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 online at:

http://www.cse.wustl.edu/~jain/cse473-25/

Student Questions

©2025 Raj Jain



Overview

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

©2025 Raj Jain



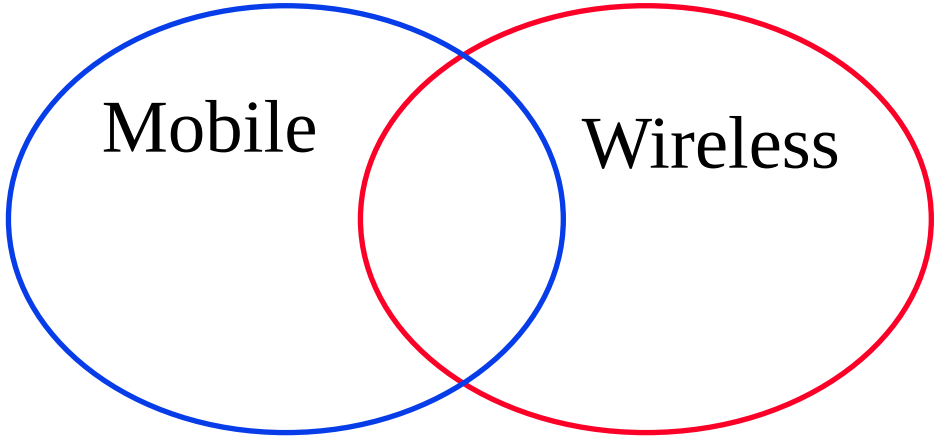
Wireless Link Characteristics

- 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

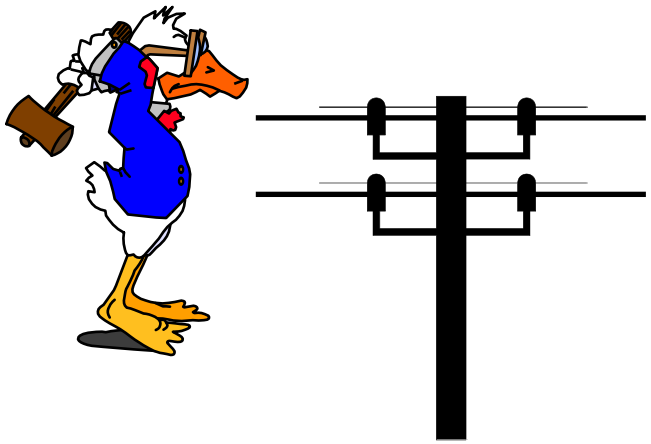
©2025 Raj Jain

Mobile vs Wireless





- Mobile vs. Stationary
- Wireless vs. Wired
- Wireless ⇒ media sharing issues
- Mobile ⇒ routing, addressing issues



Student Questions

- What layers of the OSI model do mobile/wireless concerns? Only physical and link layers?

It's mostly Layer 1 and 2, but other layers (3, 4, 5) may also need minor changes for wireless.

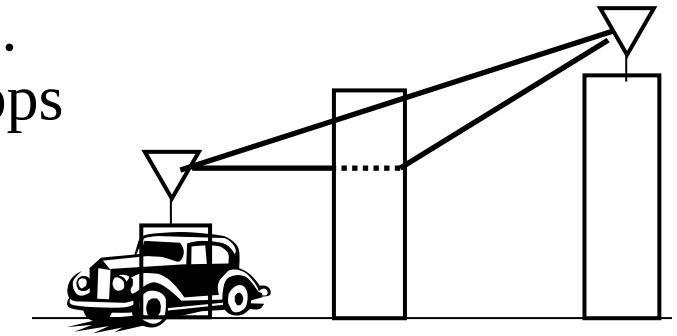
- Can I say the phone charging cable is mobile and wired?

Wired or wireless is generally used for communication endpoints, not cables.

©2025 Raj Jain

Wireless Networking Challenges

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



Student Questions

- ❑ When new buildings are constructed, do the builders consider that it may obstruct wireless signals?

No. No such study has been done. Carriers and enterprises have to structure their wireless afterward.

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

Each bit is split into multiple paths.

- ❑ How is the Doppler effect considered when receiving or transmitting signals?

The physical layer design determines 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, and analog words are in seconds.

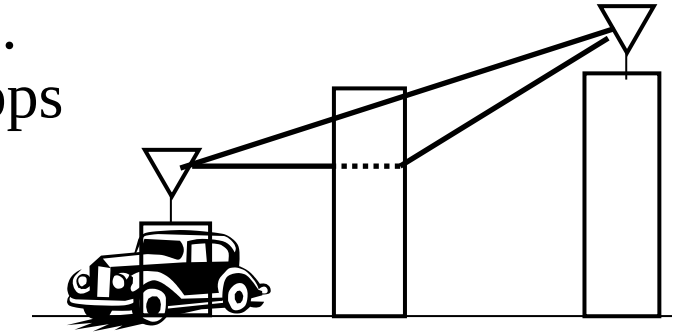
- ❑ Could you explain how the data rate physically works for wireless? What allows us to achieve faster data rates?

It will be covered in this chapter.

©2025 Raj Jain

Wireless Networking Challenges

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



Student Questions

- ❑ Are there any traffic issues in wireless transmission?

Yes. Multiple transmissions interfere with each other like sounds in a room.

- ❑ How to separate multipath signals?

Signal analysis techniques.

- ❑ Does multipath only happen in wireless networking? *Yes.*
- ❑ Does 5G transmission use less power than 4G? *This will be discussed later.*
- ❑ How will frequency affect the power required for transmission?

Lower frequency travels farther.

- ❑ Can you explain multipath again? *Sure.*

Could you explain again what you mean by #5: License-Exempt Spectrum?

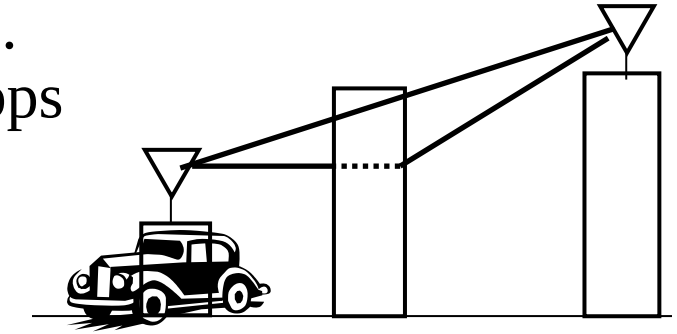
Most telecom spectrum is auctioned by the government and licensed for the exclusive use of the company paying for it.

How is the Doppler effect dealt with? Do wireless receivers adjust the frequency based on their movement speed?

The receiver allows for variability.

Wireless Networking Challenges

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



Student Questions

- ❑ How does MAC have anything to do with the License-Exempt spectrum?

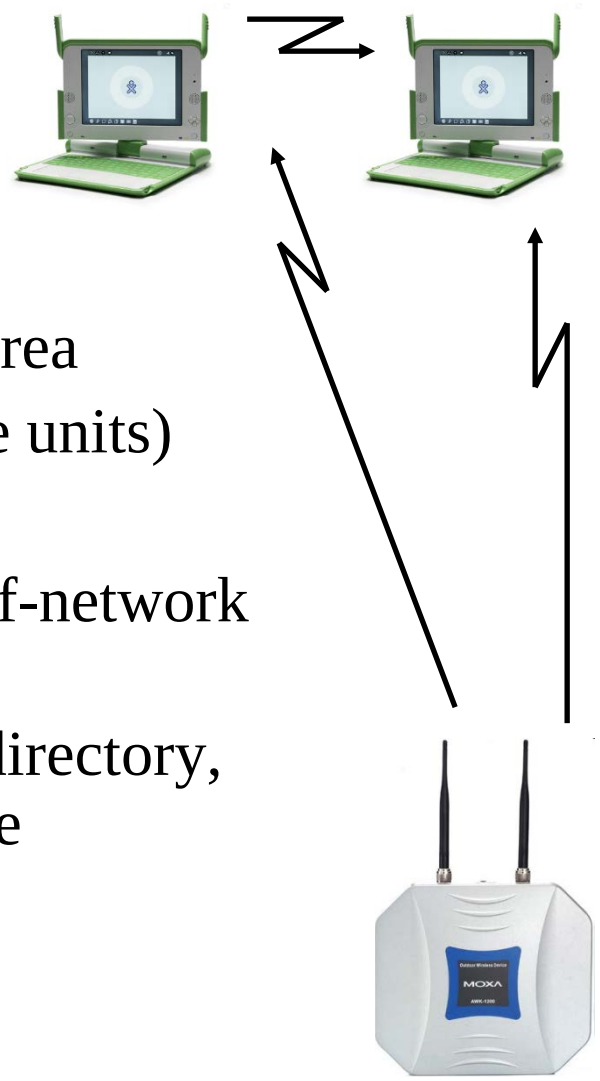
If you pay for licensed spectrum, you control who goes first (MAC).

- ❖ Is multipath propagation always a bad thing, or can it sometimes improve the reception of a wireless signal?

It is in MIMO to improve the signal.

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.
  - The base provides a connection for off-network traffic
  - The base provides location tracking, directory, and authentication ⇒ Scalable to large networks
- IEEE 802.11 provides both.



Student Questions

- If three computers are in a small area but have no base stations, is it also called an 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. BitTorrent is between computers 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.*
- Are hotspots peer-to-peer?

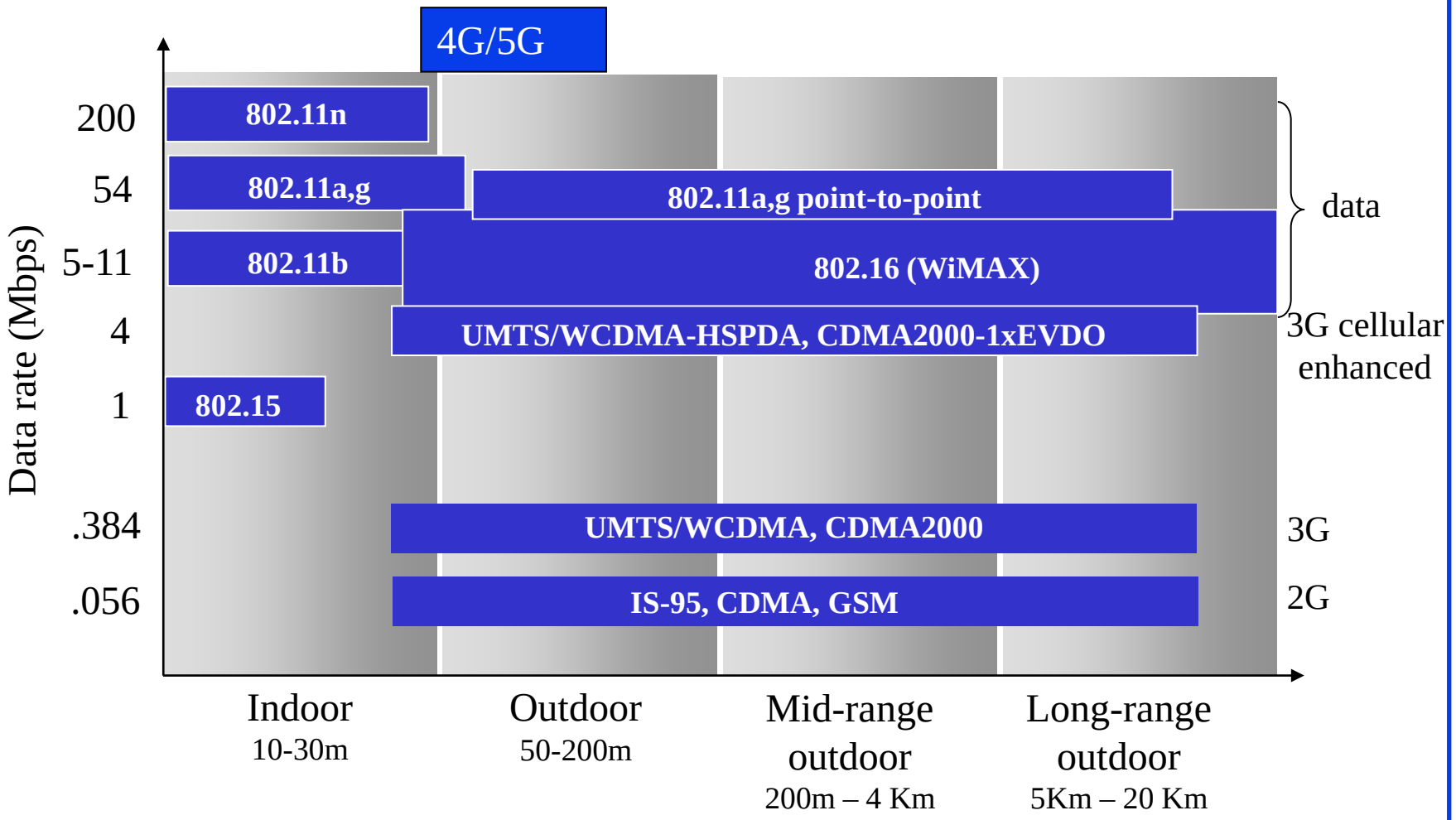
A hotspot serves as an access point.

- Does this mean Wi-Fi can be used in ad-hoc mode? *Yes.*
- Does blockchain use ad-hoc as the peer-to-peer connection? *No.*
- When it says the station, does it mean the same thing as the host in the textbook? *Yes*
- Do computers require extra hardware to enable peer-to-peer communication, or is it just more software?

This can be done in software.

©2025 Raj Jain

Characteristics of Selected Wireless Link Standards



Student Questions

- ❑ For the same power provided, does a lower data rate (longer wavelength) mean a longer distance?

  Longer wavelength => Lower frequency => Lower Hz. Coding determines Bits/Hz. So, the data rate depends on Coding and wavelength. For the same power and coding, longer wavelengths and longer distances will have a lower data rate.
- ❑ What is the meaning of the data label on the right side of the slide for the 802.11a,g point-to-point, and 802.16 (WiMAX) link standards?

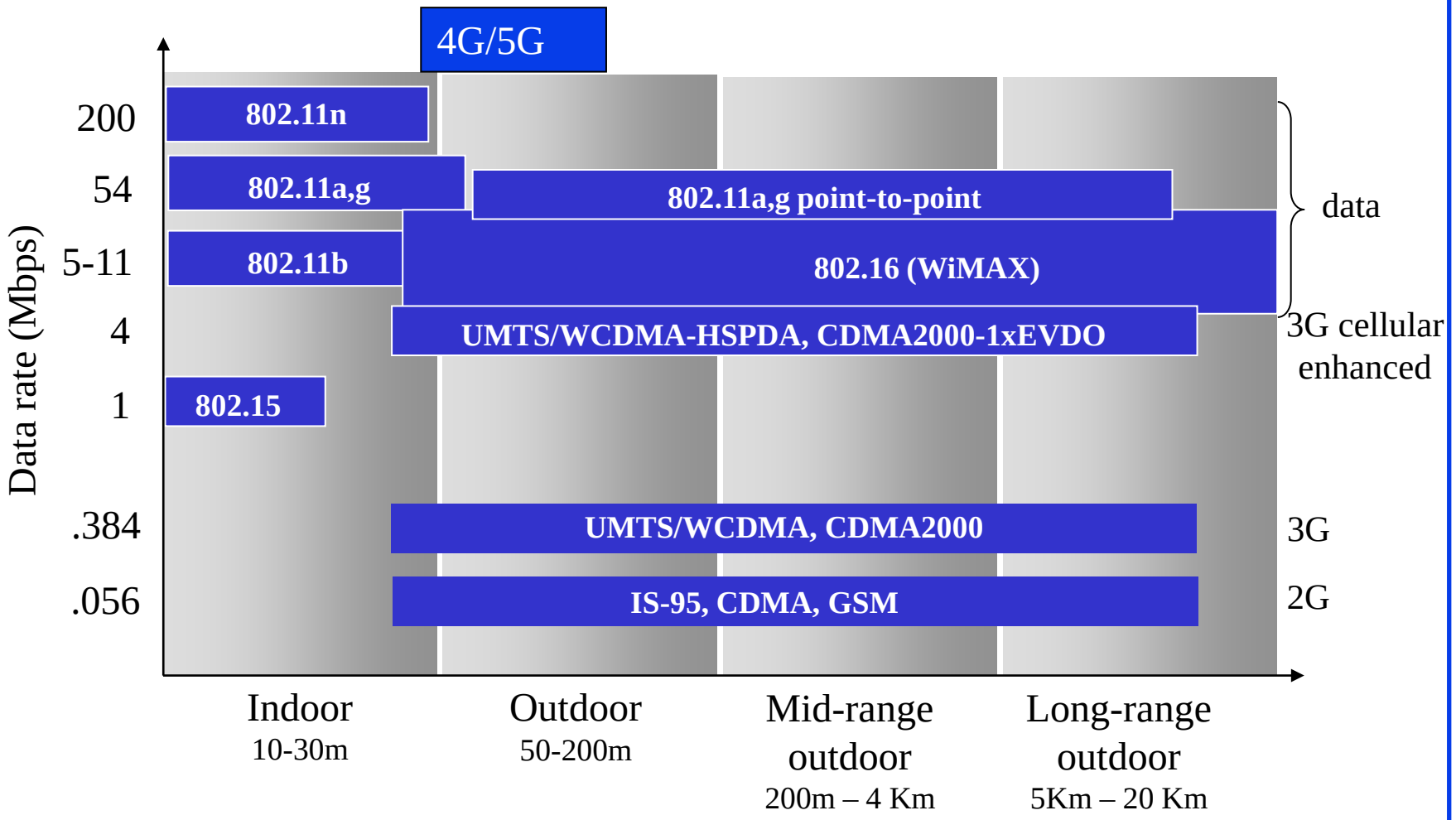
  Point-to-point = Two nodes are connected via a directional antenna and are pointed at each other.
- ❑ *What is the difference between CDMA and GSM*

  GSM is a 2G technology. CDMA is a technique.
- ❑ *Do 4G and 5G cover more ranges at a higher data rate?*

  They are covered later in this module.

©2025 Raj Jain

Characteristics of Selected Wireless Link Standards

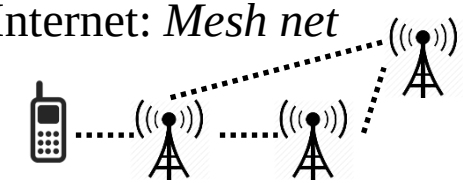
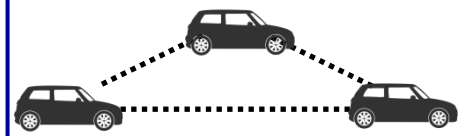


Student Questions

- ❑ Would a VPN count as a multi-hop with infrastructure?
  VPN is related to security and privacy not hops.
- ❑ Where are 4G and 5G in the plot? Do they share standards with older versions?
  Non-802 are all telecom standards.

©2025 Raj Jain

Wireless Network Taxonomy

	Single hop	Multiple hops
Infrastructure (Access Points, Towers)	Host connects to base station (Wi-Fi, WiMAX, cellular) which connects to larger Internet 	Host may have to relay through several wireless nodes to connect to larger Internet: *Mesh net*  Relay to reach others. Mobile Ad-hoc Network (MANET), Vehicular Ad-hoc Network (VANET) 
No Infrastructure	No base station (Bluetooth, ad hoc nets) 	

Student Questions

- ❑ The hop here is a link over wireless transmission. Then will those stations 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 ad-hoc nets? Is it just the difference in the number of devices?

Mobile means moving. Two computers communicating in Ad-hoc mode may or 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?

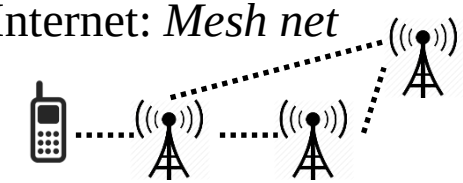
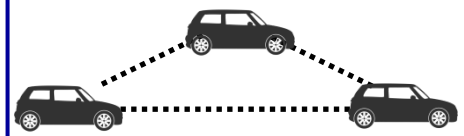
M=Mobile. It could be between a walking person and the tower.

V=Vehicle-to-vehicle without a tower.

- ❑ Does Wi-Fi always use single hop?

Yes. But you can go multiple hops via Access Points.

Wireless Network Taxonomy

	Single hop	Multiple hops
Infrastructure (Access Points, Towers)	Host connects to base station (Wi-Fi, WiMAX, cellular) which connects to larger Internet 	Host may have to relay through several wireless nodes to connect to larger Internet: *Mesh net* 
No Infrastructure	No base station (Bluetooth, ad hoc nets) 	Relay to reach others. Mobile Ad-hoc Network (MANET), Vehicular Ad-hoc Network (VANET) 

Student Questions

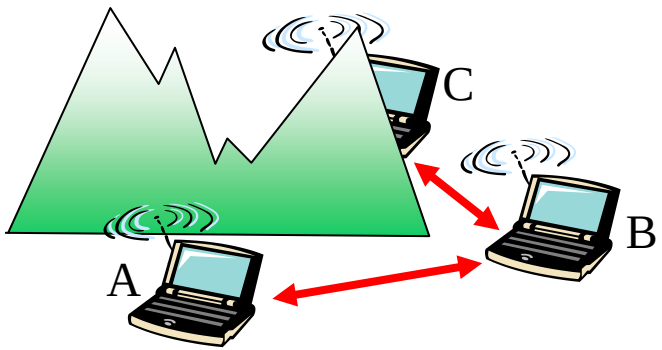
- ❑ Does VANET use Bluetooth?

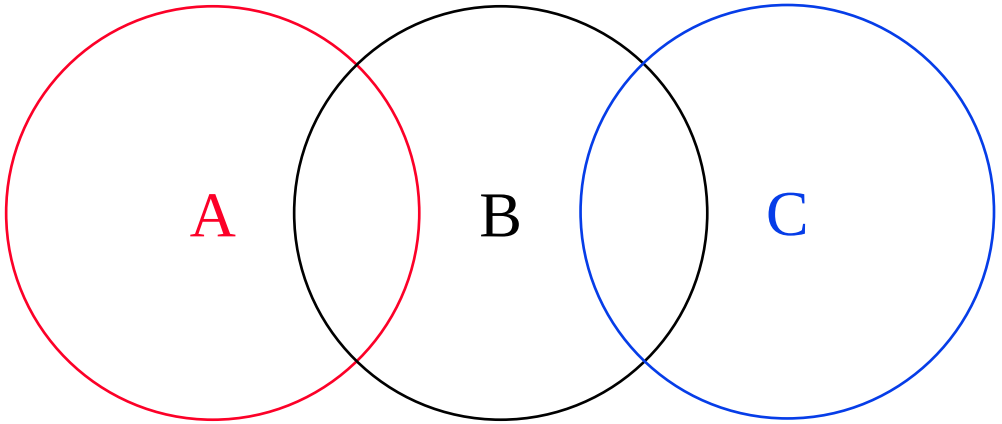
No. There is a separate standard.

- ❑ In mesh Wi-Fi networks, do access points provide actual hops to the base station, or do they extend the signal?

Mesh Wi-Fi nodes connect via a backbone wireless network. Each node is a base station or access point.

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 collisions.
- Only the receiver can help avoid collisions.

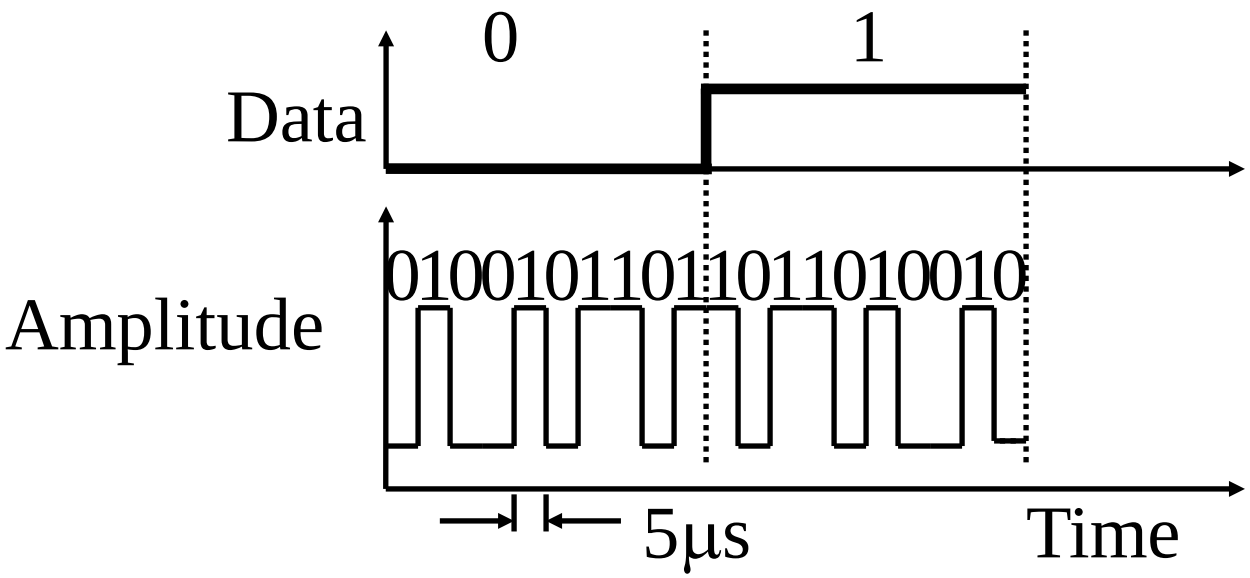
Student Questions

- Can the receiver (B) of both the colliding transmitters send some "jam" signal (similar to CSMA/CD) to the two transmitters to also resolve the hidden node problem? *Yes. This is the last point on the slide.*
- How is CSMA/CA implemented for A and C in this case? *They both ask B if there is a collision using RTS.*
- What prevents A and C from hearing each other? The slide shows a physical barrier between them. Is the hidden node problem caused by physical barriers or something else?

Signal degrades with distance, barriers, and reflections, …

©2025 Raj Jain

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 × data bandwidth
- Code sequence synchronization
- Correlation between codes ⇒ Interference ⇒ Orthogonal

Student Questions

Would you clarify the meaning of "bandwidth" here?
Band = Frequency Band
Bandwidth=Width of the Frequency Band
(See next slide)

What's an example of an orthogonal code?
See the example on slide 7.12

❑For best orthogonality, can we just use 1's comp negated 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.*

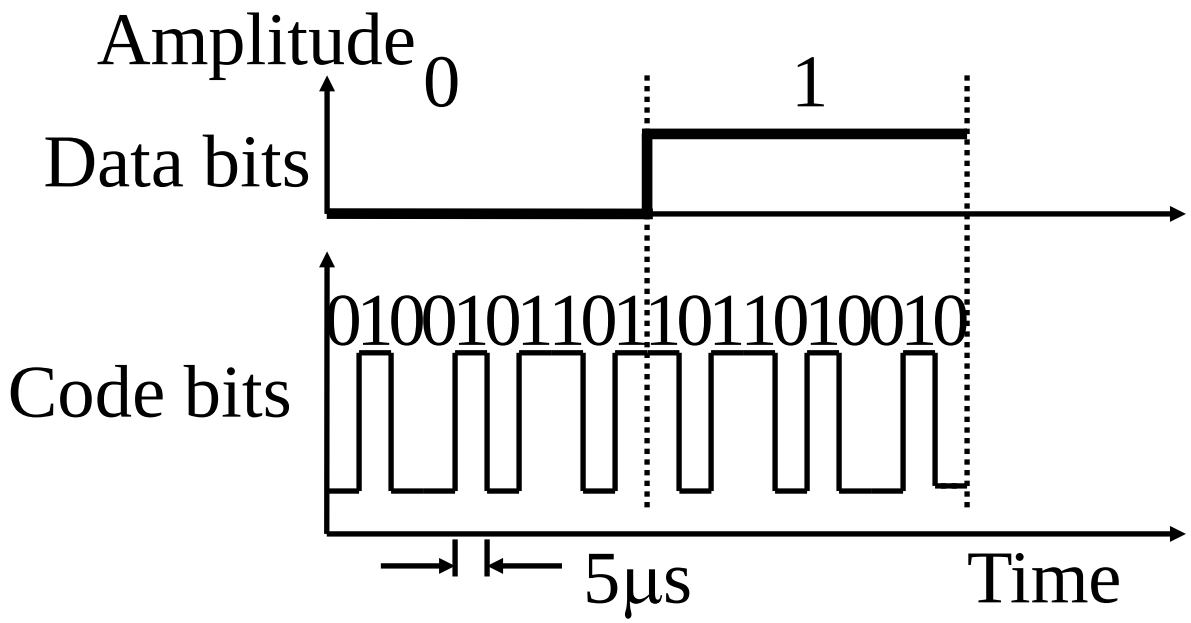
❑Once set, will the code of a transmitter be changed?
Yes. It is changed frequently in "code division multiple access (CDMA)."

❑When the bits sent by multiple senders are mixed, how does the CDMA receiver recover the original bits sent? *See the example in the next few slides.*

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

©2025 Raj Jain

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 × data bandwidth
- Code sequence synchronization
- Correlation between codes ⇒ Interference ⇒ Orthogonal

Student Questions

- Why did the FCC decide on 10 bits to be the minimum? *So that a small number of users can share the space.*
- If CDMA sends 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.

- Are the codes representing 0 and 1 opposite each other on every code bit?

Yes. In n-dimensional space, 0 and 1 should be as far apart as possible. This is achieved by making the code for 0 a complement of the code for one and vice versa.

- What are code bits and data bits?

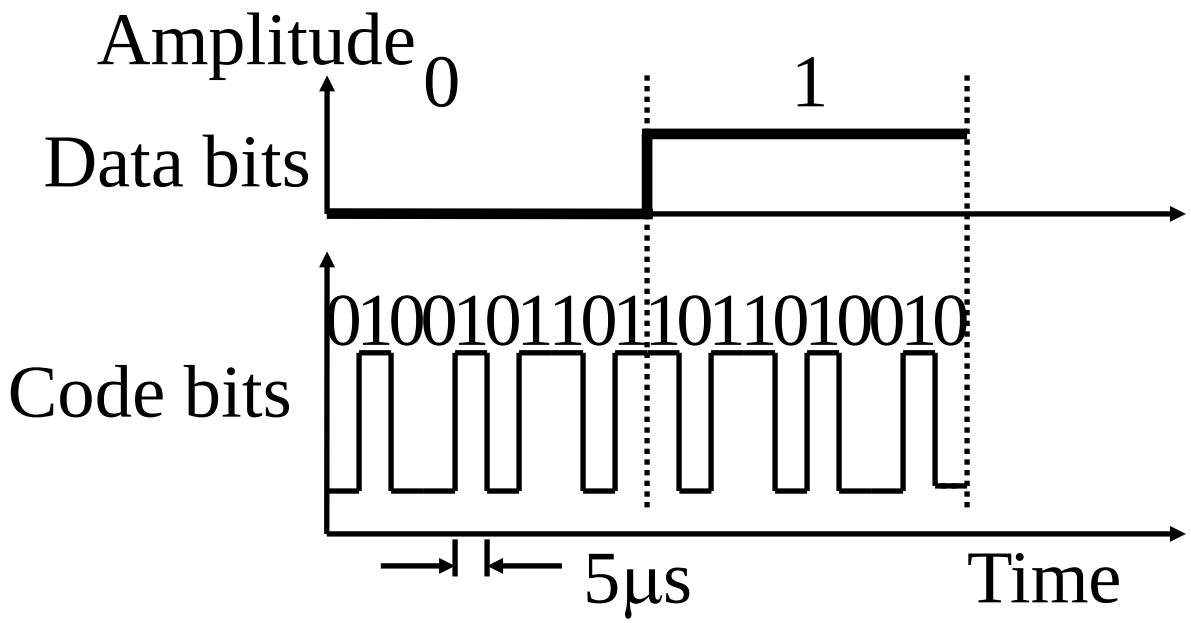
The slide has been updated to show the two types clearly.

- Can you clarify what bandwidth means? Are they two separate components like band and width joined together?

Bandwidth = Width of the frequency range used

©2025 Raj Jain

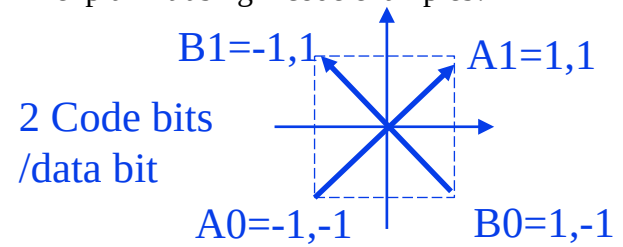
Direct-Sequence Spread Spectrum CDMA



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

Student Questions

- What does the orthogonal mean? Could you explain it using 2 code examples?



A0×B0=-1+1=0, A0×B1=1-1=0
A1×B0=1-1=0, A1×B1=-1+1=0

- What happens on coincidental uses of the same code by different pairs of computers?

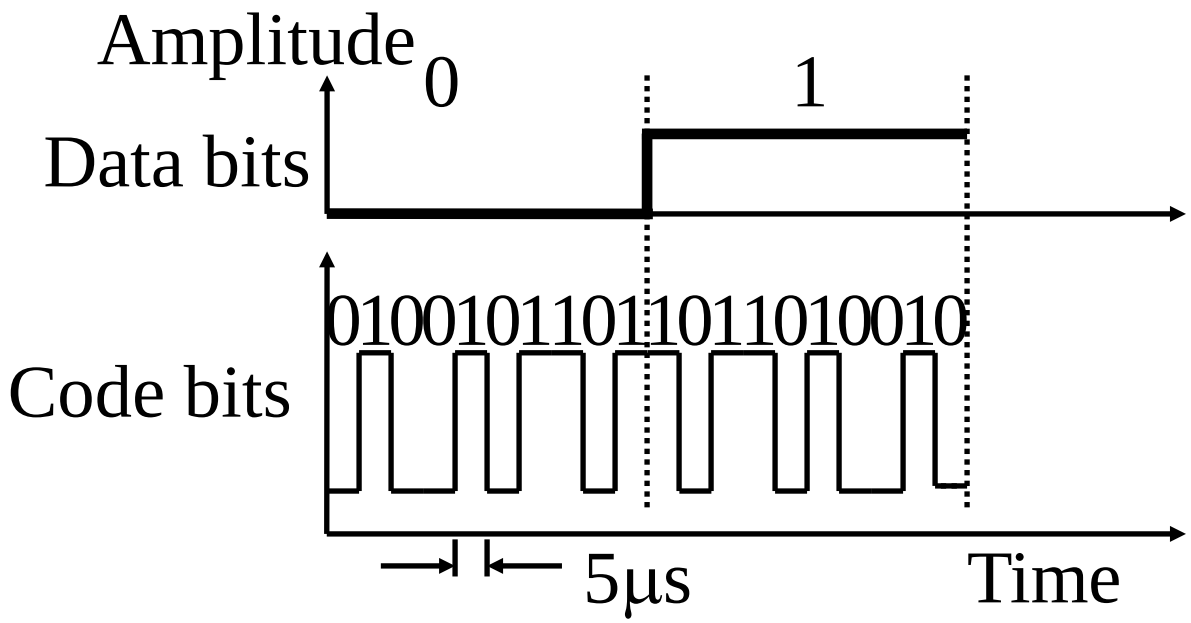
Two pairs using the same code/language will interfere with each other.

- Why was this spreading factor considered worth it, given the great loss in data sent per bit?

Allows interference mitigation and sharing.

©2025 Raj Jain

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 × data bandwidth
- Code sequence synchronization
- Correlation between codes ⇒ Interference ⇒ Orthogonal

Student Questions

- What is CDMA's relationship to DSSS? Is it just the procedure with which DSSS is implemented?

Both spread the spectrum as shown on the next slide.

- How do codes get assigned and communicated?

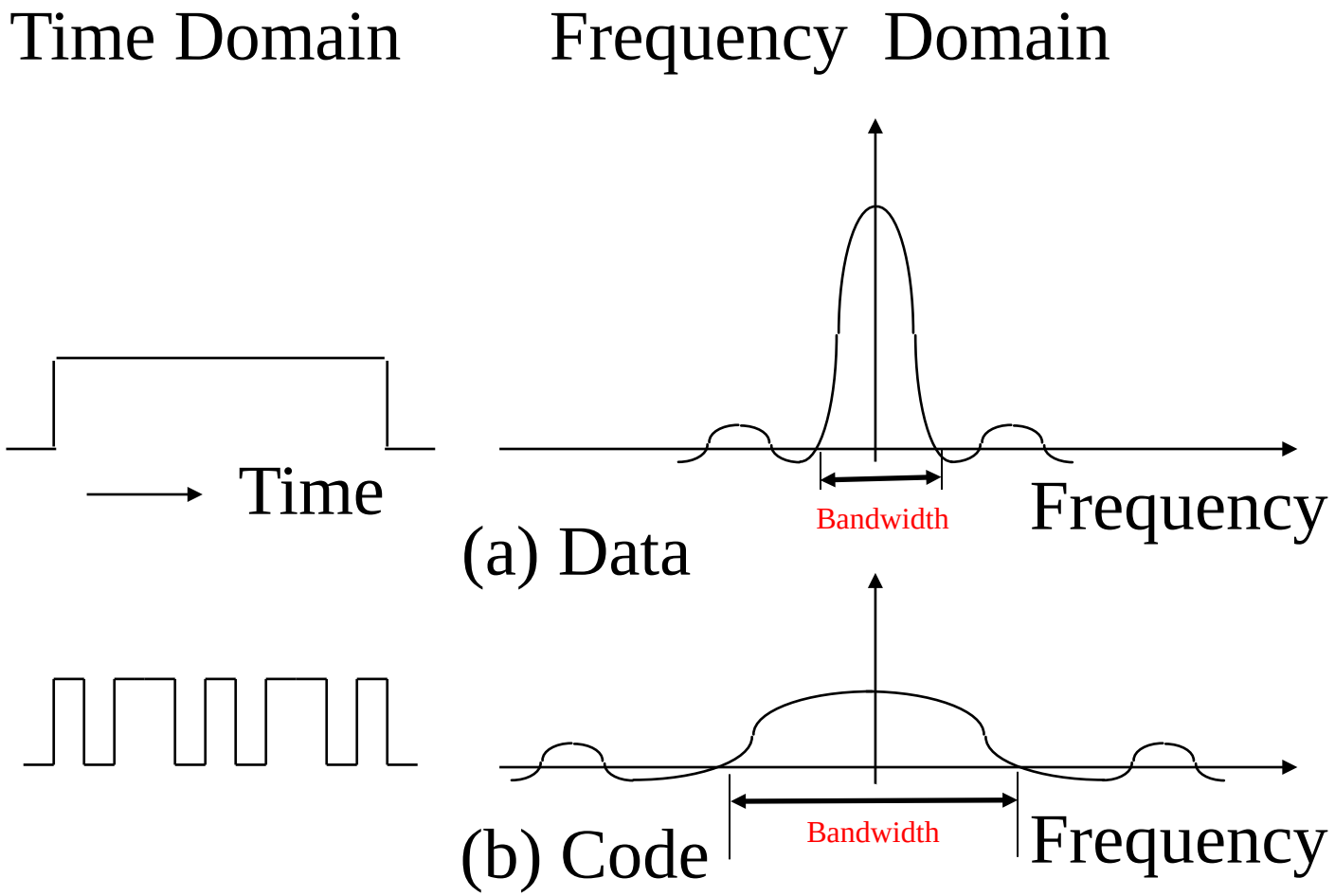
The base station assigns it.

- Does the military having 10,000 code bits per data bit mean each receiver can technically receive and recover 10,000 distinct signals?

Anything can be done at a cost. The larger the number, the more expensive it is. So it is difficult to interfere or intercept.

©2025 Raj Jain

DS Spectrum



Student Questions

- Why is the second graph horizontally stretched?

It has a higher frequency bandwidth.

- Could you re-explain this slide? Is the benefit of this transmission method to allow two signals to 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?

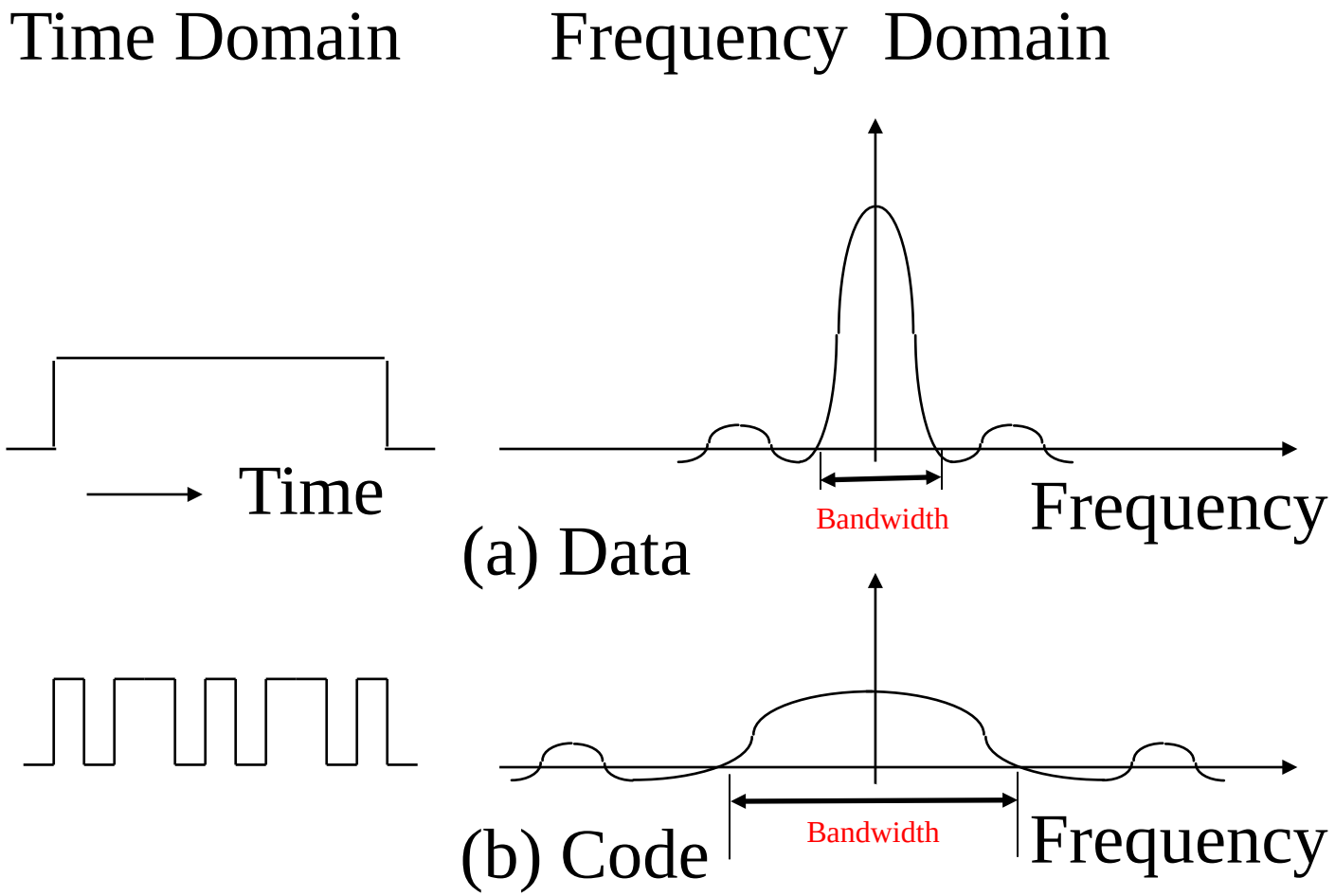
Random number generators and seeds are exchanged at the beginning of communication and periodically. The range is up to the users and standard bodies.

- 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

©2025 Raj Jain

DS Spectrum



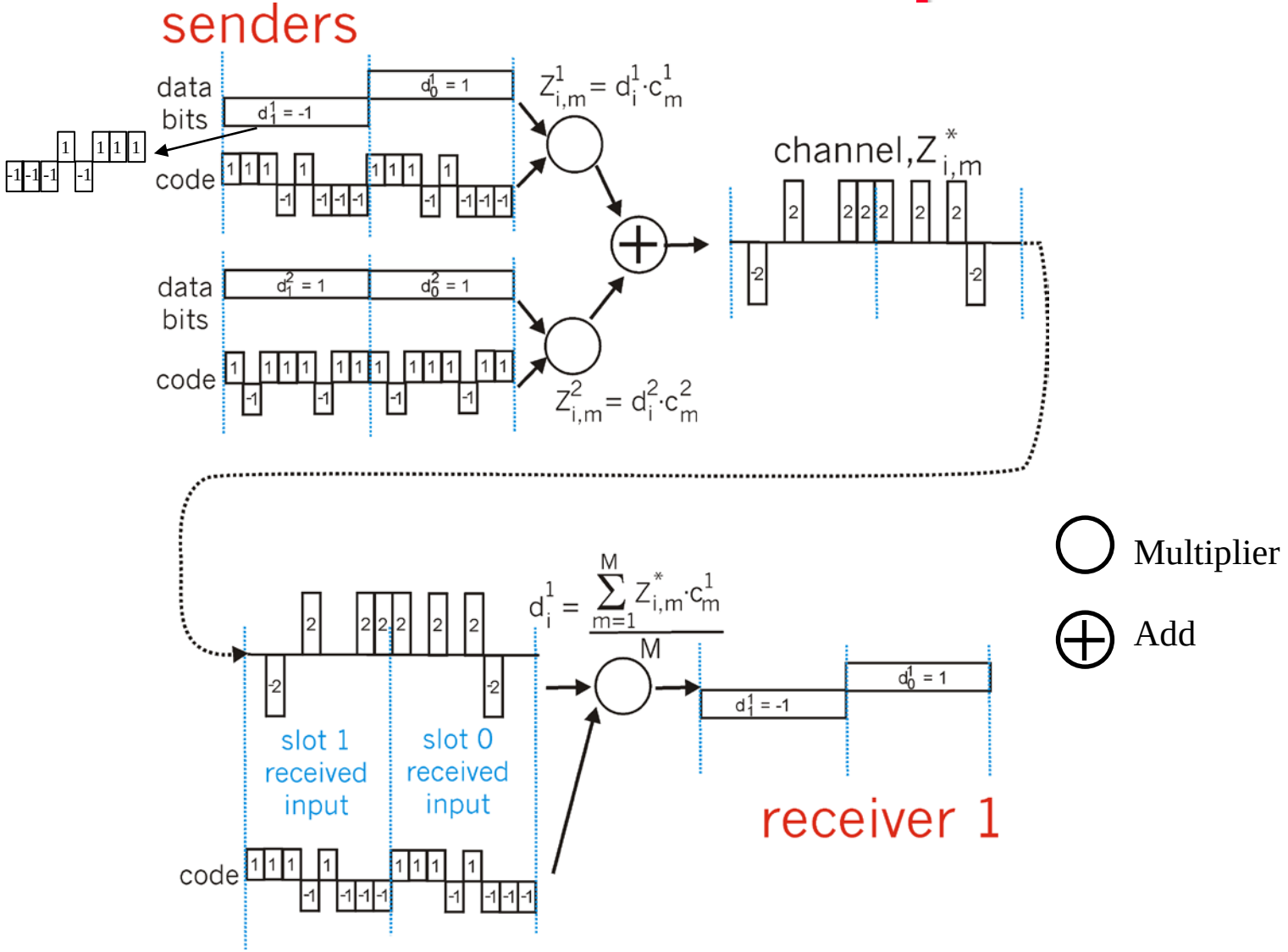
Student Questions

- ❑ What is the meaning of the vertical axis?
  Signal power
- ❑ Will Fourier transform be discussed in this course?

No.

©2025 Raj Jain

Two Sender CDMA Example



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?

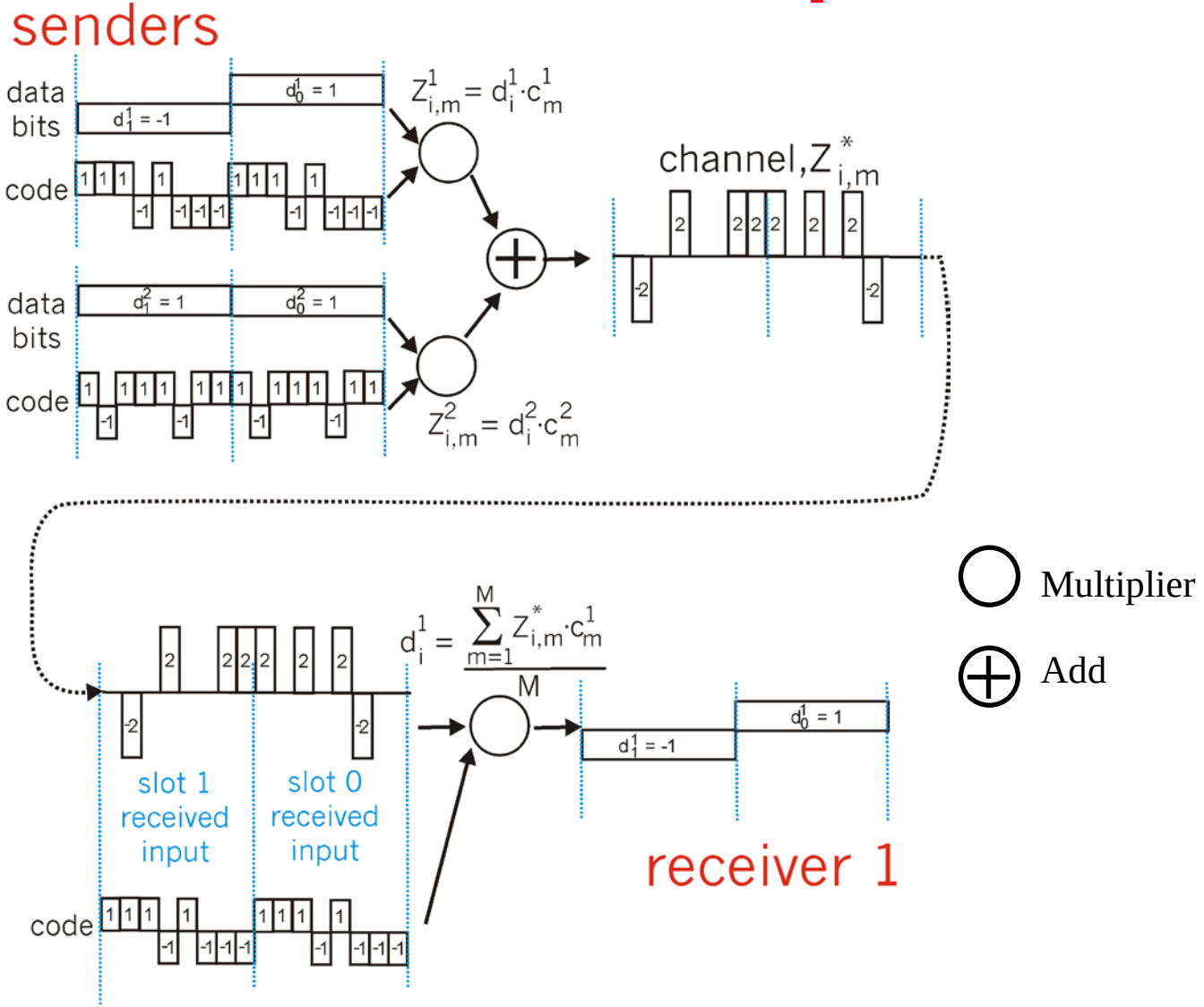
Number of code bits/data bits. M=8 in the example as shown.

- Page 541 in the book says, "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 the data cannot be recovered correctly if the sender codes are not orthogonal. Orthogonality is defined as* $\sum_{m=1}^{M} Z_{1,m} Z_{2,m} = 0$
- Can you review this slide again and the error in the slide?

All errors were corrected on the day they were discovered.

©2025 Raj Jain

Two Sender CDMA Example



Student Questions

- Why do we use +1 and -1 codes instead of 1 and 0? *Yes*
- How do they separate the two senders if they mix? *As shown in the bottom part*
- How are 2 and -2 represented in real life?

Negative/Positive voltage. 0/180 degree phase, low/high amplitude, different frequencies, depending upon the amplitude, phase, or frequency modulation.

- Can you go over this again?

Sure.

- Do we need to remember this process in our exam?

Yes. There is also homework.

©2025 Raj Jain

Homework 7A: CDMA Coding

- [6 points] Two CDMA senders use the codes (1, -1, 1, -1) and (1, -1, -1, 1). The first sender transmits data bit 1 while the 2nd transmits –1 simultaneously. What is the combined signal waveform seen by a receiver? Draw the waveform.

Student Questions

- Which of those codes corresponds to 0 and 1?

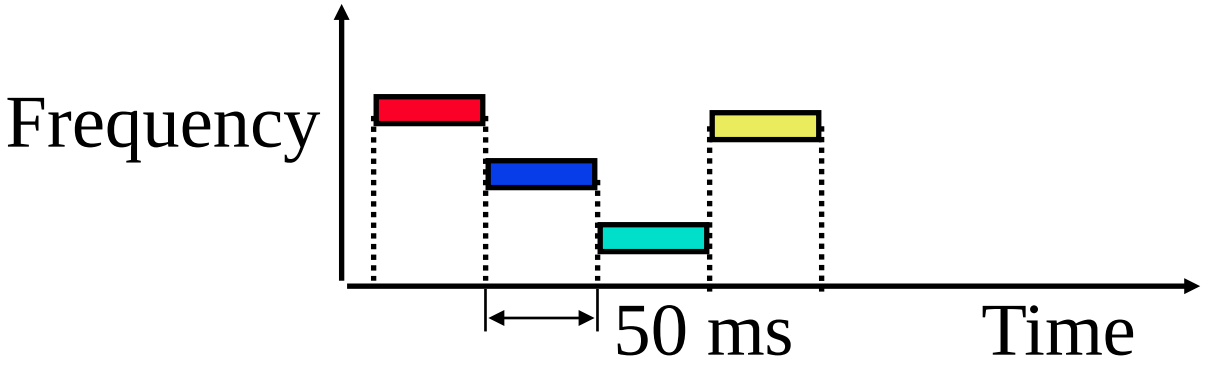
1 data = code seq
0 data = -code seq
User 1:
1 ={1, -1, 1, -1}
0 = {-1, 1, -1, 1}

- What does waveform mean? Are they the ones and the negative ones in the previous slide?

See the square waves on the previous slide.

©2025 Raj Jain

Frequency Hopping Spread Spectrum



- Pseudo-random frequency hopping
- Spreads the power over a broad 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 that the sender will change the frequency constantly?

The sender changes the frequency all the time. The receiver knows what frequency will be when.

- Does the Frequency Hopping Spread Spectrum work better than the Direct-Sequence Spread Spectrum since it's more familiar?

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?

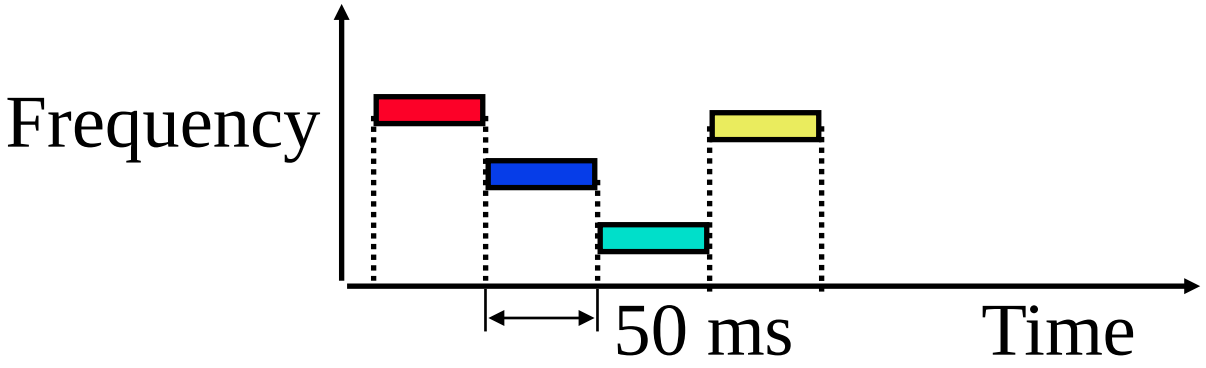
To avoid interference.

- Is the frequency hopping spread spectrum considered CDMA?

Yes.

©2025 Raj Jain

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

- Is this called "pseudo-random" because it is not "truly random"? If two people start with the same seed, will they have the same sequence of numbers? *Yes.*
- Can a random number generated by a selected seed be considered pseudo-random? *Yes.*
- Could someone jam all the possible frequency channels to interfere with the signal? *Yes.*
- What is the format of the "combined signal waveform"? *A code is used for each frequency. The waveform depends on the coding.*
- What does “narrowband interference can’t jam” mean?

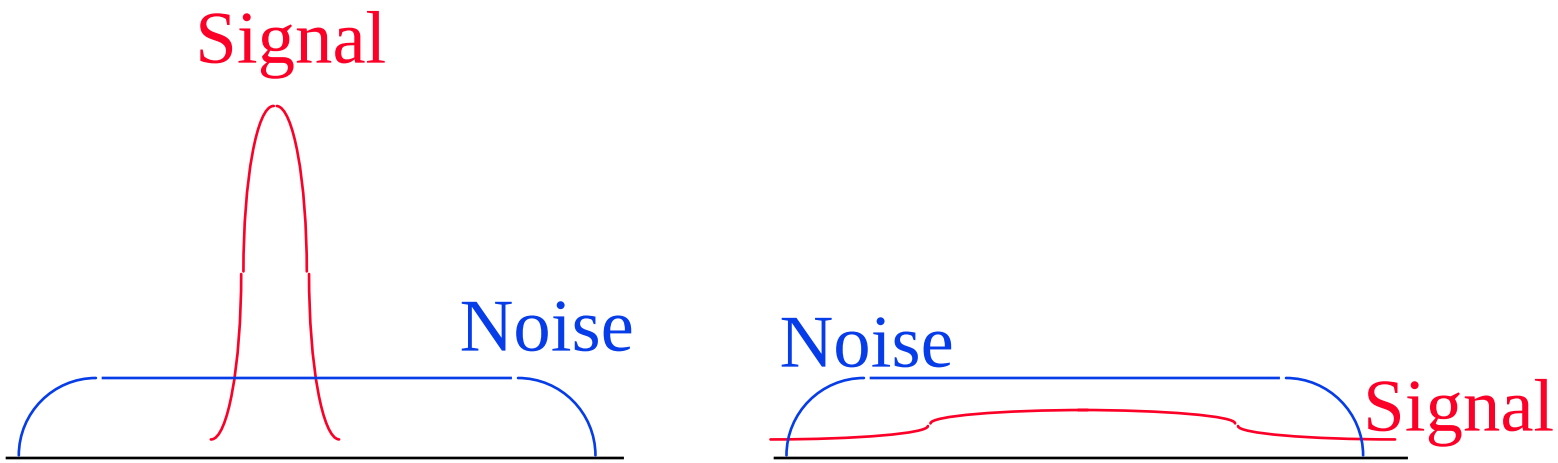
Interference that does not jam the entire band.

- The receiver knows what frequency will be when, but how?

Frequencies are generated using a pseudo-random number generator, e.g., $f_n = (af_{n-1}+b) \bmod c$

©2025 Raj Jain

Spectrum



(a) Normal (b) Frequency Hopping

Student Questions

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

Transmitting at the same frequency at the same time

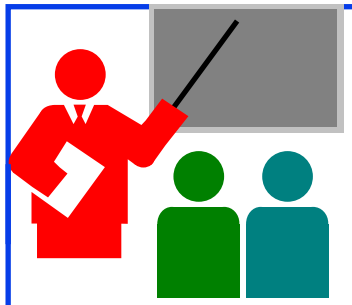
- What's the advantage of getting signal strength lower than noise strength?

Others don't know that there is communication going on here.

- Could you explain how frequency hopping is advantageous in this case? If the signal is below the noise threshold, does this not make it hard to differentiate the noise and the signal?

Over a long period, the average signal is below the average noise. But at all times, the power at the transmitting frequency is more than the noise at that frequency.

©2025 Raj Jain



Review: Wireless Link Characteristics

1. Wireless is different from mobile.
   However, most mobile nodes are wireless.
2. A wireless signal is affected by shadows, multipath, interference, and 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

- 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 that 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 should have corrected Q & A. I have corrected the answer above.

©2025 Raj Jain



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

©2025 Raj Jain

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 the 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 the physical layer?

Code division multiplexing

- Need to remember details for each version?

Yes.

- What is the MAC layer?

Please reread Chapter 6.

- What type of CDMA do these use most commonly?

DSSS as indicated.

- Is it important that 5.8 GHz = 2 * 2.4 GHz? Why?

*No. 5.8 is not 2*2.4*

- What do multiple priorities mean?

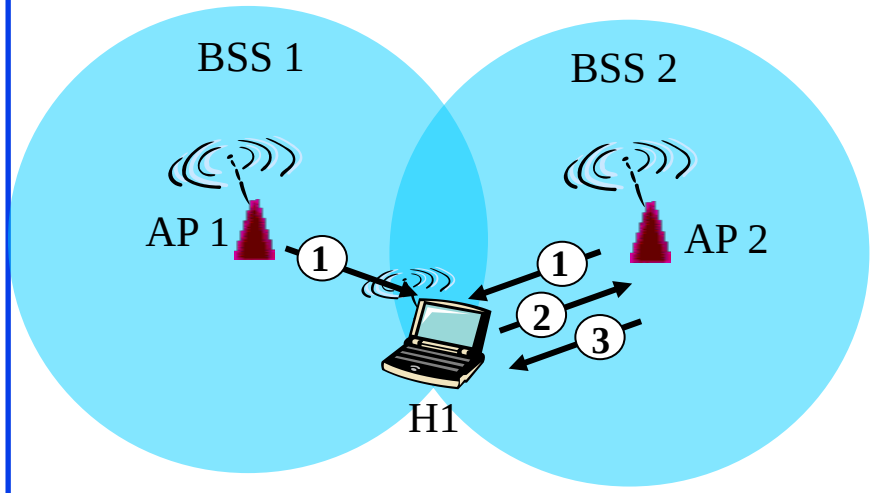
Higher-priority traffic goes first.

- What does time-critical mean?

Traffic that needs to be there in time, e.g., voice and video.

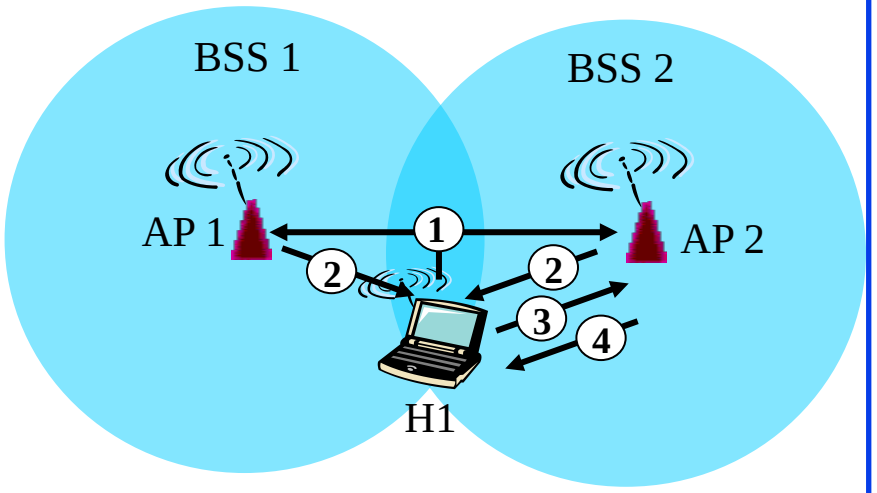
©2025 Raj Jain

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:

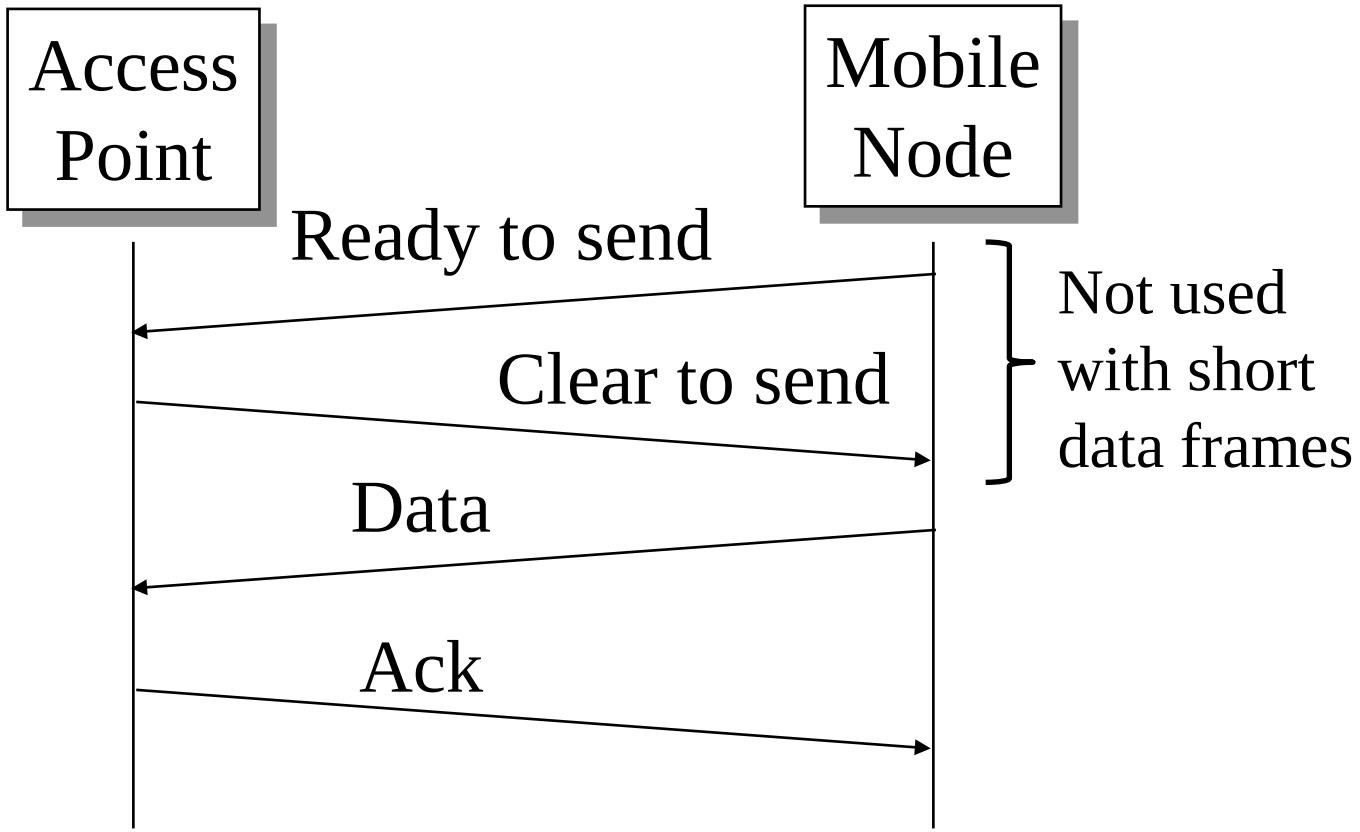
(1) **Probe Request** frame broadcast from H1
(2) Probes response frame sent from APs
(3) Association Request frame sent: H1 to selected AP
(4) Association Response frame sent: selected AP to H1

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.*
- What is AP? *Access point*
- Are both passive and active scanning used, or is one method dominant?
  Both are used.
- In which scenarios should we use passive scanning? And in which scenarios should we use active scanning?
  Active scanning is required if an AP does not announce for security.

©2025 Raj Jain

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.

- Is a 3-way handshake dramatically faster? Why not always use this 4-way model for some of the protocols we have previously seen that use a 3-way handshake?

All protocols have different requirements.

- Is CTS transmitted to every node in the network or just the node that sent the RTS?

Everyone hears everything.

- So CSMA/CA prevents collision but cannot detect a collision?

Yes.

- Is it possible for multiple nodes to send an RTS simultaneously? If so, what happens in this case?

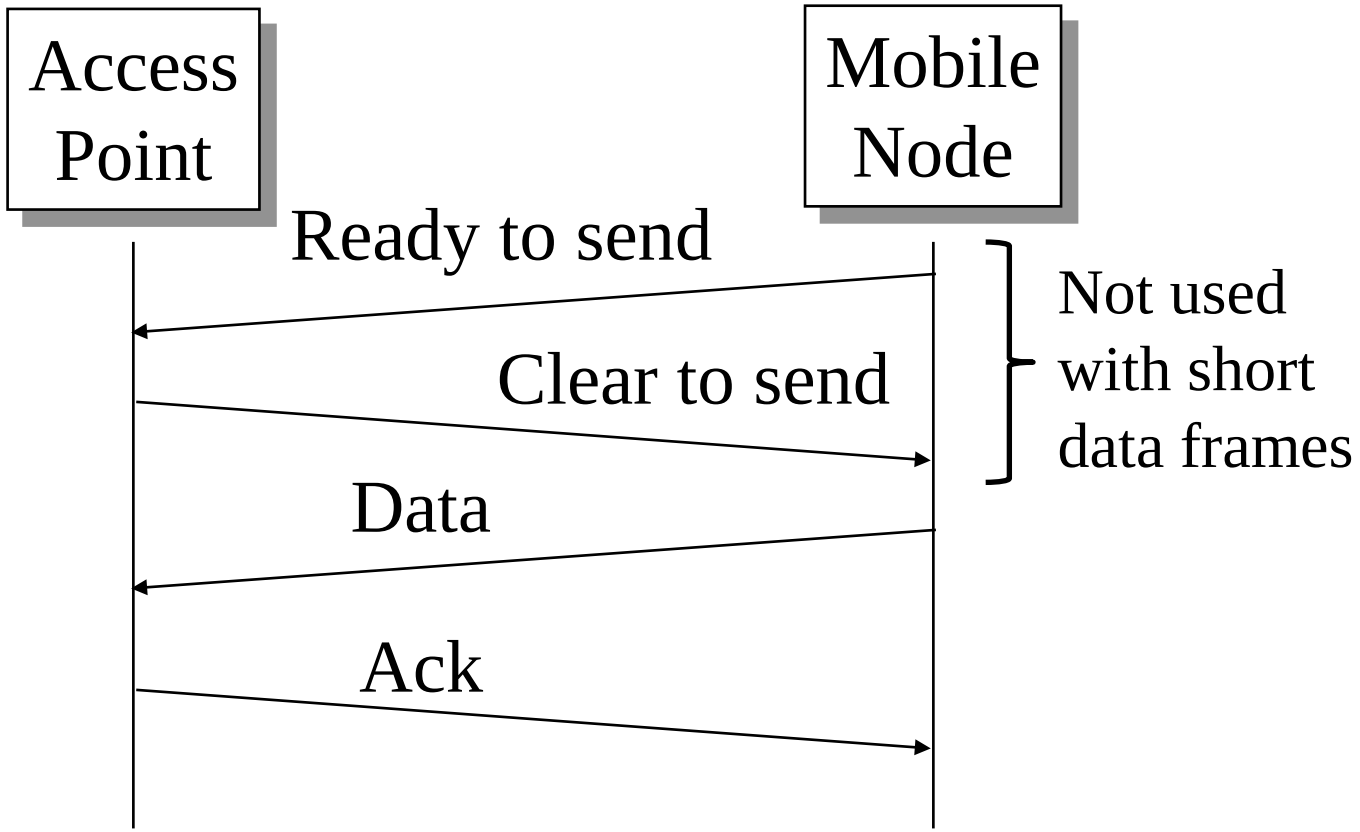
- *RTS is lost. They don't get a CTS and try again later.*

- Is there a handshake process for peer-to-peer?

- *Yes, since there could be other peers around.*

©2025 Raj Jain

4-Way Handshake



Student Questions

- Chapter 7.3, fig. 7-12: When deferring access to the wireless channel after receiving a CTS message, do non-transmitting nodes wait for a predetermined time (sent in the CTS) or do they wait indefinitely until the ACK is received?

They wait for SIFS+CTS+SIFS+SIFS.

- Is there a buffer added to the CTS delay to account for processing delay?

SIFS allows for processing delay.

©2025 Raj Jain

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 the destination address and duration of the message. It tells everyone to back off for the duration.
- The destination sends: Clear to send (CTS)
- Can not detect collision ⇒ Each packet is acked.
- MAC level retransmission if not acked.

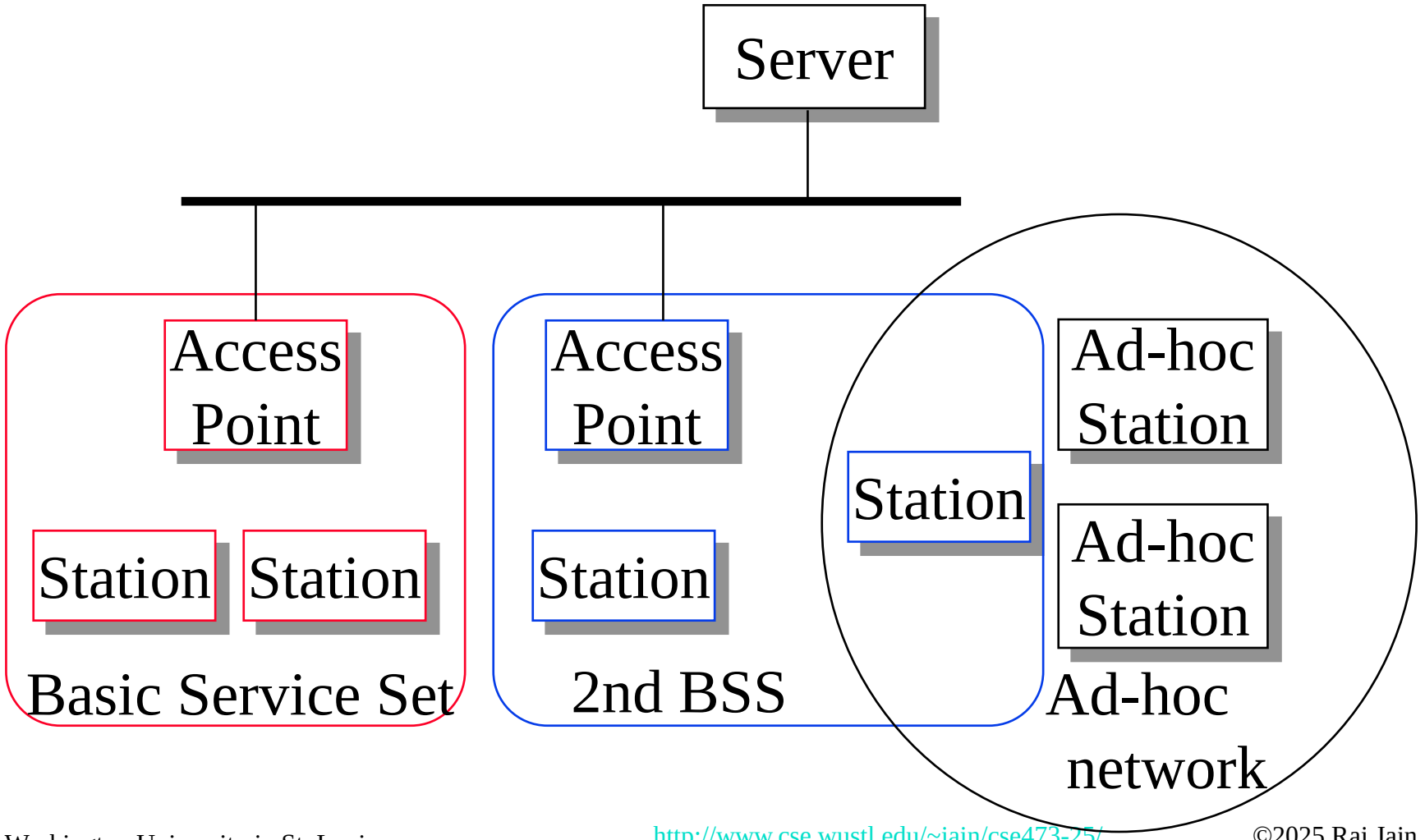
Student Questions

- Multiple nodes may send the RTS simultaneously, but only one will receive CTS.

Yes.

©2025 Raj Jain

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 identical SSID
- Basic Service Set (BSS)
  = Set of stations associated with an AP ={MAC_1,…,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.

- What is the relationship between BSA and BSS?

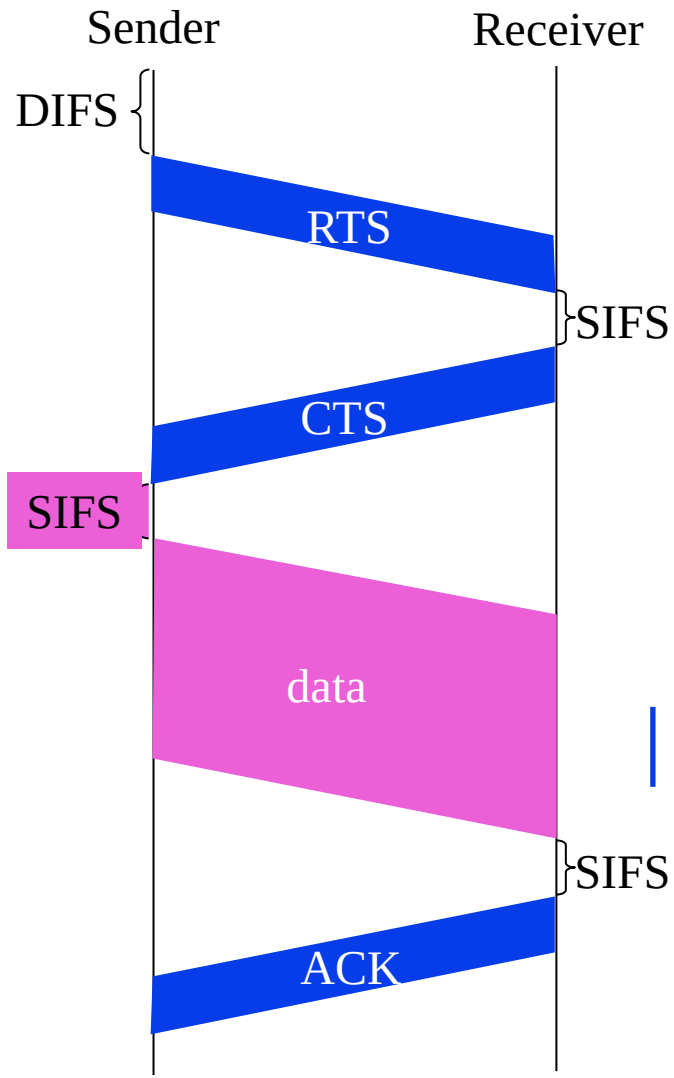
BSA is the area (Geographic)
BSS is the set of stations

- So an ESA can consist of BSSs that are not physically adjacent and have the identical SSID?

- *Exactly. They may or may not be adjacent.*

©2025 Raj Jain

Transmission Example



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

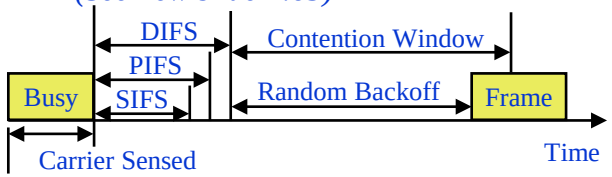
RTS, CST, and ACK are each one slot time long.

Each frame has a duration field. Everyone hears every frame.

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.

- Why do we need to have different values for DIFS and SIFS?

No one transmits if they hear RTS/CTS/Data—so there is a shorter wait.

©2025 Raj Jain

Homework 7B: Wi-Fi Transmission

- [6 points] Suppose an 802.11b station is configured permanently to reserve the channel with the RTS/CTS sequence. Suppose this station suddenly wants to transmit 2,000 bytes of data, and all other stations are idle at this time. Assume a frame without data is 32 bytes long and has a transmission rate of **10** Mbps. Using SIFS of 30us and DIFS of 60us, ignoring propagation delay and assuming no bit errors, calculate the time required to transmit the frame and receive the acknowledgment.

Ref: Problem P7

Student Questions

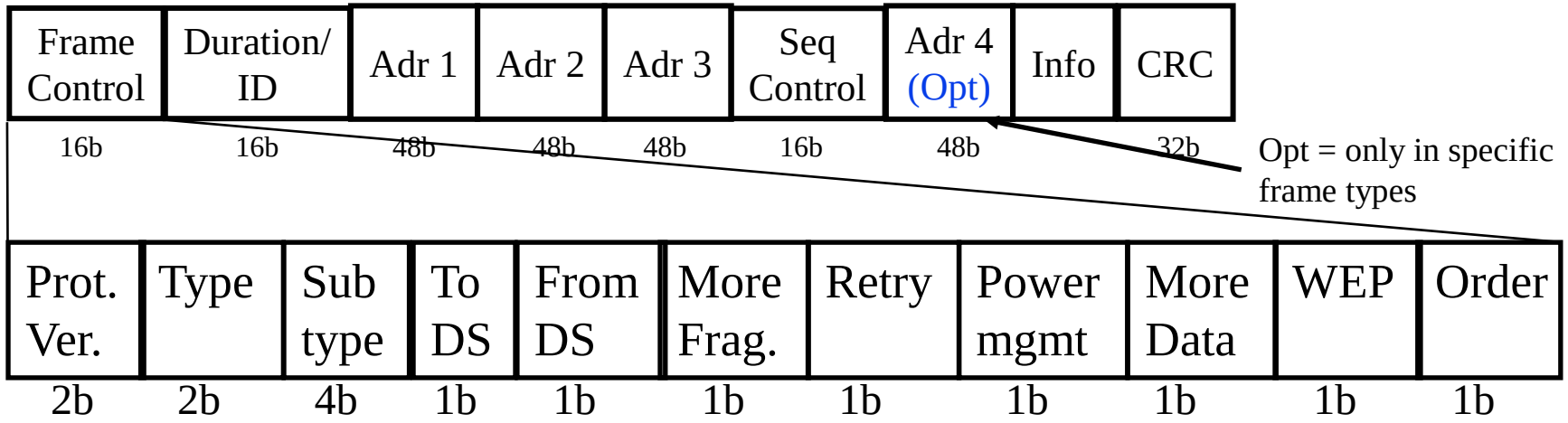
- Could you go over HW 7B? Is there a specific formula we use to calculate time?

You need to know the bit rate of 802.11b. It is 11 Mbps.

- Could you explain why the total size of the data frame is 2032 bytes instead of just 2000 bytes?

Data=Payload. Need 32 bytes of header.

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.

- What do the subtypes entail?

See the list in the slide.

©2025 Raj Jain

MAC Frame Fields

- **Duration/Connection ID**:
  - If used as a duration field, it indicates the time (in μs) channel will be allocated for successfully transmitting the MAC frame. Includes time until the end of Ack
  - In some control frames, it contains an 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 the MAC frame on the Internet?

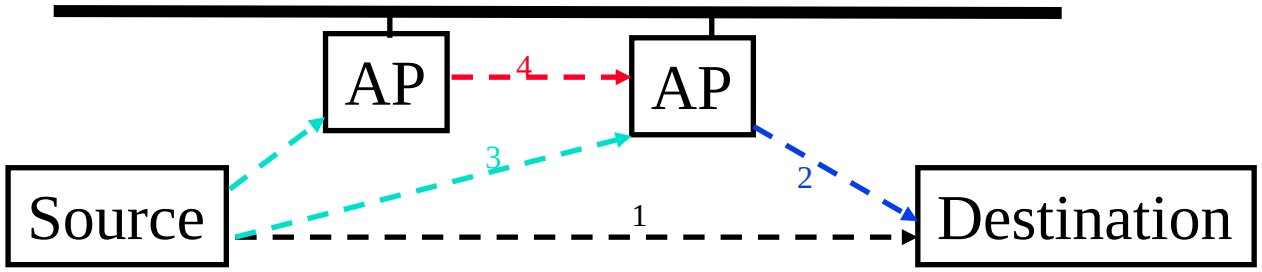
Mac Frame = Wi-Fi Frame

- When do control frames have association identifiers and when do they not?

©2025 Raj Jain

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 a multicast to all base stations on this SSID. Any AP can receive and forward. The packet is addressed to a specific AP identified by the receiver address in the last row.

- Is the BSS ID the Access Point address? Why does the first row need a 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 a private plane.

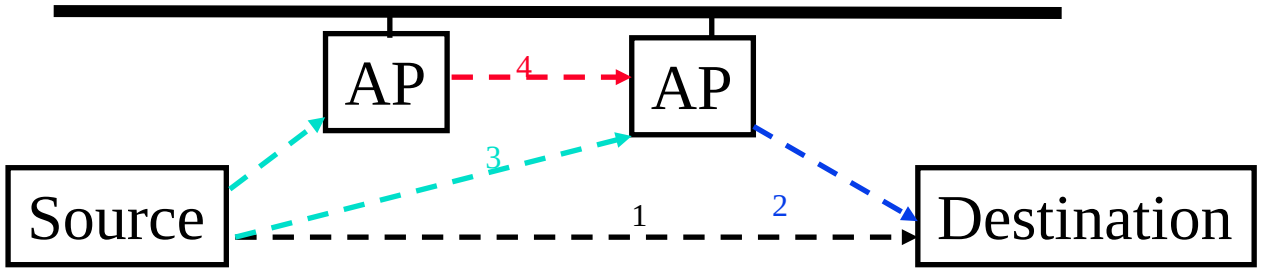
- Are source and destination stations or BSS?

The source is the first station on the wireless, and the destination is the last. They are all in the same BSS.

©2025 Raj Jain

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

- Is the destination address the final destination address or the address of the destination for the individual link (i.e., one of the APs)

Transmitter, Receiver, Source, and Destination are four different terms.

- What does a distributed system mean?

Access Points

- Where are the addresses 1-4 stored?
- *In the Wi-Fi header.*
- Why is there a BSS ID field in the first row if frames with 0/0 don't involve an access point? Are these frames always part of ad-hoc connections?
- *The direct link is a new feature introduced in later versions of Wi-Fi. The two nodes have to follow the rules of the BSS. This can be used even without Ad-hoc.*

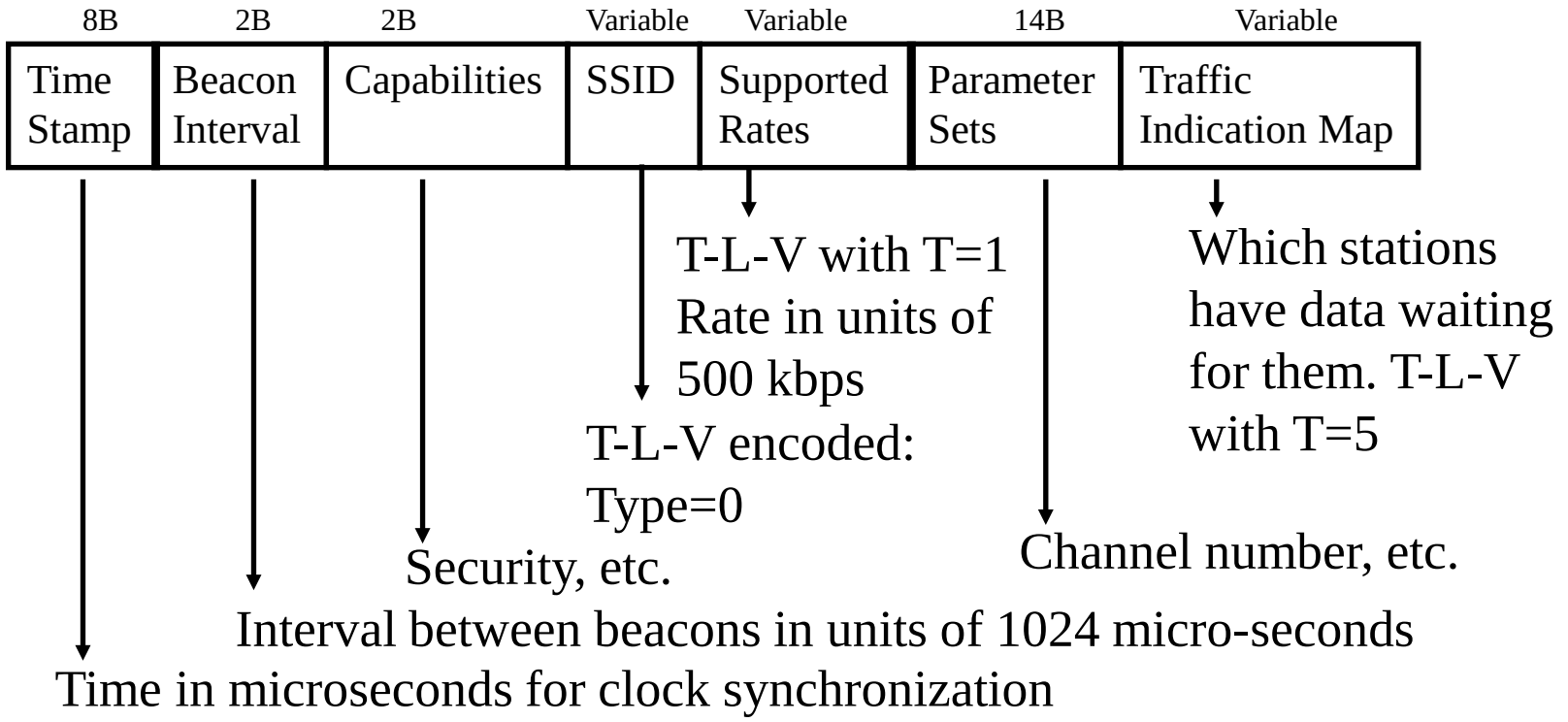
- Are the distribution systems base stations?

Distribution system = backend network to which base stations are connected.

End of Part 1 Next Q 31c

Beacon Frame Format

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



Ref: Nayarasi, "802.11 Mgmt: Beacon Frame," https://mrncciew.com/2014/10/08/802-11-mgmt-beacon-frame/
Washington University in St. Louis http://www.cse.wustl.edu/~jain/cse473-25/

©2025 Raj Jain

Student Questions

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

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

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

SNR = Cause

BER = Effect

Coding and retransmission decide acceptable BER ⇒ 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 identical SSIDs? If yes, how would a host be able to tell?

Multiple APs can serve the identical SSID, but multiple owners cannot have the identical SSID in the exact location, like two different Raj Jains living in my house address.

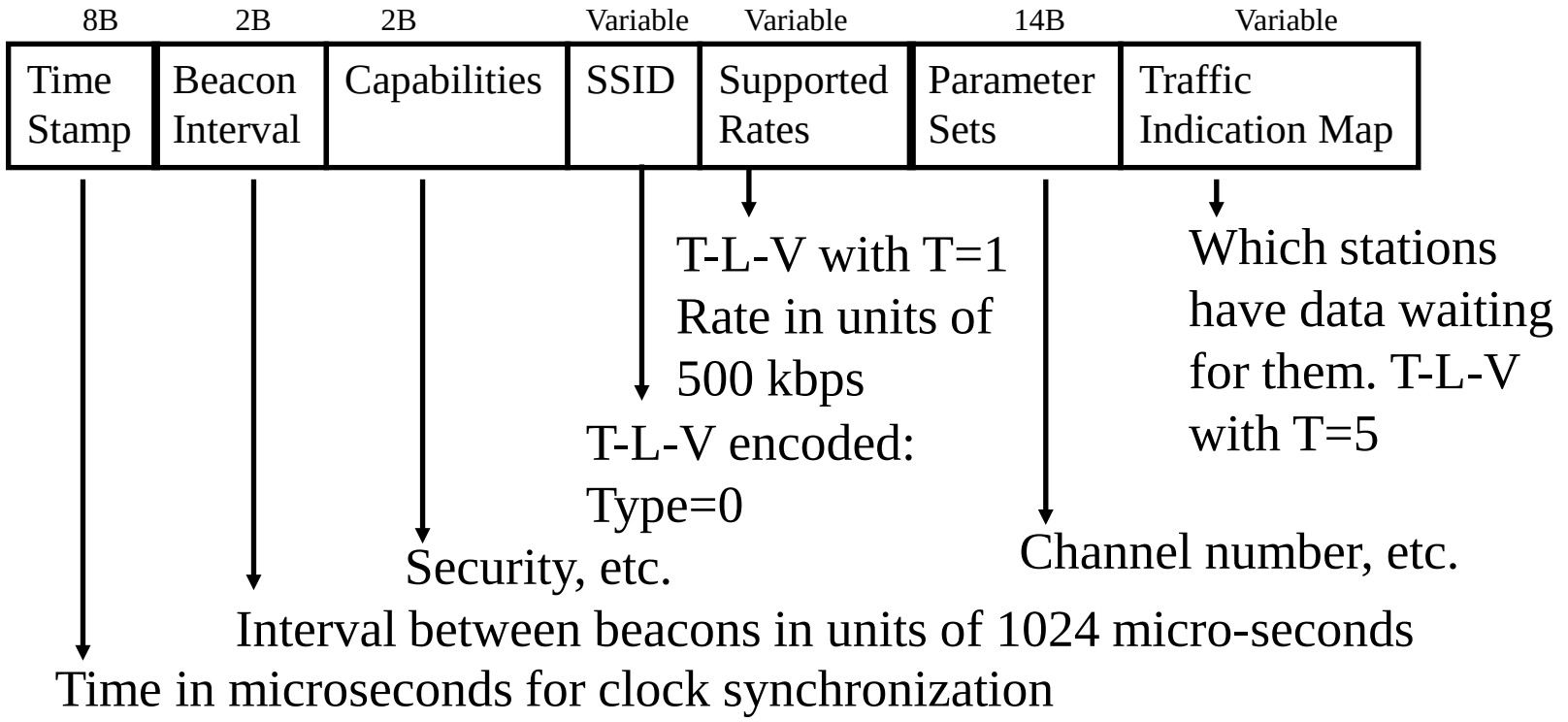
- Could you explain TLV again?

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)



Ref: Nayarasi, "802.11 Mgmt: Beacon Frame," https://mrncciew.com/2014/10/08/802-11-mgmt-beacon-frame/
Washington University in St. Louis http://www.cse.wustl.edu/~jain/cse473-25/

©2025 Raj Jain

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?

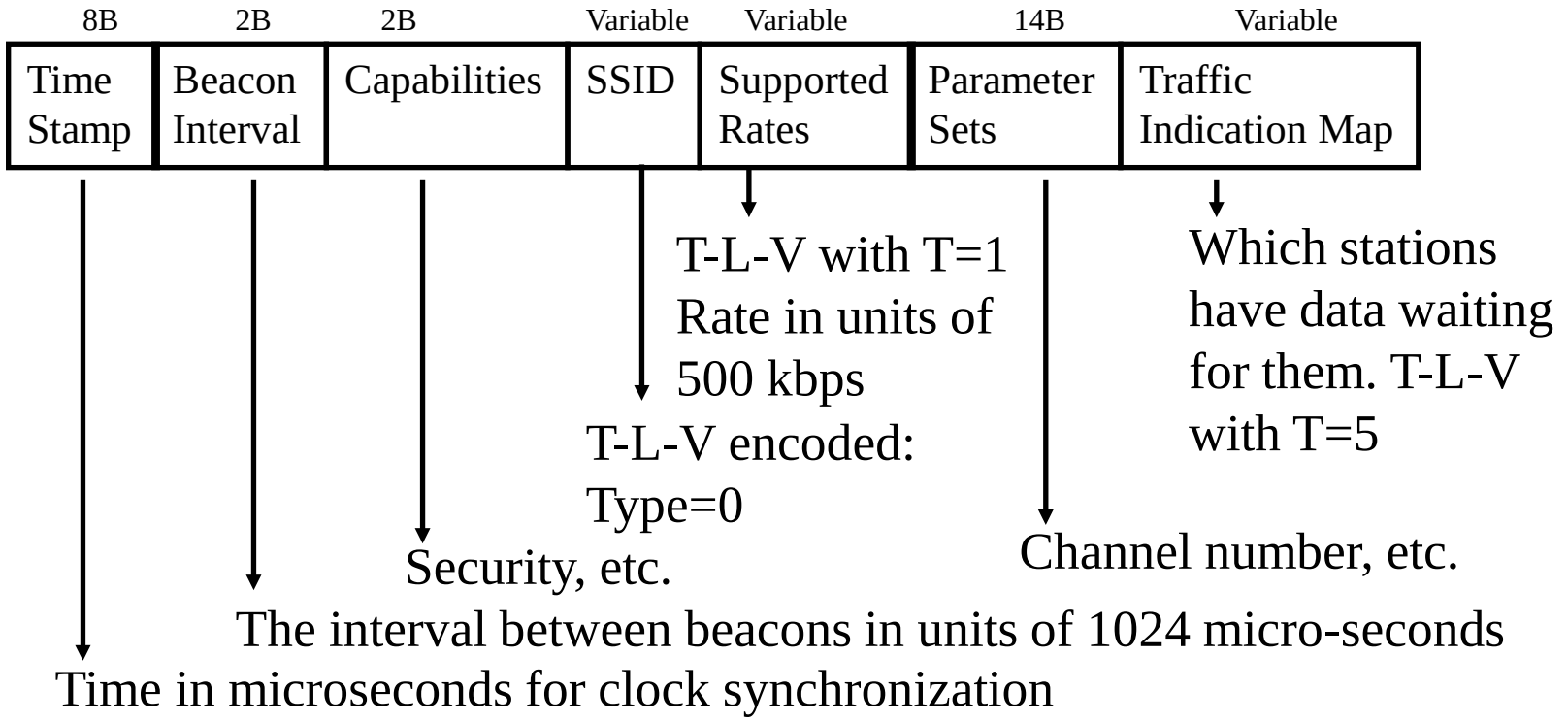
Capabilities: WEP, WPA, WPA2, …

- 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)



Ref: Nayarasi, "802.11 Mgmt: Beacon Frame," https://mrncciew.com/2014/10/08/802-11-mgmt-beacon-frame/
Washington University in St. Louis http://www.cse.wustl.edu/~jain/cse473-25/

©2025 Raj Jain

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, 2nd element is the length, and 3rd element is the field's value. It is commonly used for variable-length fields. In this slide:
Type:
0=SSID
1=Rate
…
5=Map

- What is the difference between an SSID and a BSSID?

SSID is the name of the network. It consists of several APs. Each AP has a BSS. AP MAC address is used as a BSS ID.

- Is the beacon frame in the info field of the Wi-Fi frame? *No. It is a separate frame.*
- Are the sizes of the fields in the Beacon Frame in Bytes or Bits? It says B on the slides, but I thought I heard you say bits in the video recording.

B=Bytes, b=bit

Lab 7:Wi-Fi

[14 Points] Download the Wireshark traces from
http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip

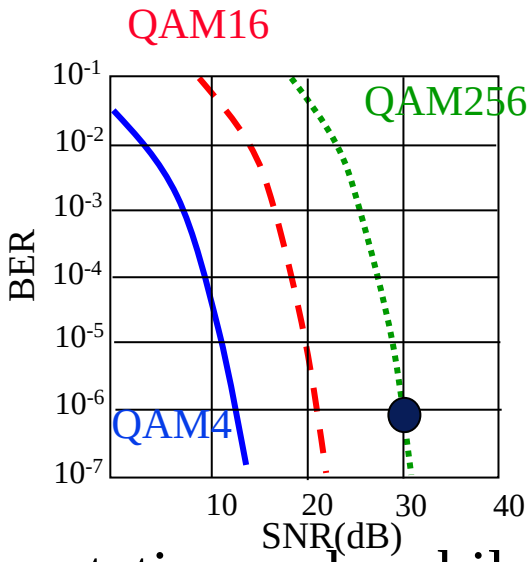
Open *Wireshark_802_11.pcap* in Wireshark. Select **View → Expand All**. Answer the following questions. There is no need to attach screen captures.

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 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 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

©2025 Raj Jain

802.11 Rate Adaptation



QAM=Quadrature Amplitude Modulation

$QAM2^n = n$ bits/Hz

dB = Deci-Bel

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

- The base station and mobile dynamically change transmission rate (physical layer modulation technique) as mobile moves, and SNR varies.
- SNR decreases ⇒BER increases as the node moves away from the base station
- When BER becomes too high, switch to a lower transmission rate but with lower BER

Student Questions

- Why does wireless network coding change due to the BER change?

Use fewer 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 once on a conference call, you need to keep track of who said what.

- Does 20 megahertz a standard? Can we temporarily raise this to 200 or more if we want to send things faster quickly?

20 MHz is a standard channel width. Some may use more than one channel, such as fitting multiple nodes in a single box.

- Does the "dB" in the slide relate to acoustic units "db"?

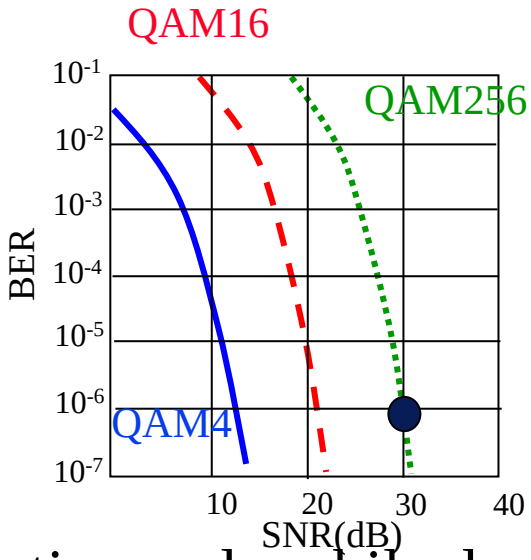
dB = decibel
DB = Deca-Bel
B is the name so consistently capital.

- How do we maximize SNR?

By increasing the signal power. But that may increase your battery consumption.

©2025 Raj Jain

802.11 Rate Adaptation



QAM=Quadrature Amplitude Modulation

$QAM2^n = n$ 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 ⇒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 enter the same area, noise increases, => SNR decreases.
=> 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

- How are bit errors detected?

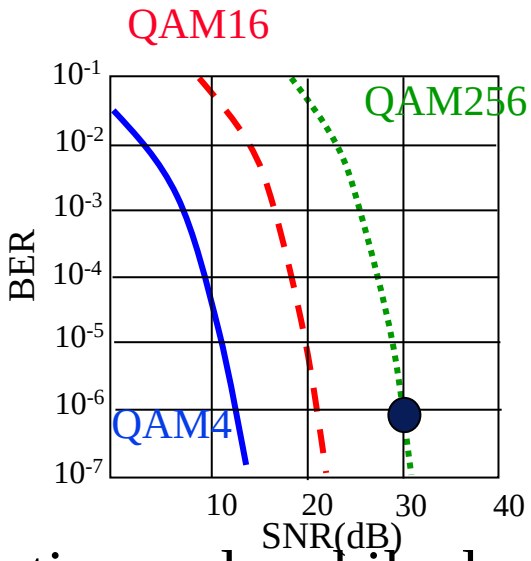
Coding

- Must the number after QAM be a power of 4?

Any power of 2 can be used. However, only even powers are generally used.

- So, does the graph's vertical axis indicate the error rate? *Yes.*

802.11 Rate Adaptation



QAM=Quadrature Amplitude Modulation

$QAM2^n = n$ 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 ⇒BER increase as the node moves away from the base station
- When BER becomes too high, switch to a lower transmission rate but with lower BER

Student Questions

- Why does a higher information rate come with a higher error rate?

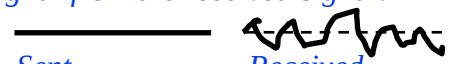
The Y-axis is "lower-is-better."

- Does changing BER imply the actual coding scheme changes between QAM or the encoding frequency?

The coding scheme is changed.

- How is noise calculated? The signal seems to be the only thing that can be measured. Is the noise assumed to be at a constant rate?

Noise can be measured by subtracting a sent signal from the received signal.

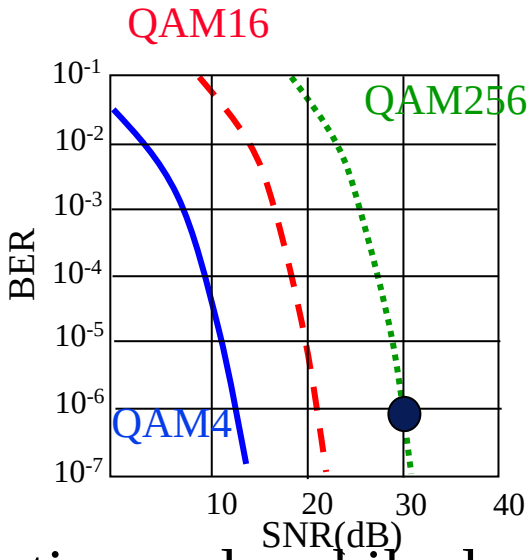


- When discussing advanced features in 802.11, could you explain mod about rate adaptation?

Question not clear.

©2025 Raj Jain

802.11 Rate Adaptation



QAM=Quadrature Amplitude Modulation

QAM2^n = n 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 ⇒BER increase as the node moves away from the base station
- When BER becomes too high, switch to a lower transmission rate but with lower BER

Student Questions

- What value is considered "high" for BER to trigger the switch?

Each designer selects a BER threshold depending upon the current state of the art and SNR.

©2025 Raj Jain

Power Management

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

Student Questions

- How large is the buffer size in AP? Will there be too much data when the station does not cool down for a long time?

If you doze, you lose. AP will save only a few frames.

- Do the dozing stations only wake up in a time-interval-based manner? Or is there some wireless hardware that has a lower-power processor that's always on and "listening"?

Since the beacons are periodic, it is okay to wake up and listen for the next beacon. The other approach is used for random events like remote boot.

- What is the point of dozing when frames are lost anyway?

The frames are saved at the AP and are not lost.

- Does the AP announce which station has frames buffered via a multicast, or only let the individual station know?

Announced in each beacon frame.

Power Management

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

Student Questions

- Is there some standard for how long a station must be dozing to be more power efficient than just constantly being on?

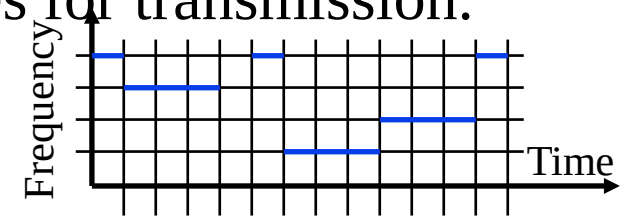
Equipment designers calculate the battery life and decide.

©2025 Raj Jain

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 μA on 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 coordinates, it will need to spend more energy, which is bad for that device.

You are right. Only bigger devices can become the primary node. For example, a Phone vs. a headset, or a computer vs. a 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?

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?

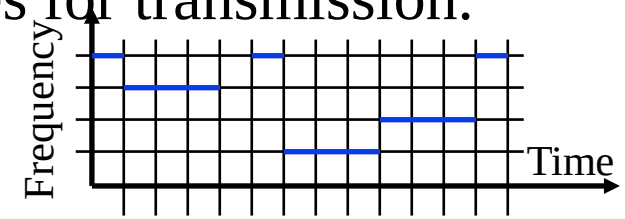
Sleep more.

©2025 Raj Jain

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 μA on 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

- 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, based on Bluetooth, piconet 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.

- Does Bluetooth use the SPI specification for the "piconet?"

Serial-Parallel Interface (SPI) is for wired networks. Bluetooth does not use SPI.

- Why is Bluetooth only for cell phone communications here?

It was started for cell phone communication.

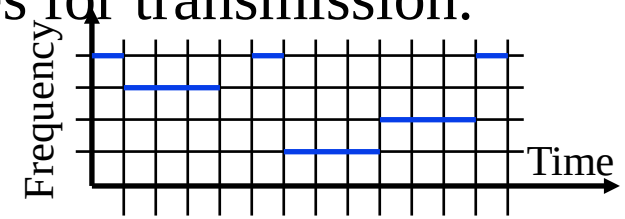
- What are the potential security risks associated with using Bluetooth, and how can we ensure that Bluetooth-enabled devices are secure? *Bluetooth's security has improved over the years.*

©2025 Raj Jain

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 μA on 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

- Why can't we abstract Bluetooth like we allocated subnets? Why can't a "slave" have its own "slaves," and the timeslots it is given from its master just get divided further amongst its slaves? *KISS*
- Why is it called a piconet?

Pico is tiny.

- How do devices coordinate communication over frequency hopping if constantly switching?

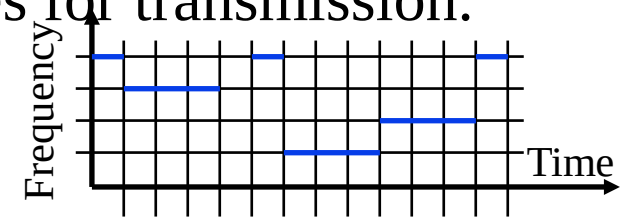
They use the same seed and the same random number generator.

©2025 Raj Jain

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 μA on 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

- For frequency hopping, Bluetooth uses a random seed to determine where to hop. Would this benefit security?

It is not secure. The seed can be easily computed since the generator is standard.

- What makes Bluetooth so cheap?

It is designed for short distances and low power with no amplifiers.

- I heard Bluetooth can reach ranges of over a kilometer. Why is it never typically used for these types of ranges?

High Cost of amplifiers

- What is the poll frame?

The master sends a poll frame to determine who will go next.

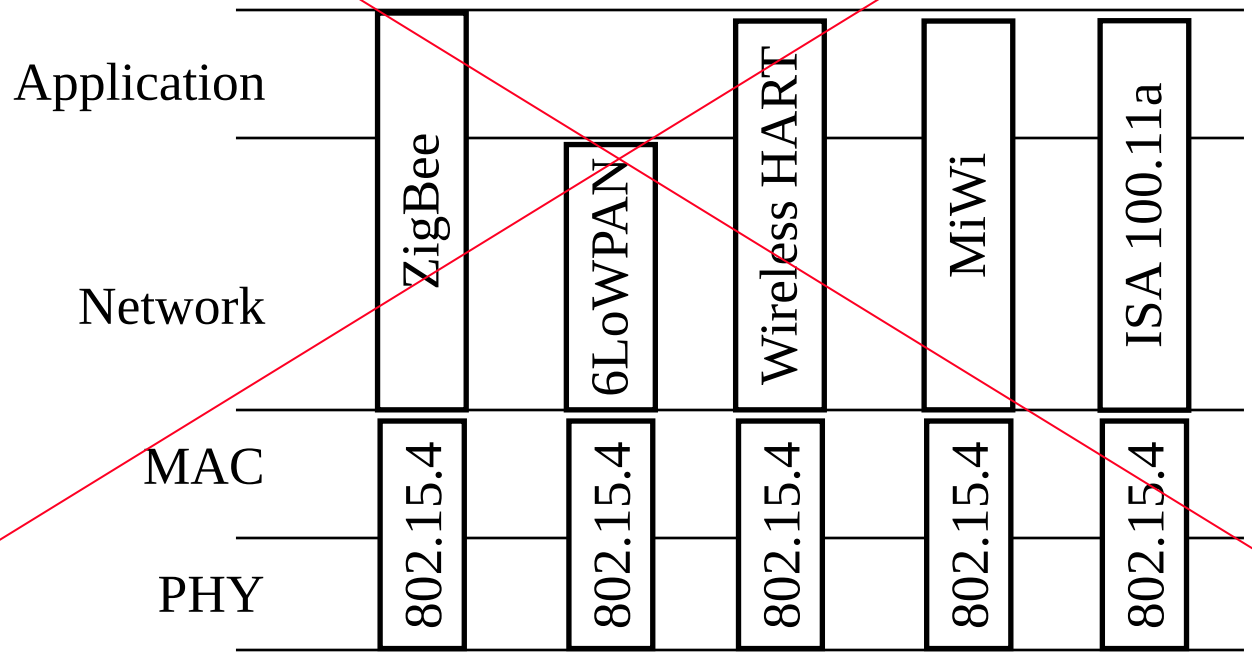
- Why is Bluetooth mainly used for audio devices or keyboards today? Why isn't it used to connect to routers, etc.?

Low power, low data rate.

©2025 Raj Jain

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 ⇒ Lower power ⇒ 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. The bank balance is your Energy, and $100 is your power.

- For ZigBee, there's a line halfway between Network and Application. What does that represent?

Applications are built into ZigBee.

- Do we have to know the specifics of each type of IoT protocol for the exam?

No. You need to know the names.

- I just wanted to confirm that these slides won't be on the exam.

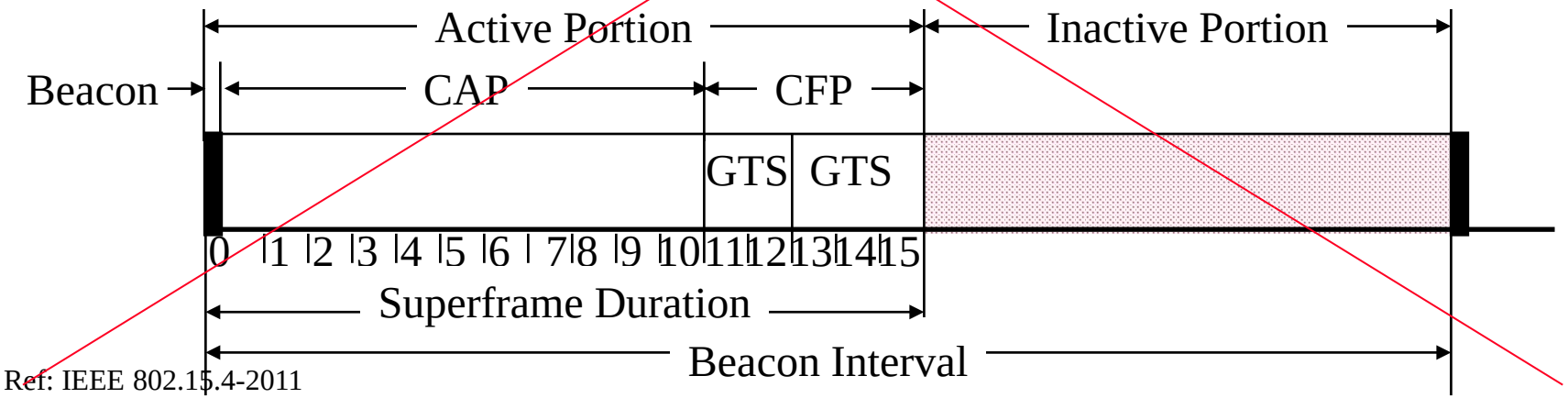
Confirmed.

©2025 Raj Jain

IEEE 802.15.4 MAC

Beacon-Enabled CSMA/CA

- The coordinator sends out beacons periodically
- Part of the beacon interval is inactive ⇒ 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.



Student Questions

- What is "superframe duration"?

Sixteen slots, as shown.

- Does the coordinator here mean access point?

They call it Hub.

- Does CFP consist of GTSs? *Yes.*
- What is the difference between the coordinator and the master?

Master-slave was used in Bluetooth.

Coordinator is used in 802.15.4.

- Why is it for short patterns?

The question needs to be clarified.

- Is the 0 slot of the superframe duration longer than other slots shown in this picture?

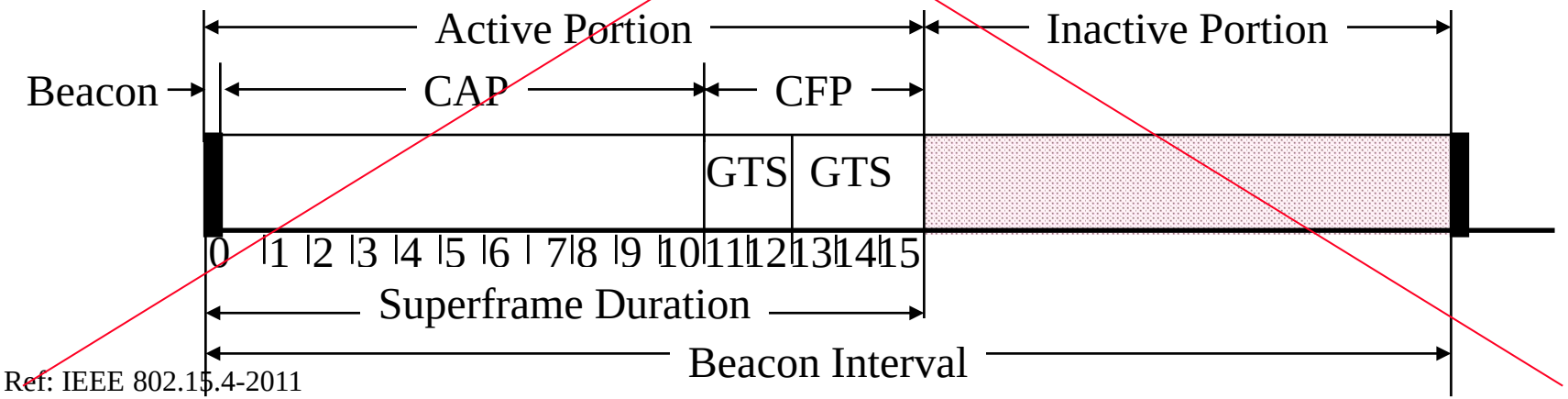
The coordinator uses the black area to announce network properties. All slots are the same size.

©2025 Raj Jain

IEEE 802.15.4 MAC

Beacon-Enabled CSMA/CA

- The coordinator sends out beacons periodically
- Part of the beacon interval is inactive ⇒ 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.



Student Questions

- Do all IEEE 802.15 devices use collision avoidance instead of collision detection? Is there a way for them to detect collisions wirelessly?

All wireless networks have a hidden node problem.

- Does CAP always get ten slots and CFP get six slots, or is this just an example?

This is just an example.

- How does the GTS work? Some examples?

Constant Bit Rate video requires fixed, say, 5 Mbps. It can use GTS.

- The graphic says "Superframe duration" what's the difference between a regular frame like we were talking about in the last chapter and super frame?

Frame = One station's transmission
Super Frame = Entire Network

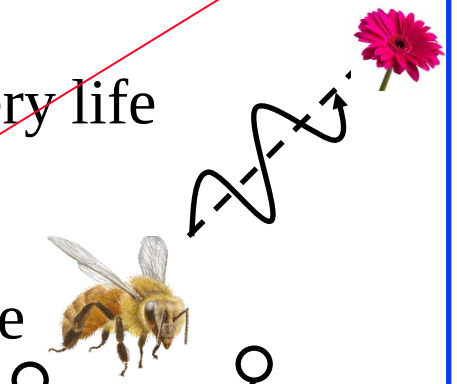
- Does the presence of loops mean there is a non-zero chance that a message will never be delivered?

Star-shaped networks do not have any loops.

©2025 Raj Jain

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

Ref: ZigBee Alliance, http://www.ZigBee.org

©2025 Raj Jain

Student Questions

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

Routing = Method.
End nodes route other end nodes' packets.

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

It is possible to have all four combinations of routing and topologies.

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

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

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

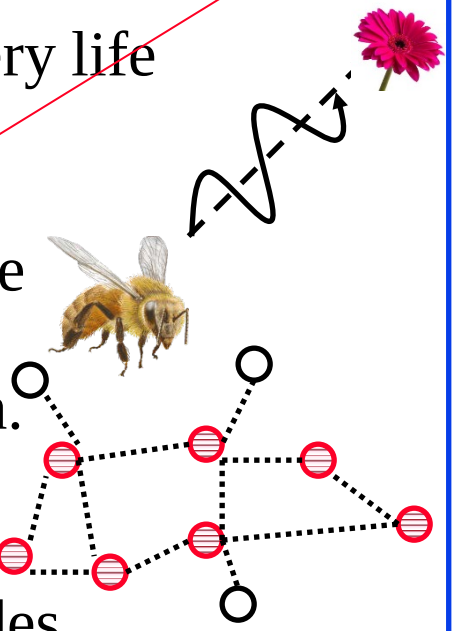
The dictionary meaning of "ad-hoc" is "created or done as necessary." or not set in advance. They can have loops.

- What distinguishes ad-hoc from mesh topology?

Mesh: It has a fixed topology. It may be a linear bus, star, 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

Ref: ZigBee Alliance, http://www.ZigBee.org

©2025 Raj Jain

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 the node, telling the primary to send those frames. After receiving the frame, most of the node goes back to sleep.

- What's the difference between Zigbee and traditional routing?

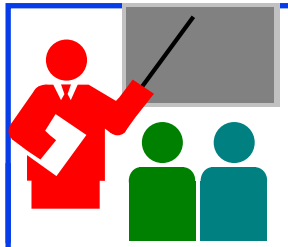
ZigBee nodes are simple and cheap.

- What is the difference between Multi-hop routing and Mesh Routing? Both seem to be used to route packets between multiple nodes in a wireless network.

The difference is indicated in the slide.

- How do mesh routing and topology differ?

Topology = Configuration
Routing = Method



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 the 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~~

Student Questions

- If APs buffer traffic for dozing stations, do the APs also send TCP acks on behalf of the dozing stations? If not, there will be many 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.

©2025 Raj Jain



Cellular Networks

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

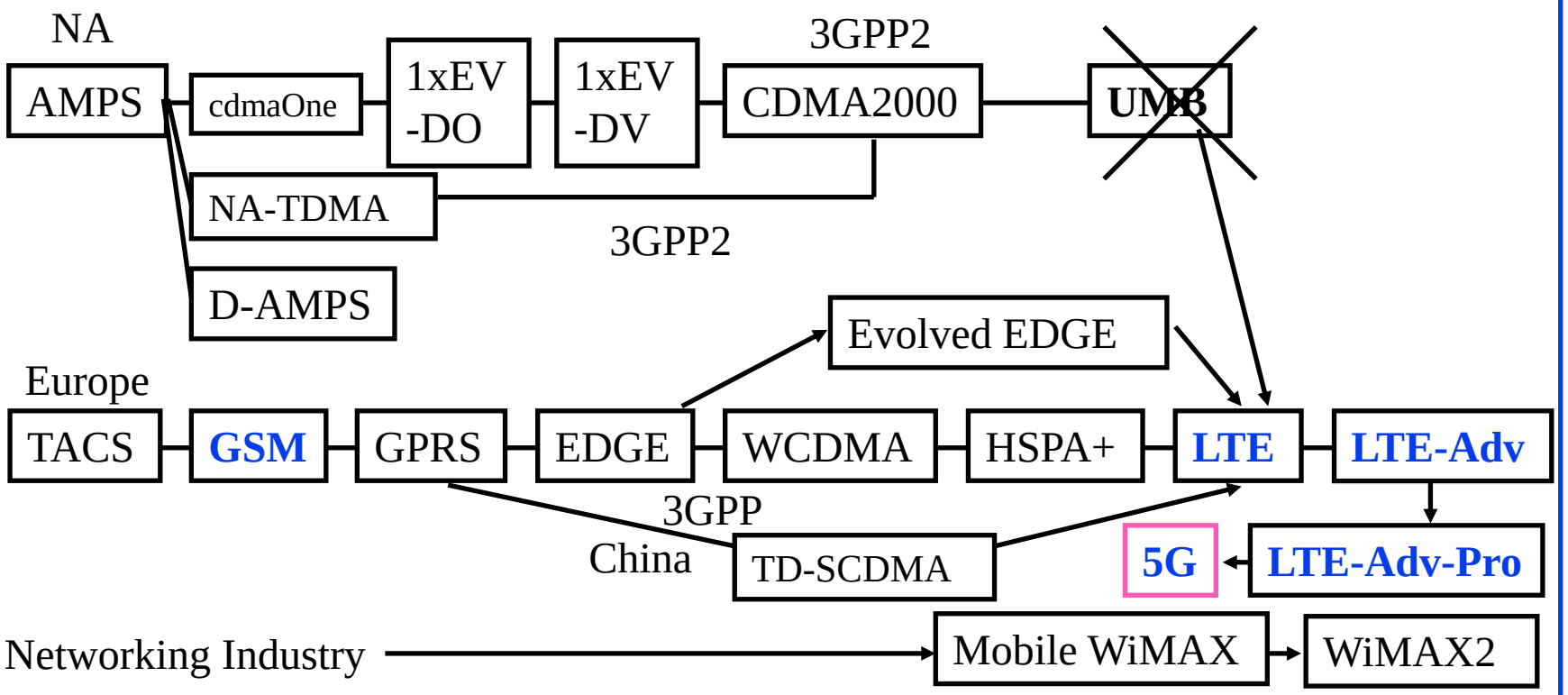
Student Questions

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

Yes. They divide the area into cells.

©2025 Raj Jain

Cellular Telephony Generations

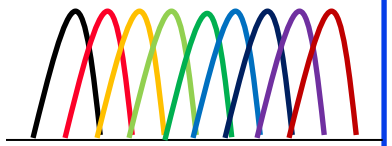


Student Questions

- ❑ Could you briefly explain what OFDMA is?

Orthogonal Frequency Division Multiplexing

Many 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, translate them back to the waveform signal.

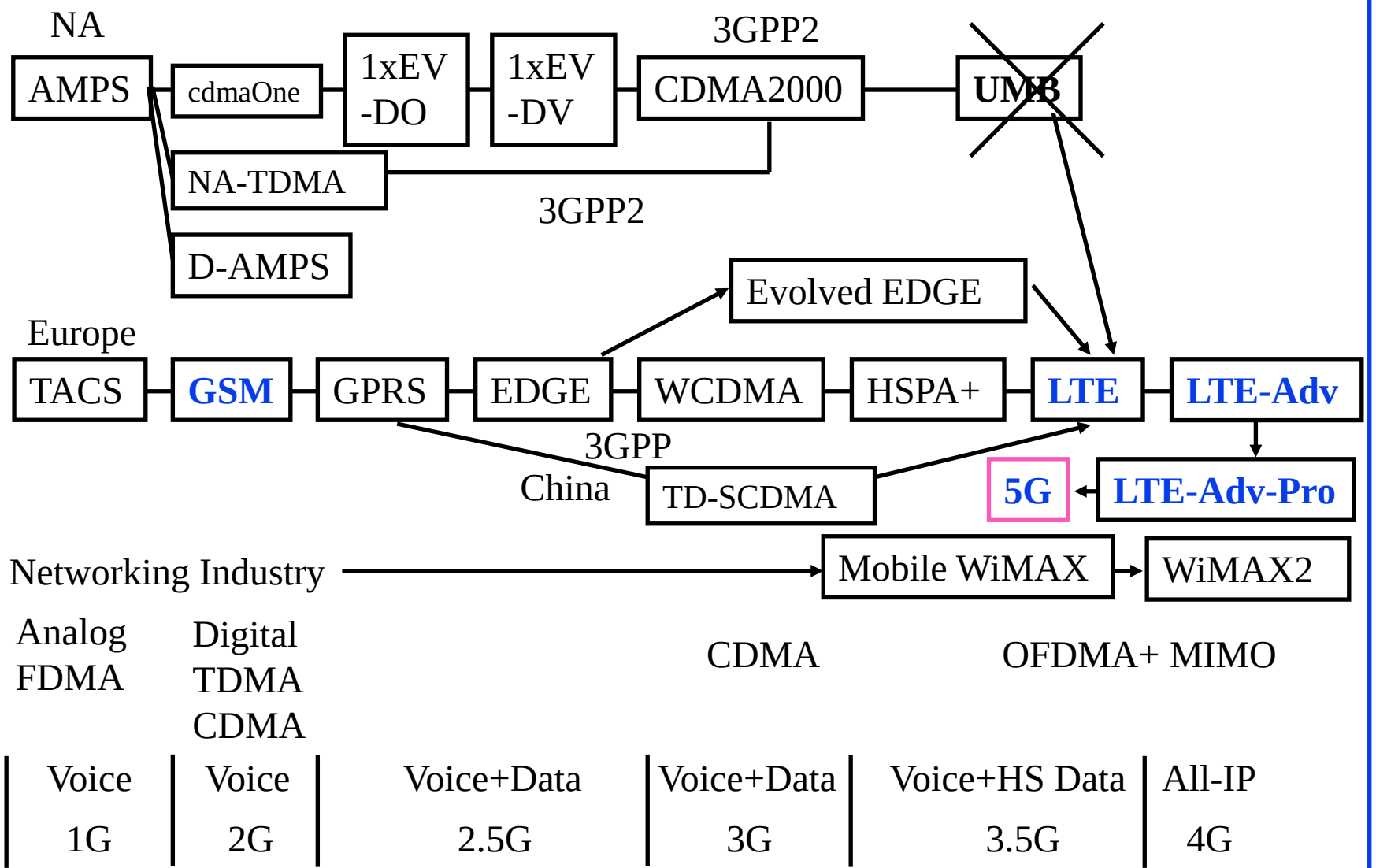
The signal travels at the same speed regardless of whether it is analog or digital. If you mean analog is "less complex," then yes, analog is less complex, but it loses much more information faster.

- ❑ What is TD-SCDMA? Does China only use it?

Yes.

©2025 Raj Jain

Cellular Telephony Generations



Student Questions

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

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

- Is there any loss during the processes that transfer analog to digital and then transfer digital back to analog?

Yes. There are quantization errors. But they are imperceptible to ears.

- Apart from 5G, are there any other changes to the graph?

Evolution will continue.

- Why do we pick CDMA or GSM over another? *Cost-performance tradeoffs.*
- Do we need to know everything from the graph above?

At least the bold-blue terms.

- What does the All-IP over 4G mean?

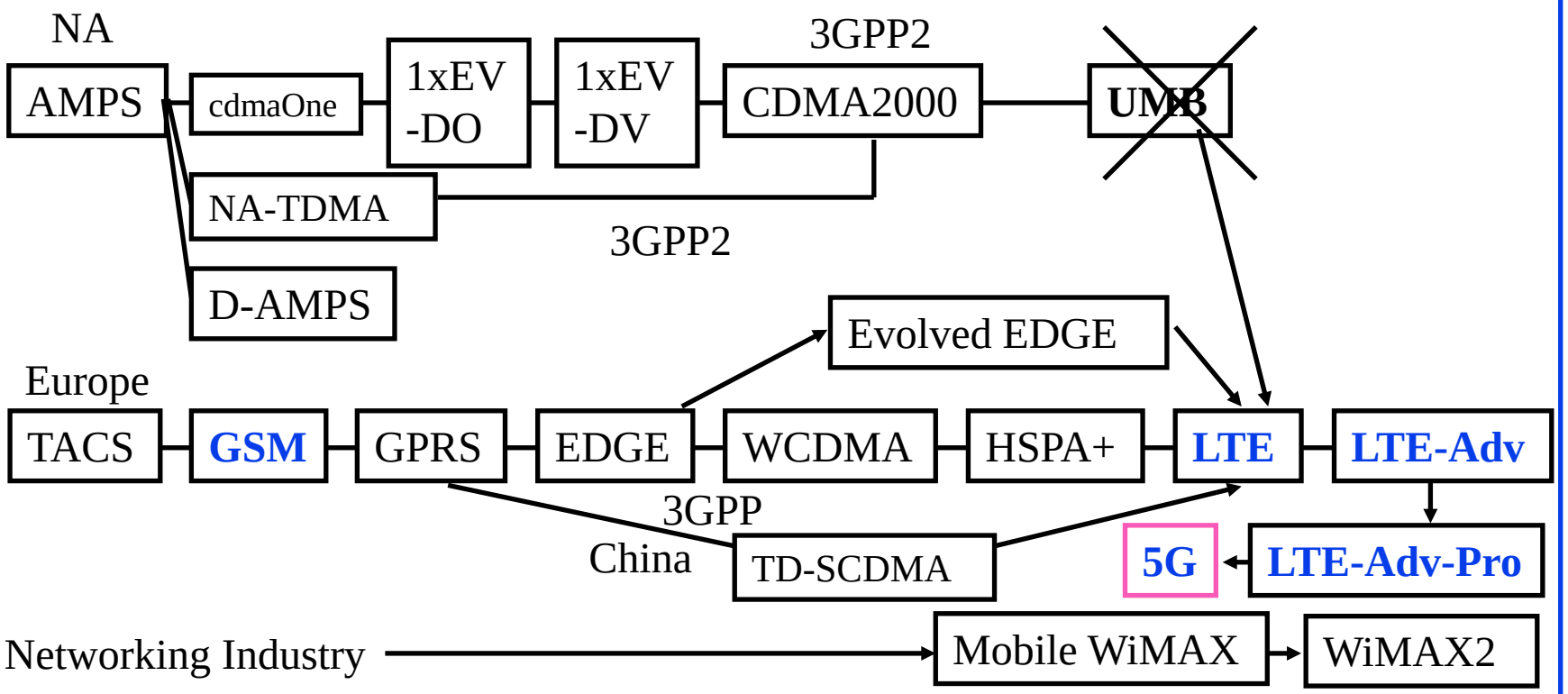
Previous protocols did not use IP.

- LTE has a speed different than 4G. Why do we still have it today?

Some towers still use LTE.

©2025 Raj Jain

Cellular Telephony Generations



Analog FDMA | **Digital TDMA CDMA** | **CDMA** | **OFDMA+ MIMO**

Voice	Voice	Voice+Data	Voice+Data	Voice+HS Data	All-IP
1G	2G	2.5G	3G	3.5G	4G/5G

Student Questions

- Could you make the bottom row with "Voice 1G, Voice 2G," etc., bold and blue so that it's more apparent that we need to know them?

Done.

- HS data=high speed data? *Yes*
- How is WiMAX different from Wi-Fi?

WiMAX is designed for long distances for carriers using licensed spectrum, while Wi-Fi is designed for short distances.

- Can you go over it?

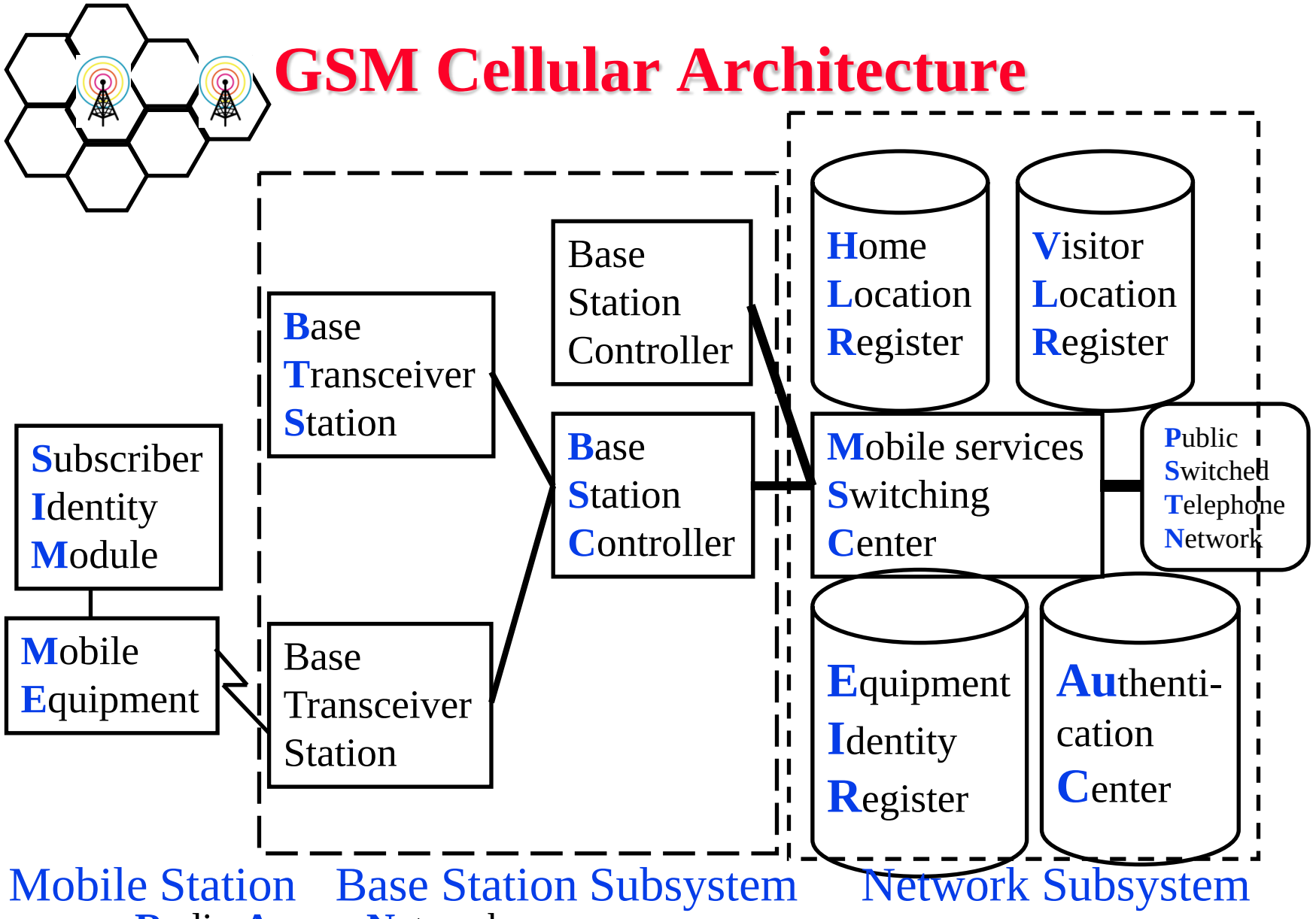
Over what?

- What does all-IP mean?

Carriers are not using legacy carrier protocols like SONET.

©2025 Raj Jain

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, they have increasingly started sharing using SDN or other virtualization techniques.

- ❑ So, does whatever device has my SIM card gain 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 iPads. This is against the original intent of SIM.

- ❑ Does the base station have control over the network?

They handle the wireless part of the network.

- ❑ Which part does RAN include?

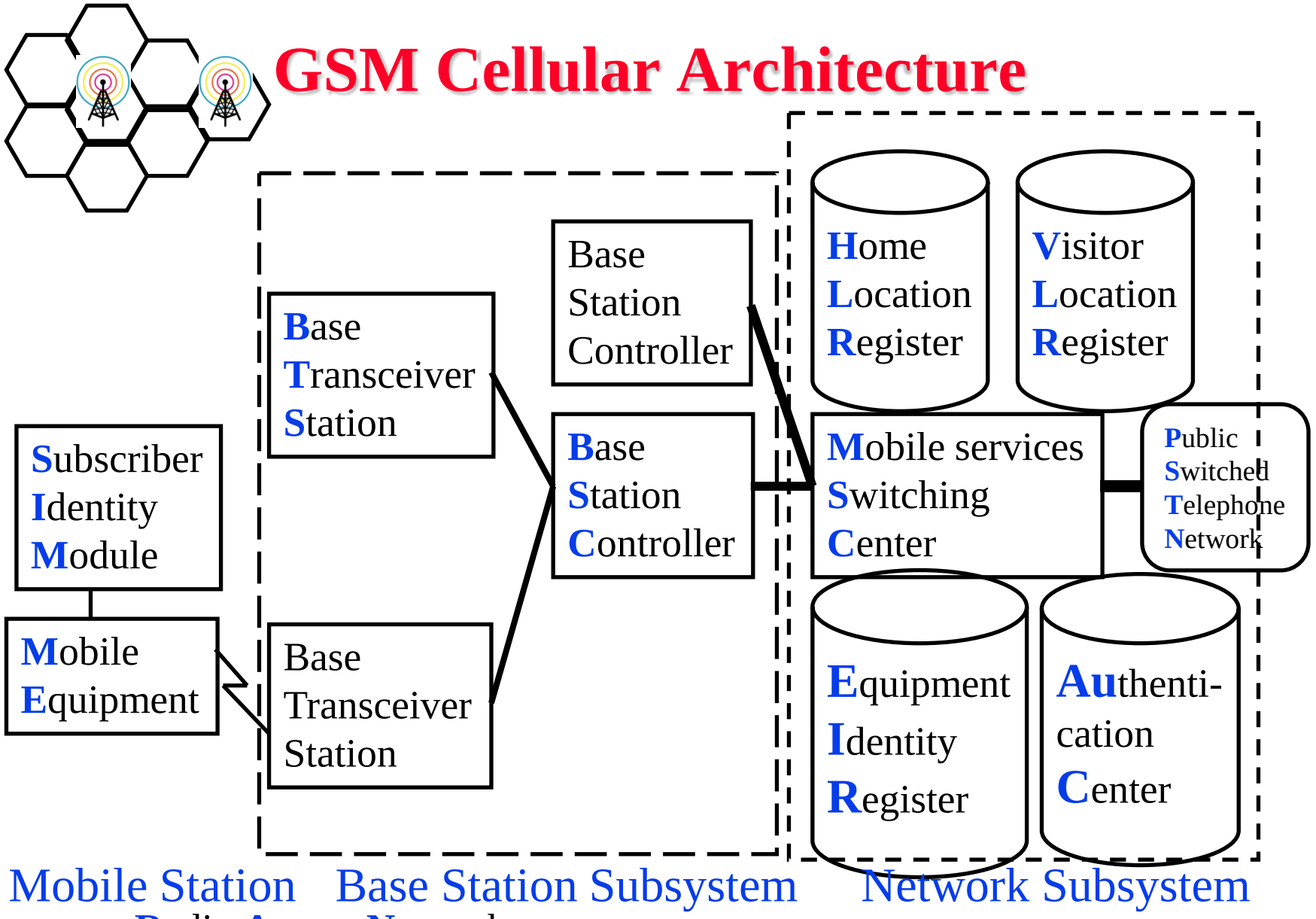
Mobile Station and Base Station Subsystem.

- ❖ Everything we learned from Slides 7-40 to 42 are for 2G to 2.5G?

Yes.

©2025 Raj Jain

GSM Cellular Architecture



Student Questions

- Does RAN manage interference between neighboring base stations, or does BSC do that?

Mobiles send the interference measurement, and BSC/MSC makes a decision.

- Can you go over it again?

Sure.

- Can you explain the physical devices represented by each of the units in the GSM architecture?

Each box is a physical device. SIM is inside the ME, but it is also physical. It can be bought separately.

- UE is user equipment, but what is MS for GSM? Is it another name for the same thing, a physical mobile device?

Yes. MS=ME+SIM

©2025 Raj Jain

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, and 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 the total bits sent.

- Would a dual-SIM cell phone have more than one BTS?

BTS is in the carrier network, not in the phones. SIM only has authentication information. Dual SIM allows info about two carriers.

- Is "Cell" referring to a single unit of the architecture or one cell phone?

The cell is the area served by a single BS.

- What does it mean that BSC controls handset power levels?

The base station tells the mobile to increase or decrease its power.

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) lists all valid mobiles.
- Authentication Center (AuC) stores the secret keys of all SIM cards.
- Each handset has an International Mobile Equipment Identity (IMEI) number.

Student Questions

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

LTE is 3.9G. Each Generation uses a different "Radio Access Networks" (RAN) technique. 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.

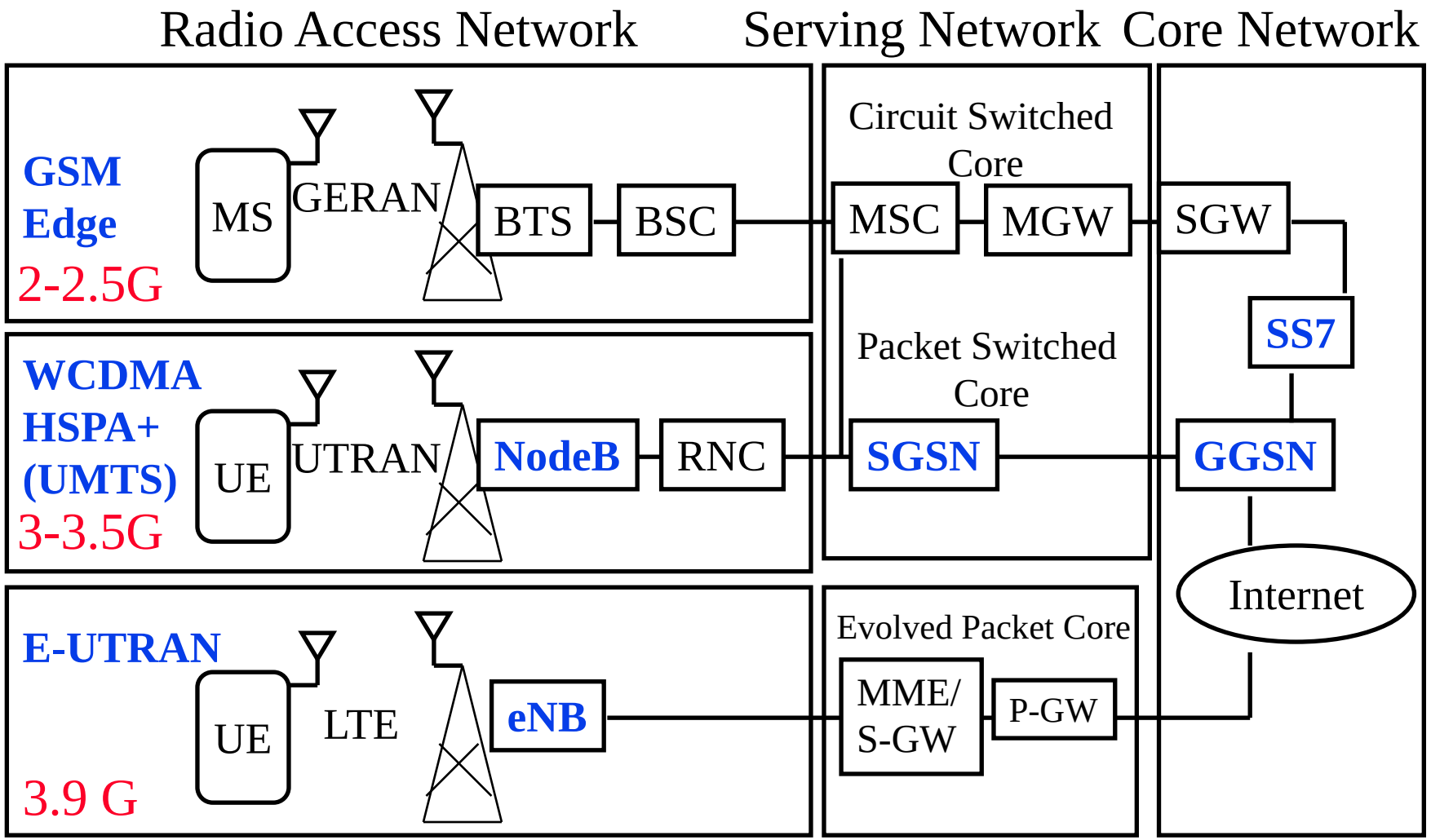
- Do phones have MAC addresses at all?

Phones with Wi-Fi have standard Wi-Fi hardware with MAC addresses.

- What is a handset?

Phone

Evolved Packet System (EPS)



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

- ❑ Is nodeB similar to BTS while RNC is similar to BSC?

Yes.

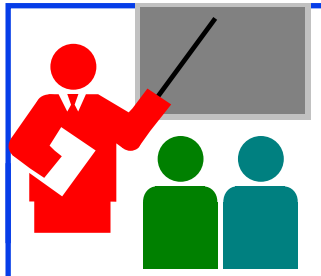
- ❑ Can you go over it again?

Sure.

- ❑ What changes were introduced with LTE's one-stop eNB towers?

Discussed in Part 3.

©2025 Raj Jain



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. ThreeG replaced RAN with UTRAN and BTS with NodeB. 4G uses eNB.

Student Questions

©2025 Raj Jain



Mobility Management

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

Student Questions

©2025 Raj Jain

Mobility: Mr. Smith Goes to Washington



Mr. Smith's office

Can I speak to Mr. Smith

Hello Senator Taylor

Jim Taylor



Can you connect me to Mr. Smith?

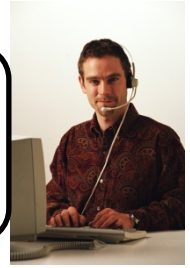
Mr. Smith! Call from Taylor

Hello Senator Taylor

Mr. Smith



Hotel Operator

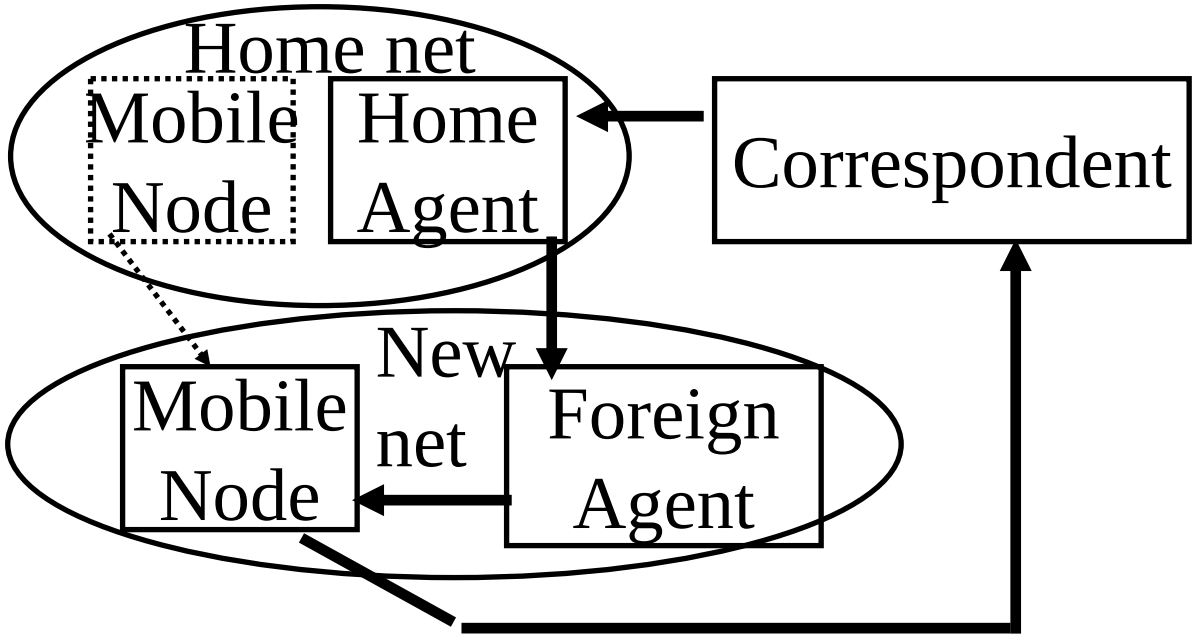


- We need:
  - An agent at a home office: Home Agent
  - An agent at a foreign office: Foreign Agent

Student Questions

©2025 Raj Jain

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.

- When you recorded the video, you mentioned that Mobile IP wasn't in use. Is anyone using Mobile IP as of now? Why?

I need to be made aware of its use.

- Why is IPv6 preferred over mobile IP?

IPv6 and Mobile IP do different things. They are not comparable.

- How do you pinpoint a user's location on his mobile phone?

Towers measure the direction and strength of the signal using multiple antennas.

- Does home/foreign agent topology provide services other than roaming and multiplexing?

They can. But not standardized.

©2025 Raj Jain

Mechanism (Cont.)

- Mobile node finds foreign agents via solicitation or advertising
- Mobile registers with the foreign agents and informs the home agent
- The home agent intercepts the 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. It 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.

- What does solicitation work?

Solicitation=Probing by the mobile

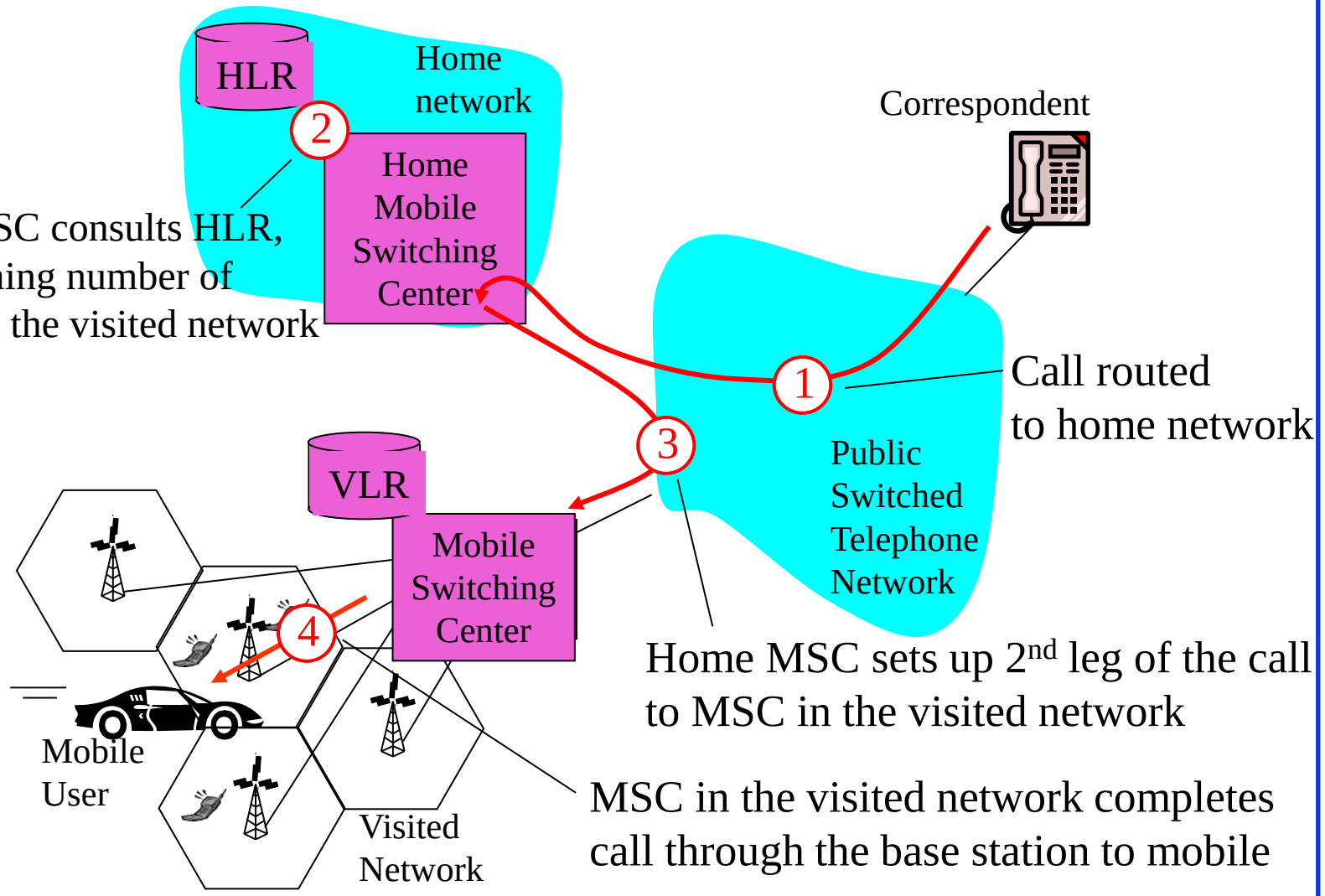
- If COA might not be the foreign agent, where is the tunnel's end?

The tunnel will end at the mobile.

- In what case would the COA not be the foreign agent?

©2025 Raj Jain

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.

- What is the relation between the systems/databases in the cylinders (HLR, EIR, etc) and the systems in boxes (MSC, PSTN)?

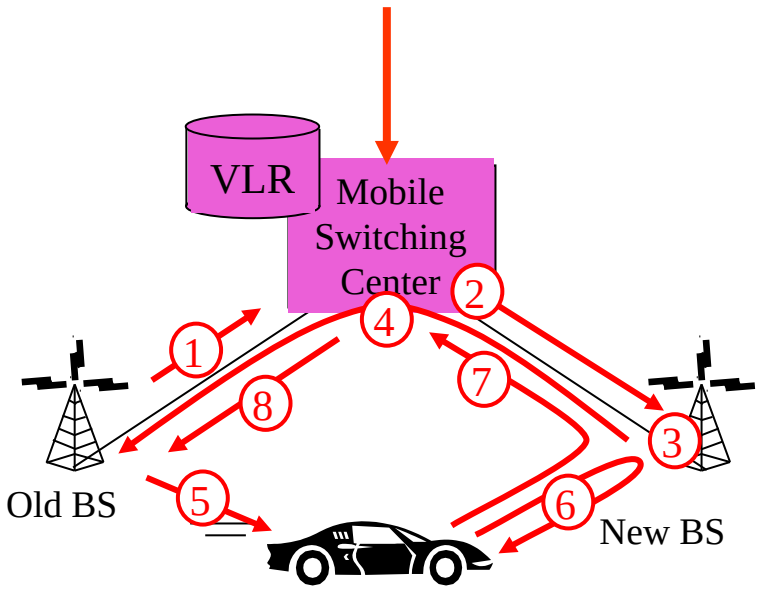
HLR is a database of all users in this area code. VLR is the database of all visitors to this area code. MSC is a system that keeps track of towers a mobile connects to or moves to. PSTN is the network.

- Are the systems aspects of MSC and PSTN, or just one of the two, or are they external systems that support them?

Sorry. The question needs to be clarified.

©2025 Raj Jain

GSM: Handoff with Common MSC



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

8 MSC-old-BS resources released

Student Questions

- How does an MSC determine the direction of a mobile UE and which BSS to hand off to? Isn't that a measure of magnitude and not a vector if it is by signal strength?

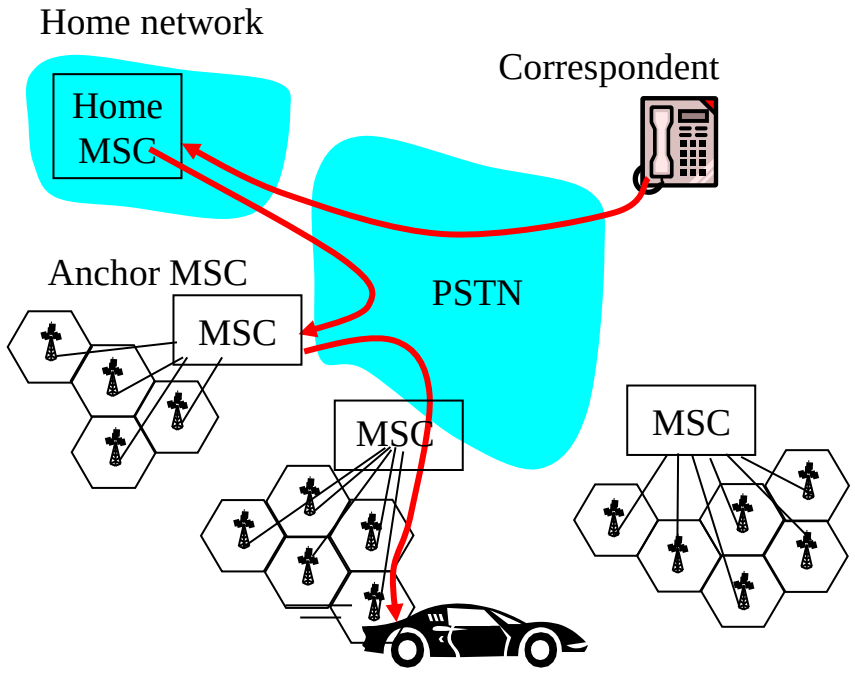
MSC asks the mobile to measure the strength of signals received from various BSs.

- How often does your phone update your location to know where you are visiting?

Every few milliseconds.

©2025 Raj Jain

GSM: Handoff between MSCs



- *Anchor MSC:* first MSC visited during a 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 the multi-MSC chain

Student Questions

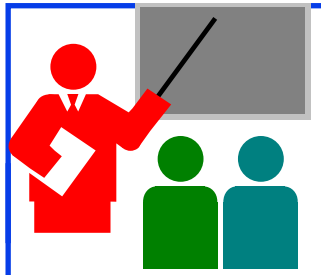
- What is the minimization step that the IS-41 provides to shorten the Multi MSC chain?

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.

- In mobile ~~IP~~ GSM, can the anchor MSC be changed to make routing more efficient? *Not in this early standard.*
- What will happen if the user moves to the anchor MSC again after traveling a lot and has many MSCs in the chain?

The chaining is not optimized in the original 2G. Later versions optimize as indicated.

©2025 Raj Jain



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.

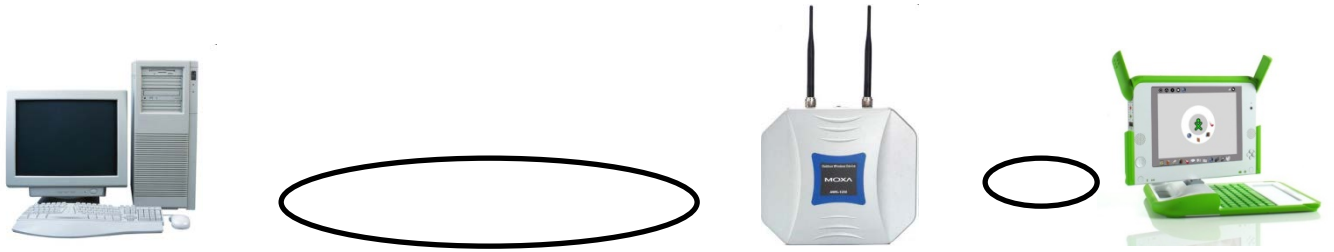
Student Questions

Ref: Sections 7.6 and 7.7, Review Exercises R18-R20

©2025 Raj Jain

Impact on Higher Layer Protocols

- Layered Architecture ⇒ Upper layers are independent of lower layers
- Wireless ⇒ High error rate ⇒ Frequent packet losses
  ⇒ 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

- Can wireless-aware TCP work on a different medium, or is the protocol a multi-layer protocol that only works with wireless?

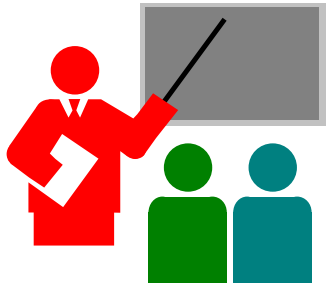
Wireless-aware TCP is more complex, but it can work on other media.

- Textbook page 625: How can the TCP sender and receiver become aware that they are transmitting over a wireless link?

One method is to notice the high probability of random losses. The other is to do cross-layer communication, i.e., Layer 4 is told what Layer 2 is running on. The layered structure is broken.

©2025 Raj Jain

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 as popular as OFDMA?

OFDMA is the latest.

- ❑ What is the range of frequency hopping? Will it be within microwave bandwidth of around 2.4GHz?

Yes, the entire 2.4 GHz band is used for frequency hopping.

- ❑ If I 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.

End of Part 2



4G/5G

1. LTE architecture and protocol stack
2. Media Access Method used in 4G/5G
3. Mobile-Base station communications and handover
4. 5G performance requirements

Student Questions

©2025 Raj Jain

LTE vs. 4G

Long-**T**erm **E**volution. 3GPP Release 8, 2009.

1. **LTE is 3.9G** (Pre-4G) cellular technology
   Sold as 4G by some providers (and by our textbook authors)

- **4G** = International Mobile Telecommunication (IMT) Advanced. Requirements in ITU M.2134-2008
- IP-based packet switch network
- 1.0 Gbps peak rate for fixed services with 100 MHz
- 100 Mbps for mobile services. High mobility to 500 km/hr

Feature	Cell	Cell Edge	Peak
DL Spectral Efficiency (bps/Hz)	2.2	0.06	15
UL Spectral Efficiency (bps/Hz)	1.4	0.03	6.75

- Seamless connectivity and global roaming with smooth handovers
- ITU has approved **LTE-Advanced** as 4G (Oct 2010)

Student Questions

- How much faster is 4G over LTE?

Speed is not the only requirement.

- Is this slide about LTE or 4G, or what LTE and 4G share in common? Or is it specifically about LTE, or specifically 4G?

The numbers are for 4G. LTE needs to satisfy these.

- What makes the handovers smooth? How are they smoother than regular Wi-Fi?

*We are talking about **inter-carrier** or **global** roaming. Wi-Fi cannot not handle this.*

- Is LTE Advanced the same as 4G? *Yes*

©2025 Raj Jain

LTE vs. 4G

Long-**T**erm **E**volution. 3GPP Release 8, 2009.

1. **LTE is 3.9G** (Pre-4G) cellular technology
   Sold as 4G by some providers (and by our textbook authors)

- **4G** = International Mobile Telecommunication (IMT) Advanced. Requirements in ITU M.2134-2008
- IP-based packet switch network
- 1.0 Gbps peak rate for fixed services with 100 MHz
- 100 Mbps for mobile services. High mobility to 500 km/hr

Feature	Cell	Cell Edge	Peak
DL Spectral Efficiency (bps/Hz)	2.2	0.06	15
UL Spectral Efficiency (bps/Hz)	1.4	0.03	6.75

- Seamless connectivity and global roaming with smooth handovers
- ITU has approved **LTE-Advanced** as 4G (Oct 2010)

Student Questions

- What does "spectral efficiency" mean?

You can send how many bits/sec given 1 Hz of spectrum. It is measured in bps/Hz.

- What does the number in the column cell and cell edge represent? Is it the area capacity? If so, in what unit?

bps/Hz

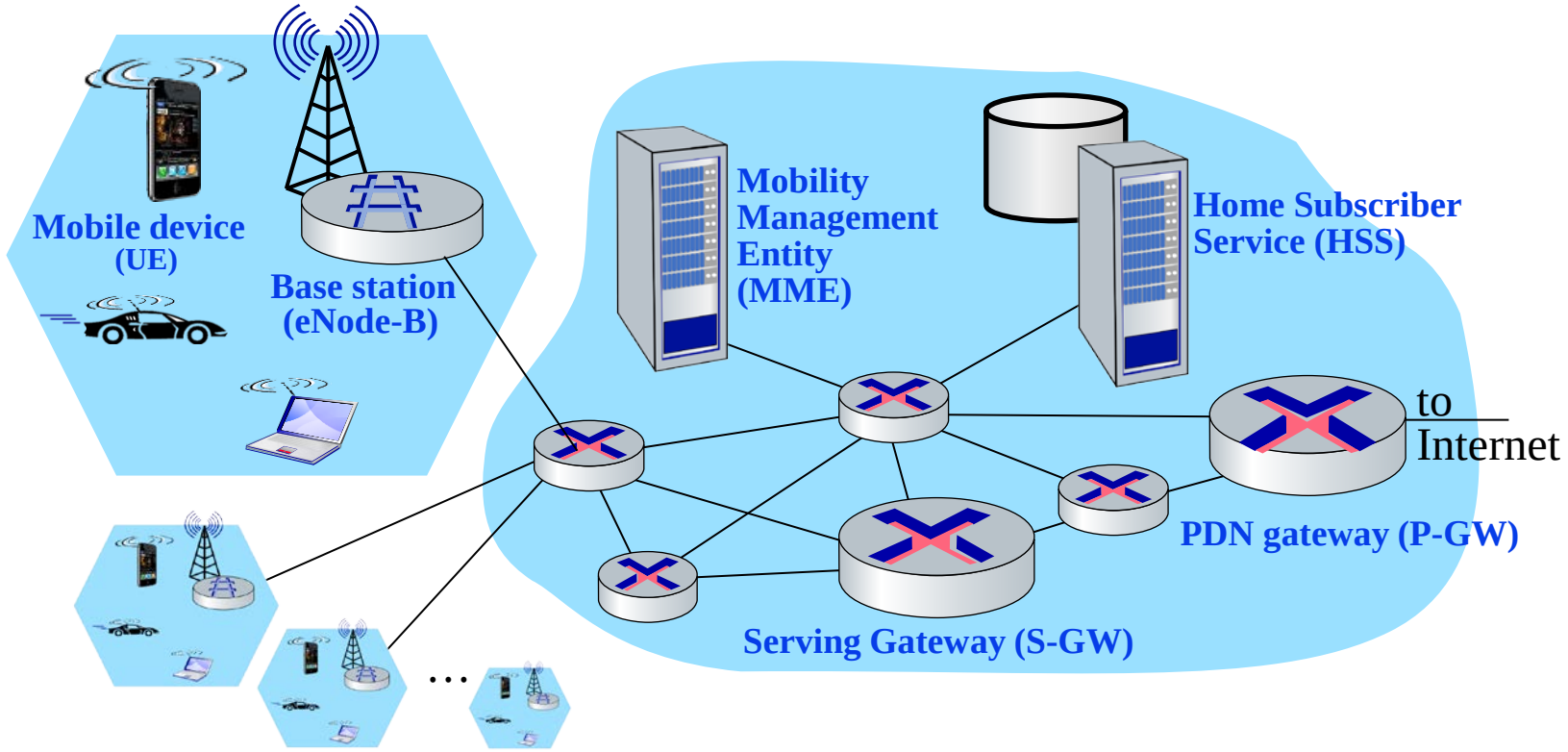
- Could you please explicitly define the difference between 4G and LTE?

LTE is 3GPP Release 8, 2009. It does not meet these 4G requirements.

©2025 Raj Jain

LTE Architecture

- Evolved Packet Systems (EPS)



Student Questions

- What/when is the process for re-connecting or re-attaching to a different base tower? Will this continuously happen as you move around?

Yes.

- The book said MME controls UEs, but somehow, HSS and P-GW also have some authentication and mobility work. Could you explain their differences?

MME moves UE from one tower to another
HSS has all the authentication and authorization data
P-GW is the router to the rest of the carrier network

- What's the difference in the role of the serving gateway (S-GW) versus the PDN gateway (P-GW)?

S-GW routes only LTE traffic, while P-GW sends traffic to external networks of other packet technologies.

- What happen to the data if a mobile device moving across different eNode-B cells?

Handovers are seamless. You do not notice the switch over.

©2025 Raj Jain

Evolved Packet System

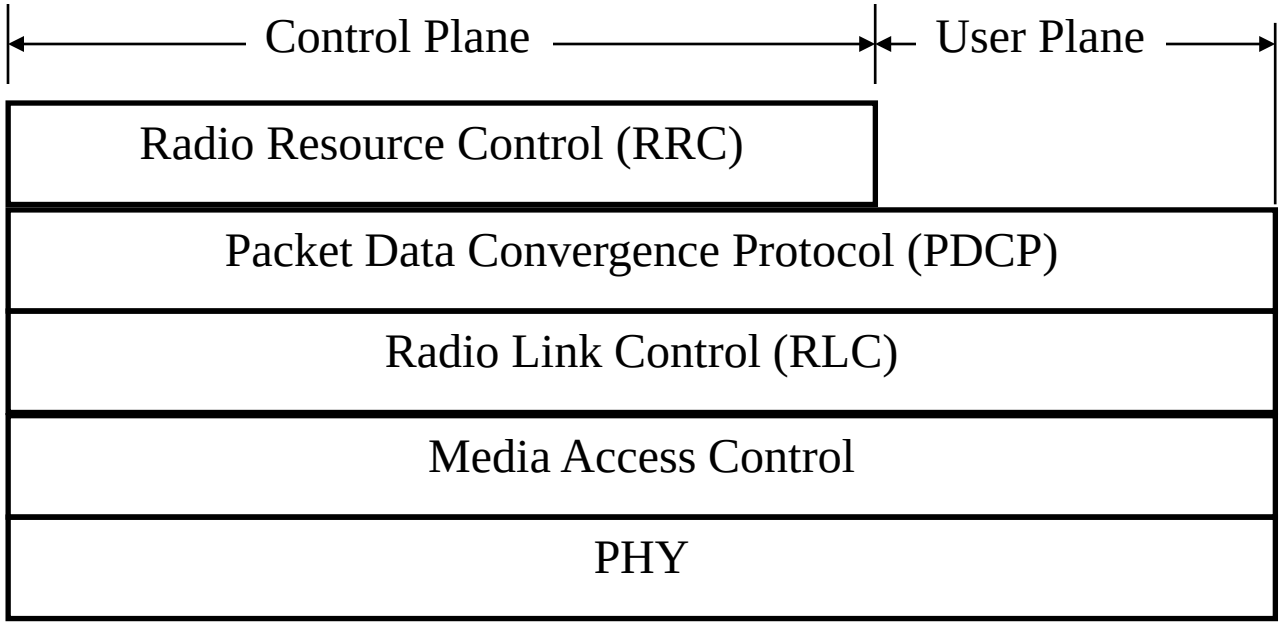
- **User Equipment (UE):** Mobile device, phone, sensors, …
- **Enhanced Node B (eNodeB):** Base Station. Similar to Wi-Fi AP. Coordinates with nearby base stations to optimize radio
- **Serving Gateway**: Demarcation point between RAN and Core. Serves as mobility anchor when terminals move
- **Packet Data Network Gateway (PGW)**: Termination of EPC towards Internet or IMS network. IP services, address allocation, deep packet inspection, policy enforcement
- **Mobility Management Entity (MME)**: Location tracking, paging, roaming, and handovers. All control plane functions related to subscriber and session management.
- **Policy and Charging Rules Function (PCRF)**: Manages QoS (not shown)

Student Questions

- What topology does the EPS use? Are loops possible?

EPS uses mesh topology like the Internet. Yes, loops are possible but are avoided by routing methods.

LTE Protocol Stack



- **Radio Resource Control (RRC):** Control plane functions of Paging, Connection, Disconnection, Mobility Management, QoS Management

Student Questions

- Only RRC is solely control plane? Are the others both control plane and data plane?

Yes.

©2025 Raj Jain

Packet Data Convergence Protocol (PDCP)

1. **Header compression** using IETF Robust Header Compression (ROHC)
2. **Integrity** Protection of control plane data using Message Authentication Code (MAC)
3. **Ciphering** (Encryption)
4. **In-sequence delivery** and duplicated elimination

Student Questions

- What is header compression?

Compression is using fewer bits than the data, e.g.,
1E12 = 1,000,000,000,000
Four characters vs 13.

- Is PDCP connectionless like UDP? Is it reliable?

Most communication in carrier networks is connection-oriented. PDCP provides integrity, in-sequence delivery, and duplicate elimination.

Radio Link Control Layer

1. Segmentation and Reassembly
2. Aggregation (Concatenation)
3. Re-order out-of-order PDUs, ARQ.

Student Questions

- Is segmentation the same as fragmentation?

Yes.

©2025 Raj Jain

Media Access Control (MAC)

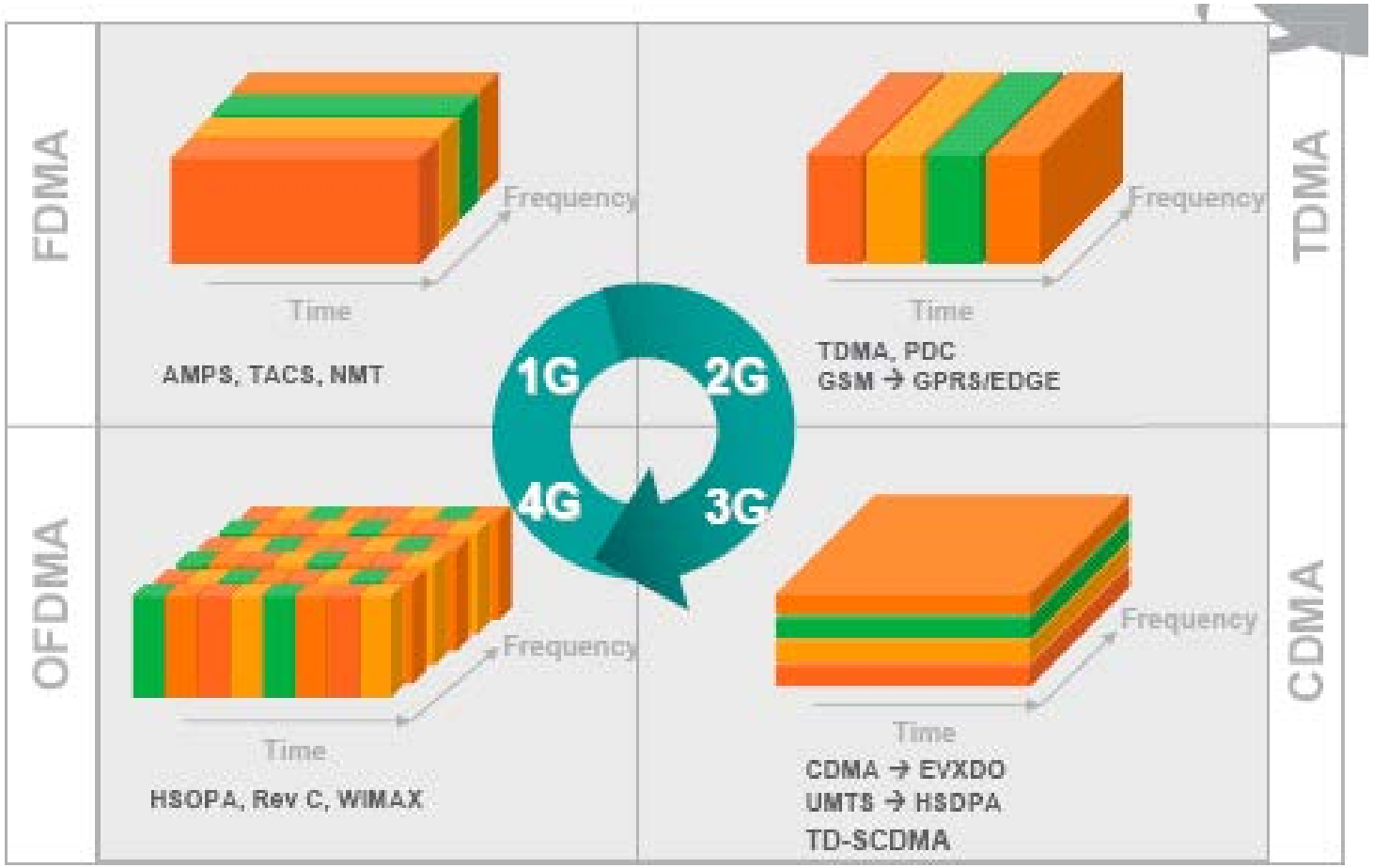
1. Multiplexing of various control and transport channels
2. Transmission scheduling
3. Error control (retransmissions)

Student Questions

- When my phone is connected through Wi-Fi and Cellular simultaneously, is it pretending to be two devices, one for each method, or is there some way the two different systems work together?

It is two subsystems under the same management.

Multiple Access Methods



Source: Nortel

Student Questions

- ❑ What's the speed difference among these generations?

Generally, a factor of 10.

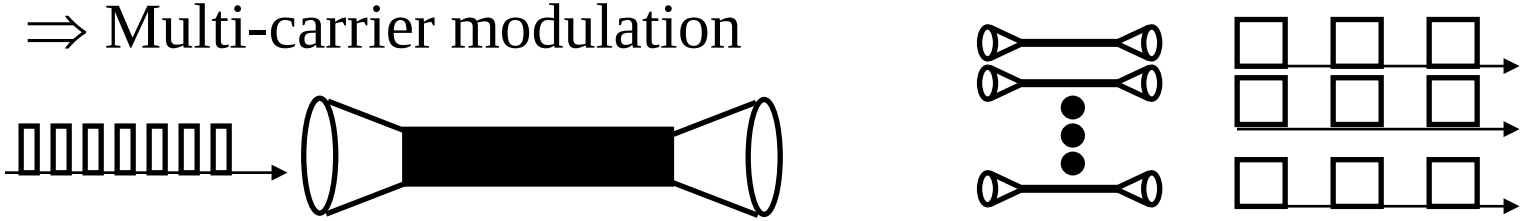
- ❑ Does 5G also do OFDMA?

Yes.

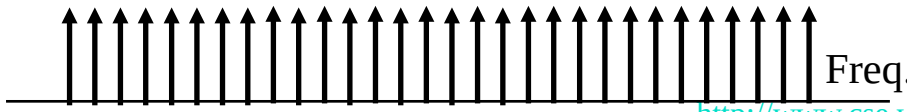
©2025 Raj Jain

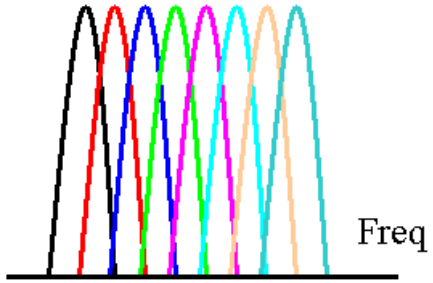
OFDM

- Orthogonal Frequency Division Multiplexing
- Ten 100 kHz channels are better than one 1 MHz Channel
  ⇒ Multi-carrier modulation



- Frequency band is divided into 256 or more sub-bands.
  Orthogonal ⇒ Peak of one at the null of others
- Each carrier is modulated with a BPSK, QPSK, 16-QAM, 64-QAM, etc., depending on the noise (Frequency selective fading)
- Used in 802.11a/g, 802.16,
  Digital Video Broadcast handheld (DVB-H)
- Easy to implement using FFT/IFFT





Student Questions

- What is multi-carrier modulation?

Multicarrier = multiple frequency signals.

- What is the input to FFT, and what is the output of it?

FFT: Time domain to Frequency domain
IFFT: Frequency domain to time domain

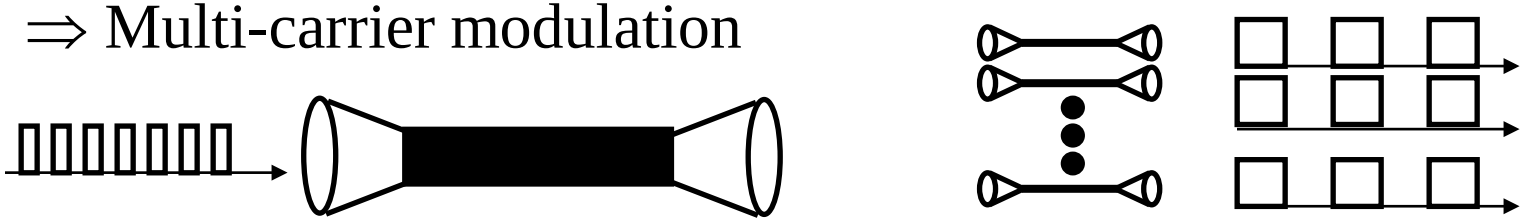
- What is FFT and IFFT? *Fast Fourier Transform and Inverse Fast Fourier Transform*
- Exactly how does Frequency selective fading choose based on the noise?

Noise is measured separately for each frequency. Lower bits per Herts are sent if noise is high.

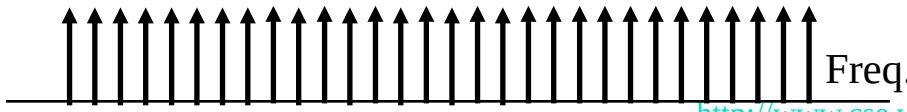
©2025 Raj Jain

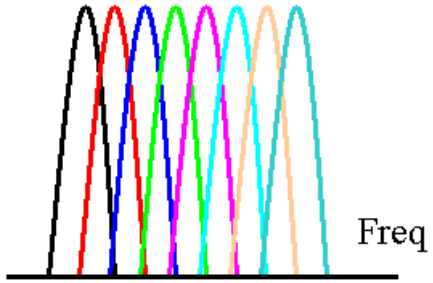
OFDM

- Orthogonal Frequency Division Multiplexing
- Ten 100 kHz channels are better than one 1 MHz Channel
  ⇒ Multi-carrier modulation



- Frequency band is divided into 256 or more sub-bands.
  Orthogonal ⇒ Peak of one at the null of others
- Each carrier is modulated with a BPSK, QPSK, 16-QAM, 64-QAM, etc., depending on the noise (Frequency selective fading)
- Used in 802.11a/g, 802.16,
  Digital Video Broadcast handheld (DVB-H)
- Easy to implement using FFT/IFFT





Student Questions

- Can you explain how a frequency band can be orthogonal to another? From a linear algebra perspective, it would be helpful.

Each signal can be represented as a series of harmonics:
$S(t)= a_0 + a_1 \sin(\omega t) + a_2 \sin(2\omega t) + \ldots$
This can be represented as a vector using FFT. As in linear algebra, the inner product of FFT vectors representing two signals is zero.

- To confirm, OFDM uses a combination of TDMA + FDMA + orthogonal bands?

Yes.

©2025 Raj Jain

Advantages of OFDM

- Easy to implement using FFT/IFFT.
  FFT/IFFT are implemented only as powers of 2 (256, 1024, …)
- Graceful degradation if an excess delay
- Robustness against frequency selective burst errors
- Allows adaptive modulation and coding of subcarriers
- Robust against narrowband interference (affecting only some subcarriers)
- Allows pilot subcarriers for channel estimation



Student Questions

- Why does OFDM have graceful degradation? *Because there are multiple carriers. Not all carriers get damaged or equally damaged.*
- What is Equalization?

Frequency-specific amplification

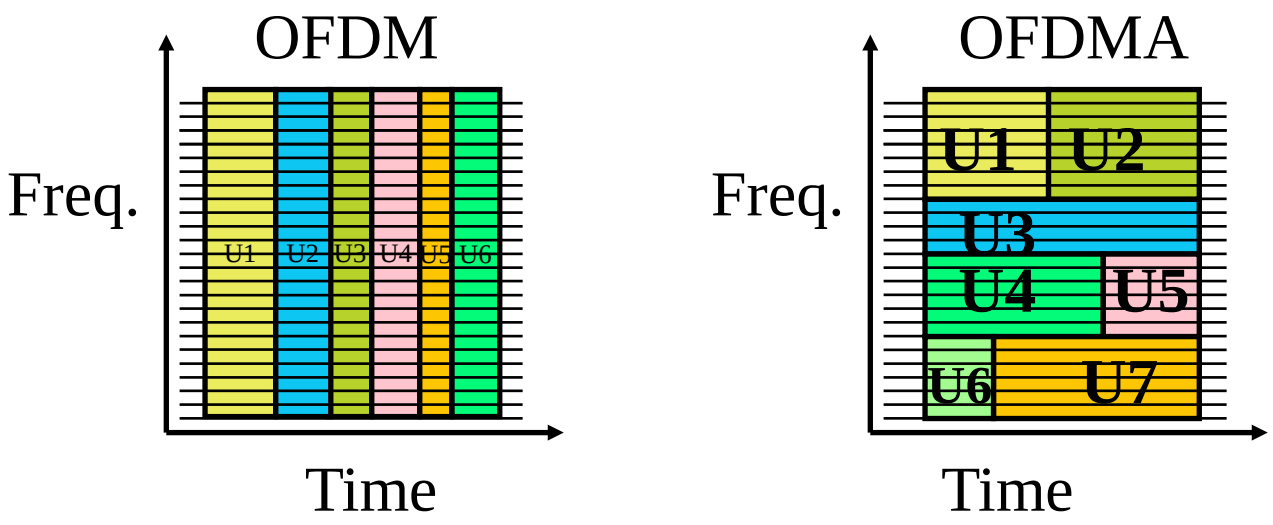
- What do frequency selective burst errors mean? *Errors that affect only some subcarriers and not the entire channel.*
- Is a subcarrier part of a channel, and is a channel part of the frequency band assigned by regulation? *Yes.*
- Would FFT/IFFT be implemented in hardware?

Yes.

©2025 Raj Jain

OFDMA

- Orthogonal Frequency Division Multiple Access
- Each user has a subset of subcarriers for a few slots
- OFDM systems may use TDM using the entire channel
- OFDMA allows Time + Freq DMA ⇒ 2D Scheduling



Student Questions

- What do you mean by 'Each user has a subset of subcarriers for a few slots"?

As shown by colored rectangles in the right diagram.

- How is the mapping decided in OFDMA?

Optimal scheduling is a complex mathematical process. We have some papers on our website about the methods we proposed.

- Is there a particular reason not to use FDMA initially? It seems FDMA is much more natural than TDMA for OFDM.

OFDM is multiplexing. Each user is fixed. It could have been done in FDM.

- Why is OFDM essentially dividing frequencies into subcarriers but said to be TDMA? Why isn't it FDMA?

See above.

- What do you mean by 2D Scheduling?

Using both frequency and time scheduling, as in the diagram on the right. The left diagram shows 1D scheduling.

©2025 Raj Jain

SC-FDMA

- Single-Carrier Frequency Division Multiple Access
- Each user gets a contiguous part of the channel



- Uses single carrier modulation and adds a cyclic prefix
- Single carrier ⇒ Not much variation in amplitude
  ⇒ Lower Peak-to-Average Power Ratio (PAPR)
  ⇒ Lower-cost Amplifiers
- Better for uplink because slight mis-synchronization among users does not affect the decoding significantly
- With OFDMA, each user's subcarriers are spread all over the band and may affect other users' subcarriers all over the band

Student Questions

- What is a cyclic prefix for?

To overcome inter-symbol interference. 1/2/4/8/16… bits coded as one symbol. Symbols become longer in time as they travel, causing interference. So the initial part is a copy of the last part.

Sent: 

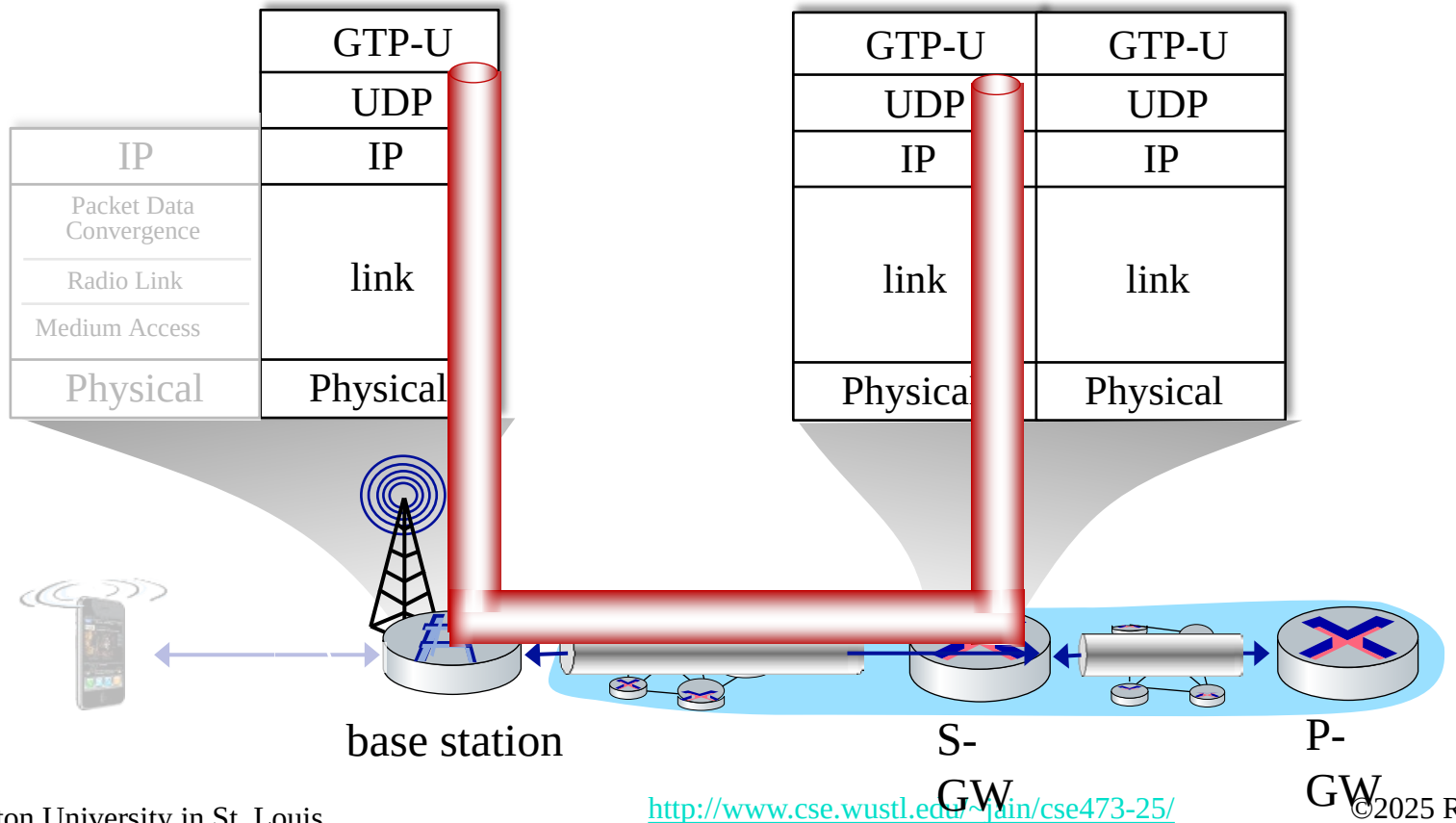
Received: 

Ref: A. Ghosh, J. Zhang, J. G. Andrews, R. Muhamed, "Fundamentals of LTE," Prentice Hall, 2010, ISBN: 0137033117, 464 pp.

©2025 Raj Jain

GPRS Tunneling Protocol (GTP)

- **General Packet Radio Service (GPRS)** transfers data in 2G/3G/4G networks. GTP uses UDP tunneling to transfer data over IP.



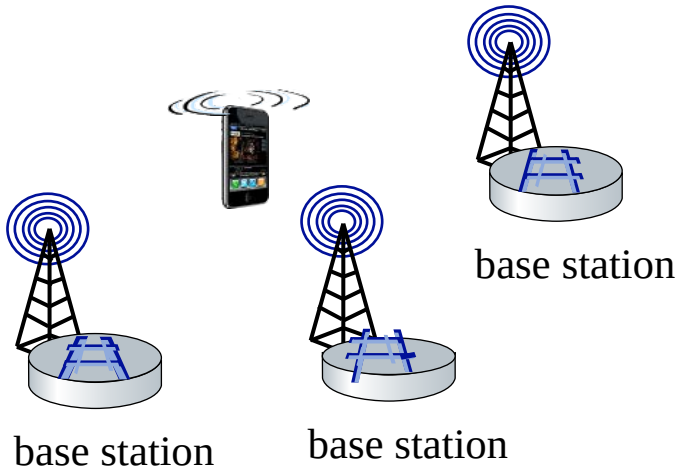
Student Questions

- With GPRS Tunneling Protocol, does that mean even 2G is now packet-based?

GPRS was designed to send packets in 2G. It is classified as 2.5G.

©2025 Raj Jain

UE Association with a BS



- Each BS broadcasts a primary synch signal every 5ms
- Mobile listens to multiple such broadcasts
  Finds channel bandwidth, configuration, carrier info
- Mobile finds a BS from its compatible carrier and associates with it
- BS authenticates the mobile, sets up all components of the control plane and data plane

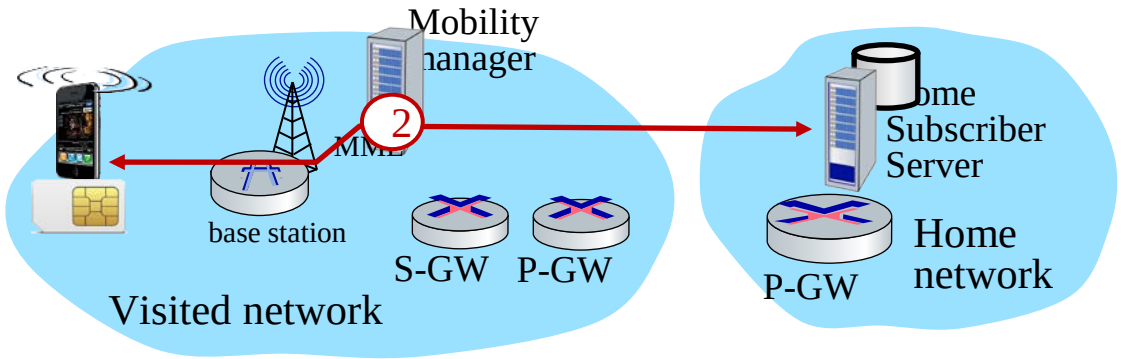
Student Questions

- Why do they broadcast every 5ms?

A shorter interval would be too much overhead. Longer intervals would result in connection and handover delays.

©2025 Raj Jain

Configuring LTE Control-Plane Elements

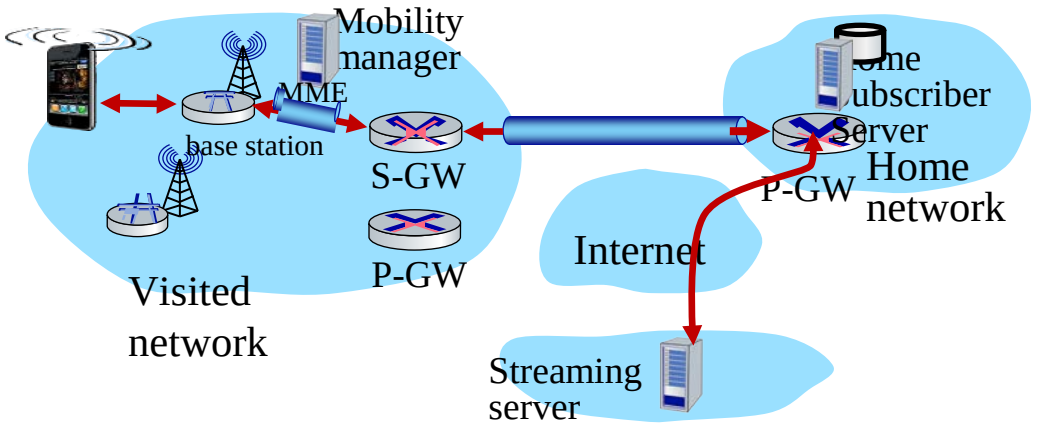


- Mobile communicates with local MME via BS control-plane channel
- MME uses mobile's IMSI info to contact mobile's home HSS
  - Retrieve authentication, encryption, network service information
  - Home HSS knows mobile now resident in the visited network
- BS, mobile select parameters for BS-mobile data-plane radio channel

Student Questions

Configuring Data-Plane Tunnels for Mobile

- S-GW to BS Tunnel: when mobile changes base stations, change the endpoint IP address of the tunnel
- S-GW to Home P-GW Tunnel: implementation of indirect routing
- Tunneling via GTP (GPRS tunneling protocol): mobile's datagram to streaming server encapsulated using GTP inside UDP, inside a datagram



Student Questions

- The textbook discusses indirect and direct routing and the triangle routing problem. How does direct routing overcome this problem?

Direct routing results in triangular routing.
Direct routing removes the triangle.

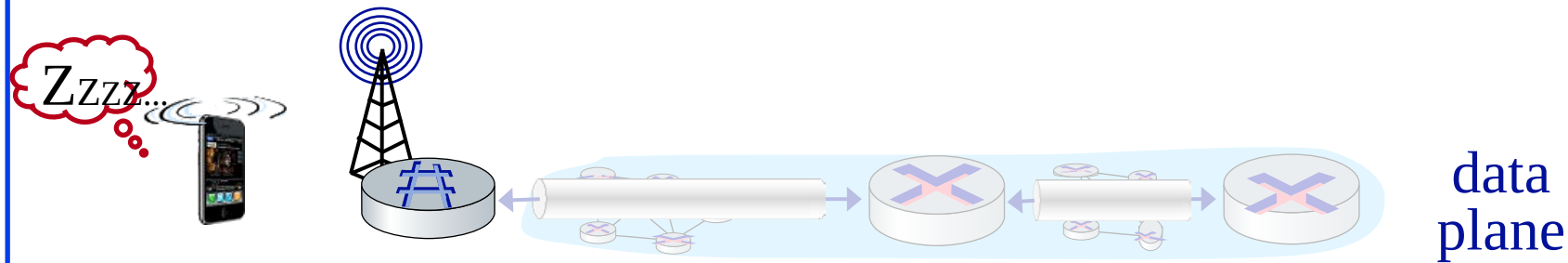


- What is the most effective solution for the triangle routing problem?

Direct routing

©2025 Raj Jain

LTE Mobile Sleep Modes



- LTE mobiles put the radio to sleep to conserve battery
- Light Sleep: Wake up periodically (100 ms). Check downstream transmissions to see if there are any calls.
- Deep Sleep: 5-10s of inactivity. It may be found that the BS has changed. Will re-establish association with a new BS.

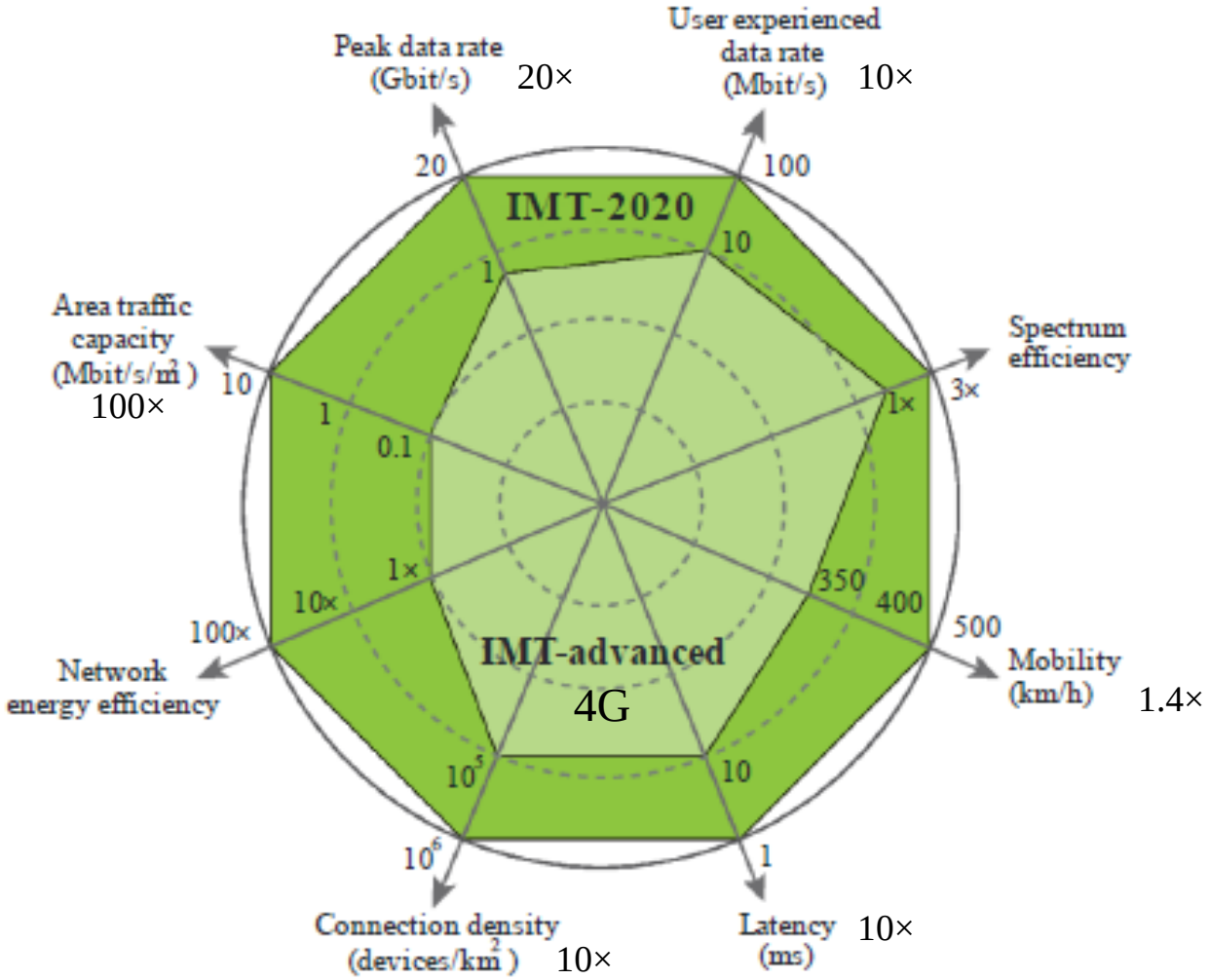
Student Questions

- How does the LTE mobile decide when to enter light sleep and when to enter deep sleep?

Light during conversations.
Deep when the conversation ends.

©2025 Raj Jain

5G Definition



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

©2025 Raj Jain

Student Questions

- How do we decide the area traffic capacity? How is it related to connection density?

Area Traffic=Total traffic at the tower = # of connections × traffic per connection

- Is it always 20x faster for every generation?

No. Set based on available options.

- Can you review the essential changes from 4G to 5G?

This slide talks about requirements. How these are achieved is beyond the scope of this course—discussed in CSE574.

- By latency changing 10x, does that mean lower latency?

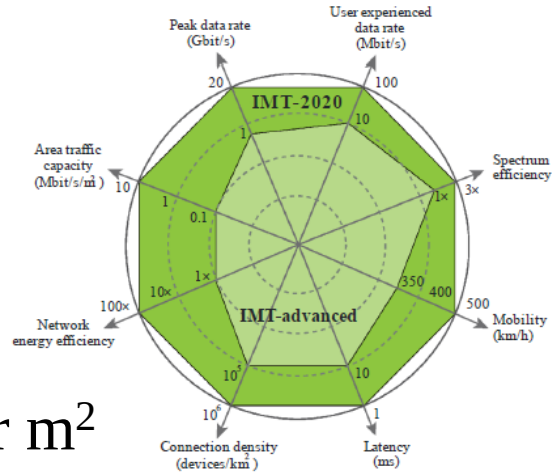
Yes, 10x lower.

- With the transition from LTE to 5G, what are the most critical speed, capacity, or latency improvements?

See this diagram.

5G Definition (Cont)

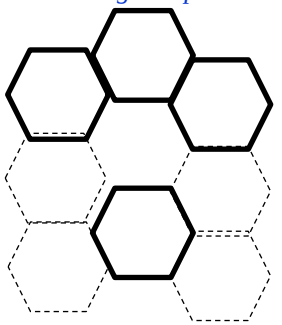
1. **Peak Data Rate**: The max rate per user under ideal conditions is 10 Gbps for mobiles and 20 Gbps under certain conditions.
2. **User experienced Data Rate**: 95% Rate across the coverage area per user. 100 Mbps in urban/suburban areas. 1 Gbps hotspot.
3. **Latency**: Radio contribution to latency between send and receive
4. **Mobility**: Max speed at which seamless handover and QoS is guaranteed
5. **Connection Density**: Devices per 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 m^2



Student Questions

- ❑ What creates a "hotspot"? Why can't there be many spread out?

Hotspots are also arranged in a hexagonal pattern but may not be everywhere.



- ❑ Why do we need both Peak Data Rate and User experienced Data Rate?

User experience excludes overhead.

- ❑ How are hotspots served? Are there more stations or higher power stations in cells with hotspots?

More base stations.

Additional Capabilities for 5G

1. **Spectrum and Bandwidth Flexibility**: Ability to operate at different frequencies and channel bandwidths
2. **Reliability**: High availability
3. **Resilience**: Continue working in the face of disasters
4. **Security and Privacy**: Confidentiality, Integrity, Authentication, Protection against hacking, denial of service, man-in-the-middle attacks
5. **Operational Lifetime**: Long battery life

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

©2025 Raj Jain

5G Applications

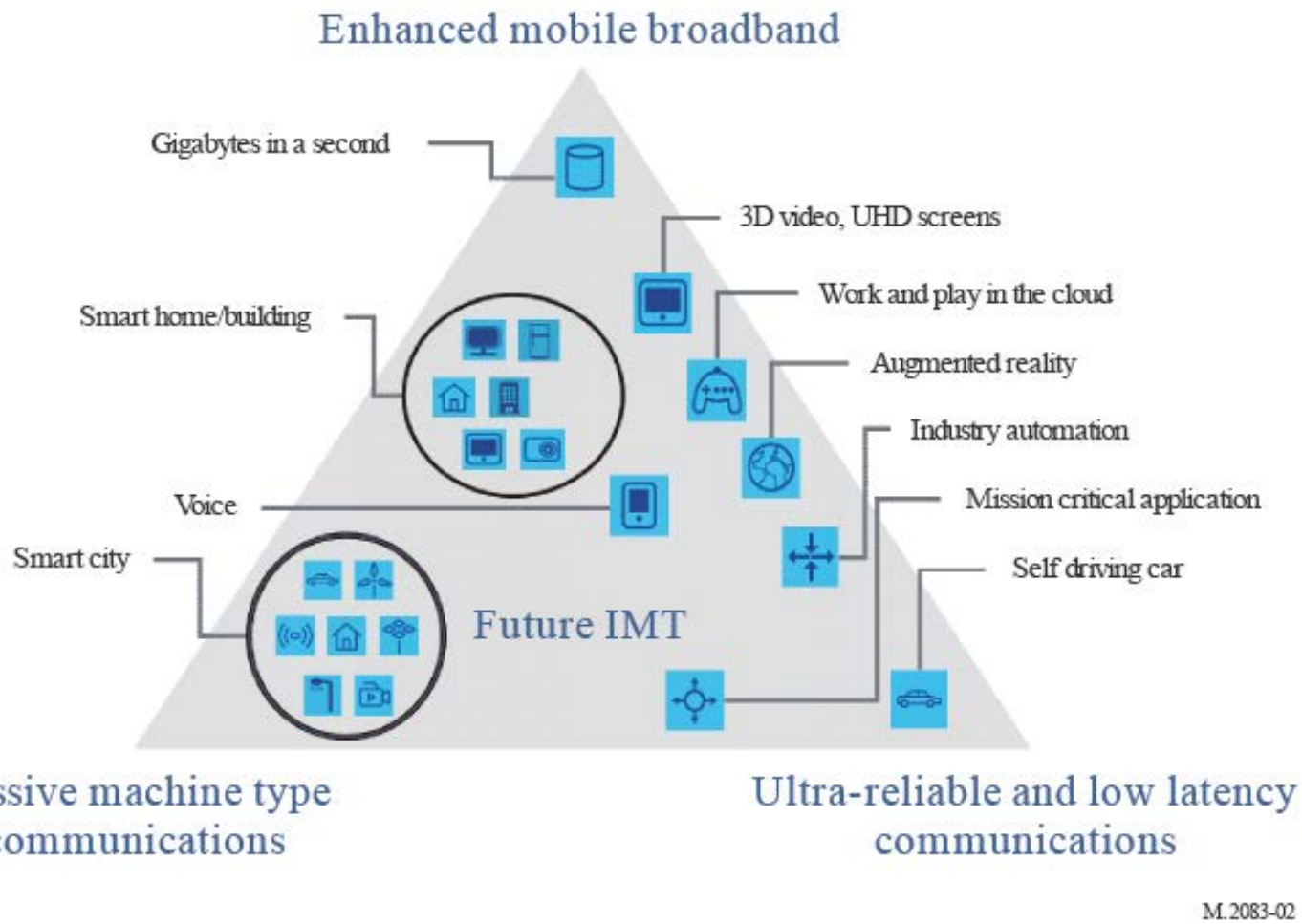
Three Key Application Areas:

1. **Enhanced Mobile Broadband (eMBB)**: Better mobile phones and hot spots. High data rates and 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)**: Many devices, low data rate, and low power. IoT with a long battery lifetime. Addition to GSM, LoRa, Zigbee, etc. Machine-centric communication.

Student Questions

©2025 Raj Jain

5G Applications (Cont)



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

Student Questions

©2025 Raj Jain

Spectrum for 5G

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

Student Questions

- Would later generations of wireless technology ever run out of available frequency ranges?

They will keep moving in higher frequency bands, and there is plenty of room at this point. Also, spectral efficiency will ensure that we use a smaller bandwidth.

- Does the specification require that all devices (i.e., smartphones) work in FR1 and FR2?

No.

- What is paired and unpaired spectrum? Is it the same as an aggregated spectrum?

Paired=Uplink & Download bands
Unpaired=Either direction

- Can a FR1 range be paired with a FR2 range?

No, if you mean uplink/downlink pairing. In advanced stages, bands can be "aggregated," which means a base station or a device can use two bands.

- What do new bands in this range mean?

New spectrum allocations in the sub-6 GHz band.

- Which devices use FR1 versus FR2?

Initial 5G devices used FR1. Newer devices (in the future) can use both.

©2025 Raj Jain

Above 6 GHz

- **Free-space loss** increases proportionately to the square of frequency and the square of the 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
- **Wide Channels**: Duplex filters cover only 3-4% of center frequency ⇒ Need carrier aggregation.
- **Antenna**: 8x8 array at 60 GHz is only 2cm x 2cm. A/D and D/A converters per antenna element may be expensive
- 2 Gbps to 1 km is feasible using mm waves

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

Student Questions

- Have solutions to the glass window problem been attempted in recent years? Or is this an inevitability of the frequency?

Every material has different light and radio-frequency properties. They will find other materials that either stop most RF or allow most RF as required.

- What are the requirements for 5G infrastructure besides the new antenna?

ITU does not set infrastructure requirements—only performance. New Antenna is not a requirement from ITU.

- Why are A/D and D/C expensive above 6 GHz?

High-frequency ⇒ High resolution

©2025 Raj Jain

Above 6 GHz (Cont)

- 100s MHz ⇒ **Multi-gigabit** data rates
- **Dense spatial reuse**
- Lower latency
- Need analog beamforming with a narrow beam width
- **Adaptive beam steering** and switching to avoid blockage from hand, body, or foliage
- Need different antenna configurations in the mobile
- **Directional antennas** with adaptable 3D beamforming and beam tracking

Student Questions

- Could you explain why we need different antenna configurations in the mobile?
- *Designing antennas is a research field in Electrical Engineering.*
- What is analog beamforming?

Digital = Using FFT
Analog = using analog circuits

- How is beam-forming accomplished? How does the tower know precisely where the phone is and form the beam in that direction?

Multiple antennae allow for the finding of direction and beam formation. It is like our two ears.

- Can you explain more about wide channels and dense spatial reuse?

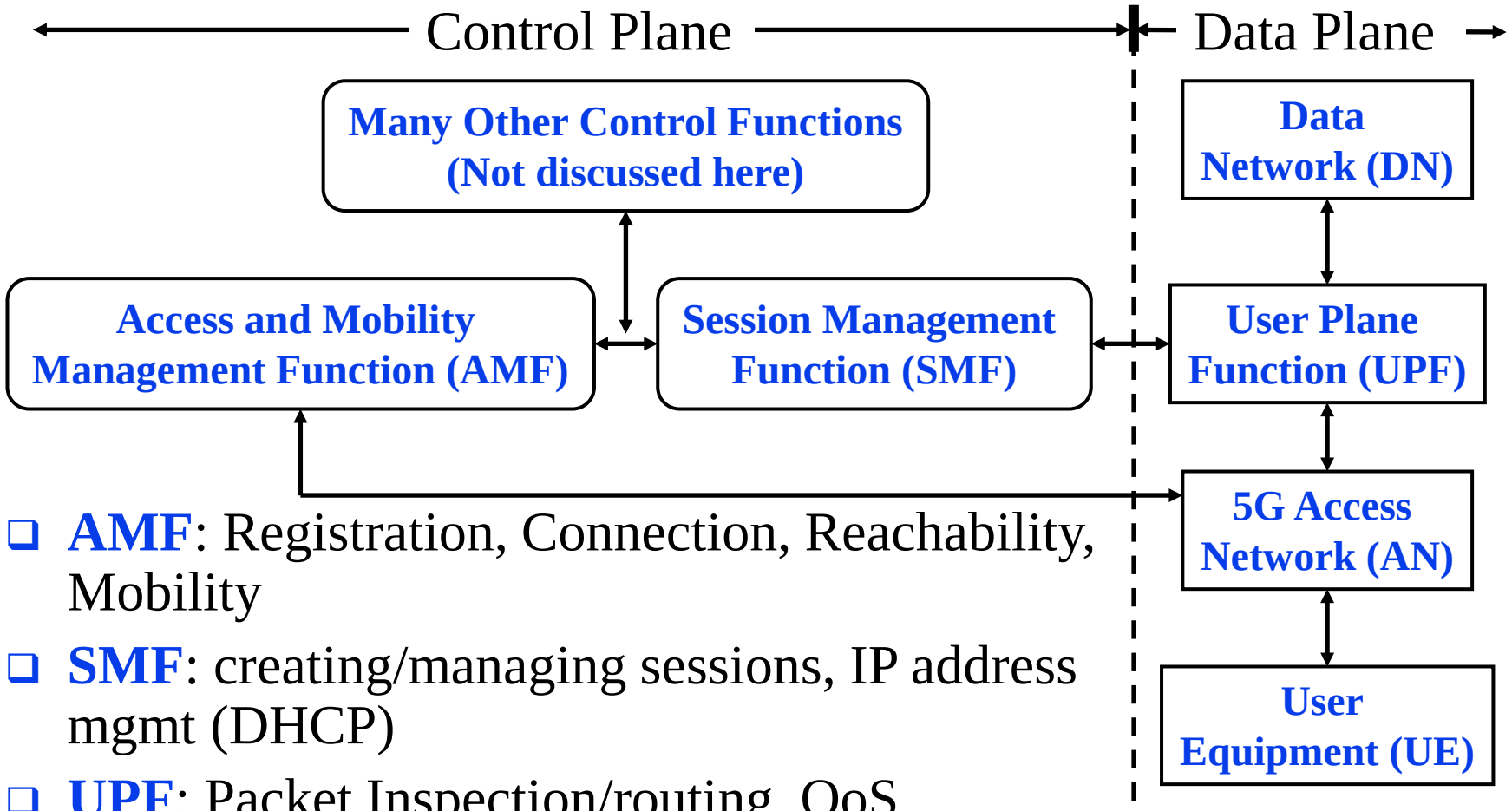
Wide=several MHz
Dense = More cells per sq km

- How about implementing the 6G network and the progress of 6G technology development so far?

Please register for CSE574 Advanced Wireless Networking for all Wi-Fi, Bluetooth, and Cellular network changes.

5G Core Architecture

- Clear separation of control plane and data plane



- **AMF**: Registration, Connection, Reachability, Mobility
- **SMF**: creating/managing sessions, IP address mgmt (DHCP)
- **UPF**: Packet Inspection/routing, QoS,

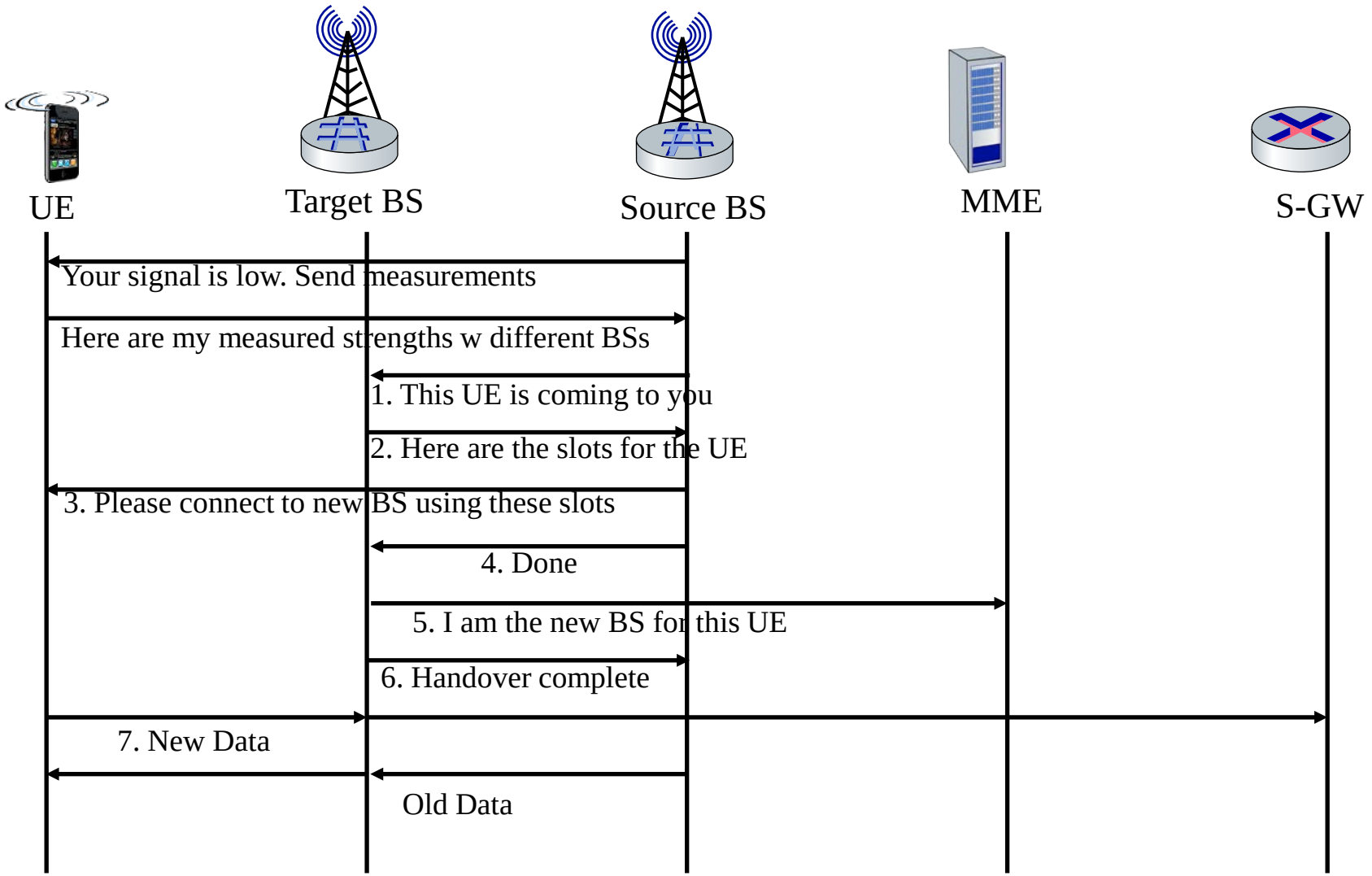
Student Questions

- Do we need to know DN and AN since they are neither mentioned in the book nor on the slide?

It is on the slide.

©2025 Raj Jain

Handover: In the Same LTE



Student Questions

- ❑ How do handoff and handover affect the delays?

They may increase the delay unless they are seamless.

- ❑ What are some of the challenges associated with implementing efficient handoff and handover processes in 5G networks?

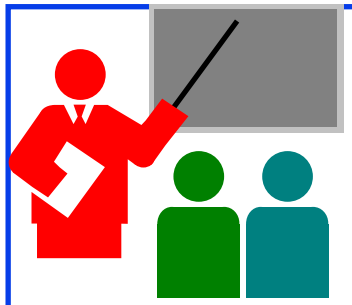
Same as in 4G: Quick and correct.

- ❖ How does handover from LTE to 2G/3G work, and vice versa?

Advanced Wireless Networking.

©2025 Raj Jain

End of Q



Review: 4G/5G

1. ITU-T sets requirements for the next generation of telecommunication networks every ten years.
2. 4G requirements are specified in the IMT-Advanced document. LTE is pre-4G technology. LTE-Advanced was approved as 4G.
3. Orthogonal Frequency Division Multiplexing Access (OFDMA) is used for media access control
4. All generations of telecommunications allow mobiles to sleep to improve battery life.
5. 5G extends improves performance over 4G by a factor of 10

Read Sections 7.4-7.8 and do R12-R31.

Student Questions

- How was Missouri's typhoon warning (sent to mobile phones across the state) some time ago realized? I have a mobile phone with a SIM card from another country that gets the alert. *Geographic Multicast*
- Sometimes, phones switch to a cellular network when the Wi-Fi signal is weak. How do they determine whether or not to switch? Does it compare the cellular and Wi-Fi signals? *Yes.*
- Does every new generation improve performance by a factor of 10? *Approximately. Different multipliers for different metrics.*

End of Part 3

©2025 Raj Jain

Acronyms

1xEV-DO	1 times Evolution to Data Optimized
1xEV	1 times Evolution
3GPP	Third Generation Partnership Project
6LowPAN	IPv6 on Low Power Personal Area Network
ACK	Acknowledgement
AD	Anno Domini (Latin for "in the year for the Lord"). After Crist.
AMF	Access and Mobility Management Function
AMPS	Advanced Mobile Phone System
AP	Access point
ARQ	Automatic Repeat Request (Retransmission)
AuC	Authentication Center
BER	Bit Error Rate
BPSK	Binary Phase Shift Keying
BS	Base Station
BSA	Basic Service Area
BSC	Base Station Controller
BSS	Basic Service Set

Student Questions

©2025 Raj Jain

Acronyms (Cont)

- BSSID Basic Service Set ID
- BTS Base transceiver station
- CA Collision Avoidance
- CAP Contention Access Period
- CDMA Code Division Multiple Access
- CEPT Committee of European Posts and Telegraph
- CFP Contention Free Period
- COA Care-of-address
- CRC Cyclic Redundancy Check
- CSE Computer Science and Engineering
- CSMA Collision Sense Multiple Access
- CTS Clear to Send
- dB deciBel
- DCN Data Communication Network
- DHCP Dynamic Host Control Protocol
- DIFS Distributed Inter-Frame Spacing

Student Questions

©2025 Raj Jain

Acronyms (Cont)

- DO Data Only
- DSSS Direct Sequence Spread Spectrum
- DV Data and Voice
- DVB Digital Video Broadcast
- EDGE Enhanced Data rate for GSM evolution
- EGPRS Enhanced GPRS
- EIA Electronic Industry Association
- EIR Equipment Identity Register
- eMBB Enhanced Mobile Broadband
- eNB Enhanced Node B
- eNodeB Enhanced Node B
- EPC Evolved Packet Core
- EPS Evolved Packet System
- ESA Extended Service Area
- ESS Extended Service Set
- FCC Federal Communications Commission

Student Questions

©2025 Raj Jain

Acronyms (Cont)

- FDMA Frequency Division Multiple Access
- FFT Fast Fourier Transform
- FR Frequency Range
- FR1 Freuqency Range 1: Sub 6-GHz
- FR2 Frequency Range 2:24.25-52.6 GHz (mm-Waves)
- 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
- GTP GPRS tunneling protocol
- GTS Guaranteed Transmission Service
- GW Gateway
- HART Highway Addressable Remote Tra
- HLR Home Location Register

Student Questions

©2025 Raj Jain

Acronyms (Cont)

- HSPA High-Speed Packet Access
- HSPDA High-Speed Packet Download Access
- HSS Home Subscriber Service
- ID Identifier
- IEEE Institution of Electrical and Electronics Engineers
- IETF Internet Engineering Task Force
- IFFT Inverse Fast Fourier Transform
- IFS Inter-frame space
- IMEI International Mobile Equipment Identifier
- IMS IP Multimedia Subsystem
- IMSI International Mobile Subscriber Identity
- IMT International Mobile Telecommunication
- IoT Internet of Things
- IP Internet Protocol
- IPv6 IP version 6
- IS International Standard

Student Questions

©2025 Raj Jain

Acronyms (Cont)

- ISA International Society of Automation
- ISDN Integrated Switched Digital Network
- ITU-R International Telecommunications Union (Radiocommunications Sector)
- ITU-T International Telecommunications Union (Telecommunication Sector)
- ITU International Telecommunications Union
- kHz kilo Hertz
- kW kilo Watts
- LAN Local Area Network
- LoRa Long Range (Wireless)
- LoRaWAN Long Range (Wireless) Wide Area Network
- LR Long-Range
- LTE Long-Term Evolution
- mA milli-Ampere
- MAC Media-Access Control
- MANET Mobile Ad-hoc Network

Student Questions

©2025 Raj Jain

Acronyms (Cont)

MGW	Media Gateway
MHz	Mega Hertz
MIMO	Multiple Input Multiple Output
MiWi	Microchip Technology (company) Wireless
MME	Mobility Management Entity
mMTC	Massive Machine Type Communications
MO	Missouri
MSC	Mobile Switching Center
mW	milli-Watt
NA	North America
NAT	Network Address Translator
NodeB	Node B (Base Station)
NR	New Radio
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
P-GW	PDN Gateway

Student Questions

©2025 Raj Jain

Acronyms (Cont)

PAN	Personal Area Network
PAPR	Peak-to-Average Power Ratio
PC	Personal Computer
PCRF	Polic and Charging Rules Function
PDCP	Packet Data Convergence Protocol
PDN	Public Data Network
PDU	Protocol Data Unit
PGW	Packet Data Network Gateway
PHY	Physical Layer
PIFS	Point-Coordination Inter-Frame space
PSTN	Public Switched Telephone Network
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RAN	Radio Access Network
RNC	Radio Network Controller
ROHC	Robust Header Compression

Student Questions

Acronyms (Cont)

- RRC Radio Resource Control
- RTS Ready to send
- S-GW Service Gateway
- SC Single Carrier
- SCDMA Synchronous CDMA
- SGSN Service GPRS Support Node
- SGW Serving Gateway
- SIFS Short Inter-Frame Spacing
- SIM Subscriber Identification Mod
- SMF Session Management Function
- SNR Signal to Noise Ratio
- SS7 Signaling System 7
- SSID Service Set Identifier
- SYN Synchronizing Frame
- SYNACK SYN Acknowledgement
- TACS Total Access Communications System
- TCP Transmission Control Protocol

Student Questions

©2025 Raj Jain

Acronyms (Cont)

- TD-SCDMA Time Duplexed Synchronous CDMA
- TD Time Duplexed
- TDMA Time Division Multiple Access
- TIA Telecom Industry Association
- TV Television
- UDP User Datagram Protocol
- UE User Element
- UK United Kingdom
- UMB Ultra Mobile Broadband
- UMTS Universal Mobile Telecommunication
- UPF User Plane Function
- URLLC Ultra-Reliable Low-Latency Communication
- USA United States of America
- UTRAN Evolved UTRAN
- UTRAN UMTS Terrestrial Radio Access
- VANET Vehicular Ad-hoc Network
- VLR Visitor Location Register

Student Questions

©2025 Raj Jain

Acronyms (Cont)

- WCDMA Wide-band CDMA
- WEP Wired Equivalent Privacy
- WPAN Wireless Personal Area Network
- WUSTL Washington University in St. Louis

Student Questions

©2025 Raj Jain

Scan This to Download These Slides



Raj Jain
http://rajjain.com

http://www.cse.wustl.edu/~jain/cse473-25/i_7wmn.htm

Student Questions

©2025 Raj Jain

Related Modules



CSE 567: The Art of Computer Systems Performance Analysis
https://www.youtube.com/playlist?list=PLjGG94etKypJEKjNAa1n_1X0bWWNyZcof

CSE473S: Introduction to Computer Networks (Fall 2011),
https://www.youtube.com/playlist?list=PLjGG94etKypJWOSPMh8Azcgy5e_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

©2025 Raj Jain