EEEN3008J: Advance wireless communications

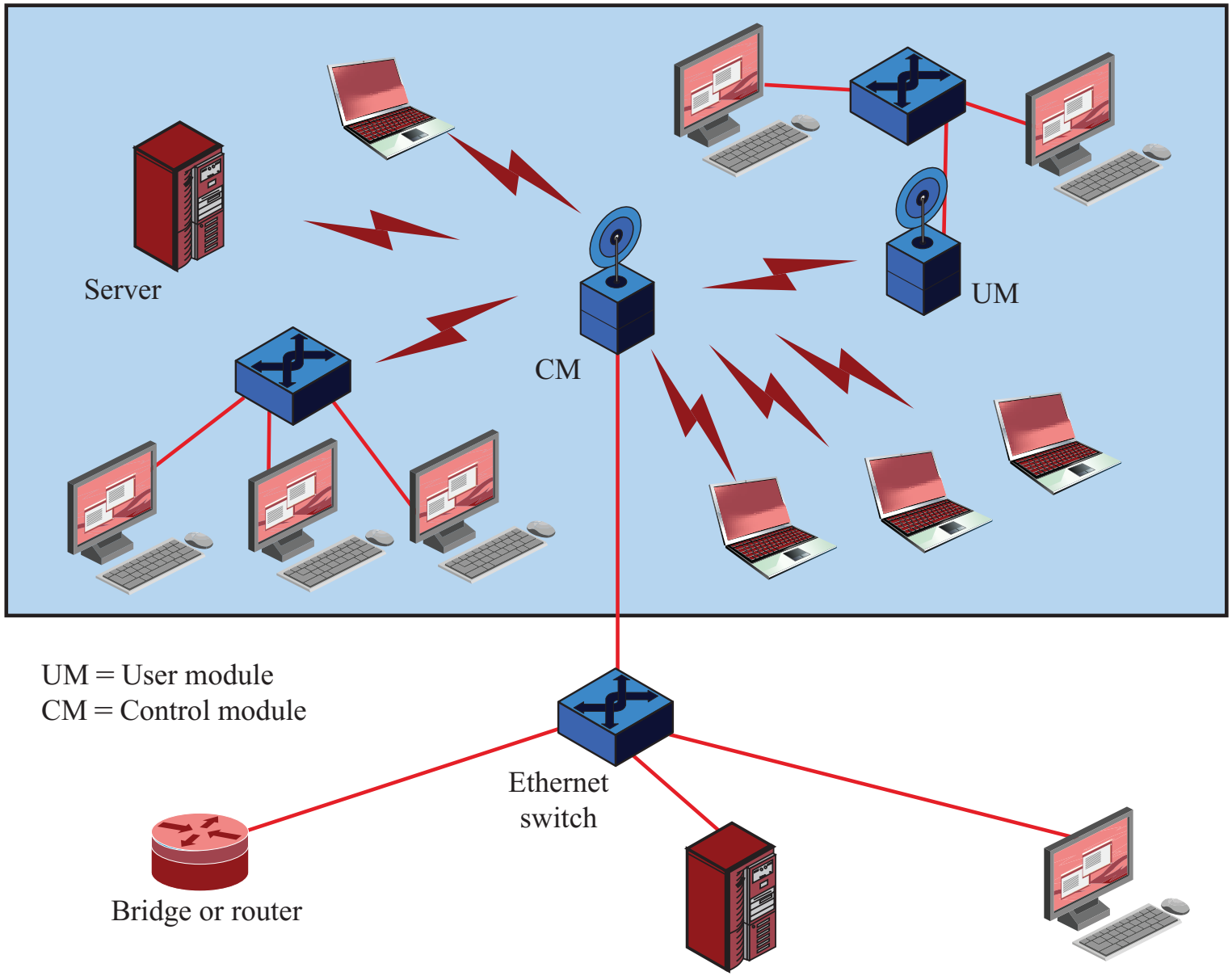
Wireless LAN Technology and the IEEE 802.11 Wireless LAN Standard

Dr Avishek Nag

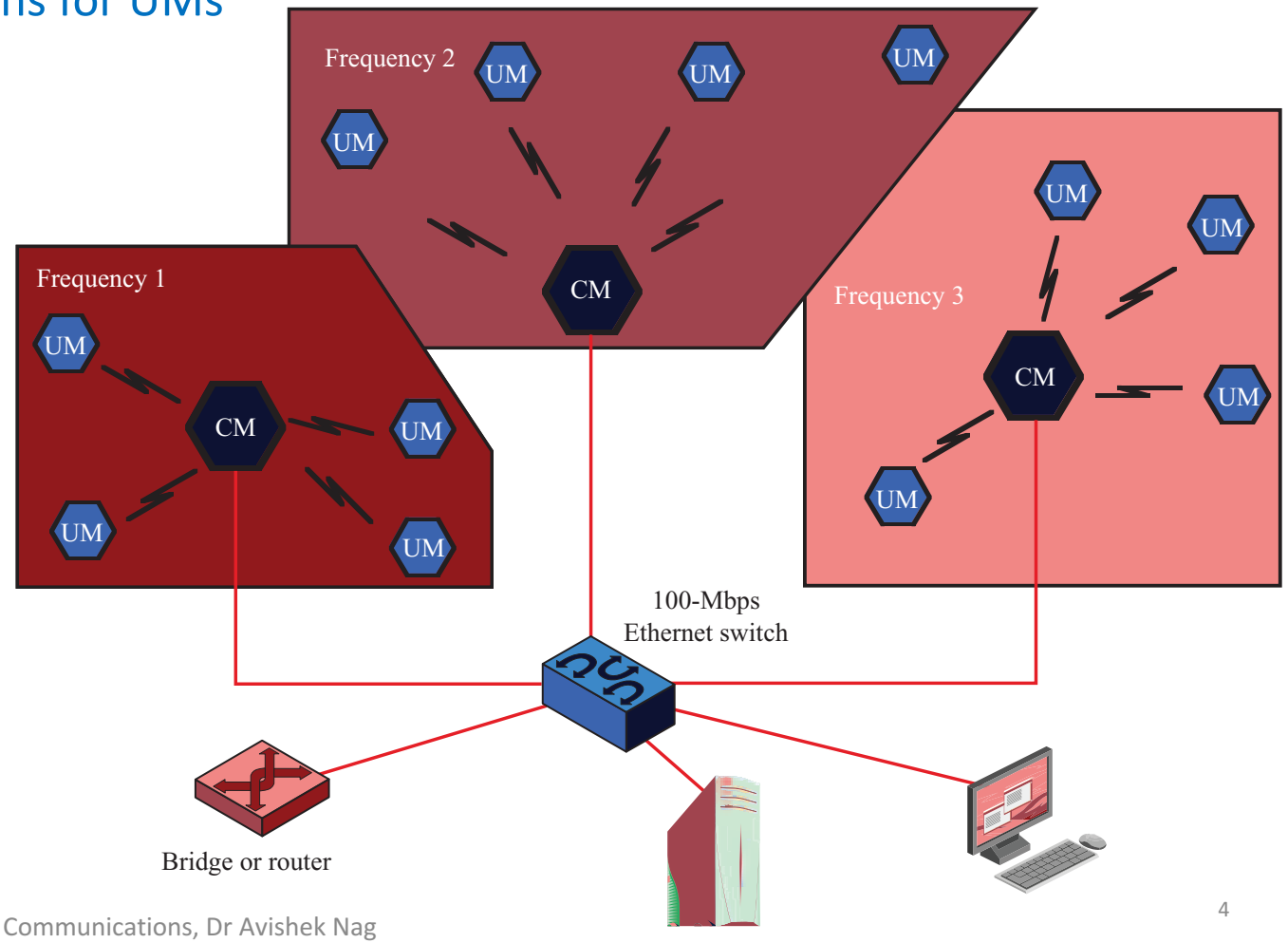
(avishek.nag@ucd.ie)

Introduction

- Wireless LANs (WLANs)
  - Indispensable 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

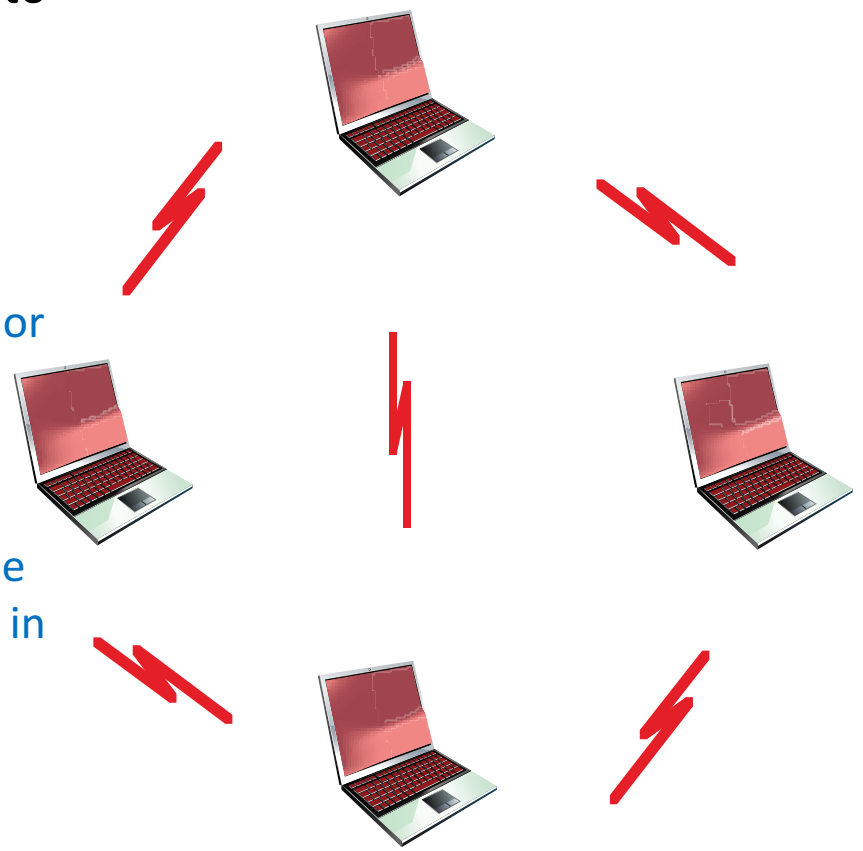

Server
CM
UM
UM = User module
CM = Control module
Ethernet
switch
Bridge or router

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



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



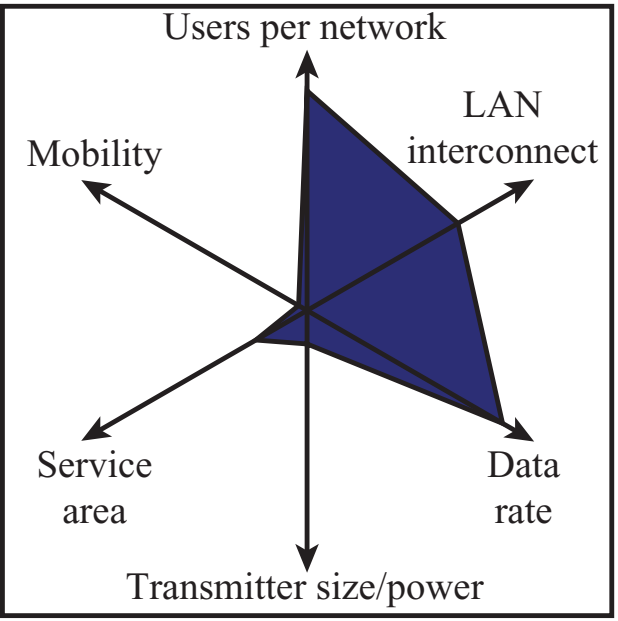
Wireless LAN motivations

- 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

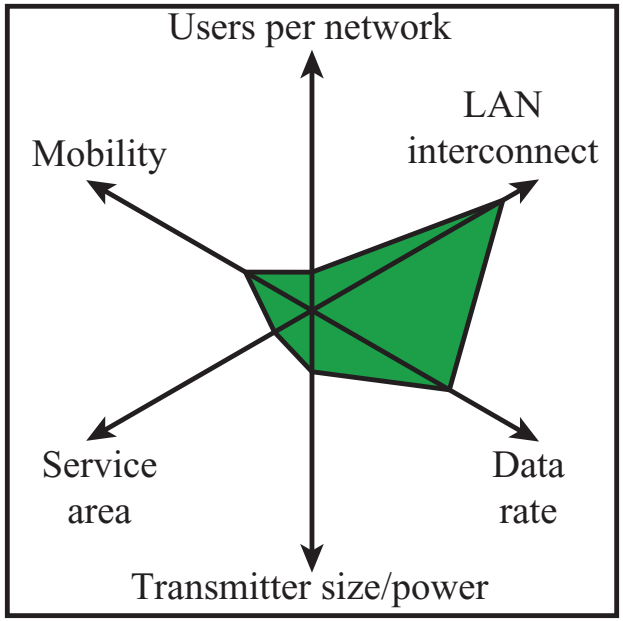
Wireless LAN Requirements

- 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

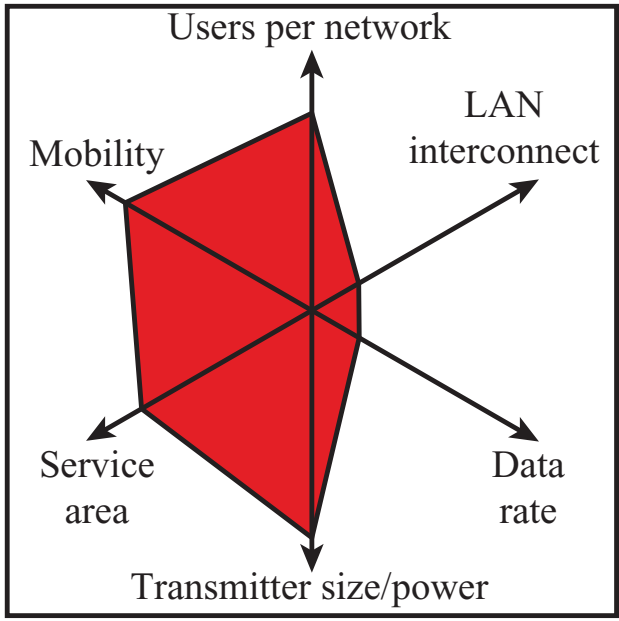
- Comparisons between WLANs, wired LANs, and mobile data networks can be visualized with Kiviat graphs.



(a) Wired LANs



(b) Wireless LANs



(c) Mobile data networks

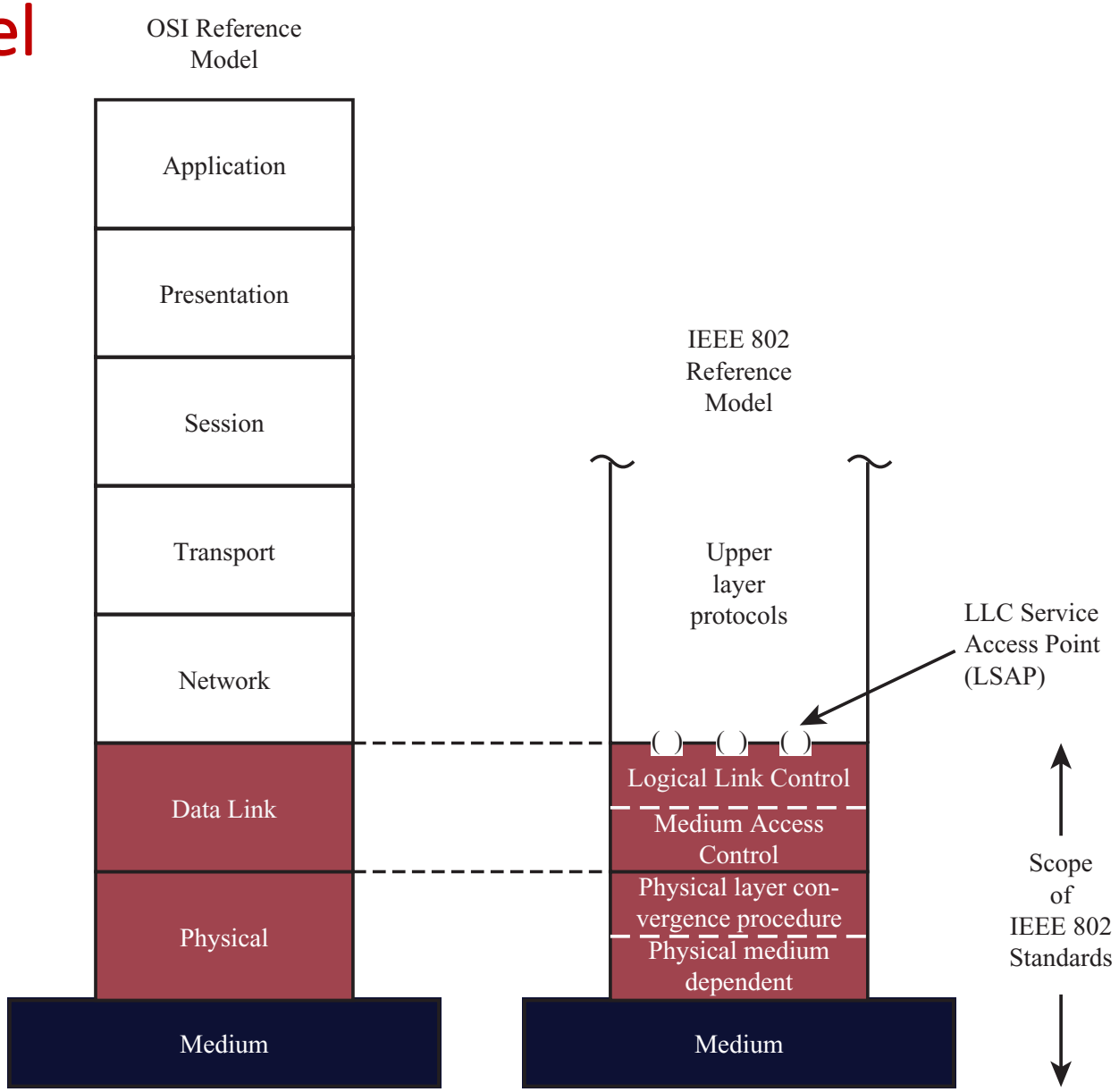
Wireless LAN physical layer

- 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
  - Next Figure relates OSI with 802.11
  - Called the IEEE 802 reference model

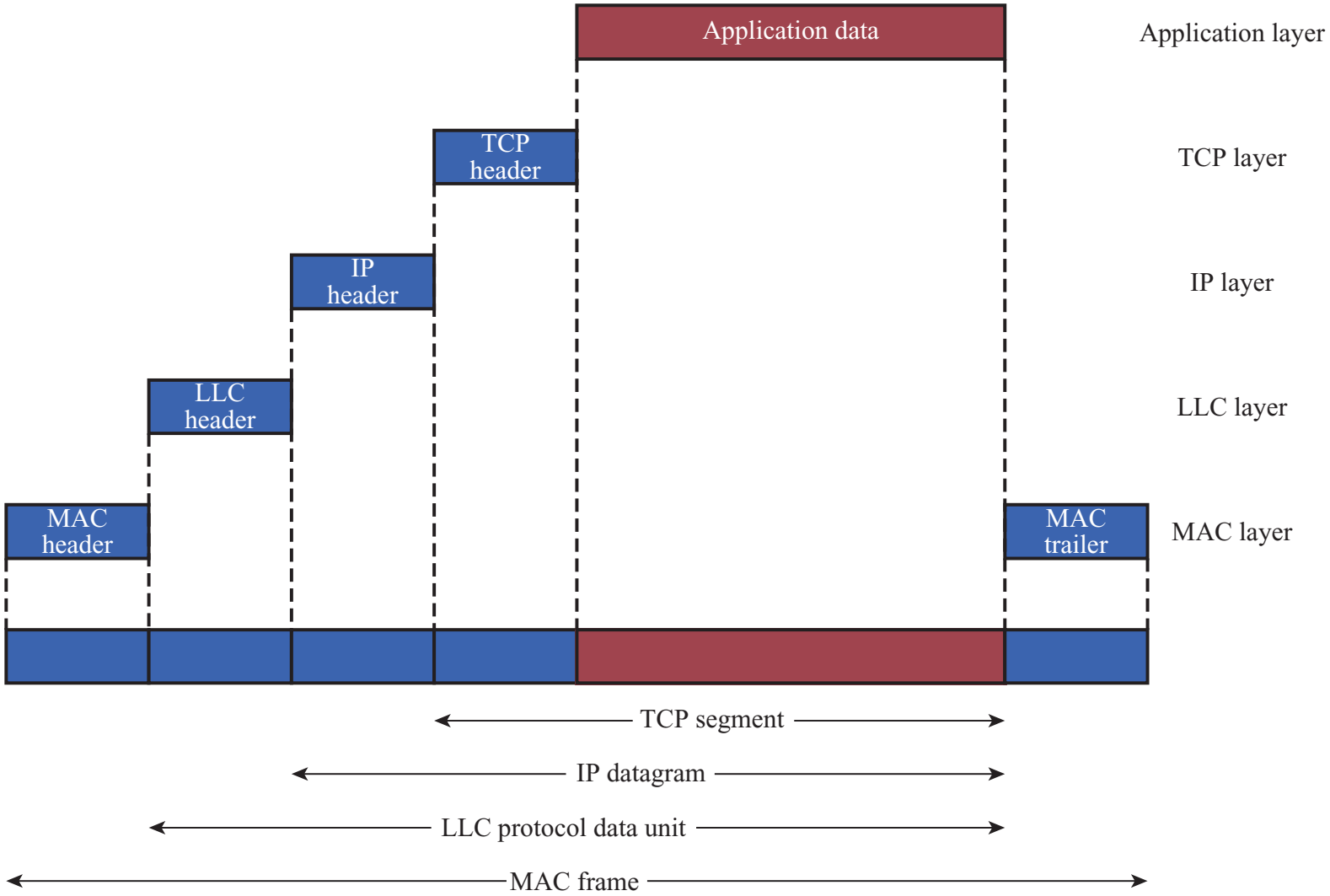
IEEE 802 Protocol Layers Compared to OSI Model



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

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

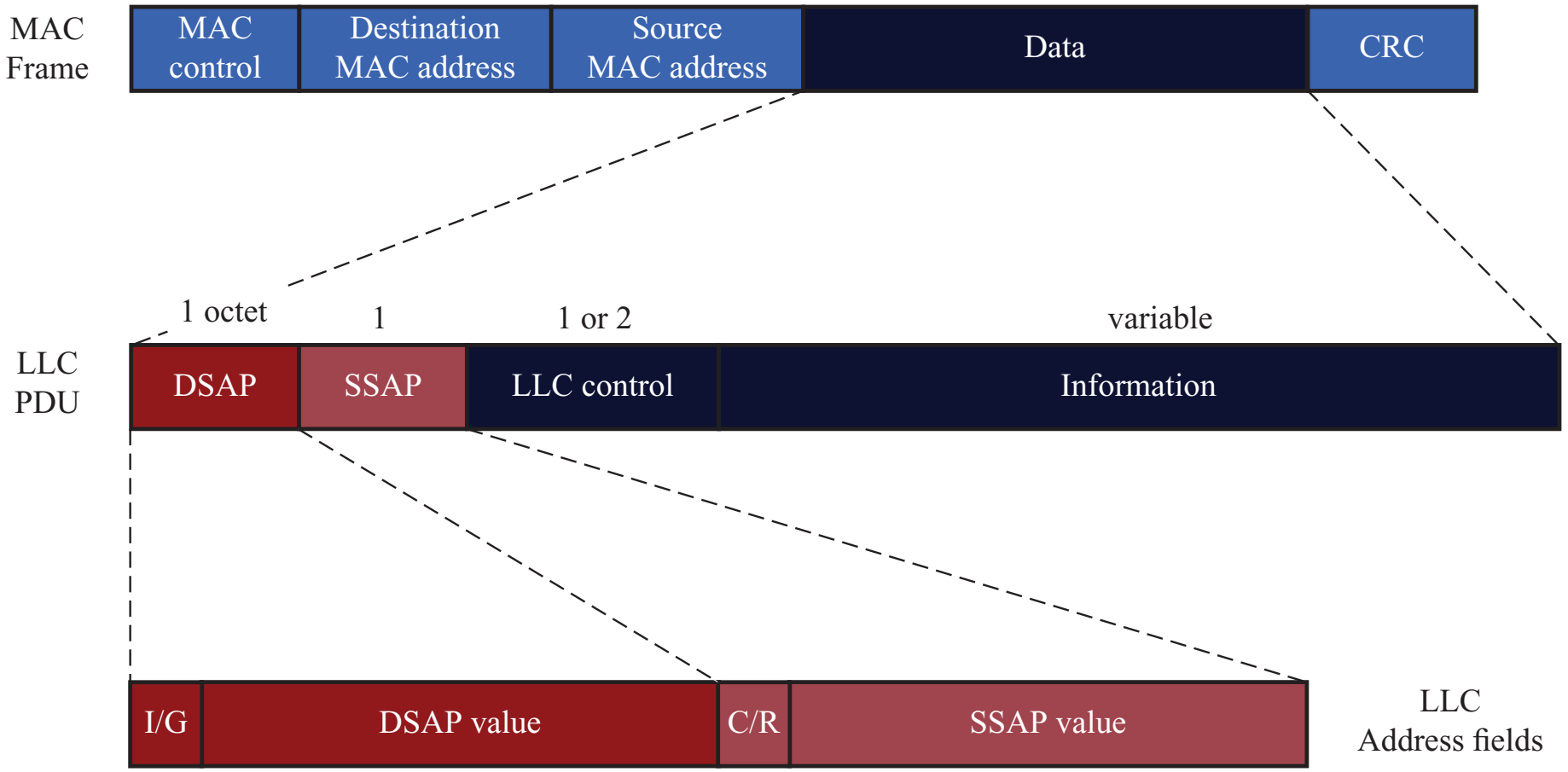
Separation of LLC and MAC

- 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

LLC PDU in a Generic MAC Frame Format



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

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

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
- T1: Unacknowledged connectionless service
  - No flow- and error-control mechanisms
  - Data delivery not guaranteed
- T2: Connection-mode service
  - Logical connection set up between two users
  - Flow- and error-control provided
- T3: Acknowledged connectionless service
  - Cross between previous two
  - Datagrams acknowledged
  - No prior logical setup

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

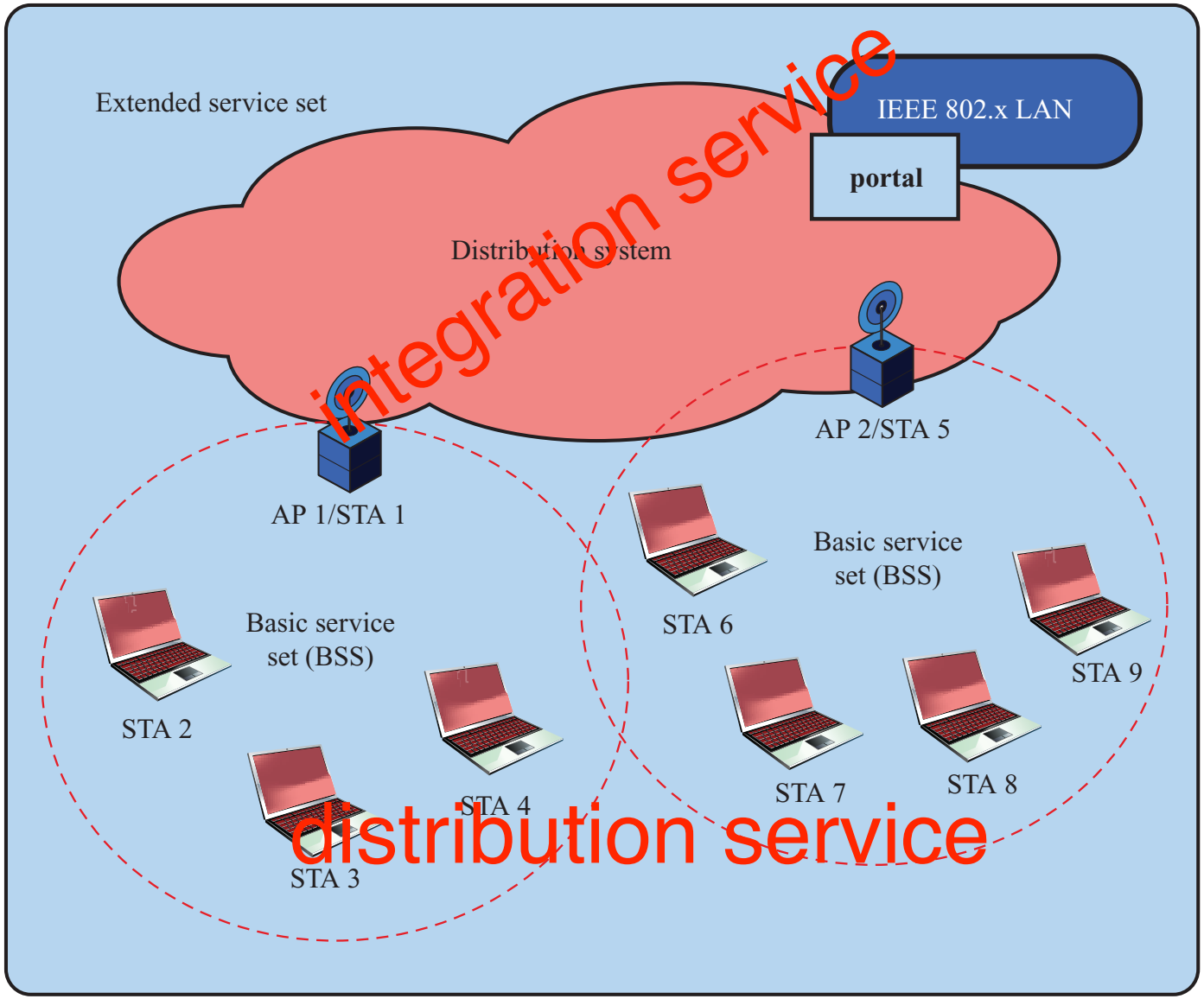
IEEE 802.11 Standards

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

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

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 a BSS in one ESS to a 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

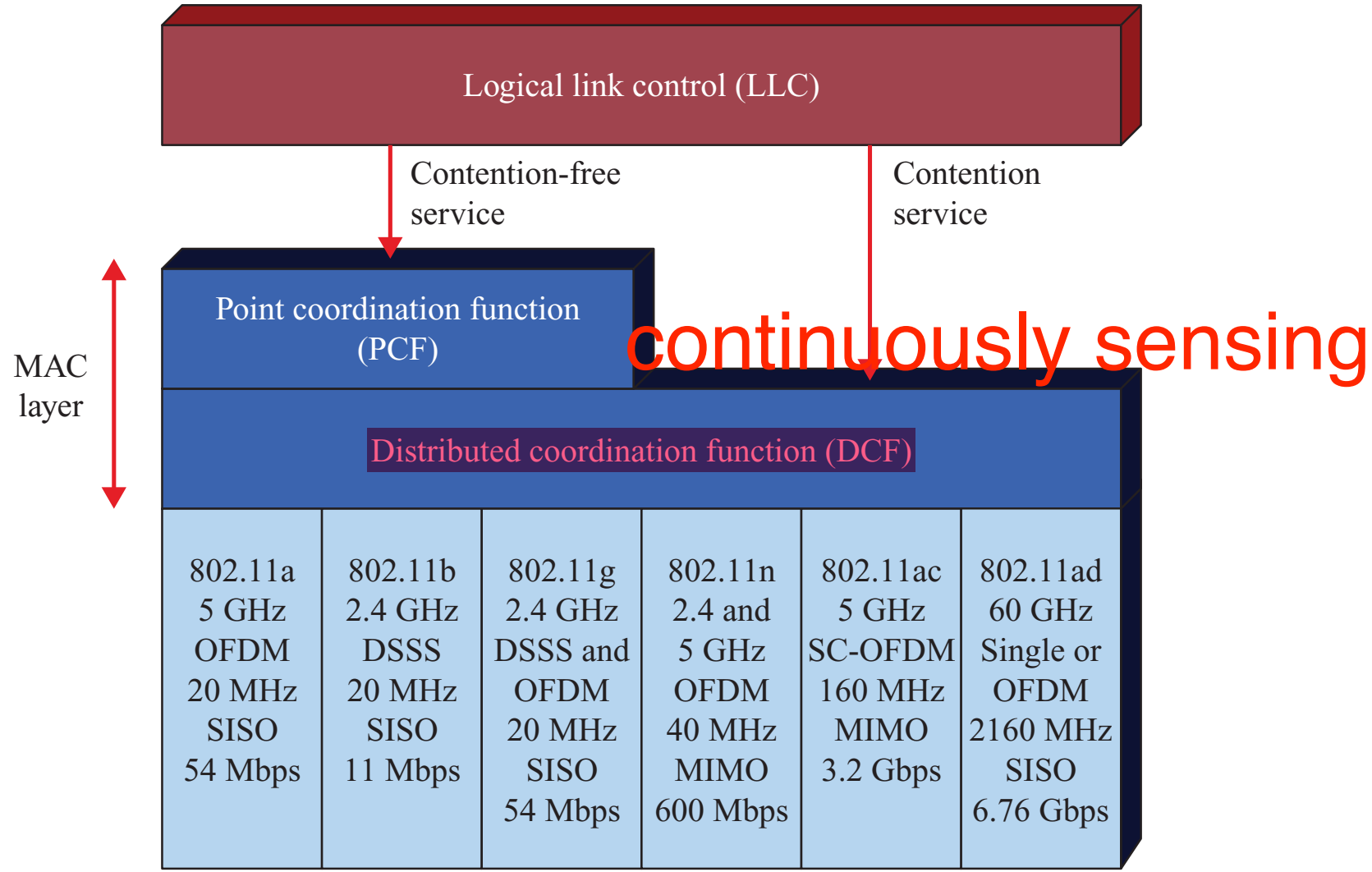
Reliable Data Delivery

- 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

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.

Binary Exponential Backoff

- Random access: binary exponential back-off
- After collision, wait a random time before trying again
- After m^{th} collision, choose K randomly from $\{0,\ldots, 2^m-1\}$
- … and wait for K*512 bit times before trying again
- Using min packet size as “slot”
- If transmission occurring when ready to send, wait until end of transmission
- Think of time as divided in slots
- After each collision, pick a slot randomly within next 2^m slots – where m is the number of collisions since last successful transmission

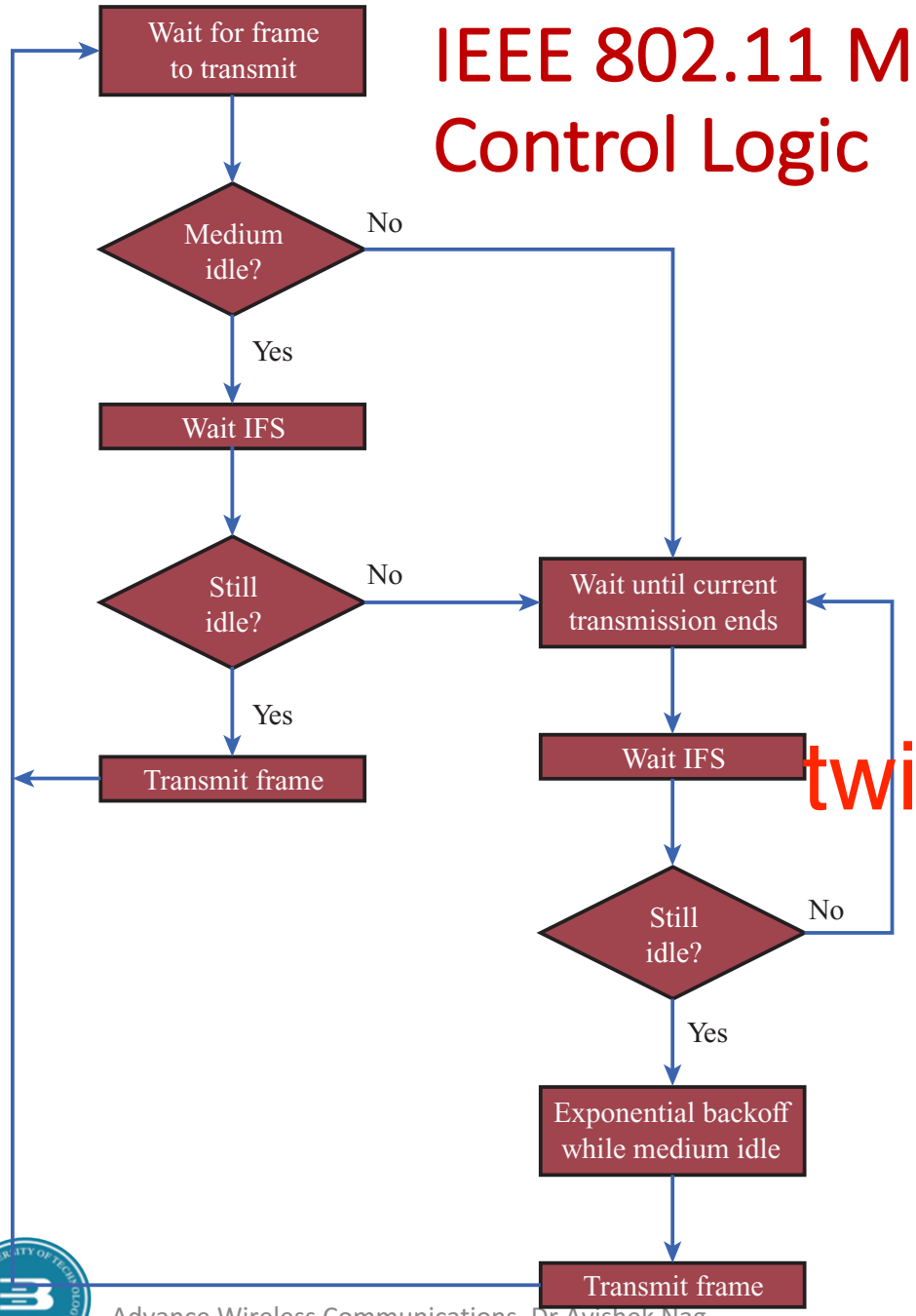
Interframe Space (IFS) Values

- 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

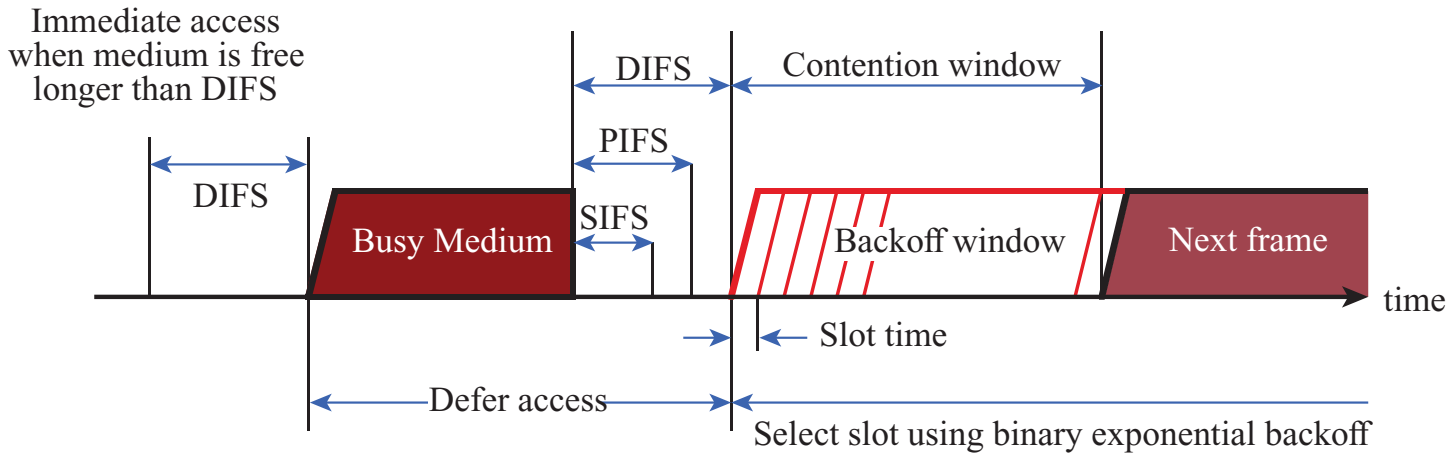
- SIFS
  - Acknowledgment (ACK)
  - Clear to send (CTS)
  - Poll response
- PIFS
  - Used by centralized controller in issuing polls
  - Takes precedence over normal contention traffic
- DIFS
  - Used for all ordinary asynchronous traffic

IEEE 802.11 Medium Access Control Logic

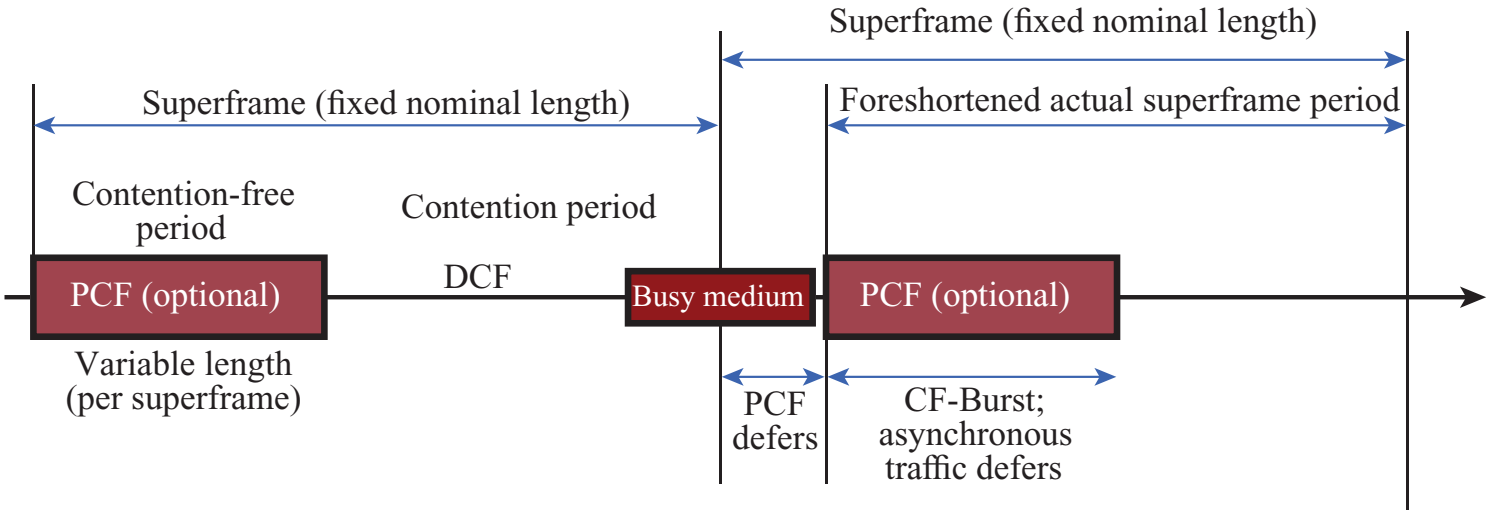


twice the previous

IEEE 802.11 MAC Timing



(a) Basic access method

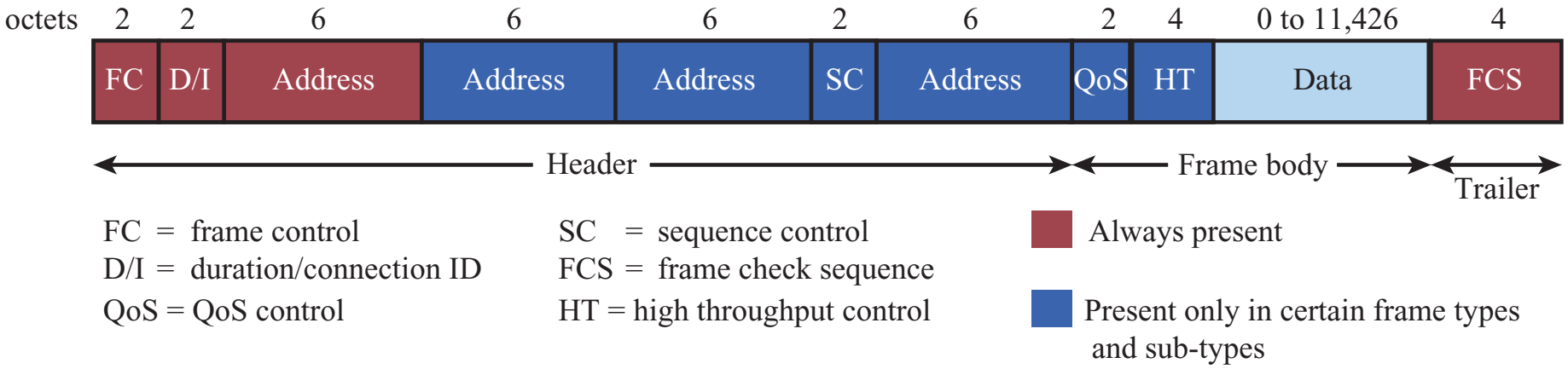


(b) PCF superframe construction

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

IEEE 802.11 MAC Frame Format



(a) MAC frame

(b) Frame control field

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
- 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

Go Through The Book

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

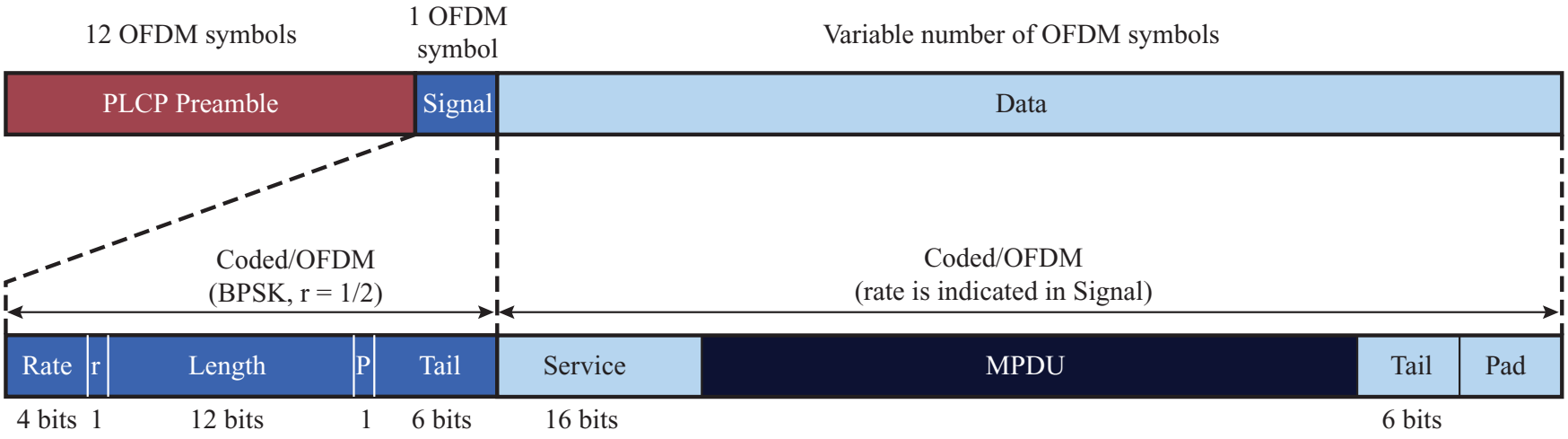
IEEE 802.11 physical layer

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

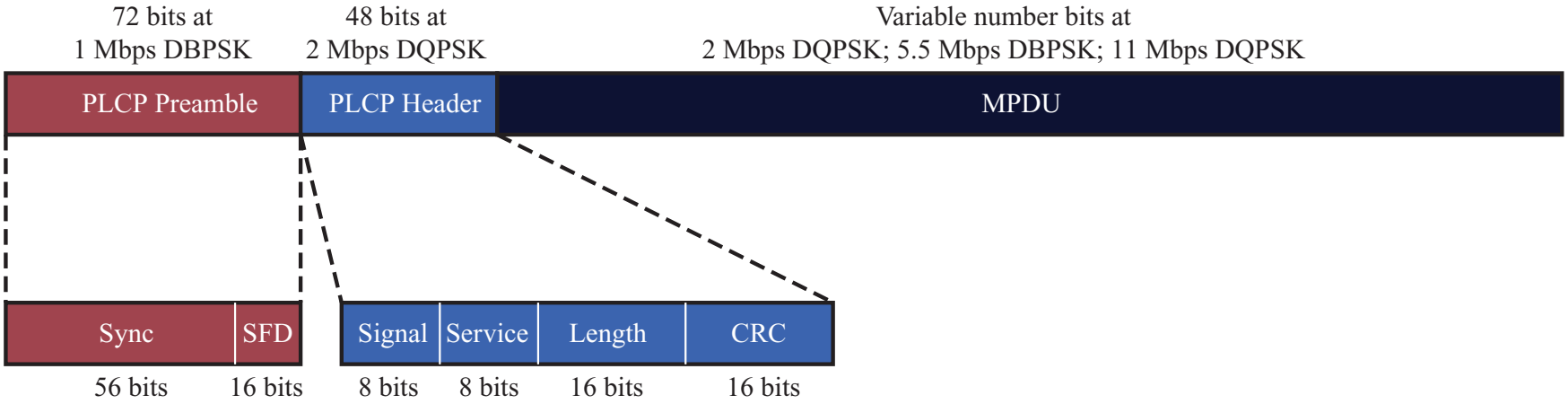
IEEE 802.11a AND IEEE 802.11b

- 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

IEEE 802 Physical-Level Protocol Data Units

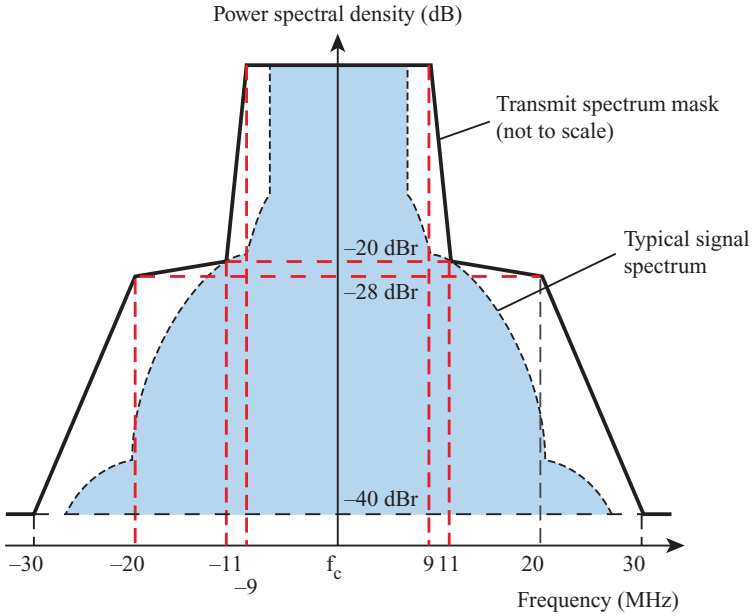


(a) IEEE 802.11a physical PDU

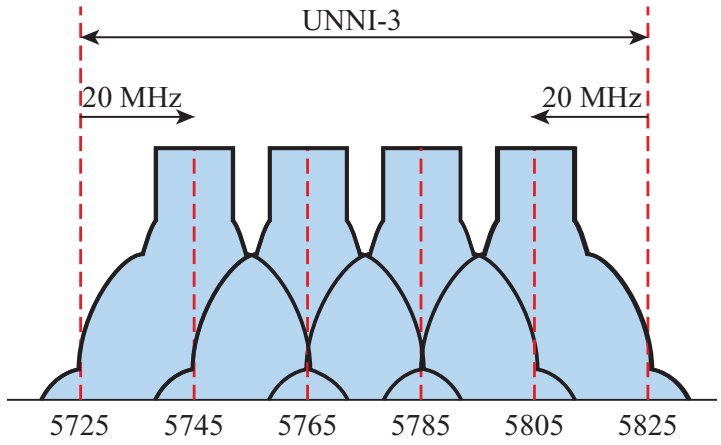


(b) IEEE 802.11b physical PDU

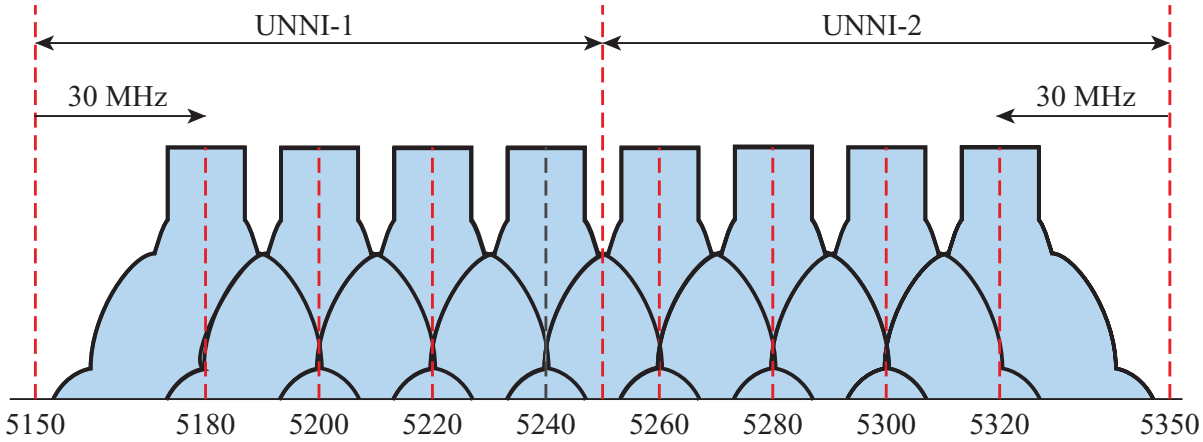
IEEE 802.11a CHANNEL SCHEME



(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

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

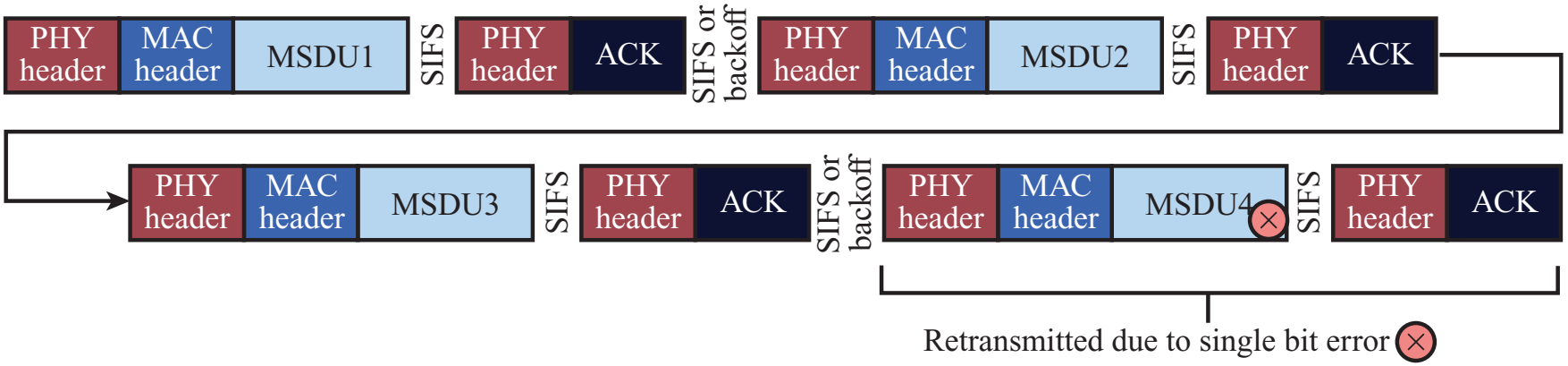
IEEE 802.11n

- 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

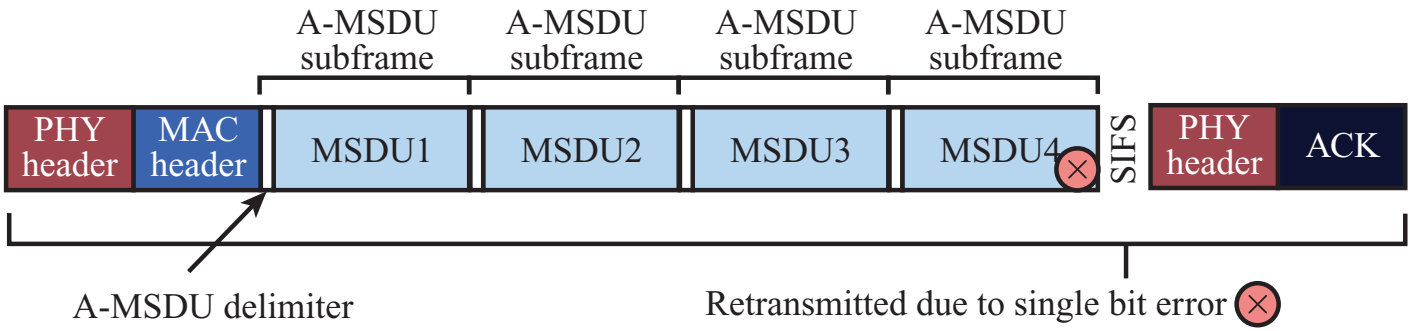
IEEE 802.11n -- MAC enhancements

- Reduce header bits, backoffs, and IFS times
- Block acknowledgements
  - One ACK to cover multiple packets
- Frame aggregation
  - Three forms
  - MSDUs (MAC service data unit) come down from the LLC layer, MPDUs come from the MAC layer
  - A-MSDU aggregation – shared PHY and MAC headers and FCS
  - A-MPDU (MAC protocol data unit) 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

Forms of Aggregation

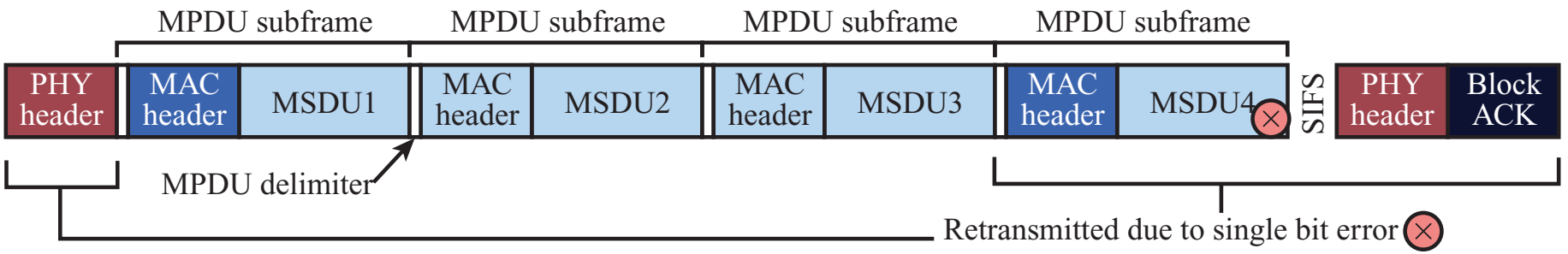


(a) No aggregation

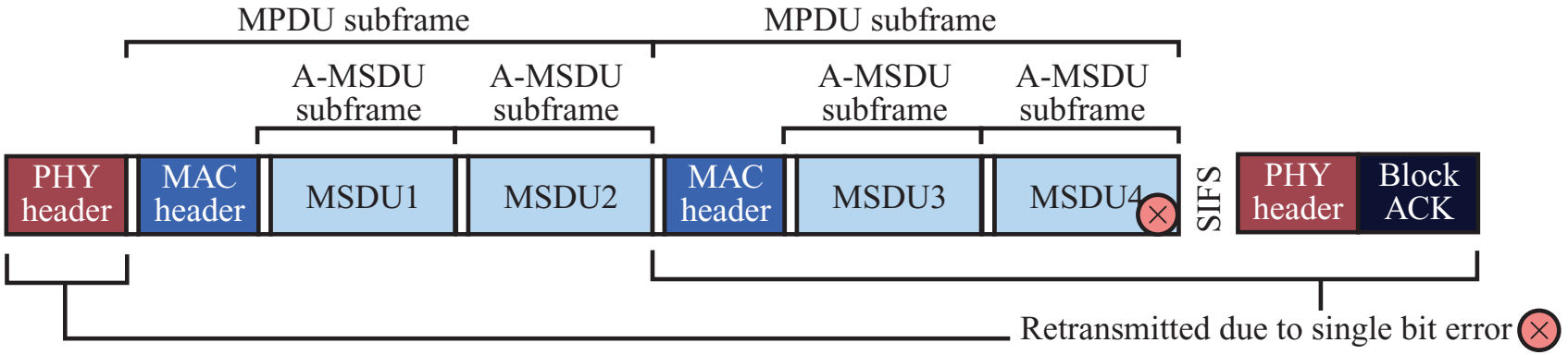


(b) A-MSDU aggregation

Forms of aggregation II



(c) A-MPDU aggregation

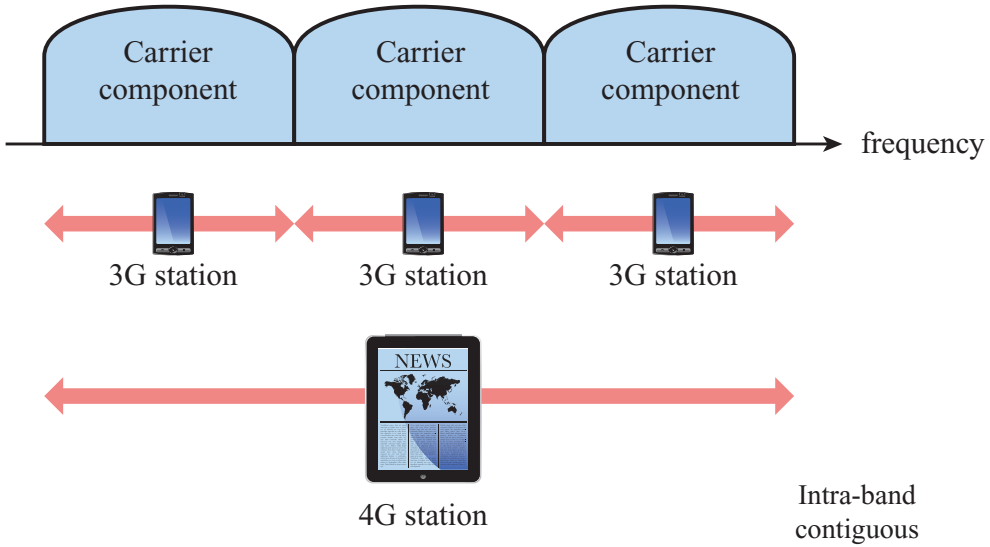


(d) A-MPDU of A-MSDU aggregation

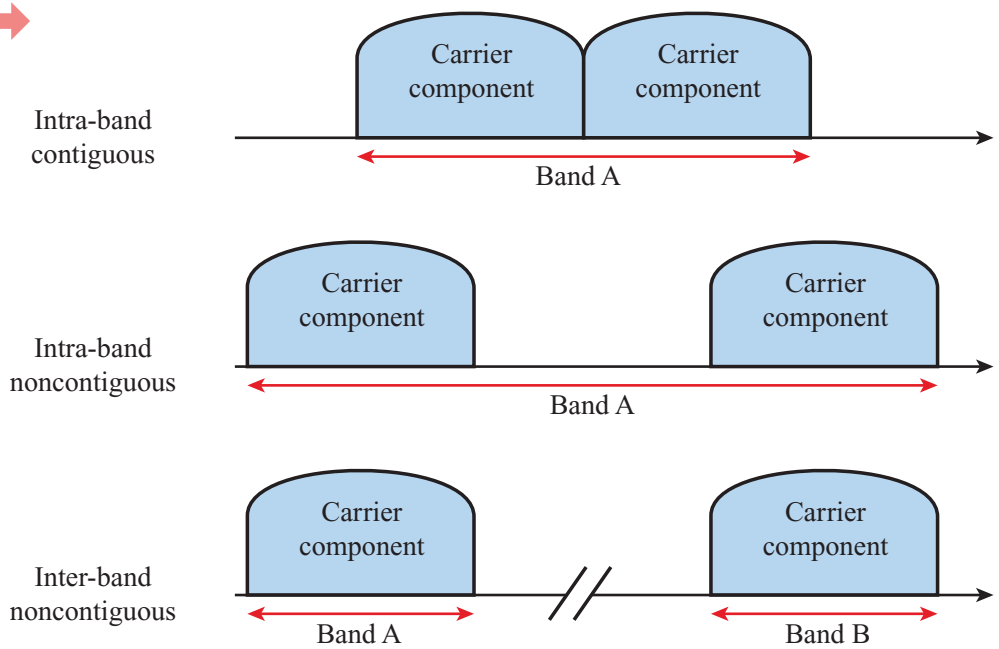
Bandwidth expansion

- A signal can only provide a limited bps/Hz
  - More bandwidth is needed
- Carrier aggregation
  - Combine multiple channels
    - Example: Fourth-generation LTE combines third-generation carriers
- Frequency reuse
  - Limit propagation range to an area
  - Use the same frequencies again when sufficiently far away
  - Use large coverage areas (macro cells) and smaller coverage areas (outdoor picocells or relays and indoor femtocells)
- Millimeter wave (mmWave)
  - Higher carrier frequencies have more bandwidth available
  - 30 to 300 GHz bands with millimeter wavelengths
  - Yet these are expensive to use and have problems with obstructions

Carrier Aggregation



(a) Logical view of carrier aggregation

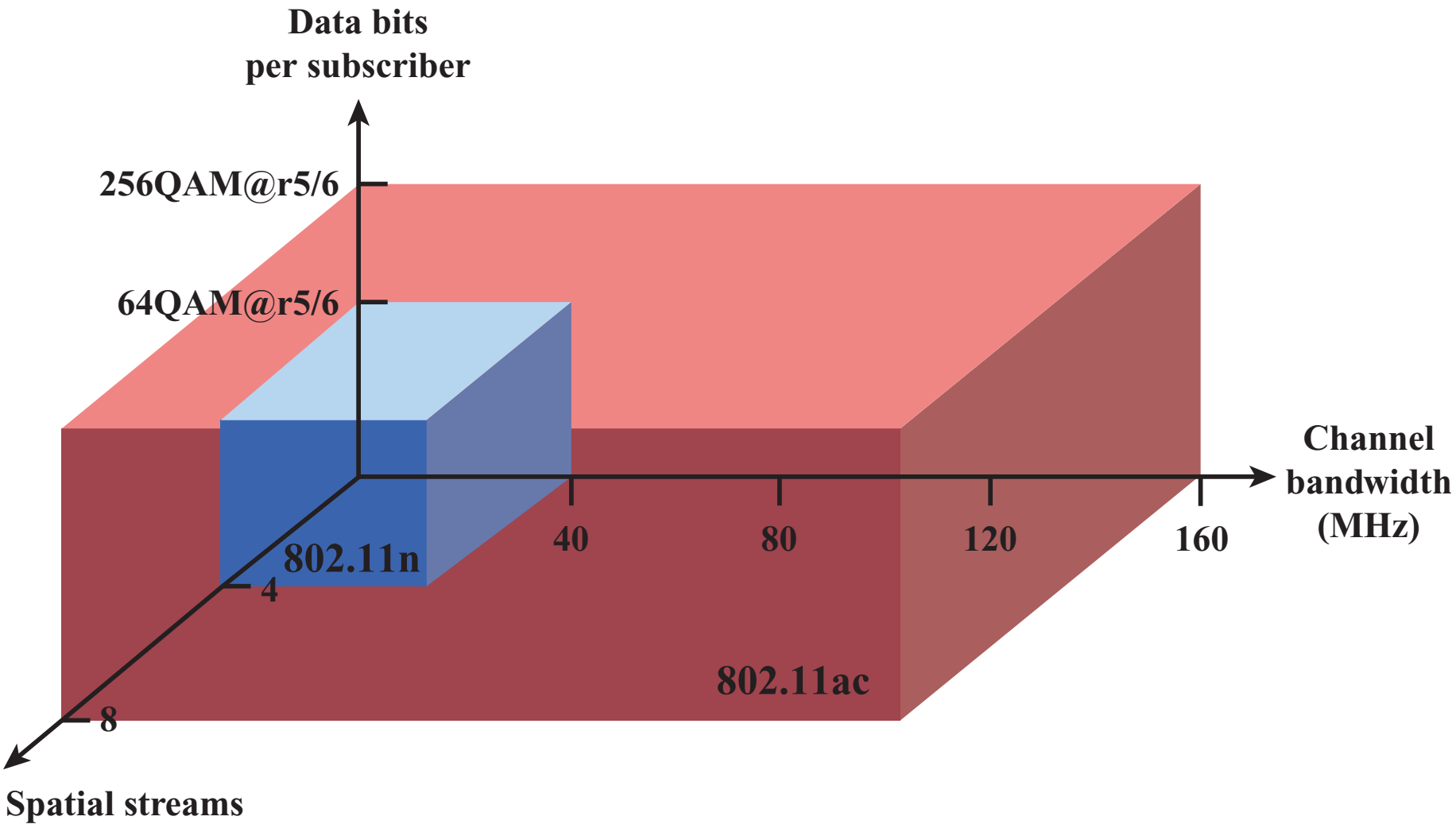


(b) Types of carrier aggregation

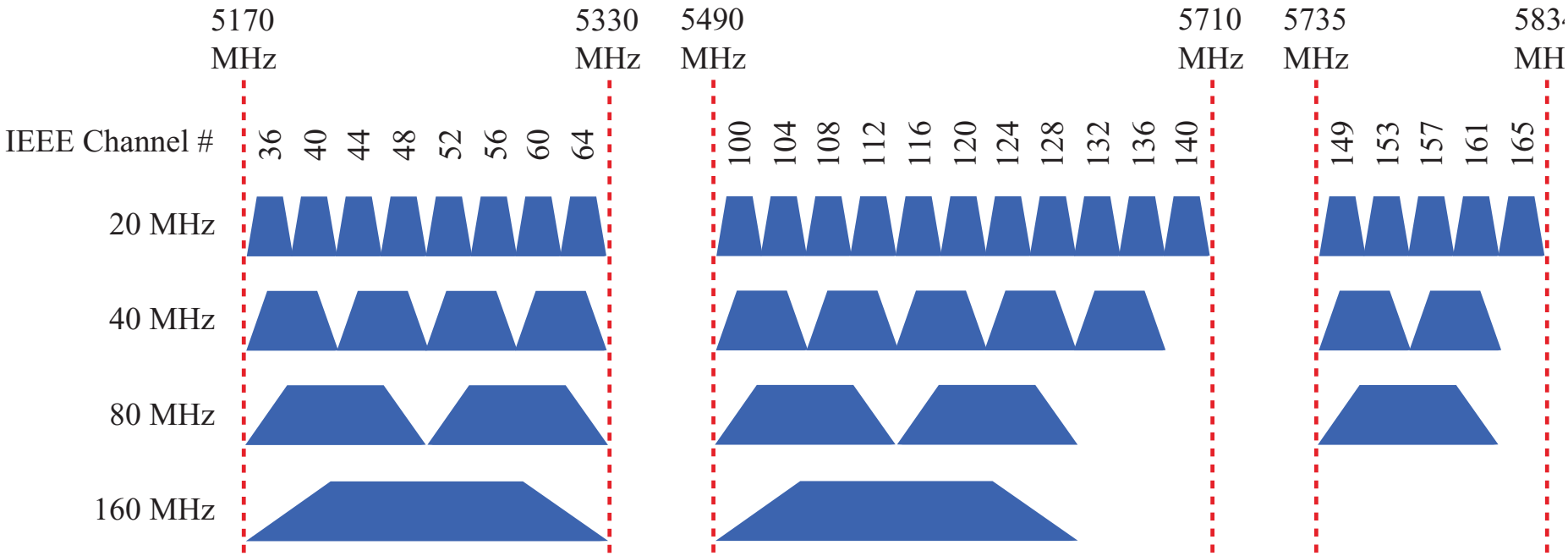
Gigabit wi-fi

- 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

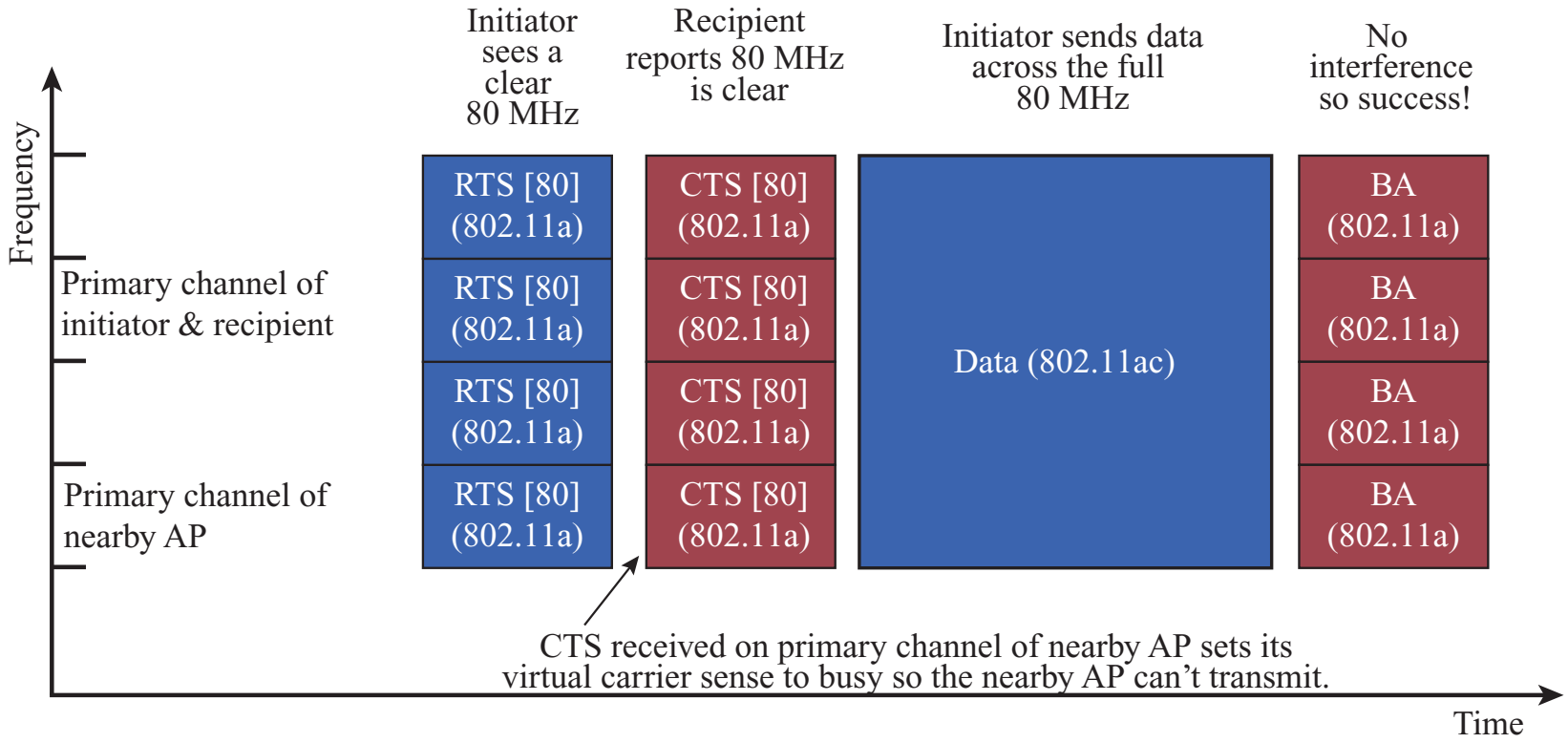
IEEE 802.11 Performance Factors



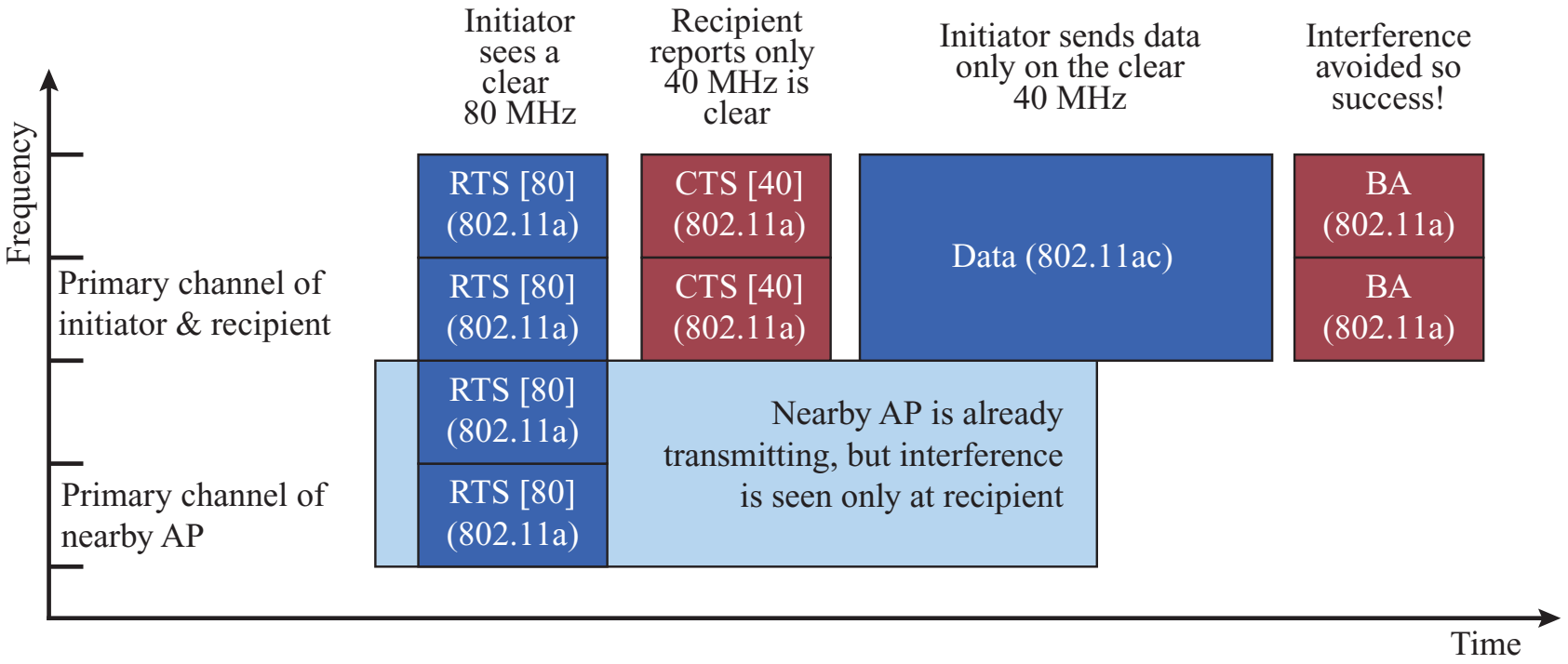
5 GHz 802.11ac CHANNEL ALLOCATIONS



RTS/CTS Enhanced with Bandwidth Signaling



(a) No interference case



(b) Interference case

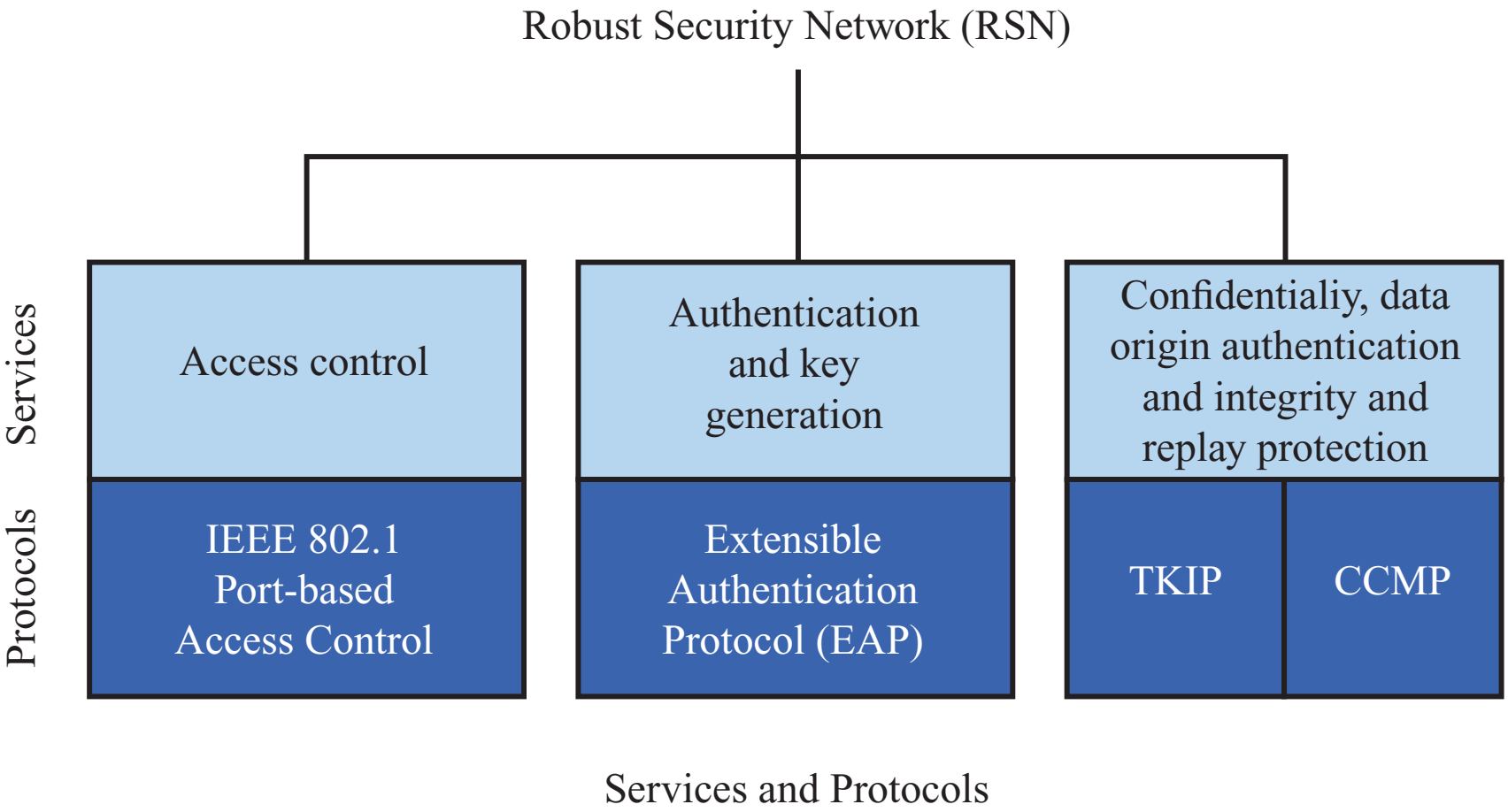
Gigabit wi-fi --- 802.11ad

- 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

ELEMENTS OF IEEE 802.11i



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

IEEE 802.11i PHASES OF OPERATION