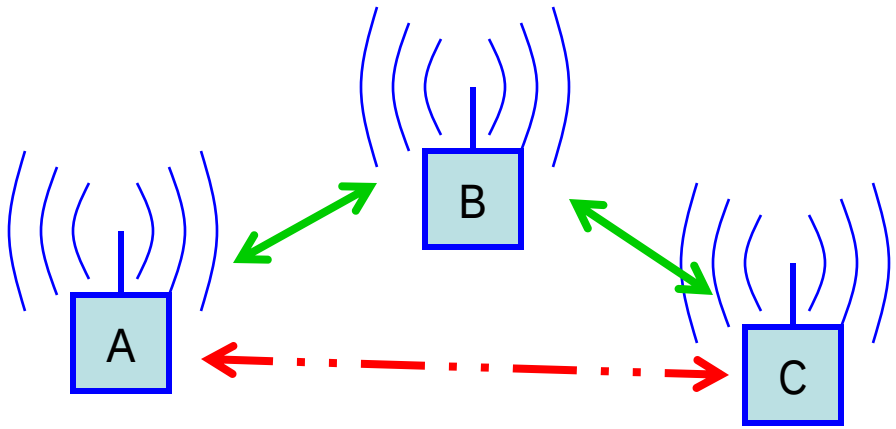
802.11 Wireless LAN Protocol

CS 571

Fall 2006

Wireless Channel Considerations

- Stations may move
  - Changing propagation delays, signal strengths, etc.
- "Non-transitive" reception
  - A can hear B, B can hear C, but A cannot hear C
- No "collision detection"!
  - Detect unsuccessful transmission by absence of acknowledgement



Wireless Channel Considerations, cont.

- Range of network limited by transmission power
  - If equipment obeys transmit power limits, no way to exceed maximum diameter
  - Therefore max end-to-end propagation delay is limited
- Radio Frequency (RF) spectrum usage is restricted by law/treaty!
  - 802.11 uses 2.4 GHz band, sometimes called ISM (Industrial, Scientific, Medicine)
  - Applications using this range of frequencies must use Spread Spectrum technology to minimize interference
  - This band subject to interference by microwave ovens (2.43 MHz), cellular phones, Bluetooth, wireless microphones, …

Pieces of the 802.11 Standard

Medium Access Control divided into two parts

- Distributed Coordination Function (DCF)
  - Symmetric, all stations (including APs) behave the same way
  - Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
  - Stations contend for access to medium
- Optional Point Coordination Function (PCF)
  - Built on DCF
  - Allows periods of contention-free operation interleaved with periods of contention
  - One station (typically AP) polls others to control who transmits
    - Note: importance of association function
  - Permits more efficient operation under heavy loads

Pieces of the 802.11 Standard

Multiple PHYs:

Original 802.11 (1999):

- 2.4 GHz frequency-hopping spread spectrum @ 1, 2 Mbps
- 2.4 GHz direct-sequence spread spectrum @ 1, 2 Mbps

802.11a (1999):

- 5 GHz orthogonal FDM @ 6, 9, 12, 18, 24, 36, 48, 54 Mbps

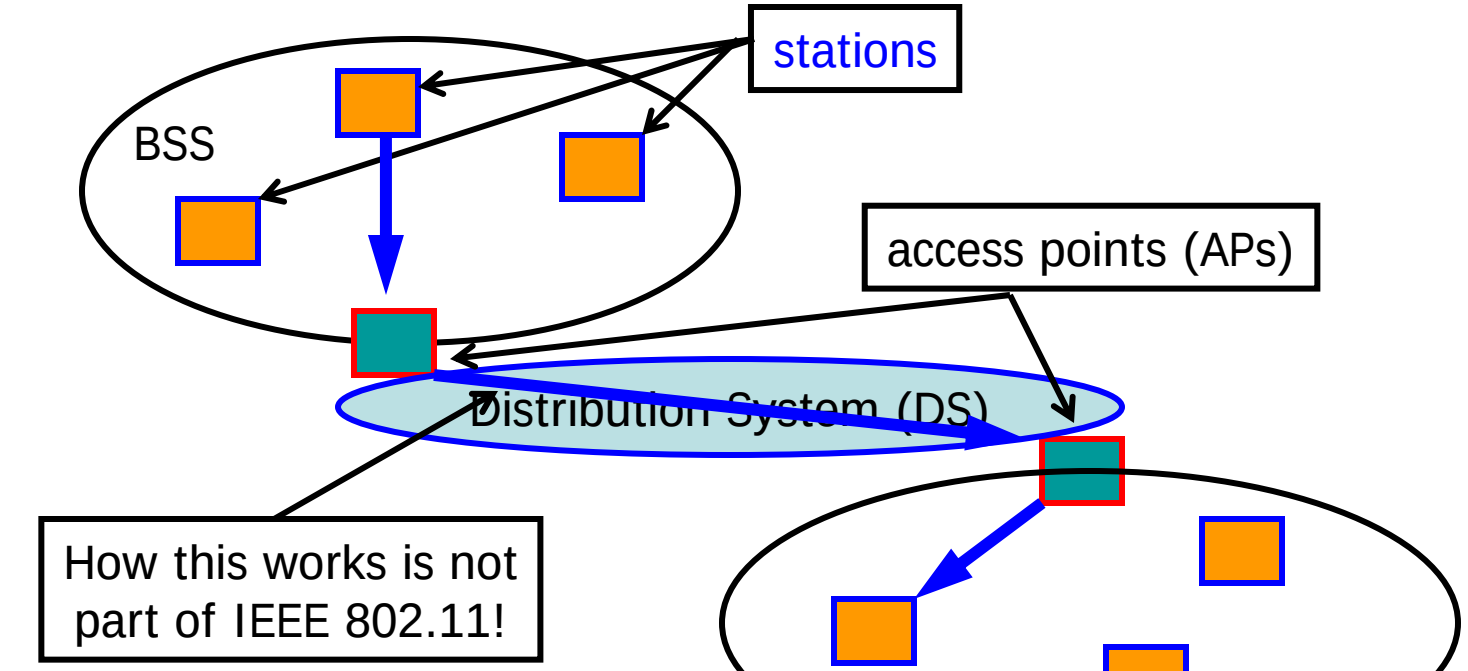
802.11b (1999):

- 2.4 GHz direct-sequence spread spectrum @ 5.5, 11 Mbps

802.11g (2003):

- 2.4 GHz orthogonal FDM @ 54 Mbps

Architecture: Components



BSS = "Basic Service Set"
≈ A group of stations communicating

MAC Protocol Design

- Different stations perceive events differently
  - ⇒ Include explicit information about MAC state in transmitted frames
    - E.g., duration of the next frame to be transmitted
    - Beacon frames inform stations about operational parameters
- Collision avoidance:
  - Stations choose a random backoff interval before colliding!
    - (Compare to CSMA/CD: backoff only after colliding)
  - Each station's backoff continues after other transmitted frames
    - (Helps with fairness)
- No collision detection: waste whole frames in collisions
  - ⇒ Try to ensure collisions don't happen long frames
    - Exchange (short) control frames to clear the channel (RTS-CTS)
  - ⇒ Include immediate ACKs as part of MAC protocol — retransmit if no ACK received

802.11 MAC Protocol Services

- Contention-based Channel Access
  - Some collisions may occur (but — "collision avoidance")
- Contention-free Channel Access (optional)
  - No collisions (requires AP)
- Authentication of stations joining a network
  - "Open System" = any station can be authenticated
- Confidentiality of data
  - Using WEP or WPA encryption
- Association with a particular network ("BSS")
- MAC-level Acknowledgements
- Fragmentation and Reassembly

MAC Protocol Design

Wireless MAC Protocol Building Blocks:

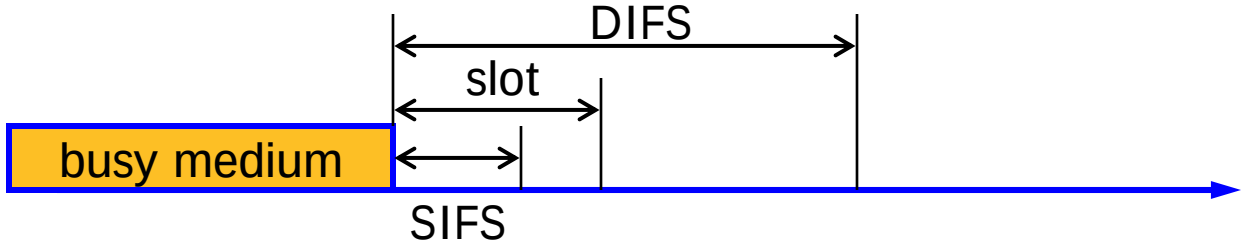
- Clear Channel Assessment function (CCA): determines whether/when medium is busy/idle
  - Virtual Carrier Sense: use "Duration" fields in frames to infer that medium should be busy, regardless of whether it is sensed busy
- Inter-Frame Spacing (IFS) parameters
  - Variable defer times allow coordination of management functions with data transfer
- Slot time: basic unit of timing for the protocol

  Equal to RxTx Turnaround Time + Channel Sensing Time + Propagation Delay + MAC processing time
- Backoff timer: counts slots until station's turn to transmit

Basic DCF MAC Protocol

Basic Time Parameters

- Slot Time: basic unit of backoff algorithm
  = Time required for station to sense end of frame, start transmitting, and beginning of frame to propagate to others
- SIFS: Short Inter-Frame Space
  = Time required for station to sense end of frame and start transmitting
- DIFS: DCF Inter-Frame Space
  = Time to wait before starting backoff interval ("contending")
  = SIFS + 2 slot times



Basic DCF MAC Protocol

If medium is free for ≥ DIFS → transmit

else back off:

Wait for medium to be free for DIFS

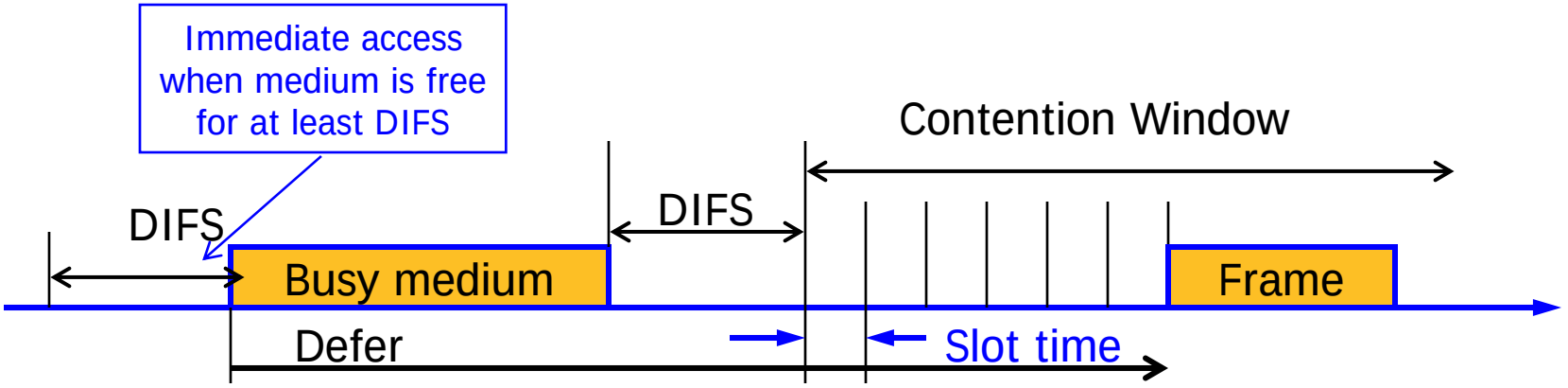
Choose a random r in [0,CW]

While r > 0:

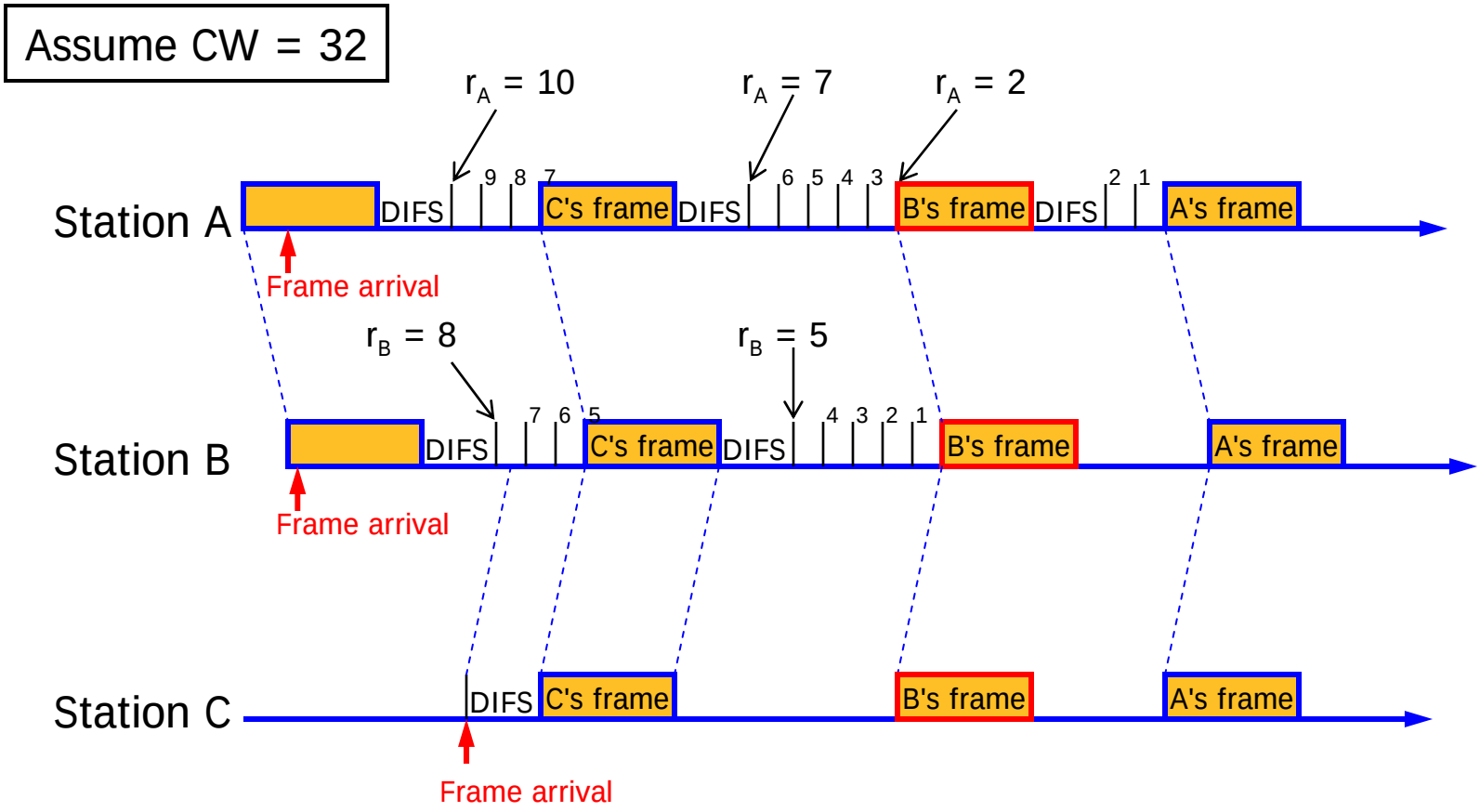
sense medium for one slot time

if medium free throughout slot → r := r – 1

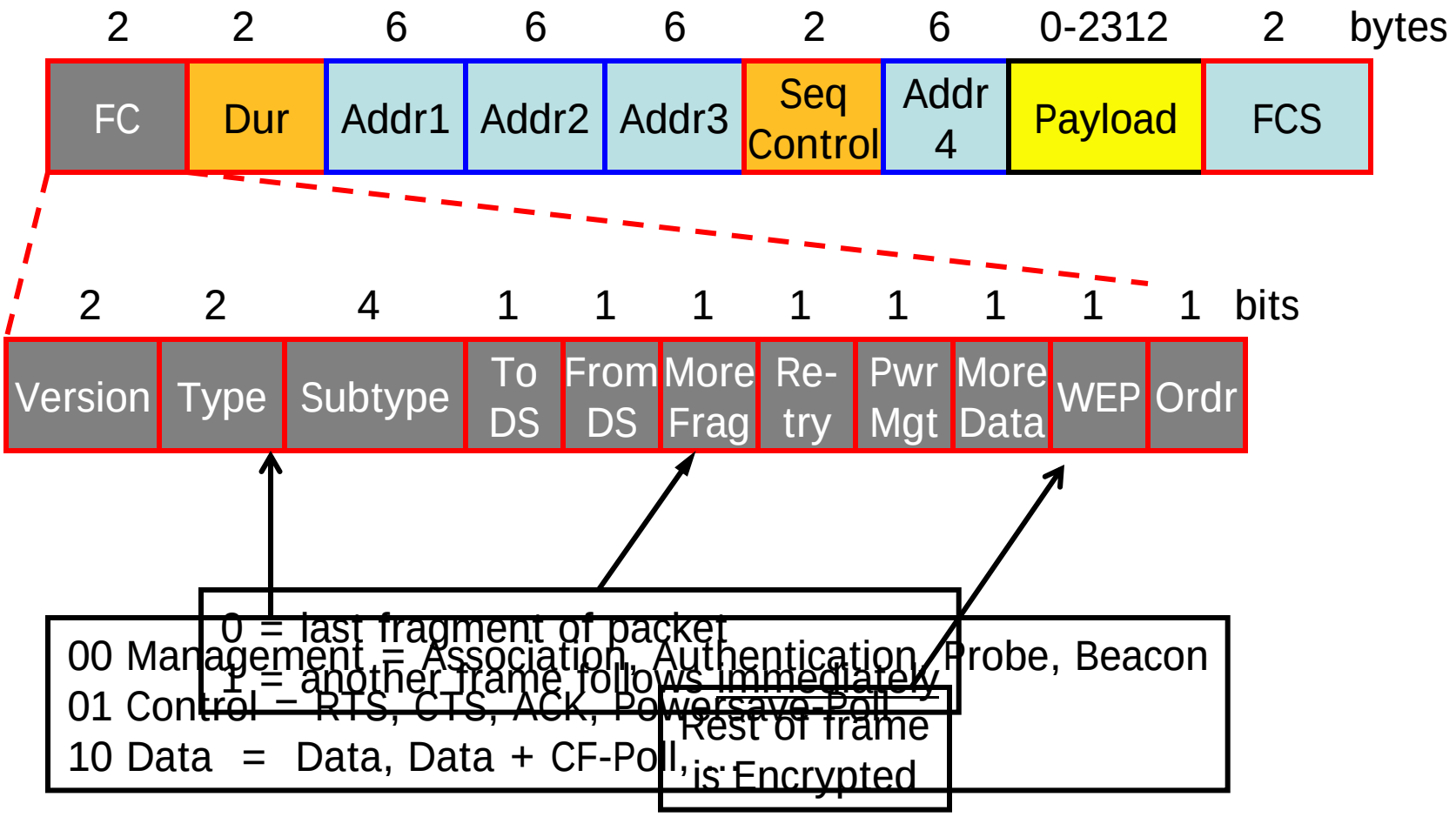
transmit frame



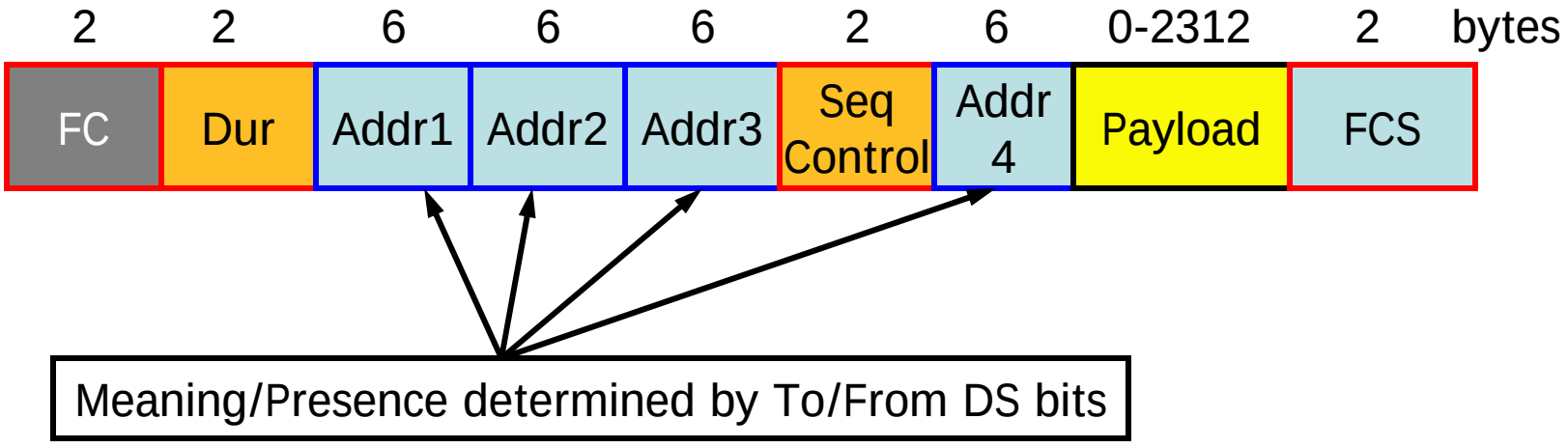
Backoff Operation



General Frame Format

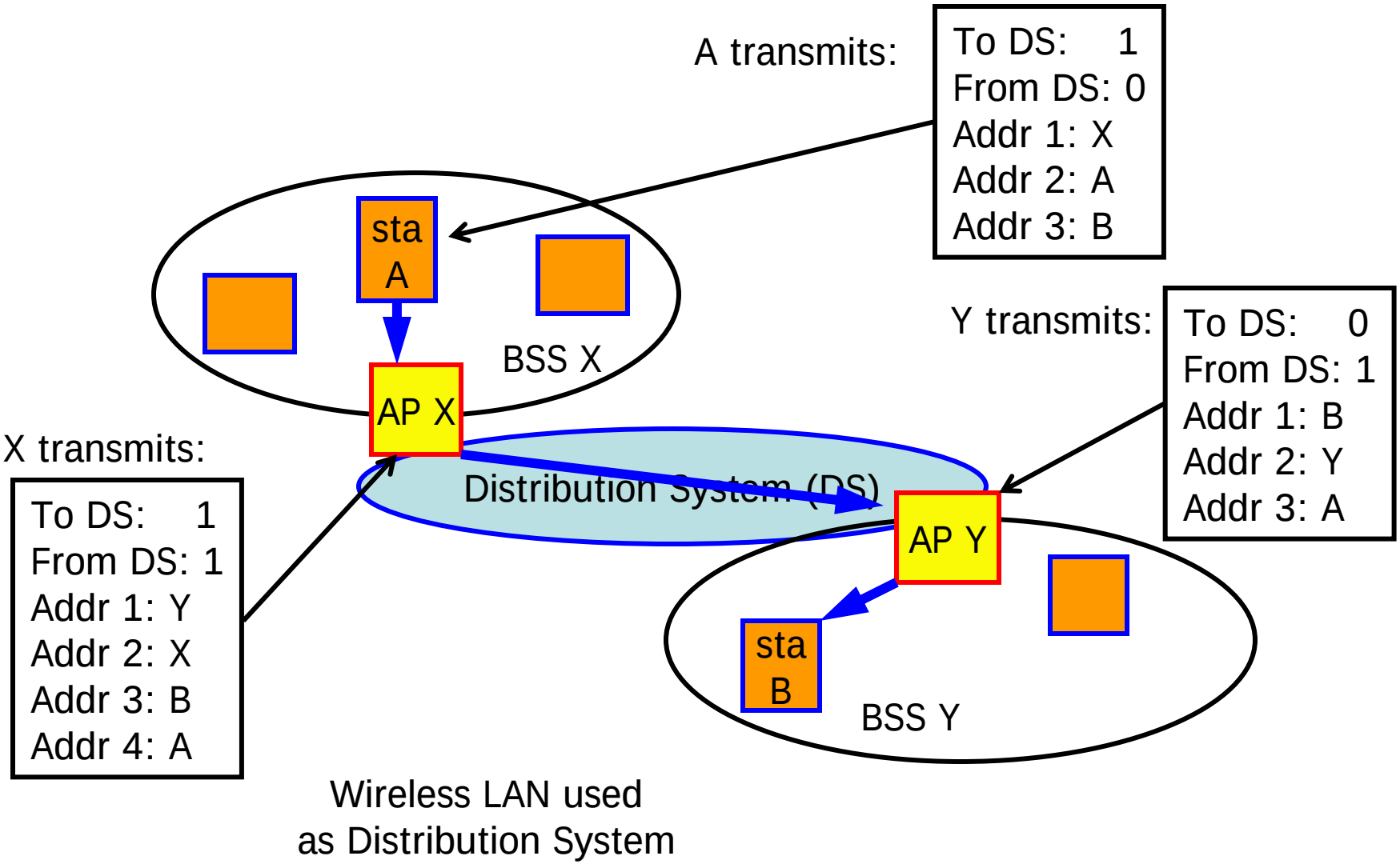


General Frame Format

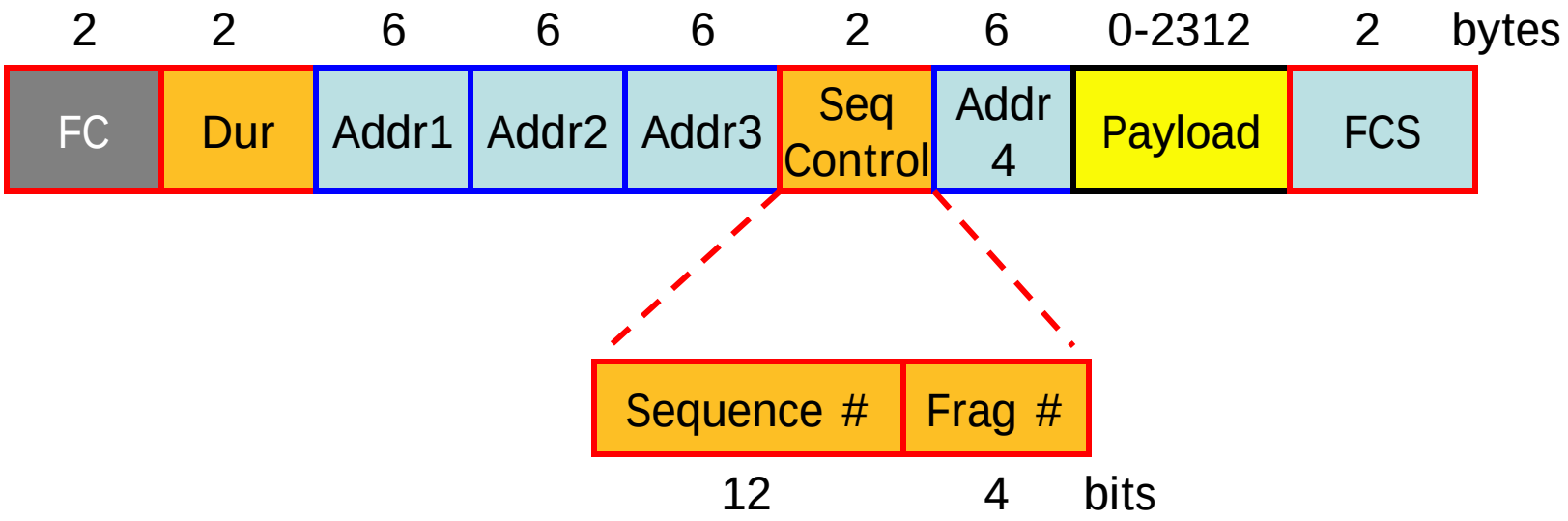


To DS	From DS	Addr 1	Addr 2	Addr 3	Addr 4
0	0	Dest	Source	BSSID	N/A
0	1	Dest	AP Addr	Source	N/A
1	0	AP Addr	Source	Dest	N/A
1	1	Receiver	Xmitter	Dest	Source

Example of Address Usage



General Frame Format

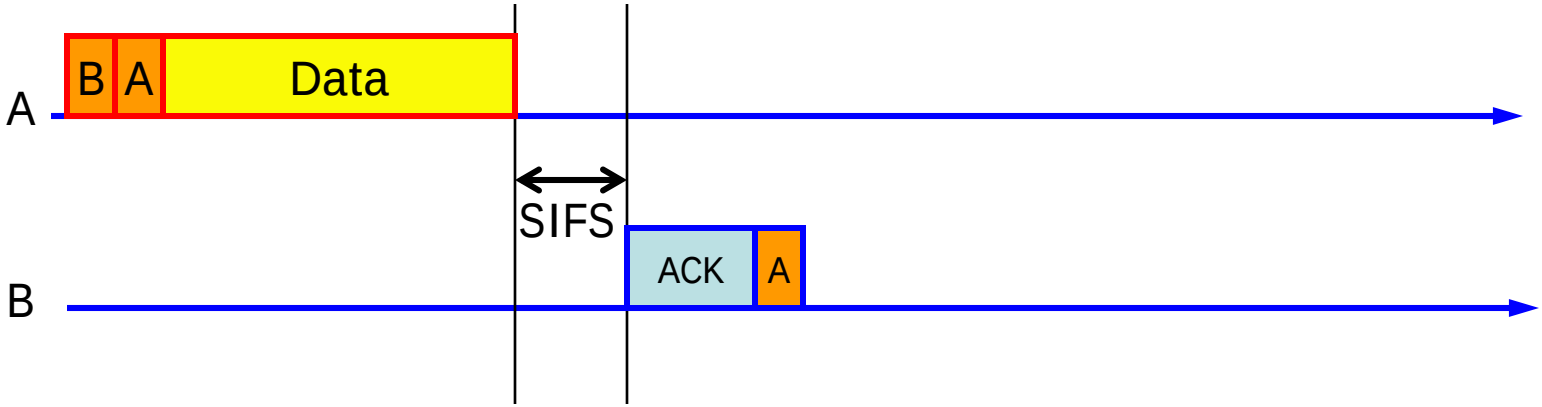


Used for fragmentation & reassembly:
Sequence number assigned to each packet;
Fragments are sent in order;
Each fragment is retransmitted until ACKed.

Seq/frag # is also used to filter duplicate retransmissions:
Each station maintains a "triple cache" of recent
(Addr2, seq#, frag#) and drops (but still ACKs) frames
whose tuples are in the cache. (Addr2 = transmitting sta)

MAC-level ACKs

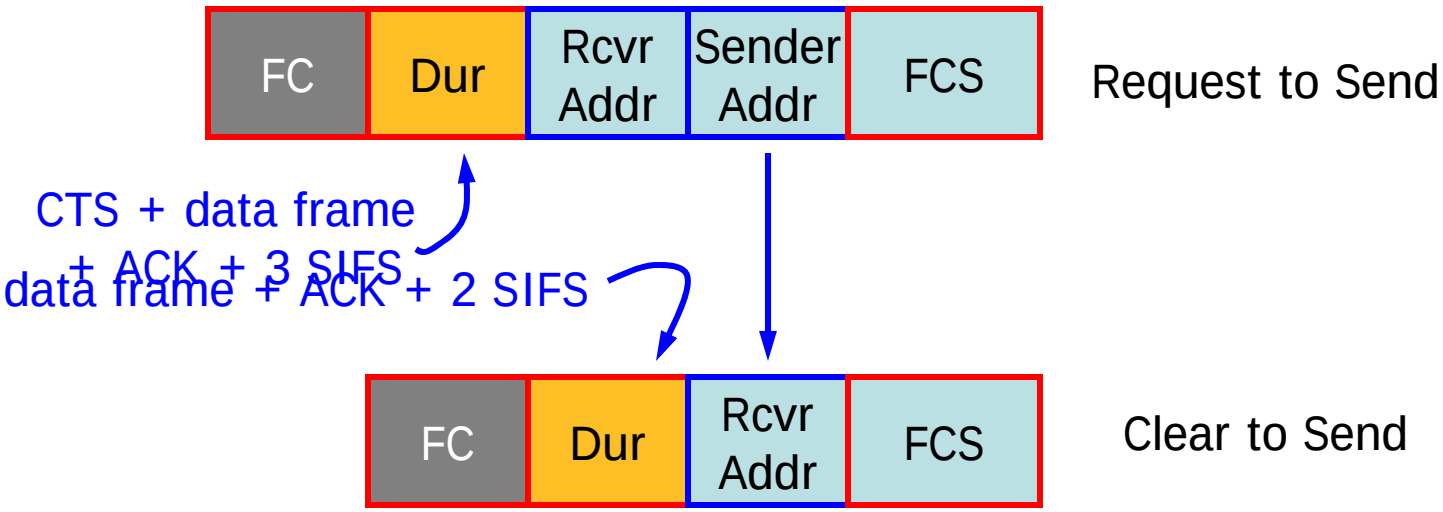
- Upon receiving a frame addressed to it with a correct FCS, a station immediately transmits an ACK frame



- If a station fails to receive a correct ACK frame within a timeout, it retransmits (setting retry flag)

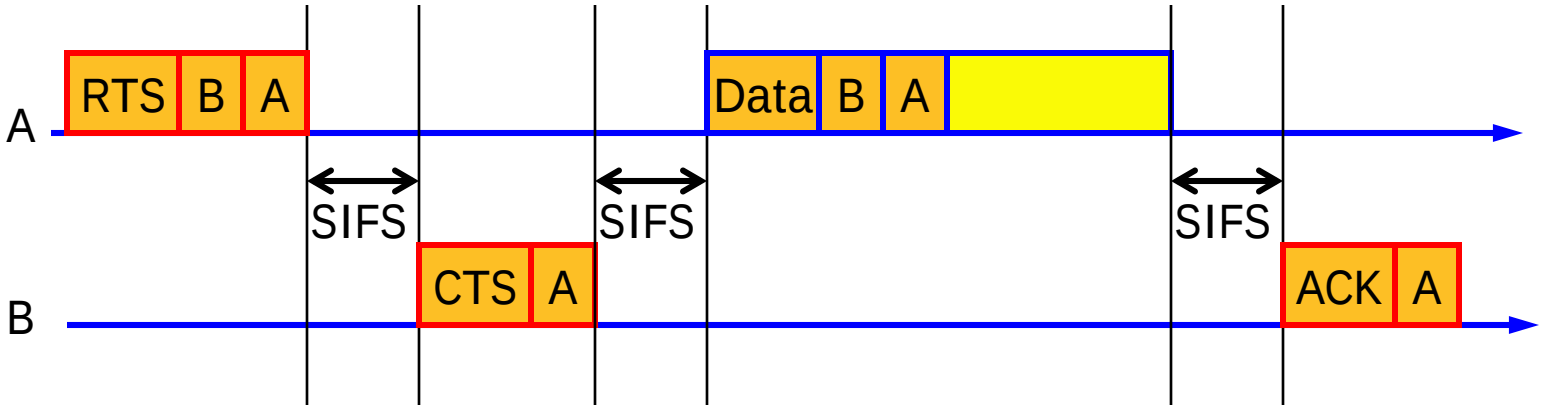
Request to Send – Clear to Send

- Before sending a long frame, send RTS
  - "long" = length greater than RTSThreshold parameter
  - RTSThreshold configurable per-station, range 0-2344+
- Recipient responds immediately with CTS
- Upon receiving CTS, immediately transmit Data



RTS-CTS Operation

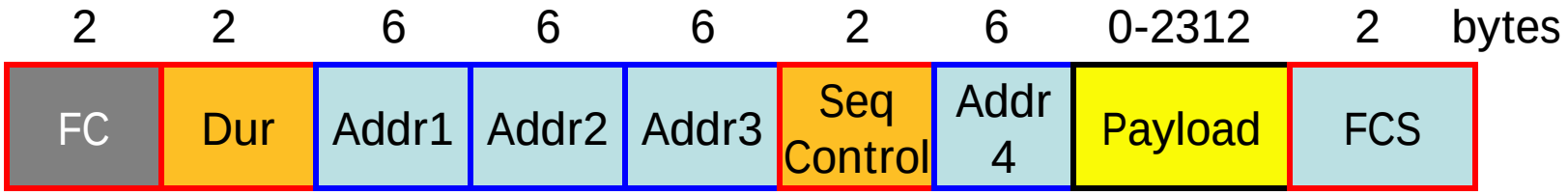
Note: SIFS is shorter than DIFS, so stations contending for access do not decrement their backoff counters during these exchanges



Network Allocation Vector (NAV)

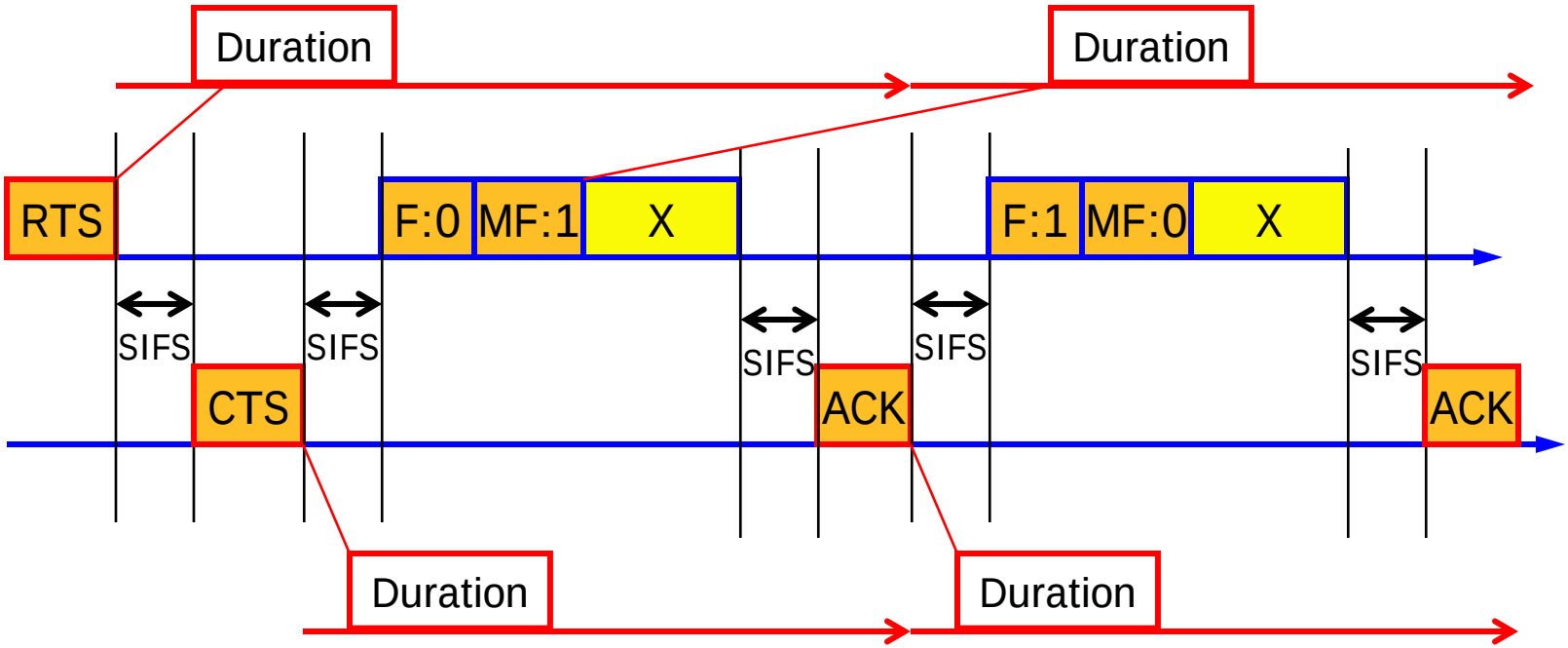
- Each station maintains a countdown timer that tells how far into the future the medium has been "reserved" by RTS/CTS exchanges
- Stations set NAV counter based on the value in the duration field of frames
  - Even if a station only hears one side of the RTS-CTS exchange, it knows how long the medium will be "busy"
- CCA function combines NAV and physical sensing
  - Medium considered busy if NAV value > 0

General Frame Format



Duration of next frame, in microsecs (max 32,767)
RTS: duration of CTS + data frame + ACK + 3 SIFS
CTS: RTS duration – CTS – SIFS
Data w/ More Frags = 1: duration of next frag
Data w/ More Frags = 0: duration of ACK + SIFS

Fragment Bursts



Management: Who's Playing?

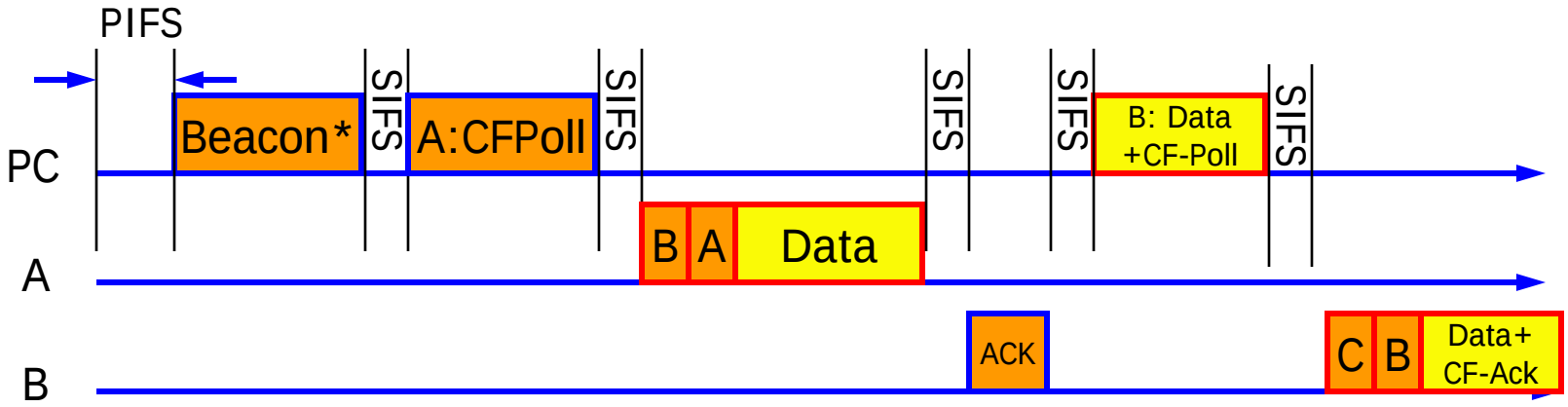
- MAC layer must provide stations a way to:
  - Learn what SS's are available
  - Associate with a particular SS (and authentication)
  - Disassociate from a SS
- Beacon Frames are broadcast periodically by the Access Point

  Contains: SS ID, Access Point address (if any), Beacon frame interval, supported data rates
- Stations may also send Probe frames to solicit information from APs (sent in Probe response msgs)
- Management frames are transmitted with higher priority
  - Implemented by using a smaller Priority Inter-frame Space

Point Coordination Function

- Idea: allow for explicit allocation of the channel
  - AP acts as Controller, polls stations
  - During a contention-free period, all stations see the medium as busy (for purposes of contention)
- Frame types:
  - Beacon (indicates start, duration of contention-free period)
  - CF-Poll, CF-Ack
  - Data+CF-Poll, Data+CF-Ack, Data+CF-Poll+CF-Ack
- When polled, station may transmit 1 (data) frame to any station

PCF Operation



- Special beacon marks beginning of CF period
  - Sent after sensing medium idle for PIFS (< DIFS)
    - Prevents other stations from contending for medium
  - Indicates duration of CF period
    - Non-PCF-capable stations set NAV to that value