CSE 3231 / CSE 5231
Computer Networks

Chapter 4
Medium Access Sub-Layer
part 1

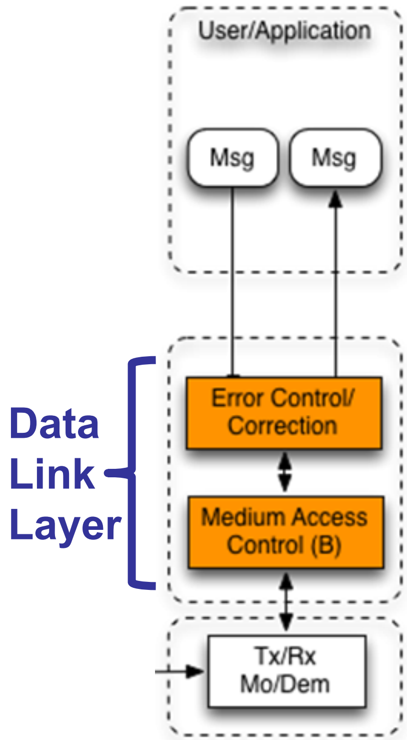
William Allen, PhD

Fall 2021

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 approach performs poorly with *bursty* traffic (frequently varies in bandwidth needed)

- 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

- More efficient than with fixed allocations

Example: Frequency Division Utilization

Five 100 MhZ channels can be shared by nodes

Node 1	1000 to 1099 MHz	90% utilization
Node 2	1100 to 1199 MHz	30% utilization
Node 3	1200 to 1299 MHz	80% utilization
Node 4	1300 to 1399 MHz	40% utilization
Node 5	1400 to 1499 MHz	60% utilization

Total available bandwidth: 500 Mhz
Total utilized bandwidth: 300 Mhz
Utilization: 300Mhz / 500 Mhz = 60%

Waiting for an available channel

Node 6
Node 7
Node 8
Node 9

While there is enough un-used bandwidth for 2 of the waiting nodes, it cannot be allocated because allocations are a fixed 100 Mhz

Example: Time Division Utilization

10 ms slots currently allocated for nodes
(number below shows how much of the time slot each node used)

node 1	node 2	node 3	node 4	node 5	node 1	node 2	node 3	node 4	node 5
10 ms	3 ms	8 ms	4 ms	6 ms	0 ms	5 ms	4 ms	10 ms	7 ms

This slot was allocated to node 1, but not used

Total available time: 100 ms
Total time used: 57 ms
Utilization: 57 ms / 100 ms = 57%

Waiting for an available channel

Node 6
Node 7
Node 8
Node 9

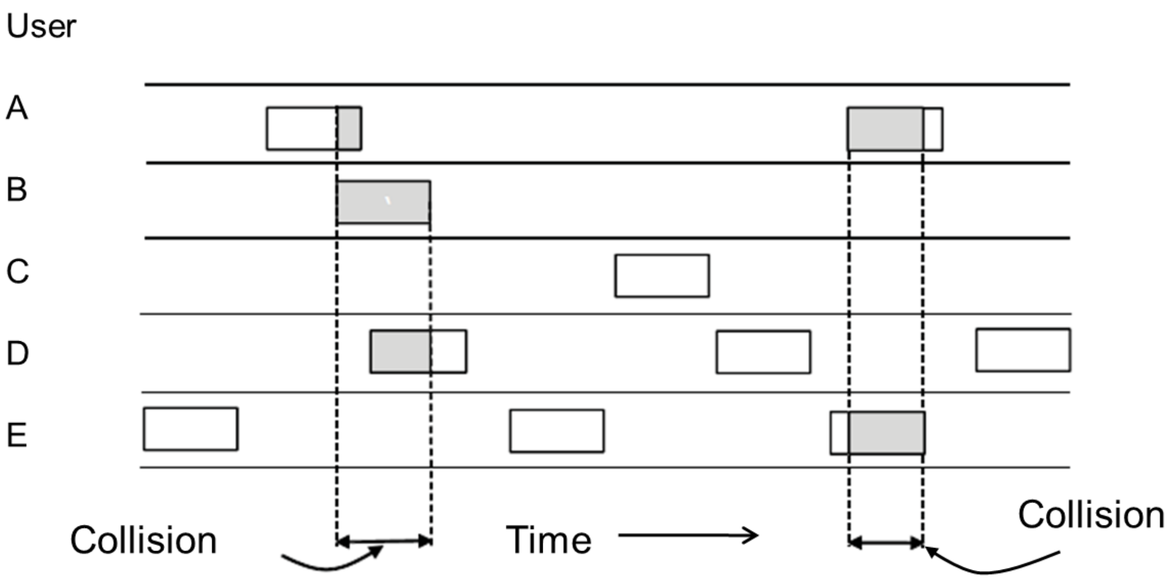
While there is enough un-used time to give each of the 4 waiting nodes 10 ms, it was not allocated.

Increasing the number of slots would also increase the delay between transmissions.

ALOHA

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

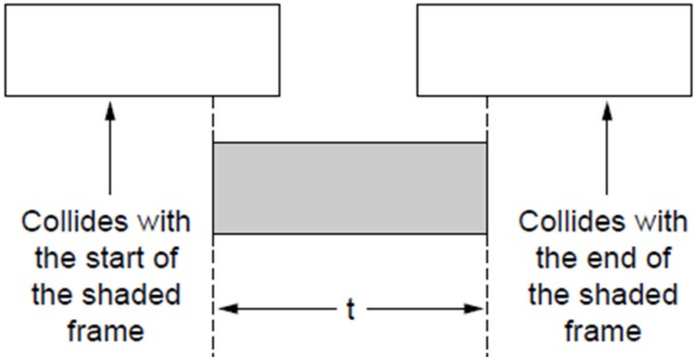
- If collisions occur, retry after a random wait time
- Under a low load this can be moderately efficient



ALOHA

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

– this can potentially impact two other user’s frames

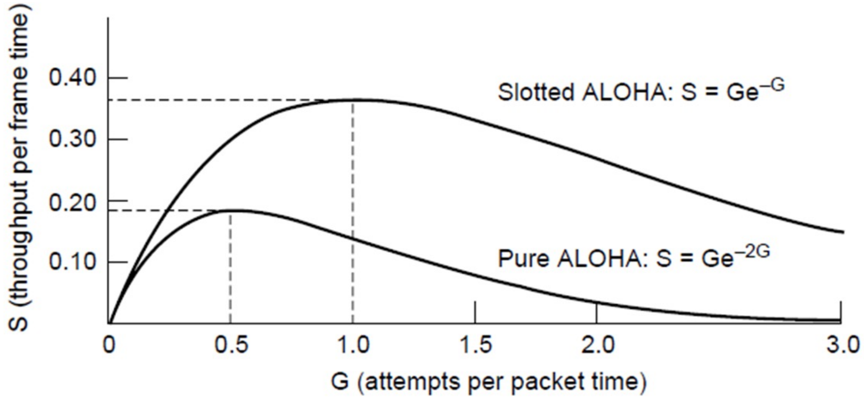


The solution was to synchronize senders into regular time slots to reduce collisions, this is called *Slotted Aloha*

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

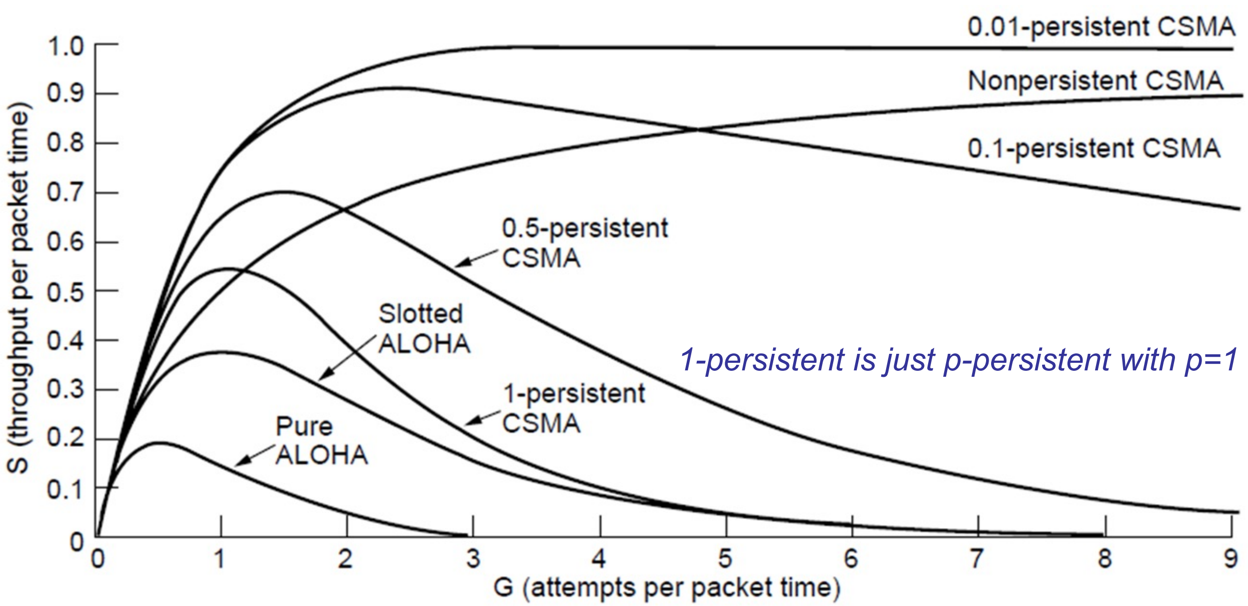


Carrier Sense Multiple Access (CSMA)

- 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) always sends another frame as soon as the channel is idle
  - *nonpersistent* CSMA (less greedy approach) if busy, always waits a random period before trying again
  - *p-persistent* CSMA (moderately greedy) if busy, tries again with probability *p*, i.e., between the other two

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

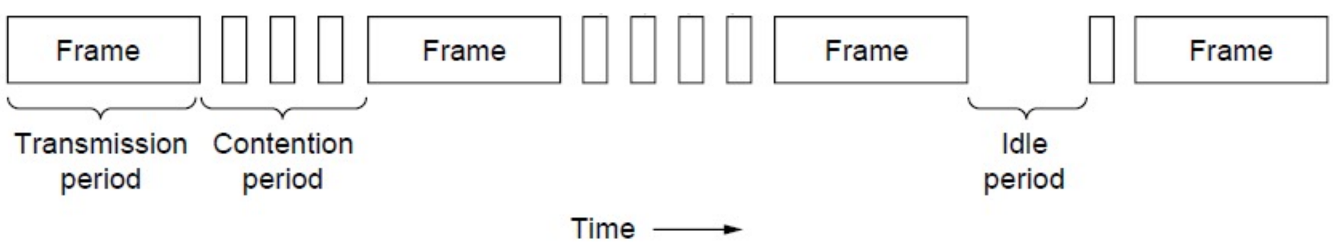
Adding Collision Detection (CD) to CSMA can detect collisions and end transmission early

- 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

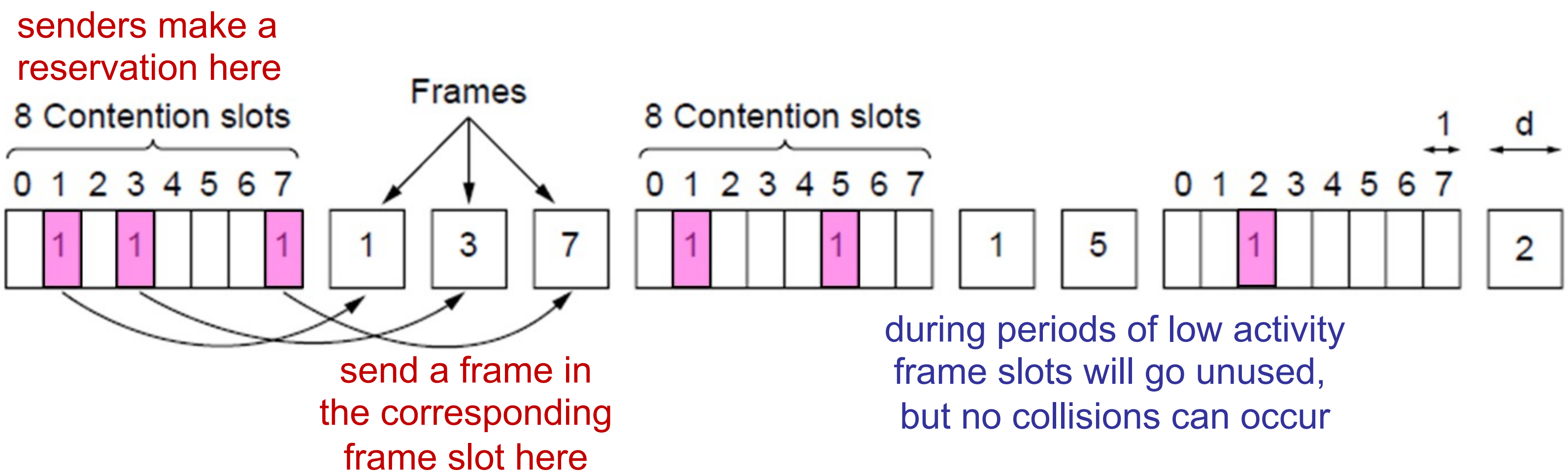
- Just because one node does not sense traffic on the network does not mean that another node that is farther away has not *already started* sending
- the *contention period* is that overlap in time



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

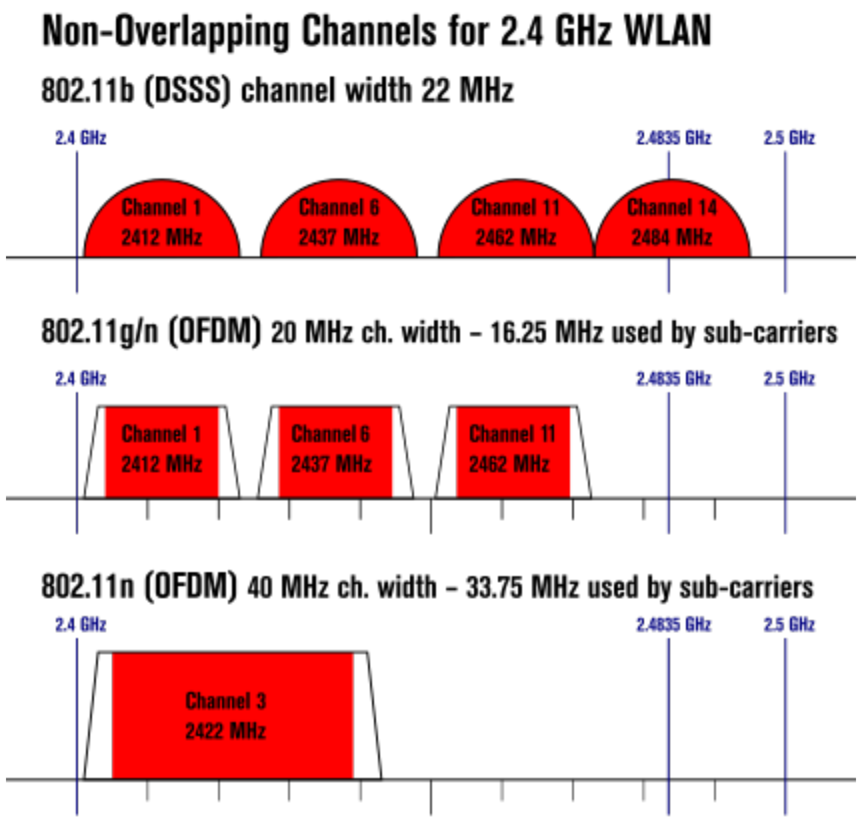
Wireless Links

- Exclusive use of a particular frequency in a particular geographic area may be allocated to a government agency or a specific corporation
  - Allocations are determined by government agencies such as the Federal Communications Commission
- Specific bands (frequency ranges) are allocated:
  - Some bands are reserved for government use
  - Other bands are used for AM radio, FM radio, televisions, satellite communications, and cell phones
  - Specific frequencies may be allocated to individual organizations for use within a geographical area.


UNITED
STATES
FREQUENCY
ALLOCATIONS
THE RADIO SPECTRUM
RADIO SERVICES COLOR LEGEND
AERONAUTICAL MOBILE
AERONAUTICAL MOBILE SATELLITE
AERONAUTICAL RADIONAVIGATION
AMATEUR
AMATEUR SATELLITE
BROADCASTING
BROADCASTING SATELLITE
EARTH EXPLORATION SATELLITE
FIXED
FIXED SATELLITE
INTER-SATELLITE
LAND MOBILE
LAND MOBILE SATELLITE
MARITIME MOBILE
MARITIME MOBILE SATELLITE
MARITIME RADIONAVIGATION
METEOROLOGICAL
METEOROLOGICAL SATELLITE
MOBILE
MOBILE SATELLITE
RADIO ASTRONOMY
RADIODETERMINATION SATELLITE
RADIOLOCATION
RADIOLOCATION SATELLITE
RADIONAVIGATION
RADIONAVIGATION SATELLITE
SPACE OPERATION
SPACE RESEARCH
STANDARD FREQUENCY AND TIME SIGNAL
STANDARD FREQUENCY AND TIME SIGNAL SATELLITE
ACTIVITY CODE
FEDERAL EXCLUSIVE
FEDERAL/NON-FEDERAL SHARED
NON-FEDERAL EXCLUSIVE
ALLOCATION USAGE DESIGNATION
SERVICE
EXAMPLE
DESCRIPTION
Primary
FIXED
Capital Letters
Secondary
Mobile
1st Capital with lower case letters
U.S. DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Office of Spectrum Management
JANUARY 2016
0 kHz
300 kHz
NOT ALLOCATED
RADIONAVIGATION
MARITIME MOBILE
FIXED
RADIONAVIGATION
AERONAUTICAL RADIONAVIGATION
300 kHz
3 MHz
3MHz
30 MHz
30 MHz
300 MHz
300 MHz
3 GHz
3 GHz
30 GHz
30GHz
300 GHz

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, 4G, 5G, etc.)

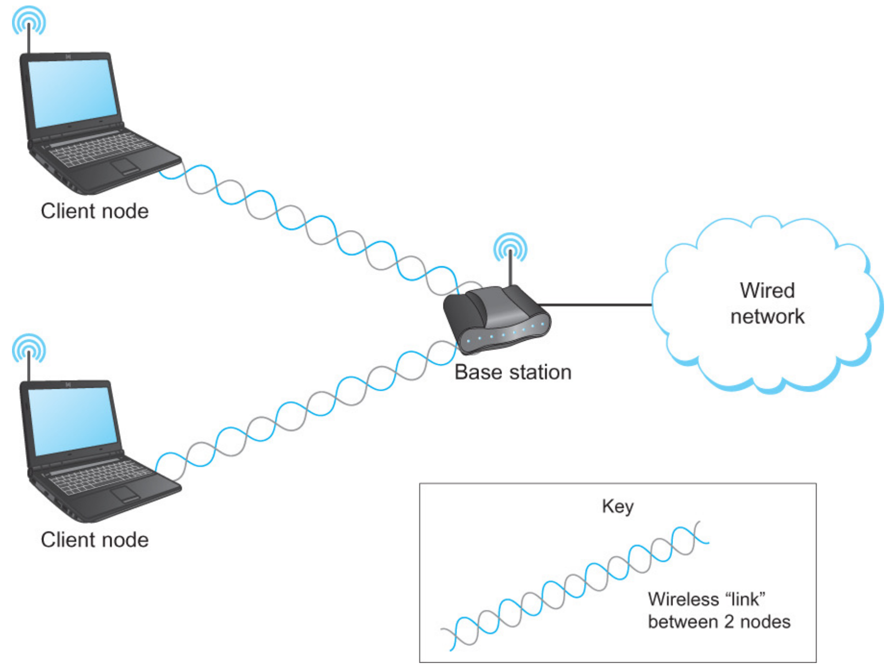
Wireless Links

	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

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



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

- Original 802.11 standard defined two radio-based physical layer methods
  - One using the frequency hopping
    - Over 79 1-MHz-wide frequency bandwidths
  - Second version using direct sequence
    - Using 11-bit chipping sequence
  - Both versions use license-exempt 2.4GHz,
    - provides up to 2Mbps

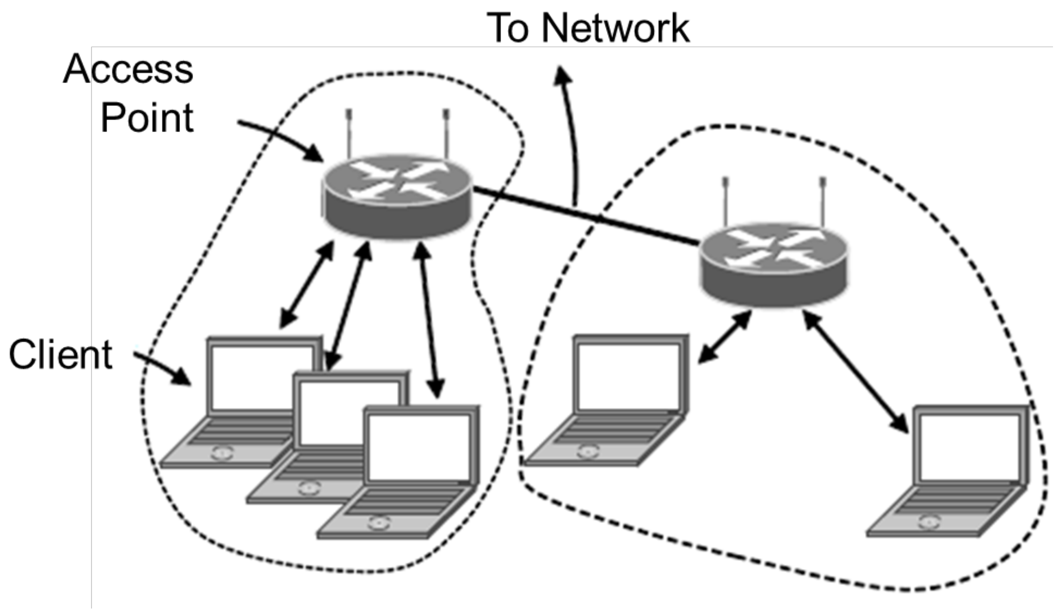
IEEE 802.11

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

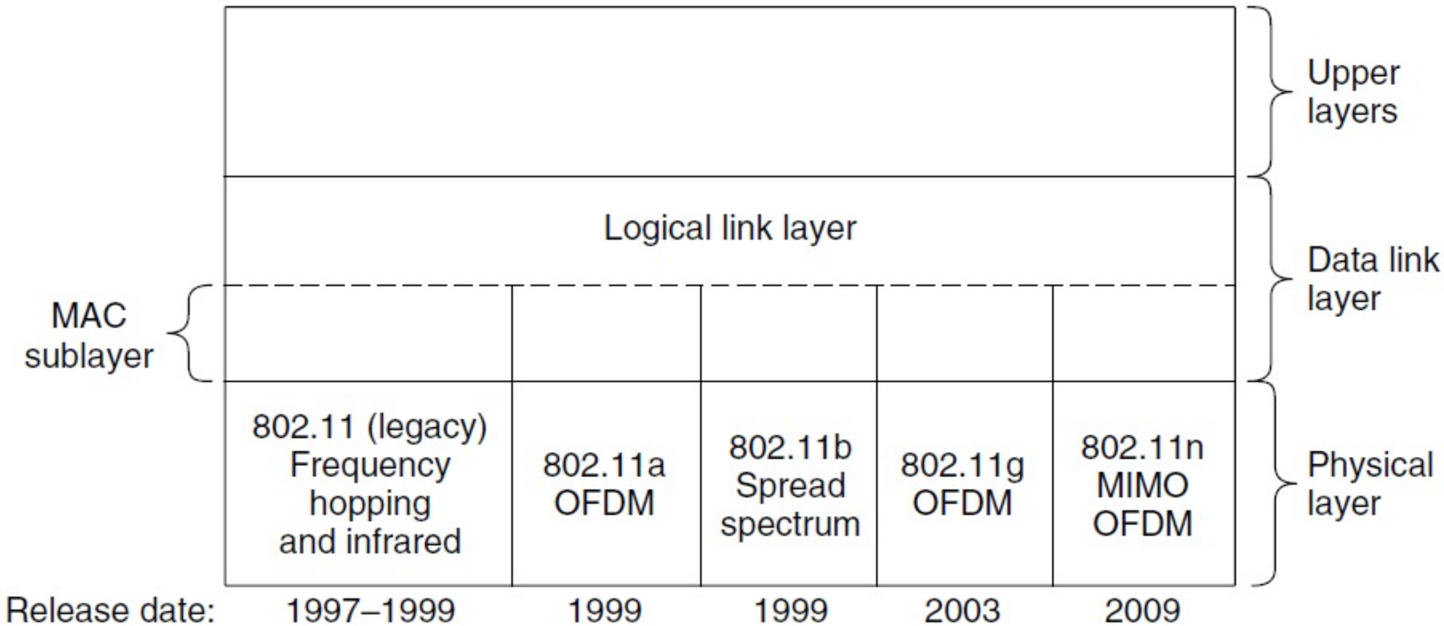
- Wireless clients connect to a wired AP (Access Point)
  - Can also be used *ad-hoc* (i.e., as needed) for node-to-node connections with no Access Point



802.11 Architecture/Protocol Stack

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

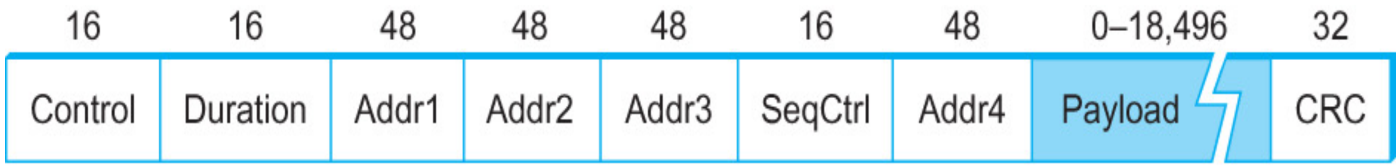
- 802.11 nodes must be able to support different protocol versions as the standards have evolved



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

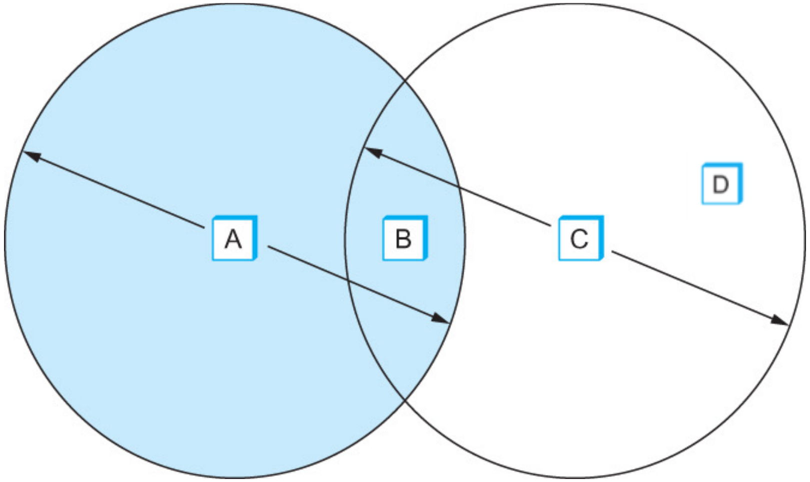


Wireless LAN Protocols

- 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

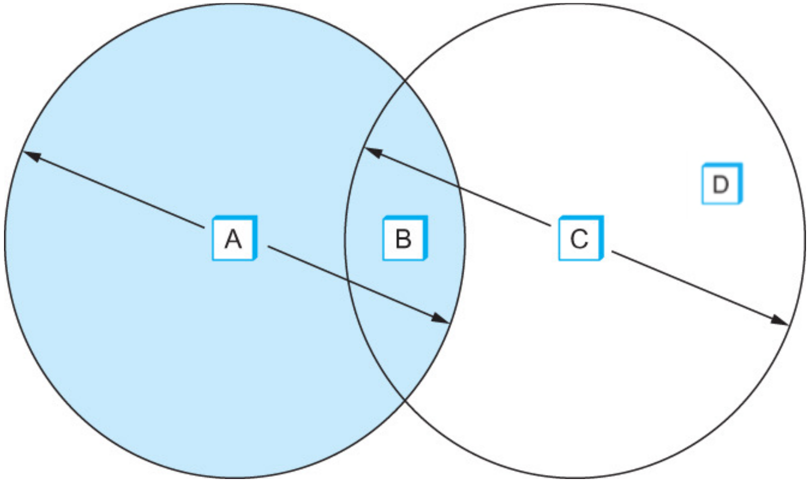
- Consider the situation in the following figure where each of four nodes is able to send and receive signals that reach just the nodes to its immediate left and right
  - For example, *B* can exchange frames with *A* and *C*, but it cannot reach *D*
  - Also, *C* can reach *B* and *D* but not *A*



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

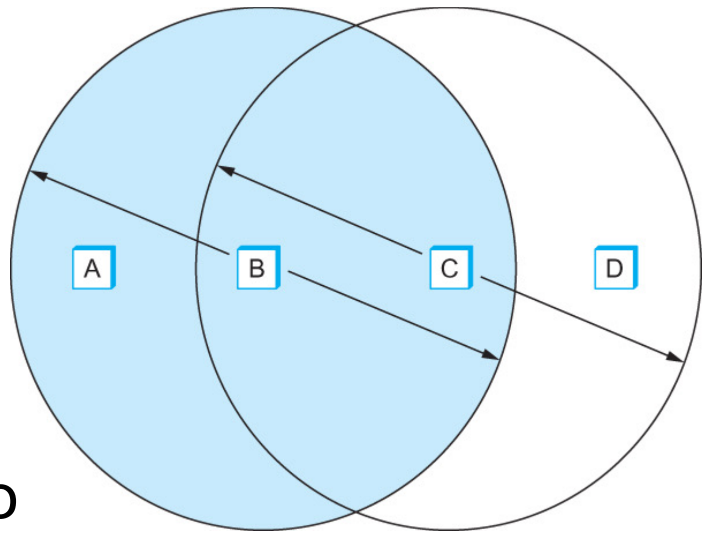
- Both *A* and *C* are *hidden nodes* with respect to each other



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

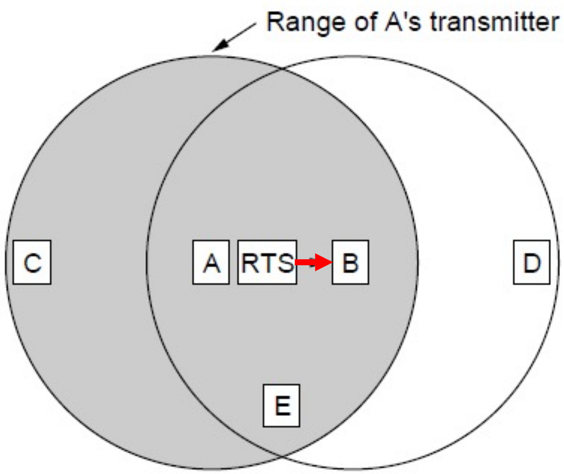
- 802.11 addresses these two problems with an algorithm called Multiple Access with Collision Avoidance (MACA).
  - Sender and receiver exchange control frames with each other before the sender transmits any data.
    - All nearby nodes know that a transmission is about to begin
  - Sender transmits 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

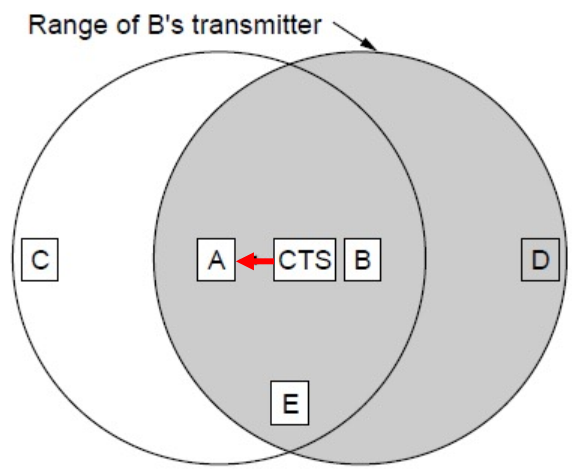
MACA protocol for node *A* to send to node *B*:

– 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



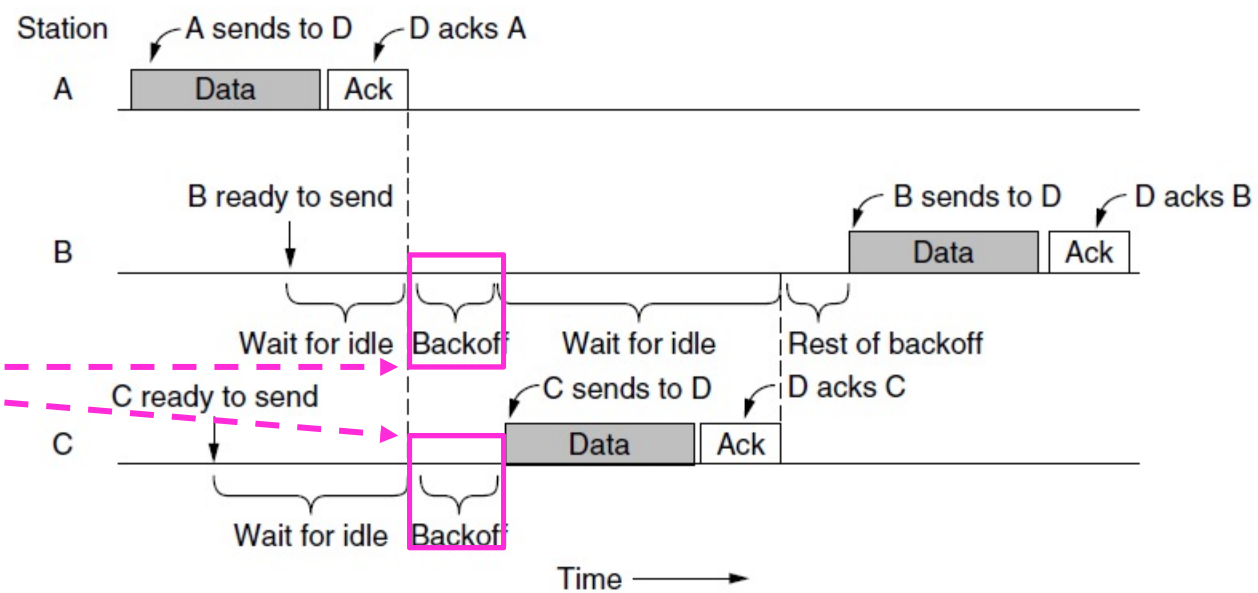
B replies with CTS
D & E receive B's CTS
and wait for the end

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

B & C sensed A was sending and waited after the ACK to make the channel was clear



Frame Format Examples

- Cloudshark - cloud-based version of Wireshark

- Example frames:
  - PPP - frames 1-5 show steps in link configuration
  - Ethernet - frames 6-7 show an exchange of frames
  - WiFi - frames 8-9 show a TCP connection request and also show the protocol layers in TCP/IP

https://www.cloudshark.org/captures/d2e34d5f1c2e