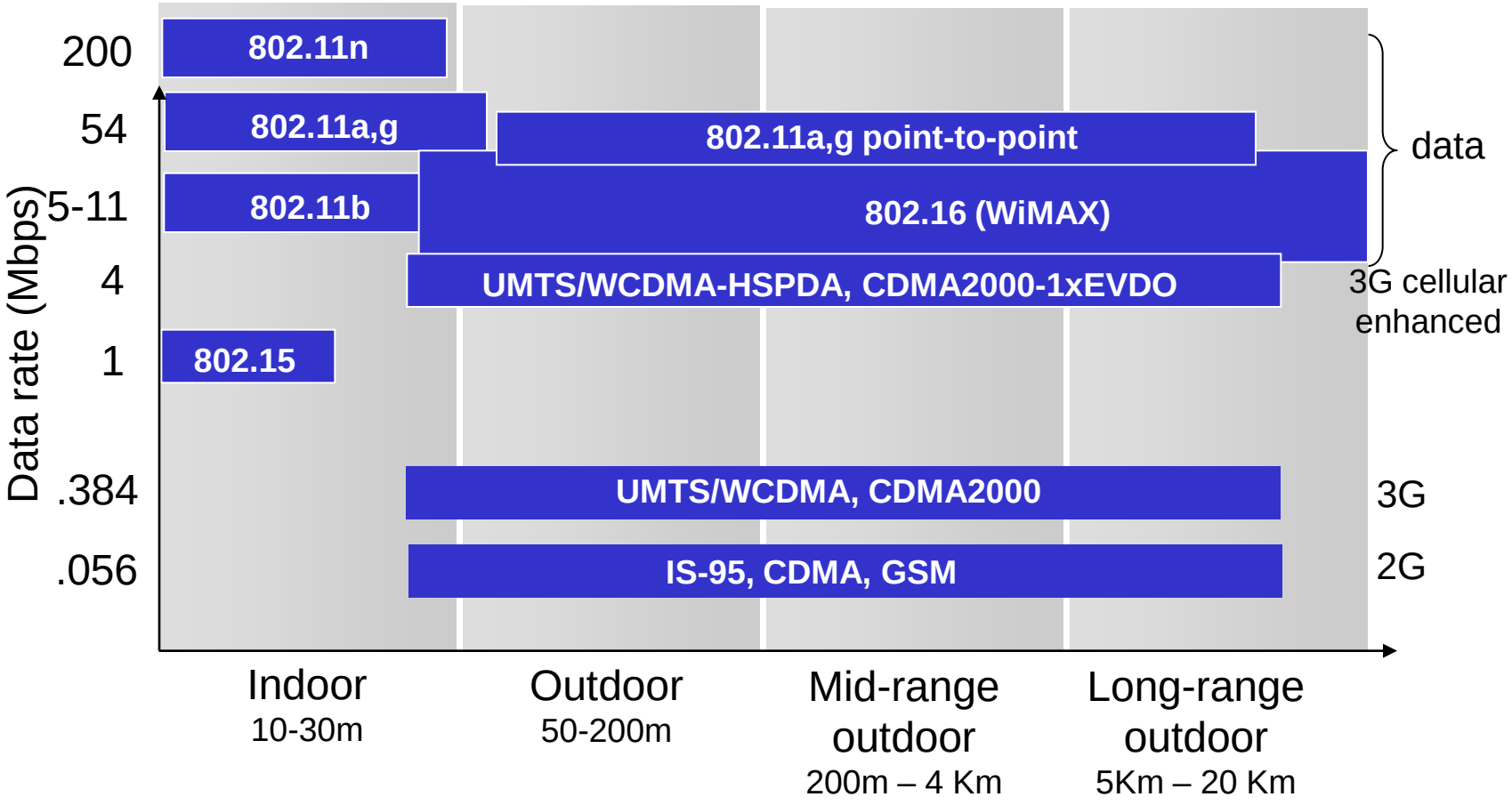
STEVENS
Institute of Technology

Introduction to Wireless Communication

IEEE 802.11 Wireless LAN

- Stimulated by availability of unlicensed spectrum
  - U.S. Industrial, Scientific, Medical (ISM) bands
  - 902-928 MHz, 2.400-2.4835 GHz, 5.725-5.850 GHz
- Targeted wireless LANs @ 20 Mbps
- MAC for high speed wireless LAN
- Ad Hoc & Infrastructure networks
- Variety of physical layers

Characteristics of selected wireless link standards



802.11 Definitions

- Basic Service Set (BSS)
  - Group of stations that coordinate their access using a given instance of MAC
  - Located in a Basic Service Area (BSA)
  - Stations in BSS can communicate with each other
  - Distinct collocated BSS's can coexist
- Extended Service Set (ESS)
  - Multiple BSSs interconnected by Distribution System (DS)
  - Each BSS is like a cell and stations in BSS communicate with an Access Point (AP)
  - Portals attached to DS provide access to Internet

IEEE 802.11 Wireless LAN

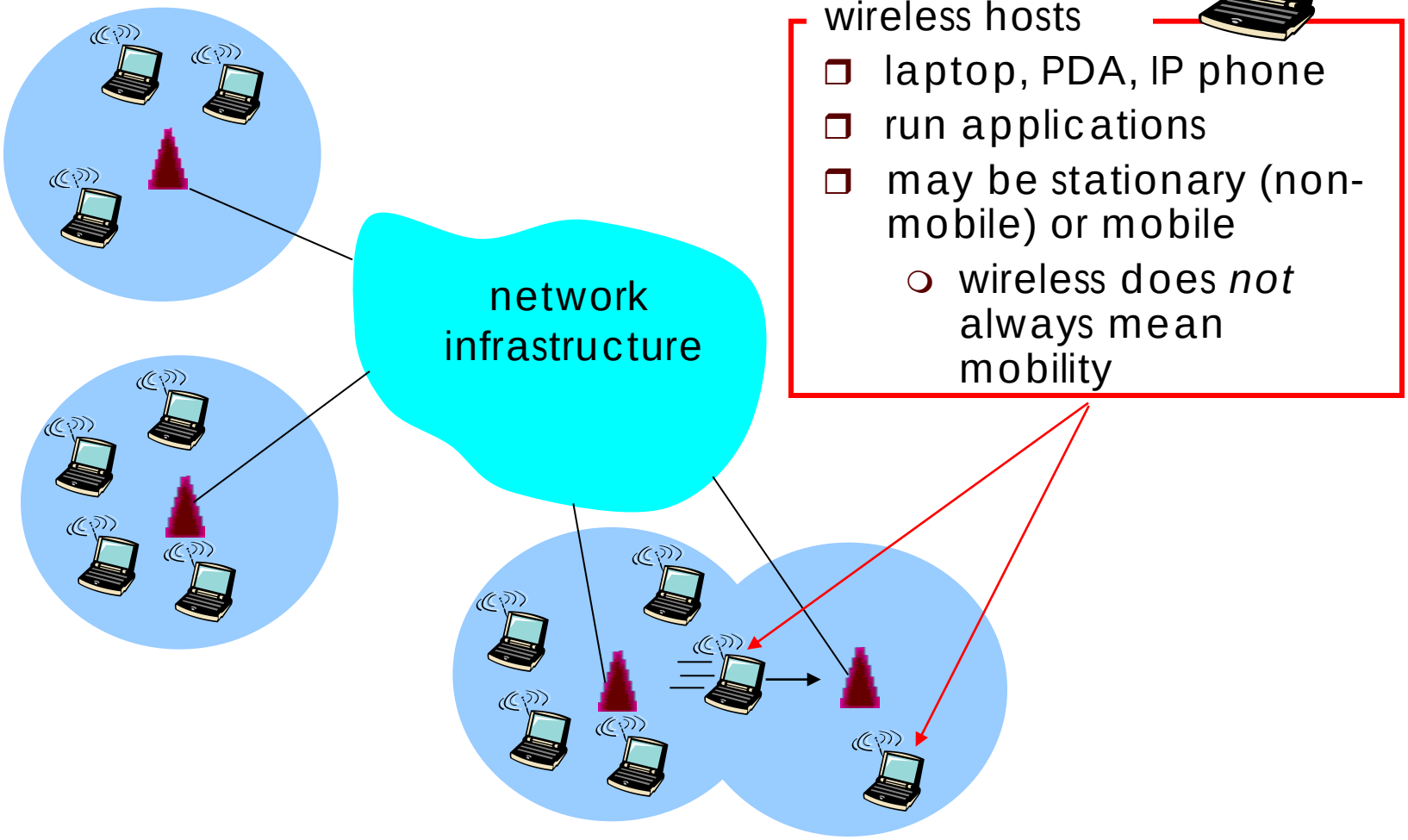
- 802.11b
  - 2.4-5 GHz unlicensed spectrum
  - up to 11 Mbps
  - direct sequence spread spectrum (DSSS) in physical layer
- 802.11a
  - 5-6 GHz range
  - up to 54 Mbps
- 802.11g
  - 2.4-5 GHz range
  - up to 54 Mbps
- 802.11n: multiple antennae
  - 2.4-5 GHz range
  - up to 200 Mbps

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

IEEE 802.11 Architecture

- Infrastructure mode
  - Basic Service Set (BSS)
  - Access Point (AP) and stations (STA) take different roles
  - Distribution system (DS) interconnect multiple BSSs to form a single network (not specified in the standard)
- Ad hoc mode
  - Independent Basic Service Set (IBSS)
  - Single-hop (the standard makes this assumption either explicitly or implicitly)

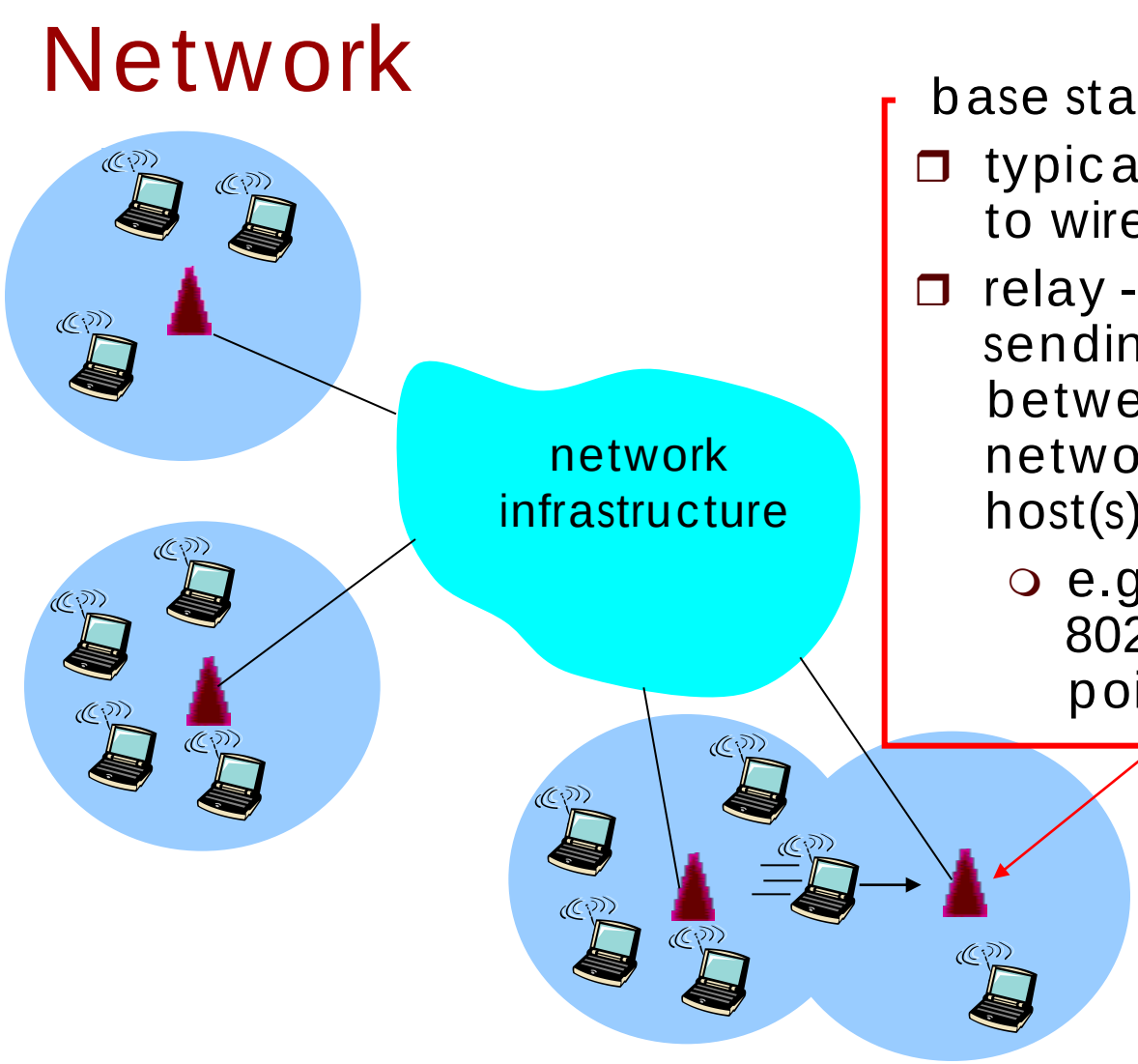
Elements of a Wireless Network



wireless hosts

- laptop, PDA, IP phone
- run applications
- may be stationary (non-mobile) or mobile
  - wireless does *not* always mean mobility

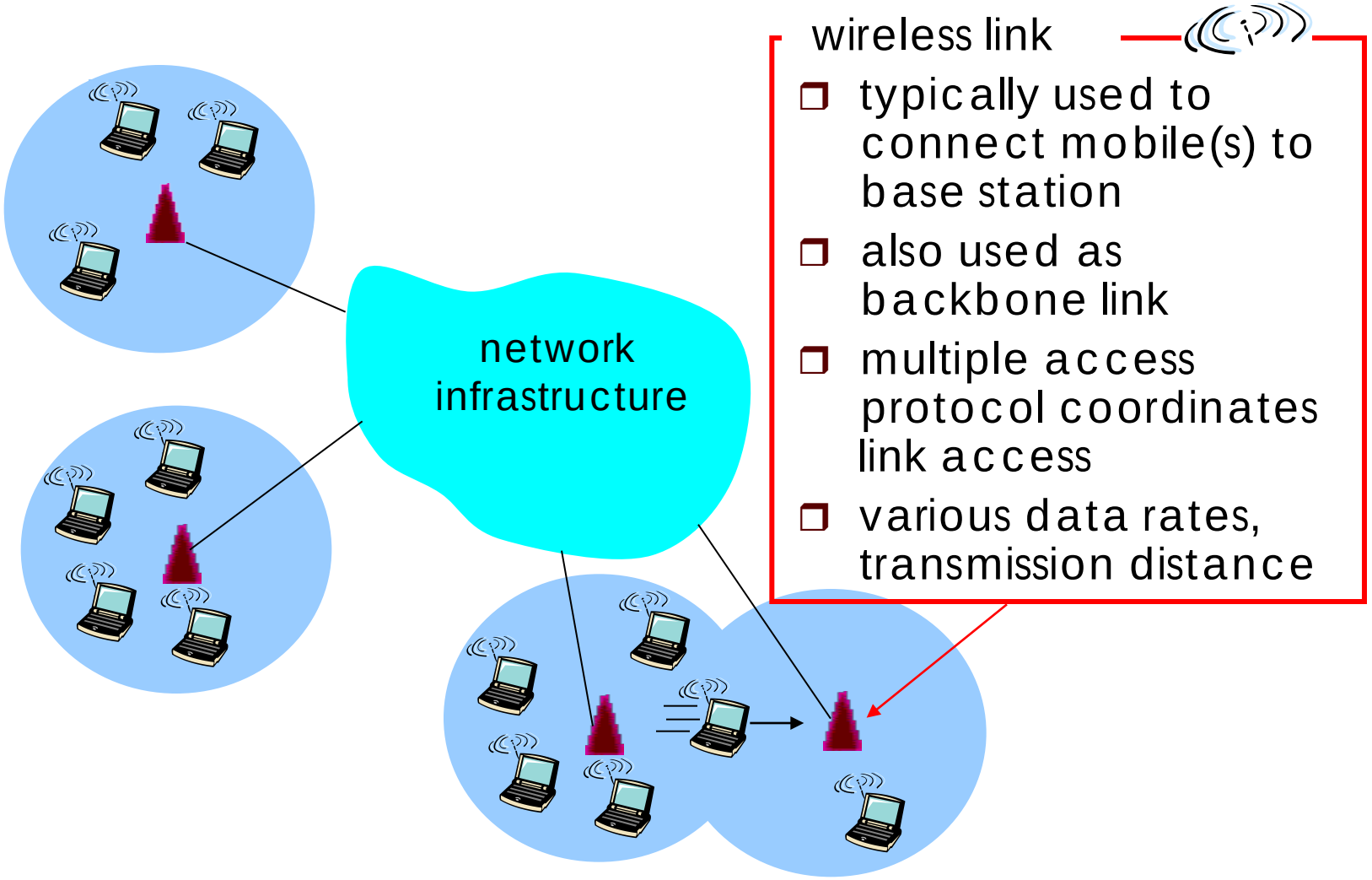
Elements of a Wireless Network



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

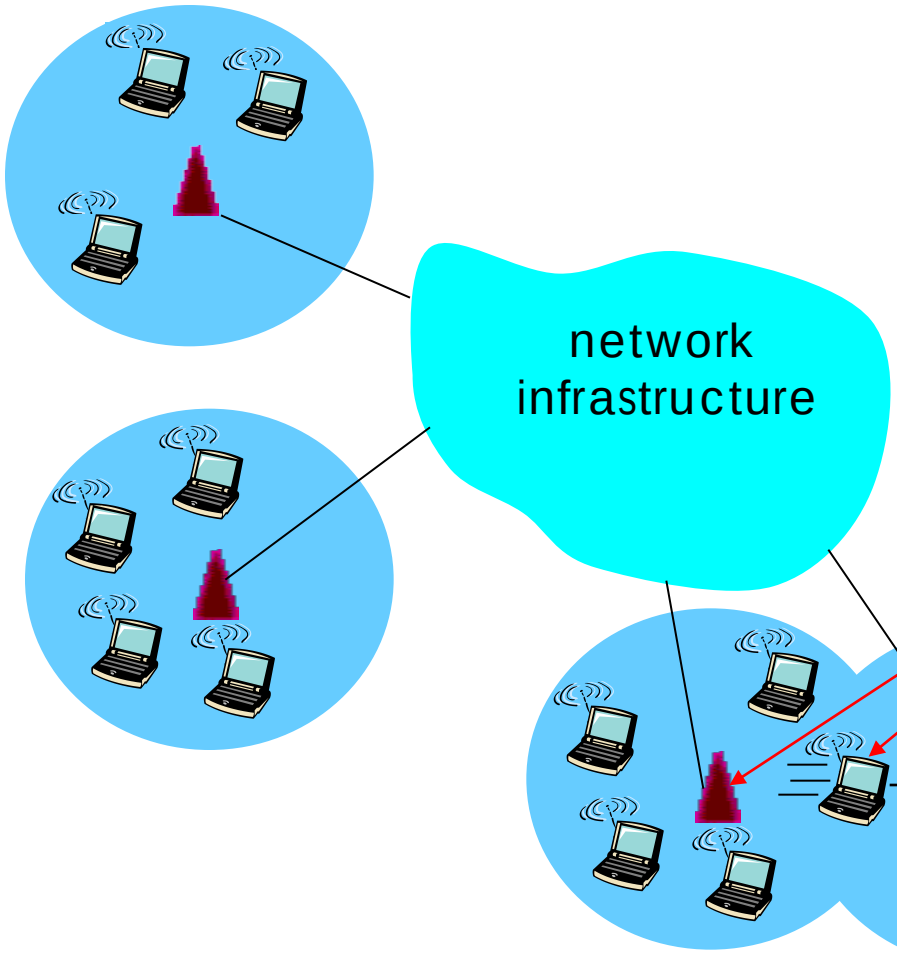
Elements of a Wireless Network



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

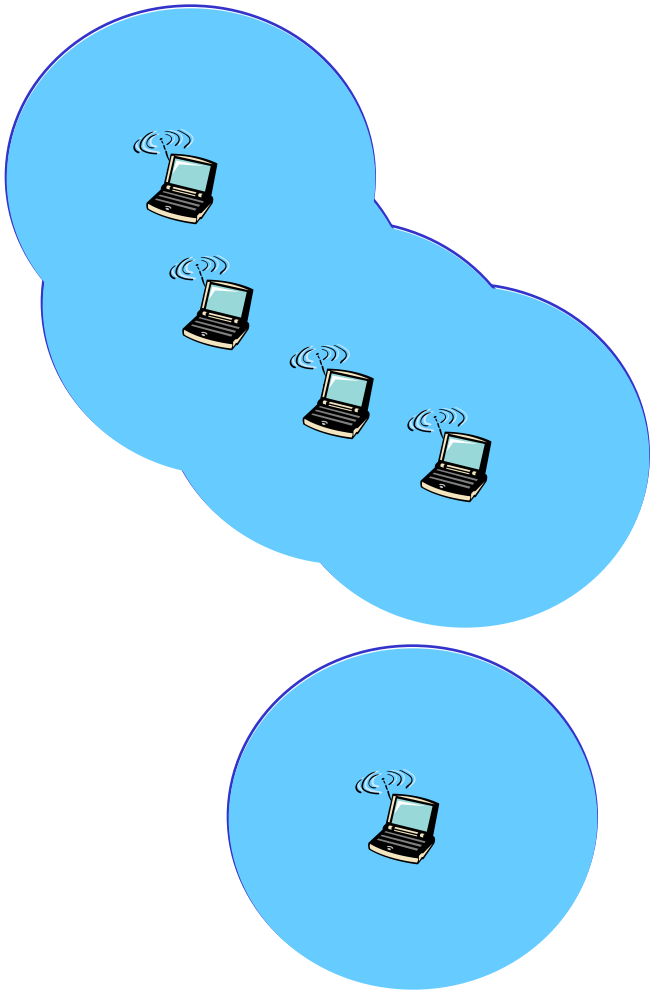
Elements of a Wireless Network



infrastructure mode

- base station connects mobiles into wired network
- handoff: mobile changes base station providing connection into 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

Infrastructure vs. Ad-Hoc Mode

- The infrastructure BSS is defined in terms of the distance from the Access Point
  - There is no restriction on the distance between the STAs (in fact they can be hidden from each other)
- In the infrastructure mode, STAs must associate (or bind) with the Access Point to obtain network services
  - STAs must initiate the association process and the Access Point may grant or deny access based on authentication

IEEE 802.11: Channels

- 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
  - will typically run DHCP to get IP address in AP's subnet

IEEE 802.11: Multiple Access

- Avoid collisions: multiple 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 Wireless MAC

- Support broadcast, multicast, and unicast

- Distributed and centralized MAC access
  - Distributed Coordination Function (DCF)
    - Basic CSMA/CA
    - RTS/CTS extension
  - Point Coordination Function (PCF)
    - contention-free polling for time-bounded service

Unreliability in wireless links

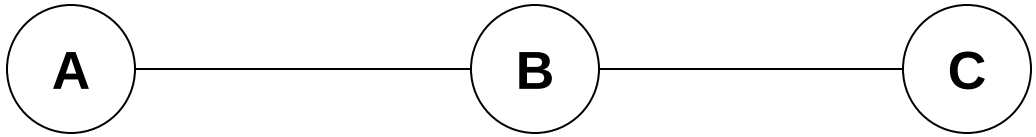
- Wireless links are prone to errors. High packet loss rate detrimental to transport-layer performance

- Mechanisms needed to reduce packet loss rate experienced by upper layers

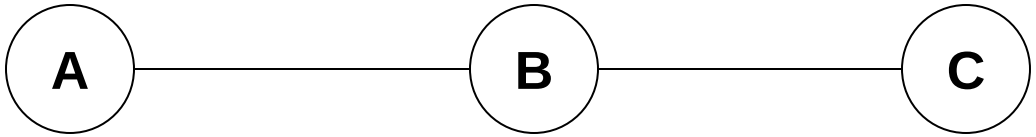
A Simple Solution to Improve Reliability

- When B receives a data packet from A, B sends an Acknowledgement (ACK) to A

- If node A fails to receive an ACK, it will retransmit the packet

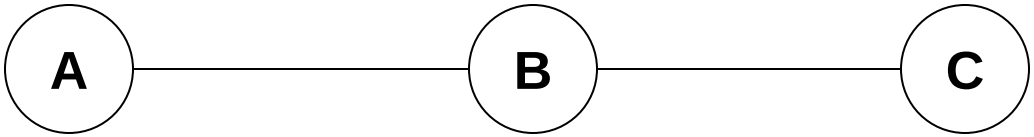


802.11 Hidden Node/Terminal Problem



- B can communicate with both A and C
- A and C cannot hear each other
- Problem
  - When A transmits to B, C cannot detect the transmission using the carrier sense mechanism
  - If C transmits, collision will occur at node B
- Solution
  - Hidden sender C needs to defer: but how?

Solving Hidden Node/Terminal Problem



- When A wants to send a packet to B, A first sends a Request-to-Send (RTS) to B
- On receiving RTS, B responds by sending Clear-to-Send (CTS), provided that A is able to receive the packet
- When C overhears a CTS, it keeps quiet for the duration of the transfer
  - Transfer duration is included in both RTS and CTS

Infrastructure Services

- Select AP and establish association with AP
  - Then can send/receive frames via AP & DS
- Re-association service to move from one AP to another AP
- Dissociation service to terminate association
- Authentication service to establish identity of other stations
- Privacy service to keep contents secret

Distribution Services

- Stations within a BSS can communicate directly with each other
- DS provides distribution services
  - Transfer MAC SDUs between APs in ESS
  - Transfer MSDUs between portals & BSSs in ESS
  - Transfer MSDUs between stations in same BSS
    - Multicast, broadcast, or station's preferences
- ESS looks like single BSS to LLC layer

IEEE 802.11 MAC Layer

- MAC layer responsibilities
  - Channel access
  - Frame addressing, formatting, error checking
  - Frame fragmentation & reassembly
- MAC security service options
  - Authentication & privacy
- MAC management services
  - Roaming within ESS
  - Power management

Source, Transmitter, Destination & Receiver

- 802.11 makes a distinction between the source and the transmitter
  - Source: created the original network layer payload
  - Transmitter: sends the MAC frame but does not create or modify the network layer payload
- Similarly, a distinction is made between the destination and the receiver
  - Destination: final location where the network layer payload is processed
  - Receiver: receives the MAC frame but does not terminate the network layer payload

CSMA (Carrier Sense Multiple Access)

- CSMA: listen before transmit:
- If channel sensed idle: transmit entire frame
- If channel sensed busy, defer transmission

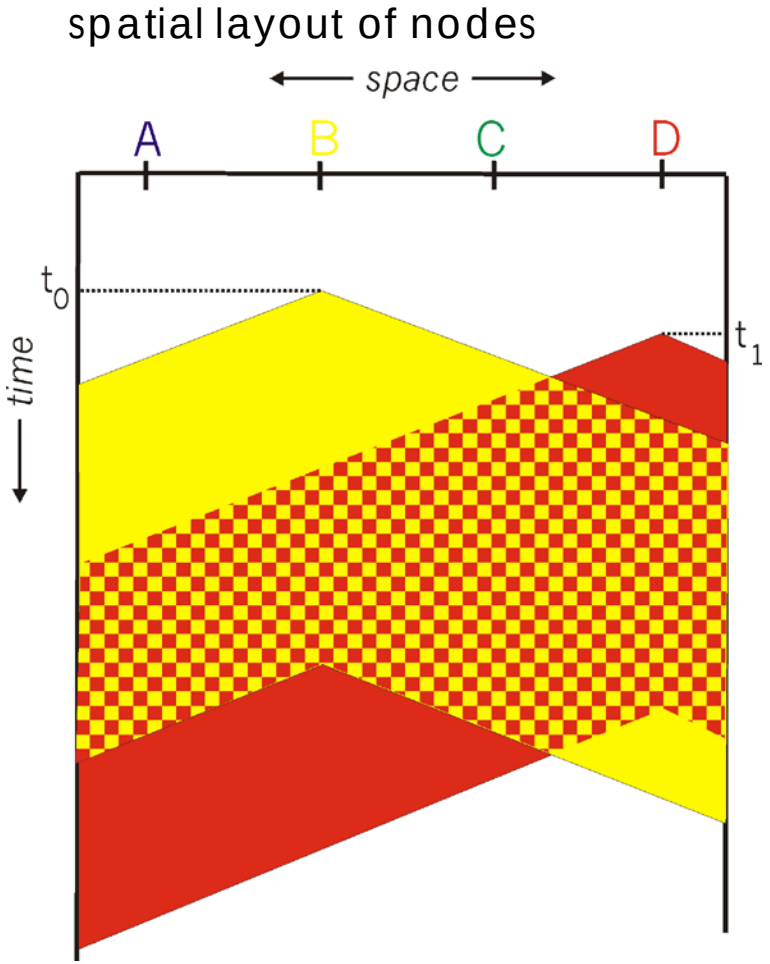
- Human analogy: don’t interrupt others!

CSMA Collisions

collisions *can* still occur:
propagation delay means two nodes may not hear each other's transmission

collision:
entire packet transmission time wasted

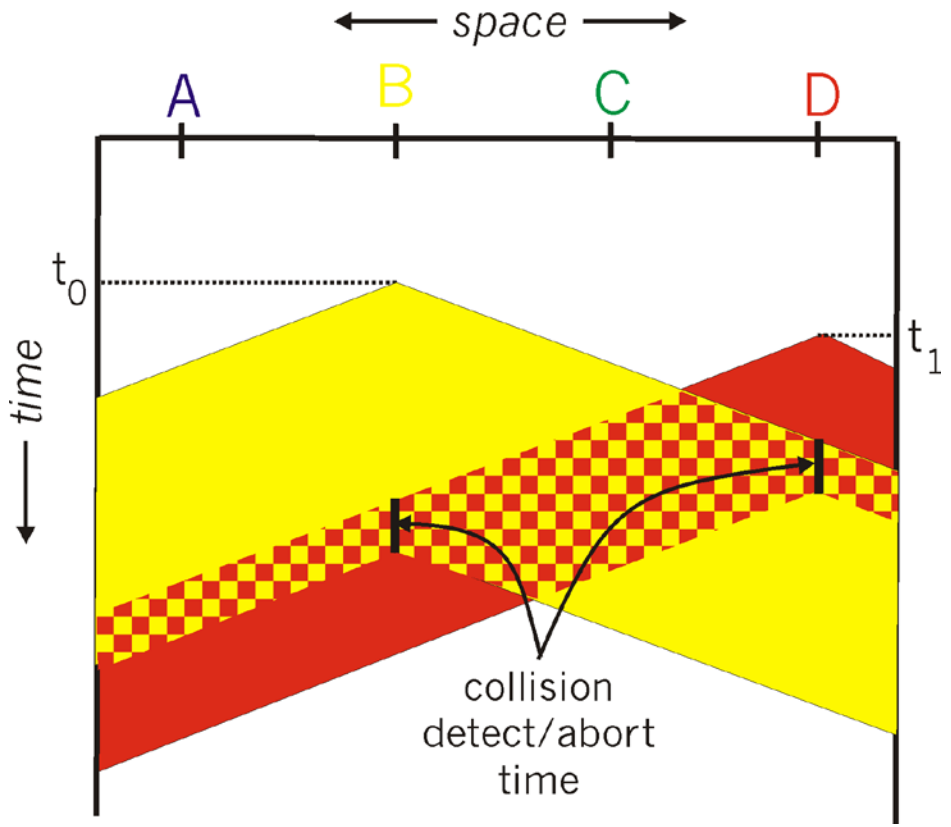
note:
role of distance & propagation delay in determining collision probability



CSMA/CD (Collision Detection)

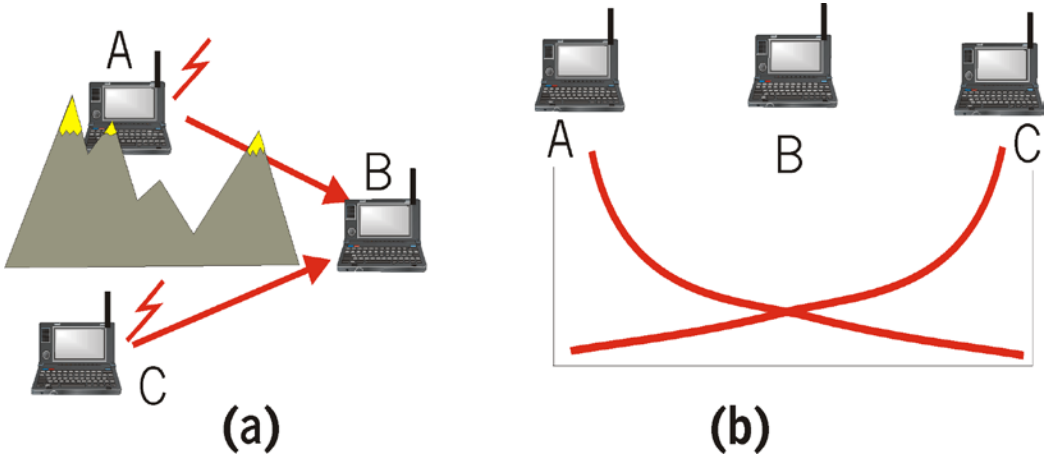
- CSMA/CD: carrier sensing, deferral as in CSMA
  - collisions detected within short time
  - colliding transmissions aborted, reducing channel wastage
- collision detection:
  - easy in wired LANs: measure signal strengths, compare transmitted, received signals
  - difficult in wireless LANs: receiver shut off while transmitting
- human analogy: the polite conversationalist

CSMA/CD Collision Detection



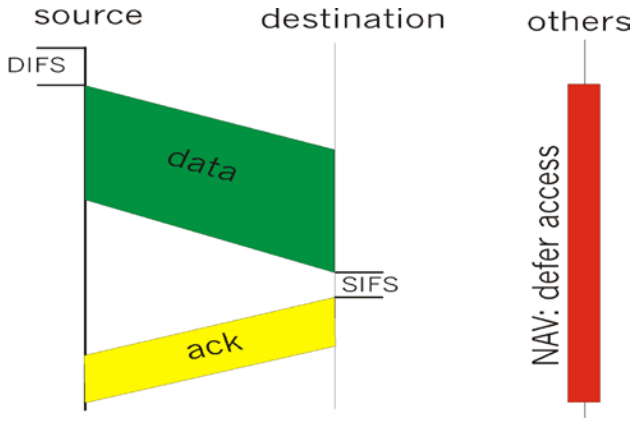
IEEE 802.11: Multiple Access

- Collision if 2 or more nodes transmit at same time
- CSMA makes sense:
  - get all the bandwidth if you're the only one transmitting
  - shouldn't cause a collision if you sense another transmission
- Collision detection doesn't work: hidden terminal problem



IEEE 802.11 MAC Protocol: CSMA/CA

- 802.11 CSMA: sender
- - if sense channel idle for DISF sec.
- then transmit entire frame (no collision detection)
- -if sense channel busy then binary backoff
- 802.11 CSMA receiver
- - if received OK
- return ACK after SIFS
- (ACK is needed due to hidden terminal problem)

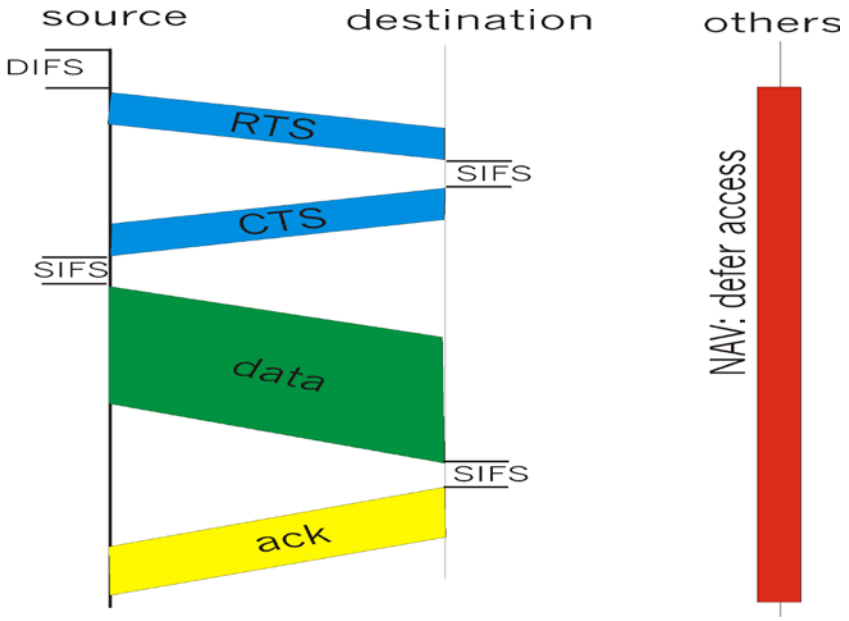


Collision Avoidance Mechanisms

- Problem:
  - two nodes, hidden from each other, transmit complete frames to base station
  - wasted bandwidth for long duration !
- Solution:
  - small reservation packets
  - nodes track reservation interval with internal “network allocation vector” (NAV)

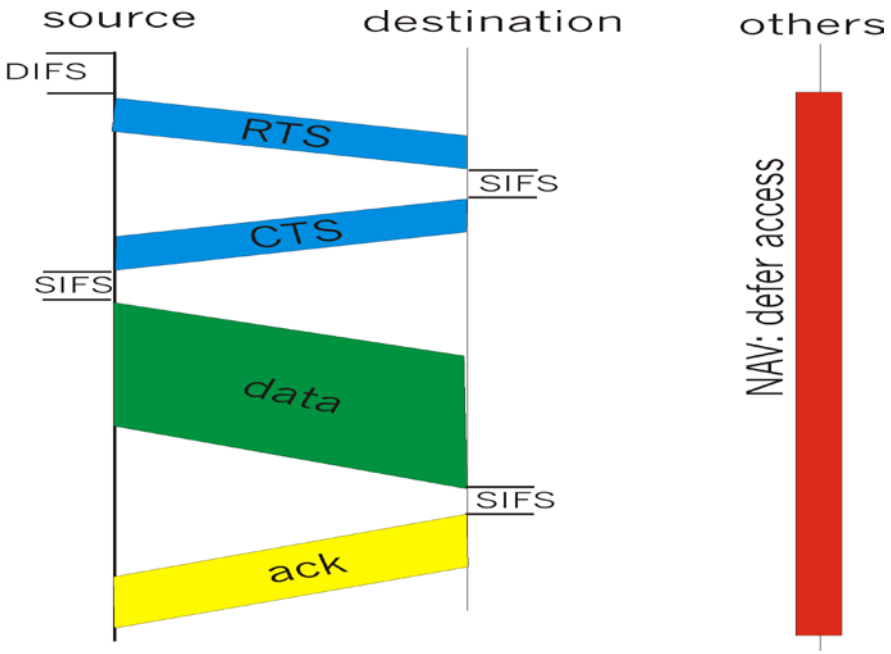
Collision Avoidance: RTS-CTS exchange

- sender transmits short RTS (request to send) packet: indicates duration of transmission
- receiver replies with short CTS (clear to send) packet
  - notifying (possibly hidden) nodes
- hidden nodes will not transmit for specified duration: NAV



Collision Avoidance: RTS-CTS exchange

- RTS and CTS short:
  - collisions less likely, of shorter duration
  - end result similar to collision detection
- IEEE 802.11 allows:
  - CSMA
  - CSMA/CA: reservations
  - polling from AP

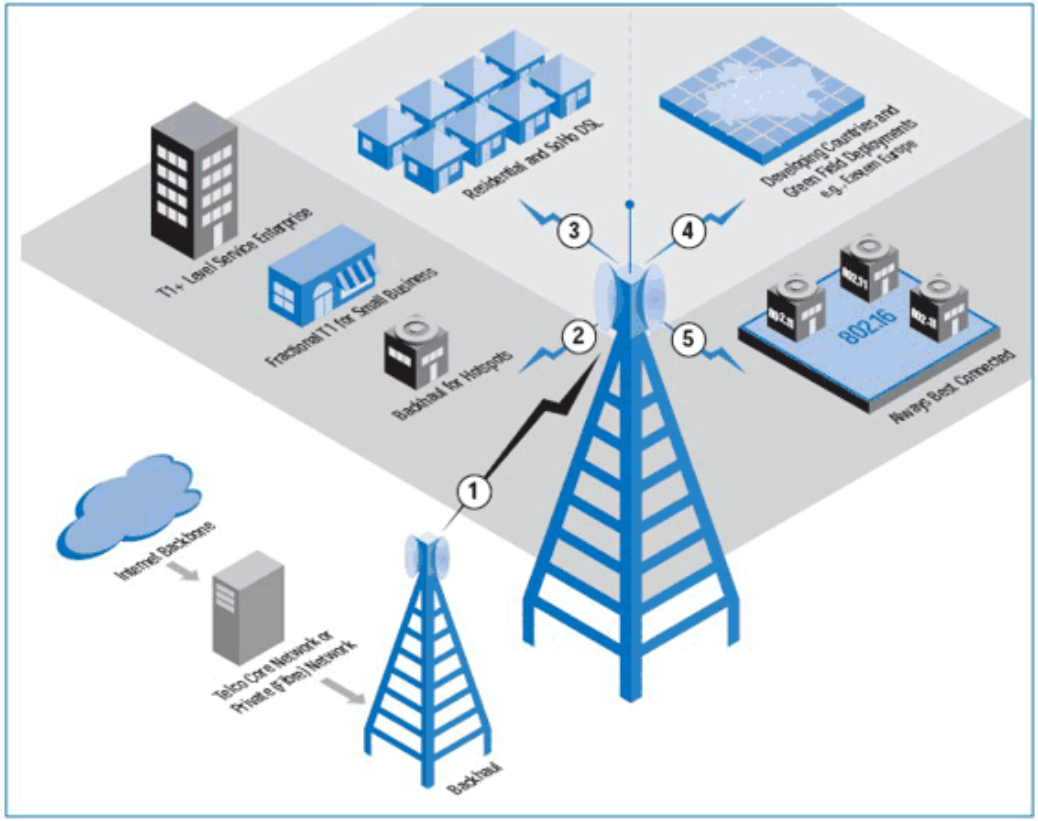


IEEE 802.16 WiMAX

- Wireless MAN Standard for Broadband Wireless Metropolitan Area Networks
- Broad bandwidth
  - Up to 134 Mbps in 10-66 GHz band
- Comprehensive and modern security
  - Packet data encryption
    - DES and AES used
  - Key management protocol
    - Use RSA to set up a shared secret between subscriber station and base station
    - Use the secret for subsequent exchange of traffic encryption keys (TEK)

IEEE 802.16 WiMAX cont'd

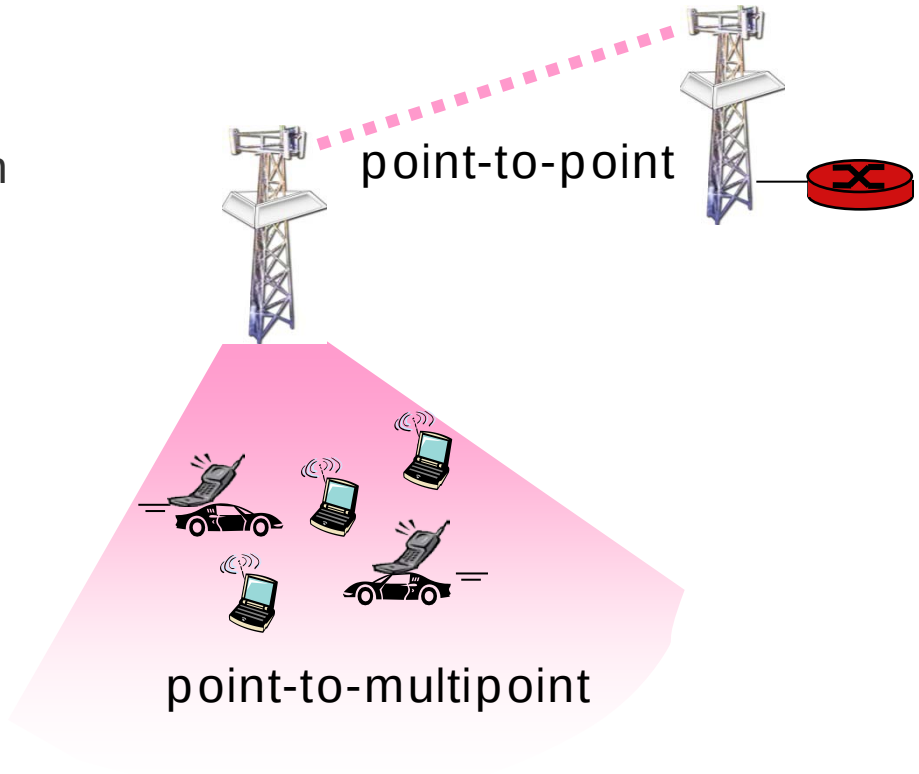
- WiMax is a broadband wireless access (BWA) technology
  - Based on IEEE 802.16 standard
  - Last mile solution
- Rich set of MAC features
  - Real-time streaming capabilities
- Two working radio spectrum
  - 2-11 GHz (non-LOS)
  - 10-66 GHz (LOS)



IEEE 802.16: WIMAX cont'd

- 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



Wireless Network Taxonomy

	single hop	multiple hops
infrastructure (e.g., APs)	host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet	host may have to relay through several wireless nodes to connect to larger Internet: *mesh net*
no infrastructure	no base station, no connection to larger Internet (Bluetooth, ad hoc nets)	no base station, no connection to larger Internet. May have to relay to reach other a given wireless node MANET, VANET

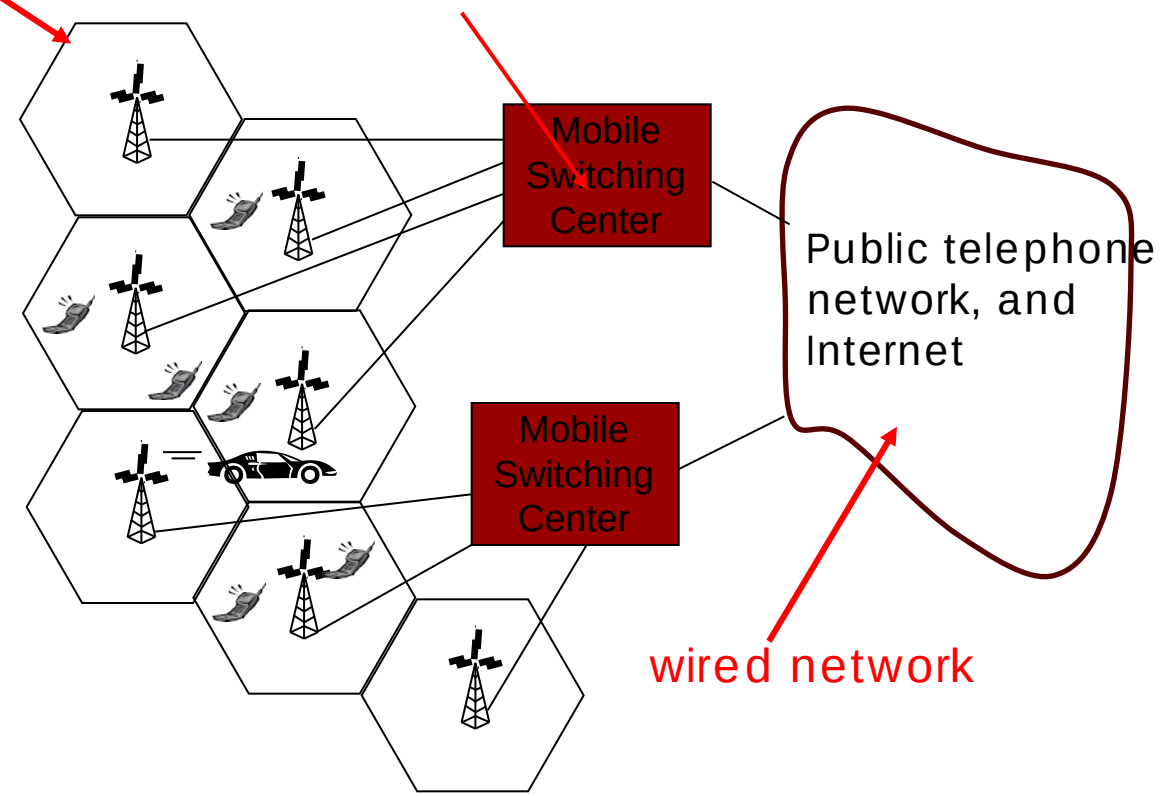
Components Of Cellular Network Architecture

MSC

- connects cells to wide area 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

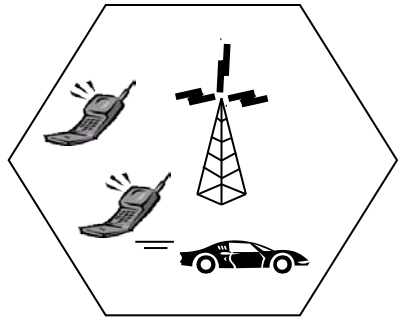


mobile switching center (MSC) is the primary service delivery node

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

- 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

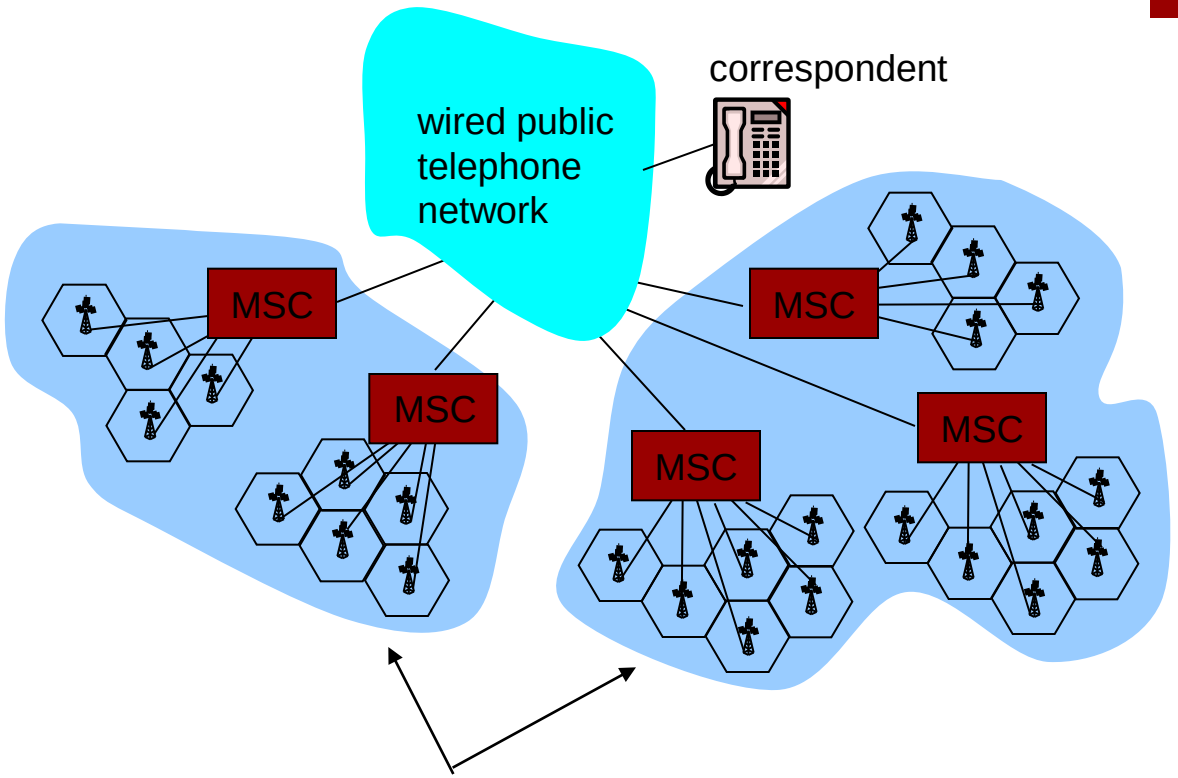
Cellular Standards Cont'd

- 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

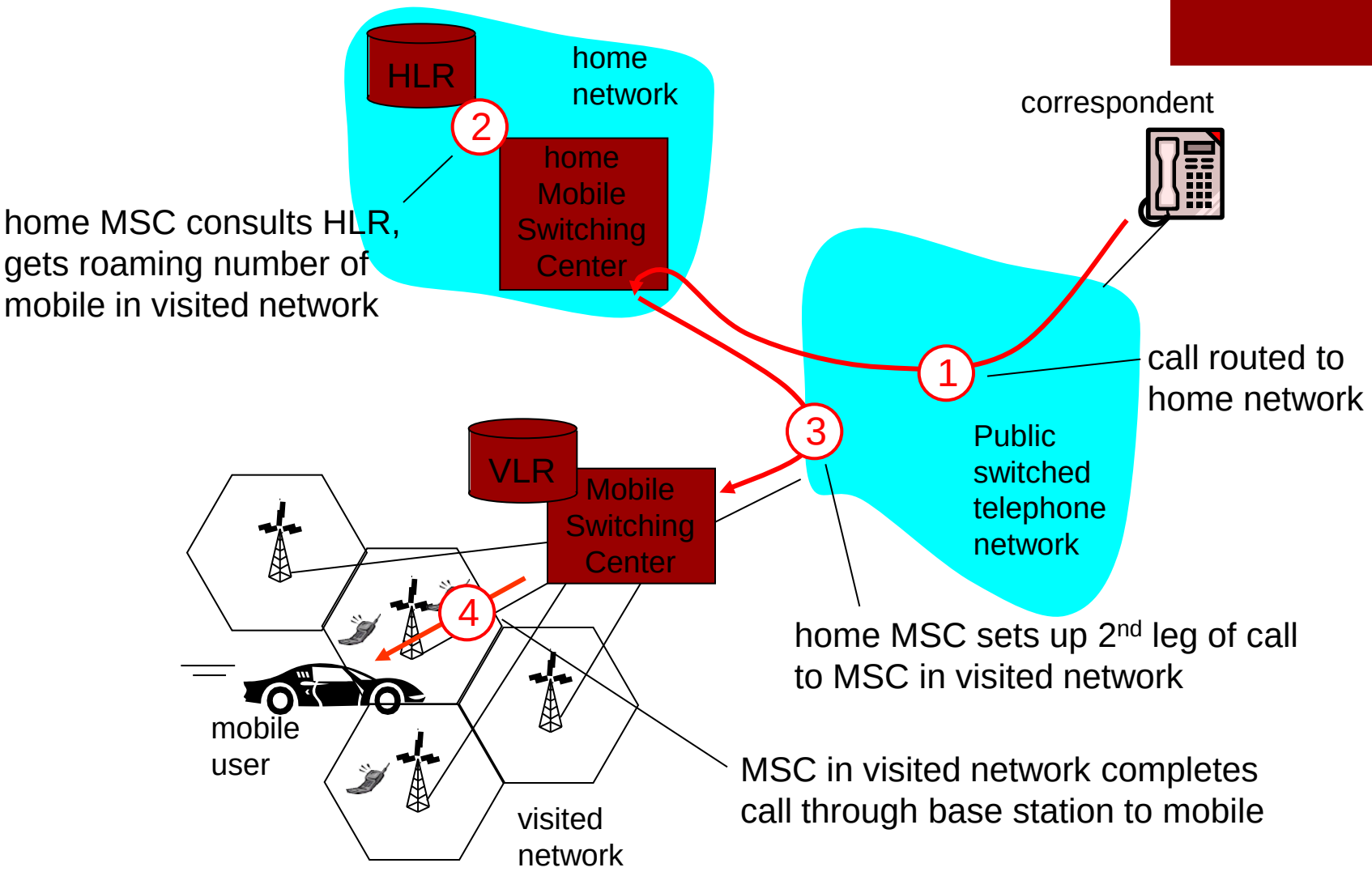
Cellular Standards

- 3G systems: voice/data
- Universal Mobile Telecommunications Service (UMTS)
  - data service: High Speed Uplink/Downlink packet Access (HSDPA/HSUPA): 3 Mbps
- CDMA-2000: CDMA in TDMA slots
  - data service: 1xEvlution Data Optimized (1xEVDO) up to 14 Mbps

Cellular Network Architecture



GSM: Indirect Routing to Mobile



Dynamic Spectrum Access

- Current paradigm of static spectrum allocation has serious drawback in terms of efficient usage of spectrum
- FCC in United States defined provisions for dynamic spectrum access recently
- Sub-900 MHz TV transmission bands made open to unlicensed services because of under-utilization of these bands
- Wireless service providers can dynamically acquire spectrum from sub-900 MHz band whenever they need
- BUT the constraint for unlicensed devices is that they have to detect licensed users (primary incumbents) and avoid interference with them
- The newly proposed IEEE 802.22 based on cognitive radio (CR) is seen as the solution to the current problem