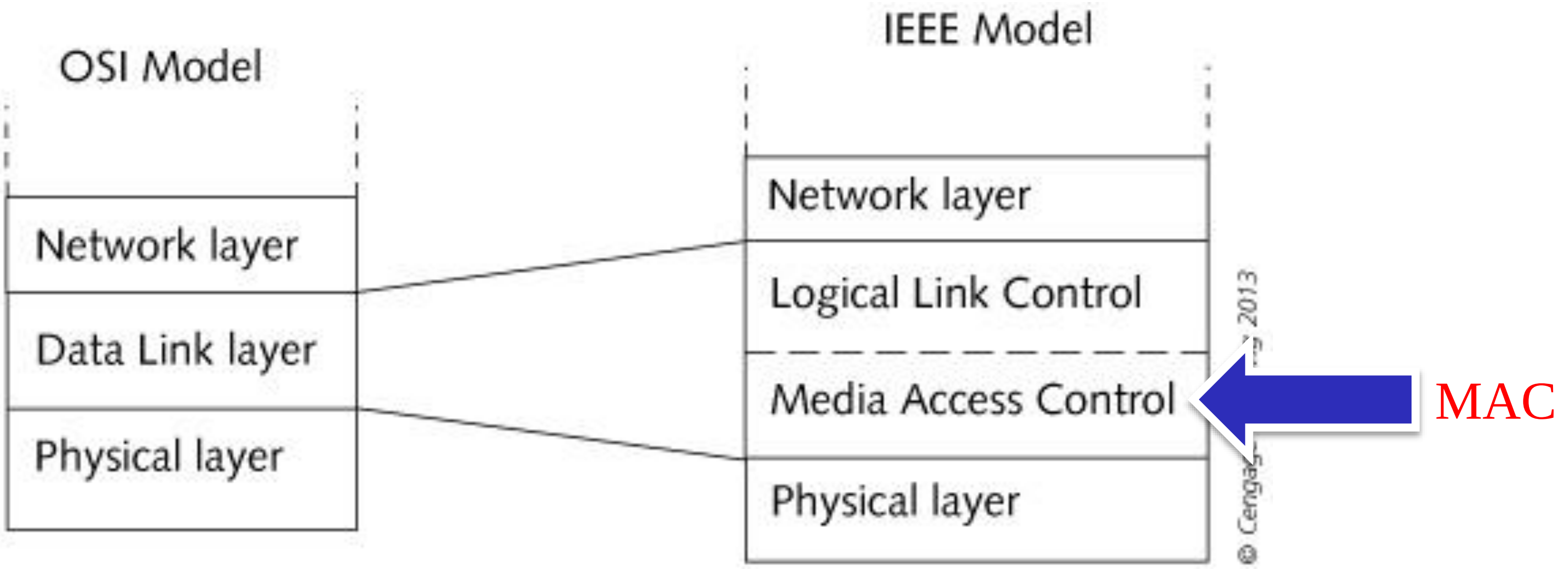
CWNA Guide to Wireless LANs, Third Edition

Chapter 6: Medium Access Control (MAC) Layer Standards

(Data Link)

MAC Layer


OSI Model
Network layer
Data Link layer
Physical layer
IEEE Model
Network layer
Logical Link Control
Media Access Control
Physical layer
MAC
© Cengage Learning 2013

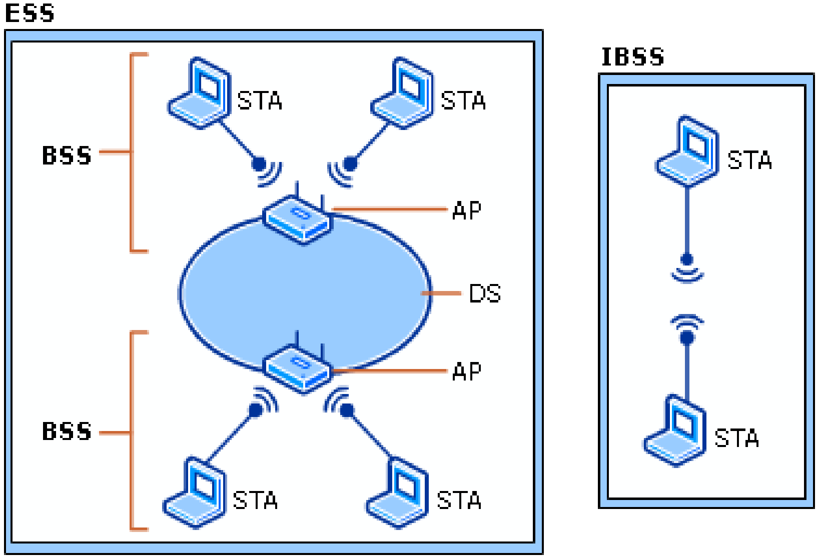
Objectives

- Describe the three WLAN service sets
- Explain the features of MAC frames and MAC frame types
- Describe the MAC functions of discovering, joining, and transmitting on a WLAN

WLAN Service Sets

- **Service set**: all of the devices that are associated with an 802.11 WLAN

- Three different WLAN service set configurations:
  - Basic Service Set (BSS)
  - Extended Service Set (ESS)
  - Independent Basic Service Set (IBSS)



Basic Service Set

- **Basic Service Set (BSS):** Group of wireless devices served by single AP
  - **Basic Service Set Identifier (BSSID)**
    - Media access control (MAC) address of the AP

- BSS must be assigned unique identifier
  - **Service Set Identifier (SSID)**
    - Serves as "network name" for BSS

- **Basic Service Area (BSA):** Geographical area of a BSS
  - Max BSA for a WLAN depends on many factors

- **Dynamic rate shifting:** As mobile devices move away from AP, transmission speed decreases

Basic Service Set

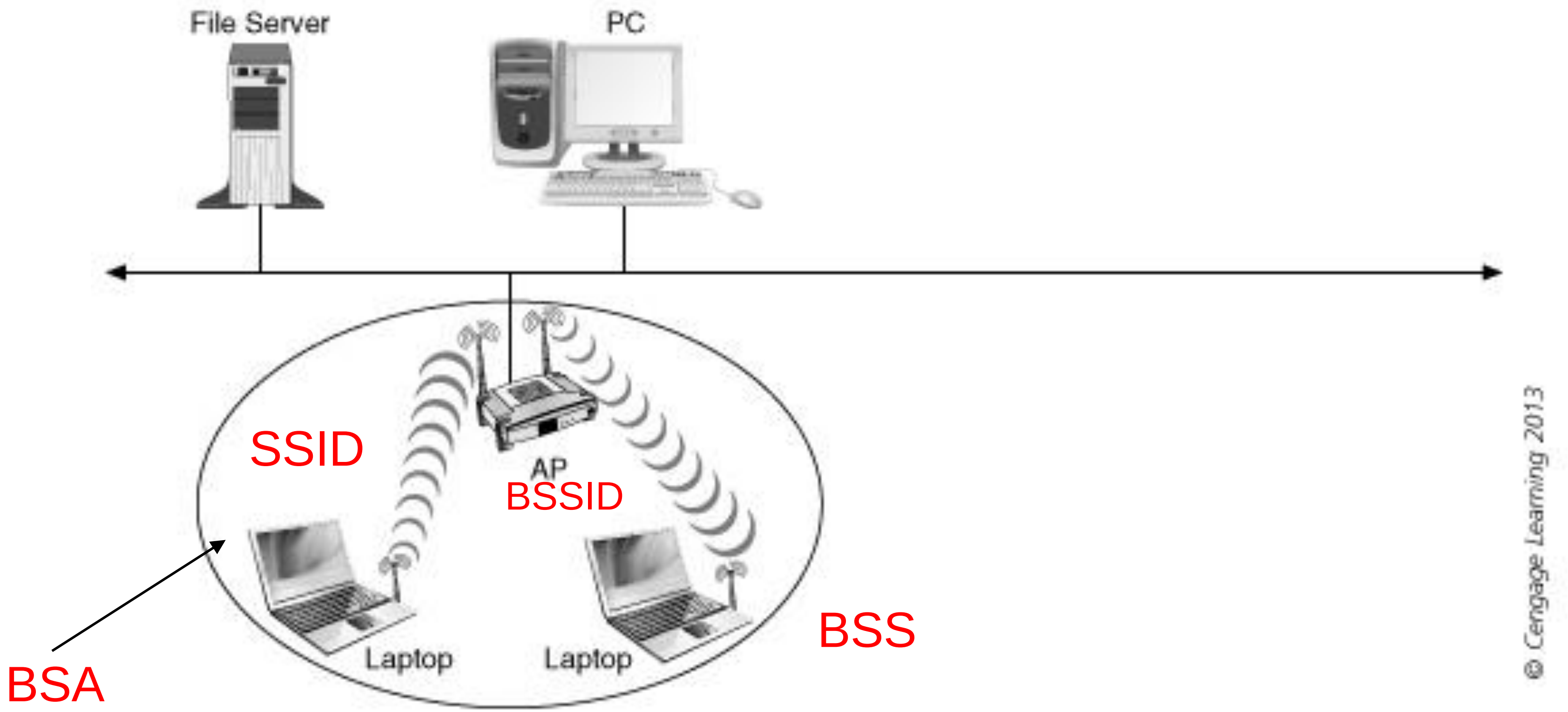


Figure 6-1 Basic Service Set (BSS)

Extended Service Set-1

- **Extended Service Set (ESS):** Comprised of two or more BSS networks connected via a common distribution system

- APs can be positioned so that cells overlap to facilitate **roaming**
  - Wireless devices choose AP based on signal strength
  - While moving, if a mobile device finds an AP with a stronger signal, the device associates with the new AP (process is called a **handoff**)
  - **Layer 2** roaming: occurs between APs on the same subnet

Extended Service Set-2

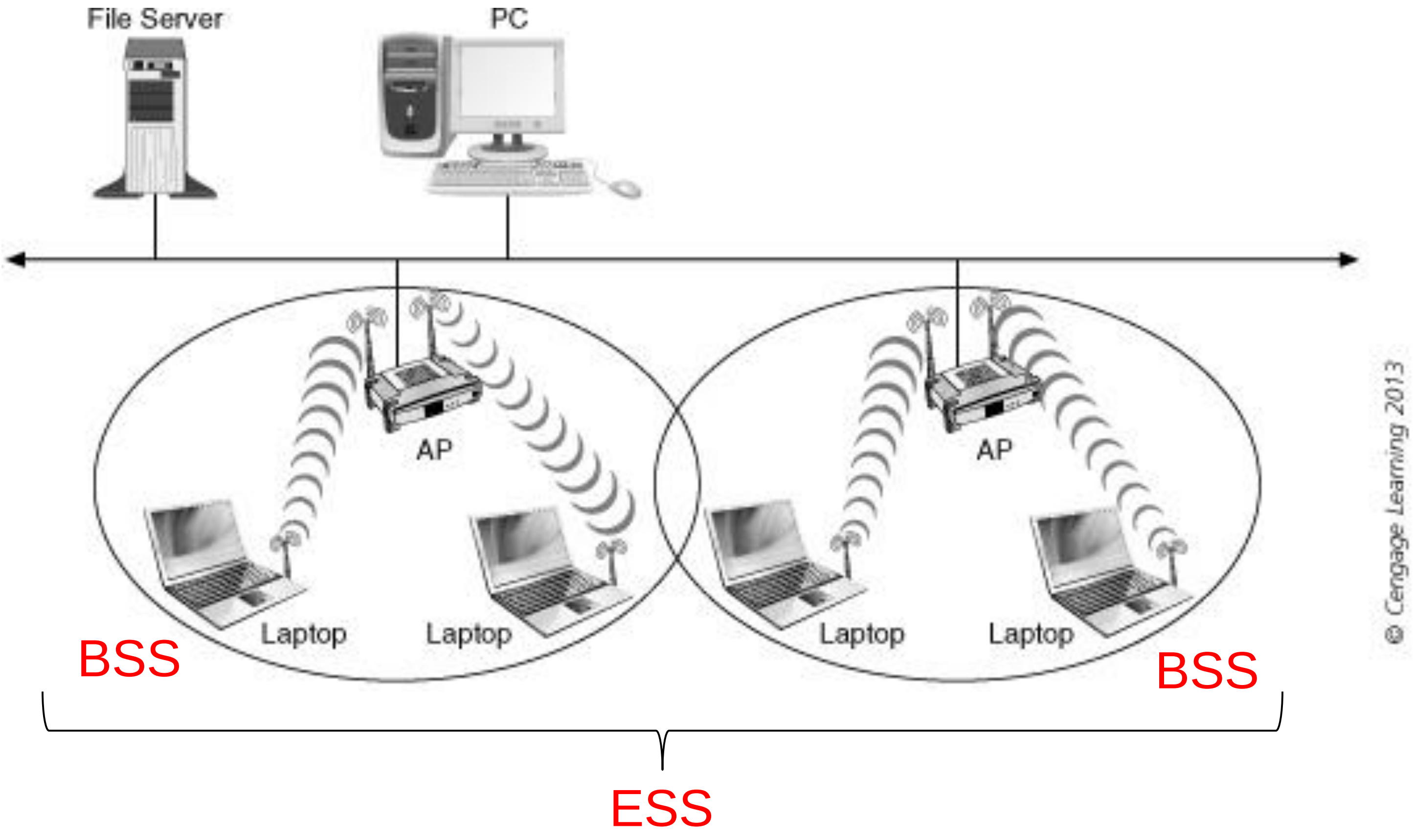


Figure 6-2 Extended Service Set (ESS)

Extended Service Set-3

- If a router separates the APs and each AP resides in a separate subnet, a new IP address must be assigned
  - Connectivity can be temporarily lost
  - Running applications may have to be restarted
  - Called **Layer 3 roaming**
- **Mobile IP**: mechanism within the TCP/IP protocol to better support mobile computing

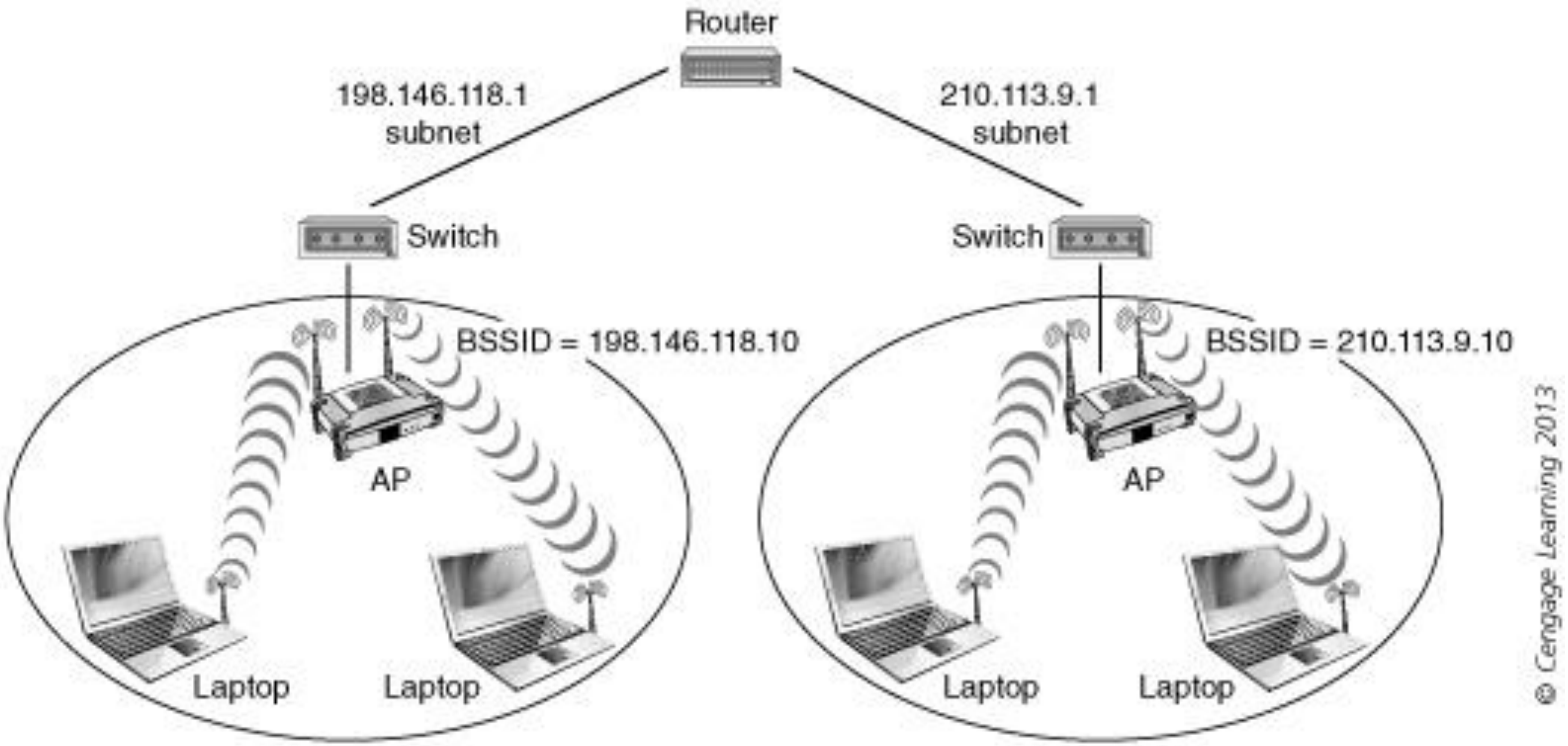
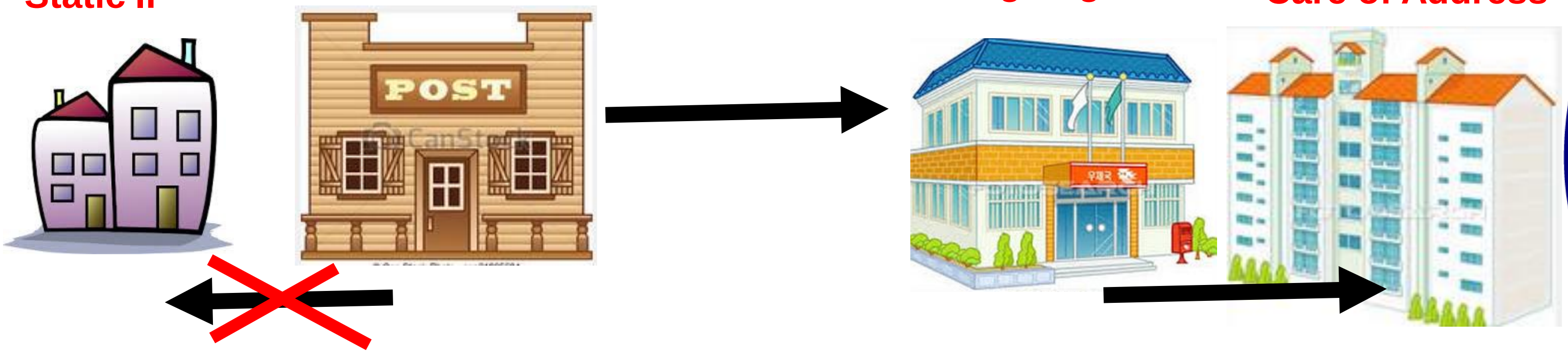


Figure 6-3 Layer 3 roaming

Mobile IP-1

- An analogy: what do you do when moving from one apartment to another?
  - Leave a forwarding address with your old post-office!
  - The old post-office forwards mails to your new post-office, which then forwards them to you
- Mobile IP:
  - Two other entities – home agent (old post-office), foreign agent (new post-office)
  - Mobile host registers with home agent the new location
  - Home agent captures packets meant for mobile host, and forwards it to the foreign agent, which then delivers it to the mobile host



Mobile IP-1

- With mobile IP, computers are given a **home address** (**Static IP** number on home network)
  - **Home agent**: forwarding mechanism that keeps track of where the mobile computer is located
  - When the computer roams to another network (**foreign network**) a **foreign agent** provides routing services to the computer
  - Foreign agent assigns a temporary IP number (known as **care-of-address**)
  - Computer then registers the care-of-address with its home agent

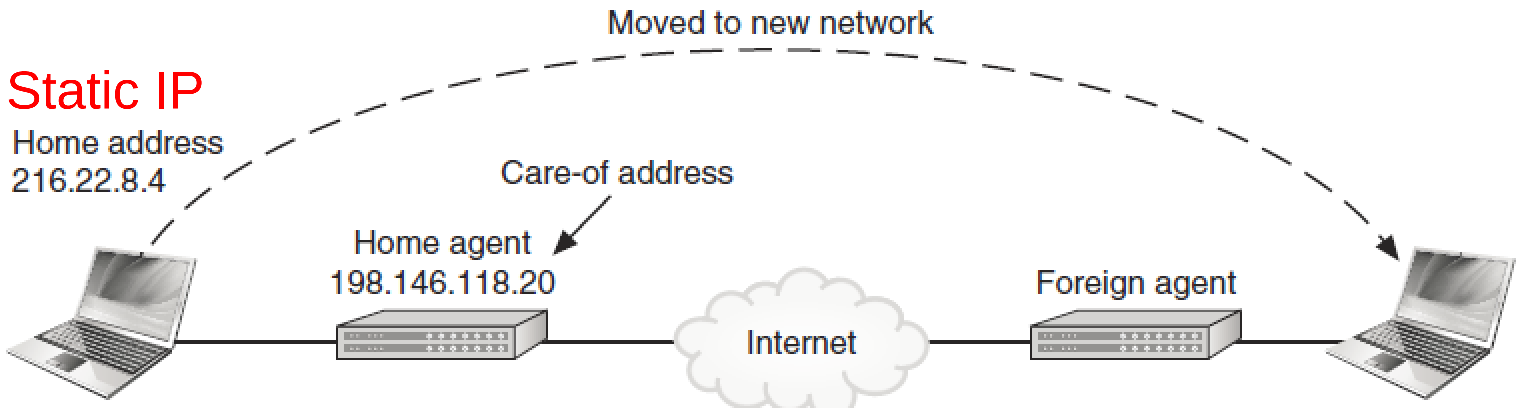


Figure 6-4 Computer relocated in Mobile IP

Mobile IP-2

- Mobile IP (continued):
  - When a frame is sent to computer's home address, the home agent intercepts the frame
  - Encapsulates that frame into a new frame with the care-of-address as the destination address
  - Redirects it to the foreign agent, which send it to the computer located on the foreign network

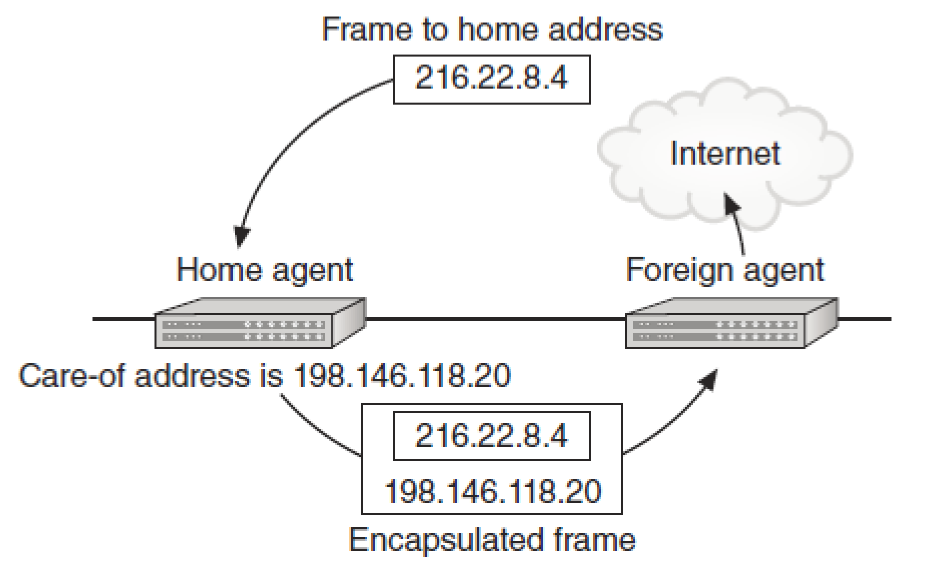
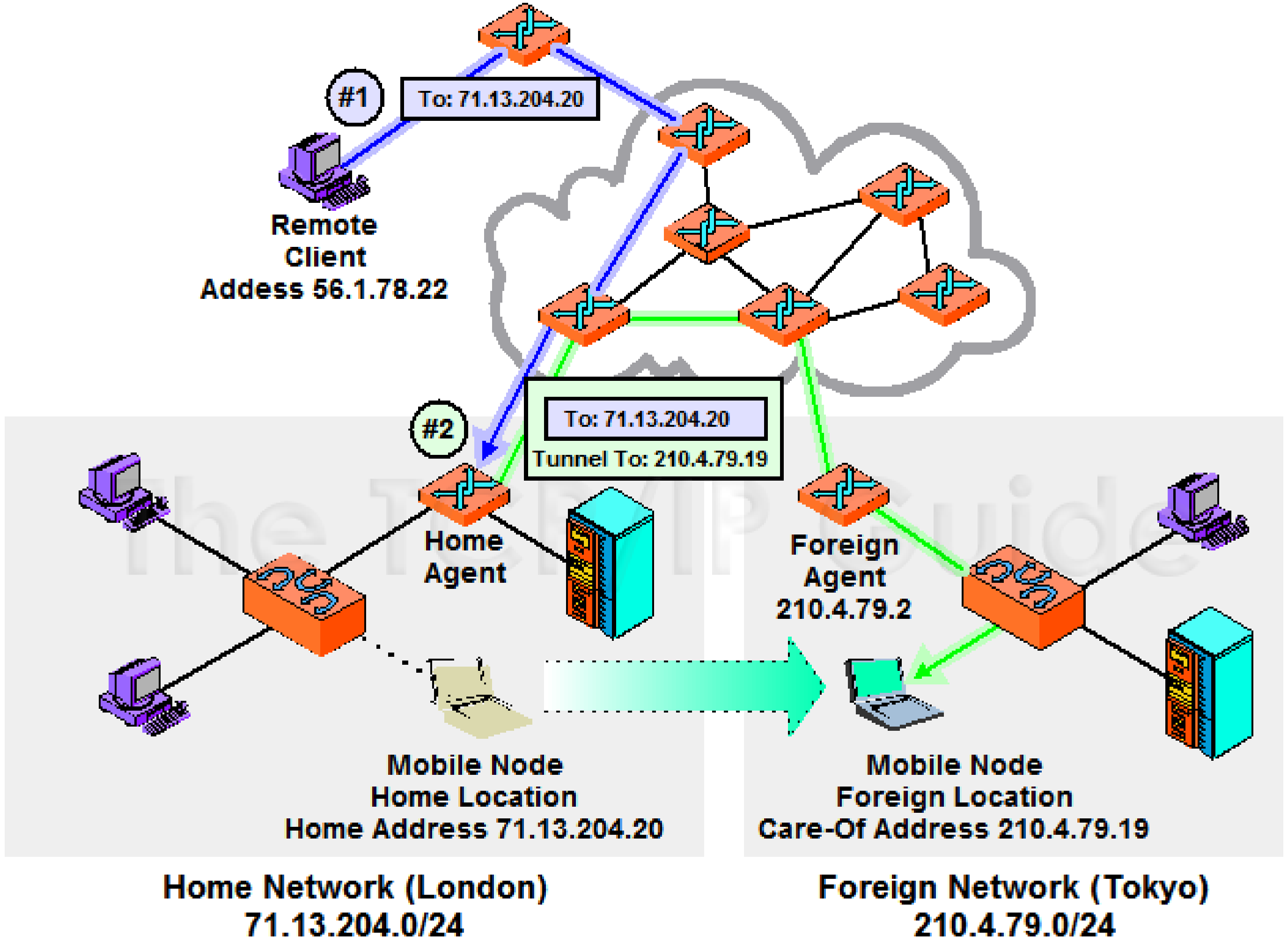


Figure 6-5 Encapsulated Mobile IP frame

© 2013 Cengage Learning

Mobile IP-2

- Mobile IP Example:



Mobile IP-3

- Mobile IP enables a host to be identified by a single IP number even as it moves from one network to another

Extended Service Set

- **Distribution system (DS):** used by an AP to determine what communication needs to take place with other APs in the ESS or with the wired network
  - Decides if it is necessary to exchange frames in their own BSSs, with a wired network, or to forward frames to another BSS
- **Distribution system media**: media that interconnects APs
- A wireless configuration that is used to connect APs is called a **wireless distribution system (WDS)**

Independent Basic Service Set

- **Infrastructure mode:** wireless network that communicates through an AP

- **Independent Basic Service Set (IBSS):** Wireless network that does not use an AP
  - Wireless devices communicate between themselves
  - **Peer-to-peer** or **ad hoc mode**
- BSS more flexible than IBSS in being able to connect to other wired or wireless networks
- IBSS useful for quickly and easily setting up wireless network
  - When no connection to Internet or external network needed

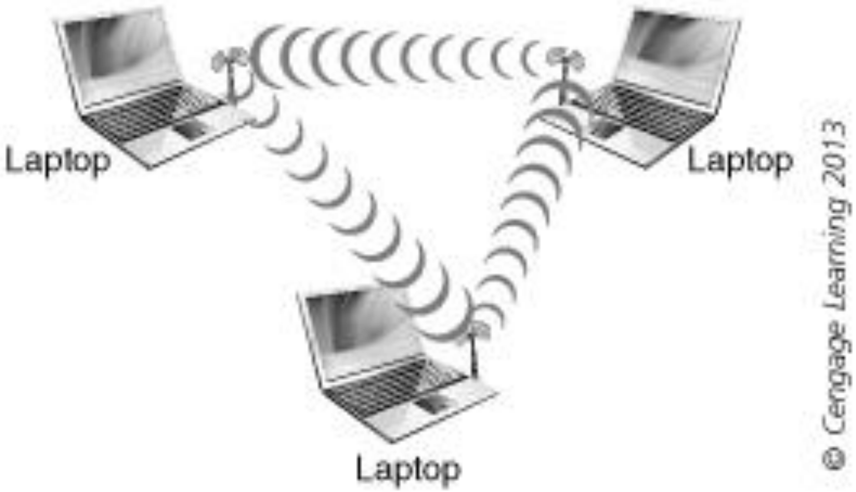
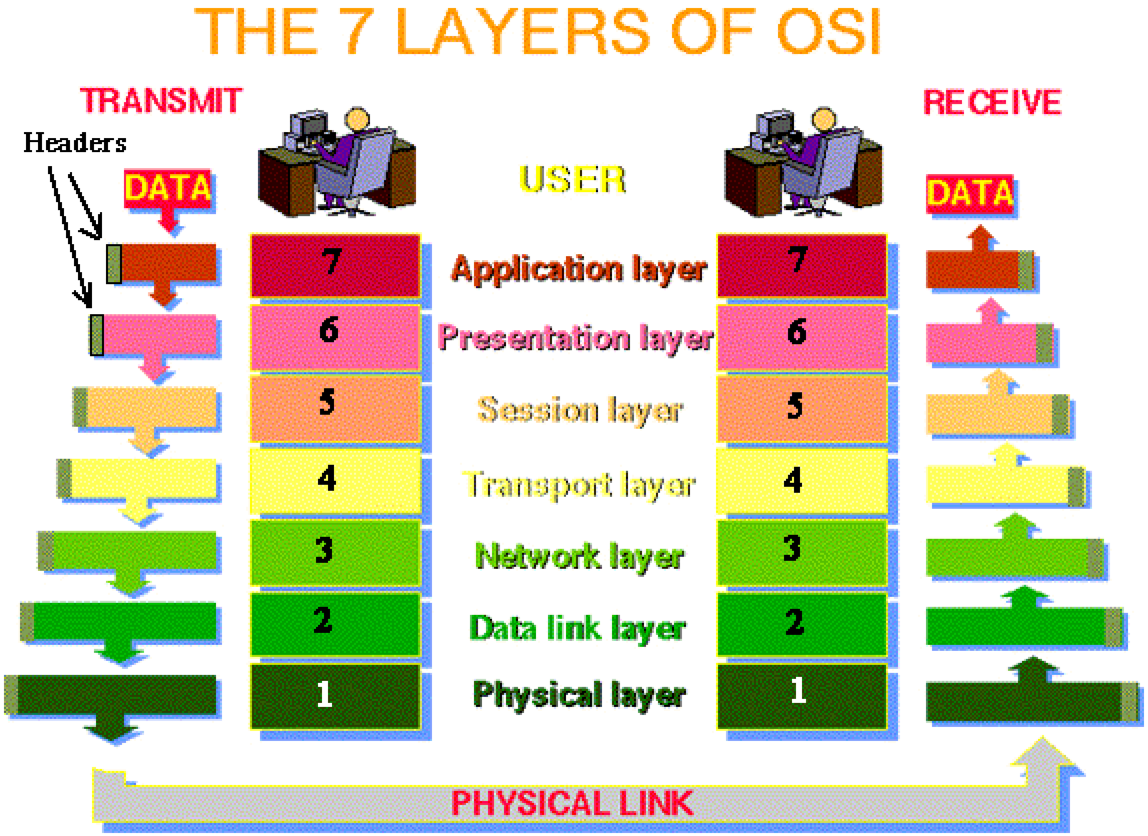


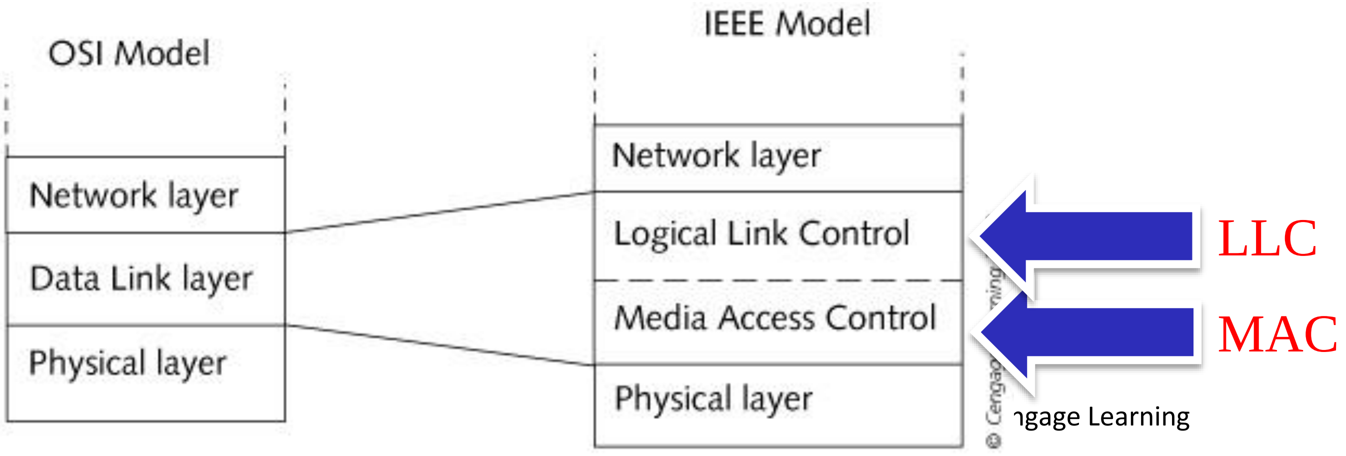
Figure 6-6 Independent Basic Service Set (IBSS)

802.11 Medium Access Control Layer (MAC) Frame Formats and Types



802.11 Medium Access Control Layer (MAC) Frame Formats and Types

- IEEE has divided the Data Link Layer into two sublayers:
  - Logical Link Control (LLC) sublayer: provides a common interface, reliability, and flow control
  - Medium Access Control (MAC) sublayer: appends physical addresses to the frame
    - Functions performed at the MAC sublayer involve different frame formats and types



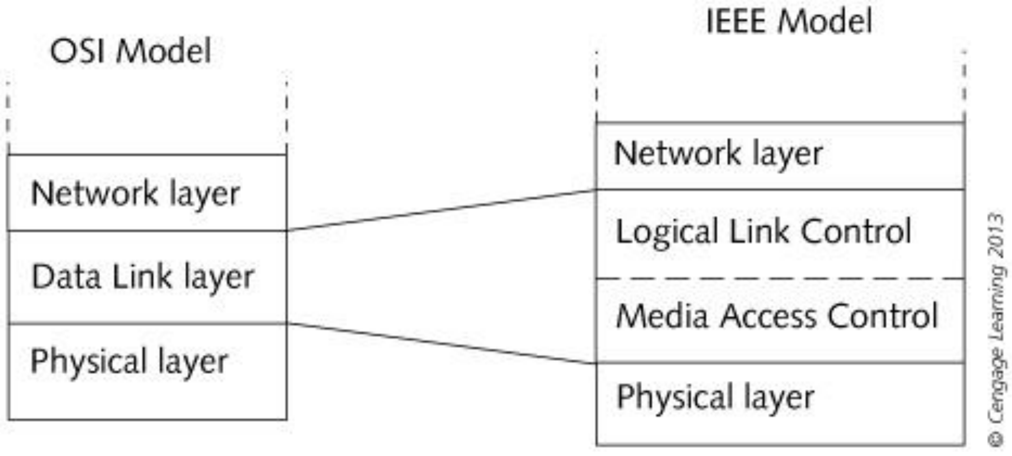
MAC Frame Formats

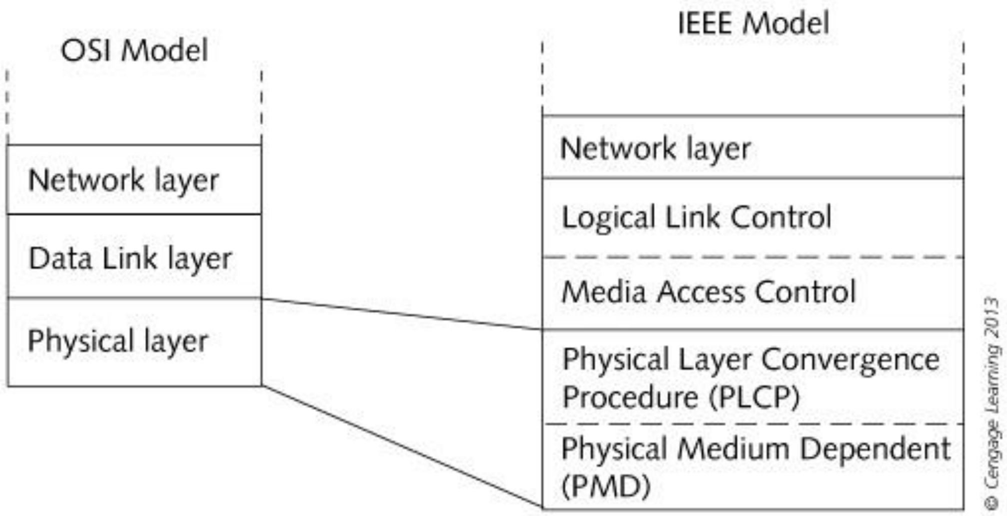
- OSI model uses the term *data unit* to describe sets of data that move through the OSI layers

- **Service Data Unit (SDU)**: specific unit of data that has been passed down from a higher OSI layer to a lower layer but has not yet been encapsulated by that lower layer

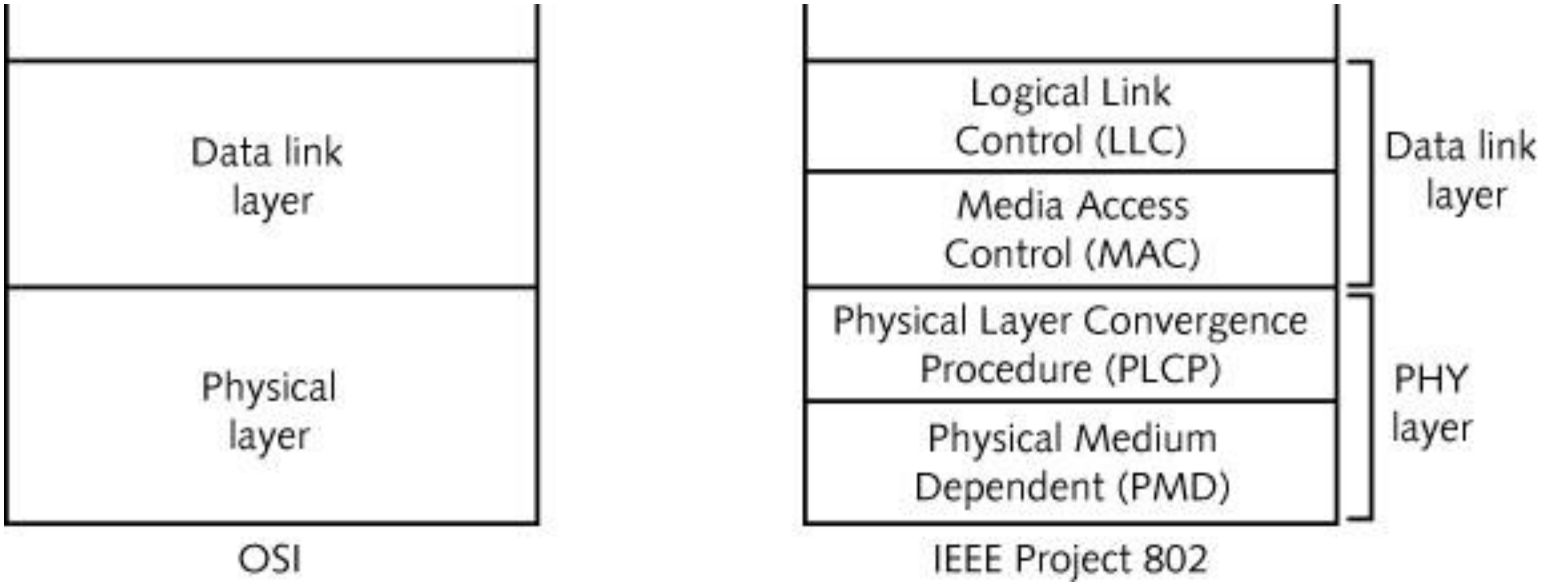
- **Protocol Data Unit (PDU)**: specifies that data will be sent to the peer protocol layer at the receiving device
  - Changing an SDU to a PDU involves an encapsulation process in which the lower layer adds headers and footers

MAC Frame Formats





MAC Frame Formats



MAC Frame Formats

- Process in a 802.11 network using SDUs and PDUs:
  - Layer 3 send data to LLC sublayer of Layer 2. Unit of data is called the MAC Service Data Unit (MSDU)
  - LLC sends data unit to MAC sublayer where MAC header information is added. Data unit is now called MAC Protocol Data Unit (MPDU) – also known as frame
  - MPDU is sent to PLCP sublayer in the Physical Layer and is then called the PLCP Service Data Unit (PSDU)
  - PSDU is passed to the PMD sublayer that creates the PLCP Protocol Data Unit (PPDU) by adding header/footer
  - PPDU is then transmitted as a series of bits

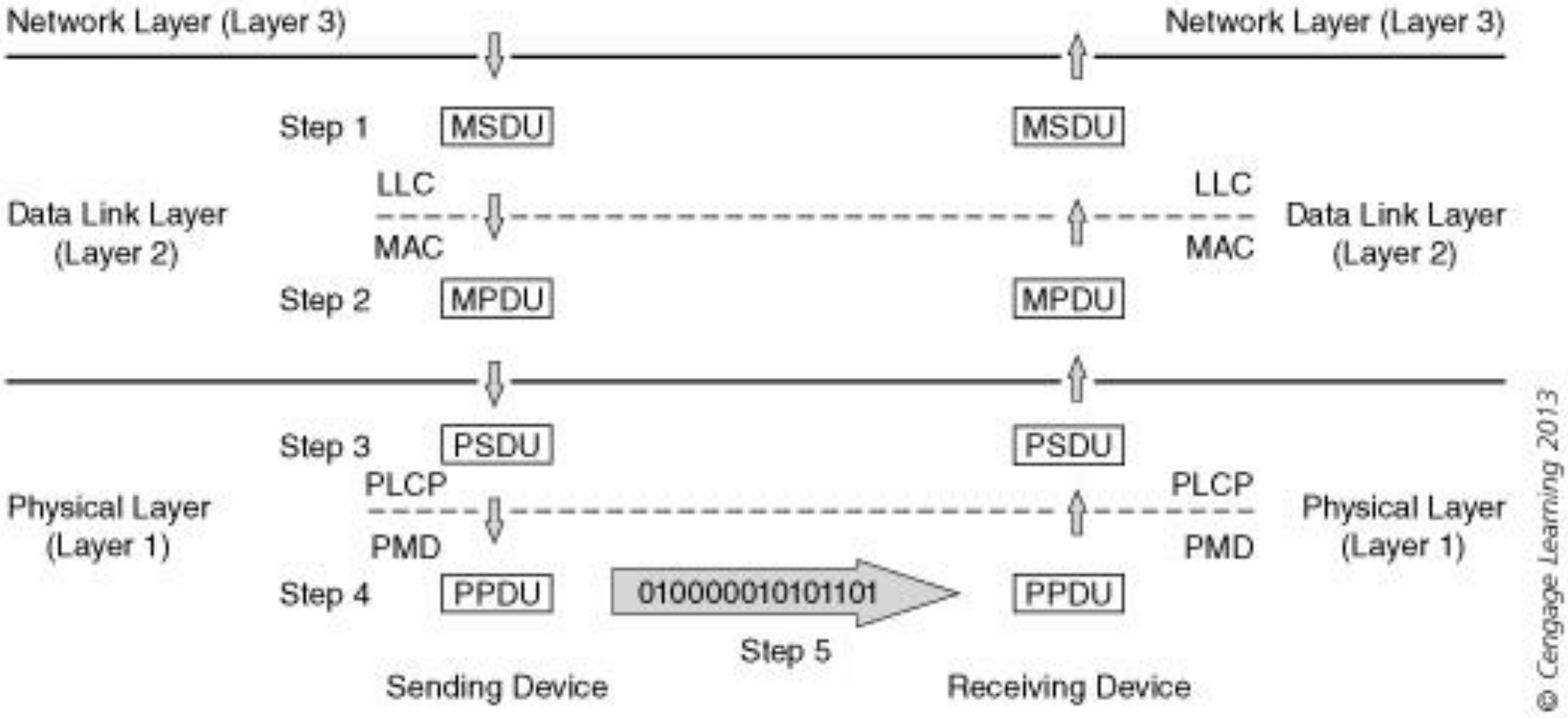
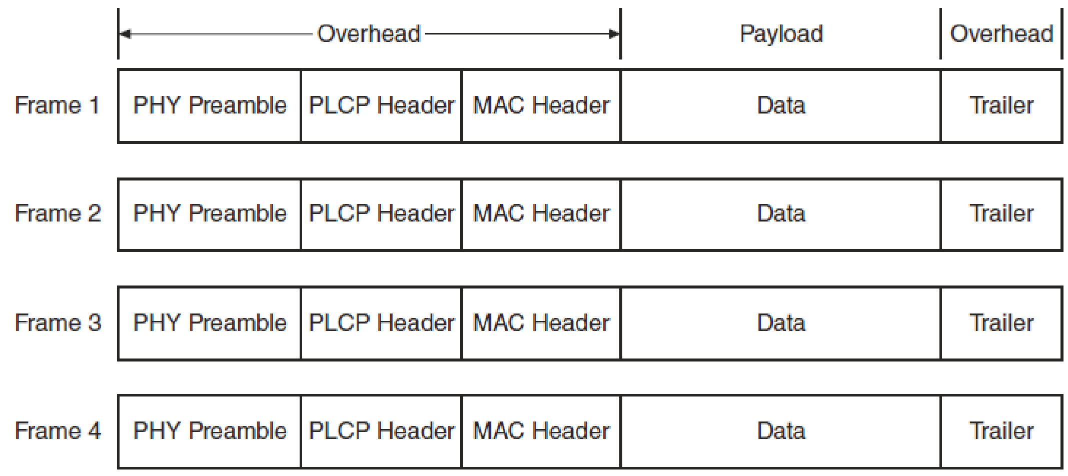


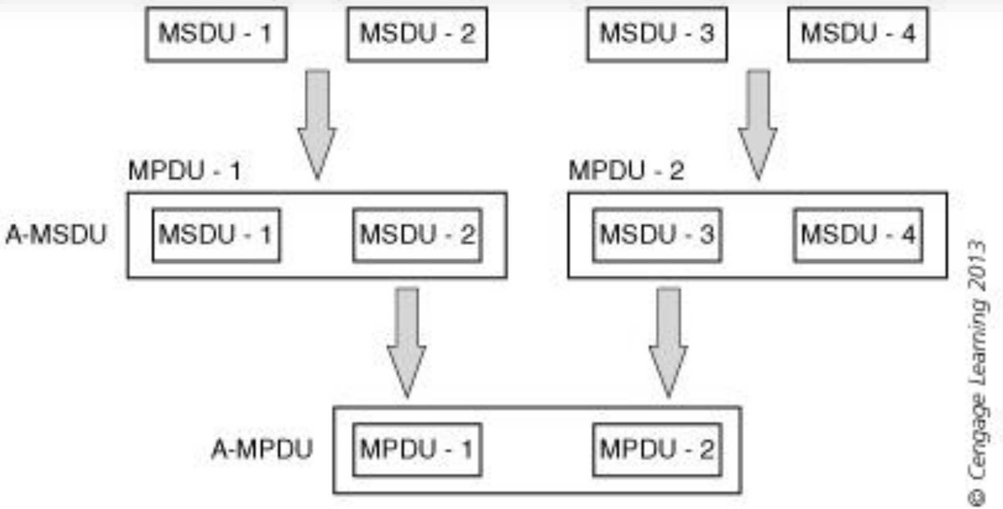
Figure 6-7 SDUs and PDUs

MAC Frame Formats



	Overhead			Payload	Overhead
Frame 1	PHY Preamble	PLCP Header	MAC Header	Data	Trailer
Frame 2	PHY Preamble	PLCP Header	MAC Header	Data	Trailer
Frame 3	PHY Preamble	PLCP Header	MAC Header	Data	Trailer
Frame 4	PHY Preamble	PLCP Header	MAC Header	Data	Trailer

Figure 6-8 802.11 Overhead and payload

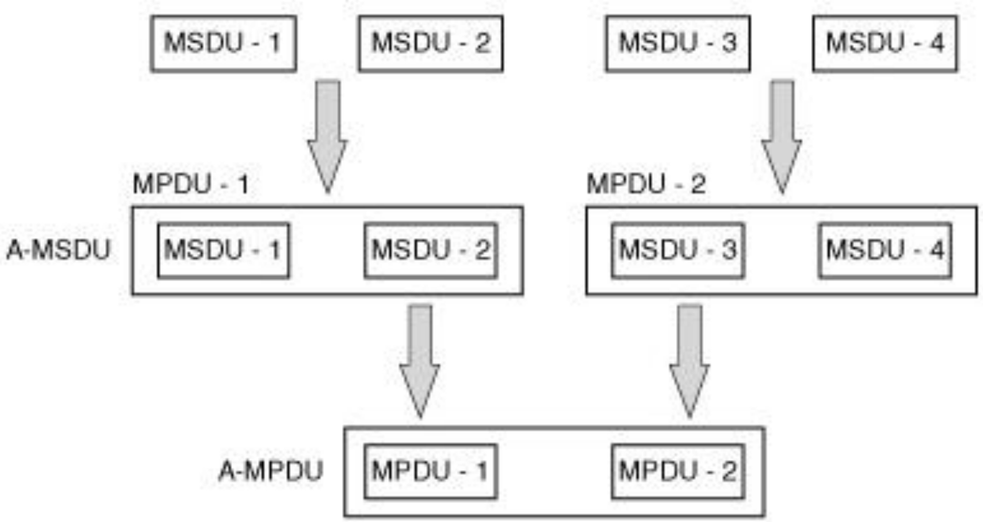


© Cengage Learning 2013

Figure 6-9 A-MSDU and A-MPDU

MAC Frame Formats

- Aggregate MAC Service Data Unit (A-MSDU): allows multiple MSDUs to be combined
- Aggregate MAC Protocol Data Unit (A-MPDU): allows multiple MPDUs to be combined



© Cengage Learning 2013

Figure 6-9 A-MSDU and A-MPDU

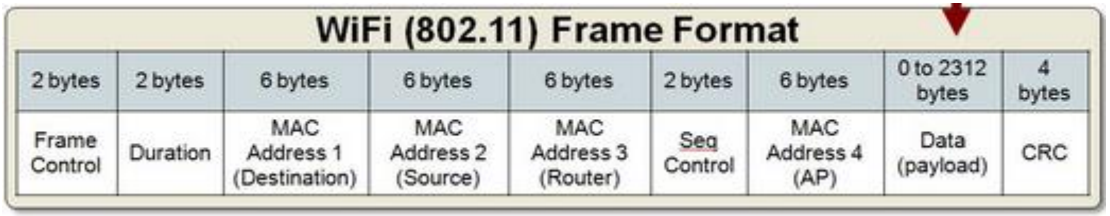
MAC Frame Formats

- Interoperability: different systems able to understand each other
- One area of difference between 802.11 and 802.3 is the frame size, known as maximum transmission unit (MTU)
- Three options to address interoperability:
  - Fragmentation
  - Jumbo frames
  - Lowest common denominator

MAC Frame Formats

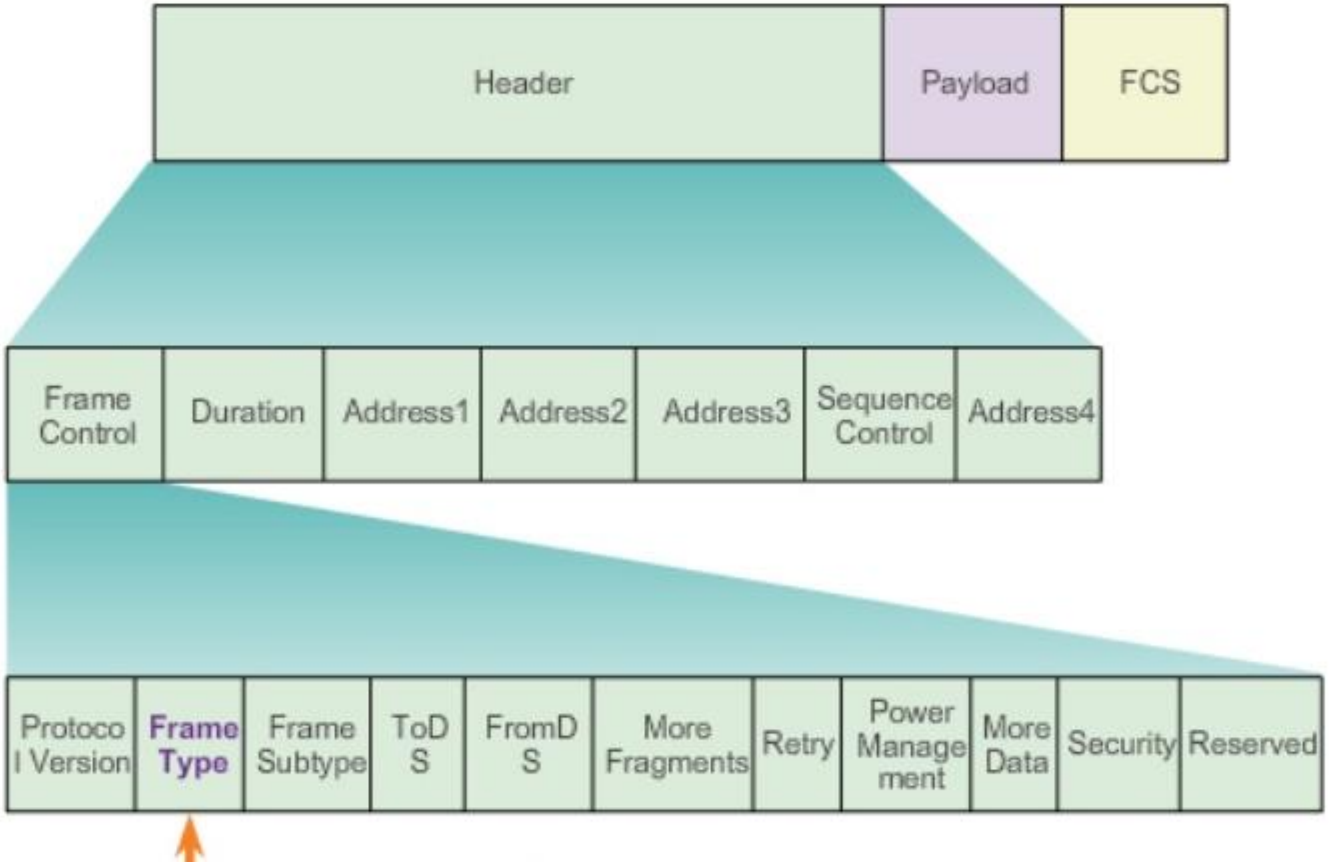
- Due to significant differences between high-throughput (HT) 802.11n and non-HT 802.11a/b/g, an AP can tell 802.11n devices to change to one of four **HT Operation Modes**:
  - *HT Greenfield Mode (Mode 0)*
  - *HT Nonmember Protection Mode (Mode 1)*
  - *HT 20 MHz Protection Mode (Mode 2)*
  - *HT Mixed Mode (Mode 3)*

MAC Frame Types



WiFi (802.11) Frame Format

2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0 to 2312 bytes	4 bytes
Frame Control	Duration	MAC Address 1 (Destination)	MAC Address 2 (Source)	MAC Address 3 (Router)	Seq Control	MAC Address 4 (AP)	Data (payload)	CRC

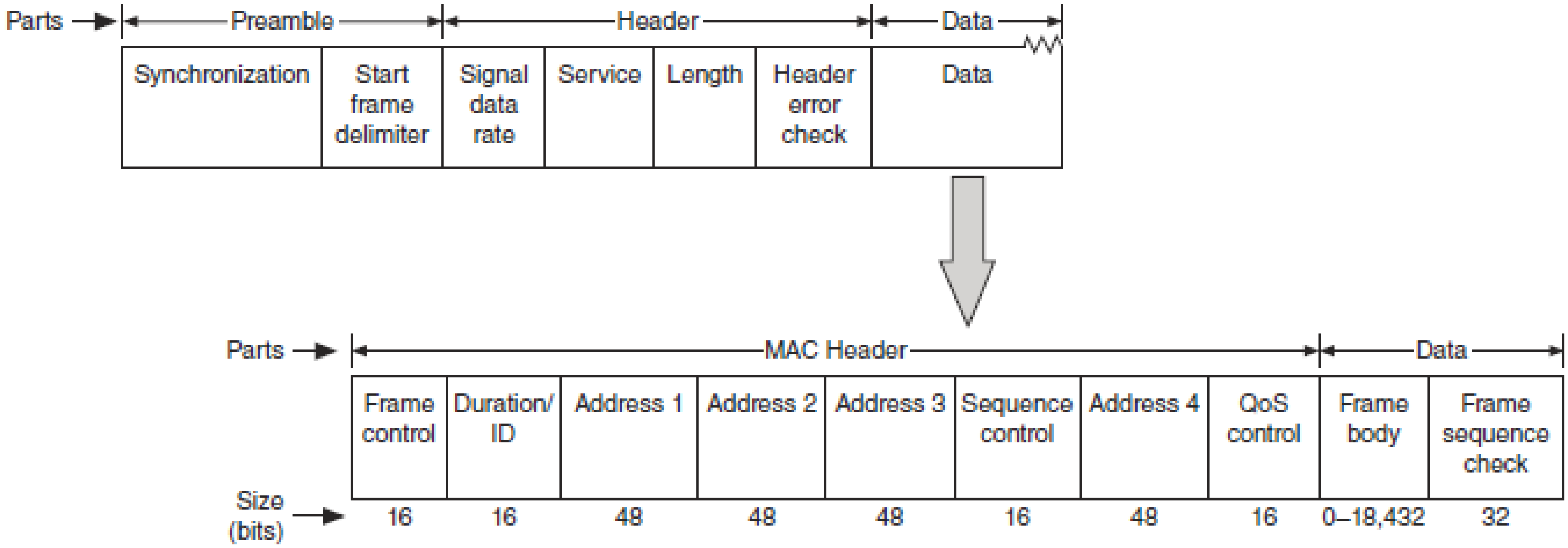


Header	Payload	FCS

Frame Control	Duration	Address1	Address2	Address3	Sequence Control	Address4

Protocol Version	Frame Type	Frame Subtype	ToDS	FromDS	More Fragments	Retry	Power Management	More Data	Security	Reserved

MAC Frame Types



Parts →	Preamble		Header				Data
	Synchronization	Start frame delimiter	Signal data rate	Service	Length	Header error check	Data

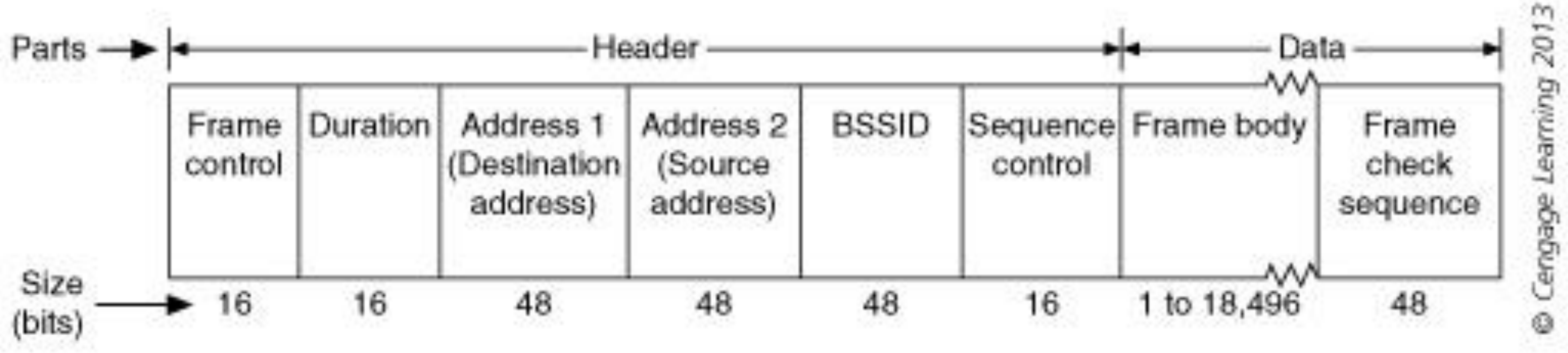
Parts →	MAC Header								Data	
	Frame control	Duration/ ID	Address 1	Address 2	Address 3	Sequence control	Address 4	QoS control	Frame body	Frame sequence check
Size (bits) →	16	16	48	48	48	16	48	16	0–18,432	32

Figure 6-10 MAC frame within PLCP frame

- There are three main types of MAC frames:
  - Management frames
  - Control frames
  - Data frames

Management Frames

- **Management Frames:** Initialize communications between device and AP (infrastructure mode) or between devices (ad hoc mode)
  - Maintain connection



Parts	Header						Data	
	Frame control	Duration	Address 1 (Destination address)	Address 2 (Source address)	BSSID	Sequence control	Frame body	Frame check sequence
Size (bits)	16	16	48	48	48	16	1 to 18,496	48

© Cengage Learning 2013

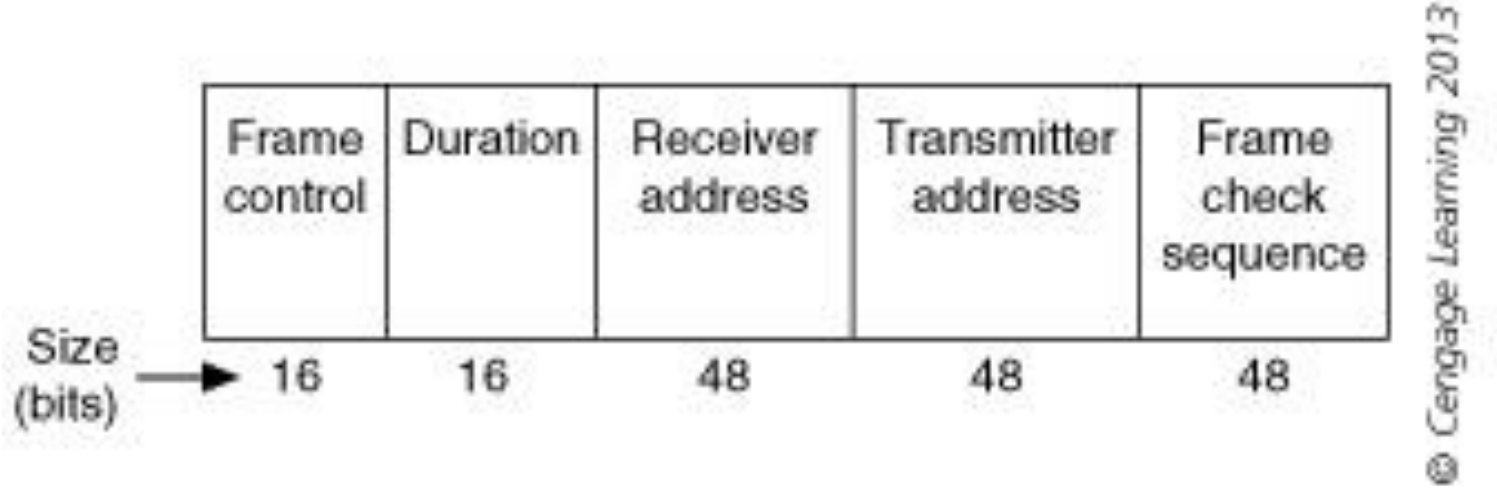
Figure 6-11 Management frame

Management Frames

- Types of management frames:
  - Authentication frame
  - Association request frame
  - Association response frame
  - Beacon frame
  - Deauthentication frame
  - Disassociation frame
  - Probe request frame
  - Probe response frame
  - Reassociation request frame
  - Reassociation response frame

Control Frames

- **Control frames:** Provide assistance in delivering frames that contain data



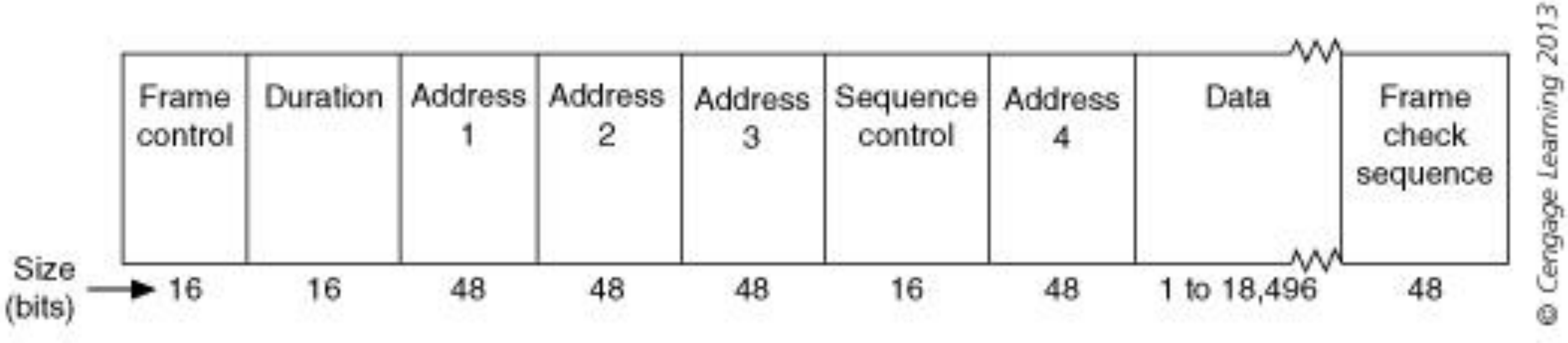
Size (bits)	Frame control	Duration	Receiver address	Transmitter address	Frame check sequence
→	16	16	48	48	48

© Cengage Learning 2013

Figure 6-12 Control frame

Data Frames

- **Data frame:** Carries information to be transmitted to destination device



	Frame control	Duration	Address 1	Address 2	Address 3	Sequence control	Address 4	Data	Frame check sequence
Size (bits) →	16	16	48	48	48	16	48	1 to 18,496	48

© Cengage Learning 2013

Figure 6-13 Data frame

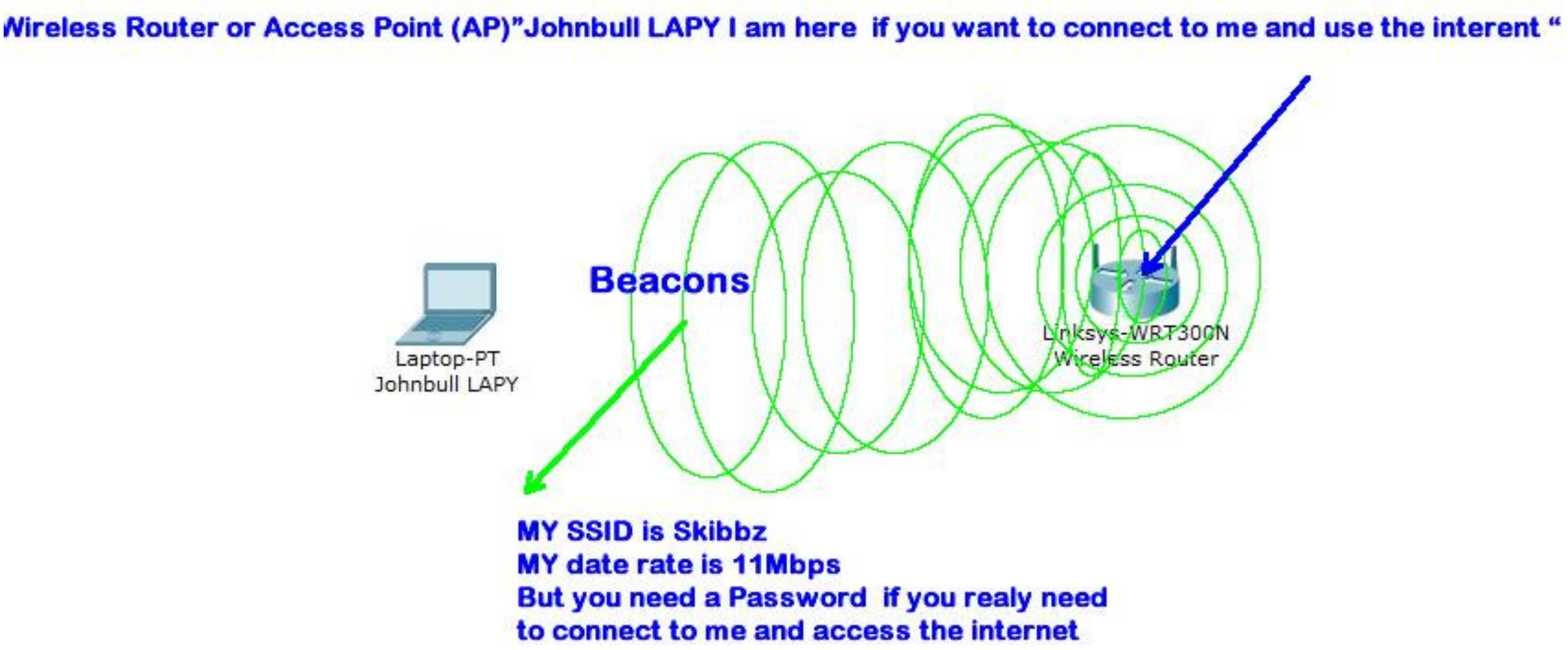
MAC Operations

- MAC layer WLAN functions:
  - Discovering a WLAN
  - Joining the WLAN
  - Transmitting on a WLAN

Discovering the WLAN (Passive Scanning)

- At regular intervals, AP (infrastructure network) or wireless device (ad hoc network) sends a beacon frame
  - Announce presence
  - Provide info for other devices to join network
  - Process is known as **beaconing**
- Beacon frame format follows standard structure of a management frame
  - Destination address always set to all ones
  - 255.255.255.255

Discovering the WLAN (Passive Scanning)



Wireless Router or Access Point (AP)"Johnbull LAPY I am here if you want to connect to me and use the interent "

MY SSID is Skibbz
MY date rate is 11Mbps
But you need a Password if you realy need
to connect to me and access the internet

Discovering the WLAN

- Beacon frame body contains following fields:
  - Beacon interval
  - Timestamp
  - Service Set Identifier (SSID)
  - Supported rates
  - Parameter sets
  - Capability information

- In ad hoc networks, each wireless device assumes responsibility for beaconing

- In infrastructure networks beacon interval normally 100 ms, but can be modified

Discovering the WLAN

- Receiving wireless device must be looking for beacon frames

- **Passive scanning**: Wireless device simply listens for beacon frame
  - Typically, on each available channel for set period

- **Active scanning**: Wireless device first sends out a management probe request frame on each available channel
  - Then waits for probe response frame from all available APs

Discovering the WLAN (Active Scanning)

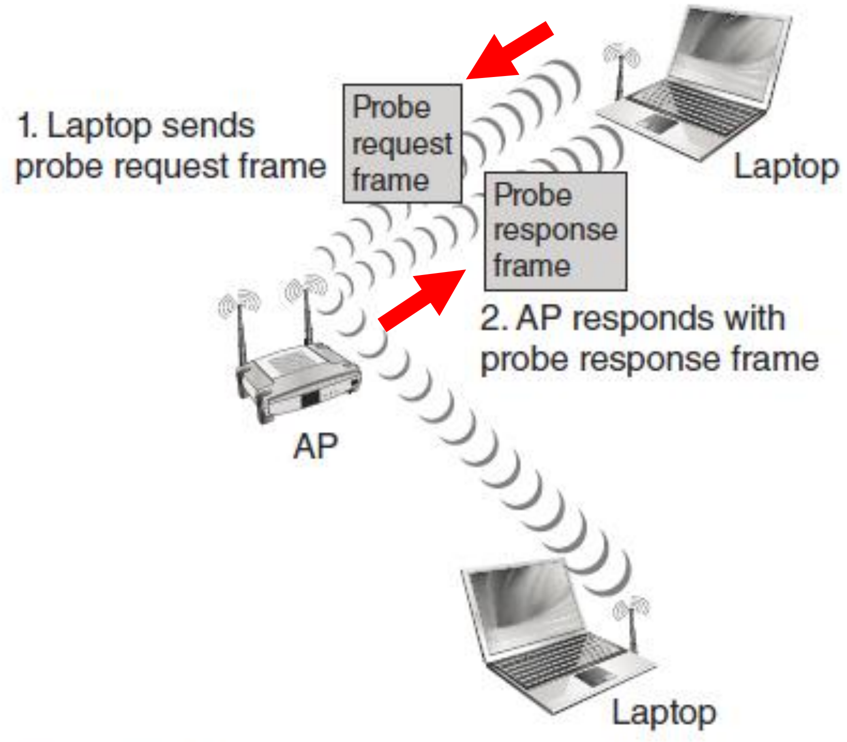

1. Laptop sends probe request frame
Probe request frame
Laptop
Probe response frame
2. AP responds with probe response frame
AP
Laptop

Figure 6-14 Active scanning

Joining the WLAN

- Unlike standard wired LANS, **authentication** performed *before* user connected to network
  - Authentication of the *wireless device*, not the user

- **IEEE 802.11 authentication:** Process in which AP accepts a wireless device

- **Open system authentication:** device sends an association request frame to an AP
  - AP responds with an association response frame
  - Virtually a "handshake" between the AP and device

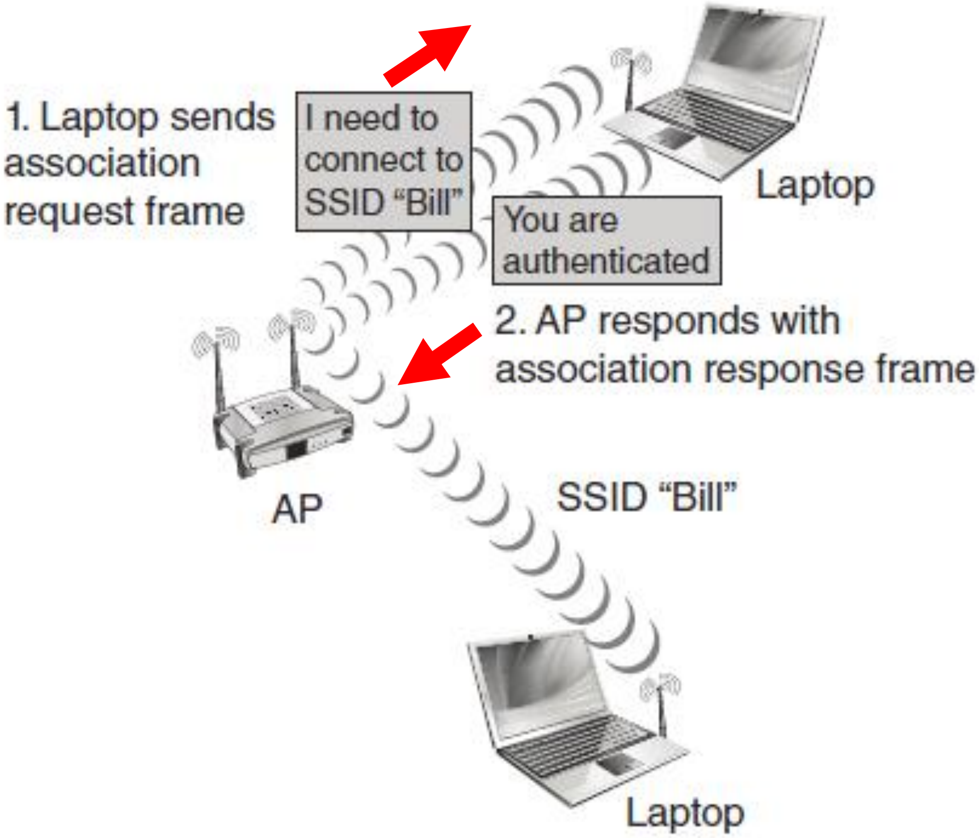

1. Laptop sends association request frame
I need to connect to SSID "Bill"
Laptop
You are authenticated
2. AP responds with association response frame
AP
SSID "Bill"
Laptop

Figure 6-15 Open system authentication

Joining the WLAN

- **Shared key authentication:** process of a station encrypting text in order to be accepted into the WLAN
  - Utilizes **challenge text**
    - Station encrypts text with a shared key value and send to AP
    - AP decrypts text and compares with its own key value to see if it matches

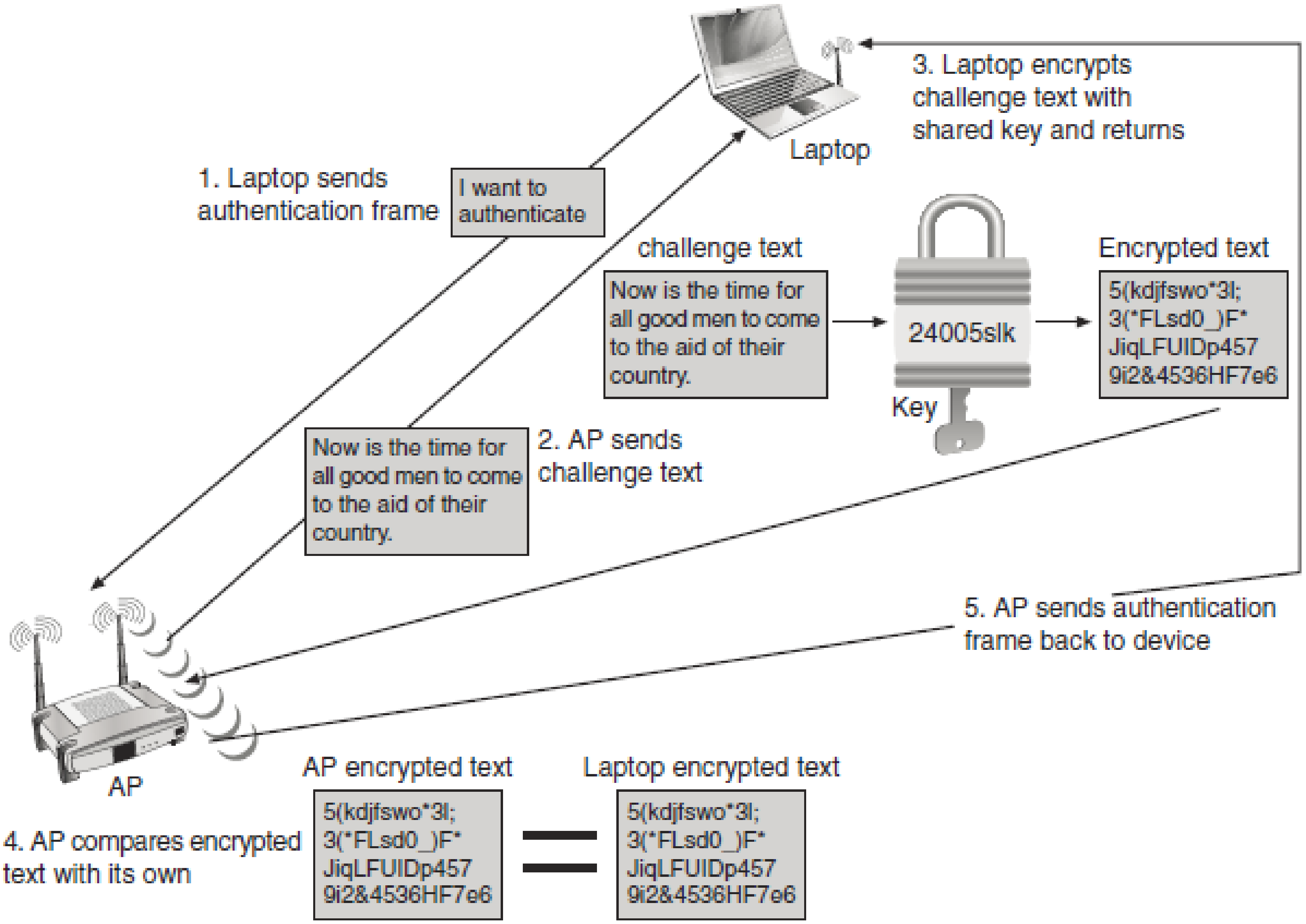
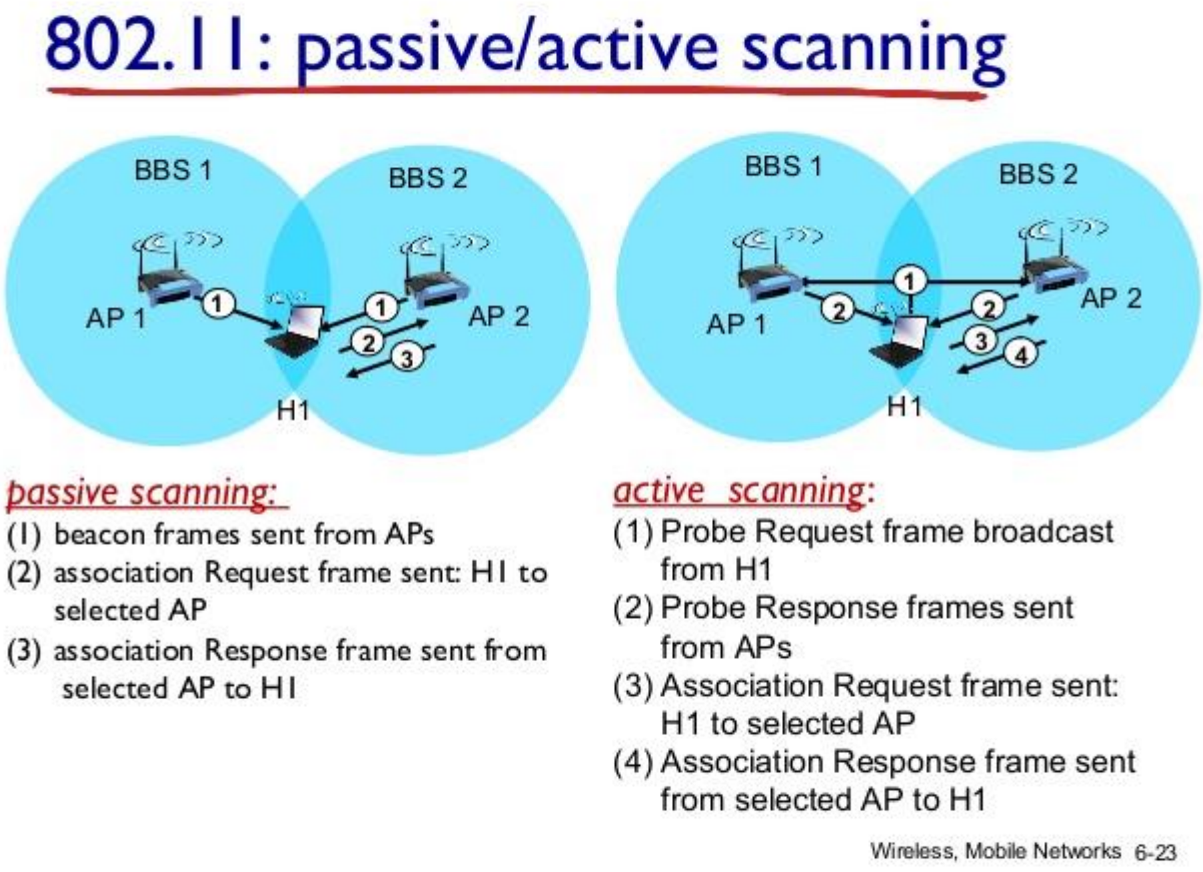

Laptop
3. Laptop encrypts challenge text with shared key and returns
1. Laptop sends authentication frame
I want to authenticate
challenge text
Now is the time for all good men to come to the aid of their country.
24005slk
Key
Encrypted text
5(kdjfswo*3l; 3(*FLsd0_)F* JiqLFUIDp457 9i2&4536HF7e6
Now is the time for all good men to come to the aid of their country.
2. AP sends challenge text
5. AP sends authentication frame back to device
AP
AP encrypted text
Laptop encrypted text
4. AP compares encrypted text with its own
5(kdjfswo*3l; 3(*FLsd0_)F* JiqLFUIDp457 9i2&4536HF7e6
=
5(kdjfswo*3l; 3(*FLsd0_)F* JiqLFUIDp457 9i2&4536HF7e6

Figure 6-16 Shared key authentication

Joining the WLAN

- **Association:** Accepting a wireless device into a wireless network
  - Final step to join WLAN
- After authentication, AP responds with association response frame
  - Contains acceptance or rejection notice
- If AP accepts wireless device, reserves memory space in AP and establishes association ID
- Association response frame includes association ID and supported data rates

Active/Passive Scanning



802.11: passive/active scanning

passive scanning:

(1) beacon frames sent from APs

(2) association Request frame sent: H1 to selected AP

(3) association Response frame sent from selected AP to H1

active scanning:

(1) Probe Request frame broadcast from H1

(2) Probe Response frames sent from APs

(3) Association Request frame sent: H1 to selected AP

(4) Association Response frame sent from selected AP to H1

Wireless, Mobile Networks 6-23

Transmitting on the WLAN

- IEEE 802.11 specifies three procedures for transmitting on the WLAN:
  - Distributed coordination function (DCF)
  - Point coordination function
  - Hybrid coordination function

Distributed Coordination Function (DCF)

- Distributed coordination function (DCF) defines two procedures:
- Carrier Sense Multiple Access with Collision Detection (CSMA/CD) and
- Request to Send/Clear to Send
- **Channel access methods:** Rules for cooperation among wireless devices
  - **Contention**: Computers compete to use medium
    - If two devices send frames simultaneously, collision results and frames become unintelligible
    - Must take steps to avoid collisions

Distributed Coordination Function (DCF)

- **Carrier Sense Multiple Access with Collision Detection (CSMA/CD):** Before networked device sends a frame, listens to see if another device currently transmitting
  - If traffic exists, wait; otherwise send
  - Devices continue listening while sending frame
    - If collision occurs, stops and broadcasts a "jam" signal
- CSMA/CD cannot be used on wireless networks:
  - Difficult to detect collisions
  - Hidden node problem (when stations are out of range of each other)

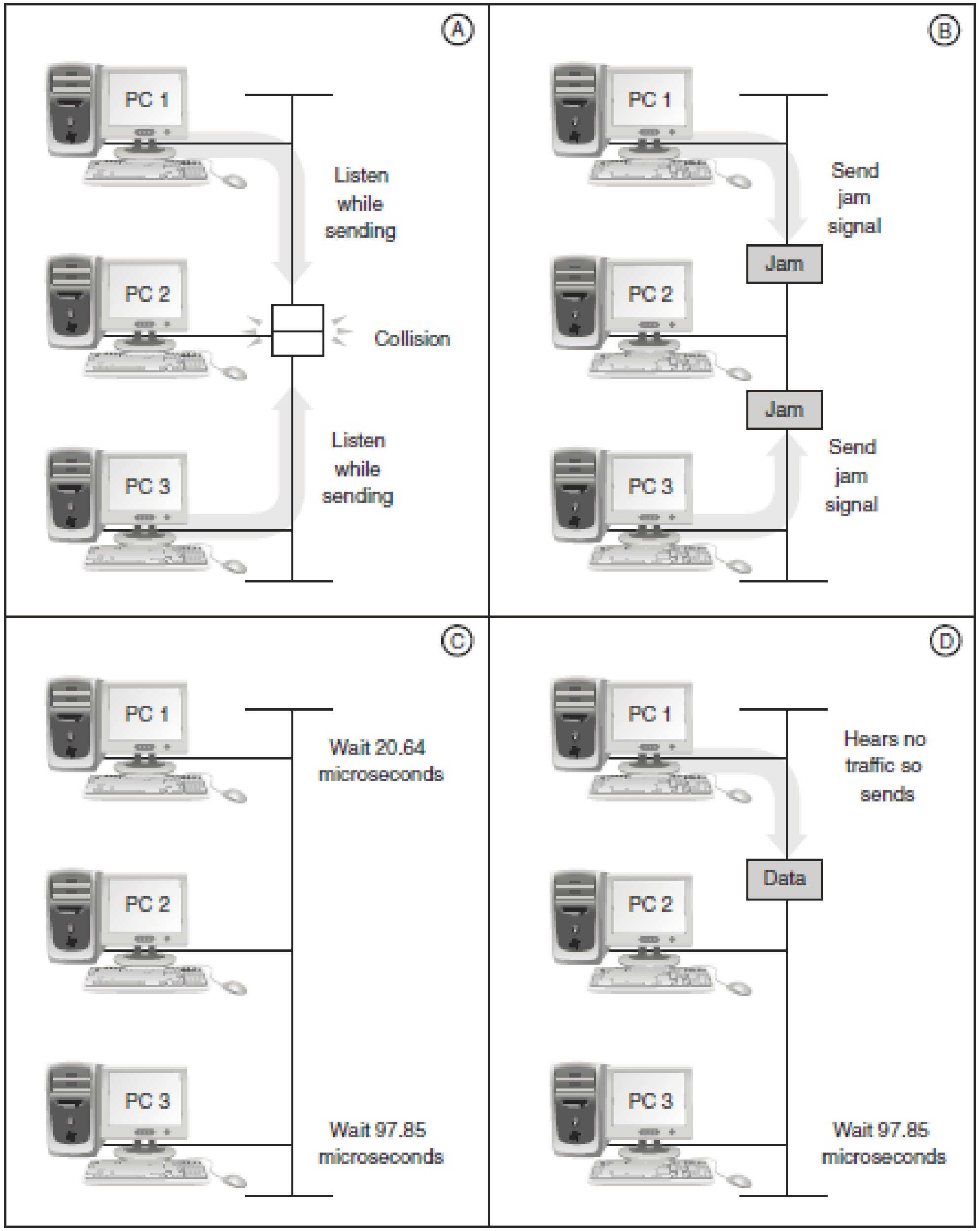


Figure 6-17 CSMA/CD

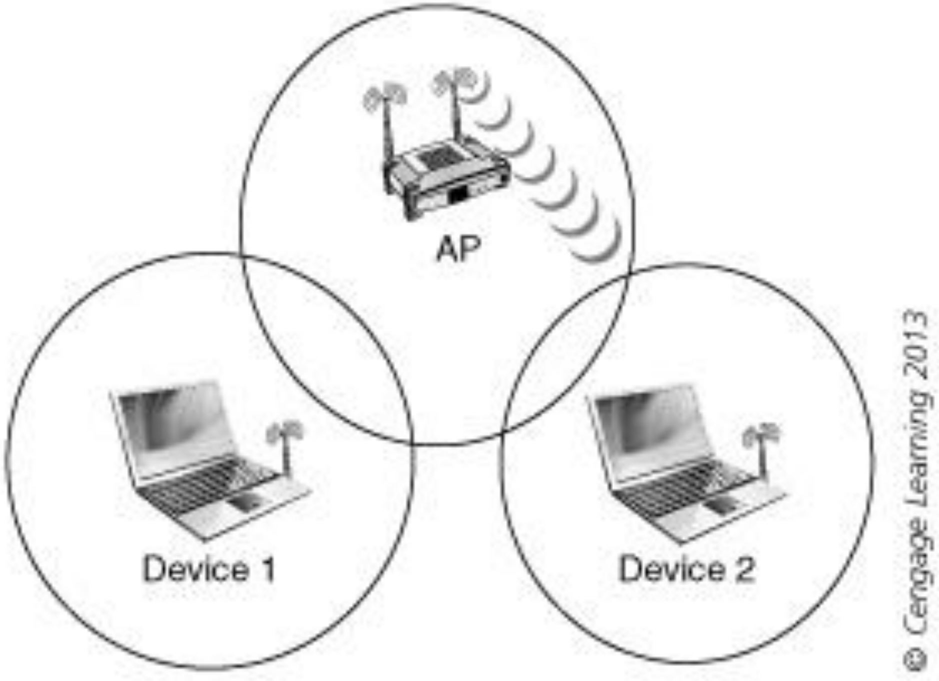


Figure 6-18 Hidden node problem

Distributed Coordination Function (DCF)

- **Distributed Coordination Function (DCF):** Specifies modified version of CSMA/CD
  - **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)**
  - Attempts to avoid collisions altogether
  - Time when most collisions occur is immediately after a station completes transmission
  - *All* stations must wait random amount of time after medium clear
    - **Slot time**

Distributed Coordination Function (DCF)

CSMA/CA

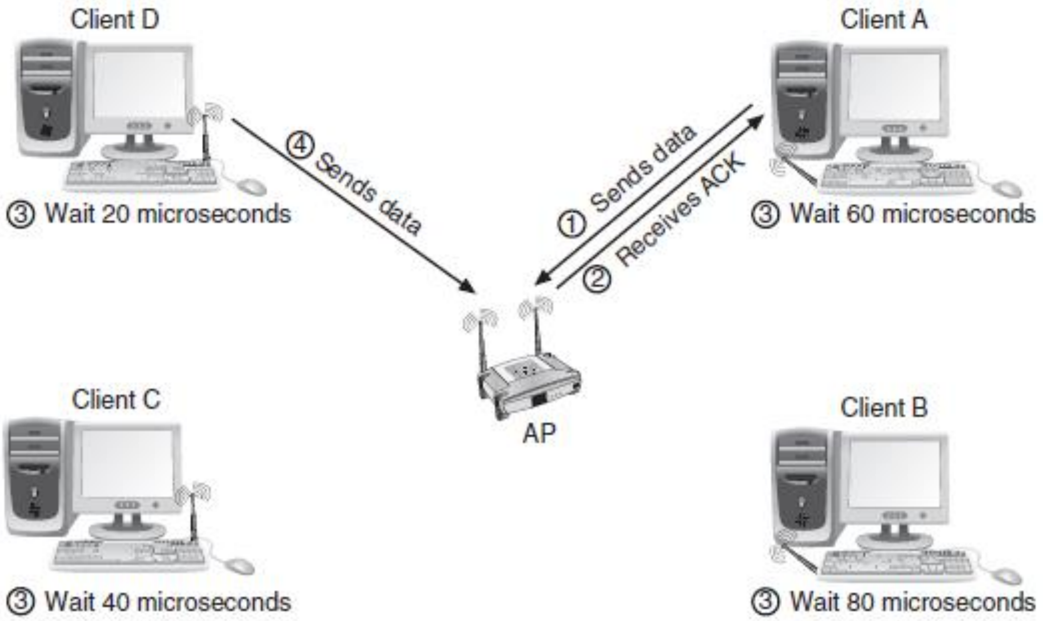


Figure 6-19 CSMA/CA and ACK

Distributed Coordination Function (DCF)

- CSMA/CA also reduces collisions via explicit **frame acknowledgment**
  - **Acknowledgment frame (ACK):** Sent by receiving device to sending device to confirm data frame arrived intact
  - If ACK not returned, transmission error assumed
- IEEE 802.11n adds a feature known as **block acknowledgment**
  - Supports multiple MPDUs in an A-MPDU
- CSMA/CA does not eliminate collisions
  - Does not solve hidden node problem

Distributed Coordination Function (DCF)

- **Request to Send/Clear to Send (RTS/CTS) protocol:** Option used to solve hidden node problem
  - Also known as virtual carrier sensing
  - Significant overhead upon the WLAN with transmission of RTS and CTS frames
    - Especially with short data packets
  - **RTS threshold:** Only packets that are longer than RTS threshold are transmitted using RTS/CTS

Distributed Coordination Function (DCF)

- **Fragmentation:** Divide data to be transmitted from one large frame into several smaller ones
  - Reduces probability of collisions
  - Reduces amount of time medium is in use
- If data frame length exceeds specific value, MAC layer fragments it
  - Receiving station reassembles fragments
- Alternative to RTS/CTS
  - High overhead
    - ACKs and additional SIFS (Short Interframe Spaces) time gaps

Distributed Coordination Function (DCF)

- Variations of RTS/CTS are used as protection mechanisms:
  - **CTS-to-self**: process used when 802.11g devices are mixed with 802.11b devices
  - **HT Dual-CTS Protection**: used with 802.11n devices in a mixed environment with 802.11a/b/g devices
    - 802.11n devices sends a RTS to the AP, which responds with two CTS frames: one in 802.11n format and one in non-802.11n format
  - **HT L-SIG Protection**: used with 802.11n devices in a mixed environment

Distributed Coordination Function (DCF)

- **Interframe spaces (IFS):** Intervals between transmissions of data frames
  - **Short IFS (SIFS):** For immediate response actions such as ACK
  - **Point Coordination Function IFS (PIFS):** Time used by a device to access medium after it has been asked and then given approval to transmit
  - **Distributed Coordination Function IFS (DIFS):** Standard interval between transmission of data frames

Distributed Coordination Function (DCF)

- Interframe spaces (IFS) continued:
  - **Extended IFS**: used when frames must be retransmitted
  - **Arbitration IFS**: used when setting priorities to different types of transmissions
  - **Reduced IFS**: reduces amount of “dead space” required between OFDM transmissions

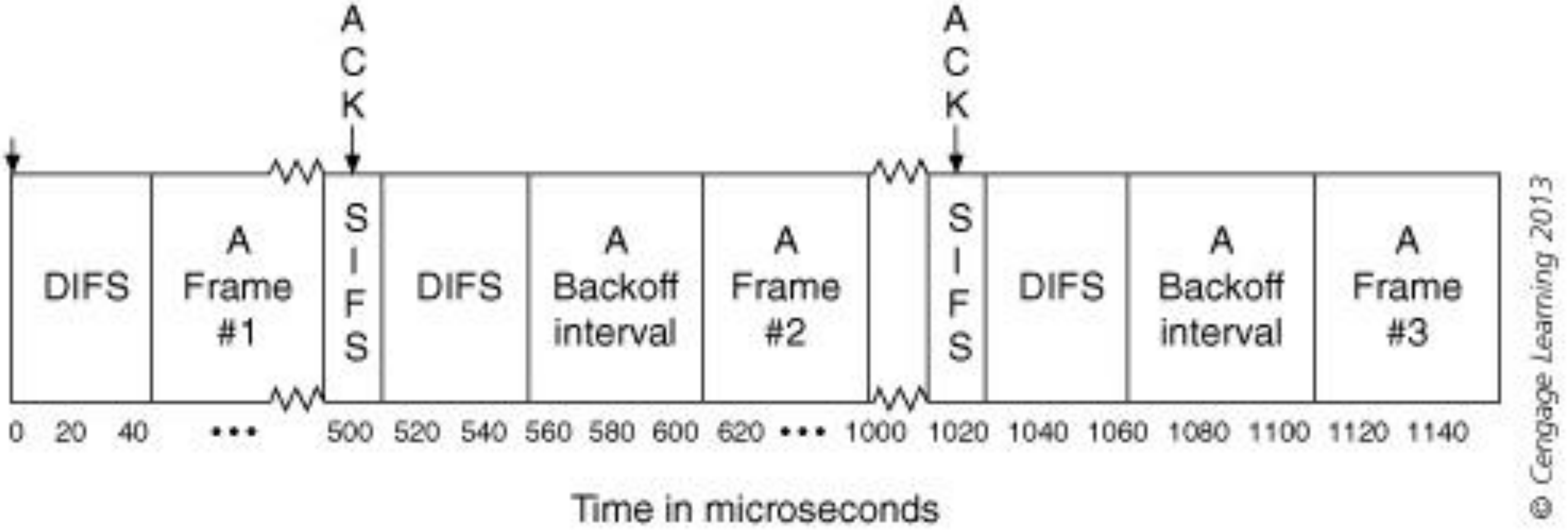


Figure 6-20 CSMA/CA with one station transmitting

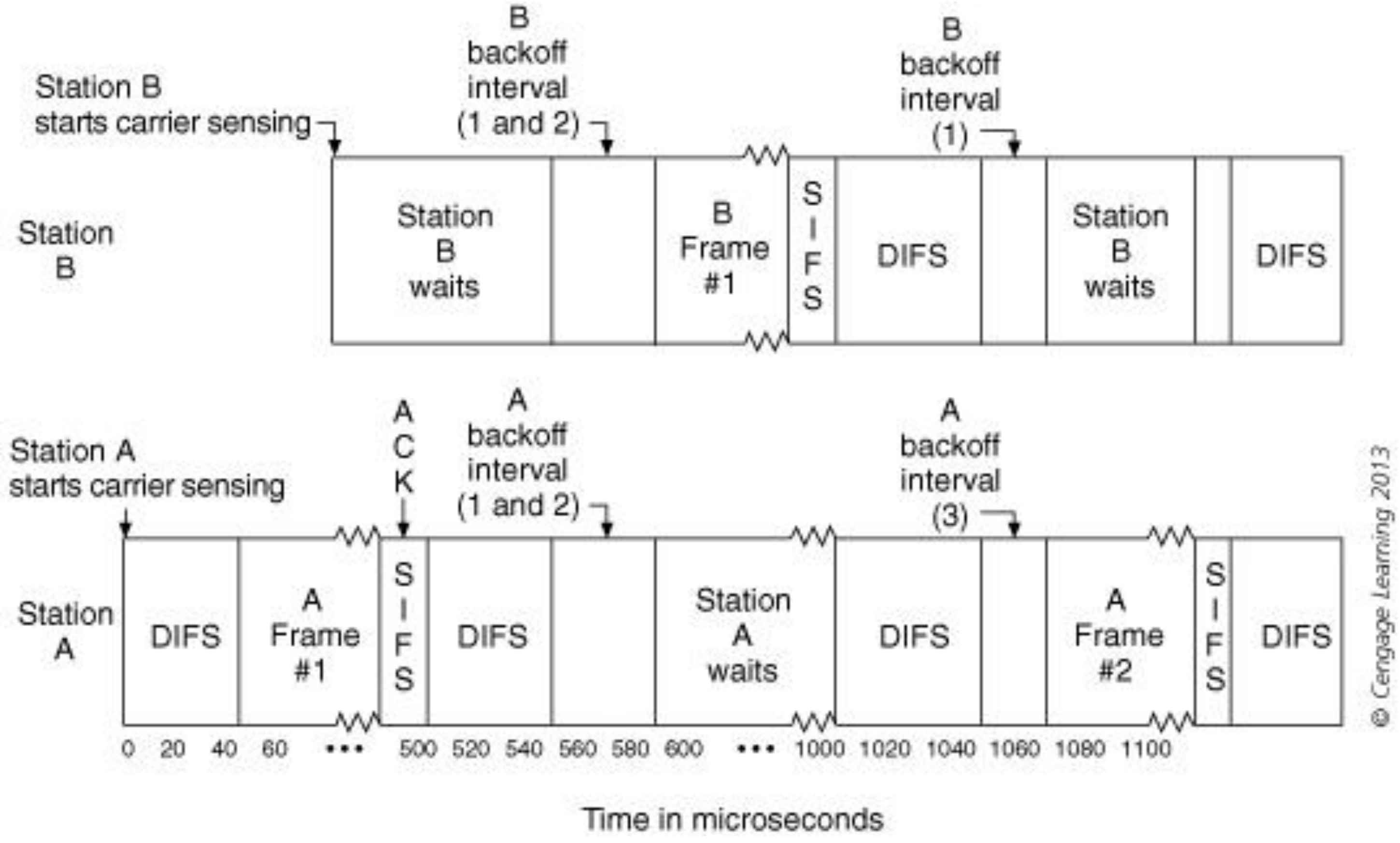


Figure 6-21 CSMA/CA with two stations transmitting

Point Coordination Function (PCF)

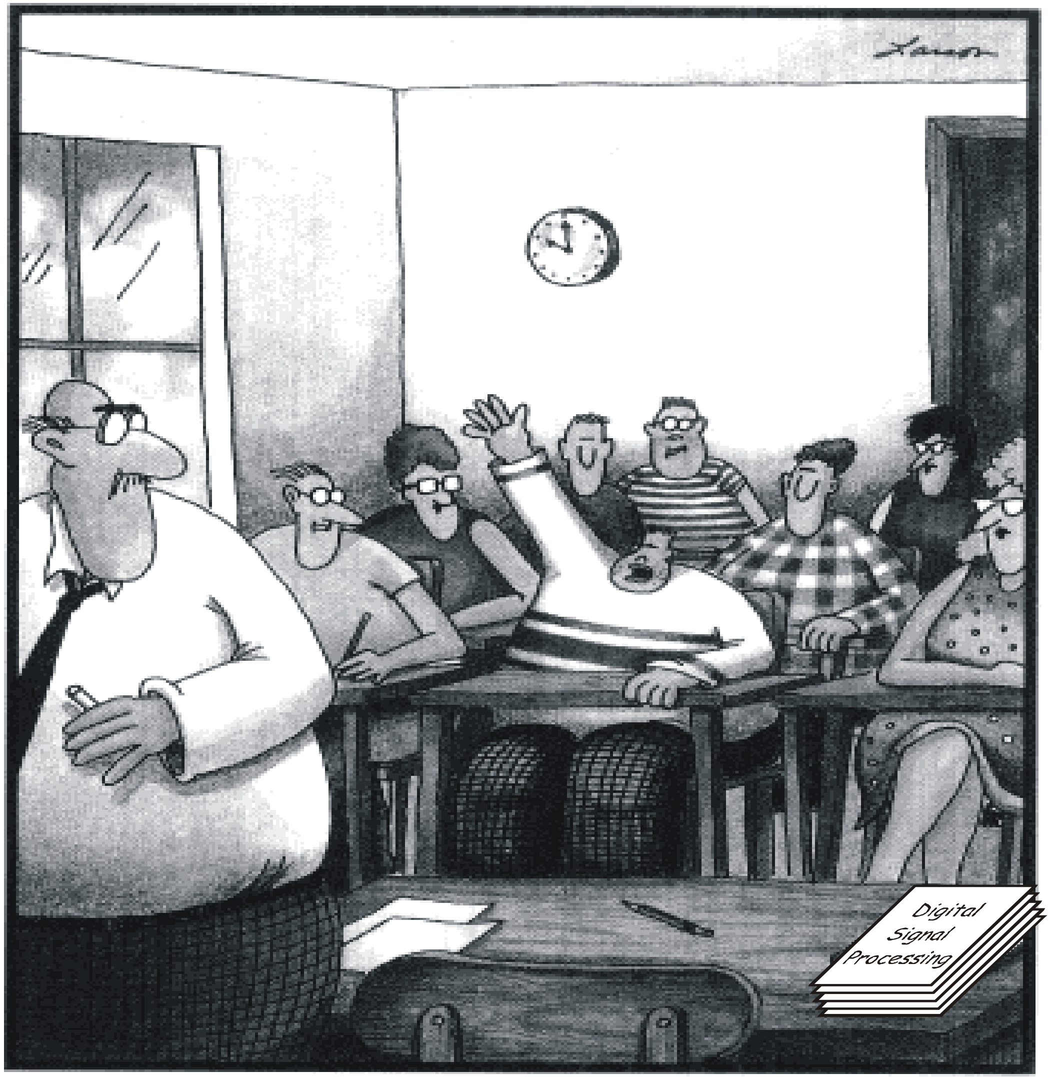
- **Polling:** Channel access method in which each device asked in sequence if it wants to transmit
  - Effectively prevents collisions
- **Point Coordination Function (PCF):** AP serves as polling device or "point coordinator"
- Point coordinator has to wait only through point **coordination function IFS (PIFS)** time gap
  - Shorter than DFIS time gap

Point Coordination Function (PCF)

- If point coordinator hears no traffic after PIFS time gap, sends out beacon frame
  - Field to indicate length of time that PCF (polling) will be used instead of DCF (contention)
    - Receiving stations must stop transmission for that amount of time
  - Point coordinator then sends frame to specific station, granting permission to transmit one frame
- 802.11 standard allows WLAN to alternate between PCF (polling) and DCF (contention)

Hybrid Coordination Function (HCF)

- **Hybrid Coordination Function (HCF)**: allows for different types of wireless traffic to be given different levels of priority
  - **Enhanced Distributed Channel Access (EDCA):** Contention-based but supports different types of traffic
    - Four **access categories (AC)**
    - Provides “relative” QoS but cannot guarantee service
  - **Hybrid Coordination Function Controlled Channel Access (HCCA):** based upon polling
    - Serves as a centralized scheduling mechanism



Professor harris, may I be excused?
My brain is full.

Summary

- A Basic Service Set (BSS) is defined as a group of wireless devices that is served by a single access point (AP)
- An Extended Service Set (ESS) is comprised of two or more BSS networks that are connected through a common distribution system
- An Independent Basic Service Set (IBSS) is a wireless network that does not use an access point
- A Service Data Unit (SDU) is a specific unit of data passed down from a higher OSI layer
- A Protocol Data Unit (PDU) specifies data that will be sent to the peer layer at the receiving device

Summary

- Because of the differences between 802.11n HT and non-HT 802.11a/b/g devices an AP can tell 802.11n devices to change to one of four HT Operation Modes in order to interoperate
- Three main types of MAC frames: management frames, control frames, and data frames
- WLAN discovery can be done by passive scanning or active scanning
- Passive scanning depends on the AP "advertising" itself
- Active scanning station send out a management probe request on an available channel

Summary

- Once a wireless device has discovered the WLAN, it requests to join the network; This is a twofold process known as authentication and association
- The IEEE 802.11 standard specifies three procedures for transmitting on the WLAN, distributed coordination function (DCF), point coordination function (PCF), and hybrid coordination function (HCF)