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



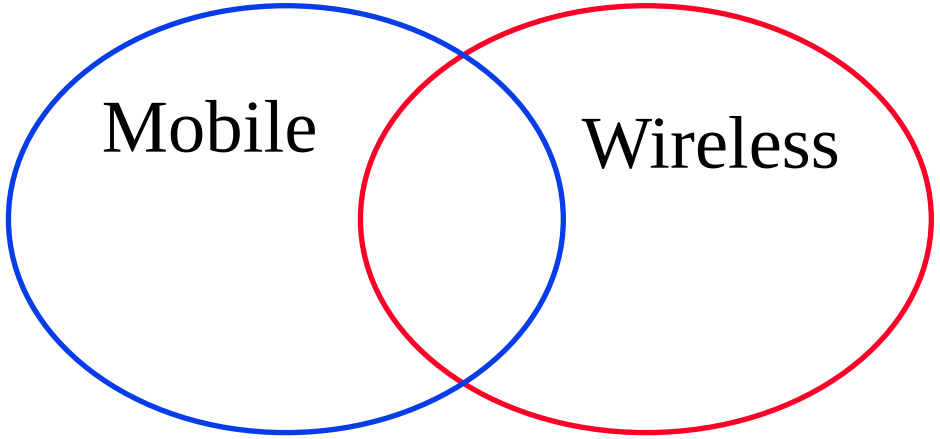
Wireless Link Characteristics

- 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

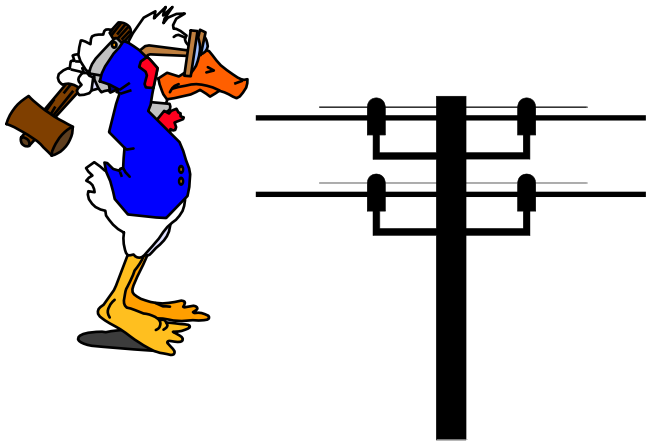
©2025 Raj Jain

Mobile vs Wireless





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

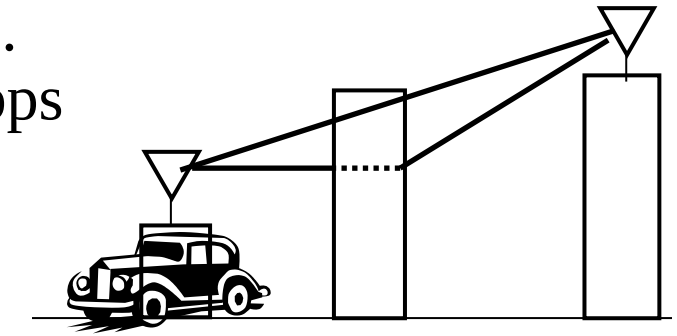


Student Questions

©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

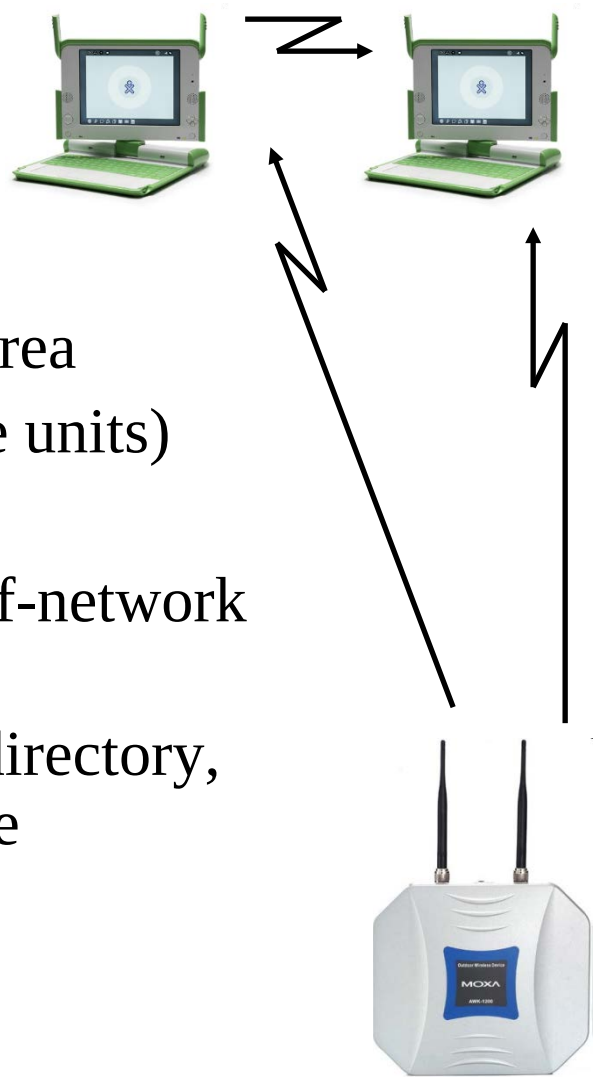


Student Questions

©2025 Raj Jain

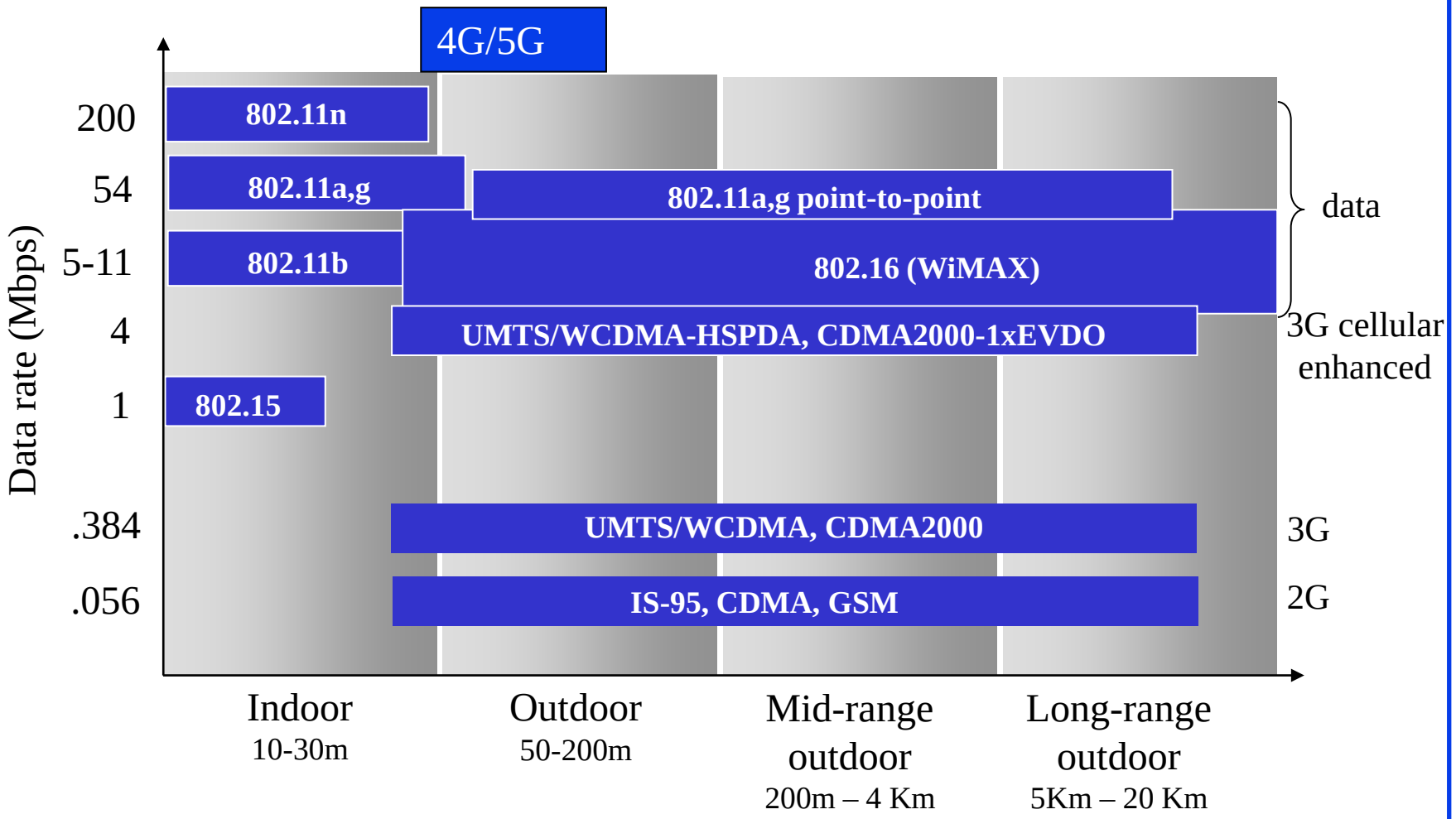
Peer-to-Peer or Base Stations?

- 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

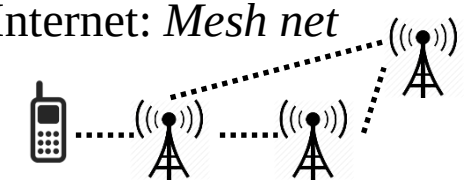
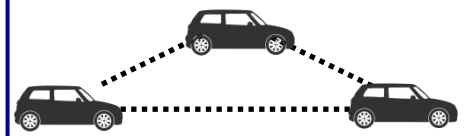
Characteristics of Selected Wireless Link Standards



Student Questions

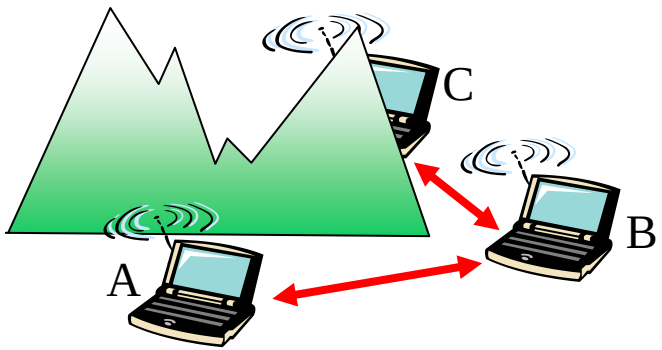
©2025 Raj Jain

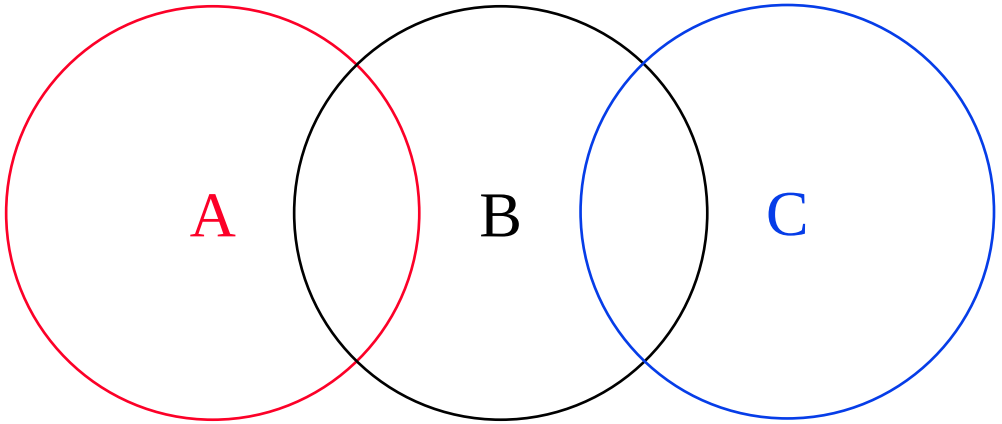
Wireless Network Taxonomy

	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* 
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

Hidden Node Problem



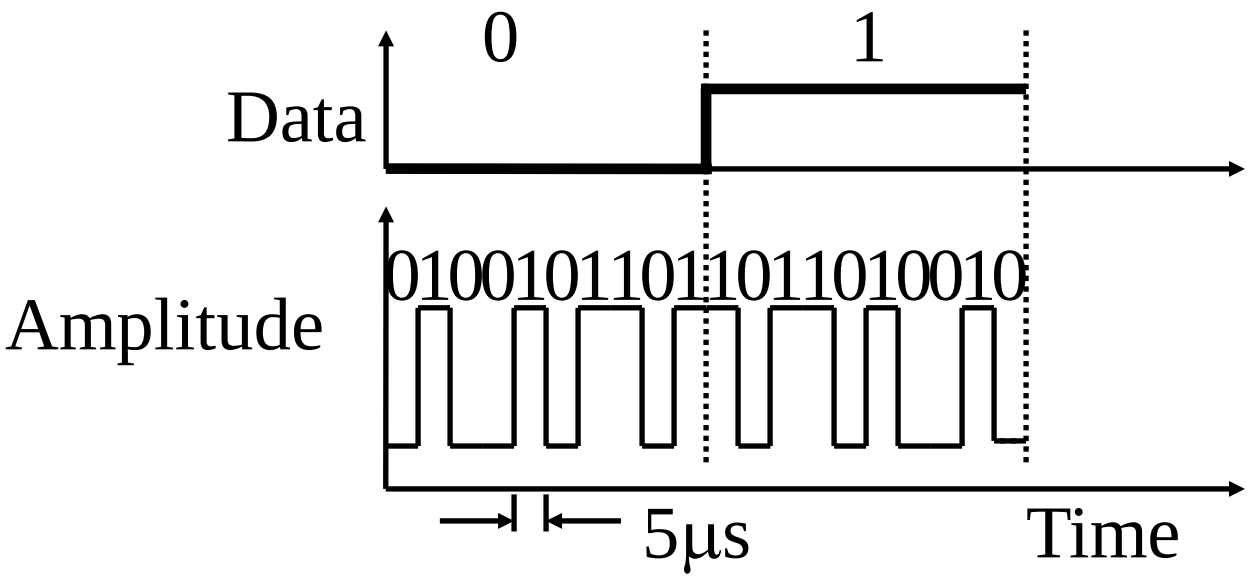


- B and A can hear each other.
  B and C can hear each other.
  A and C cannot hear each other.
  ⇒ C is hidden for A and vice versa.
- C may start transmitting while A is also transmitting.
  A and C can't detect collisions.
- Only the receiver can help avoid collisions.

Student Questions

©2025 Raj Jain

Direct-Sequence Spread Spectrum CDMA

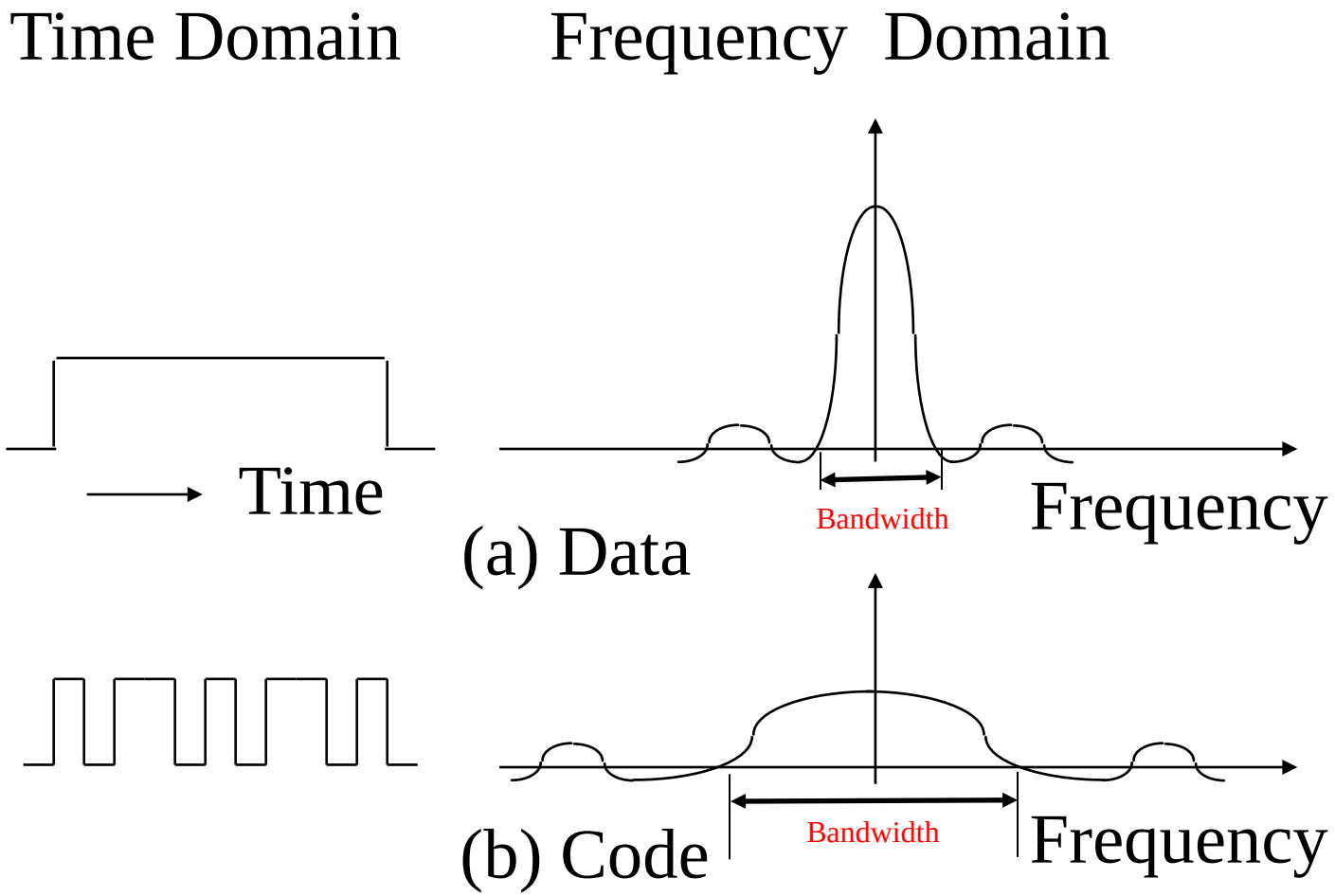


- Spreading factor = Code bits/data bit, 10-100 commercial (Min 10 by FCC), 10,000 for military
- Signal bandwidth >10 × data bandwidth
- Code sequence synchronization
- Correlation between codes ⇒ Interference ⇒ Orthogonal

Student Questions

©2025 Raj Jain

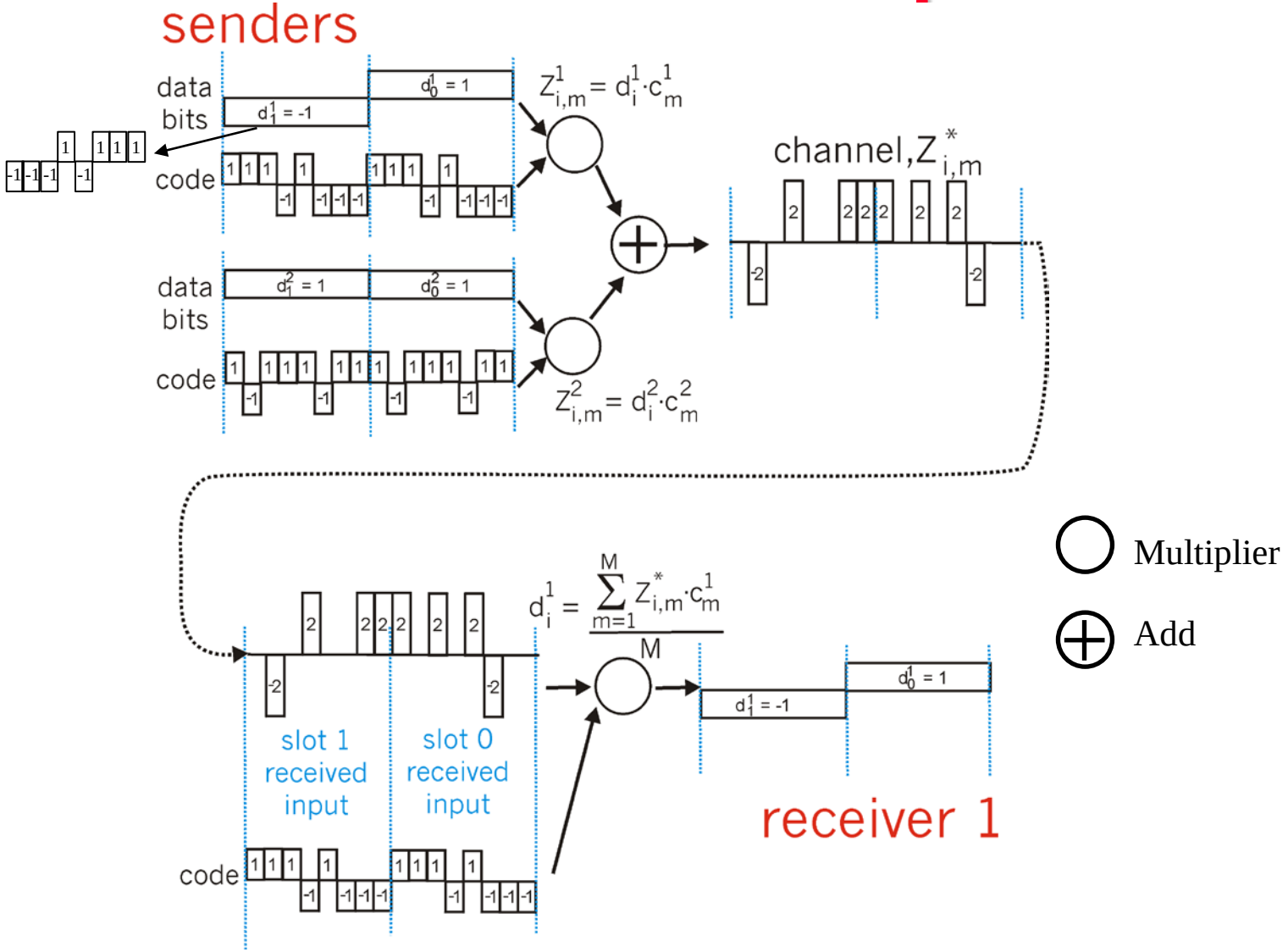
DS Spectrum



Student Questions

©2025 Raj Jain

Two Sender CDMA Example



Student Questions

©2025 Raj Jain

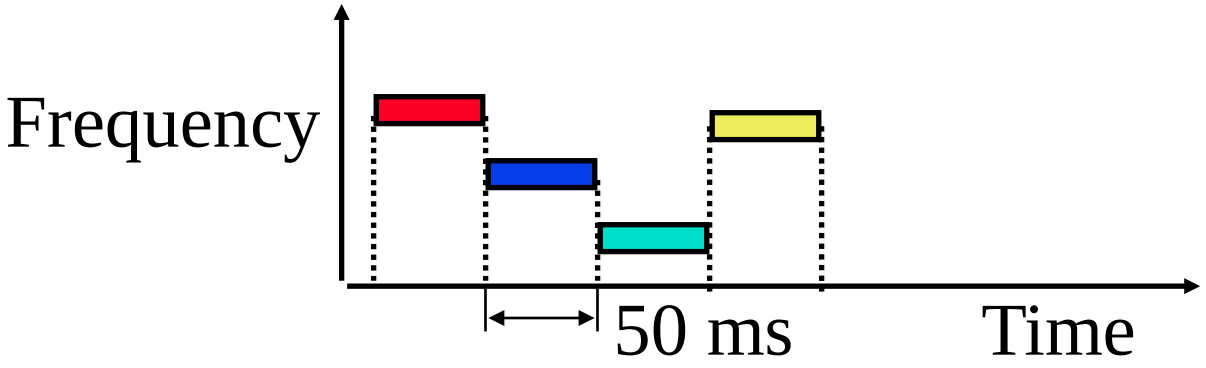
Homework 7A: CDMA Coding

- [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

©2025 Raj Jain

Frequency Hopping Spread Spectrum

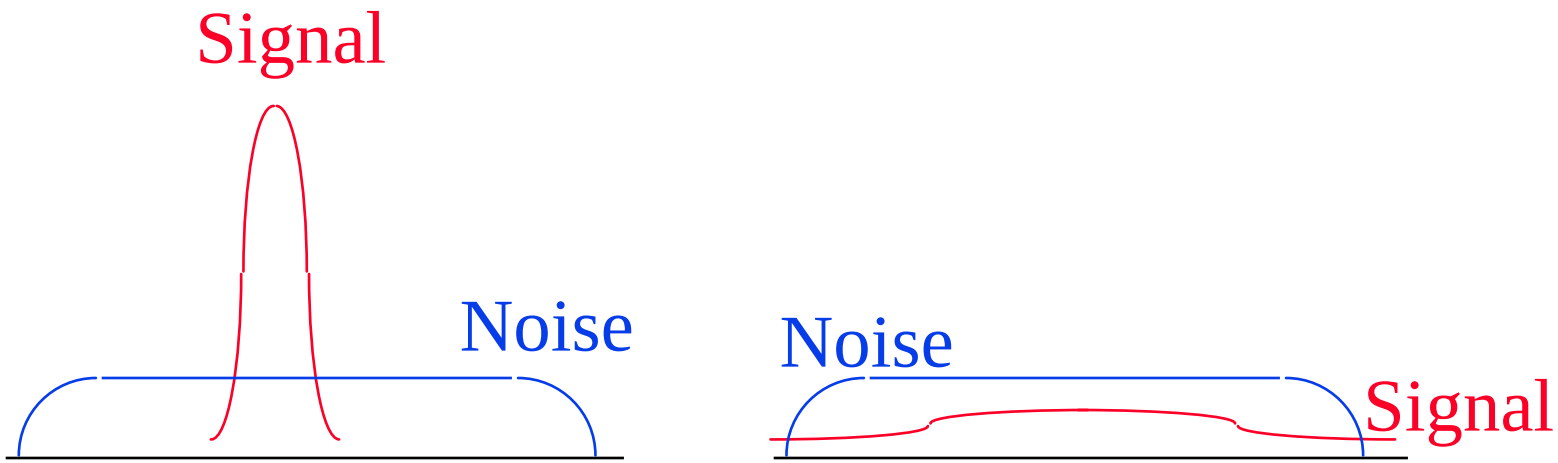


- Pseudo-random frequency hopping
- Spreads the power over a broad spectrum
  ⇒ Spread Spectrum
- Developed initially for military
- Patented by actress Hedy Lamarr (1942)
- Narrowband interference can't jam

Student Questions

©2025 Raj Jain

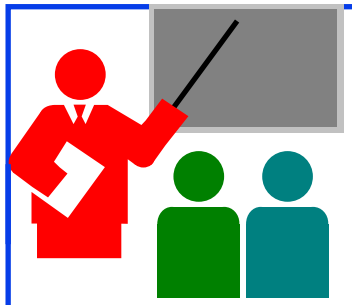
Spectrum



(a) Normal (b) Frequency Hopping

Student Questions

©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

Ref: Section 7.2, Review Exercises R3-R4

©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

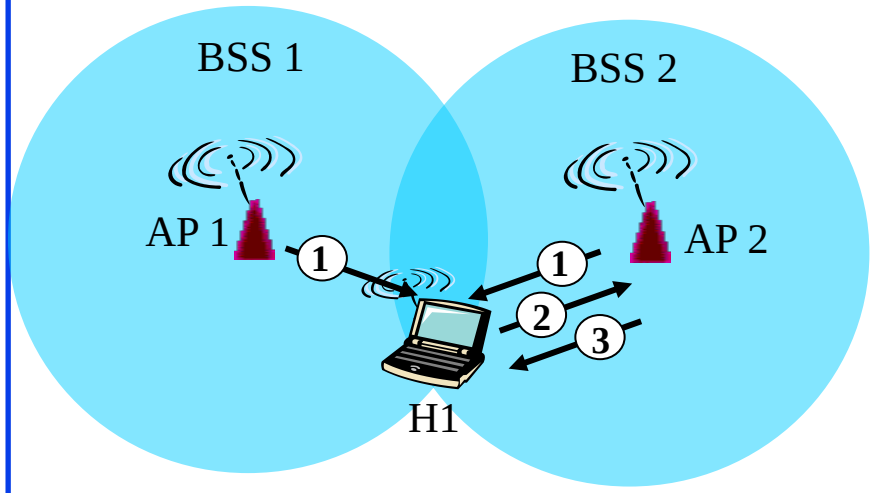
IEEE 802.11 Wireless LAN PHYs

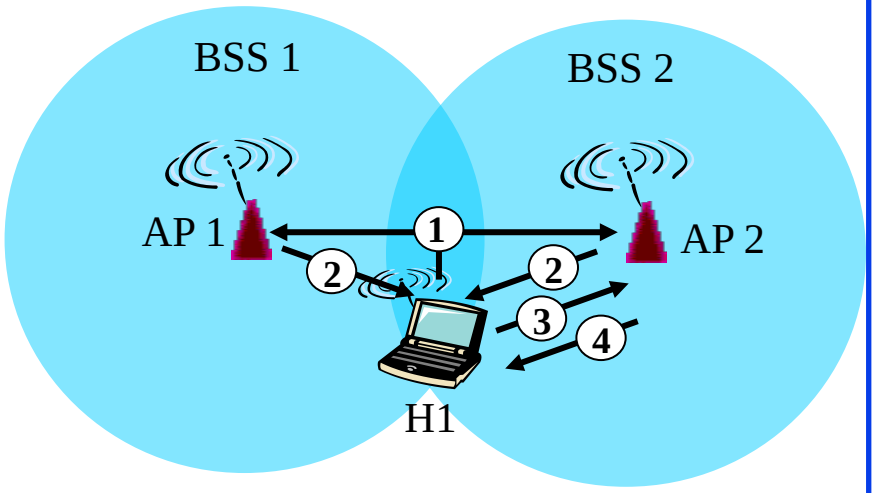
- **802.11**: 2.4 GHz, 1-2 Mbps
- **802.11b**: 2.4 GHz, 11 Mbps nominal
  - Direct sequence spread spectrum (DSSS) in the physical layer
  - All hosts use the same chipping code
- **802.11a**: 5.8 GHz band, 54 Mbps nominal
- **802.11g**: 2.4 GHz band, 54 Mbps nominal
- **802.11n**: 2.4 or 5.8 GHz, Multiple 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

©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

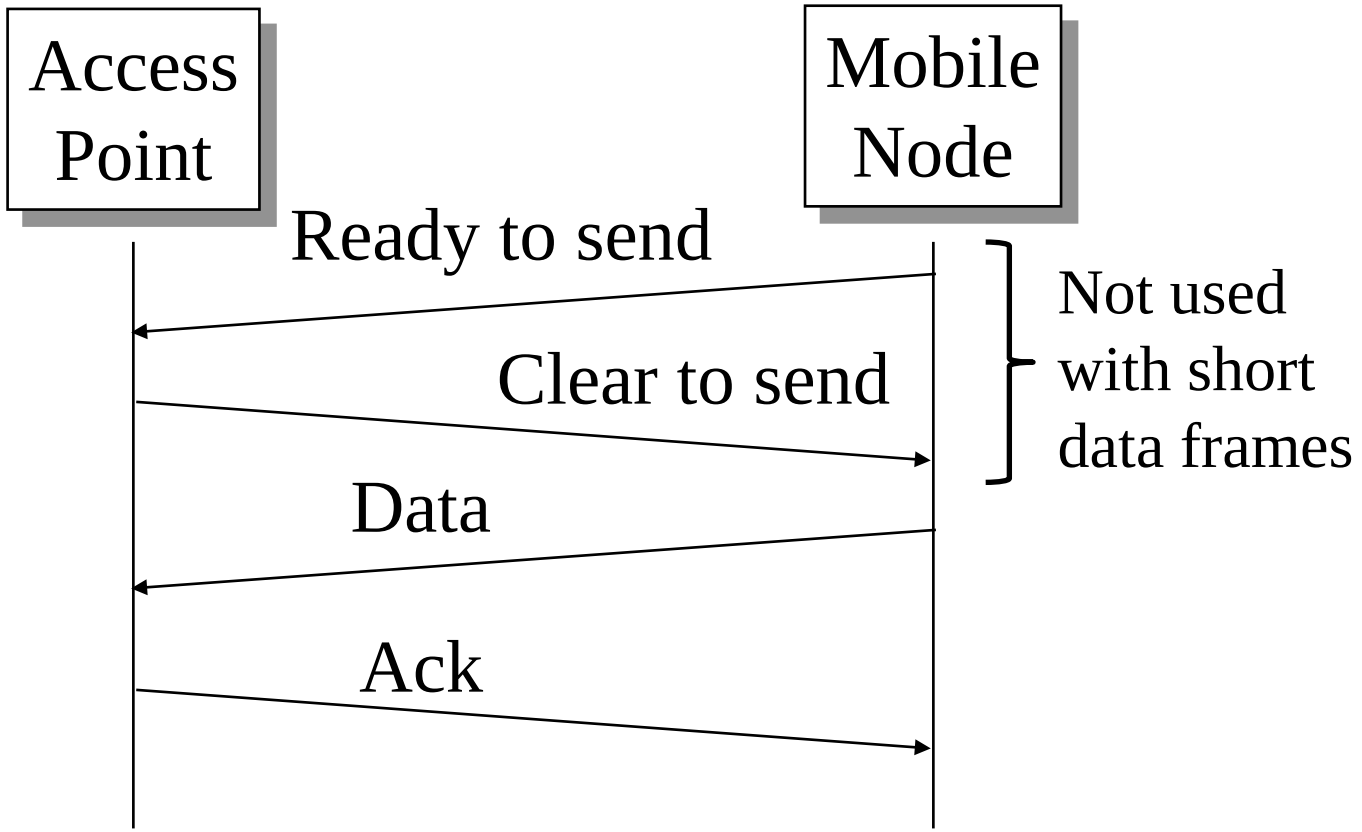
Active Scanning:

(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

©2025 Raj Jain

4-Way Handshake



Student Questions

©2025 Raj Jain

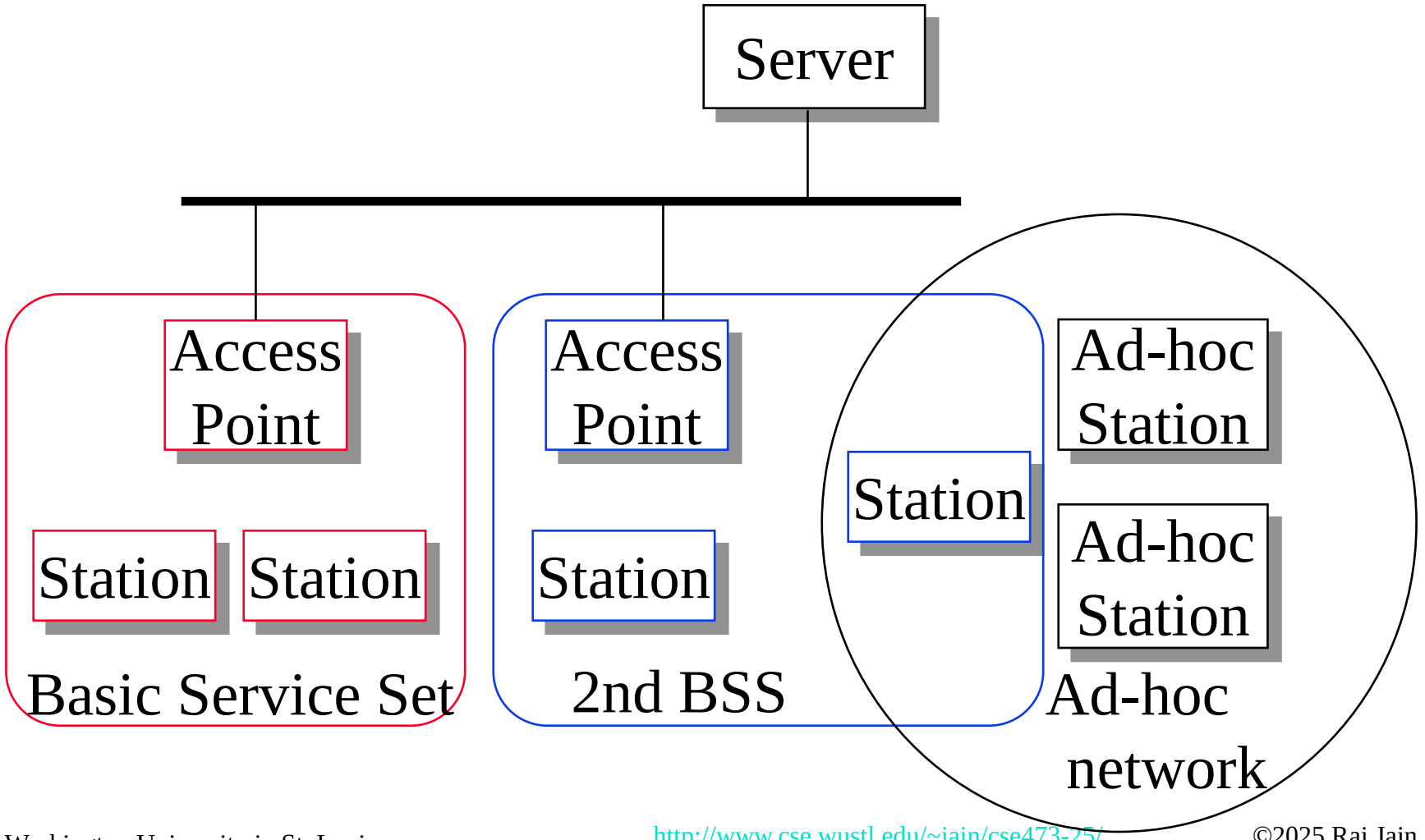
IEEE 802.11 MAC

- 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

©2025 Raj Jain

IEEE 802.11 Architecture



Student Questions

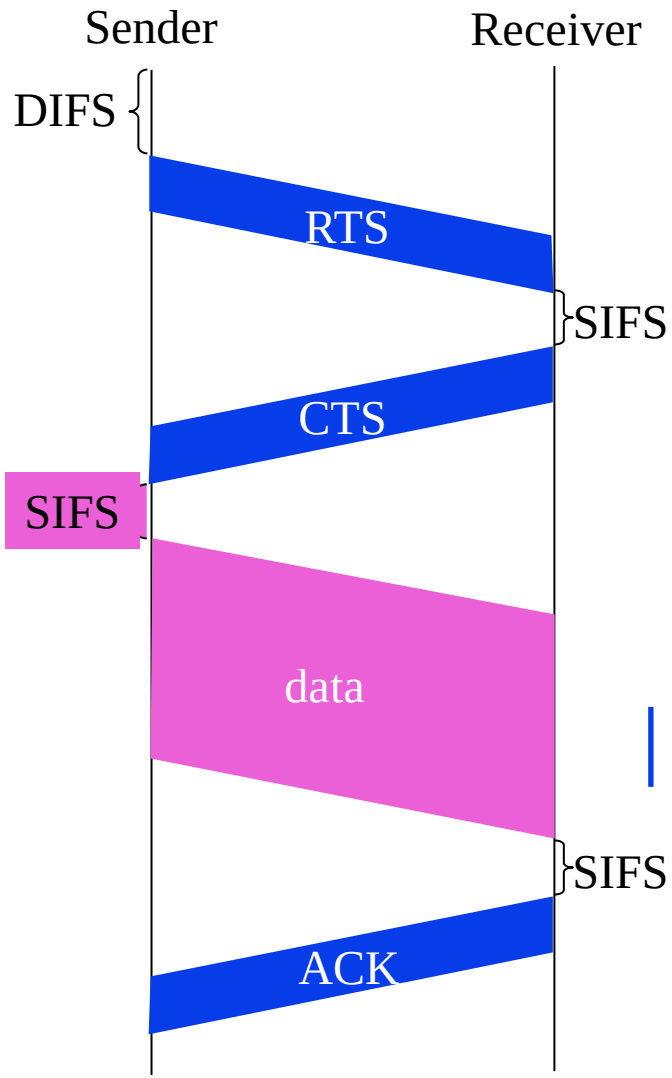
Architecture (Cont.)

- 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 = $\{MAC_1,\ldots,MAC_n\}$.
  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

©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

©2025 Raj Jain

Homework 7B: Wi-Fi Transmission

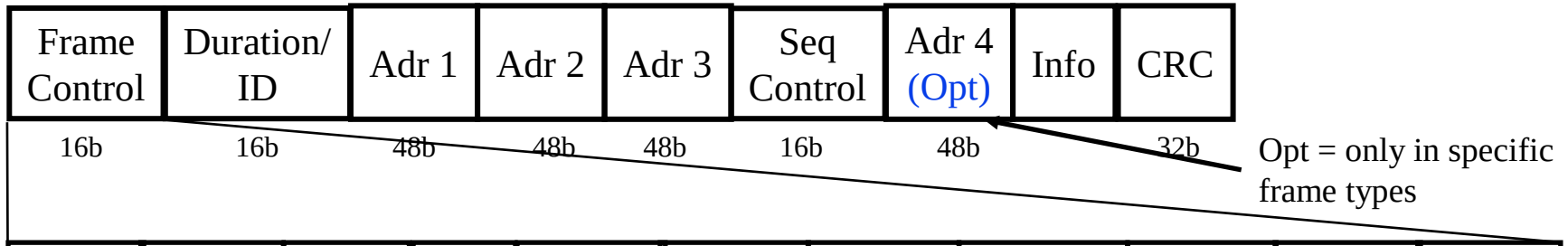
- [6 points] Suppose an 802.11b station is configured permanently to reserve the channel with the RTS/CTS sequence. Suppose this station suddenly wants to transmit 2,000 bytes of data, and all other stations are idle at this time. Assume a frame without data is 32 bytes long and has a transmission rate 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.

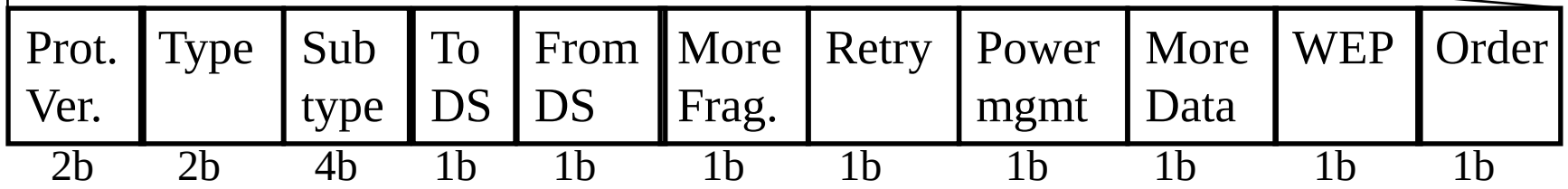
Student Questions

Ref: Problem P7

©2025 Raj Jain

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

©2025 Raj Jain

MAC Frame Fields

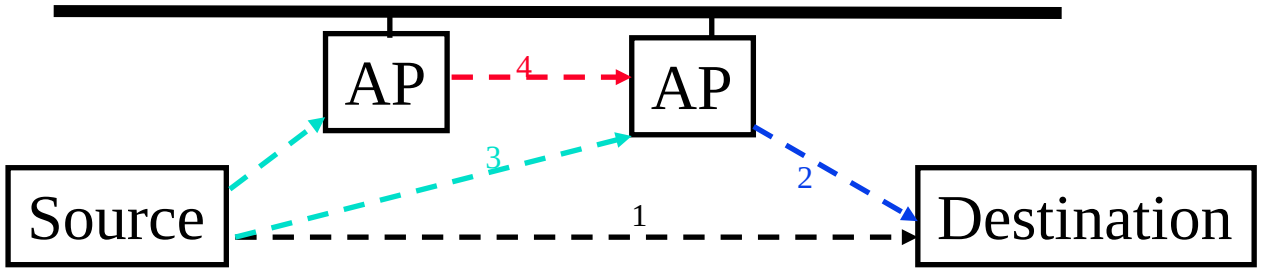
- **Duration/Connection ID**:
  - If used as a duration field, it indicates the time (in μs) channel will be allocated for successfully transmitting the MAC frame. Includes time until the end of Ack
  - In some control frames, it contains an association or connection identifier
- **Sequence Control**:
  - 4-bit fragment number subfield
    - For fragmentation and reassembly
  - 12-bit sequence number
  - Number frames between given transmitter and receiver

Student Questions

©2025 Raj Jain

802.11 Frame Address Fields

- All stations filter on "Address 1"



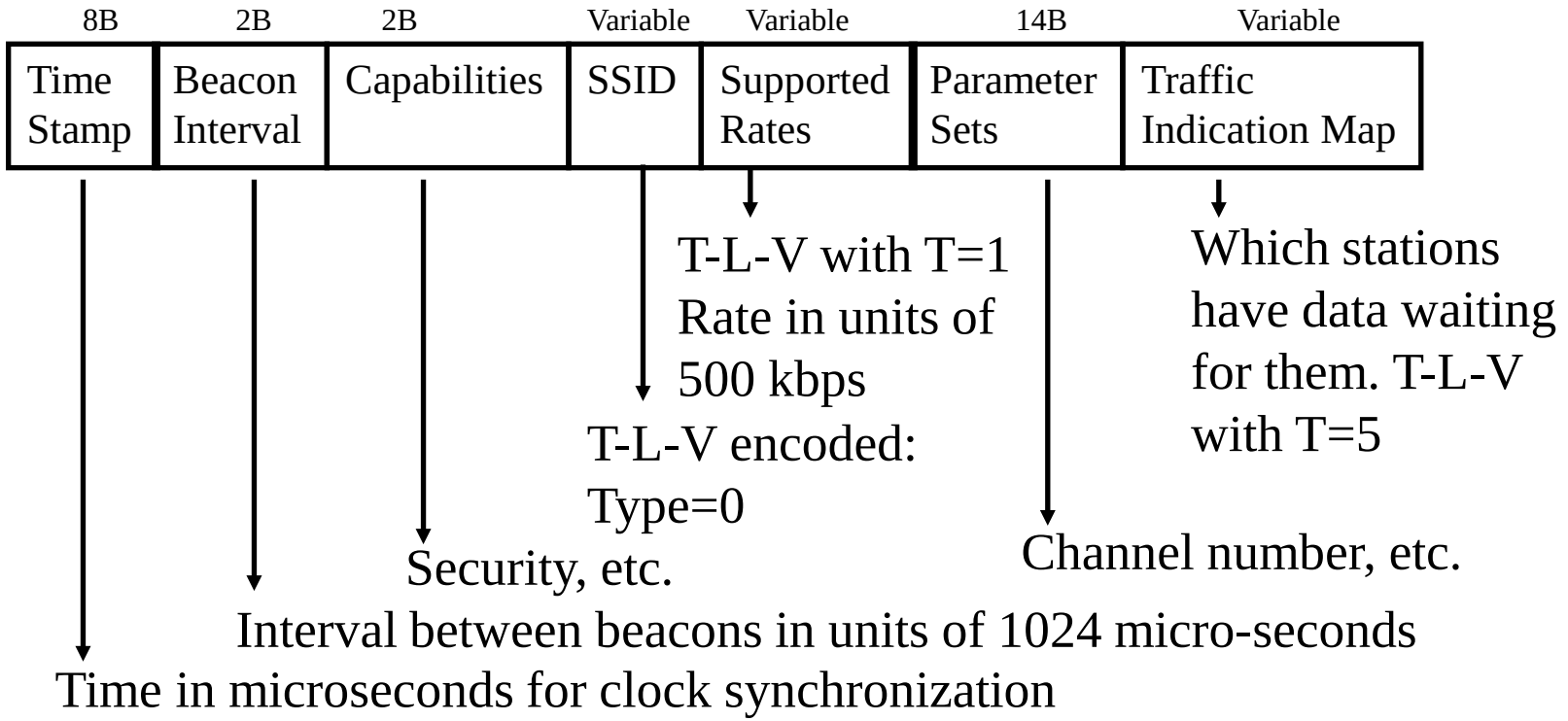
	To Distribution System	From Distribution System	Address 1	Address 2	Address 3	Address 4
1	0	0	Destination Address	Source Address	BSS ID	-
2	0	1	Destination Address	BSS ID	Source Address	-
3	1	0	BSS ID	Source Address	Destination Address	-
4	1	1	Receiver AP Address	Transmitter AP Address	Destination Address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

Student Questions

End of Part 1

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

Lab 7:Wi-Fi

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

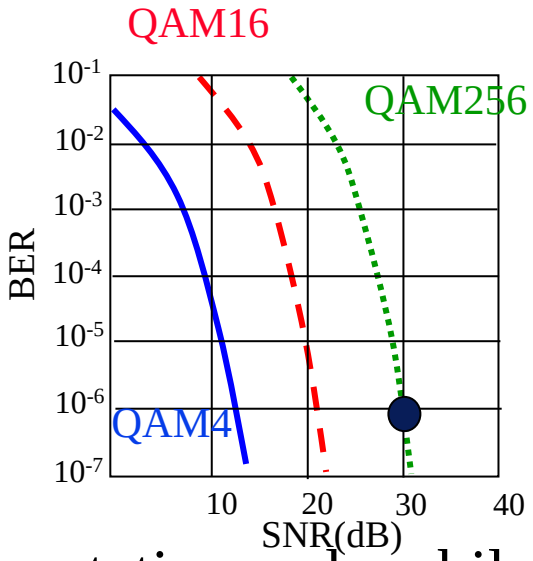
Open *Wireshark_802_11.pcap* in Wireshark. Select **View → Expand All**. Answer the following questions. There is no need to attach screen captures.

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

©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.

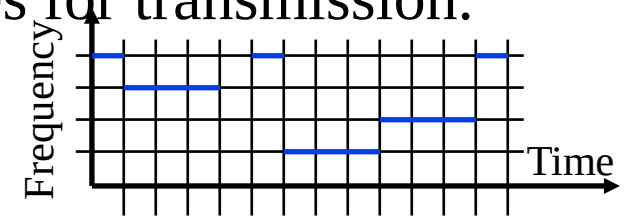
Student Questions

©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

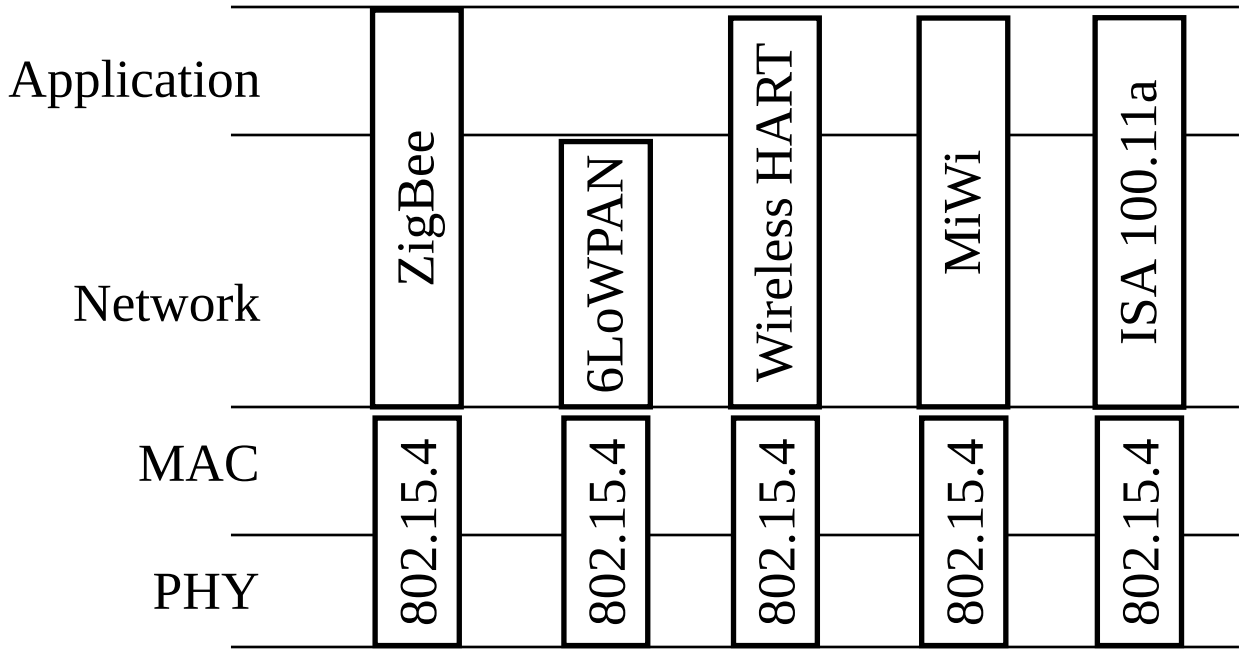


Student Questions

©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



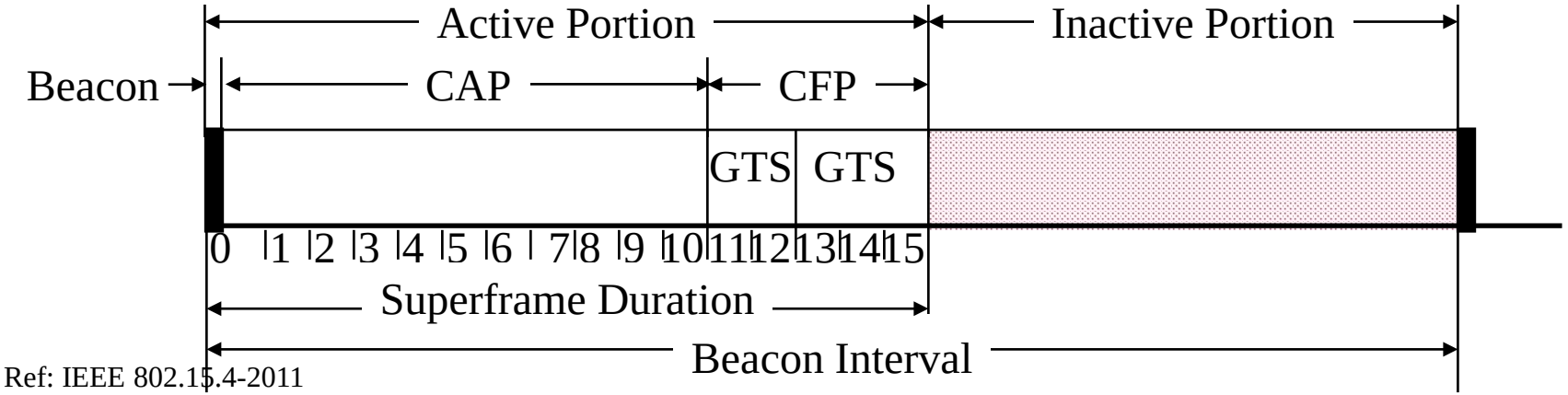
Student Questions

©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.



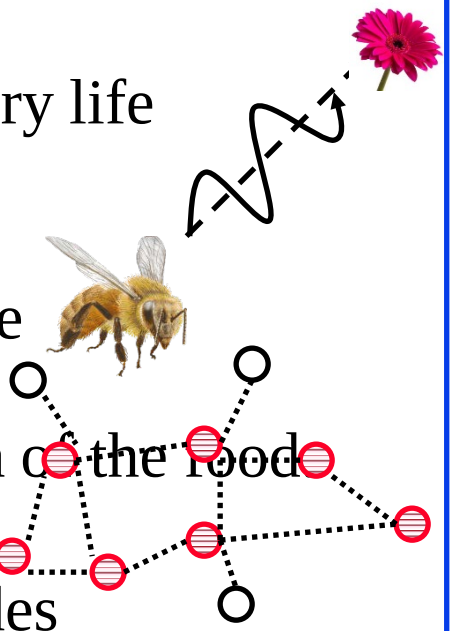
Ref: IEEE 802.15.4-2011

Student Questions

©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

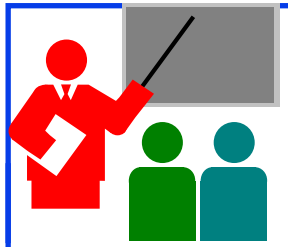
Mesh Routing: End nodes help route messages to others

Mesh Topology: Loops possible

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

©2025 Raj Jain

Student Questions



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

Ref: Section 7.3, Review Exercises R5-R12

Student Questions

©2025 Raj Jain



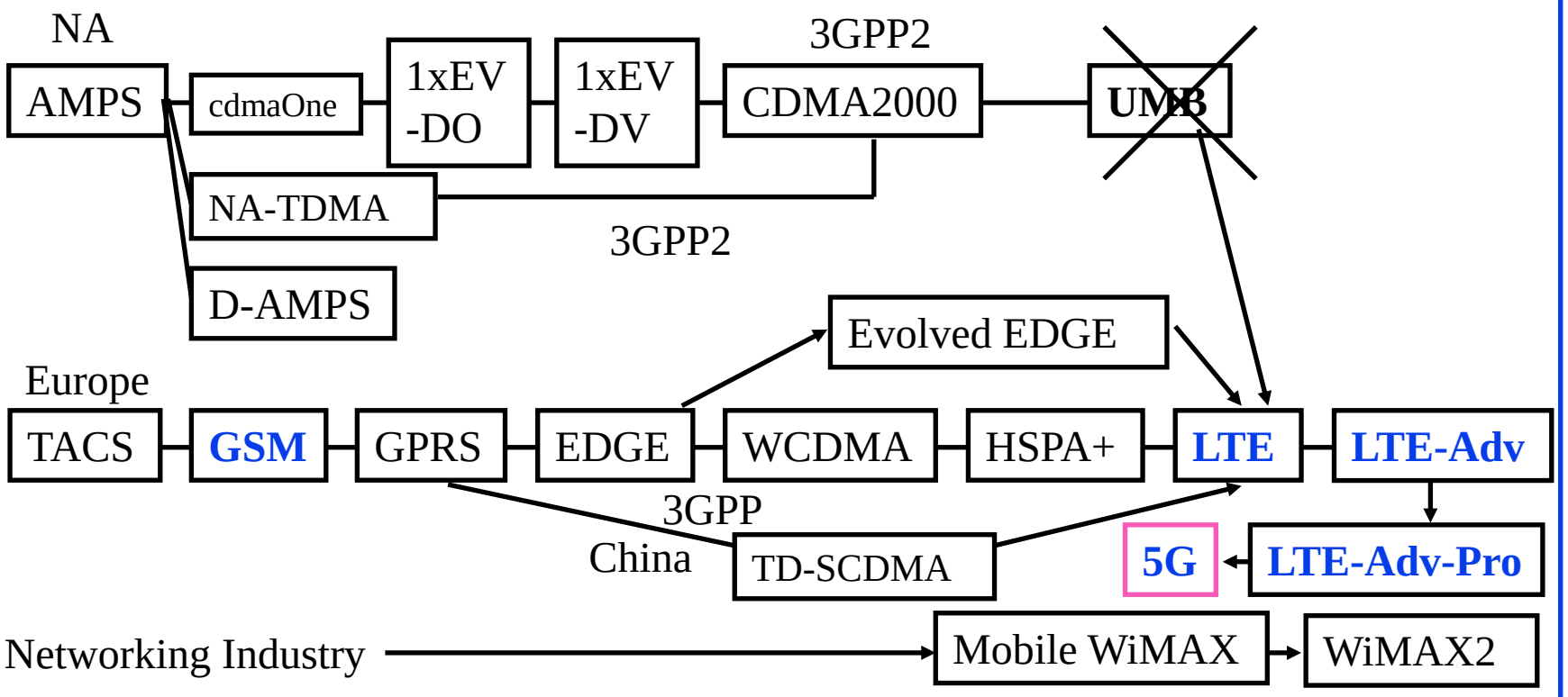
Cellular Networks

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

Student Questions

©2025 Raj Jain

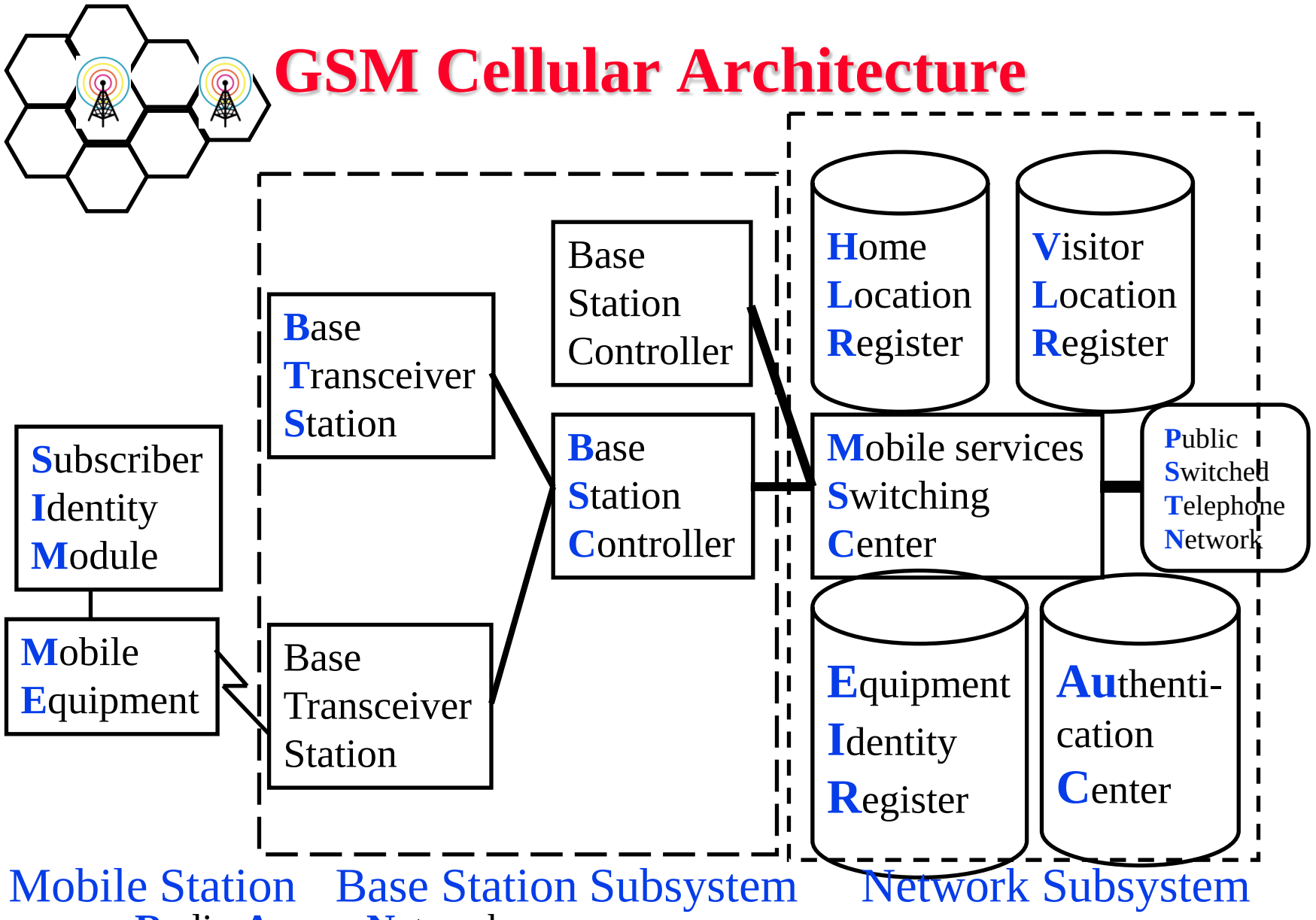
Cellular Telephony Generations



Student Questions

©2025 Raj Jain

GSM Cellular Architecture



Student Questions

©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

©2025 Raj Jain

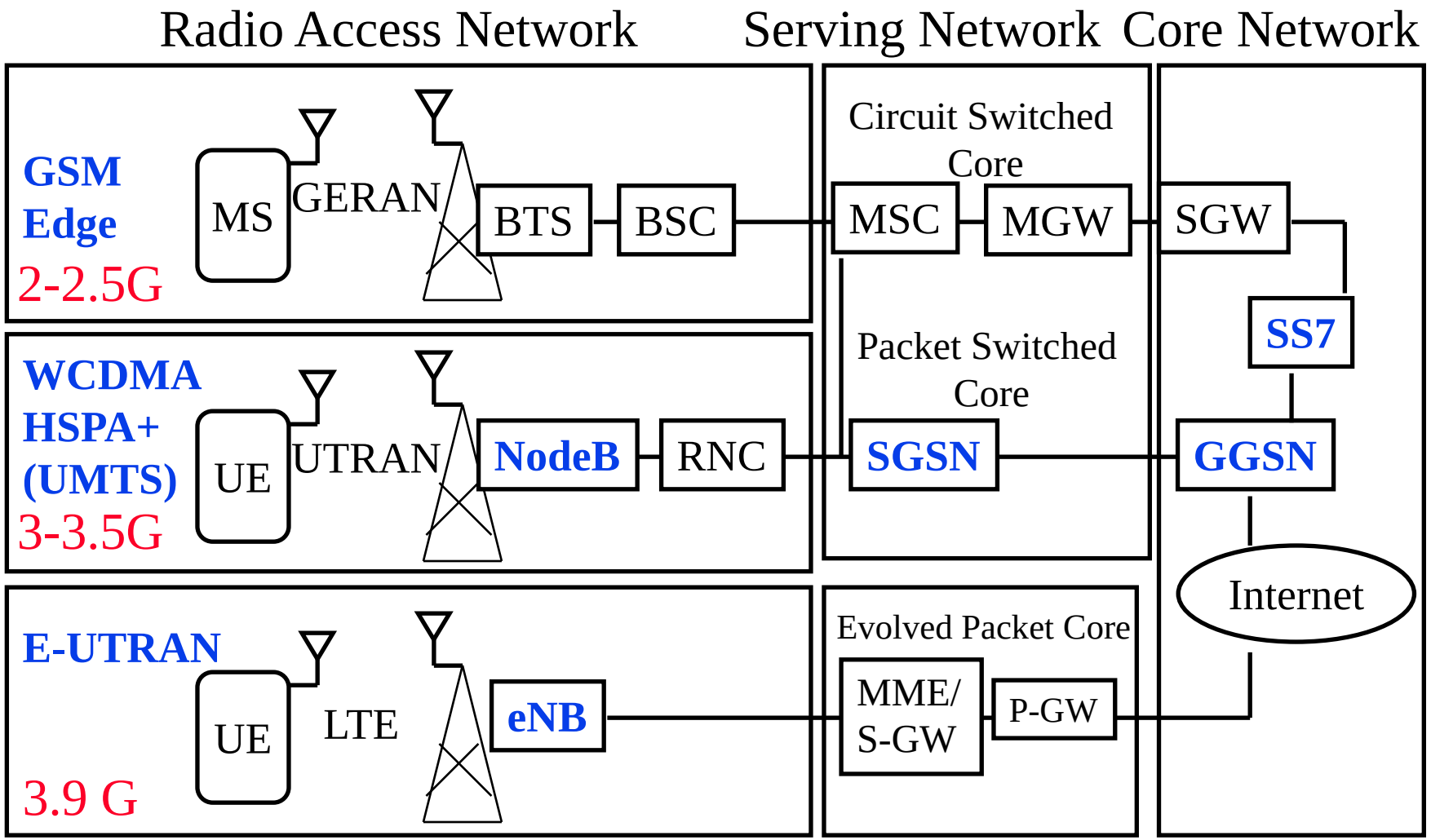
Cellular Architecture (Cont.)

- 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

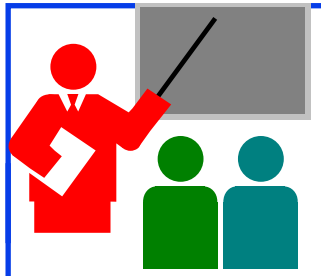
©2025 Raj Jain

Evolved Packet System (EPS)



Student Questions

©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?

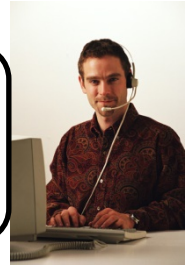
Mr. Smith! Call from Taylor

Hello Senator Taylor

Mr. Smith



Hotel Operator

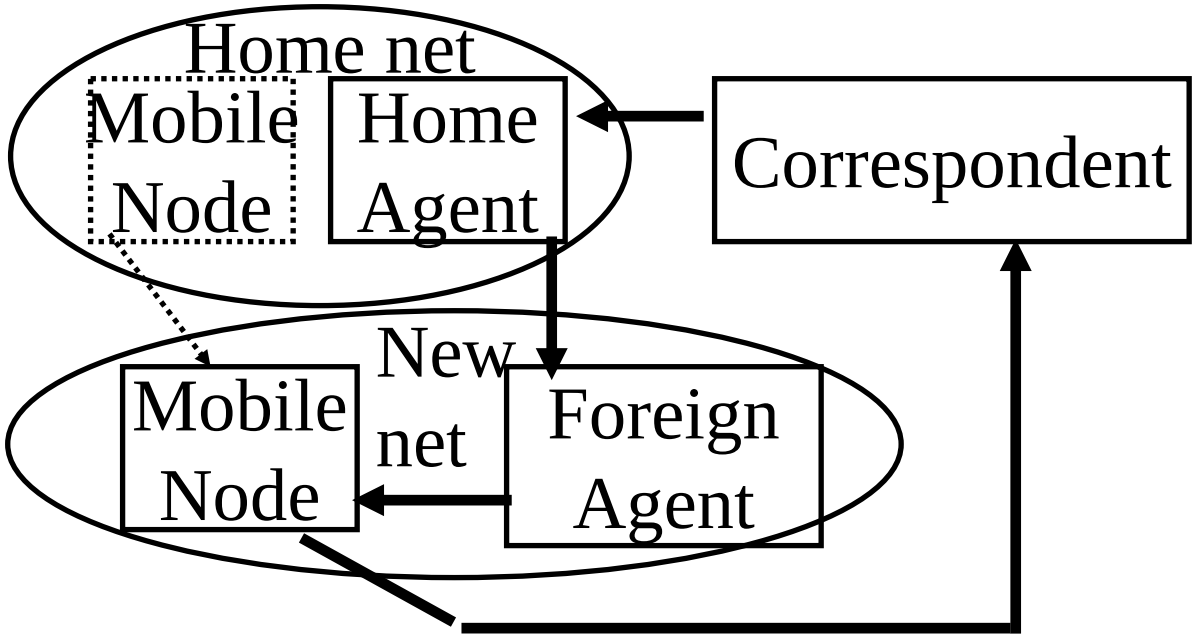


- We need:
  - An agent at a home office: Home Agent
  - An agent at a foreign office: Foreign Agent

Student Questions

©2025 Raj Jain

Mobile IP: Mechanisms







Student Questions

©2025 Raj Jain

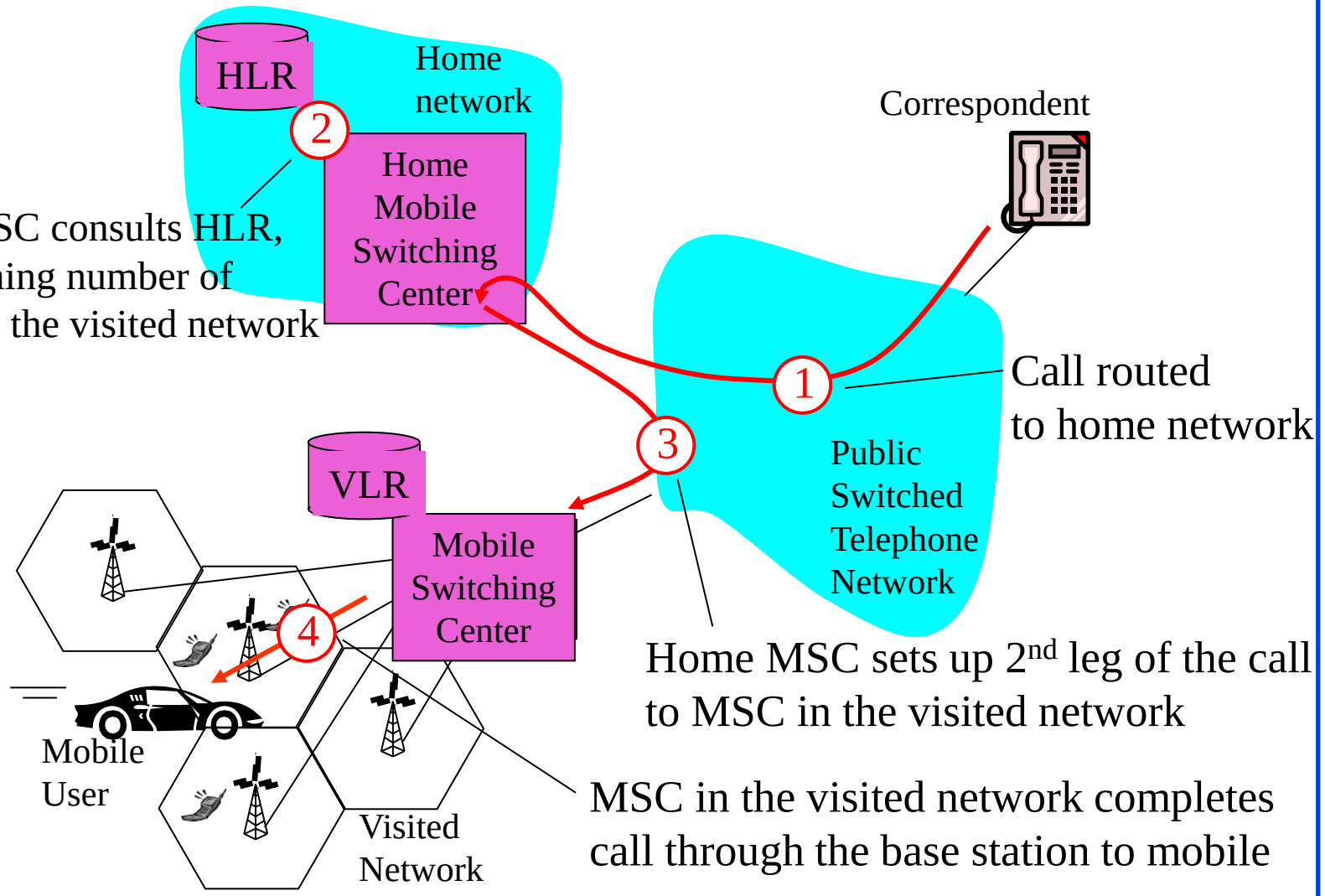
Mechanism (Cont.)

- 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

©2025 Raj Jain

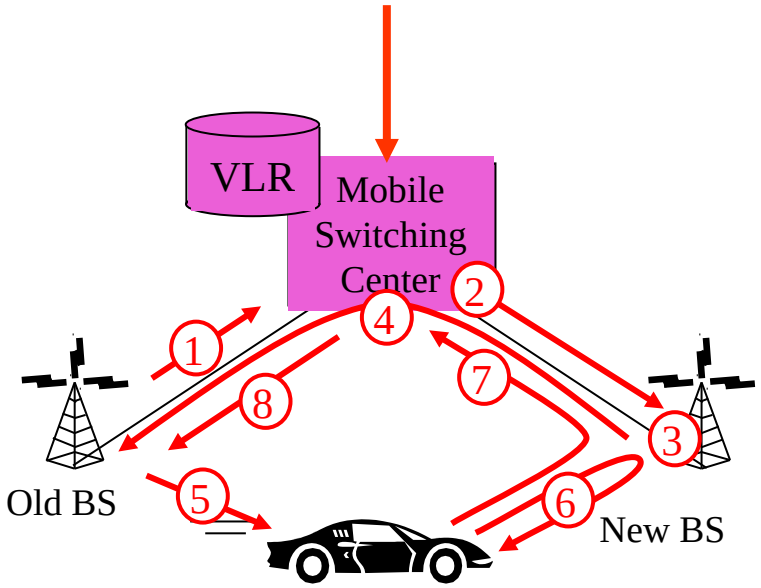
GSM: Routing to Mobile



Student Questions

©2025 Raj Jain

GSM: Handoff with Common MSC



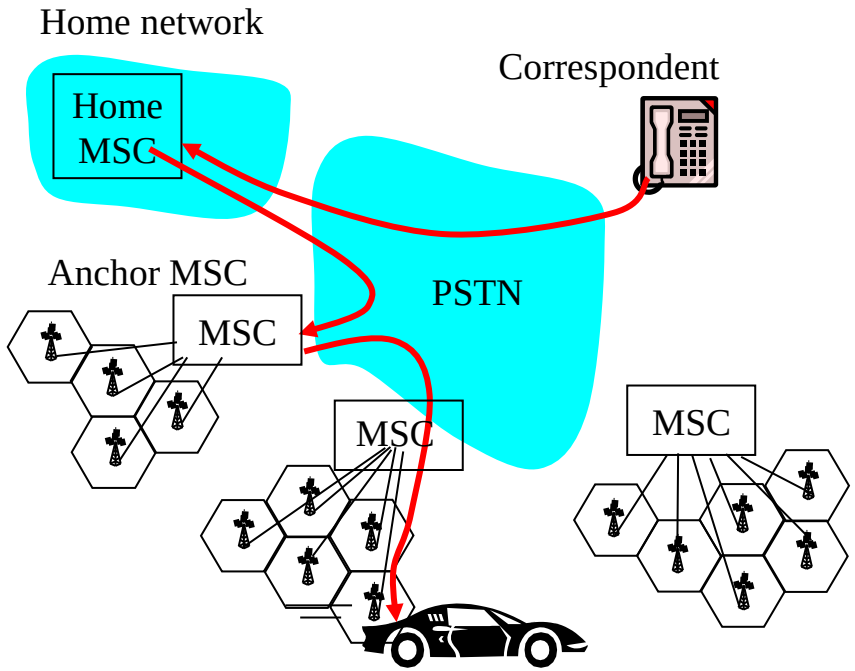
1. Old BS informs MSC of impending handoff, provides a list of 1^+ new BSs
2. MSC sets up a path (allocates resources) to new BS
3. New BS allocates radio channel for use by mobile
4. New BS signals MSC, old BS: ready
5. Old BS tells mobile: perform handoff to new BS
6. Mobile, new BS signal to activate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

8 MSC-old-BS resources released

Student Questions

©2025 Raj Jain

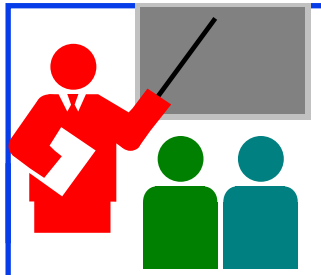
GSM: Handoff between MSCs



- *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

©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.

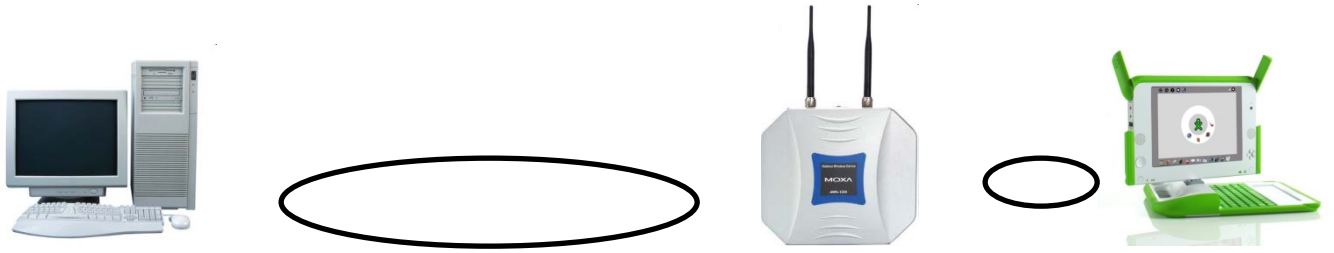
Student Questions

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

©2025 Raj Jain

Impact on Higher Layer Protocols

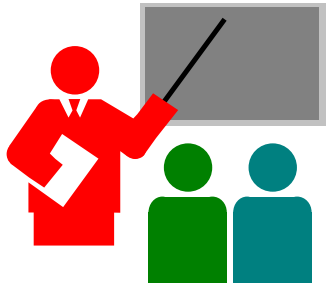
- Layered Architecture ⇒ Upper layers are independent of lower layers
- Wireless ⇒ High error rate ⇒ Frequent packet losses
  ⇒ Triggers TCP congestion control even if there is no overload
- TCP modifications:
  - Local Recovery: Link-level retransmissions and error correction
  - Wireless-aware TCP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



Student Questions

©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

End of Part 2

©2025 Raj Jain



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

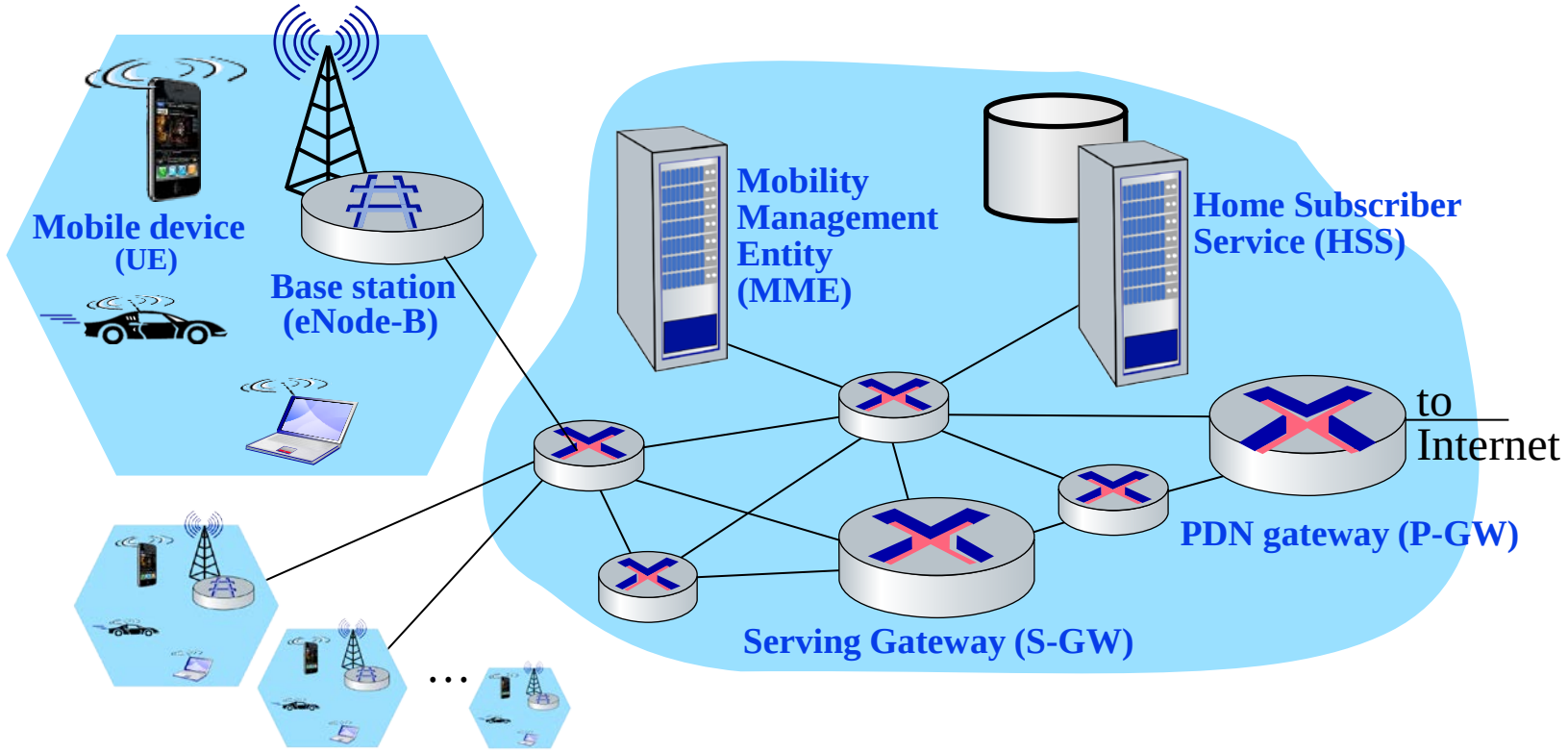
- Seamless connectivity and global roaming with smooth handovers
- ITU has approved **LTE-Advanced** as 4G (Oct 2010)

Student Questions

©2025 Raj Jain

LTE Architecture

- Evolved Packet Systems (EPS)



Student Questions

©2025 Raj Jain

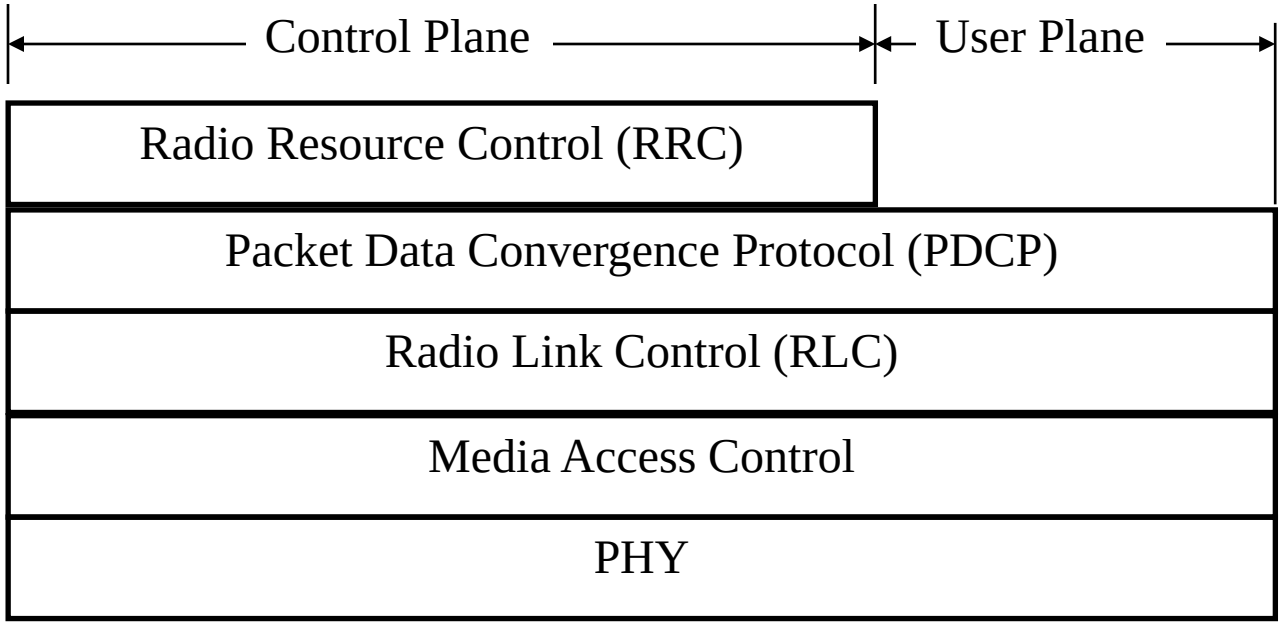
Evolved Packet System

- **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

©2025 Raj Jain

LTE Protocol Stack



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

Student Questions

©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

©2025 Raj Jain

Radio Link Control Layer

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

Student Questions

©2025 Raj Jain

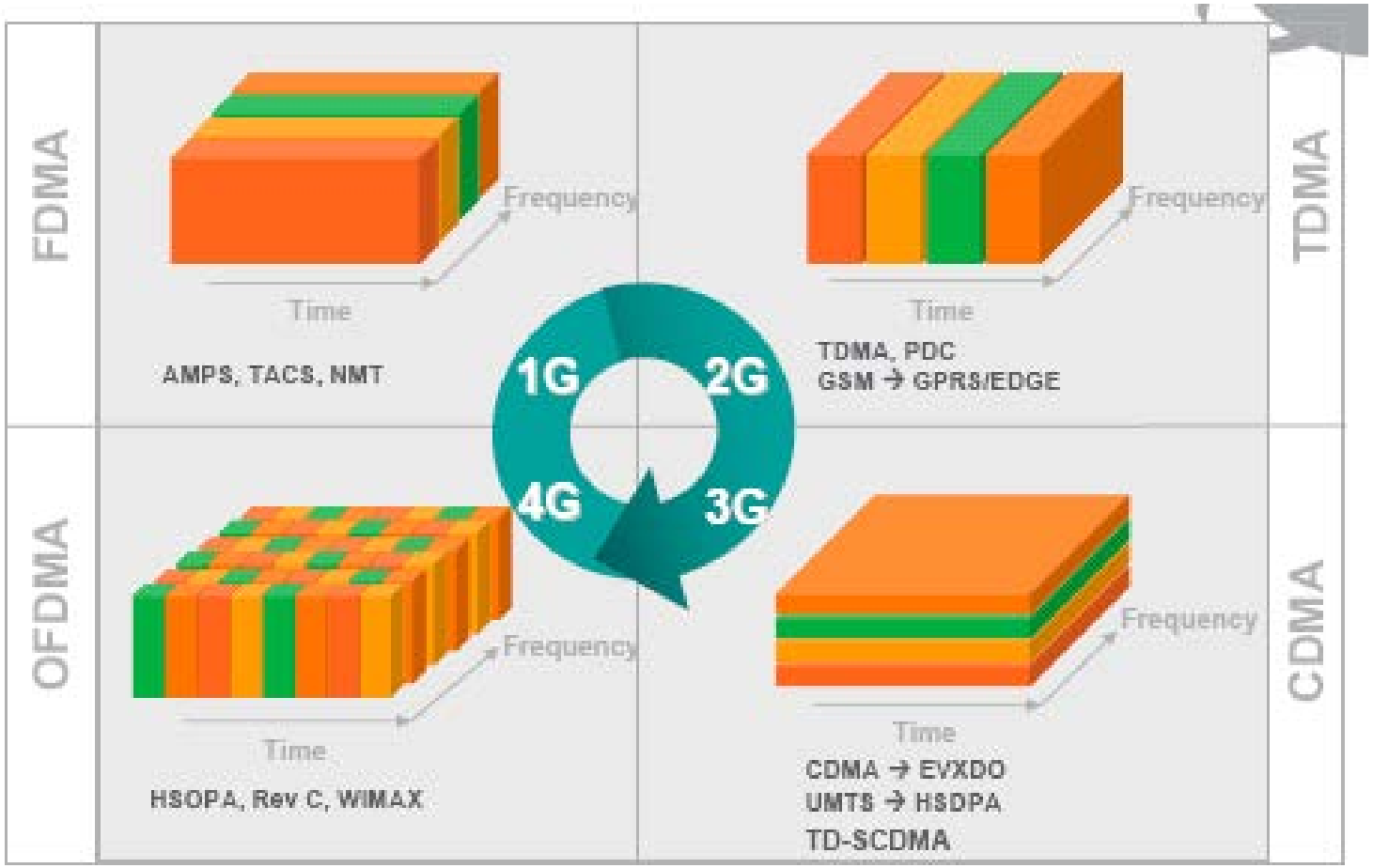
Media Access Control (MAC)

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

Student Questions

©2025 Raj Jain

Multiple Access Methods



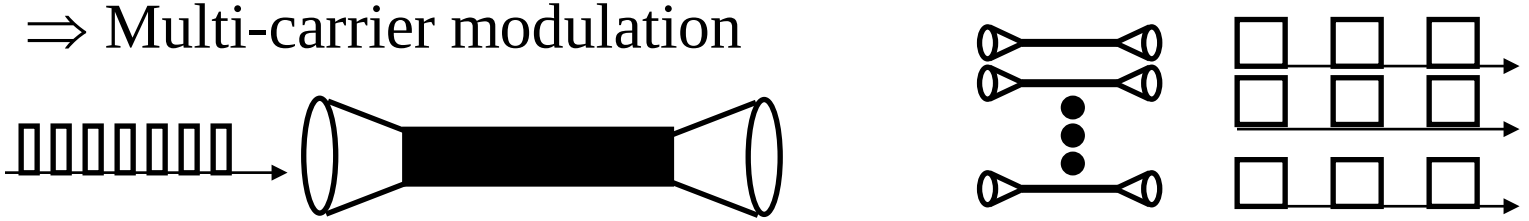
Source: Nortel

Student Questions

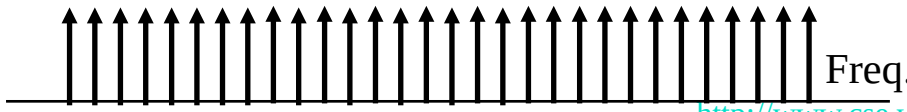
©2025 Raj Jain

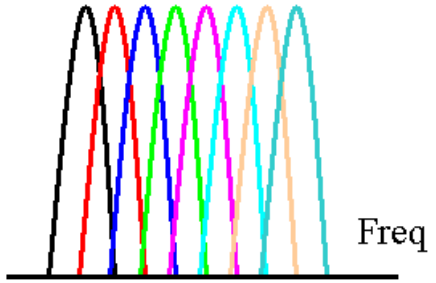
OFDM

- 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

©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

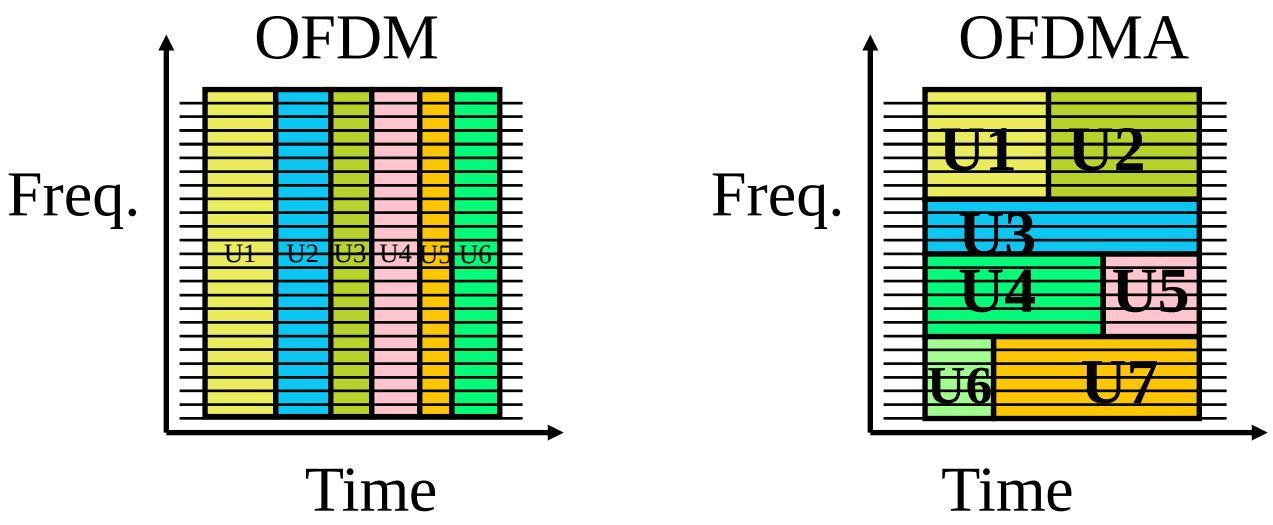


Student Questions

©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

©2025 Raj Jain

SC-FDMA

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

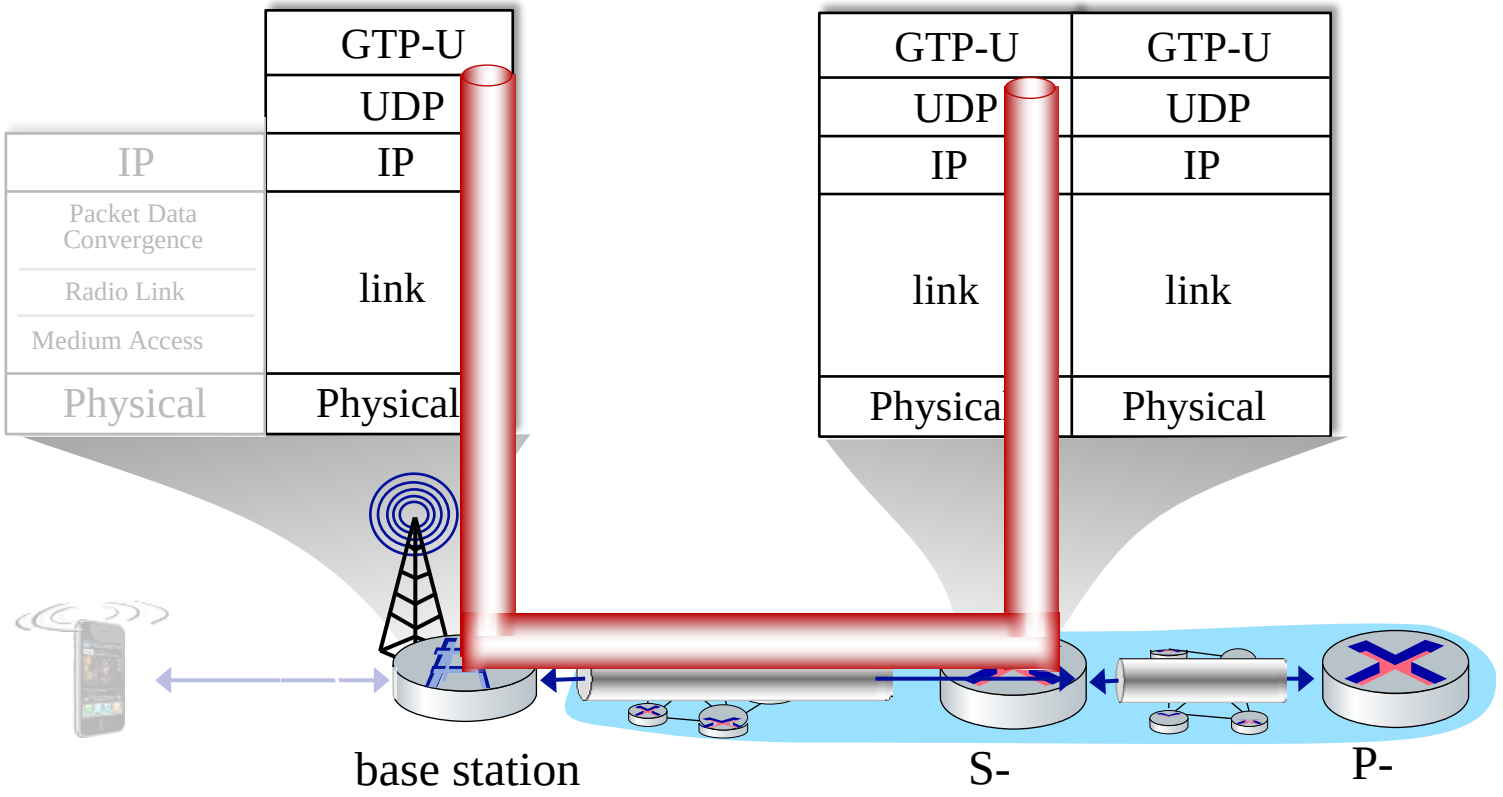


- Uses single carrier modulation and adds a cyclic prefix
- Single carrier ⇒ Not much variation in amplitude
  ⇒ Lower Peak-to-Average Power Ratio (PAPR)
  ⇒ Lower-cost Amplifiers
- Better for uplink because slight mis-synchronization among users does not affect the decoding significantly
- With OFDMA,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

Student Questions

GPRS Tunneling Protocol (GTP)

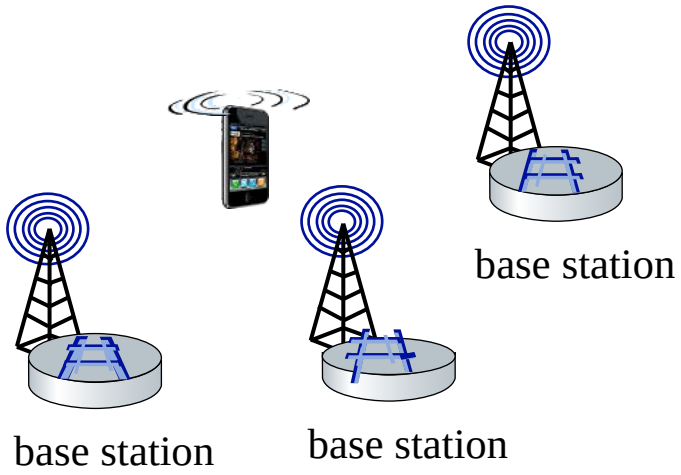
- **General Packet Radio Service (GPRS)** transfers data in 2G/3G/4G networks. GTP uses UDP tunneling to transfer data over IP.



Student Questions

©2025 Raj Jain

UE Association with a BS

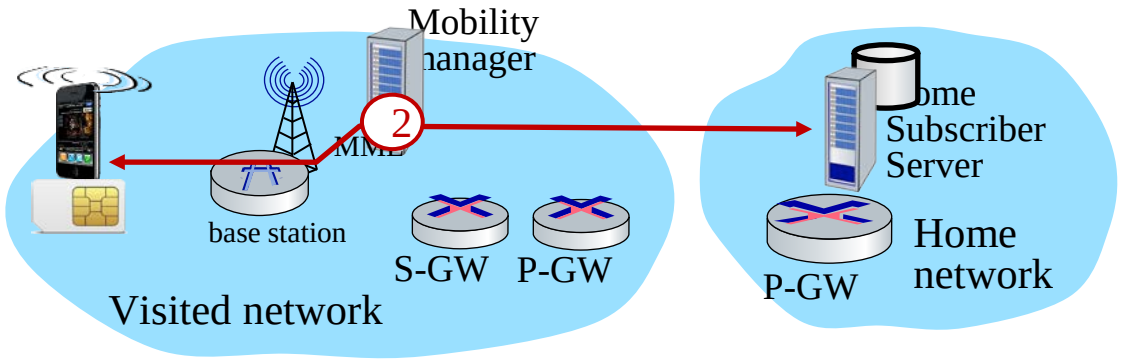


- Each BS broadcasts a primary synch signal every 5ms
- Mobile listens to multiple such broadcasts
  Finds channel bandwidth, configuration, carrier info
- Mobile finds a BS from its compatible carrier and associates with it
- BS authenticates the mobile, sets up all components of the control plane and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

Student Questions

©2025 Raj Jain

Configuring LTE Control-Plane Elements

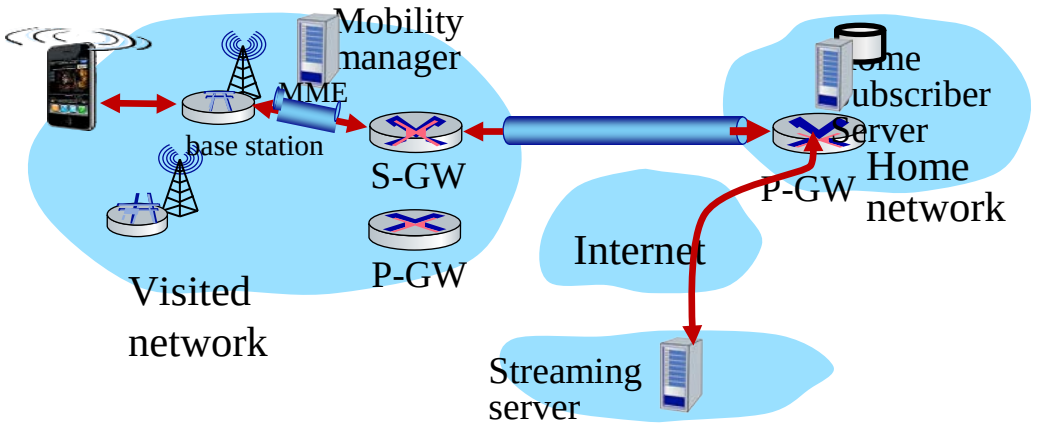


- Mobile communicates with local MME via BS control-plane channel
- MME uses mobile's IMSI info to contact mobile's home HSS
  - Retrieve authentication, encryption, network service information
  - Home HSS knows mobile now resident in the visited network
- BS, mobile select parameters for BS-mobile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

Student Questions

Configuring Data-Plane Tunnels for Mobile

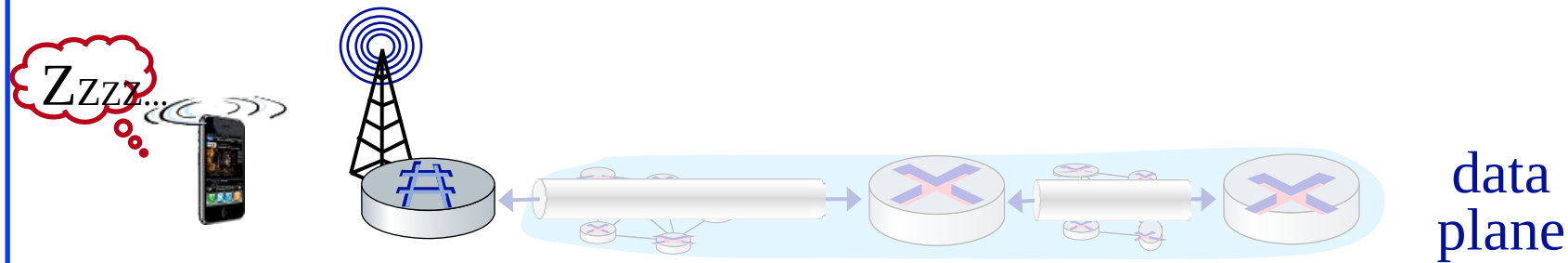
- S-GW to BS Tunnel: when mobile changes base stations, change the endpoint IP address of the tunnel
- S-GW to Home P-GW Tunnel: implementation of indirect routing
- Tunneling via GTP (GPRS tunneling protocol): mobile's datagram to streaming server encapsulated using GTP inside UDP, inside a datagram



Student Questions

©2025 Raj Jain

LTE Mobile Sleep Modes

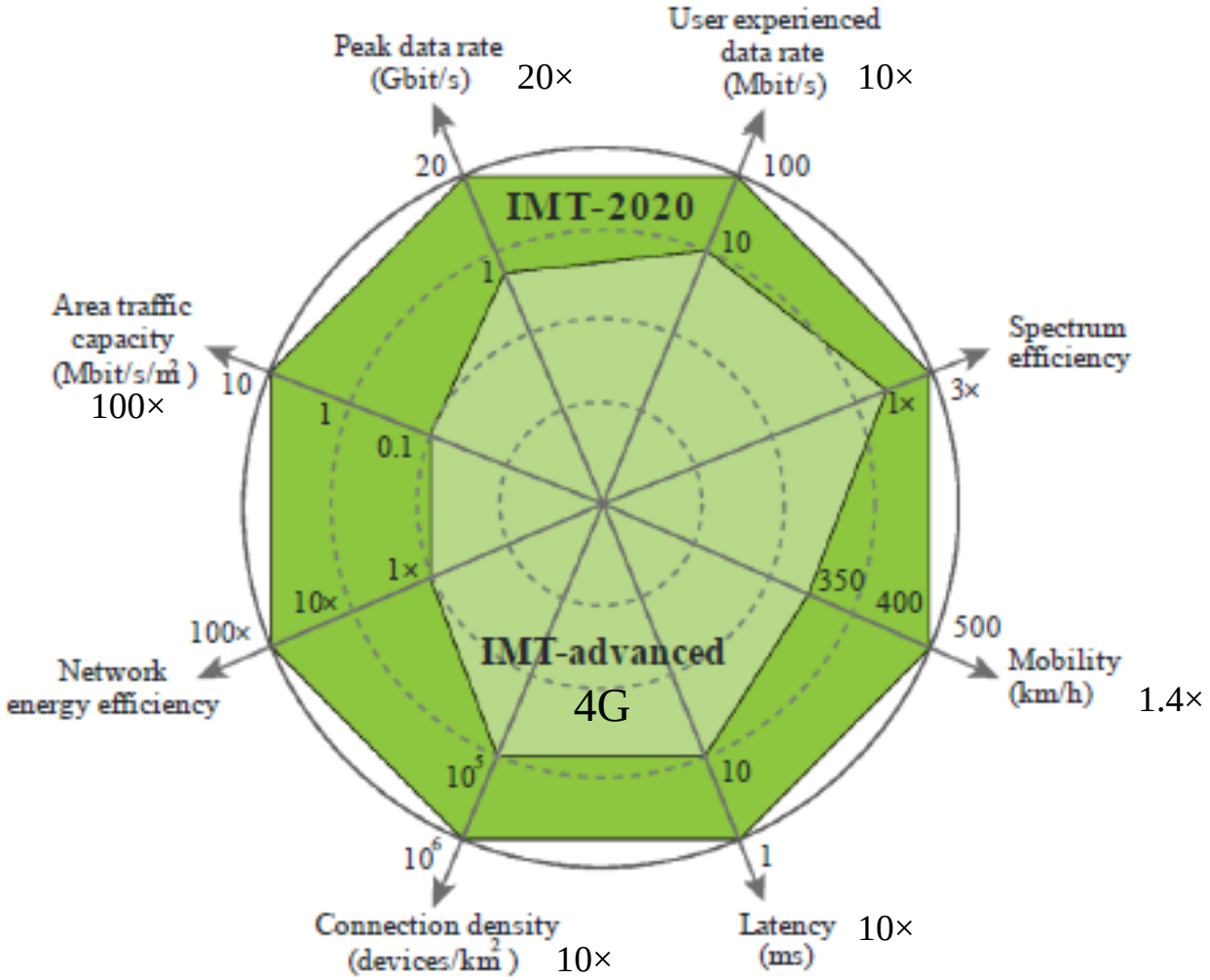


- LTE mobiles put the radio to sleep to conserve battery
- Light Sleep: Wake up periodically (100 ms). Check downstream transmissions to see if there are any calls.
- Deep Sleep: 5-10s of inactivity. It may be found that the BS has changed. Will re-establish association with a new BS.

Student Questions

©2025 Raj Jain

5G Definition



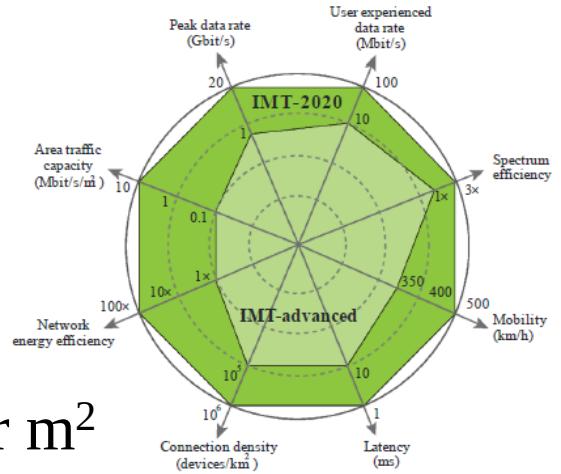
Ref: ITU-R Recommendation M.2083-0, "IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond," Sep. 2015, 21 pp., https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf

Student Questions

©2025 Raj Jain

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

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

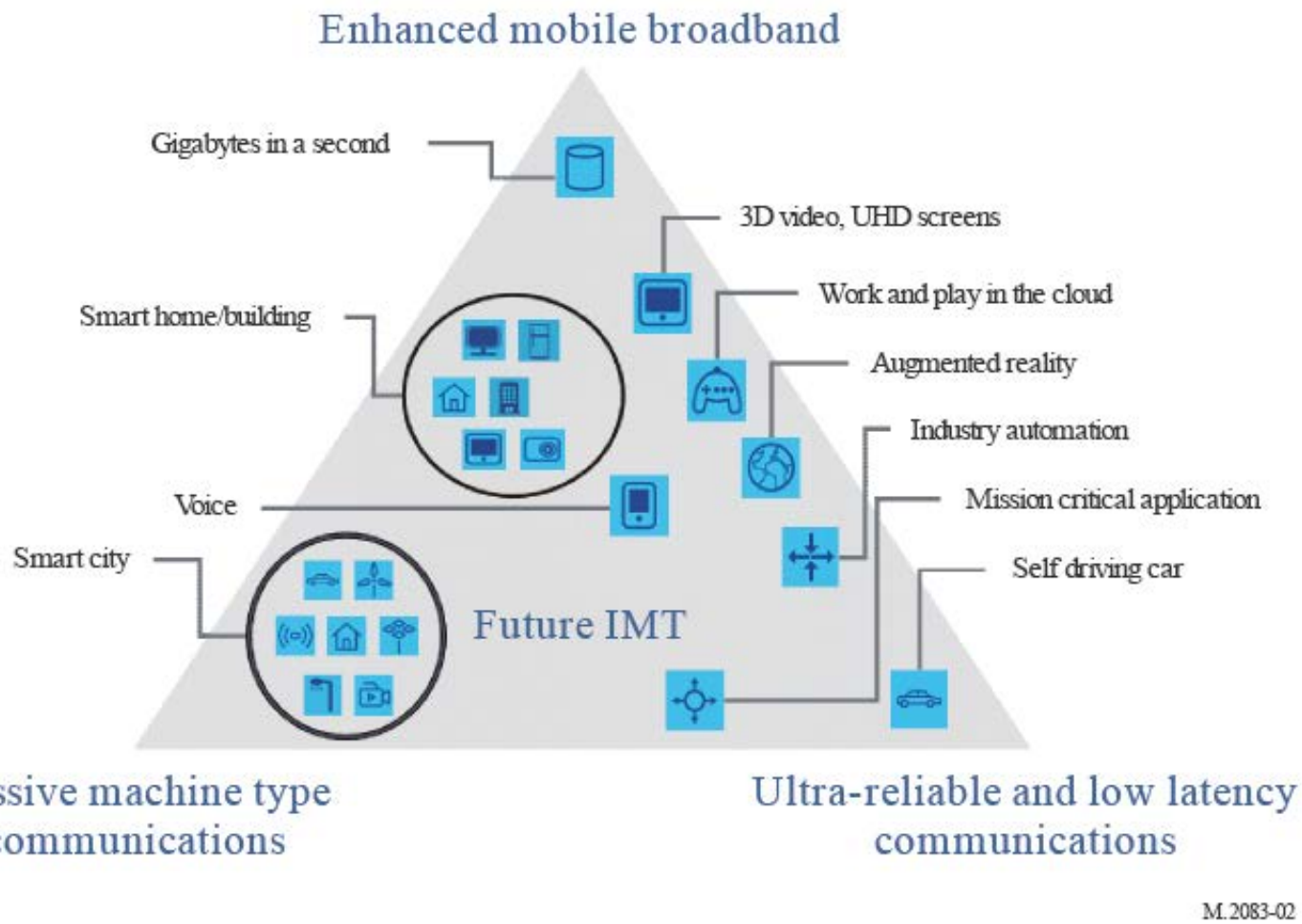
Three Key Application Areas:

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

©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

©2025 Raj Jain

Above 6 GHz (Cont)

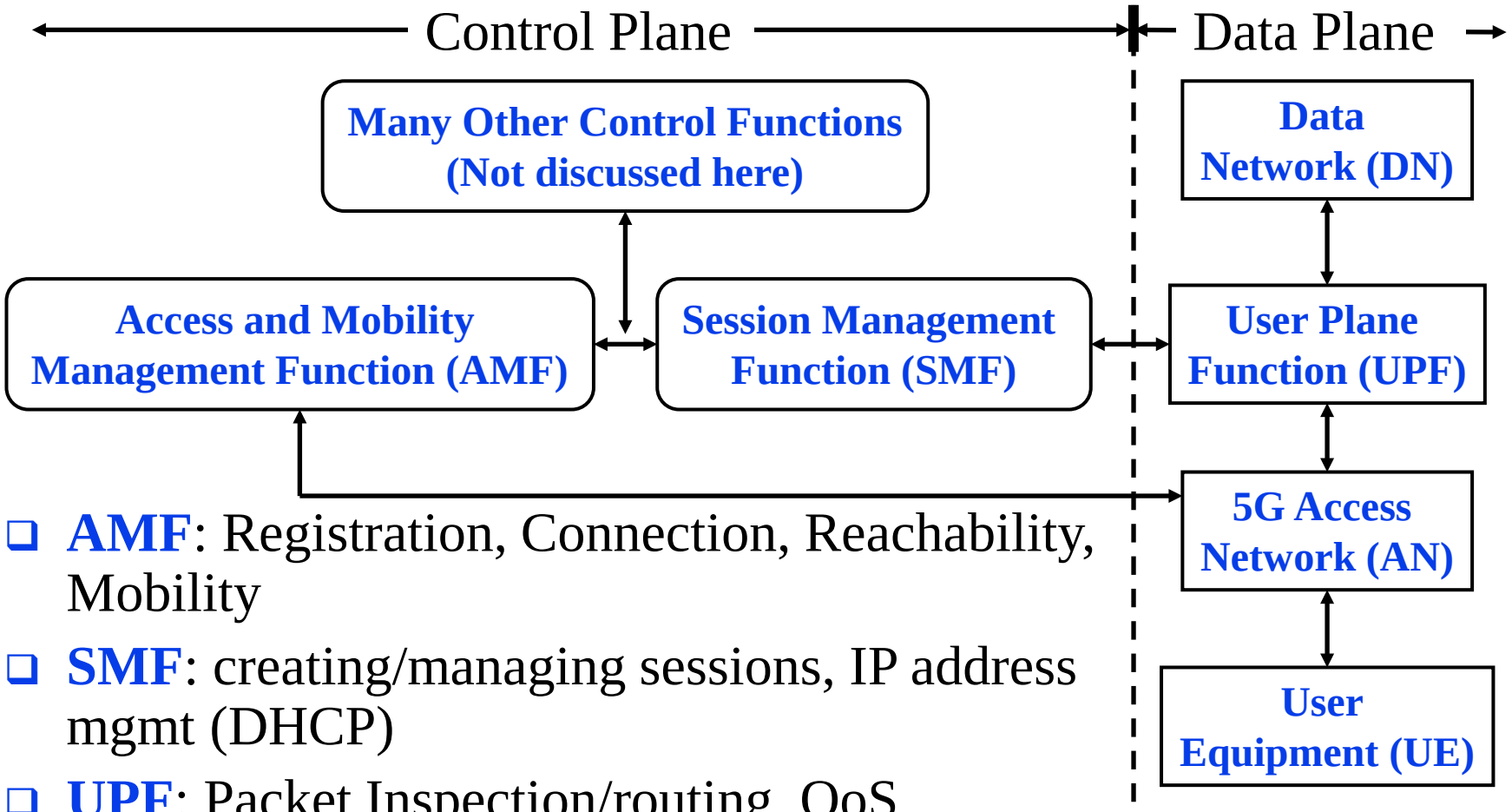
- 100s MHz ⇒ **Multi-gigabit** data rates
- **Dense spatial reuse**
- Lower latency
- Need analog beamforming with a narrow beam width
- **Adaptive beam steering** and switching to avoid blockage from hand, body, or foliage
- Need different antenna configurations in the mobile
- **Directional antennas**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

Student Questions

©2025 Raj Jain

5G Core Architecture

- Clear separation of control plane and data plane

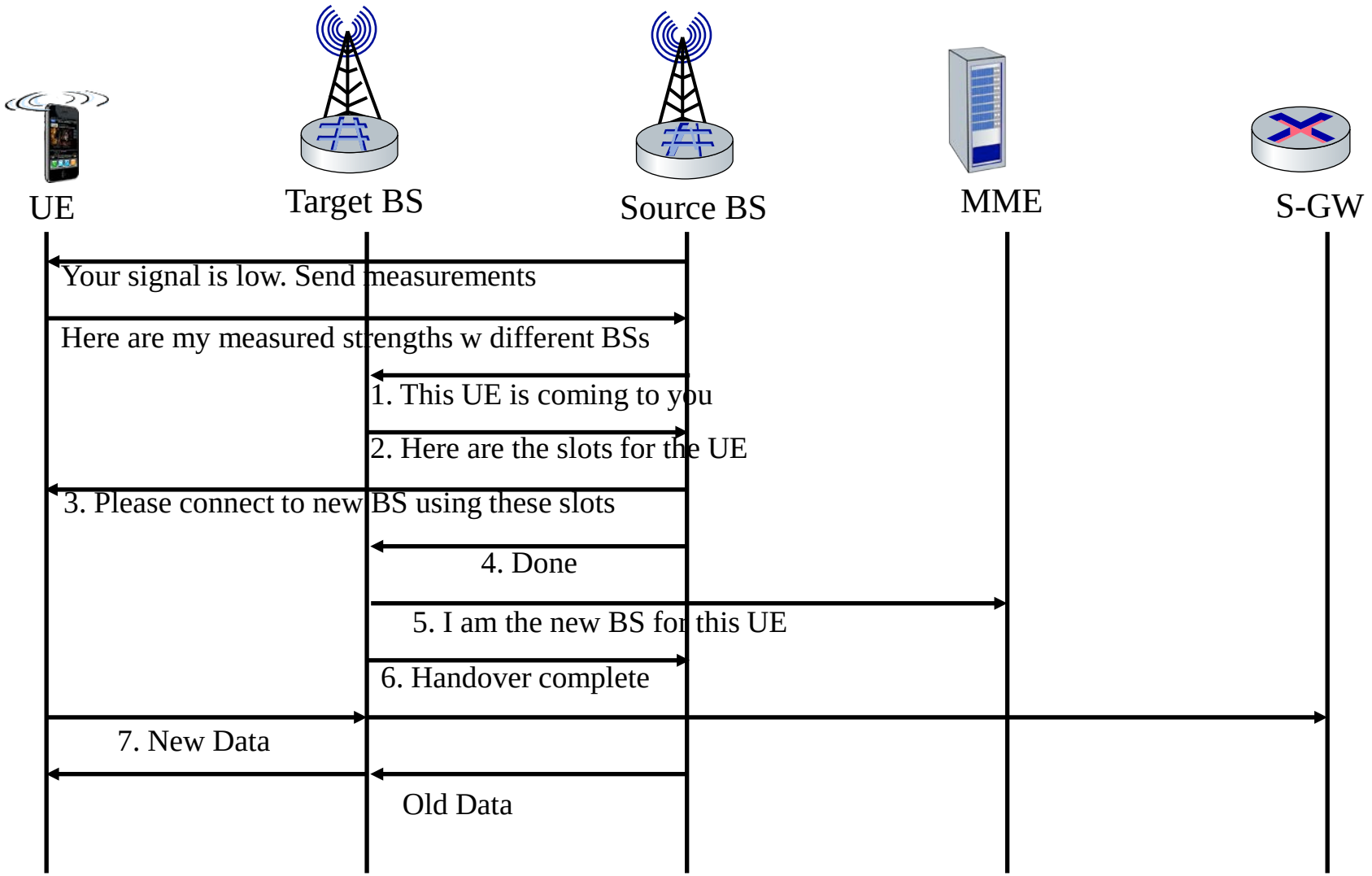


- **AMF**: Registration, Connection, Reachability, Mobility
- **SMF**: creating/managing sessions, IP address mgmt (DHCP)
- **UPF**: Packet Inspection/routing, QoS,

Student Questions

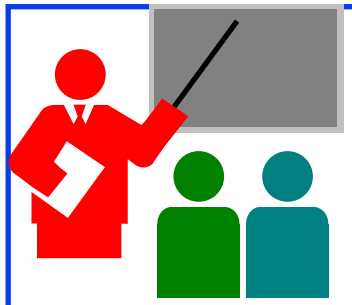
©2025 Raj Jain

Handover: In the Same LTE



Student Questions

©2025 Raj Jain



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

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

©2025 Raj Jain

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