Wireless Networks

Tom Kelliher, CS 325

May 7, 2008

1 Administrivia

Announcements

Exam: Thursday, May 15, 3:00–5:00 pm.

Assignment

From Last Time

Link layer.

Outline

1. Introduction.
2. Wireless network characteristics.
3. WiFi — 802.11.

Coming Up

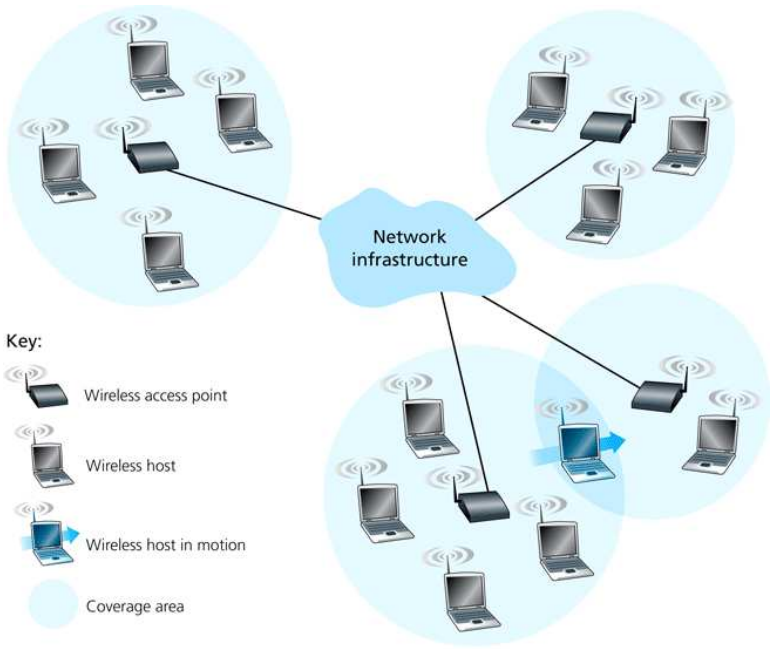
Exam.

2 Introduction

Wireless devices are radio transmitters/receivers. 802.11b/g devices operate at 2.4–2.485 GHz. 802.11a at 5.1–5.8 GHz. 802.11n at *both*.

These frequencies are broken into channels.

Wireless network components:



1. Access point (AP) — The base station.

   In general, an AP does not contain a switch. APs have no analogue in the wired world.

   The AP connects the wireless hosts to a switch through a single wired connection.

   Wireless hosts share bandwidth between AP and switch.

2. Wireless hosts.

3. Wireless links between hosts and access points.

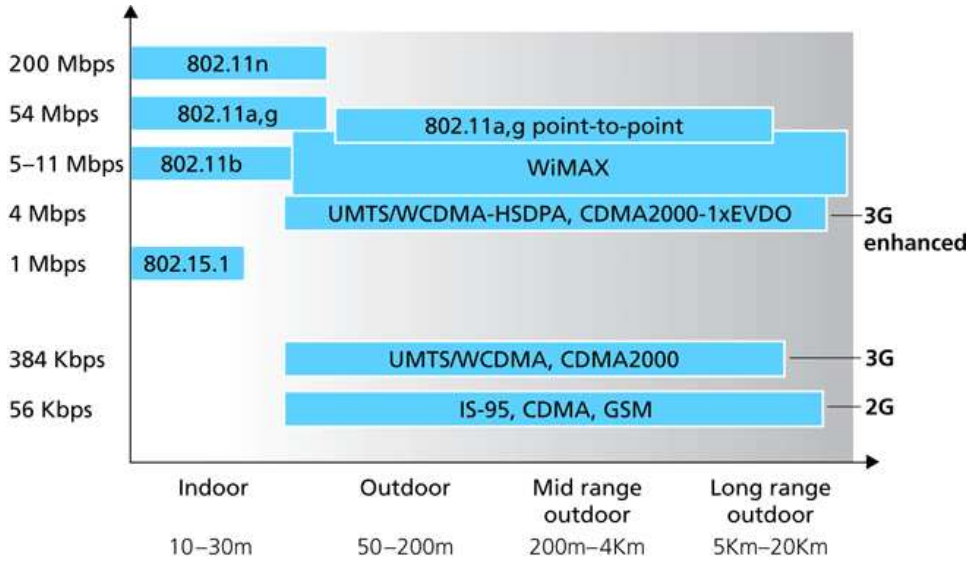
   A wireless host is associated with one AP.

   A *handoff* may be used to transfer a mobile wireless host between wireless networks.

Types of wireless networks

1. Infrastructure — includes an AP and other networking infrastructure.
2. Ad Hoc — no AP. Wireless hosts cooperate to form a standalone network.

Various wireless networking standards:



Notes:

1. 802.11 is for short-range networks.
2. Cellular wireless adapters are 3G enhanced devices (Verizon's 1xEVDO).
3. WiMAX is coming.

3 Wireless Network Characteristics

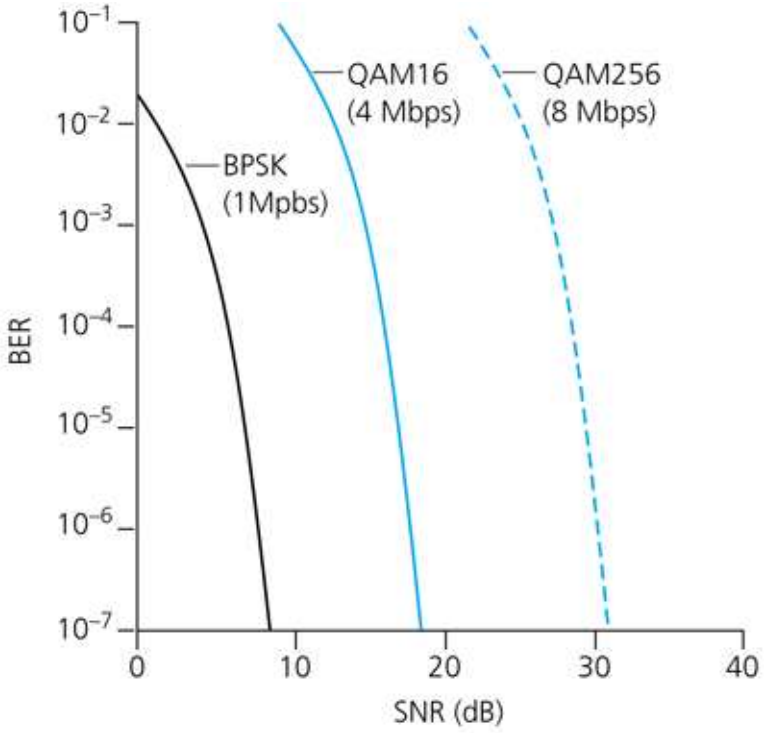
Basic characteristics:

1. Radio signal strength decreases with square of distance.

2. Interference. Other devices operate at 2.4 GHz: microwave ovens, cordless phones, baby monitors, other wireless networks, etc.

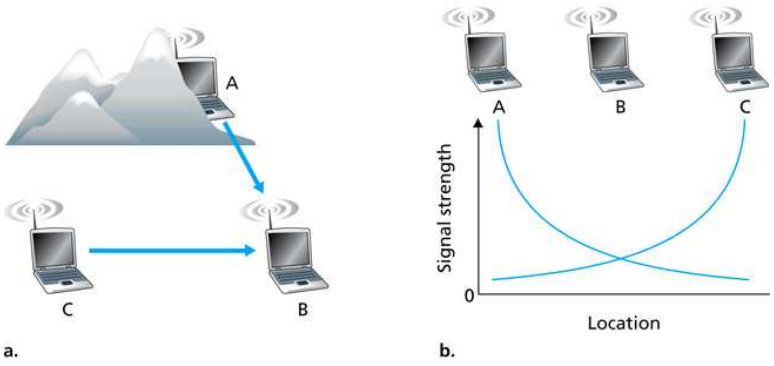
3. Multipath propagation — radio wave reflections result in multipath signal distortion.

These characteristics lead to varying SNR values. Lower SNR values lead to high bit error rates. Various bit encoding (modulation) techniques will be used to yield acceptable transmission characteristics:



Basically, transmit more slowly as SNR decreases.

Hidden terminal problem:



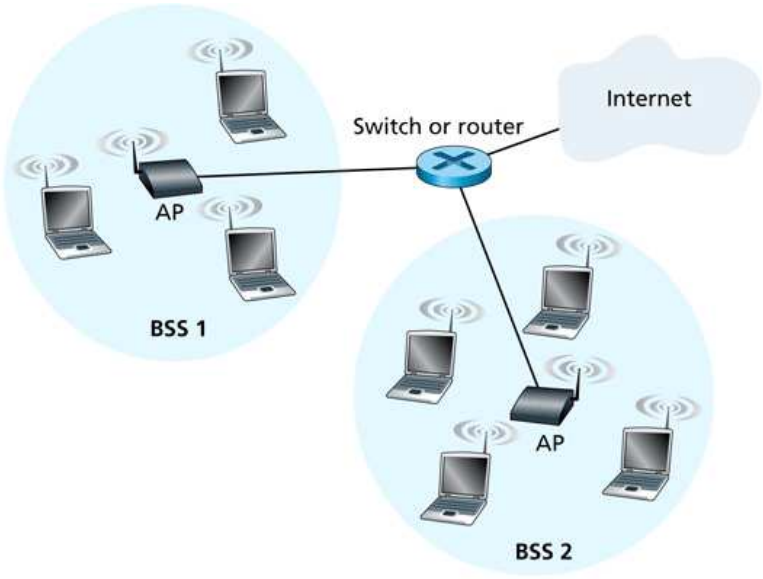
Two hosts may be within range of the AP, but not each other — they are hidden from each other.

Wireless networks employ CDMA (Code Division Multiple Access) to partition the bandwidth. *Collisions* can still occur.

4 WiFi — 802.11

1. Uses CSMA/CA — Carrier Sense Multiple Access, Collision Avoidance.

2. Basic Service Set (BSS): AP and wireless hosts.



3. The AP had two MAC addresses — one for the wireless side; one for the wired side.

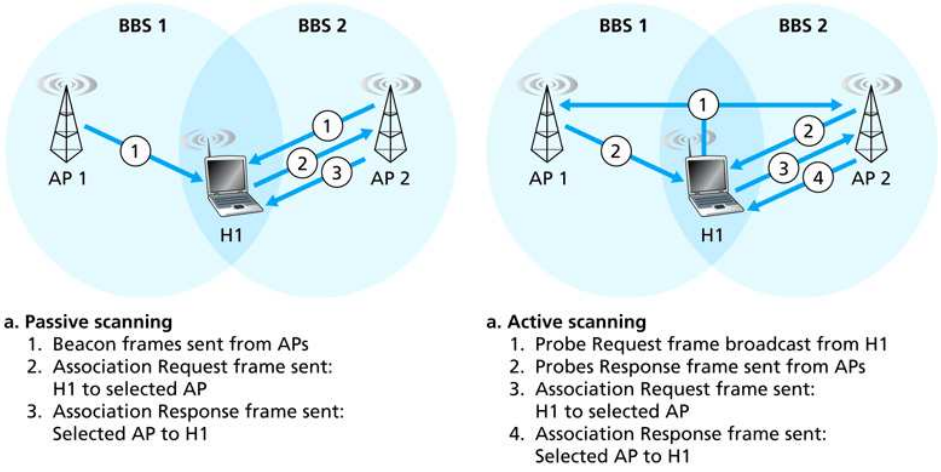
A "roaming" wireless host must first associate with a BSS

1. Each BSS assigned a Service Set ID (SSID).

2. An AP is assigned one of 11 channels to use.

3. Wireless host scans the channels, searching for beacon frames.

   Scanning may be done passively or actively:



a. 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

a. 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

   Beacon frame includes AP's SSID and MAC address.

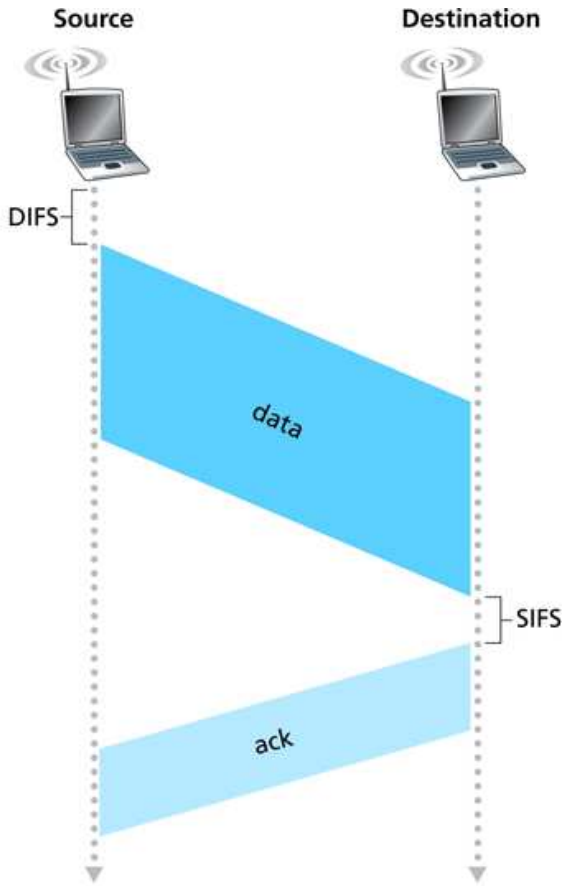
4. User is presented with list of available networks, and selects one with which to associate.

4.1 802.11 MAC Protocol

1. CSMA/CA — Collision avoidance, rather than collision detection due to hidden terminal problem and expense of building collision detection hardware (transmitted signal *much* strong than received signal — received signal may appear to be "random" noise).

   As a result, frames are transmitted in their entirety — never aborted.

2. Due to high bit error rate, link-layer acknowledgements are used:



Sender retransmits if ACK not received after a short wait.

3. CSMA/CA protocol:

   (a) If channel idle, wait DIFS (distributed inter-frame space) time and then transmit frame.

   (b) If channel busy, choose random backoff value and count down while channel idle.

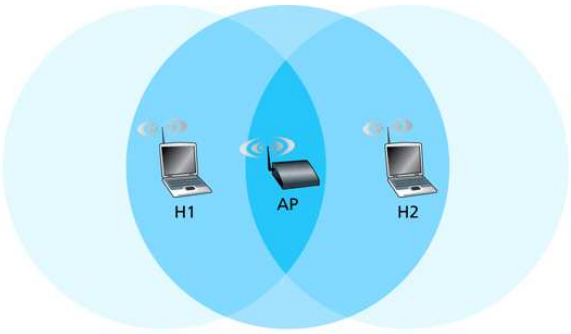
   When counter reaches zero, transmit frame.

   (c) If ACK received, return to step 2 to send next frame.

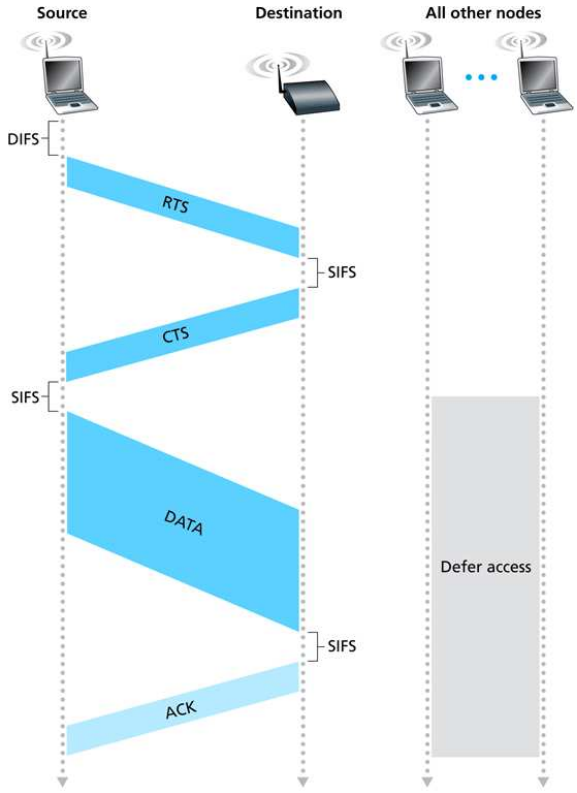
   Otherwise, backoff, using a larger choice interval, and retransmit.

   The random countdown helps to ensure that two hosts won't transmit at the same time after sensing the channel go from busy to idle — collision avoidance.

4. Hidden terminals are still a problem:



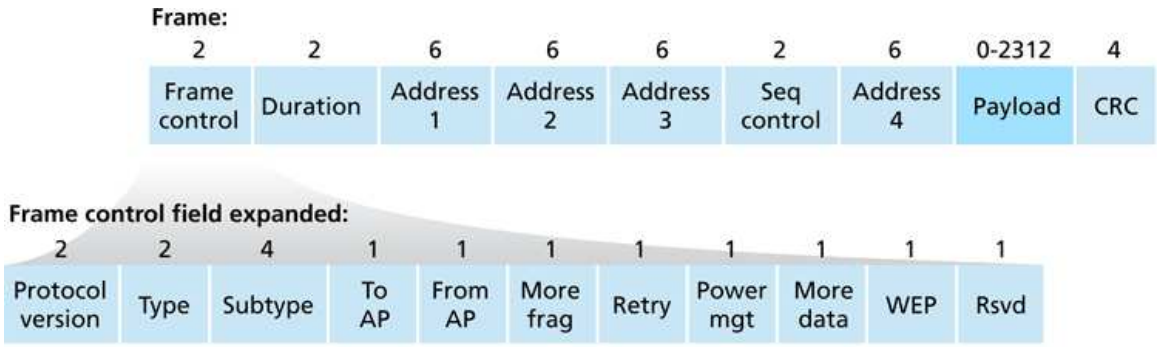
Hidden terminal collisions can be avoided by reserving a transmission slot:



(a) Host sends RTS frame, indicating total transmission time.

(b) AP responds with broadcast CTS frame, giving host permission to transmit and informing other hosts to remain silent.

4.2 802.11 Frame



Frame fields:

1. Frame Control:
   (a) Protocol version: Which version of 802.11 protocol.
   (b) Type and subtype: Which type of frame — data, RTS, CTS, beacon, etc.
   (c) More frag: Link layer fragmentation indication.
   (d) Retry: Retransmit indication.
   (e) Power management: Inform AP that host will be sleeping to save; power.

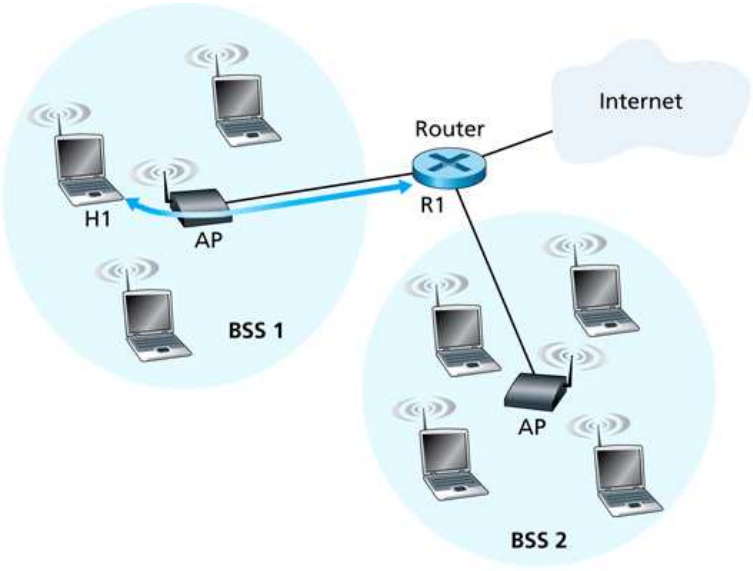
   Host will awaken just before beacon frame sent. Beacon frame will contain list of hosts for which frames have been buffered.

   (f) More data: AP informing host not to return to sleep.
2. Duration: Length of transmission in μs.
3. Address 1: Destination's MAC address.
4. Address 2: Source's MAC address.

5. Address 3: MAC address of router interface attached to AP.

   Why three addresses? The AP needs a MAC address, but it's not a part of the network.

   Example:



   R1 to H1:

   (a) R1 uses ARP to get H1's MAC address; sends an Ethernet frame out the appropriate interface.

   (b) AP receives frame, constructs an 802.11 frame with H1's MAC address in address 1, its MAC address in address 2, and R1's address in address 3.

   H1 to R1:

   (a) H1 constructs an 802.11 frame with AP's MAC address in address 1, H1's MAC address in address 2, R1's address in address 3.

       H1 only knows R1's address because it appeared in prior frame's address 3 field.

6. Sequence control: Used for fragment reassembly.

Advanced features:

1. Rate adaptation: Two consecutive retransmits results in backing down to the next lowest transmission rate.

   10 successful frames in a row (no retransmits) or fallback timer timeout results in increasing to next highest transmission rate.

2. Power management: Previously discussed. Sleep time can be 99% of total time.