Data and Computer Communications

Tenth Edition

by William Stallings

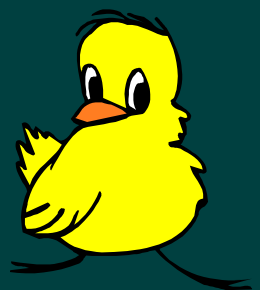
CHAPTER 13

Wireless LANs

Investigators have published numerous reports of birds taking turns vocalizing; the bird spoken to gave its full attention to the speaker and never vocalized at the same time, as if the two were holding a conversation.

Researchers and scholars who have studied the data on avian communication carefully write the (a) the communication code of birds such has crows has not been broken by any means; (b) probably all birds have wider vocabularies than anyone realizes; and (c) greater complexity and depth are recognized in avian communication as research progresses.

—The Human Nature of Birds,
Theodore Barber



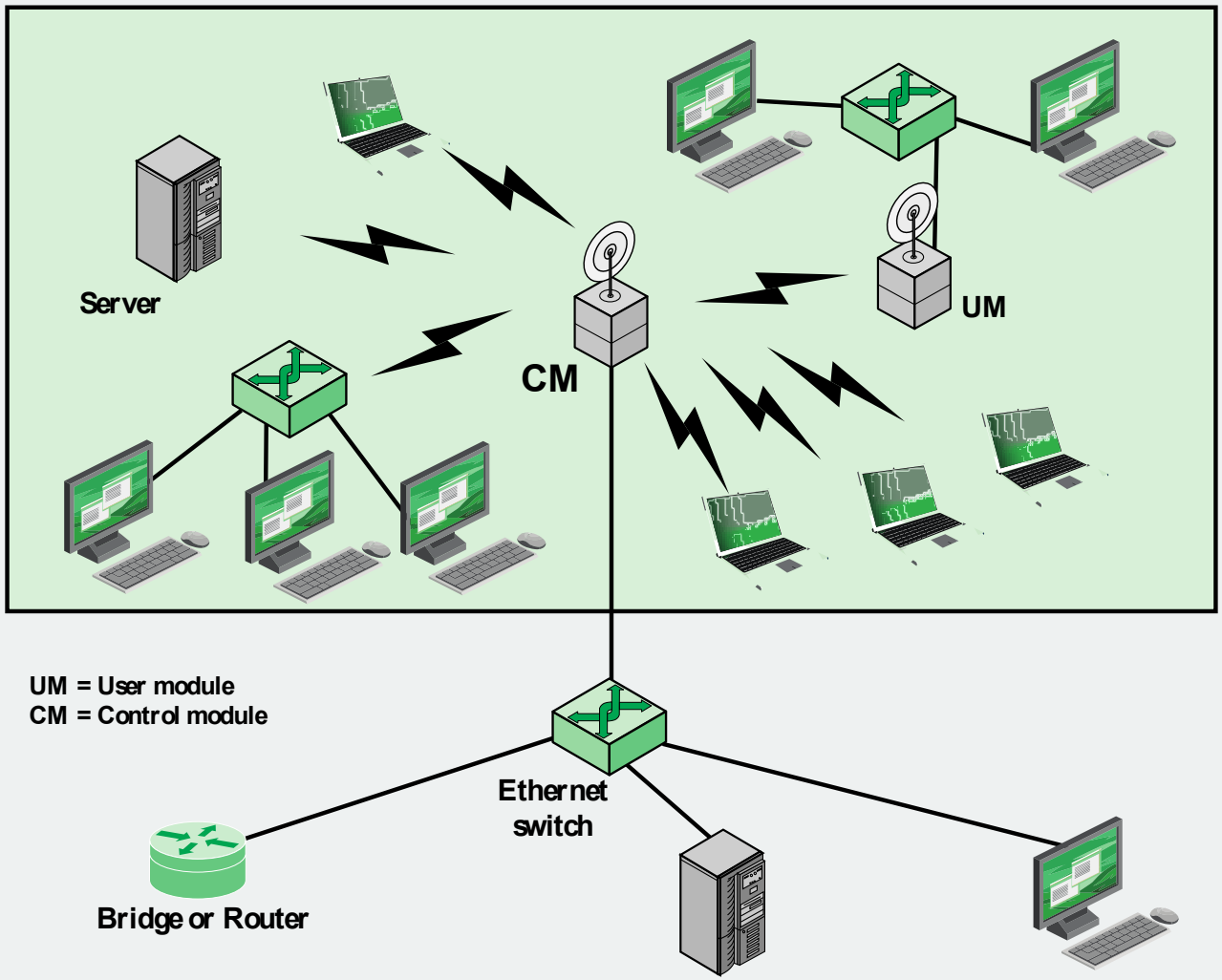


Figure 13.1 Example Single-Cell Wireless LAN Configuration

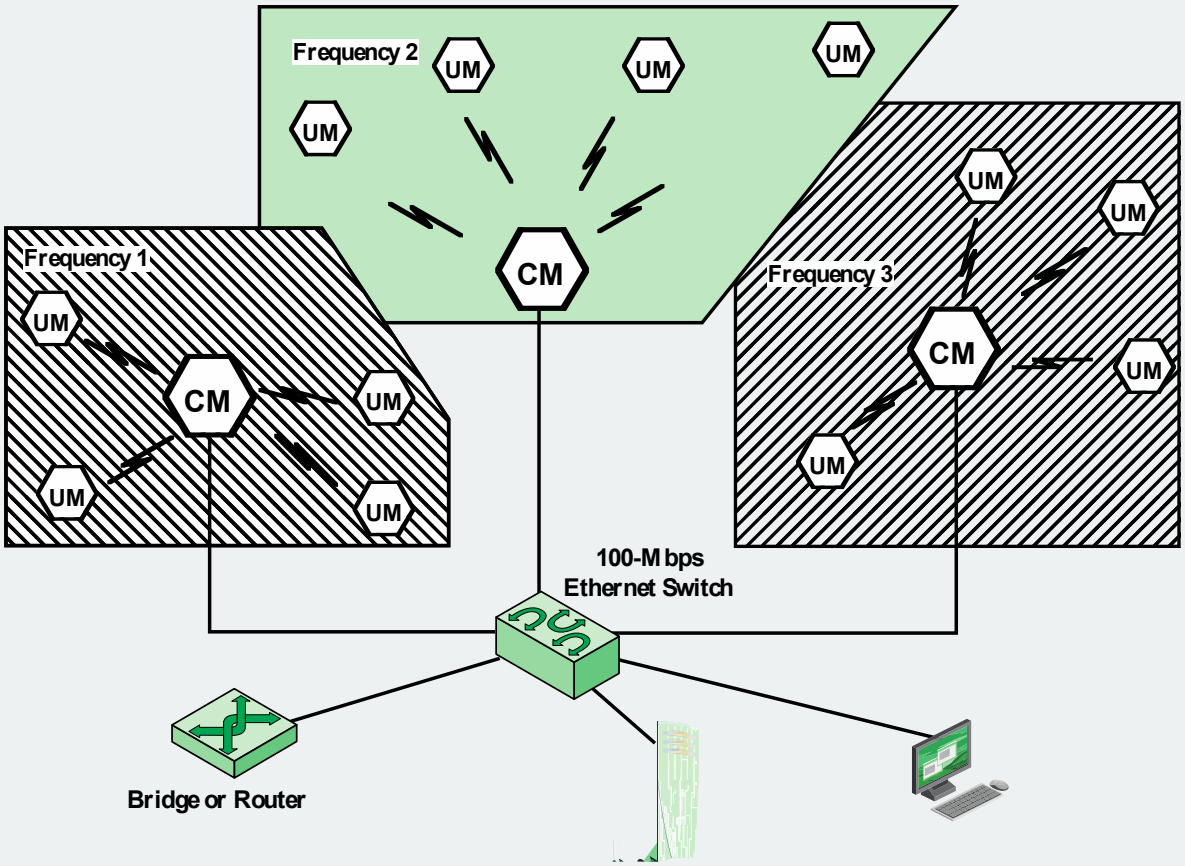


Figure 13.2 Example Multiple-Cell Wireless LAN Configuration

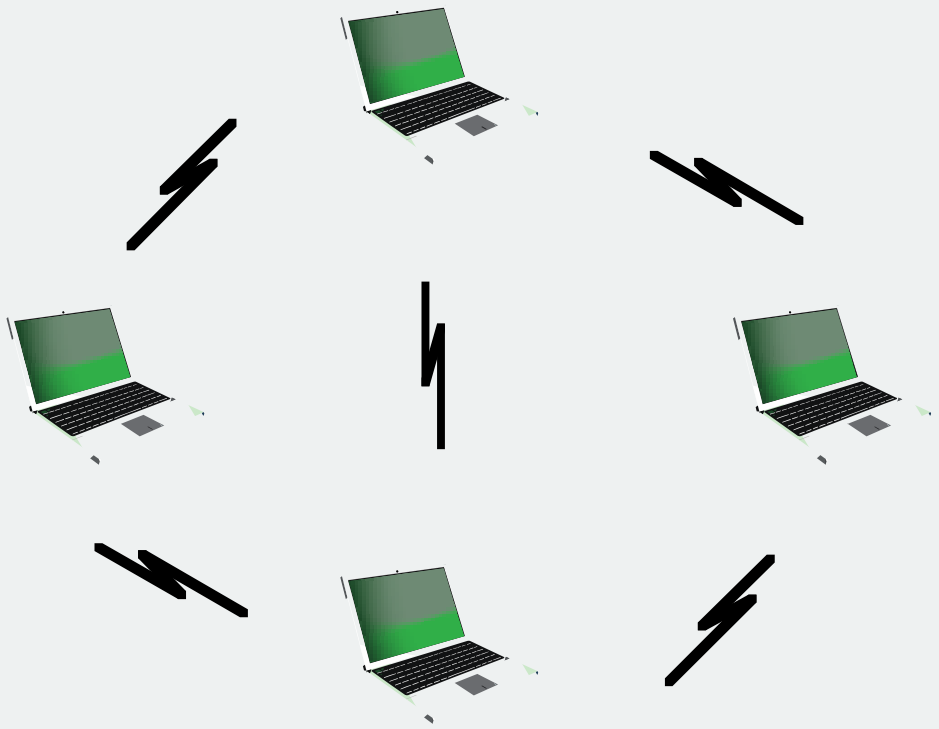


Figure 13.3 Ad Hoc Wireless LAN Configuration

Wireless LAN Requirements

- Throughput
- Number of nodes
- Connection to backbone LAN
- Service area
- Battery power consumption
- Transmission robustness and security
- Collocated network operation
- License-free operation
- Handoff/roaming
- Dynamic configuration

Table 13.1
Key IEEE 802.11 Standards

Standard	Scope
IEEE 802.11a	Physical layer: 5-GHz OFDM at rates from 6 to 54 Mbps
IEEE 802.11b	Physical layer: 2.4-GHz DSSS at 5.5 and 11 Mbps
IEEE 802.11c	Bridge operation at 802.11 MAC layer
IEEE 802.11d	Physical layer: Extend operation of 802.11 WLANs to new regulatory domains (countries)
IEEE 802.11e	MAC: Enhance to improve quality of service and enhance security mechanisms
IEEE 802.11g	Physical layer: Extend 802.11b to data rates >20 Mbps
IEEE 802.11i	MAC: Enhance security and authentication mechanisms
IEEE 802.11n	Physical/MAC: Enhancements to enable higher throughput
IEEE 802.11T	Recommended practice for the evaluation of 802.11 wireless performance
IEEE 802.11ac	Physical/MAC: Enhancements to support 0.5–1 Gbps in 5-GHz band
IEEE 802.11ad	Physical/MAC: Enhancements to support ≥ 1 Gbps in the 60-GHz band

(Table can be found on page 424 in the textbook)

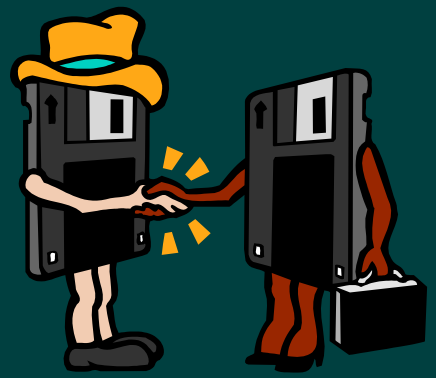
Table 13.2
IEEE 802.11 Terminology

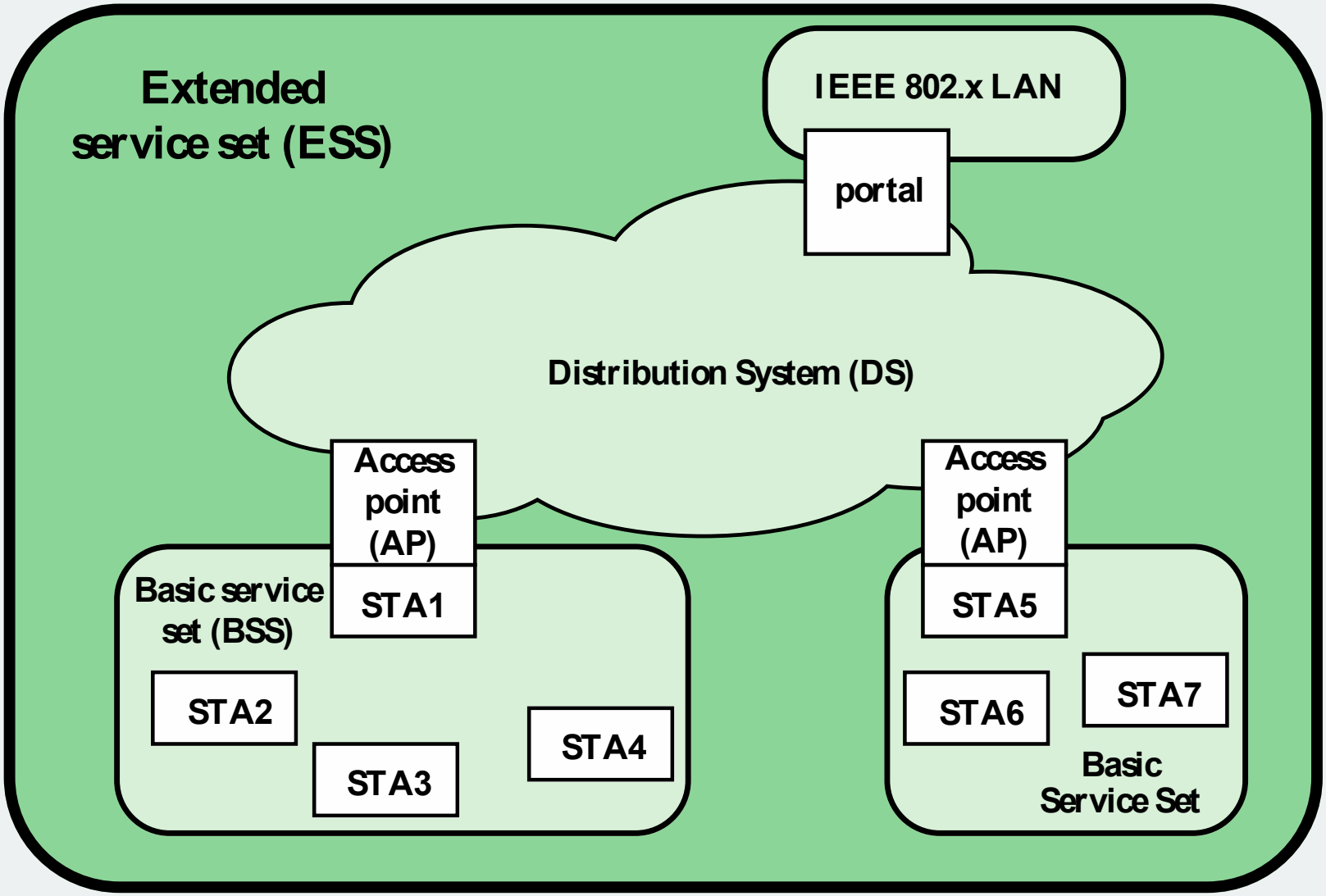
Access point (AP)	Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations
Basic service set (BSS)	A set of stations controlled by a single coordination function
Coordination function	The logical function that determines when a station operating within a BSS is permitted to transmit and may be able to receive PDUs
Distribution system (DS)	A system used to interconnect a set of BSSs and integrated LANs to create an ESS
Extended service set (ESS)	A set of one or more interconnected BSSs and integrated LANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs
Frame	Synonym for MAC protocol data unit
MAC protocol data unit (MPDU)	The unit of data exchanged between two peer MAC entities using the services of the physical layer
MAC service data unit (MSDU)	Information that is delivered as a unit between MAC users
Station	Any device that contains an IEEE 802.11 conformant MAC and physical layer

(Table can be found on page 424 in the textbook)

Wi-Fi Alliance

- There is always a concern whether products from different vendors will successfully interoperate
- Wireless Ethernet Compatibility Alliance (WECA)
  - Industry consortium formed in 1999
- Renamed the Wi-Fi (Wireless Fidelity) Alliance
  - Created a test suite to certify interoperability for 802.11 products





STA = station

Figure 13.4 IEEE 802.11 Architecture

Table 13.3
IEEE 802.11 Services

Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Dissassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery
Privacy	Station	LAN access and security
Reassocation	Distribution system	MSDU delivery

Distribution of Messages Within a DS

Integration service

- Enables transfer of data between a station on an IEEE 802.11 LAN and a station on an integrated IEEE 802.x LAN
- Takes care of any address translation and media conversion logic required for the exchange of data

Distribution service

- Primary service used by stations to exchange MAC frames when frame must traverse the DS to get from a station in one BSS to a station in another BSS
- If stations are in the same BSS, distribution service logically goes through the single AP of that BSS

Association-Related Services

- DS requires information about stations within the ESS that is provided by the association-related services
- Station must be associated before DS can deliver data to or accept data from it
- 3 mobility transition types:

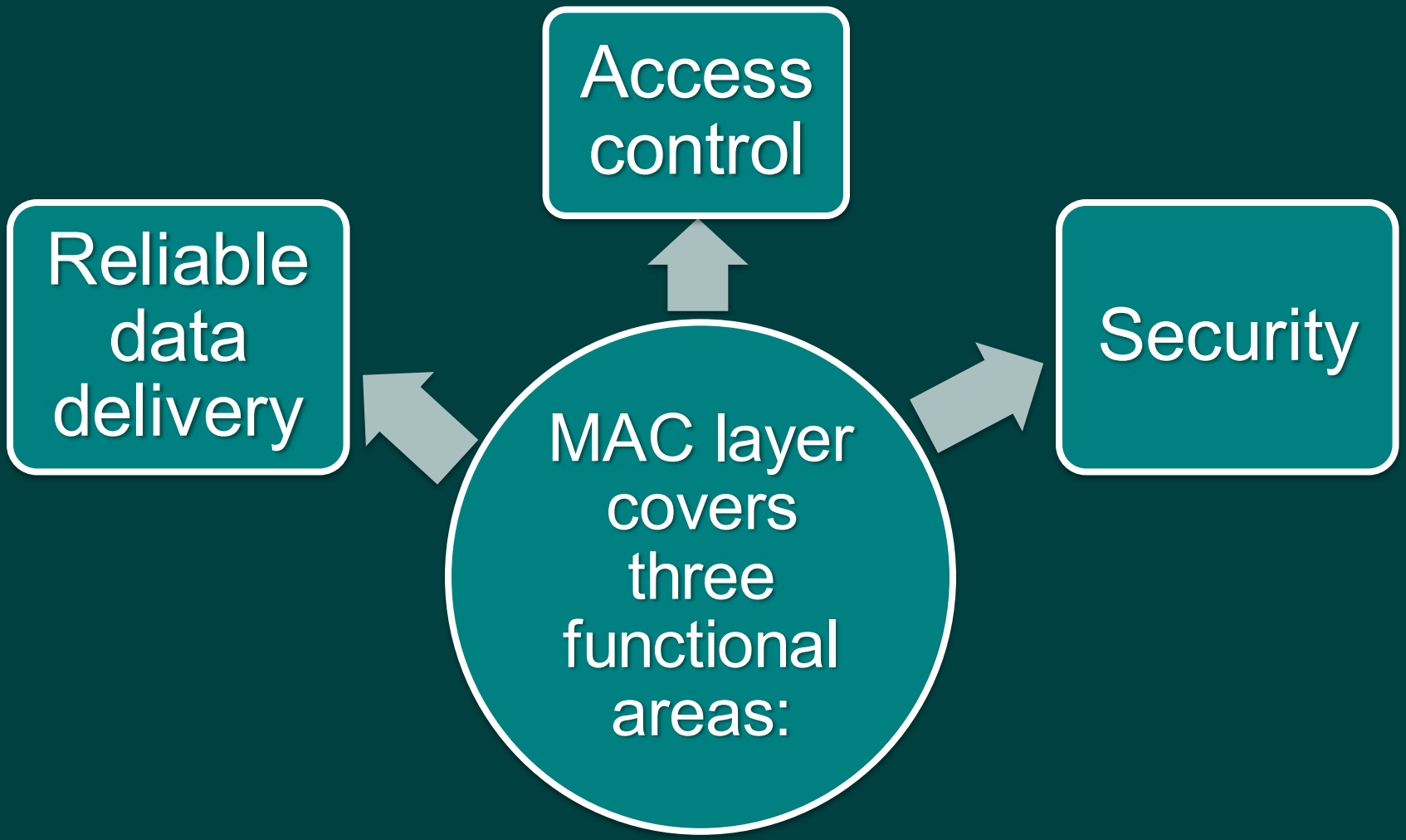
Association Related Services

- DS needs to know the identity of the AP to which the message should be delivered
  - Stations must maintain association with AP within current BSS

3 services relate to this requirement:

- *Association* - establishes initial association between station and AP
- *Reassociation* – enables an established association to be transferred from one AP to another
- *Disassociation* – a notification from either a station or an AP that an existing association is terminated

Medium Access Control



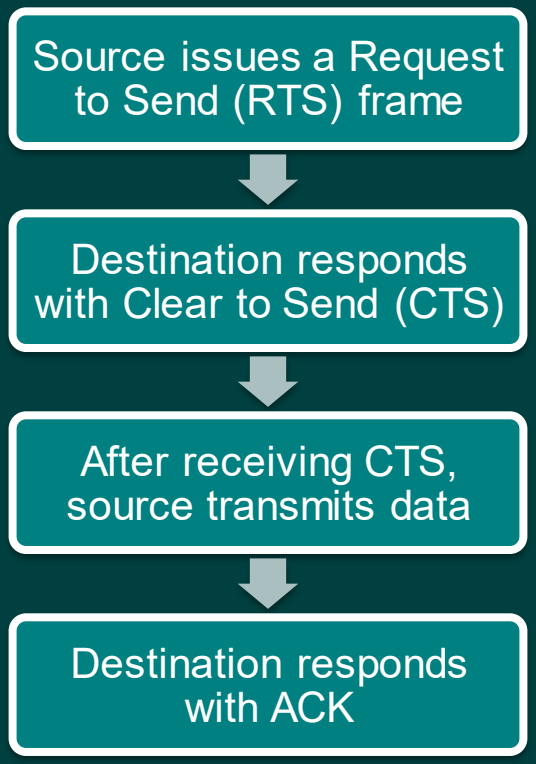
Reliable Data Delivery

- Can be dealt with at a higher layer
- More efficient to deal with errors at MAC level
- 802.11 includes frame exchange protocol
  - Station receiving frame returns acknowledgment (ACK) frame
  - Exchange treated as atomic unit
  - If no ACK within short period of time, retransmit
- 802.11 physical and MAC layers unreliable
  - Noise, interference, and other propagation effects result in loss of frames
  - Even with error-correction codes, frames may not successfully be received

Four Frame Exchange

- RTS alerts all stations within range of source that exchange is under way
- CTS alerts all stations within range of destination
- Other stations don't transmit to avoid collision
- RTS/CTS exchange is a required function of MAC but may be disabled

- Can use four-frame exchange for better reliability



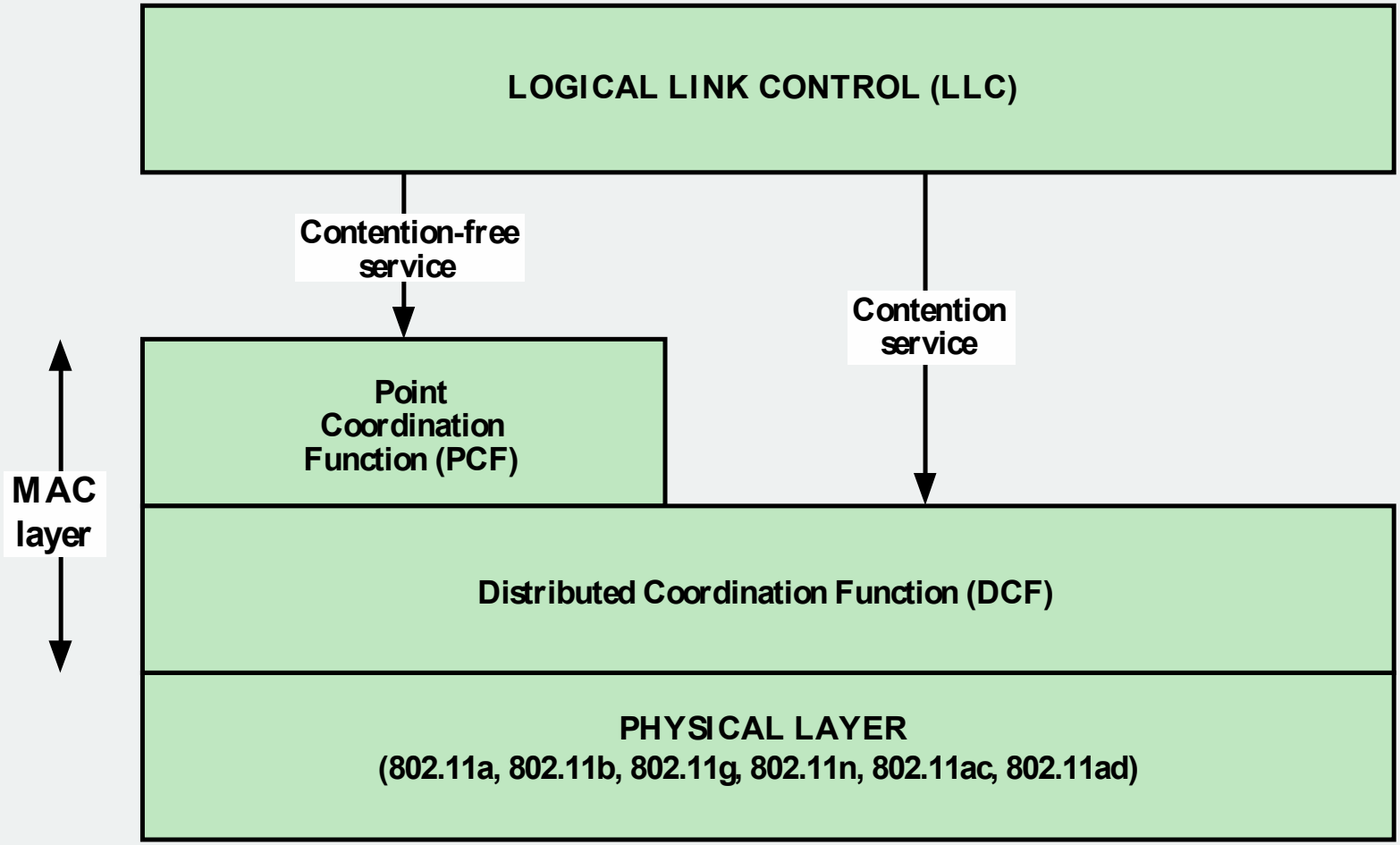
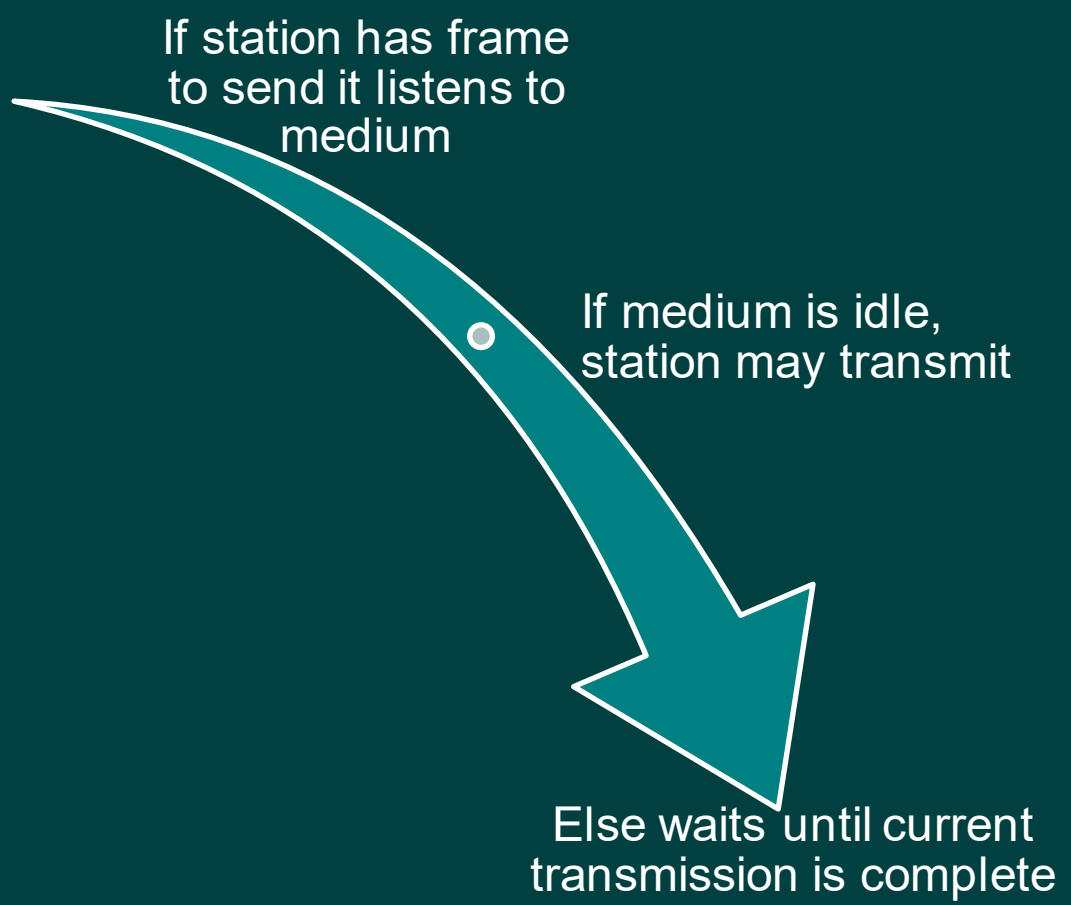


Figure 13.5 IEEE 802.11 Protocol Architecture

Distributed Coordination Function (DCF)

- DCF sublayer uses CSMA algorithm
- Does not include a collision detection function because it is not practical on a wireless network
- Includes a set of delays that amounts as a priority scheme



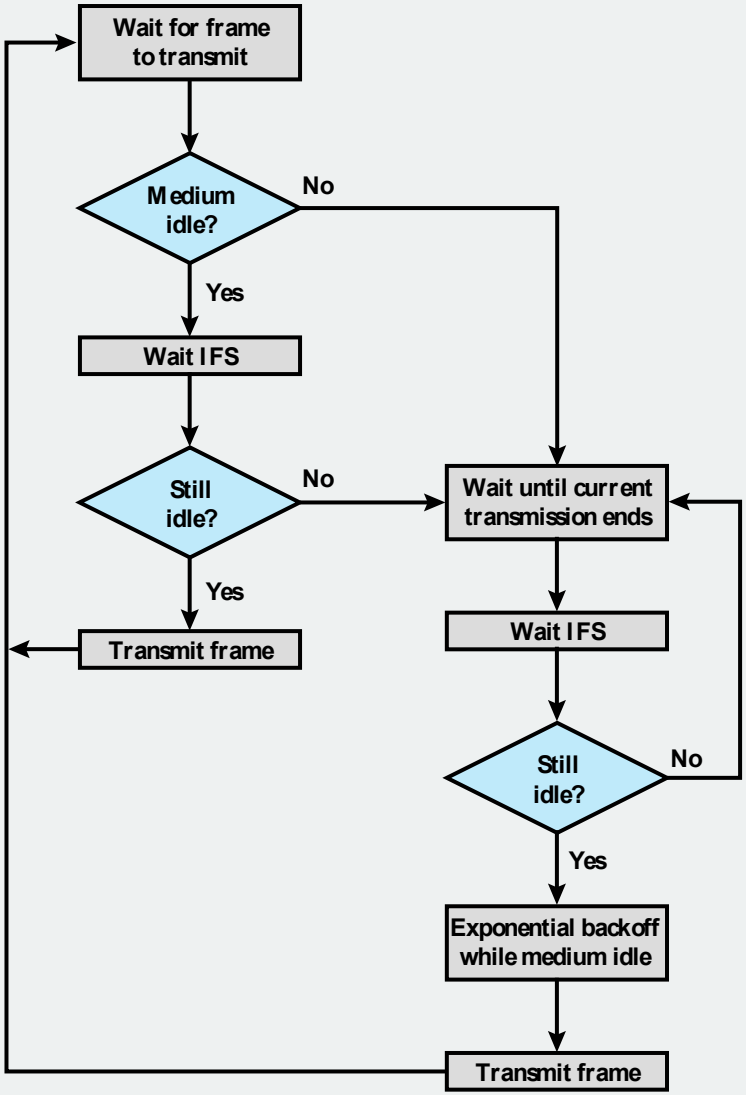


Figure 13.6 IEEE 802.11 Medium Access Control Logic

Priority IFS Values

SIFS

(short IFS)

For all immediate response actions

PIFS

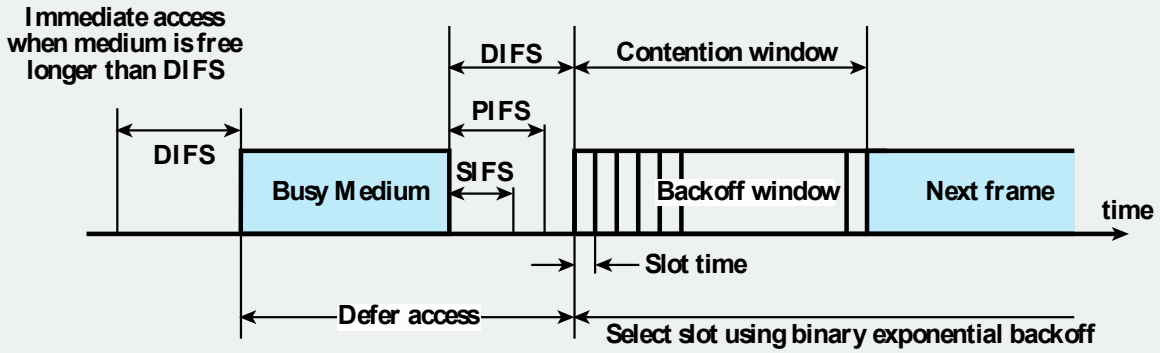
(point coordination function IFS)

Used by the centralized controller in PCF scheme when issuing polls

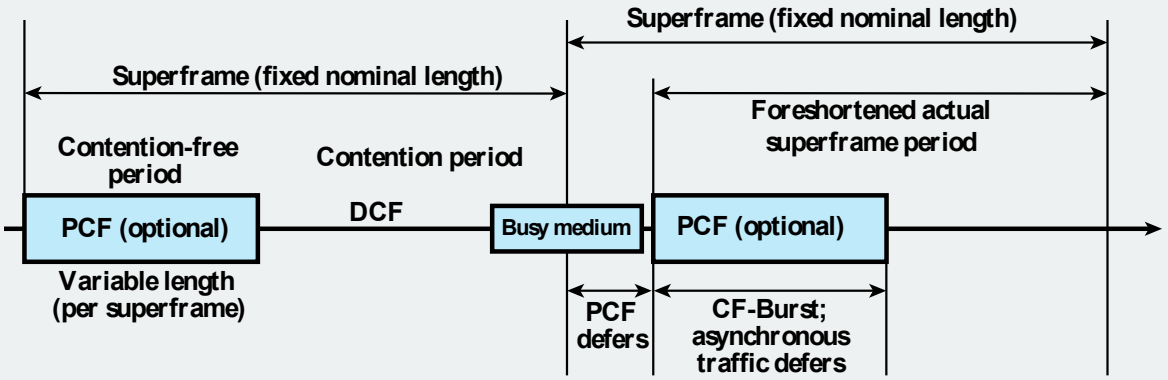
DIFS

(distributed coordination function IFS)

Used as minimum delay for asynchronous frames contending for access



(a) Basic Access Method



(b) PCF Superframe Construction

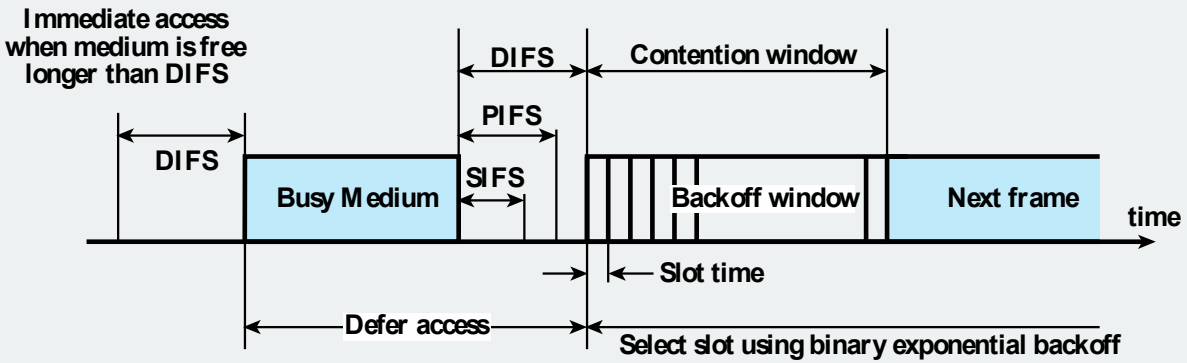
Figure 13.7 IEEE 802.11 MAC Timing

SIFS

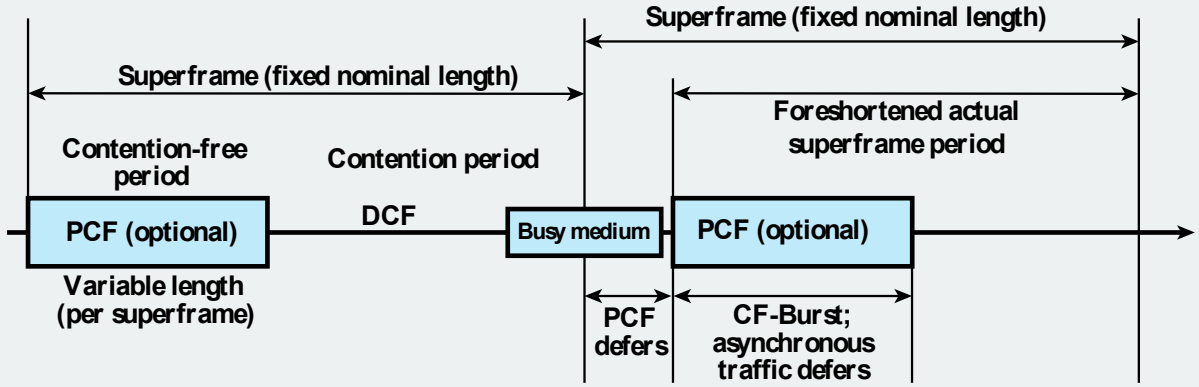
- Any station using SIFS to determine transmission opportunity has the highest priority
- Used in the following circumstances:
  - Acknowledgment (ACK)
    - Station responds with an ACK frame after waiting only for a SIFS gap
    - Provides for efficient collision recovery
  - Clear to Send (CTS)
    - Station ensures data frame gets through by issuing RTS
  - Poll response

Point Coordination Function (PCF)

- Alternative access method implemented on top of DCF
- Polling by centralized polling master (point coordinator)
- Uses PIFS when issuing polls
- Point coordinator polls in round-robin to stations configured for polling
- When poll issued, polled station may respond using SIFS
- If point coordinator receives response, it issues another poll using PIFS
- If no response during expected turnaround time, coordinator issues poll
- Coordinator could lock out asynchronous traffic by issuing polls
- Have a superframe interval defined



(a) Basic Access Method



(b) PCF Superframe Construction

Figure 13.7 IEEE 802.11 MAC Timing

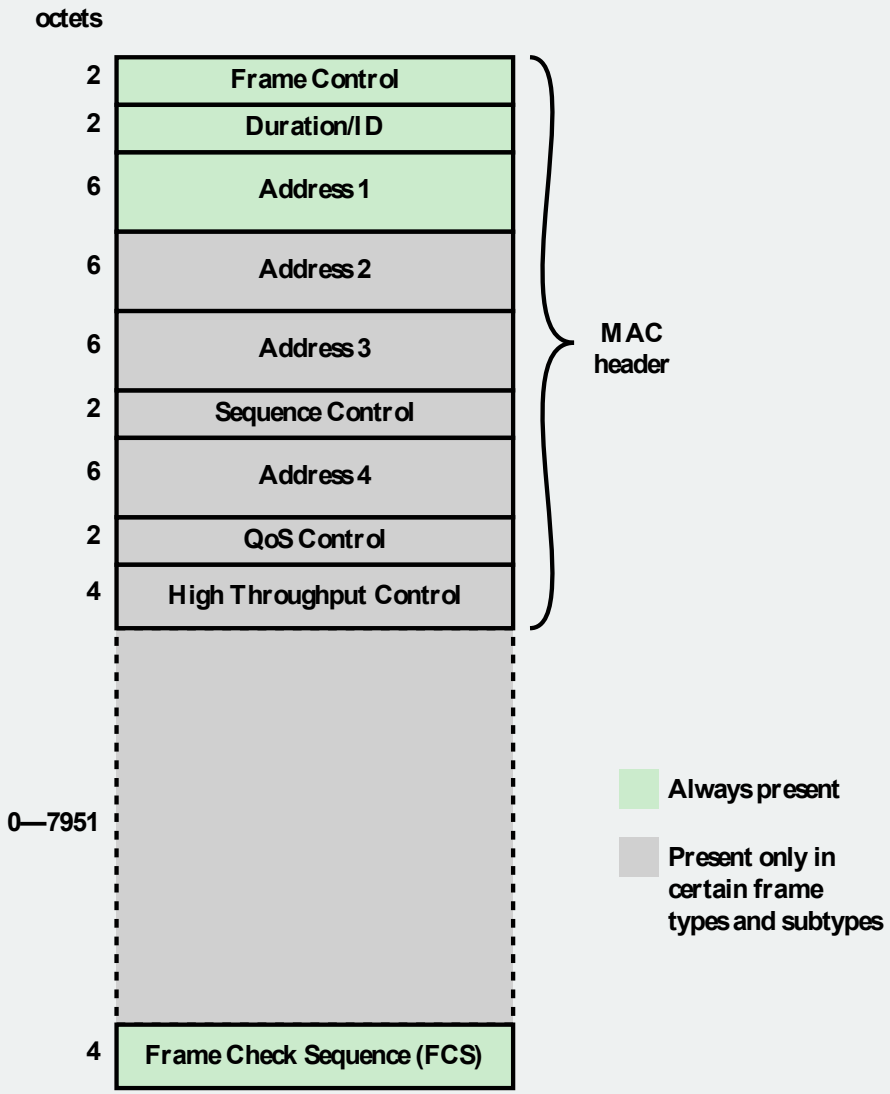


Figure 13.8 IEEE 802.11 MAC Frame Format

Control Frames

Power Save-Poll (PS-Poll)

- Request AP transmit buffered frame when in power-saving mode

Request to Send (RTS)

- First frame in four-way frame exchange

Clear to Send (CTS)

- Second frame in four-way exchange

Acknowledgment (ACK)

- Acknowledges correct receipt

Contention-Free (CF)-end

- Announces end of contention-free period part of PCF

CF-End + CF-Ack:

- Acknowledges CF-end to end contention-free period and release stations from associated restrictions

Data Frames

- Eight data frame subtypes
  - Organized in two groups
    - First four carry upper-level data
    - Remaining do not carry any user data
- Data
  - Simplest data frame, contention or contention-free use
- Data + CF-Ack
  - Carries data and acknowledges previously received data during contention-free period
- Data + CF-Poll
  - Used by point coordinator to deliver data and request send
- Data + CF-Ack + CF-Poll
  - Combines Data + CF-Ack and Data + CF-Poll

Management Frames

Used to manage communications between stations and APs

Management of associations

- Request, response, reassociation, dissociation, and authentication

Table 13.4
IEEE 802.11 Physical Layer Standards

Standard	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ad
Year introduced	1999	1999	2003	2000	2012	2014
Maximum data transfer speed	54 Mbps	11 Mbps	54 Mbps	65 to 600 Mbps	78 Mbps to 3.2 Gbps	6.76 Gbps
Frequency band	5 GHz	2.4 GHz	2.4 GHz	2.4 or 5 GHz	5 GHz	60 GHz
Channel bandwidth	20 MHz	20 MHz	20 MHz	20, 40 MHz	40, 80, 160 MHz	2160 MHz
Highest order modulation	64 QAM	11 CCK	64 QAM	64 QAM	256 QAM	64 QAM
Spectrum usage	DSSS	OFDM	DSSS, OFDM	OFDM	SC-OFDM	SC, OFDM
Antenna configuration	1 1 SISO	1 1 SISO	1 1 SISO	Up to 4 4 MIMO	Up to 8 8 MIMO, MU-MIMO	1 1 SISO

(Table is on page 436 in textbook)

IEEE 802.11b

- Extension of 802.11 DSSS scheme
  - Data rates of 5.5 and 11 Mbps
- Chipping rate 11 MHz
  - Same as original DSSS scheme
  - Complementary Code Keying (CCK) modulation gives higher data rate with same bandwidth and chipping rate
  - Packet Binary Convolutional Coding (PBCC) for future higher rate use

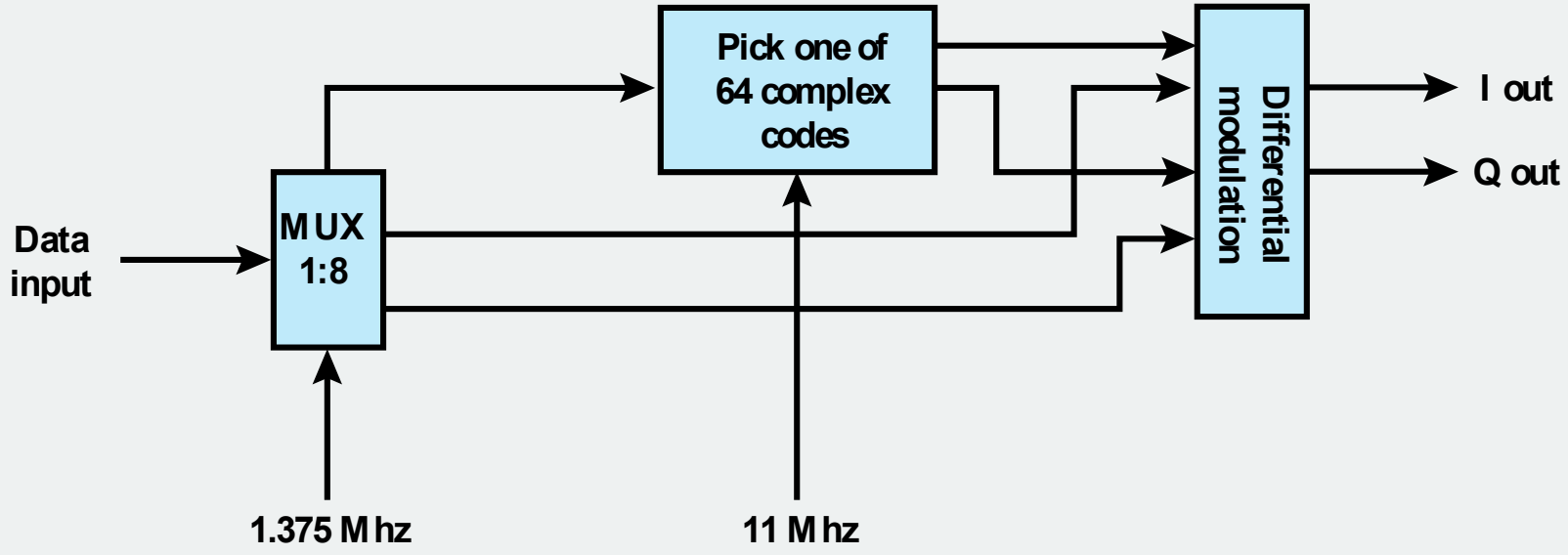
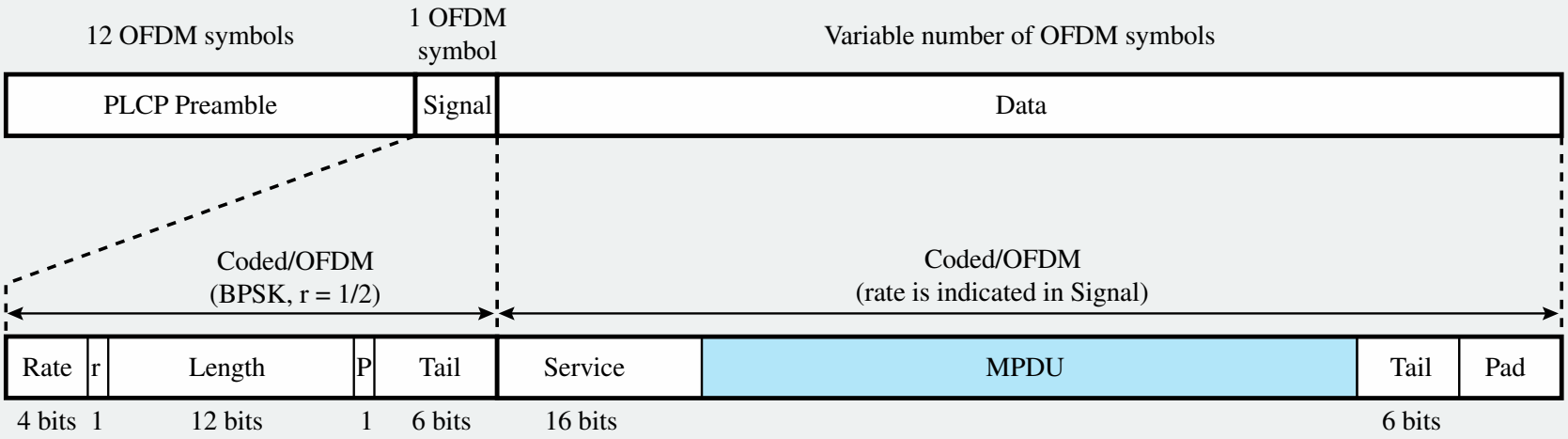
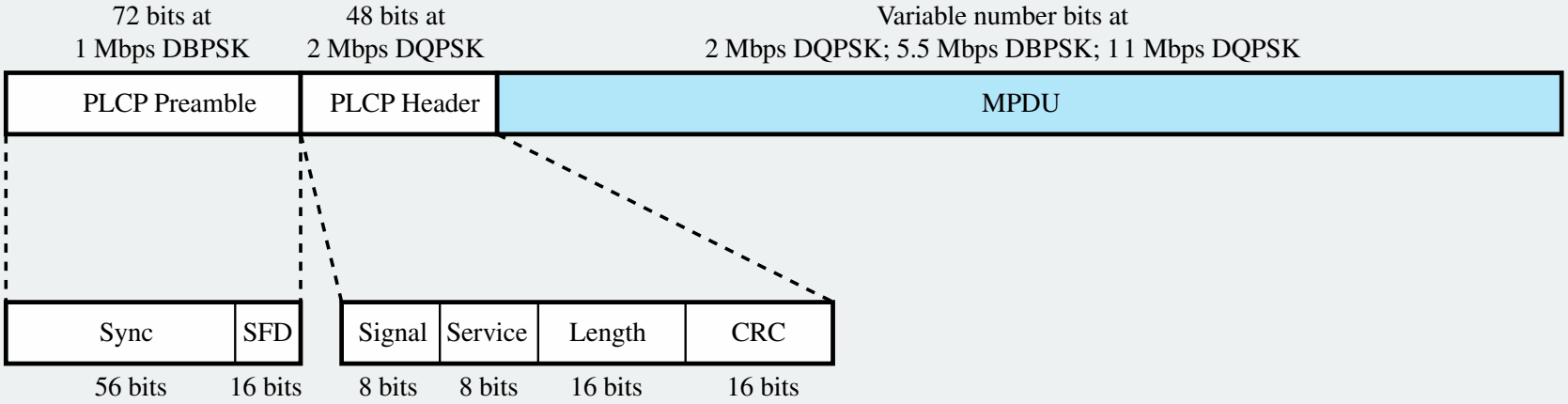


Figure 13.9 11-Mbps CCK Modulation Scheme



(a) IEEE 802.11a physical PDU



(b) IEEE 802.11b physical PDU

Figure 13.10 IEEE 802 Physical-Level Protocol Data Units

PLCP Header

- Follows the preamble and is transmitted at 2 Mbps using DQPSK
- Consists of the following subfields:
  - Signal
    - Specifies the data rate at which the MPDU portion of the frame is transmitted
  - Service
    - Only 3 bits of this 8-bit field are used in 802.11b
  - Length
    - Indicates the length of the MPDU field by specifying the number of microseconds necessary to transmit the MPDU
  - CRC
    - A 16-bit error-detection code used to protect the Signal, Service, and Length fields

IEEE 802.11a

- Universal Networking Information Infrastructure (UNNI)
  - UNNI-1 band (5.15 to 5.25 GHz) for indoor use
  - UNNI-2 band (5.25 to 5.35GHz) for indoor or outdoor
  - UNNI-3 band (5.725 to 5.825 GHz) for outdoor
- Advantages over IEEE 802.11b/g:
- IEEE 802.11a
  - Utilizes more available bandwidth
  - Provides much higher data rates
  - Uses a relatively uncluttered frequency spectrum (5 GHz)

Physical-Layer Frame Structure

- Primary purpose of layer is to transmit MAC protocol data units as directed by the 802.11 MAC layer
- Signal field consists of:
  - Rate
    - Specifies the data rate at which the data field portion of the frame is transmitted
  - r:
    - Reserved for future use
  - Length
    - Number of octets in the MAC PDU
  - P:
    - An even parity bit for the 17 bits in the Rate, r, and Length subfields
  - Tail
    - Consists of 6 zero bits appended to the symbol to bring the convolutional encoder to zero state

Data field consists of four subfields:

- Service
- MAC PDU
- Tail
- Pad

IEEE 802.11g

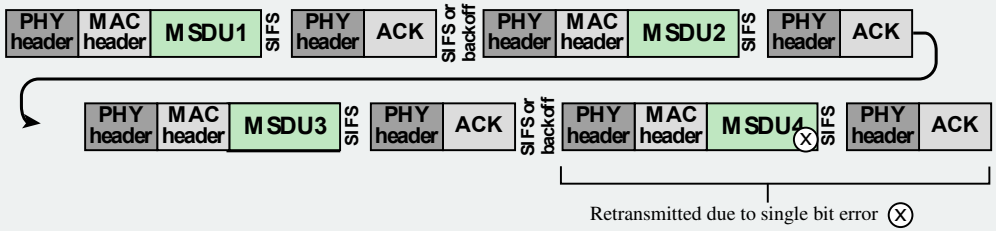
- Higher-speed extension to 802.11b
- Operates in 2.4GHz band
- Compatible with 802.11b devices
- Combinesphysical layer encoding techniques used in 802.11 and 802.11b to provide service at a variety of data rates
  - ERP-OFDM for 6, 9, 12, 18, 24, 36, 48, 54Mbps rates
  - ERP-PBCC for 22 and 33Mbps rates

Table 13.5
Estimated Distance (m) Versus Data Rate

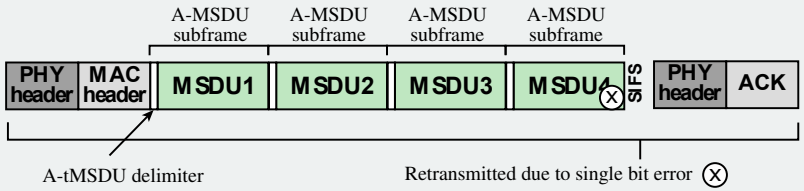
Data Rate (Mbps)	802.11b	802.11a	802.11g
1	90+	—	90+
2	75	—	75
5.5(b)/6(a/g)	60	60+	65
9	—	50	55
11(b)/12(a/g)	50	45	50
18	—	40	50
24	—	30	45
36	—	25	35
48	—	15	25
54	—	10	20

IEEE 802.11n

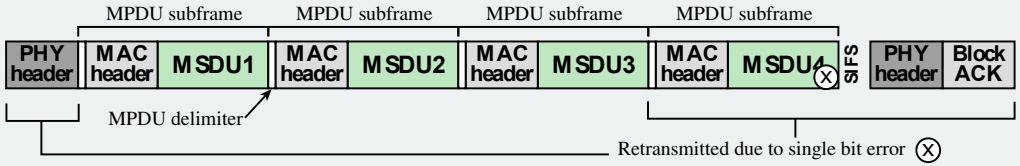
- Has enhancements in three general areas:
  - Multiple-input-multiple-output (MIMO) antenna architecture
    - Most important enhancement
  - Radio transmission scheme
    - Increased capacity
  - MAC enhancements
    - Most significant change is to aggregate multiple MAC frames into a single block for transmission



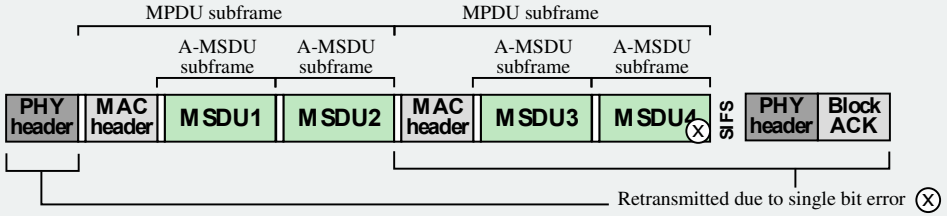
(a) No aggregation



(b) A-MSDU aggregation



(c) A-MPDU aggregation



(d) A-MPDU of A-MSDU aggregation

Figure 13.11 Forms of Aggregation

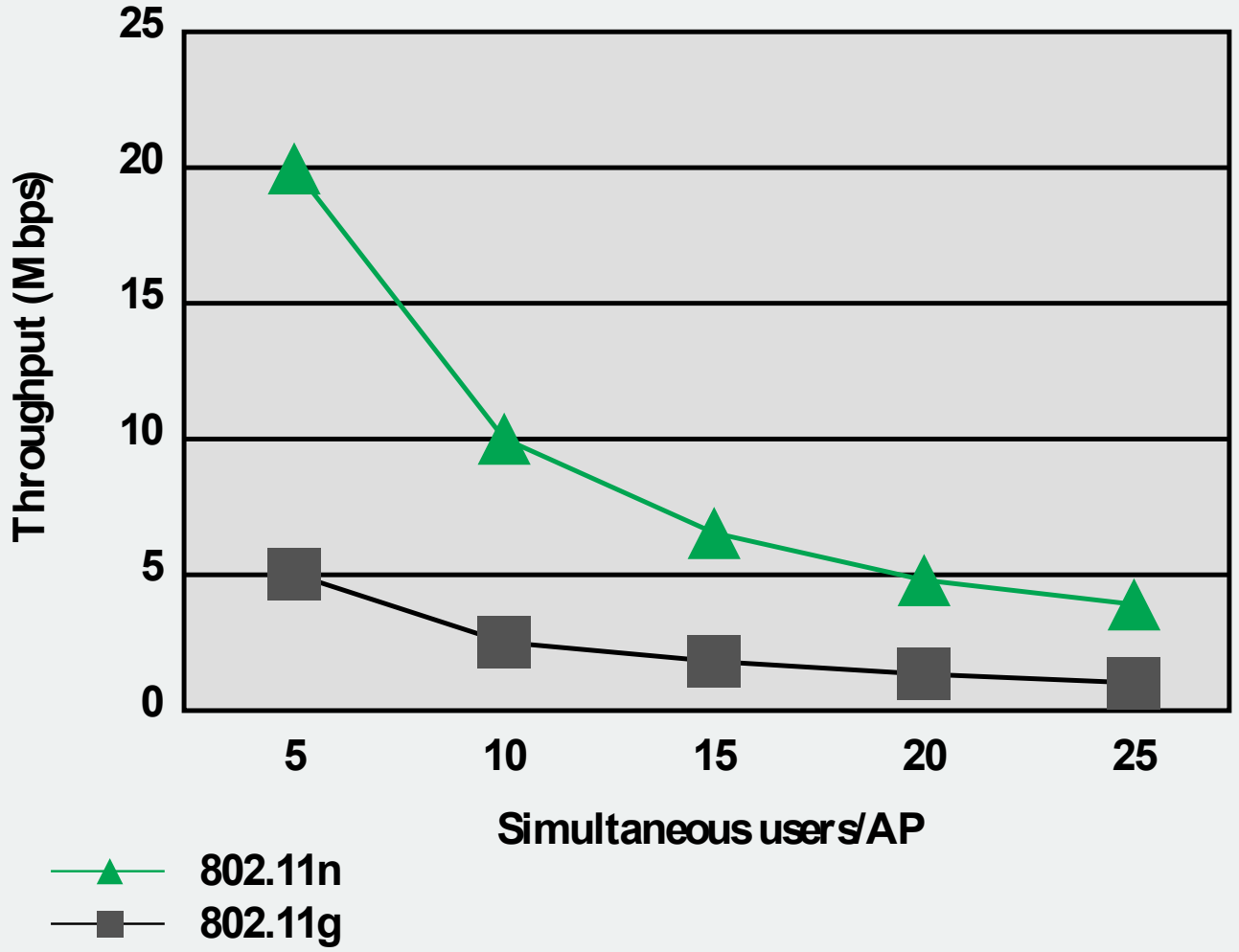


Figure 13.12 Average Throughput per User

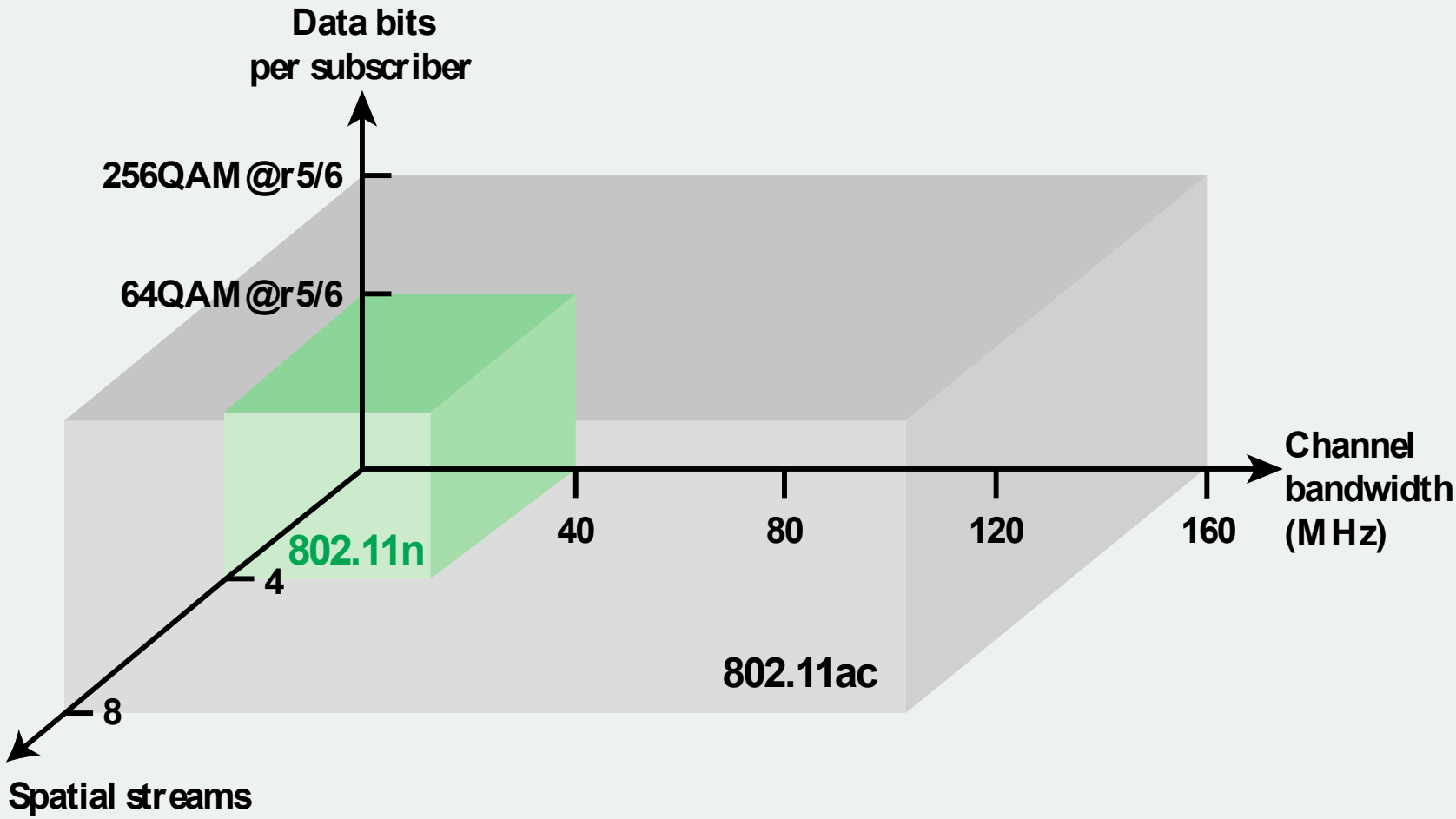


Figure 13.13 IEEE 802.11 Performance Factors

IEEE 802.11ac

- Includes the option of multiuser MIMO (MU-MIMO)
  - On the downlink the transmitter is able to use its antenna resources to transmit multiple frames to different stations, all at the same time and over the same frequency spectrum
  - Each antenna of a MU-MIMO AP can simultaneously communicate with a different single-antenna device, such as a smartphone or tablet
- Requires that every 802.11ac transmission be sent as an A-MPDU aggregate

IEEE 802.11ad

- A version of 802.11 operating in the 60-GHz frequency band
  - Offers the potential for much wider channel bandwidth than the 5-GHz band
  - Few devices operate in the 60-GHz which means communications would experience less interference than in the other bands used by 802.11
- Undesirable propagation characteristics:
  - Losses are much higher in this range than in the ranges used for traditional microwave systems
  - Multipath losses can be quite high
  - Millimeter-wave signals generally don't penetrate solid objects

802.11ac and 802.11ad Differences

802.11ac

- Supports a MIMO antenna configuration

802.11ad

- Is designed for single-antenna operation
- Has a huge channel bandwidth of 2160 MHz

Table 13.6
IEEE 802.11ad Modulation and Coding Schemes

Physical Layer	Coding	Modulation	Raw Bit Rate
Control (CPHY)	1/2 LDPC, 32 spreading	π/2-DBPSK	27.5 Mbps
Single carrier (SCPHY)	1/2 LDPC 1/2 LDPC, 5/8 LDPC 3/4 LDPC 13/16 LDPC	π/2-BPSK, π/2-QPSK, π 2-16QAM	385 Mbps to 4.62 Gbps
OFDM (OFDMPHY)	1/2 LDPC, 5/8 LDPC 3/4 LDPC 13/16 LDPC	OFDM-OQPSK OFDM-QPSK OFDM-16QAM OFDM-64QAM	693 Mbps to 6.76 Gbps
Low-power single carrier (LPSCPHY)	RS(224,208) + Block Code(16/12/9/8,8)	π/2-BPSK, π/2-QPSK	636 Mbps to 2.5 Gbps

BPSK = binary phase-shift keying
DBPSK = differential binary phase-shift keying
LDPC = low density parity check code
OFDM = orthogonal frequency-division multiplexing
OQPSK = offset quadrature phase-shift keying
QAM = quadrature amplitude modulation
QPSK = quadrature phase-shift keying
RS = Reed-Solomon

Access and Privacy Services - Authentication

- Used to establish station identity
- Wired LANs assume physical connection gives authority to use LAN
- Not a valid assumption for wireless LANs
- 802.11 supports several authentication schemes
- Does not mandate any particular scheme
- From relatively insecure handshaking to public-key encryption
- 802.11 requires mutually acceptable, successful authentication before association

Access and Privacy Services Deauthentication and Privacy

- Deauthentication
  - Invoked whenever an existing authentication is to be terminated

- Privacy
  - Used to prevent messages being read by others
  - 802.11 allows optional use of encryption
- Original WEP security features were weak
- Subsequently 802.11i and WPA alternatives evolved giving better security

Summary

- Wireless LAN configurations
- Wireless LAN requirements
- IEEE 802.11 architecture and services
  - The Wi-Fi alliance
  - IEEE 802.11 architecture
  - IEEE 802.11 services
- IEEE 802.11 medium access control
  - Reliable data delivery
  - Medium access control
  - MAC frame
- IEEE 802.11 physical layer
  - IEEE 802.11b
  - IEEE 802.11a
  - IEEE 802.11g
  - IEEE 802.11n
- Gigabit Wi-Fi
  - IEEE 802.11ac
  - IEEE 802.11ad
- IEEE 802.11 security considerations
  - Access and privacy services
  - Wireless LAN security standards