Wireless and Mobile Networks

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@wustl.edu

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

http://www.cse.wustl.edu/~jain/cse473-10/

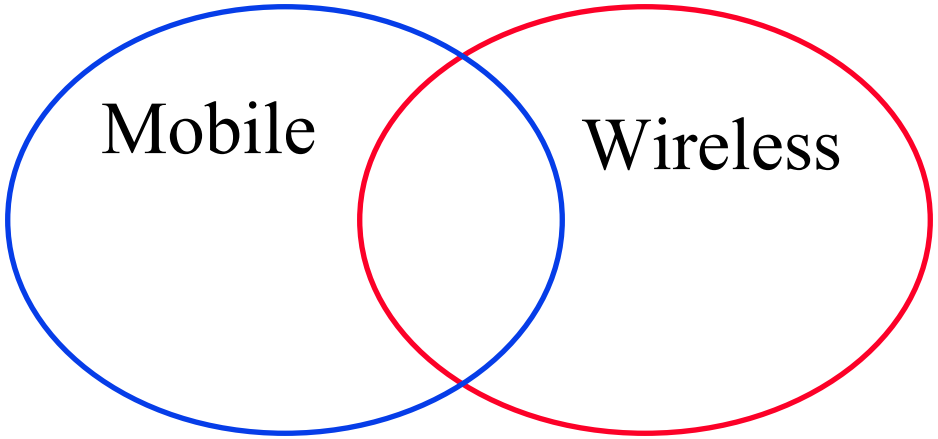
1. Wireless issues: Interference, CDMA, Hidden nodes
2. IEEE 802.11 (Wi-Fi)
3. Other Networks: Bluetooth, WiMAX, Cellular
4. Mobility: Mobile IP and Mobility in Cellular Networks

Note: This class lecture is based on Chapter 6 of the textbook (Kurose and Ross) and the figures provided by the authors.

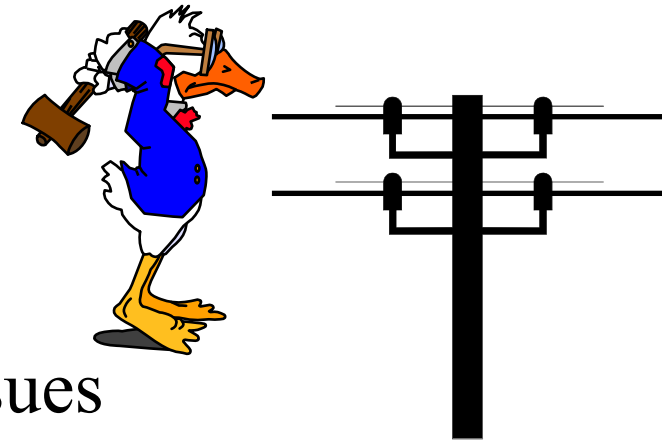
IEEE 802.11 Wi-Fi

1. Mobile vs. Wireless
2. Wireless Networking Challenges
3. Code Division Multiple Access
4. IEEE 802.11 Wireless LAN PHYs
5. IEEE 802.11 MAC
6. IEEE 802.11 Architecture
7. 802.11 Frame Format and Addressing
8. 802.11 Rate Adaptation and Power Management

Mobile vs Wireless

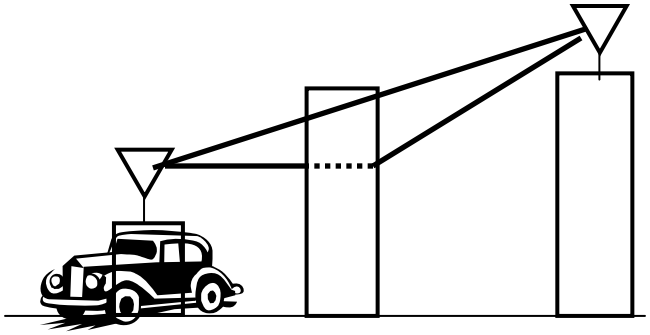


- Mobile vs Stationary
- Wireless vs Wired
- Wireless ⇒ media sharing issues
- Mobile ⇒ routing, addressing issues

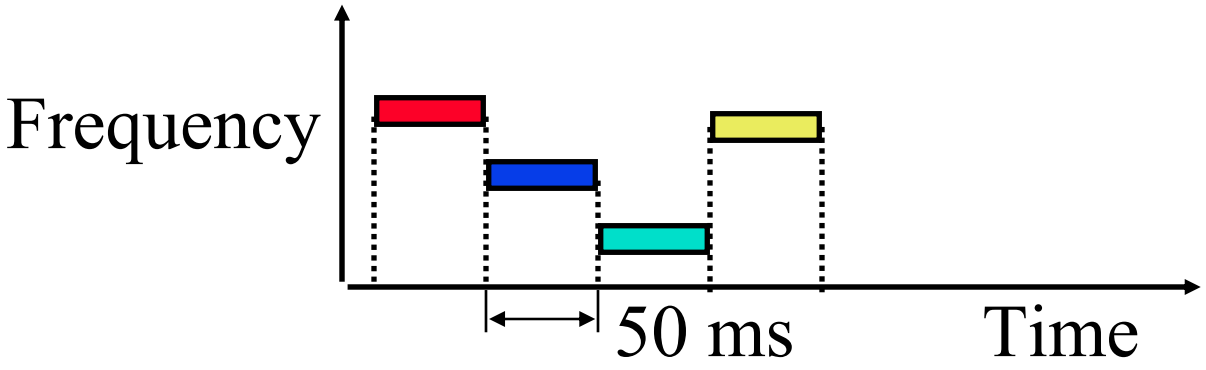


Wireless Networking Challenges

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 WiFi base station vs. 100 kW TV tower
5. Unlicensed spectrum ⇒ Media Access Control
6. Limited spectrum ⇒ Limited data rate
   Original WiFi (1997) was 2 Mbps.
   New standards allow up to 200 Mbps
7. No physical boundary ⇒ Security
8. Mobility ⇒ Seamless handover

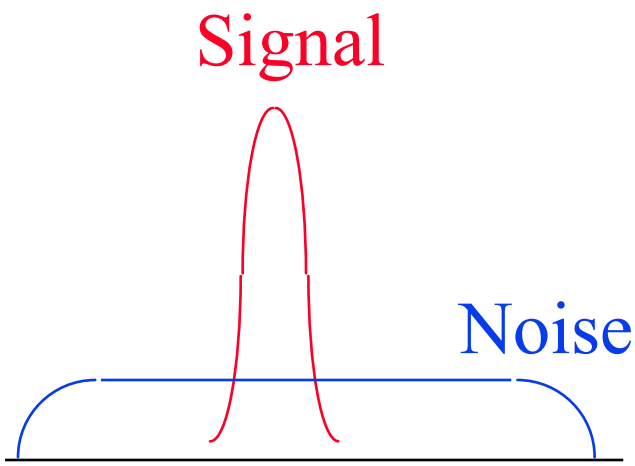


Frequency Hopping Spread Spectrum

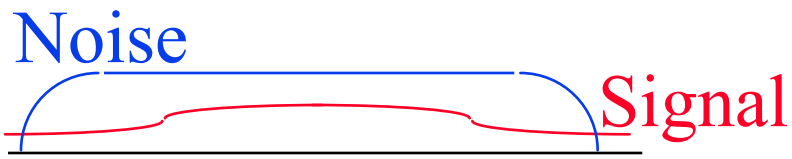


- Pseudo-random frequency hopping
- Spreads the power over a wide spectrum
  $\Rightarrow$ Spread Spectrum
- Developed initially for military
- Patented by actress Hedy Lamarr (1942)
- Narrowband interference can't jam

Spectrum

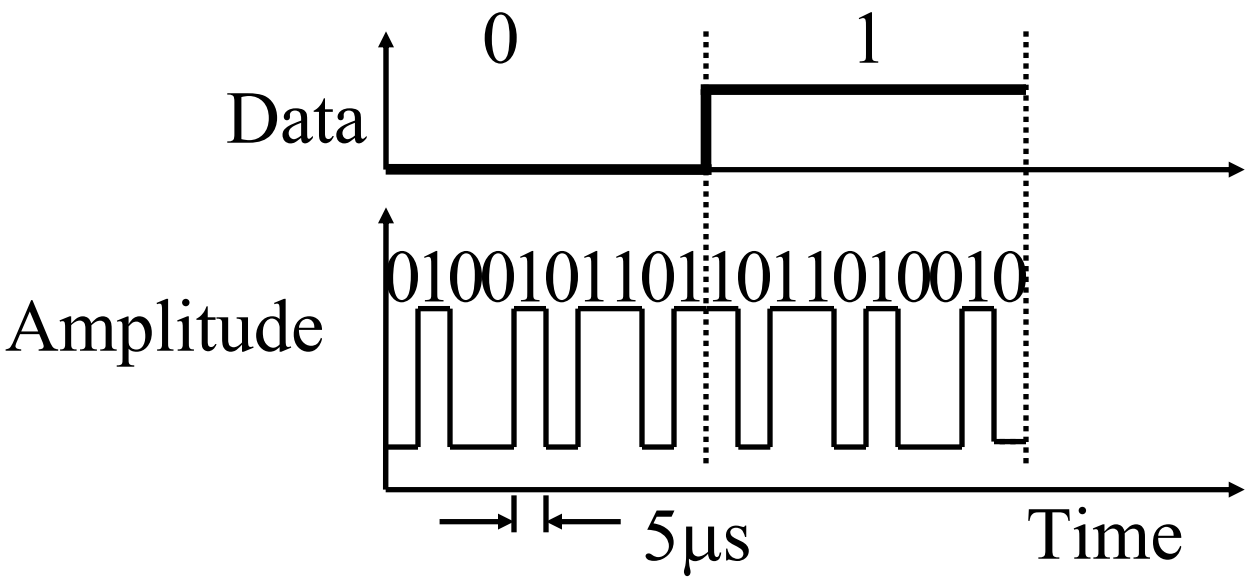


(a) Normal



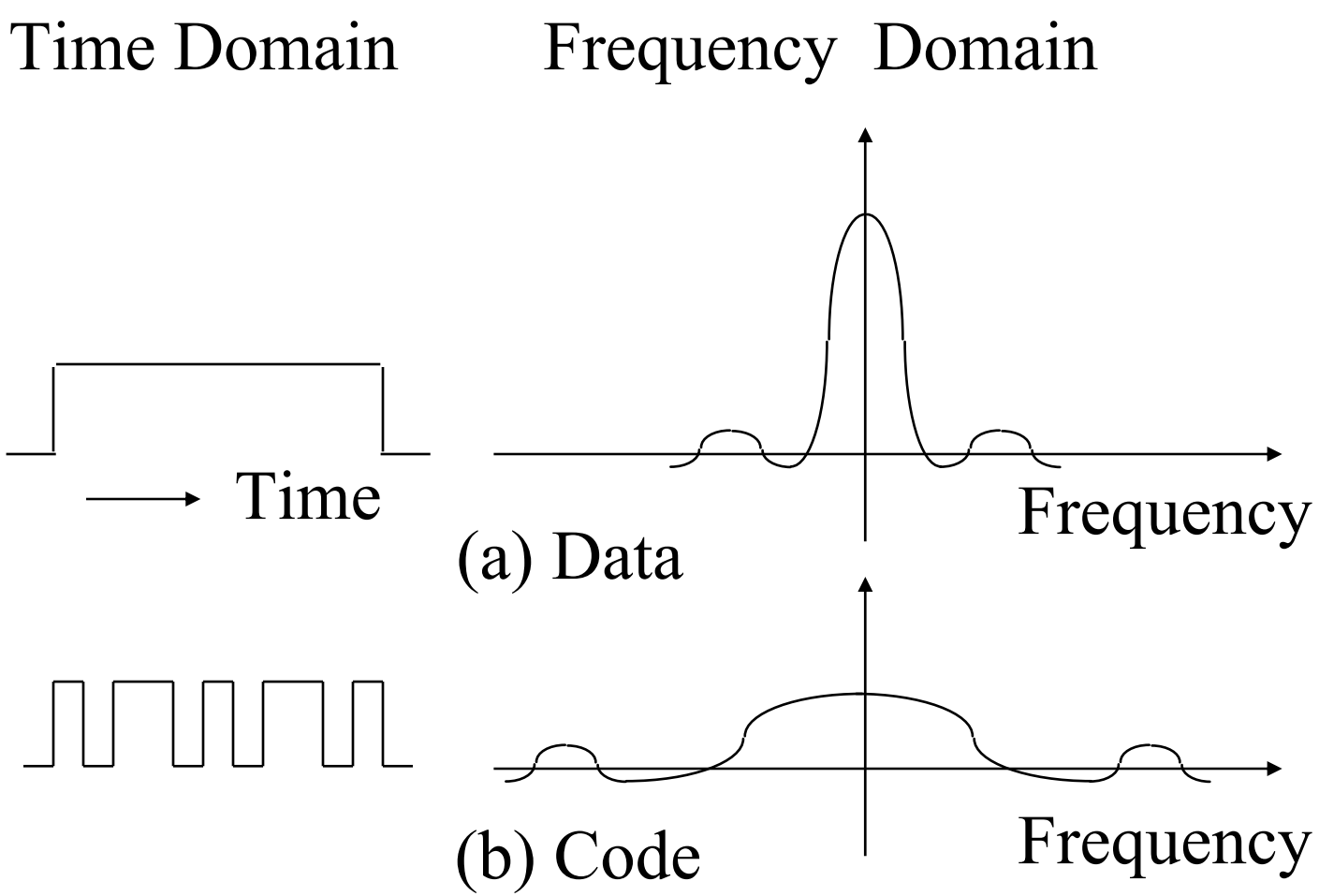
(b) Frequency Hopping

Direct-Sequence Spread Spectrum CDMA

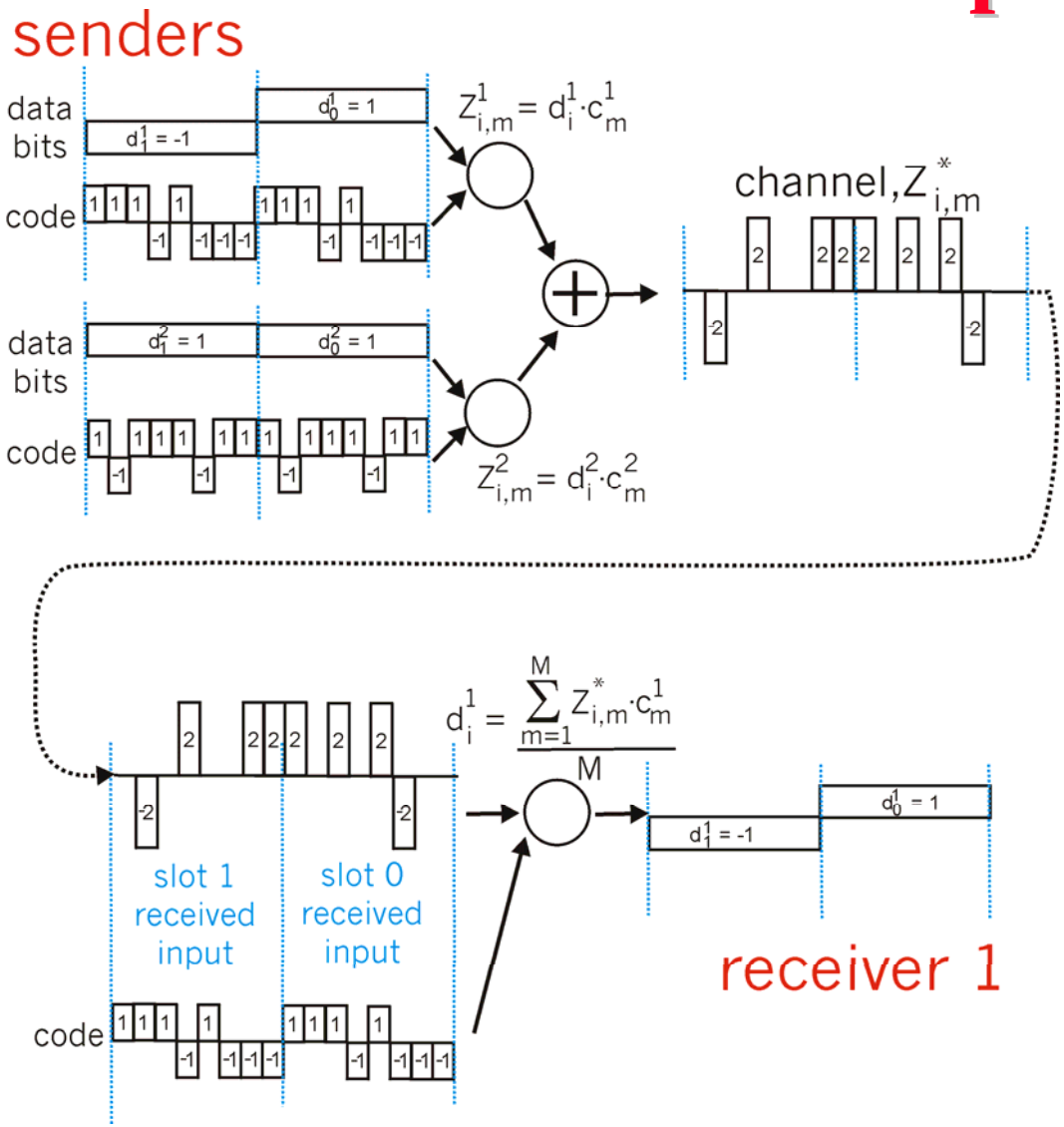


- Spreading factor = Code bits/data bit, 10-100 commercial (Min 10 by FCC), 10,000 for military
- Signal bandwidth >10 × data bandwidth
- Code sequence synchronization
- Correlation between codes ⇒Interference⇒Orthogonal

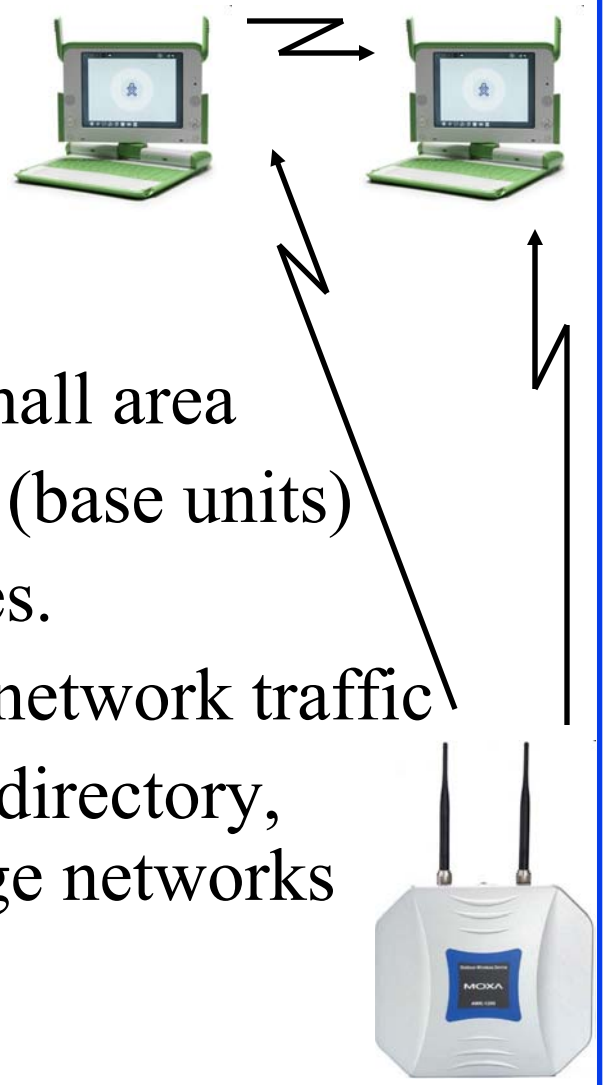
DS Spectrum


Time Domain
Frequency Domain
Time
Frequency
(a) Data
(b) Code
Frequency

Two Sender CDMA Example

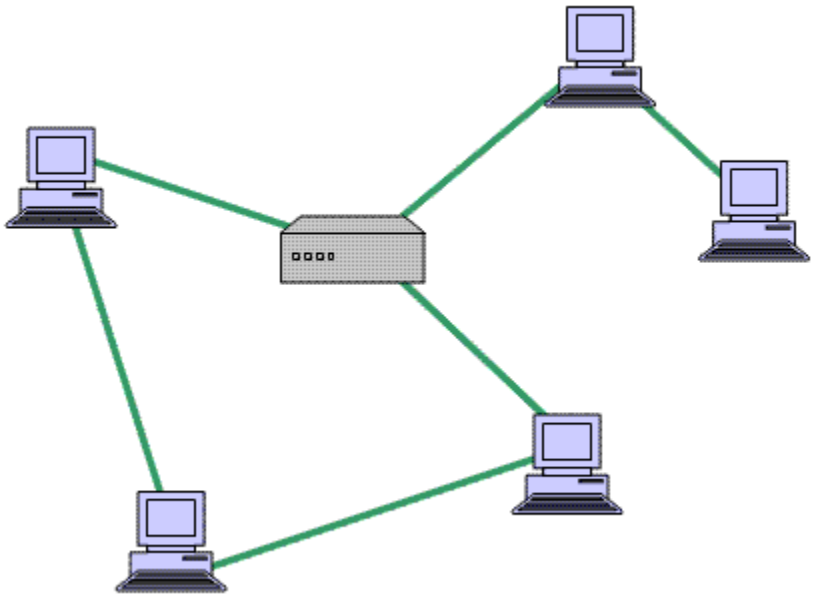


Peer-to-Peer or Base Stations?



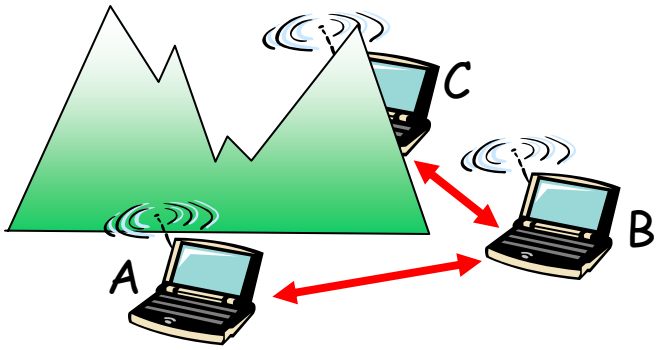
- Ad-hoc (Autonomous) Group:
  - Two stations can communicate
  - All stations have the same logic
  - No infrastructure, Suitable for small area
- Infrastructure Based: Access points (base units)
  - Stations can be simpler than bases.
  - Base provide connection for off-network traffic
  - Base provides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

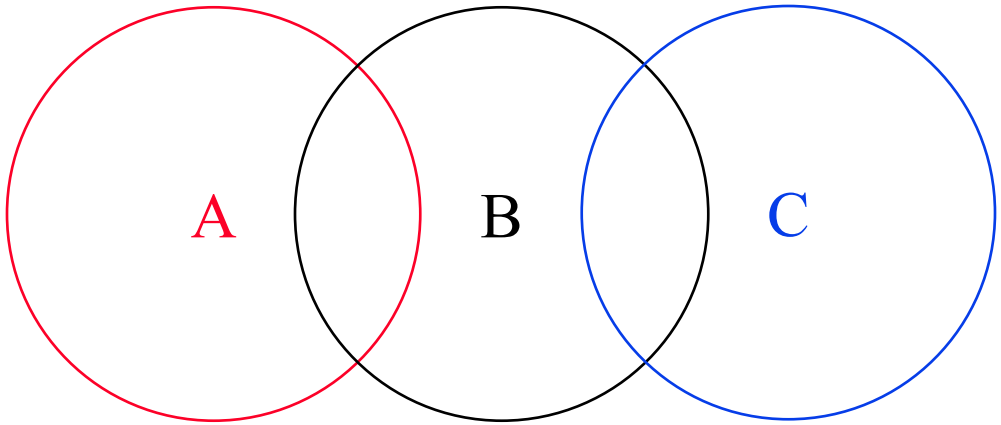
Single-Hop vs. Multi-Hop



- Infrastructure-based multi-hop: Mesh
- Ad-Hoc Multi-hop: Mobile Ad-hoc Network (MANET)

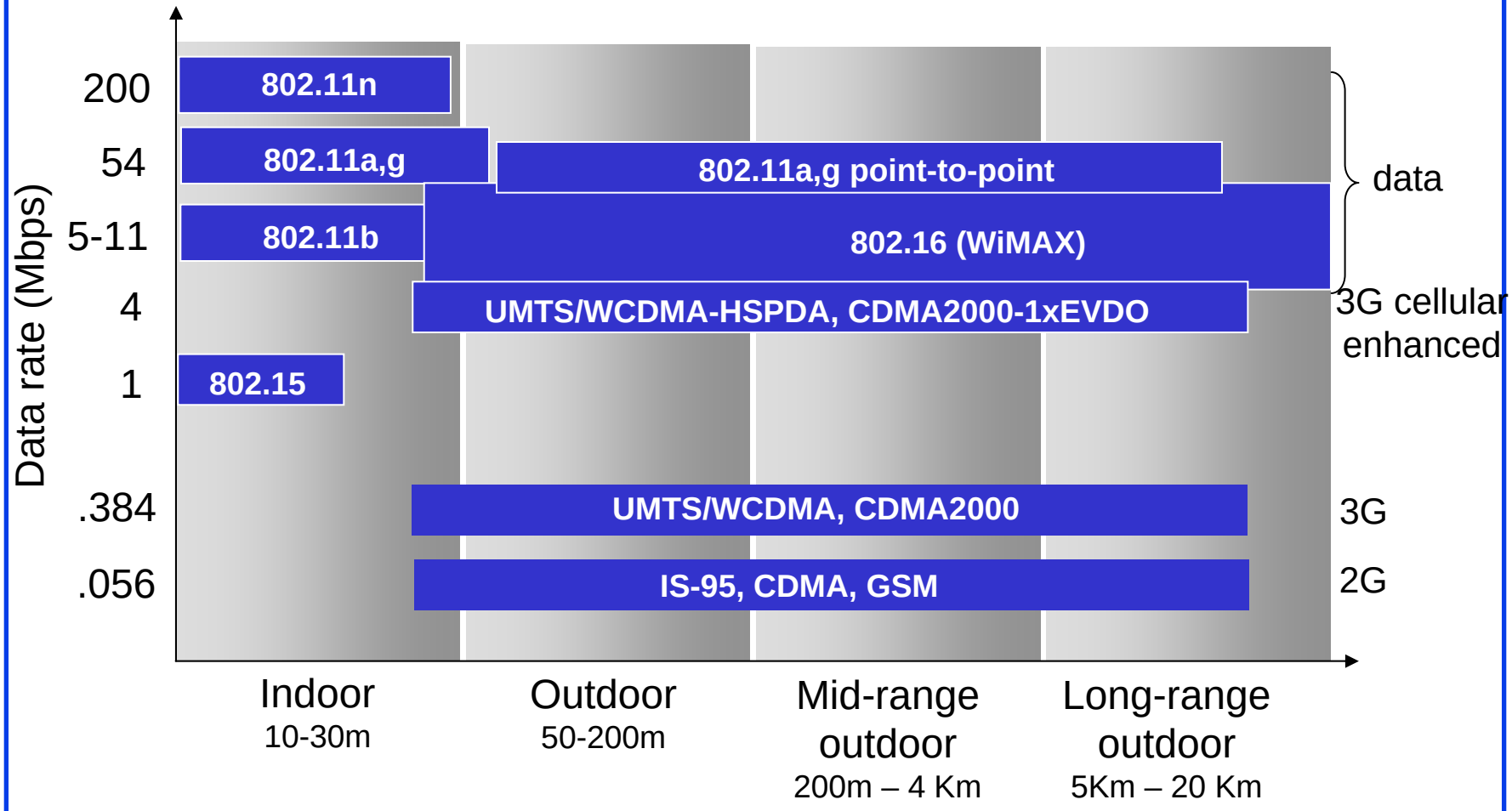
Hidden Node Problem





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

Characteristics of selected wireless standards



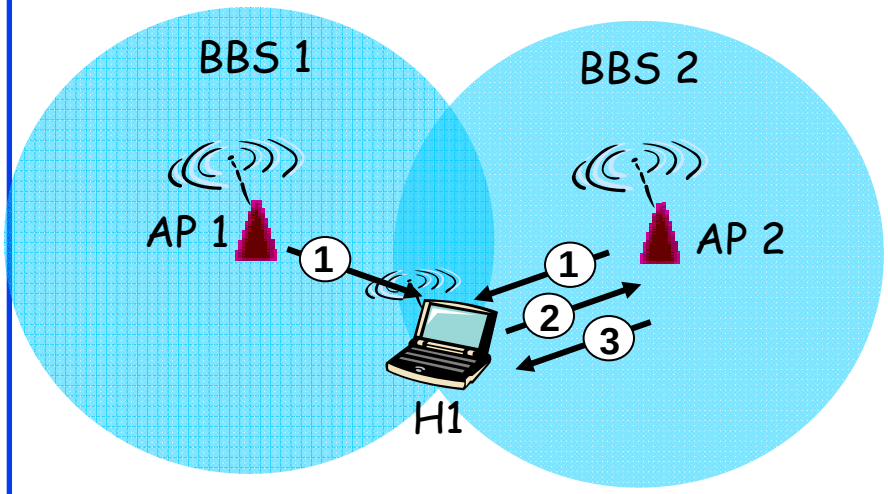
IEEE 802.11 Wireless LAN PHYs

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

802.11: Channels and Association

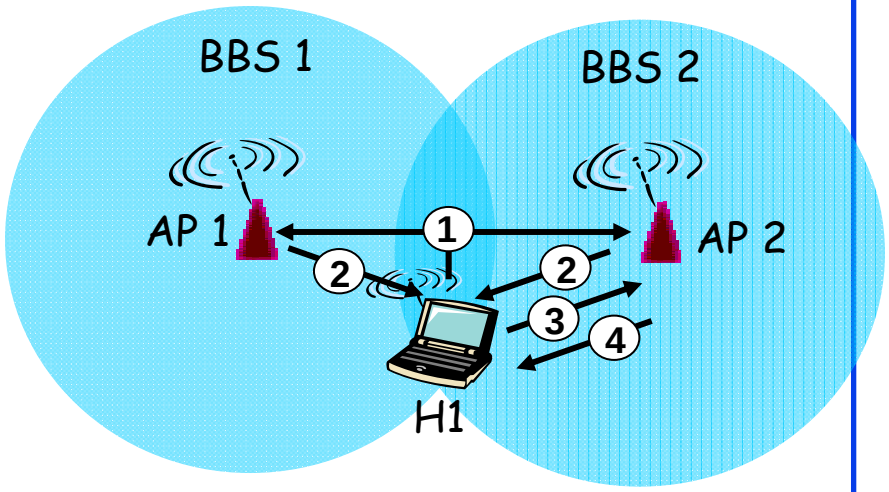
- 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
  - Access Point (AP) admin chooses frequency for AP
  - Interference possible: If two APs use the same channel
- Host must *associate* with an AP
  - Scans channels, listening for *beacon frames* containing AP's name (SSID) and MAC address
  - Selects AP to associate with
  - May perform authentication
  - Will typically run DHCP to get IP address in AP's subnet

802.11: Passive/Active Scanning



Passive Scanning:

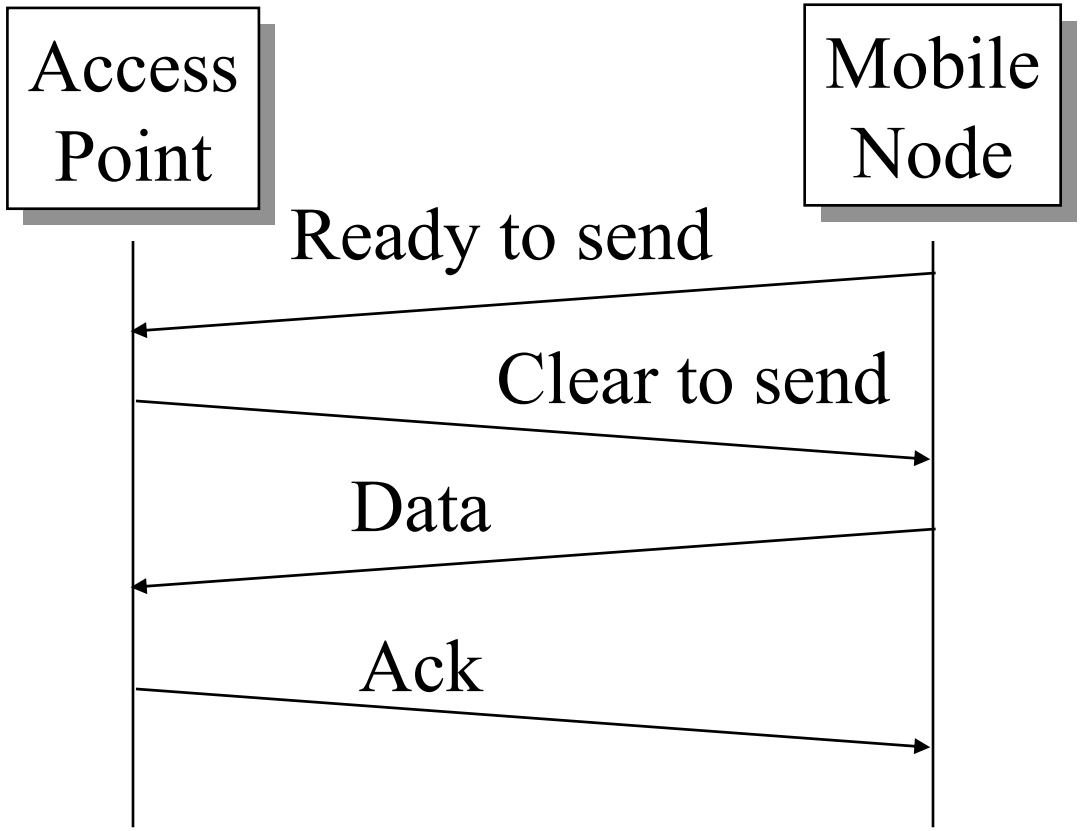
(1) Beacon frames sent from APs
(2) Association Request frame sent: H1 to selected AP
(3) Association Response frame sent: selected AP to H1



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

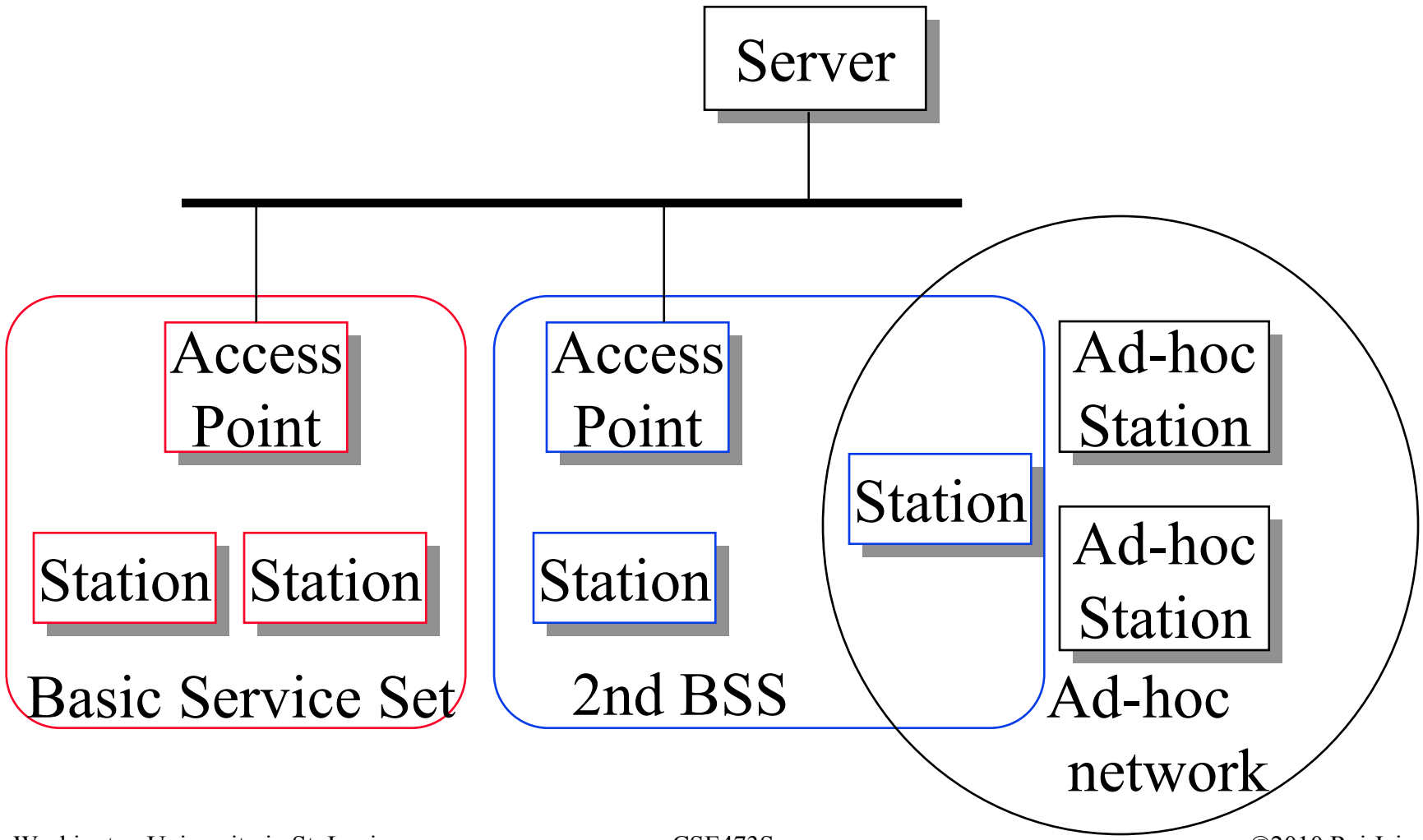
4-Way Handshake



IEEE 802.11 MAC

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

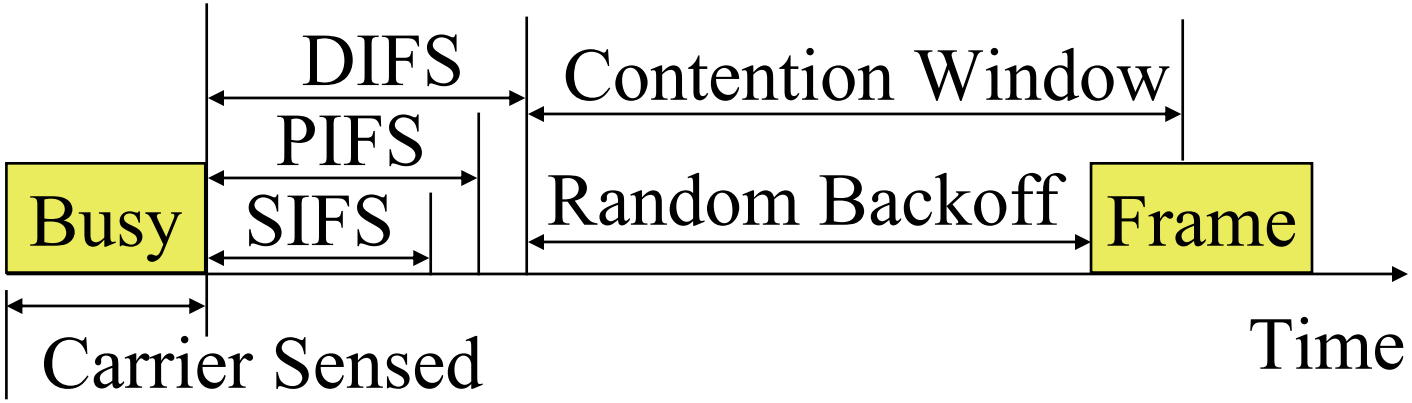
IEEE 802.11 Architecture



Architecture (Cont)

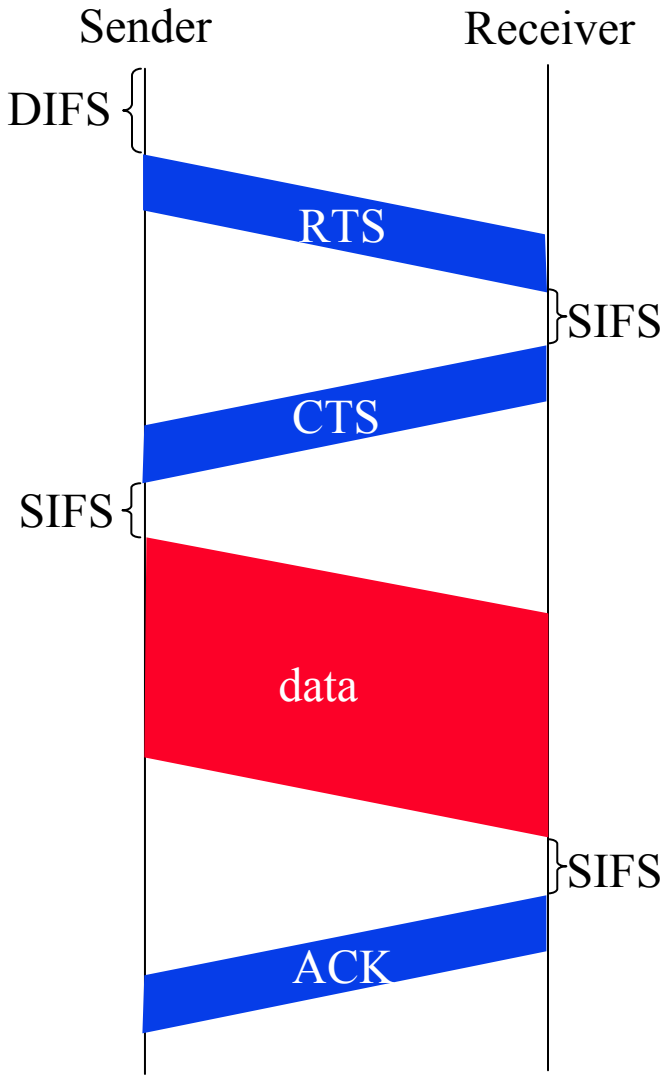
- Basic Service Area (BSA) = Cell
- Each BSA may have several wireless LANs
- Extended Service Area (ESA) = Multiple BSAs interconnected via Access Points (AP)
- Basic Service Set (BSS)
  = Set of stations associated with an AP
- Extended Service Set (ESS)
  = Set of stations in an ESA
- Ad-hoc networks coexist and interoperate with infrastructure-based networks.

IEEE 802.11 Priorities

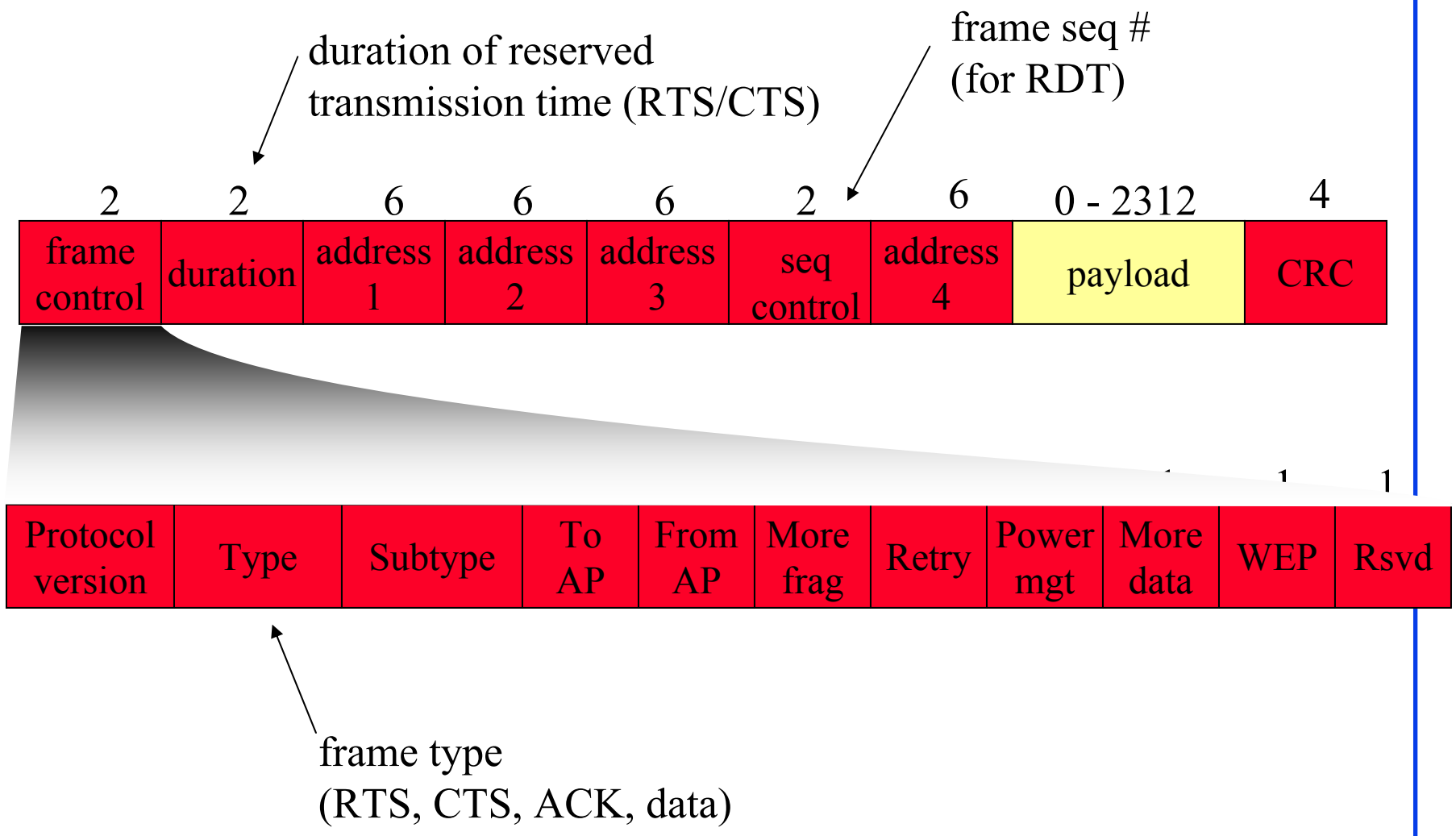


- Initial interframe space (IFS)
- Highest priority frames, e.g., Acks, use short IFS (SIFS)
- Medium priority time-critical frames use "Point Coordination Function IFS" (PIFS)
- Asynchronous data frames use "Distributed coordination function IFS" (DIFS)

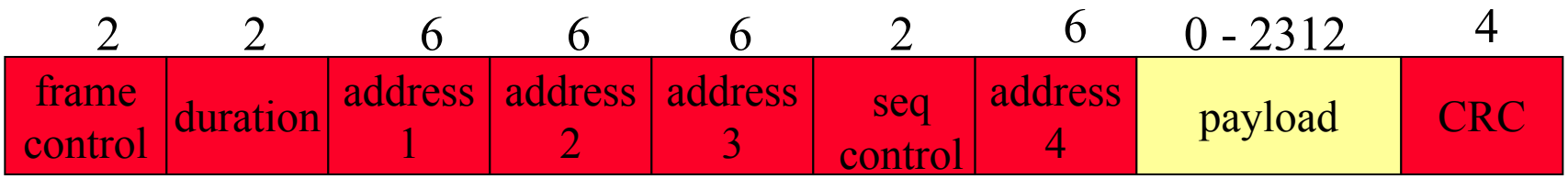
Transmission Example



802.11 Frame Format



802.11 Frame Addressing



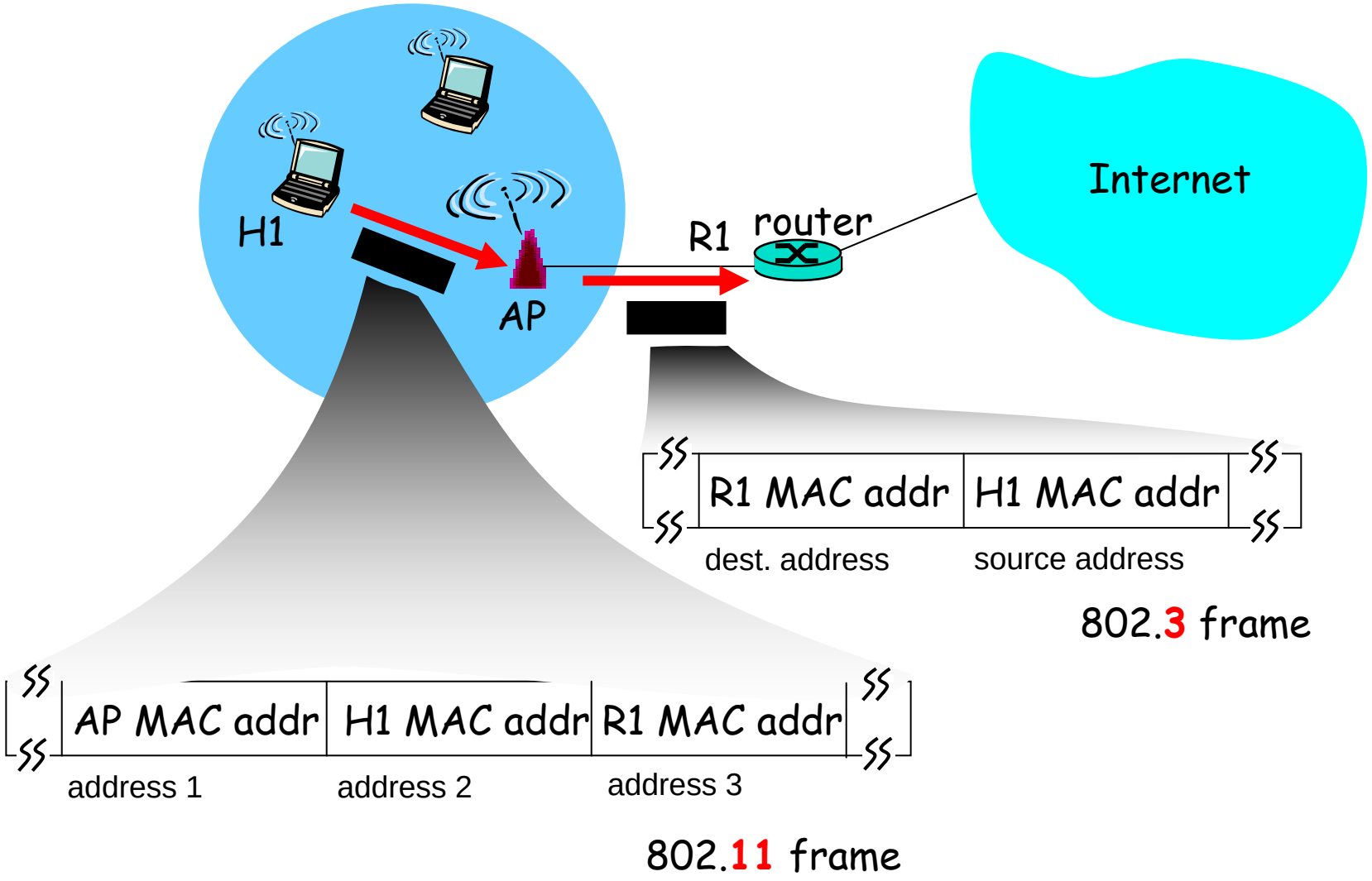
Address 1: MAC address of wireless host or AP to receive this frame

Address 2: MAC address of wireless host or AP transmitting this frame

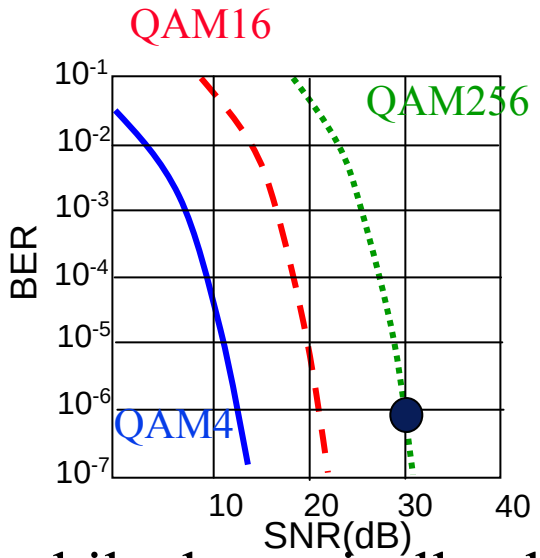
Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

802.11 Frame Addressing (Cont)



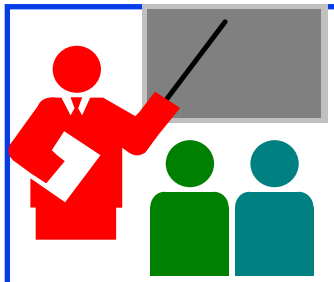
802.11 Rate Adaptation



- 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

Power Management

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



IEEE 802.11 LAN: Review

1. Code Division Multiple Access uses multiple chips to encode each bit
2. IEEE 802.11 PHYs: 11, 11b, 11g, 11a, 11n, …
3. IEEE 802.11 MAC uses CSMA/CA with a 4-way handshake: RTS, CTS, data, and ack
4. IEEE 802.11 network consists of extended service set consisting of multiple basic service sets each with an AP.
5. 802.11 Frame Format has 4 addresses and includes final destination's MAC which may not be wireless
6. 802.11 has automatic rate adaptation based on error rate. Power management allows stations to sleep.

Review Exercises

- Try in a group. Do not submit.
- Review questions: R1-R8, R9-R11
- Problems: P1, P2, P3, P4, P5 (Skip P6, P7, P8)

- Read Pages 523 through 554 (Section 6-1 through 6.3.5)

Homework 6A

- Submit answer to following (modified problem P7)
- Suppose an 802.11b station is configured to always reserve the channel with the RTS/CTS sequence. Suppose this station suddenly wants to transmit 1,000 bytes of data, and all other stations are idle at this time. Using SIFS of 10us and DIFS of 50us, and ignoring propagation delay and assuming no bit errors, calculate the time required to transmit the frame and receive the acknowledgment. Assume a frame without data is 32 bytes long and the transmission rate is 11 Mbps.

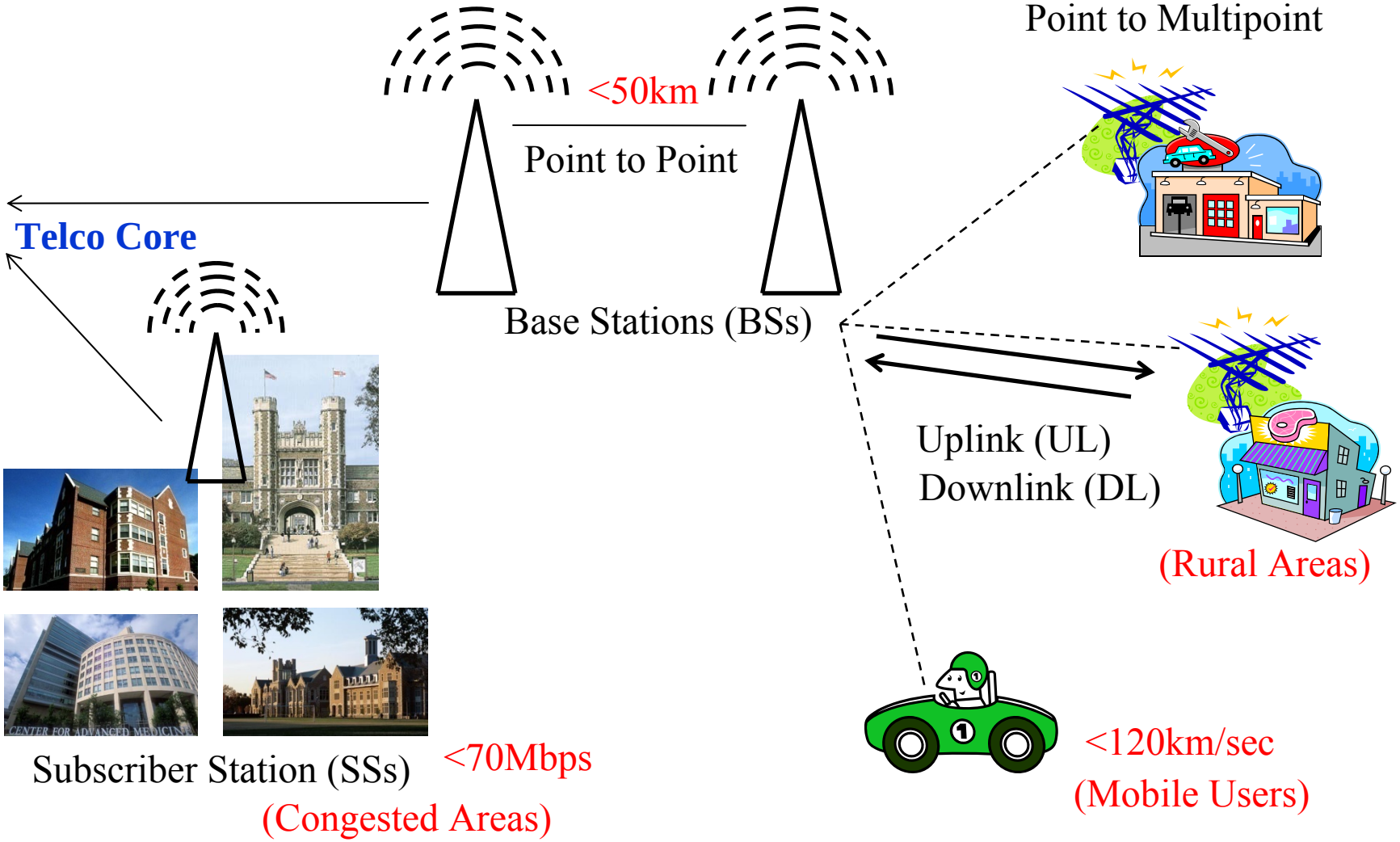
Other Wireless Networks and Mobility

1. Bluetooth
2. WiMAX
3. Cellular Networks
4. Cellular Generations
5. GSM
6. Mobile IP
7. Mobility in GSM

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 in standby, 50 mA while transmitting
  - Cheap: $5 per device
  - Small: 9 mm^2 single chips
- A piconet consists of a master and several slaves. Master determines the timing and polls slaves for transmission.

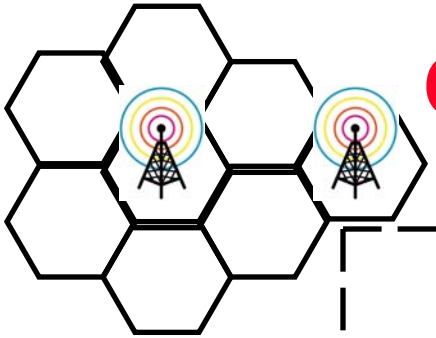
WiMAX


Point to Multipoint
<50km
Point to Point
Telco Core
Base Stations (BSs)
Uplink (UL)
Downlink (DL)
(Rural Areas)
Subscriber Station (SSs)
<70Mbps
(Congested Areas)
<120km/sec
(Mobile Users)

Key Features of WiMAX

- Works on many bands: 2.3 GHz, 2.5 GHz, 3.5 GHz, …
- Scalable ⇒ Can use any available spectrum width: 1.25 MHz to 28 MHz
- Strong security
- Open technology like WiFi
- Reach and mobility like Cellular but much higher data rates
  - High data rate, up to 70Mbps
  - Long distance, up to 50kms
  - Mobility, up to 120 to 150 km/hour
- Data rate vs. Distance trade off using adaptive modulation. 64QAM to BPSK ⇒ Different rate to different stations (Called Opportunistic scheduling)
- Offers non-line of site (NLOS) operation
- Strong QoS ⇒ Guaranteed services for data, voice, and video

Cellular Architecture



Base Transceiver Station

Base Station Controller

Base Station Controller

Home Location Register

Visitor Location Register

Subscriber Identity Module

Mobile Equipment

Base Transceiver Station

Mobile services Switching Center

PSTN

Equipment Identity Register

Authenti-cation Center

Mobile Station Base Station Subsystem Network Subsystem

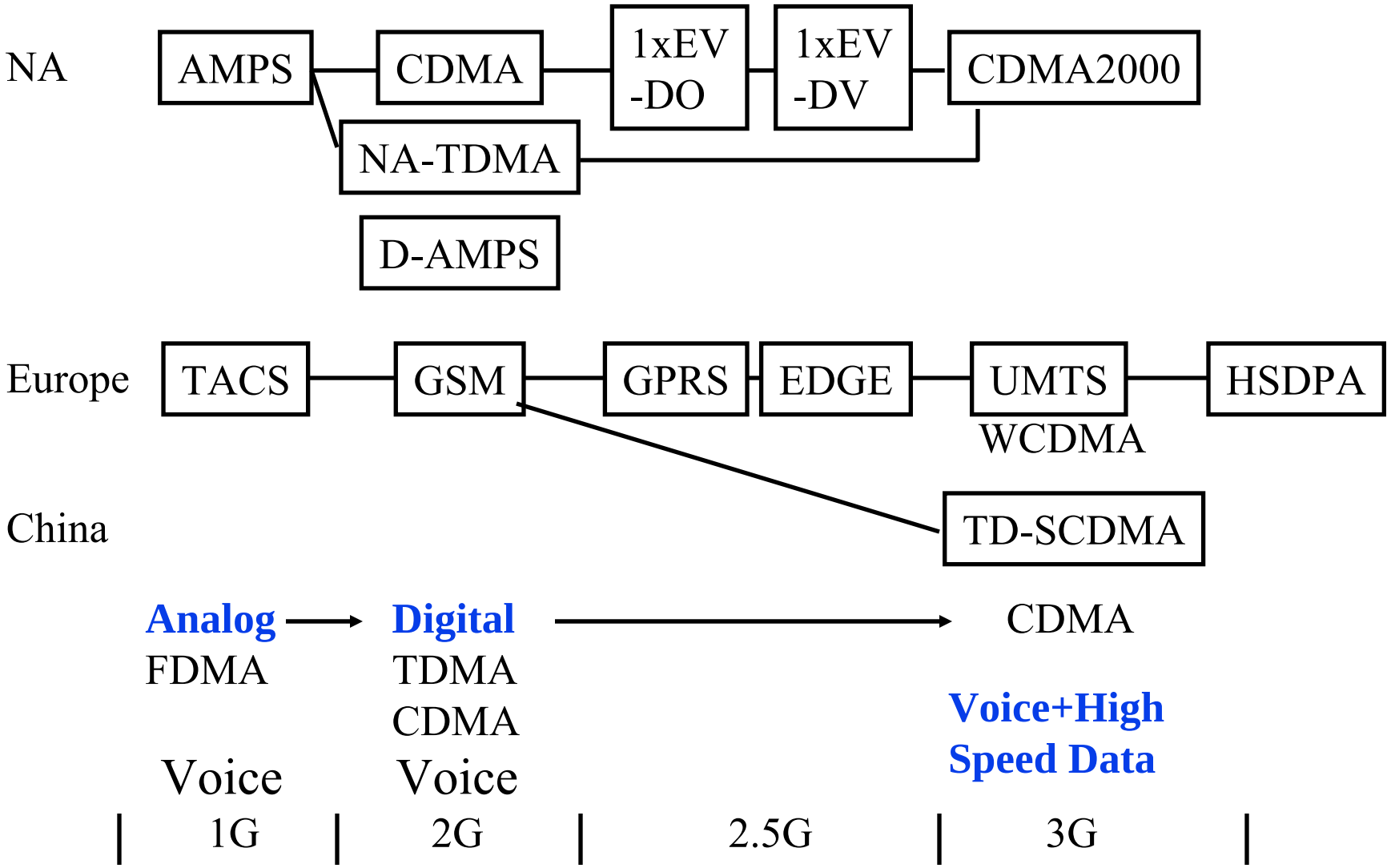
Cellular Architecture (Cont)

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

Cellular Architecture (Cont)

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

Evolution of Cellular Technologies



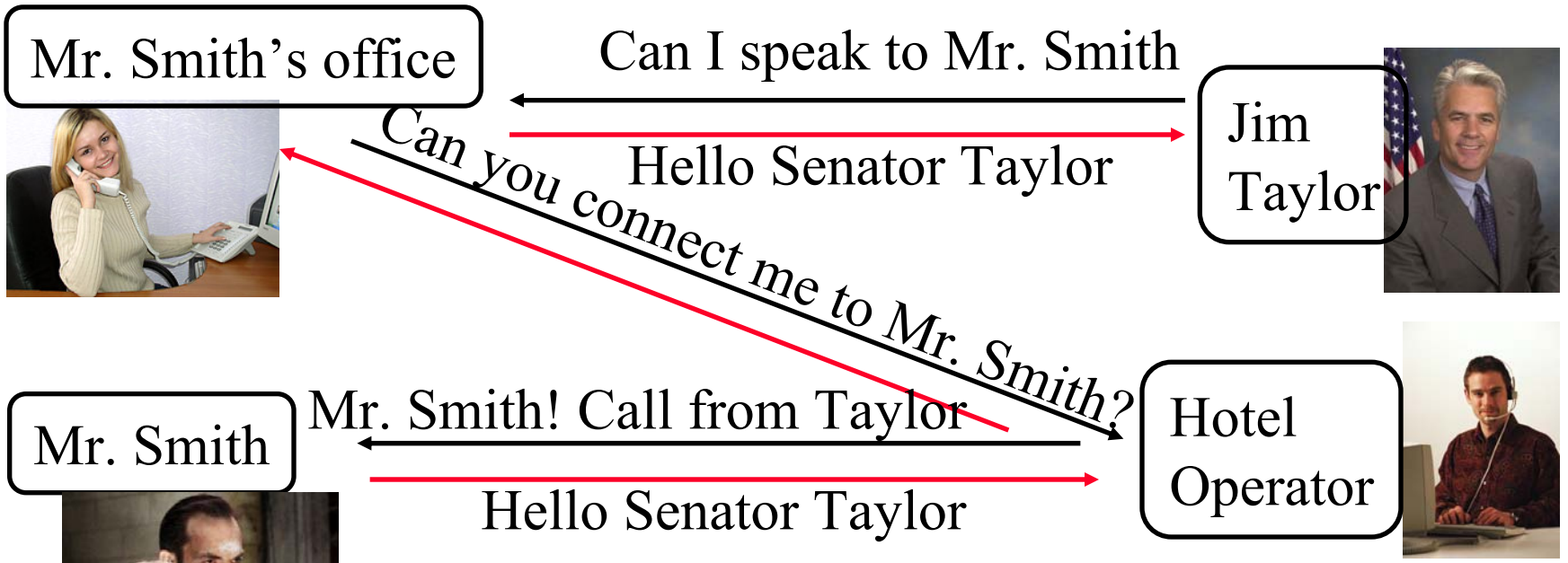
Wireless Generations (Cont)

- Acronyms:
  - Advanced Mobile Phone System (AMPS)
  - Total Access Communication System (TACS)
  - Interim Standard (IS) from Electronic Industry Association (EIA)/Telecommunications Industry Association (TIA)
  - Digital Advanced Mobile Phone System (D-AMPS)
  - Global system for mobile communication (GSM)
  - Digital Communication Network (DCN)
  - North America (NA)
  - Frequency/Time/Code division multiple access (FDMA/TDMA/CDMA)

GSM

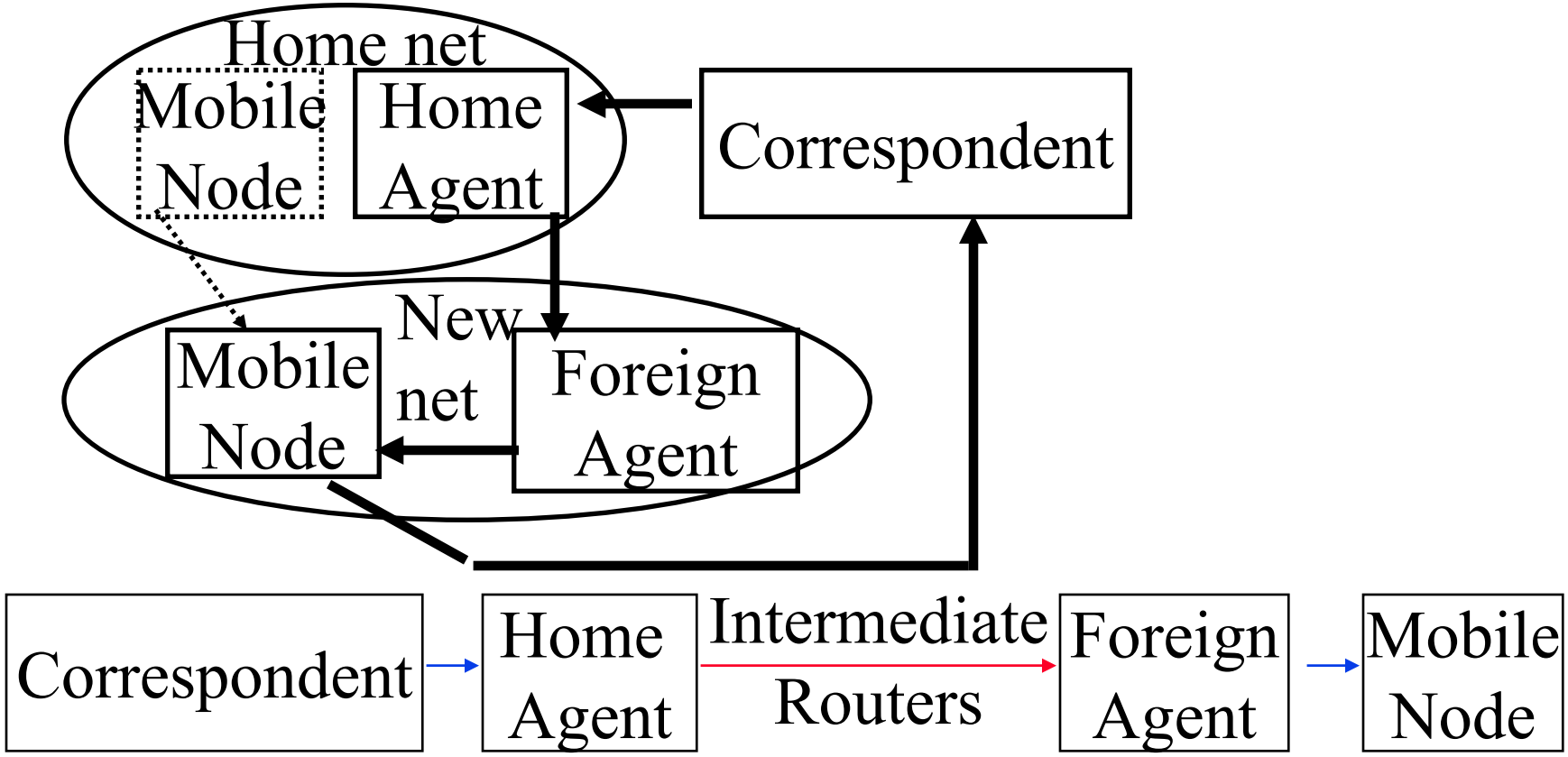
- Global System for Mobile Communication (GSM)
- 1982: Started as "Groupe Special Mobile" by Conference of European Posts and Telecom (CEPT)
- Good speech quality, ISDN compatibility, and fraud secure.
- Specs completed in 1990, Service began in 1992.
- 900 MHz in Europe, 1800 MHz in UK/Russia/Germany, 1900 MHz in USA
- General Packet Radio Service (**GPRS**) provides 56-114 kbps data
- Enhanced Data Rates for GSM Evolution (**EDGE** or EGPRS) provides 400-1000 kbps
- Universal Mobile Telecommunications System (**UMTS**) is the 3G technology and provides even higher speed data

Mobility: Mr. Smith Goes to Washington



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

Mobile IP: Mechanisms



Mechanism (Cont)

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

Mobile IP: Processes

- **Agent Discovery**: To find agents
  - Home agents and foreign agents advertise periodically on network layer and optionally on datalink
  - They also respond to solicitation from mobile node
  - Mobile can send solicitation to Mobile agent multicast group 224.0.0.11
  - Mobile selects an agent and gets/uses care-of-address
- **Registration**
  - Mobile registers its care-of-address with home agent. Either directly or through foreign agent
  - Home agent sends a reply to the CoA
  - Each "Mobility binding" has a negotiated lifetime limit
  - To continue, reregister within lifetime

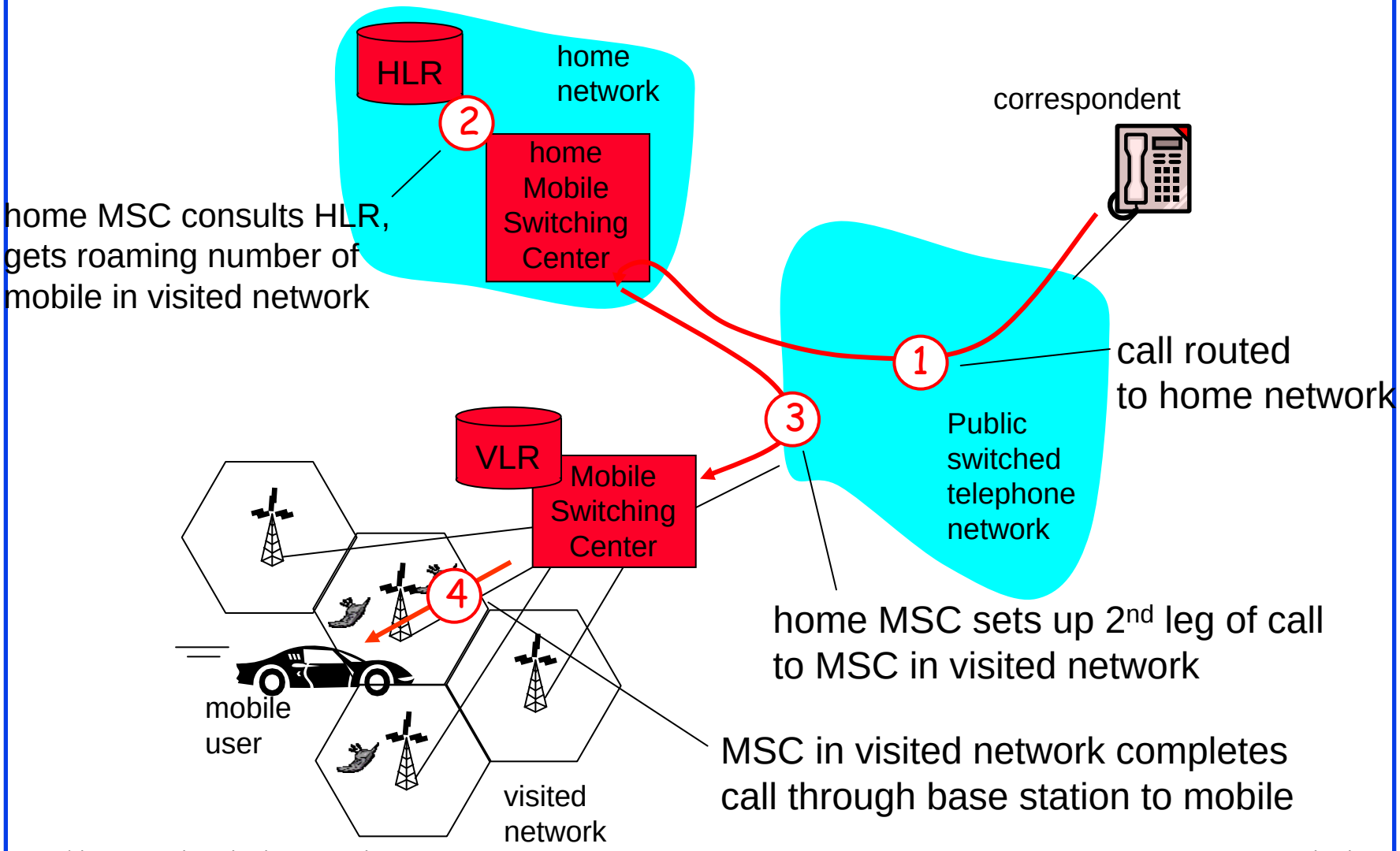
Processes (Cont)

- **Return to Home**:
  - Mobile node deregisters with home agent
    sets care-of-address to its permanent IP address
  - Lifetime = 0 $\Rightarrow$ Deregistration
- Deregistration with foreign agents is not required.
  Expires automatically
- Simultaneous registrations with more than one COA allowed (for handoff)

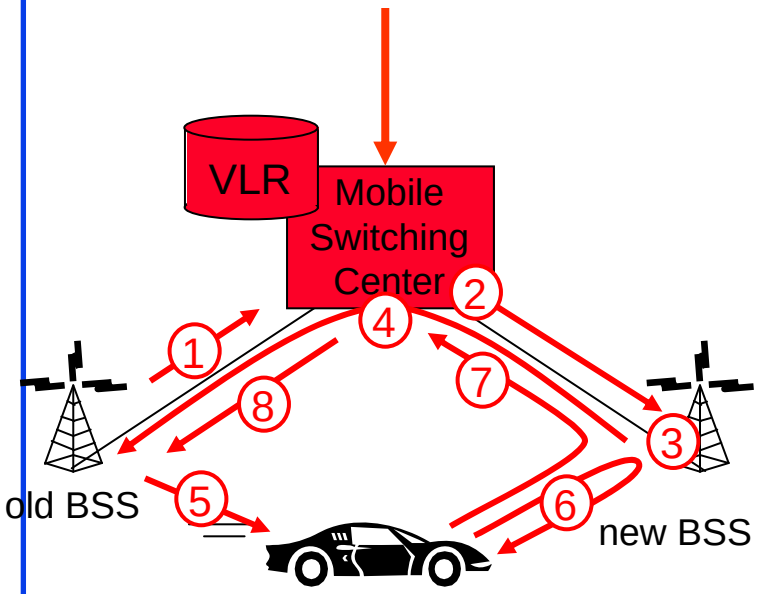
Encapsulation/Tunneling

- Home agent intercepts mobile node's datagrams and forwards them to care-of-address
- Care of Address can be the Foreign Agent or it can be co-located in the mobile host
- Home agent tells local nodes and routers to send mobile node's datagrams to it
- De-encapsulation: Datagram is extracted and sent to mobile node

GSM: Routing to Mobile



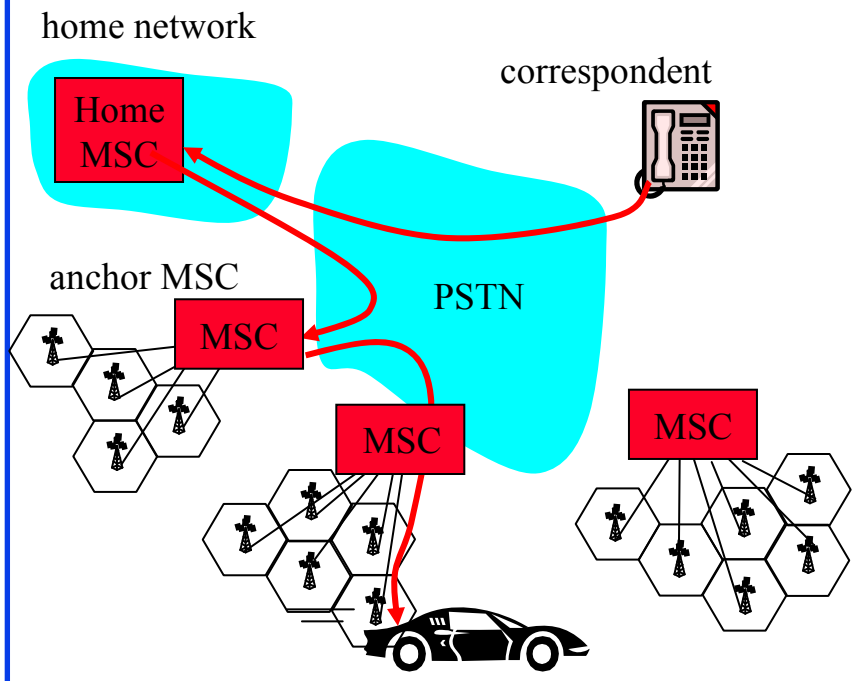
GSM: Handoff with Common MSC



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

8 MSC-old-BSS resources released

GSM: Handoff between MSCs



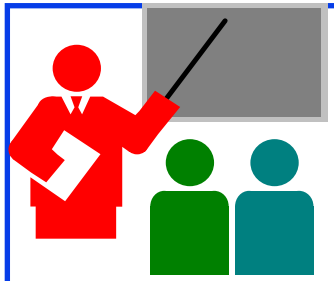
- *Anchor MSC:* first MSC visited during call
  - call remains routed through anchor MSC
- New MSCs add on to end of MSC chain as mobile moves to new MSC
- IS-41 allows optional path minimization step to shorten multi-MSC chain

Mobility: GSM versus Mobile IP

GSM element	Comment on GSM element	Mobile IP element
Home system	Network to which mobile user's permanent phone number belongs	**Home network**
Gateway Mobile Switching Center, or "home MSC". Home Location Register (HLR)	Home MSC: point of contact to obtain routable address of mobile user. HLR: database in home system containing permanent phone number, profile information, current location of mobile user, subscription information	**Home agent**
Visited System	Network other than home system where mobile user is currently residing	**Visited network**
Visited Mobile services Switching Center. Visitor Location Record (VLR)	Visited MSC: responsible for setting up calls to/from mobile nodes in cells associated with MSC. VLR: temporary database entry in visited system, containing subscription information for each visiting mobile user	**Foreign agent**
Mobile Station Roaming Number (MSRN), or "roaming number"	Routable address for telephone call segment between home MSC and visited MSC, visible to neither the mobile nor the correspondent.	**Care-of-address**

Impact on Higher Layer Protocols

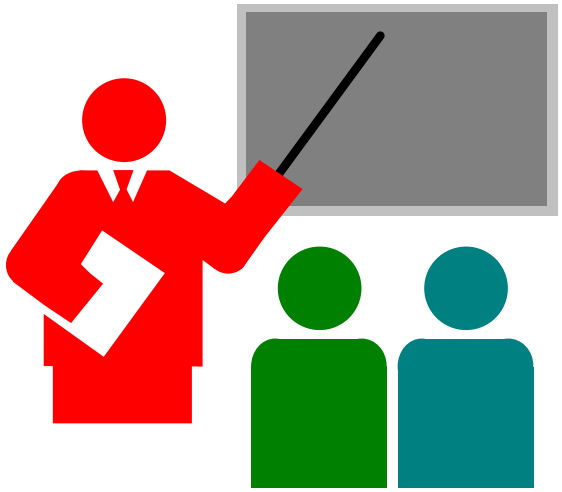
- Layered Architecture ⇒ Upper layers are independent of lower layers
- Wireless ⇒ High error rate ⇒ Frequent packet losses
  ⇒ Triggers TCP congestion control even if no overload
- TCP modifications:
  - Local Recovery: Link level retrans and error correction
  - Wireless-aware TCP Sender:
    Distinguish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



Other Wireless Networks: Review

1. Bluetooth is a low-rate short-distance low-cost wireless technology
2. WiMAX is a high-data rate, metropolitan area wireless data network
3. Cellular Networks have evolved from analog voice (1G), digital voice (2G), to high speed data (3G).
4. GSM is the most commonly used 2G cellular technology. It separates
5. Mobile IP uses home agents to forward packets to care-of-address of the mobile nodes.
6. In GSM, Home location register and visitor location registers help locate a mobile node. MSC's chain up to forward packets as mobile moves from one MSC to next.

Summary



- IEEE 802.11b/a/g/n are high-speed wireless LANs
- Bluetooth is a wirelss PAN
- WiMAX and Cellular networks are MAN
- Key issues are power management and mobility

Review Exercises

- Try in a group. Do not submit.
- Review questions: R15-R21
- Problems: P12, P13, P15 (Skip P9, P10, P11, P14, P16)

- Read pages 554 through 587 (Sections 6.3.6 through 6.9)

Homework 6B

- Submit answer to Problem P12
- Suppose the correspondent in Figure 6.22 were mobile. Sketch the additional network-layer infrastructure that would be needed to route the datagram from the original mobile user to the (now mobile) correspondent. Show the structure of the data gram(s) between the original mobile user and the (now mobile) correspondent, as in Figure 6.23.

Problem 6P1

- Two CDMA sender uses the codes of (1, -1, 1, -1) and (-1, 1, -1, 1). First sender transmits data bit 1 while the 2nd transmits –1 at the same time. What is the combined signal waveform seen by a receiver? Draw the waveform.
- 1st Senders signal: 1 –1 1 –1
- 2nd Senders Signal: 1 –1 1 –1
- Combined Signal: 2 –2 2 -2