

# Wireless and Mobile Networks

**Raj Jain**

Washington University in Saint Louis

Saint Louis, MO 63130

Jain@wustl.edu

Audio/Video recordings of this lecture are available on-line at:

<http://www.cse.wustl.edu/~jain/cse473-22/>

## Student Questions

**Note:** Questions discussed during regular Q&A sessions are marked with □. New questions asked during Exam 3 review are marked with ❖



1. Wireless Link Characteristics
2. Wireless LANs and PANs
3. Cellular Networks
4. Mobility Management
5. Impact on Higher Layers

**Note:** This class lecture is based on Chapter 7 of the textbook (Kurose and Ross) and the figures provided by the authors.

## Student Questions

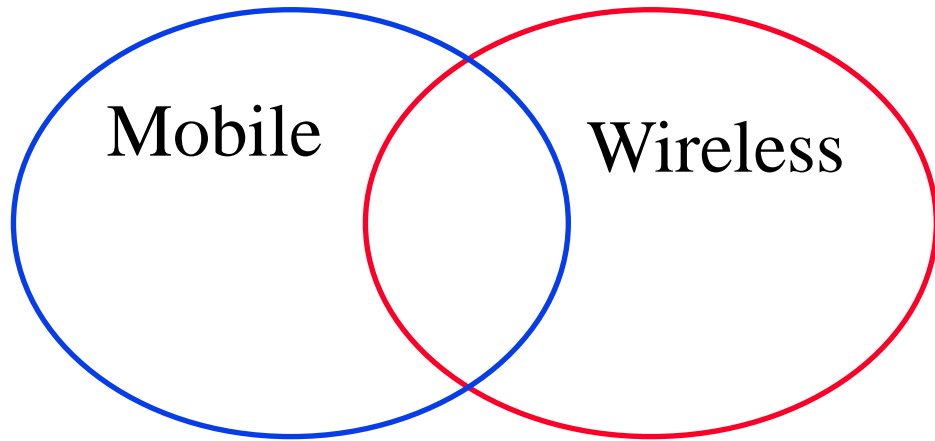


# Wireless Link Characteristics

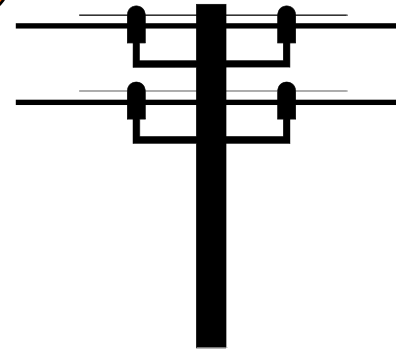
- ❑ Mobile vs. Wireless
- ❑ Wireless Networking Challenges
- ❑ Peer-to-Peer or Base Stations?
- ❑ Code Division Multiple Access (CDMA)
  - Direct-Sequence Spread Spectrum
  - Frequency Hopping Spread Spectrum

## Student Questions

# Mobile vs Wireless



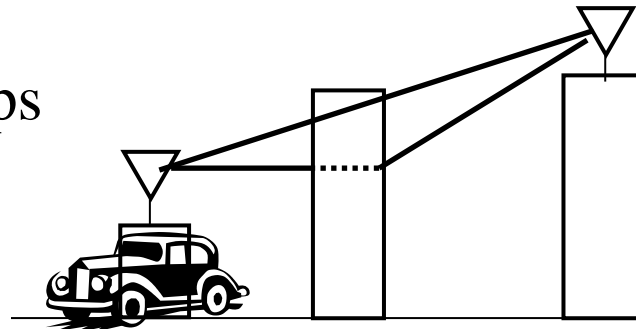
- ❑ Mobile vs Stationary
- ❑ Wireless vs Wired
- ❑ Wireless  $\Rightarrow$  media sharing issues
- ❑ Mobile  $\Rightarrow$  routing, addressing issues



## Student Questions

# Wireless Networking Challenges

1. Propagation Issues: Shadows, Multipath
2. Interference  $\Rightarrow$  High loss rate, Variable Channel  
 $\Rightarrow$  Retransmissions and Cross-layer optimizations
3. Transmitters and receivers moving at high speed  
 $\Rightarrow$  Doppler Shift
4. Low power transmission  $\Rightarrow$  Limited reach  
100mW in WiFi base station vs. 100 kW TV tower
5. License-Exempt spectrum  $\Rightarrow$  Media Access Control
6. Limited spectrum  $\Rightarrow$  Limited data rate  
Original WiFi (1997) was 2 Mbps.  
New standards allow up to 200 Mbps
7. No physical boundary  $\Rightarrow$  Security
8. Mobility  $\Rightarrow$  Seamless handover



## Student Questions

- When new buildings are constructed do the builders take into account that it may obstruct wireless signals?

*No. No such study is done. Carriers and enterprises have to structure their wireless afterwards.*

- Is the multipath meaning in each signal transmission? It will split to multi-subparts and follow different paths

*Each bit is split into multiple paths.*

- How is the Doppler effect taken into account when receiving or transmitting signals?

*Physical layer design takes care of the maximum speed allowed. Networks designed for cars will not work for airplanes.*

- Why does radio not suffer from the same propagation issues as wireless?

*It also suffers from the same issues. Analog and digital have different timescales. Bits are in microseconds or nanoseconds. Analog words are in seconds.*

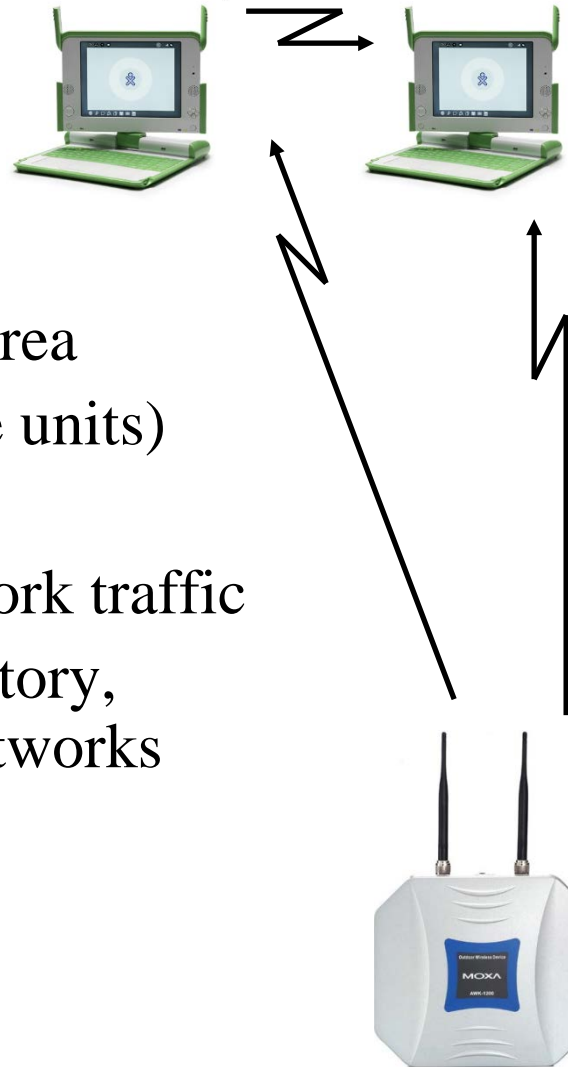
- Could you explain how the data rate physically works for wireless? What allows us to achieve faster data rates?

*It will be covered in this chapter.*

- Is there any traffic issues in wireless transmission?  
*Yes. Multiple transmissions interfere with each other like sounds in a room.*

# Peer-to-Peer or Base Stations?

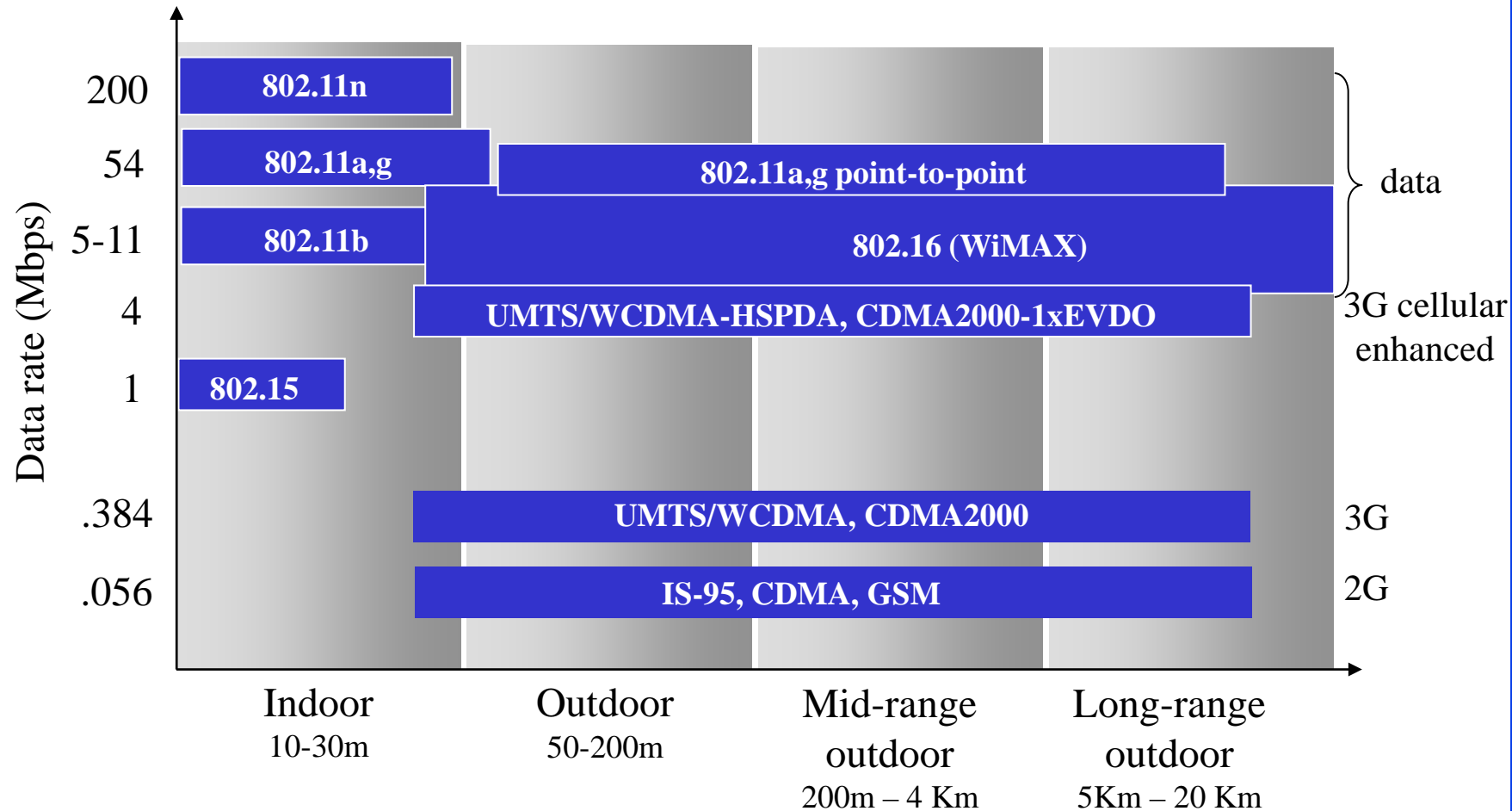
- ❑ Ad-hoc (Autonomous) Group:
  - Two stations can communicate
  - All stations have the same logic
  - No infrastructure, Suitable for small area
- ❑ Infrastructure Based: Access points (base units)
  - Stations can be simpler than bases.
  - Base provide connection for off-network traffic
  - Base provides location tracking, directory, authentication ⇒ Scalable to large networks
- ❑ IEEE 802.11 provides both.



## Student Questions

- ❑ If there are three computers in small area but no base stations, is it also called Ad-hoc Group?  
*Yes. Any number of stations can form an ad-hoc group for communication.*
- ❑ Does Ad-hoc have anything to do with P2P we discussed before, like BitTorrent?  
*No. Bit torrent is between computers far away in different countries. Here, we are talking about computers in the same room.*
- ❑ Is using base station more common than peer-to-peer?  
*Yes, base stations are common.*



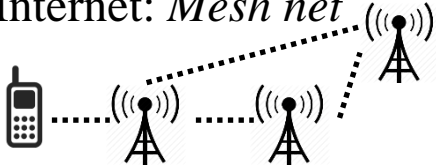

# Characteristics of Selected Wireless Link Standards



## Student Questions

- For same power provided, lower data rate (longer wavelength) means longer distance?  
*Longer wavelength => Lower frequency => Lower Hz. Coding determines Bits/Hz. So data rate depends on Coding and wavelength. For the same power and coding, longer wavelengths will have lower data rate and longer distances.*

# Wireless Network Taxonomy

	Single hop	Multiple hops
<p>Infrastructure (Access Points, Towers)</p> <p>No Infrastructure</p>	<p>Host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet</p>  <p>No base station (Bluetooth, ad hoc nets)</p> 	<p>Host may have to relay through several wireless nodes to connect to larger Internet: <i>Mesh net</i></p>  <p>Relay to reach other a given wireless node. Mobile Ad-hoc Network (MANET), Vehicular Ad-hoc Network (VANET)</p> 

## Student Questions

- The hop here is link over wireless transmission, right? Then those station will eventually be wired into the Internet?

*Sometimes, wireless is used over multiple hops without wires. That is multi-hop wireless.*

- What is the difference between Mobile Ad-hoc and hoc nets? Is it just the difference of numbers of devices?

*Mobile means moving. Two computers communicating in Ad-hoc mode may are may not be mobile. A mobile ad-hoc network means at least one of the nodes is moving.*

- So VANETs do not yet exist?

*Not common. Emergency vehicles (fire brigades and military) use it.*

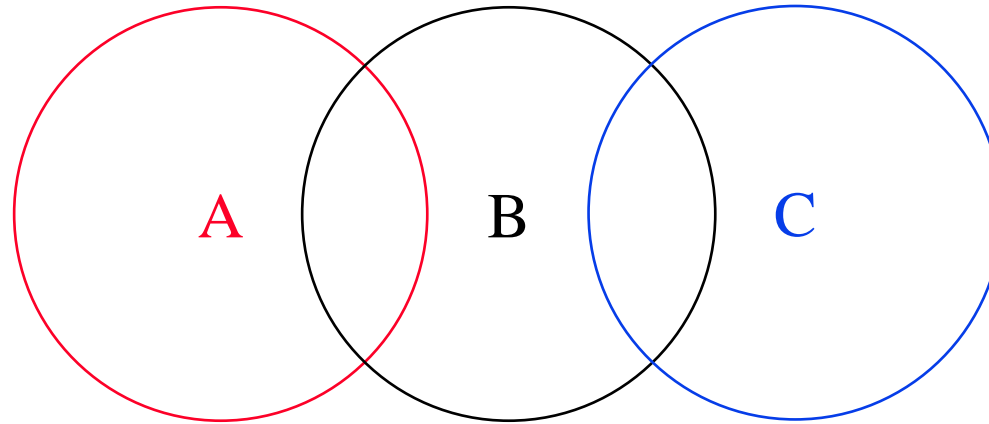
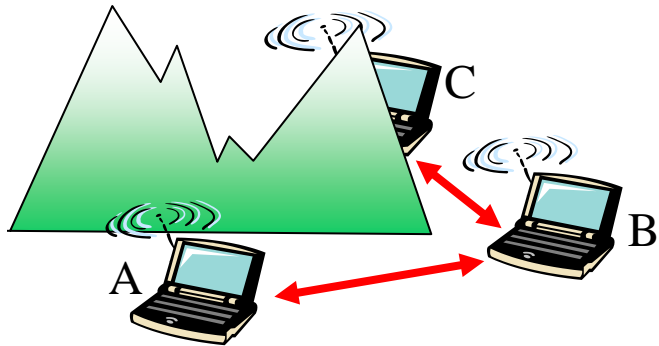
- What is the difference between MANET and VANET again? Is VANET the next generation of MANET?

*M=Mobile. Could be between a walking person and the tower.*

*V=Vehicle-to-vehicle without a tower.*



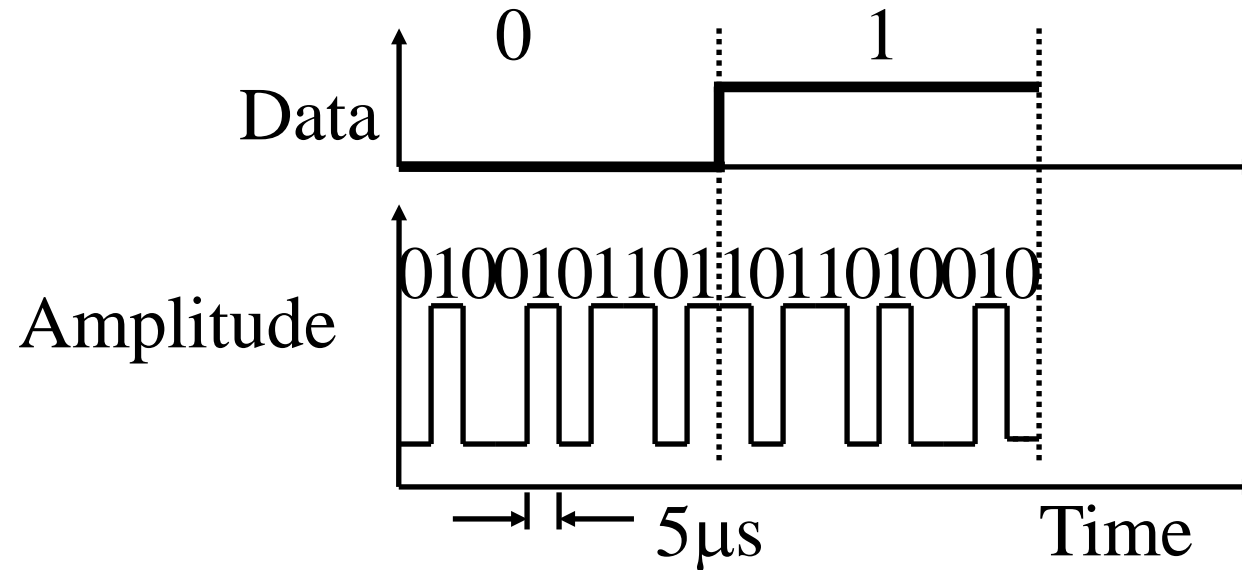
# Hidden Node Problem



- ❑ B and A can hear each other
- ❑ B and C can hear each other
- ❑ A and C cannot hear each other  
⇒ C is hidden for A and vice versa
- ❑ C may start transmitting while A is also transmitting  
A and C can't detect collision.
- ❑ Only the receiver can help avoid collisions

## Student Questions

# Direct-Sequence Spread Spectrum CDMA



- ❑ Spreading factor = Code bits/data bit, 10-100 commercial (Min 10 by FCC), 10,000 for military
- ❑ Signal bandwidth  $> 10 \times$  data bandwidth
- ❑ Code sequence synchronization
- ❑ Correlation between codes  $\Rightarrow$  Interference  $\Rightarrow$  Orthogonal

## Student Questions

- ❑ Would you clarify the meanings of "bandwidth" here?

*Band = Frequency Band*

*Bandwidth = Width of the Frequency Band  
(See next slide)*

- ❑ What's an example of orthogonal code?

*See example on slide 7-12*

- ❑ For best orthogonality, can we just use 1's complement of 0's code bit sequence for 1's code bit sequence?

*Orthogonality requires using only some of the bit combinations. 1-Bit transmission requires at least two code bits for orthogonality.*

- ❑ Once set, will the code of a transmitter be changed?  
*Yes. It is changed frequently in "code division multiple access (CDMA)."*

- ❑ When the bits sent by multiple senders are mixed, how does the CDMA receiver recover the original bits sent?

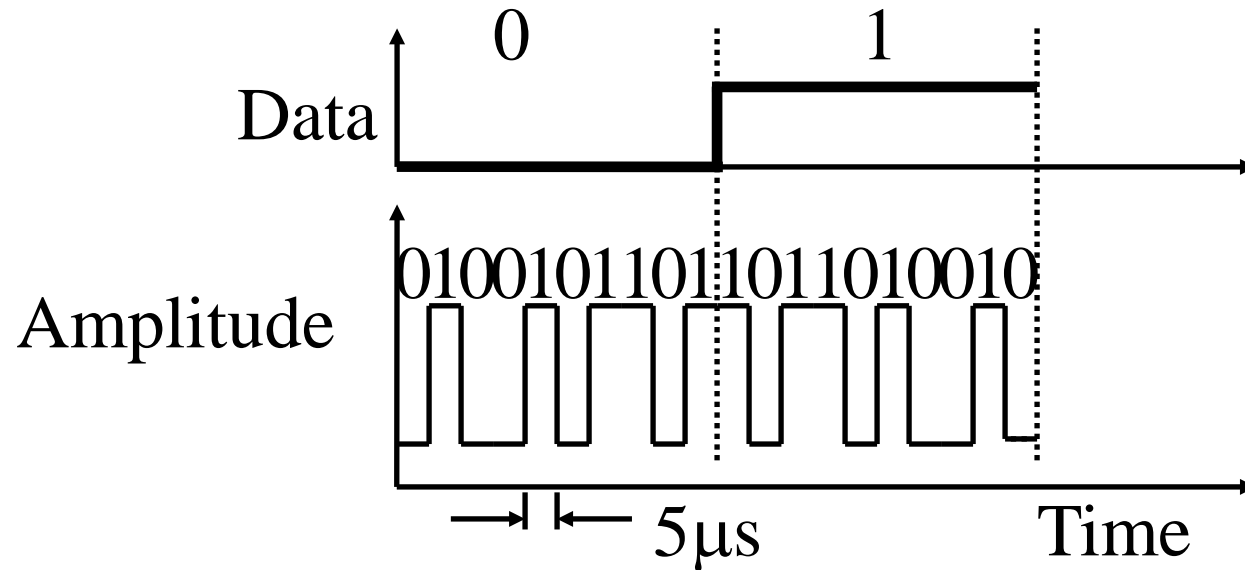
*See example in the next few slides.*

- ❑ What is meant by "Interference -> Orthogonal"?  
*Interference leads to a need for orthogonal coding.*

- ❑ Why did the FCC decide on 10 bits to be the minimum?

*So that some small number of users can share the space.*

# Direct-Sequence Spread Spectrum CDMA



- ❑ Spreading factor = Code bits/data bit, 10-100 commercial (Min 10 by FCC), 10,000 for military
- ❑ Signal bandwidth  $> 10 \times$  data bandwidth
- ❑ Code sequence synchronization
- ❑ Correlation between codes  $\Rightarrow$  Interference  $\Rightarrow$  Orthogonal

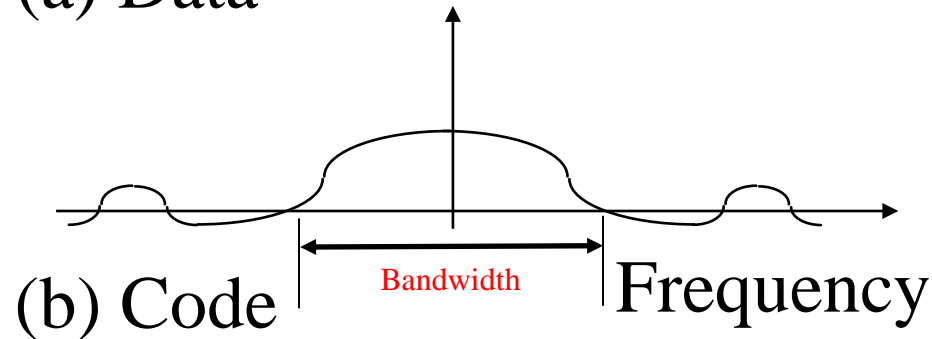
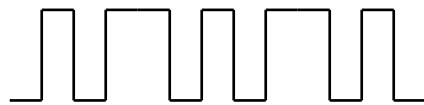
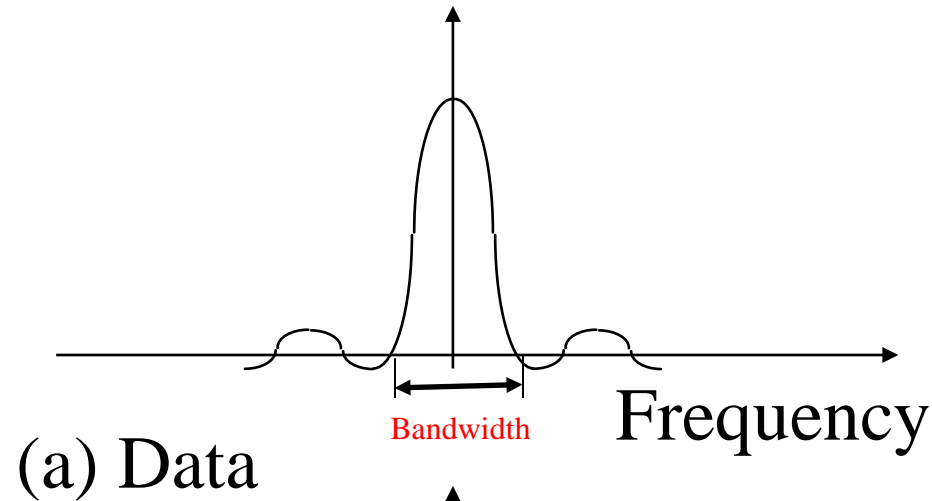
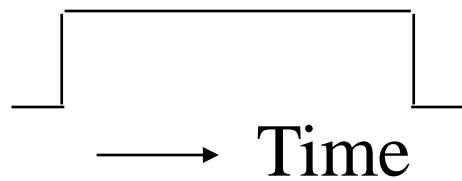
## Student Questions

- ❑ If CDMA is sending different codes to a different host, what's the difference between CDMA and TDMA?  
*In CDMA, all users transmit simultaneously. Time is not divided.*  
*In TDMA they take a turn. Time is divided into time slots.*
- ❖ Do the codes representing 0 and 1 must be opposite each other on every code bit?  
*Yes. In  $n$ -dimensional space, 0 and 1 should be as far from each other as possible. This is achieved by making the code for 0 a complement of the code for 1 and vice versa.*

# DS Spectrum

Time Domain

Frequency Domain



## Student Questions

- ❑ Why is the second graph horizontally stretched?  
*It has higher frequency bandwidth.*
- ❑ Could you reexplain this slide? Is the benefit of this transmission method to allow two signals be transmitted at once? Unsure how this improves things.

*Allows user multiplexing.*

*FDMA = Frequency Division (1G)*

*TDMA = Time Division (2G)*

*CDMA = Code Division (3G)*

- 
- ❑ Can you explain these line graphs again?

*Sure.*

- ❑ In FHSS, when should we tell the receiver the random generator seed we use? What is the range of the random number generated?

*Random number generator and seeds are exchanged at the beginning of communication and periodically.*

*Range is up to the users and standard bodies.*

- ❑ What are the advantages of spreading the spectrum? Is it just to increase the range of frequencies where the peak is at the highest?

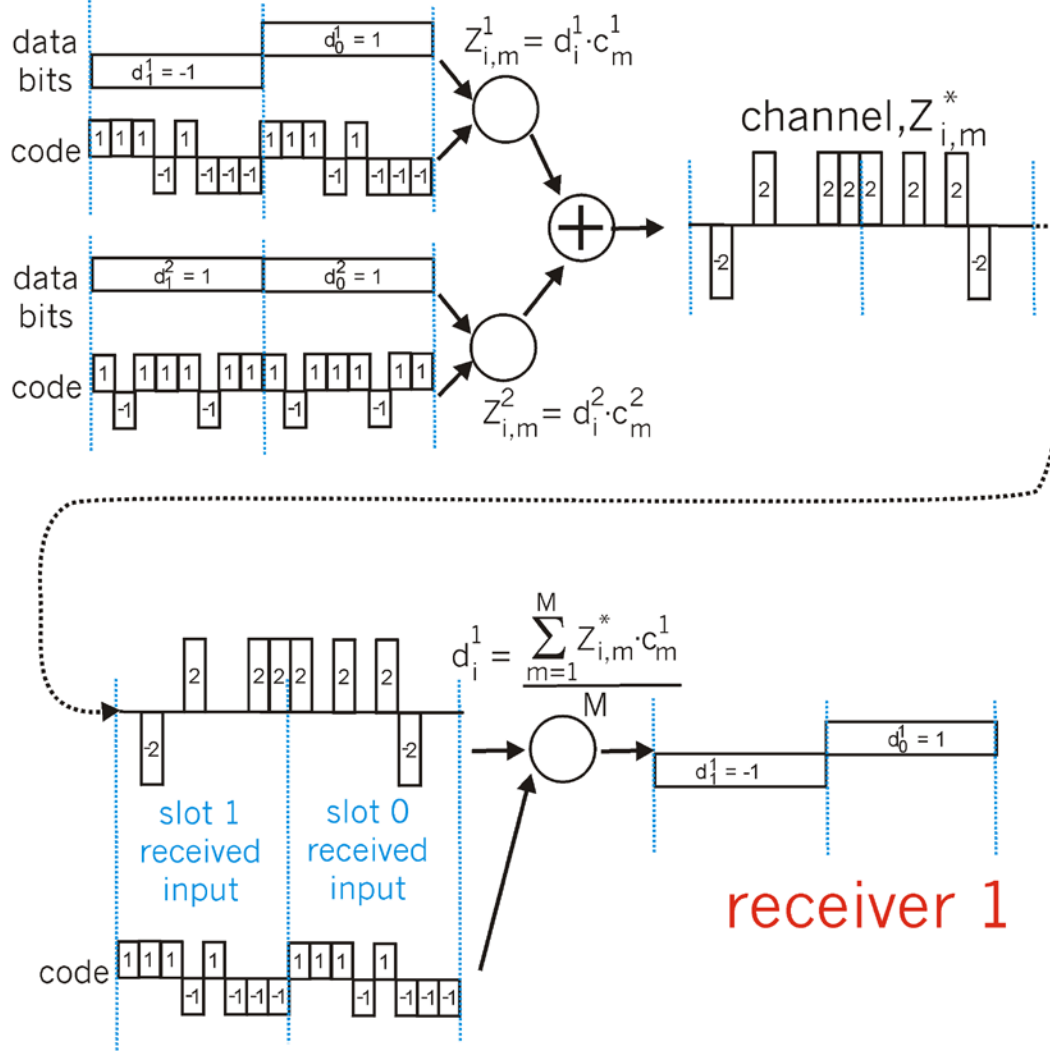
*Allows code division multiplexing*

- ❑ What is the meaning of vertical axis?

*Signal power*

# Two Sender CDMA Example

senders



○ Multiplier  
 ⊕ Add

## Student Questions

□ What are the codes for 0 and 1, respectively, in this depiction?  
 0 is -1. 1 is +1  
 User 1: 1 data = 11101000 code  
 User 2: 1 data = 10111011 code

□ Can you go over this diagram again?  
 Sure.

❖ What is the M in the equation at the bottom?  
 Number of code bits/data bit. M=8 in the example as shown.

❖ Page 541 in the book says that "if the senders' codes are chosen carefully, each receiver can recover the data sent by a given sender." Is there a simple example to illustrate that if you don't choose carefully, you can't complete the case where the receiver accepts the corresponding sender?

The correct statement is that if the sender codes are not orthogonal, the data cannot be recovered correctly. Orthogonality is defined as

$$\sum_{m=1}^M Z_{1,m} Z_{2,m} = 0$$

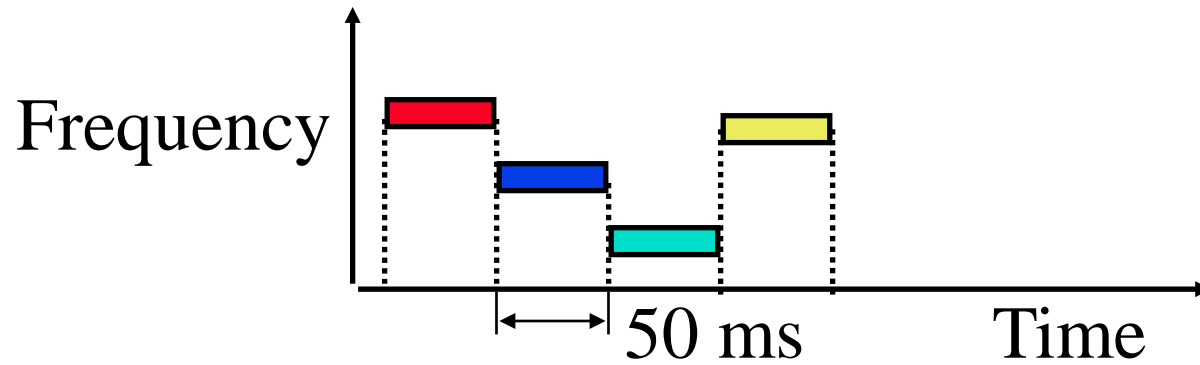
# Homework 7A: CDMA Coding

- [6 points] Two CDMA sender use the codes of  $(1, -1, 1, -1)$  and  $(1, -1, -1, 1)$ . First sender transmits data bit 1 while the 2<sup>nd</sup> transmits  $-1$  at the same time. What is the combined signal waveform seen by a receiver? Draw the waveform.

## Student Questions

- Which of those codes corresponds to 0 and 1?  
*1 data = code seq*  
*0 data = -code seq*  
**User 1:**  
*1 = {1, -1, 1, -1}*  
*0 = {-1, 1, -1, 1}*
-

# Frequency Hopping Spread Spectrum



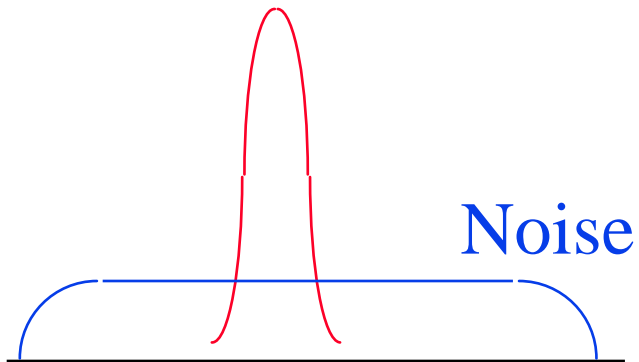
- ❑ Pseudo-random frequency hopping
- ❑ Spreads the power over a wide spectrum  
⇒ Spread Spectrum
- ❑ Developed initially for military
- ❑ Patented by actress Hedy Lamarr (1942)
- ❑ Narrowband interference can't jam

## Student Questions

- ❑ When you said "just keep hopping", does the receiver know how will the sender change the frequency all the time?  
*Sender changes the frequency all the time. Receiver knows what frequency will be when.*
- ❑ Does Frequency Hopping Spread Spectrum work better than Direct-Sequence Spread Spectrum since it's more common?  
*Both are used.*
- ❑ How do the two devices agree on the first number to send through the number generators?  
*The number is exchanged at the connection initiation.*
- ❑ How does the receiver keep track of the frequency changes from the transmitter?  
*Both sender and transmitter use the same random number generator with the same seed.*
- ❑ What is the purpose of using a random-generation formula? Is it for security purposes?  
*To avoid interference.*
- ❑ Is this called "pseudo-random" because it is not "truly random", if 2 people start with the same seed they will have the same sequence of numbers?  
*Yes.*

# Spectrum

Signal



(a) Normal

Noise



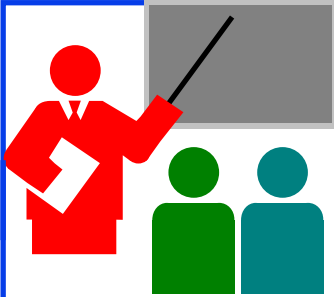
(b) Frequency Hopping

## Student Questions

- How do adversaries jam a non-frequency hopping signal?

*Transmitting at the same frequency at the same time*





# Review: Wireless Link Characteristics

1. Wireless is not the same as mobile. However, most mobile nodes are wireless.
2. Wireless signal is affected by shadows, multipath, interference, Doppler shift
3. A wireless network can be ad-hoc or infrastructure based.
4. Multi-hop ad-hoc networks are called MANET
5. It is not possible to do collision detection in wireless
6. Code division multiple access is commonly used in wireless

## Student Questions

- What is the difference between a MANET and a VANET?

*MANET = Mobile Ad-Hoc Network*

*VANET = Vehicular Area Network*

- Is it possible to do collision detection in ad-hoc mode?

*No. Ad-hoc is almost similar to Infrastructure based. The nodes perform the functions performed by the base station.*

- ❖ *Can you clarify in the slide you mention "It is not possible to do collision detection in wireless," but in the Q&A, your answer to the question "Is it possible to do collision detection in ad-hoc?" is "Yes." Which is correct?*

*I was wrong in Q&A. I have corrected the answer above.*



# Wireless LANs and PANs

- ❑ IEEE 802.11 Wireless LAN PHYs
- ❑ 4-Way Handshake
- ❑ IEEE 802.11 MAC
- ❑ 802.11 Frame Format
- ❑ 802.11 Frame Addressing
- ❑ 802.11 Rate Adaptation
- ❑ Power Management
- ❑ IEEE 802.15.4
- ❑ IEEE 802.15.4 MAC
- ❑ ZigBee Overview

## Student Questions

# IEEE 802.11 Wireless LAN PHYs

- ❑ **802.11**: 2.4 GHz, 1-2 Mbps
- ❑ **802.11b**: 2.4 GHz, 11 Mbps nominal
  - Direct sequence spread spectrum (DSSS) in physical layer
  - All hosts use the same chipping code
- ❑ **802.11a**: 5.8 GHz band, 54 Mbps nominal
- ❑ **802.11g**: 2.4 GHz band, 54 Mbps nominal
- ❑ **802.11n**: 2.4 or 5.8 GHz, Multiple antennae, up to 200 Mbps
- ❑ These are different PHY layers. All have the same MAC layer.
- ❑ All use CSMA/CA for multiple access
- ❑ All have base-station and ad-hoc network versions
- ❑ Supports multiple priorities
- ❑ Supports time-critical and data traffic
- ❑ Power management allows a node to doze off

## Student Questions

- ❑ Can you explain the benefits of raising the frequency from 2.4GHz to 5.8GHz

*More available spectrum*

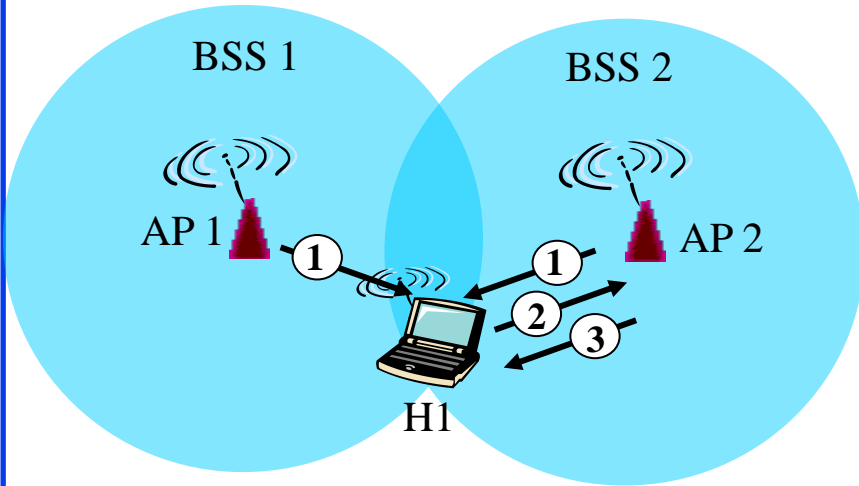
- ❑ Why 2.4/5.8GHz, not other frequencies?

*All frequencies are allocated.*

- ❑ Can you please explain the purpose of DSSS in physical layer?

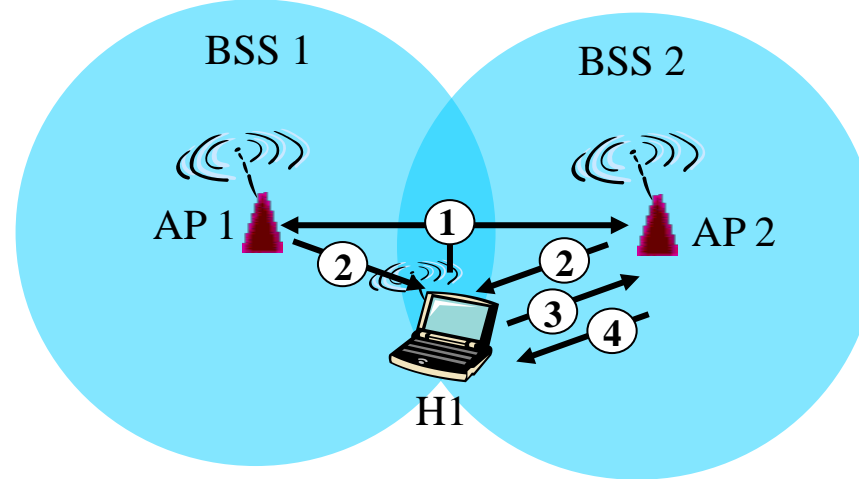
*Code division multiplexing*

# 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:

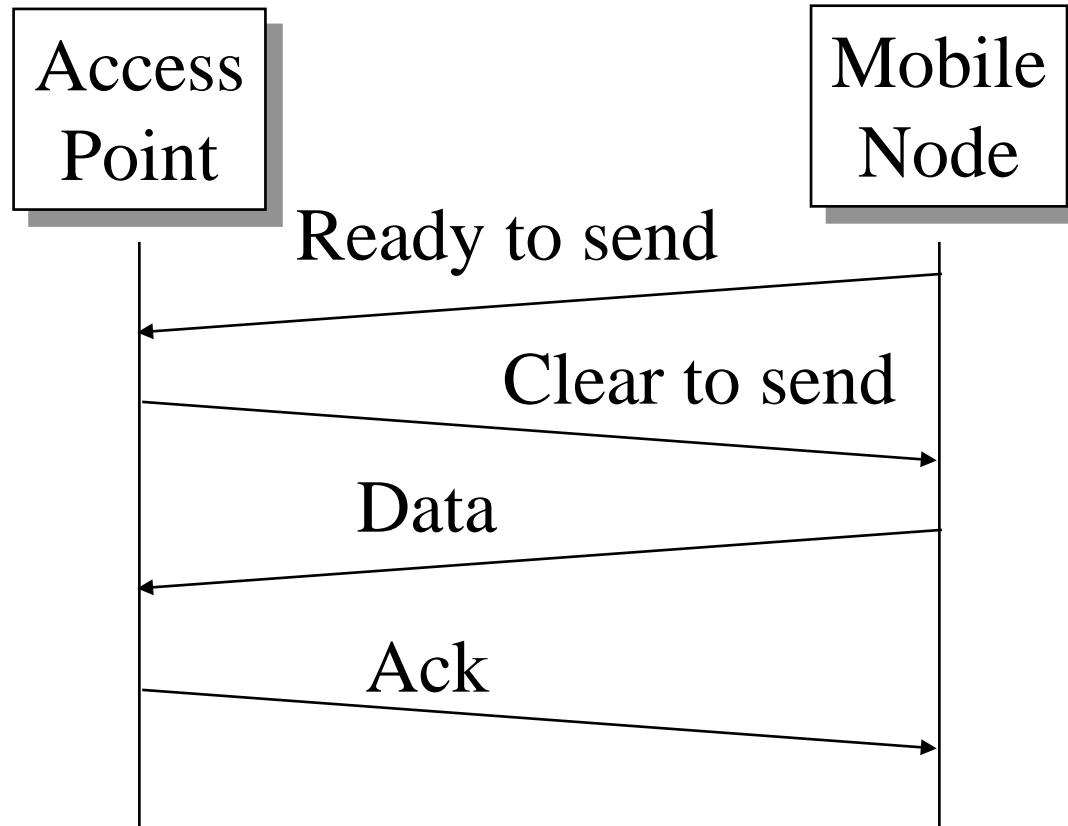
- (1) **Probe Request** frame broadcast from H1
- (2) Probes response frame sent from APs
- (3) Association Request frame sent: H1 to selected AP
- (4) Association Response frame sent: selected AP to H1

## Student Questions

- ❖ When we search for **Wi-Fi** on our device, we can see some "hidden networks," which require the name of that network (SSID) to connect. Do these hidden networks have anything to do with passive/active scanning (just guessing)?

*When setting up your network, you can choose to announce or not announce your SSID. These hidden networks respond to their names but do not announce their names. This increases security.*

# 4-Way Handshake



## Student Questions

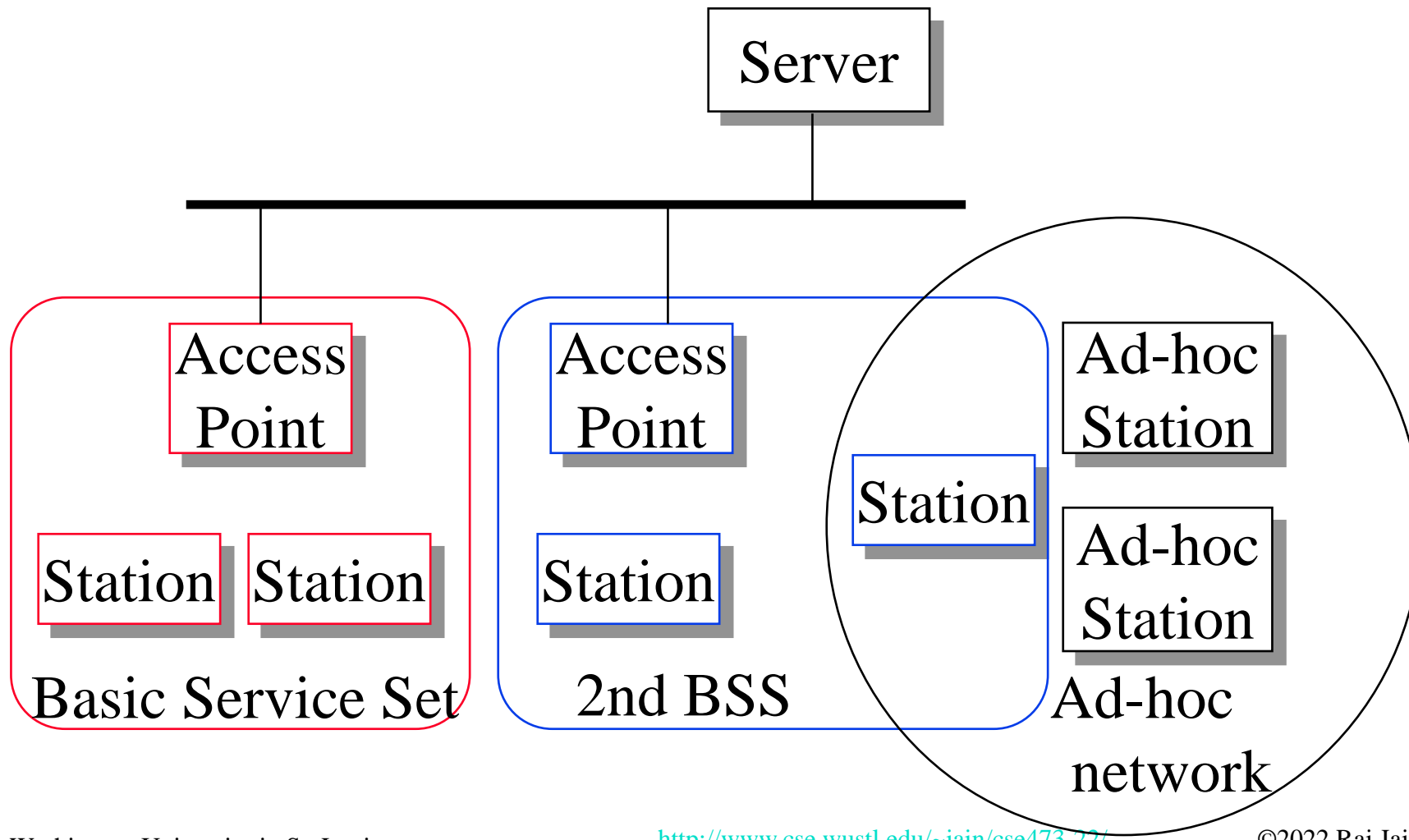
- Why don't we do a 3-way handshake like TCP?  
*In TCP, multiple users do not interfere with each other.*

# IEEE 802.11 MAC

- ❑ Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
- ❑ Listen before you talk. If the medium is busy, the transmitter backs off for a random period.
- ❑ Avoids collision by sending a short message:  
Ready to send (RTS)  
RTS contains dest. address and duration of message.  
Tells everyone to backoff for the duration.
- ❑ Destination sends: Clear to send (CTS)
- ❑ Can not detect collision  $\Rightarrow$  Each packet is acked.
- ❑ MAC level retransmission if not acked.

## Student Questions

# IEEE 802.11 Architecture



## Student Questions

# Architecture (Cont.)

- ❑ Basic Service Area (BSA) = Cell  
Area: Geographical area = a room, or a building
- ❑ Each BSA may have several wireless LANs
- ❑ Extended Service Area (ESA) = Multiple BSAs interconnected via Access Points (AP) = Multiple rooms in your home with different extenders advertising the same SSID
- ❑ Basic Service Set (BSS)  
= Set of stations associated with an AP =  $\{MAC_1, \dots, MAC_n\}$ .  
Each BSS has a Service Set ID (SSID), e. g., WUSTL-Guest
- ❑ Extended Service Set (ESS)  
= Set of stations in an ESA
- ❑ Ad-hoc networks coexist and interoperate with infrastructure-based networks.

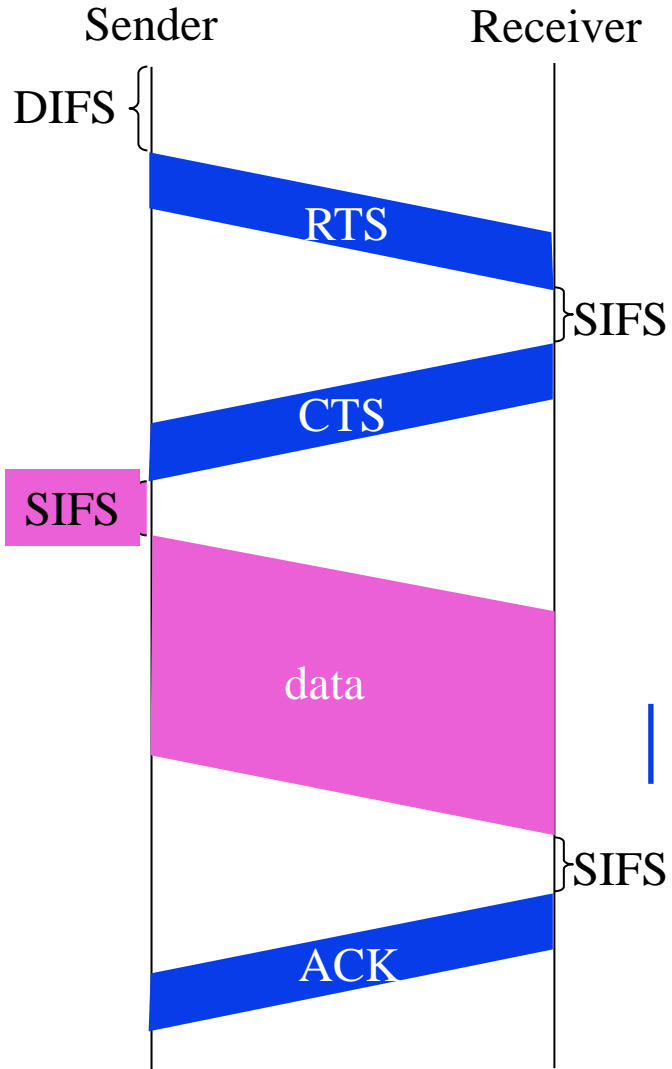
## Student Questions

- ❑ What is the difference between SSID and BSSID?

*BSSID is the SSID of the BSS.*



# Transmission Example



SIFS, DIFS are intervals set by the standards. 11b and 11ac have different values.

RTS, CTS, ACK are each one slot time long.

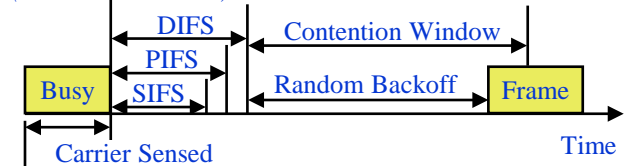
Each frame has a duration field.

Every frame is heard by every one.

## Student Questions

- What is DIFS and what are 11b and 11ac?

*DIFS = Distributed Inter-Frame Spacing*  
(See new slide 7-63)



- Initial inter-frame space (IFS)
- Highest priority frames, e.g., Acks, use short IFS (SIFS)
- Medium priority time-critical frames use "Point Coordination Function IFS" (PIFS)
- Asynchronous data frames use "Distributed coordination function IFS" (DIFS)

- How long is one slot time here?

*Each standard defines the slot time.*

# Homework 7B: WiFi Transmission

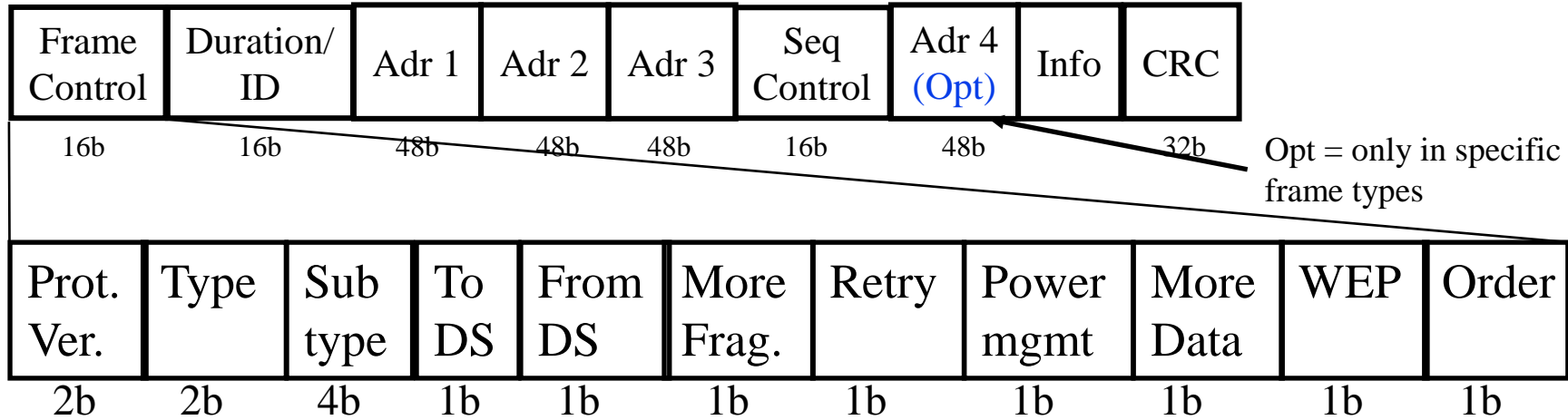
- ❑ [6 points] Suppose an 802.11b station is configured always to reserve the channel with the RTS/CTS sequence. Suppose this station suddenly wants to transmit 1,200 bytes of data, and all other stations are idle at this time. Using SIFS of  $13\mu\text{s}$  and DIFS of  $60\mu\text{s}$ , ignoring propagation delay and assuming no bit errors, calculate the time required to transmit the frame and receive the acknowledgment.
- ❑ Hint: For 802.11b, a frame without data (RTS/CTS/Ack) is 64 bytes long, and the transmission rate is 11 Mbps.

Ref: Problem P7

## Student Questions

- ❖ Could you go over HW 7B? Is there a specific formula we use to calculate time?  
*You need to know the bit rate of 802.11b. It is 11 Mbps.*

# Wi-Fi Frame Format



- Type: Control, management, or data
- Sub-Type: Association, disassociation, re-association, probe, authentication, de-authentication, CTS, RTS, Ack, ...
- Retry/retransmission
- Going to Power Save mode
- More buffered data at AP for a station in power save mode
- Wireless Equivalent Privacy (Security) info in this frame
- Strict ordering

## Student Questions

- Why is there no offset?  
*Header size is known.*
- Given the more frags field, how does fragmentation work with Wi-Fi? Is there still the interframe space between fragments?  
*Seq. Control = Sequence number + Fragment #*  
*More data => Do not go to sleep. You have more coming (nothing to do with fragmentation).*
- What are the subtypes here?  
*Different types of control and management frames.*

# MAC Frame Fields

## ❑ Duration/Connection ID:

- If used as duration field, indicates time (in  $\mu\text{s}$ ) channel will be allocated for successful transmission of MAC frame.  
Includes time until the end of Ack
- In some control frames, contains association or connection identifier

## ❑ Sequence Control:

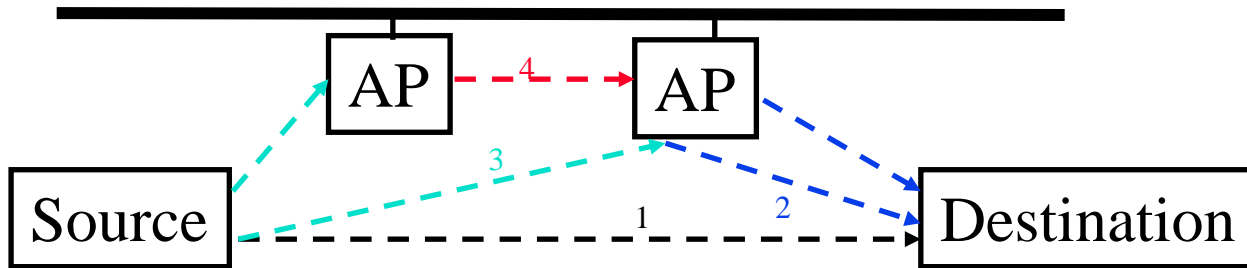
- 4-bit fragment number subfield
  - ❑ For fragmentation and reassembly
- 12-bit sequence number
- Number frames between given transmitter and receiver

## Student Questions

- ❑ What is the function of MAC frame in Internet?  
*Mac Frame = Wi-Fi Frame*

# 802.11 Frame Address Fields

- All stations filter on “Address 1”



	To Distribution System	From Distribution System	Address 1	Address 2	Address 3	Address 4
1	0	0	Destination Address	Source Address	BSS ID	-
2	0	1	Destination Address	BSS ID	Source Address	-
3	1	0	BSS ID	Source Address	Destination Address	-
4	1	1	Receiver AP Address	Transmitter AP Address	Destination Address	Source Address

## Student Questions

- Why doesn't the last row need a BSS ID?
- *BSS ID is basically a multicast to all base stations on this SSID. Any AP can receive and forward. In the last row, the packet is addressed to a specific AP identified by the receiver address.*
- Is the BSS ID the Access Point address, why first row need BSS ID?

*In General:*

*Adr1 = This hop Wi-Fi Receiver*

*Adr2 = This hop Wi-Fi Transmitter*

*Adr3 = BSSID\*/Source\*/Destination\* (in order)*

*Adr4 = Source\**

*\*if not specified in the earlier fields*

*A Wi-Fi node can be on multiple BSS. In other cases, we know the BSS from other addresses. In case 1, It needs to be explicitly identified.*

*Analogy: Destination: New York City*

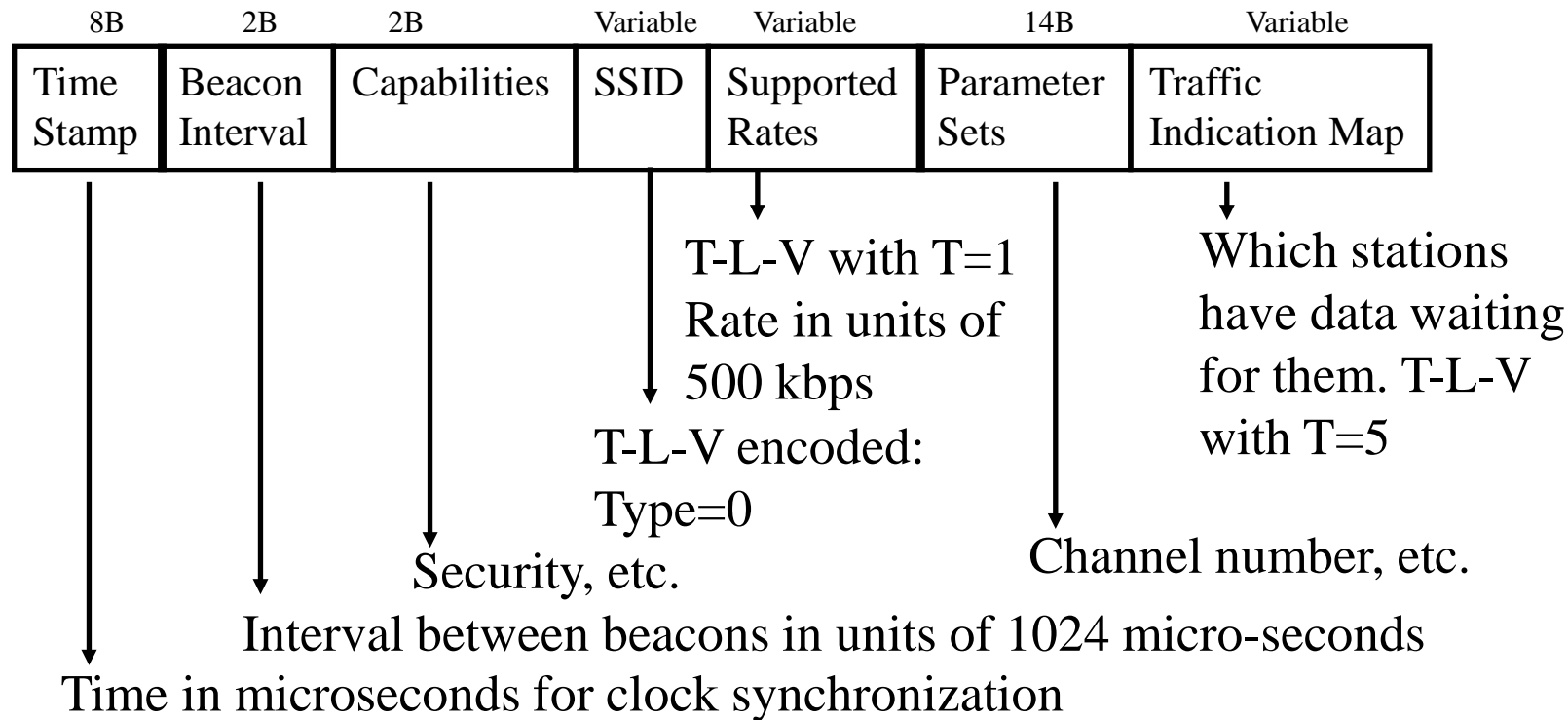
*BSS ID: Airport (LaGuardia or JFK)*

*AP Address: Airline*

*Case 1 is private plane.*

# Beacon Frame Format

- Info field in the 802.11 frame (after Address 4)



## Student Questions

- Why do SNR ratios use deciBels over another unit of measurement?

Ratios are divisions. It is easy to deal with ratios in log scale. dB is a log scale unit.

- Is there a tradeoff between SNR and BER? Is there an extent that an SNR that is too high starts to cause problems (like in machine learning with bias variance tradeoff)?

$SNR = Cause$

$BER = Effect$

Coding and retransmission decide acceptable BER  
 $\Rightarrow SNR$

- What kinds of values are stored in SSID's '\v'?

Sample SSID values are WUSTL 2.0, WUSTL Guest, Public Free Wi-Fi, etc.

- Can multiple networks have the same SSID? If yes, how would a host be able to tell?

Multiple AP can serve the same SSID but multiple owners cannot have the same SSID in the same location. Like two different Raj Jains living in my house address.

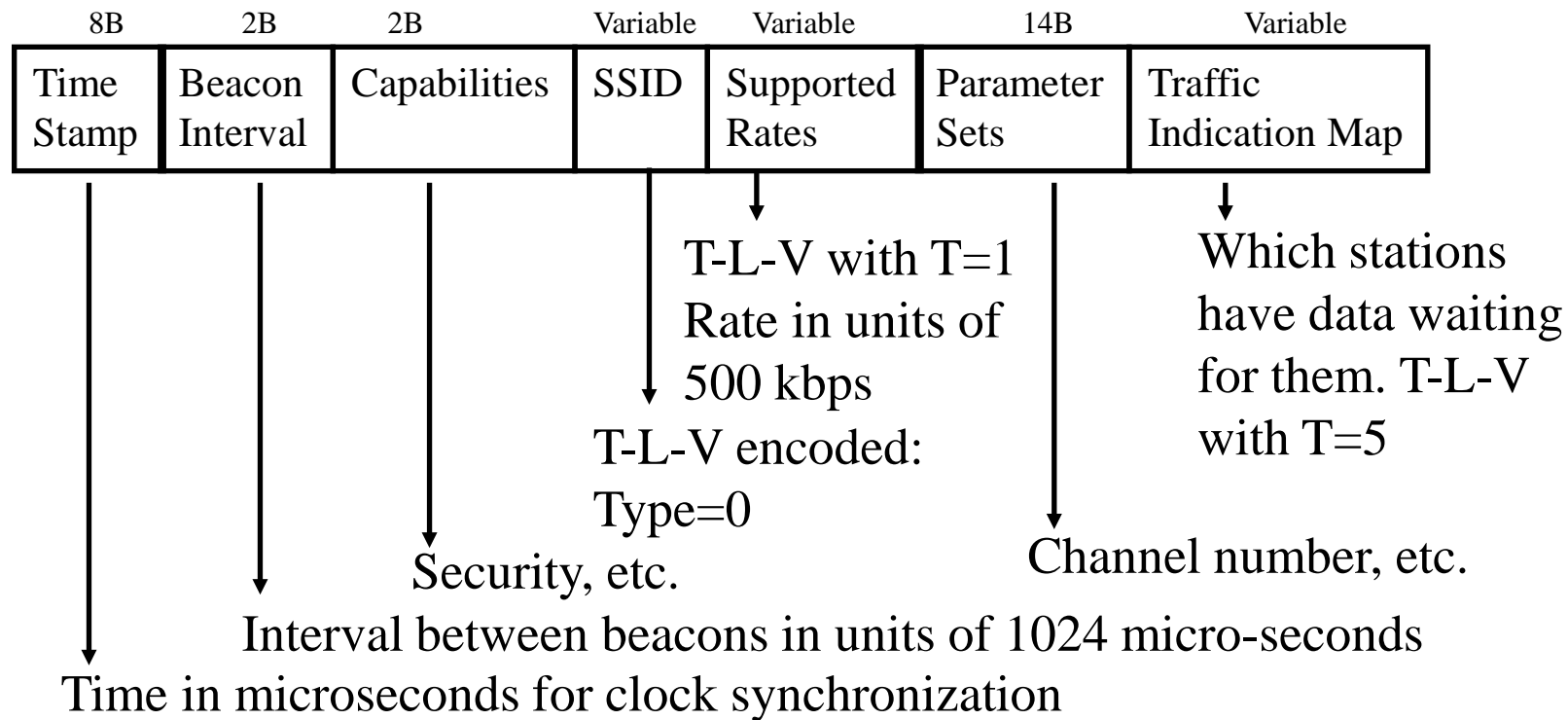
- Could you explain TLV again?

Type-Length-Value.

Example: Type=0, Length=9, Value=WUSTL 2.0

# Beacon Frame Format

- Info field in the 802.11 frame (after Address 4)



## Student Questions

- How do you separate T, L, and V from each other in the SSID and Supported Rates fields? If the V has a variable length, how do you know how many bits are required for L?

*Type: SSID, Rate or Map*

*Length: How many bytes are in the value*

*Value: Actual value of the field*

*Example: Student Names*

*Type: First, Last, Middle, Suffix*

*Length: 3*

*Value: Raj*

- Can you explain more about capabilities in terms of security?

*Capabilities: WEP, WPA, WPA2, ...*

- Can you comment on the tradeoff between SNR and BER?

*SNR=Signal to Noise Ratio*

*BER= Bit Error Rate*

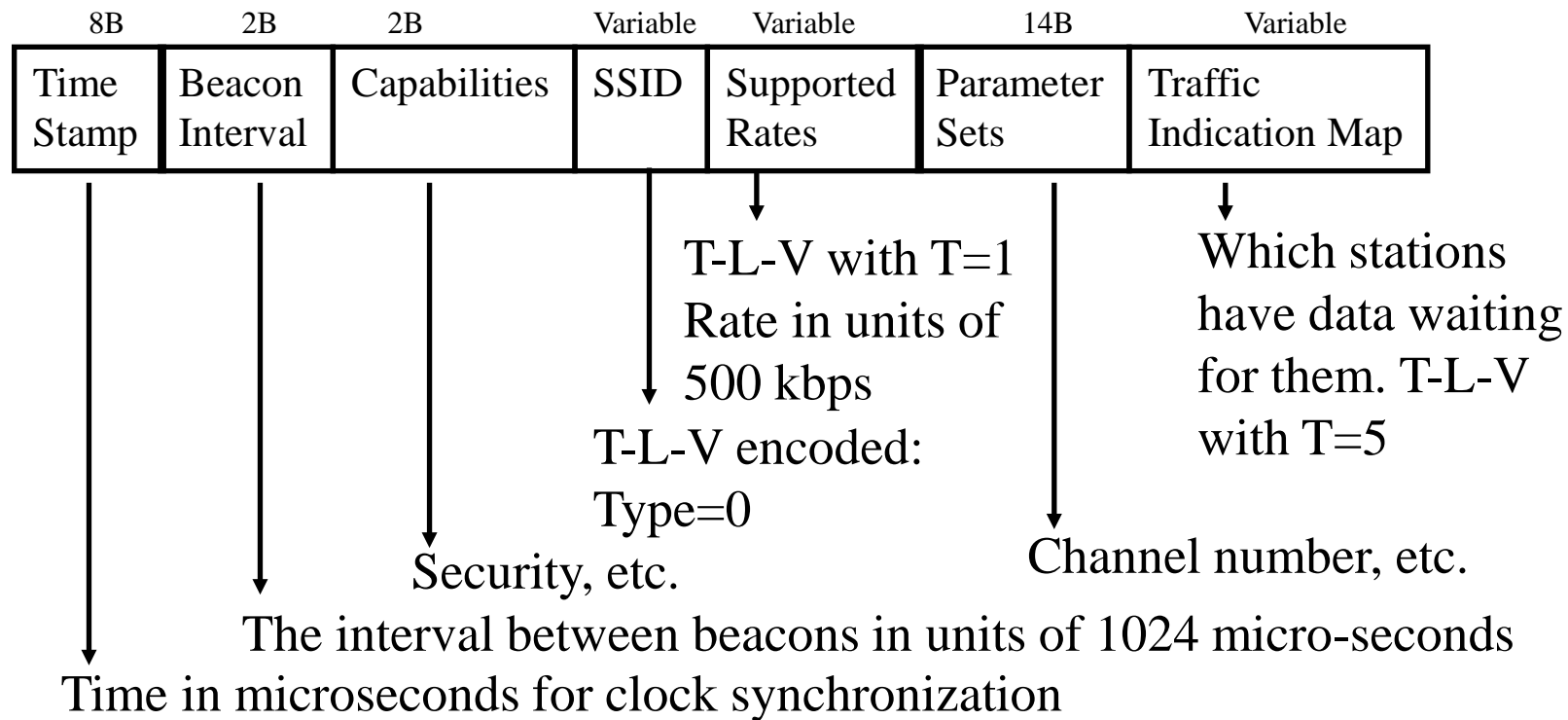
*Higher noise => Lower Signal to Noise*

*=> More bit errors*

*There is no trade-off here. SNR causes BER.*

# Beacon Frame Format

- Info field in the 802.11 frame (after Address 4)



## Student Questions

- ❖ Can you go over T-L-V encoding again?  
 $T=L-V=\{Type, Length, Value\}$   
 A vector of 3 elements. The first element is the type, 2<sup>nd</sup> element is the length, and 3<sup>rd</sup> element is the value of the field. It is commonly used for variable-length fields. In this slide:  
 Type:

0=SSID  
 1=Rate  
 ...  
 5=Map



# Lab 7: WiFi

[14 Points] Download the Wireshark traces from

<http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip>

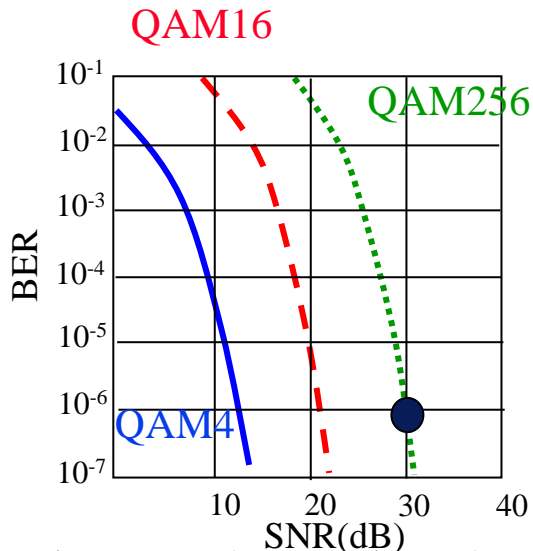
Open *Wireshark\_802\_11.pcap* in Wireshark. Select **View → Expand All**.

Answer the following questions. There is no need to attach screen captures.

1. Frame 1 is a beacon frame. Ignore the first 24 bytes. (The frame control field is 80:00.) What is the SSID of the access point that is issuing this beacon frame?
2. What (in hexadecimal notation) is the source MAC address on Frame 1.
3. What (in hexadecimal notation) is the destination MAC address on the Frame 1?
4. What (in hexadecimal notation) is the MAC BSS ID in Frame 1?
5. Frame 50 is a Probe Request and Frame 51 is a Probe response. What are the sender, receiver and BSS ID MAC addresses in these frames? What is the purpose of these two types of frames?

## Student Questions

# 802.11 Rate Adaptation



QAM=Quadrature Amplitude Modulation

$\text{QAM}2^n = n \text{ bits/Hz}$

dB = Deci-Bel

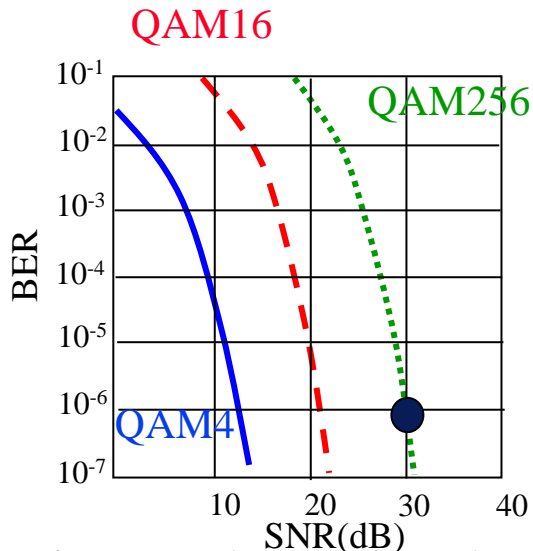
$$= 10 \log_{10} \frac{\text{Power Out}}{\text{Power In}}$$

- ❑ Base station and mobile dynamically change transmission rate (physical layer modulation technique) as mobile moves, SNR varies
- ❑ SNR decreases  $\Rightarrow$  BER increase as node moves away from base station
- ❑ When BER becomes too high, switch to lower transmission rate but with lower BER

## Student Questions

- ❑ Why does wireless network coding change due to the BER change?  
*Use less bits per second if BER is high*
- ❑ Does the station have to keep track of all mobiles it connects to? Wouldn't that require heavy computation power and storage?  
*Yes. If you are talking to 5 people at ones on a conference call, you need to keep track of who said what.*
- ❑ Does 20 megahertz a standard? If we want to send things faster in a short time, can a temporary raise this to 200 or more?  
*20 MHz is a standard channel width. Some may use more than one channel. Like fitting multiple nodes in a single box.*
- ❑ Does the "dB" in the slide relate to acoustic units "db"?  
*dB = deci-Bel  
DB = Deca-Bel  
B is the name and so always capital.*
- ❑ How do we maximize SNR?  
*By increasing the signal power. But that may increase your battery consumption.*

# 802.11 Rate Adaptation



QAM=Quadrature Amplitude Modulation

$\text{QAM}2^n = n \text{ bits/Hz}$

dB = Deci-Bel

$$= 10 \log_{10} \frac{\text{Power Out}}{\text{Power In}}$$

- ❑ Base station and mobile dynamically change transmission rate (physical layer modulation technique) as mobile moves, SNR varies
- ❑ SNR decreases  $\Rightarrow$  BER increase as node moves away from base station
- ❑ When BER becomes too high, switch to lower transmission rate but with lower BER

## Student Questions

- ❑ Is it similar to TCP congestion control?  
*Not at all.*
- ❑ What causes SNR/BER to change?  
*If more devices come into the same area, noise increases  $\Rightarrow$  SNR decreases.  $\Rightarrow$  BER increases.*
- ❑ Is there a benefit to measuring the power in log units?  
*Yes. Everything here multiplies. In log units, they add.*
- ❖ Chapter 7.2: Why does higher SNR result in lower BER?  
*SNR=Signal/Noise ratio  
Higher SNR = Higher Signal or Lower Noise or both  
Higher signal results in lower bit errors*

# Power Management

- ❑ A station can be in one of three states:
  - Transmitter on
  - Receiver only on
  - Dozing: Both transmitter and receivers off.
- ❑ Access point (AP) buffers traffic for dozing stations.
- ❑ AP announces which stations have frames buffered. Traffic indication map included in each beacon. All multicasts/broadcasts are buffered.
- ❑ Dozing stations wake up to listen to the beacon. If there is data waiting for it, the station sends a poll frame to get the data.

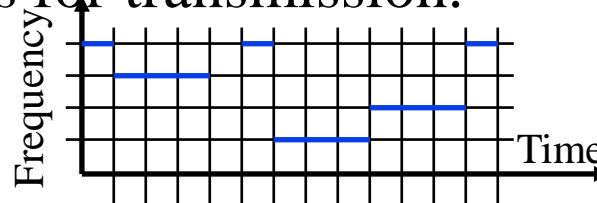
## Student Questions

- ❑ How large is the buffer size in AP? Will it be too much data when the station becomes dozing for a long time?  
*If you doze, you lose. AP will save only a few frames.*

# Bluetooth



- ❑ Started with Ericsson's Bluetooth Project in 1994
- ❑ Named after Danish king Herald Blatand (AD 940-981) who was fond of blueberries
- ❑ Radio-frequency communication between cell phones over short distances
- ❑ IEEE 802.15.1 approved in early 2002 is based on Bluetooth
- ❑ Key Features:
  - Lower Power: 10  $\mu$ A in standby, 50 mA while transmitting
  - Cheap: \$5 per device
- ❑ A piconet consists of a master and several slaves. Master determines the timing and polls slaves for transmission.
- ❑ Frequency hopping spread spectrum



## Student Questions

- ❑ Does being the primary node on a piconet have advantages? Since it is coordinating, it will need to spend more energy as far as I can think of, which is bad for that device.

*You are right. Only bigger devices can become the primary node. For example, Phone vs. headset. Computer vs. Phone.*

- ❑ Is piconet an example of ad-hoc?  
*No. In ad-hoc, there is no master.*
- ❑ Do Bluetooth transmitters use MAC addresses or IP addresses to distinguish each other?

*Yes, they use 48-bit IEEE 802 addresses (similar to Ethernet and Wi-Fi).*

- ❑ Can the number of participating hosts in a Bluetooth network be more than two?

*Yes. You can connect two headsets to some phones at the same time.*

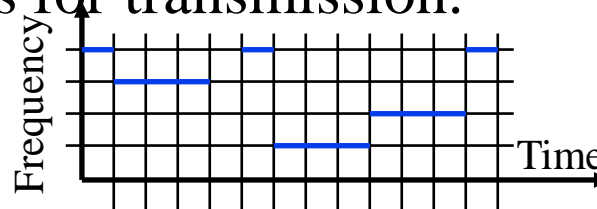
- ❑ How does Bluetooth Low Energy (BLE) use even less energy than regular Bluetooth?

*Sleep more.*

# Bluetooth



- ❑ Started with Ericsson's Bluetooth Project in 1994
- ❑ Named after Danish king Herald Blatand (AD 940-981) who was fond of blueberries
- ❑ Radio-frequency communication between cell phones over short distances
- ❑ IEEE 802.15.1 approved in early 2002 is based on Bluetooth
- ❑ Key Features:
  - Lower Power: 10  $\mu$ A in standby, 50 mA while transmitting
  - Cheap: \$5 per device
- ❑ A piconet consists of a master and several slaves. Master determines the timing and polls slaves for transmission.
- ❑ Frequency hopping spread spectrum



## Student Questions

- ❑ The Bluetooth assigns different frequencies to multiple devices.

*No. Everyone uses the entire 2.4 GHz band*

- ❑ How wide is the band?

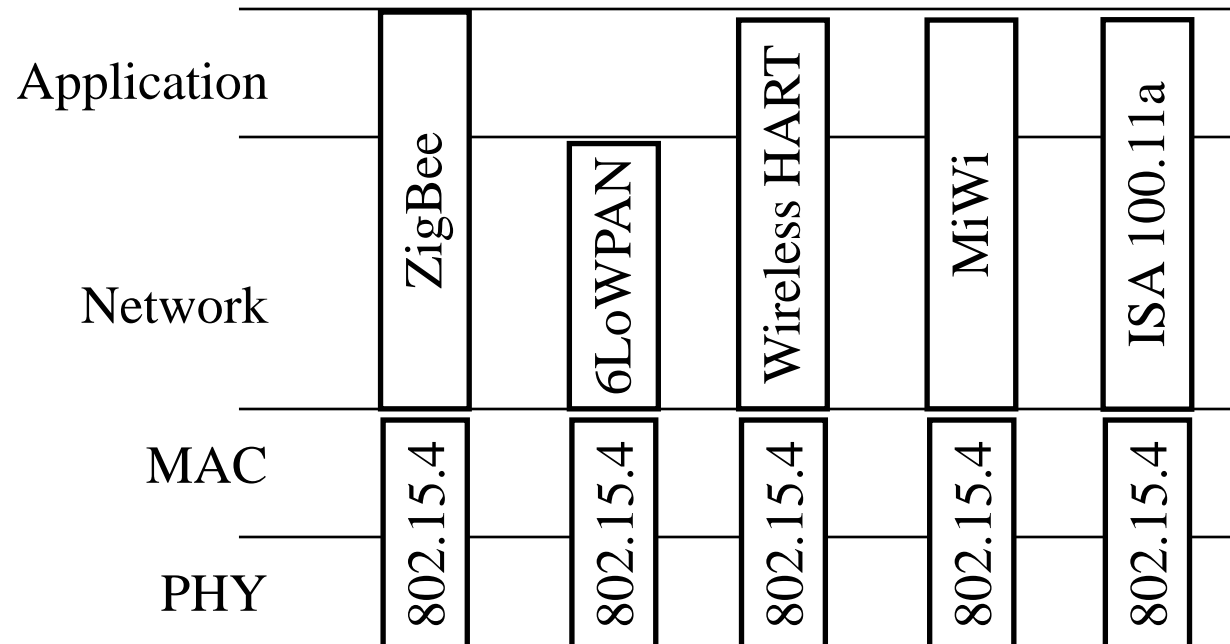
*2400-2483.5 MHz*

- ❖ Bluetooth is an example of ad-hoc. However, piconet based on Bluetooth is no longer an example of ad-hoc. Is this right?

*Ad-hoc = Peer-to-peer with no primary node  
Bluetooth nodes dynamically select a primary node.*

# IEEE 802.15.4

- ❑ Low Rate Wireless Personal Area Network (LR-WPAN)
- ❑ Used by several “Internet of Things” protocols:  
ZigBee, 6LoWPAN, Wireless HART, MiWi, and ISA 100.11a
- ❑ Lower rate, short distance  $\Rightarrow$  Lower power  $\Rightarrow$  Low energy



## Student Questions

- ❑ What's the distinction between power and energy?

*Power is the rate of Energy usage.*

*Power is measured in Watts.*

*Energy is measured in Joules.*

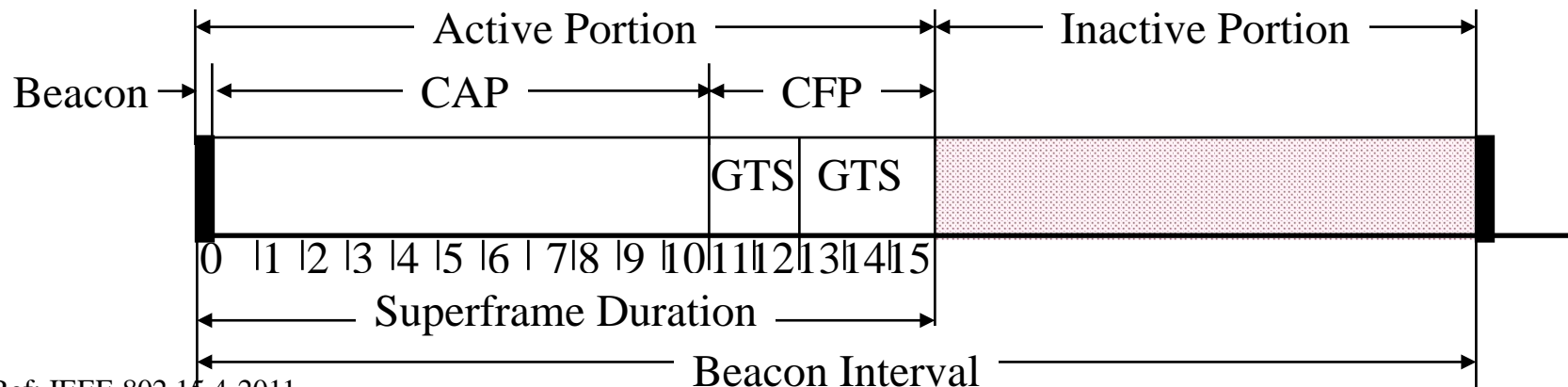
*Analogy: If you spend \$100 per day. You will exhaust your \$1000 bank balance in 10 days.*

*Bank balance is the Energy. \$100 is your power.*

# IEEE 802.15.4 MAC

## Beacon-Enabled CSMA/CA

- ❑ Coordinator sends out beacons periodically
- ❑ Part of the beacon interval is inactive  $\Rightarrow$  Everyone sleeps
- ❑ Active interval consists of 16 slots
- ❑ Contention Access Period (CAP). Slotted CSMA.
- ❑ Contention Free Period (CFP)
  - Guaranteed Transmission Services (GTS): For real-time services. Periodic reserved slots.



Ref: IEEE 802.15.4-2011

Washington University in St. Louis

<http://www.cse.wustl.edu/~jain/cse473-22/>

©2022 Raj Jain

## Student Questions

- ❑ What is "superframe duration"?  
*16 slots, as shown.*
- ❑ Does the coordinator here mean access point?  
*They call it Hub.*



# ZigBee Overview

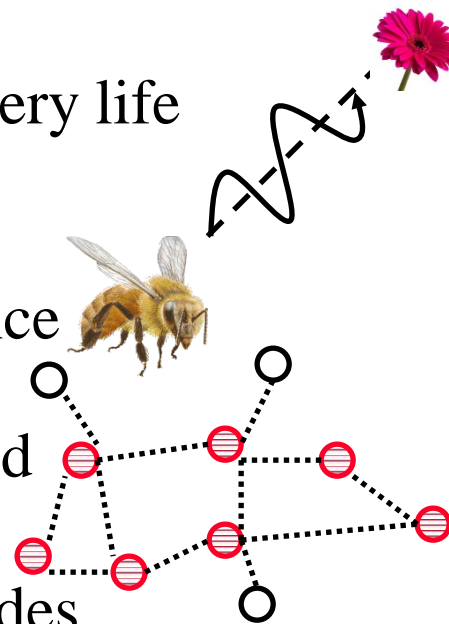
- ❑ Industrial monitoring and control applications requiring small amounts of data, turned off most of the time (<1% duty cycle), e.g., wireless light switches, meter reading
- ❑ Ultra-low power, low-data rate, multi-year battery life
- ❑ **Range:** 1 to 100 m, up to 65000 nodes.
- ❑ IEEE 802.15.4 MAC and PHY.  
Higher layer, interoperability by ZigBee Alliance
- ❑ Named after zigzag dance of the honeybees  
Direction of the dance indicates location of food
- ❑ Multi-hop ad-hoc mesh network

**Multi-Hop Routing:** message to non-adjacent nodes

**Ad-hoc Topology:** No fixed topology. Nodes discover each other

**Mesh Routing:** End-nodes help route messages for others

**Mesh Topology:** Loops possible



## Student Questions

- ❑ Can you explain more on the difference between Mesh Routing and Mesh Topology?

*Routing = Method.*

*End nodes route other end node's packets*

*Topology: The nodes are connected not in a star or bus but as a mesh.*

*It is possible to have all 4 combination of routing and topologies.*

- ❑ Is the increased distance of ZigBee because of multi-hops? What happens if there are only two nodes 100m apart?

*They will each will need enough power to reach 100 m. However, if there are hundreds of nodes, they will each need power to go, say, 1 m and still be able to talk to someone 100m away.*

- ❑ Does this mean that ad-hoc topology can't have a loop?

*Dictionary meaning of "ad-hoc" is "created or done as necessary." or not set in advance. They can have loops.*

- ❑ What distinguishes ad-hoc from mesh topology?

*Mesh: There is a fixed topology. It may be a linear bus or star, or a triangle, etc.*

# ZigBee Overview

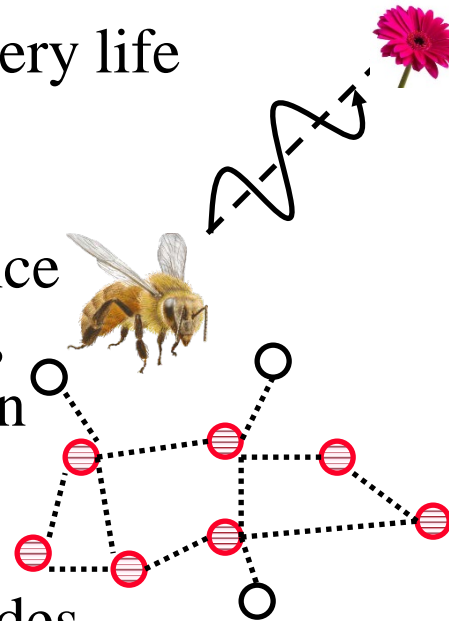
- ❑ Industrial monitoring and control applications requiring small amounts of data, turned off most of the time (<1% duty cycle), e.g., wireless light switches, meter reading
- ❑ Ultra-low power, low-data rate, multi-year battery life
- ❑ **Range:** 1 to 100 m, up to 65000 nodes.
- ❑ IEEE 802.15.4 MAC and PHY.  
Higher layer, interoperability by ZigBee Alliance
- ❑ Named after the zigzag dance of the honeybees  
The direction of the dance indicates the location of the food
- ❑ Multi-hop ad-hoc mesh network

**Multi-Hop Routing:** message to non-adjacent nodes

**Ad-hoc Topology:** No fixed topology. Nodes discover each other

**Mesh Routing:** End-nodes help route messages to others

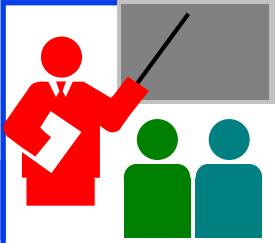
**Mesh Topology:** Loops possible



## Student Questions

- ❖ How do devices that are turned off most of the time know when to turn themselves back on?

One part of the receiver comes on frequently to listen to beacons. Beacons contain the list of nodes that have frames waiting. That part then wakes up the node, telling the primary to send those frames. After receiving the frame, most of the node goes back to sleep.



# Review: Wireless LANs and PANs

1. IEEE 802.11 PHYs: 11, 11b, 11g, 11a, 11n, ...
2. IEEE 802.11 MAC uses CSMA/CA with a 4-way handshake: RTS, CTS, data, and ack
3. IEEE 802.11 network consists of ESS consisting of multiple BSSs each with an AP.
4. 802.11 Frame Format may have up to 4 addresses and includes final destination's MAC which may not be wireless
5. Power management allows stations to sleep.
6. Bluetooth uses frequency hopping spread spectrum
7. IEEE 802.15.4 PHY layer allows coordinators to schedule transmissions of other nodes
8. ZigBee uses IEEE 802.15.4

Ref: Section 7.3, Review Exercises R5-R12

Washington University in St. Louis

<http://www.cse.wustl.edu/~jain/cse473-22/>

©2022 Raj Jain

## Student Questions

- If APs buffer traffic for dozing stations, do the APs also send TCP acks on behalf of the dozing stations? If not, then it seems like there will be a lot of timeouts and redundant TCP segments.

*No APs are MAC-layer devices. They do not understand L3 or L4 and do not send any TCP acks. They may send L2 MAC Acks. Stations should wake up frequently enough to avoid TCP timeouts, if they have a TCP connection.*

- Does Zigbee also use frequency hopping?  
*Yes.*



# Cellular Networks

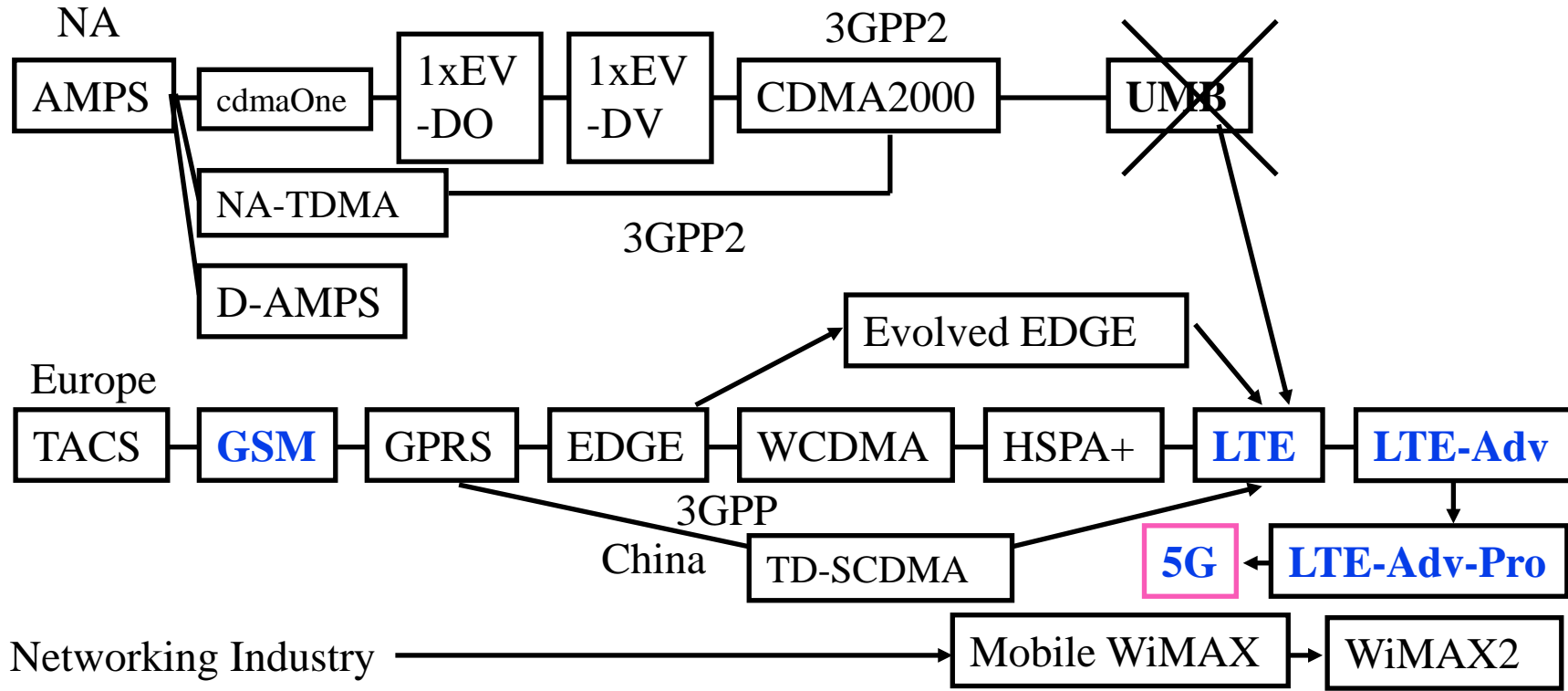
- ❑ Evolution of Cellular Technologies
- ❑ GSM Cellular Architecture
- ❑ Evolved Packet System (EPS)

## Student Questions

- ❑ Why is it called "cellular"? from the topology?

*Yes. They divide the area in to cells.*

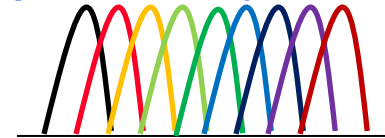
# Cellular Telephony Generations



Analog FDMA	Digital TDMA CDMA	CDMA		OFDMA+ MIMO		
Voice 1G	Voice 2G	Voice+Data 2.5G	Voice+Data 3G	Voice+HS Data 3.5G	All-IP 4G	

## Student Questions

- Could you briefly explain what OFDMA is?  
*Orthogonal Frequency Division Multiplexing*  
A large number of subcarriers are orthogonal (all others are zero when one peaks). A user is assigned several subcarriers.



- Regardless of the correction, is analog faster than digital? Since it doesn't need to convert the waveform to 0 or 1, then translate them back to the waveform signal.

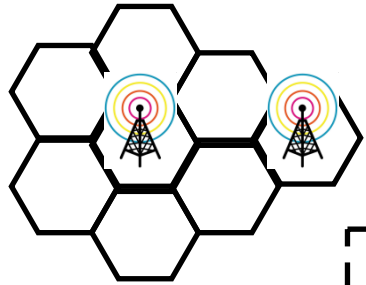
*Signal travels at the same speed regardless of analog or digital. If you mean analog is "less complex," then yes, analog is less complex but it loses a lot more information a lot faster.*

- What is TD-SCDMA? Is it only used by China?

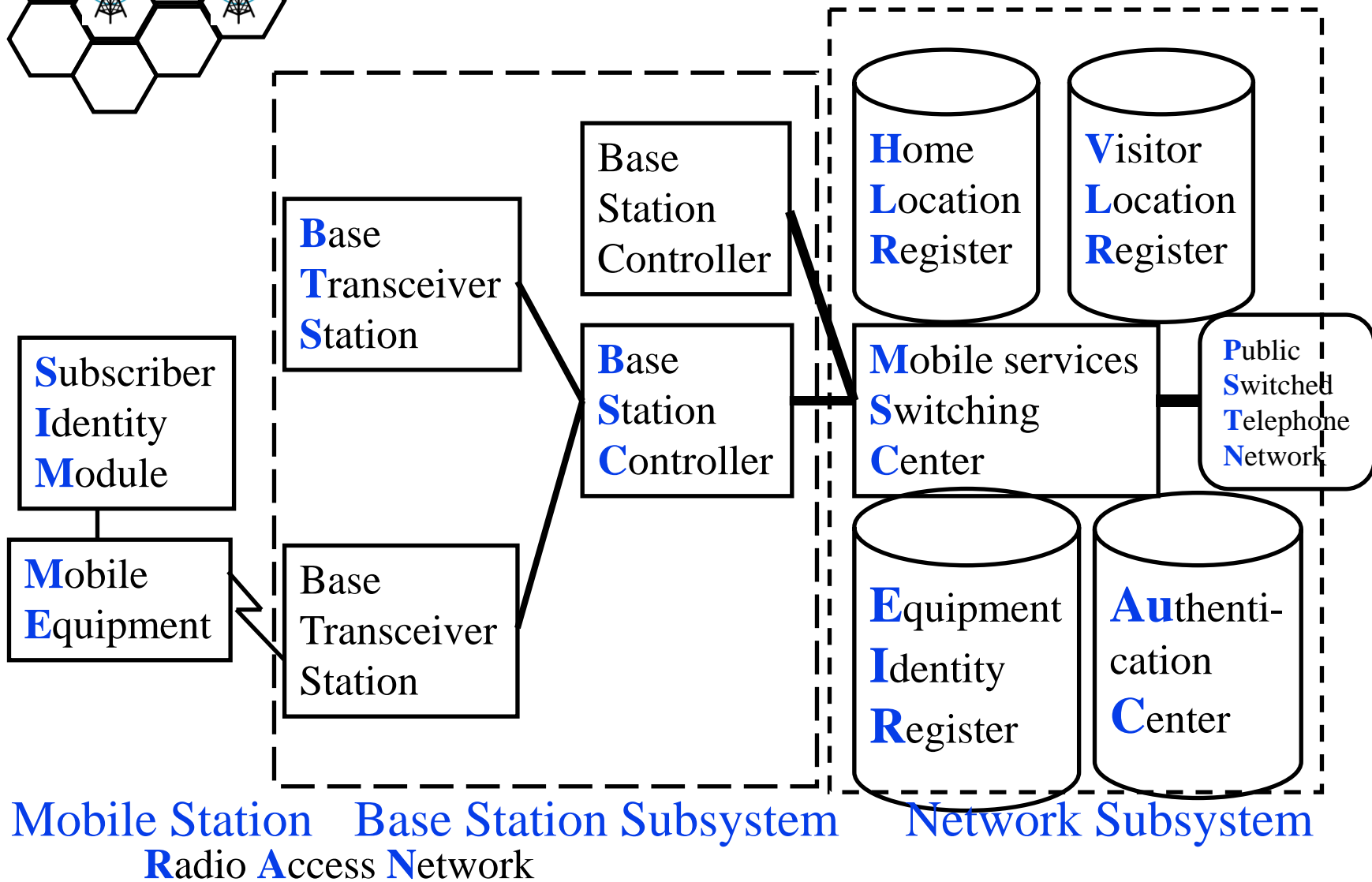
*Yes.*

- In general, does 5G still use OFDMA+MIMO?

*Yes. The main change is in the use of IP and smaller cells.*



# GSM Cellular Architecture



## Student Questions

- Does each carrier have its PSTN or do all share a common PSTN?

*Each carrier is supposed to have its PSTN. However, increasingly they have started sharing using SDN or other virtualization techniques.*

- So whatever device has my SIM card gains access to that provider's network, or do you need to configure it somehow?

*Any device should be able to use any SIM cards. However, many carriers restrict phone SIMs to phones and do not allow them to be used on iPad. This is against the original intent of SIM.*

# Cellular Architecture (Cont.)

- ❑ Base station controller (BSC) and Base transceiver station (BTS)
- ❑ One BTS per cell.
- ❑ One BSC can control multiple BTS.
  - Allocates radio channels among BTSs.
  - Manages call handoffs between BTSs.
  - Controls handset power levels
- ❑ Mobile Switching Center (MSC) connects to PSTN and switches calls between BSCs. Provides mobile registration, location, authentication. Contains Equipment Identity Register.

## Student Questions

- ❑ What is the unit of BER?  
*BER is dimensionless. It is the ratio of bits in error to total bits sent.*

# Cellular Architecture (Cont.)

- ❑ Home Location Register (HLR) and Visitor Location Register (VLR) provide call routing and roaming
- ❑ VLR+HLR+MSC functions are generally in one equipment
- ❑ Equipment Identity Register (EIR) contains a list of all valid mobiles.
- ❑ Authentication Center (AuC) stores the secret keys of all SIM cards.
- ❑ Each handset has a International Mobile Equipment Identity (IMEI) number.

## Student Questions

- ❑ So LTE is not like 3G, 3.5G, but it is more like a Radio access network, like UTRAN or GERAN?

*LTE is 3.9G. Each Generation uses a different technique in its "Radio Access Networks" (RAN). UTRAN and GERAN are examples of RAN.*

- ❑ How can my host get IP in a cellular network?

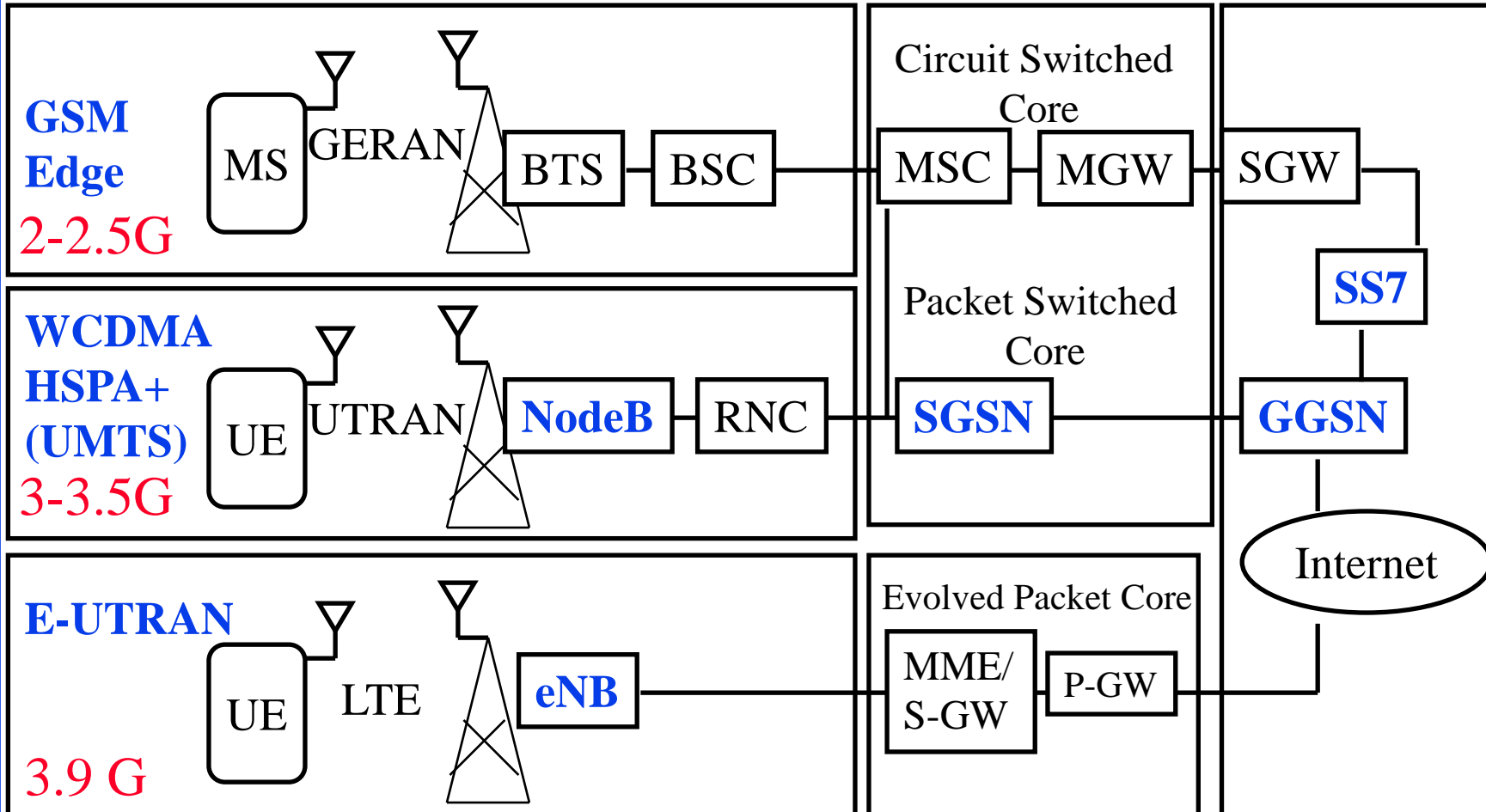
*The cellular network now provides IP services (e.g., DHCP, routing using IP addresses) and traditional phone services that do not use the IP address.*



# Evolved Packet System (EPS)

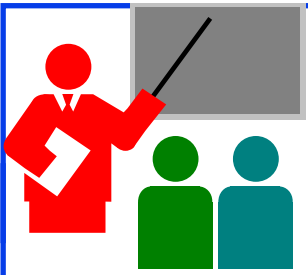
Radio Access Network

Serving Network Core Network



## Student Questions

- ❖ As LTE is 3.5G, why did you put it in positions like GERAN and UTRAN?  
*LTE is 3.9G. I have corrected the previous slide.*
- ❖ Is the final connection to the Internet typically via Ethernet?  
*PPP=Point-to-point protocol*



# Review: Cellular Networks

1. 1G was Analog voice, 2G was Digital voice, 3G was CDMA with voice and high-speed data, 4G is high-speed data
2. A cellular system has a RAN with BTS, BSC and a network subsystem with HLR, VLR, MSC, EIR, and AuC
3. 3G replaced RAN with UTRAN and BTS with NodeB. 4G uses eNB.

## Student Questions



# Mobility Management

- Mobile IP
- GSM: Routing to Mobile
- GSM Handoff
- Mobility: GSM versus Mobile IP

## Student Questions

# Mobility: Mr. Smith Goes to Washington

Mr. Smith's office



Can I speak to Mr. Smith

Jim Taylor



Hello Senator Taylor

*Can you connect me to Mr. Smith?*

Mr. Smith



Mr. Smith! Call from Taylor

Hotel Operator

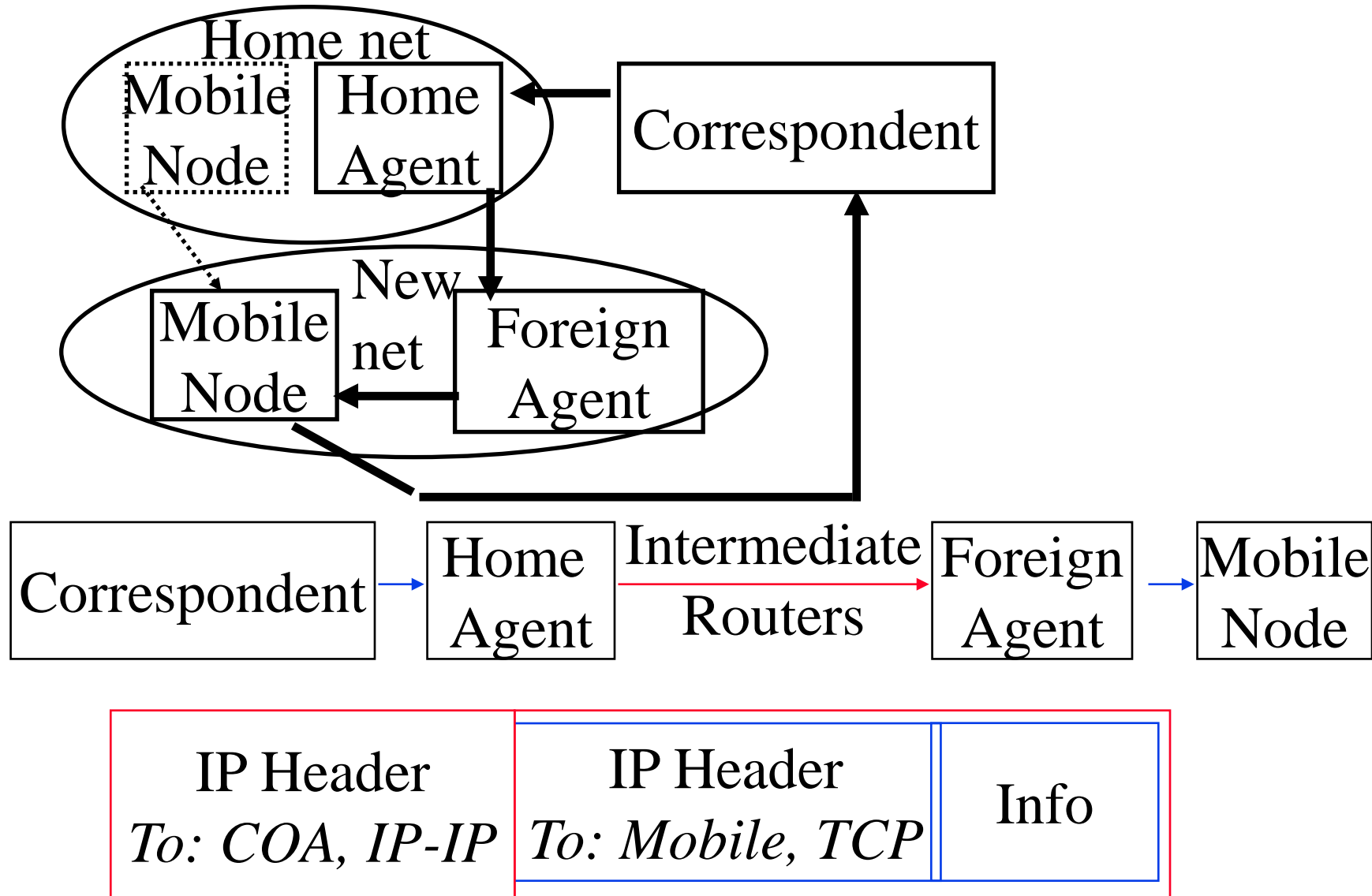


Hello Senator Taylor

- We need:
  - An agent at home office: Home Agent
  - An agent at foreign office: Foreign Agent

## Student Questions

# Mobile IP: Mechanisms



## Student Questions

- ❑ What is the difference between GSM and GPRS?  
*Original GSM was designed for digital voice. GPRS is an improvement to GSM for digital data transmission.*

# Mechanism (Cont.)

- ❑ Mobile node finds foreign agents via solicitation or advertising
- ❑ Mobile registers with the foreign agents and informs the home agent
- ❑ Home agent intercepts mobile node's datagrams and forwards them to the care-of-address
- ❑ Care-of-address (COA): Address of the end-of-tunnel towards the mobile node. May or may not be a foreign agent
- ❑ At COA, the datagram is extracted and sent to mobile

## Student Questions

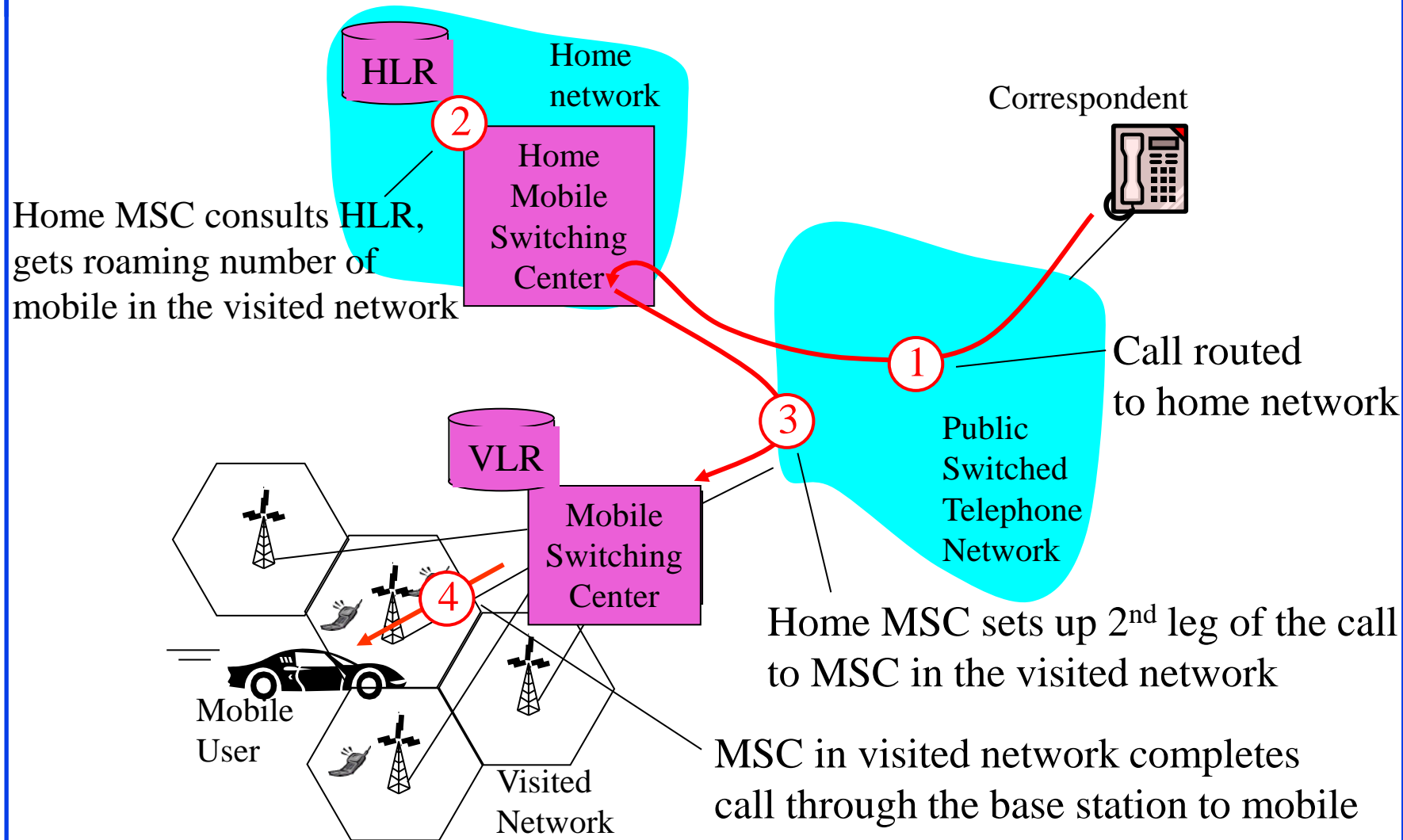
- ❑ Where does the home agent forward the message if the mobile device is not "home"?

*The home agent's job is to keep track of the mobile. (It is like your secretary, girl/boyfriend, wife/husband.)*

- ❑ How does my home agent know I am on vacation?

*See above.*

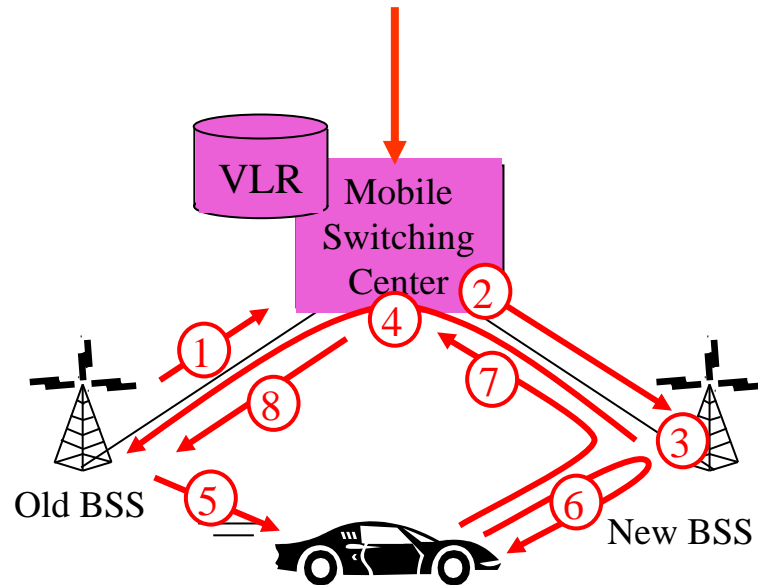
# GSM: Routing to Mobile



## Student Questions

- Could you go over the example again? *Sure.*
- What is the second leg of the call? *It happens all in the home area. It consists of Home MSC consulting HLR.*

# GSM: Handoff with Common MSC

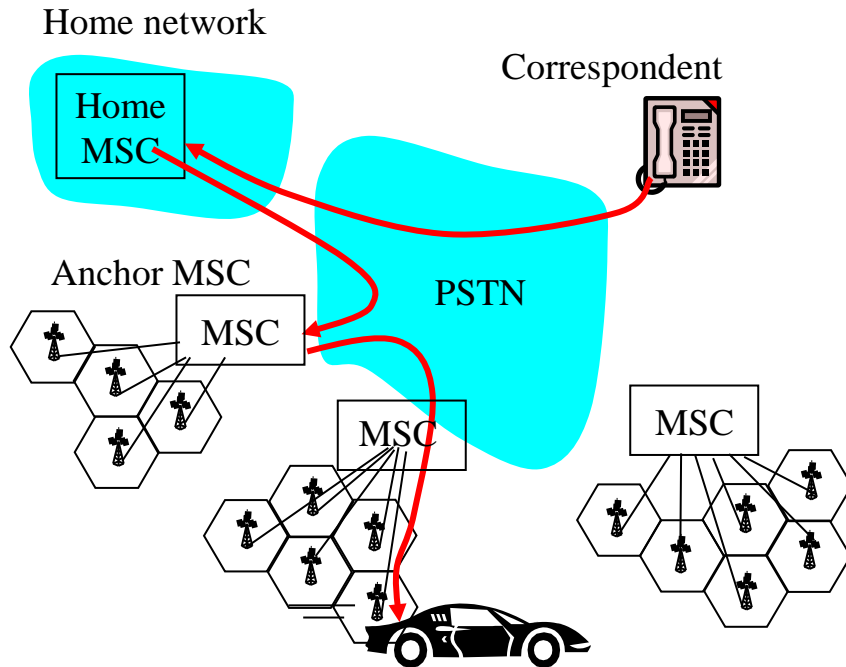


1. Old BSS informs MSC of impending handoff, provides a list of 1+ new BSSs
2. MSC sets up a path (allocates resources) to new BSS
3. New BSS allocates radio channel for use by mobile
4. New BSS signals MSC, old BSS: ready
5. Old BSS tells mobile: perform handoff to new BSS
6. Mobile, new BSS signal to activate the new channel
7. Mobile signals via new BSS to MSC: handoff complete. MSC reroutes call
8. MSC-old-BSS resources released

## Student Questions



# GSM: Handoff between MSCs

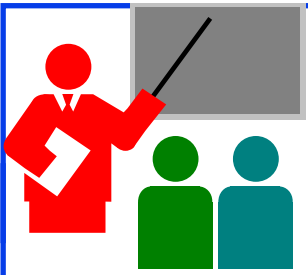


- ❑ *Anchor MSC*: first MSC visited during call
  - Call remains routed through anchor MSC
- ❑ New MSCs add on to end of MSC chain as mobile moves to new MSC
- ❑ IS-41 allows optional path minimization step to shorten multi-MSC chain

## Student Questions

- ❑ What is the minimization step that the IS-41 provides to shorten the Multi MSC chain?

*You can bypass many intermediate hops and go straight to the mobile. In the original method, the call went through each tower that you visited during that call.*



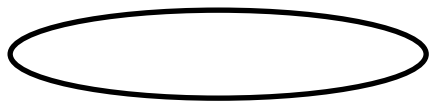
## Review: Mobility Management

- ❑ Mobile IP uses Home Agent as an Anchor  
Packets are tunneled from Home Agent to Care-of-Address
- ❑ GSM uses HLR and VLR for mobility. All packets are routed through the home network
- ❑ Handoff between towers in a single network is done through MSC

### Student Questions

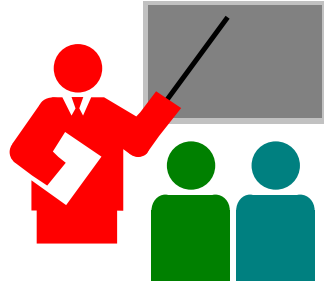
# Impact on Higher Layer Protocols

- ❑ Layered Architecture  $\Rightarrow$  Upper layers are independent of lower layers
- ❑ Wireless  $\Rightarrow$  High error rate  $\Rightarrow$  Frequent packet losses  
 $\Rightarrow$  Triggers TCP congestion control even if there is no overload
- ❑ TCP modifications:
  - Local Recovery: Link level retransmissions and error correction
  - Wireless-aware TCP Sender:  
Distinguish overload (sustained) and random errors
  - Split-Connection: Host1-to-AP + AP-to-Host2



## Student Questions

# Summary



1. Code division multiple access “was” commonly used in wireless networks
2. IEEE 802.11 uses CSMA/CA with RTS, CTS, data, and ack. A frame may have up to 4 addresses.
3. Bluetooth and ZigBee are PANs that use very little energy
4. Cellular networks have evolved from analog voice to digital voice and finally to high-speed data.
5. Mobile IP uses home agents as anchors.
6. Cellular networks use MSCs to manage mobility.
7. Frequent packet losses due to errors may confuse TCP as network congestion.

## Student Questions

- Is the FHSS not popular as OFDMA?  
*OFDMA is the latest.*
- What is the range of frequency hopping?  
Will it be within microwave bandwidth around 2.4GHz?  
*Yes, the entire 2.4 GHz band is used for frequency hopping.*
- If I were to trace a route from my PC to Google, is there a way to determine where connections were wireless and wired?  
*You can do a traceroute. But it does not tell you the speed or technology on any hop.*
- Could you explain the significance of spreading the spectrum using code?  
*Code-division multiple access (CDMA) allows multiple senders to speak simultaneously without interfering.*

# CSE 574S: Wireless and Mobile Networking

1. How is wireless different from wired communication?
2. What are the protocols that are used in **IoT**?
3. Why do we need new protocols for IoT?
4. How does **WiFi** work? How 10 Mbps to 10 Gbps?
5. How is **Bluetooth** different from WiFi?
6. How is **ZigBee** different from WiFi?
7. What are other newer wireless protocols for IoT? **LORAWAN**
8. What is the basic difference between 1G/2G/3G/4G/5G
9. What new features came in with **4G**?
10. What new techniques enabled **5G**?
11. What about 6G? When and how?

## Student Questions

# Acronyms

- ❑ 1xEV-DO 1 times Evolution to Data Only
- ❑ 1xEV-DV 1 times Evolution to Data and Voice
- ❑ 3GPP1 3rd Generation Partnership Project
- ❑ 6LowPAN IPv6 over Low Power Personal Area Networks
- ❑ ACK Acknowledgement
- ❑ AMPS Advanced Mobile Phone System
- ❑ AP Access Point
- ❑ BER Bit Error Rate
- ❑ BSA Basic Service Area
- ❑ BSC Base station controller
- ❑ BSS ID Basic Service Set Identifier
- ❑ BTS Base transceiver station
- ❑ CA Collision Avoidance
- ❑ CAP Contention Access Period
- ❑ CDMA Code Division Multiple Access
- ❑ CEPT Committee of European Posts and Telecom

## Student Questions

# Acronyms (Cont)

- ❑ CFP                    Contention Free Period
- ❑ COA                    Care-Of-Address
- ❑ CRC                    Cyclic Redundancy Check
- ❑ CSMA                    Carrier Sense Multiple Access
- ❑ CTS                    Clear to Transmit
- ❑ D-AMPS                Digital Advanced Mobile Phone System
- ❑ dB                    Deci-Bel
- ❑ DCN                    Data Communication Network
- ❑ DHCP                    Dynamic Host Control Protocol
- ❑ DIFS                    Distributed Inter-Frame Spacing
- ❑ DSSS                    Direct Sequence Spread Spectrum
- ❑ E-UTRAN                Evolved UTRAN
- ❑ EDGE                    Enhanced Data rate for GSM evolution
- ❑ EGPRS                    Enhanced GPRS
- ❑ EIA                    Electronic Industry Association
- ❑ EIR                    Equipment Identity Register

## Student Questions

# Acronyms (Cont)

- ❑ eNB evolved Node B
- ❑ ESA Extended Service Area
- ❑ ESS Extended Service Set
- ❑ FCC Federal Communications Commission
- ❑ FDMA Frequency Division Multiple Access
- ❑ GERAN GSM Enhanced Radio Access Network
- ❑ GGSN Gateway GPRS Support Node
- ❑ GHz Giga-Hertz
- ❑ GPRS General Packet Radio Service
- ❑ GSM Global System for Mobile Communications
- ❑ GTS Guaranteed Transmission Service
- ❑ GW Gateway
- ❑ HART Highway Addressable Remote Transducer Protocol
- ❑ HLR Home Location Register
- ❑ HSPA High Speed Packet Access
- ❑ HSPDA High Speed Packet Download Access

## Student Questions



# Acronyms (Cont)

- ❑ ID Identifier
- ❑ IEEE Institution of Electrical and Electronics Engineers
- ❑ IFS Inter-frame space
- ❑ IMEI International Mobile Equipment Identity
- ❑ IP Internet Protocol
- ❑ IS International Standard
- ❑ ISA International Society of Automation
- ❑ ISDN Integrated Switched Digital Network
- ❑ kW Kilo-Watt
- ❑ LAN Local Area Network
- ❑ LR Long-Range
- ❑ LTE Long-Term Evolution
- ❑ mA Milli-Ampere
- ❑ MAC Media Access Control
- ❑ MANET Mobile Ad-hoc Network
- ❑ MGW Media Gateway

## Student Questions

# Acronyms (Cont)

- ❑ MHz Mega Hertz
- ❑ MIMO Multiple Input Multiple Output
- ❑ MME Mobility Management Entity
- ❑ MS Mobile Subscriber
- ❑ MSC Mobile Switching Center
- ❑ mW Milli-Watt
- ❑ NA North America
- ❑ NAT Network Address Translator
- ❑ NodeB Node B (Base Station)
- ❑ PAN Personal Area Network
- ❑ PC Personal Computer
- ❑ PHY Physical Layer
- ❑ PIFS Point-Coordination Inter-Frame Spacing
- ❑ PSTN Public Switched Telephone Network
- ❑ QAM Quadrature Amplitude Modulation

## Student Questions

# Acronyms (Cont)

- ❑ RAN Radio Access Network
- ❑ RNC Radio Network Controller
- ❑ RTS Ready to send
- ❑ SCDMA Synchronous CDMA
- ❑ SGSN Service GPRS Support Node
- ❑ SGW Serving Gateway
- ❑ SIFS Short Inter-Frame Spacing
- ❑ SIM Subscriber Identification Module
- ❑ SNR Signal to Noise Ratio
- ❑ SS7 Signaling System 7
- ❑ SSID Service Set Identifier
- ❑ SYN Synchronizing Frame
- ❑ TACS Total Access Communications System
- ❑ TCP Transmission Control Protocol
- ❑ TD-SCDMA Time Duplexed Synchronous Code Division Multiple Access
- ❑ TDMA Time Division Multiple Access

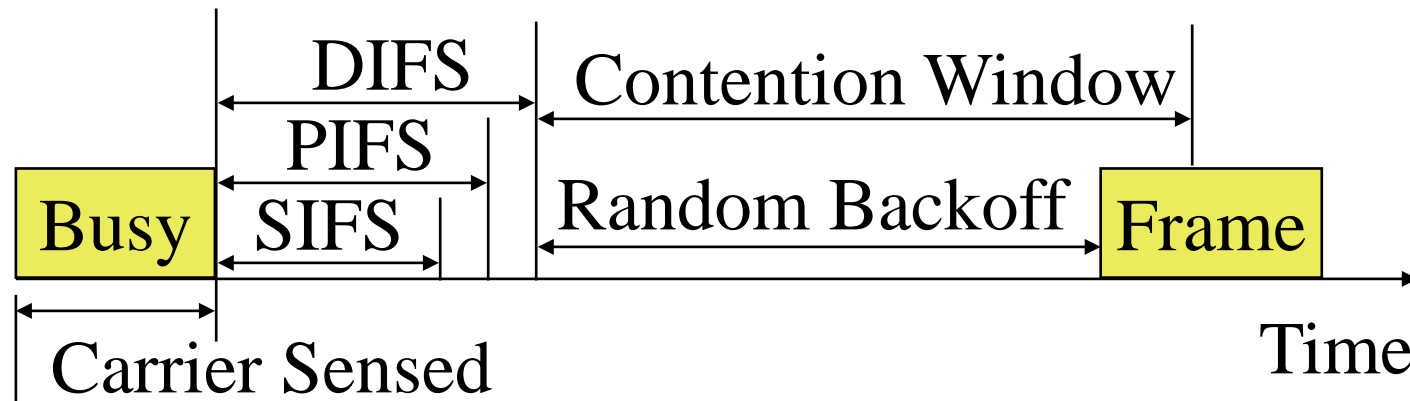
## Student Questions

# Acronyms (Cont)

- ❑ TIA Telecom Industry Association
- ❑ TV Television
- ❑ UE User Element
- ❑ UK United Kingdom
- ❑ UMB Ultra Mobile Broadband
- ❑ UMTS Universal Mobile Telecommunications System
- ❑ UTRAN UMTS Terrestrial Radio Access Network
- ❑ VANET Vehicular Ad-hoc Network
- ❑ VLR Visitor Location Register
- ❑ WCDMA Wide-band CDMA
- ❑ WEP Wired Equivalend Privacy
- ❑ WiFi Wireless Fidelity
- ❑ WPAN Wireless Personal Area Network

## Student Questions

# IEEE 802.11 Priorities



- ❑ Initial inter-frame space (IFS)
- ❑ Highest priority frames, e.g., Acks, use short IFS (SIFS)
- ❑ Medium priority time-critical frames use “Point Coordination Function IFS” (PIFS)
- ❑ Asynchronous data frames use “Distributed coordination function IFS” (DIFS)

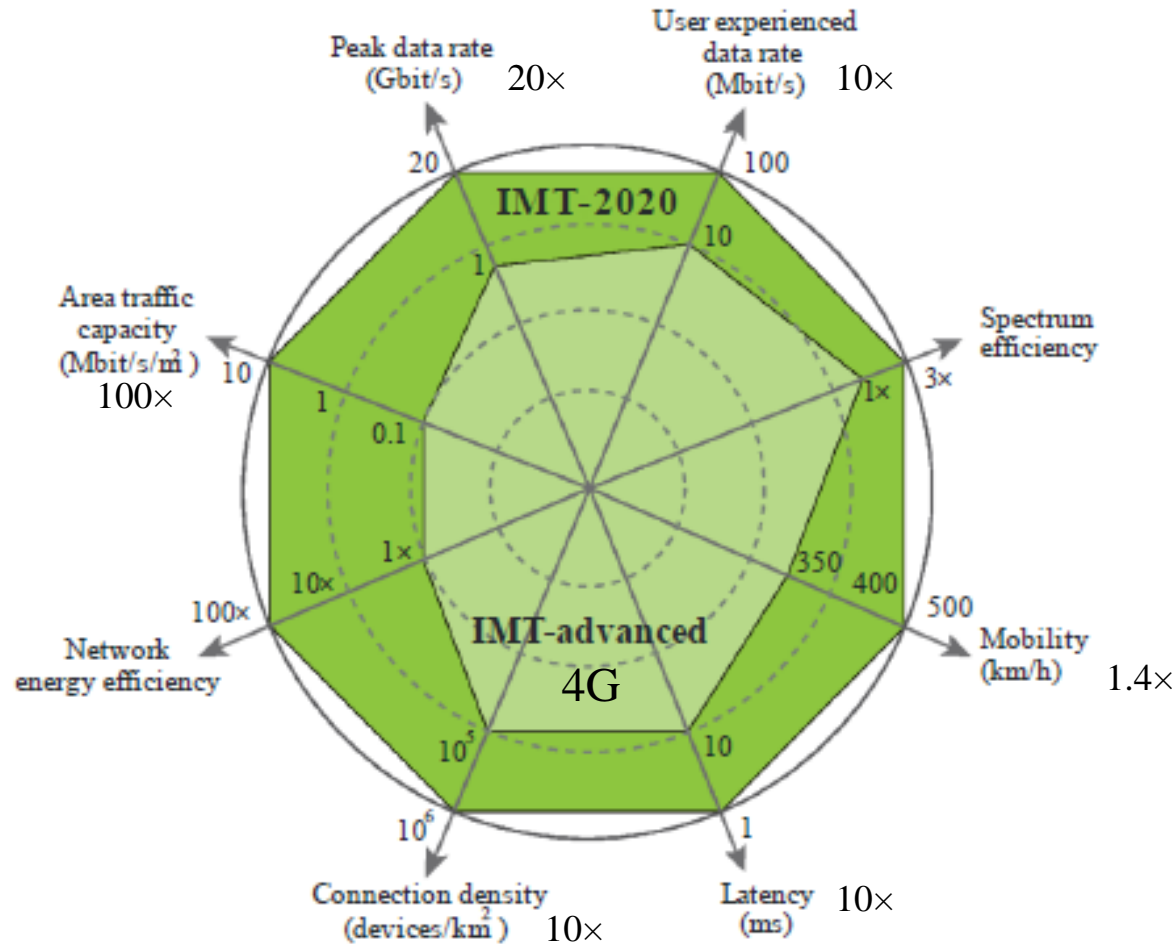
## Student Questions

- ❖ Chapter 7.3.2: How is the value for DIFS and SIFS decided? I know they are determined in the standards, but how are the values computed?

*They are based on the distances to be covered by the networks and the precision of timers.*

# 5G Definition

5G = International Mobile Telecommunications 2020

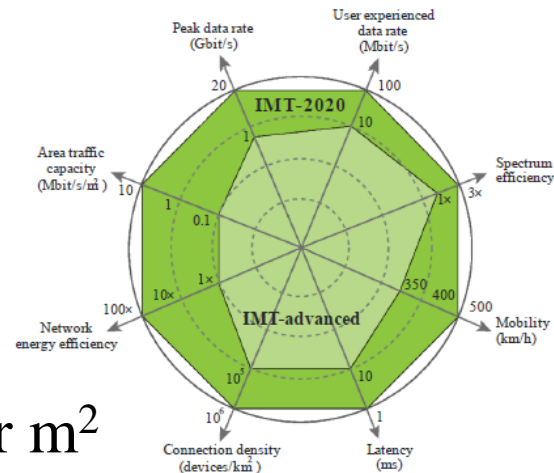


## Student Questions

Ref: ITU-R Recommendation M.2083-0, "IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond," Sep. 2015, 21 pp., [https://www.itu.int/dms\\_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf](https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf)

# 5G Definition (Cont)

1. **Peak Data Rate:** max rate per user under ideal conditions. 10 Gbps for mobiles, 20 Gbps under certain conditions.
2. **User experienced Data Rate:** 95% Rate across the coverage area per user. 100 Mbps in urban/suburban areas. 1 Gbps hotspot.
3. **Latency:** Radio contribution to latency between send and receive
4. **Mobility:** Max speed at which seamless handover and QoS is guaranteed
5. **Connection Density:** Devices per  $\text{km}^2$
6. **Energy Efficiency:** Network bits/Joule, User bits/Joule
7. **Spectrum Efficiency:** Throughput per Hz per cell
8. **Area Traffic Capacity:** Throughput per  $\text{m}^2$



## Student Questions

# 5G Applications

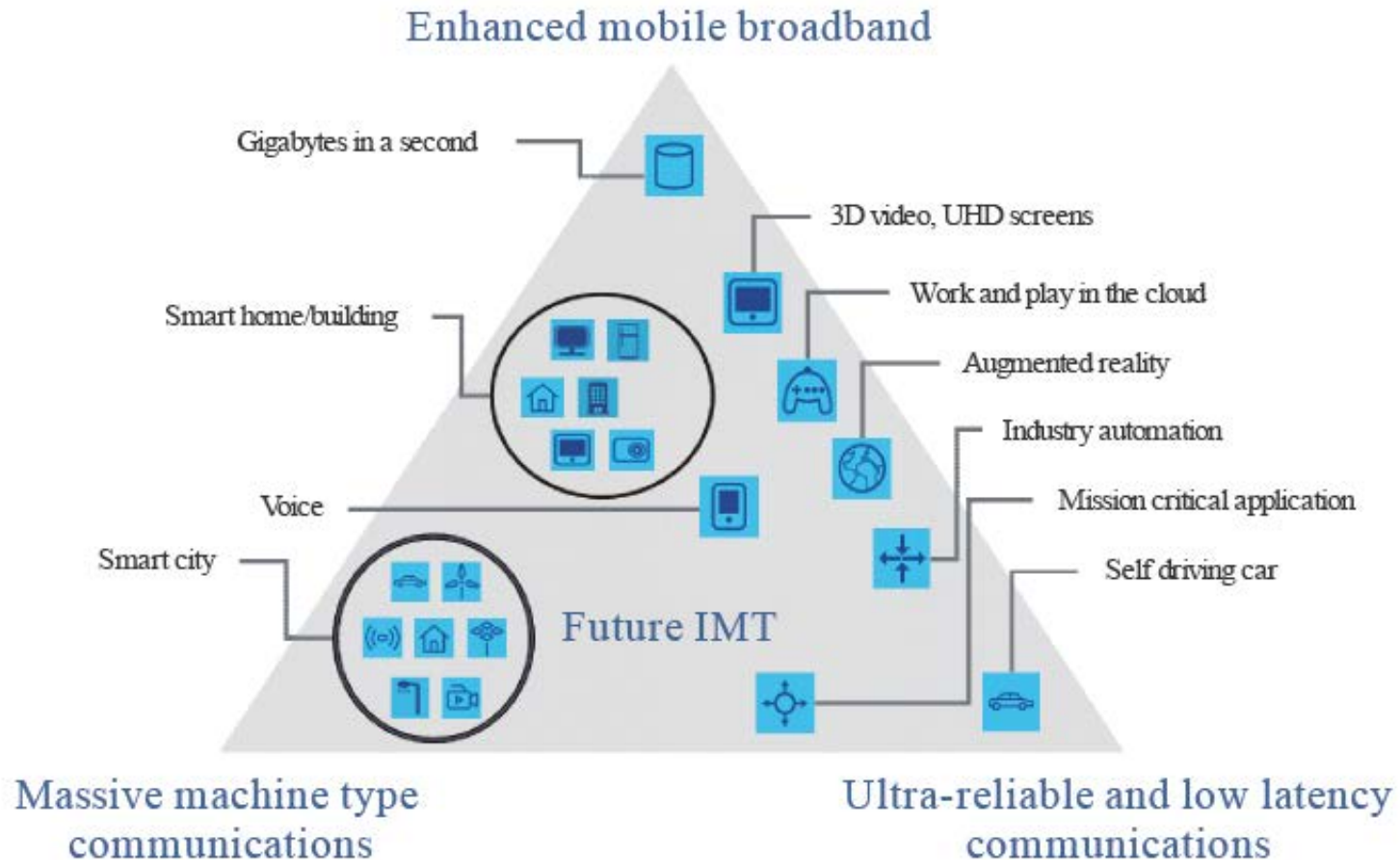
Three Key Application Areas:

1. **Enhanced Mobile Broadband (eMBB)**: Better mobile phones and hot spots. High data rates, high user density. Human centric communications
2. **Ultra-Reliable and Low-Latency Communications (URLLC)**: Vehicle-to-Vehicle communication, Industrial IoT, 3D Gaming. Human and Machine centric communication
3. **Massive Machine Type Communications (mMTC)**: Very large number of devices, low data rate, low power. IoT with long battery life time. Addition to GSM, LoRa, Zigbee, etc. Machine-centric communication.

## Student Questions



# 5G Applications (Cont)



## Student Questions

M.2083-02

Ref: ITU-R M.2083-0, "IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond,"  
Sep. 2015. [https://www.itu.int/dms\\_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf](https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf)

Washington University in St. Louis

<http://www.cse.wustl.edu/~jain/cse473-22/>

©2022 Raj Jain

# Spectrum for 5G

- ❑ World Radio-communications Conference (WRC) determines the spectrum requirements
- ❑ Two Frequency Ranges (FRs)
  - **FR1**: Sub 6-GHz. Several new bands in this range.
  - **FR2**: 24.25-52.6 GHz (mm-Waves)
    - ⇒ Good for high throughput in small cells
  - NR (New Radio) can use both paired and unpaired spectrum  
NR specs list 26 operating bands for FR1 and 3 for FR2.

## Student Questions

# Above 6 GHz

- ❑ **Free-space loss** increases in proportion to square of frequency and square of distance. 88 dB loss with 30 GHz at 20 m  
⇒ 10-100 m cell radius
- ❑ **Outdoor-to-Indoor**: Glass windows add 20-40 dB
- ❑ **Mobility**: Doppler shift is proportional to frequency and velocity. Multipath results in varying Doppler shifts  
⇒ Lower mobility
- ❑ 100s MHz ⇒ **Multi-gigabit** data rates
- ❑ **Dense spatial reuse**
- ❑ Lower latency
- ❑ **Directional antennas** with adaptable 3D beamforming and beam tracking

Ref: ITU-R M2376-0, "Technical Feasibility of IMT in bands above 6 GHz," July 2015,  
[http://www.itu.int/dms\\_pub/itu-r/opb/rep/R-REP-M.2376-2015-PDF-E.pdf](http://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2376-2015-PDF-E.pdf)

## Student Questions

**Scan This to Download These Slides**



Raj Jain

<http://rajjain.com>

**Student Questions**

[http://www.cse.wustl.edu/~jain/cse473-22/i\\_7wmn.htm](http://www.cse.wustl.edu/~jain/cse473-22/i_7wmn.htm)

# Related Modules



CSE 567: The Art of Computer Systems Performance Analysis

[https://www.youtube.com/playlist?list=PLjGG94etKypJEKjNAa1n\\_1X0bWWNyZcof](https://www.youtube.com/playlist?list=PLjGG94etKypJEKjNAa1n_1X0bWWNyZcof)

CSE473S: Introduction to Computer Networks (Fall 2011),

[https://www.youtube.com/playlist?list=PLjGG94etKypJWOSPMh8Azcg5e\\_10TiDw](https://www.youtube.com/playlist?list=PLjGG94etKypJWOSPMh8Azcg5e_10TiDw)



CSE 570: Recent Advances in Networking (Spring 2013)

<https://www.youtube.com/playlist?list=PLjGG94etKypLHyBN8mOgwJLHD2FFIMGq5>

CSE571S: Network Security (Spring 2011),

<https://www.youtube.com/playlist?list=PLjGG94etKypKvzfVtutHcPFJXumyyg93u>



Video Podcasts of Prof. Raj Jain's Lectures,

<https://www.youtube.com/channel/UCN4-5wzNP9-ruOzQMs-8NUw>

## Student Questions