Wireless Networks

Sangtae Ha

CSCI 4273/5273 Network Systems

http://ngn.cs.colorado.edu/~sangtaeha/courses/csci4273/fall15/

Note: The slides are adapted from the materials from Prof. Richard Han at CU Boulder and Profs. Jennifer Rexford and Mike Freedman at Princeton University.

Announcements

- PS #1 is out and due next Thu 11:55pm, Sept 17
- No class on Sept 15

Wireless Links

Widespread Deployment

- Worldwide cellular subscribers
  - 1993: 34 million
  - 2005: more than 2 billion
  - 2009: more than 4 billion

    > landline subscribers

- Wireless local area networks
  - Wireless adapters built in to most laptops, and even PDAs
  - More than 220,000 known WiFi locations in 134 countries
  - Probably many, many more (e.g., home networks, corporate networks, …)

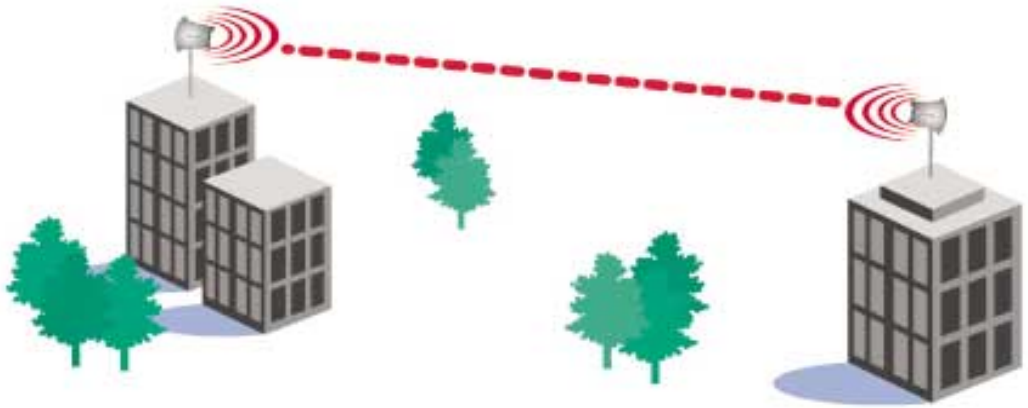
Wireless Properties

- Interference / bit errors
  - More sources of corruption compared to wired
- Multipath propagation
  - Signal does not travel in a straight line
- Broadcast medium
  - All traffic to everyone who is within range
- Power trade-offs
  - Important for power constrained devices

too much power causes battery to lose charge too fast

Wireless Links: High Bit Error Rate

- Decreasing signal strength
  - Disperses as it travels greater distance
  - Attenuates as it passes through matter

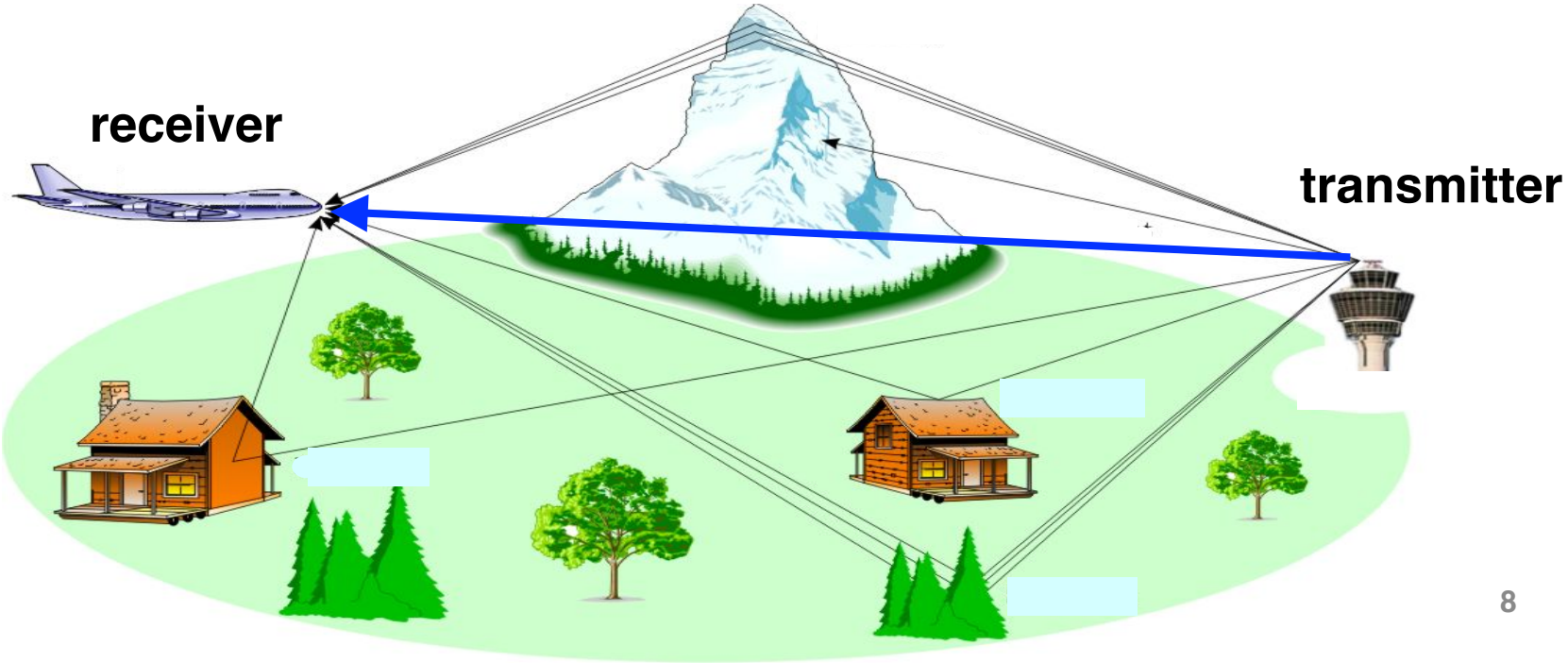


Wireless Links: High Bit Error Rate

- Interference from other sources
  - Radio sources in same frequency band
  - E.g., 2.4 GHz wireless phone interferes with 802.11b wireless LAN
  - Electromagnetic noise (e.g., microwave oven)

Wireless Links: High Bit Error Rate

- Multi-path propagation
  - Electromagnetic waves reflect off objects
  - Taking many paths of different lengths
  - Causing blurring of signal at the receiver



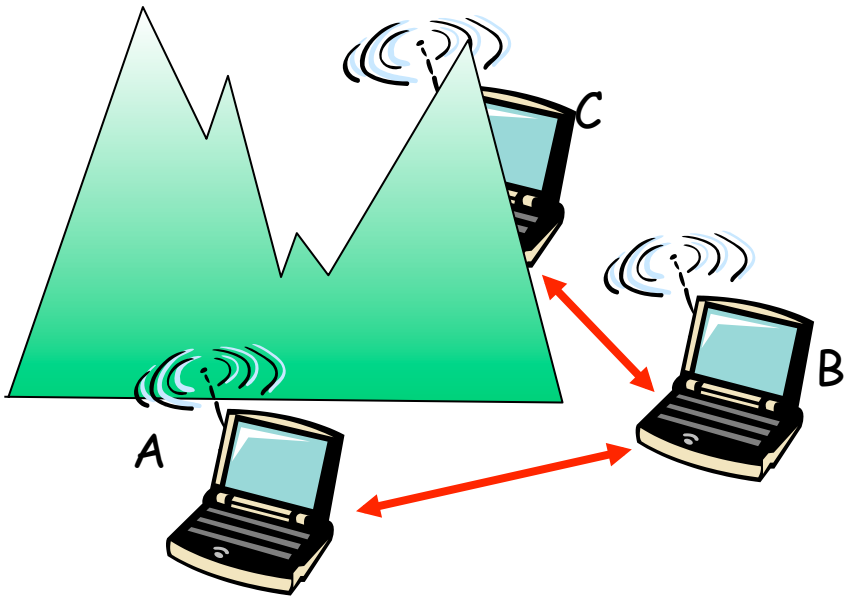
Dealing With Bit Errors

- Wireless vs. wired links
  - Wired: most loss is due to congestion
  - Wireless: higher, time-varying bit-error rate

- Dealing with high bit-error rates
  - Sender could increase transmission power
    - Requires more energy (bad for battery-powered hosts)
    - Creates more interference with other senders
  - Stronger error detection and recovery
    - More powerful error detection/correction codes
    - Link-layer retransmission of corrupted frames

Wireless Links: Broadcast Limitations

- Wired broadcast links
  - E.g., Ethernet bridging, in wired LANs
  - All nodes receive transmissions from all other nodes
- Wireless broadcast: hidden terminal problem



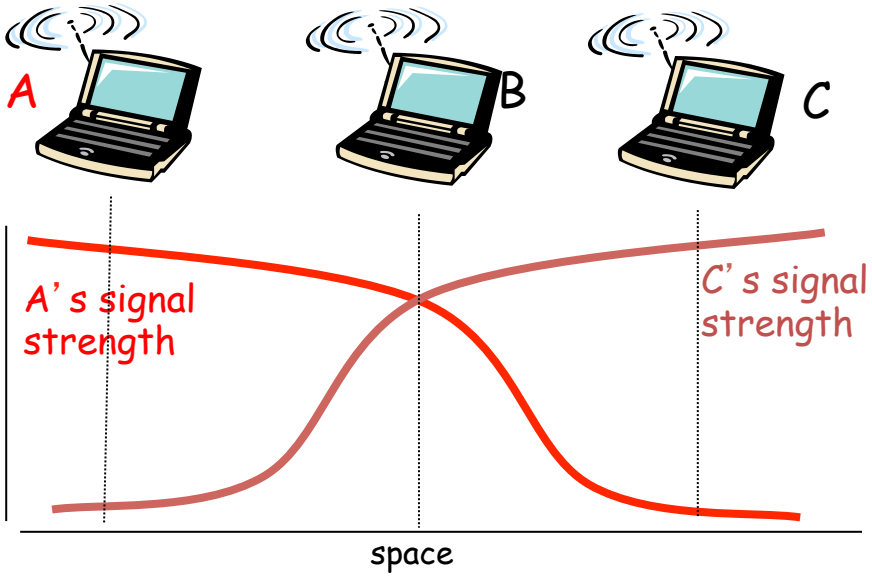
Can't know about all interference and collisions because of hidden terminals unlike wired

- **A and B hear each other**
- **B and C hear each other**
- **But, A and C do not**

So, A and C are unaware of their interference at B

Wireless Links: Broadcast Limitations

- Wired broadcast links
  - E.g., Ethernet bridging, in wired LANs
  - All nodes receive transmissions from all other nodes
- Wireless broadcast: fading over distance



- **A and B hear each other**
- **B and C hear each other**
- **But, A and C do not**

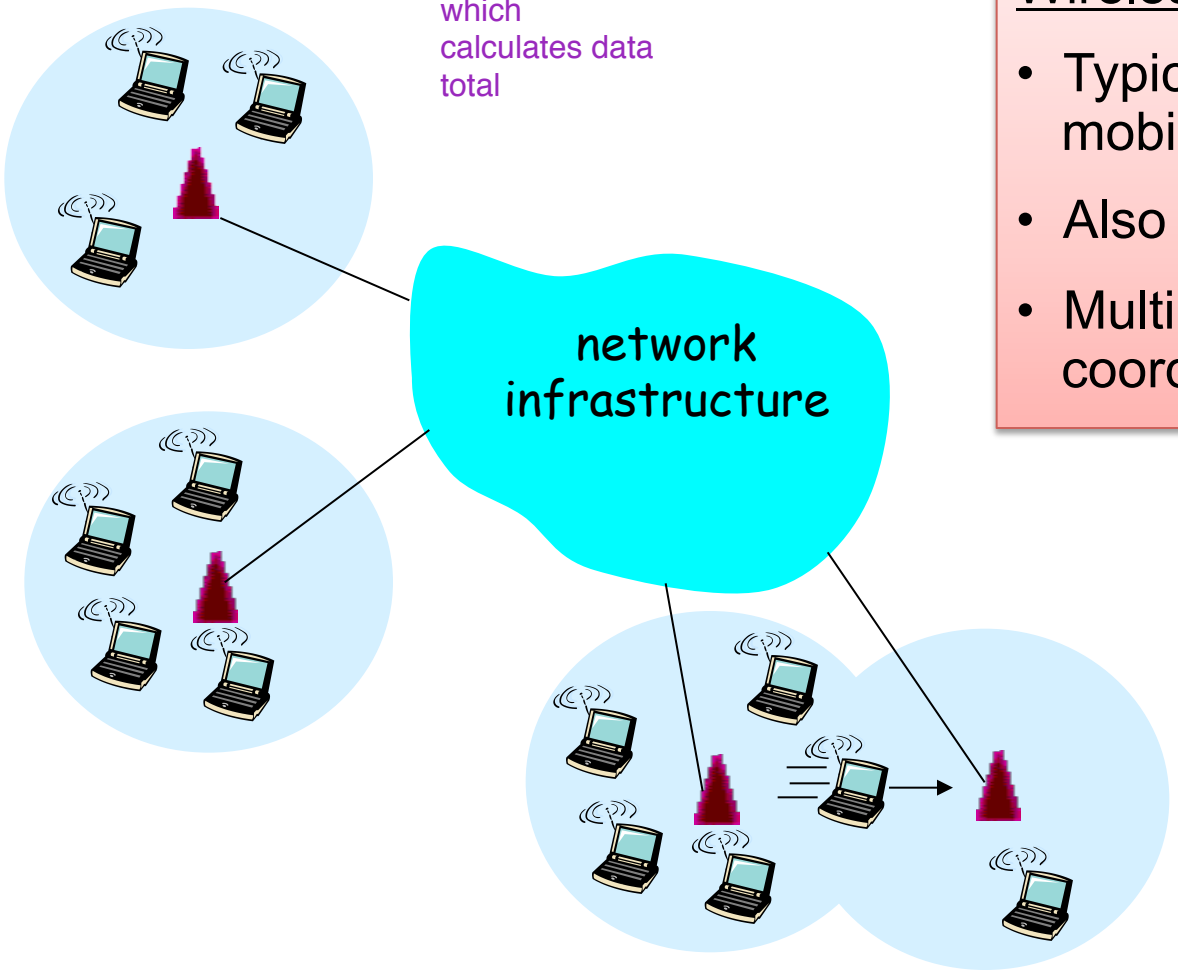
So, A and C are unaware of their interference at B

Example Wireless Link Technologies

- Data networks
  - 802.15.1 (Bluetooth): 2.1 Mbps – 10 m
  - 802.11b (WiFi): 5-11 Mbps – 100 m
  - 802.11a and g (WiFi): 54 Mbps – 100 m
  - 802.11n (WiFi): 200 Mbps – 100 m
  - 802.16 (WiMax): 70 Mbps – 10 km
- Cellular networks, outdoors
  - 2G: 56 Kbps
  - 3G: 384 Kbps
  - 3G enhanced: 4 Mbps
  - 4G LTE: 100Mbps
  - LTE Advanced: 1Gbps

Wireless Network: Wireless Link

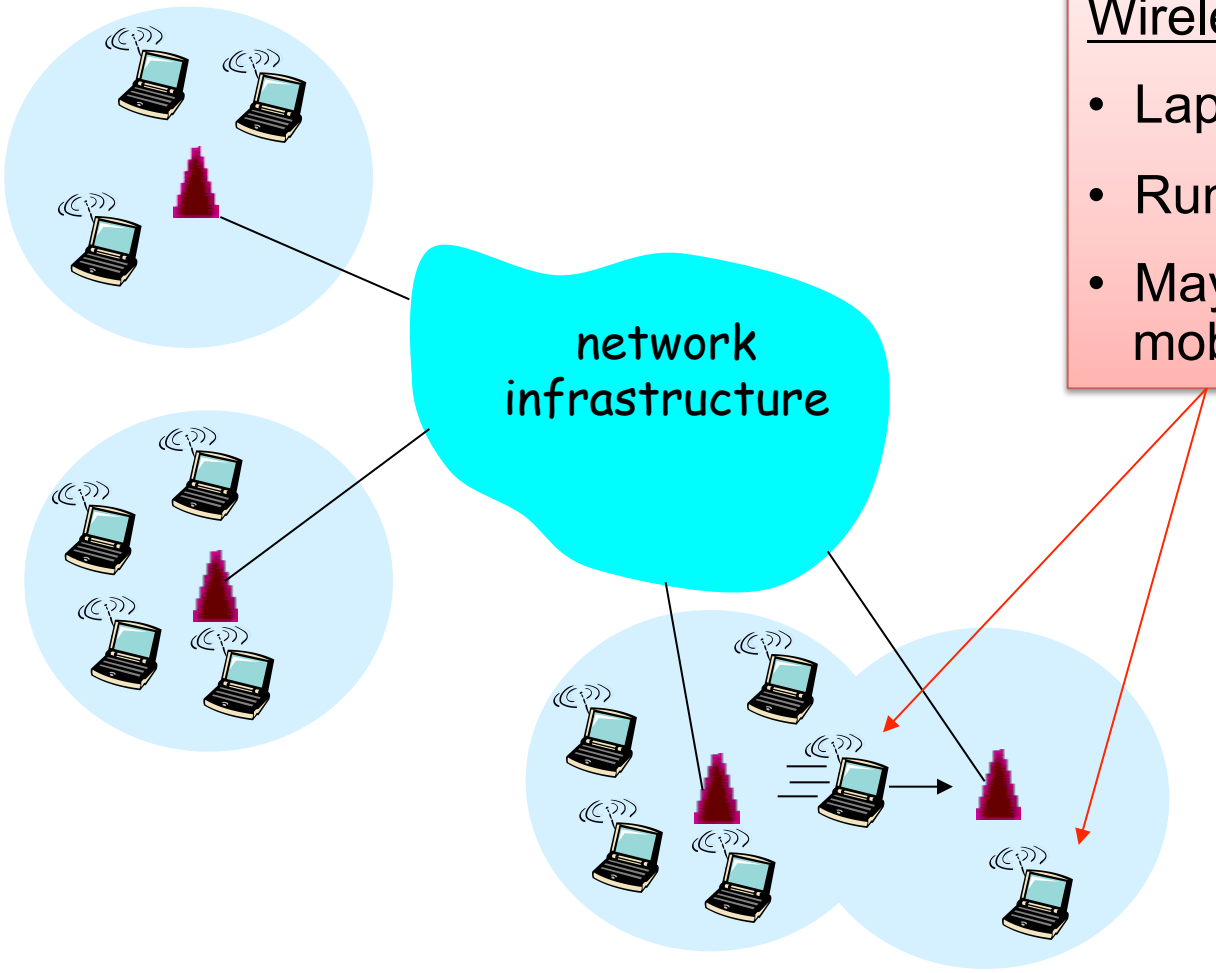
Cell phone to
cell tower
to network
infrastructure
which
calculates data
total



Wireless link

- Typically used to connect mobile(s) to base station
- Also used as backbone link
- Multiple access protocol coordinates link access

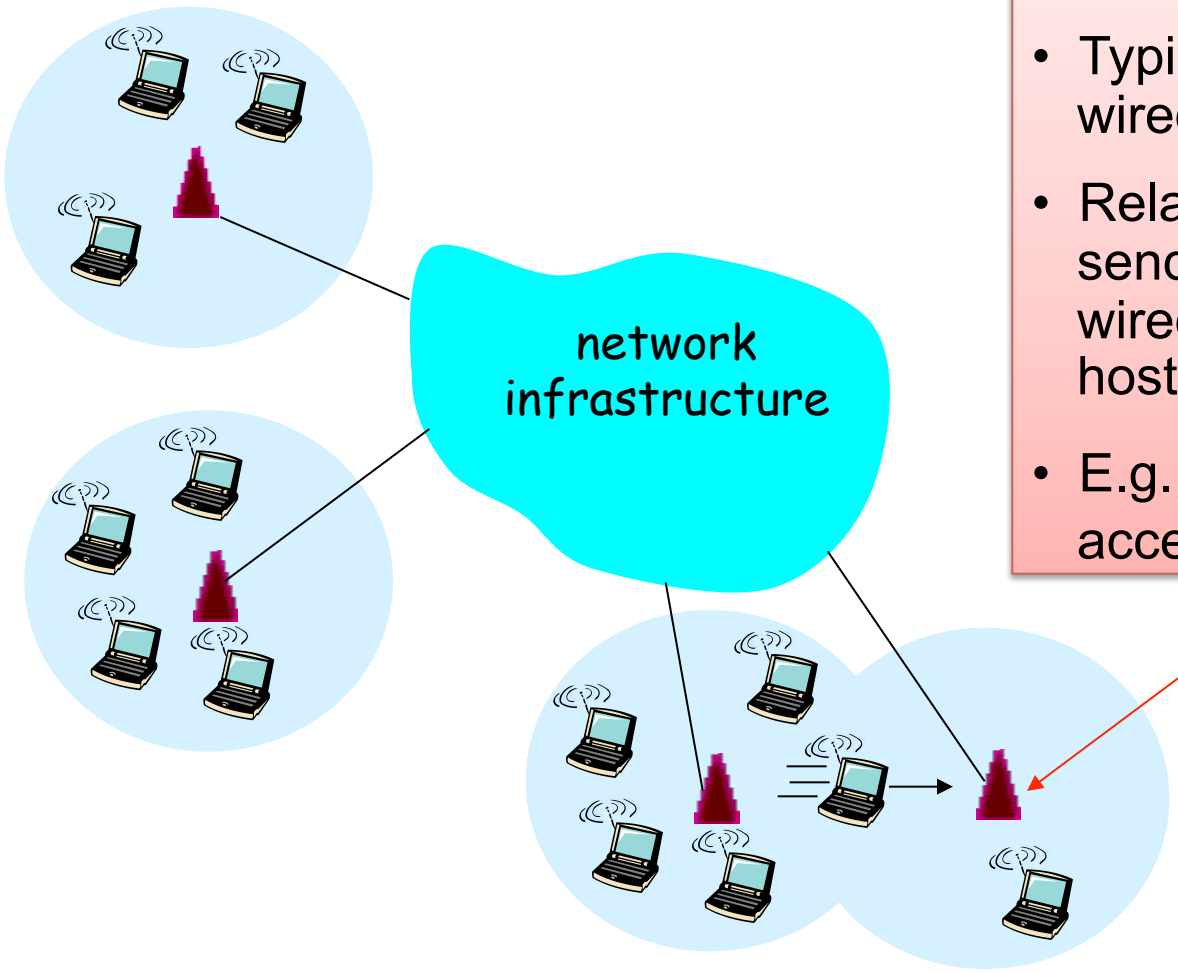
Wireless Network: Wireless Hosts



Wireless host

- Laptop, PDA, IP phone
- Run applications
- May be stationary (non-mobile) or mobile

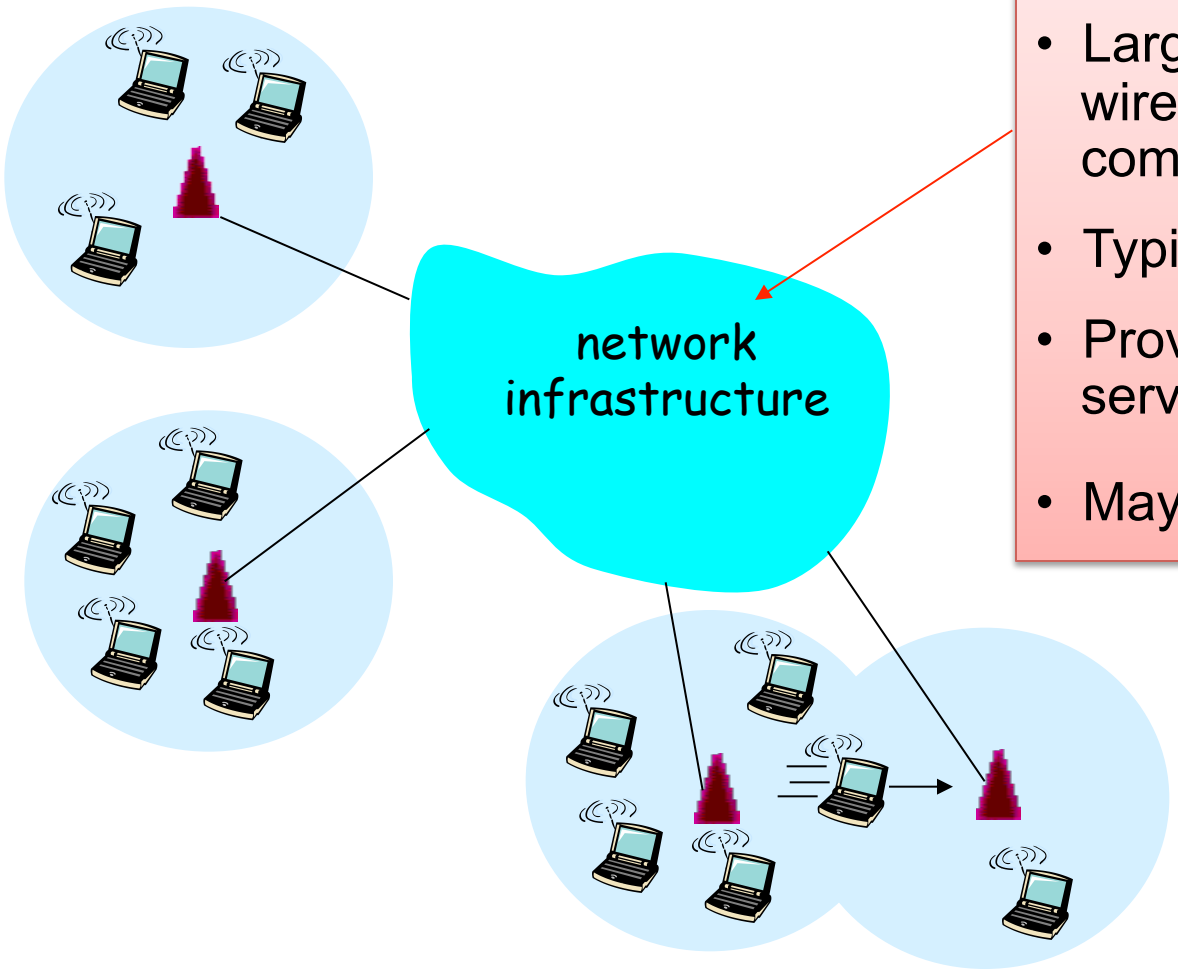
Wireless Network: Base Station



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

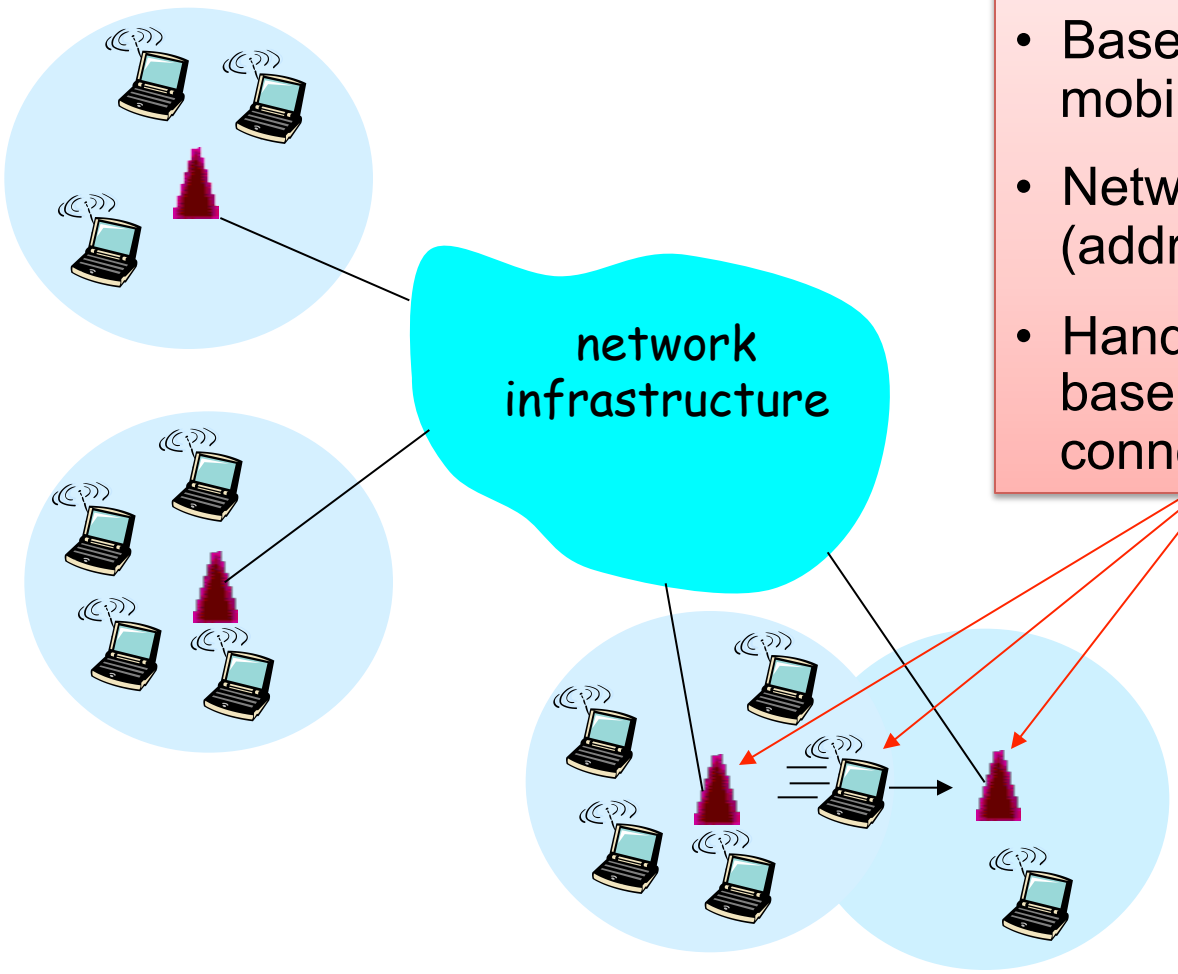
Wireless Network: Infrastructure



Network infrastructure

- Larger network with which a wireless host wants to communicate
- Typically a wired network
- Provides traditional network services
- May not always exist

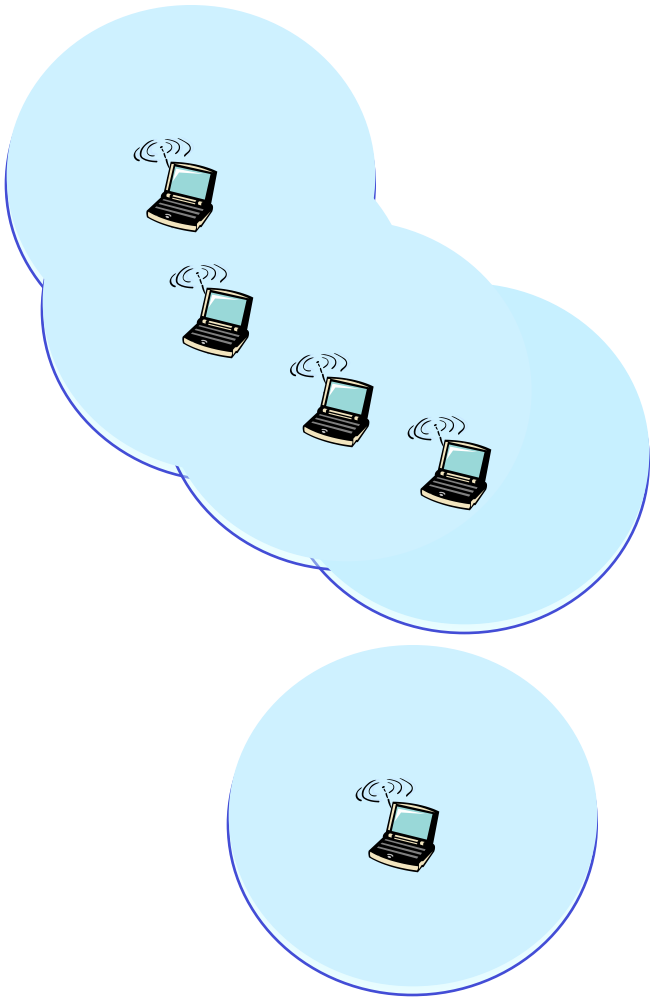
Scenario #1: Infrastructure Mode



Infrastructure mode

- Base station connects mobiles into wired network
- Network provides services (addressing, routing, DNS)
- Handoff: mobile changes base station providing connection to wired network

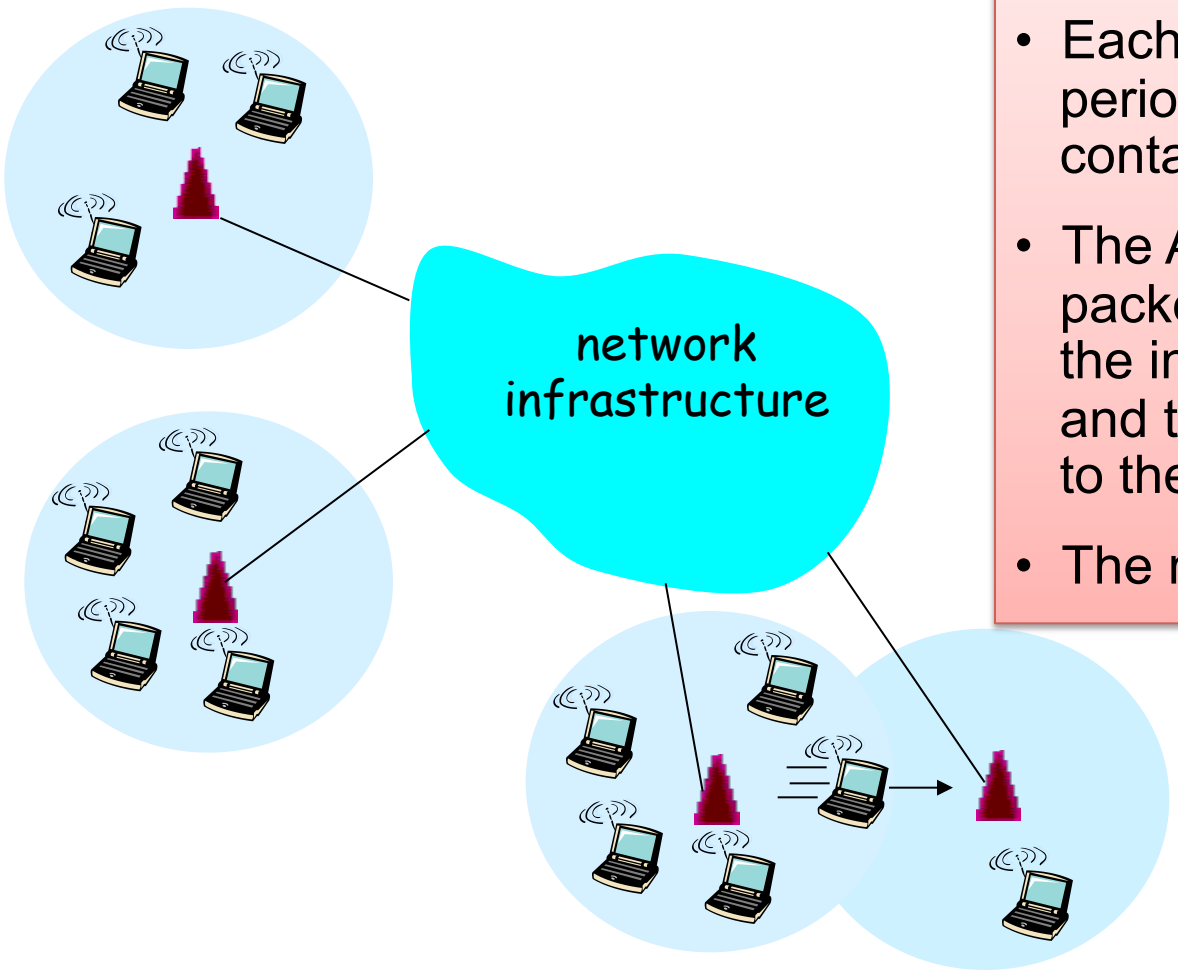
Scenario #2: Ad-Hoc Mode



Ad hoc mode

- No base stations
- Nodes can only transmit to other nodes within link coverage
- Nodes self-organize and route among themselves

Scenario #3: Power Save Mode



Power save mode

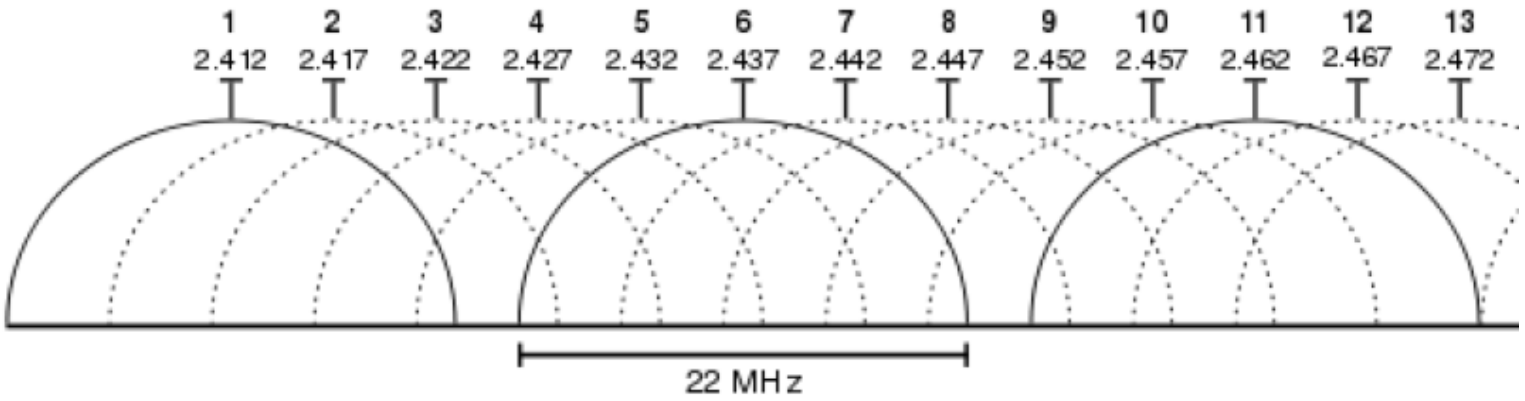
- Each client node sleeps and periodically wakes up, contacting the AP
- The AP has buffered any packets that have arrived in the interim for each node, and transmits these packets to the awake node
- The node returns to sleep

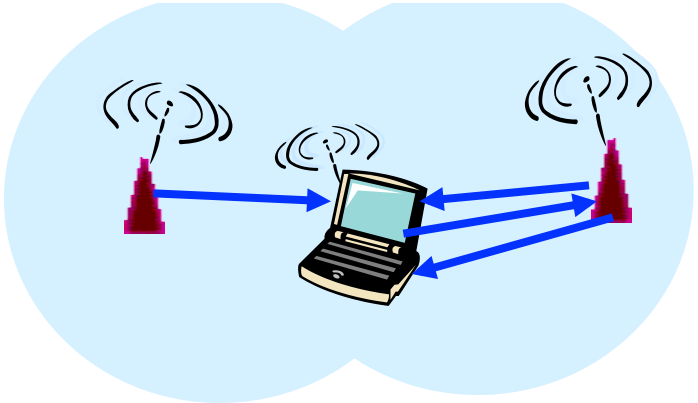
Infrastructure vs. Ad Hoc

- Infrastructure mode
  - Wireless hosts are associated with a base station
  - Traditional services provided by the connected network
  - E.g., address assignment, routing, and DNS resolution
- Ad hoc networks
  - Wireless hosts have no infrastructure to connect to
  - Hosts themselves must provide network services
- Similar in spirit to the difference between
  - Client-server communication
  - Peer-to-peer communication

Channels and Association

- Multiple channels at different frequencies
  - Network administrator chooses frequency for AP
  - Interference if channel is same as neighboring AP

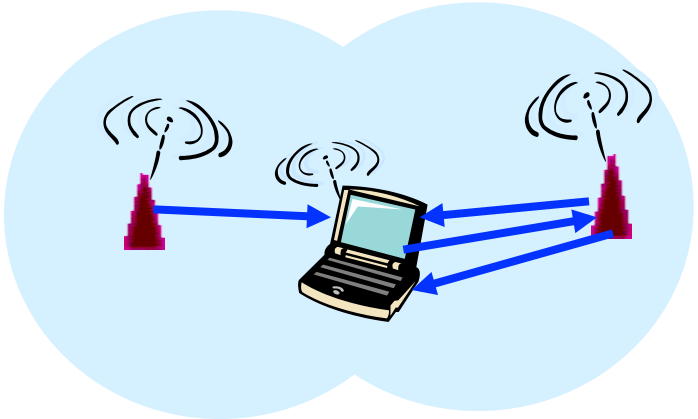




- Beacon frames from APs
- Associate request from host
- Association response from AP

Channels and Association

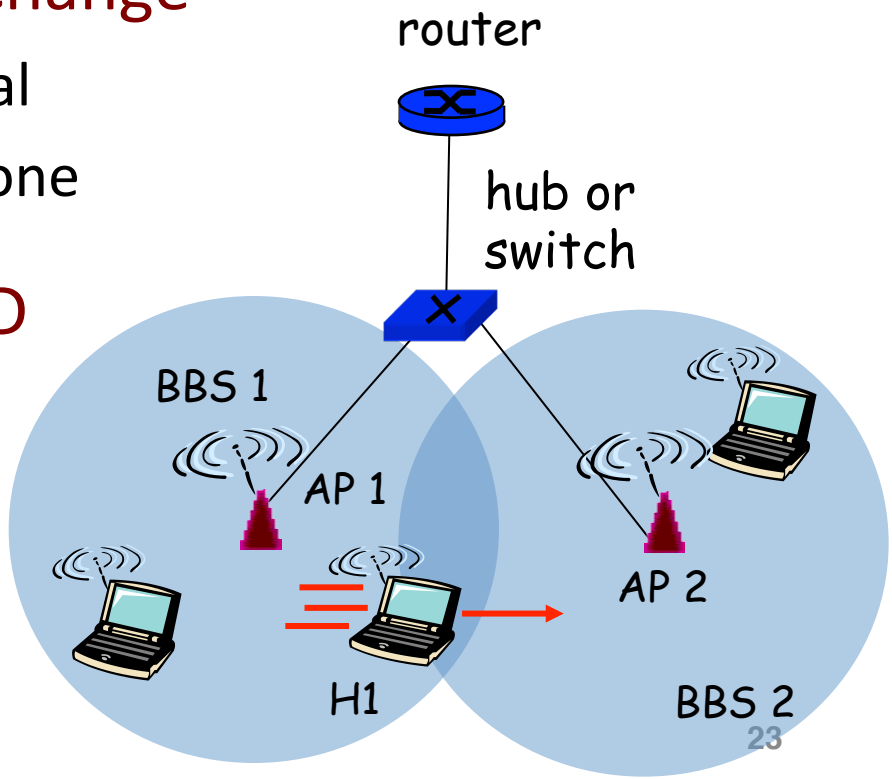
- Multiple channels at different frequencies
  - Network administrator chooses frequency for AP
  - Interference if channel is same as neighboring AP
- Access points send periodic beacon frames
  - Containing AP's name (SSID) and MAC address
  - Host scans channels, listening for beacon frames
  - Host selects an access point to associate with



- Beacon frames from APs
- Associate request from host
- Association response from AP

Mobility Within the Same Subnet

- H1 remains in same IP subnet
  - IP address of the host can remain same
  - Ongoing data transfers can continue uninterrupted
- H1 recognizes the need to change
  - H1 detects a weakening signal
  - Starts scanning for stronger one
- Changes APs with same SSID
  - H1 disassociates from one
  - And associates with other
- Switch learns new location
  - Self-learning mechanism



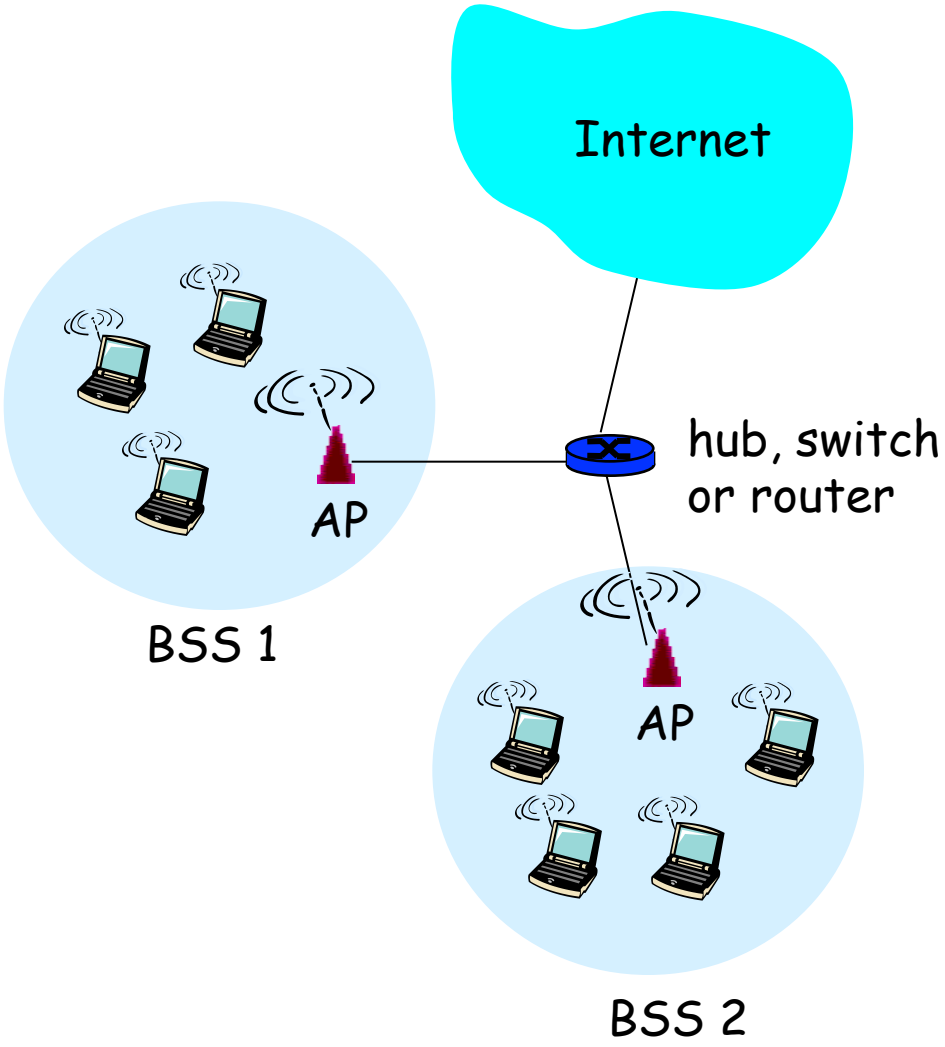
Questions

- Loss is primary caused by bit errors
  - (A) Ethernet (Wired)
  - (B) 802.11 (Wireless)
  - (C) Both
  - (D) Neither
- All hosts on subnet see all communication
  - (A) Ethernet (Wired)
  - (B) 802.11 (Wireless)
  - (C) Both
  - (D) Neither

Signal can't be seen around obstacles or long distances for wireless

WiFi: 802.11 Wireless LANs

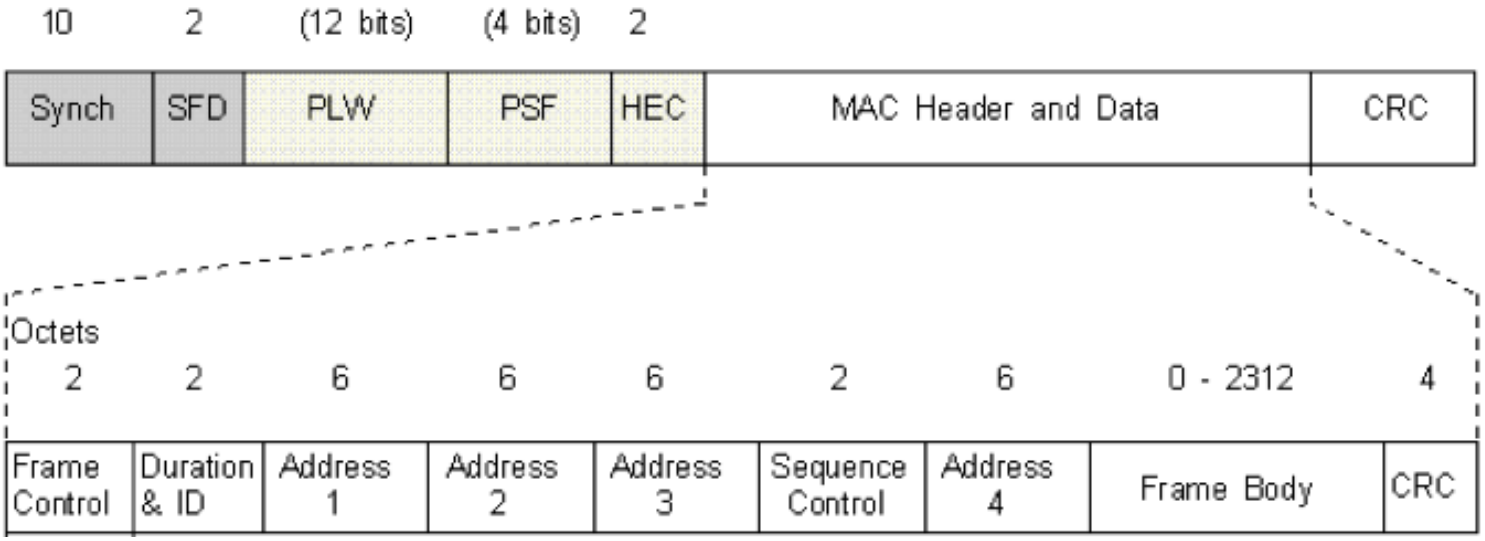
802.11 LAN Architecture



- Access Point (AP)
  - Base station that communicates with the wireless hosts
- Basic Service Set (BSS)
  - Coverage of one AP
  - AP acts as the master
  - Identified by an "network name" known as an SSID

SSID: Service Set Identifier

Wireless LAN addressing and bridging

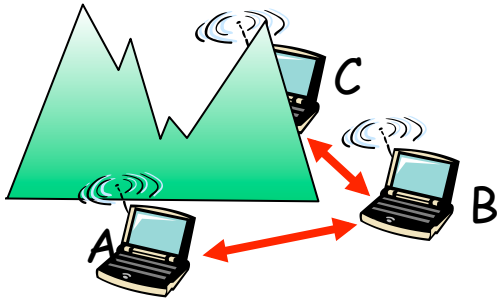


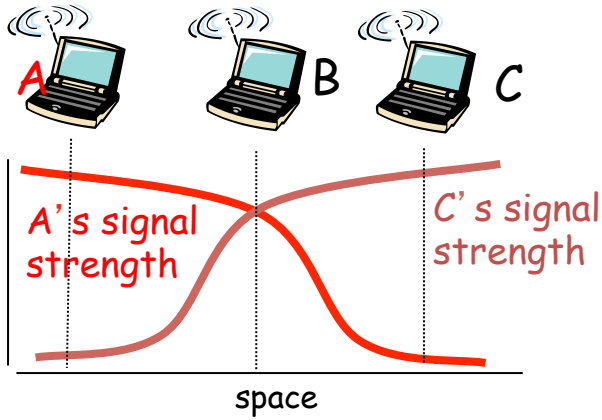
Why 4 addresses: Provide roaming between bridged APs

Function	Addr 1 (Receiver)	Addr 2 (Transmitter)	Addr 3	Addr 4
Intra-BSS	Dest	Source		
To AP	BSS ID	Source	Dest	
From AP	Dest	BSS ID	Source	
Bridged APs	Reciever	Transmitter	Dest	Source

CSMA: Carrier Sense, Multiple Access

- Multiple access: channel is shared medium
  - Station: wireless host or access point
  - Multiple stations may want to transmit at same time
- Carrier sense: sense channel before sending
  - Station doesn't send when channel is busy
  - To prevent collisions with ongoing transfers
  - But, detecting ongoing transfers isn't always possible

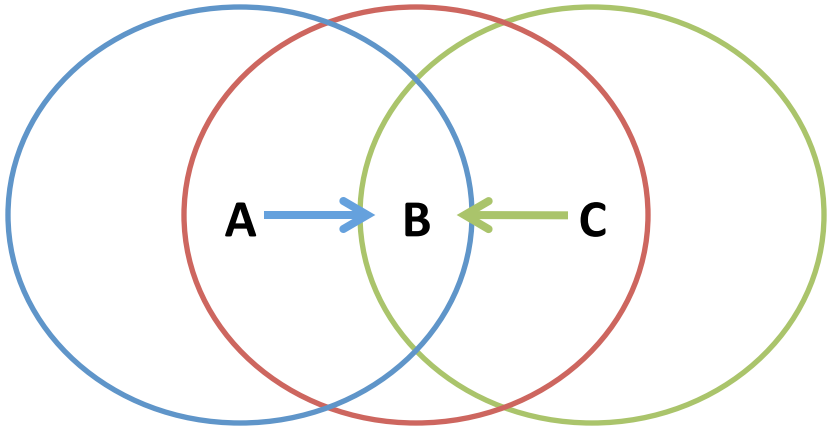




CA: Collision Avoidance, Not Detection

- Collision detection in wired Ethernet
  - Station listens while transmitting
  - Detects collision with other transmission
  - Aborts transmission and tries sending again
- Problem #1: cannot detect all collisions
  - Hidden terminal problem
  - Fading
- Problem #2: listening while sending
  - Strength of received signal is much smaller
  - Expensive to build hardware that detects collisions
- So, 802.11 does collision avoidance, not detection

Hidden Terminal Problem



- A and C can't see each other, both send to B
- Occurs b/c 802.11 relies on physical carrier sensing, which is susceptible to hidden terminal problem

Virtual carrier sensing

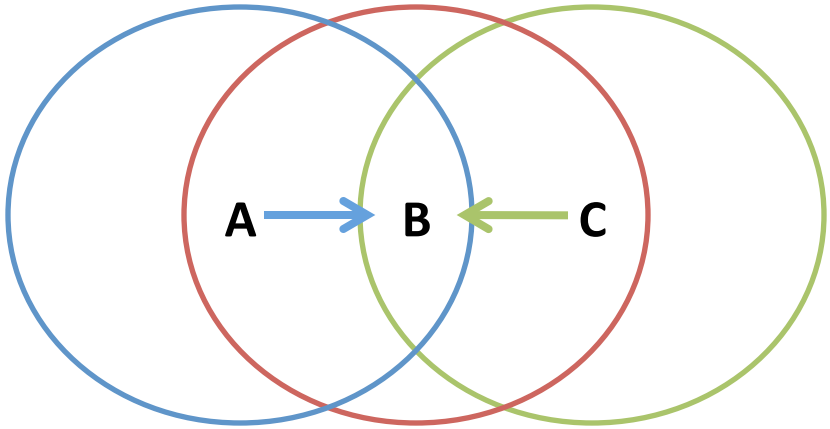
- First exchange control frames before transmitting data
  - Sender issues "Request to Send" (RTS), incl. length of data
  - Receiver responds with "Clear to Send" (CTS)
- If sender sees CTS, transmits data (of specified length)
- If other node sees CTS, will idle for specified period
- If other node sees RTS but not CTS, free to send

A -> B
A: sends RTS(B)
B sends CTS(A) <- Doesn't issue
any transmission from B->C. Co
is idle.

When to Resume Sending?

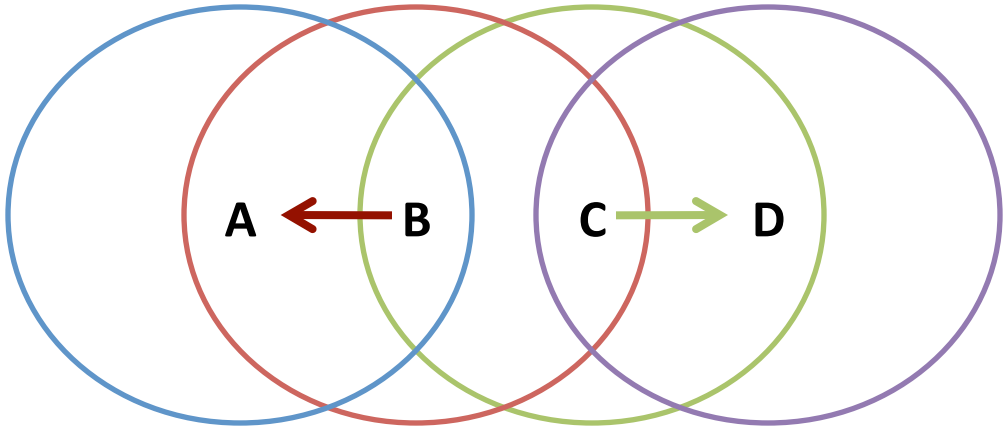
- How does host C know when to resume sending?
  - RTS & CTS both include a Network Allocation Vector (NAV) indicating the length of their upcoming transmission
  - Data frame also contains a "NAV" to indicate the length of transmission
  - After Host A has finished sending its data, Host B sends an ACK; Host C hears B's ACK and knows the data transmission is over

Hidden Terminal Problem



- A and C can't see each other, both send to B
- RTS/CTS can help
  - Both A and C would send RTS that B would see first
  - B only responds with one CTS (say, echo'ing A's RTS)
  - C detects that CTS doesn't match and won't send

Exposed Terminal Problem



- B sending to A, C wants to send to D
- As C receives B's packets, carrier sense would prevent it from sending to D, even though wouldn't interfere
- RTS/CTS can help
  - C hears RTS from B, but not CTS from A
  - C knows it's transmission will not interfere with A
  - C is safe to transmit to D

Questions

- When using RTS/CTS, what prevents a hidden terminal from clobbering the packets that another node is sending?

  Hidden terminal would see the CTS of the sender's desired destination, but not the RTS of the sender, and choose not to send to the same destination as had sent the CTS.

- When using RTS/CTS, how does an exposed terminal decide it is safe to send?

  Exposed terminal would see the RTS of another node, but not the corresponding CTS (from the other node's destination), and know it's safe to send.

Impact on Higher-Layer Protocols

- Wireless and mobility change path properties
  - Wireless: higher packet loss, not from congestion
  - Mobility: transient disruptions, and changes in RTT
- Logically, impact should be minimal …
  - Best-effort service model remains unchanged
  - TCP and UDP can (and do) run over wireless, mobile

Fix: performance enhancing proxy (PEP), adda proxy

- But, performance definitely *is* affected
  - TCP treats packet loss as a sign of congestion
  - TCP tries to estimate the RTT to drive retransmissions
  - TCP does not perform well under out-of-order packets

TCP designed for wired not wireless

- Internet not designed with these issues in mind

Conclusions

- Wireless
  - Already a major way people connect to the Internet
  - Gradually becoming more than just an access network
- Mobility (not discussed)
  - Today's users tolerate disruptions as they move
  - … and applications try to hide the effects
  - Tomorrow's users expect seamless mobility
- Challenges the design of network protocols
  - Wireless breaks the abstraction of a link, and the assumption that packet loss implies congestion
  - Mobility breaks association of address and location
  - Higher-layer protocols don't perform as well