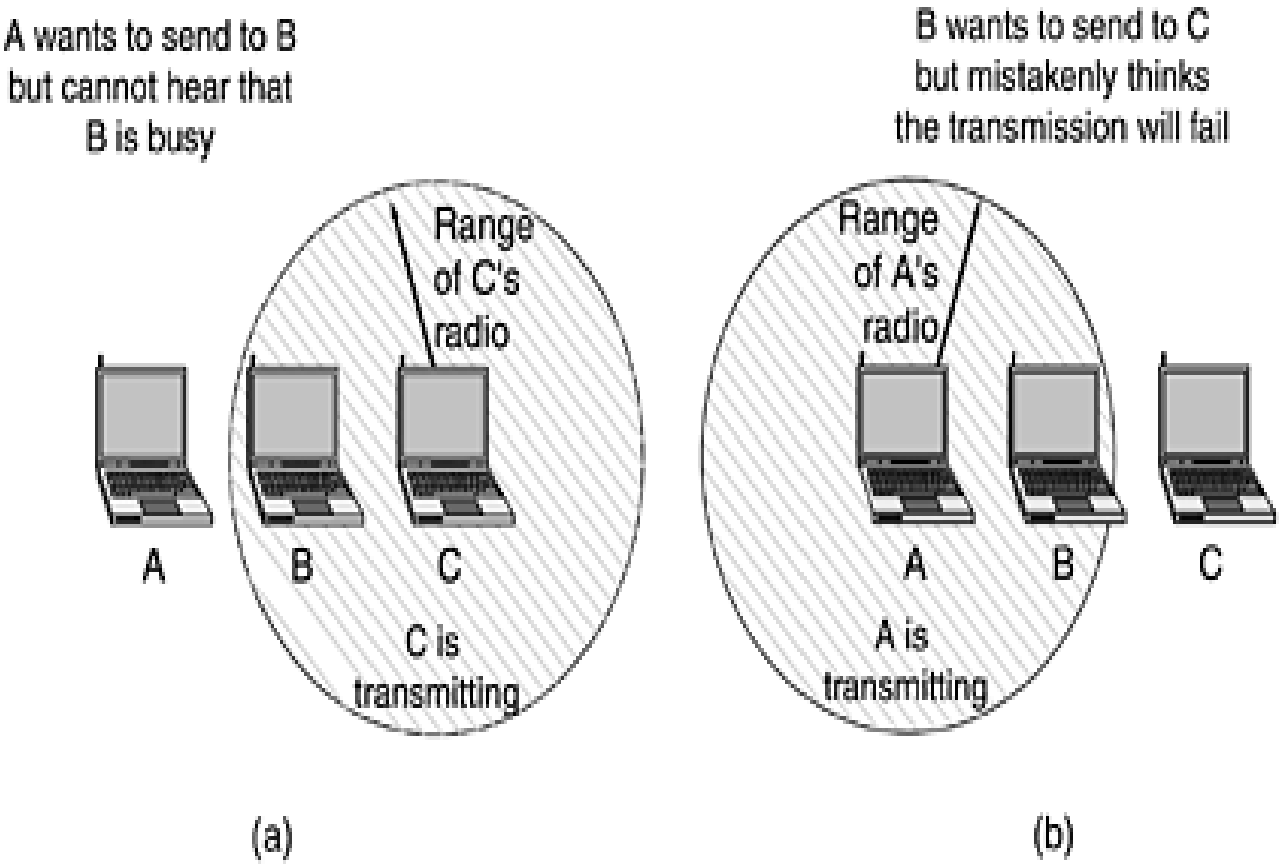
The 802.11 MAC Sublayer Protocol

Figure 4-26. (a) The hidden station problem. (b) The exposed station problem.



- Most radios are half duplex, meaning that they cannot transmit and listen for noise bursts at the same time on a single frequency.
- As a result of these problems, 802.11 does not use CSMA/CD, as Ethernet does.
- To deal with this problem, 802.11 supports two modes of operation:

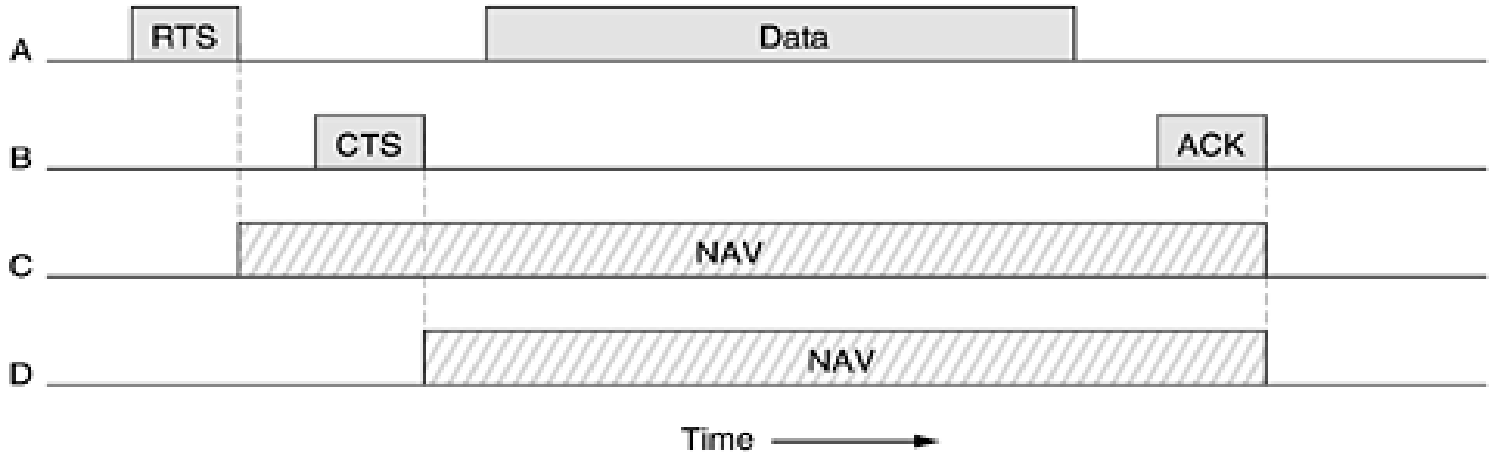
- **DCF** (**Distributed Coordination Function**), does not use any kind of central control
- **PCF** (**Point Coordination Function**), uses the base station to control all activity in its cell.

- All implementations must support DCF but PCF is optional.
- When DCF is employed, 802.11 uses a protocol called **CSMA/CA** (**CSMA with Collision Avoidance**).
- In this protocol, both physical channel sensing and virtual channel sensing are used.
- Two methods of operation are supported by CSMA/CA.

- In the first method, when a station wants to transmit, it senses the channel. If it is idle, it just starts transmitting.
- If the channel is busy, the sender waits until it goes idle and then starts transmitting.
- If a collision occurs, the colliding stations wait a random time, using the Ethernet binary exponential backoff algorithm, and then try again later.
- The other mode of CSMA/CA operation uses **virtual channel sensing.**

- In this example, *A* wants to send to *B*. C is a station within range of *A* . *D* is a station within range of *B* but not within range of *A*.

Figure 4-27. The use of virtual channel sensing using CSMA/CA.

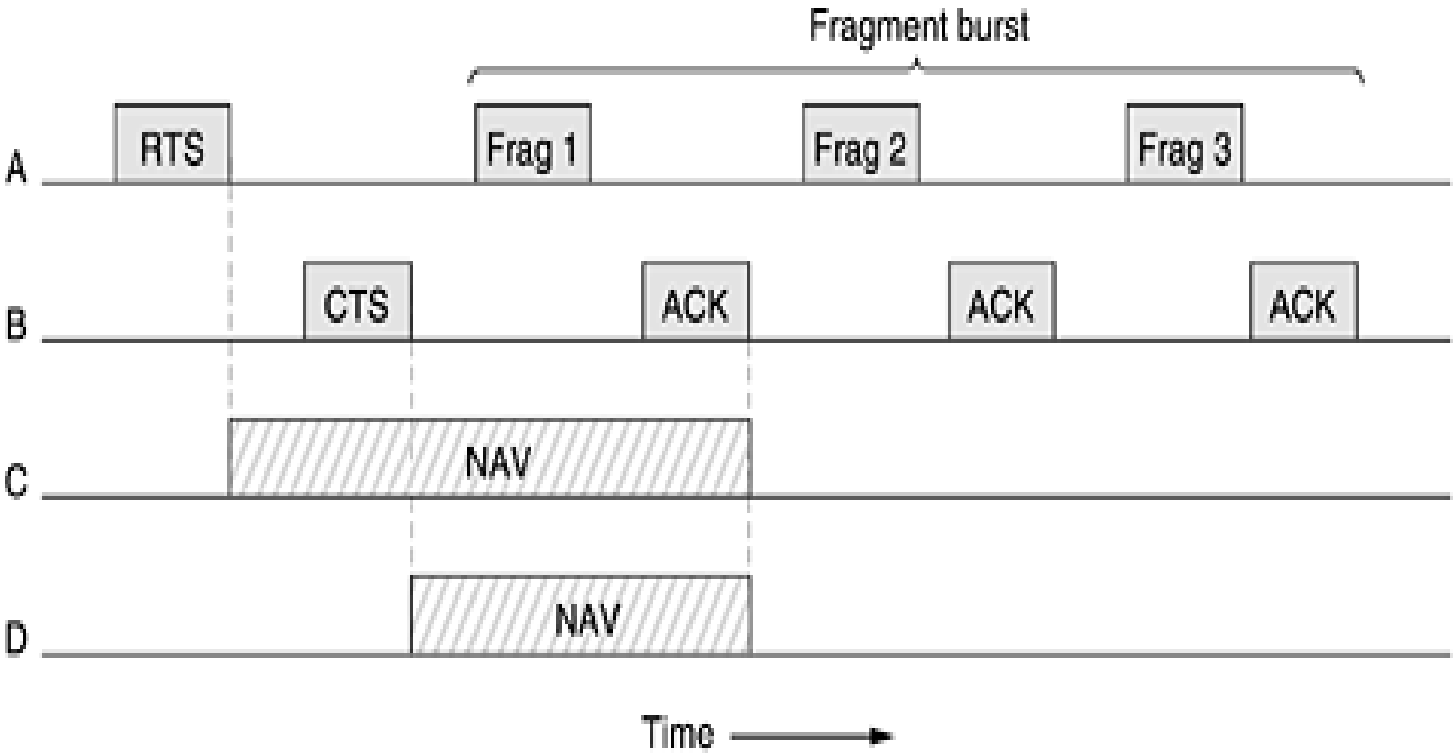


- The protocol starts when *A* decides it wants to send data to *B*. It begins by sending an RTS frame to *B* to request permission to send it a frame.
- When *B* receives this request, it may decide to grant permission, in which case it sends a CTS frame back.
- Upon receipt of the CTS, *A* now sends its frame and starts an ACK timer.
- Upon correct receipt of the data frame, *B* responds with an ACK frame, terminating the exchange.
- If *A*'s ACK timer expires before the ACK gets back to it, the whole protocol is run again.

- Now let us consider this exchange from the viewpoints of *C* and *D*. *C* is within range of *A*, so it may receive the RTS frame. If it does, it realizes that someone is going to send data soon, so for the good of all it desists from transmitting anything until the exchange is completed.
- From the information provided in the RTS request, it can estimate how long the sequence will take, including the final ACK, so it asserts a kind of virtual channel busy for itself, indicated by **NAV** (**Network Allocation Vector**).
- *D* does not hear the RTS, but it does hear the CTS, so it also asserts the *NAV* signal for itself. Note that the *NAV* signals are not transmitted; they are just internal reminders to keep quiet for a certain period of time.

- If a frame is too long, it has very little chance of getting through undamaged and will probably have to be retransmitted.
- To deal with the problem of noisy channels, 802.11 allows frames to be fragmented into smaller pieces, each with its own checksum.
- 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**.

Figure 4-28. A fragment burst.

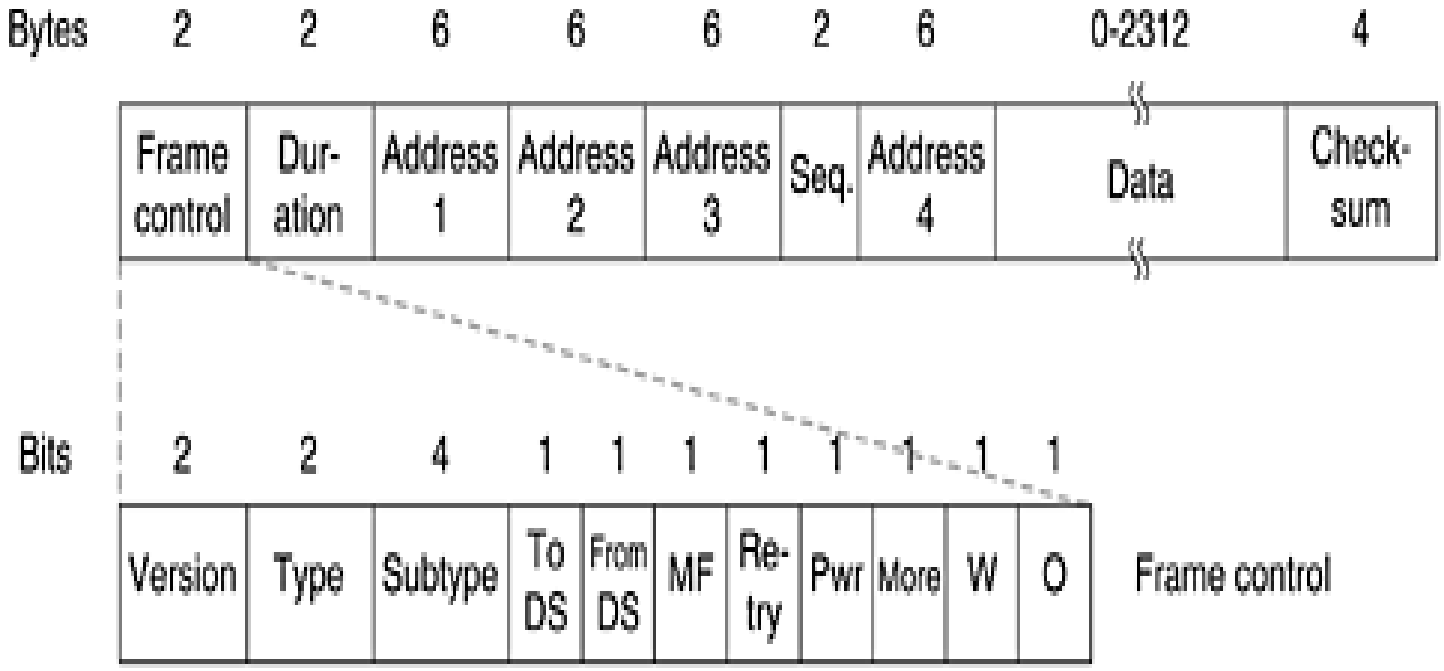


- Fragmentation increases the throughput by restricting retransmissions to the bad fragments rather than the entire frame.
- All of the above discussion applies to the 802.11 DCF(Distributed Coordination Function) mode. In this mode, there is no central control.
- The other allowed mode is PCF (Point Coordination Function), in which the base station polls the other stations, asking them if they have any frames to send.
- Since transmission order is completely controlled by the base station in PCF mode, no collisions ever occur.

The 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.

Figure 4-30. The 802.11 data frame.



- *Frame Control* field: It itself has 11 subfields.
- ***Protocol version*:** The first of these is the *Protocol version*, which allows two versions of the protocol to operate at the same time in the same cell.
- **Type:** data, control, or management
- ***Subtype*** fields (e.g., RTS or CTS).
- ***To DS , From DS :*** The *To DS* and *From DS* bits indicate the frame is going to or coming from the intercell distribution system.
- **MF:** The *MF* bit means that more fragments will follow.

- ***Retry*:** The *Retry* bit marks a retransmission of a frame sent earlier.
- **Pwr:** The *Power management* bit is used by the base station to put the receiver into sleep state or take it out of sleep state.
- **More:** The *More* bit indicates that the sender has additional frames for the receiver.
- **W:** The *W* bit specifies that the frame body has been encrypted using the **WEP** (**Wired Equivalent Privacy**) algorithm.
- **O:** Finally, the *O* bit tells the receiver that a sequence of frames with this bit on must be processed strictly in order.

- ***Duration*:** The second field of the data frame, the *Duration* field, tells how long the frame and its acknowledgement will occupy the channel. This field is also present in the control frames and is how other stations manage the NAV mechanism.
- **Address:** The frame header contains four addresses, all in standard IEEE 802 format.
- The source and destination are obviously needed, but what are the other two for?
- Frames may enter or leave a cell via a base station. The other two addresses are used for the **source** and **destination base stations** for intercell traffic.

- ***Sequence*:** The *Sequence* field allows fragments to be numbered. Of the 16 bits available, 12 identify the frame and 4 identify the fragment.
- ***Data* field:** The *Data* field contains the payload, up to 2312 bytes, followed by *Checksum*.

- **Management frames:** Have a format similar to that of data frames, except without one of the base station addresses, because management frames are restricted to a single cell.
- **Control frames** are shorter still, having only one or two addresses, no *Data* field, and no *Sequence* field. The key information here is in the *Subtype* field, usually RTS, CTS, or ACK.