802.11 Framing in Detail

Outline

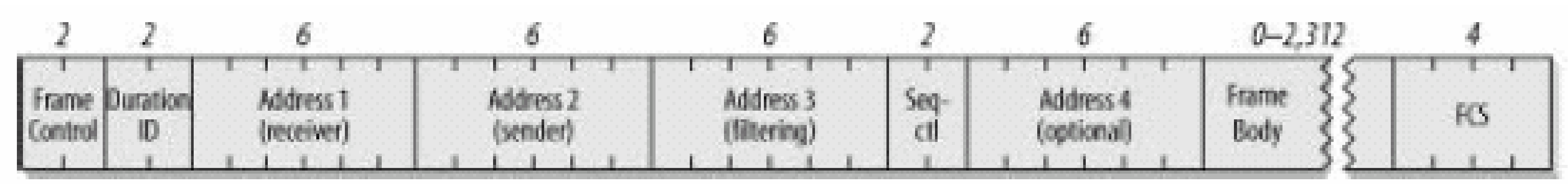
- Introduction
- Data Frames
- Control Frames
- Management Frames
- Frame Transmission and Association and Authentication States

Introduction

- Three major frame types exist：
  - Data frames are the pack horses of 802.11
    - hauling data from station to station.
  - Control frames are used in conjunction with data frames to perform：
    - area clearing operations
    - channel acquisition
    - carrier-sensing maintenance functions
    - positive acknowledgment of received data
  - Management frames perform supervisory functions：
    - join and leave wireless networks
    - move associations from access point to access point.

Data Frames

- Data frames carry higher-level protocol data in the frame body.



Duration

- The Duration field carries the value of the (NAV). Four rules：
  1. Contention-free period：Duration = 32768
  2. Frames transmitted to a broadcast or multicast destination have a duration of 0.
  3. If the More Fragments bit is 0, Duration = SIFS+ACK
  4. If the More Fragments bit is1, Duration = fragment+3xSIFS+2xACK

Addressing and DS Bits

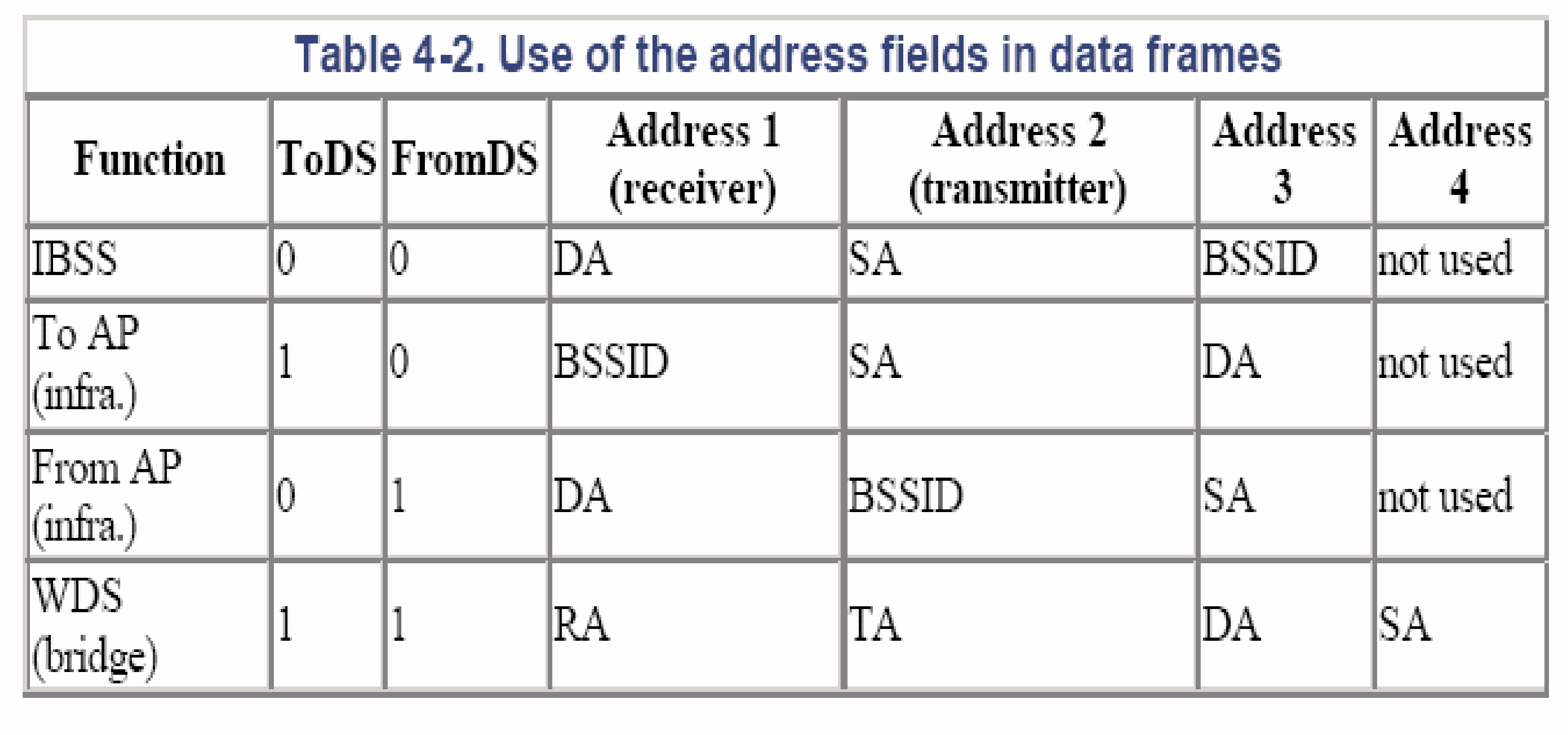
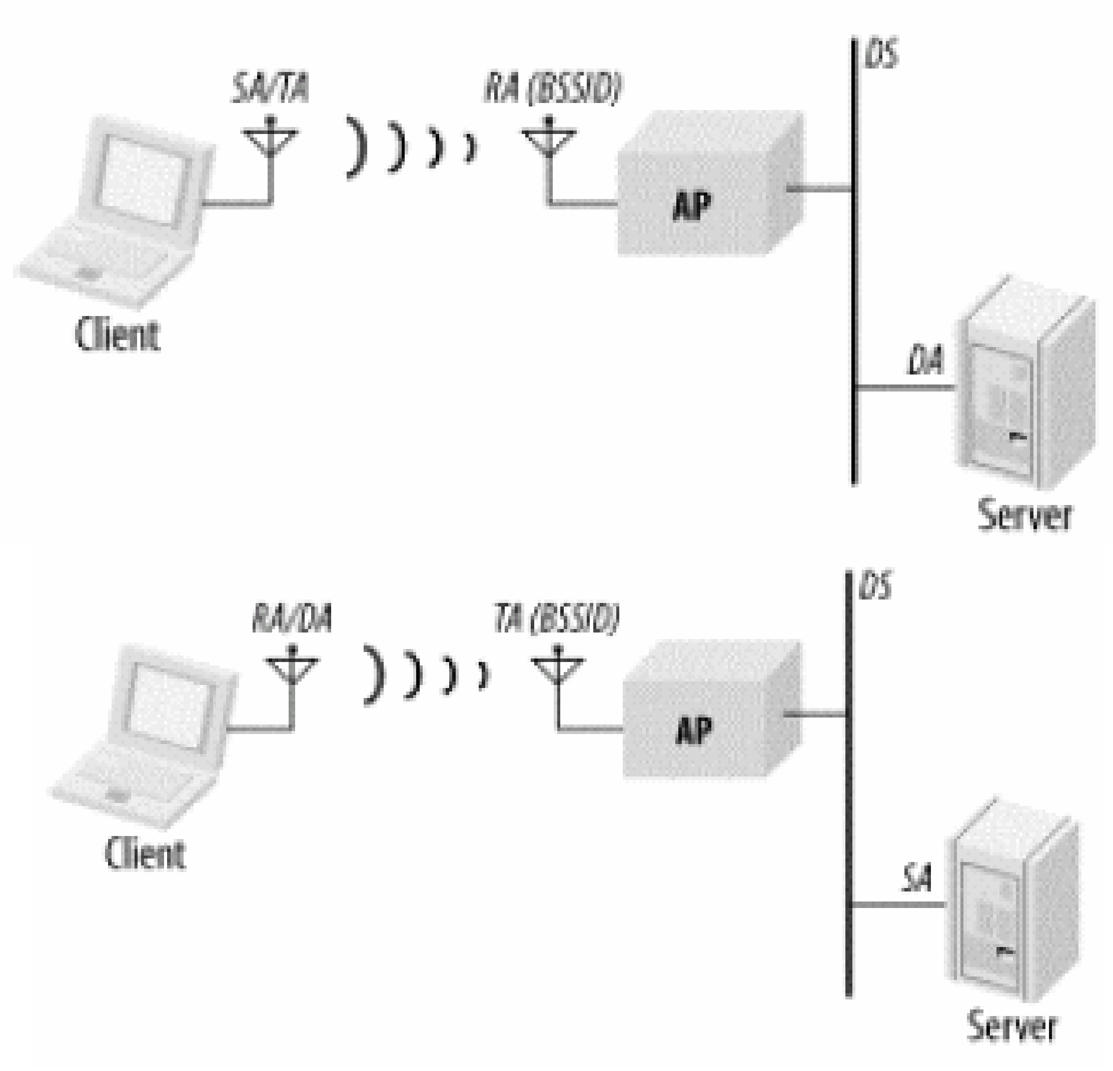


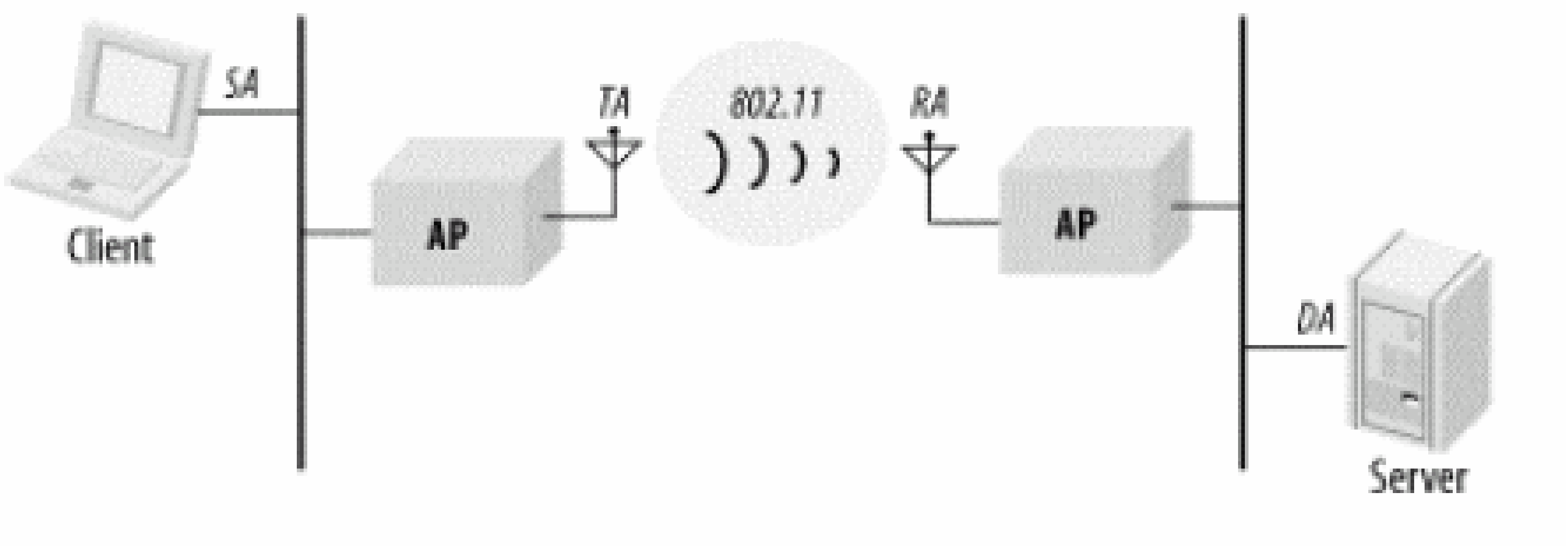
Table 4-2. Use of the address fields in data frames

Function	ToDS	FromDS	Address 1 (receiver)	Address 2 (transmitter)	Address 3	Address 4
IBSS	0	0	DA	SA	BSSID	not used
To AP (infra.)	1	0	BSSID	SA	DA	not used
From AP (infra.)	0	1	DA	BSSID	SA	not used
WDS (bridge)	1	1	RA	TA	DA	SA

Addressing and DS Bits

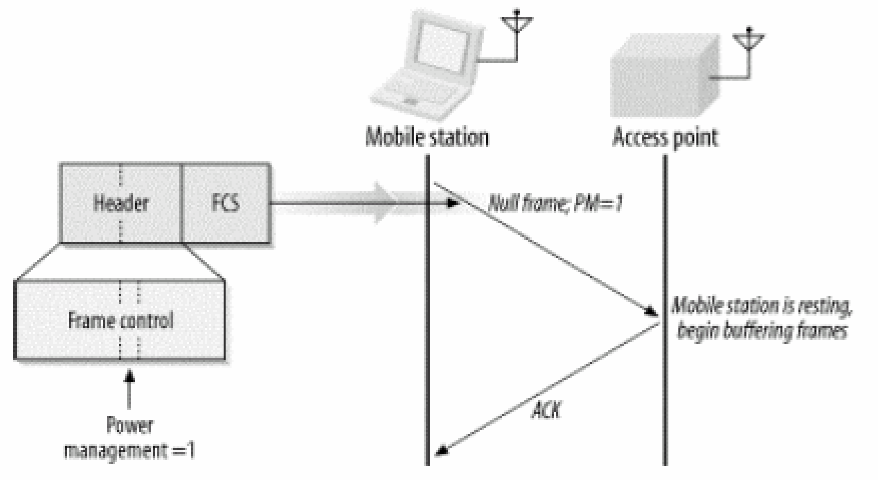


Addressing and DS Bits

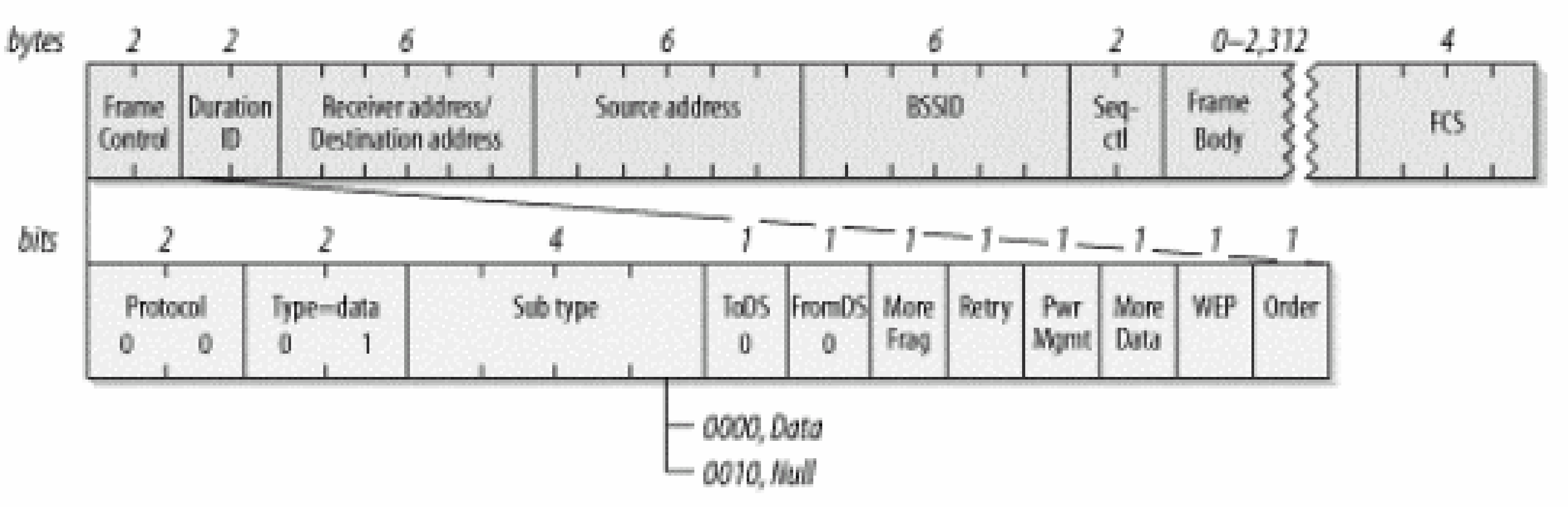


Type on the Data Frame

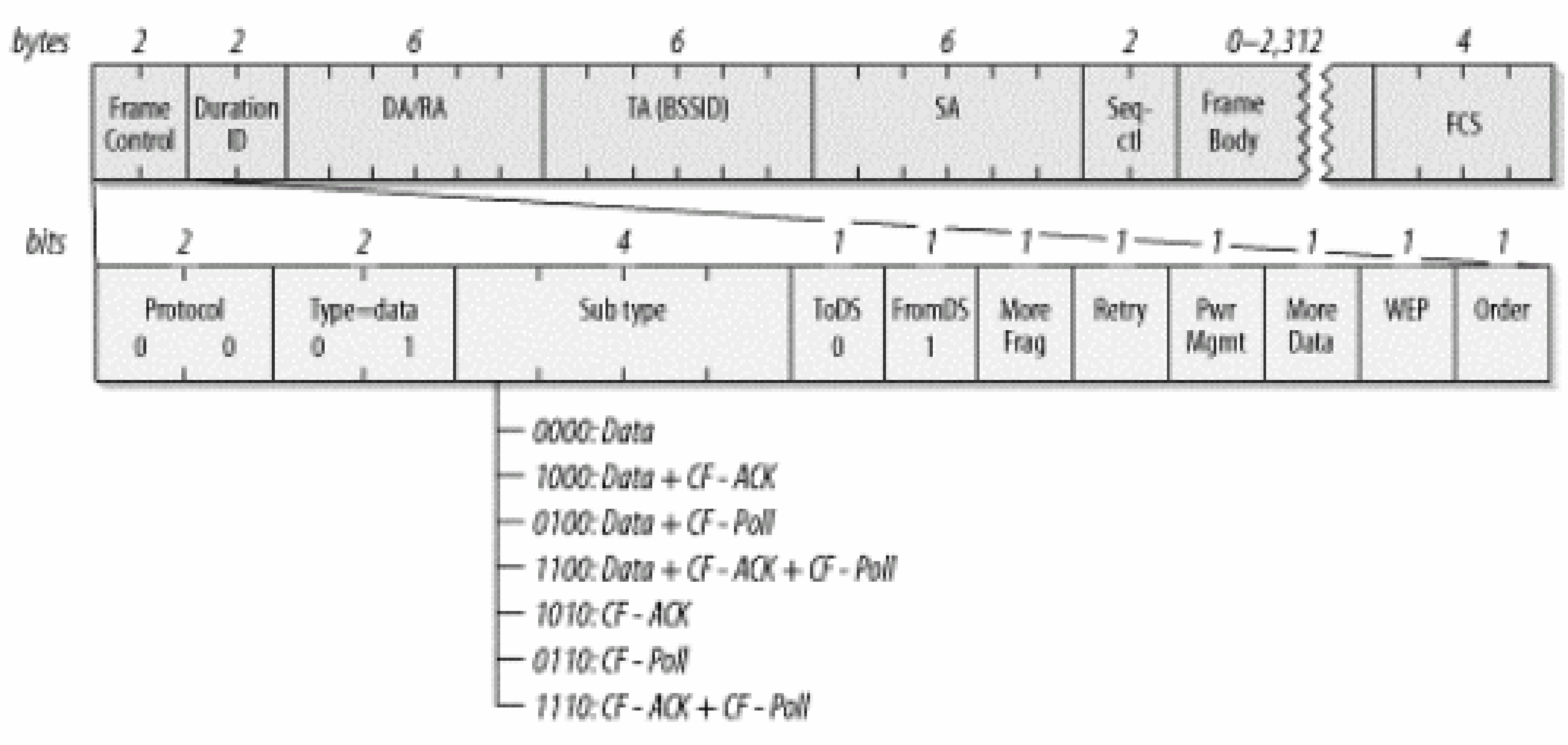
- Data：
  Moving the frame body from one station to another.
- Null：
  They consist of a MAC header followed by the FCS trailer.



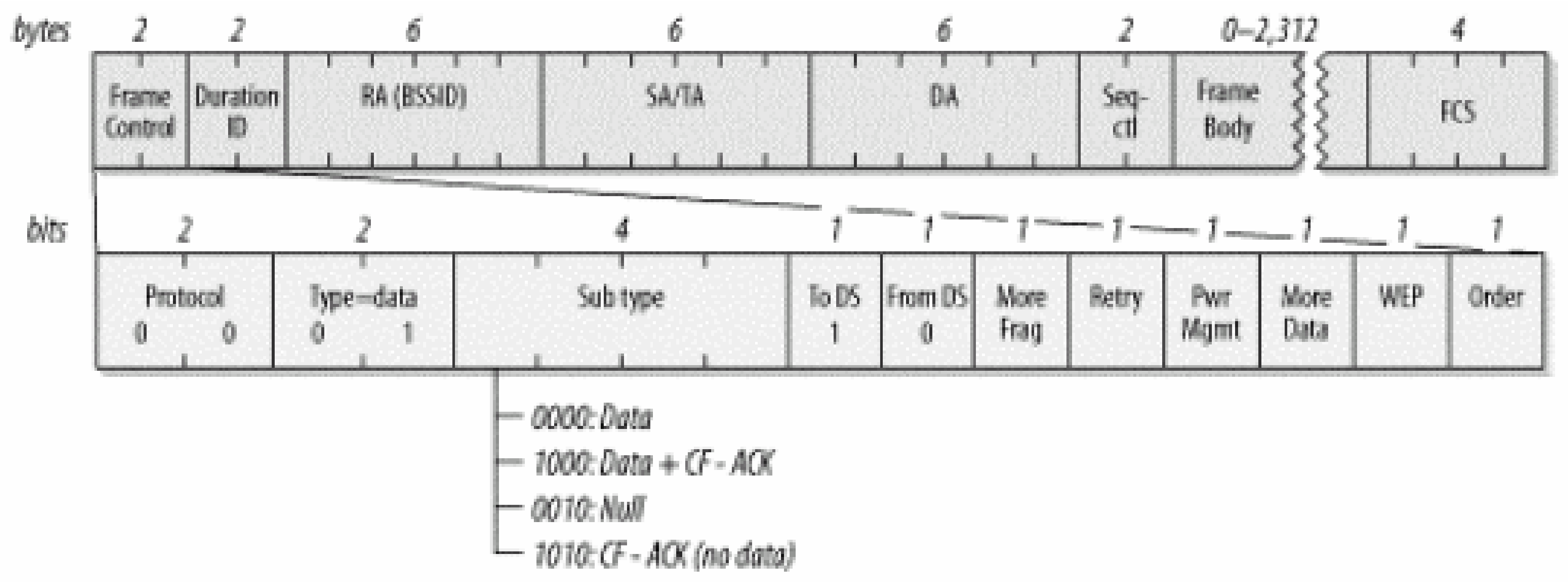
IBSS frames


bytes
2
2
6
6
6
2
0–2,312
4
Frame Control
Duration ID
Receiver address/ Destination address
Source address
BSSID
Seq-ctl
Frame Body
FCS
bits
2
2
4
1
1
1
1
1
1
1
1
Protocol
0 0
Type=data
0 1
Sub type
ToDS
0
FromDS
0
More Frag
Retry
Pwr Mgmt
More Data
WEP
Order
0000, Data
0010, Null

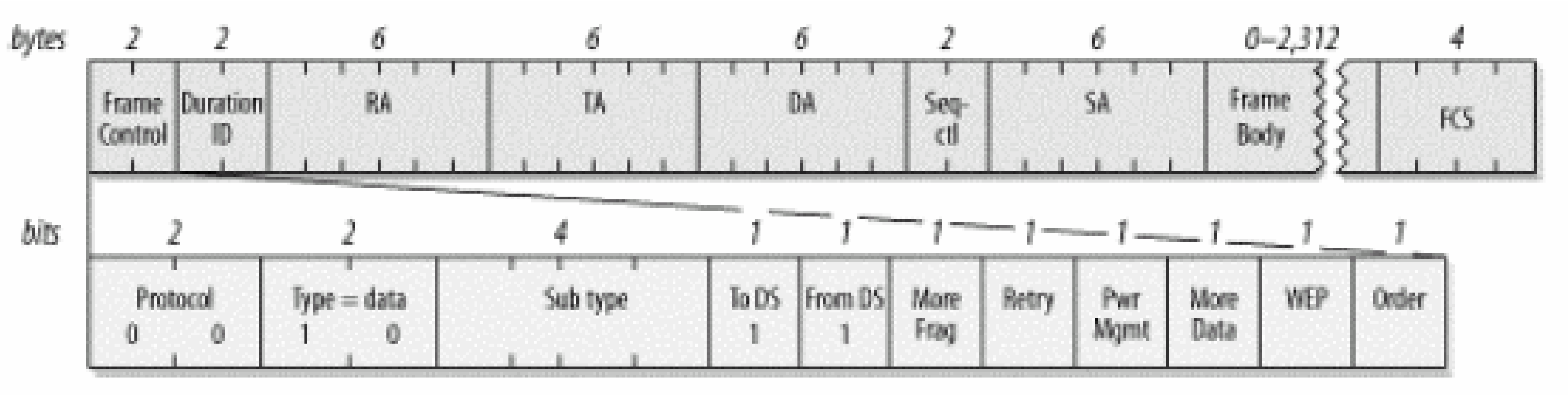
Frames from the AP



Frames to the AP

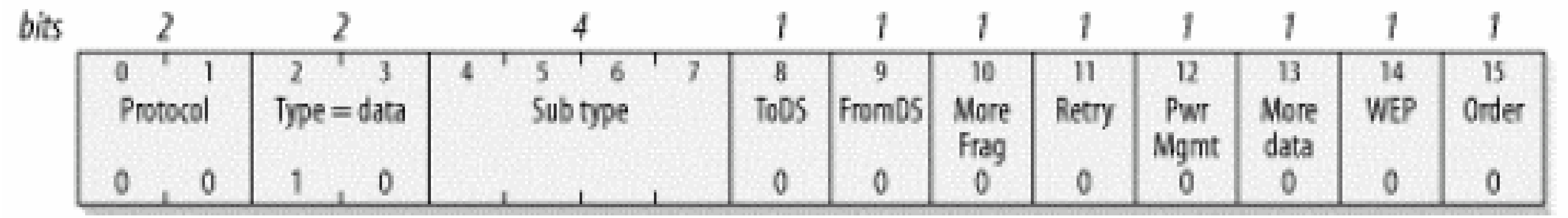


Frames in a WDS



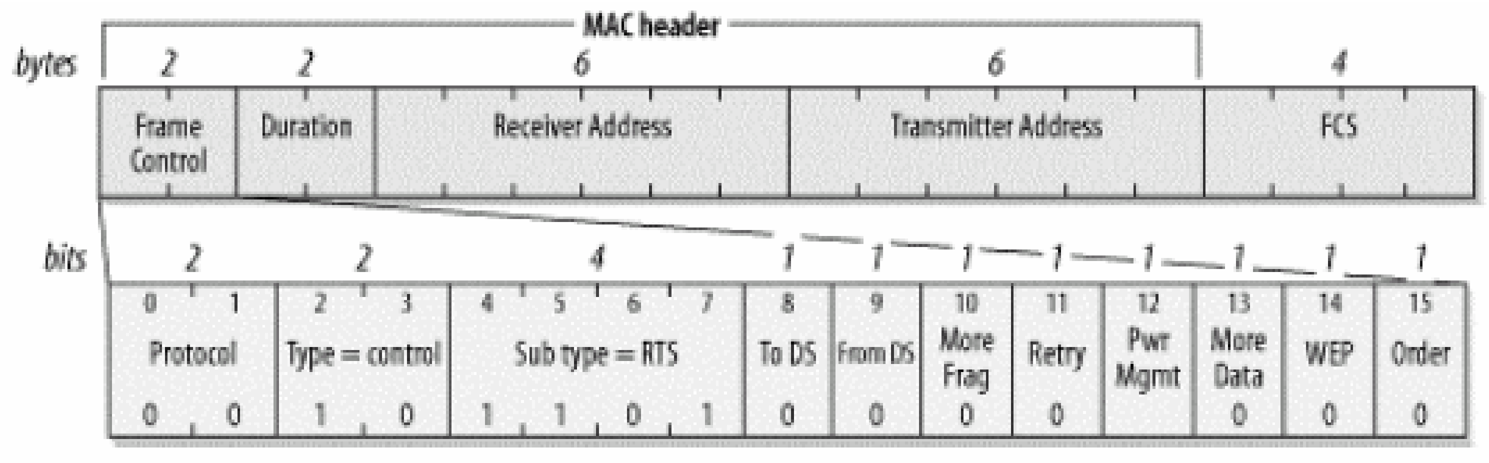
Control Frames

- Control frames assist in the delivery of data frames.
- All control frames use the same Frame Control field：



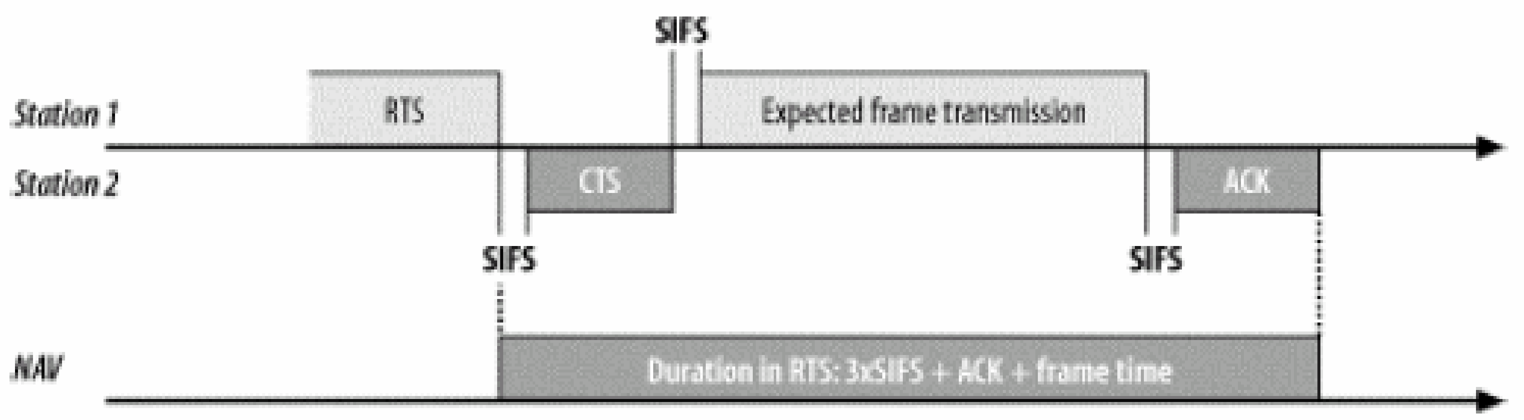
bits	2	2	4	1	1	1	1	1	1	1	1
	0 1	2 3	4 5 6 7	8	9	10	11	12	13	14	15
	Protocol	Type = data	Sub type	ToDS	FromDS	More Frag	Retry	Pwr Mgmt	More data	WEP	Order
	0 0	1 0		0	0	0	0	0	0	0	0

Request to Send (RTS)

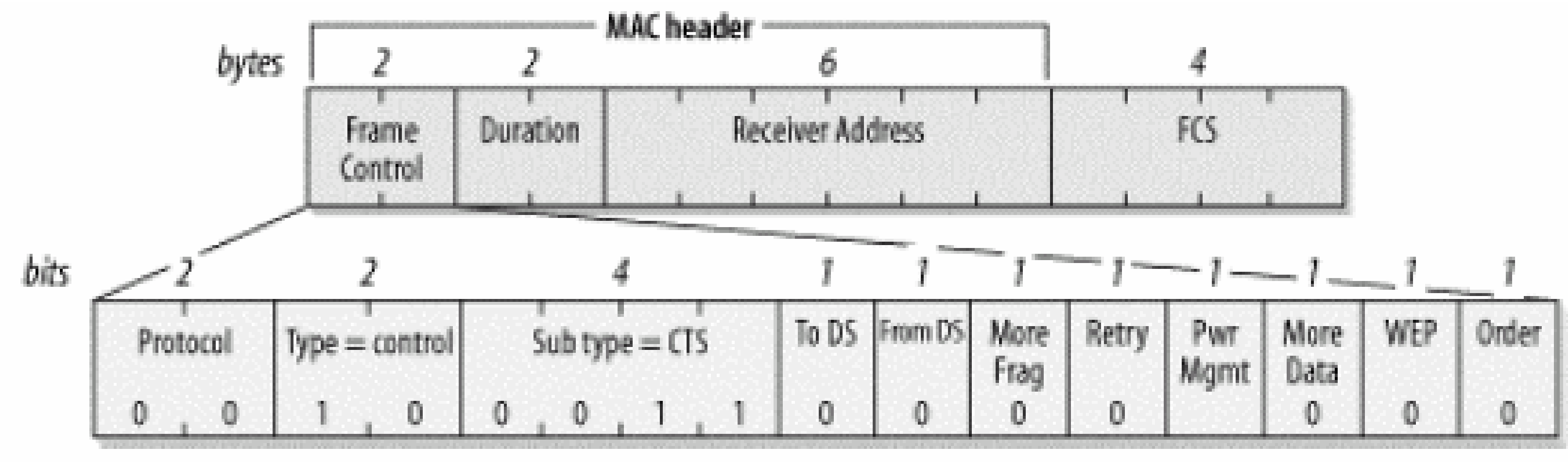


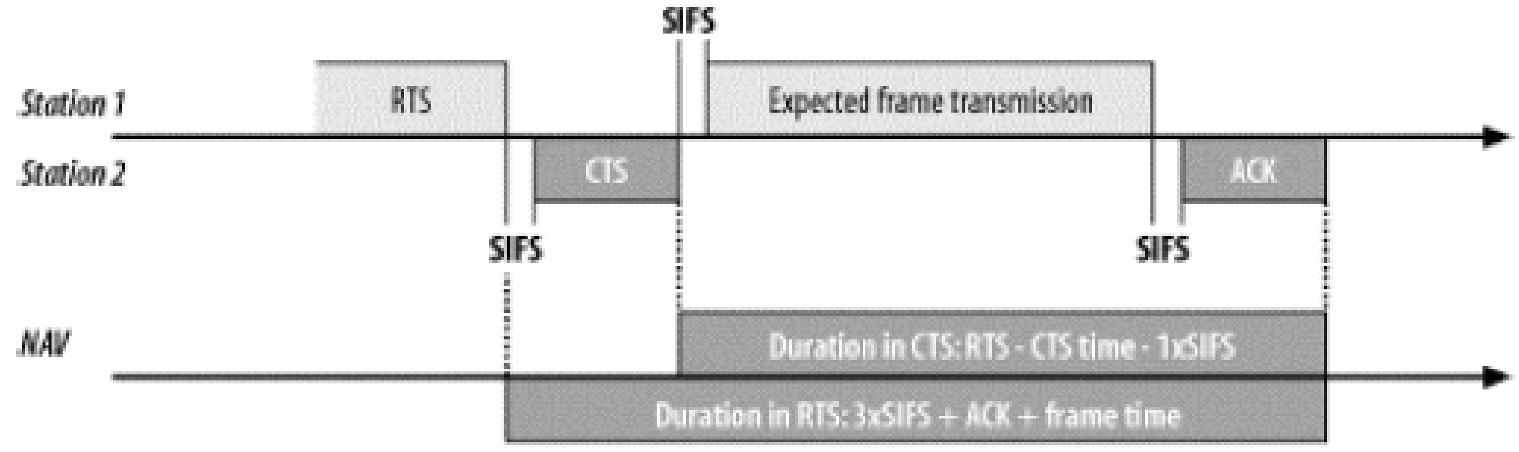
	MAC header				
bytes	2	2	6	6	4
	Frame Control	Duration	Receiver Address	Transmitter Address	FCS

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

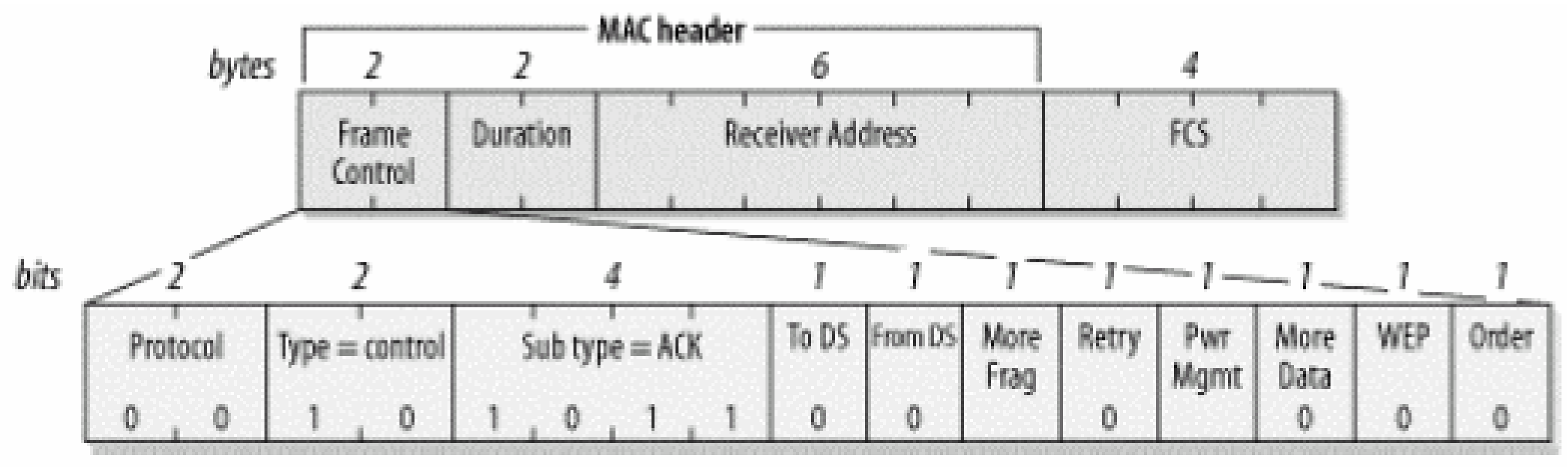

SIFS
Station 1
RTS
Expected frame transmission
Station 2
CTS
ACK
SIFS
SIFS
NAV
Duration in RTS: 3xSIFS + ACK + frame time

Clear to Send (CTS)



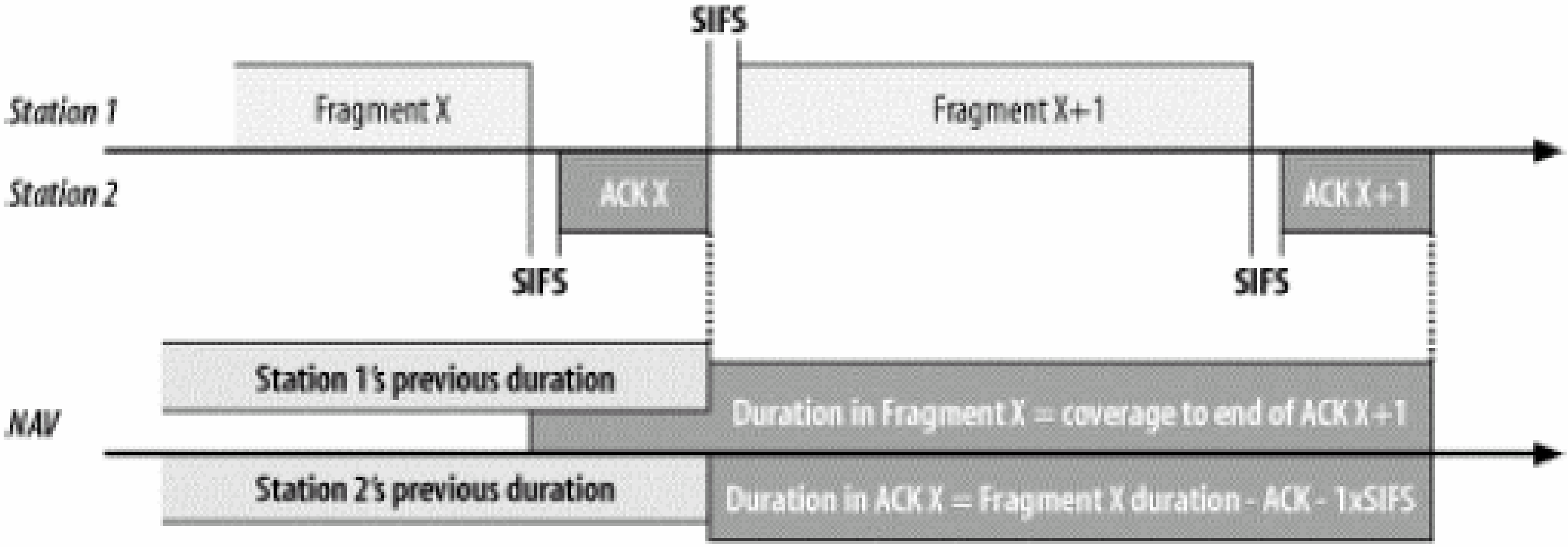

SIFS
Station 1
RTS
Expected frame transmission
Station 2
CTS
ACK
SIFS
SIFS
NAV
Duration in CTS: RTS - CTS time - 1xSIFS
Duration in RTS: 3xSIFS + ACK + frame time

Acknowledgment (ACK)

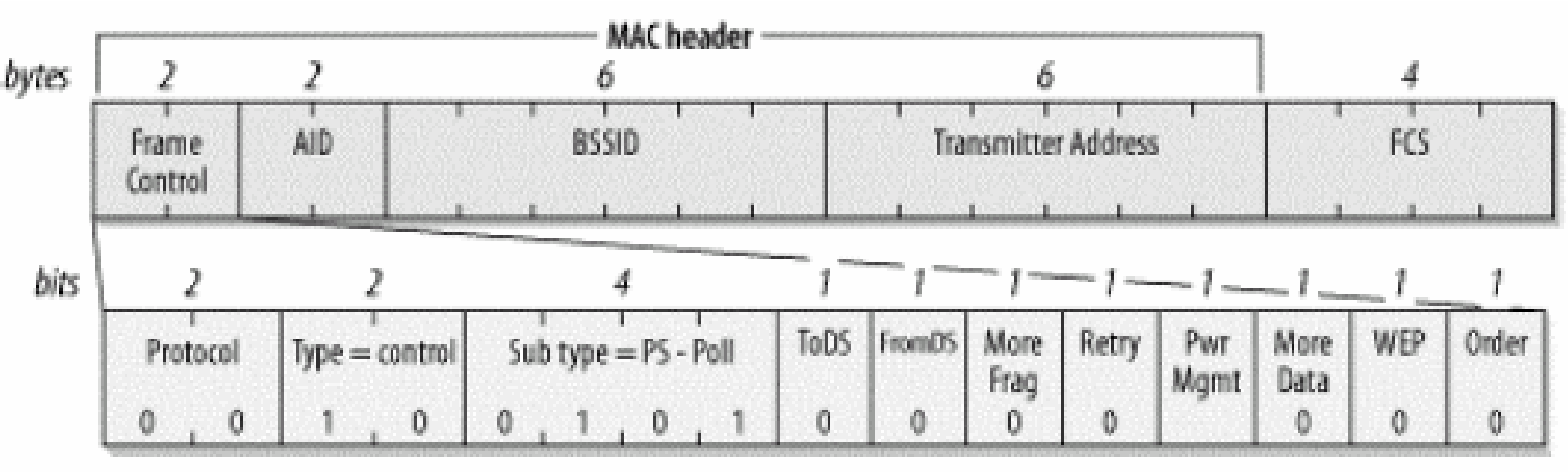


Acknowledgment (ACK)

Figure 4-18. Duration in non-final ACK frames


SIFS
Station 1
Fragment X
Fragment X+1
Station 2
ACK X
ACK X+1
SIFS
SIFS
Station 1's previous duration
NAV
Duration in Fragment X = coverage to end of ACK X+1
Station 2's previous duration
Duration in ACK X = Fragment X duration - ACK - 1xSIFS

Power-Save Poll (PS-Poll)

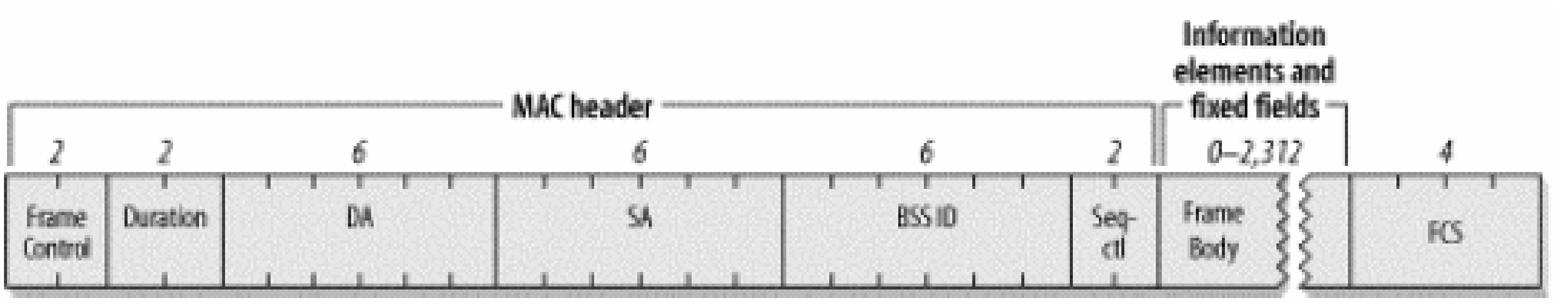


Management Frames

- Identity of a network station can be broken into three components：
  1. Mobile stations in search of connectivity must first locate a compatible wireless network to use for access.
  2. Network must authenticate mobile stations
  3. mobile stations must associate with an AP

The Structure of Management Frames

- The MAC header is the same in all management frames



Frame body

- Most of the data contained in the frame body is：
  - *fixed fields*：fixed-length, or
  - *information elements*：variable-length

Fixed-Length Management Frame Components

- Fixed-length fields are often referred to simply as *fields*
- Ten fixed-length fields may appear in management frames.

Fields

- **Authentication Algorithm Number**

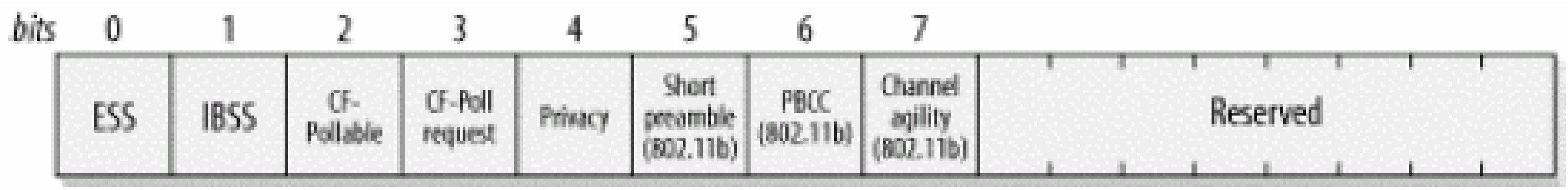
Value	Meaning
0	Open System authentication
1	Shared Key authentication
2-65535	Resvered

Fields

- **Authentication Transaction Sequence Number**
  - Used to track progress through the authentication exchange.
- **Beacon interval**
  - Set to the number of *time units* between Beacon transmissions.

Fields

- **Capability Information**
  - Used in Beacon transmissions to advertise the network's capabilities.
  - Each bit is used as a flag to advertise a particular function of the network.



bits	0	1	2	3	4	5	6	7	
	ESS	IBSS	CF-Pollable	CF-Poll request	Privacy	Short preamble (802.11b)	PBCC (802.11b)	Channel agility (802.11b)	Reserved

Fields

- **Capability Information**
  - *ESS/IBSS*
  - *Privacy*
  - *Short Preamble*
  - *PBCC*
  - *Channel Agility*
  - *Contention-free polling bits*

Fields

- **Current AP Address**
  - Indicate the MAC address of the access point with which they are associated.
- **Listen interval**
  - is the number of Beacon intervals that stations wait between listening for Beacon frames.

Fields

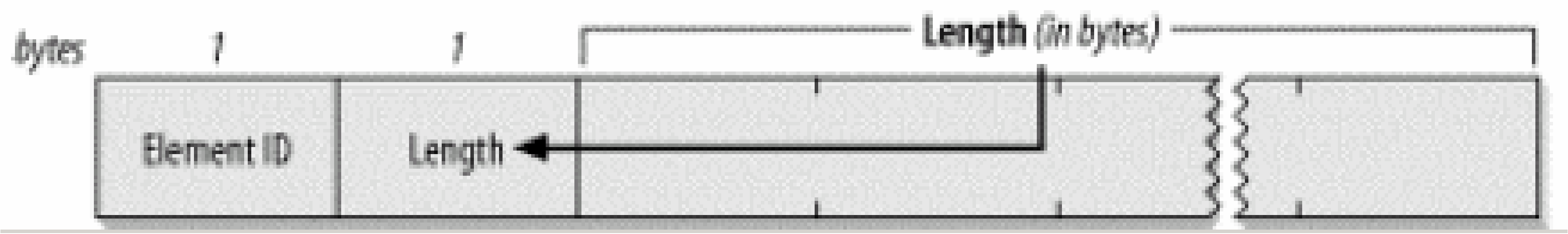
- **Association ID**
  - When stations associate with an access point, they are assigned an Association ID to assist with control and management functions.
- **Timestamp**
  - Used to synchronization between the stations in a BSS.

Fields

- **Reason Code**
  - Stations may send Disassociation or Deauthentication frames in response to traffic when the sender has not properly joined the network. Part of the frame is a 16-bit Reason Code field.
- **Status Code**
  - Indicate the success or failure of an operation.

Management Frame Information Elements

- A generic information element has：
  - □ ID number
  - □ Length
  - □ Variable-length component



Information Elements

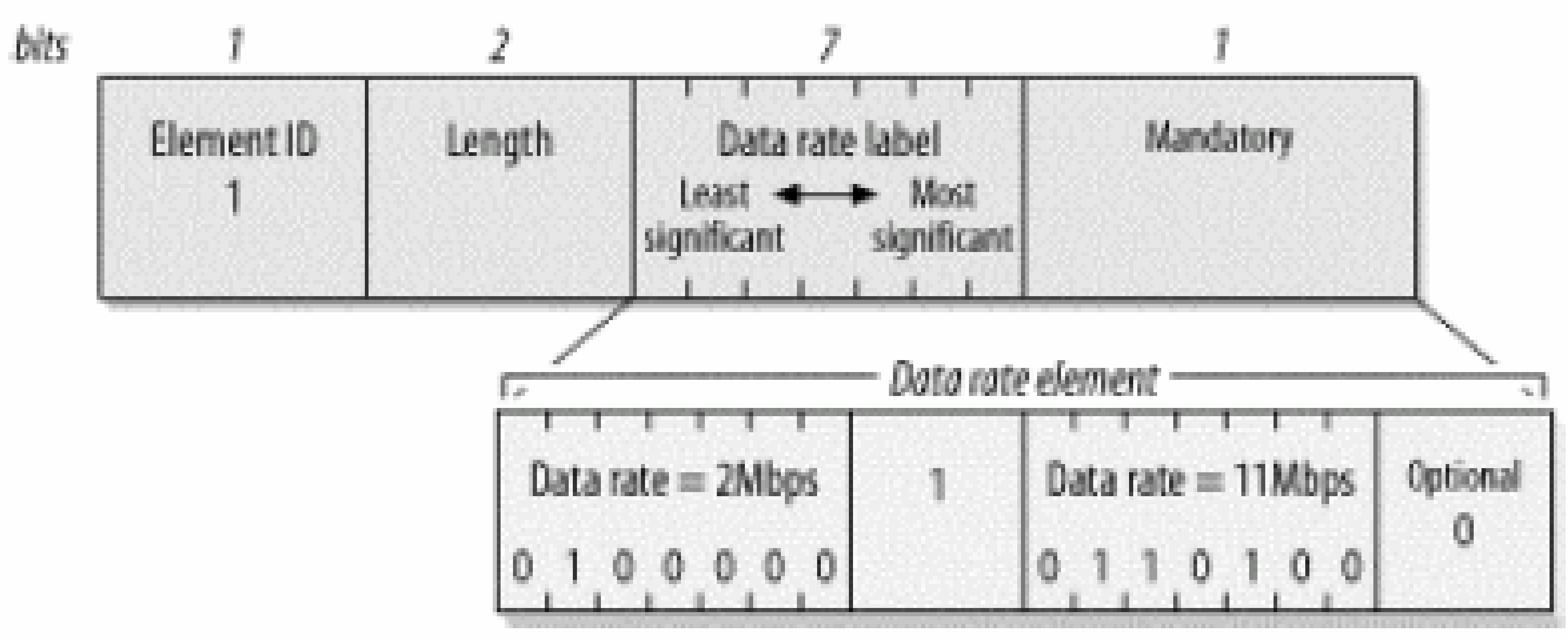
- **Service Set Identity (SSID)**
  - □ allows network managers to assign an identifier to the service set.
  - □ Stations attempting to join a network may scan an area for available networks and join the network with a specified SSID.
  - □ The SSID is the same for all the basic service areas composing an extended service area.

Information Elements

- **Supported Rates**
  - It consists of a string of bytes
  - Each byte uses：
    - the seven low-order bits for the data rate
    - the most significant bit indicates whether the data rate is mandatory
  - Up to eight rates may be encoded in the information element.

Information Elements

- **Supported Rates**



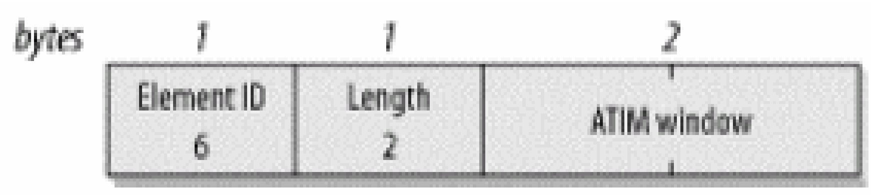
Information Elements

- **FH Parameter Set**
- **DS Parameter Set**
- **CF Parameter Set**
- **Traffic Indication Map (TIM)**

1	1	1	1	1	1-251
Element ID	Length	DTIM Count	DTIM Period	Bitmap Control	Partial Virtual Bitmap

Information Elements

- **IBSS Parameter Set**

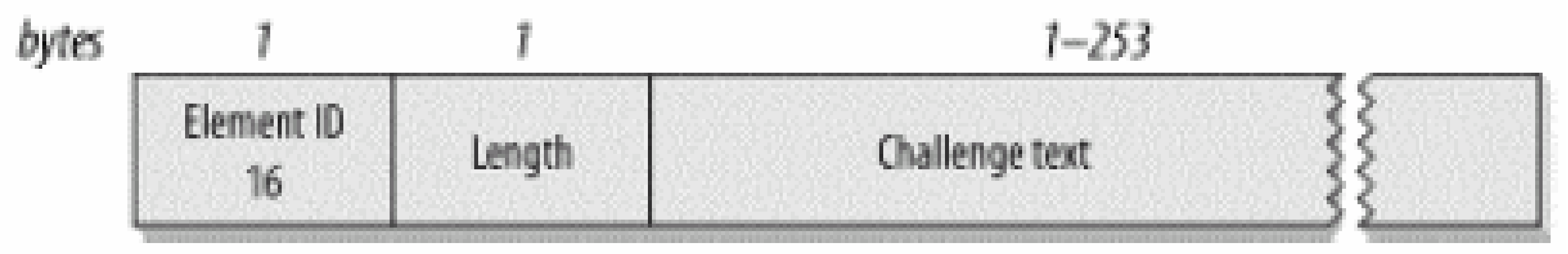


bytes	1	1	2
	Element ID 6	Length 2	ATIM window

  - ATIM windows indicates the number of time units between ATIM frames in an IBSS.

Information Elements

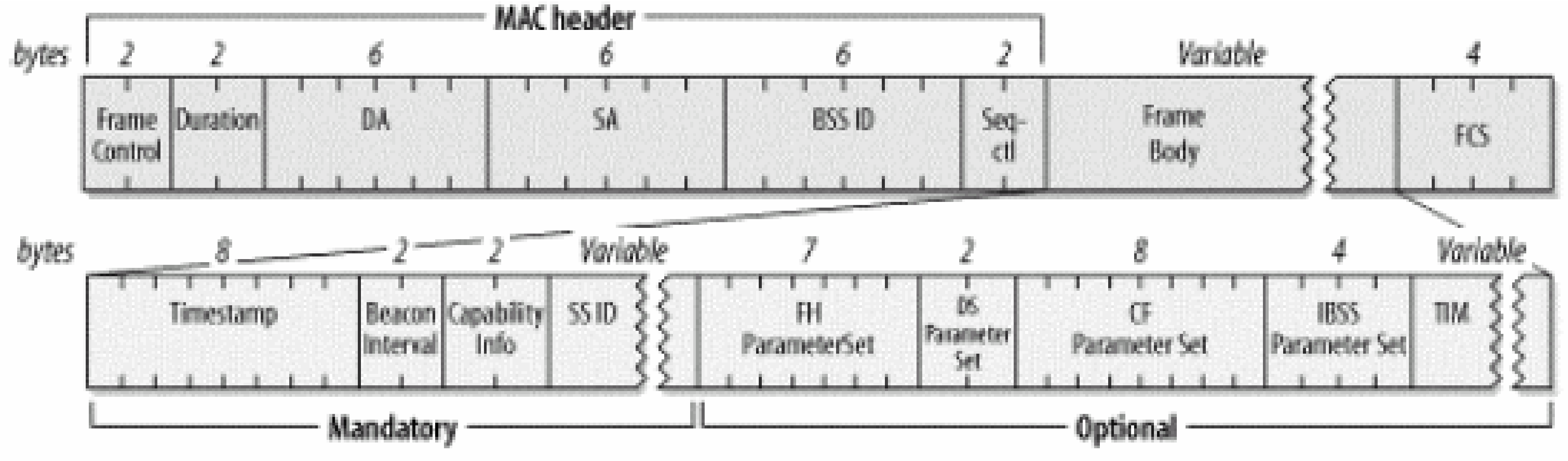
- **Challenge Text**



bytes	1	1	1–253
	Element ID 16	Length	Challenge text

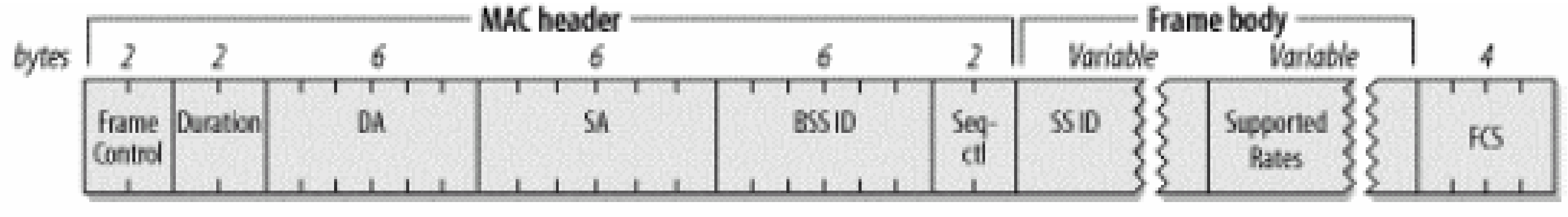
Types of Management Frames

- **Beacon**
  - Are an important part of many network maintenance tasks.



Types of Management Frames

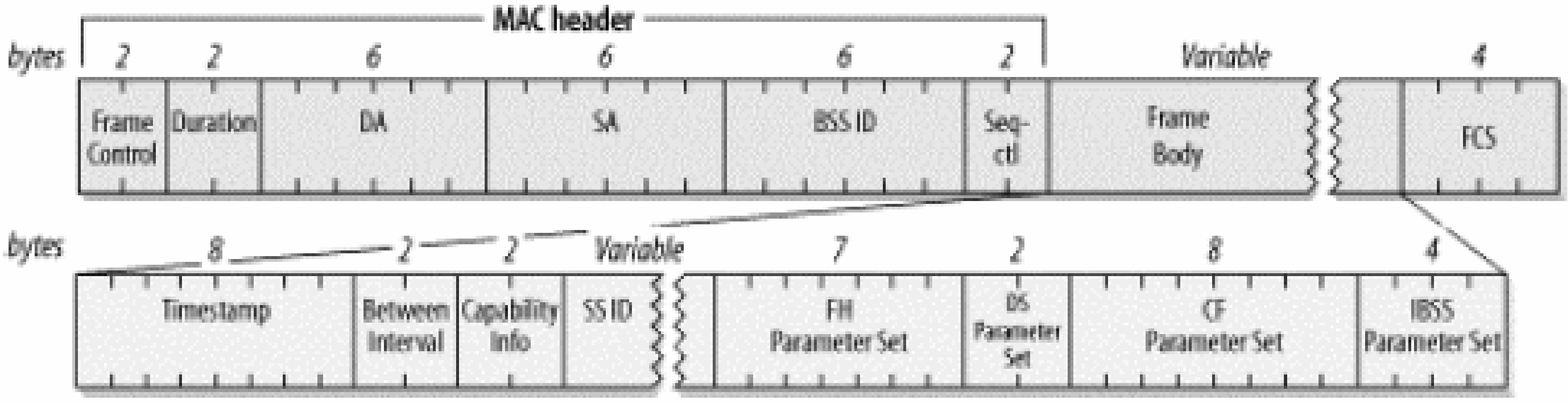
- **Probe Request**
  - Mobile stations use Probe Request frames to scan an area for existing 802.11 networks.



	MAC header						Frame body		
bytes	2	2	6	6	6	2	Variable	Variable	4
	Frame Control	Duration	DA	SA	BSS ID	Seq-ctl	SS ID	Supported Rates	FCS

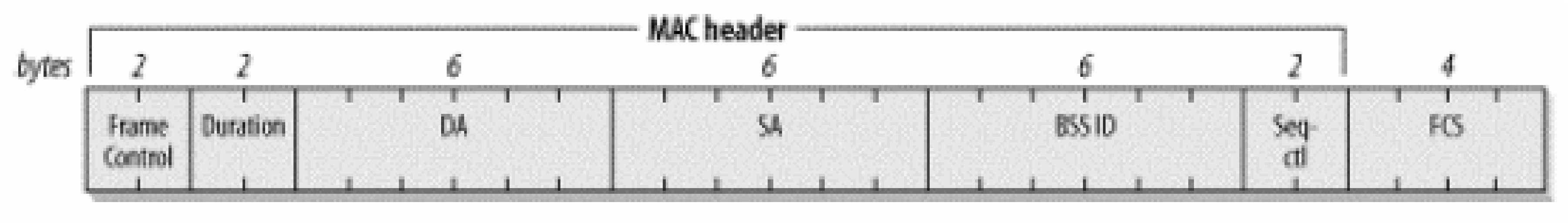
Types of Management Frames

- **Probe Response**
  - □ If a Probe Request encounters a network with compatible parameters, the network sends a Probe Response frame.



Types of Management Frames

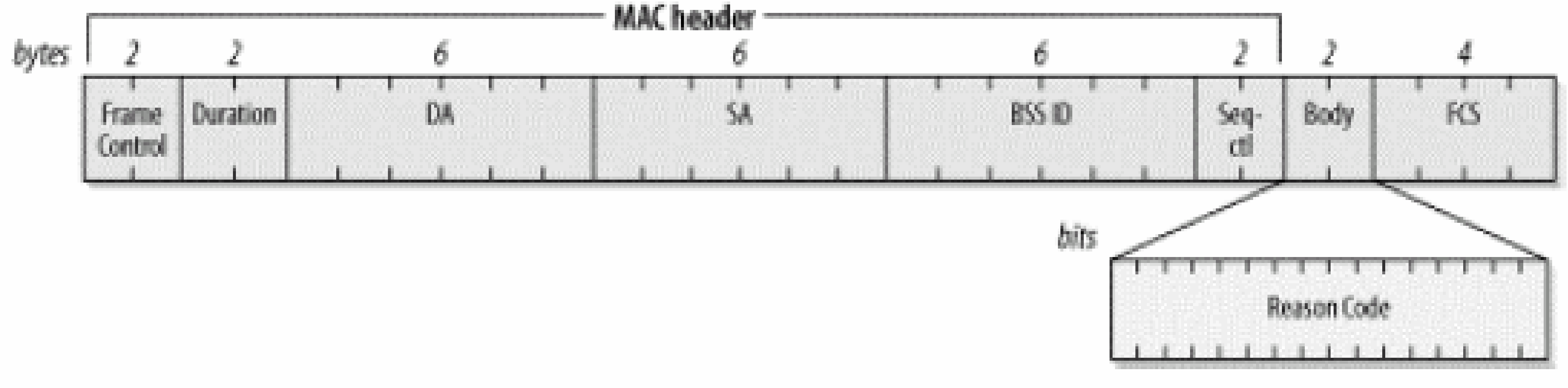
- **IBSS announcement traffic indication map (ATIM)**
  - When a station in an IBSS has buffered frames for a receiver in low-power mode, it sends an ATIM frame during the delivery period to notify the recipient it has buffered data.



	MAC header						
bytes	2	2	6	6	6	2	4
	Frame Control	Duration	DA	SA	BSS ID	Seq-ctl	FCS

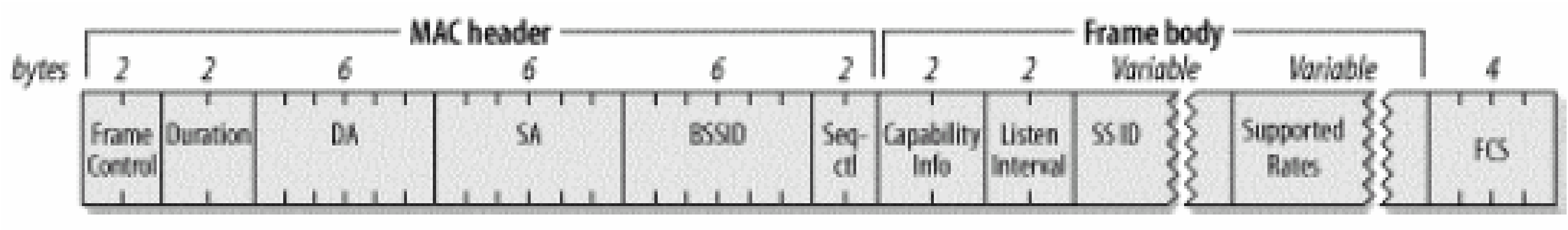
Types of Management Frames

- **Disassociation and Deauthentication**

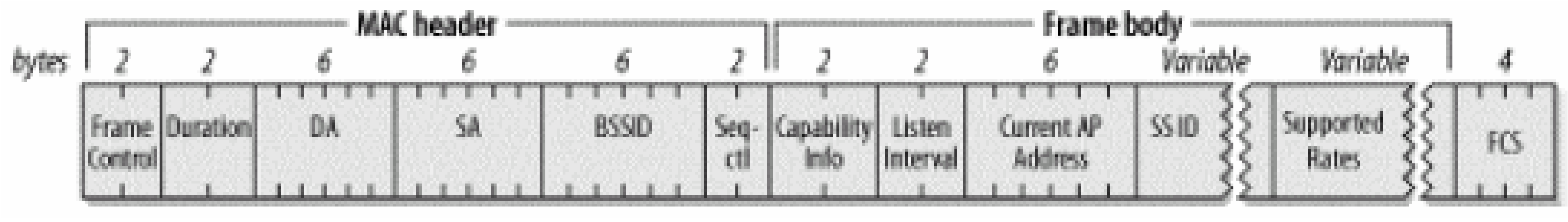


Types of Management Frames

- Association Request

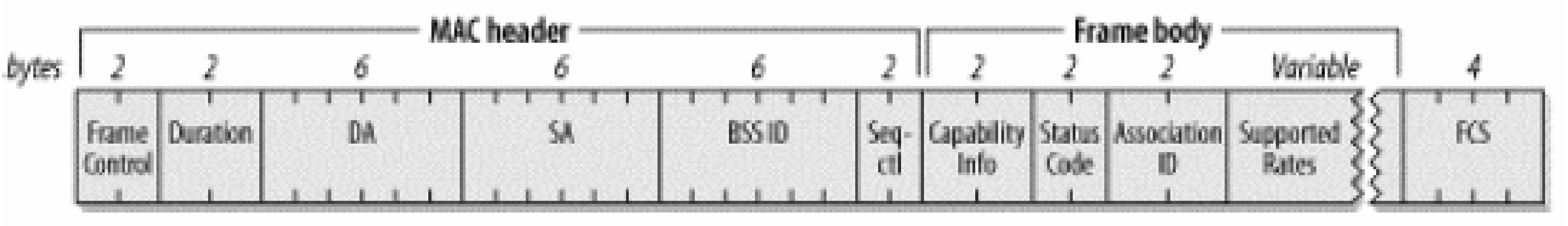


- Reassociation Request



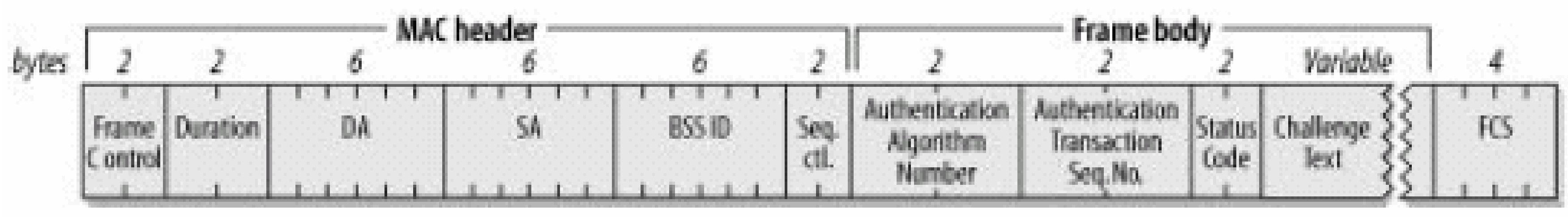
Types of Management Frames

- **Association Response and Reassociation Response**



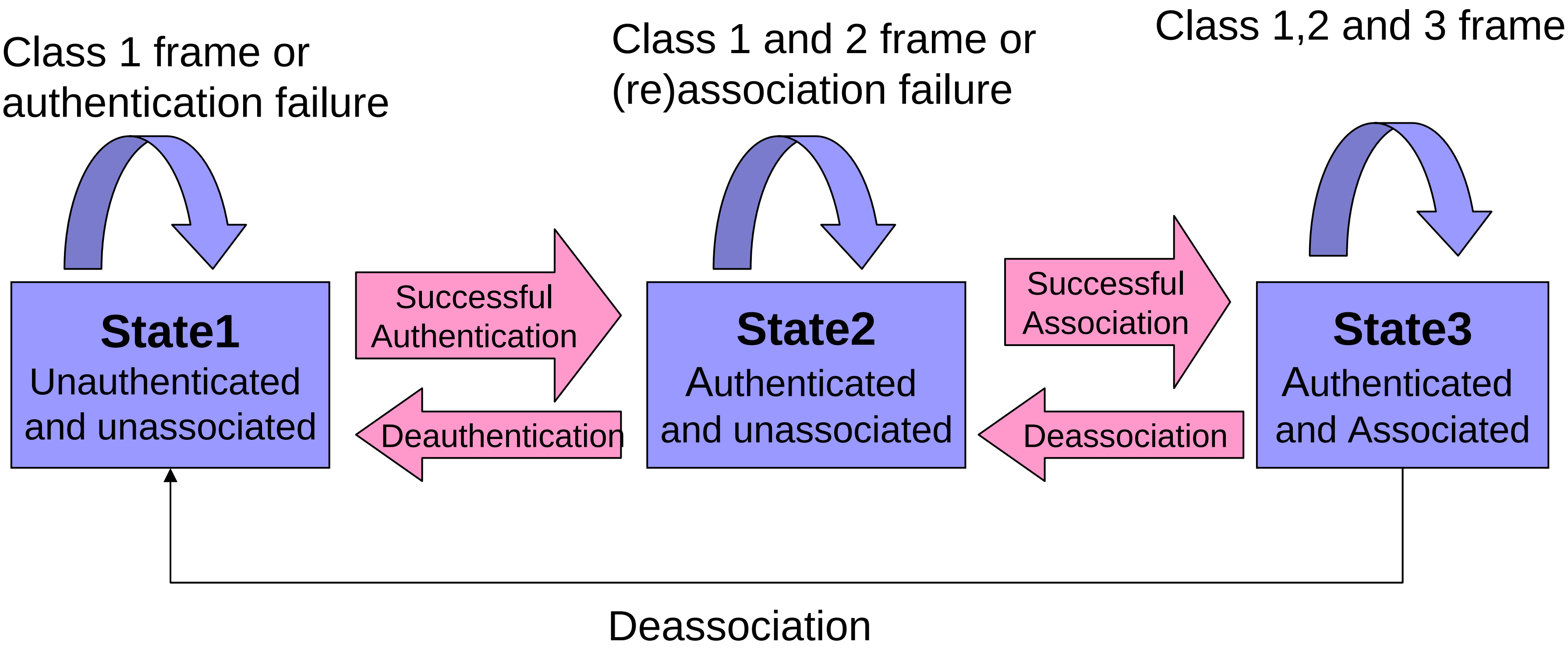
	MAC header						Frame body				
bytes	2	2	6	6	6	2	2	2	2	Variable	4
	Frame Control	Duration	DA	SA	BSS ID	Seq-ctl	Capability Info	Status Code	Association ID	Supported Rates	FCS

- **Authentication**



	MAC header						Frame body				
bytes	2	2	6	6	6	2	2	2	2	Variable	4
	Frame Control	Duration	DA	SA	BSS ID	Seq. ctl.	Authentication Algorithm Number	Authentication Transaction Seq.No.	Status Code	Challenge Text	FCS

Frame Transmission and Association and Authentication States



Class 1 frame or authentication failure

Class 1 and 2 frame or (re)association failure

Class 1,2 and 3 frame

State1
Unauthenticated and unassociated

Successful Authentication

Deauthentication

State2
Authenticated and unassociated

Successful Association

Deassociation

State3
Authenticated and Associated

Deassociation

Frame Transmission and Association and Authentication States

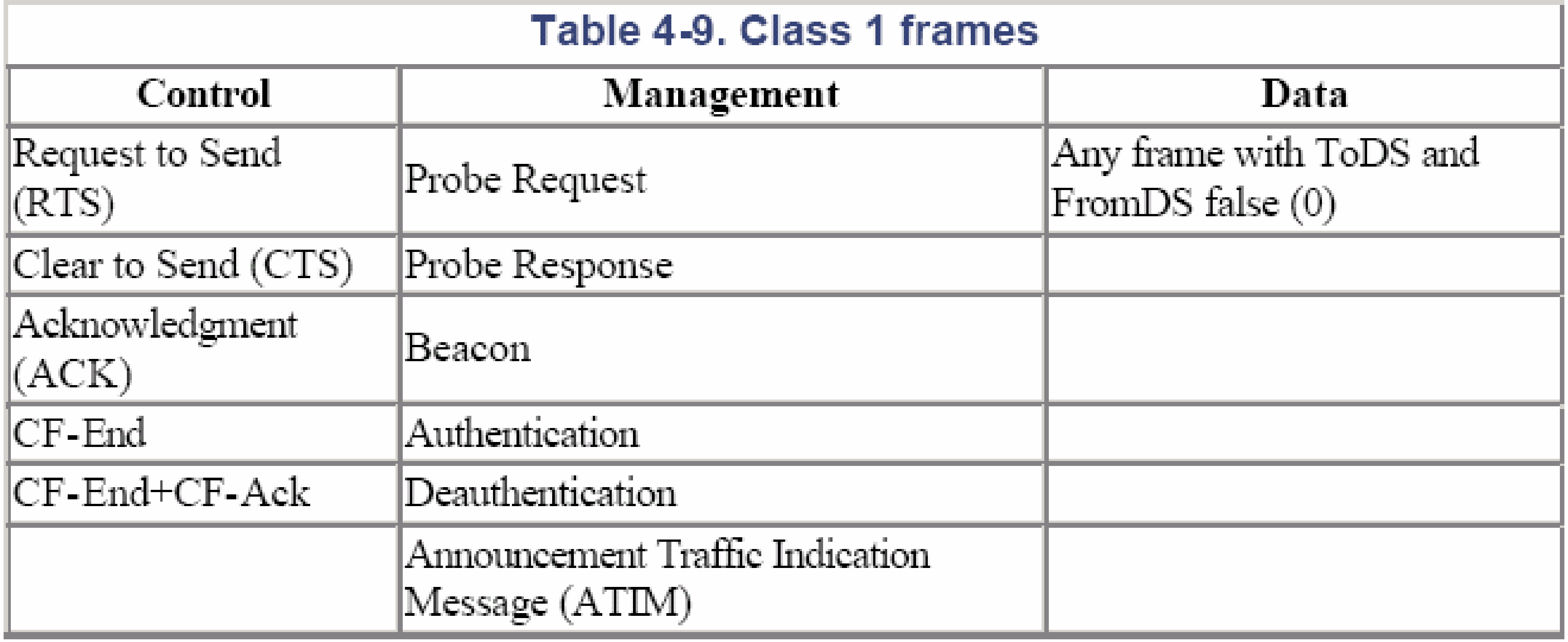


Table 4-9. Class 1 frames

Control	Management	Data
Request to Send (RTS)	Probe Request	Any frame with ToDS and FromDS false (0)
Clear to Send (CTS)	Probe Response	
Acknowledgment (ACK)	Beacon	
CF-End	Authentication	
CF-End+CF-Ack	Deauthentication	
	Announcement Traffic Indication Message (ATIM)	

Frame Transmission and Association and Authentication States

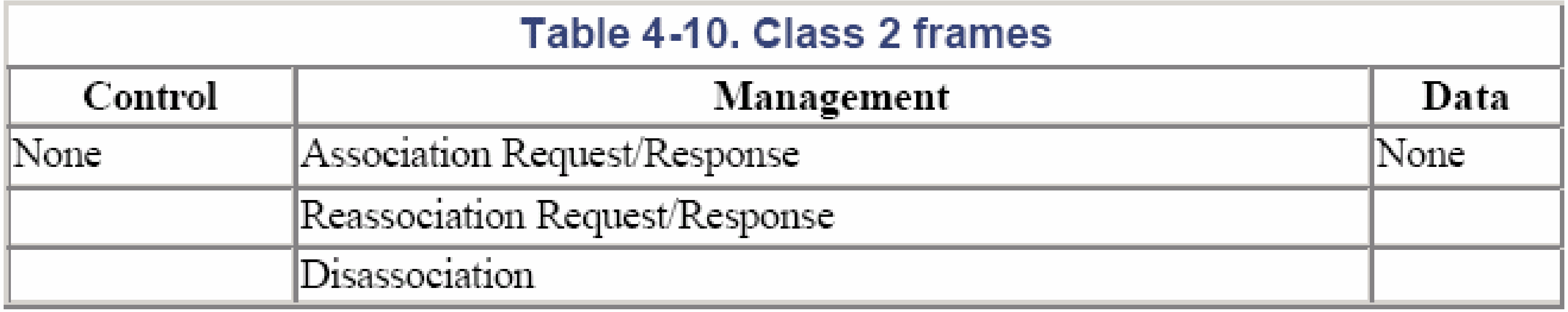


Table 4-10. Class 2 frames

Control	Management	Data
None	Association Request/Response	None
	Reassociation Request/Response	
	Disassociation	

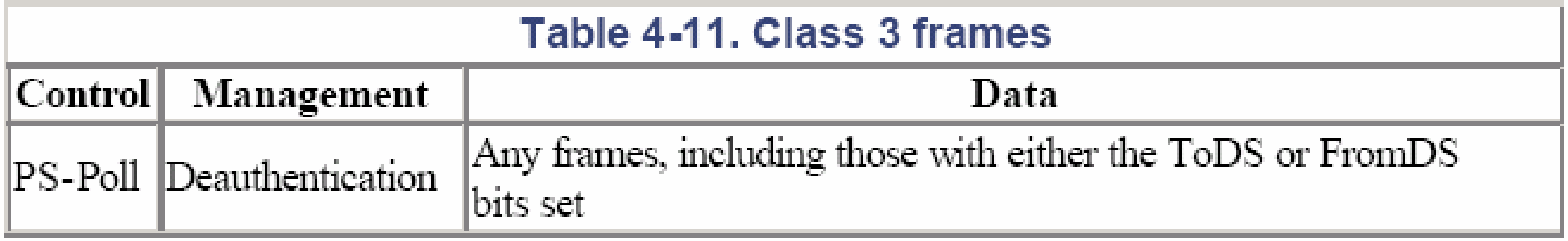


Table 4-11. Class 3 frames

Control	Management	Data
PS-Poll	Deauthentication	Any frames, including those with either the ToDS or FromDS bits set