CS5530
Mobile/Wireless Systems
Medium Access Control (MAC)

Yanyan Zhuang

Department of Computer Science

http://www.cs.uccs.edu/~yzhuang

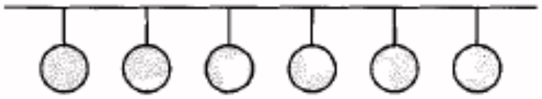
Outline

- Access links
- Access control
- Channel allocation
  - Static allocation
  - Dynamic allocation
- Carrier sense protocols

Access Links

- Point-to-point links
  - Easy coordination
- Broadcast links
  - More than two stations transmit at the same time: collision
  - Challenge: determine who gets to use the channel when there is competition

(a) Point-to-point



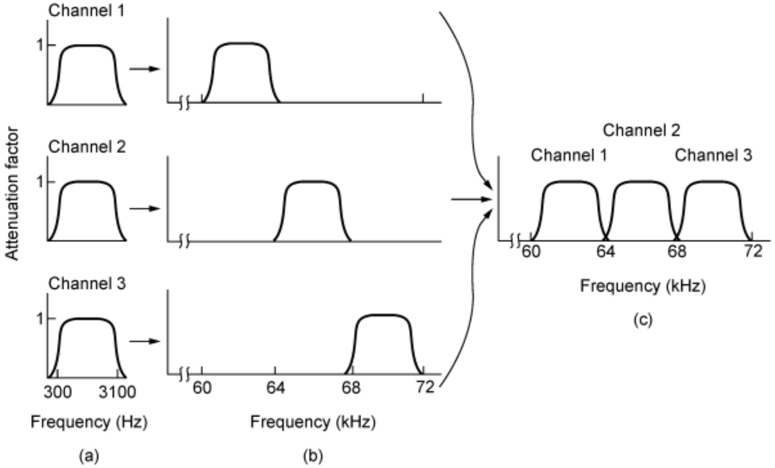
(b) Multipoint-broadcast network

Access Control

- Access control
  - Ensure only one station transmits
  - Ensure no collision occur
- MAC (Medium Access Control)
  - The protocols used to determine who goes next on a broadcast channel
  - Above physical layer, below IP layer

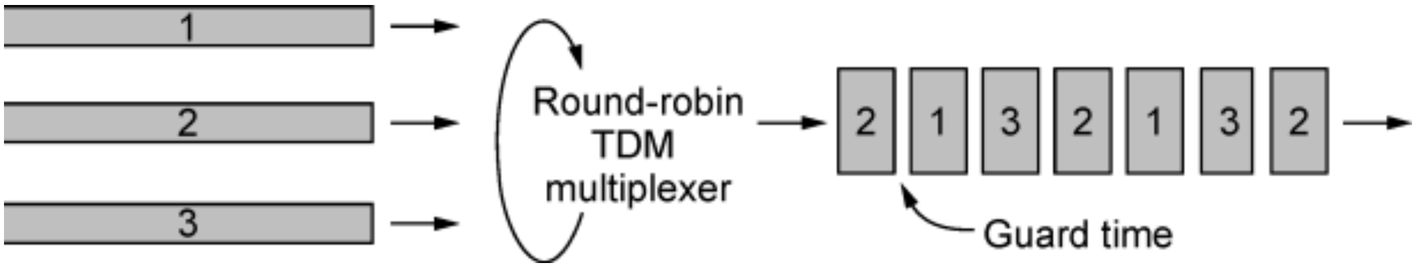
Channel Allocation Problem

- How to allocate a single broadcast channel among competing users
- Static Channel Allocation
  - FDM (Frequency Division Multiplexing)
    - Divides spectrum into frequency bands, with each user having exclusive possession of some band to send their signal



Channel Allocation Problem

- How to allocate a single broadcast channel among competing users
- Static Channel Allocation
  - FDM (Frequency Division Multiplexing)
  - TDM (Time Division Multiplexing)
    - Users take turns (round-robin), each one periodically getting entire bandwidth for a little burst of time



Channel Allocation Problem

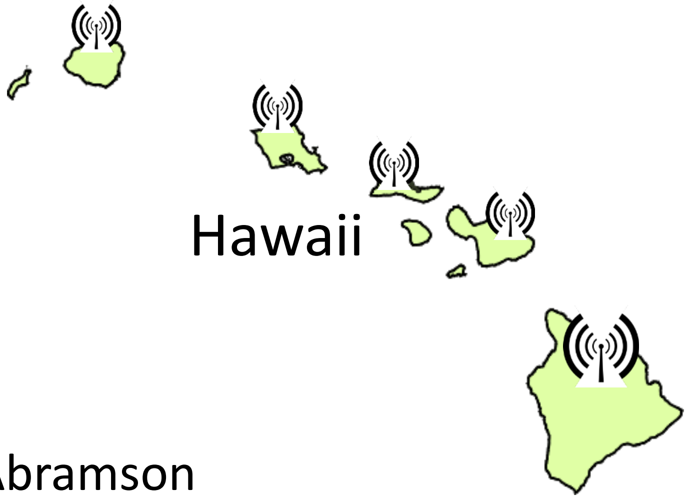
- How to allocate a single broadcast channel among competing users
- Static Channel Allocation
  - FDM (Frequency Division Multiplexing)
  - TDM (Time Division Multiplexing)
  - Advantage/disadvantage
    - A small and constant # of users, each has a steady stream of traffic, static allocation is simple and efficient
    - When # of senders is large and varying or the traffic is bursty: inefficient

Channel Allocation Problem

- How to allocate a single broadcast channel among competing users
- Static Channel Allocation
- Dynamic Channel Allocation
  - No base station/central entity involved, purely distributed

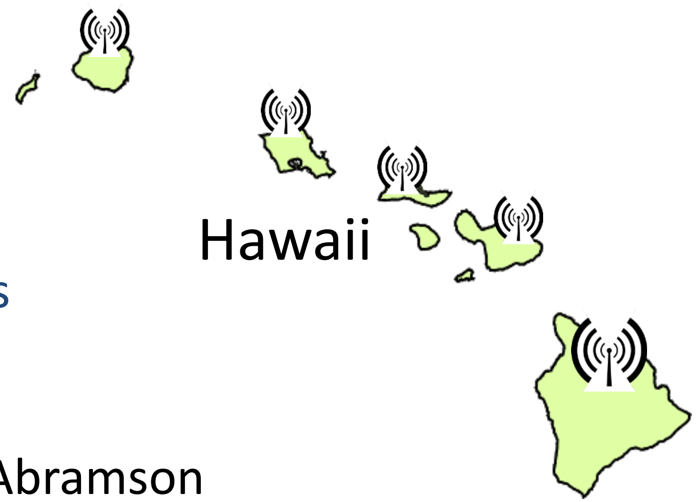
Dynamic Channel Allocation

- Aloha
  - Seminal computer network
    connecting Hawaiian islands in late 1960s
    - When should nodes send?
    - A new protocol was devised by Norm Abramson


Hawaii

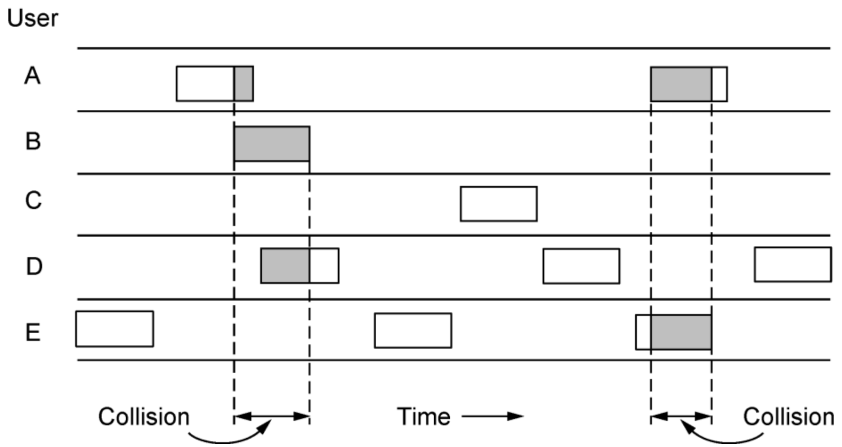
Dynamic Channel Allocation

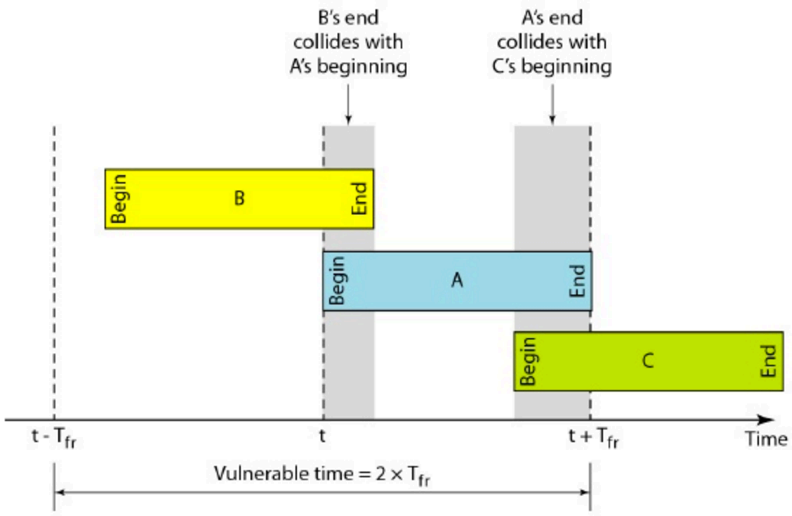
- Aloha
  - Seminal computer network
    connecting Hawaiian islands in late 1960s
    - When should nodes send?
    - A new protocol was devised by Norm Abramson
  - Simple idea
    - Node just sends when it has traffic (no carrier sensing)
    - If there was a collision (no ACK received) then wait a **random time** (called backoff time) and resend



Dynamic Channel Allocation

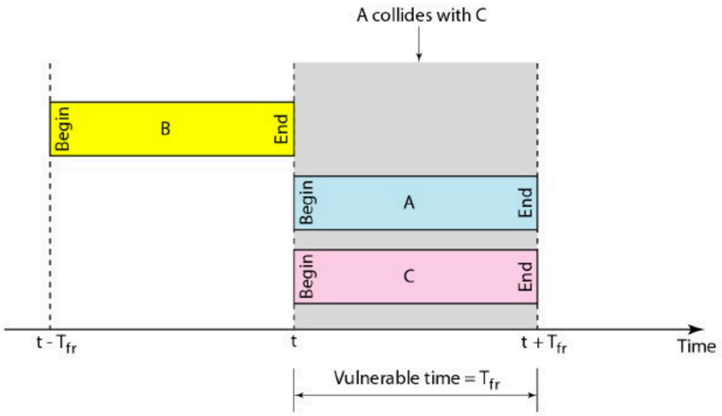
- Aloha
  - Pure Aloha
    - Stations transmit at any time
    - For analysis, assume same length
    - Vulnerable time: 2T

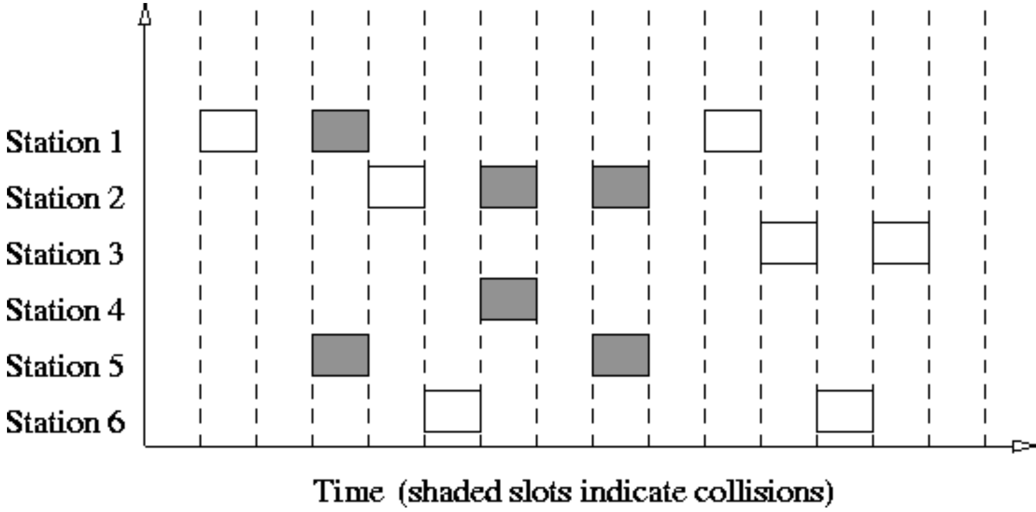




Dynamic Channel Allocation

- Aloha
  - Slotted Aloha
    - Stations transmit only in a slot
    - Vulnerable time: T



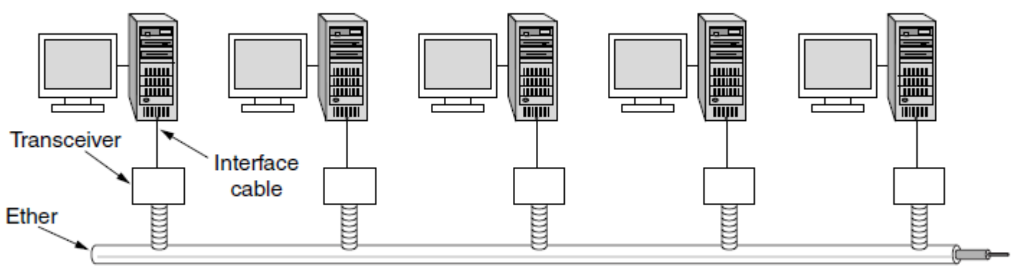


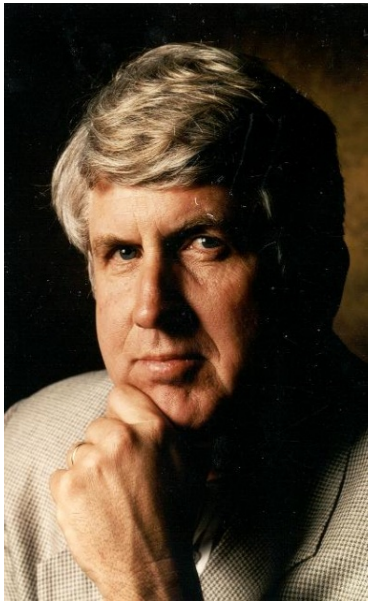
Dynamic Channel Allocation

- Aloha's low efficiency
  - Stations transmit at will, without knowing what others are doing → many collisions
- (W)LANs
  - Possible for stations to detect what others are doing, and thus adapt their behavior accordingly
- Carrier Sense Multiple Access (CSMA) Protocols
  - Protocols in which stations listen for a carrier (i.e., a transmission) and act accordingly

Carrier Sense Protocols

- ALOHA inspired Bob Metcalfe to invent Ethernet for LANs in 1973
  - Nodes share 10 Mbps coaxial cable
  - Hugely popular in 1980s, 1990s





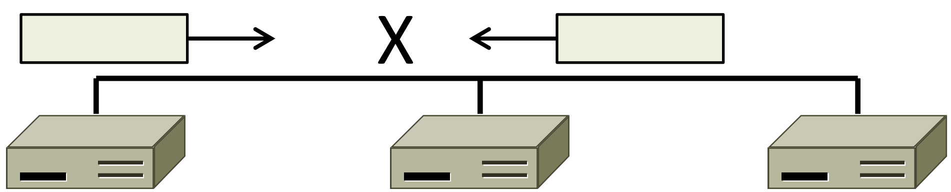
: © 2009 IEEE

Carrier Sense Protocols

- CSMA improves ALOHA by listening before send (Doh!)
  - Can do easily with wires, not wireless
- 1-persistent CSMA
  - A station has data to send: listens to the channel
    - If channel is idle, station sends data
    - If channel is busy, station waits until idle, then transmits a frame
    - If a collision occurs, station waits a random time and starts all over

Carrier Sense Protocols

- Still possible to listen and hear nothing when another node is sending because of **delay**
  - Just after a station begins sending, another station becomes ready to send and sense the channel
  - If the first station's signal has not yet reached the second one, the latter will sense an idle channel and begin sending, resulting in a collision



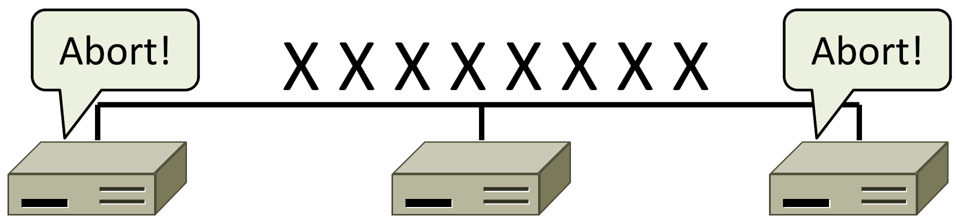
- CSMA is a good defense against collisions only when delay is small

Carrier Sense Protocols

- p-persistent CSMA: applies to **slotted** channels
  - If channel is idle, it transmits with a probability p
    - With a probability q = 1 − p, it defers until the next slot
  - If the station senses that the channel is busy, it waits until the next slot
    - If next slot is also idle, it either transmits or defers again, with probabilities p and q

CSMA/CD (with Collision Detection)

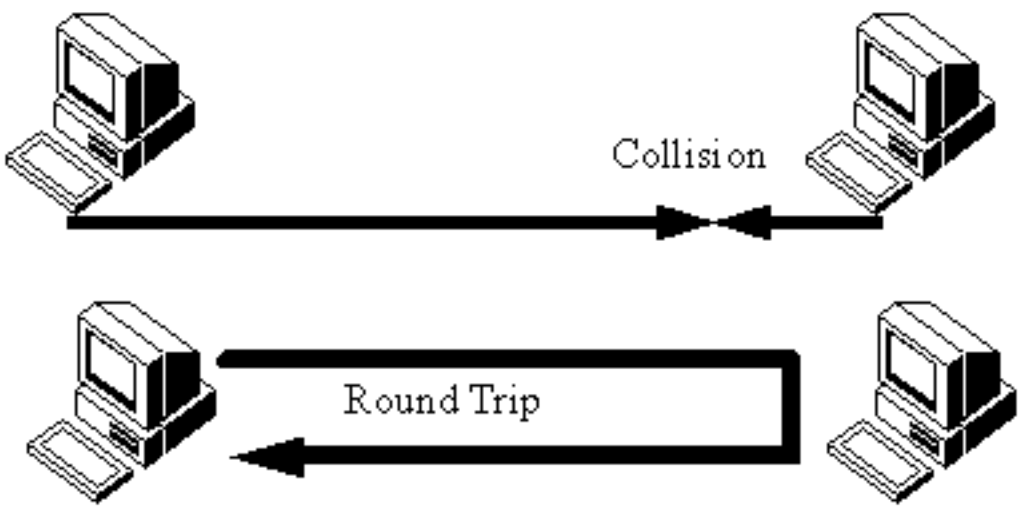
- Reduce the cost of collisions by detecting them and aborting the rest of the frame time
  - Again, we can do this with wires



  - Collision detection is an analog process
    - Hardware must listen to channel while it is transmitting
    - If the signal it reads back is different from the signal it put out, then a collision is occurring
    - Implication: a received signal must **not** be tiny compared to the transmitted signal
      - Difficult for wireless, as received signals may be 1,000,000 times weaker than transmitted signals

CSMA/CD (with Collision Detection)

- How does a station detect a collission? Minimum packet length
  - Tt: transmission time, time to transmit a packet out (decided by length and link bandwidth)
  - Tp: propagation time, time to transmit a packet to another station (decid



CSMA/CD (with Collision Detection)

- Minimum packet length
  - Assume Tp = 1 hour
  - Case 1 A and B transmit simultaneously
    - 10am stations A and B starts transmitting
    - 10:30am collision happens
    - 11am A and B receive collision signal
  - Case 2 A transmits before B
    - 10am A starts transmitting
    - 10:59:59am B starts transmitting
    - 11am collision happens
    - 12pm A receives collision signal
  - In worst case, the time to detect a collision is 2*Tp

CSMA/CD (with Collision Detection)

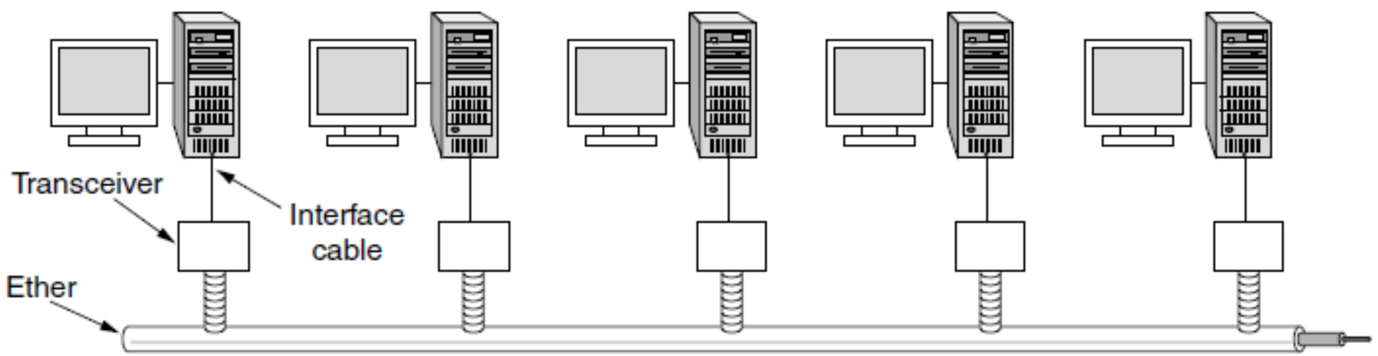
- Minimum packet length
  - In worst case, the time to detect a collision is 2*Tp
  - Detecting collision
    - Receive collision signal while transmitting
    - Tt >= 2*Tp, where Tt = Length (bits) /B (bits per sec)
  - Example: Tp = 1msec, B = 1Mbps, what's the minimum packet length for CSMA/CD?
    - Tt = Length/B >= 2*Tp. Length >= 2*Tp*B = 2*10^(-3)*10^6 = 2000 bits
    - What if a packet is shorter than 2000 bits? Padding
  - CSMA/CD used for Ethernet

CSMA/CD (with Collision Detection)

- Should I resend right away?
- Binary Exponential Backoff (BEB): cleverly estimates probability
  - 1st collision, wait 0 or 1 frame times (0…2^1-1)
  - 2nd collision, wait from 0 to 3 times (0…2^2-1)
  - 3rd collision, wait from 0 to 7 times (0…2^3-1) …
- BEB doubles interval for each successive collision
  - Quickly gets large enough to work
  - Very efficient in practice

Classic Ethernet, or IEEE 802.3

- Most popular LAN of the 1980s, 1990s
  - Multiple access with “1-persistent CSMA/CD with BEB”

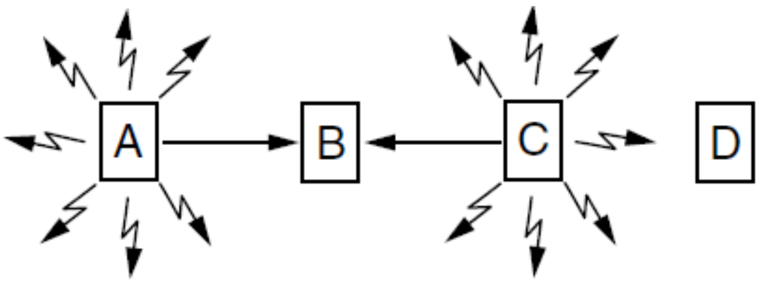


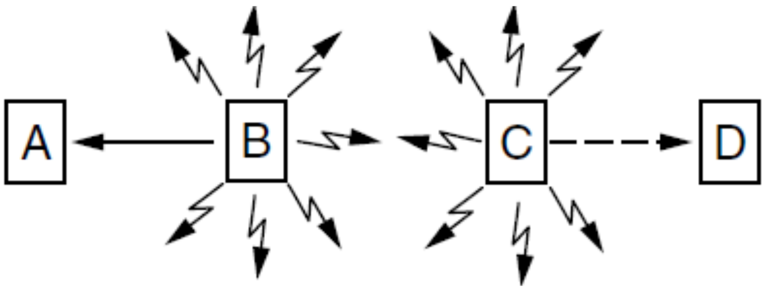
Wireless LAN Protocols

- Different from Ethernet
  - A wireless system cannot detect a collision while it is occurring
    - The received signal at a station may be a million times weaker than transmitted signal
  - A station on a wireless LAN may not be able to transmit frames to, or receive frames from all other stations because of the limited range
    - In wired LANs, when one station sends a frame, all other stations receive it (with some delay)
- A naive approach
  - Try CSMA: just listen for other transmissions and only transmit if no one else is doing so
  - What’s the problem?

Wireless LAN Protocols

- Remember hidden terminals and exposed terminals?





1. Nodes may have different areas of coverage – doesn't fit Carrier Sense
2. Nodes can't hear while sending – can't Collision Detect

MACA (Multiple Access with Collision Avoidance)

- MACA uses a short handshake instead of CSMA (Karn, 1990)
  - 802.11 uses a refinement of MACA
- Protocol rules:
  1. A sender node transmits a RTS (Request-To-Send, with frame length)
  2. The receiver replies with a CTS (Clear-To-Send, with frame length)
  3. Sender transmits the frame while other nodes hearing the CTS stay silent
     - Collisions on the RTS/CTS are still possible, but less likely

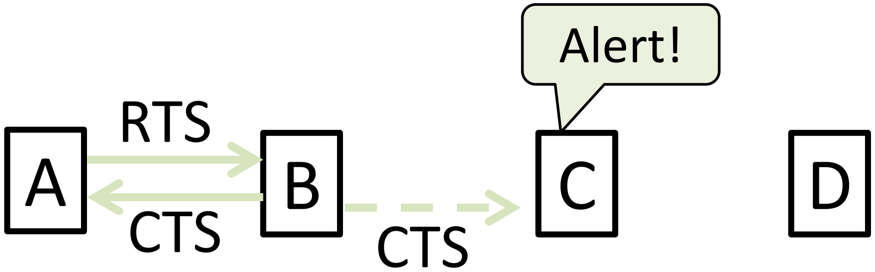
MACA – Hidden Terminals (1)

- A→B with hidden terminal C
  1. A sends RTS, to B

MACA – Hidden Terminals (2)

- A→B with hidden terminal C

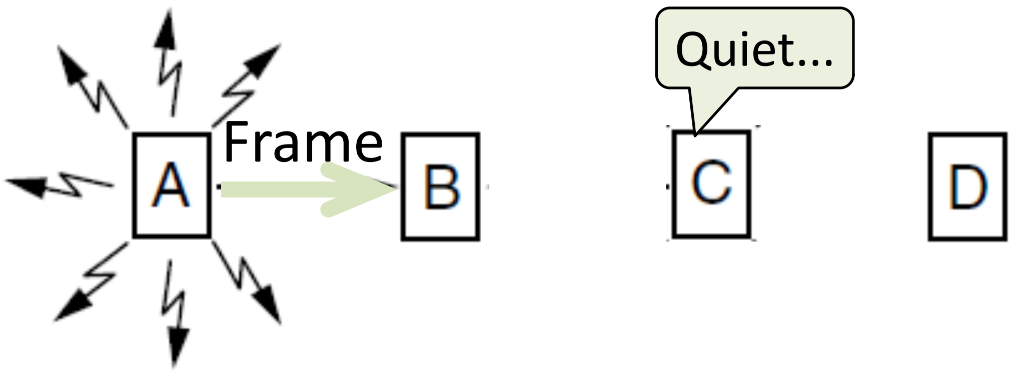
2. B sends CTS, to A, and C too



Ref. CN5E, NT@UW, WUSTL

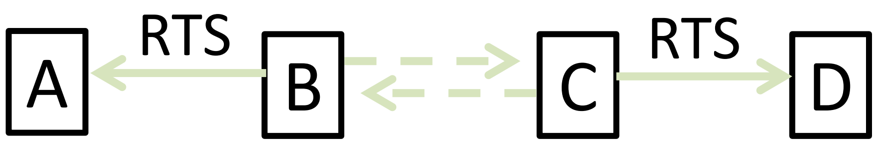
MACA – Hidden Terminals (3)

- A→B with hidden terminal C
    3. A sends frame while C defers



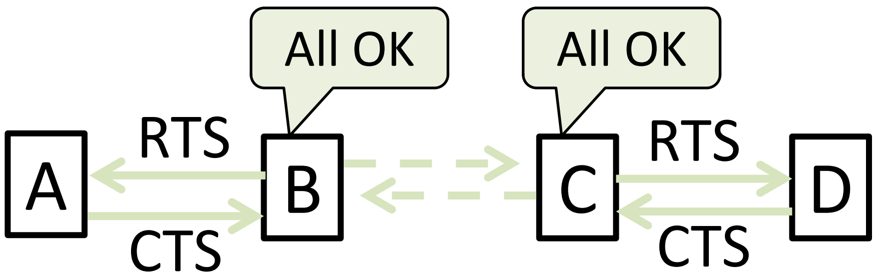
MACA – Exposed Terminals (1)

- B→A, C→D as exposed terminals
  - B and C send RTS to A and D



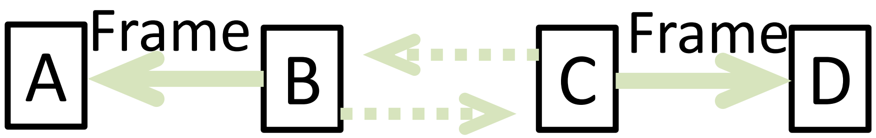
MACA – Exposed Terminals (2)

- B→A, C→D as exposed terminals
  - A and D send CTS to B and C



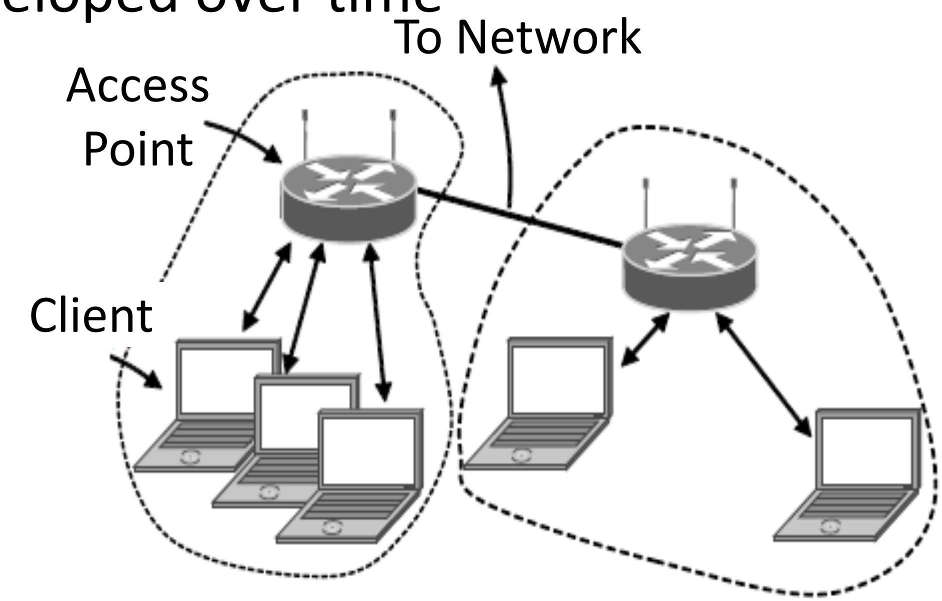
MACA – Exposed Terminals (3)

- B→A, C→D as exposed terminals
  - B sends frame to A while C sends frame to D



802.11, or WiFi

- Very popular wireless LAN started in the 1990s
- Clients get connectivity from a (wired) AP (Access Point)
- It's a multi-access problem ☺
- Various flavors have been developed over time
  - Faster, more features



802.11, or WiFi

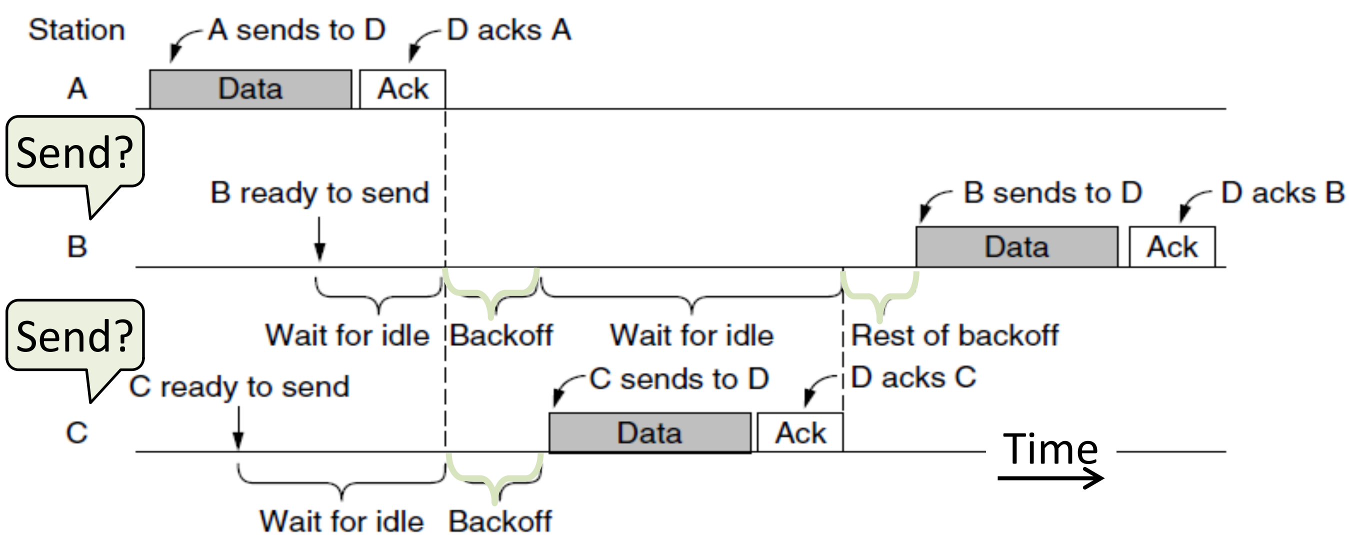
- 802.11 MAC sublayer protocol different from that of Ethernet
  - Radios are nearly always half duplex: cannot transmit and listen for collision at the same time
  - Transmission ranges of different stations may be different
    - With a wire, the system is engineered so that all stations can hear each other
- 802.11 tries to avoid collisions with a protocol called CSMA/CA (CSMA with Collision Avoidance)
  - Conceptually similar to Ethernet's CSMA/CD, with channel sensing before sending and exponential back off after collisions

CSMA/CA

- A station that has a frame to send starts with a random backoff
  - It does not wait for a collision
  - The number of slots to backoff is chosen in the range 0 to, say, 15
- Waits until the channel is idle, and counts down idle slots
  - Idle: by sensing that there is no signal for a short period of time
  - Count down pauses when frames are sent by other stations
  - Sends its frame when the counter reaches 0
- If frame gets through, destination sends a short ack
  - Lack of an ack is inferred as an error, whether a collision or otherwise
  - The sender doubles the backoff period and tries again
    - Continues with exponential backoff until (1) the frame has been successfully transmitted, or (2) the maximum # of retransmissions has been reached

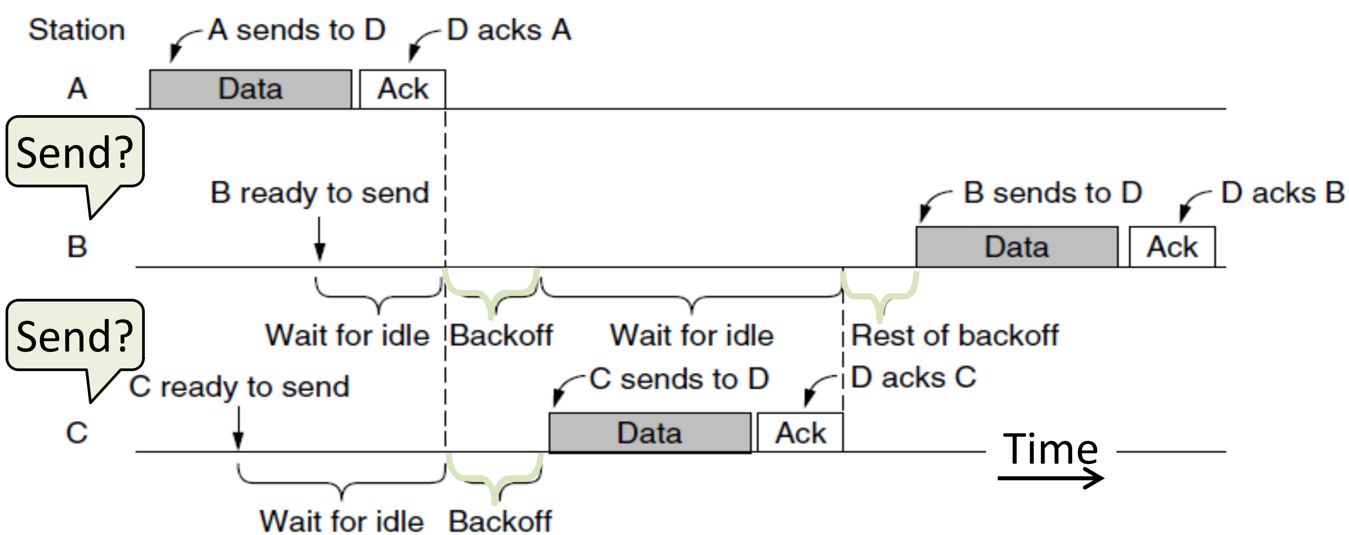
CSMA/CA

- Station *A* is the first to send a frame to D
- While *A* is sending, stations *B* and *C* become ready to send
  - They see that the channel is busy and wait for it to become idle
  - Shortly after *A* receives an acknowledgement, the channel goes idle
  - Rather than sending a frame right away and colliding, *B* and *C* both perform a backoff



CSMA/CA

- While *A* is sending, stations *B* and *C* become ready to send
  - C picks a short backoff, and thus sends first
  - *B* pauses its countdown while it senses that *C* is using the channel, and resumes after *C* has received an acknowledgement
  - *B* then completes its backoff and sends its frame



CSMA/CA

- Difference compared to CSMA/CD
  - Starting backoffs early helps to avoid collisions
    - This avoidance is worthwhile because collisions are expensive, as the entire frame is transmitted even if one occurs
  - Acknowledgements are used to infer collisions because collisions cannot be detected

802.11 Services

- Association service
  - Mobile stations connect to APs
  - Typically used after a station moves in radio range of an AP
  - Upon arrival, station learns the identity and capabilities of the AP (from beacon frames or by directly asking AP)
    - Capabilities include data rates, security arrangements, power-saving capabilities, quality of service support, etc.
  - Station sends a request to associate with AP. The AP may accept or reject the request.

802.11 Services

- Re-association
  - Lets a station change its preferred AP
  - Useful for mobile stations moving from one AP to another AP in the same extended 802.11 LAN
- Disassociate
  - Either station or AP may disassociate – breaking the relationship
  - A station uses this before shutting down or leaving the network
  - AP may use it before going down for maintenance

802.11 Services

- Authentication service
  - Stations must authenticate before sending frames via AP
  - Authentication is handled in different ways depending on the choice of security scheme
    - If the 802.11 network is ‘‘open,’’ anyone is allowed to use it.
    - Otherwise, credentials are needed to authenticate

802.11 Services

- Authentication service
  - Stations must authenticate before sending frames via AP
  - Authentication is handled in different ways depending on the choice of security scheme
    - If the 802.11 network is ‘‘open,’’ anyone is allowed to use it.
    - Otherwise, credentials are needed to authenticate
      - WPA2 (WiFi Protected Access 2): AP talks to an authentication server that has a username and password database
      - WEP (Wired Equivalent Privacy): Use is discouraged because of design flaws that make WEP easy to compromise

802.11 Services

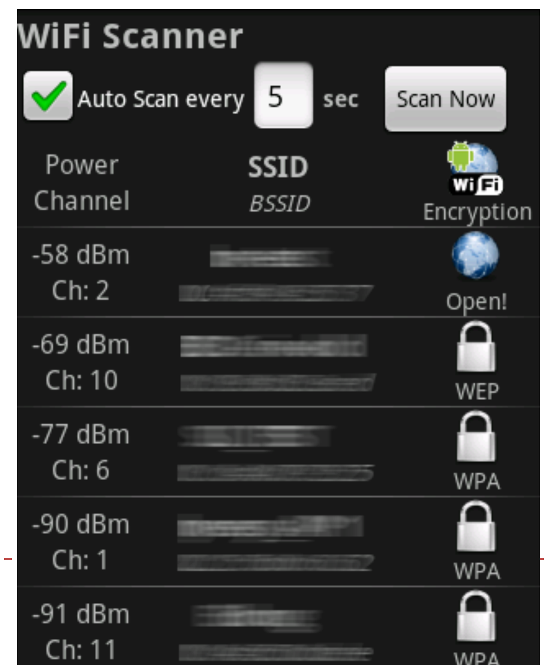
- Distribution service
  - Once frames reach the AP, distribution service determines how to route them
    - If destination is local to AP, frames sent out directly over the air
    - Otherwise, forwarded over the wired network
- Integration service
  - Handles translation needed for a frame to be sent outside 802.11 LAN, or to arrive from outside 802.11 LAN
    - The common case: connecting the wireless LAN to the Internet

802.11 Services

- Privacy service
  - For information sent over a wireless LAN to be kept confidential, it must be encrypted
  - Manages details of encryption and decryption
    - The encryption algorithm for WPA2 is based on AES (Advanced Encryption Standard)
- QoS traffic scheduling service
  - Handles traffic with different priorities
    - Give voice and video traffic preferential treatment compared to best-effort and background traffic

802.11/WiFi Summary

- CSMA/CA
  - Cannot detect collision → passively avoid instead
- Various WiFi services
  - Association, authentication, privacy, etc.
- Android



Bluetooth

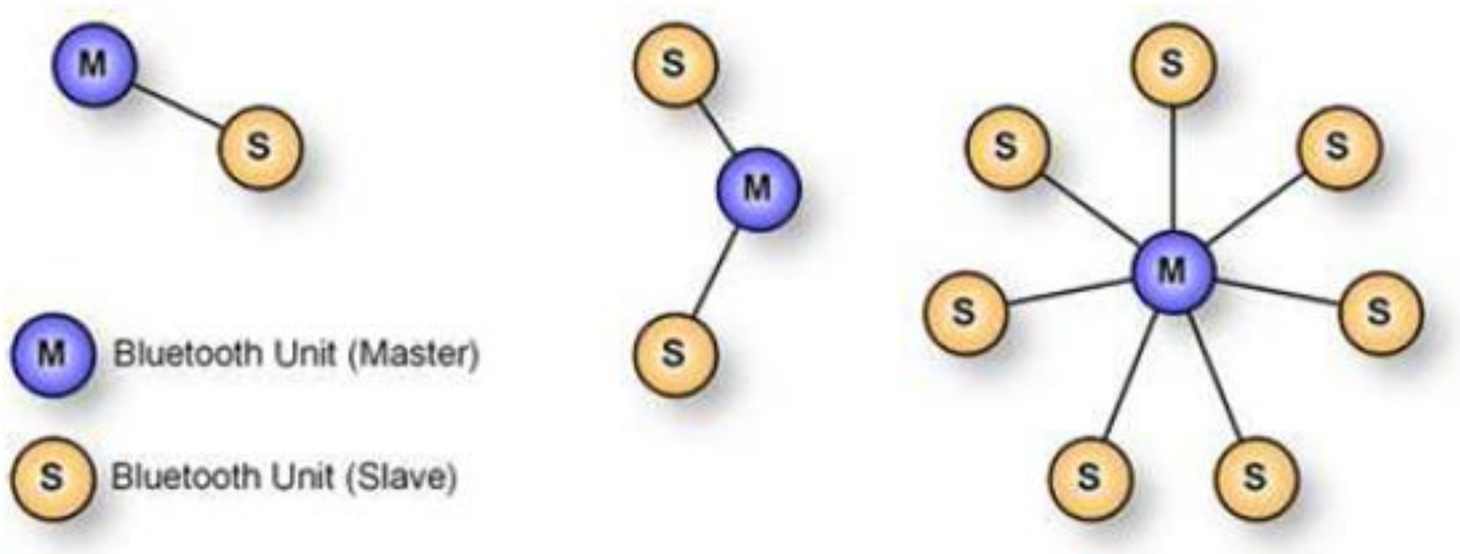
- In 1994, the L. M. Ericsson company
  - Connecting mobile phones to other devices (e.g., laptops) without cables
  - With four other companies (IBM, Intel, Nokia, and Toshiba), formed a SIG (Special Interest Group, i.e., consortium) in 1998 to develop a wireless standard
    - Interconnecting computing and communication devices and accessories using short-range, low-power, inexpensive wireless radios
    - Named after Harald Blaatand (Bluetooth) II (940–981), a Viking king who unified Denmark and Norway

Bluetooth

- A brief history
  - Bluetooth 1.0 released in July 1999
  - Higher data rates were added to Bluetooth 2.0 in 2004
  - 3.0 release in 2009: device pairing in combination with 802.11
  - 4.0 release in December 2009 specified low-power operation
  - 5 release June 2016: IoT technology, 4x range, 2x speed, 8x increase in broadcasting capacity of low energy transmissions
- Bluetooth protocol
  - Let devices find and connect to each other, an act called **pairing**, and securely transfer data

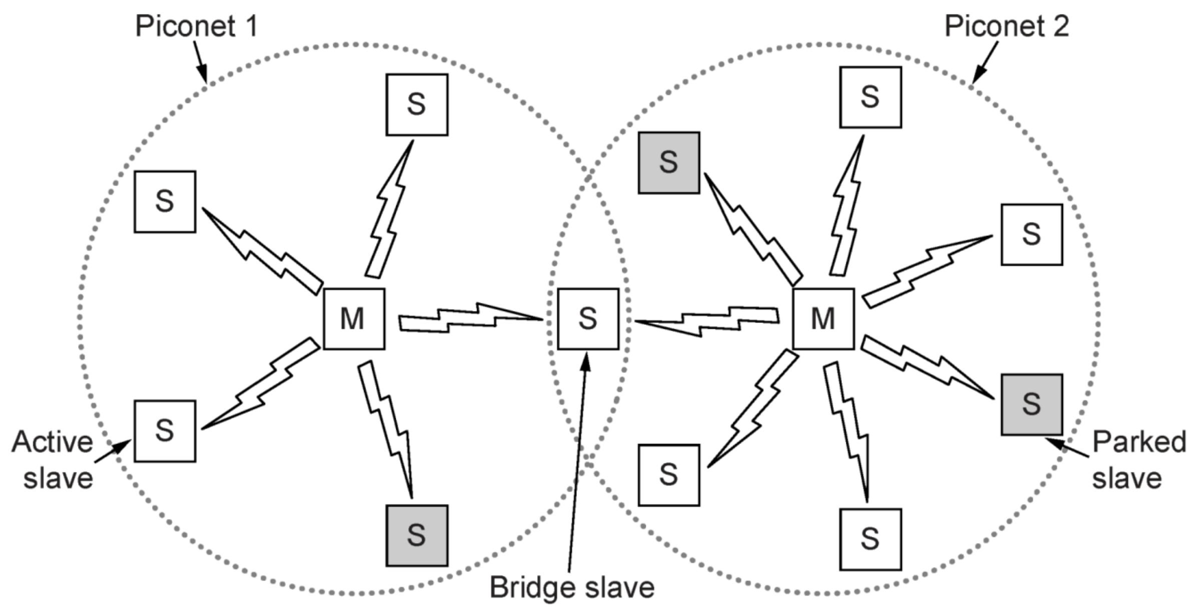
Bluetooth Architecture

- Basic unit of a Bluetooth system is a piconet
  - Consists of a master node and up to seven **active** slave nodes
    - Older tech: within a distance of 10 meters



Bluetooth Architecture

- Multiple piconets can co-exist & connected via a bridge node in multiple piconets
  - An interconnected collection of piconets is called a scatternet



Two piconets can be connected to form a scatternet.

Bluetooth Architecture

- A piconet is essentially a centralized TDM
  - Master controlling the clock and determining which device gets to communicate in which time slot
  - All communication is between the master and a slave; no direct slave-slave communication
- In a piconet, there can be up to 255 parked nodes
  - Devices switched to a low-power state to reduce battery drain
  - Cannot do anything except respond to an activation or beacon signal from master

Bluetooth Applications

- Bluetooth specifies particular applications and provides different protocol stacks
  - Applications are called profiles
- Audio and video
  - **Intercom profile** allows two telephones to connect as walkie-talkies
  - **Headset and hands-free profiles** provide voice communication between a headset and its base station
    - Used for hands-free telephony while driving a car

Bluetooth Applications

- Human interface device profile
  - For connecting keyboards and mice to computers
  - Let a mobile phone or other computer receive images from a camera or send images to a printer
  - Use a mobile phone as a remote control for a (Bluetooth-enabled) TV
- Generic access profile
  - On which all of the other profiles are built, provides a way to establish and maintain secure links between master and slaves

Bluetooth MAC Layers

- Has a link control layer, similar to MAC layer
- Master defines a series of 625-µsec time slots
  - Master's transmissions starting in even slots, slaves' transmissions in the odd ones (TDM)
  - Payload of frame can be encrypted for confidentiality with a key chosen when the master and slave connect

Bluetooth MAC Layers

- Link manager protocol
  - **Pairing** procedure: to make sure devices are allowed to communicate
    - *Secure simple pairing* enables users to confirm that both devices display the same passkey (device generated), or observe a passkey on one device and type it into the second device

Bluetooth MAC Layers

- Link manager protocol
  - **Pairing** procedure: to make sure devices are allowed to communicate
  - Link manager protocol sets up logical channels, called **links**
    - SCO (Synchronous Connection Oriented) link: used for real-time data, such as telephone connections, allocates a fixed slot in each direction
    - ACL (Asynchronous Connection-Less) link: used for packet-switched data (occur at irregular intervals), delivered on a best-effort basis – No guarantees

Bluetooth Summary

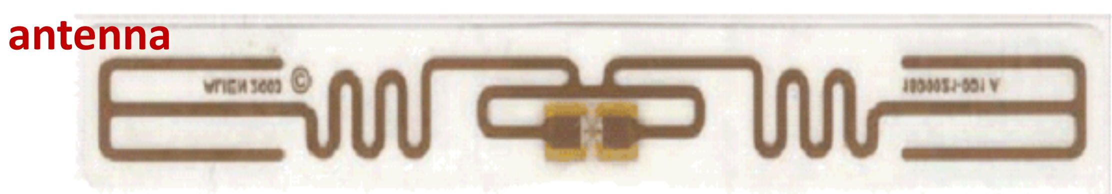
- Short range, low power
- Piconet, scatternet
  - Essentially TDM
- Application profiles
- Pairing, links

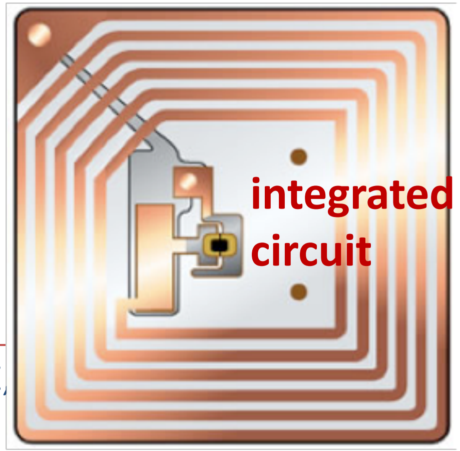
RFID (Radio Frequency IDentification)

- NFC (Near Field Communication) and UHF (Ultra High Frequency)
- EPC (Electronic Product Code): focus of this section
  - Auto-ID Center at the Massachusetts Institute of Technology in 1999
  - Replacement for barcodes
    - Carry a larger amount of information
    - Electronically readable up to 10 m, even when it is not visible

RFID Architecture

- Two components: tags and readers
  - Tags are small, inexpensive devices
    - Have a unique 96-bit EPC identifier and a small amount of memory that can be read and written by reader
    - Memory might be used to record the location history of an item, e.g., as it moves through the supply chain
    - Have no battery and must gather power from transmissions of a nearby **reader**



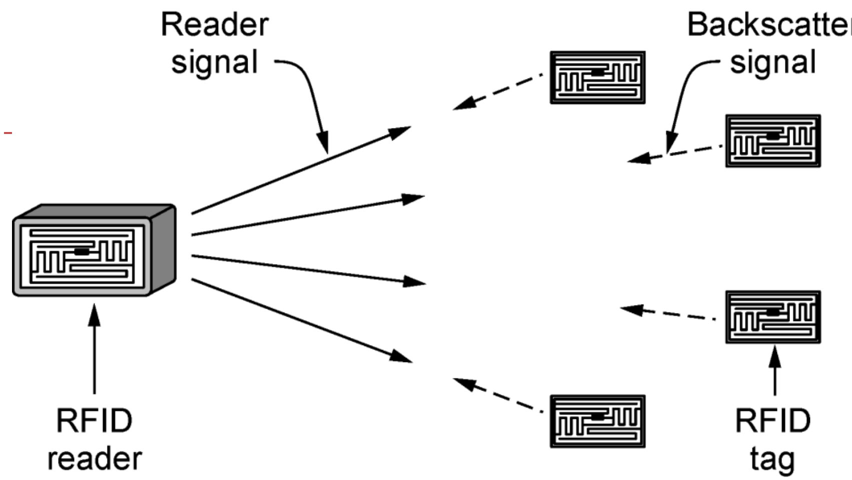


Architecture

- Two key components: tags and readers
  - Readers are like access points in WiFi networks – much more powerful than tags
    - Have power sources, multiple antennas
    - In charge of when tags send and receive messages
    - Must solve multiple access issue caused by tags within reading range
    - Inventory tags: to discover identifiers of nearby tags

Architecture

- Reader always transmits
  - To send bits to tags
- Tags
  - Harvest signal to get power
  - To send data, a tag changes whether it is reflecting the signal from the reader or absorbing it: **backscatter**
    - A low-energy way for tags to create a weak signal that shows up at the reader



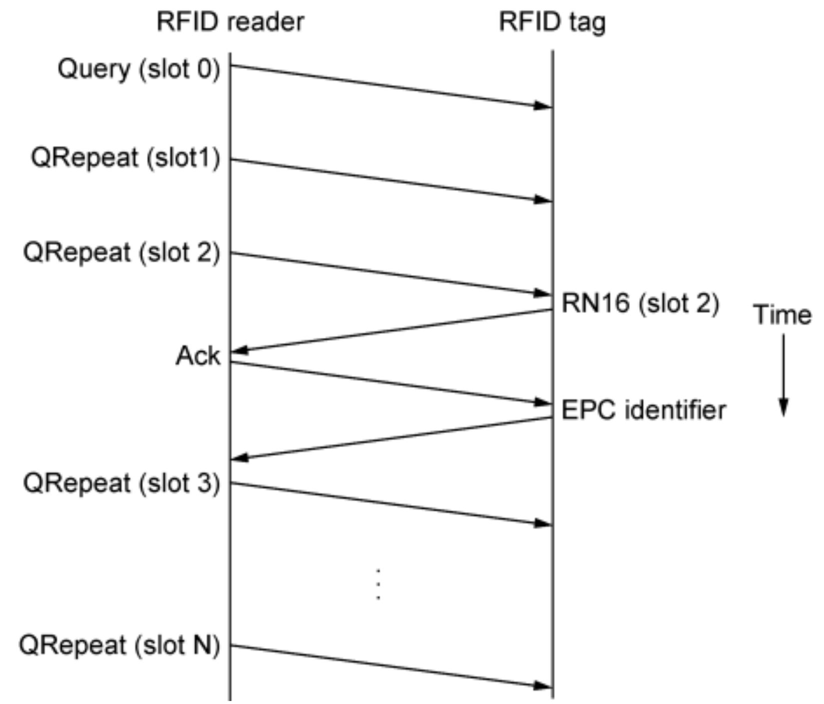
RFID architecture.

Multiple Access

- To inventory nearby tags
  - Reader needs to receive data from each tag that gives its ID
  - A multiple access problem
    - Reader broadcasts a query to ask tags for IDs
    - Tags that replied right away would collide like in an Ethernet

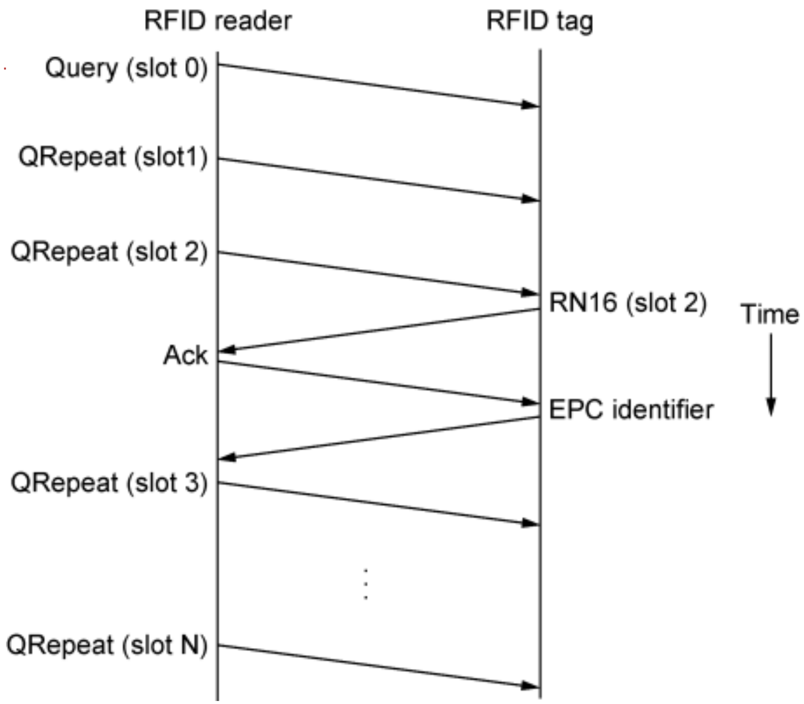
Multiple Access

- Slot 0
  - Reader sends a Query message
  - QRepeat advances to next slot



Multiple Access

- Slot 0
  - Reader sends a Query message
  - QRepeat advances to next slot
- ….Slot 2
  - Tags pick slot 2 to reply
  - Tags do not send IDs when they first reply
    - Sends a short 16-bit random number in an RN16 message
    - If there is no collision, the reader sends an ACK message
    - The tag has acquired the slot and sends its identifier



Multiple Access

- Message exchange
  - IDs are long → collisions on ID messages are expensive
    - A short exchange to test if tag can safely use the slot to send ID
  - Once ID has been transmitted, tag temporarily stops responding to Query messages
    - All remaining tags can be identified