Wireless and WiFi

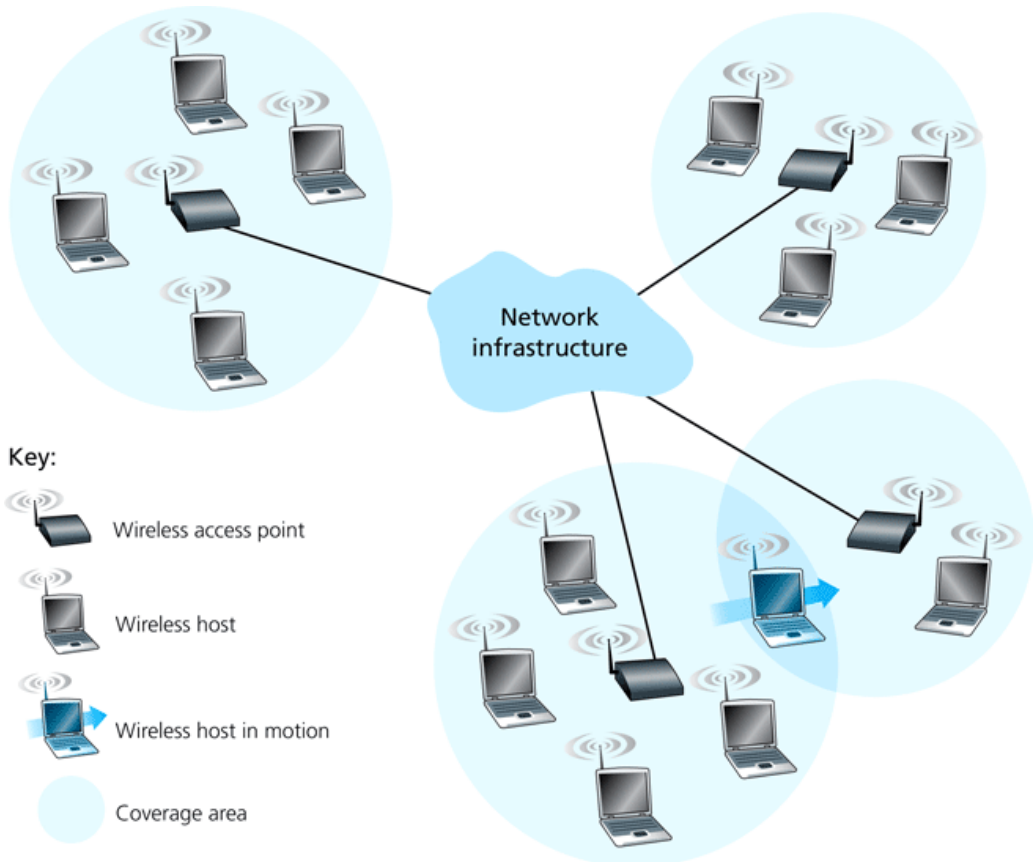
Daniel Zappala

CS 460 Computer Networking
Brigham Young University

Wireless Networks

- **mobile phone subscribers now outnumber wired phone subscribers**
- similar trend likely with Internet use
  - Internet-enabled cell phones
  - popularity of wireless access protocols
- many challenges
  - communication over a highly lossly wireless link
  - providing last-hop connectivity to mobile Internet users
  - providing connectivity in networks of mobile users

Wireless Networks



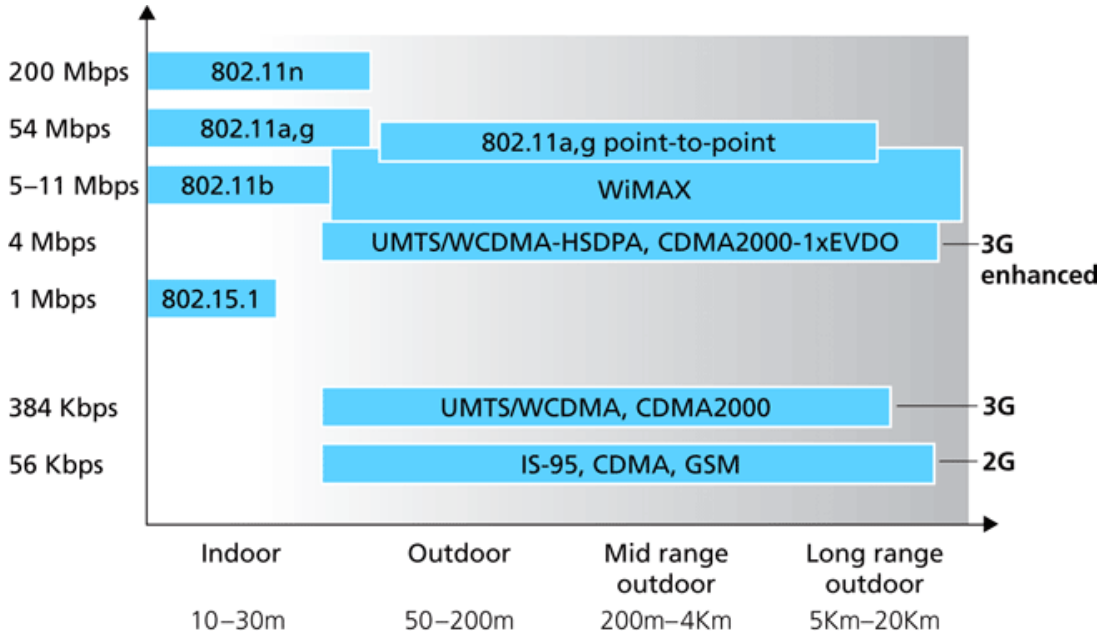
- access point/base station/cell tower: relay between wireless and wired nodes
- handoff for mobile devices

Types of Networks

- **single hop, infrastructure**: base station that provides access to the Internet for mobile devices
- **single hop, infrastructure-less**: peer-to-peer connections between devices, e.g. WiFi P2P, Bluetooth
- **multiple hop, infrastructure**: provide Internet access through multiple wireless hops, e.g. wireless mesh, sensor networks
- **multiple hop, infrastructure-less**: provide wireless connectivity when the Internet is not available, e.g. mobile ad hoc networks, vehicular ad hoc networks, developing countries or battlefields

Wireless Links and Networks Characteristics

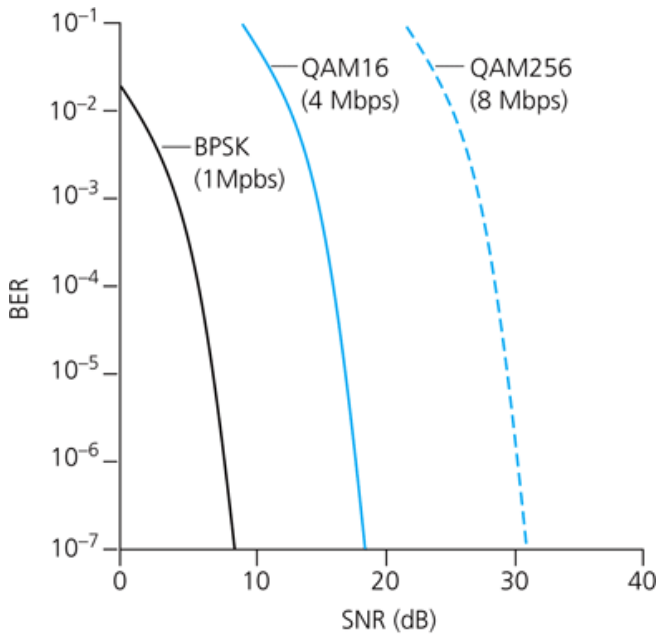
Wireless Technologies



- radio signal strength weakens as it propagates
- interference from other sources and other devices (phones, motors) can cause packet loss
- radio signal can bounce off objects, arriving at destination multiple times

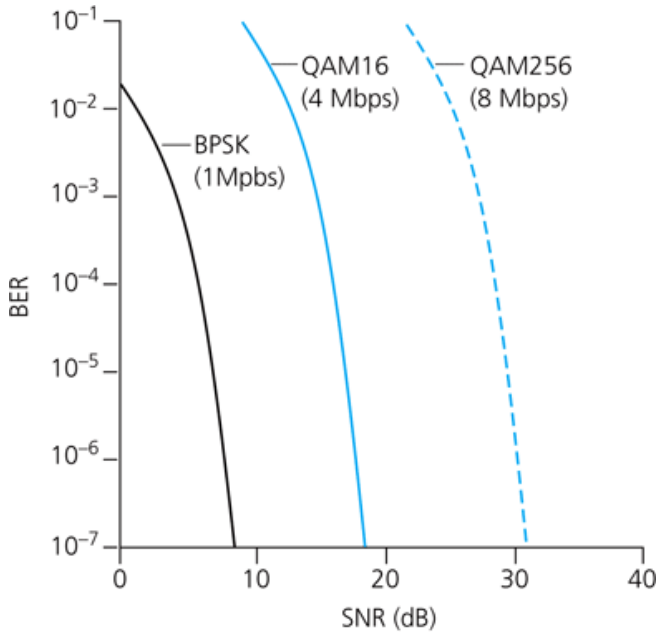
Wireless Signals

- BER: bit error rate
- SNR: signal-to-noise ratio
- BPSK : modulation scheme used in 802.11
- QAM: modulation scheme used in cable modems, digital TV



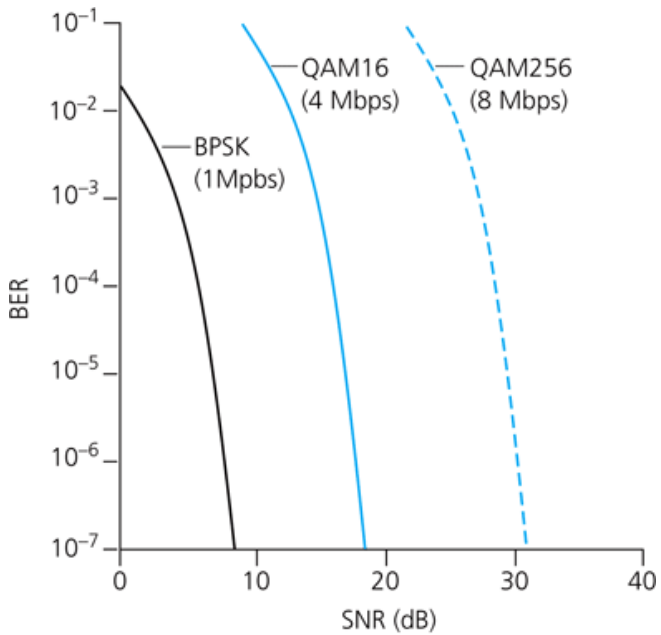
Wireless Signals

- for a given modulation scheme, the higher the SNR, the lower the BER
  - increase transmission power to lower SNR
  - too high, and you interfere with other wireless users and you don't gain much in BER



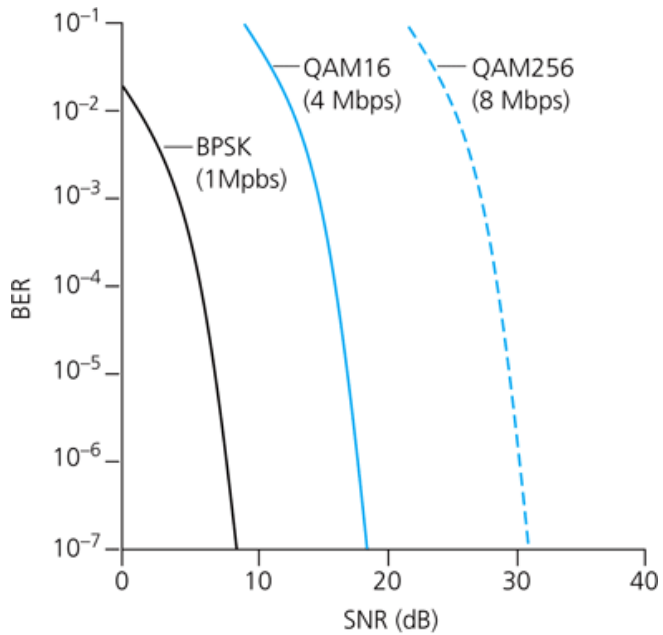
Wireless Signals

- for a given SNR, a modulation technique with higher transmission rate will have a higher BER



Wireless Signals

- for a given transmission power, dynamically adjust the modulation technique to adapt to changing SNR

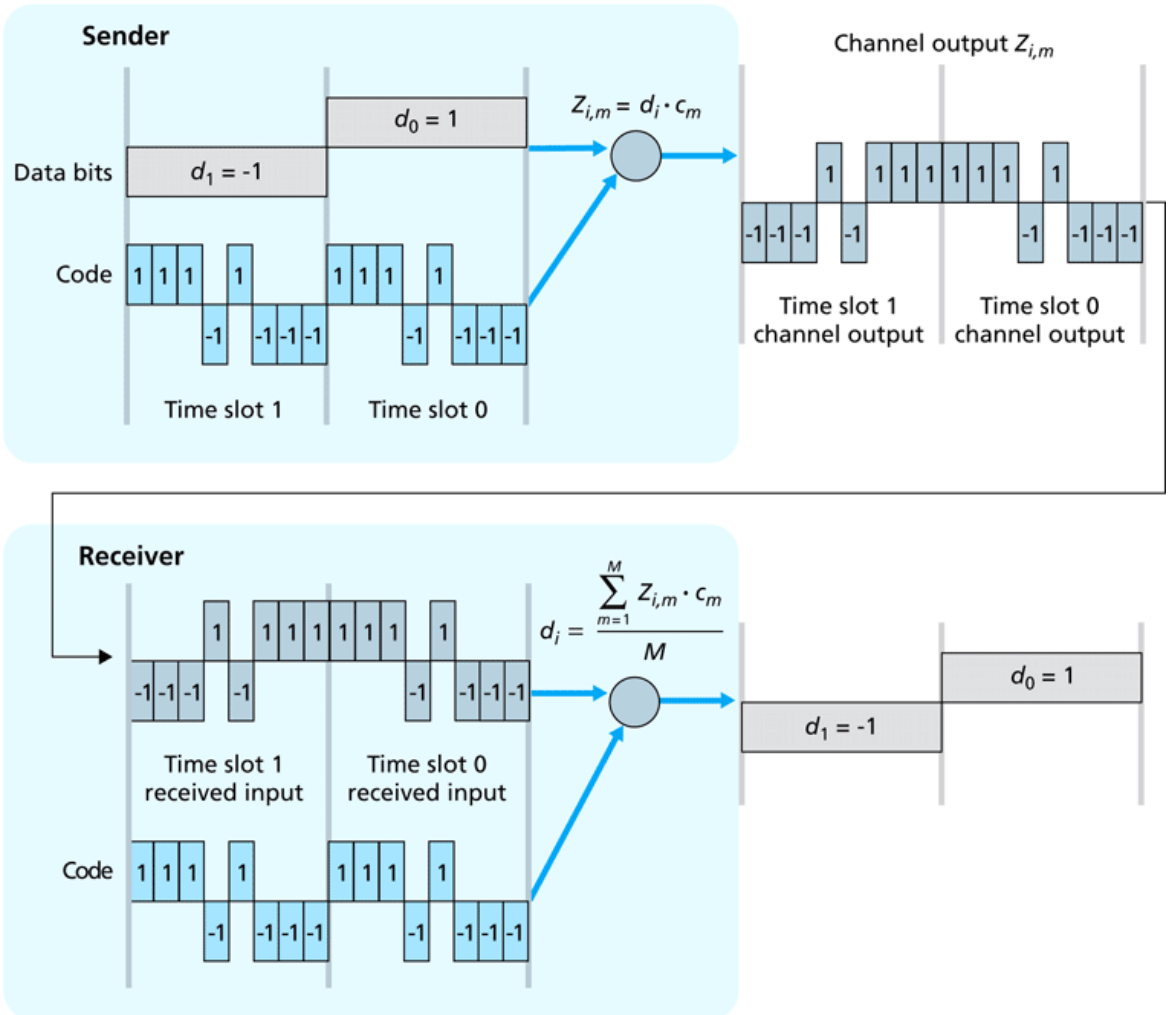


CDMA

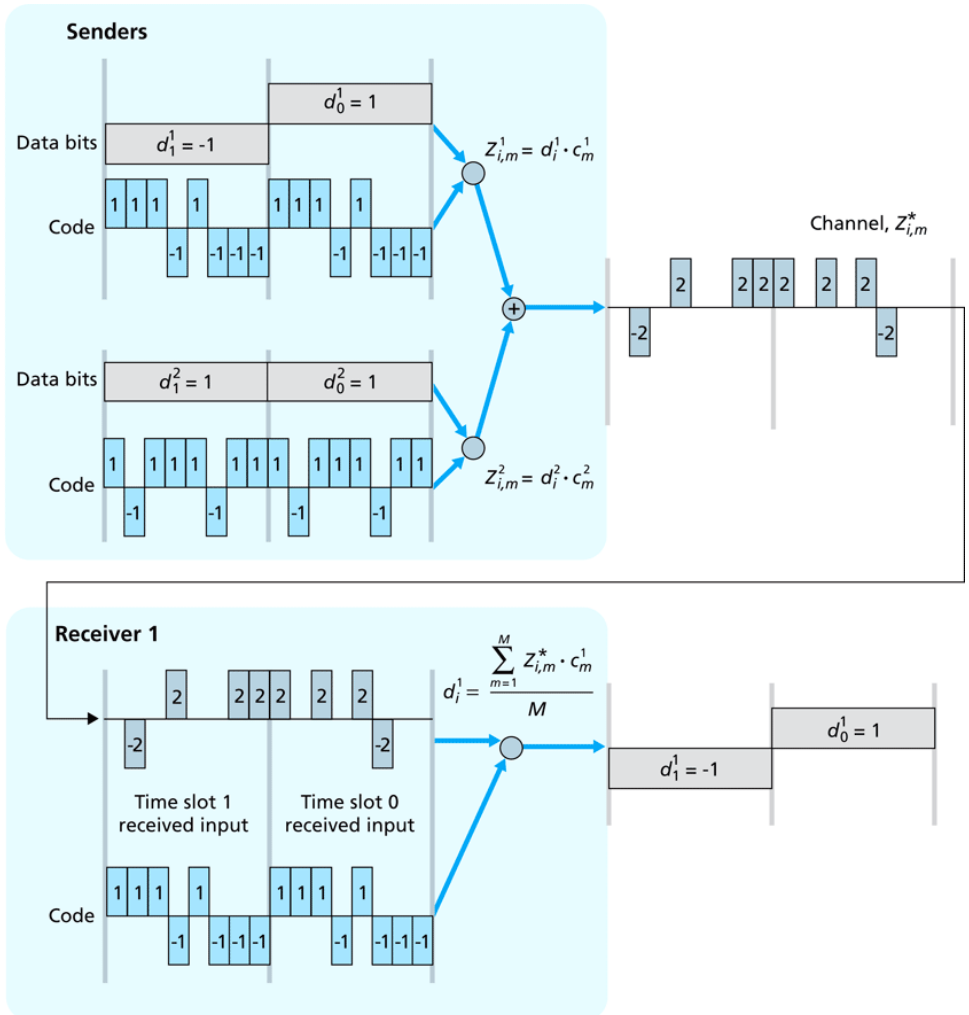
CDMA: Code Division Multiple Access

- first described on paper by an actress and a musician: Hedy Lamarr and George Antheil in 1941
  - described a secure radio link to control torpedos
  - ignored by U.S. Army, forgotten until 1980s
- used in several wireless standards (cellular, satellite)
- unique code assigned to each user, use code (chipping sequence) to encode and decode signal
- multiple users coexist and transmit at the same time with minimal interference if codes are chosen correctly

CDMA Encoding and Decoding



CDMA With Two Senders



CDMA advantages

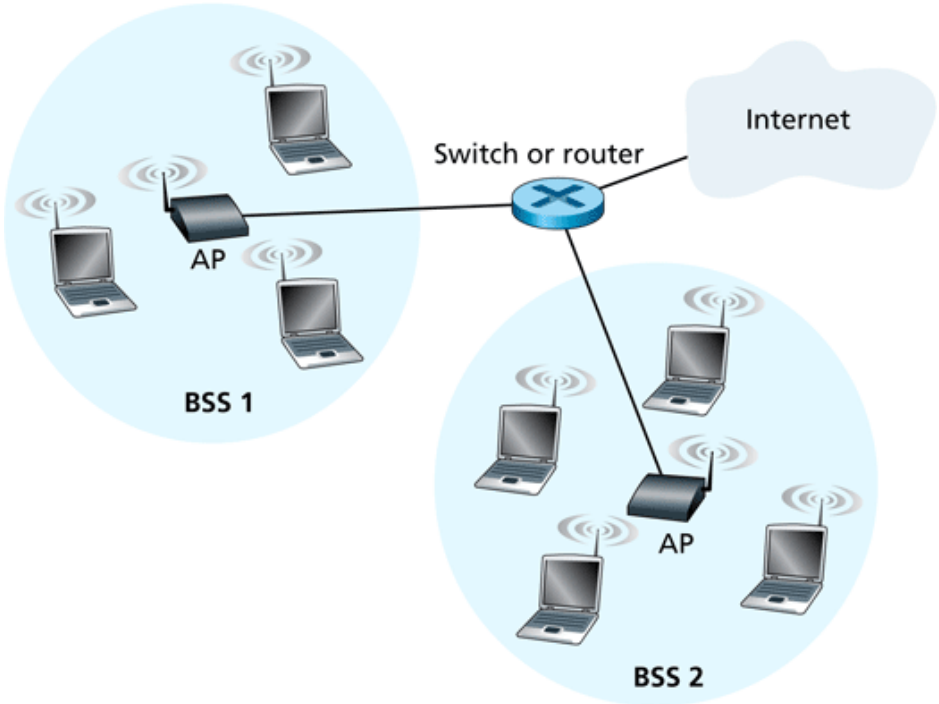
- number of codes is essentially infinite
- avoids the overhead of continually allocating and deallocating time or frequency slots as with TDMA and FDMA
- simply send when you have something to say, and go off the air when you don't
- $\Rightarrow$ ideally suited to large numbers of transmitters, each generating a small amount of traffic at irregular intervals

WiFi

IEEE 802.11 Wireless Standards

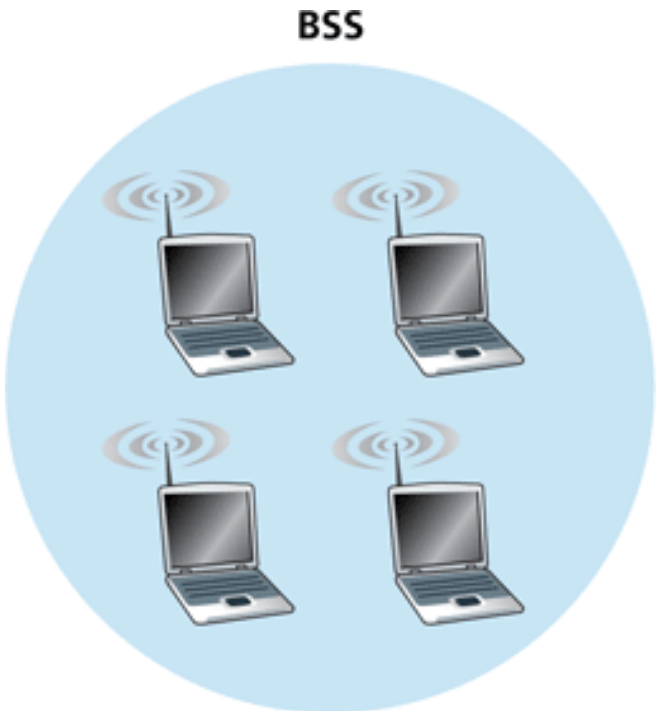
- 802.11b
  - 2.4 - 5 GHz unlicensed spectrum
  - up to 11 Mbps (6 - 7 in practice)
  - direct sequence spread spectrum (DSSS) - type of CDMA with all hosts use the same chipping code
- 802.11a
  - 5 - 6 GHz regulated frequency
  - less interference, but need more access points
  - up to 54 Mbps (25 Mbps in practice)
- 802.11g
  - 2.4 - 5 GHz
  - up to 54 Mbps (25 Mbps in practice)
- all use CSMA/CA for multiple access

802.11 LAN Architecture



- AP = Access Point
- BSS = Basic Service Set (cell) - collection of AP and hosts within its range

802.11 Ad Hoc Networks

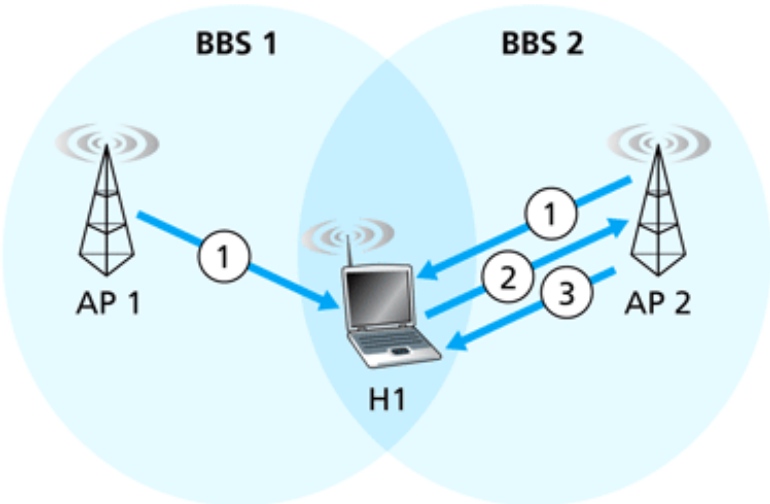


- self-organize to form a network without access points
- between laptops and handheld devices in a conference room, train, or car, on the battlefield or in a search and rescue operation

Channels and Association

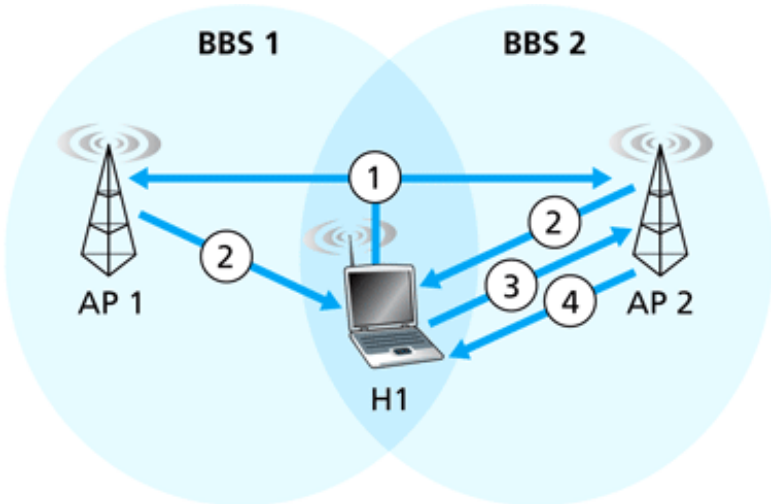
- 802.11b: spectrum divided into 11 channels
  - set frequency manually at AP
  - interference possible if another AP using the same frequency
- host must associate with an AP
  - scan channels listening for beacon frames containing SSID and MAC address
  - select AP to associate with
  - may perform authentication
  - run DHCP to get IP address in AP's subnet

Passive and Active Scanning



a. Passive scanning

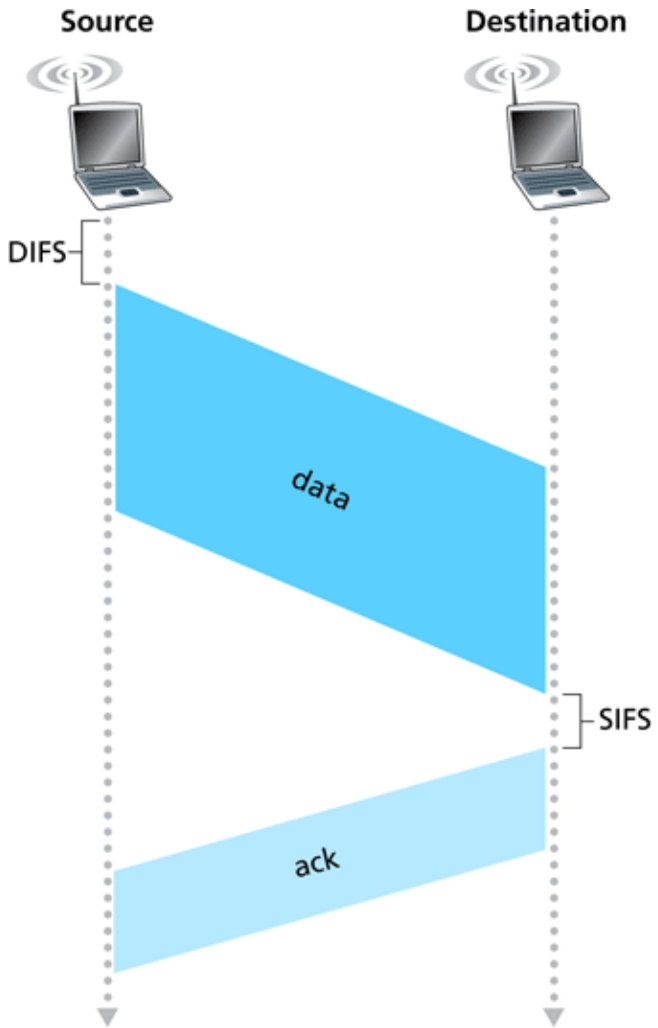
1. Beacon frames sent from APs
2. Association Request frame sent: H1 to selected AP
3. Association Response frame sent: Selected AP to H1



a. Active scanning

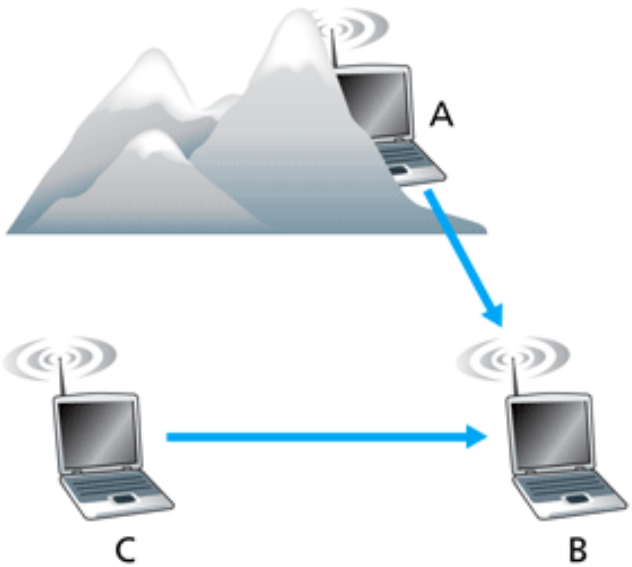
1. Probe Request frame broadcast from H1
2. Probes Response frame sent from APs
3. Association Request frame sent: H1 to selected AP
4. Association Response frame sent: Selected AP to H1

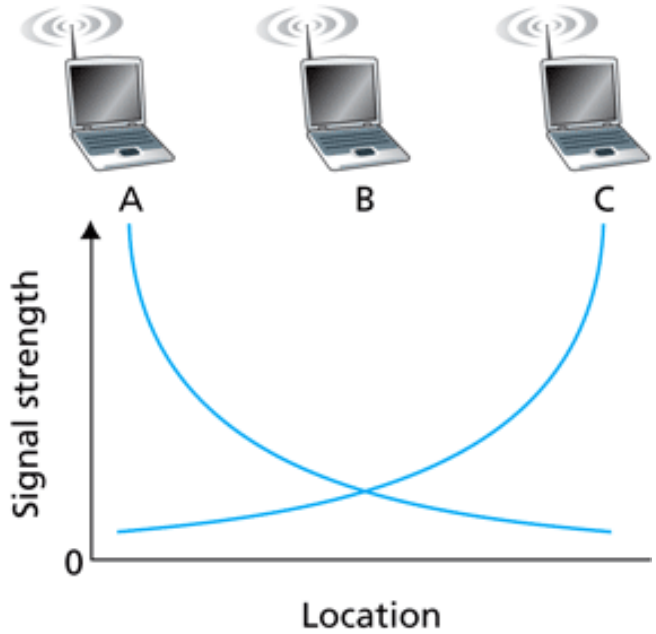
CSMA/CA



- sense before transmitting
- if channel idle for DIFS, send frame
- if channel busy then backoff a random time
- double backoff interval with each successive collision
- if receiver gets frame OK, wait SIFS and then ACK

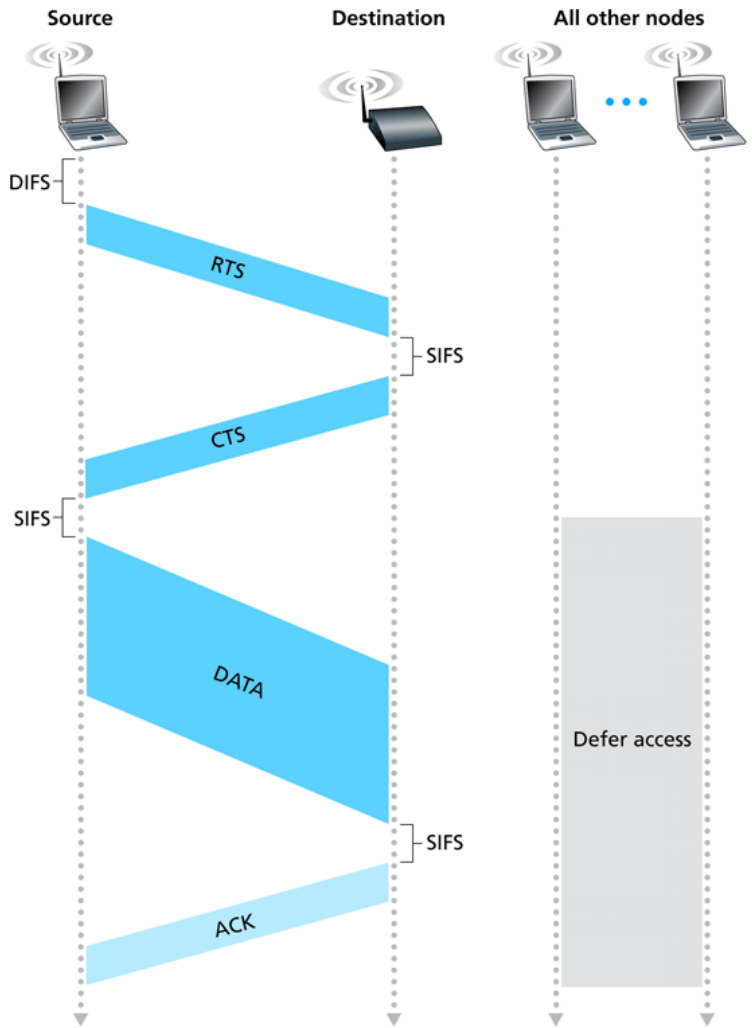
Hidden Terminal Problem and Signal Fading





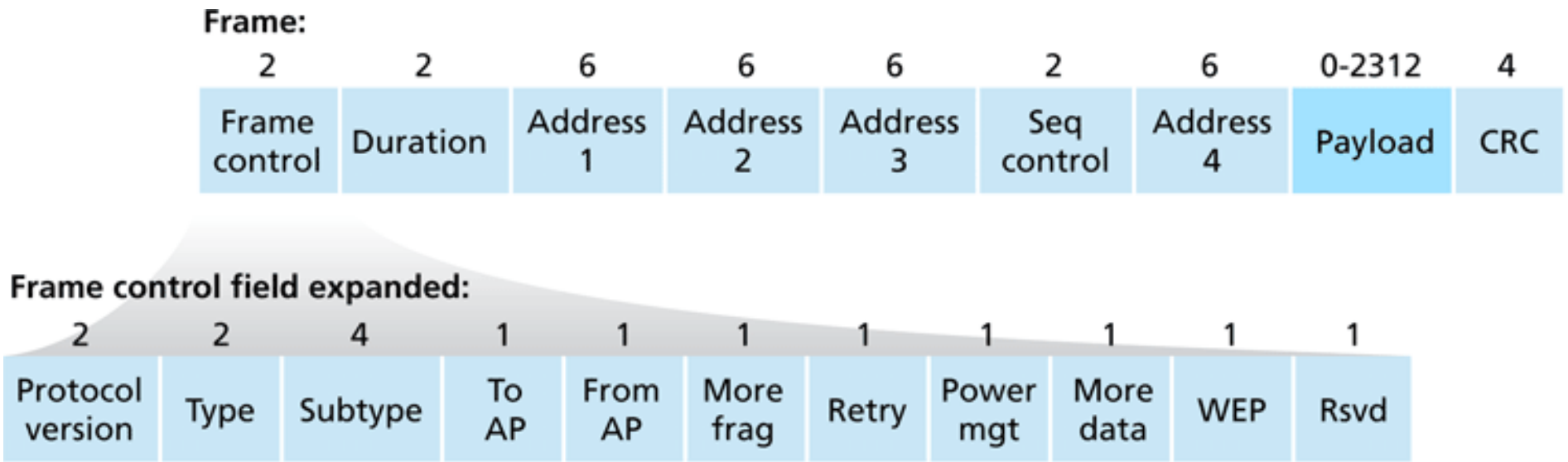
- A and C communicate with B but cannot hear each other due to obstacles or signal fading

Using RTS/CTS



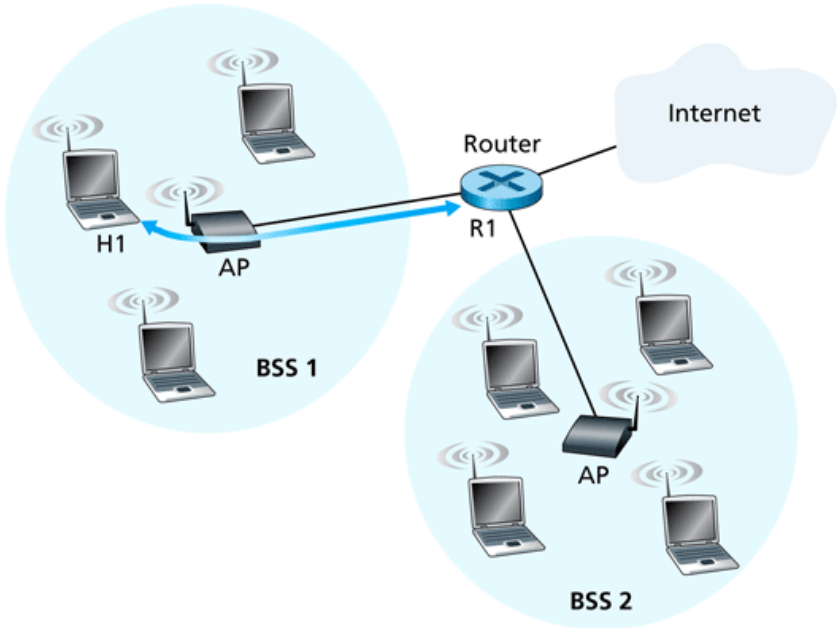
- use RTS/CTS frames to reserve channel
- RTS/CTS are small so collision doesn't waste as much time, avoids collisions with longer data frames

Frame Format



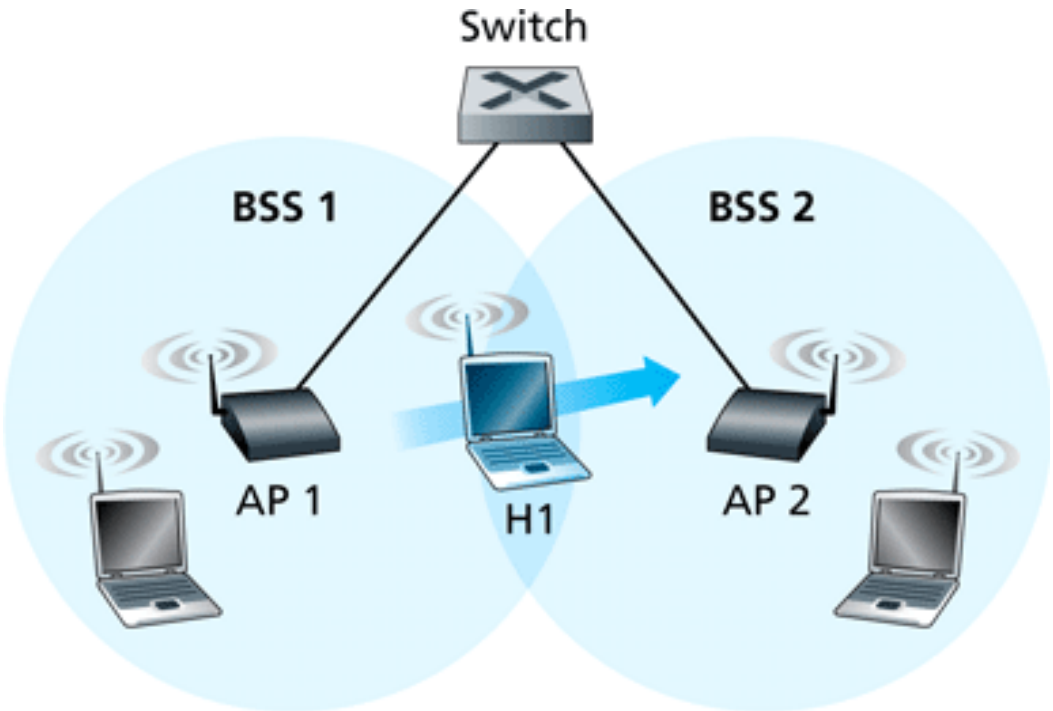
- MAC address 1: wireless destination
- MAC address 2: wireless source
- MAC address 3: router interface to which AP is attached
- MAC address 4: for ad hoc mode
- duration: reserved time
- sequence control: sequence number

Use of Address Fields



- R1 sends frames to H1, H1 sends frames to R1 – the AP is transparent to the connection at the IP level
- When the AP sends a message to H1, or when H1 sends a message to the AP, they put R1's MAC address in the Address 3 field

Mobility



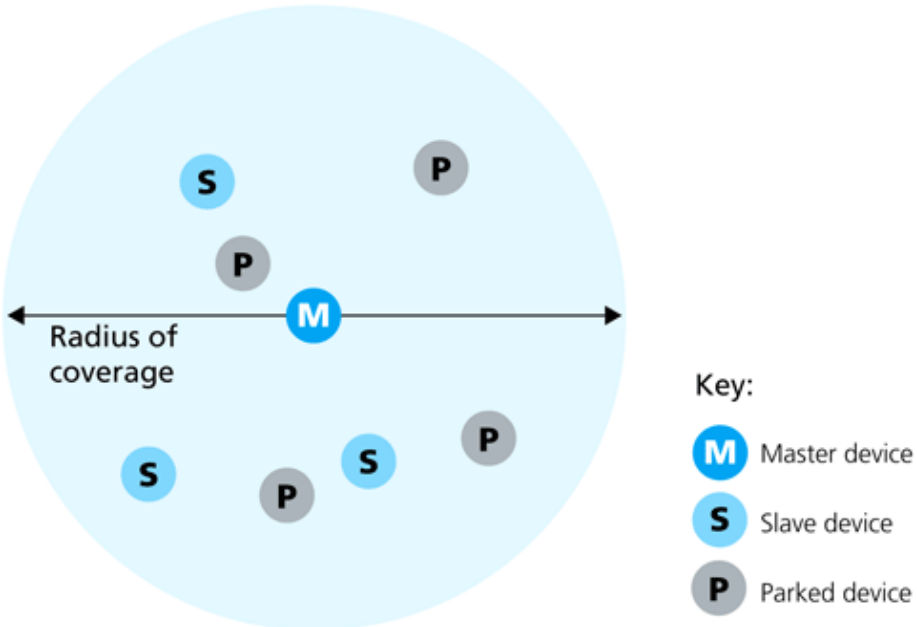
- H1 remains on the same IP subnet but changes APs
- switch must use self-learning to remember which AP H1 is associated with

Rate Adaptation and Power Management

- rate adaptation
  - when a user moves farther from an access point, change the modulation scheme
  - moving farther = higher BER
  - generally switch to a lower bit rate, rather than increasing transmission power
  - fall to lower rate if two frames in a row without an ACK
  - increase rate if 10 frames in a row successful, or a timer fires
- power management
  - put interface to sleep to save power
  - notify AP when sleeping by setting a bit in the frame header
  - wake up every 100 ms to hear the next beacon frame
  - AP buffers frames and sends when node wakes up

Low Power

BlueTooth



- 802.15
  - 2.4 - 2.5 GHz
  - 721 Kbps
- less than 10 m diameter
- replacement for cables (mouse, keyboard, headphones)
- slave devices request permission to send to master devices
- wearable computing

Zigbee

- 802.14.5
  - 915 Mhz in USA
  - 20, 40, 100, 250 Kbps
- designed for low power, low data rate, low duty cycle applications
- temperature and light sensors, sprinklers, security devices
- full-function and reduced-function devices, like Bluetooth
  - full-function devices can act as a mesh
  - uses beacon frames, link-layer ACKs, carrier-sense, random access, allocation of slots
- alternating sleep and active periods, to conserve power