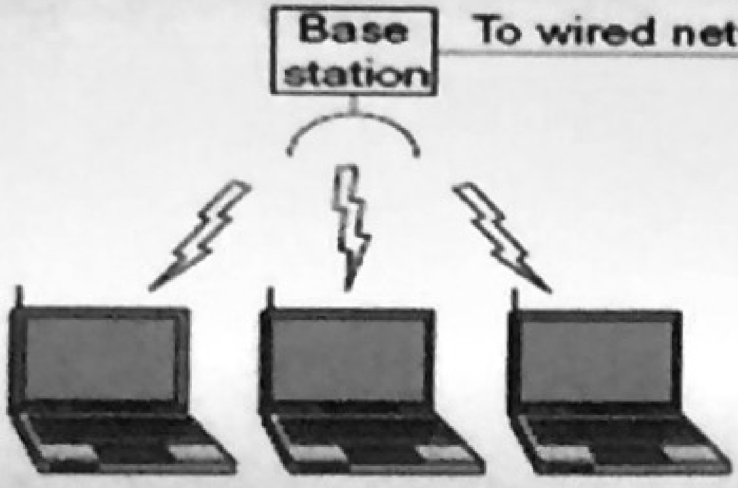
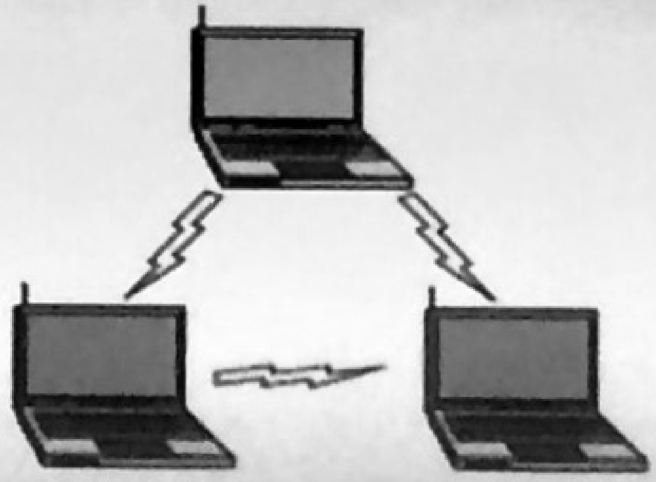
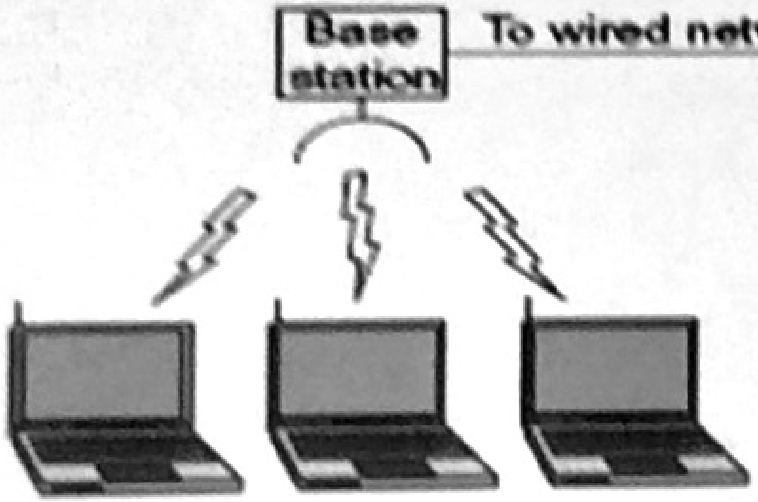
❑ Wireless network – commonly known as WiFi

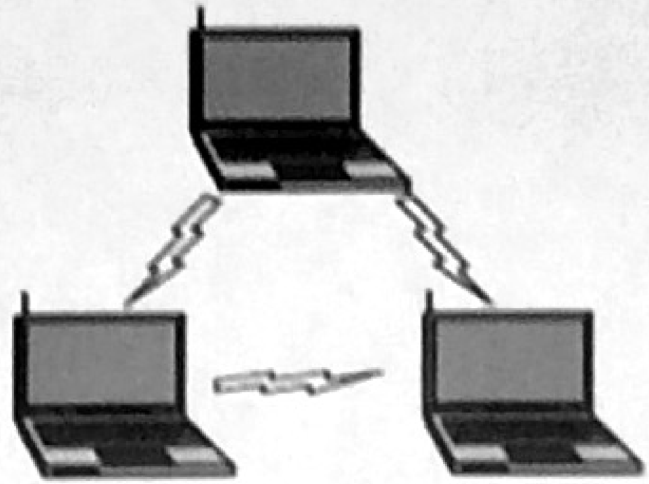




- ➢ Works in two modes
  - In presence of base stations, also called "access points" (cellular n/w)
  - Without base stations/ access points, also called Ad-hoc network
- ➢ Considerations in designing wireless network standard
  - ❖ Choosing a frequency band (carrier frequency & bandwidth) suitable for worldwide use
  - ❖ Dealing with finite range of radio signals
  - ❖ Ensuring user's privacy/ security (WEP – Wired Equivalent Privacy)
  - ❖ Compatibility with existing network technology
    - o IEEE standard 802.11 is designed for total compatibility with Ethernet (802.3) above Data Link (specifically MAC) layer

- Wireless network – commonly known as WiFi

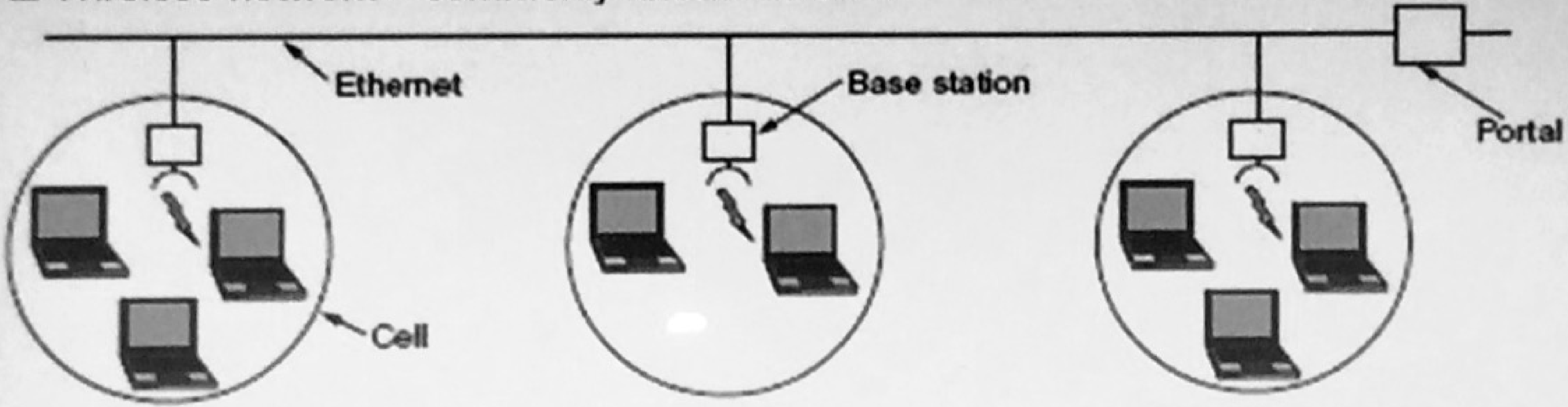




- ➢ Works in two modes
  - In presence of base stations, also called "access points" (cellular n/w)
  - Without base stations/ access points, also called Ad-hoc network
- ➢ Considerations in designing wireless network standard
  - ❖ Choosing a frequency band (carrier frequency & bandwidth) suitable for worldwide use
  - ❖ Dealing with finite range of radio signals
  - ❖ Ensuring user's privacy/ security (WEP – Wired Equivalent Privacy)
  - ❖ Compatibility with existing network technology
    - o IEEE standard 802.11 is designed for total compatibility with Ethernet (802.3) above Data Link (specifically MAC) layer

- Wireless network – commonly known as WiFi
  - Considerations in designing wireless network standard (cont.)
    - Issues/ differences with wired Ethernet specially at the Data Link/ MAC layer
      - CSMA does not work/ is not fool proof
      - Multi-path fading
        - Radio signals are reflected from solid surfaces
        - Signals can be & are usually received multiple times along multiple reflected paths of different lengths
        - Constructive/ destructive interference between multipath signals cause periodic signal strength variation(waxing & waning)
      - Stations are mobile – existing software for Ethernet/ other wired LAN not designed for mobile stations
        - A resource on wired station may no longer be available to a mobile station when it moves away, e.g., a non-networked printer
        - Hand-off
          - A station moves away from range of one base station/access point (a cell) into the range of another one
          - Mechanism is needed for smooth handover from one base station to the other
          - This 'handover' should preferably be transparent to the mobile station

- Wireless network – commonly known as WiFi

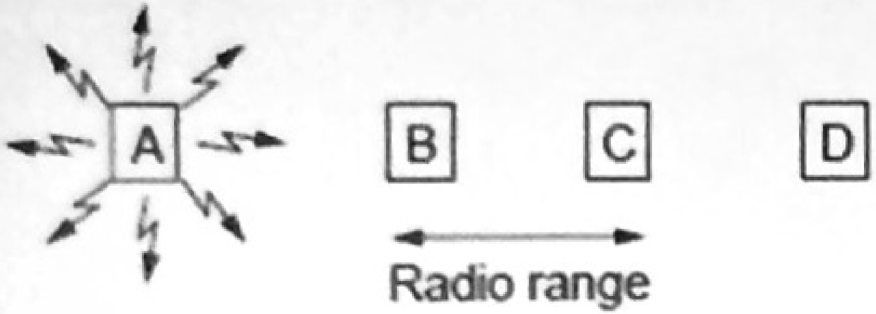


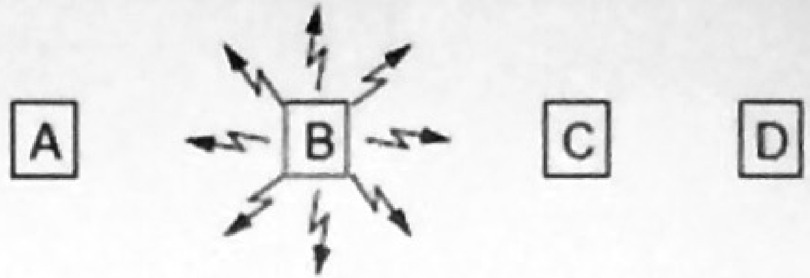
- The IEEE 802.11 wireless protocol works seamlessly with the 802.3 protocol & is designed to make the combined network look like an Ethernet to external world
- Basically a wired Ethernet
  - Several non-mobile stations connected directly to the 'wire'
  - Several non-mobile base stations/ access points connected to the 'wire' via portal (h/w kind)
  - Each access-point forms a cell; cells may be overlapping (ensures smooth hand-off/ unbroken coverage)
  - Mobile stations are within range of at least one cell (maybe more) & are formally associated with one particular cell at any point of time
  - A mobile station communicates with inter-cell, intra-cell & other wired non-mobile stations through the access point of its current cell

- Wireless network – LAN protocols
  - Transmission from a wired Ethernet station is heard by all other fixed stations within at most time τ
  - Transmission from a mobile wireless station may not be heard by another if the two are out of range of each other
  - Simultaneous transmission by two out of range stations to a third station that is within range of both results in collision without any of the transmitting stations being aware; receiving station gets garbled frame

  - Hidden station problem
    - A starts transmitting to B
    - C senses the medium, does not hear A's transmission & assumes it safe to transmit to B
    - C starts transmitting to B. This interferes with transmission from A in the vicinity of B; so frames from A to B, as well as those from C to B get garbled at B
    - A & C do not hear this collision as A's signal does not reach C & C's signal also does not reach A

❑ Wireless network – LAN protocols

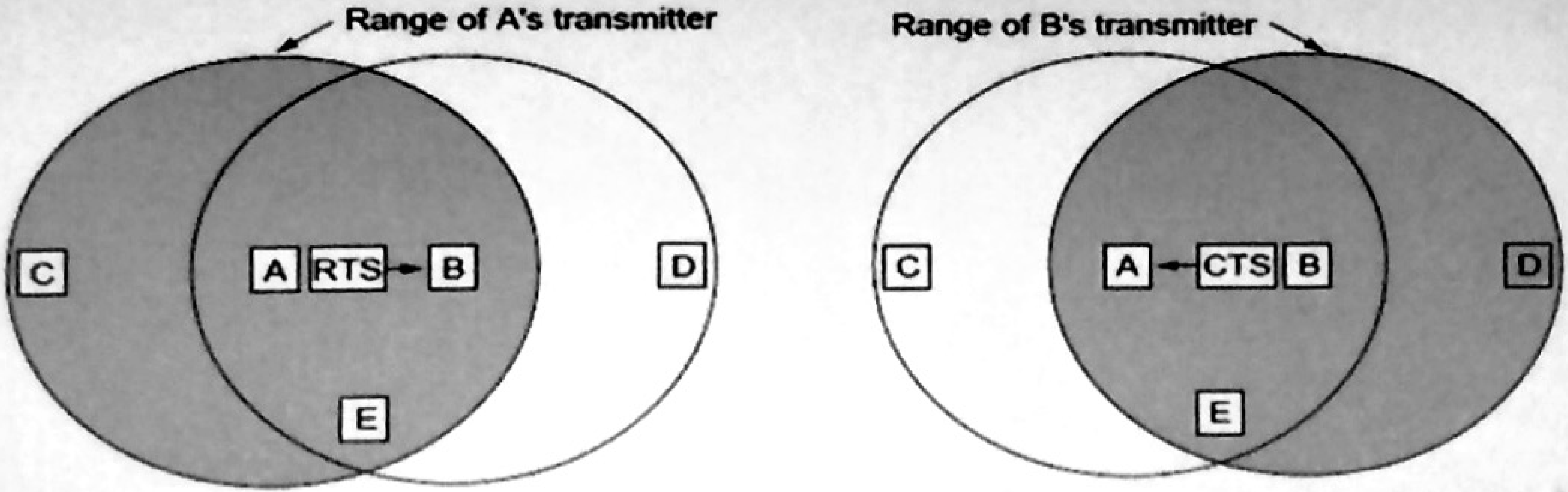




- Exposed station problem
  - B transmits to A
  - C senses the medium and finds that there is an ongoing transmission
  - C concludes (false conclusion) that it is unsafe to transmit, even to D
    - A transmission by C will cause interference in the range between B & C
    - There will be no interference at the receiving stations A or D, since C's signal does not reach A and B's signal does not reach D
- Thus CS does not work effectively here
- In wired Ethernet there can be only one collision free transmission at a time
- In wireless environment there can be multiple simultaneous collision free transmissions
  - All transmissions use same frequency band
  - Each of the multiple transmissions are to different destination stations
  - No destination station is within range of two or more active transmitting stations
  - Two transmitting stations may or may not be within range

❑ Wireless network – LAN protocols

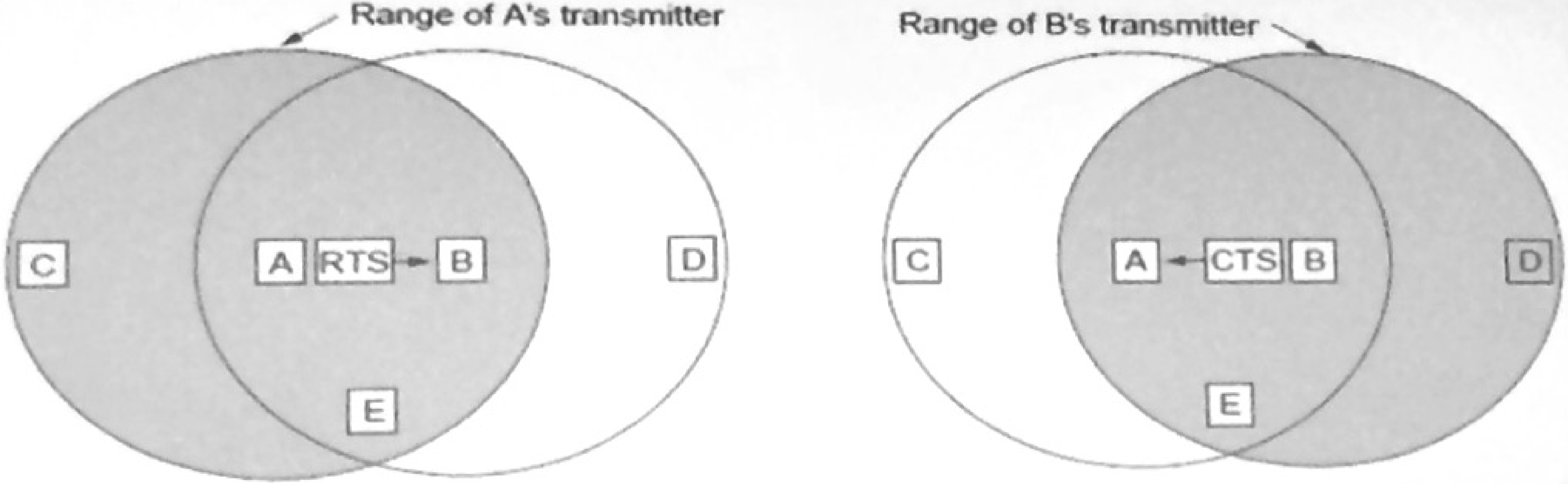
➤ Multiple Access Collision Avoidance (MACA) protocol



➤ A to B transmission

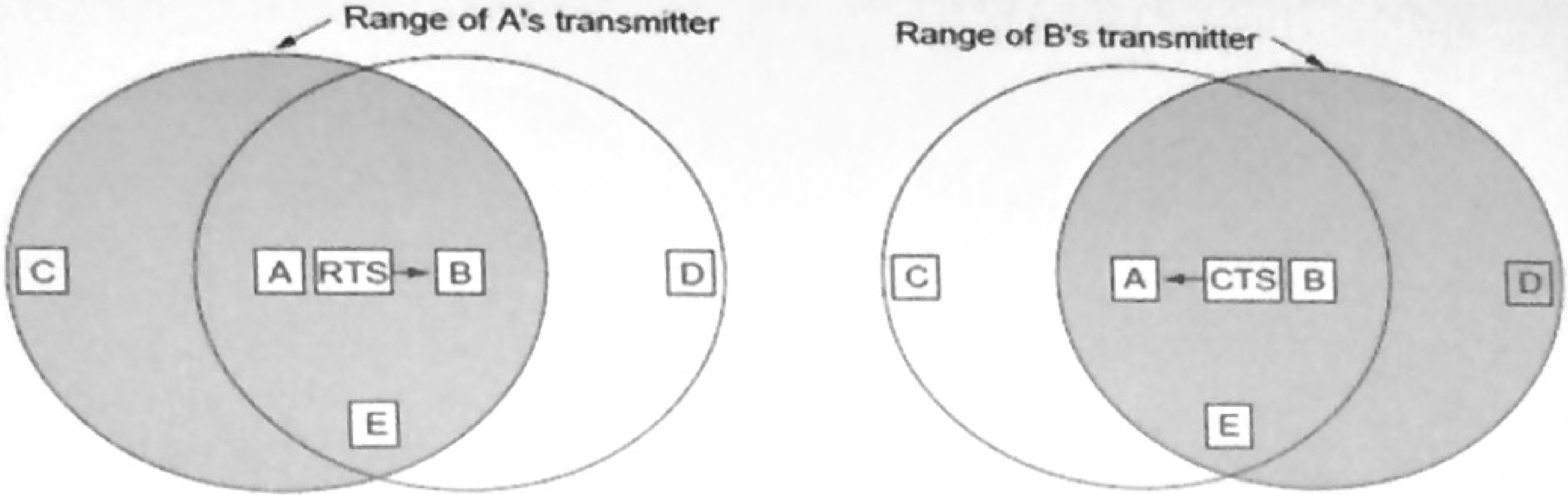
- ❖ A senses medium and transmits Request To Send (RTS) control frame to B
- ❖ RTS heard by all stations in range of A
- ❖ All these stations except B refrain from transmitting for specified time
- ❖ B receives RTS & if ready to receive data frame, sends Clear To Send (CTS) control frame to A
- ❖ All stations in range of B hear this CTS and refrain from transmitting for the duration of anticipated up-comming data frame from A
- ❖ A receives CTS and begins transmitting data frame to B
- ❖ This transmission heard by all stations in A's range
- ❖ Stations in range of A but not B can now transmit if required

- Wireless network – LAN protocols
  - Multiple Access Collision Avoidance (MACA) protocol



- A to B transmission –some observations
  - Station hearing RTS but not CTS is close to transmitter A but out of range of receiver B; it must wait long enough for A to receive CTS & then it can start transmitting to other station
  - Station hearing CTS but not RTS is close to receiver B but out of range of transmitter A; it has to wait until transmission of entire data frame from A (which it cannot hear) is over
  - Station hearing both RTS & CTS is in the range of both A & B and has to remain silent until entire transmission (between A, B) is over; it can hear the entire conversation

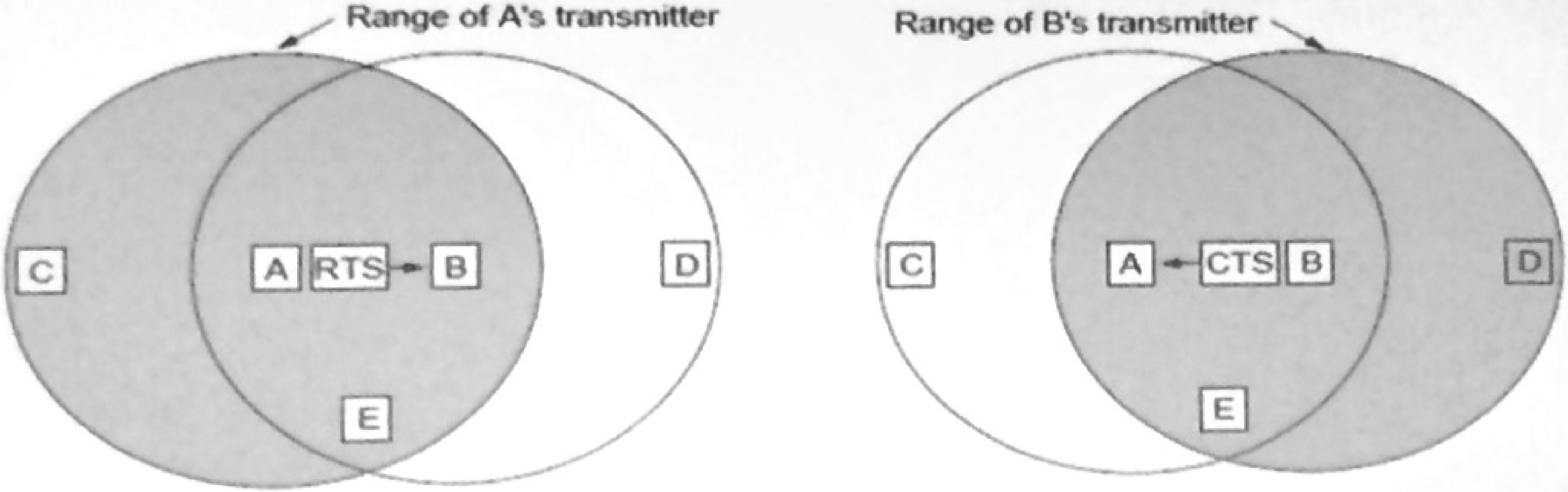
- Wireless network – LAN protocols
  - Multiple Access Collision Avoidance (MACA) protocol



- A to B transmission –some observations (cont.)
  - Collision can still occur, e.g., C and B sense medium at the same time & both send RTS to A
  - Collision occurs at A which receives a garbled frame
  - B & C both wait until time-out for a CTS from A, which ultimately does not arrive
  - B & C now use exponential binary back-off before sending their next RTS to A

❑ Wireless network – LAN protocols

➢ Multiple Access Collision Avoidance for Wireless(MACAW) protocol

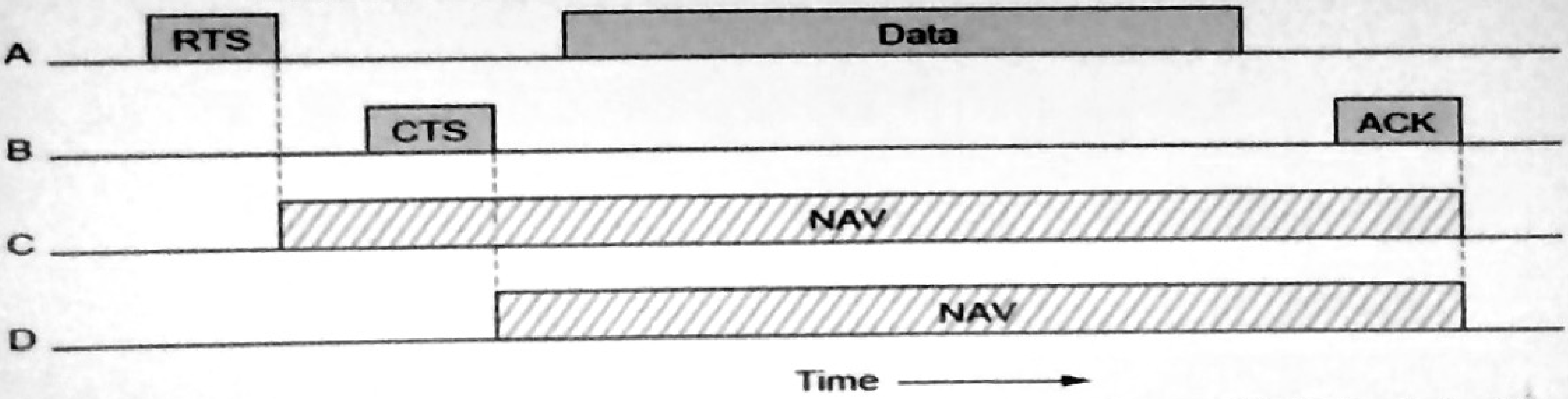


- Improved MACA
- Additional facility for sending Ack. frames form receiver to sender
- Some collisions avoided by providing limited carrier sense capability
  - Stations within range of each other can avoid sending RTS simultaneously to the same station
- Stations exchange congestion information periodically; this allows the exponential binary backoff algorithm to be more effective

- Wireless network – LAN protocols
  - IEEE 802.11 & its variants
  - Original 802.11 had a speed of 1/ 2 Mbps – considered too slow
  - Three new variants
    - 802.11a – uses higher centre frequency & wider bandwidth; effective speed up to 54 Mbps
    - 802.11b – uses same frequency & bandwidth as 802.11 but employs a different modulation technique; effective speed up to 11 Mbps; has a longer range compared to 802.11a
    - 802.11g – uses best of both versions, a & b
      - Frequency band of 802.11a
      - Modulation technique of 802.11b
  - Original 802.11 is possibly slated to die out
  - Operating mode – 802.11a/b/g supports two modes
    - Distributed Coordination Function (DCF)
      - Does not have any form of central control
      - More suited for Ad-hoc networks
      - Has some similarity with wired Ethernet
    - Point Coordination Function (PCF)
      - Uses base stations/ access points to control all intra-cell activities
      - Inter-cell communication is also through their corresponding access points (& wired network to which they are connected)
  - All 802.11a/b/g implementations must support DCF; PCF support is optional

- Wireless network – 802.11a/b/g DCF & PCF
  - DCF uses CSMA/ CA protocol & has two operating methods
    - Physical Channel Sensing
      - Transmitting station senses actual channel, if idle, entire frame is transmitted (collision sensing not attempted; not feasible with single carrier frequency)
      - Collisions can & do happen; sensed by absence of ACK. from receiver till time-out
      - Exponential Binary Back-off or some variant used to retransmit frame in case of collision

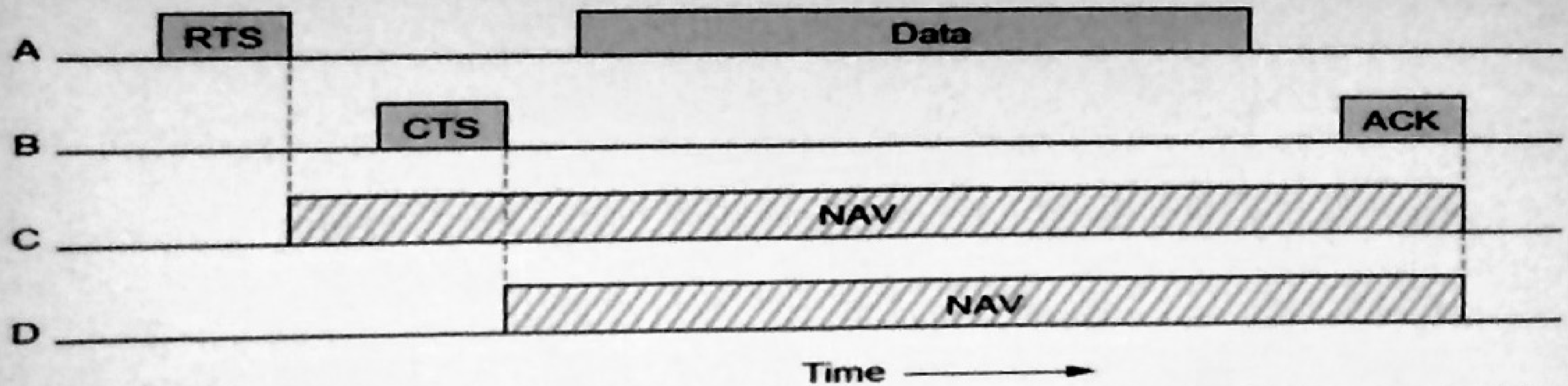
- Wireless network – 802.11a/b/g DCF & PCF
  - DCF uses CSMA/ CA protocol & has two operating methods (cont.)
    - Virtual Channel Sensing
      - Based on MACAW



C within range of A, possibly B also (not important), D within range of B, possibly C also but not A

- A to B data frame transmission
  - A transmits short RTS frame (30 bytes approx) to B; RTS contains info on frame length/ transmission duration
  - B, if free, respond with CTS; frame length/ transmission duration info copied into CTS by B
  - A hears CTS from B; starts transmitting data frame to it; also starts an ACK time-out timer
  - B receives data frame(s) from A; after completion, sends back an ACK to A

- Wireless network – 802.11a/b/g DCF & PCF
  - DCF uses CSMA/ CA protocol & has two operating methods
    - Virtual Channel Sensing (cont.)



C within range of A, possibly B also (not important), D within range of B, possibly C also but not A

- A to B data frame transmission
  - C hears RTS from A & possibly CTS from B as well; generates a time estimate for A to B transmission (end of RTS from A to end of ACK from B)
  - C starts a self imposed 'channel busy'/ 'silence period' for this duration by setting an internal interval/ timer called Network Allocation Vector (NAV)
  - D does not hear RTS from A but does hear CTS FROM B, gets accurate time estimate for period from end of CTS to end of ACK from B
  - D starts self imposed 'channel busy'/ 'silence period' by setting appropriate value for its own NAV
  - NAVs are strictly internal vectors to disable station's transmission for a

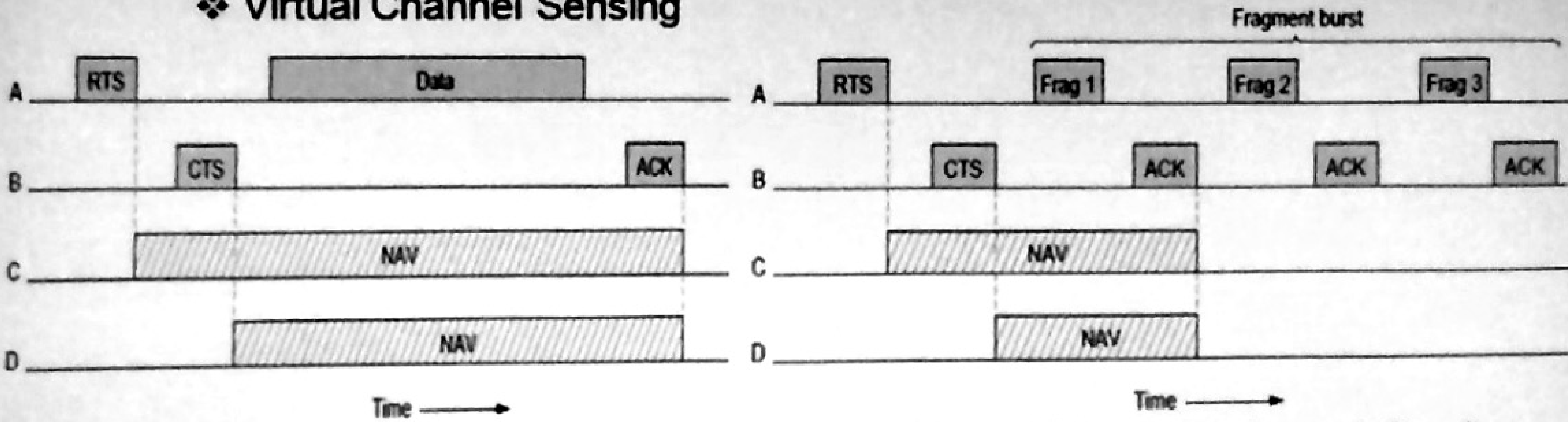
- Wireless network – 802.11a/b/g DCF & PCF
  - DCF uses CSMA/ CA protocol & has two operating methods
    - Virtual Channel Sensing (cont.)
    - General idea
      - Stations hearing RTS but not CTS are within range of transmitter but not receiver; they must wait for transmitter to receive the CTS & then they can transmit to some other station
      - Stations hearing CTS but not RTS are within range of receiver but not transmitter, they must remain silent for entire duration of data transfer including final ACK from receiver
      - Stations hearing both RTS & CTS must remain silent for entire period, i.e., RTS from transmitter to ACK from receiver
    - Wireless networks are very noisy & error prone
      - Let p be the probability of a bit being in error
      - Probability of a n-bit frame received correctly is $(1 - p)^n$
      - Example – A full Ethernet frame (1500 bytes data) is 12144 bits long

        For $p = 10^{-4}$: correctly received frames is < 30%

        $p = 10^{-5}$: about 1 frame in every 9 will have errors

        $p = 10^{-6}$: about 1% damaged frames
    - 802.11 counters problem by allowing frame fragmentation
      - Each fragment has own checksum
      - Fragments individually numbered & acknowledged
      - Simple stop – and – wait protocol used for fragment transmission

- Wireless network – 802.11a/b/g DCF & PCF
  - DCF uses CSMA/ CA protocol & has two operating methods
    - Virtual Channel Sensing



- After acquiring channel through the RTS – CTS mechanism, station A transmits 1st frame fragment, Frag1, to B which sends back an ACK
- Fragment size for different cells may vary; set by cell's access-point
- A , however, does not need to use RTS – CTS again to acquire channel before transmitting next frame fragment
- A keeps transmitting Frag2, ..., Fragn,.known as 'fragment burst' & each frame fragment is acknowledged individually by station B
- NAV mechanism keeps other stations (C & D) silent till the end of ACK for Frag1 from B (as in case on full frame transmission)
- Separate mechanism is used to keep them silent till end of last ACK from station B in response to last fragment in the burst