
Additional materials were collected by Philip McKinley at Michigan State University from various Internet sources.

**Topics**

We will briefly cover the following topics related to wireless and mobile networks:

- Wireless LANs
- Mobile IP
Elements of a wireless network

- **Network infrastructure**

  - **Wireless hosts**
    - laptop, smartphone
    - run applications
    - may be stationary or mobile
      - NOTE: wireless does not always mean mobility
Elements of a wireless network

- **base station**
  - Typically connected to wired network
  - Relay - responsible for sending packets between wired network and wireless host(s) in its "area" (usually one hop)
  - E.g., cell towers, 802.11 access points

- **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
**Wireless network characteristics**

Multiple wireless senders and receivers create additional problems (beyond multiple access):

- **Hidden terminal problem**
  - B, A hear each other
  - B, C hear each other
  - A, C can not hear each other 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

---

**IEEE 802.11 Standards**

- **802.11b**
  - 2.4-5 GHz unlicensed spectrum
  - up to 11 Mbps

- **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
Connecting to an Access Point

- **802.11b:**
  - 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
  - AP administrator chooses frequency for AP
  - interference is possible: channel might be same as that chosen by neighboring AP (think coffee shop)

- **host must **associate** with an AP**
  - scans channels, listening for **beacon frames** containing AP’s name (SSID) and MAC address
  - host (or the user) selects an AP
    - may perform authentication
  - host then typically uses DHCP to get IP address, subnet mask, etc. in AP’s subnet

**MAC protocol: CSMA/CA (not CD)**

- Like 802.3, 802.11 uses CSMA - sense before transmitting
  - Don’t transmit during ongoing transmission by other node!
- Unlike 802.3, however, 802.11 does not use collision detection! Reasons:
  - It is difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
  - Can’t sense all collisions in any case, due to hidden terminals, fading signal strength
  - So the goal is to **avoid collisions**: CSMA with C(ollision)A(voidance)
CSMA/CA Operation

**802.11 sender**
Sense channel
If idle for DIFS sec then
  transmit entire frame (no CD)
If busy then
  start random backoff timer
  timer counts down while channel idle
  NOTE: paused if channel becomes busy
  transmit when timer expires
  if no ACK received, increase random backoff
  interval, repeat

**802.11 receiver**
If frame is received OK
  return ACK after SIFS sec
  (ACK needed due to hidden terminal problem – another
  node sending but not heard by sender – as well as
  noise level)

CA vs. CD

- Recall 802.3 is 1-persistent
  - if two nodes sense a 3rd is sending, both nodes wait
    until idle and send unconditionally
  - If collision is detected, both stop sending (CD) and
    enter backoff protocol with small frames

- But we do not have CD, frames are sent in
  their entirety
  - So, enter backoff protocol immediately and hope
    nodes choose different numbers
  - If ACK is not received (possibly due to collision),
    double the backoff interval as in 802.3
**RTS/CTS**

- Optional component of 802.11 protocol
- Basic 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 base station using CSMA
  - RTSs may still collide with each other (but they’re short)
- Base station broadcasts clear-to-send
- CTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions
- NOTE: typically only applied to long frames; the default size is beyond max frame size of most WLANs

**RTS-CTS Operation**

[Diagram showing RTS/CTS operation with time axis and nodes A, B, and AP]
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
**Mobile IP**

- DHCP handles cases where a laptop is closed and carried to a different network
- Mobile IP addresses how to remain connected while moving among networks
  - Standardized in 2002 (RFC 3344) and revised in 2010 (RFC 5944)
- Three main components to Mobile IP:
  - agent discovery
  - registration with home agent
  - indirect routing of datagrams

**Indirect routing**

- Packets forwarded by “home agent” to the current location of the mobile host:
  - Permanent address: 128.119.40.186
  - Care-of address: 79.129.13.2
  - Dest: 79.129.13.2
  - Packet sent by correspondent
  - Packet sent by home agent to foreign agent: a *packet within a packet*
  - Foreign-agent-to-mobile packet: dest: 128.119.40.186
Agent discovery

- Mobile host needs to register with an agent in the visited network to receive forwarded packets
- Agent will provide a “care of” address to the mobile node
- *Agent advertisement:* foreign agents advertise service by broadcasting ICMP messages (typefield = 9)

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

Mobile IP: registration example

```
visited network: 79.129.13/24
home agent
HA: 128.119.40.7

foreign agent
COA: 79.129.13.2

mobile agent
MA: 128.119.40.186

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
....
```

```
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
....

registration reply
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
identification: 714
....
```
Packet delivery

- Packets arriving at home agent are **encapsulated** in packets with care of address and tunneled to the foreign agent.
- Foreign agent will deliver encapsulated packets to mobile host.
- If mobile host moves to another network, it will register with a new foreign agent and repeat process.

![Packet Delivery Diagram]

A few bits about IP and cellular...

- Important: Typically, only the last hop is wireless.
- Cell model enables re-use of frequencies.

**MSC**
- connects cells to wired tel. net.
- manages call setup
- handles mobility

**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
Cellular Generations (high-level)

- New generation about every 10 years
- **1G ~ 1980s:**
  - Analog voice, circuit switched, frequency modulation
- **2G ~ 1990s:**
  - Digitized voice as well as text messaging, TDMA
- **3G ~ 2000s:**
  - Parallel access to phone network and Internet
  - Former is circuit-switched, latter is packet-switched
  - Emergence of smartphones
- **4G ~ 2010s:**
  - All-IP core, everything is packet switched
  - IP telephony, mobile Internet, television, gaming...
- **5G ~ emerging now:**
  - Multi-gigabit speeds, very fast tracking, etc., etc...

---

2G (voice) network architecture

![2G network architecture diagram]
3G versus 4G LTE architecture

3G

4G-LTE

IP in Cellular Networks

- Your cell phone has two IP-capable interfaces
  - Wifi - when you are near an access point
  - Cellular data - otherwise

- Cellular data mode
  - Think about your home cellular network as a huge coffee shop
  - Service provider assigns (network-internal) IP address with DHCP-like protocol when you turn on your device (leased)
  - NAT used to translate internal IP/port numbers to external IP/port numbers when accessing the Internet

- Amazing developments in the past 20 years. Stay tuned!