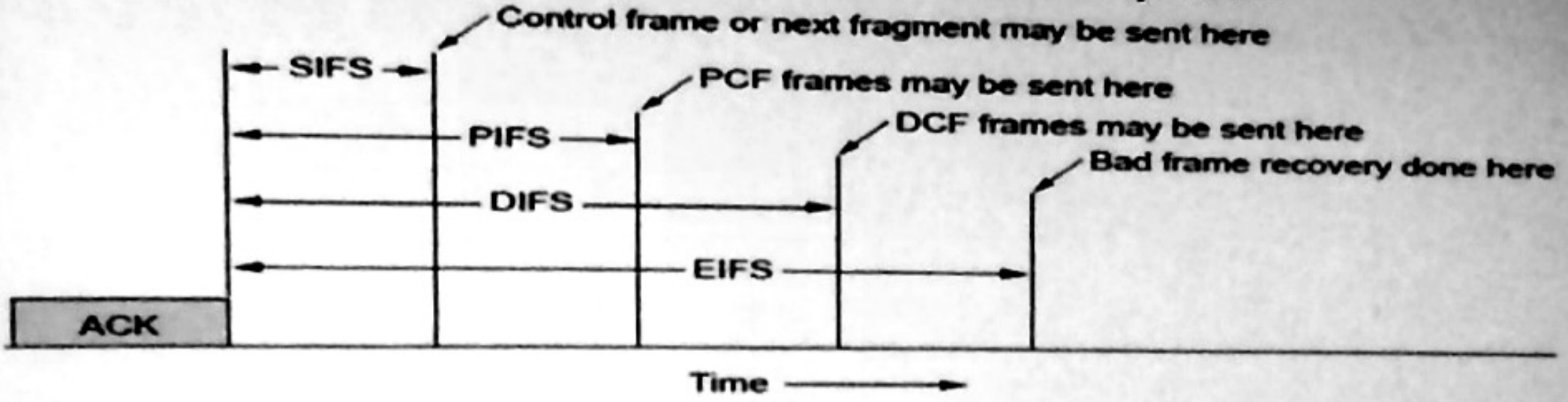
- Wireless network – 802.11a/b/g
  - PCF
    - Access point polls stations in a cell, so no chance of a collision
    - Polling mechanism specified by 802.11 standard
    - Polling frequency, order, station priority, etc., implementation dependent
    - Access point transmits different types of frames
      - Beacon frame – sent out at regular intervals(10 to 100 times/ sec)
        - Contains info on cell system parameters (eg., channel frequency & b/w, modulation technique, encryption. etc,) to allow mobile stations to synchronise with access point
        - Allows new stations entering a cell to associate themselves with cell (sign-up with the access point)
      - Polling frame
        - Stations associated with a cell are regularly polled by its access point
        - Checks to see if station has a frame to transmit
        - Allows collision free transmission by all stations in a cell in an equitable manner
        - Polling order may be round robin, station priority dependent, dependent on whether station remained silent/ transmitted in previous poll slot, etc.
        - Station priority may be fixed (purchased) or dynamically altered by access point

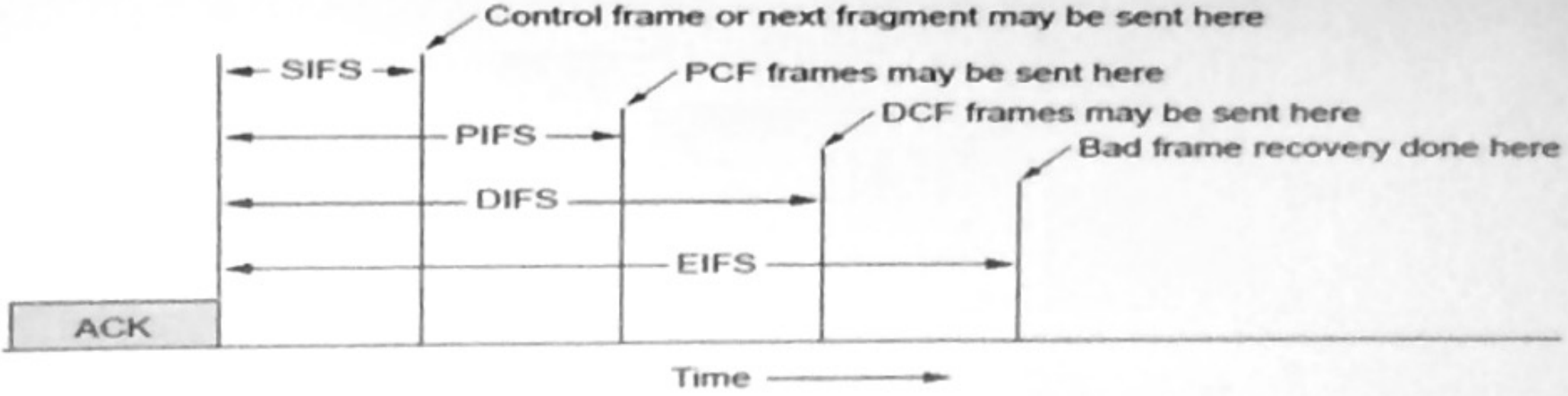
- Wireless network – 802.11a/b/g
  - PCF
    - Access point transmits different types of frames
      - Control frames – allows access point to perform functions other than new station sign-up & existing station polling
    - Power management – battery life is critical
      - Access point can send a station to hibernate/ sleep mode to conserve its power
      - All frames sent to this station is then temporarily buffered by the access point, to be delivered later when station reverts back to active mode
      - Station can be brought out of hibernation either by its user or by access point through a control frame
  - PCF and DCF allowed simultaneously in same cell by 802.11
    - After a frame transmission, station needs some 'dead time' before it can transmit again
    - Dead time requirement exploited to precisely define certain time intervals known as inter – frame – spacing (IFS)
    - Simultaneous distributed (DCF) and centralised (PCF) control realised using inter – frame – spacings
    - Four different IFS defined

- Wireless network – 802.11a/b/g
  - PCF and DCF allowed simultaneously in same cell by 802.11



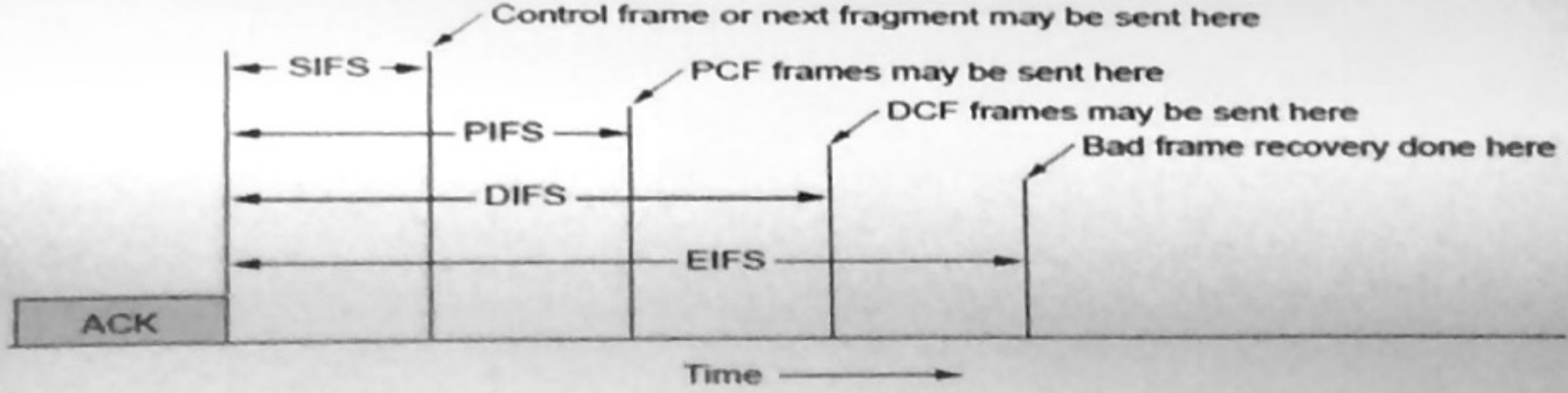
  - SIFS (Short Interframe Spacing)
    - Station which transmitted last frame or frame-fragment is in control of channel during SIFS
    - Receiving station
      - Can send CTS in response to earlier RTS
      - Can send an ACK in response to a received frame or frame fragment
    - Sending station
      - Can send the next fragment of a fragment burst without going through RTS – CTS handshaking again
      - Station not transmitting between end of SIFS & before end of PIFS means it has nothing more to send for now
    - Any other station can take control of channel now

- Wireless network – 802.11a/b/g
  - PCF and DCF allowed simultaneously in same cell by 802.11



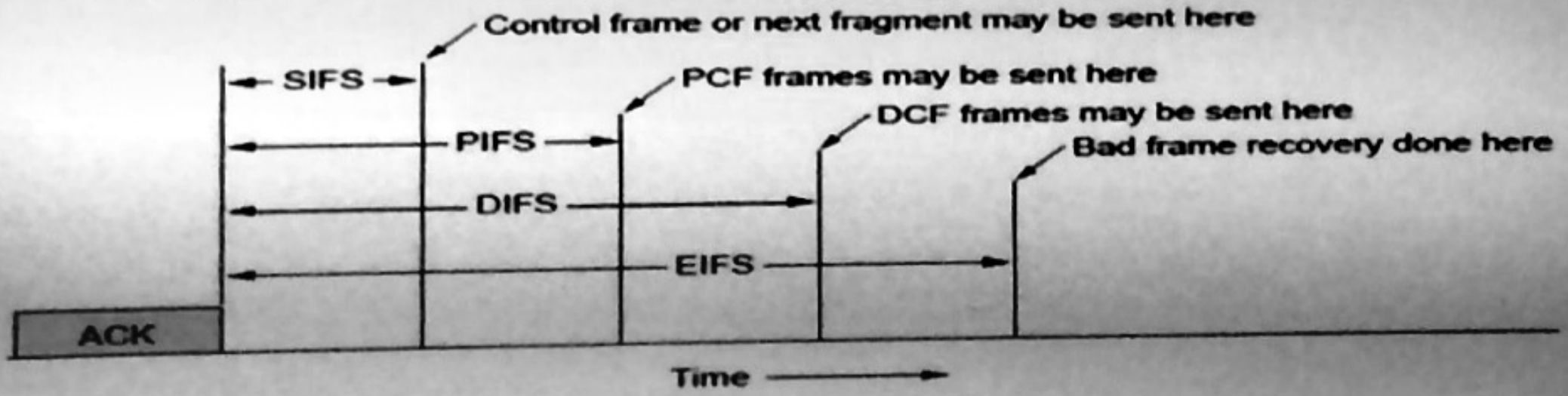
  - PIFS (PCF Interframe Spacing)
    - If channel is free (as heard by cell access point & all stations within cell) at the end of PIFS interval, access point acquires channel & PCF comes into effect
    - Access point can transmit
      - A beacon frame & any new incomming station requiring 'sign-up' under PCF can respond
      - A control frame & target station can act appropriately or send back a response frame or do both, as needed
      - A polling frame & target station can send a frame or frame fragment if it needs to

- Wireless network – 802.11a/b/g
  - PCF and DCF allowed simultaneously in same cell by 802.11



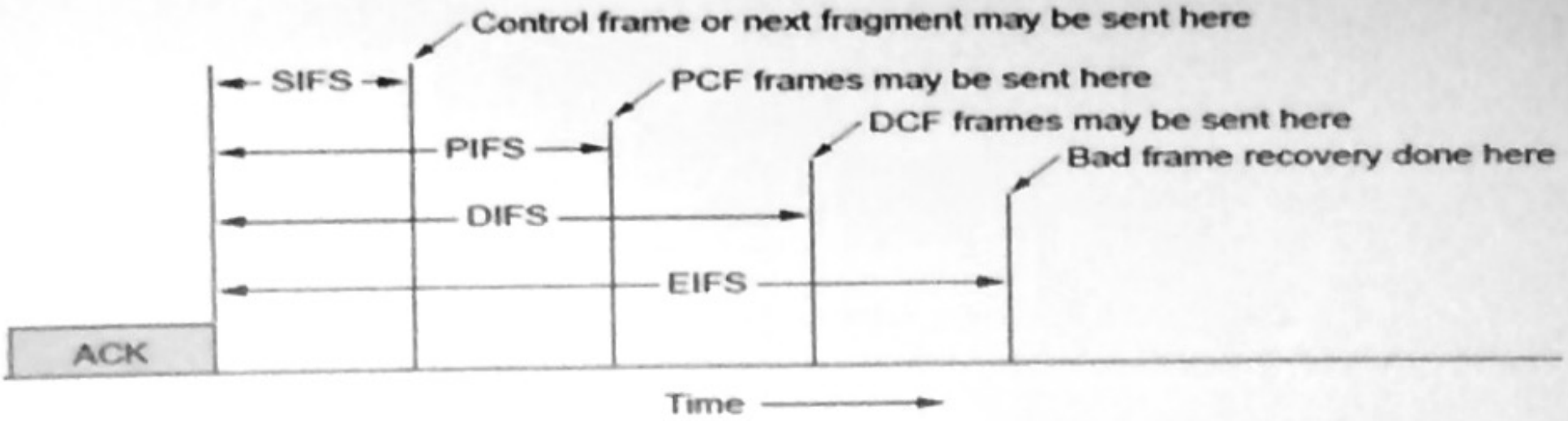
  - DIFS (DCF Interframe Spacing)
    - If channel is free at the end of DIFS, DCF protocol comes into effect now
    - Any station (usually ad-hoc n/w stations) can attempt to acquire channel
    - Full contention environment
    - Usual RTS – CTS – ACK frame exchange required to ensure collision free data transfer
    - NAV & SIFS used to ensure silence of other station during transmission of full frame or fragment burst
    - MACA or MACAW used
    - Exponential Binary Backoff or some variant of this used in case of collision

- Wireless network – 802.11a/b/g
  - PCF and DCF allowed simultaneously in same cell by 802.11



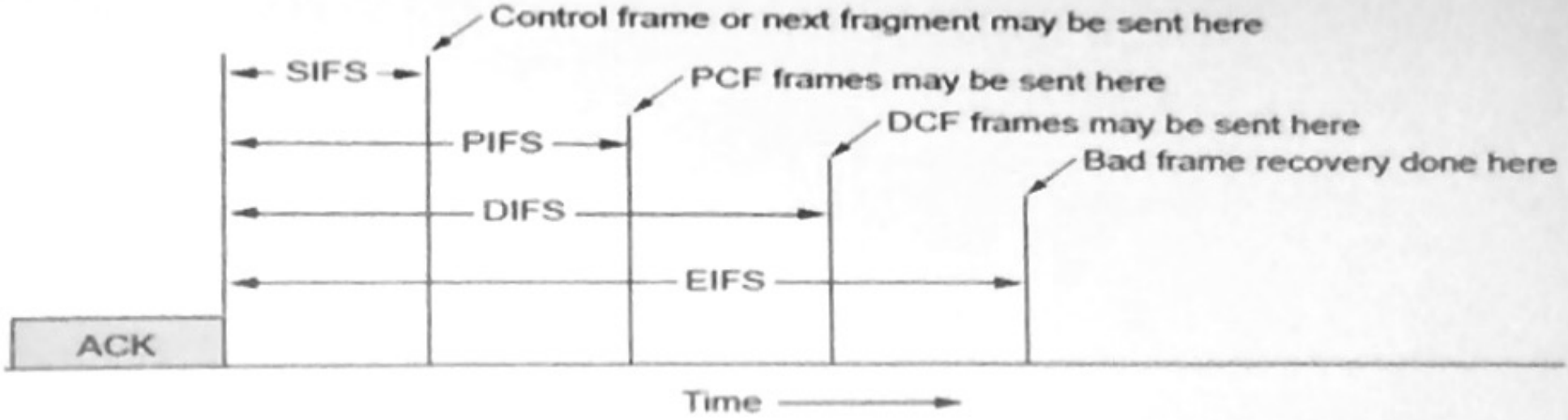
  - PIFS (PCF Interframe Spacing)
    - If channel is free (as heard by cell access point & all stations within cell) at the end of PIFS interval, access point acquires channel & PCF comes into effect
    - Access point can transmit
      - A beacon frame & any new incomming station requiring 'sign-up' under PCF can respond
      - A control frame & target station can act appropriately or send back a response frame or do both, as needed
      - A polling frame & target station can send a frame or frame fragment if it needs to

- Wireless network – 802.11a/b/g
  - PCF and DCF allowed simultaneously in same cell by 802.11



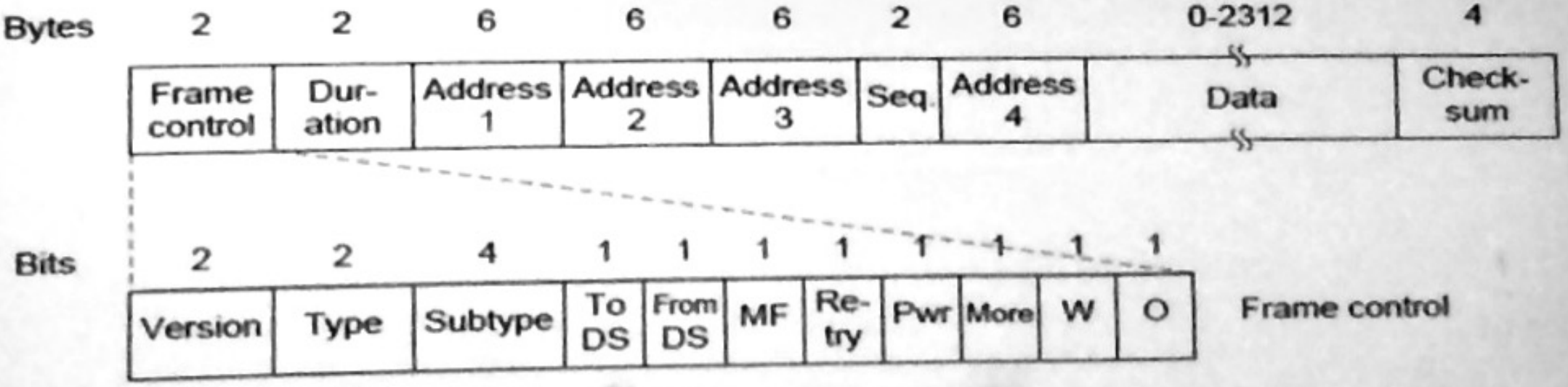
  - EIFS (Extended Interframe Spacing)
    - If channel is free at the end of EIFS, a station receiving a bad frame, or one with contents that makes no sense, etc., reports this as error through a control or data frame or both
    - Reporting normally done to cell access point
    - Error reporting is deferred to the end to ensure that it is really an error & an irrecoverable one
      - Station getting bad frame normally has no idea about 'why or how'
      - Station waits for sometime for clarification/ correction frame(s) from some other station(s)
      - If nothing received, station assumes it to be a actual error
      - Station reports error to access point which initiates error recovery

- Wireless network – 802.11a/b/g
  - PCF and DCF allowed simultaneously in same cell by 802.11



  - Order/ priority of communication
    - On-going transmission (PCF or DCF) allowed to complete first
    - Intra – cell transmissions (data, control, management, etc.) under PCF come next
    - Ad-hoc network stations communicate (both data & error handling) under DCF using wireless contention protocol
    - Intra – cell error reporting from stations under PCF

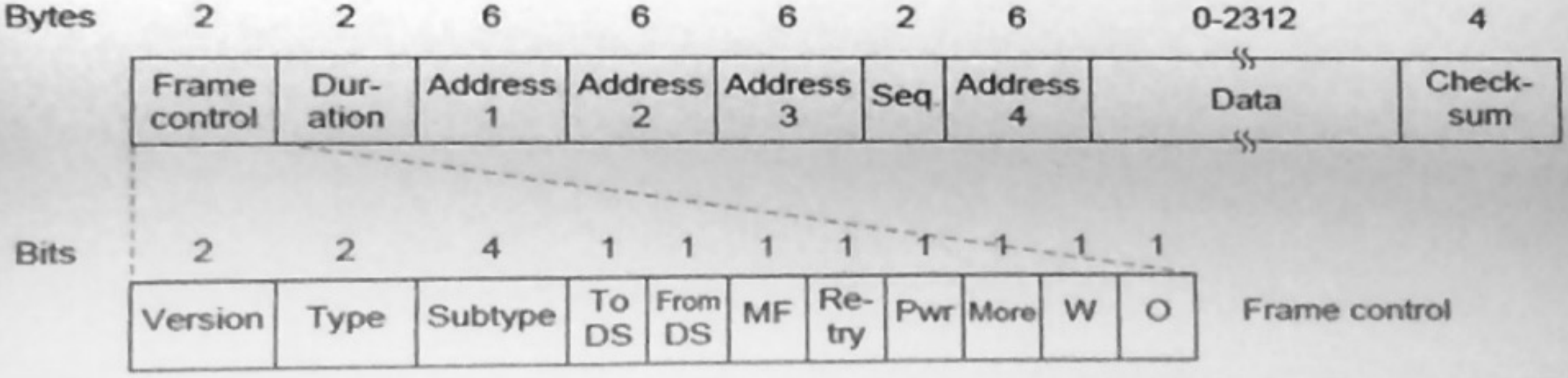
- Wireless network – 802.11a/b/g (frame format)
  - Three types of frames
    - Data
    - Control
    - Management
  - Fields



- Frame control – has eleven sub – fields
  - Version – allows simultaneous use of two or more versions of a protocol in same network
  - Type - Data, Control or Management
  - Subtype – type of data, control or management frame, e.g., CTS or RTS control frame
  - To DS & From DS – frame is from inter-cell distribution system, e.g., from 802.3 to 802.11 or vice versa

❑ Wireless network – 802.11a/b/g (frame format)

➢ Fields

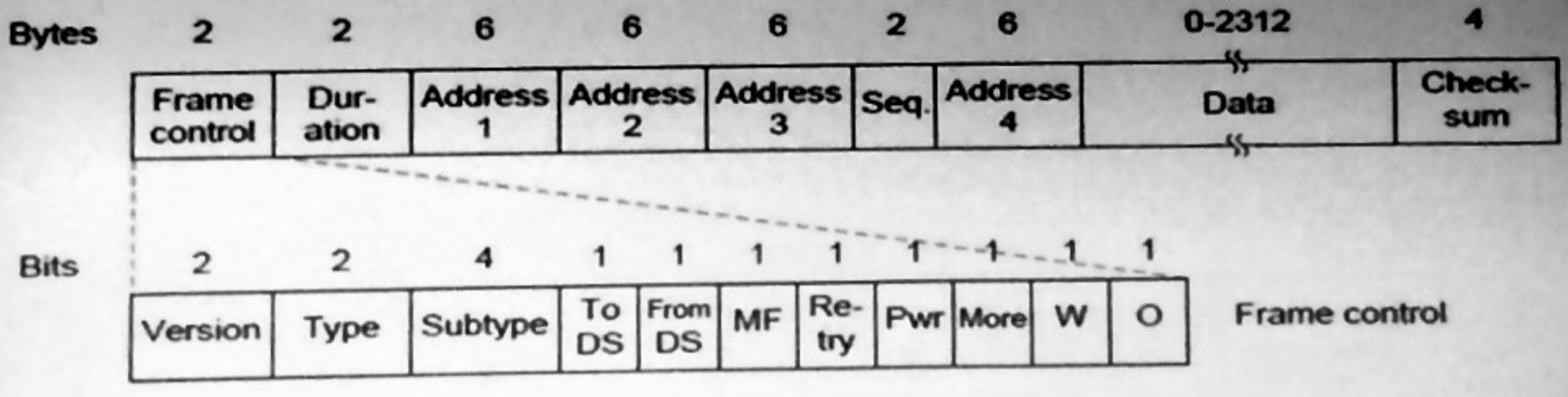


❖Frame control (cont.)

- MF – more fragments to come, i.e., frame burst not yet over
- Retry- this frame is retransmission of an earlier frame
- Pwr – a management frame, used by access point to send station into hibernate/ active mode
- More – sender has more frames to send
- W – frame body/ payload encrypted using some WEP algorithm (Wired Equivalent Privacy)
- O – processing sequence; O = 1→ sequence of frames must be processed strictly in order

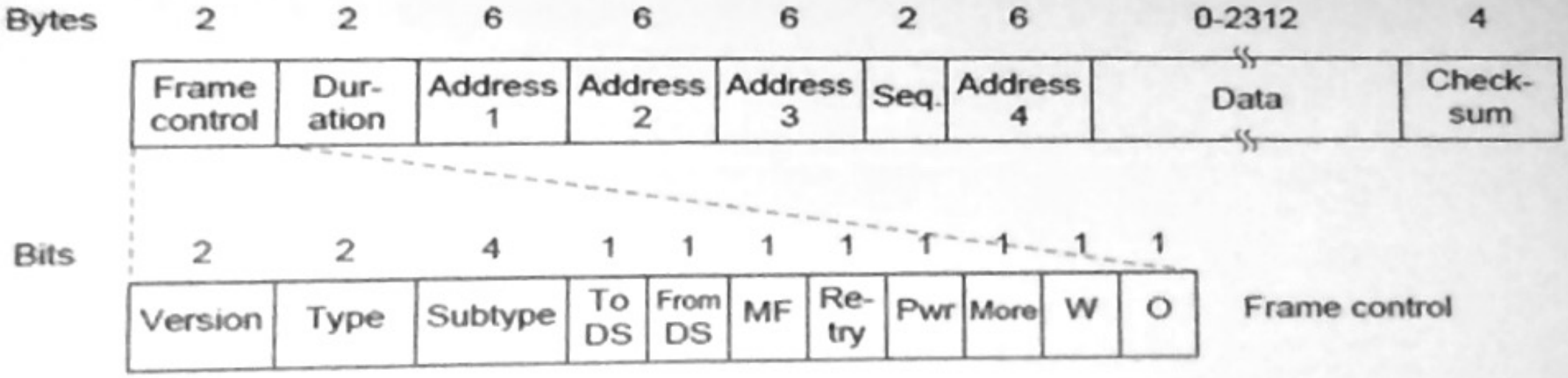
❑ Wireless network – 802.11a/b/g (frame format)

➢ Fields (cont.)



- ❖ Duration – total time for which the frame & its ACK (from receiver) will keep the channel busy; used by other stations to set their NAV values
- ❖ Address1 – source station address
- ❖ Address2 – destination station address
- ❖ Address3 – source base station/ access point address
- ❖ Address4 – destination base station/ access point address
- ❖ Seq – used to number frames & frame fragments
  - o 12-bit frame no.
  - o 4-bit fragment no.
- ❖ Data – variable sized frame payload (2312 bytes max)
- ❖ Checksum – 32-bit CRC

❑ Wireless network – 802.11a/b/g (frame format)



- Management frame
  - Function performed by individual access points, effect restricted to one cell
  - Only three address fields
  - Data field either empty or has parameter values needed for particular management function
- Control frame
  - Only two address fields (source & destination)
  - No data field
  - No Seq field
  - Subtype field defines nature of control involved

- Wireless network – 802.11a/b/g Services
  - Any 802.11 LAN must provide nine services
  - Five distribution services
    - Applicable for both intra & inter cell communication
    - Normally provided by base station/ access point
  - Four station services
    - Only for intra cell communication
    - Usually provided by mobile stations
  - Distribution services
    - Association – used by mobile station to associate with an access point after arriving into its cell
      - Station announces itself in response to a beacon frame from access point - provides identity, communication parameters, e.g., data rate, PCF or DCF, power management details, etc.
      - Access point may accept or reject – if accepted, station must authenticate itself
    - Disassociation – association between a station & an access point/ cell is broken
      - Initiated by mobile station moving away from a cell
      - Initiated by base station/ access point for
        - Maintenance shut down after handoff of all stations under it to a nearby overlapping cell
        - Prevention of errant/ unauthorised activity by a station

- Wireless network – 802.11a/b/g Services
  - Distribution services (cont.)
    - Reassociation
      - A station already associated with a base station/ access point may change to another one, i.e., move to another cell using this service
      - Absolutely no discontinuity or data loss during handoff, if executed correctly
      - Faster, better & more efficient than full disassociation followed by fresh association
    - Distribution
      - Deals with routing of frames received by base station/ access point
        - Intra-cell/ local – sent direct 'over the air' to another station within the cell
        - Inter-cell/ non-local
          - transmitted over wired n/w (802.3 perhaps) by source cell base station to destination cell base station
          - at destination cell, base station transmits frame 'over the air' to destination station within cell
        - Conversion between frame formats for different protocols
        - Changeover between multiple protocols & back
    - Integration
      - Applicable when frames are to be sent over non 892.11 networks
      - Service provides translation 802.11 frame to the format of the

- Wireless network – 802.11a/b/g Services
  - Station services
    - Authentication
      - Done immediately after a new station is initially accepted by a base station/ access point
      - Base station/ access point sends a special 'challenge' frame to new station
      - Station encrypts this frame with current 'secret' key of the cell & returns to base station/ access point
      - Station permitted to associate with a cell must know its current 'key'
      - Base station checks encrypted frame for correctness of 'key', if so, formally associates the station
      - Station is now a regular member of the cell & can communicate through its base station/ access point
      - Base station/ access points do not have to authenticate themselves to new mobile stations (future 802.11 version may include this)
    - Deauthentication
      - A station must request for deauthentication before leaving a cell
      - Base station/ access point responds by removing station from its 'association' list
      - Station can no longer use services of this cell
      - After a deauthentication base station/ access point may change its 'key' – involves appreciable overhead

- Wireless network – 802.11a/b/g Services
  - Station services (cont.)
    - Privacy
      - Data transmitted by wireless (radio) channel can be easily intercepted by third party
      - 802.11 requires all frames to be sent 'over the air' in encrypted form to ensure security/ privacy
      - Encryption done using RC4 algorithm (Ronald Rivest, M.I.T.)
    - Data delivery
      - 802.11 is modeled after Ethernet (802.3) which does not provide 100% reliability
      - 802.11 also does not provide 100% guarantee on frame delivery or accuracy; it's a 'best effort' service
      - Errors not rectified by 802.11 (802.3 as well) are dealt with by higher layer, e.g., Network layer retransmitting packet through different route
  - An 802.11 cell has parameters that can be inspected &, in some cases adjusted
  - Cell parameters relate to encryption, time-out interval, data rate, beacon frequency, station priority adjustment, etc.

- Wireless network – 802.16 broadband wireless N/W (wireless MAN, WLL)
  - Need for a separate standard : 802.11 Vs 802.16
    - Static Vs Mobile
      - 802.16 provides wireless connection to buildings from static base stations
      - Much of 802.3 deals with mobility (both PCF & DCF)
    - Single Vs multiple stations in one location
      - 802.11 stations are usually a single entity – mostly, had held devices
      - Buildings can & do have multiple stations – handled by 802.16
    - Sophisticated high power Vs simple low power transceivers/ radio equipment
      - 802.11 mobile stations keep radio transceivers simple (half – duplex) because of cost/ size constraints, are highly power constrained (battery operated), have limited radio range
      - 802.16 transceivers & other radio equipment usually have non of these constraints; they are sophisticated state-of-the-art systems with full – duplex communication
    - Simple Vs elaborate security/ privacy mechanism
      - 802.11 is essentially for indoor use – an extended wireless 802.3 where perceived security threat level is appreciable lower as compared unrestricted outdoor urban environment
      - 802.16 wireless broadband 'MAN' needs elaborate security mechanism to ensure WEP