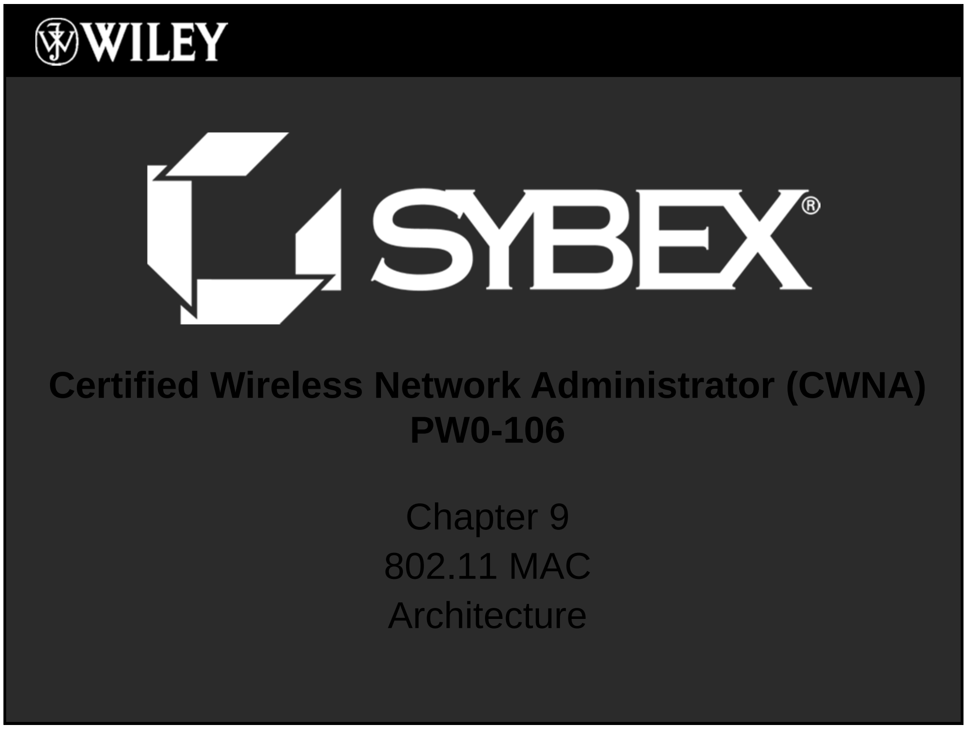
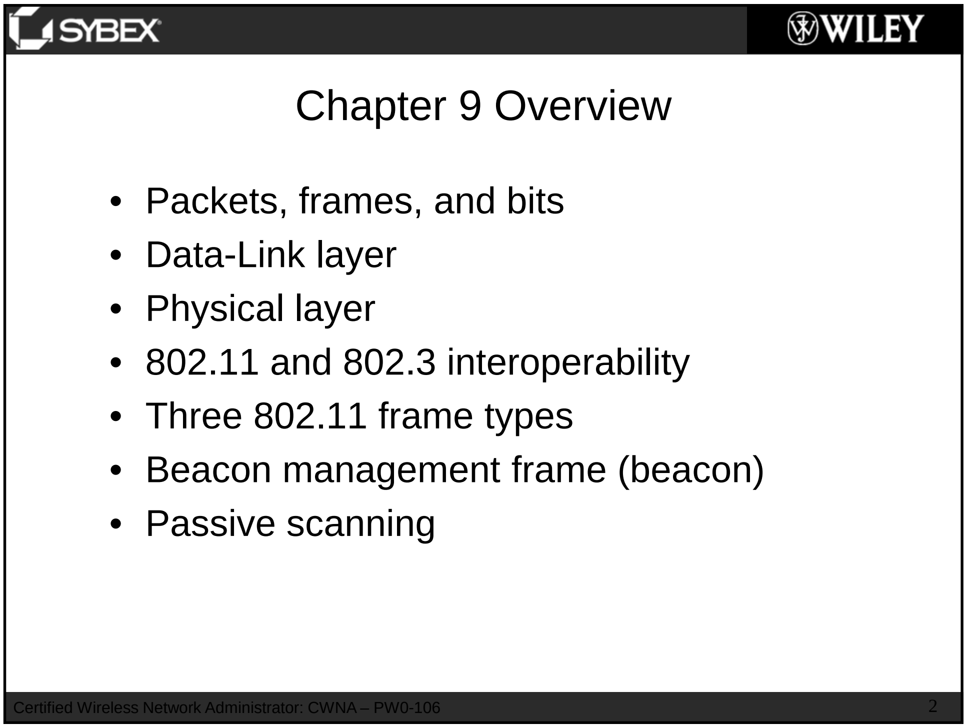


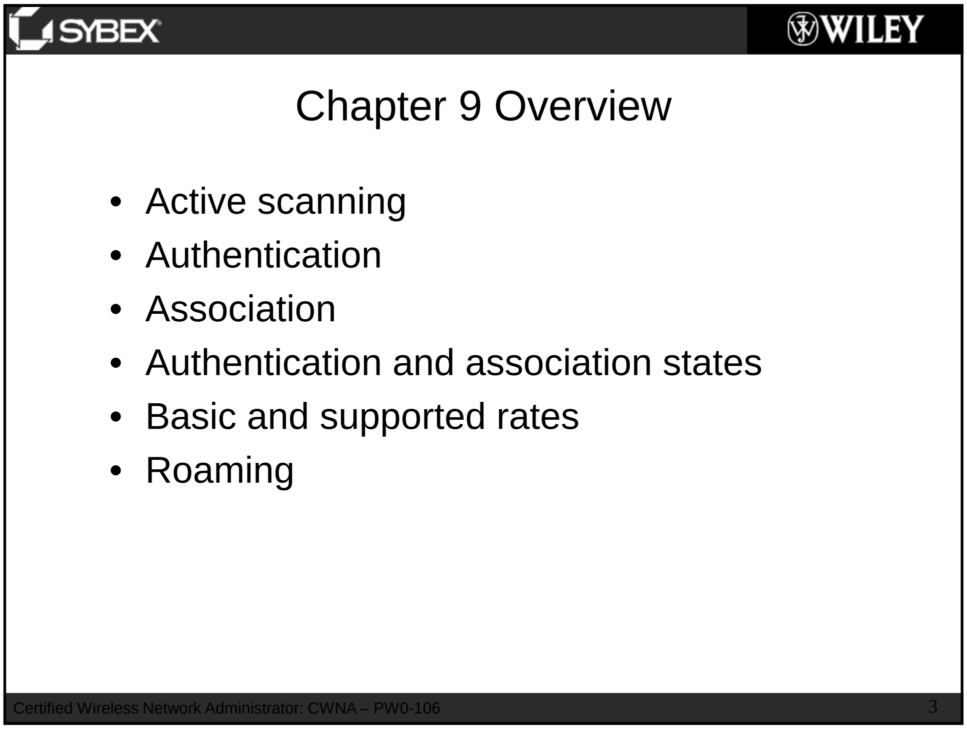
Certified Wireless Network Administrator (CWNA) PW0-106

Chapter 9
802.11 MAC
Architecture



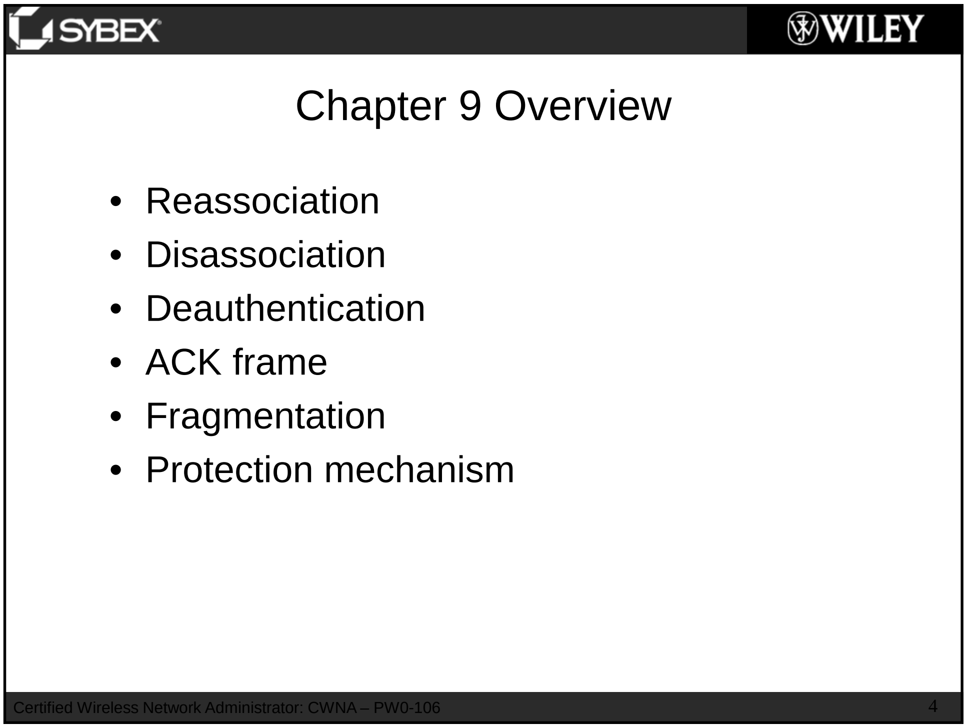
Chapter 9 Overview

- Packets, frames, and bits
- Data-Link layer
- Physical layer
- 802.11 and 802.3 interoperability
- Three 802.11 frame types
- Beacon management frame (beacon)
- Passive scanning



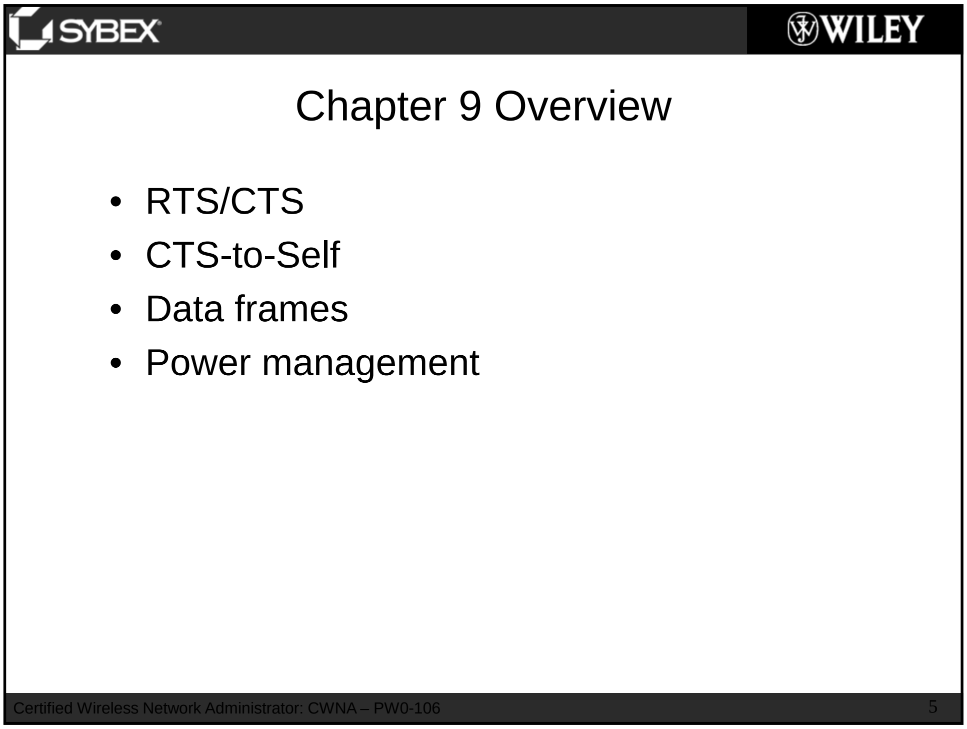
Chapter 9 Overview

- Active scanning
- Authentication
- Association
- Authentication and association states
- Basic and supported rates
- Roaming



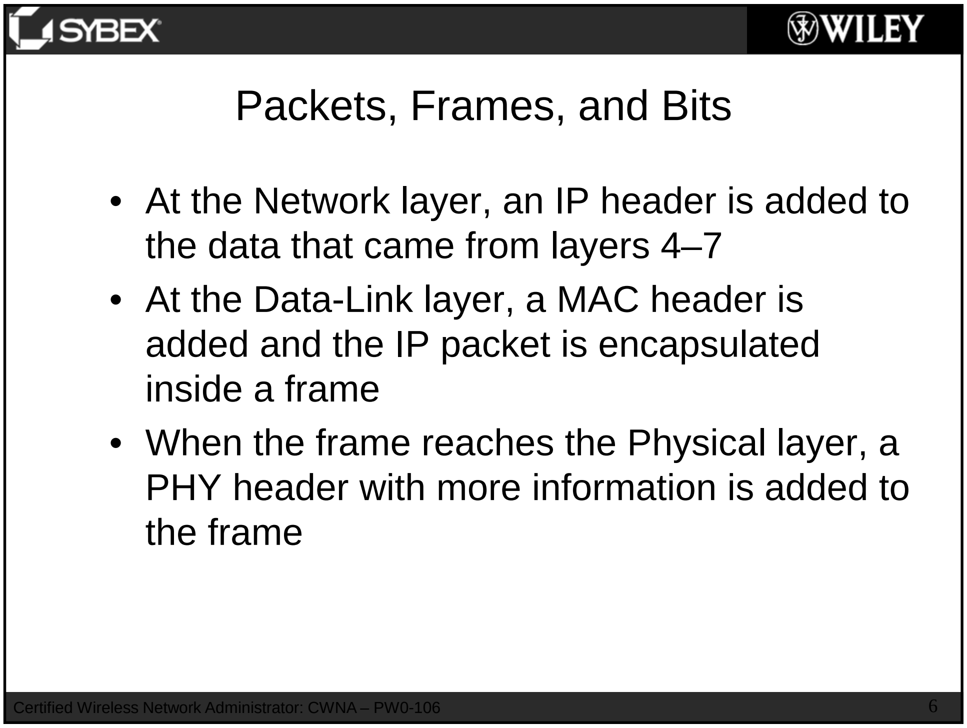
Chapter 9 Overview

- Reassociation
- Disassociation
- Deauthentication
- ACK frame
- Fragmentation
- Protection mechanism



Chapter 9 Overview

- RTS/CTS
- CTS-to-Self
- Data frames
- Power management



Packets, Frames, and Bits

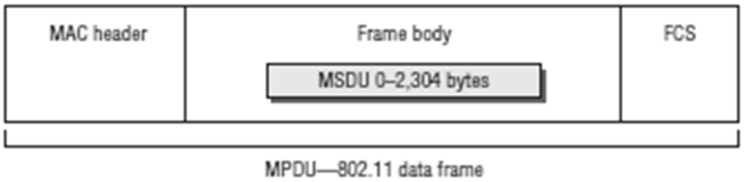
- At the Network layer, an IP header is added to the data that came from layers 4–7
- At the Data-Link layer, a MAC header is added and the IP packet is encapsulated inside a frame
- When the frame reaches the Physical layer, a PHY header with more information is added to the frame

Data-Link Layer

- Two sublayers
  - 802.2 Logical Link Control (LLC) sublayer
  - 802.11 Media Access Control (MAC) sublayer
- Data handed off to the LLC becomes known as the MAC Service Data Unit (MSDU)
- When handed to the MAC sublayer, the MSDU is encapsulated in a MAC Protocol Data Unit (MPDU).

802.11 MPDU

- MAC Header
- Frame Body
- Frame Check Sequence (FCS)



MAC header

Frame body

MSDU 0–2,304 bytes

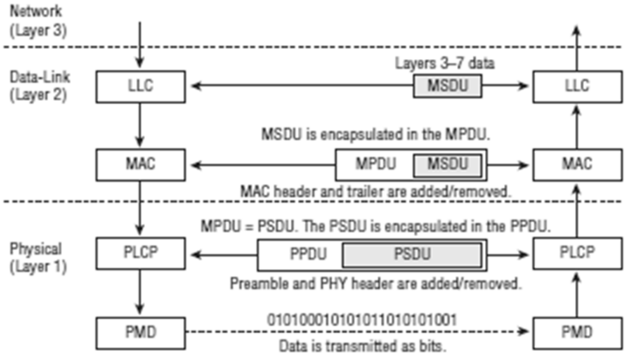
FCS

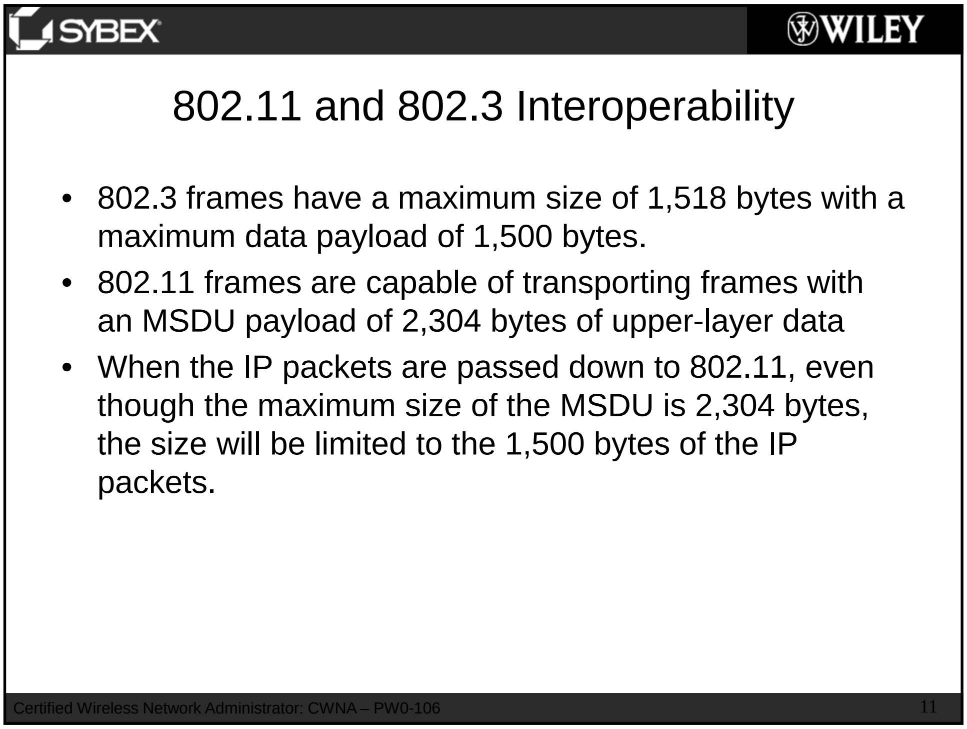
MPDU—802.11 data frame

Physical Layer

- Two sublayers
  - Physical Layer Convergence Procedure (PLCP) sublayer
  - Physical Medium Dependent (PMD) sublayer
- PLCP Service Data Unit (PSDU) is a view of the MPDU from the Physical layer
- PLCP Protocol Data Unit (PPDU).adds a preamble and PHY header to the PSDU

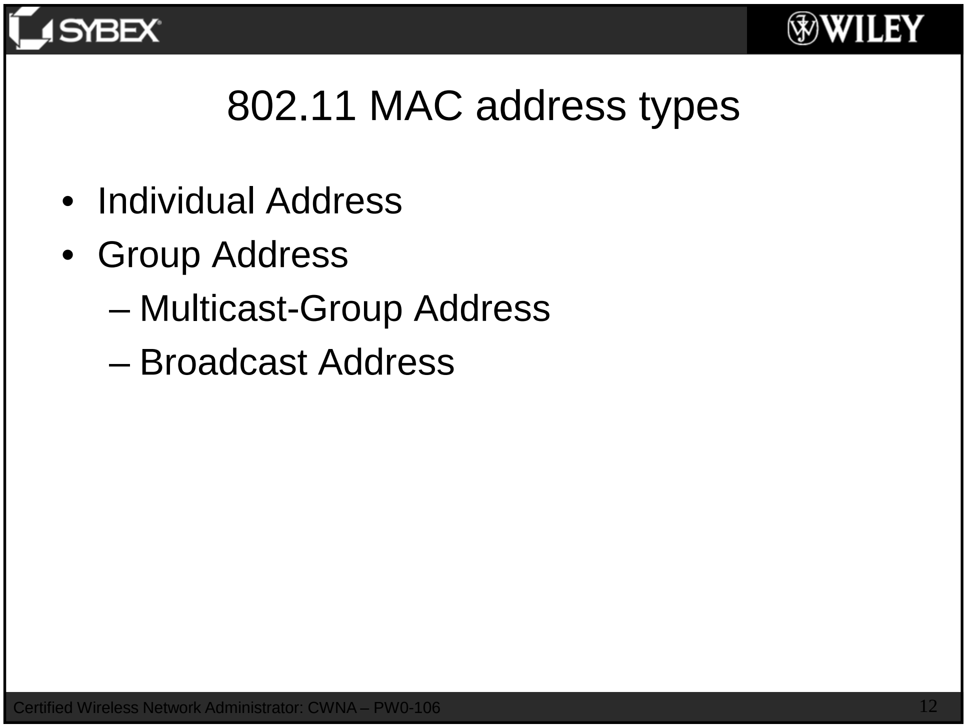
Data-Link and Physical layers


Network (Layer 3)
Data-Link (Layer 2)
Physical (Layer 1)
LLC
Layers 3–7 data
MSDU
LLC
MSDU is encapsulated in the MPDU.
MAC
MPDU
MSDU
MAC
MAC header and trailer are added/removed.
MPDU = PSDU. The PSDU is encapsulated in the PPDU.
PLCP
PPDU
PSDU
PLCP
Preamble and PHY header are added/removed.
PMD
0101000101010110101010001
Data is transmitted as bits.
PMD



802.11 and 802.3 Interoperability

- 802.3 frames have a maximum size of 1,518 bytes with a maximum data payload of 1,500 bytes.
- 802.11 frames are capable of transporting frames with an MSDU payload of 2,304 bytes of upper-layer data
- When the IP packets are passed down to 802.11, even though the maximum size of the MSDU is 2,304 bytes, the size will be limited to the 1,500 bytes of the IP packets.

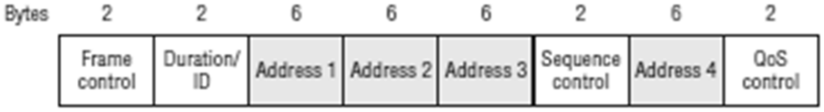


802.11 MAC address types

- Individual Address
- Group Address
  - Multicast-Group Address
  - Broadcast Address

802.11 MAC header

- Five MAC address fields in the layer 2 header
  - Source Address (SA)
  - Destination Address (DA)
  - Transmitter Address (TA)
  - Receiver Address (RA)
  - Basic Service Set Identifier (BSSID)

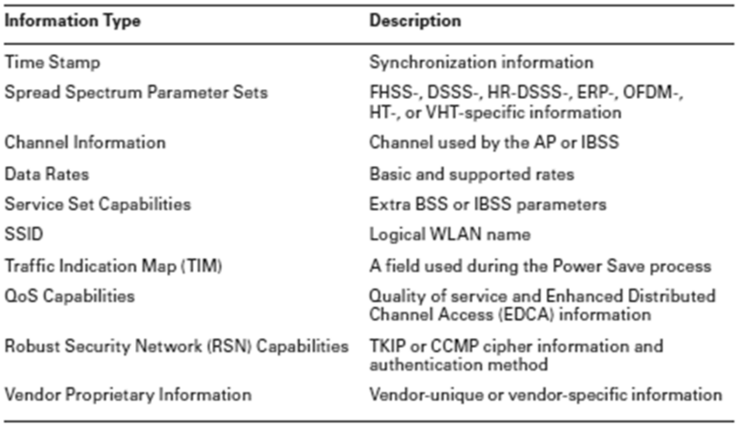


Bytes	2	2	6	6	6	2	6	2
	Frame control	Duration/ ID	Address 1	Address 2	Address 3	Sequence control	Address 4	QoS control

Three 802.11 Frame Types

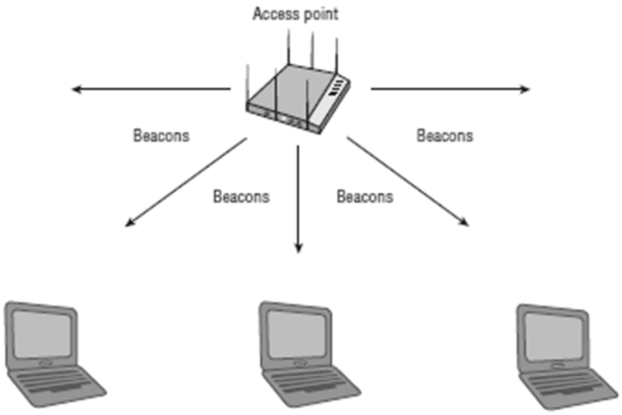
- Management Frames
  - Used by wireless stations to join and leave the basic service set (BSS)
- Control Frames
  - Assist with the delivery of the data frames and are transmitted at one of the basic rates
- Data Frames
  - Carry the actual data that is passed down from the higher-layer protocols.

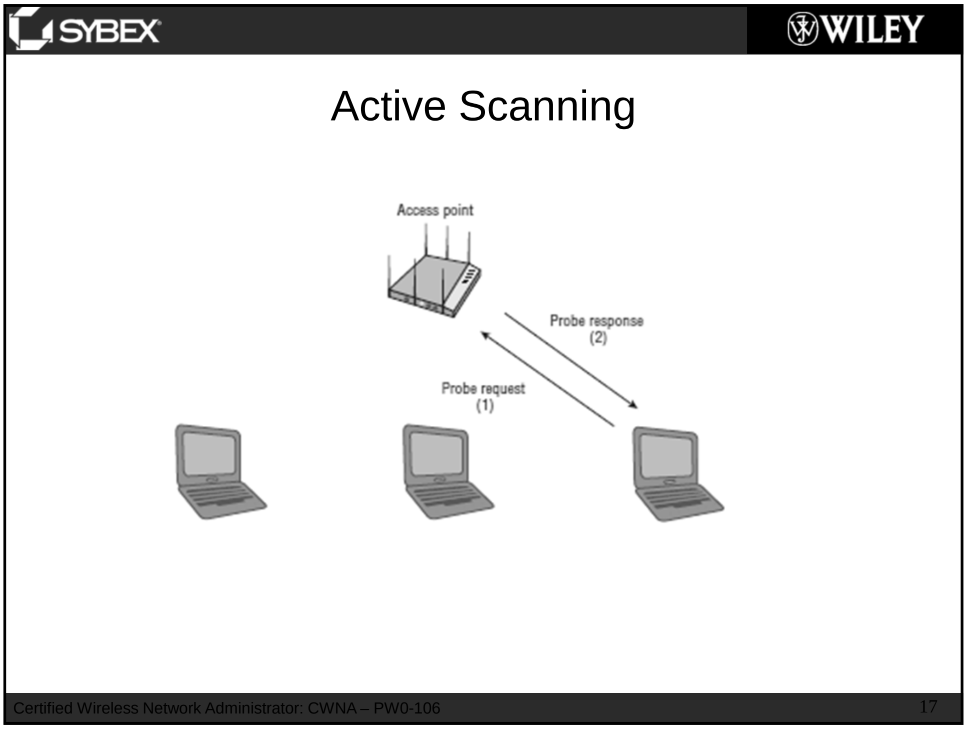
Beacon Management Frame



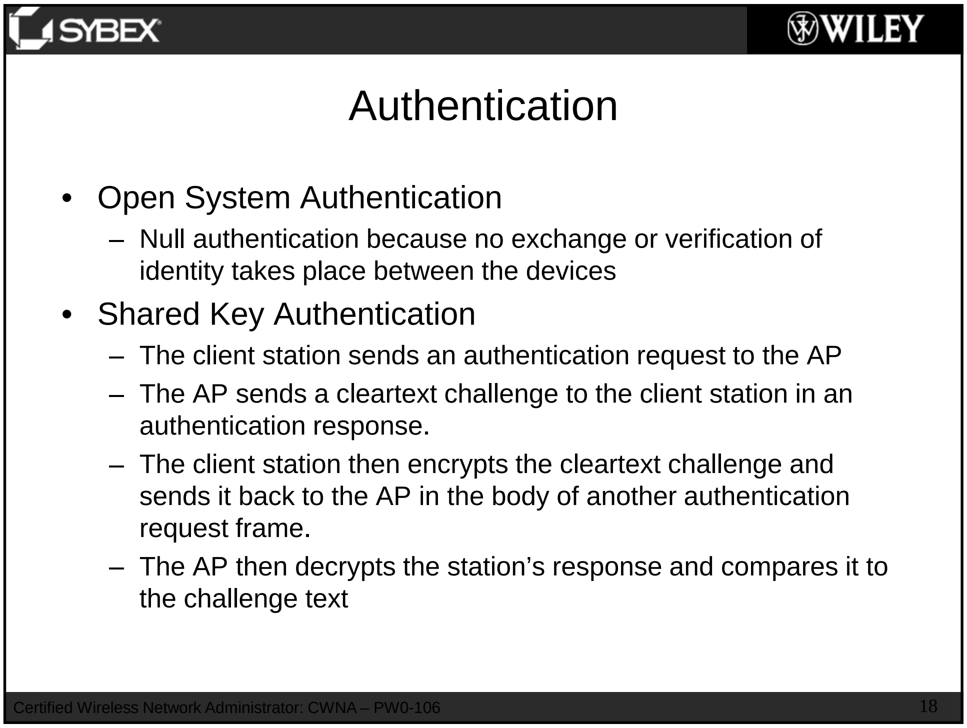
Information Type	Description
Time Stamp	Synchronization information
Spread Spectrum Parameter Sets	FHSS-, DSSS-, HR-DSSS-, ERP-, OFDM-, HT-, or VHT-specific information
Channel Information	Channel used by the AP or IBSS
Data Rates	Basic and supported rates
Service Set Capabilities	Extra BSS or IBSS parameters
SSID	Logical WLAN name
Traffic Indication Map (TIM)	A field used during the Power Save process
QoS Capabilities	Quality of service and Enhanced Distributed Channel Access (EDCA) information
Robust Security Network (RSN) Capabilities	TKIP or CCMP cipher information and authentication method
Vendor Proprietary Information	Vendor-unique or vendor-specific information

Passive Scanning





Active Scanning



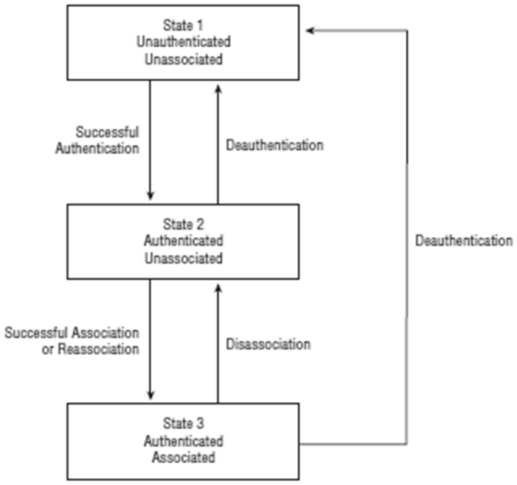
Authentication

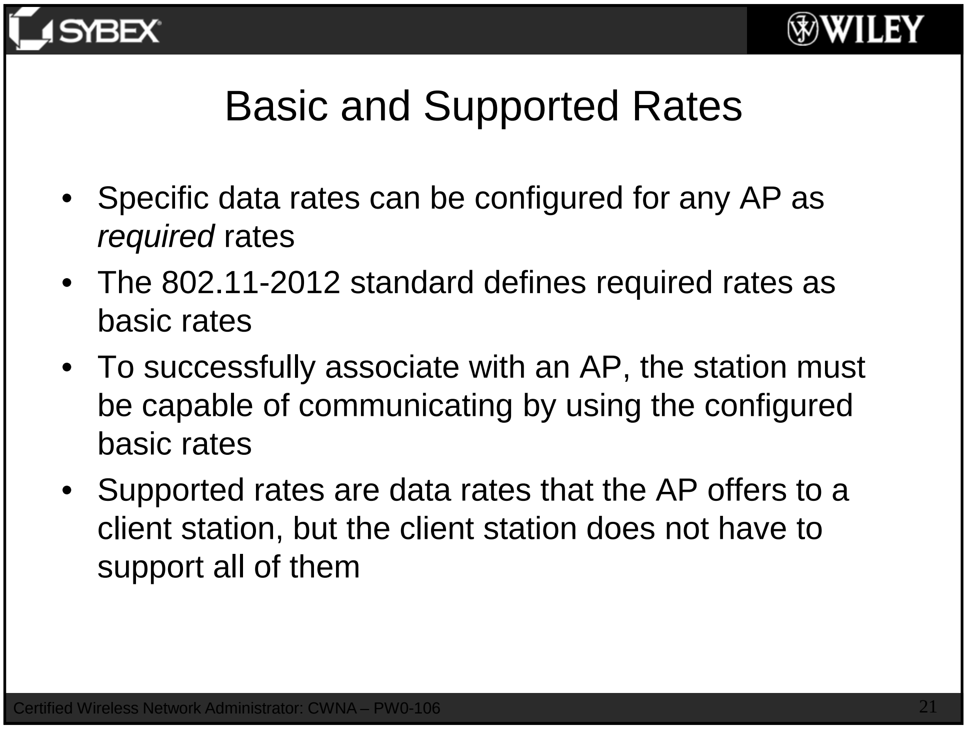
- Open System Authentication
  - Null authentication because no exchange or verification of identity takes place between the devices
- Shared Key Authentication
  - The client station sends an authentication request to the AP
  - The AP sends a cleartext challenge to the client station in an authentication response.
  - The client station then encrypts the cleartext challenge and sends it back to the AP in the body of another authentication request frame.
  - The AP then decrypts the station’s response and compares it to the challenge text

Association

- Means that the client station can send data through the AP and on to the distribution system medium.
- Occurs after Shared Key or Open System authentication
- Three states
  - State 1: initial start state, unauthenticated and unassociated
  - State 2: authenticated and unassociated
  - State 3: authenticated and associated (pending security mechanisms

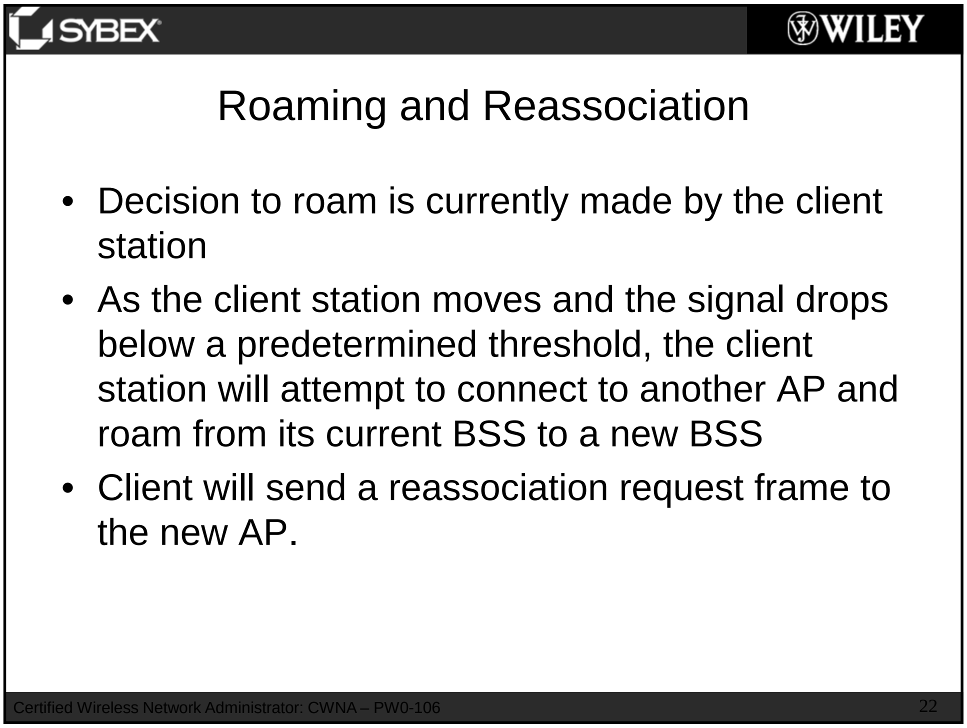
Authentication and association states





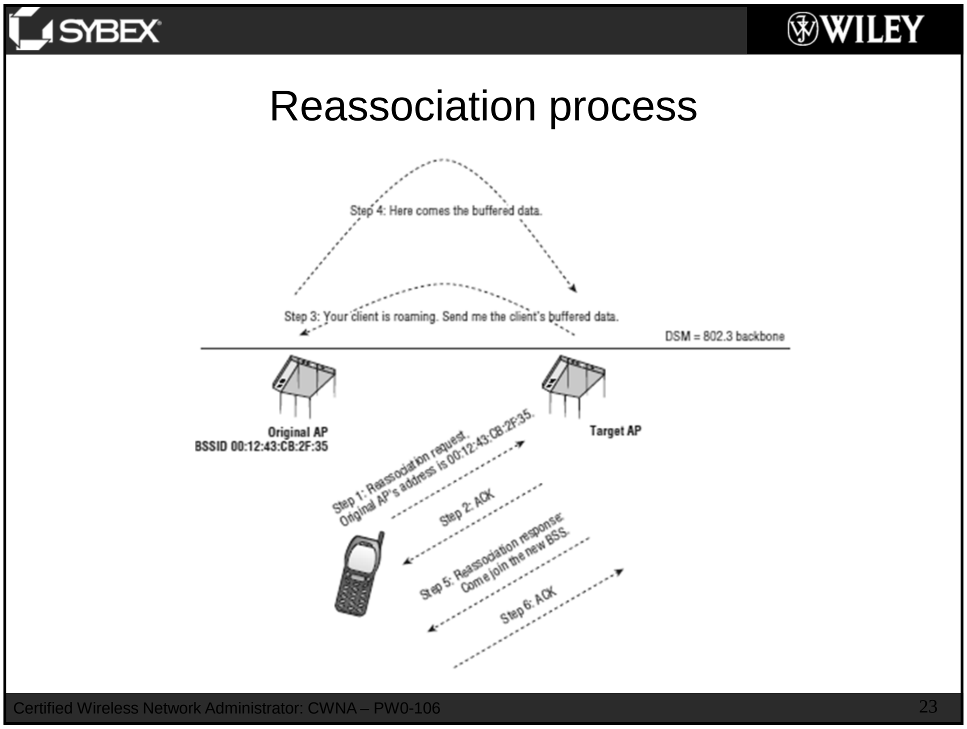
Basic and Supported Rates

- Specific data rates can be configured for any AP as *required* rates
- The 802.11-2012 standard defines required rates as basic rates
- To successfully associate with an AP, the station must be capable of communicating by using the configured basic rates
- Supported rates are data rates that the AP offers to a client station, but the client station does not have to support all of them



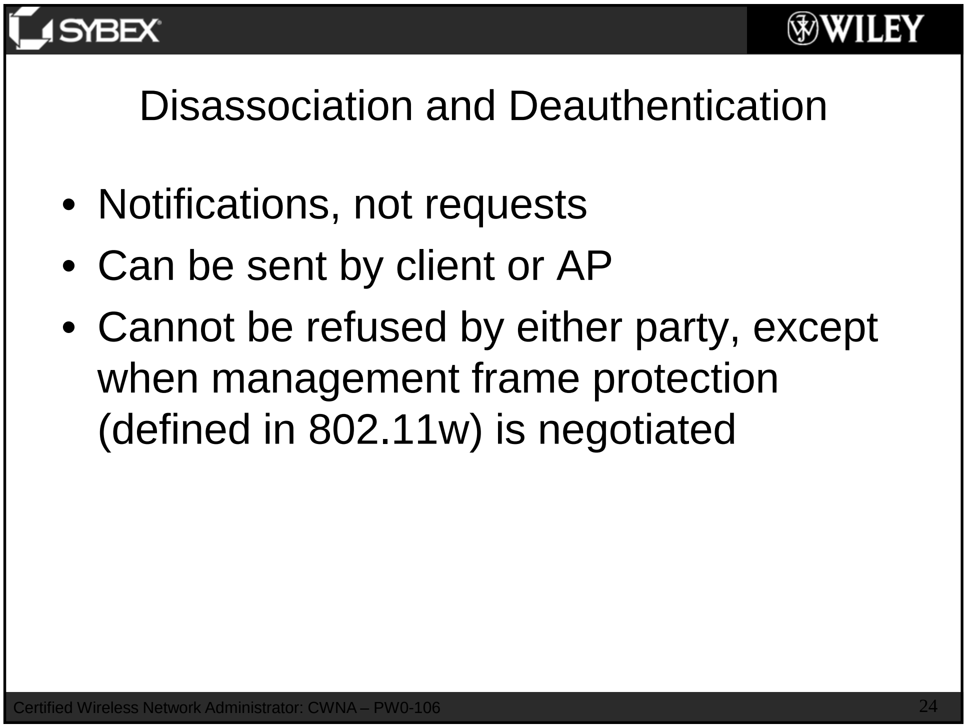
Roaming and Reassociation

- Decision to roam is currently made by the client station
- As the client station moves and the signal drops below a predetermined threshold, the client station will attempt to connect to another AP and roam from its current BSS to a new BSS
- Client will send a reassociation request frame to the new AP.



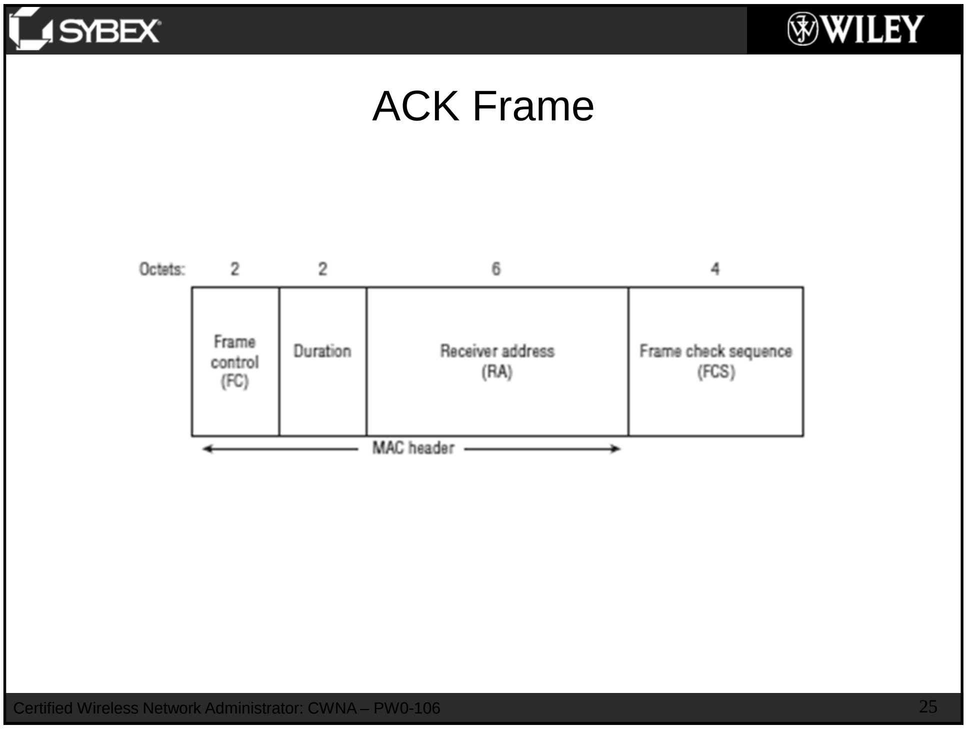
Reassociation process

Step 4: Here comes the buffered data.
Step 3: Your client is roaming. Send me the client's buffered data.
DSM = 802.3 backbone
Original AP
BSSID 00:12:43:CB:2F:35
Target AP
Step 1: Reassociation request.
Original AP's address is 00:12:43:CB:2F:35.
Step 2: ACK
Step 5: Reassociation response:
Come join the new BSS.
Step 6: ACK



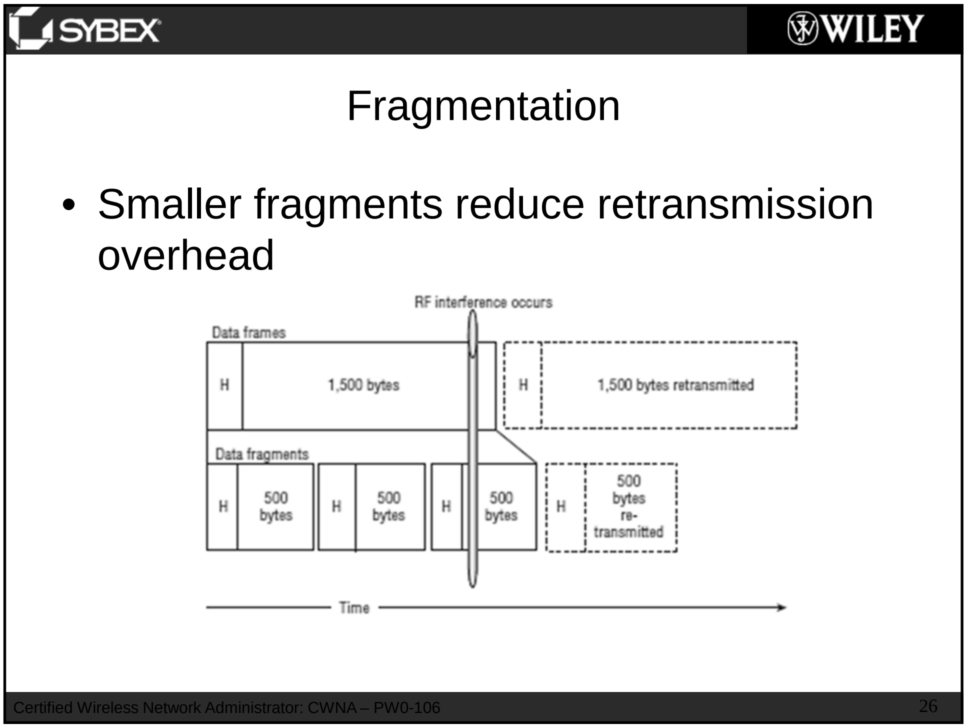
Disassociation and Deauthentication

- Notifications, not requests
- Can be sent by client or AP
- Cannot be refused by either party, except when management frame protection (defined in 802.11w) is negotiated



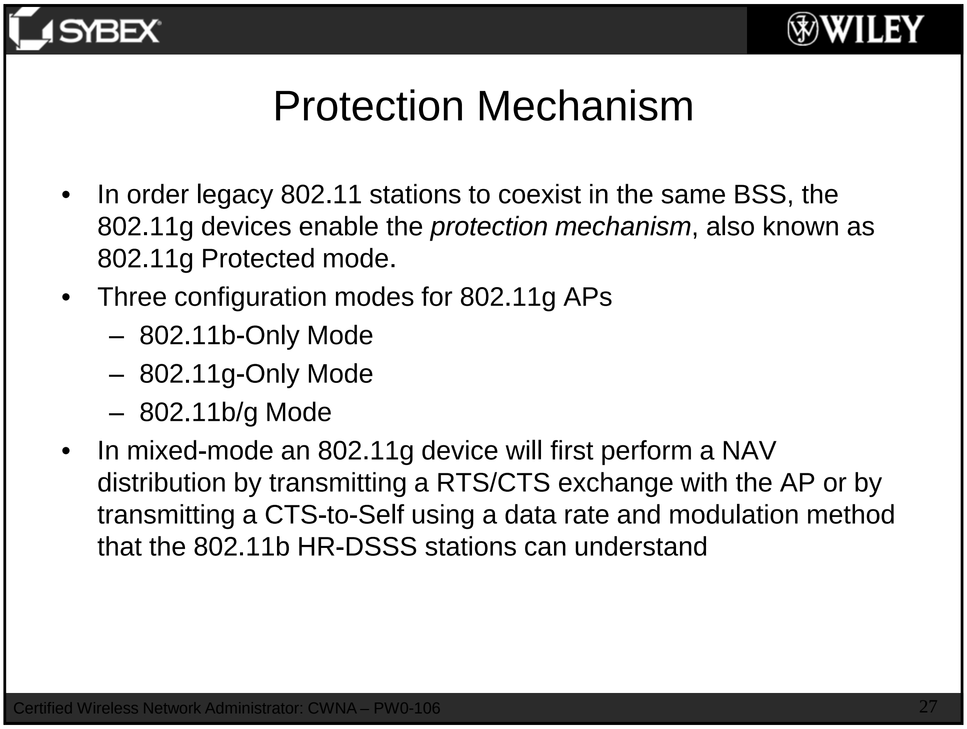
ACK Frame

Octets:	2	2	6	4
	Frame control (FC)	Duration	Receiver address (RA)	Frame check sequence (FCS)



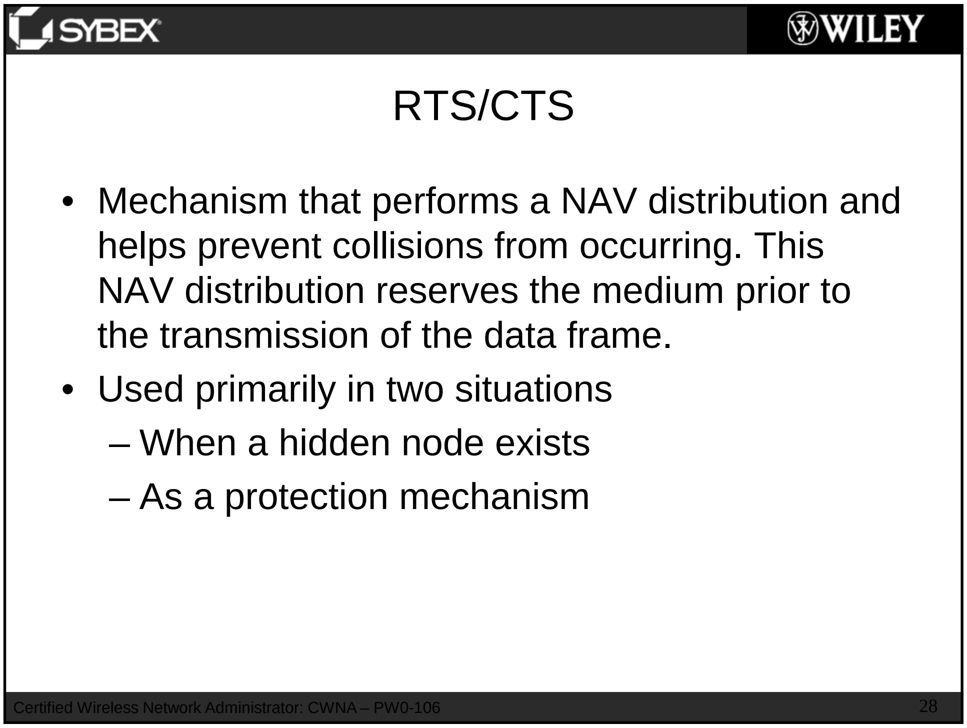
Fragmentation

- Smaller fragments reduce retransmission overhead



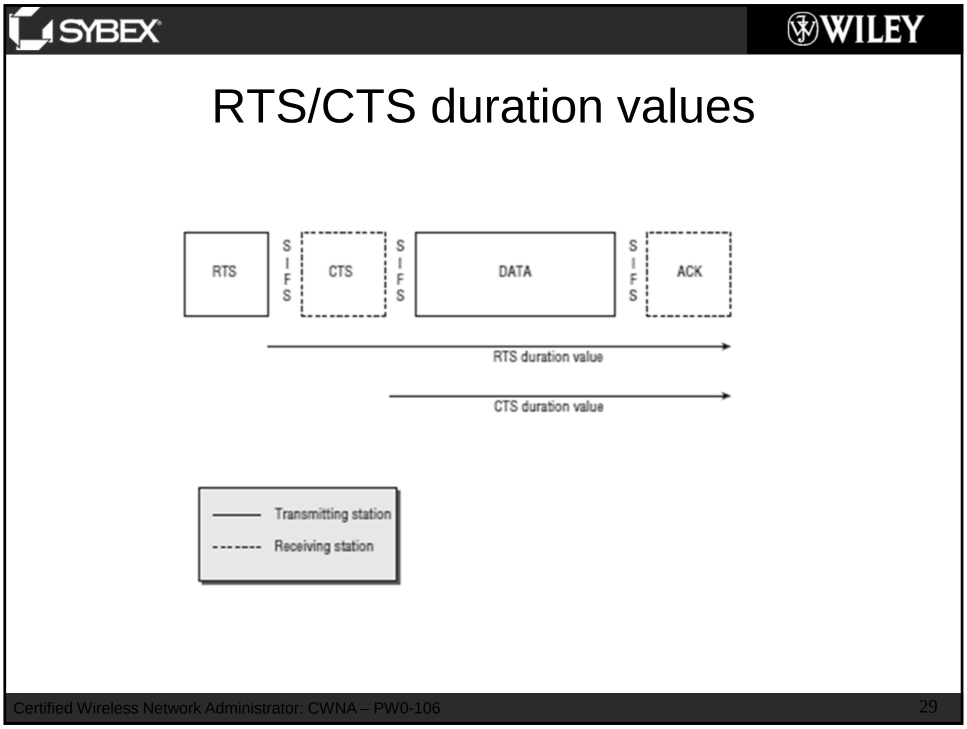
Protection Mechanism

- In order legacy 802.11 stations to coexist in the same BSS, the 802.11g devices enable the *protection mechanism*, also known as 802.11g Protected mode.
- Three configuration modes for 802.11g APs
  - 802.11b-Only Mode
  - 802.11g-Only Mode
  - 802.11b/g Mode
- In mixed-mode an 802.11g device will first perform a NAV distribution by transmitting a RTS/CTS exchange with the AP or by transmitting a CTS-to-Self using a data rate and modulation method that the 802.11b HR-DSSS stations can understand

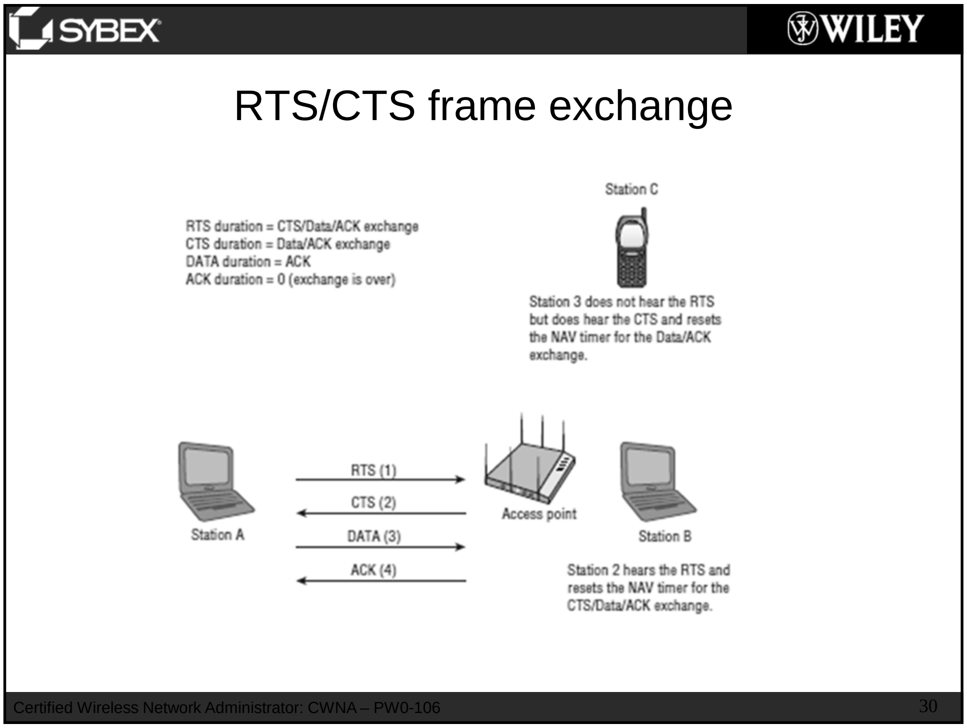


RTS/CTS

- Mechanism that performs a NAV distribution and helps prevent collisions from occurring. This NAV distribution reserves the medium prior to the transmission of the data frame.
- Used primarily in two situations
  - When a hidden node exists
  - As a protection mechanism



RTS/CTS duration values

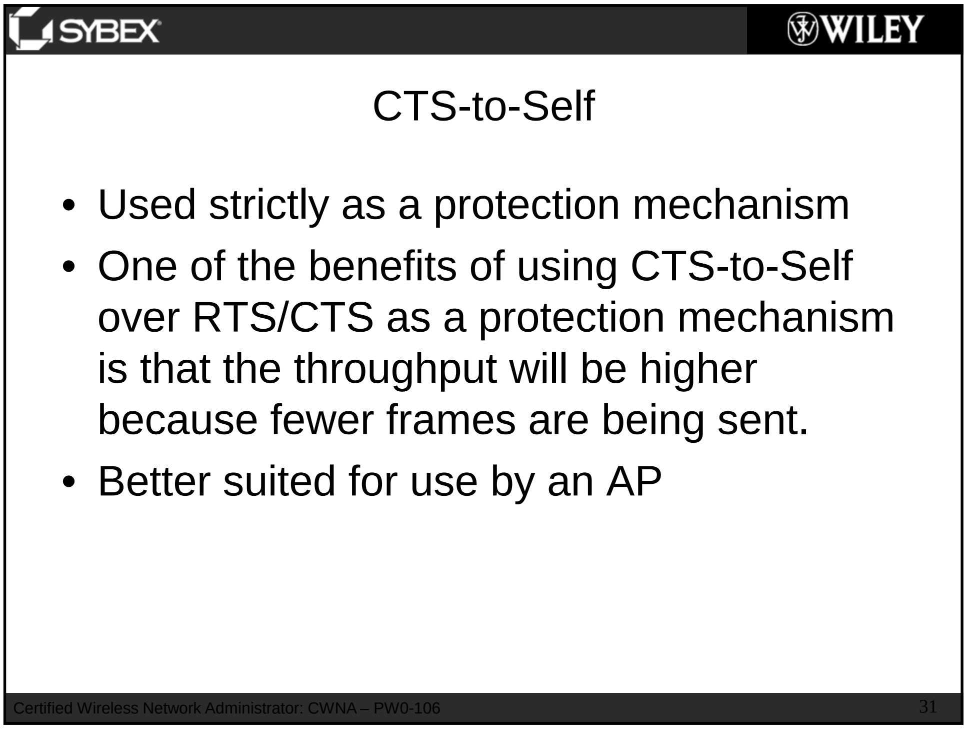


RTS/CTS frame exchange

RTS duration = CTS/Data/ACK exchange
CTS duration = Data/ACK exchange
DATA duration = ACK
ACK duration = 0 (exchange is over)

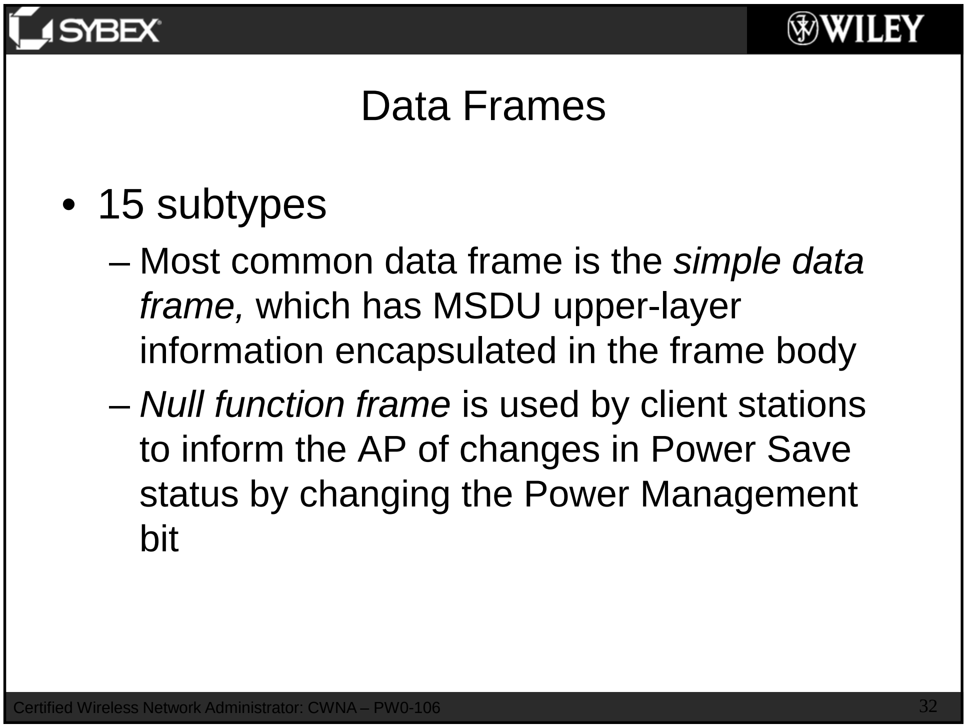
Station 3 does not hear the RTS but does hear the CTS and resets the NAV timer for the Data/ACK exchange.

Station 2 hears the RTS and resets the NAV timer for the CTS/Data/ACK exchange.



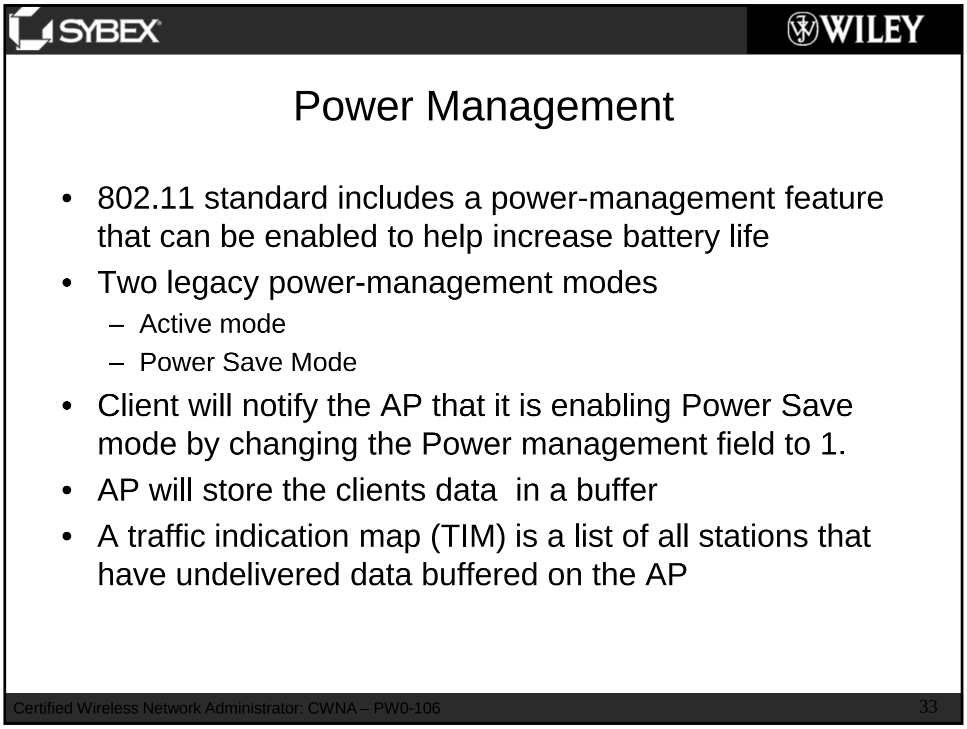
CTS-to-Self

- Used strictly as a protection mechanism
- One of the benefits of using CTS-to-Self over RTS/CTS as a protection mechanism is that the throughput will be higher because fewer frames are being sent.
- Better suited for use by an AP



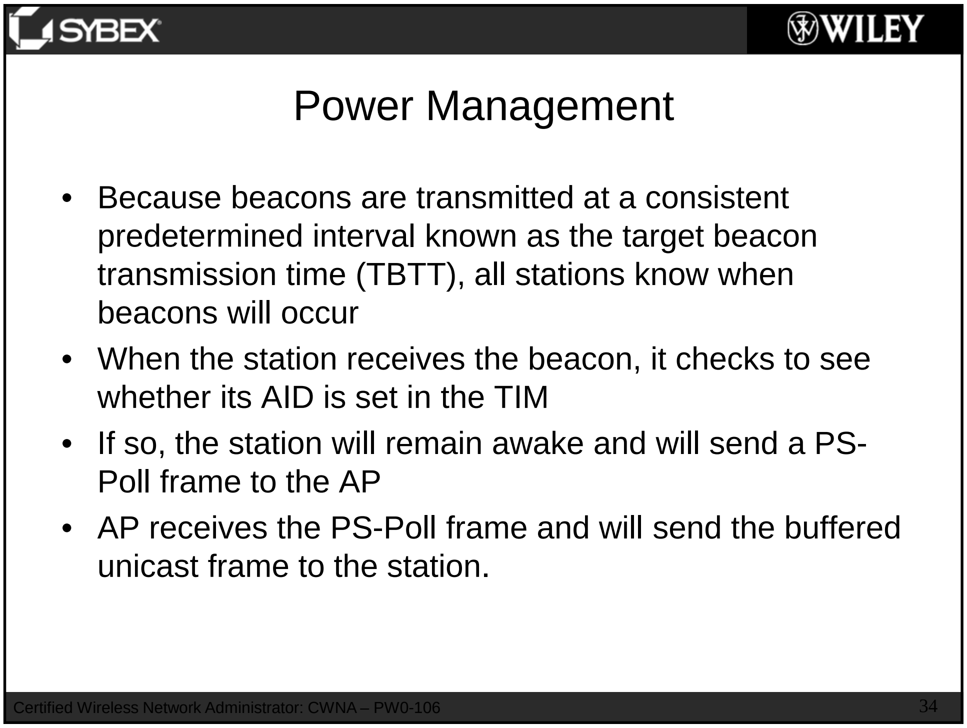
Data Frames

- 15 subtypes
  - Most common data frame is the *simple data frame,* which has MSDU upper-layer information encapsulated in the frame body
  - *Null function frame* is used by client stations to inform the AP of changes in Power Save status by changing the Power Management bit



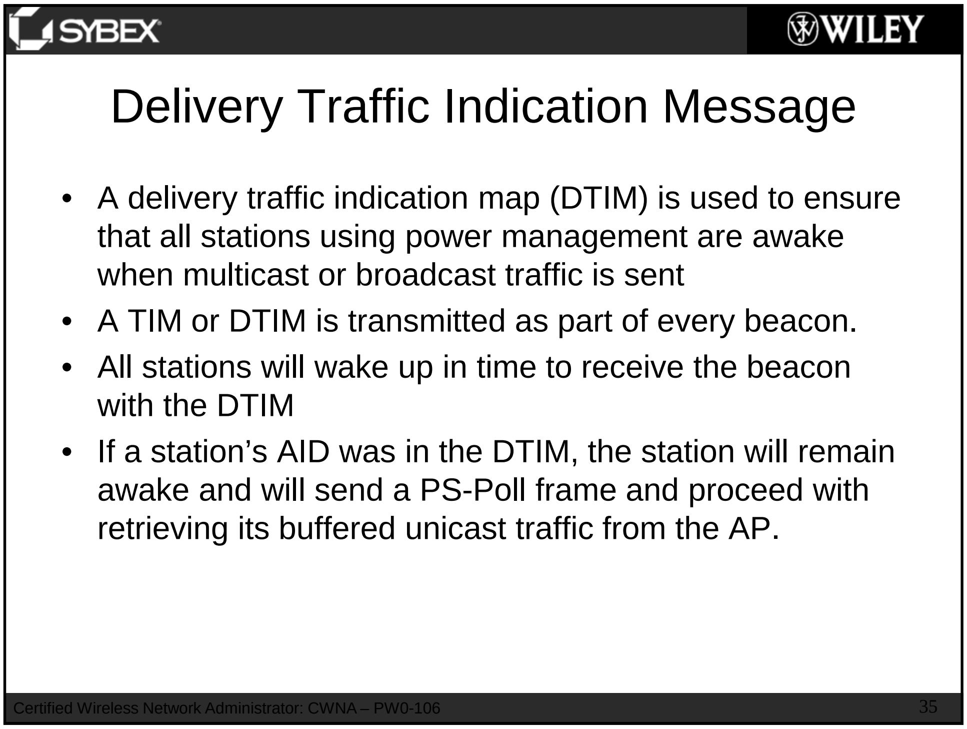
Power Management

- 802.11 standard includes a power-management feature that can be enabled to help increase battery life
- Two legacy power-management modes
  - Active mode
  - Power Save Mode
- Client will notify the AP that it is enabling Power Save mode by changing the Power management field to 1.
- AP will store the clients data in a buffer
- A traffic indication map (TIM) is a list of all stations that have undelivered data buffered on the AP



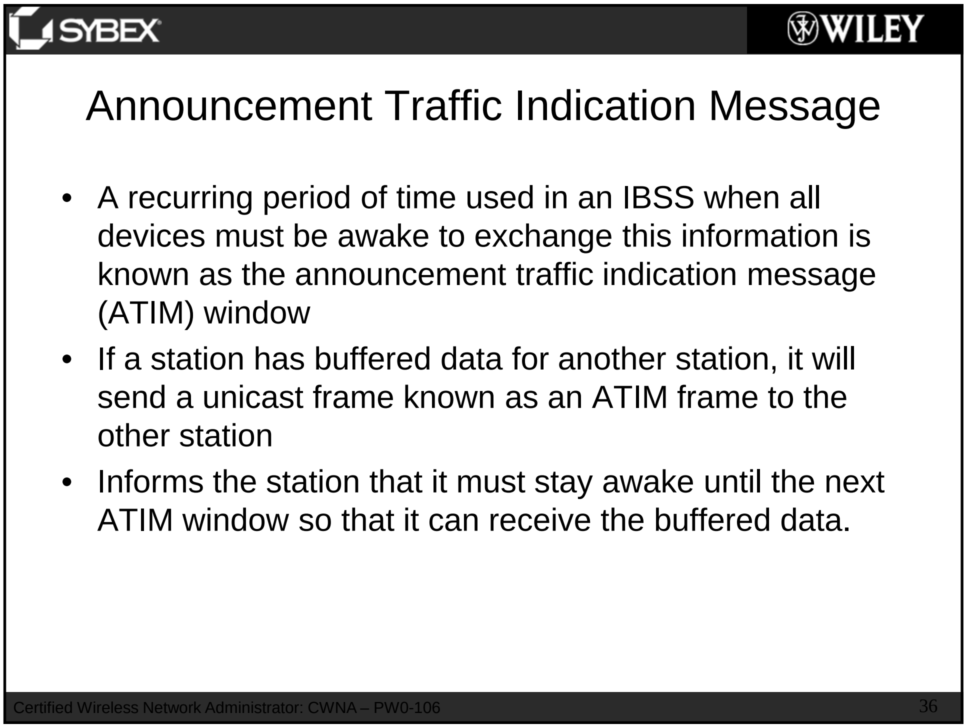
Power Management

- Because beacons are transmitted at a consistent predetermined interval known as the target beacon transmission time (TBTT), all stations know when beacons will occur
- When the station receives the beacon, it checks to see whether its AID is set in the TIM
- If so, the station will remain awake and will send a PS-Poll frame to the AP
- AP receives the PS-Poll frame and will send the buffered unicast frame to the station.



Delivery Traffic Indication Message

- A delivery traffic indication map (DTIM) is used to ensure that all stations using power management are awake when multicast or broadcast traffic is sent
- A TIM or DTIM is transmitted as part of every beacon.
- All stations will wake up in time to receive the beacon with the DTIM
- If a station's AID was in the DTIM, the station will remain awake and will send a PS-Poll frame and proceed with retrieving its buffered unicast traffic from the AP.



Announcement Traffic Indication Message

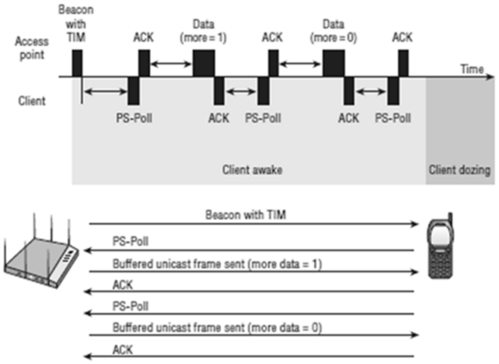
- A recurring period of time used in an IBSS when all devices must be awake to exchange this information is known as the announcement traffic indication message (ATIM) window
- If a station has buffered data for another station, it will send a unicast frame known as an ATIM frame to the other station
- Informs the station that it must stay awake until the next ATIM window so that it can receive the buffered data.

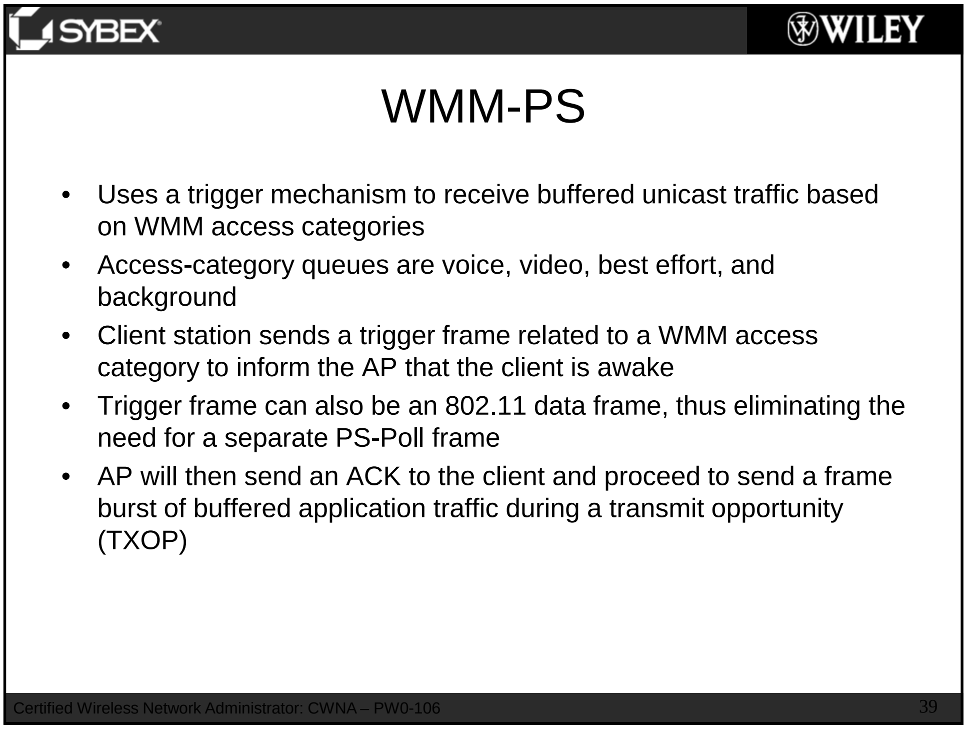
WMM Power Save and U-APSD

- IEEE 802.11e amendment introduced an enhanced power-management method called *automatic power save delivery*
- Two APSD methods are defined
  - Scheduled automatic power save delivery (S-APSD)
  - Unscheduled automatic power save delivery (U-APSD).
- Wi-Fi Alliance’s WMM Power Save (WMM-PS) certification is based on U-APSD
  - Goal of WMM-PS is to have client devices spend more time in a doze state and consume less power

Legacy power management limitations

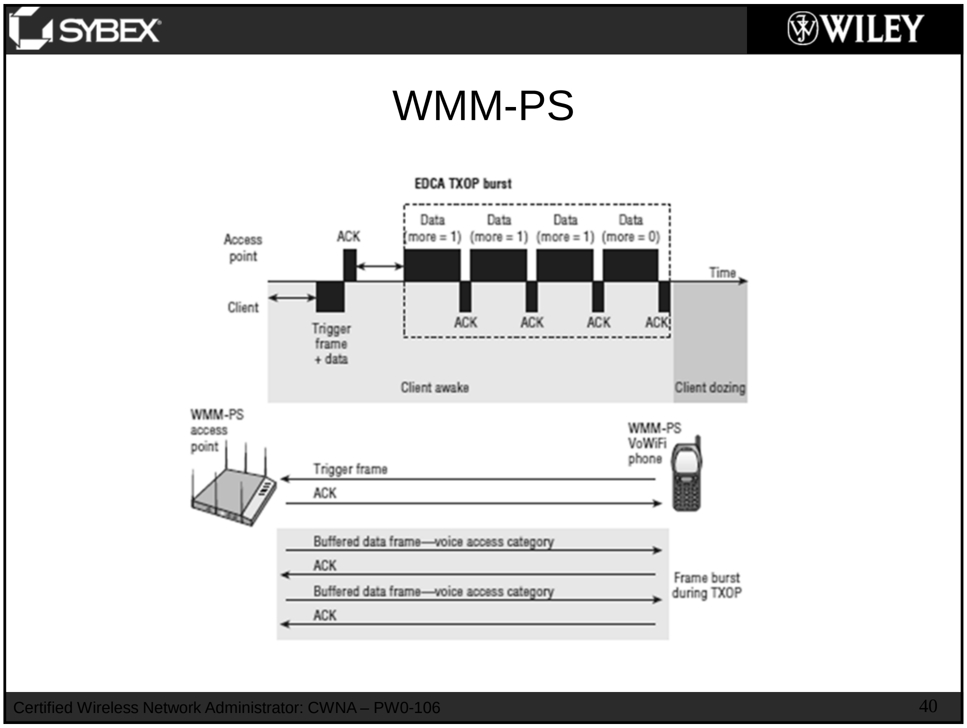
- Client must first wait for a beacon with a TIM and must also send a unique PS-Poll frame to the AP for every single buffered unicast frame



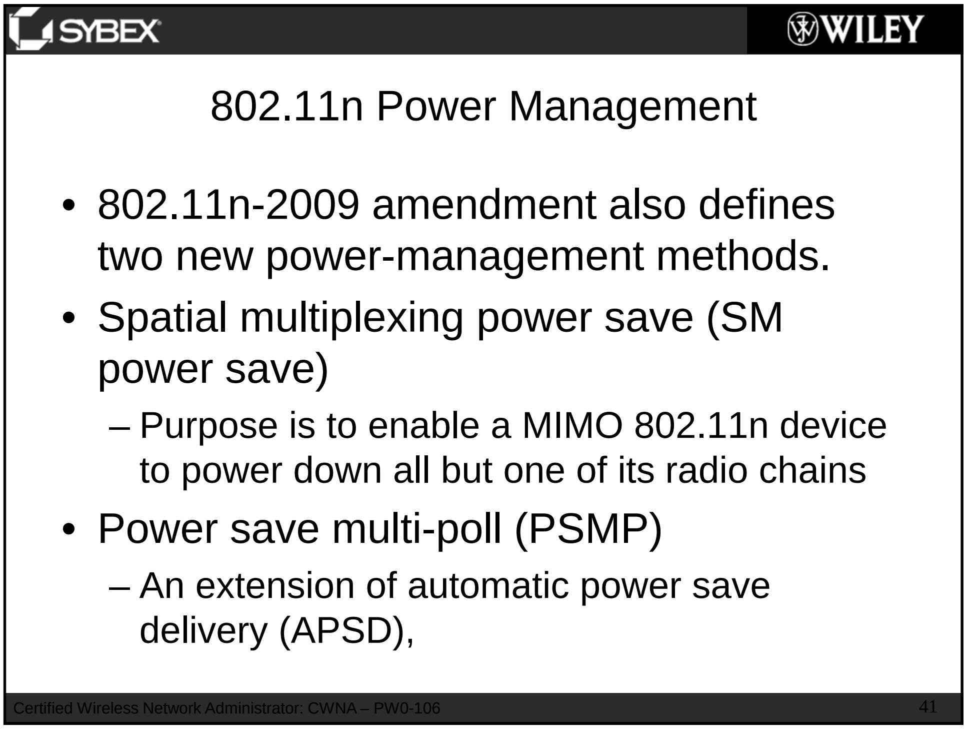


WMM-PS

- Uses a trigger mechanism to receive buffered unicast traffic based on WMM access categories
- Access-category queues are voice, video, best effort, and background
- Client station sends a trigger frame related to a WMM access category to inform the AP that the client is awake
- Trigger frame can also be an 802.11 data frame, thus eliminating the need for a separate PS-Poll frame
- AP will then send an ACK to the client and proceed to send a frame burst of buffered application traffic during a transmit opportunity (TXOP)

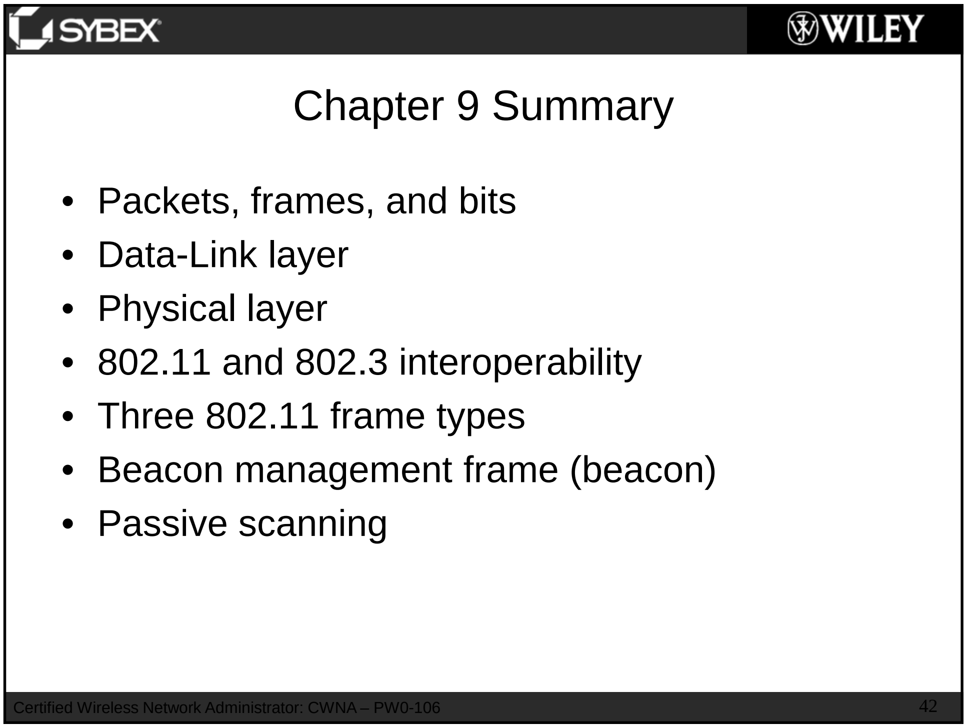


WMM-PS



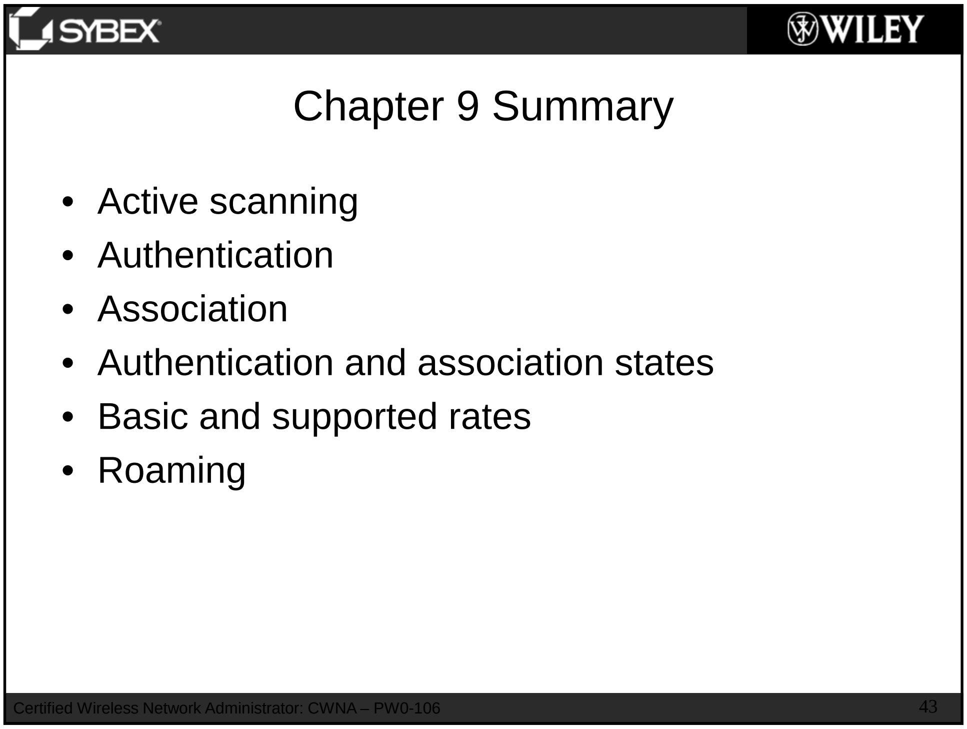
802.11n Power Management

- 802.11n-2009 amendment also defines two new power-management methods.
- Spatial multiplexing power save (SM power save)
  - Purpose is to enable a MIMO 802.11n device to power down all but one of its radio chains
- Power save multi-poll (PSMP)
  - An extension of automatic power save delivery (APSD),



Chapter 9 Summary

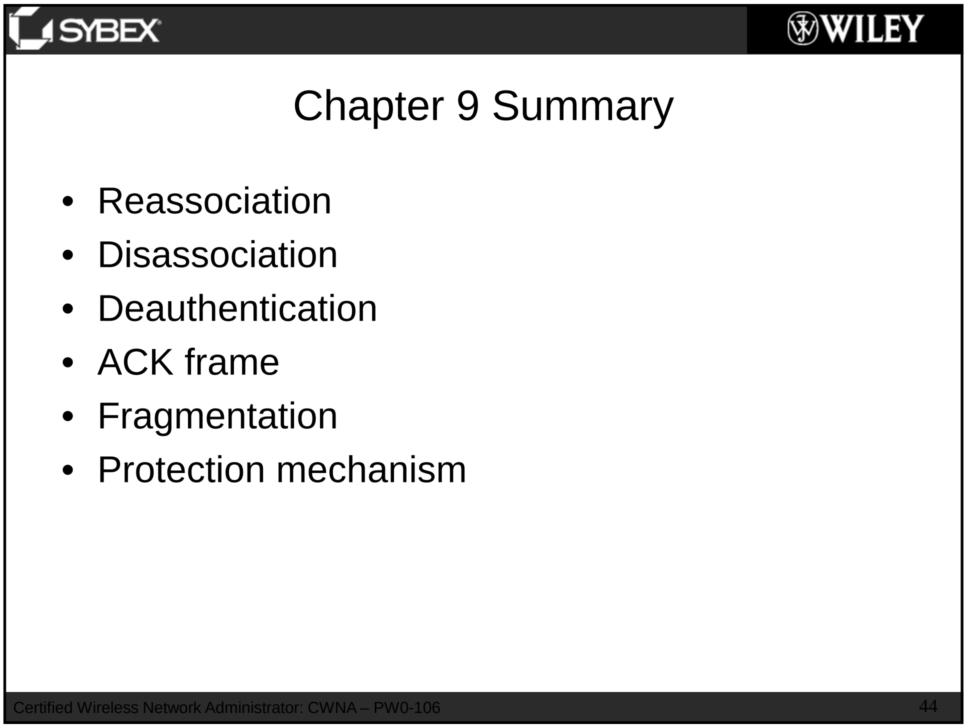
- Packets, frames, and bits
- Data-Link layer
- Physical layer
- 802.11 and 802.3 interoperability
- Three 802.11 frame types
- Beacon management frame (beacon)
- Passive scanning



Chapter 9 Summary

- Active scanning
- Authentication
- Association
- Authentication and association states
- Basic and supported rates
- Roaming

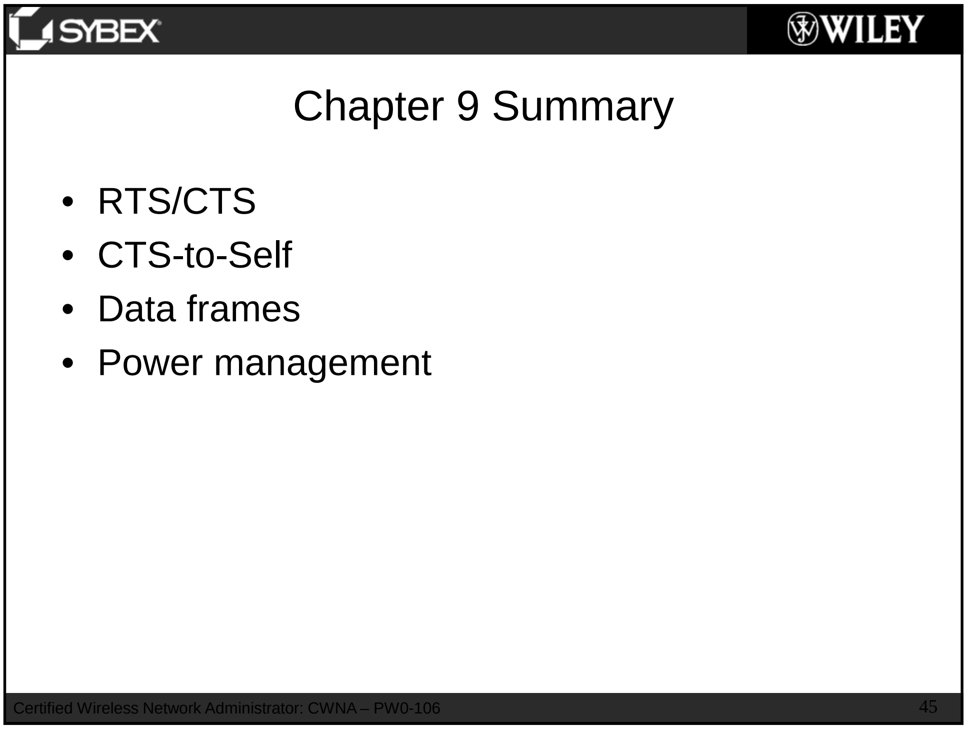
Certified Wireless Network Administrator: CWNA – PW0-106 43



Chapter 9 Summary

- Reassociation
- Disassociation
- Deauthentication
- ACK frame
- Fragmentation
- Protection mechanism

Certified Wireless Network Administrator: CWNA – PW0-106 44



Chapter 9 Summary

- RTS/CTS
- CTS-to-Self
- Data frames
- Power management

Certified Wireless Network Administrator: CWNA – PW0-106 45