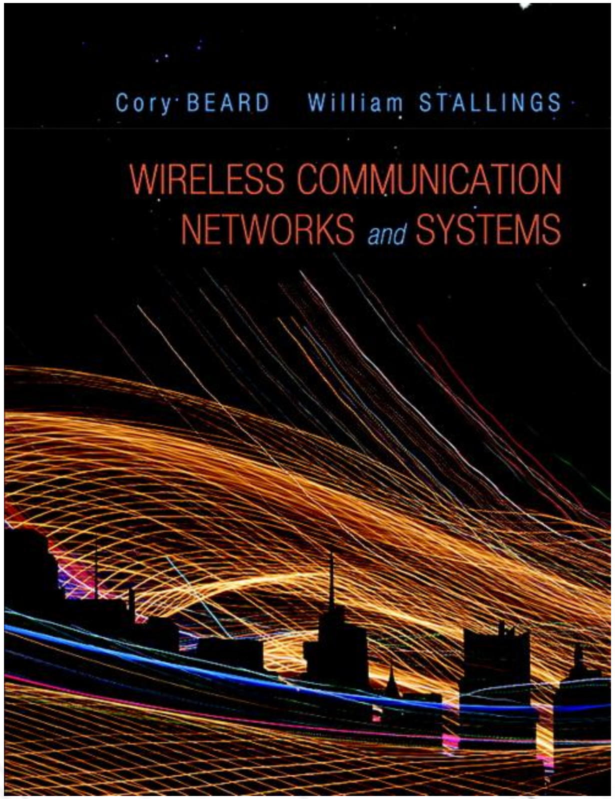
# CHAPTER 2
# WIRELESS LAN TECHNOLOGY AND THE IEEE 802.11 WIRELESS LAN STANDARD


Cory BEARD William STALLINGS
WIRELESS COMMUNICATION NETWORKS and SYSTEMS

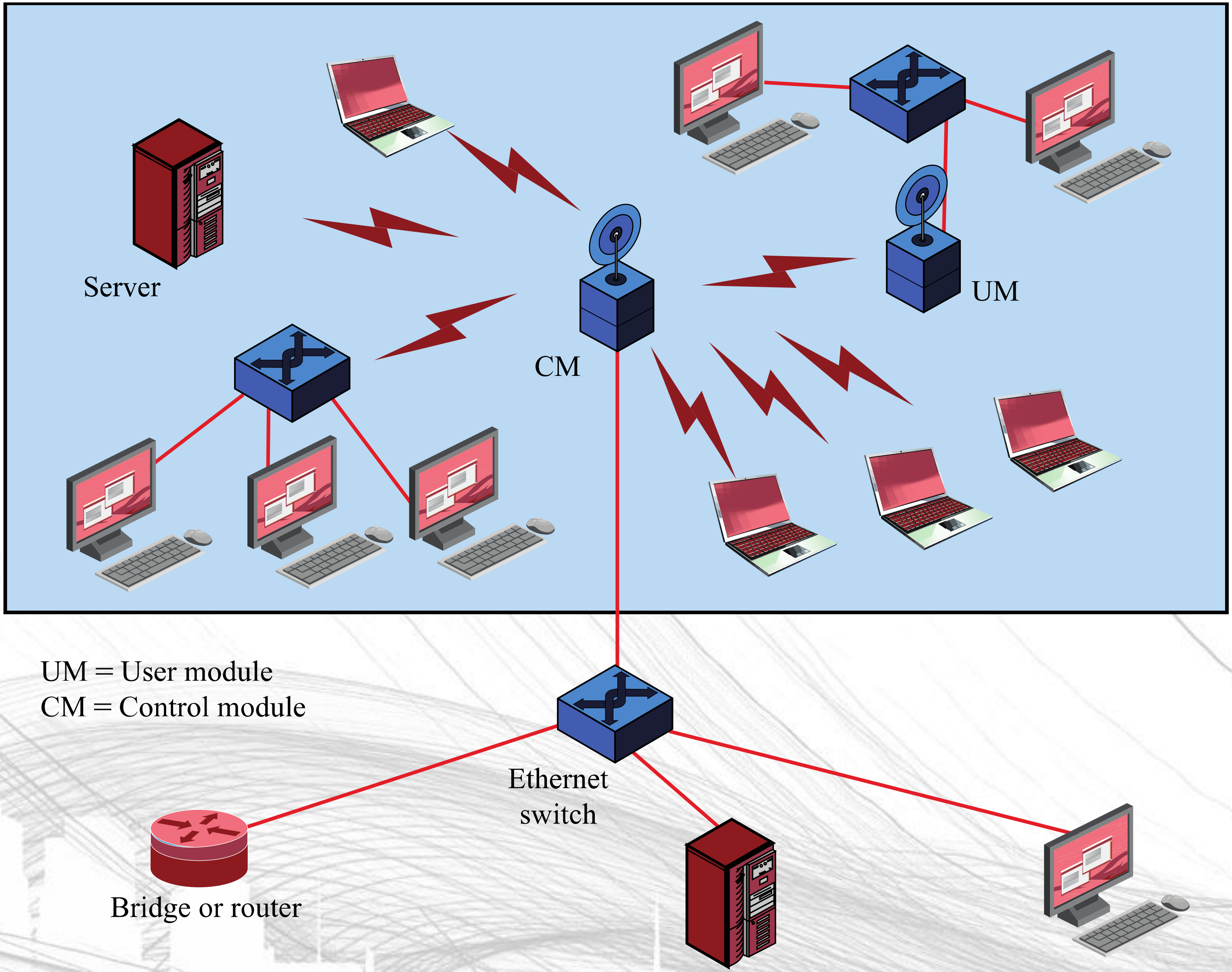
These slides are made available to faculty in PowerPoint form. Slides can be freely added, modified, and deleted to suit student needs. They represent substantial work on the part of the authors; therefore, we request the following.

If these slides are used in a class setting or posted on an internal or external www site, please mention the source textbook and note our copyright of this material.

**Wireless Communication Networks and Systems**
1st edition
**Cory Beard, William Stallings**

# INTRODUCTION

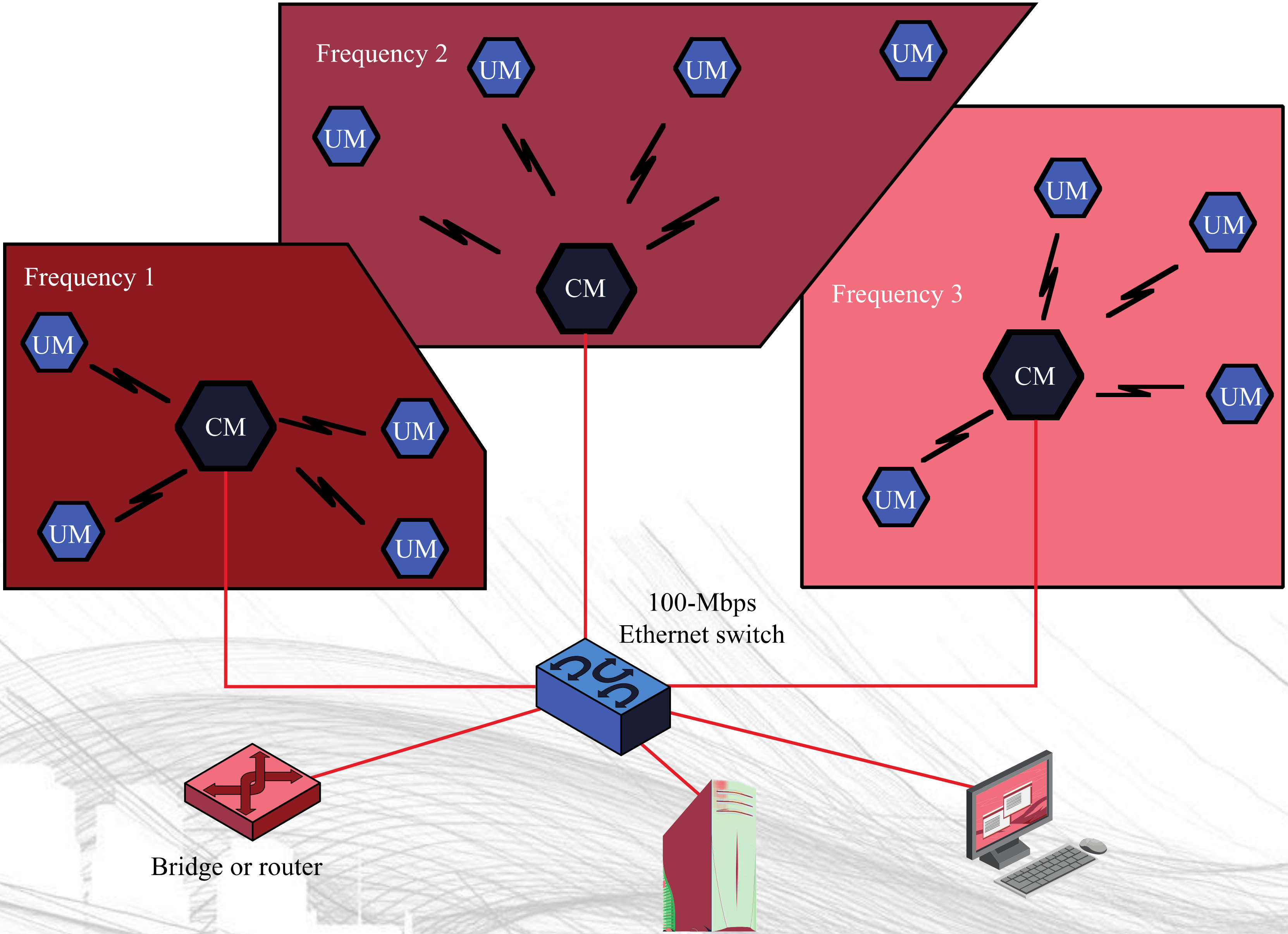
- Wireless LANs (WLANs)
  - Indispensible adjunct to wired LANs
  - Wireless devices use WLANs
    - As their only source of connectivity
    - Or to replace cellular coverage
- Simple WLAN configuration
  - There is a backbone wired LAN
  - User modules include workstations, servers, devices
  - Control module (CM) interfaces to WLAN
    - Providing bridge or router functionality
    - May have control logic to regulate access
    - May provide wireless connectivity to other wired networks



# 11.1 EXAMPLE SINGLE-CELL WIRELESS LAN CONFIGURATION

# INTRODUCTION

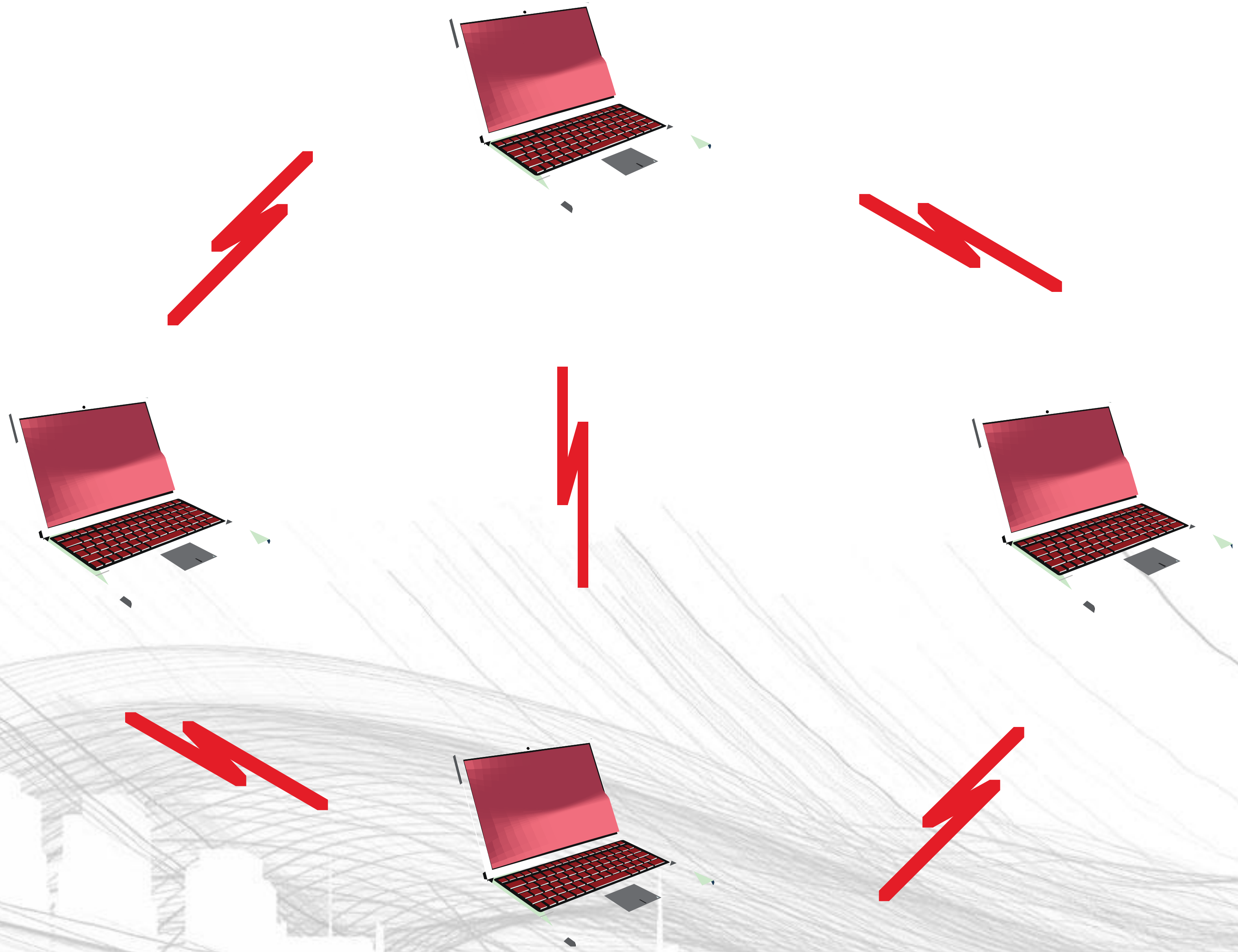
- Multiple-cell wireless LAN
  - Multiple CMs connected by a wired LAN
  - Creates many issues for balancing cell loading and providing best connections for Ums



# 11.2 EXAMPLE MULTIPLE-CELL WIRELESS LAN CONFIGURATION

# AD HOC NETWORKING

- Temporary peer-to-peer network set up to meet immediate need
  - Peer-to-peer, no centralized server
  - Maybe a temporary network
  - Wireless connectivity provided by WLAN or Bluetooth, ZigBee, etc.
- Example:
  - Group of employees with laptops convene for a meeting; employees link computers in a temporary network for duration of meeting



# 11.3 AD HOC WIRELESS LAN CONFIGURATION

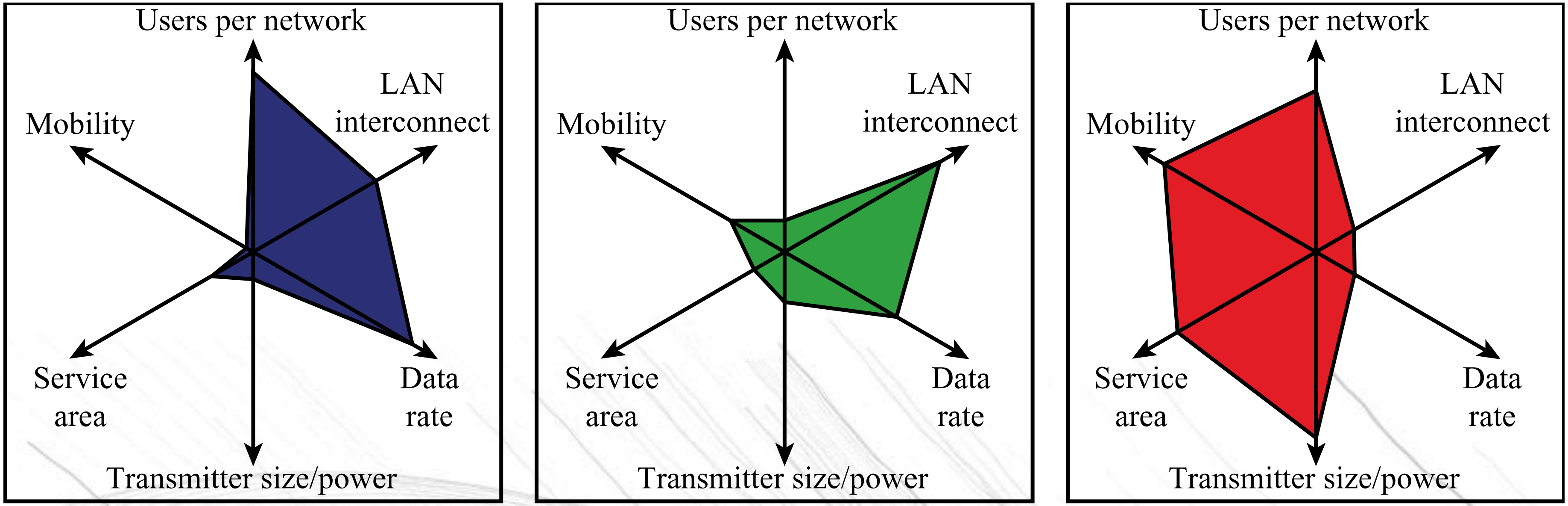
# WIRELESS LAN MOTIVATIONS

- Cellular data offloading
  - WLANs may provide higher data rates and more available capacity
  - Cellular providers may encourage this to offload demand on their networks
- Sync/file transfer
  - Avoid use of cables
- Internet access
- Multimedia streaming

# 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

- Comparisons between WLANs, wired LANs, and mobile data networks can be visualized with Kiviat graphs.



**(a) Wired LANs** **(b) Wireless LANs** **(c) Mobile data networks**

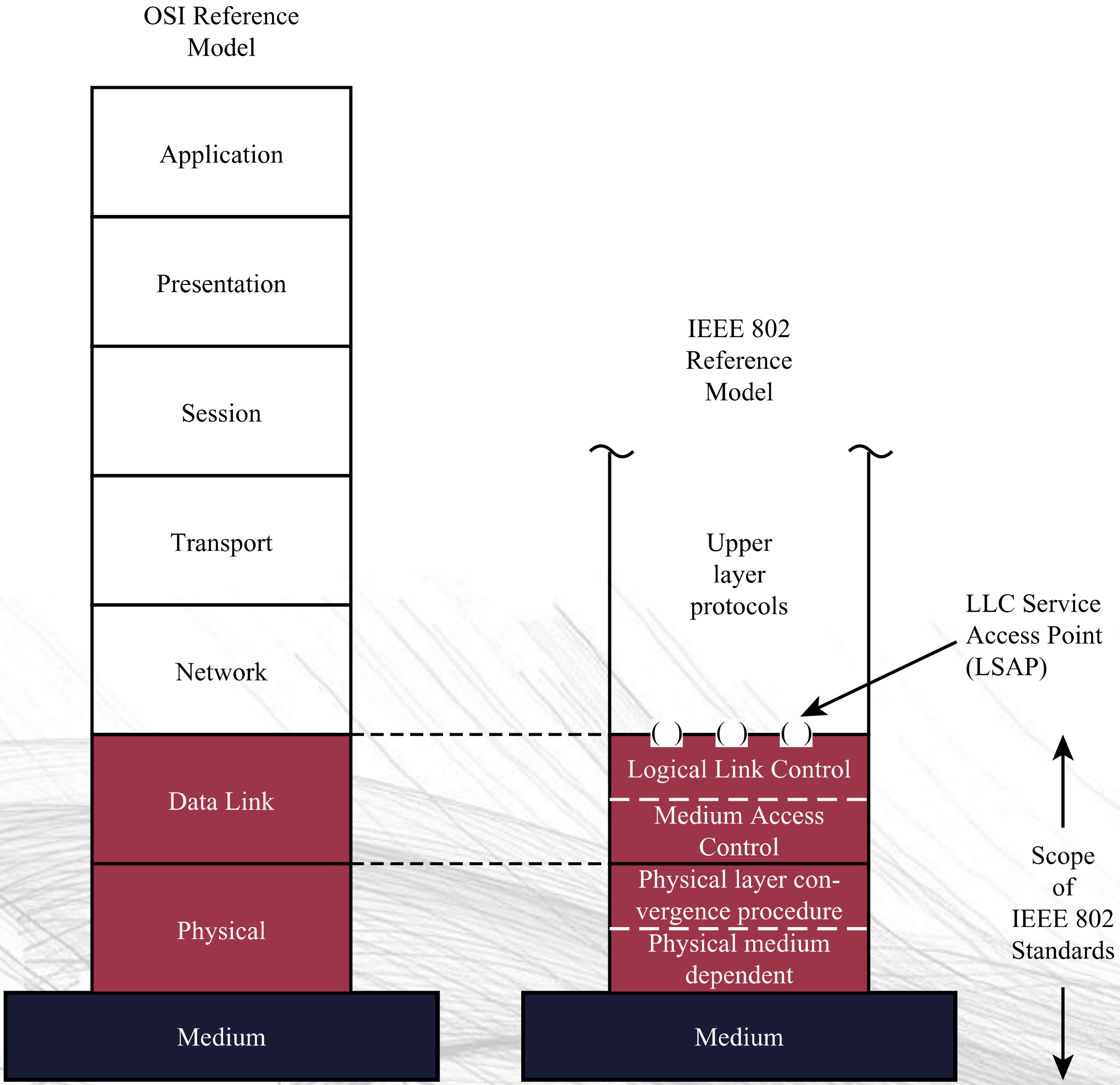
# 11.4 KIVIAT GRAPHS FOR DATA NETWORKS

# WIRELESS LAN PHYSICAL LAYER

- Multi-cell arrangement
- Transmission Issues
  - No licensing needed – Four microwave bands
    - 902-928 MHz
    - 2.4-2.5 GHz
    - 5.725-5.875 GHz
    - 58-64 GHz (60-GHz mmWave bands)
      - Higher capacity
      - Less competition
      - More expensive equipment
  - Spread spectrum
    - DSSS CDMA or OFDM
    - Over 1 Gbps possible with OFDM, channel bonding, and MIMO

# PROTOCOL ARCHITECTURE

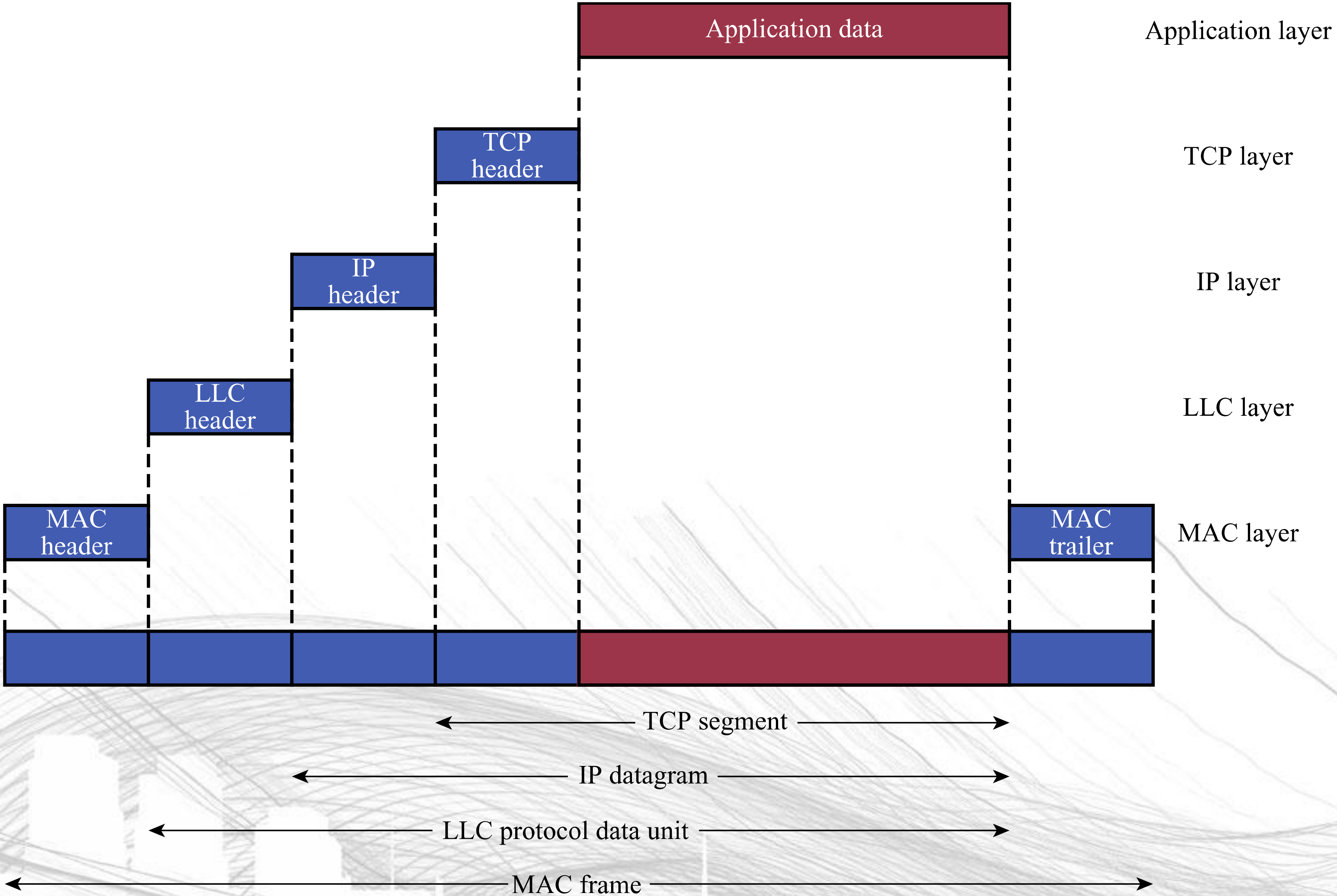
- Developed by the IEEE 802.11 working group
- Uses layering of protocols
- LAN protocols focus on the lower layers of the OSI model
  - Figure 11.5 relates OSI with 802.11
  - Called the IEEE 802 reference model



# 11.5 IEEE 802 PROTOCOL LAYERS COMPARED TO OSI MODEL

# PROTOCOL ARCHITECTURE

- Functions of physical layer:
  - Encoding/decoding of signals
  - Preamble generation/removal (for synchronization)
  - Bit transmission/reception
  - Includes specification of the transmission medium
- Sublayers
  - Physical medium dependent sublayer (PMD)
    - Transmitting and receiving user data through a wireless medium
  - Physical layer convergence procedure (PLCP)
    - Mapping 802.11 MAC layer protocol data units (MPDUs) into a framing format
    - Sending and receiving between stations using same PMD sublayer



# 11.6 IEEE 802 PROTOCOLS IN CONTEXT

# PROTOCOL ARCHITECTURE

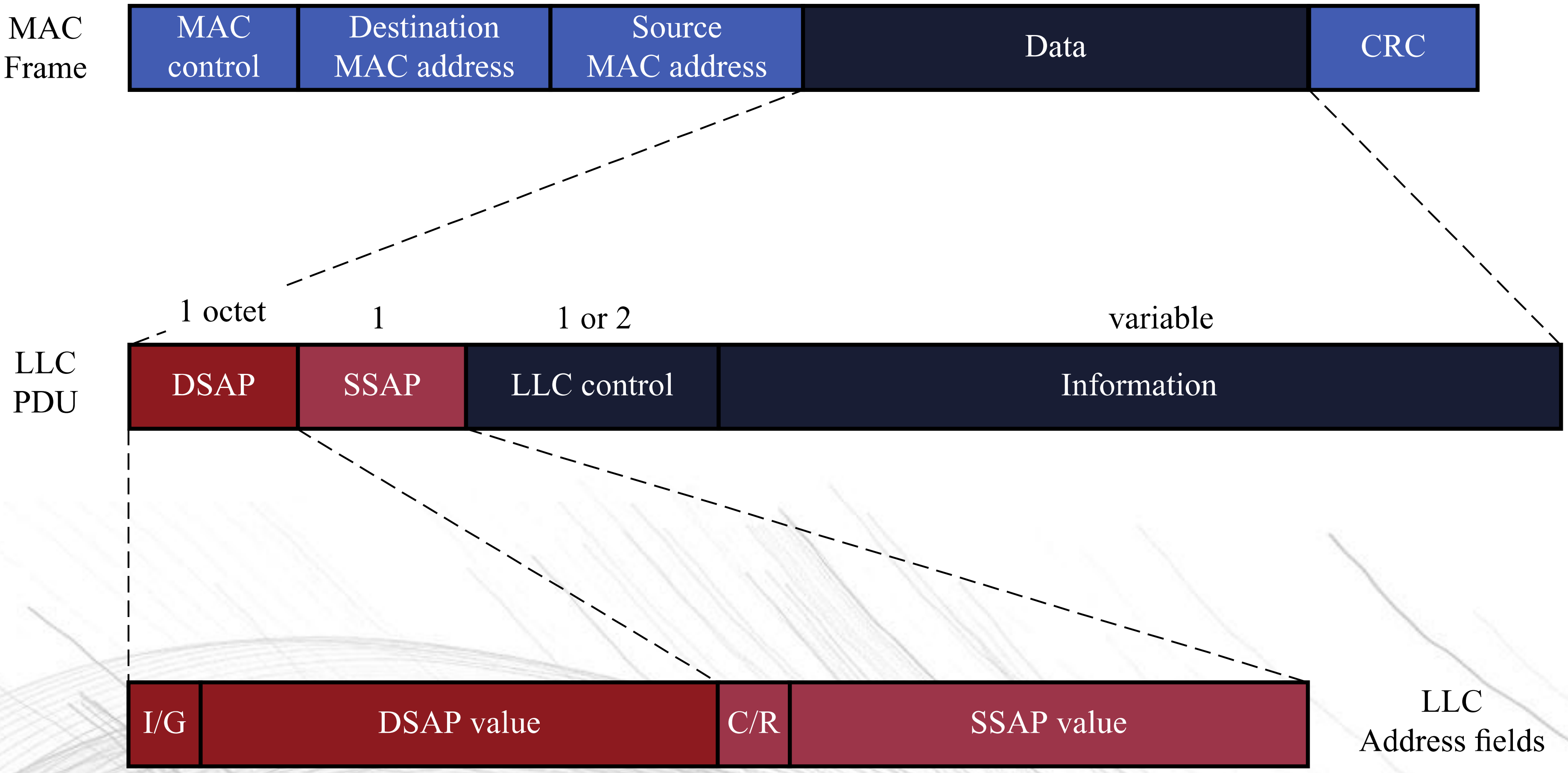
- Functions of medium access control (MAC) layer:
  - On transmission, assemble data into a frame with address and error detection fields
  - On reception, disassemble frame and perform address recognition and error detection
  - Govern access to the LAN transmission medium
- Functions of logical link control (LLC) Layer:
  - Provide an interface to higher layers and perform flow and error control

# SEPARATION OF LLC AND MAC

- The logic required to manage access to a shared-access medium not found in traditional layer 2 data link control
- For the same LLC, several MAC options may be provided

# MAC FRAME FORMAT

- MAC control
  - Contains Mac protocol information
- Destination MAC address
  - Destination physical attachment point
- Source MAC address
  - Source physical attachment point
- CRC
  - Cyclic redundancy check



MAC Frame

MAC control | Destination MAC address | Source MAC address | Data | CRC

LLC PDU

1 octet | 1 | 1 or 2 | variable

DSAP | SSAP | LLC control | Information

LLC Address fields

I/G | DSAP value | C/R | SSAP value

I/G = individual/group
C/R = command/response

DSAP = destination service access point
SSAP = source service access point

# 11.7 LLC PDU IN A GENERIC MAC FRAME FORMAT

# LOGICAL LINK CONTROL

- Characteristics of LLC not shared by other control protocols:
  - Must support multi-access, shared-medium nature of the link
  - Relieved of some details of link access by MAC layer

# LLC SERVICES

- Unacknowledged connectionless service
  - No flow- and error-control mechanisms
  - Data delivery not guaranteed
- Connection-mode service
  - Logical connection set up between two users
  - Flow- and error-control provided
- Acknowledged connectionless service
  - Cross between previous two
  - Datagrams acknowledged
  - No prior logical setup

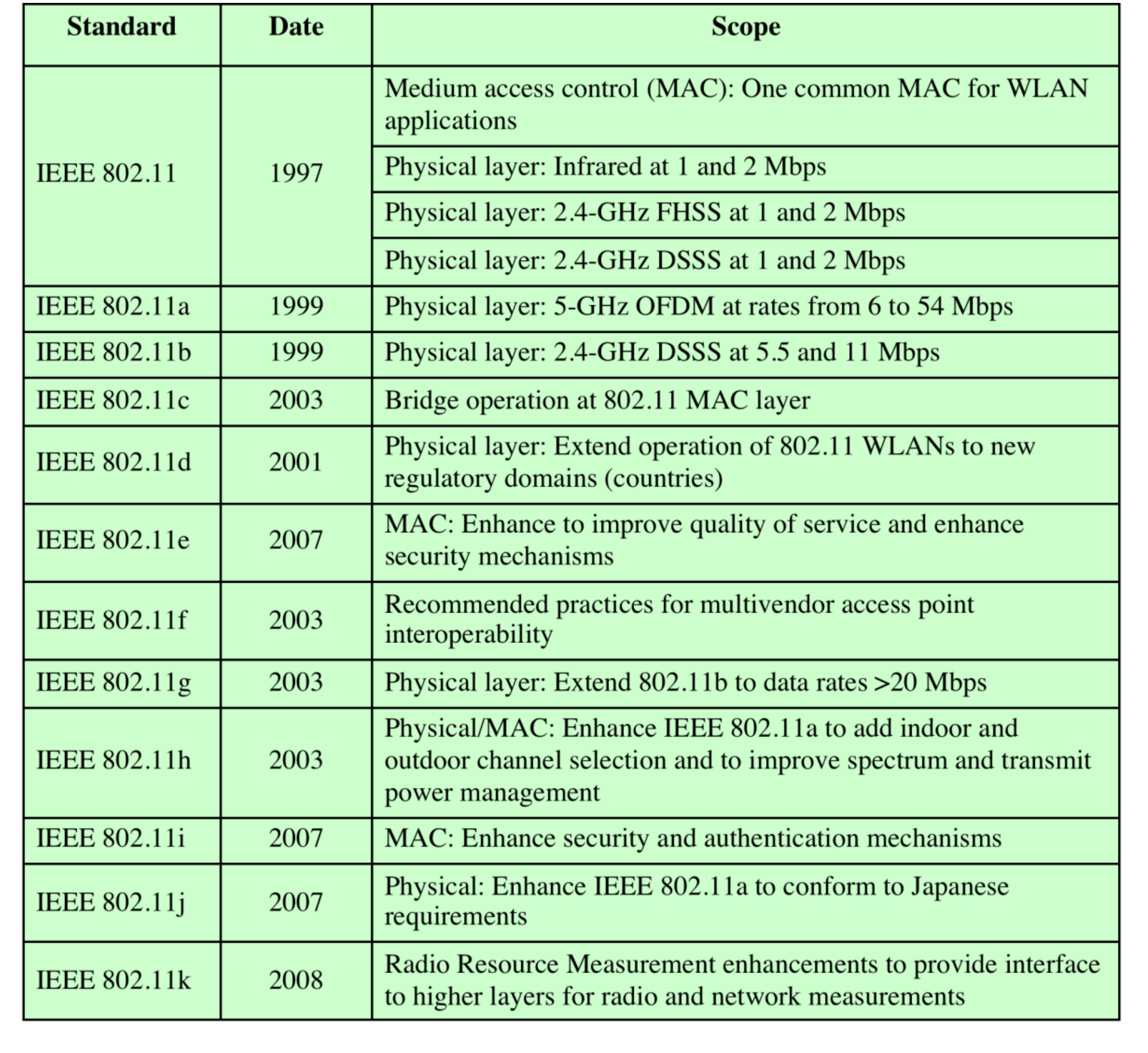
# DIFFERENCES BETWEEN LLC AND HDLC

- LLC uses asynchronous balanced mode of operation of HDLC (type 2 operation)
- LLC supports unacknowledged connectionless service (type 1 operation)
- LLC supports acknowledged connectionless service (type 3 operation)
- LLC permits multiplexing by the use of LLC service access points (LSAPs)

# IEEE 802.11

- Started in 1990
  - MAC and physical medium specifications
- Wi-Fi Alliance
  - Industry consortium
  - Creates test suites to certify interoperability of products
    - May identify a subset of the standard for certification
  - Concerned with a range of market areas for WLANs
- IEEE 802.11 has an ever expanding list of standards

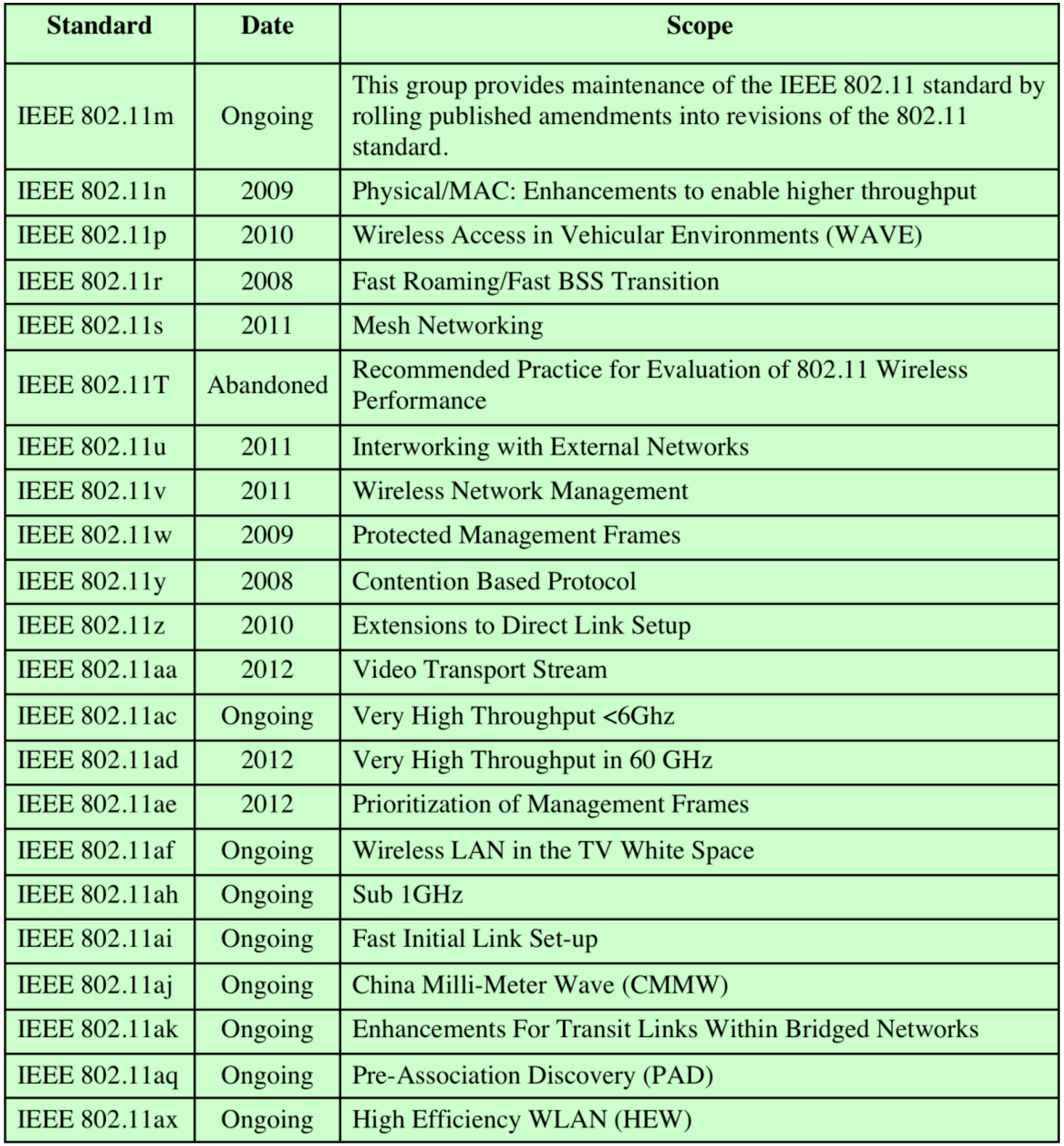
# IEEE 802.11 STANDARDS



| Standard | Date | Scope |
|---|---|---|
| IEEE 802.11 | 1997 | Medium access control (MAC): One common MAC for WLAN applications |
| | | Physical layer: Infrared at 1 and 2 Mbps |
| | | Physical layer: 2.4-GHz FHSS at 1 and 2 Mbps |
| | | Physical layer: 2.4-GHz DSSS at 1 and 2 Mbps |
| IEEE 802.11a | 1999 | Physical layer: 5-GHz OFDM at rates from 6 to 54 Mbps |
| IEEE 802.11b | 1999 | Physical layer: 2.4-GHz DSSS at 5.5 and 11 Mbps |
| IEEE 802.11c | 2003 | Bridge operation at 802.11 MAC layer |
| IEEE 802.11d | 2001 | Physical layer: Extend operation of 802.11 WLANs to new regulatory domains (countries) |
| IEEE 802.11e | 2007 | MAC: Enhance to improve quality of service and enhance security mechanisms |
| IEEE 802.11f | 2003 | Recommended practices for multivendor access point interoperability |
| IEEE 802.11g | 2003 | Physical layer: Extend 802.11b to data rates >20 Mbps |
| IEEE 802.11h | 2003 | Physical/MAC: Enhance IEEE 802.11a to add indoor and outdoor channel selection and to improve spectrum and transmit power management |
| IEEE 802.11i | 2007 | MAC: Enhance security and authentication mechanisms |
| IEEE 802.11j | 2007 | Physical: Enhance IEEE 802.11a to conform to Japanese requirements |
| IEEE 802.11k | 2008 | Radio Resource Measurement enhancements to provide interface to higher layers for radio and network measurements |

## TABLE 11.1 IEEE 802.11 STANDARDS

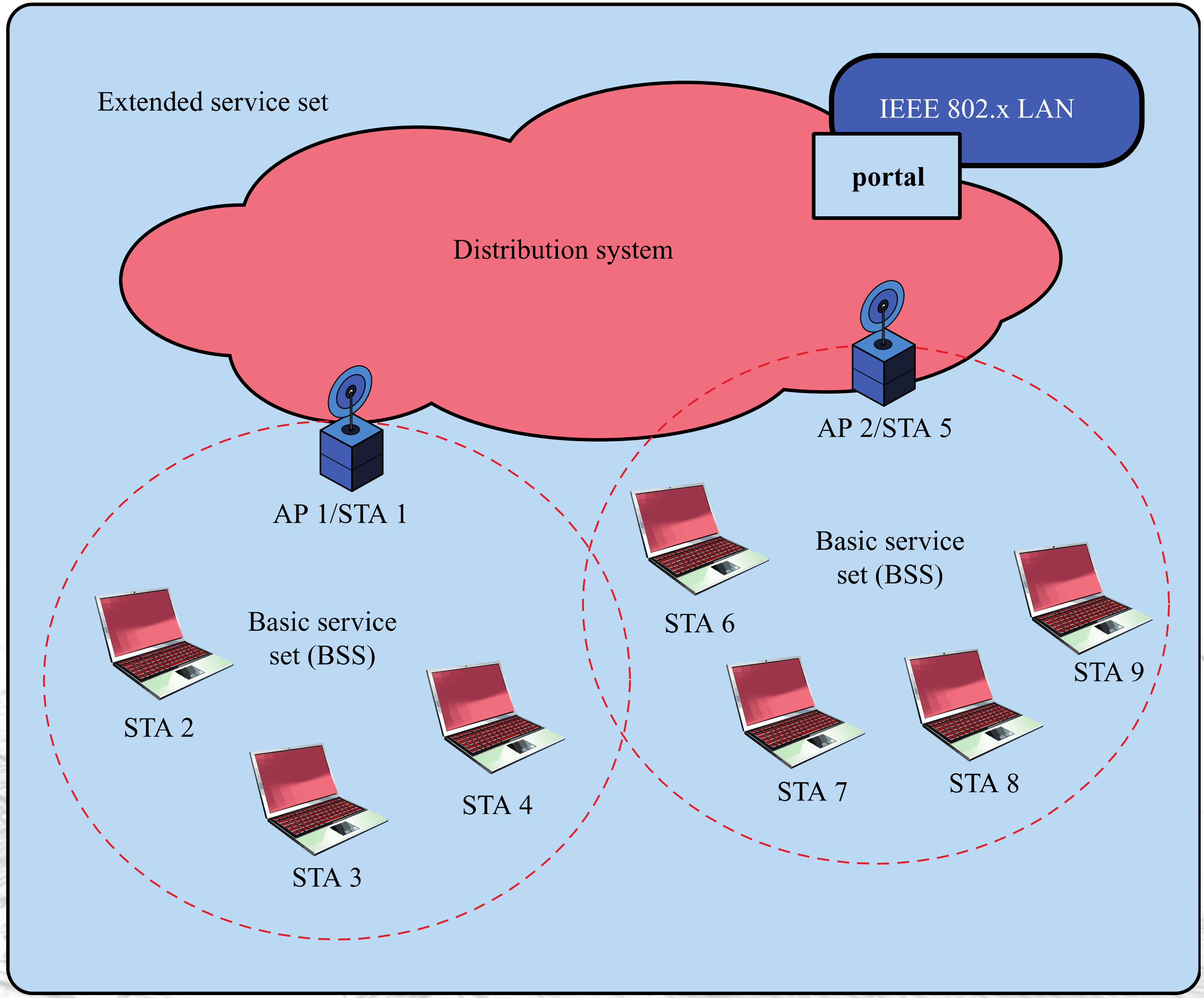
# IEEE 802.11 STANDARDS



| Standard | Date | Scope |
|---|---|---|
| IEEE 802.11m | Ongoing | This group provides maintenance of the IEEE 802.11 standard by rolling published amendments into revisions of the 802.11 standard. |
| IEEE 802.11n | 2009 | Physical/MAC: Enhancements to enable higher throughput |
| IEEE 802.11p | 2010 | Wireless Access in Vehicular Environments (WAVE) |
| IEEE 802.11r | 2008 | Fast Roaming/Fast BSS Transition |
| IEEE 802.11s | 2011 | Mesh Networking |
| IEEE 802.11T | Abandoned | Recommended Practice for Evaluation of 802.11 Wireless Performance |
| IEEE 802.11u | 2011 | Interworking with External Networks |
| IEEE 802.11v | 2011 | Wireless Network Management |
| IEEE 802.11w | 2009 | Protected Management Frames |
| IEEE 802.11y | 2008 | Contention Based Protocol |
| IEEE 802.11z | 2010 | Extensions to Direct Link Setup |
| IEEE 802.11aa | 2012 | Video Transport Stream |
| IEEE 802.11ac | Ongoing | Very High Throughput <6Ghz |
| IEEE 802.11ad | 2012 | Very High Throughput in 60 GHz |
| IEEE 802.11ae | 2012 | Prioritization of Management Frames |
| IEEE 802.11af | Ongoing | Wireless LAN in the TV White Space |
| IEEE 802.11ah | Ongoing | Sub 1GHz |
| IEEE 802.11ai | Ongoing | Fast Initial Link Set-up |
| IEEE 802.11aj | Ongoing | China Milli-Meter Wave (CMMW) |
| IEEE 802.11ak | Ongoing | Enhancements For Transit Links Within Bridged Networks |
| IEEE 802.11aq | Ongoing | Pre-Association Discovery (PAD) |
| IEEE 802.11ax | Ongoing | High Efficiency WLAN (HEW) |

# IEEE 802.11 ARCHITECTURE

- Distribution system (DS)
- Access point (AP)
- Basic service set (BSS)
  - Stations competing for access to shared wireless medium
  - Isolated or connected to backbone DS through AP
- Extended service set (ESS)
  - Two or more basic service sets interconnected by DS



## 11.8 IEEE 802.11 ARCHITECTURE

# DISTRIBUTION OF MESSAGES WITHIN A DS

- Distribution service
  - Used to exchange MAC frames from station in one BSS to station in another BSS
- Integration service
  - Transfer of data between station on IEEE 802.11 LAN and station on integrated IEEE 802.x LAN

# TRANSITION TYPES BASED ON MOBILITY

- No transition
  - Stationary or moves only within BSS
- BSS transition
  - Station moving from one BSS to another BSS in same ESS
- ESS transition
  - Station moving from BSS in one ESS to BSS within another ESS

# ASSOCIATION-RELATED SERVICES

- Association
  - Establishes initial association between station and AP
- Reassociation
  - Enables transfer of association from one AP to another, allowing station to move from one BSS to another
- Disassociation
  - Association termination notice from station or AP

# IEEE 802.11 MEDIUM ACCESS CONTROL

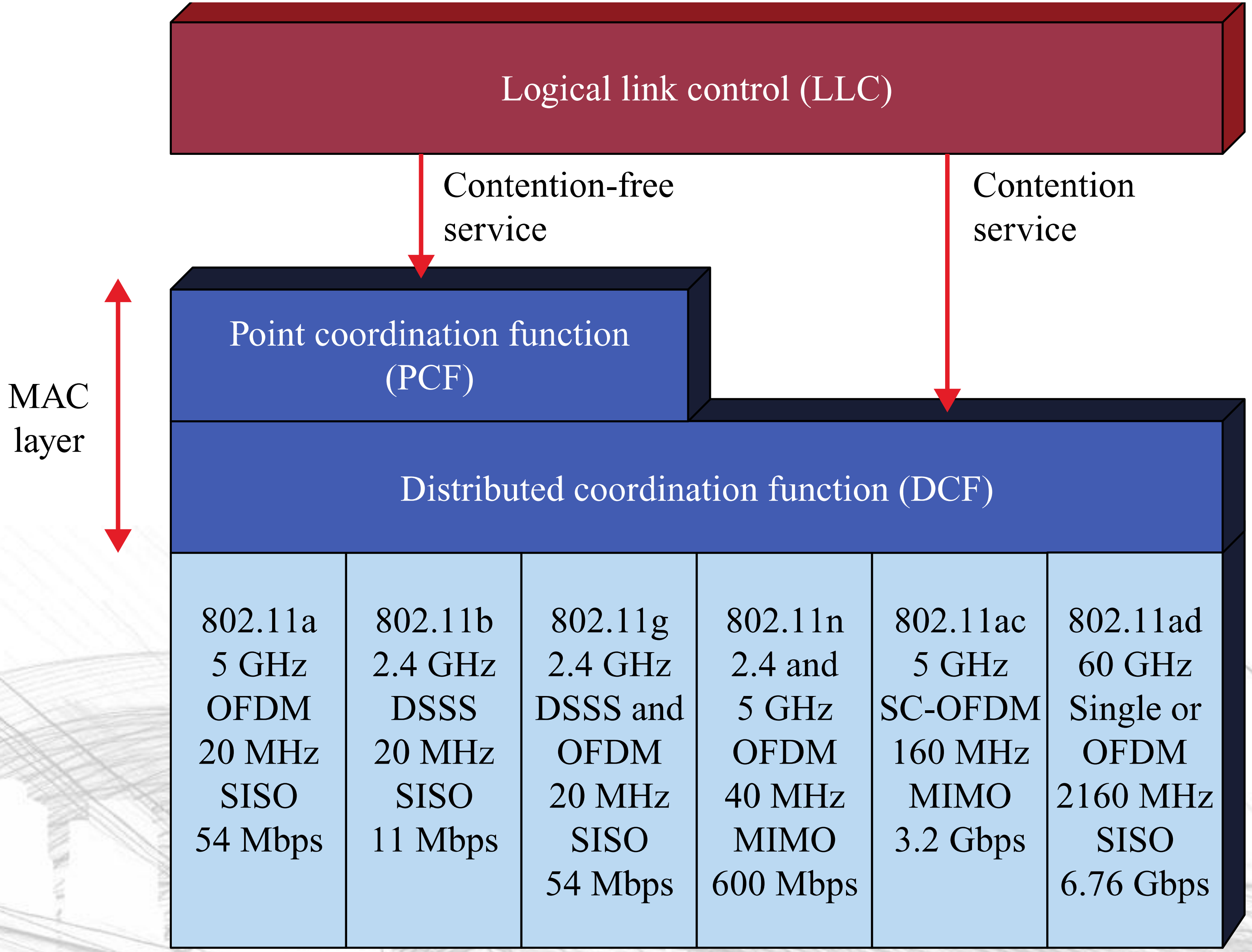
- MAC layer covers three functional areas:
  - – Reliable data delivery
  - – Access control
  - – Security

# RELIABLE DATA DELIVERY

- More efficient to deal with errors at the MAC level than higher layer (such as TCP)
- Frame exchange protocol
  - Source station transmits data
  - Destination responds with acknowledgment (ACK)
  - If source doesn‘t receive ACK, it retransmits frame
- Four frame exchange
  - Source issues request to send (RTS)
  - Destination responds with clear to send (CTS)
  - Source transmits data
  - Destination responds with ACK

# ACCESS CONTROL

- Centralized and decentralized mechanisms together
  - Distributed foundation wireless MAC (DFWMAC)
- Distributed coordination function (DCF)
  - Decentralized
- Point coordination function (PCF)
  - Centralized
- Both are available to the LLC layer



Logical link control (LLC)

Contention-free service

Contention service

MAC layer

Point coordination function (PCF)

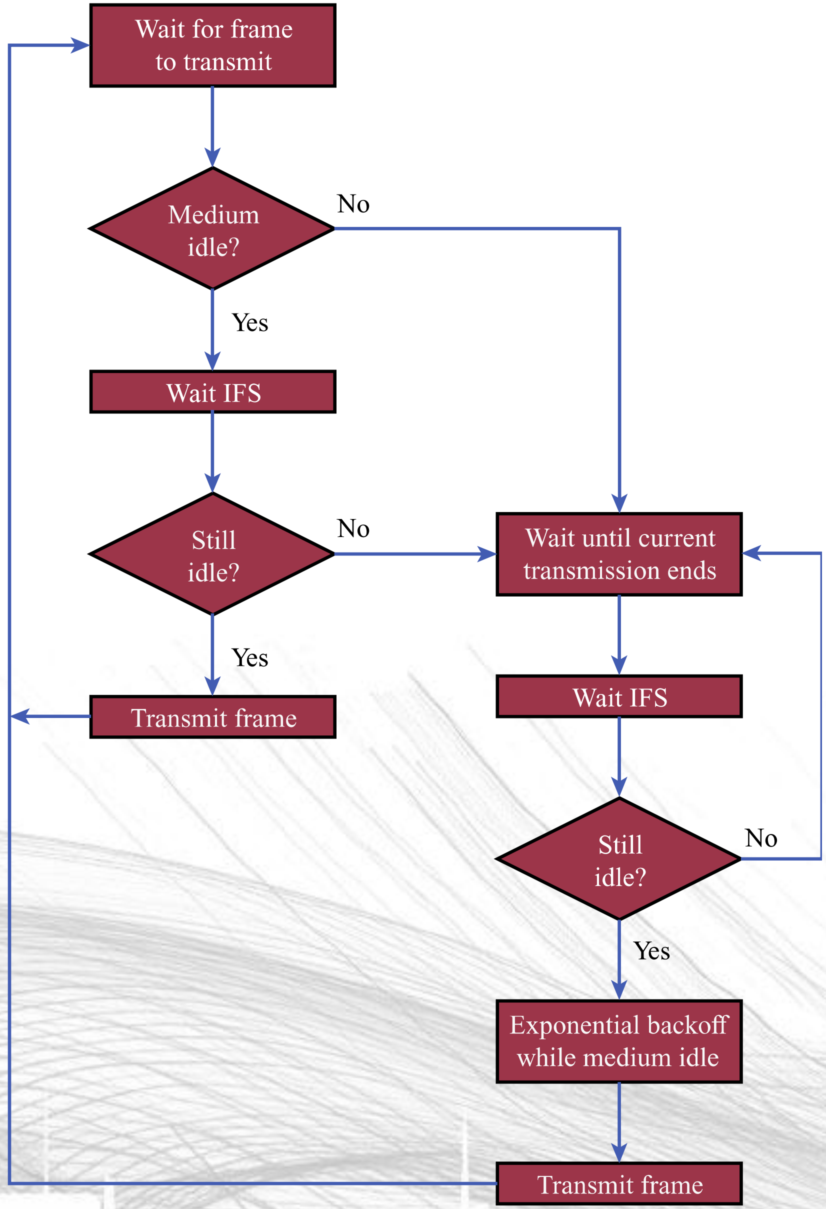
Distributed coordination function (DCF)

| 802.11a | 802.11b | 802.11g | 802.11n | 802.11ac | 802.11ad |
|---|---|---|---|---|---|
| 5 GHz | 2.4 GHz | 2.4 GHz | 2.4 and 5 GHz | 5 GHz | 60 GHz |
| OFDM | DSSS | DSSS and OFDM | OFDM | SC-OFDM | Single or OFDM |
| 20 MHz | 20 MHz | 20 MHz | 40 MHz | 160 MHz | 2160 MHz |
| SISO | SISO | SISO | MIMO | MIMO | SISO |
| 54 Mbps | 11 Mbps | 54 Mbps | 600 Mbps | 3.2 Gbps | 6.76 Gbps |

# 11.9 IEEE 802.11 PROTOCOL ARCHITECTURE

# DISTRIBUTED COORDINATION FUNCTION

- Decentralized
- Carrier sense multiple access (CSMA)
  - Listen to the medium
  - If idle, then transmit
  - If not, wait a random time
    - If busy again, expand the mean waiting time, randomly wait, and try again.
  - *Binary exponential backoff* describes this procedure
    - The backoff is the waiting process
    - Mean random waiting times get exponentially larger
      - By a factor of 2 each time, hence the term *binary*.
  - This process responds to heavy loads
    - Since nodes do not know the loads of other nodes trying to send.


Wait for frame to transmit
Medium idle?
No
Yes
Wait IFS
Still idle?
No
Yes
Transmit frame
Wait until current transmission ends
Wait IFS
Still idle?
No
Yes
Exponential backoff while medium idle
Transmit frame

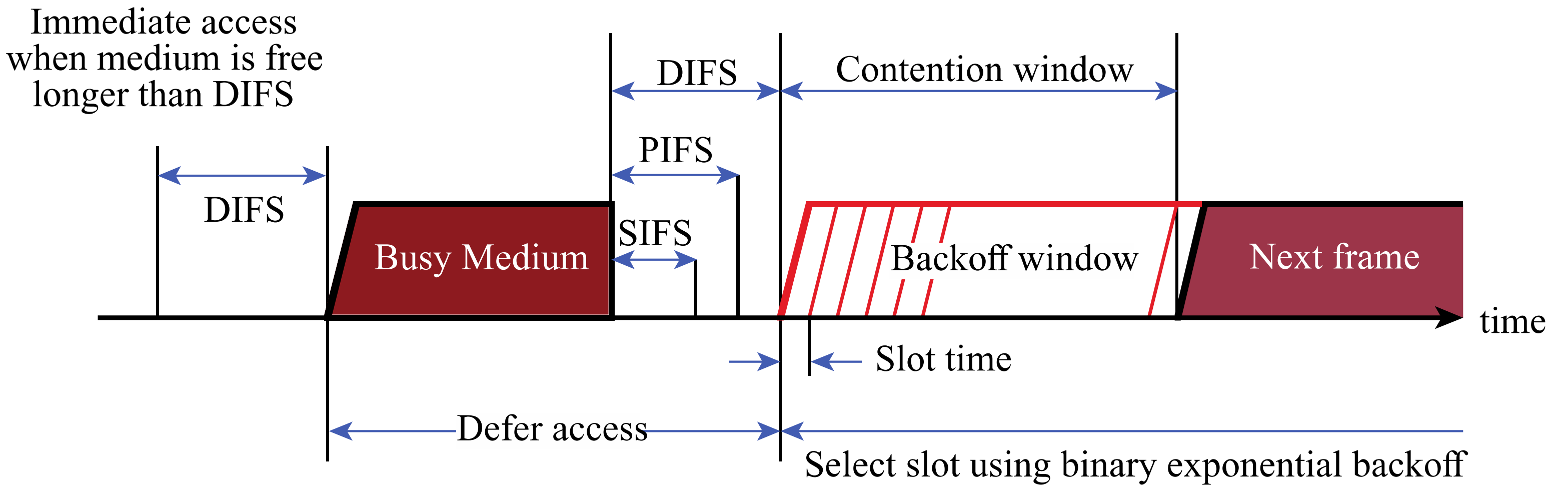
# 11.10 IEEE 802.11 MEDIUM ACCESS CONTROL LOGIC

# INTERFRAME SPACE (IFS) VALUES

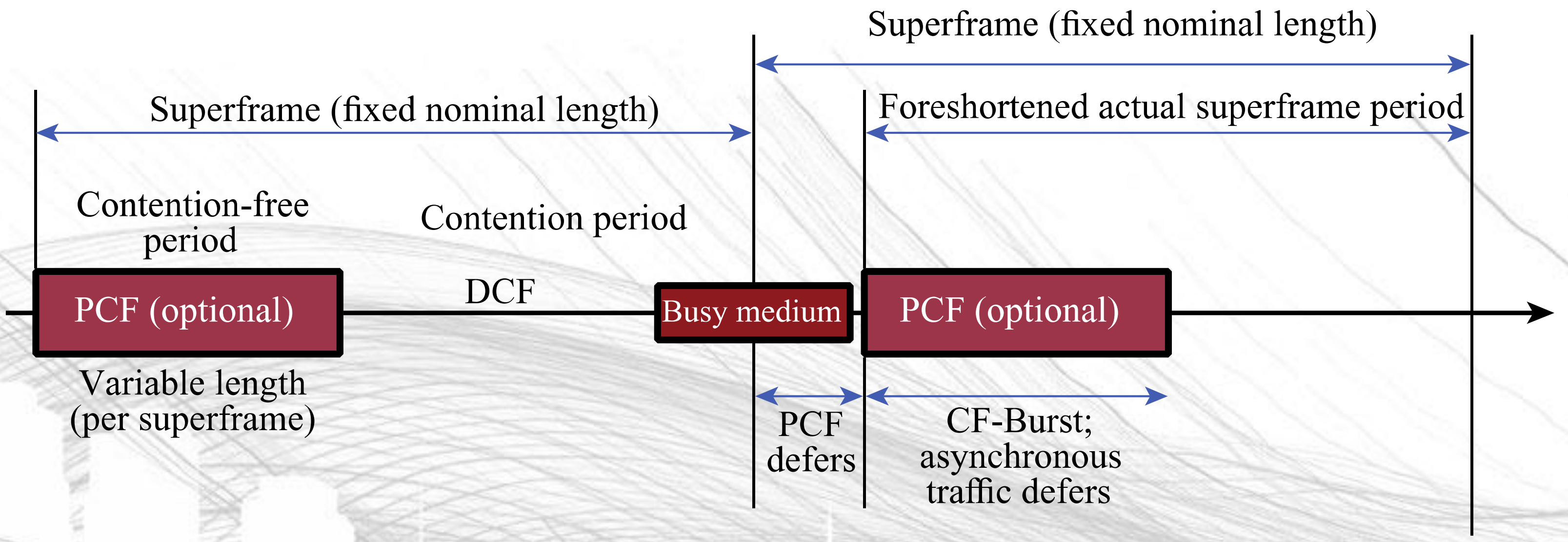
- Short IFS (SIFS)
  - Shortest IFS
  - Used for immediate response actions
- Point coordination function IFS (PIFS)
  - Midlength IFS
  - Used by centralized controller in PCF scheme when using polls
- Distributed coordination function IFS (DIFS)
  - Longest IFS
  - Used as minimum delay of asynchronous frames contending for access

# IFS USAGE

- SIFS
  - Acknowledgment (ACK)
  - Clear to send (CTS)
  - Poll response
- PIFS
  - Used by centralized controller in issuing polls
  - Takes precedence over normal contention traffic
- DIFS
  - Used for all ordinary asynchronous traffic


Immediate access when medium is free longer than DIFS
DIFS
Busy Medium
DIFS
PIFS
SIFS
Contention window
Backoff window
Next frame
time
Slot time
Defer access
Select slot using binary exponential backoff

**(a) Basic access method**

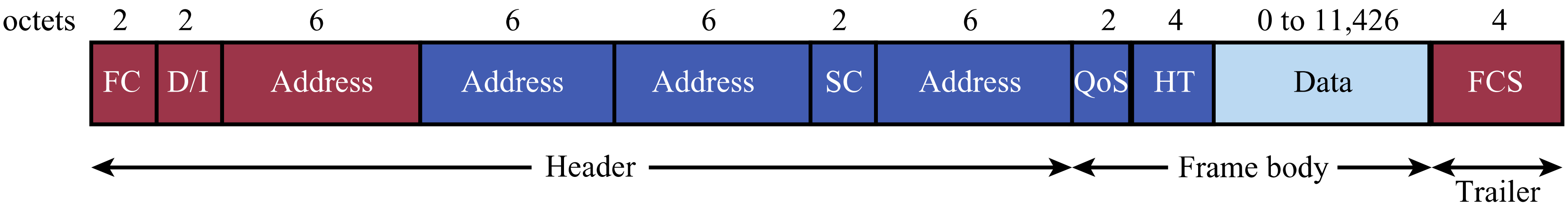

Superframe (fixed nominal length)
Superframe (fixed nominal length)
Foreshortened actual superframe period
Contention-free period
Contention period
PCF (optional)
DCF
Busy medium
PCF (optional)
Variable length (per superframe)
PCF defers
CF-Burst; asynchronous traffic defers

**(b) PCF superframe construction**

# 11.11 IEEE 802.11 MAC TIMING

# POINT COORDINATION FUNCTION

- Centralized control
- Point coordinator polls devices
  - To give them permission to send
  - On a schedule the point coordinator determines
- The *superframe* allows time to be shared between DCF and PCF
  - PCF starts the superframe and can only use a certain part of the superframe time



| octets | 2 | 2 | 6 | 6 | 6 | 2 | 6 | 2 | 4 | 0 to 11,426 | 4 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | FC | D/I | Address | Address | Address | SC | Address | QoS | HT | Data | FCS |

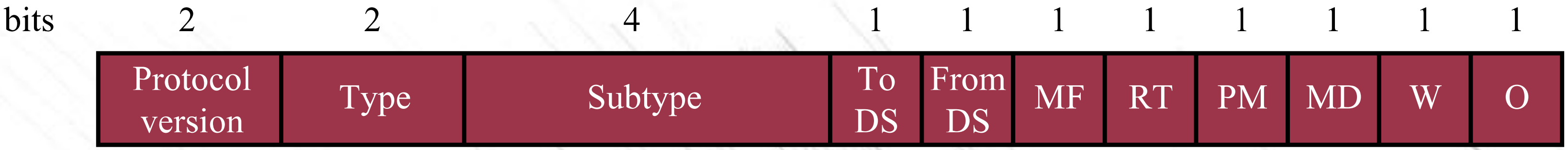
FC = frame control
D/I = duration/connection ID
QoS = QoS control

SC = sequence control
FCS = frame check sequence
HT = high throughput control

🟥 Always present

🟦 Present only in certain frame types and sub-types

**(a) MAC frame**



| bits | 2 | 2 | 4 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Protocol version | Type | Subtype | To DS | From DS | MF | RT | PM | MD | W | O |

DS = distribution system
MF = more fragments
RT = retry
PM = power management

MD = more data
W = wired equivalent privacy bit
O = order

**(b) Frame control field**

# 11.12 IEEE 802.11 MAC FRAME FORMAT

# MAC FRAME FIELDS

- Frame Control – frame type, control information
- Duration/connection ID – channel allocation time
- Addresses – context dependent, types include source and destination
- Sequence control – numbering and reassembly
- Frame body – MSDU or fragment of MSDU
- Frame check sequence – 32-bit CRC

# FRAME CONTROL FIELDS

- Protocol version – 802.11 version
- Type – control, management, or data
- Subtype – identifies function of frame
- To DS – 1 if destined for DS
- From DS – 1 if leaving DS
- More fragments – 1 if fragments follow
- Retry – 1 if retransmission of previous frame

# FRAME CONTROL FIELDS

- Power management – 1 if transmitting station is in sleep mode
- More data – Indicates that station has more data to send
- WEP – 1 if Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA) is implemented
- Order – 1 if any data frame is sent using the Strictly Ordered service

# CONTROL FRAME SUBTYPES

- Power save – poll (PS-Poll)
- Request to send (RTS)
- Clear to send (CTS)
- Acknowledgment
- Contention-free (CF)-end
- CF-end + CF-ack

# DATA FRAME SUBTYPES

- Data-carrying frames
  - Data
  - Data + CF-Ack
  - Data + CF-Poll
  - Data + CF-Ack + CF-Poll
- Other subtypes (don’t carry user data)
  - Null Function
  - CF-Ack
  - CF-Poll
  - CF-Ack + CF-Poll

# MANAGEMENT FRAME SUBTYPES

- Association request
- Association response
- Reassociation request
- Reassociation response
- Probe request
- Probe response
- Beacon

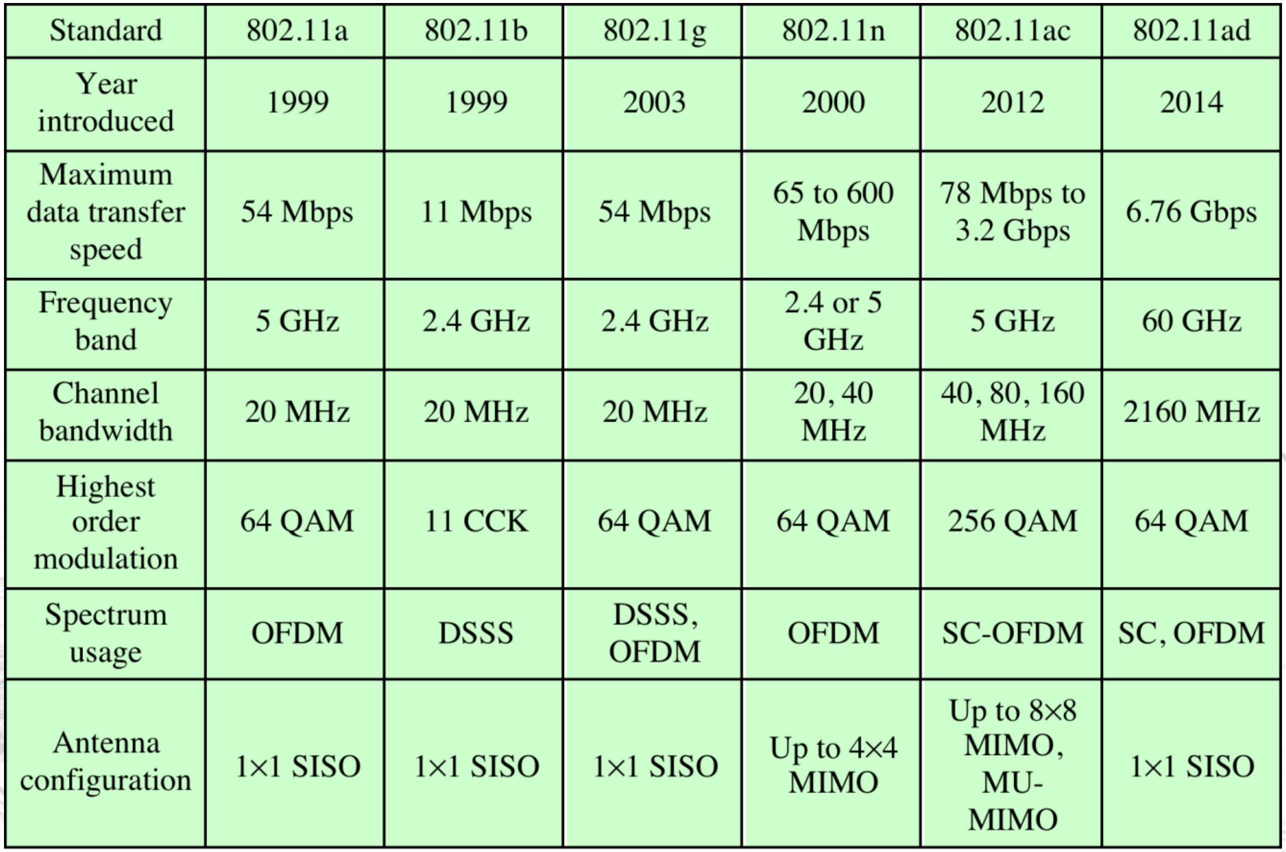
# MANAGEMENT FRAME SUBTYPES

- Announcement traffic indication message
- Dissociation
- Authentication
- Deauthentication

# AUTHENTICATION

- Open system authentication
  - Exchange of identities, no security benefits
- Shared Key authentication
  - Shared Key assures authentication

# IEEE 802.11 PHYSICAL LAYER

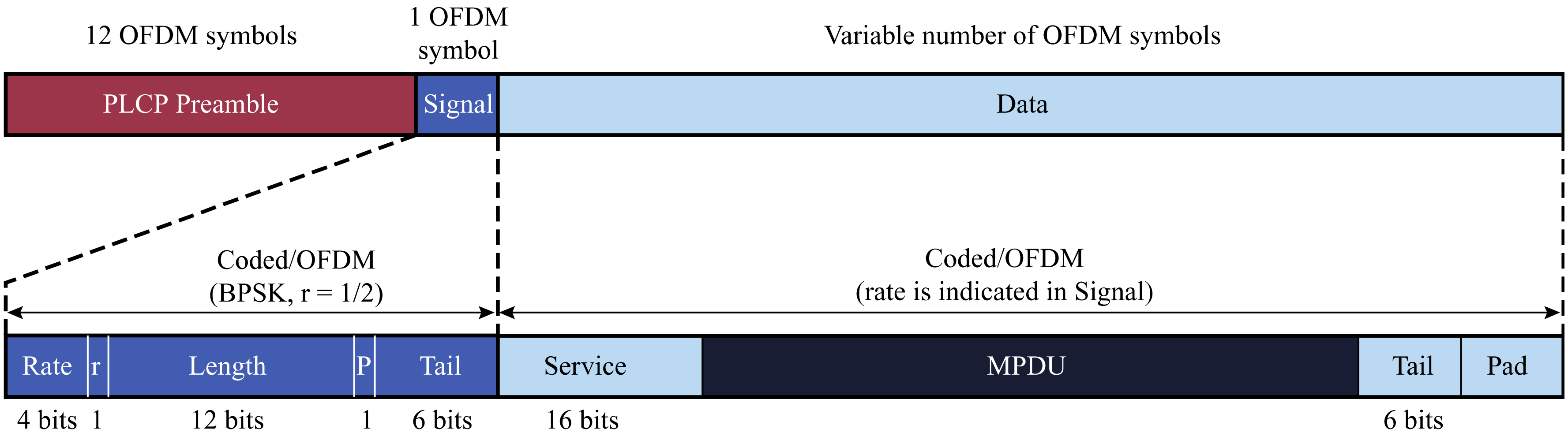


| Standard | 802.11a | 802.11b | 802.11g | 802.11n | 802.11ac | 802.11ad |
|---|---|---|---|---|---|---|
| Year introduced | 1999 | 1999 | 2003 | 2000 | 2012 | 2014 |
| Maximum data transfer speed | 54 Mbps | 11 Mbps | 54 Mbps | 65 to 600 Mbps | 78 Mbps to 3.2 Gbps | 6.76 Gbps |
| Frequency band | 5 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 | OFDM | DSSS | 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 11.5 IEEE 802.11 PHYSICAL LAYER STANDARDS

# IEEE 802.11a AND IEEE 802.11b

- IEEE 802.11b
  - DSSS
  - Provides data rates of 5.5 and 11 Mbps
  - Complementary code keying (CCK) and packet binary convolution coding (PBCC) modulation schemes
  - First standard to make Wi-Fi become popular
- IEEE 802.11a
  - Makes use of 5-GHz band
  - Provides rates of 6, 9 , 12, 18, 24, 36, 48, 54 Mbps
  - Uses orthogonal frequency division multiplexing (OFDM)
  - Subcarrier modulated using BPSK, QPSK, 16-QAM or 64-QAM
  - Never became popular, but its formats and channel schemes are used for later releases of 802.11



12 OFDM symbols

1 OFDM symbol

Variable number of OFDM symbols

PLCP Preamble

Signal

Data

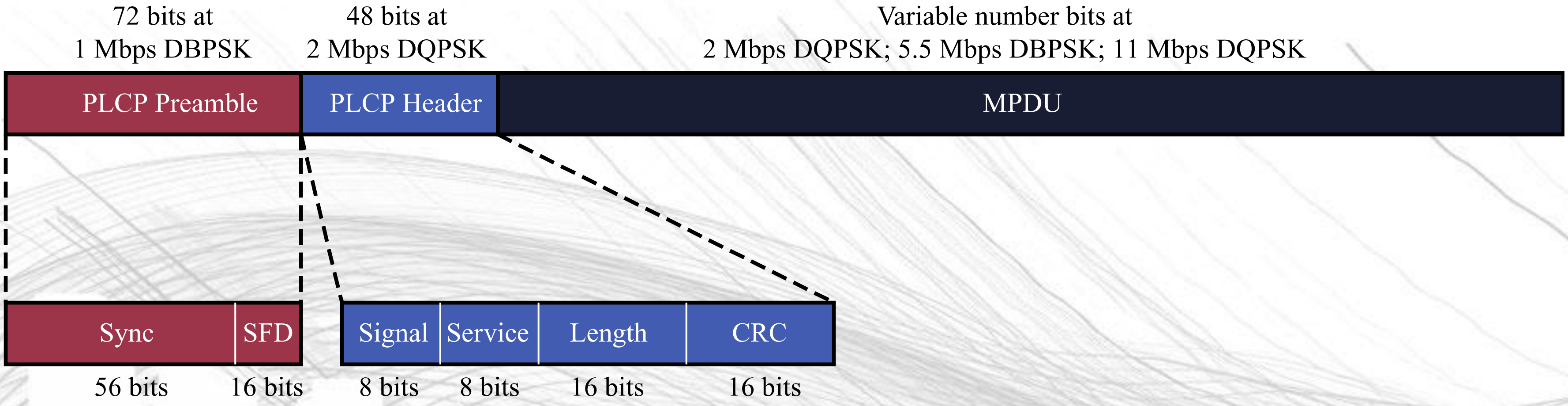
Coded/OFDM (BPSK, r = 1/2)

Coded/OFDM (rate is indicated in Signal)

Rate | r | Length | P | Tail | Service | MPDU | Tail | Pad

4 bits | 1 | 12 bits | 1 | 6 bits | 16 bits | | 6 bits |

**(a) IEEE 802.11a physical PDU**



72 bits at 1 Mbps DBPSK

48 bits at 2 Mbps DQPSK

Variable number bits at 2 Mbps DQPSK; 5.5 Mbps DBPSK; 11 Mbps DQPSK

PLCP Preamble

PLCP Header

MPDU

Sync | SFD

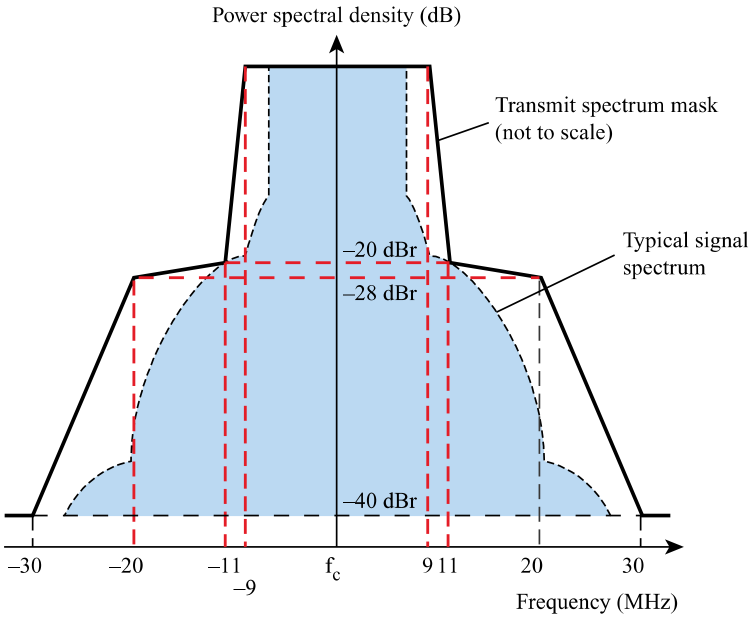
56 bits | 16 bits

Signal | Service | Length | CRC

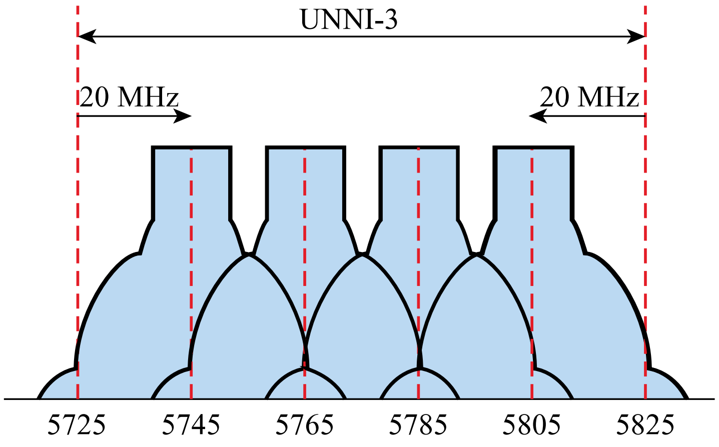
8 bits | 8 bits | 16 bits | 16 bits

**(b) IEEE 802.11b physical PDU**

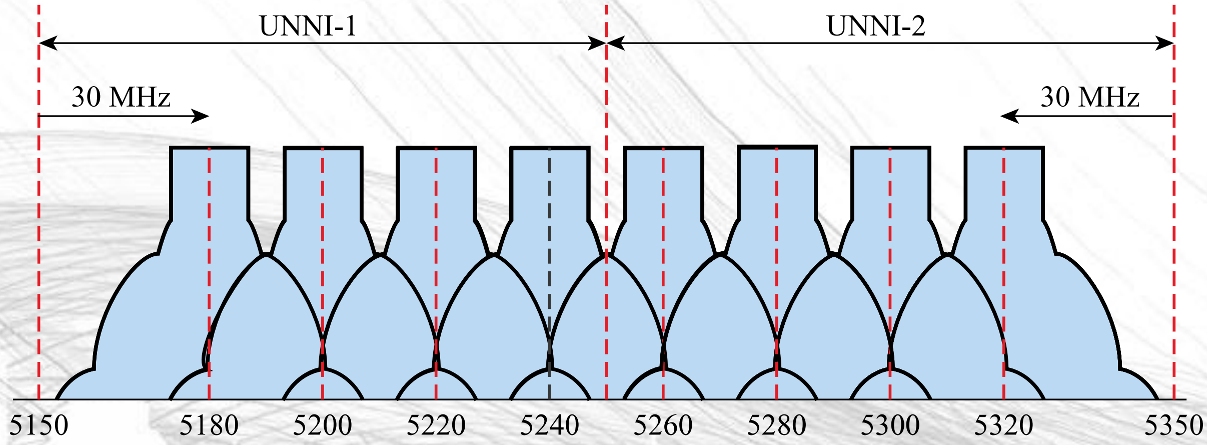
# 11.13 IEEE 802 PHYSICAL-LEVEL PROTOCOL DATA UNITS



**(a) Transmit spectrum mask**



**(b) Upper U-NII bands: 4 carriers in 100 MHz with 20 MHz spacing**



**(c) Lower and Middle U-NII bands: 8 carriers in 200 MHz with 20 MHz spacing**

# 11.14 IEEE 802.11a CHANNEL SCHEME

# IEEE 802.11g

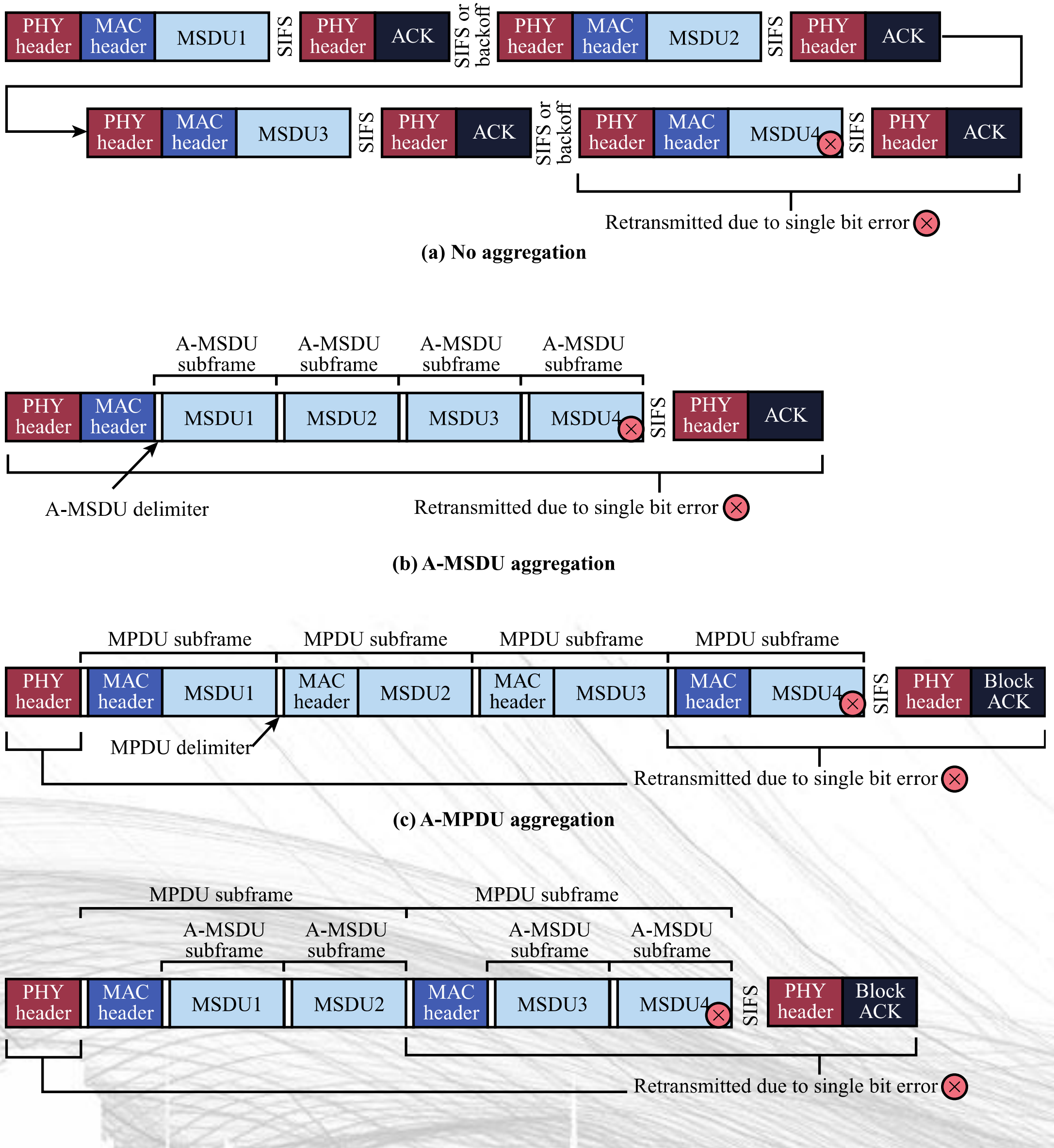
- Extended rates up to 54 Mbps in 2.4-GHz band
- Continued and extended PBCC from 802.11b that used DSSS
  - Rates up to 33 Mbps
- Also used OFDM for rates up to 54 Mbps

# IEEE 802.11n

- Operates in both 2.4-GHz and 5-GHz bands
- MIMO
  - Multiple parallel streams (up to 4 × 4), beamforming, or diversity
- Radio transmission schemes
  - Channel bonding to combine two 20 MHz channels
    - From 48 subcarriers per 20 MHz to 108 carriers per 40 MHz (2.25 times increase in available bandwidth)
    - Can only use 20 MHz channels if other nodes are active
  - Shorter 400 ns guard band (11% increase in data rate)
  - Higher coding rate of 5/6 (11% increase)
  - 150 Mbps per 40 MHz, 600 Mbps for 4 parallel streams

# IEEE 802.11n

- MAC enhancements
  - Reduce header bits, backoffs, and IFS times
  - Block acknowledgements
    - One ACK to cover multiple packets
  - Frame aggregation
    - Three forms
    - MSDUs come down from the LLC layer, MPDUs come from the MAC layer
    - A-MSDU aggregation – shared PHY and MAC headers and FCS
    - A-MPDU aggregation – shared PHY header
      - Still keep separate MAC headers, to less header reduction
      - But not as much to retransmit if there is an error
    - A-MPDU and A-MSDU aggregation – balances the two



**(a) No aggregation**

**(b) A-MSDU aggregation**

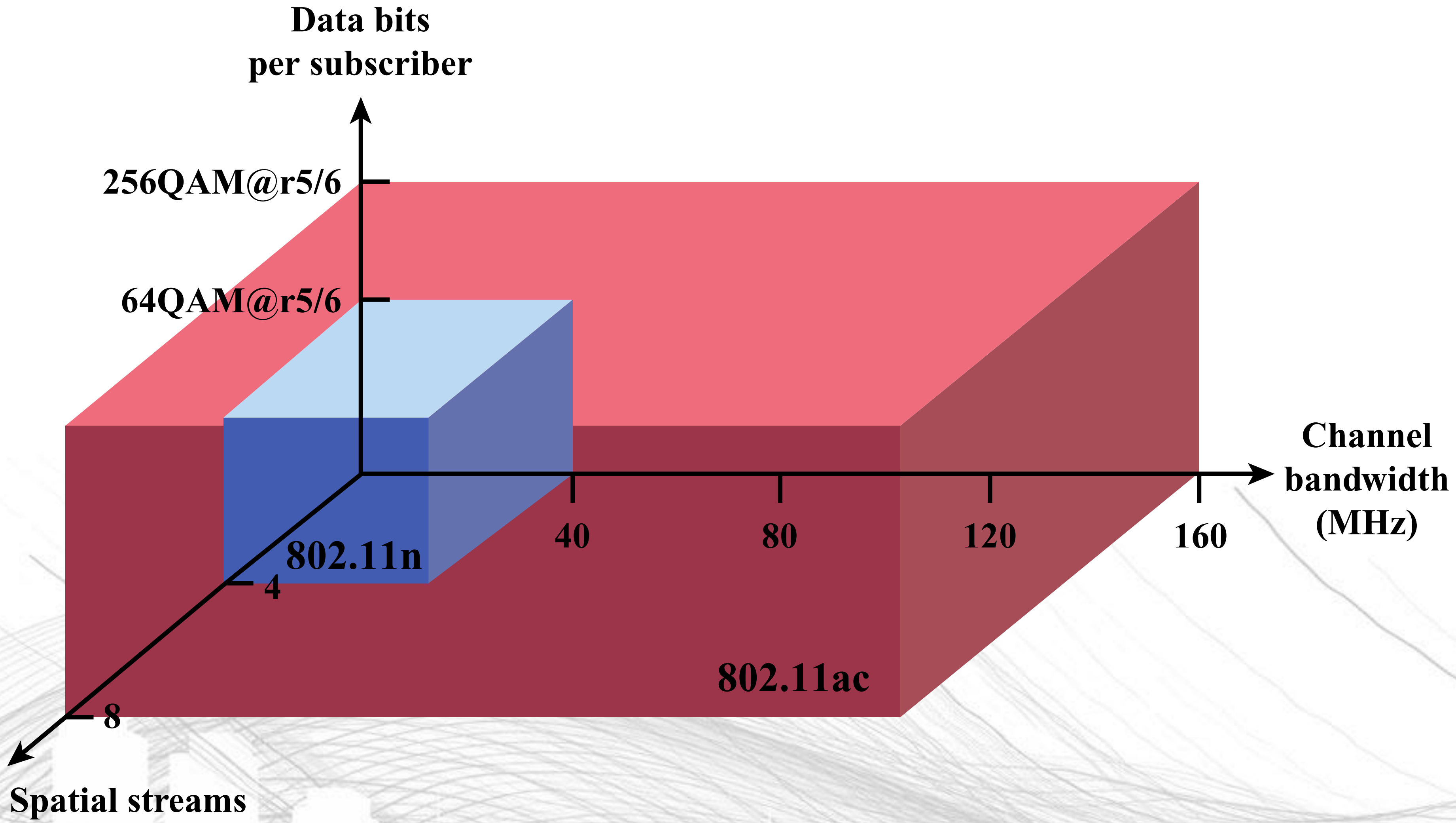
**(c) A-MPDU aggregation**

**(d) A-MPDU of A-MSDU aggregation**

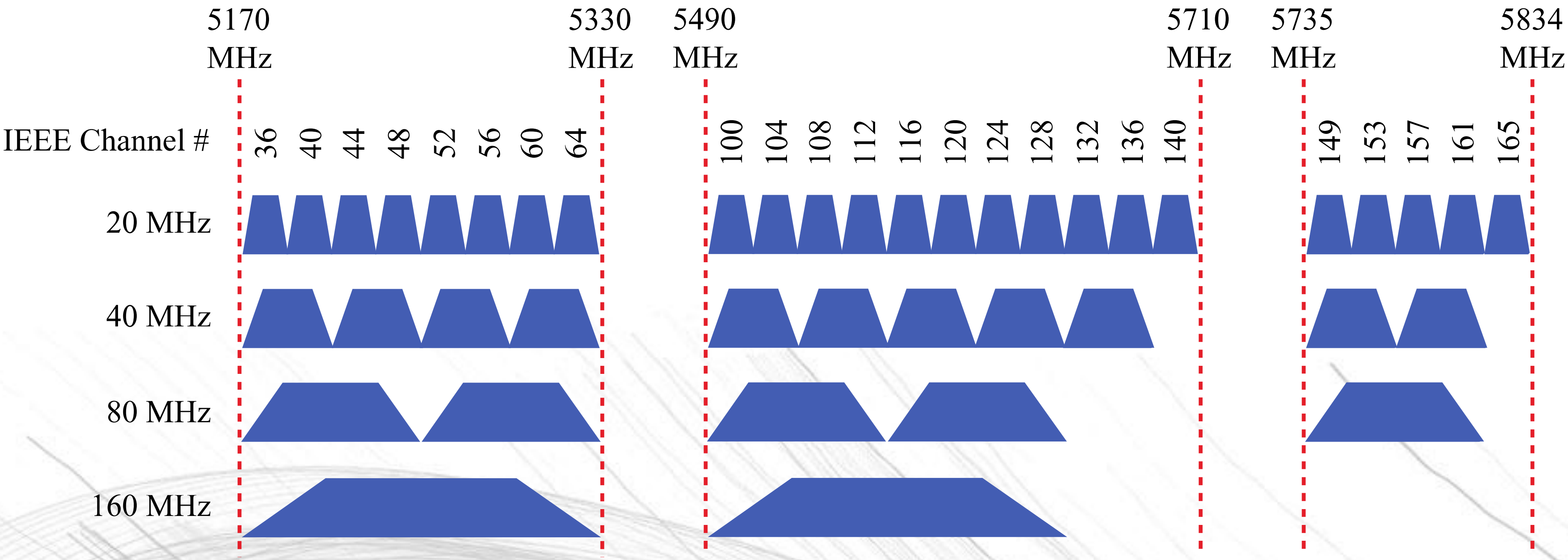
# 11.16 FORMS OF AGGREGATION

# GIGABIT WI-FI

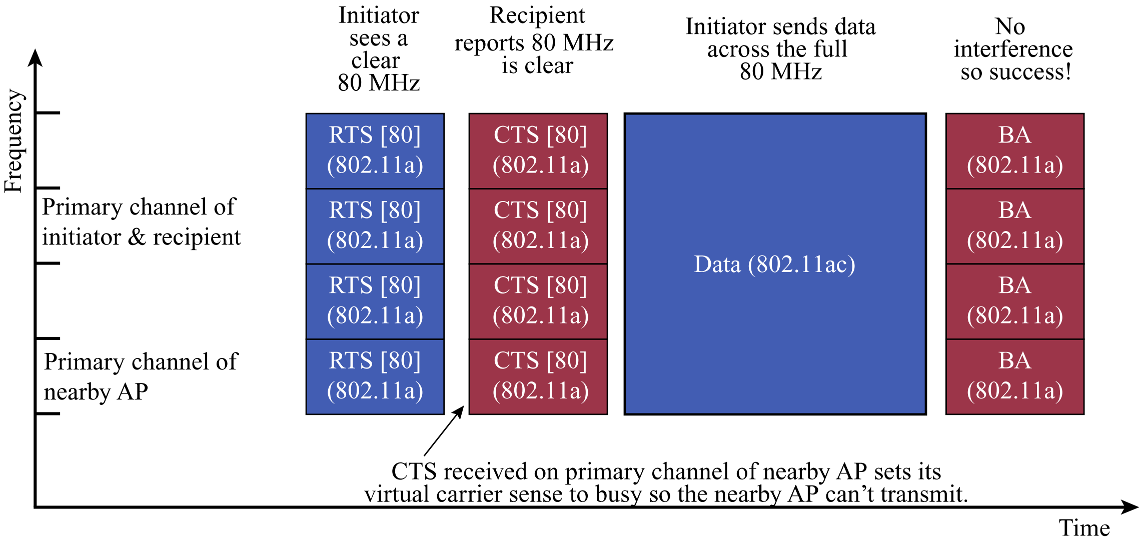
- 802.11ac
  - Up to 6.937 Gbps
  - 5-GHz only operation
  - Up to 8 × 8 MIMO
  - Up to 160 MHz (8 × 20 MHz channels)
    - Special RTS/CTS to check for legacy devices
  - Up to 256 QAM
  - Multiuser MIMO
    - Simultaneous beams to multiple stations
    - Advanced channel measurements
  - Larger frame size
  - A-MDPU is required
  - “Wave 1” products up to 1.3 Gbps
  - “Wave 2” products use 160 MHz channels and four spatial streams



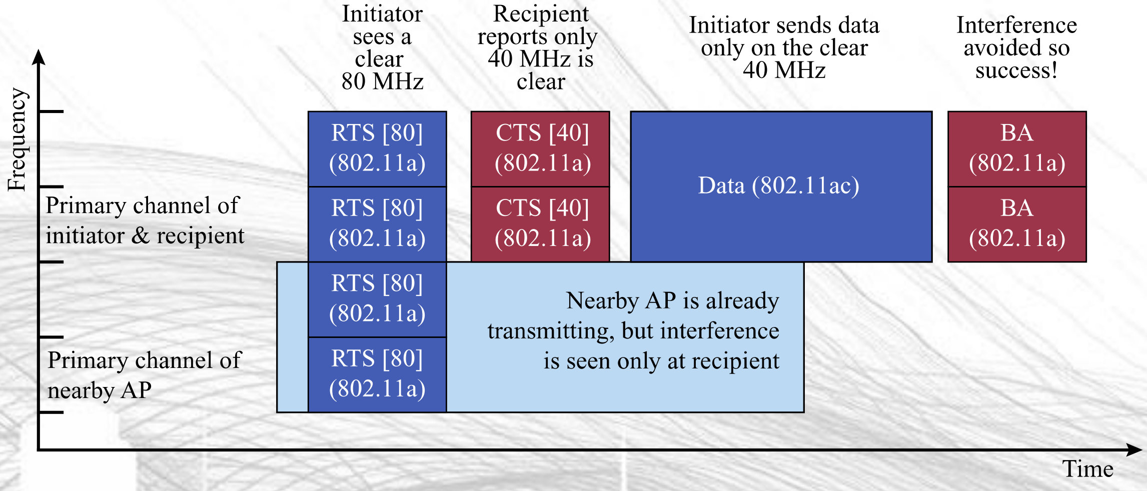
## 11.17 IEEE 802.11 PERFORMANCE FACTORS



# 11.18 5 GHz 802.11ac CHANNEL ALLOCATIONS


Initiator sees a clear 80 MHz
Recipient reports 80 MHz is clear
Initiator sends data across the full 80 MHz
No interference so success!
Frequency
Primary channel of initiator & recipient
Primary channel of nearby AP
RTS [80] (802.11a)
RTS [80] (802.11a)
RTS [80] (802.11a)
RTS [80] (802.11a)
CTS [80] (802.11a)
CTS [80] (802.11a)
CTS [80] (802.11a)
CTS [80] (802.11a)
Data (802.11ac)
BA (802.11a)
BA (802.11a)
BA (802.11a)
BA (802.11a)
CTS received on primary channel of nearby AP sets its virtual carrier sense to busy so the nearby AP can't transmit.
Time

**(a) No interference case**


Initiator sees a clear 80 MHz
Recipient reports only 40 MHz is clear
Initiator sends data only on the clear 40 MHz
Interference avoided so success!
Frequency
Primary channel of initiator & recipient
Primary channel of nearby AP
RTS [80] (802.11a)
RTS [80] (802.11a)
RTS [80] (802.11a)
RTS [80] (802.11a)
CTS [40] (802.11a)
CTS [40] (802.11a)
Data (802.11ac)
BA (802.11a)
BA (802.11a)
Nearby AP is already transmitting, but interference is seen only at recipient
Time

**(b) Interference case**

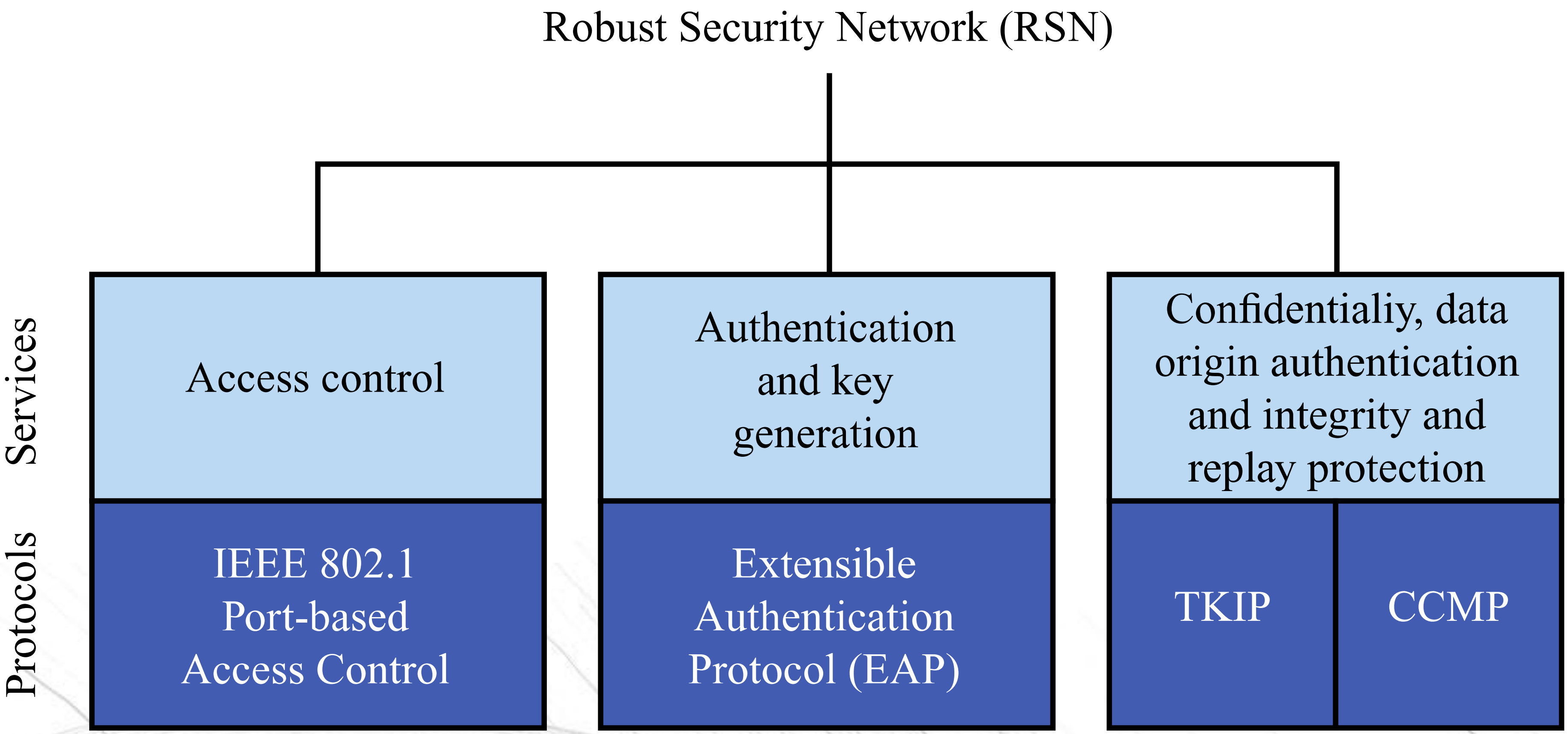
# 11.19 RTS/CTS ENHANCED WITH BANDWIDTH SIGNALING

# GIGABIT WI-FI

- 802.11ad
  - WiGig
  - Up to 7 Gbps
    - Replacement of wires for video to TVs and projectors
  - Uses 60-GHz bands
    - Called millimeter waves (mmWave)
    - Fewer devices operate in these bands
    - Higher free space loss
    - Poor penetration of objects
    - Likely only useful in a single room
  - Adaptive beamforming and high gain directional antennas
    - Can even find reflections when direct path is obstructed
  - Four modulation and coding schemes
  - Personal BSS so devices can talk directly

# WLAN SECURITY

- Three points of attack
  - Client
  - Access Point
  - Wireless medium
- Original Wired Equivalent Privacy (WEP) was much too weak
  - 802.11i provided stronger Wi-Fi Protected Access (WPA)
  - Robust Security Network (RSN) is the final 802.11i standard
- 802.11i services
  - Authentication through an authentication server
  - Access control
  - Encryption for privacy with message integrity



Robust Security Network (RSN)

Services

Protocols

Access control

Authentication and key generation

Confidentialiy, data origin authentication and integrity and replay protection

IEEE 802.1 Port-based Access Control

Extensible Authentication Protocol (EAP)

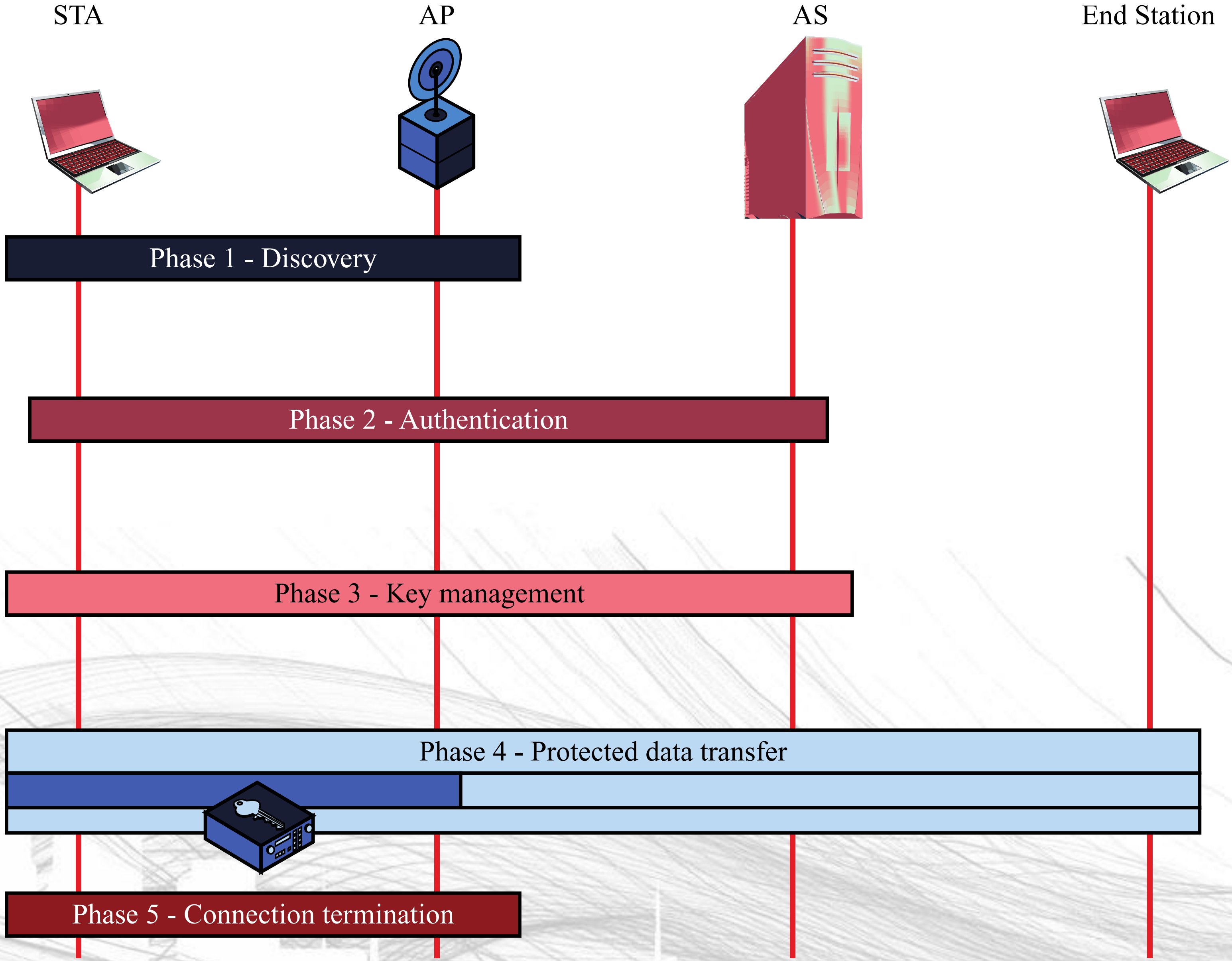
TKIP

CCMP

Services and Protocols

| | | |
|---|---|---|
| CCMP | = | Counter Mode with Cipher Block Chaining MAC Protocol |
| TKIP | = | Temporal Key Integrity Protocol |

## 11.20 ELEMENTS OF IEEE 802.11i



# 11.21 IEEE 802.11i PHASES OF OPERATION