802.11 MAC

Outline

- Challenges for the MAC
- MAC Access Modes and Timing
- Contention-Based Access Using the DCF
- Fragmentation and Reassembly
- Frame Format
- Encapsulation of Higher-Layer Protocols Within 802.11
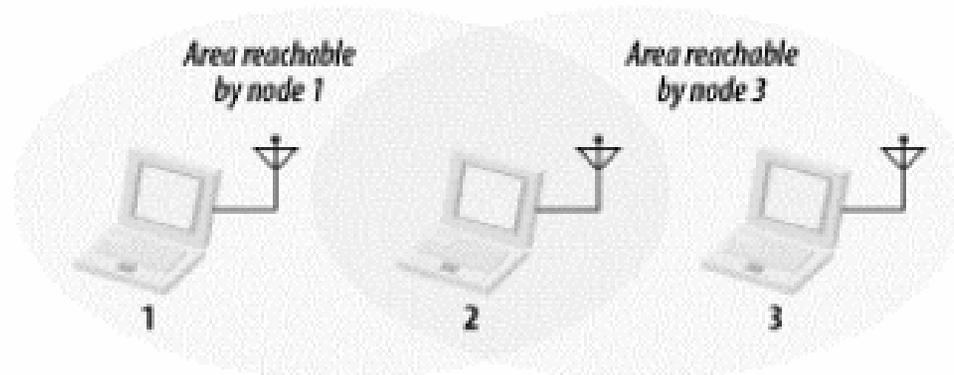- Contention-Based Data Service

Challenges for the MAC

- **RF Link Quality**
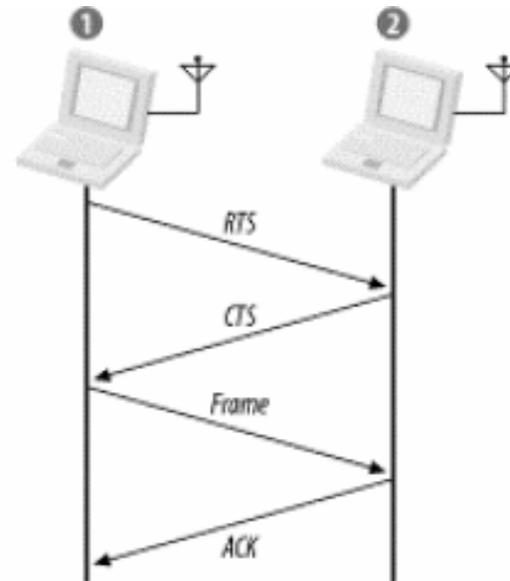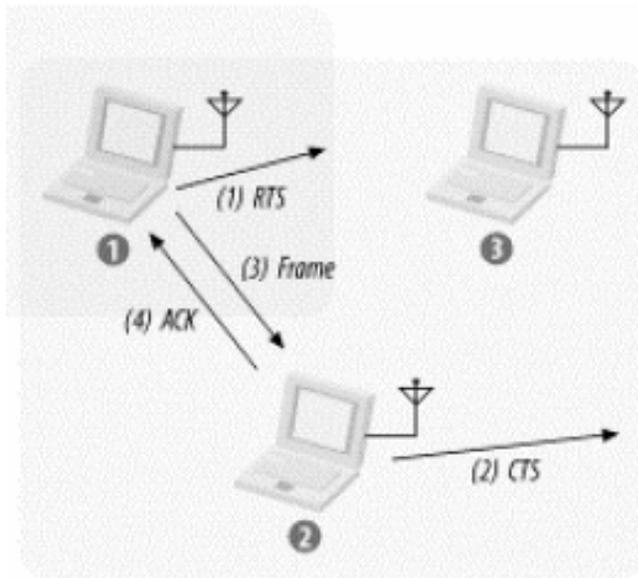 802.11 incorporates positive ACK.
- **The Hidden Node Problem**

Figure 3-2. Nodes 1 and 3 are "hidden"

Area reachable by node 1

Area reachable by node 3

1   2   3

Challenges for the MAC

■ Request to Send (RTS) and Clear to Send (CTS)

MAC Access Modes and Timing

- **DCF (Distributed coordination function)**
  Like Ethernet, it first checks to see that the radio link is clear before transmitting. To avoid collisions, stations use a random backoff after each frame, with the first transmitter seizing the channel.

- **PCF (point coordination function)**
  Point coordination provides contention-free services. Special stations called point coordinators are used to ensure that the medium is provided without contention.

Carrier-Sensing Functions

- Carrier sensing is used to determine if the medium is available.

  - physical carrier-sensing
    provided by the physical layer

  - virtual carrier-sensing
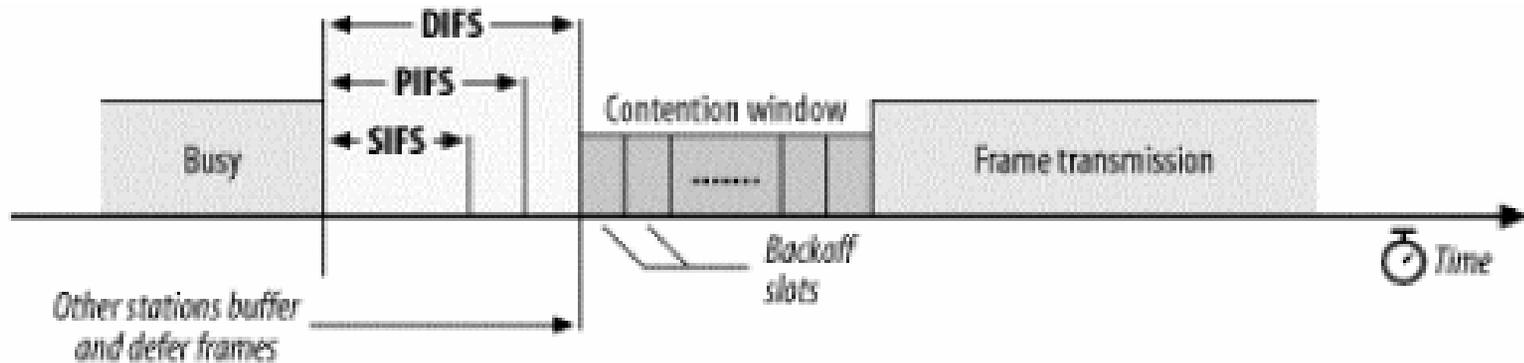   Network Allocation Vector (NAV)

Network Allocation Vector

- 802.11 frames carry a duration field, which can be used to reserve the medium for a fixed time period.

- The NAV is a timer that indicates the amount of time the medium will be reserved.

Network Allocation Vector
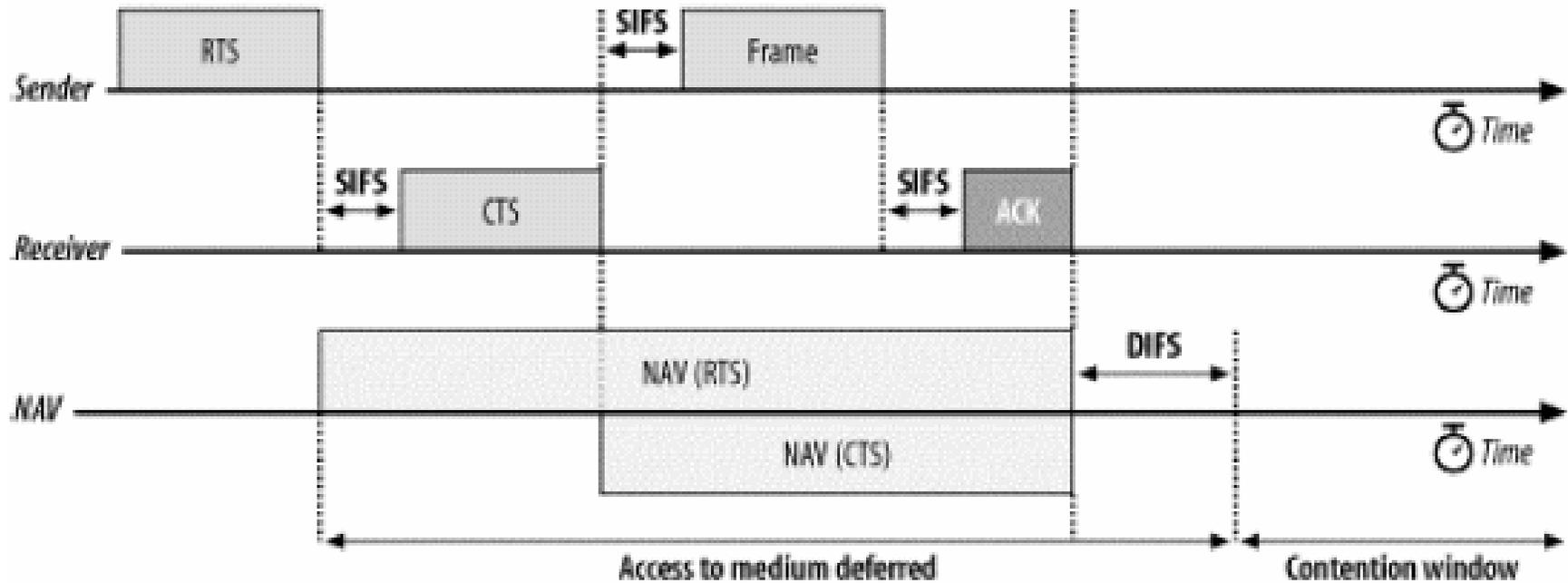
Interframe Spacing

Interframe Spacing

- **Short interframe space (SIFS)**
  - □ The SIFS is used for the highest-priority transmissions, such as RTS/CTS frames and positive ACK.
- **PCF interframe space (PIFS)**
  - □ The PIFS is used by the PCF during contention-free operation.
- **DCF interframe space (DIFS)**
  - □ The DIFS is the minimum medium idle time for contention-based services. Stations may have immediate access to the medium if it has been free for a period longer than the DIFS.
- **Extended interframe space (EIFS)**
  - □ It is used only when there is an error in frame transmission.

Contention-Based Access Using the DCF

■ Basic rules

1. If the medium has been idle for longer than the DIFS, transmission can begin immediately.

2. If the medium is busy, the station must wait for the channel to become idle.

Contention-Based Access Using the DCF

- Additional rules
  - Error recovery is the responsibility of the station sending a frame.
  - The following types of frames can be transmitted after the SIFS and thus receive maximum priority:
    - acknowledgments
    - the CTS in an RTS/CTS exchange sequence
    - fragments in fragment sequences

Contention-Based Access Using the DCF
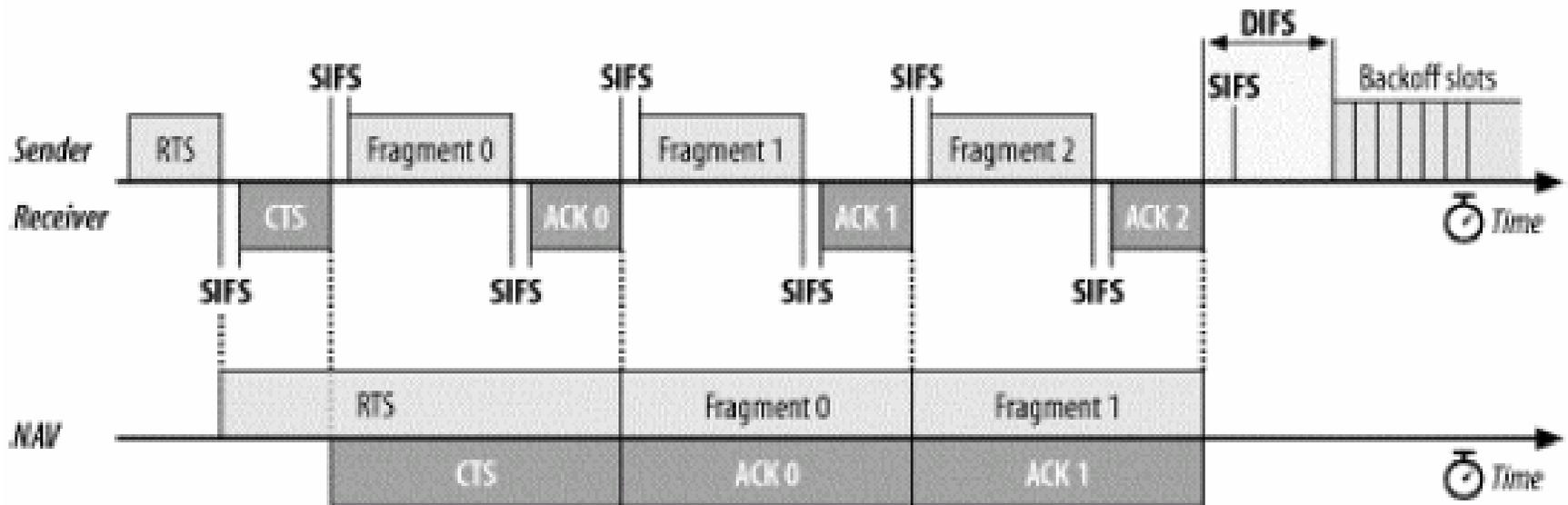
- Additional rules
  - Packets larger than the RTS threshold must have RTS/CTS exchange.
  - Packets larger than the fragmentation threshold must be fragmented.
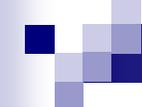
Fragmentation and Reassembly

- Fragmentation takes place when a higher-level packet's length exceeds the fragmentation threshold

- Fragments all have the same frame sequence number but have ascending fragment numbers to aid in reassembly.

- Frame control information also indicates whether more fragments are coming.
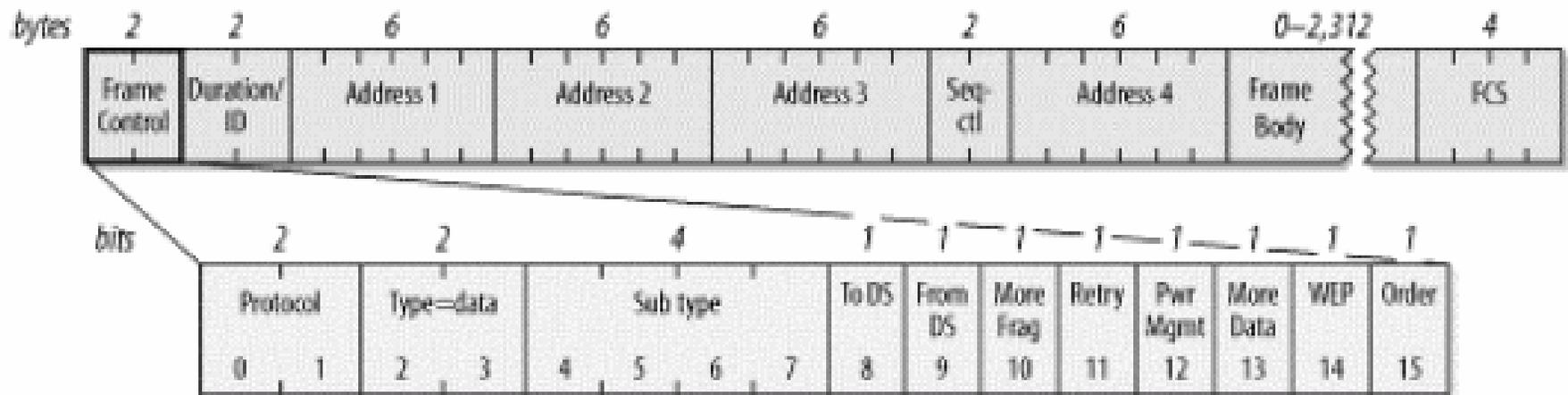
Fragmentation and Reassembly

Frame Format

Figure 3-9. Generic 802.11 MAC frame

2	2	6	6	6	2	6	0–2,312	4
Frame Control	Duration/ID	Address 1	Address 2	Address 3	Seq-ctl	Address 4	Frame Body	FCS

Frame Control

bytes	2	2	6	6	6	2	6	0–2,312	4
	Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Seq-ctl	Address 4	Frame Body	FCS

bits	2	2	4	1	1	1	1	1	1	1	1
	Protocol	Type=data	Sub type	To DS	From DS	More Frag	Retry	Pwr Mgmt	More Data	WEP	Order
	0 1	2 3	4 5 6 7	8	9	10	11	12	13	14	15

Frame Control

- Protocol version

- Type and subtype fields

- ToDS and FromDS bits
 - These bits indicate whether a frame is destined for the distribution system.

Frame Control

	ToDS=0	ToDS=1
FromDS=0	■All management and control frames ■Data frames within an IBSS	■Data frames transmitted from a wireless station in an infrastructure network
FromDS=1	■Data frames received for a wireless station in an infrastructure network	■Data frames on a "wireless bridge"

Frame Control

- *More fragments bit*
- *Retry bit*
- *Power management bit*
- *More data bit*
- *WEP bit*
- *Order bit*

Duration/ID Field
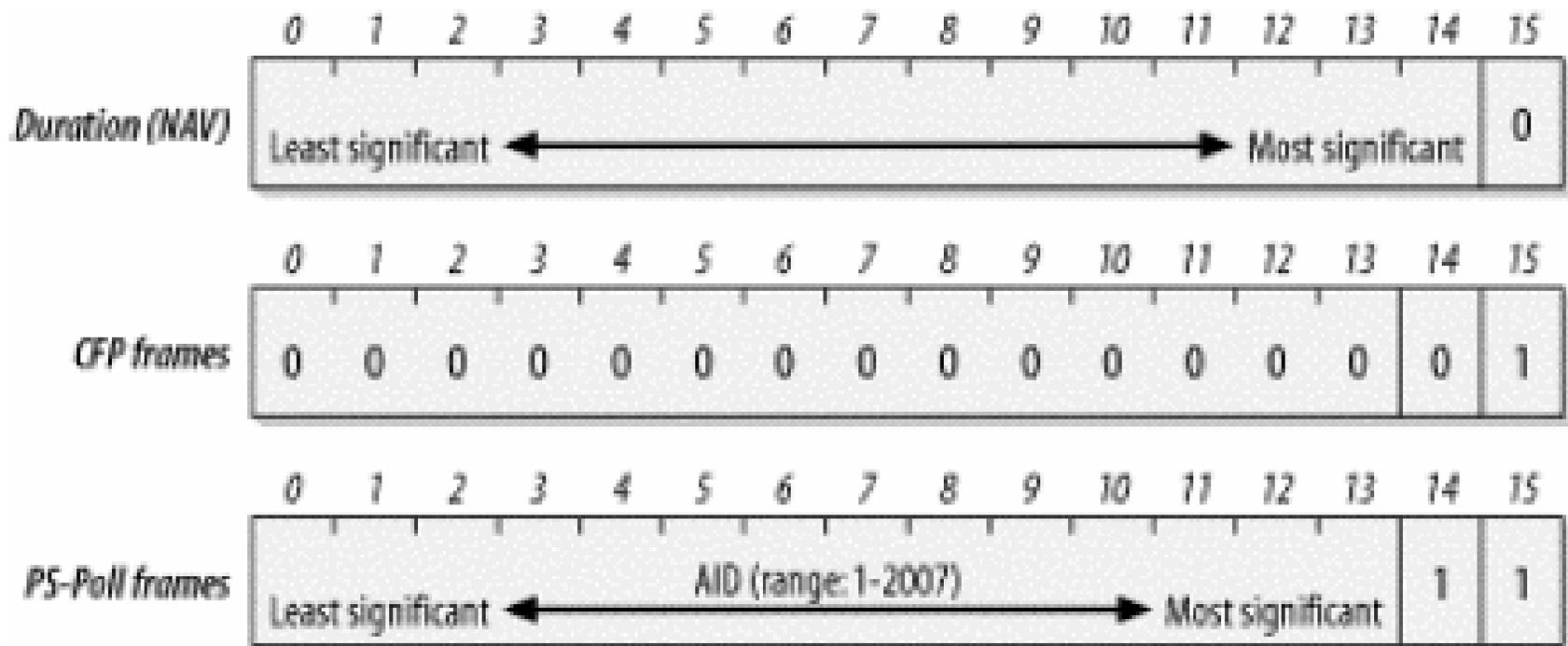
Duration/ID Field

- **NAV**
  When bit 15 is 0, the duration/ID field is used to set the NAV.

- **CFP**
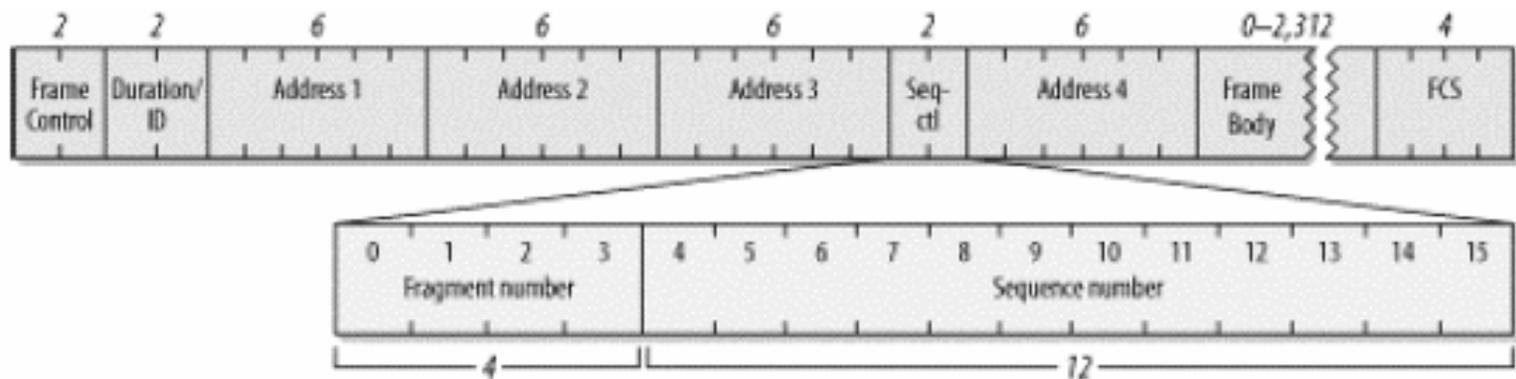 Duration/ID field takes a value of 32,768. This value is interpreted as a NAV.

- **PS-Poll**
  Stations awaking from their slumber transmit a PS-Poll frame to retrieve any buffered frames from the access point.

Address Fields

- *Destination address*
- *Source address*
- *Receiver address*
- *Transmitter address*
- *Basic Service Set ID (BSSID)*

Sequence Control Field

Frame Body

- 802.11 can transmit frames with a maximum payload of 2,304 bytes of higher level data.

- 802.2 LLC headers use 8 bytes for a maximum network protocol payload of 2,296 bytes.

Frame Check Sequence

- As with Ethernet, the 802.11 frame closes with a frame check sequence (FCS).

- The FCS is often referred to as the CRC because of the underlying mathematical operations.

Encapsulation of Higher-Layer Protocols Within 802.11

- Two different methods can be used to encapsulate LLC data for transmission
  - RFC 1042
  - 802.1h
- Both RFC 1042 and 802.1h are derivatives of 802.2's *sub-network access protocol* (SNAP).

Encapsulation of Higher-Layer Protocols Within 802.11
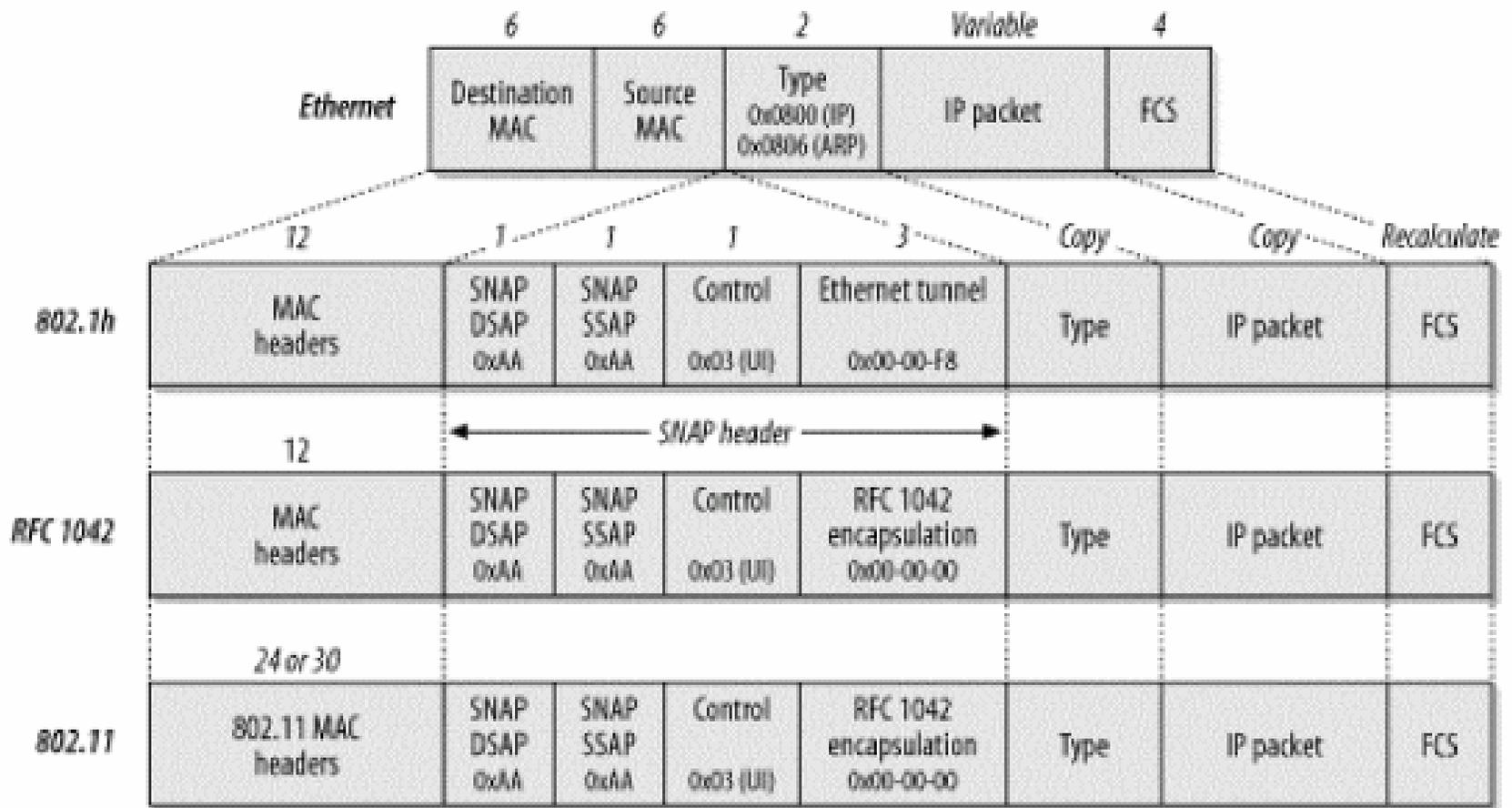
Encapsulation of Higher-Layer Protocols Within 802.11

- SNAP Header
  - *Destination Service Access Point* (DSAP)
  - *Source Service Access Point* (SSAP)
  - Control   Set to 0x03 to denote unnumbered information
  - Organizationally Unique Identifier (OUI)
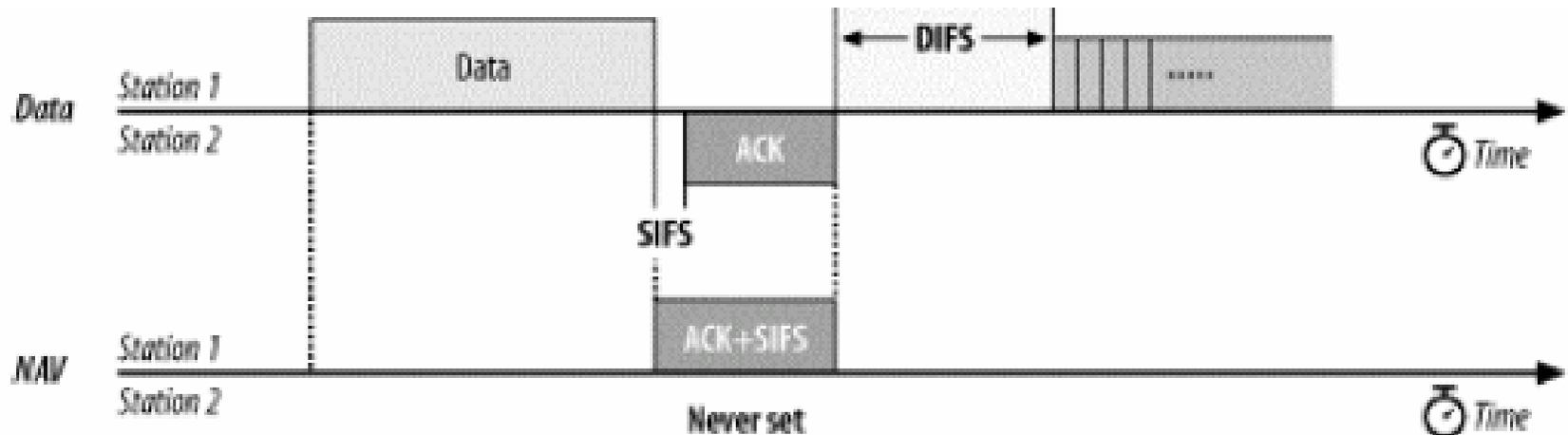
Contention-Based Data Service

- atomic exchanges that move data on an 802.11 LAN.
  - □ Broadcast and Multicast Data or Management Frames
  - □ Unicast Frames
  - □ Power-Saving Sequences

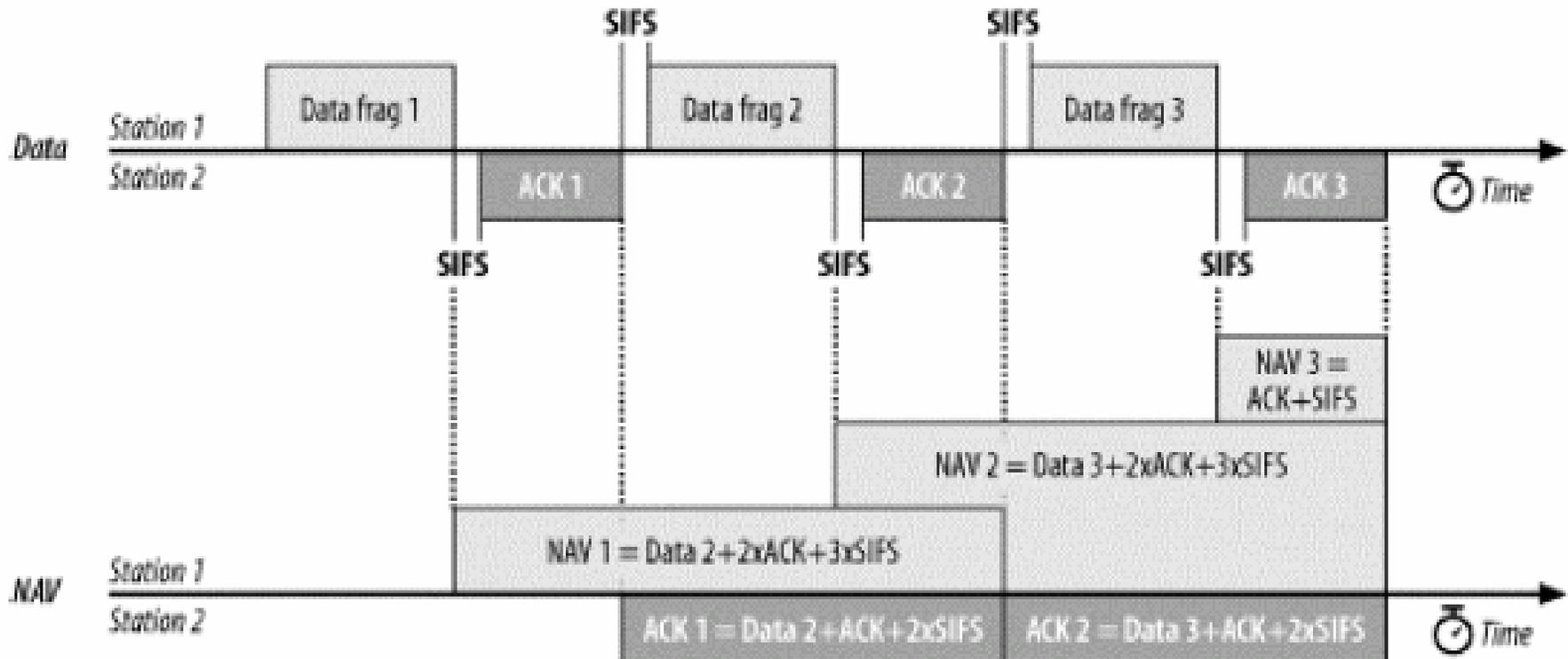# Broadcast and Multicast Data or Management Frames
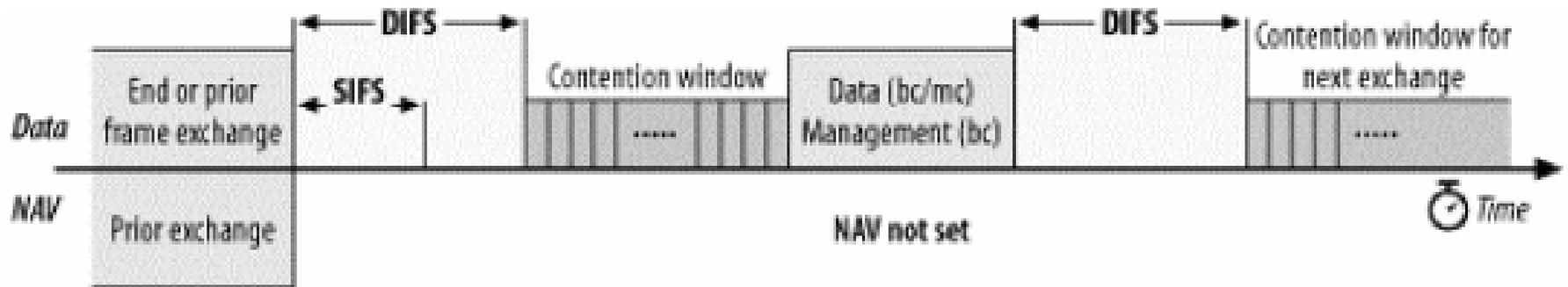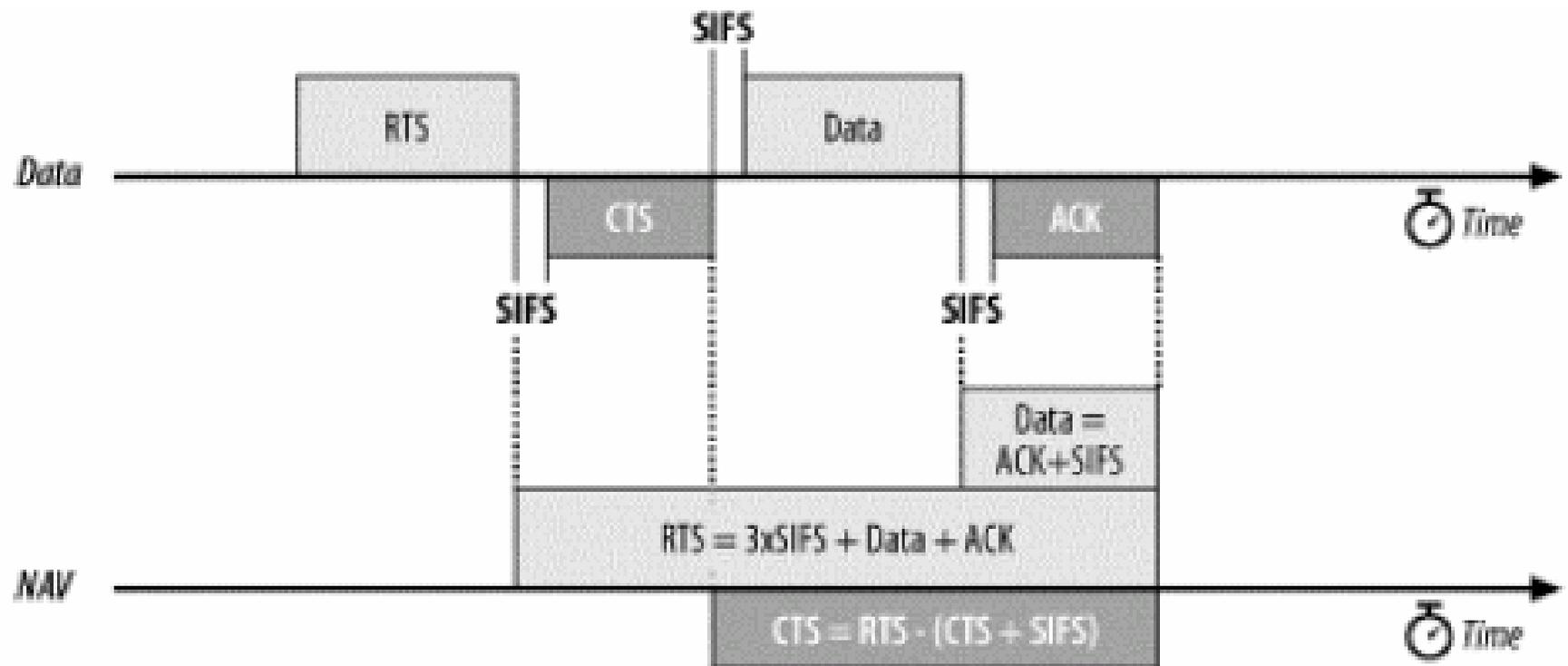
Unicast Frames

- **Basic positive acknowledgment**

Unicast Frames

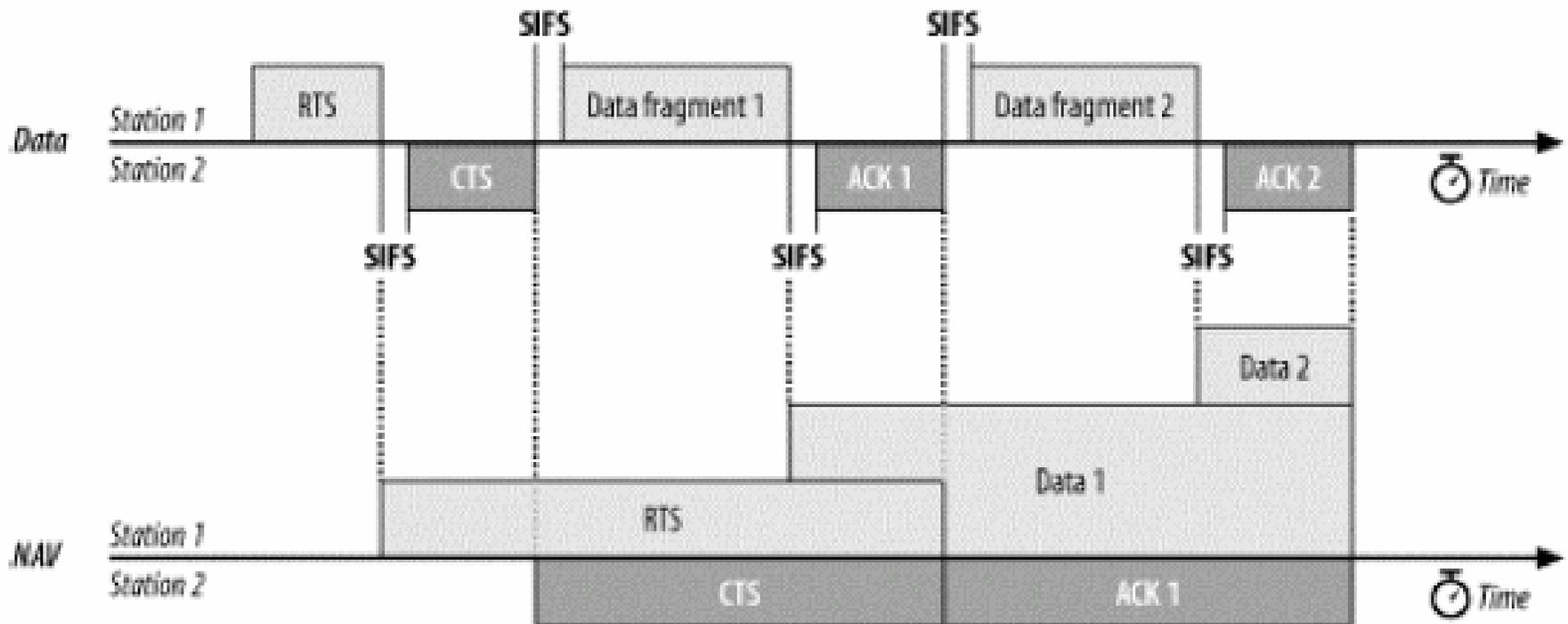■ **Fragmentation**
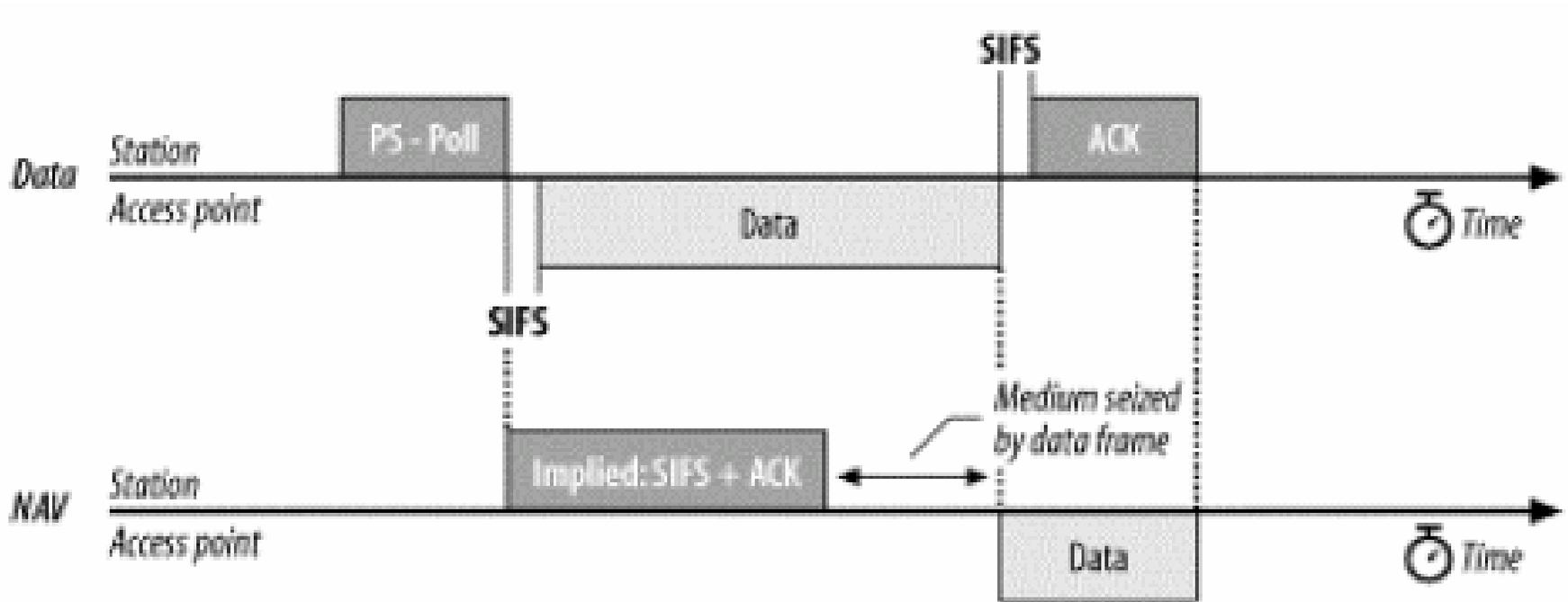
Unicast Frames

- **RTS/CTS**

Unicast Frames

- **RTS/CTS with fragmentation**

Power-Saving Sequences

■ **Immediate response**

Power-Saving Sequences

- **Deferred response**