CSE 3231
Computer Networks

Chapter 4
The Data Link Layer
part 1

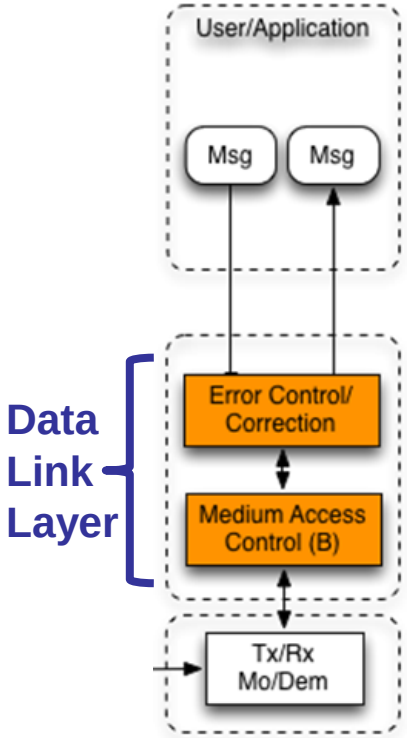
William Allen, PhD

Fall 2020

The MAC Sublayer

The Medium Access Control (MAC) sublayer determines which node can transmit on a multi-access link

- MAC is part of the Data Link layer and interfaces directly with the Physical Layer so it can monitor network activity
- Details vary from one protocol to the next



Channel Allocation Problem

For a fixed channel with traffic from *N* users

- We could divide the available bandwidth using FDM, TDM, CDMA, etc.
- This creates a *static* allocation, e.g., FM radio

But, this static allocation approach performs poorly with *bursty* traffic

- The allocation to a user will sometimes go unused
- Other users cannot access that unused bandwidth

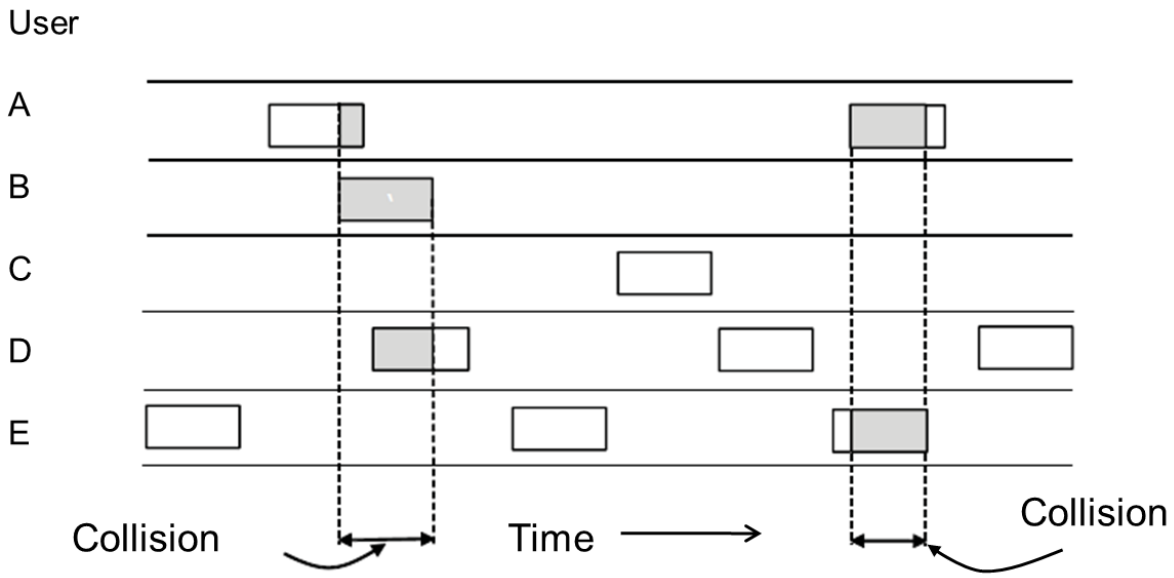
Dynamic allocation only gives a user access to the channel when they need it

- Better resource sharing than fixed allocations

ALOHA

In the original (pure) ALOHA, users can transmit frames whenever they have data to send

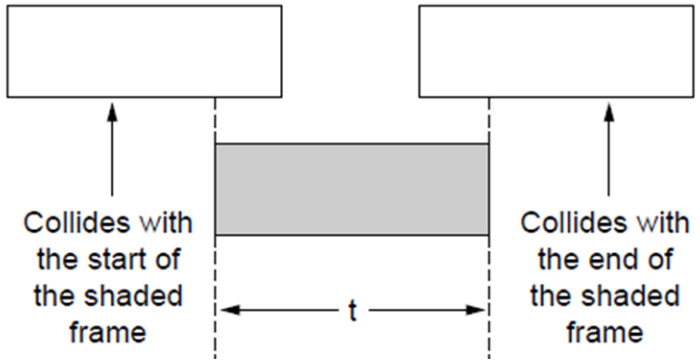
- If collisions occur, retry after a random wait time
- Under a low load this can be moderately efficient



ALOHA

However, collisions will happen when another user transmits during an overlapping period

– this can potentially impact two other user's frames

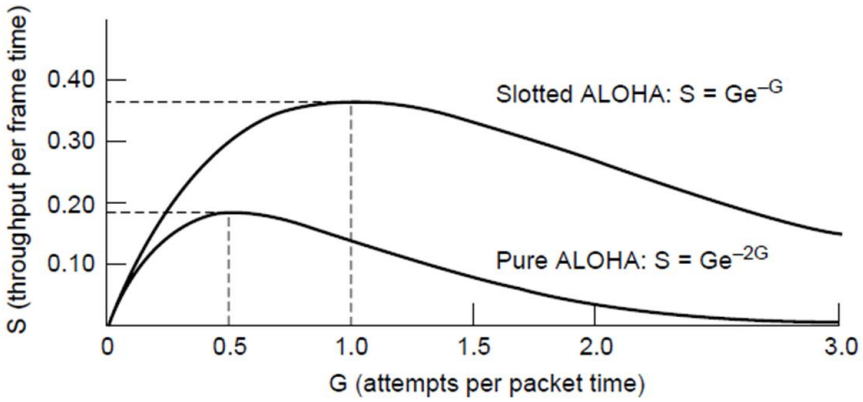


The solution was to synchronize senders into regular time slots to reduce collisions, this is called *Slotted Aloha*

ALOHA

Users can only transmit at the beginning of a pre-determined time slot

- This did not stop collisions, but limited their impact
  - a collision will affect only one time slot
- Experiments showed that Slotted ALOHA is twice as efficient as the original ALOHA
  - Low load wastes slots, but high loads can cause collisions



Carrier Sense Multiple Access (CSMA)

CSMA improves on ALOHA by monitoring the channel to discover (*sense*) if it is busy

- Users don't transmit if the channel is already in use

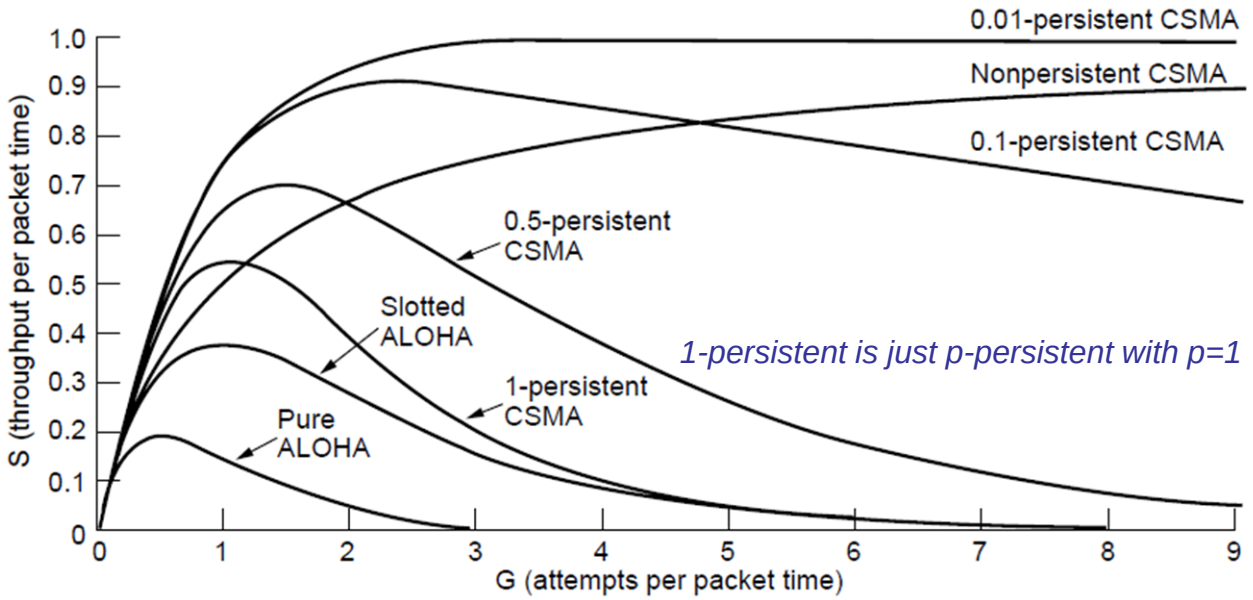
There are several variations on what to do if the channel is busy:

- *1-persistent* CSMA (a greedy approach) sends another frame as soon as the channel is idle
- *nonpersistent* CSMA (a less greedy approach) waits for a random wait time and then tries again
- *p-persistent* CSMA sends again with probability *p*, if the channel is still busy, it repeats the same process

CSMA Performance

All versions of CSMA outperform ALOHA

- *p-persistent* with lower values of *p* performs better under high loads than the other versions of CSMA
  - 802.11 (WiFi) uses a version of p-persistent



CSMA – Adding Collision Detection

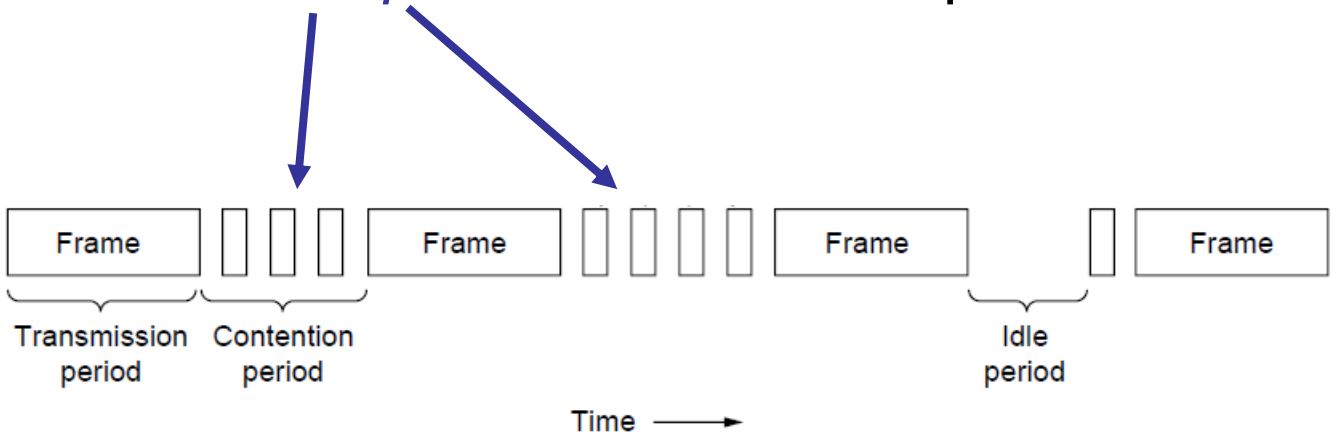
Adding Collision Detection (CD) to CSMA can detect collisions and end transmission early

- The combination is referred to as CSMA/CD
- Detecting collisions early reduces the length of time the collision occurs and clears the channel faster
- However, the distance between nodes determines the delay from the time that one node transmits until another node senses that transmission
  - This may put a practical limit on the length of wired links
- Several approaches have been developed to deal with this problem

CSMA – Adding Collision Detection

Contention (i.e., two or more users colliding) can occur because of the time it takes for a frame to travel along the transmission media

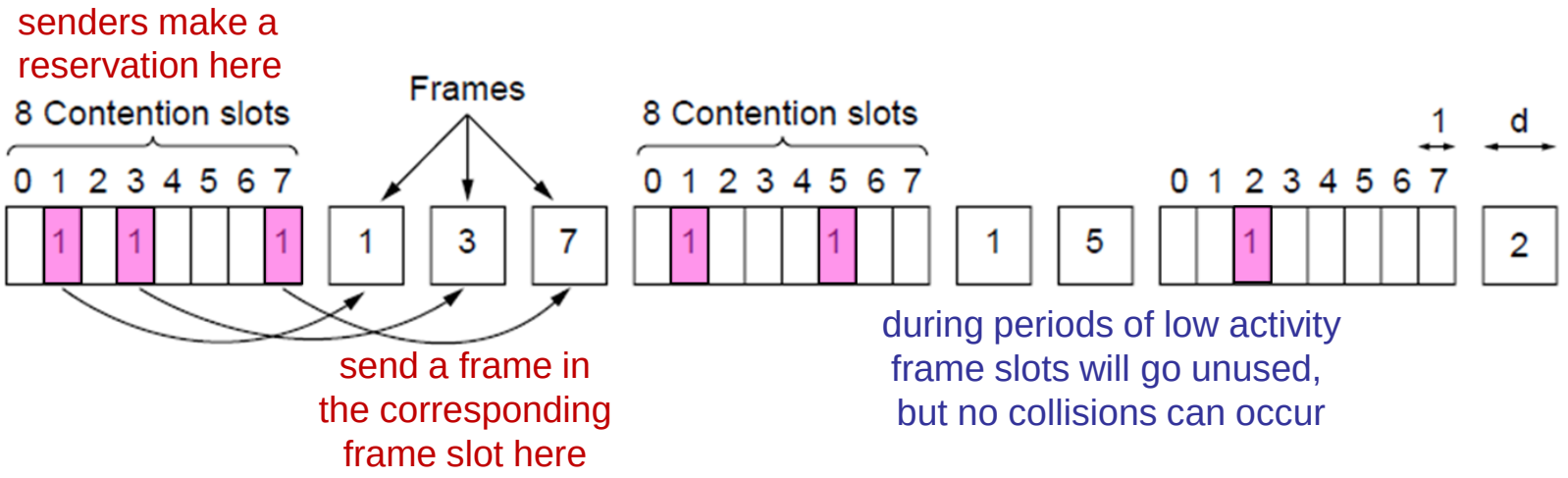
- Just because one node does not sense traffic on the network does not mean that another node that is farther away has not *already started* sending
- the *contention period* is that overlap in time



Collision-Free – Bitmap-Based

This collision-free protocol avoids collisions entirely by allowing *reservations* for frame slots

- Senders know when it will be their turn to send and they *set a bit* in the corresponding contention slot
- That reserves a frame slot for their exclusive use
- If they don't need to send, they do nothing



Collision-Free – Token Ring

This approach uses a special frame called a *token* to pass control of the channel from one user to another, it is specified in *IEEE 802.5*

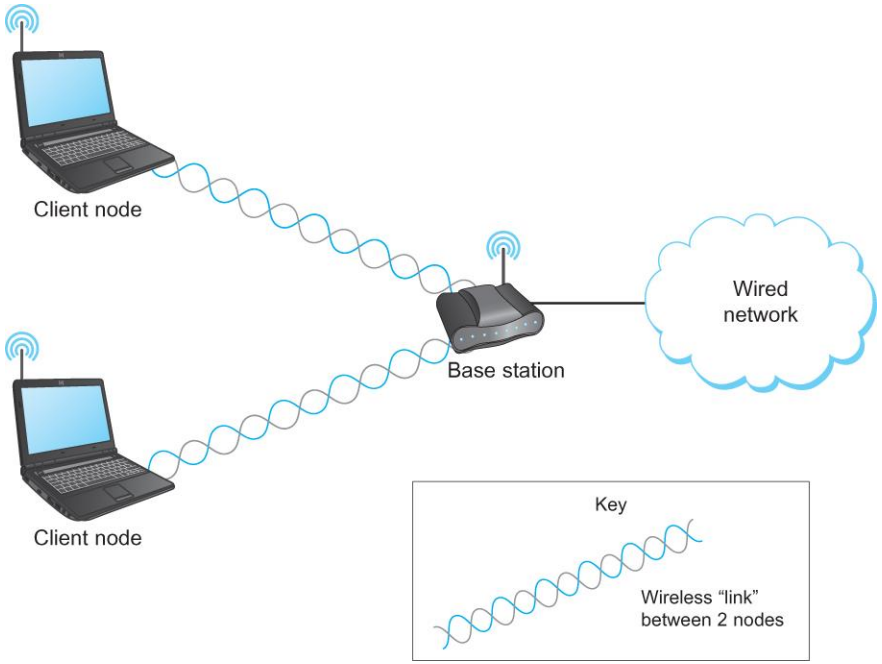
- The network is organized as a ring or loop and the token is continually passed from node to node
- If a node wants to send a frame, it *holds the token* to prevent anyone else from transmitting
- After it sends the frame, it *releases the token* so someone else can use it
- Only one node can hold the token at a time, avoiding collisions, and each node gets their turn to send

Wireless Links

- Wireless links transmit electromagnetic signals
  - Radio, microwave, infrared
- Wireless links all share the same transmission medium
  - The challenge is to share it efficiently without unduly interfering with each other
  - Sharing is accomplished by dividing the medium along the dimensions of frequency and space
- Different media can be shared in different ways
  - e.g., microwave transmission is directional, radio is not, infrared doesn't work well over long distances

Wireless LANs

- Many widely-used wireless LANs today are asymmetric
  - The two end-points are different kinds of nodes
    - One end-point usually has no mobility, but has wired connection to the Internet and is known as the base station or Access Point (AP)
    - The node at the other end of the link is often mobile



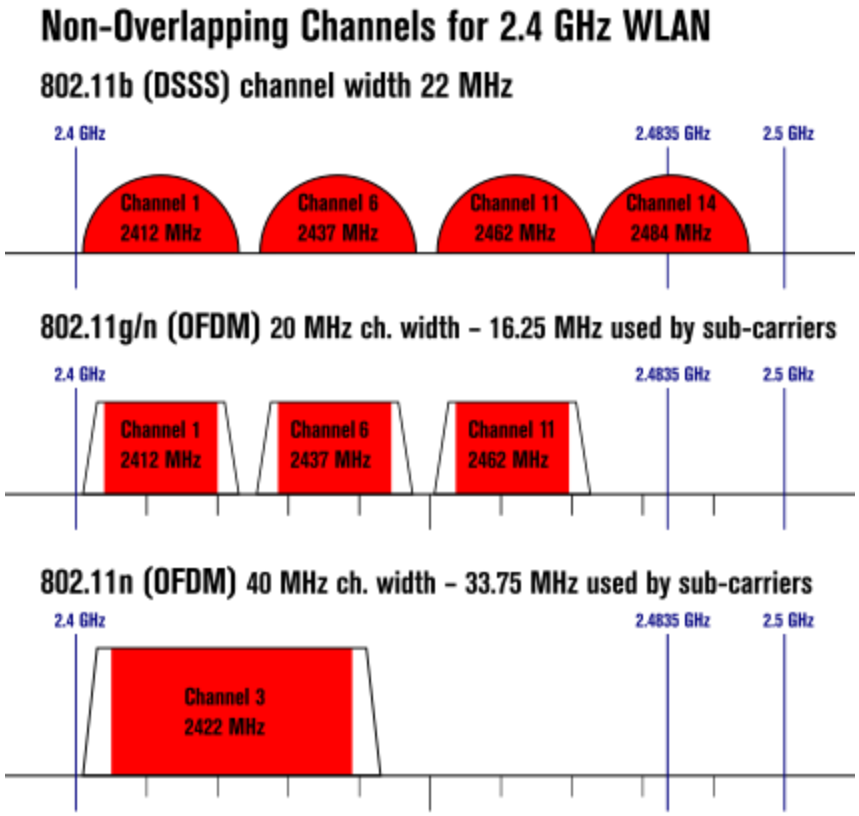
UNITED STATES FREQUENCY ALLOCATIONS

THE RADIO SPECTRUM

U.S. DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Office of Spectrum Management
JANUARY 2016

Example: WiFi Frequencies

- Frequency Bands: 2.4 GHz, 3.6 GHz, 4.9 GHz, 5 GHz, and 5.9 GHz
- Channels are allocated within each Band
  - channels can overlap adjacent channels



Wireless Links

- Finally, there are several frequency bands set aside for "license exempt" usage
  - Bands in which a license is not needed
  - For example: cordless phones, radio control devices, remote controls, etc.
- Devices that use license-exempt frequencies are still subject to certain restrictions
  - Transmission power is limited, which limits the signal range, reducing interference with other devices
    - A cordless phone might have a range of about 100 feet.
    - Bluetooth & Wi-Fi transmitters are limited to 100 milliWatts.

Wireless Links

- Restrictions on specific bands may require the use of a Spread Spectrum technique which spreads the signal over a wider frequency band
  - Minimizes the impact of interference from other devices
  - One technique is called *Frequency hopping* which transmits the signal over a pre-selected set of frequencies in a random sequence
  - First transmit at one frequency, then a second, then a third…
    - The sequence is computed by a specific algorithm
    - The receiver uses the same algorithm as the sender and is able to hop frequencies in sync with the transmitter to correctly receive the data frames

WiFi Interference

- The 2.4 GHz band is shared by many non-networking applications which can cause interference with wireless networking
  - some models of cordless phone, microwave ovens, wireless microphones and alarms
  - newer devices have better shielding to avoid ‘leaking’ signals or have better rejection of signals on adjacent channels
  - another solution is to use a different band

Wireless Links

- Wireless technologies differ in a variety of dimensions
  - How much bandwidth they provide
  - How far apart the communication nodes can be
- Four prominent wireless technologies
  - Bluetooth
  - Wi-Fi (more formally known as 802.11)
  - WiMAX (802.16)
  - cellular wireless (3G, LTE, etc.)

Wireless Links

	Bluetooth (802.15.1)	Wi-Fi (802.11)	3G Cellular
Typical link length	10 m	100 m	Tens of kilometers
Typical data rate	2 Mbps (shared)	54 Mbps (shared)	Hundreds of kbps (per connection)
Typical use	Link a peripheral to a computer	Link a computer to a wired base	Link a mobile phone to a wired tower
Wired technology analogy	USB	Ethernet	DSL

Overview of selected wireless technologies

IEEE 802.11

- Also known as Wi-Fi
- Like its Ethernet and token ring siblings, 802.11 is designed for use in a limited geographical area (homes, office buildings, campuses)
  - Primary challenge is to mediate access to a shared communication medium – in this case, radio signals propagating through space
- 802.11 supports additional features
  - e.g., power management and security mechanisms
  - The 802.11 standard has been updated many times to add features and bandwidth

IEEE 802.11

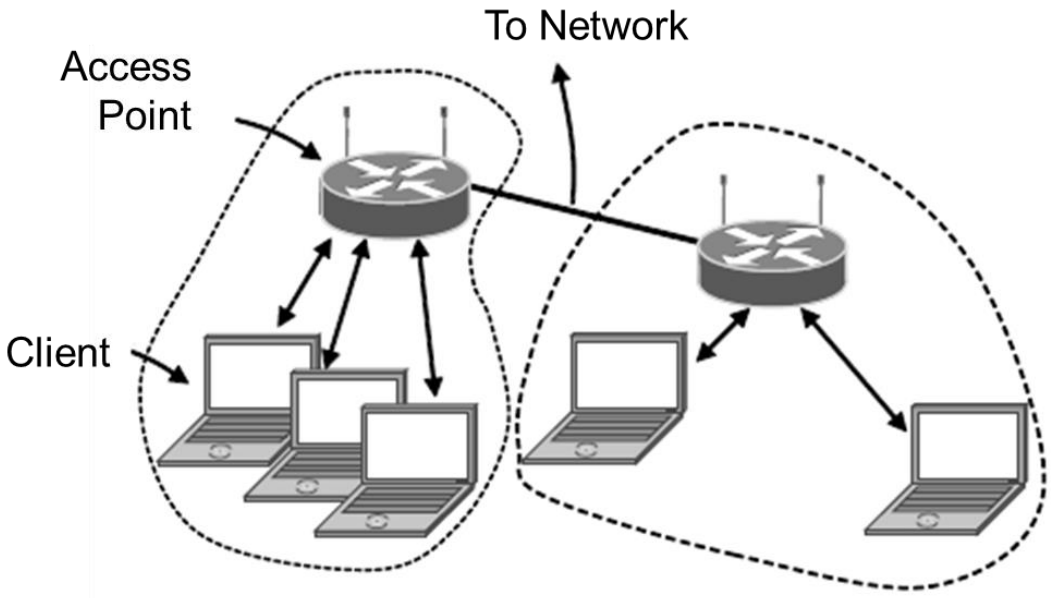
Then new physical layer standards were added

- 802.11a runs on a license-exempt 5-GHz band and delivers up to 54 Mbps using OFDM
- 802.11b uses a variant of direct sequence to provide 11 Mbps
- A more recent standard, 802.11g, is backward compatible with 802.11b
- 802.11n can use either 2.4GHz or 5GHz bands, up to 600Mbps
- 802.11ac and newer versions focus on higher bandwidth, often by using other frequency bands

802.11 Architecture/Protocol Stack

Wireless clients connect to a wired AP (Access Point)

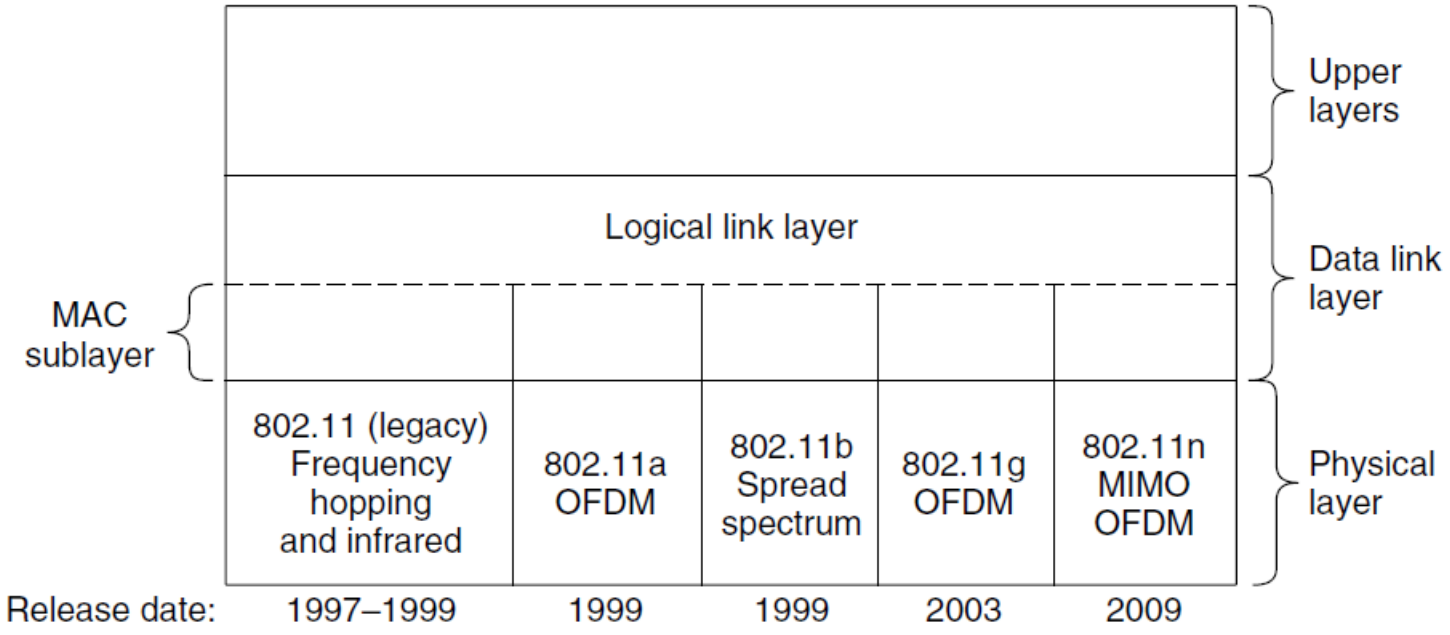
– There is also an *ad-hoc* (i.e., as needed) for node-to-node connections with no Access Point



802.11 Architecture/Protocol Stack

Medium Access Control interfaces different physical layers, depending on the devices

- 802.11 nodes must be able to support different protocol versions as the standards have evolved



IEEE 802.11 – Frame Format

There is a standard frame format for 802.11:

- The Control field contains parameters and options, many of which depend on the type of frame
- Some fields are optional, based on the type of frame
- Address fields are 48 bits
- Besides Address 1 (receiver) and Address 2 (source), Address 3 specifies the destination past the AP
- The payload can contain up to 2304 bytes of data
- After the payload, a 32-bit CRC checks for errors

Wireless LAN Protocols

Wireless LANs encounter unique complications, when compared to wired networks

Due to limitations in radio range, nodes may have different coverage regions

- This can lead to *hidden* and *exposed* nodes

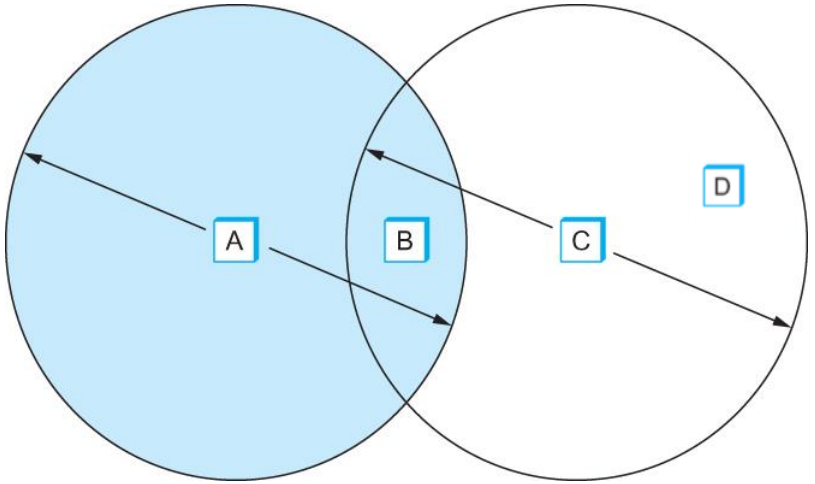
Radio-based nodes can't detect collisions (i.e., *sense*) while they are transmitting

- Thus, collisions can continue for a longer time
- This makes collisions expensive and it is clearly important to find a way to avoid them

IEEE 802.11 – Hidden Node Problem

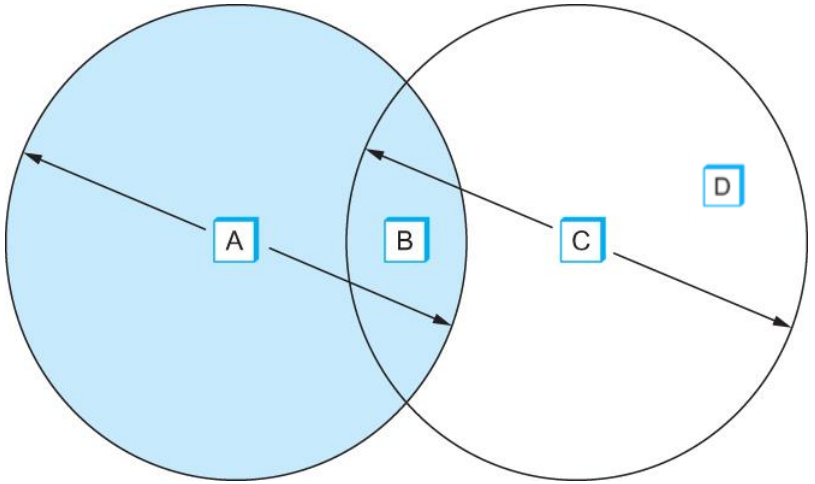
- Consider the situation in the following figure where each of four nodes is able to send and receive signals that reach just the nodes to its immediate left and right
  - For example, *B* can exchange frames with *A* and *C*, but it cannot reach *D*
  - Also, *C* can reach

    B and *D* but not *A*



IEEE 802.11 – Hidden Node Problem

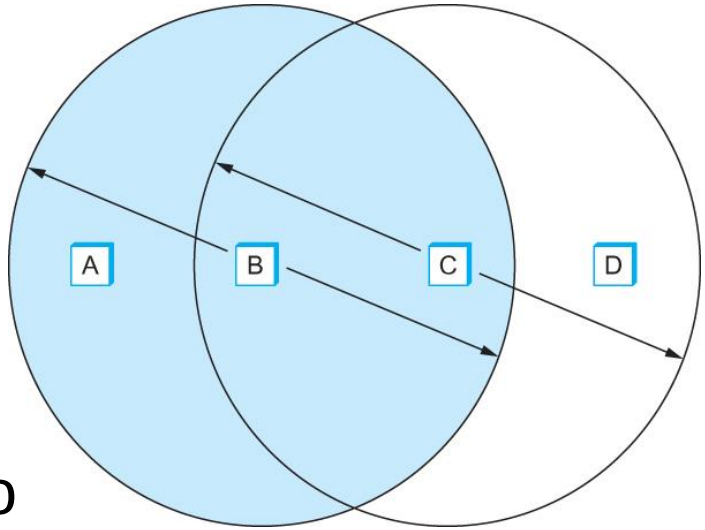
- Suppose both *A* and *C* want to communicate with *B* and so they each send it a frame.
  - Both *A* and *C* are unaware of each other since their signals do not carry that far
  - These two frames will collide with each other at *B*
    - But unlike an Ethernet, neither *A* nor *C* is aware of this collision
- Both *A* and *C* are *hidden nodes* with respect to each other



IEEE 802.11 – Exposed Node Problem

The *exposed node* problem can also occur

- Suppose *B* is sending to *A*.
  - Node *C* is aware of this communication because it hears *B*'s transmission.
- But, it would be a mistake for *C* to conclude that it cannot transmit to anyone just because it can hear *B*'s transmission.
- Suppose *C* wants to transmit to node *D*.
- This is also not a problem since *C*'s transmission to *D* will not interfere with *A*'s ability to receive from *B*.



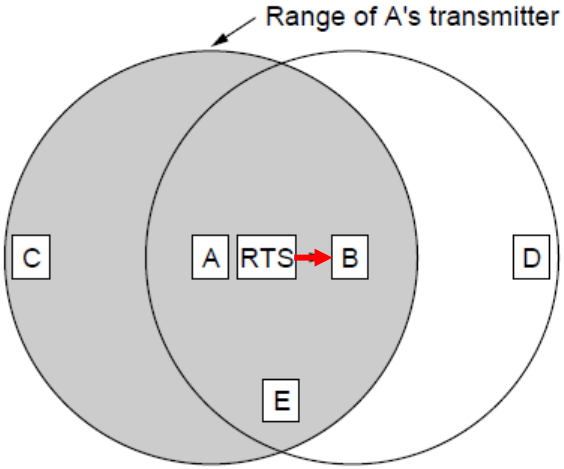
IEEE 802.11 – Collision Avoidance

- 802.11 addresses these two problems with an algorithm called Multiple Access with Collision Avoidance (MACA).
  - Sender and receiver exchange control frames with each other before the sender transmits any data.
    - All nearby nodes know that a transmission is about to begin
  - Sender transmits a *Request to Send* (RTS) frame to the receiver.
    - The RTS frame includes a field that indicates how long the sender wants to hold the medium
      - Length of the data frame to be transmitted
  - Receiver replies with a *Clear to Send* (CTS) frame
    - This frame echoes this length field back to the sender

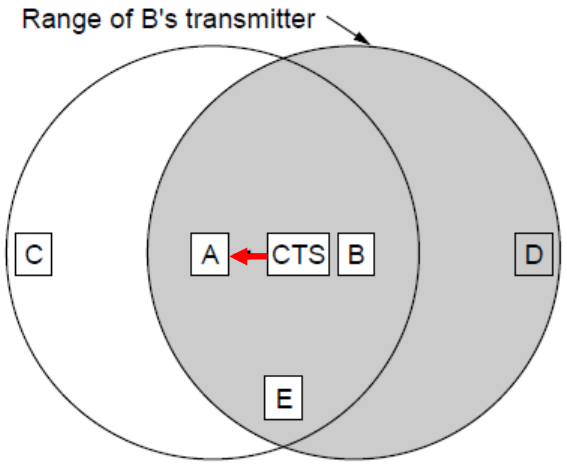
IEEE 802.11 – Collision Avoidance

MACA protocol for node *A* to send to node *B*:

- Node *A* sends RTS to *B*
- Node *B* replies with CTS and node *A* can now safely transmit data to Node *B*



A sends RTS to B,
C & E receive A's RTS
and wait for the CTS

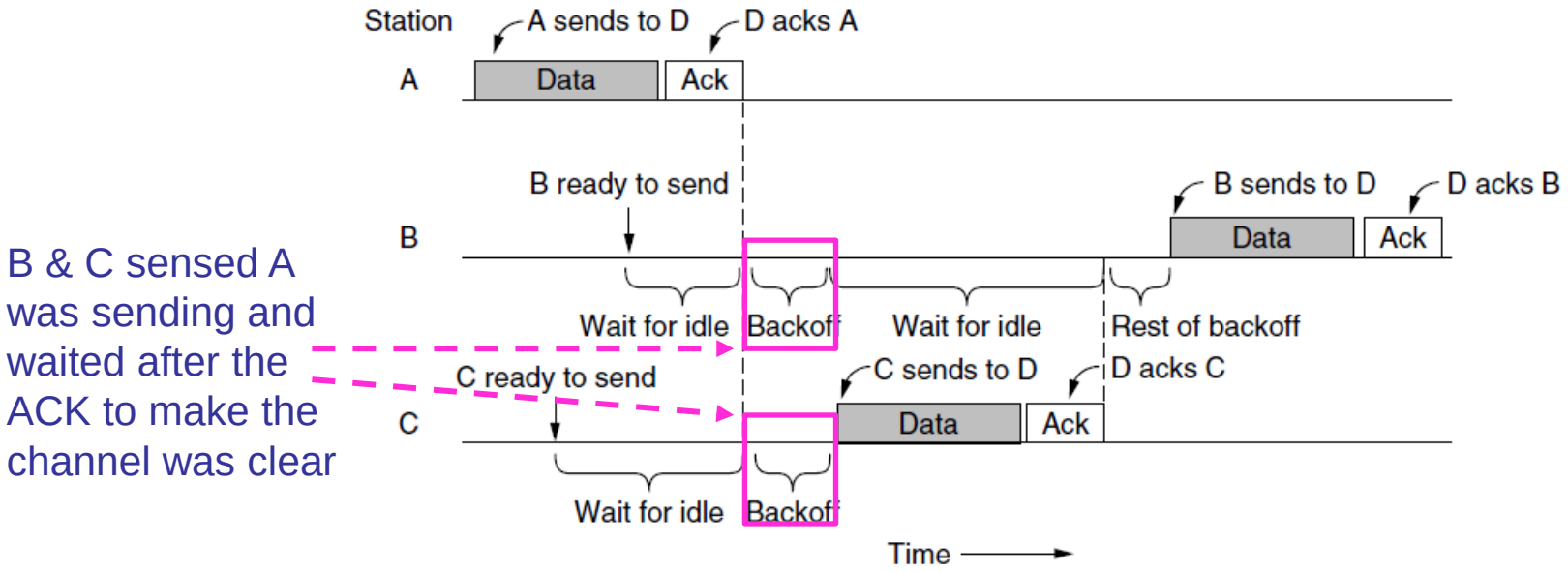


B replies with CTS
D & E receive B's CTS
and wait for the end

802.11 CSMA/CA

To avoid collisions, CSMA/CA can insert *backoff slots* to provide gaps between frames

An ACK is sent if the frame is received, but if no ACK is received the frame will be resent



Bluetooth

- Very short range communication between mobile phones, PDAs, notebook computers and other personal or peripheral devices
  - Operates in the license-exempt band at 2.4 GHz
  - Has a range of 10 m to 100m with longer ranges for newer versions of the protocol
  - Versions run from 1.0 to (currently) 5.2
- Communication devices typically are associated with one individual or group
  - May be categorized as Personal Area Network (PAN)

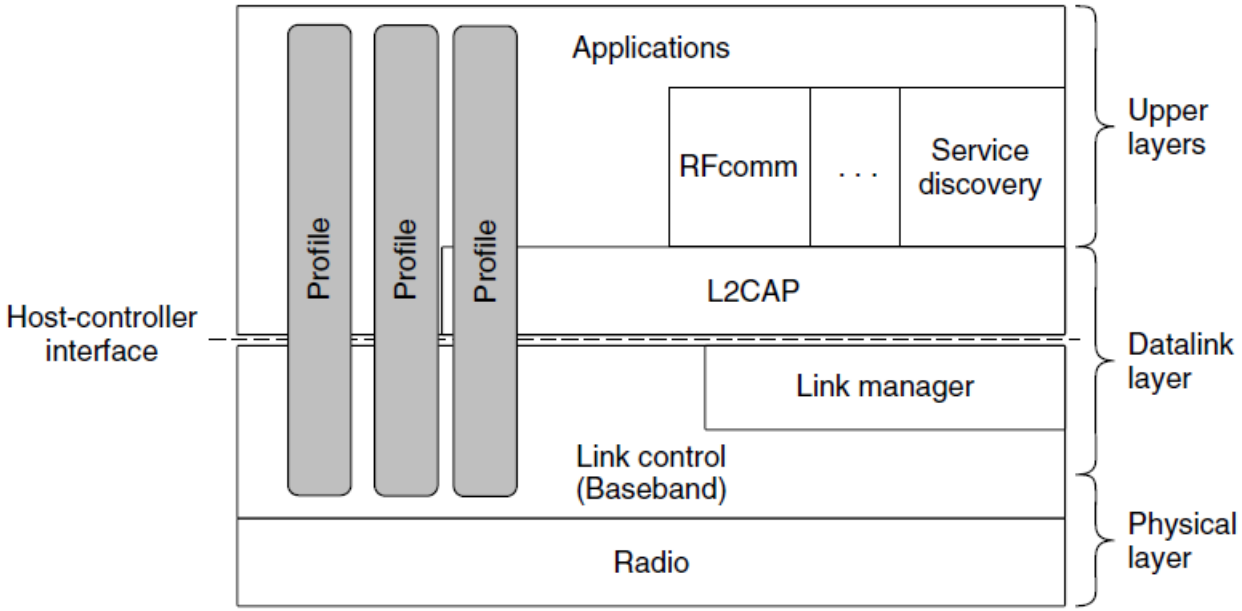
Bluetooth

- Originally specified by IEEE 802.15, now by an industry consortium called the Bluetooth Special Interest Group
- It specifies an entire suite of protocols, going beyond the link layer to define application protocols, which it calls *profiles*, for a range of applications
  - One profile gives a mobile computer access to a wired LAN
  - Another is a profile for synchronizing a PDA with personal computer, etc.
- The basic network configuration is called a *piconet*
  - Consists of a master device and up to seven connected devices
  - All communication is between the master and other devices
  - Devices can be *parked*: set to an inactive, low-power state
  - Two piconets can be bridged into a *scatternet*

Bluetooth Applications / Protocol Stack

Profiles specify protocols for a given application

– Can have up to 25 profiles for devices like headset, streaming audio, remote control, intercom, personal area network, etc.



Bluetooth Radio / Link Layers

Radio layer:

- Uses adaptive frequency hopping in 2.4 GHz band

Link layer:

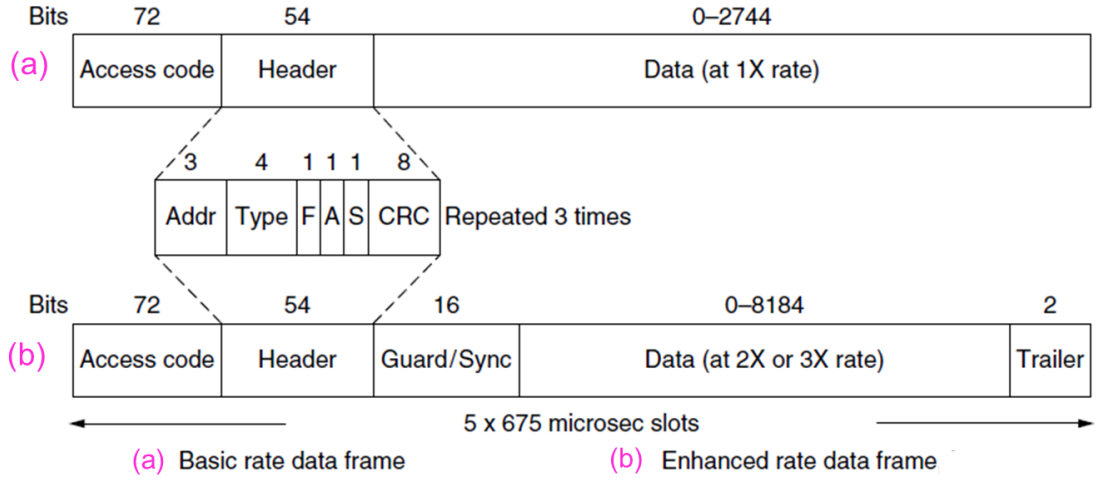
- TDM with timeslots for each device
- Synchronous Connection-Oriented link is used for real-time data and has a fixed slot in each direction
- Asynchronous Connection-Less link is used for packet-switched data with no fixed slots allocated
  - best-effort delivery: packets may be lost or delayed
- Links undergo pairing (user confirms with passkey or PIN) to authorize them before use

Bluetooth Frames

Time slots are fixed size, enhanced data rate just puts more data in the frame, reducing frame overhead

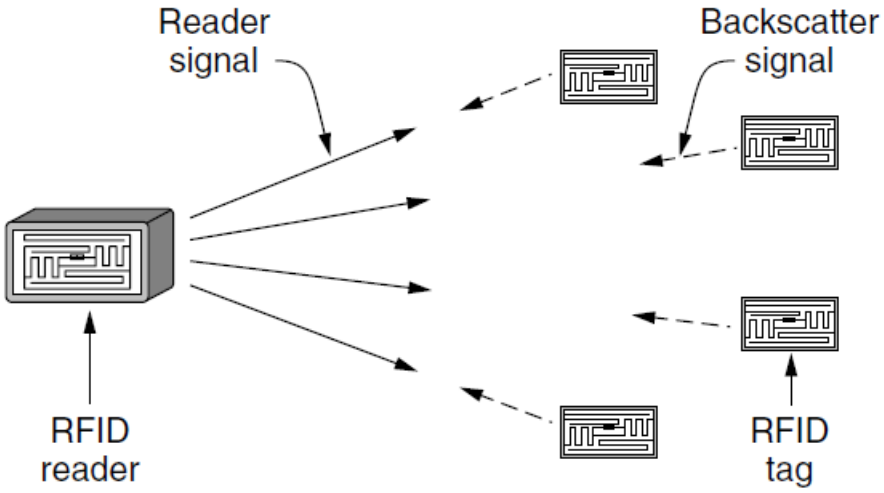
The header is actually repeated 3 times per frame

- With only 8 devices, addresses are 3 bits in length
- Flow control pauses sends when receiver is busy (F bit)
- Acknowledgements can be piggybacked (A bit)
- Uses a stop-and-wait protocol with 1-bit synchronization (S bit)



Radio Frequency Identification (RFID)

- Passive identification mechanism, widely used
- RFID reader transmits a signal that powers the tags, tags reply with a *backscatter* signal
- These slides describe the Electronic Product Code (EPC) version of RFID



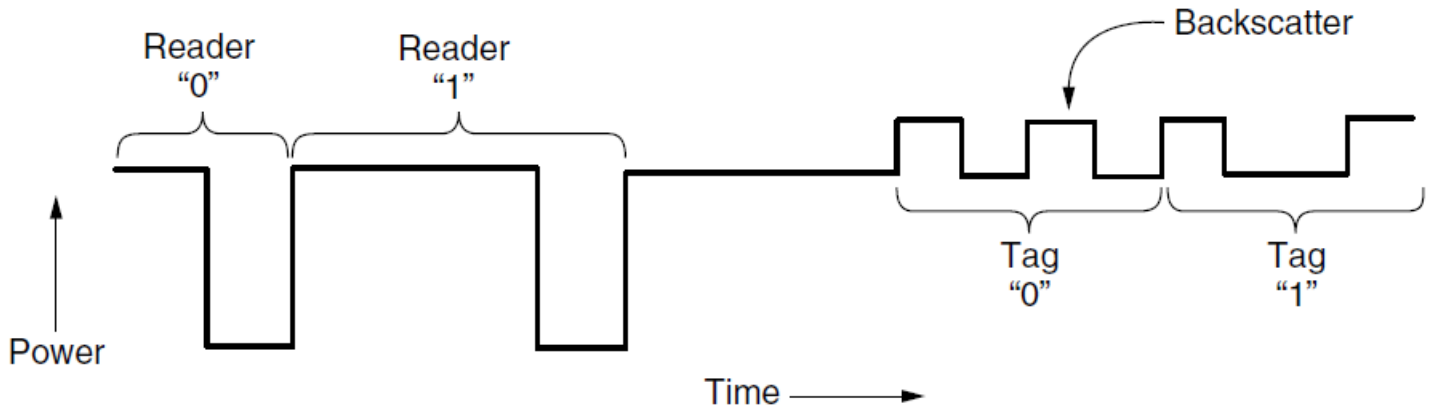
RFID (EPC) Gen 2 Physical Layer

The link is half-duplex with Amplitude Shift Keying

Reader is always transmitting a fixed carrier signal to power the tags and sends 0 or 1 to trigger a tag's reply

– Bits are transmitted in bursts of different lengths, for example, a 1 bit is longer than a 0 bit

Tags backscatter the reader's carrier signal and modulate it in pulses to send 0's and 1's



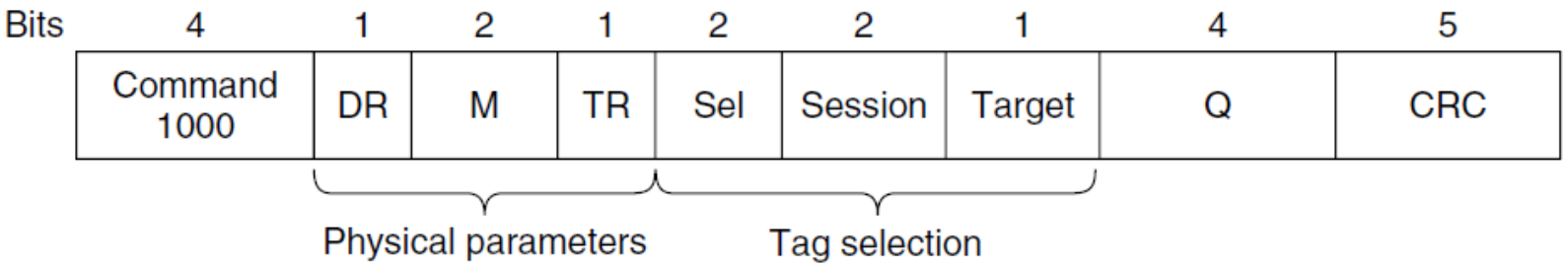
Gen 2 Frames

Reader frame formats vary depending on type

- Query frame has parameters and error detection
- Parameters indicate which tag, which slots to use for the reply, response rate, etc.

Tag responses are simply data

- Reader sets timing and knows the expected format



Query message

Gen 2 Tag Identification Layer

- Reader sends tag queries in slots it controls
- Tags reply with a random number in a random slot (they may collide)
- If no collision, reader then sends an ACK to ask the tag for its identifier
- This gives that tag the slot and it replies with its ID
- This process continues until all tags are ID'd