Chapter 6
Wireless and Mobile Networks

A note on the use of these ppt slides:
We’re making these slides freely available to all (faculty, students, readers). They’re in PowerPoint form so you can add, modify, and delete slides (including this one) and slide content to suit your needs. They obviously represent a lot of work on our part. In return for use, we only ask the following:

- If you use these slides (e.g., in a class) in substantially unaltered form, that you mention their source (after all, we’d like people to use our book!)
- If you post any slides in substantially unaltered form on a www site, that you note that they are adapted from (or perhaps identical to) our slides, and note our copyright of this material.

Thanks and enjoy! JFK/KWR

All material copyright 1996-2007
J.F Kurose and K.W. Ross, All Rights Reserved
Chapter 6: Wireless and Mobile Networks

Background:

- # wireless (mobile) phone subscribers now exceeds # wired phone subscribers!
- computer nets: laptops, palmtops, PDAs, Internet-enabled phone promise anytime untethered Internet access
- two important (but different) challenges
  - wireless: communication over wireless link
  - mobility: handling the mobile user who changes point of attachment to network
Chapter 6 outline

6.1 Introduction

Wireless
- 6.2 Wireless links, characteristics
  - CDMA
- 6.3 IEEE 802.11 wireless LANs ("wi-fi")
- 6.4 Cellular Internet Access
  - architecture
  - standards (e.g., GSM)

Mobility
- 6.5 Principles: addressing and routing to mobile users
- 6.6 Mobile IP
- 6.7 Handling mobility in cellular networks
- 6.8 Mobility and higher-layer protocols

6.9 Summary
Elements of a wireless network

- **network infrastructure**
  - wireless hosts
    - laptop, PDA, IP phone
    - run applications
    - may be stationary (non-mobile) or mobile
      - wireless does *not* always mean mobility
Elements of a wireless network

- **network infrastructure**
- **base station**
  - typically connected to wired network
  - relay - responsible for sending packets between wired network and wireless host(s) in its “area”
  - e.g., cell towers, 802.11 access points
Elements of a wireless network

- **network infrastructure**
- **wireless link**
  - typically used to connect mobile(s) to base station
  - also used as backbone link
  - multiple access protocol coordinates link access
  - various data rates, transmission distance
Characteristics of selected wireless link standards

- **Indoor**: 10-30m
- **Outdoor**: 50-200m
- **Mid-range outdoor**: 200m – 4 Km
- **Long-range outdoor**: 5 Km – 20 Km

Data rate (Mbps)

- **2G**: IS-95, CDMA, GSM
- **UMTS/WCDMA, CDMA2000**: 802.15
- **UMTS/WCDMA-HSPDA, CDMA2000-1xEVDO**: 802.11a,g point-to-point, 802.16 (WiMAX)
- **3G cellular enhanced**: 802.11a,g, 802.11n
- **3G**: UMTS/WCDMA, CDMA2000-1xEVDO
Elements of a wireless network

- Infrastructure mode:
  - Base station connects mobiles into a wired network.
  - Handoff: Mobile changes base station providing connection into a wired network.
Elements of a wireless network

- **ad hoc mode**
  - no base stations
  - nodes can only transmit to other nodes within link coverage
  - nodes organize themselves into a network: route among themselves
## Wireless network taxonomy

<table>
<thead>
<tr>
<th>Infrastructure (e.g., APs)</th>
<th>Single hop</th>
<th>Multiple hops</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Infrastructure</strong></td>
<td>host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet</td>
<td>host may have to relay through several wireless nodes to connect to larger Internet: <em>mesh net</em></td>
</tr>
<tr>
<td><strong>No infrastructure</strong></td>
<td>no base station, no connection to larger Internet (Bluetooth, ad hoc nets)</td>
<td>no base station, no connection to larger Internet. May have to relay to reach other a given wireless node MANET, VANET</td>
</tr>
</tbody>
</table>
Wireless Link Characteristics (1)

Differences from wired link ....

- **decreased signal strength**: radio signal attenuates as it propagates through matter (path loss)
- **interference from other sources**: standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well
- **multipath propagation**: radio signal reflects off objects ground, arriving ad destination at slightly different times

.... make communication across (even a point to point) wireless link much more “difficult”
**Wireless Link Characteristics (2)**

- **SNR:** signal-to-noise ratio
  - larger SNR - easier to extract signal from noise (a “good thing”)
- **SNR versus BER tradeoffs**
  - *given physical layer:* increase power -> increase SNR -> decrease BER
  - *given SNR:* choose physical layer that meets BER requirement, giving highest throughput
    - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)
Multiple wireless senders and receivers create additional problems (beyond multiple access):

- B, A hear each other
- B, C hear each other
- A, C can not hear each other

**Hidden terminal problem**

- Means A, C unaware of their interference at B

**Signal attenuation:**

- B, A hear each other
- B, C hear each other
- A, C can not hear each other interfering at B
Code Division Multiple Access (CDMA)

- used in several wireless broadcast channels (cellular, satellite, etc) standards
- unique "code" assigned to each user; i.e., code set partitioning
- all users share same frequency, but each user has own "chipping" sequence (i.e., code) to encode data
- **encoded signal** = (original data) $\times$ (chipping sequence)
- **decoding**: inner-product of encoded signal and chipping sequence
- allows multiple users to "coexist" and transmit simultaneously with minimal interference (if codes are "orthogonal")
CDMA Encode/Decode

sender

data bits

code

d_1 = -1

d_0 = 1

slot 1

slot 0

channel output Z_{i,m} = d_i \cdot c_m

receiver

received input

code

slot 1

slot 0

D_i = \sum_{m=1}^{M} Z_{i,m} \cdot c_m

M

d_1 = -1

d_0 = 1

slot 1

slot 0
CDMA: two-sender interference

senders

data bits

code

channel, $Z_{i,m}^*$

$Z_{i,m}^1 = d_i^1 \cdot c_m^1$

$Z_{i,m}^2 = d_i^2 \cdot c_m^2$

receiver 1

$\phi_1^i = \sum_{m=1}^{M} Z_{i,m}^* \cdot c_m^1$

$\phi_0^i = 1$

2 2 2 2 2

2 2 2 2

$\phi_1^i = 1$

2 2 2 2 2

2 2 2 2

$\phi_0^i = 1$

1 1 1 1 1

-1 -1 -1 -1

1 1 1 1 1

-1 -1 -1 -1

1 1 1 1 1

-1 -1 -1 -1

slot 1 received input

slot 0 received input
Chapter 6 outline

6.1 Introduction

Wireless
- 6.2 Wireless links, characteristics
  - CDMA
- 6.3 IEEE 802.11 wireless LANs (“wi-fi”)
- 6.4 cellular Internet access
  - architecture
  - standards (e.g., GSM)

Mobility
- 6.5 Principles: addressing and routing to mobile users
- 6.6 Mobile IP
- 6.7 Handling mobility in cellular networks
- 6.8 Mobility and higher-layer protocols

6.9 Summary
IEEE 802.11 Wireless LAN

- **802.11b**
  - 2.4-5 GHz unlicensed spectrum
  - up to 11 Mbps
  - direct sequence spread spectrum (DSSS) in physical layer
    - all hosts use same chipping code

- **802.11a**
  - 5-6 GHz range
  - up to 54 Mbps

- **802.11g**
  - 2.4-5 GHz range
  - up to 54 Mbps

- **802.11n**: multiple antennae
  - 2.4-5 GHz range
  - up to 200 Mbps

- all use CSMA/CA for multiple access
- all have base-station and ad-hoc network versions
802.11 LAN architecture

- Wireless host communicates with base station
  - Base station = access point (AP)
- Basic Service Set (BSS) (aka “cell”) in infrastructure mode contains:
  - Wireless hosts
  - Access point (AP): base station
  - Ad hoc mode: hosts only
802.11: Channels, association

- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
  - AP admin chooses frequency for AP
  - interference possible: channel can be same as that chosen by neighboring AP!

- 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 [Chapter 8]
  - will typically run DHCP to get IP address in AP’s subnet
Passive Scanning:
(1) beacon frames sent from APs
(2) association Request frame sent: H1 to selected AP
(3) association Response frame sent: H1 to selected AP

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: H1 to selected AP
IEEE 802.11: multiple access

- avoid collisions: 2+ nodes transmitting at same time
- 802.11: CSMA - sense before transmitting
  - don’t collide with ongoing transmission by other node
- 802.11: no collision detection!
  - difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
  - can’t sense all collisions in any case: hidden terminal, fading
  - goal: *avoid collisions*: CSMA/C(ollision)A(voidance)*
IEEE 802.11 MAC Protocol: CSMA/CA

802.11 sender
1 if sense channel idle for DIFS then
   transmit entire frame (no CD)
2 if sense channel busy then
   start random backoff time
   timer counts down while channel idle
   transmit when timer expires
   if no ACK, increase random backoff interval, repeat 2

802.11 receiver
- if frame received OK
  return ACK after SIFS (ACK needed due to hidden terminal problem)
Avoiding collisions (more)

**idea:** allow sender to “reserve” channel rather than random access of data frames: avoid collisions of long data frames

- sender first transmits *small* request-to-send (RTS) packets to BS using CSMA
  - RTSs may still collide with each other (but they’re short)
- BS broadcasts clear-to-send CTS in response to RTS
- CTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions

**avoid data frame collisions completely using small reservation packets!**
Collision Avoidance: RTS-CTS exchange

- RTS(A) sent by A
- RTS(B) sent by B
- Reservation collision
- CTS(A) sent by AP
- DATA (A) sent by A
- ACK(A) sent by B
- defer
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

Address 4: used only in ad hoc mode
**802.11 frame: addressing**

The diagram illustrates the process of addressing in a wireless network. The AP (Access Point) is connected to the Internet via R1 (router). The AP's MAC address, H1's MAC address, and R1's MAC address are shown in the diagram.

**802.11 frame**

```
<table>
<thead>
<tr>
<th>AP MAC addr</th>
<th>H1 MAC addr</th>
<th>R1 MAC addr</th>
</tr>
</thead>
<tbody>
<tr>
<td>address 1</td>
<td>address 2</td>
<td>address 3</td>
</tr>
</tbody>
</table>
```

**802.3 frame**

```
<table>
<thead>
<tr>
<th>R1 MAC addr</th>
<th>H1 MAC addr</th>
</tr>
</thead>
<tbody>
<tr>
<td>dest. address</td>
<td>source address</td>
</tr>
</tbody>
</table>
```

This diagram is relevant to the study of wireless and mobile networks.
# 802.11 frame: more

802.11 frame contains the following fields:

- **Protocol version**: 2 bytes
- **Type**: 2 bytes
- **Subtype**: 4 bytes
- **To AP**: 1 byte
- **From AP**: 1 byte
- **More frag**: 1 byte
- **Retry**: 1 byte
- **Power mgt**: 1 byte
- **More data**: 1 byte
- **WEP**: 1 byte
- **Rsvd**: 1 byte

### Frame Control
- **Duration**: 2 bytes
- **Address 1**: 6 bytes
- **Address 2**: 6 bytes
- **Address 3**: 6 bytes
- **Sequence control**: 2 bytes
- **Address 4**: 6 bytes
- **Frame seq #**: 0-2312 bytes
- **Payload**: 4 bytes
- **CRC**: 4 bytes

### Frame Control Description
- **Frame type**:
  - RTS
  - CTS
  - ACK
  - Data

### Duration of Reserved Transmission Time (RTS/CTS)
- Specifies the duration of reserved transmission time for RTS/CTS frames.

### Frame Seq # (for RDT)
- Represents the sequence number for RDT frames.

---

**Image Details**

- Diagram illustrating the structure of an 802.11 frame.
- Key fields are labeled with their respective positions and types.

---

**Extra Information**

- For more detailed information on each field, refer to the relevant section in 6: Wireless and Mobile Networks.
H1 remains in same IP subnet: IP address can remain same

- switch: which AP is associated with H1?
  - self-learning (Ch. 5): switch will see frame from H1 and “remember” which switch port can be used to reach H1
802.11: advanced capabilities

Rate Adaptation

- base station, mobile dynamically change transmission rate (physical layer modulation technique) as mobile moves, SNR varies

1. SNR decreases, BER increase as node moves away from base station
2. When BER becomes too high, switch to lower transmission rate but with lower BER
802.11: advanced capabilities

*Power Management*

- node-to-AP: “I am going to sleep until next beacon frame”
  - AP knows not to transmit frames to this node
  - node wakes up before next beacon frame
- beacon frame: contains list of mobiles with AP-to-mobile frames waiting to be sent
  - node will stay awake if AP-to-mobile frames to be sent; otherwise sleep again until next beacon frame
802.15: personal area network

- less than 10 m diameter
- replacement for cables (mouse, keyboard, headphones)
- ad hoc: no infrastructure
- master/slaves:
  - slaves request permission to send (to master)
  - master grants requests
- 802.15: evolved from Bluetooth specification
  - 2.4-2.5 GHz radio band
  - up to 721 kbps

M Master device
S Slave device
P Parked device (inactive)
802.16: WiMAX

- like 802.11 & cellular: base station model
  - transmissions to/from base station by hosts with omnidirectional antenna
  - base station-to-base station backhaul with point-to-point antenna

- unlike 802.11:
  - range ~ 6 miles ("city rather than coffee shop")
  - ~14 Mbps
802.16: WiMAX: downlink, uplink scheduling

- transmission frame
  - down-link subframe: base station to node
  - uplink subframe: node to base station

- WiMAX standard provide mechanism for scheduling, but not scheduling algorithm
Chapter 6 outline

6.1 Introduction

Wireless
- 6.2 Wireless links, characteristics
  - CDMA
- 6.3 IEEE 802.11 wireless LANs (“wi-fi’’)
- 6.4 Cellular Internet Access
  - architecture
  - standards (e.g., GSM)

Mobility
- 6.5 Principles: addressing and routing to mobile users
- 6.6 Mobile IP
- 6.7 Handling mobility in cellular networks
- 6.8 Mobility and higher-layer protocols

6.9 Summary
Components of cellular network architecture

- **MSC**
  - connects cells to wide area net
  - manages call setup (more later!)
  - handles mobility (more later!)

- **cell**
  - covers geographical region
  - *base station (BS)* analogous to 802.11 AP
  - *mobile users* attach to network through BS
  - *air-interface:* physical and link layer protocol between mobile and BS

- **Mobile Switching Center**

- Public telephone network, and Internet

- Wired network
Cellular networks: the first hop

Two techniques for sharing mobile-to-BS radio spectrum

- **combined FDMA/TDMA:** divide spectrum in frequency channels, divide each channel into time slots

- **CDMA:** code division multiple access
Cellular standards: brief survey

2G systems: voice channels

- IS-136 TDMA: combined FDMA/TDMA (north america)

- GSM (global system for mobile communications): combined FDMA/TDMA
  - most widely deployed

- IS-95 CDMA: code division multiple access

Don’t drown in a bowl of alphabet soup: use this for reference only
Cellular standards: brief survey

2.5 G systems: voice and data channels
- for those who can’t wait for 3G service: 2G extensions
- general packet radio service (GPRS)
  - evolved from GSM
  - data sent on multiple channels (if available)
- enhanced data rates for global evolution (EDGE)
  - also evolved from GSM, using enhanced modulation
  - data rates up to 384K
- CDMA-2000 (phase 1)
  - data rates up to 144K
  - evolved from IS-95
Cellular standards: brief survey

3G systems: voice/data

- Universal Mobile Telecommunications Service (UMTS)

- CDMA-2000: CDMA in TDMA slots
  - data service: 1xEvolution Data Optimized (1xEVDO) up to 14 Mbps

..... more (and more interesting) cellular topics due to mobility (stay tuned for details)
Chapter 6 outline

6.1 Introduction

Wireless
- 6.2 Wireless links, characteristics
  - CDMA
- 6.3 IEEE 802.11 wireless LANs ("wi-fi")
- 6.4 Cellular Internet Access
  - architecture
  - standards (e.g., GSM)

Mobility
- 6.5 Principles: addressing and routing to mobile users
- 6.6 Mobile IP
- 6.7 Handling mobility in cellular networks
- 6.8 Mobility and higher-layer protocols

6.9 Summary
What is mobility?

- spectrum of mobility, from the network perspective:

  no mobility

  mobile wireless user, using same access point

  high mobility

  mobile user, connecting/disconnecting from network using DHCP.

  mobile user, passing through multiple access point while maintaining ongoing connections (like cell phone).
**Mobility: Vocabulary**

- **home network**: permanent "home" of mobile (e.g., 128.119.40/24)

- **home agent**: entity that will perform mobility functions on behalf of mobile, when mobile is remote

- **Permanent address**: address in home network, can always be used to reach mobile e.g., 128.119.40.186

![Diagram showing home network, home agent, and correspondent]
**Mobility: more vocabulary**

*Permanent address*: remains constant (e.g., 128.119.40.186)

*Care-of-address*: address in visited network. (e.g., 79.129.13.2)

*visited network*: network in which mobile currently resides (e.g., 79.129.13/24)

*wide area network*

*foreign agent*: entity in visited network that performs mobility functions on behalf of mobile.

*correspondent*: wants to communicate with mobile
How do you contact a mobile friend:

Consider friend frequently changing addresses, how do you find her?
- search all phone books?
- call her parents?
- expect her to let you know where he/she is?

I wonder where Alice moved to?
Mobility: approaches

- **Let routing handle it:** routers advertise permanent address of mobile-nodes-in-residence via usual routing table exchange.
  - routing tables indicate where each mobile located
  - no changes to end-systems

- **Let end-systems handle it:**
  - **indirect routing:** communication from correspondent to mobile goes through home agent, then forwarded to remote
  - **direct routing:** correspondent gets foreign address of mobile, sends directly to mobile
Mobility: approaches

- Let routing handle it: routers advertise permanent address of mobile nodes in residence via usual routing table exchange.
  - Routing tables indicate where each mobile located.
  - No changes to end systems.
- Let end-systems handle it:
  - **Indirect routing:** communication from correspondent to mobile goes through home agent, then forwarded to remote.
  - **Direct routing:** correspondent gets foreign address of mobile, sends directly to mobile

Not scalable to millions of mobiles.
Mobility: registration

End result:
- Foreign agent knows about mobile
- Home agent knows location of mobile


**Mobility via Indirect Routing**

1. Correspondent addresses packets using home address of mobile.
2. Home agent intercepts packets, forwards to foreign agent.
3. Foreign agent receives packets, forwards to mobile.
4. Mobile replies directly to correspondent.

**Diagram Notes:**
- Home network
- Wide area network
- Visited network
- Home agent
- Foreign agent

---

6: Wireless and Mobile Networks
6-49
Indirect Routing: comments

- Mobile uses two addresses:
  - **permanent address**: used by correspondent (hence mobile location is *transparent* to correspondent)
  - **care-of-address**: used by home agent to forward datagrams to mobile
- Foreign agent functions may be done by mobile itself
- **triangle routing**: correspondent-home-network-mobile
  - inefficient when correspondent, mobile are in same network
Indirect Routing: moving between networks

- suppose mobile user moves to another network
  - registers with new foreign agent
  - new foreign agent registers with home agent
  - home agent update care-of-address for mobile
  - packets continue to be forwarded to mobile (but with new care-of-address)

- mobility, changing foreign networks transparent: *ongoing connections can be maintained!
Mobility via Direct Routing

1. Correspondent requests, receives foreign address of mobile.
2. Correspondent forwards to foreign agent.
3. Foreign agent receives packets, forwards to mobile.
4. Mobile replies directly to correspondent.

- Home network
- Wide area network
- Visited network

6: Wireless and Mobile Networks
Mobility via Direct Routing: comments

- overcome triangle routing problem
- non-transparent to correspondent: correspondent must get care-of-address from home agent
  - what if mobile changes visited network?
Accommodating mobility with direct routing

- anchor foreign agent: FA in first visited network
- data always routed first to anchor FA
- when mobile moves: new FA arranges to have data forwarded from old FA (chaining)
Chapter 6 outline

6.1 Introduction

Wireless
- 6.2 Wireless links, characteristics
  - CDMA
- 6.3 IEEE 802.11 wireless LANs ("wi-fi")
- 6.4 Cellular Internet Access
  - architecture
  - standards (e.g., GSM)

Mobility
- 6.5 Principles: addressing and routing to mobile users
- 6.6 Mobile IP
- 6.7 Handling mobility in cellular networks
- 6.8 Mobility and higher-layer protocols

6.9 Summary
Mobile IP

- RFC 3344
- has many features we've seen:
  - home agents, foreign agents, foreign-agent registration, care-of-addresses, encapsulation (packet-within-a-packet)
- three components to standard:
  - indirect routing of datagrams
  - agent discovery
  - registration with home agent
**Mobile IP: indirect routing**

- Permanent address: 128.119.40.186
- Care-of address: 79.129.13.2

Packet sent by home agent to foreign agent: a *packet within a packet*

- Dest: 79.129.13.2
- Dest: 128.119.40.186

Packet sent by correspondent: 128.119.40.186

Foreign-agent-to-mobile packet: 128.119.40.186

Care-of address: 79.129.13.2
Mobile IP: agent discovery

- **agent advertisement**: foreign/home agents advertise service by broadcasting ICMP messages (typefield = 9)

![Diagram of Mobile IP: agent advertisement]

- **H,F bits**: home and/or foreign agent
- **R bit**: registration required

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Code</th>
<th>Checksum</th>
<th>Router Address</th>
<th>Length</th>
<th>Sequence #</th>
<th>Registration Lifetime</th>
<th>RBHFMGV Bits</th>
<th>Reserved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Code</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Checksum</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router Addr</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Length</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seq #</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reg Life</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RBHMGV</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reserved</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

0 or more care-of-addresses
Mobile IP: registration example

visited network: 79.129.13/24

Mobile agent
MA: 128.119.40.186

ICMP agent adv.
COA: 79.129.13.2

registration req.
COA: 79.129.13.2
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 9999
identification: 714
encapsulation format
....

registration req.
COA: 79.129.13.2
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 9999
identification: 714
encapsulation format
....

registration reply
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
encapsulation format
....

registration reply
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
encapsulation format
....

registration reply
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
encapsulation format
....

registration reply
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
encapsulation format
....

registration reply
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
encapsulation format
....

registration reply
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
encapsulation format
....

registration reply
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
encapsulation format
....

registration reply
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
encapsulation format
....

registration reply
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
encapsulation format
....

registration reply
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
encapsulation format
....

registration reply
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
encapsulation format
....

registration reply
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
encapsulation format
....

registration reply
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
encapsulation format
....

registration reply
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
encapsulation format
....

registration reply
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
encapsulation format
....

registration reply
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
encapsulation format
....

registration reply
HA: 128.119.40.7
MA: 128.119.40.186
 Lifetime: 4999
Identification: 714
encapsulation format
....

registration reply
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
encapsulation format
....

registration reply
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
encapsulation format
....

registration reply
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
encapsulation format
....
Components of cellular network architecture

Recall:

- Different cellular networks, operated by different providers

- Wired public telephone network

- Correspondent

Diagrams showing the architecture of cellular networks with nodes labeled "MSC" and connections illustrating the network topology.
Handling mobility in cellular networks

- **home network**: network of cellular provider you subscribe to (e.g., Sprint PCS, Verizon)
  - **home location register (HLR)**: database in home network containing permanent cell phone #, profile information (services, preferences, billing), information about current location (could be in another network)

- **visited network**: network in which mobile currently resides
  - **visitor location register (VLR)**: database with entry for each user currently in network
  - could be home network
GSM: indirect routing to mobile

1. Call routed to home network
2. Home MSC consults HLR, gets roaming number of mobile in visited network
3. Home MSC sets up 2nd leg of call to MSC in visited network
4. MSC in visited network completes call through base station to mobile

- HLR (Home Location Register)
- VLR (Visitor Location Register)
- Mobile Switching Center
- Public switched telephone network
- Correspondent
- Home network
- Visited network
- Mobile user
GSM: handoff with common MSC

- Handoff goal: route call via new base station (without interruption)
- Reasons for handoff:
  - Stronger signal to/from new BSS (continuing connectivity, less battery drain)
  - Load balance: free up channel in current BSS
  - GSM doesn’t mandate why to perform handoff (policy), only how (mechanism)
- Handoff initiated by old BSS
**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

(a) before handoff
**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

(b) after handoff
## Mobility: GSM versus Mobile IP

<table>
<thead>
<tr>
<th>GSM element</th>
<th>Comment on GSM element</th>
<th>Mobile IP element</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Home system</strong></td>
<td>Network to which mobile user’s permanent phone number belongs</td>
<td><strong>Home network</strong></td>
</tr>
<tr>
<td><strong>Gateway Mobile Switching Center, or “home MSC”. Home Location Register (HLR)</strong></td>
<td>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</td>
<td><strong>Home agent</strong></td>
</tr>
<tr>
<td><strong>Visited System</strong></td>
<td>Network other than home system where mobile user is currently residing</td>
<td><strong>Visited network</strong></td>
</tr>
<tr>
<td><strong>Visited Mobile services Switching Center. Visitor Location Record (VLR)</strong></td>
<td>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</td>
<td><strong>Foreign agent</strong></td>
</tr>
<tr>
<td><strong>Mobile Station Roaming Number (MSRN), or “roaming number”</strong></td>
<td>Routable address for telephone call segment between home MSC and visited MSC, visible to neither the mobile nor the correspondent.</td>
<td><strong>Care-of-address</strong></td>
</tr>
</tbody>
</table>
Wireless, mobility: impact on higher layer protocols

- logically, impact *should* be minimal ...
  - best effort service model remains unchanged
  - TCP and UDP can (and do) run over wireless, mobile

- ... but performance-wise:
  - packet loss/delay due to bit-errors (discarded packets, delays for link-layer retransmissions), and handoff
  - TCP interprets loss as congestion, will decrease congestion window un-necessarily
  - delay impairments for real-time traffic
  - limited bandwidth of wireless links
Chapter 6 Summary

Wireless
- wireless links:
  - capacity, distance
  - channel impairments
  - CDMA
- IEEE 802.11 (“wi-fi”)
  - CSMA/CA reflects wireless channel characteristics
- cellular access
  - architecture
  - standards (e.g., GSM, CDMA-2000, UMTS)

Mobility
- principles: addressing, routing to mobile users
  - home, visited networks
  - direct, indirect routing
  - care-of-addresses
- case studies
  - mobile IP
  - mobility in GSM
- impact on higher-layer protocols