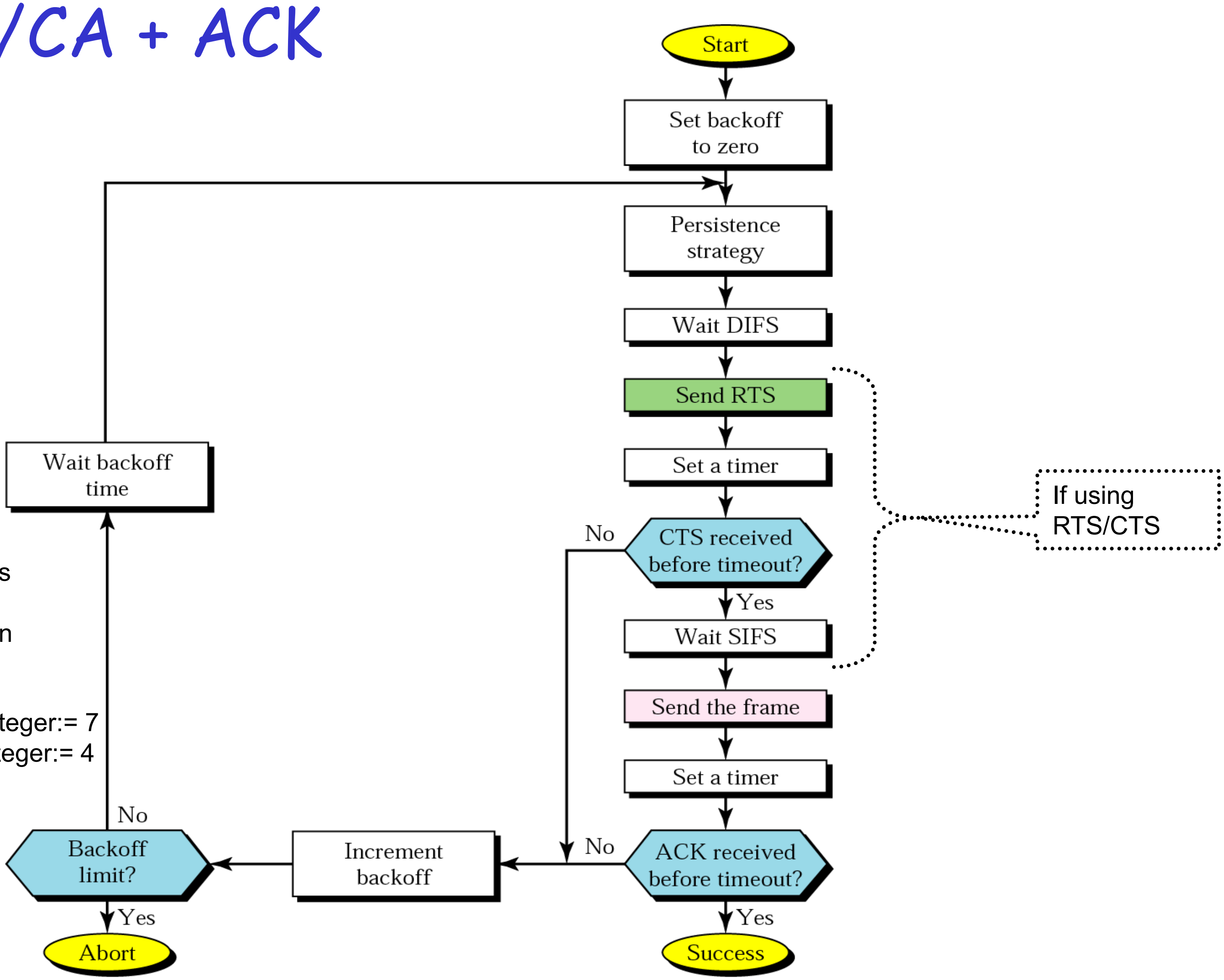
Duration of upcoming data frame + CTS + ACK + (3 x SIFS)

	bytes 2	2	6	6	4
RTS	frame control	duration	receiver address	transmitter address	CRC

Duration field in RTS frame – CTS – SIFS

	bytes 2	2	6	4
CTS	frame control	duration	receiver address	CRC

CSMA/CA + ACK

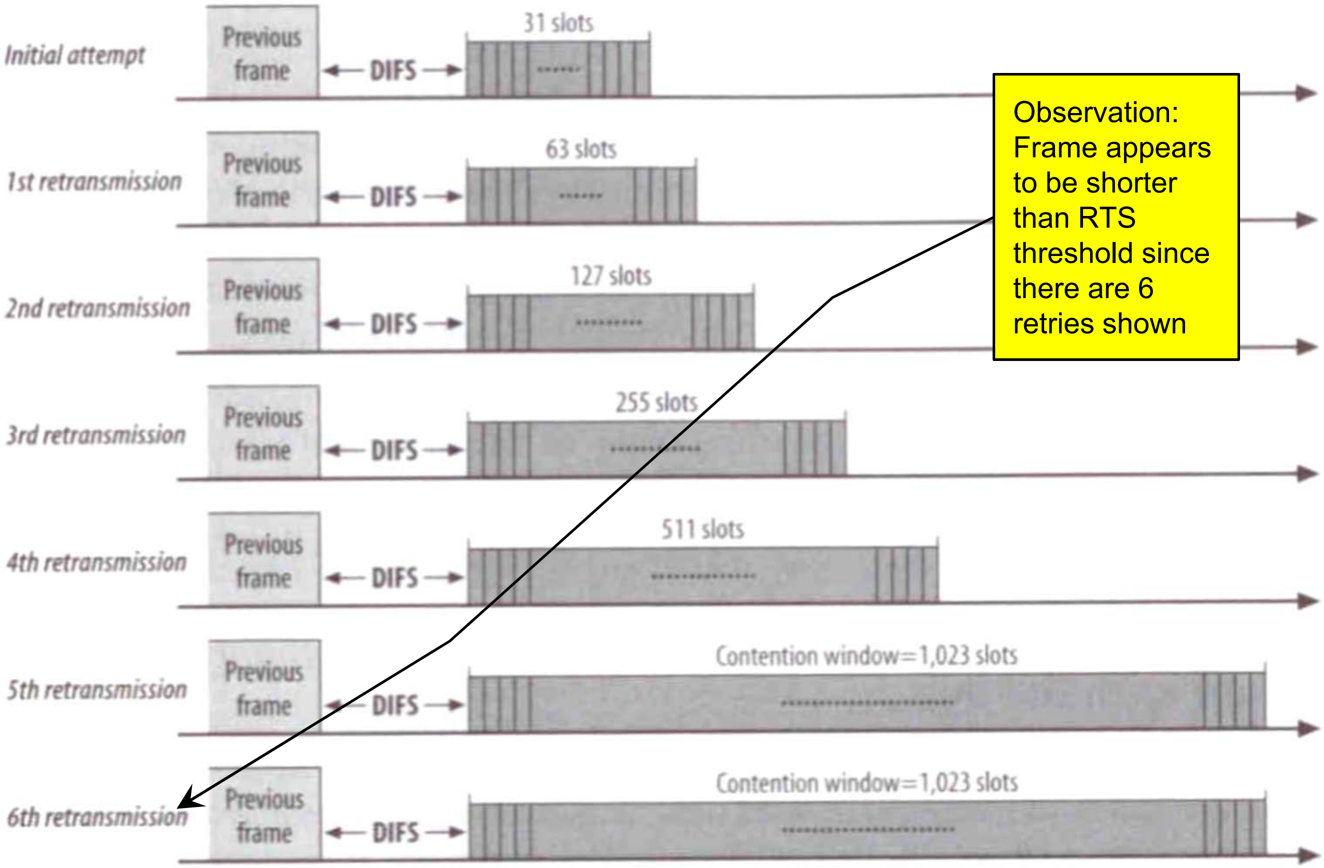


Backoff limit depends on whether frame is shorter or longer than RTS threshold

dot11ShortRetryLimit Integer:= 7
dot11LongRetryLimit Integer:= 4

DCF Backoff (Contention window)

- System adaptively sets the contention window
  - Too low: high probability of collisions
  - Too high: unnecessary delays
- Exponential backoff
  - Each time a collision occurs, the contention window doubles up to a maximum CW_{max}



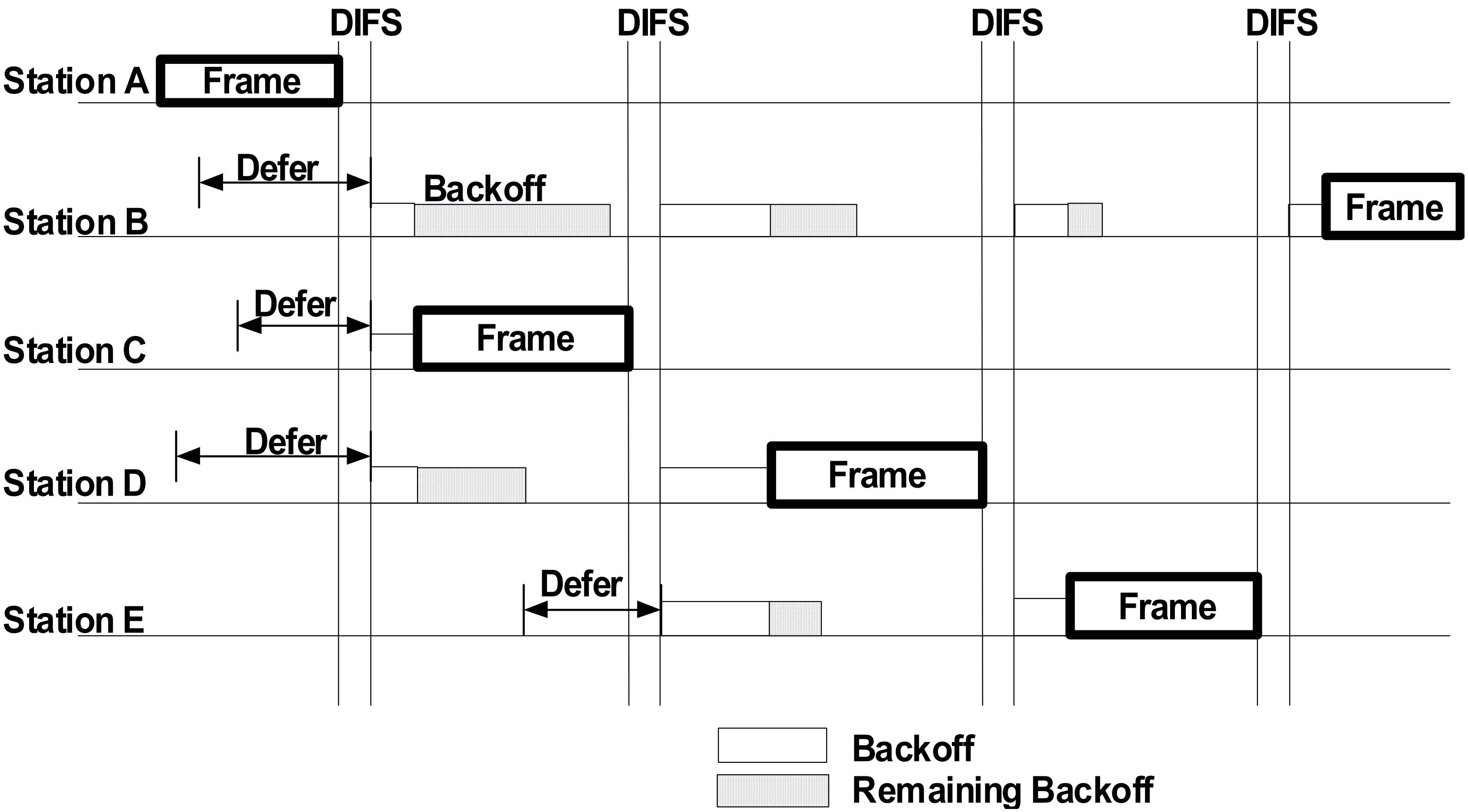
Observation: Frame appears to be shorter than RTS threshold since there are 6 retries shown

Backoff Timer

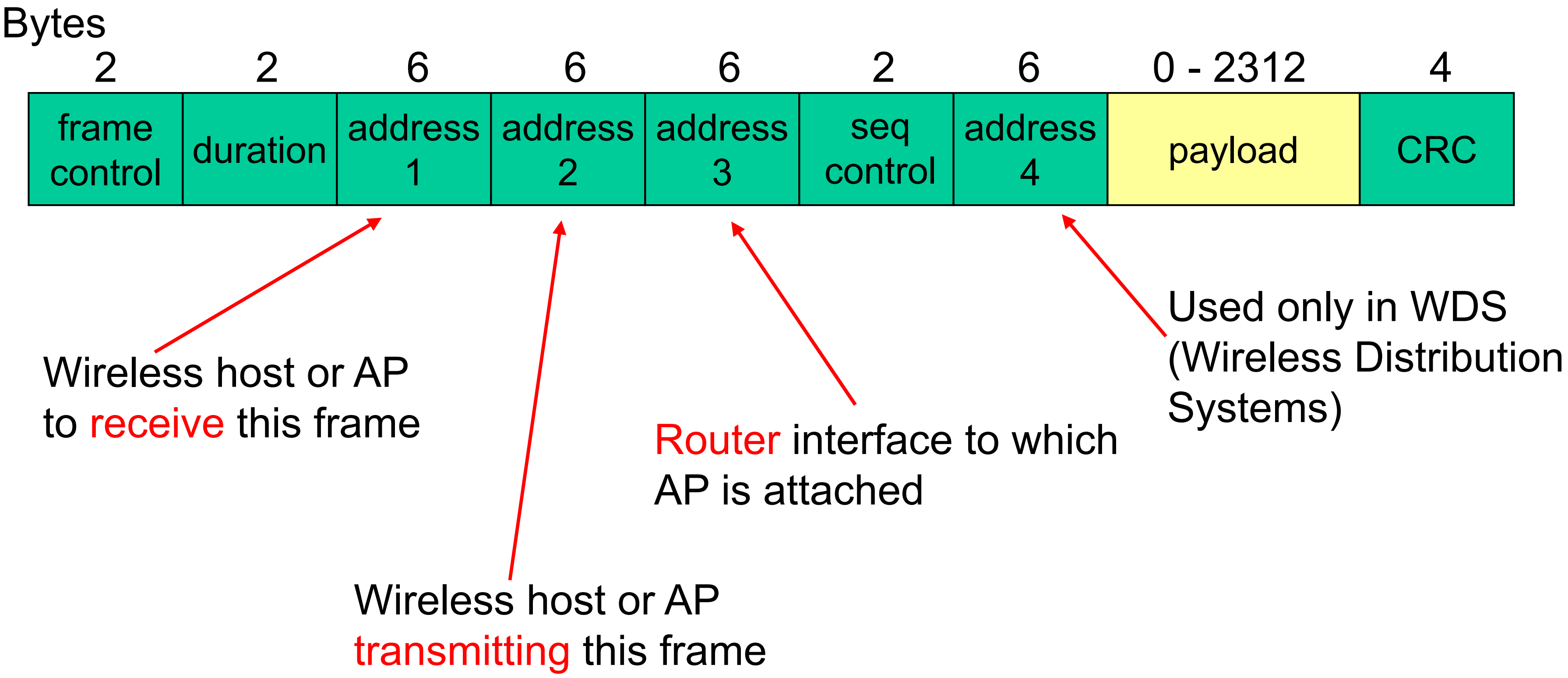
- Stations choose a random waiting time/slots w/i contention window
- If the station does not gain access to the medium in its first cycle,
  - it stops its backoff timer,
  - waits for the medium to be free for DIFS and then
  - starts the timer again
- A deferred station has a better chance to get access to the medium in the next cycle
  - Note: if a collision occurs the next time, a new random backoff timer will be chosen (retransmissions are not privileged)
- A station that completes a frame transmission is not allowed to transmit immediately
  - Must first perform a backoff procedure

Contention Resolution

- Backoff timer decrements only after DIFS has been detected



802.11 Data Frame: Addressing



Bytes

2	2	6	6	6	2	6	0 - 2312	4
frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC

Wireless host or AP to receive this frame

Wireless host or AP transmitting this frame

Router interface to which AP is attached

Used only in WDS (Wireless Distribution Systems)

Address Fields

Wireless host or AP to receive this frame

Wireless host or AP transmitting this frame

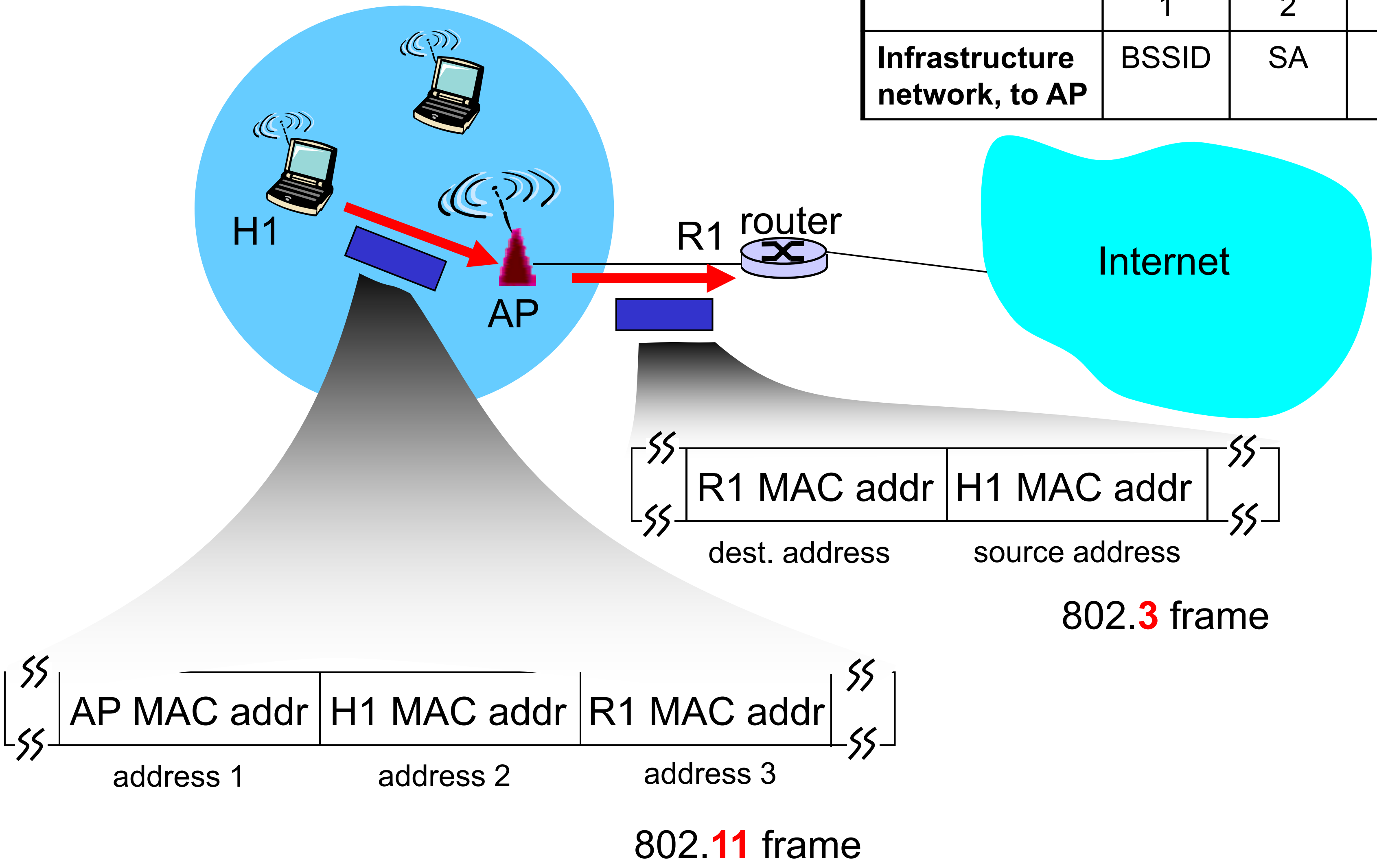
Router interface to which AP is attached

	To DS	From DS	Addr 1	Addr 2	Addr 3	Addr 4
ad hoc network All management and control frames Data frames within an IBSS (never infrastructure data frames)	0	0	DA	SA	BSSID	-
Infrastructure network, from AP Data frames received for a wireless station in an infrastructure network	0	1	DA	BSSID	SA	-
Infrastructure network, to AP Data frames transmitted from a wireless station in an infrastructure network	1	0	BSSID	SA	DA	-
Infrastructure network, within DS Transmission between two APs Data frames on a wireless bridge – Wireless Distribution System	1	1	RA	TA	DA	SA

“Destination” will process network-layer packet within frame
“Receiver” will attempt to decode radio waves to form a frame

802.11 Frame: Addressing

	Addr 1	Addr 2	Addr 3
Infrastructure network, to AP	BSSID	SA	DA



R1 MAC addr | H1 MAC addr

dest. address | source address

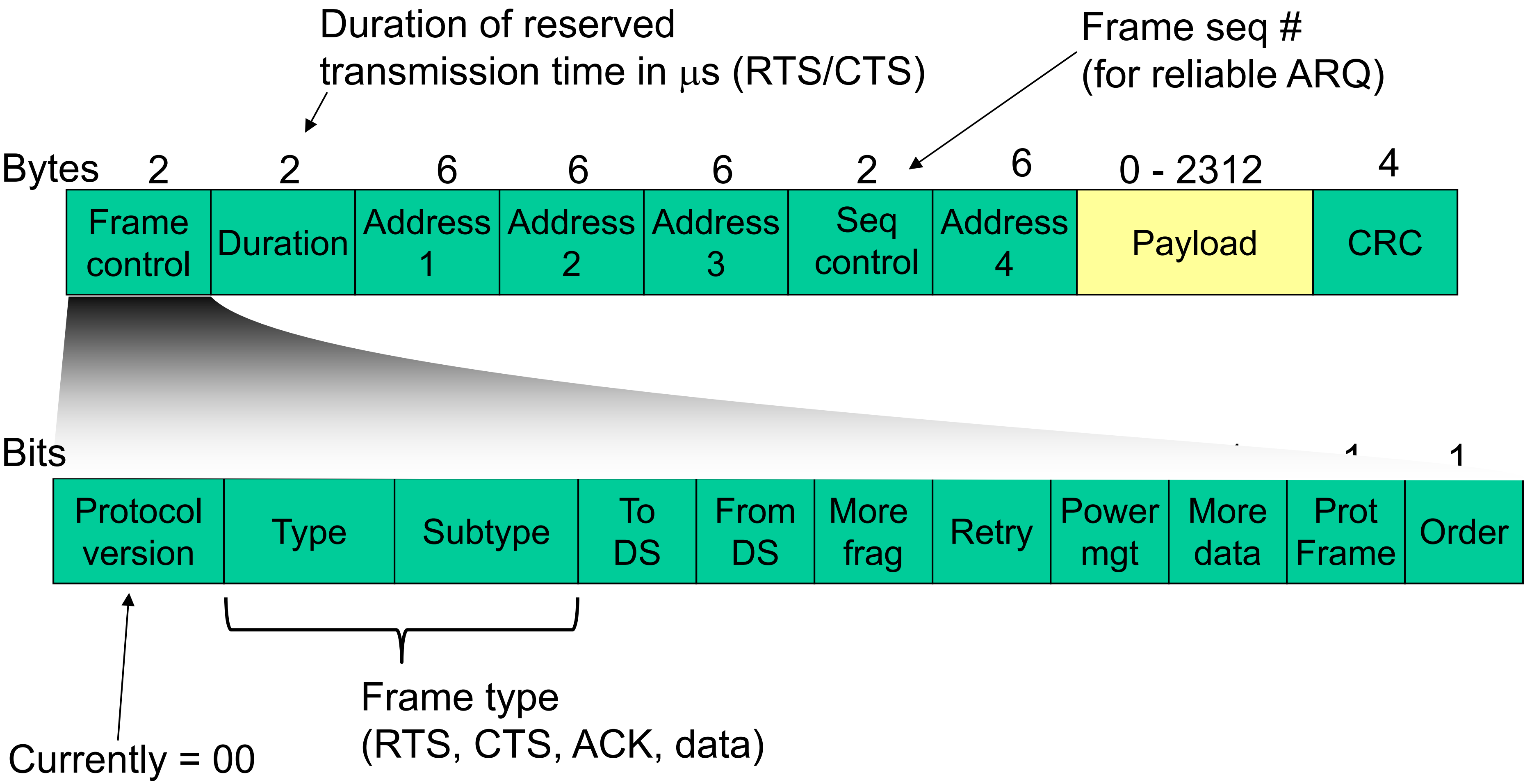
802.3 frame

AP MAC addr | H1 MAC addr | R1 MAC addr

address 1 | address 2 | address 3

802.11 frame

802.11 Frame Format - MAC Layer



Duration of reserved transmission time in μs (RTS/CTS)

Frame seq # (for reliable ARQ)

Bytes	2	2	6	6	6	2	6	0 - 2312	4
	Frame control	Duration	Address 1	Address 2	Address 3	Seq control	Address 4	Payload	CRC

Bits										1	1
	Protocol version	Type	Subtype	To DS	From DS	More frag	Retry	Power mgt	More data	Prot Frame	Order

Currently = 00

Frame type (RTS, CTS, ACK, data)

MAC Frames

- Duration
  - Period of time the medium is expected to be occupied, in µs
  - Used to set NAV (Network Allocation Vector)
    - A virtual carrier sensing mechanism
  - Values above 32,768 are reserved
- Sequence control
  - Sequence numbers to filter out duplicates
  - First 4 bits for fragment number; last 12 for sequence number
- CRC
  - 32-bit checksum

Frame Control

- Type:
  - Management (00)
  - Control (01)
  - Data (10)
  - Reserved (11)
- Subtype
  - Assoc request (0000)
  - Beacon (1000)
  - RTS (1011)
  - CTS (1100)

Type value (b3 b2)	**Subtype value (b7 b6 b5 b4)**	**Frame Function**
Management Type ('00)	0000	Association request
	0001	Association response
	0010	Reassociation request
	0011	Reassociation response
	0100	Probe request
	0101	Probe response
	0110–0111	Reserved
	1000	Beacon
	1001	ATIM
	1010	Disassociation
	1011	Authentication
	1100	Deauthentication
	1101	Action
	1110–1111	Reserved
Control Type (01)	0000–0111	Reserved
	1000	Block Ack Request (BlockAckReq)
	1001	Block Ack (BlockAck)
	1010	PS-Poll
	1011	RTS
	1100	CTS
	1101	ACK
	1110	CF-End
	1111	CF-End + CF-Ack
Data Type (10)	0000	Data
	0001	Data + CF-Ack
	0010	Data + CF-Poll
	0011	Data + CF-Ack + CF-Poll
	0100	Null (no data)
	0101	CF-Ack (no data)
	110	CF-Poll (no data)
	0111	CF-Ack + CF-Poll (no data)
Reserved (11)	0000–1111	Reserved

Frame Control

- More fragments: more fragments of the same MAC service data unit (MSDU) follow
- Retry: flag is set if this is a retransmission
- Power management: indicates whether station will stay active (0) or go into power-save mode (1) after transmission
- More data: AP has buffered data to transmit to host in power save mode (sleeping) – tells host to not go to sleep
- Protected Frame: information has been processed by a cryptographic encapsulation algorithm
- Order: if flag is set, received frames must be processed in order

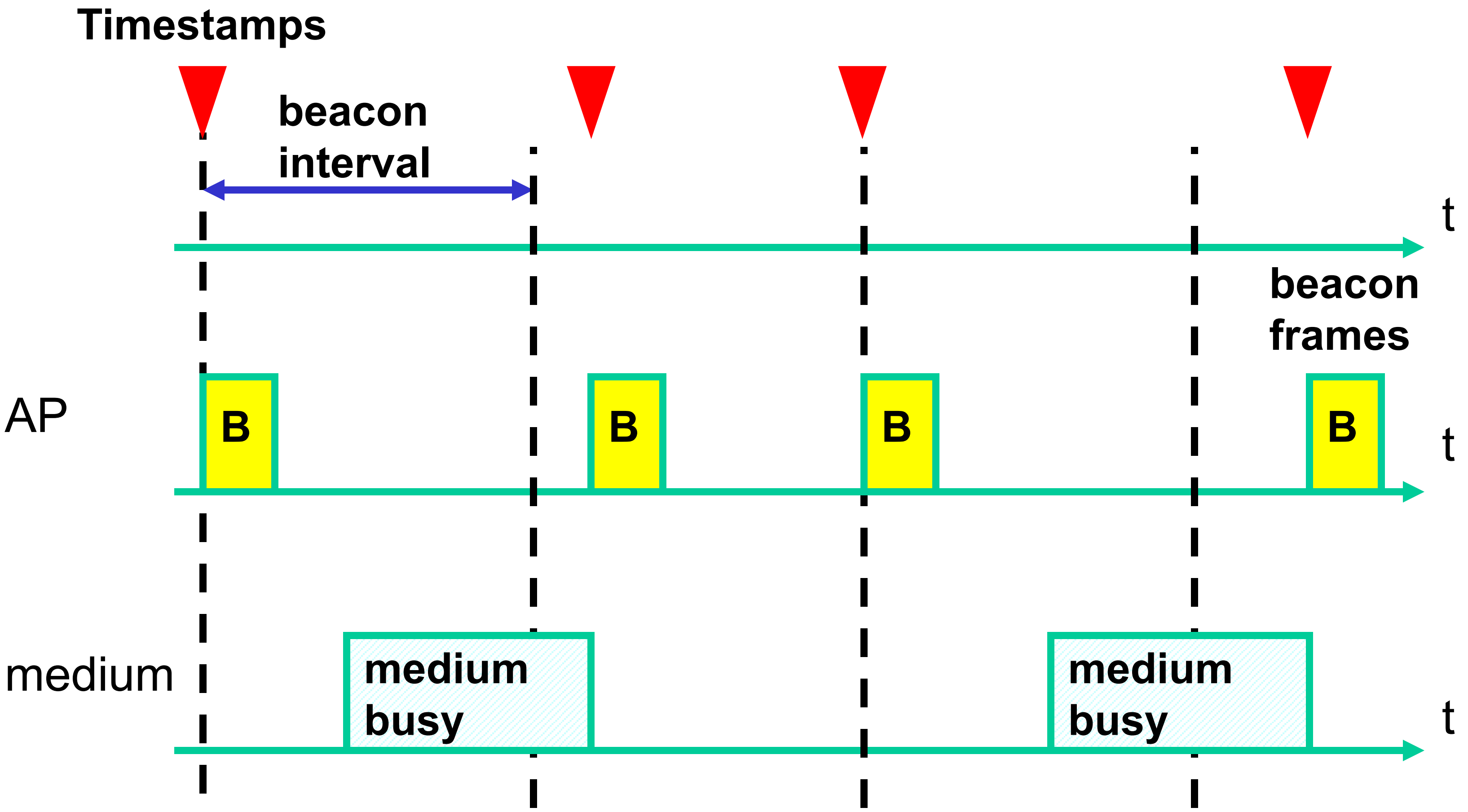
Synchronization

- Purpose is to find a WLAN and synchronize internal clocks

- All stations synchronize their internal clocks by listening to (quasi) periodic beacon signals
    - In infrastructure mode, APs transmit beacon signals
    - In ad hoc mode, any station may transmit a beacon signal
    - They may have to defer a scheduled transmission of the beacon signal when the medium is busy

- Beacon signals contain
    - Timestamp
    - Roaming information (identification of the BSS)

Beacon Frames: Infrastructure Mode



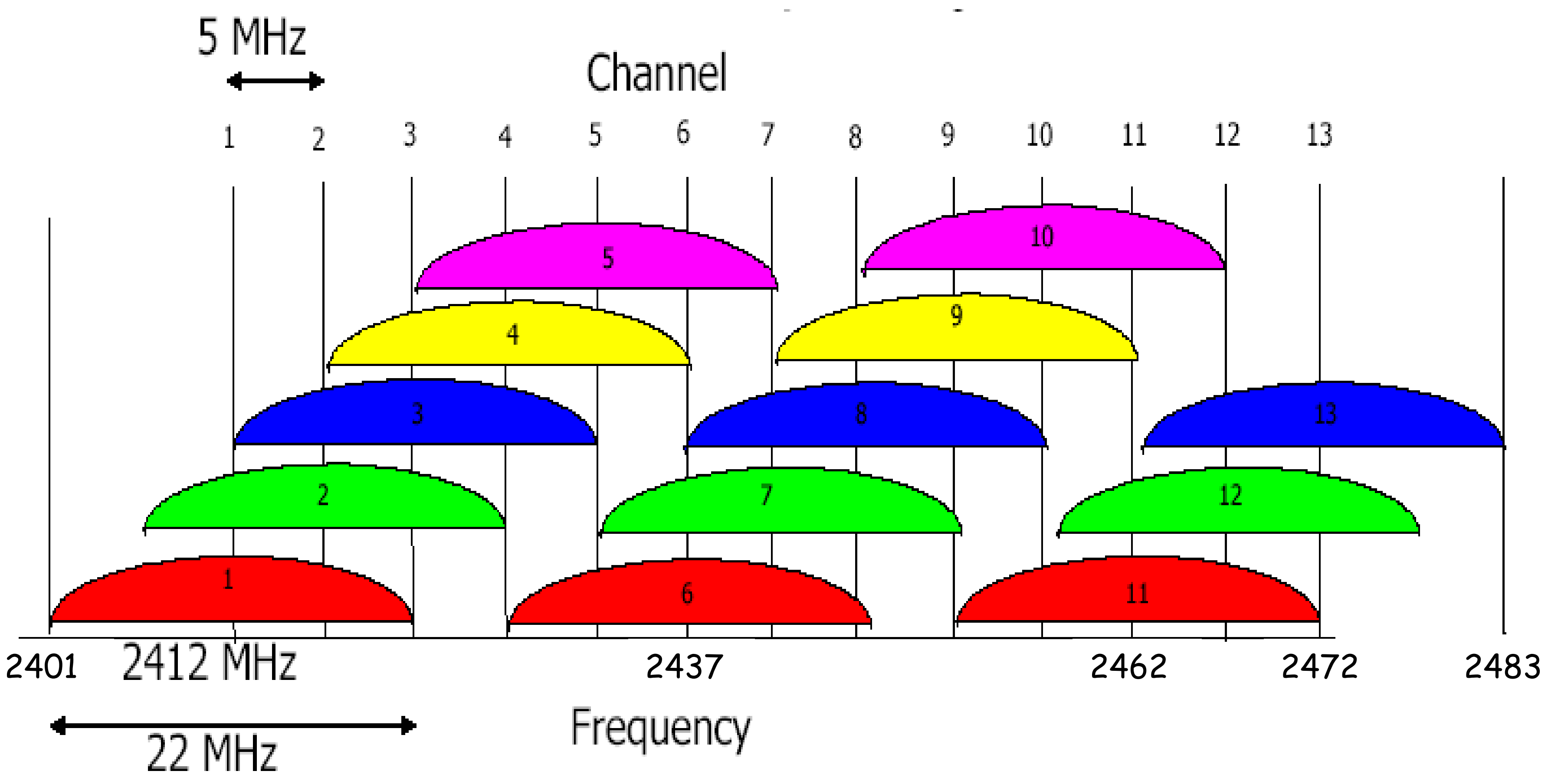
802.11b Channels

- 802.11b: 2.4 GHz - 2.4835 GHz spectrum divided into 11 channels at different frequencies
  - Administrator chooses frequency for AP
  - Interference possible: channel can be same as that chosen by neighboring AP!

Channel	Freq. (MHz)	US / Can	Eur.	Japan
1	2412	●	●	●
2	2417	●	●	●
3	2422	●	●	●
4	2427	●	●	●
5	2432	●	●	●
6	2437	●	●	●
7	2442	●	●	●

Channel	Freq.	US / Can	Eur.	Japan
8	2447	●	●	●
9	2452	●	●	●
10	2457	●	●	●
11	2462	●	●	●
12	2467		●	●
13	2472		●	●
14	2484			●

802.11b/g Channels



802.11a/b/g are Multi-rate Devices

- Typical transmission range
  - 802.11a
    - 120 m outdoor, 35 m indoor
      - 54 Mbit/s up to 5 m
      - 48 up to 12 m
      - 36 up to 25 m
      - 24 up to 30 m
      - 18 up to 40 m
      - 12 up to 60 m
      - and so on
  - 802.11b/g
    - 140 m outdoor, 38 m indoor
    - Max. data rate ~10 m indoor