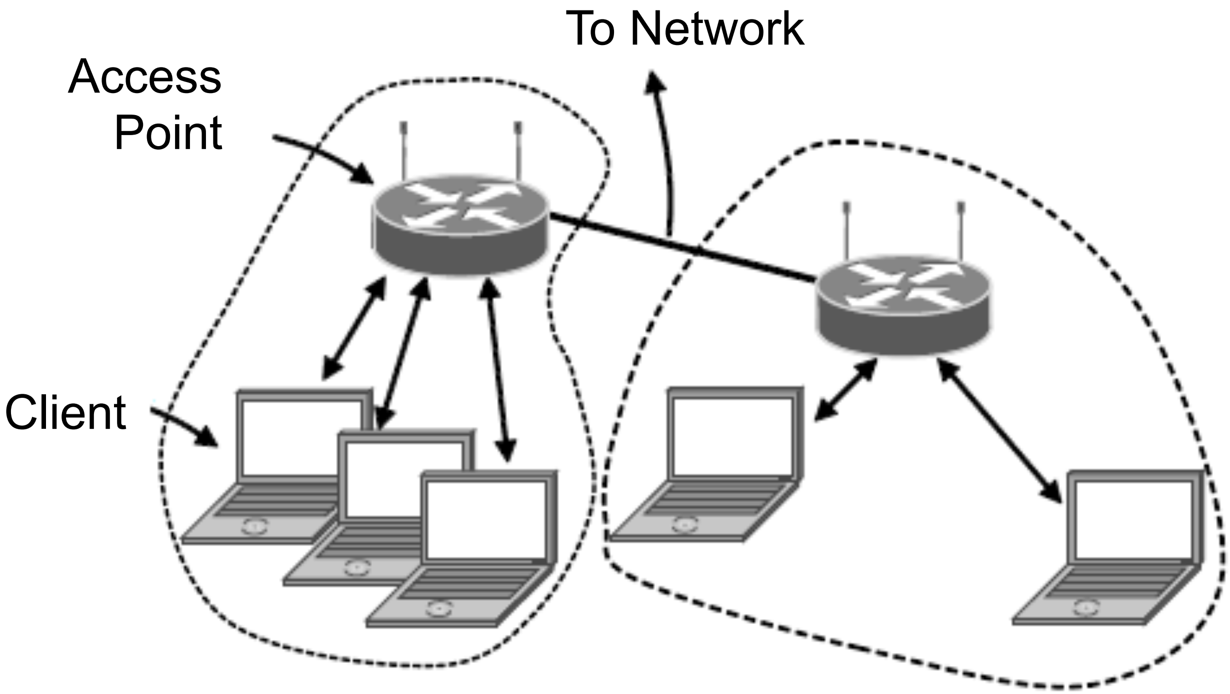
IEEE 802.11 – Wi-Fi

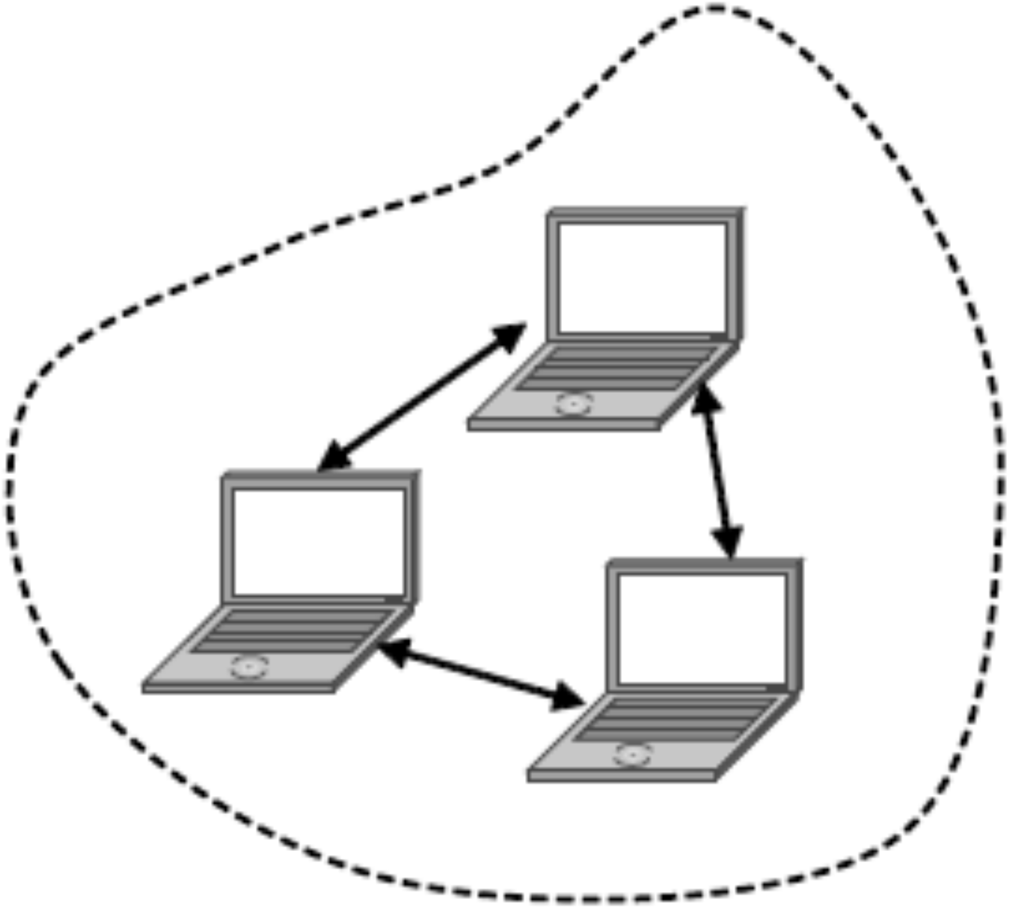
802.11 Architecture

- Wireless clients associate to a wired AP (Access Point)
  - Called infrastructure mode; there is also an ad-hoc mode (see next slide) with no AP, but that is rare.

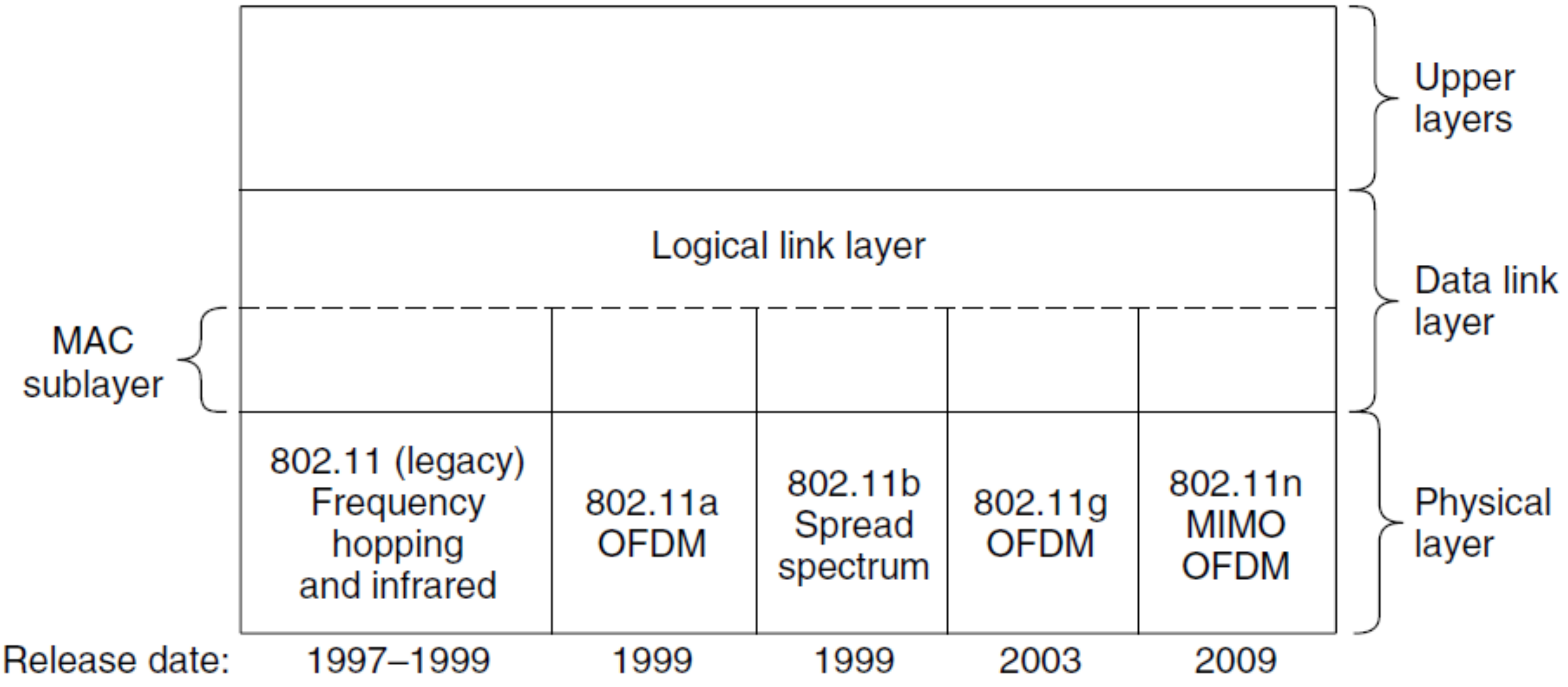


802.11 Architecture

- Ad-hoc mode



802.11 Protocol Stack



Upper layers

Logical link layer

Data link layer

MAC sublayer

802.11 (legacy) Frequency hopping and infrared

802.11a OFDM

802.11b Spread spectrum

802.11g OFDM

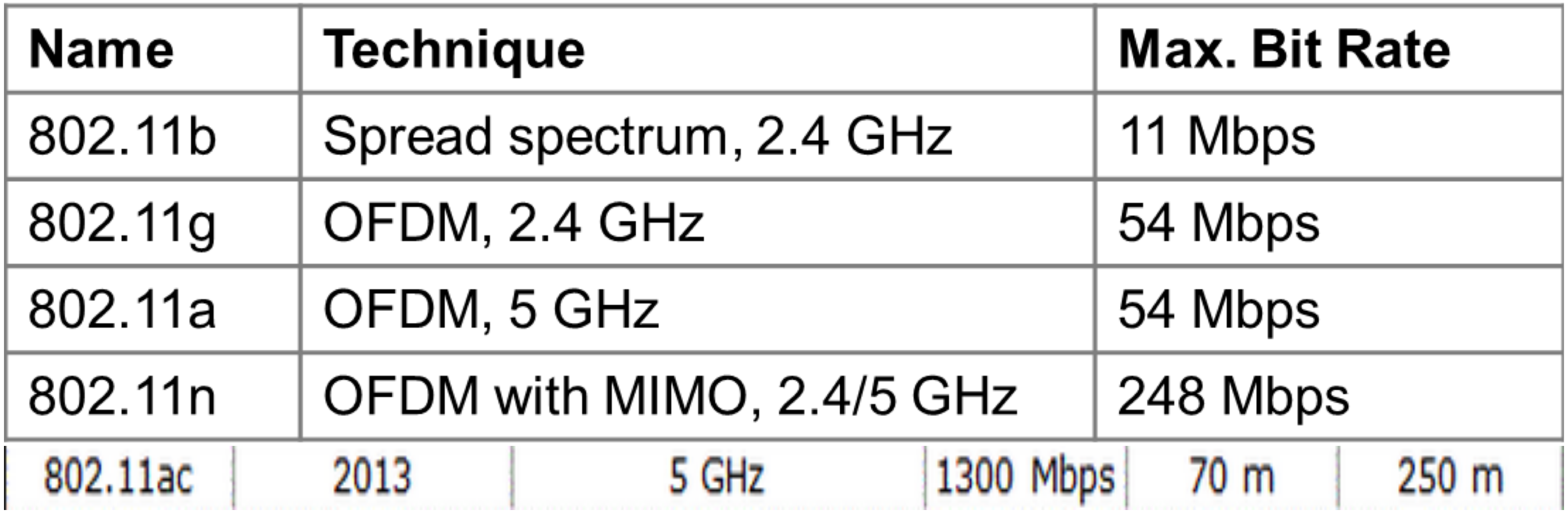
802.11n MIMO OFDM

Physical layer

Release date: 1997–1999 1999 1999 2003 2009

802.11 Physical Layer

- NICs are compatible with multiple physical layers
  E.g., 802.11 a/b/g



Name	Technique	Max. Bit Rate
802.11b	Spread spectrum, 2.4 GHz	11 Mbps
802.11g	OFDM, 2.4 GHz	54 Mbps
802.11a	OFDM, 5 GHz	54 Mbps
802.11n	OFDM with MIMO, 2.4/5 GHz	248 Mbps

802.11ac	2013	5 GHz	1300 Mbps	70 m	250 m

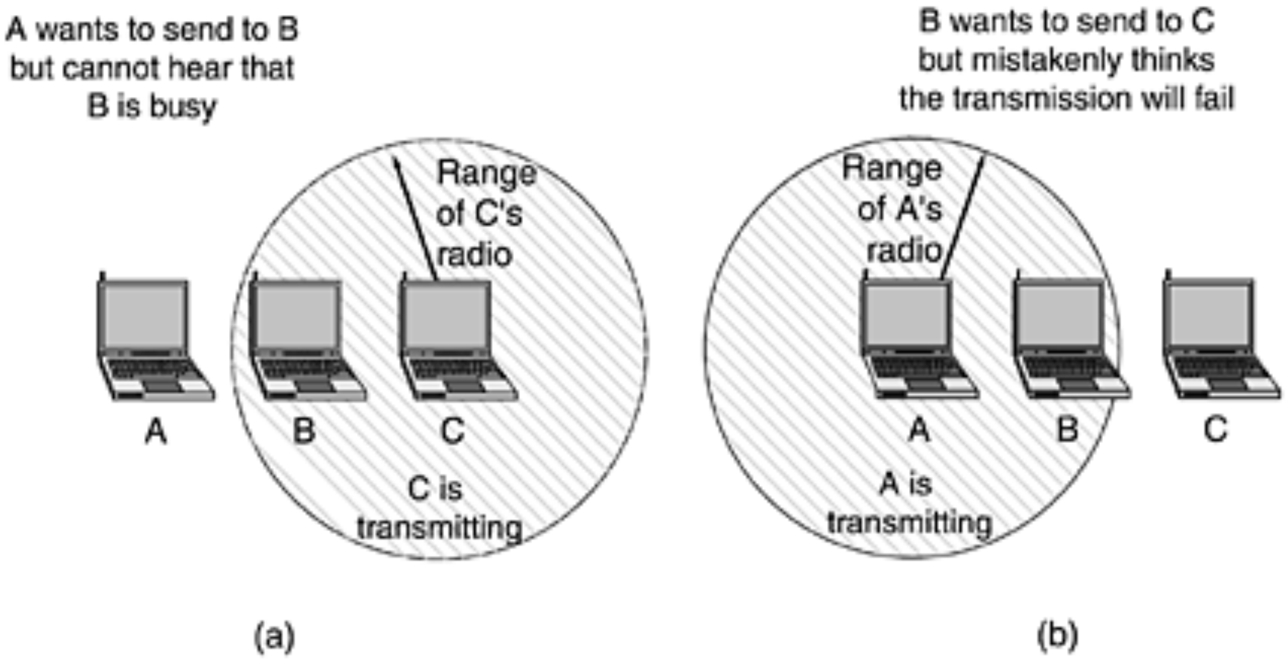
802.11 MAC Sub-layer Protocol

- The 802.11 MAC protocol is different from Ethernet due to the complexity of the wireless environment.

- In 802.3 if media is silent, station transmits a frame. If no noise burst is received within the first 64 bytes (minimum frame size), then the frame will assuredly be delivered. This situation does not hold true for wireless.

(a) Hidden Station Problem and (b) Exposed Station Problem

- Since not all stations are within radio range of each other, transmissions going on in one part of a cell may not be received elsewhere in the same cell.


A wants to send to B but cannot hear that B is busy
Range of C's radio
A
B
C
C is transmitting
(a)
B wants to send to C but mistakenly thinks the transmission will fail
Range of A's radio
A
B
C
A is transmitting
(b)

- To deal with these problems, 802.11 supports two modes of operation: DCF and PCF.

Distributed Coordination Function (DCF) mode

- Does not use any kind of central control (like Ethernet). When DCF is employed, 802.11 uses CSMA/CA (CSMA with Collision Avoidance) as the MAC protocol.

- Both physical channel sensing and virtual channel sensing are used. Two modes are supported by CSMA/CA.

- Mode 1 (CSMA):

1. When a station wants to transmit, it senses the channel. If idle, transmit. It does not sense the channel during transmission; rather it transmits the entire frame, which may be destroyed due to interference at receiver station.
2. If channel is busy, sender waits till channel goes idle and then transmits.
3. If collision occurs, the colliding stations wait a random amount of time, using the Ethernet binary exponential backoff algorithm, and then try again later.

In this case, collision is detected if no ACK is received.

Distributed Coordination Function (DCF)

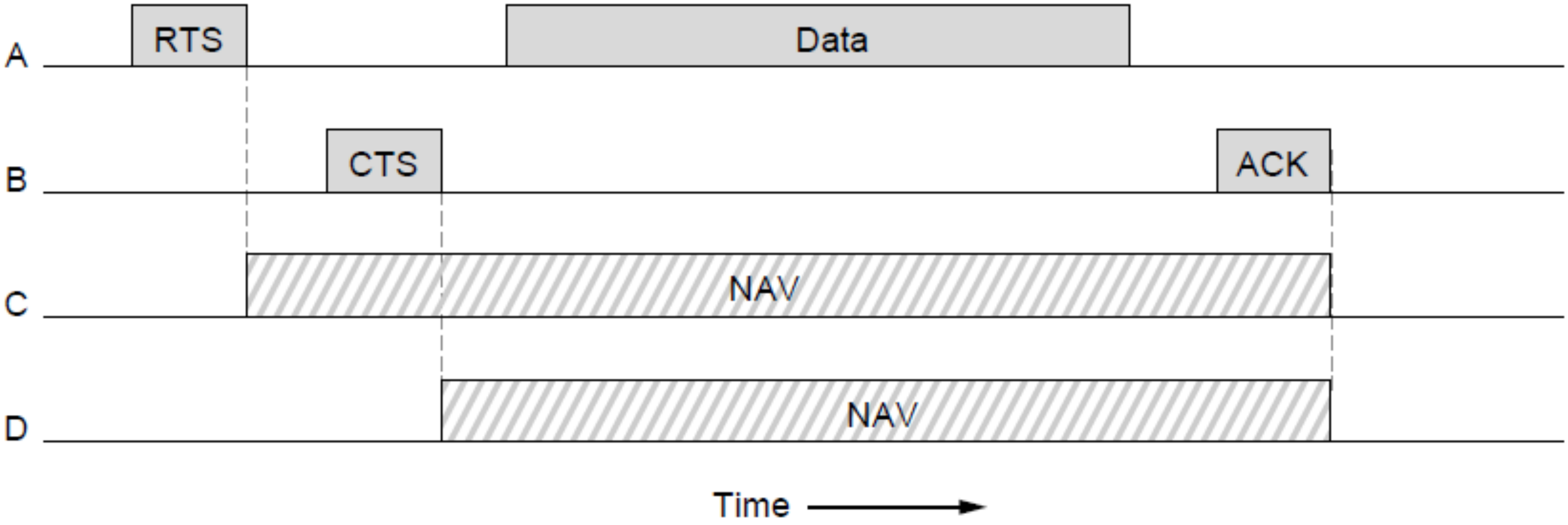
- Mode 2 (CA):

This uses virtual channel sensing as shown in the next slide.

Topology:

A wants to send to *B*. *C* is a station within *A*'s range and *D* is a station within *B*'s range but not within range of *A*.

DCF: Use of Virtual Channel Sensing Using CSMA/CA

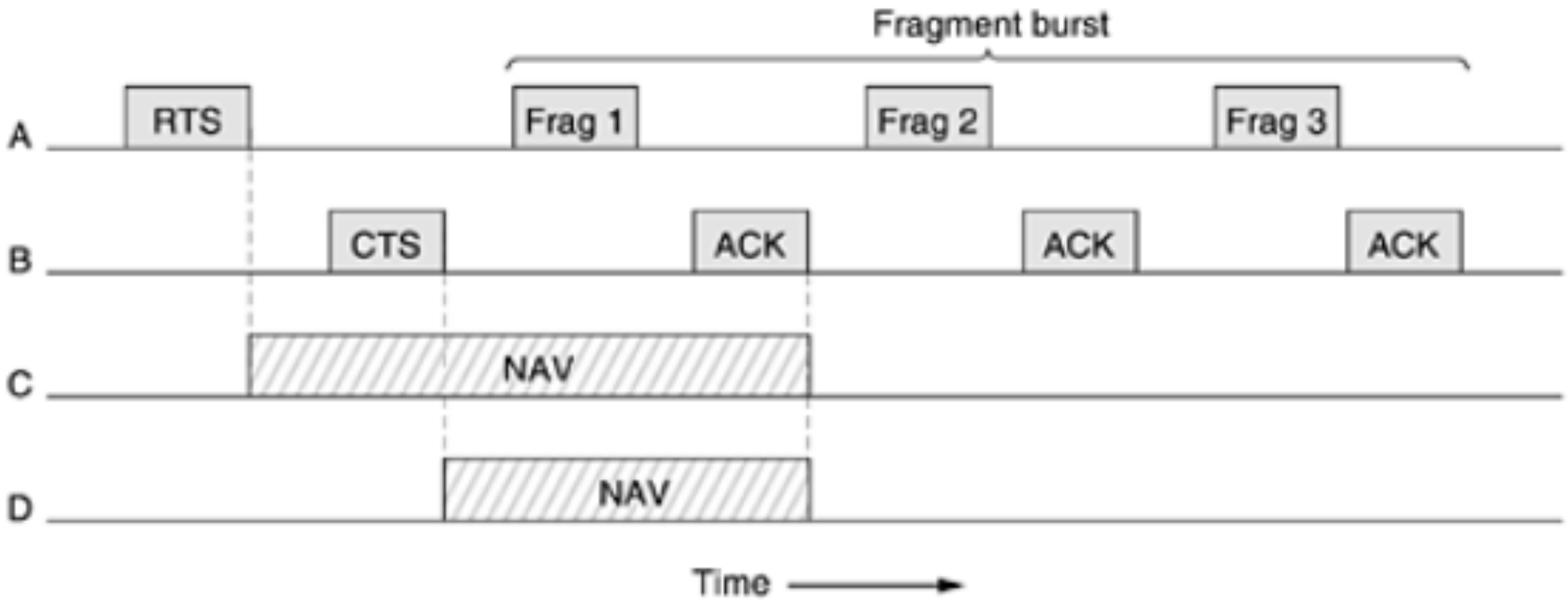


This leads to CSMA/CA.

DCF:
Fragmentation of Frames

- Wireless networks are noisy and unreliable compared to wired networks. So the probability of a frame making it through successfully decreases with frame length (longer the frame, less likely it will get through without errors).

- If a frame is too long, it has very little chance of getting through without damage and would lead to retransmission. To solve this frame of noisy channels, 802.11 allows frames to be fragmented, each with its own checksum.



DCF:
Fragmentation of Frames

- The fragments are individually numbered and ACKed using a stop-and-wait protocol.

- Once the channel has been acquired using RTS and CTS, multiple fragments can be sent in a row. Sequence of fragments is called a *fragment burst*.

- Fragmentation increases the throughput by restricting retransmissions to the bad fragments rather than the entire frame.

- The NAV mechanism keeps other stations quiet only until the next ACK, but another mechanism is used to allow an entire fragment burst to be sent without interference.

- All this is part of the DCF mode. In this mode, there is no central control and stations compete for air time, just as they do with the Ethernet.

Point Coordination Function (PCF) mode

- In this mode the base station polls the other stations, asking if they have any frames to send. Since transmission order is completely controlled by the base station, no collisions ever occur.

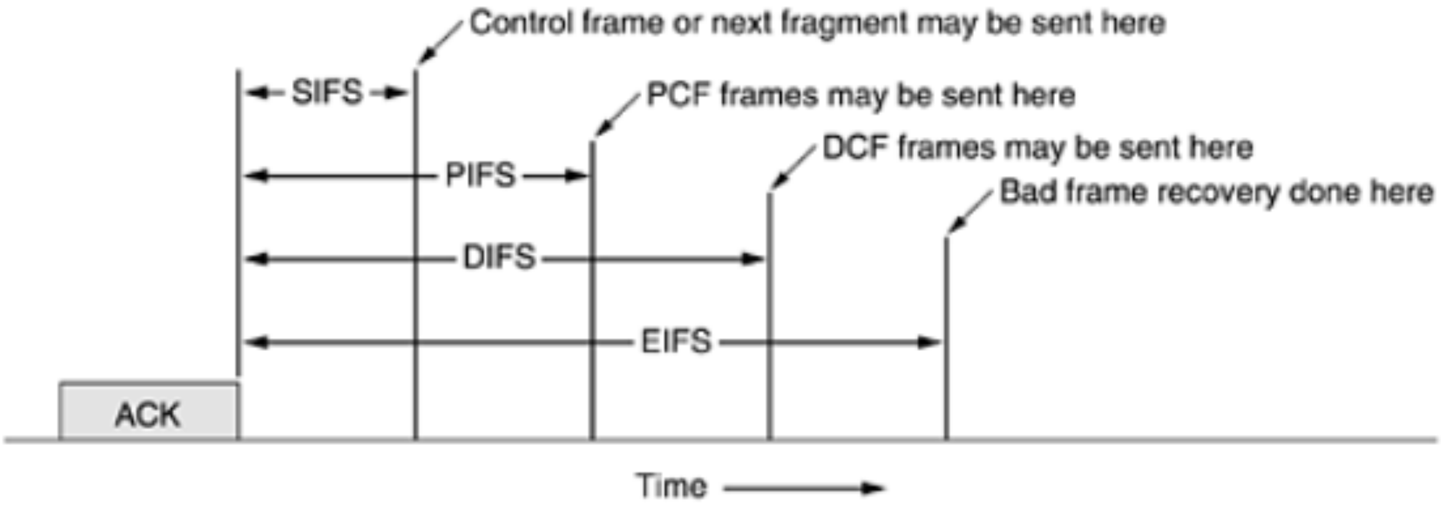
- Base station broadcasts a *beacon frame* periodically. The beacon frame contains system parameters such as hop sequence and dwell time (for FHSS), clock synchronization etc.

- Base station also invites new stations to sign up for polling service. Once a station has signed up for polling service at a certain rate, it is guaranteed a certain fraction of the bandwidth.

Interframe Spacing

- Both DCF and PCF modes can coexist within one cell. This works by carefully defining the interframe time interval. After a frame has been sent, a certain amount of time of dead time is required before any station may send a frame.

- Four different intervals are defined, each for a different purpose.


Control frame or next fragment may be sent here
SIFS
PCF frames may be sent here
PIFS
DCF frames may be sent here
DIFS
Bad frame recovery done here
EIFS
ACK
Time

Interframe Spacing

- **Short Interframe Spacing (SIFS)**:
  - It is used to allow the parties in a single dialog the chance to go first. This includes letting the receiver send a CTS to respond to an RTS, letting the receiver send an ACK for a fragment or full data frame, and letting the sender of a fragment burst transmit the next fragment without having to send an RTS again. There is always exactly one station that is entitled to respond after a SIFS interval.

- **PCF Interframe Spacing (PIFS)**:
  - If the station entitled to respond after a SIFs interval fails to make use of its chance and a time PIFS (PCF InterFrame Spacing) elapses, the base station may send a beacon frame or poll frame. This mechanism allows a station sending a data frame or fragment sequence to finish its frame without anyone else getting in the way, but gives the base station a chance to grab the channel when the previous sender is done without having to compete with eager users.

- **DCF Interframe Spacing (DIFS)**:
  - If the base station has nothing to say and a time DIFS (DCF InterFrame Spacing) elapses, any station may attempt to acquire the channel to send a new frame. The usual contention rules apply, and binary exponential backoff may be needed if a collision occurs.

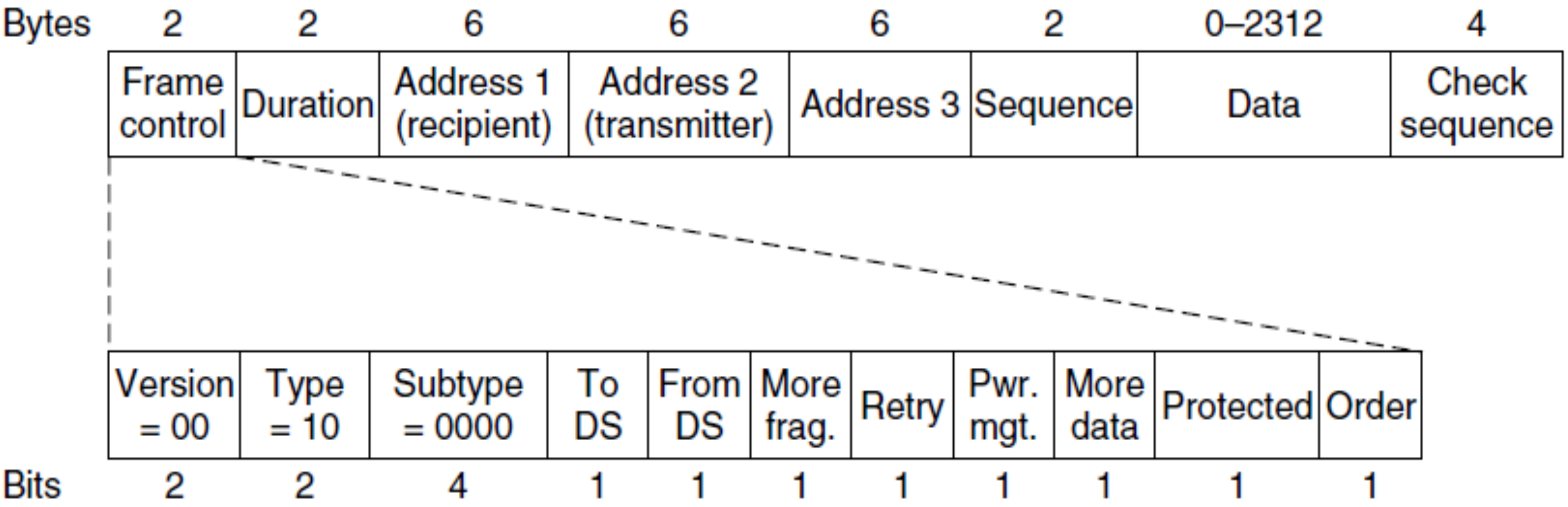
Interframe Spacing

- **Extended Interframe Spacing (EIFS)**:
  - The last time interval, EIFS (Extended InterFrame Spacing), is used only by a station that has just received a bad or unknown frame to report the bad frame. The idea of giving this event the lowest priority is that since the receiver may have no idea of what is going on, it should wait a substantial time to avoid interfering with an ongoing dialog between two stations.

802.11 Frame Structure

- The 802.11 standard defines three different classes of frames on the wire: data, control, and management. Each of these has a header with a variety of fields used within the MAC sublayer.

- The format of the data frame is shown below.



Bytes	2	2	6	6	6	2	0–2312	4
	Frame control	Duration	Address 1 (recipient)	Address 2 (transmitter)	Address 3	Sequence	Data	Check sequence

	Version = 00	Type = 10	Subtype = 0000	To DS	From DS	More frag.	Retry	Pwr. mgt.	More data	Protected	Order
Bits	2	2	4	1	1	1	1	1	1	1	1

802.11 Frame Structure

- ***Frame Control*** field is 2-bytes long and has 11 subfields:

Protocol (2-bits) : version of protocol used

Type (2-bits): specifies type of frame whether data, control, or management

Subtype (4-bits): e.g. RTS or CTS or ACK

To DS and **From DS** bits: indicate whether the frame is going to or coming from the inter-cell distribution system (e.g., Ethernet).

MF bit: more fragments to follow

Retry bit: marks a retransmission of a frame sent earlier

Power management bit: a station can indicate that it is going into a "sleep" or low-power state to the access point through a status bit in a frame header. The access point then buffers packets for the station instead of forwarding them to the station as soon as they are received. The sleeping station periodically wakes up to receive beacons from the access point. The beacons include information about whether frames are being buffered for the station. The station then sends a request (when polled) to the access point to send the buffered frames. After receiving the frames, the station can go back to sleep.

802.11 Frame Structure

More bit: indicates that the sender has additional frames for the receiver

Protected bit: specifies that the frame body has been encrypted

Order bit: tells the receiver that a sequence of frames with this bit on must be processed strictly in order

802.11 Frame Structure

Duration (2-bytes): tells how long the frame and its acknowledgement will occupy the channel and is how other stations manage the NAV mechanism.

3 MAC addresses (6-bytes each): Two addresses are for the source and destination. Third address is for the destination base station and is used for inter-cell traffic.

Sequence (2-bytes): allows fragments to be numbered. Of the 16 bits available, 12 identify the frame and 4 identify the fragment. So there can be at most $2^4 = 16$ fragments per frame.

Data field (0 to 2312 bytes): contains the payload (IP packet)

Checksum (4-bytes)

802.11 LAN with Ethernet Connectivity

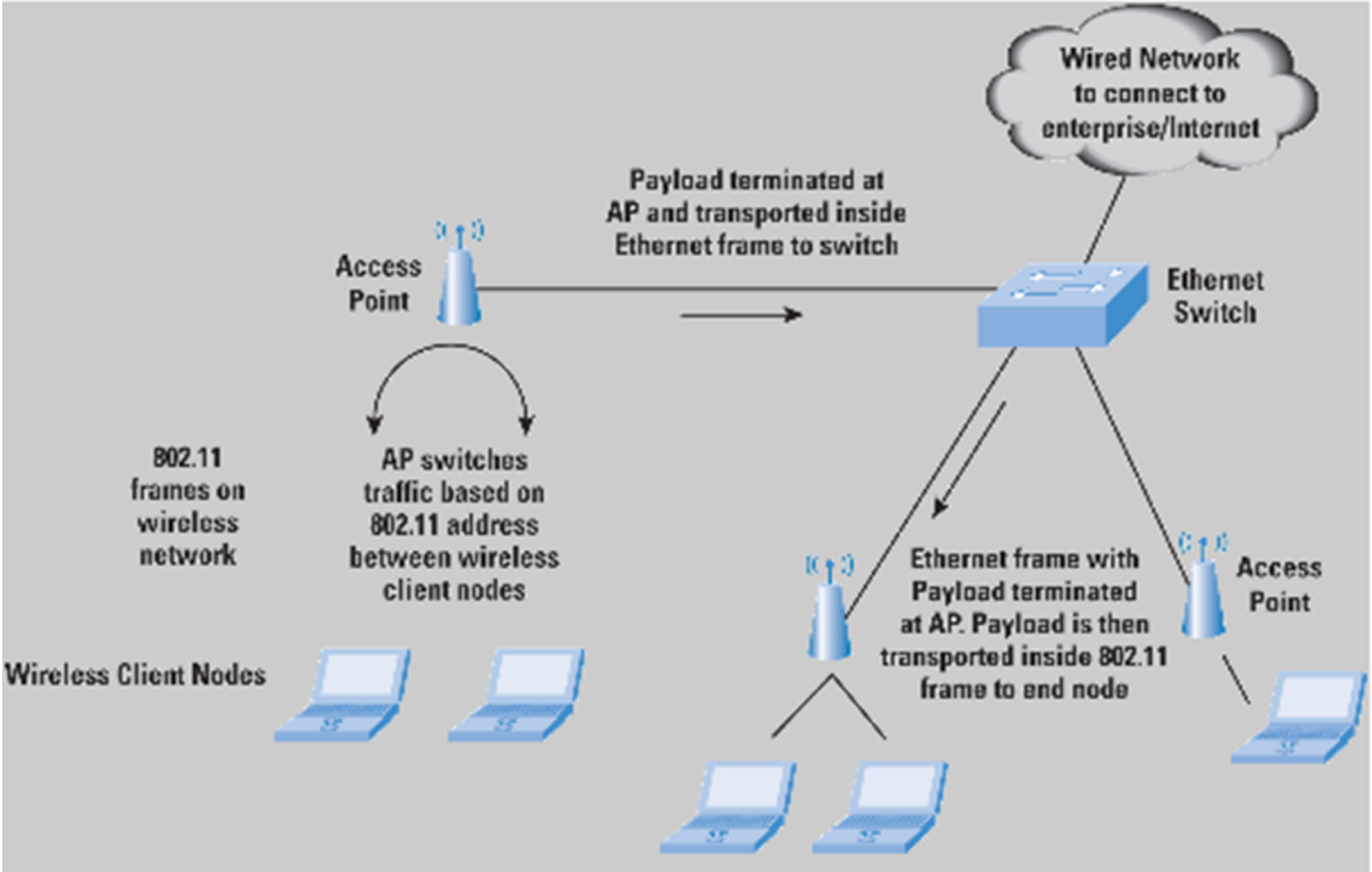

Wired Network to connect to enterprise/Internet
Payload terminated at AP and transported inside Ethernet frame to switch
Access Point
Ethernet Switch
802.11 frames on wireless network
AP switches traffic based on 802.11 address between wireless client nodes
Ethernet frame with Payload terminated at AP. Payload is then transported inside 802.11 frame to end node
Access Point
Wireless Client Nodes

Figure 1a: WLAN Network with Ethernet Connectivity

802.11 Services

- The 802.11 standard states that each conformant wireless LAN must provide nine services. These services are divided into two categories: five distribution services and four station services. The distribution services relate to managing cell membership and interacting with stations outside the cell. In contrast, the station services relate to activity within a single cell.

- Five distribution Services are:

Association. This service is used by mobile stations to connect themselves to base stations. Typically, it is used just after a station moves within the radio range of the base station. Upon arrival, it announces its identity and capabilities. The capabilities include the data rates supported, need for PCF services (i.e., polling), and power management requirements. The base station may accept or reject the mobile station. If the mobile station is accepted, it must then authenticate itself.

Disassociation. Either the station or the base station may disassociate, thus breaking the relationship. A station should use this service before shutting down or leaving, but the base station may also use it before going down for maintenance.

802.11 Services

- Distribution Services (continued):

Reassociation. A station may change its preferred base station using this service. This facility is useful for mobile stations moving from one cell to another. If it is used correctly, no data will be lost as a consequence of the handover. (But 802.11, like Ethernet, is just a best-efforts service.)

Distribution. This service determines how to route frames sent to the base station. If the destination is local to the base station, the frames can be sent out directly over the air. Otherwise, they will have to be forwarded over the wired network.

Integration. If a frame needs to be sent through a non-802.11 network with a different addressing scheme or frame format, this service handles the translation from the 802.11 format to the format required by the destination network.

802.11 Services

- The remaining four services are intracell (i.e., relate to actions within a single cell). They are used after association has taken place and are as follows.

- **Authentication.** Because wireless communication can easily be sent or received by unauthorized stations, a station must authenticate itself before it is permitted to send data. After a mobile station has been associated by the base station (i.e., accepted into its cell), the base station sends a special challenge frame to it to see if the mobile station knows the secret key (password) that has been assigned to it. It proves its knowledge of the secret key by encrypting the challenge frame and sending it back to the base station. If the result is correct, the mobile is fully enrolled in the cell.

- **Deauthentication.** When a previously authenticated station wants to leave the network, it is deauthenticated. After deauthentication, it may no longer use the network.

- **Privacy.** For information sent over a wireless LAN to be kept confidential, it must be encrypted. This service manages the encryption and decryption. The encryption algorithm specified is RC4, invented by Ronald Rivest of M.I.T.

- **Data delivery.** Finally, data transmission is what it is all about, so 802.11 naturally provides a way to transmit and receive data. Since 802.11 is modeled on Ethernet and transmission over Ethernet is not guaranteed to be 100% reliable, transmission over 802.11 is not guaranteed to be reliable either. Higher layers must deal with detecting and correcting errors.