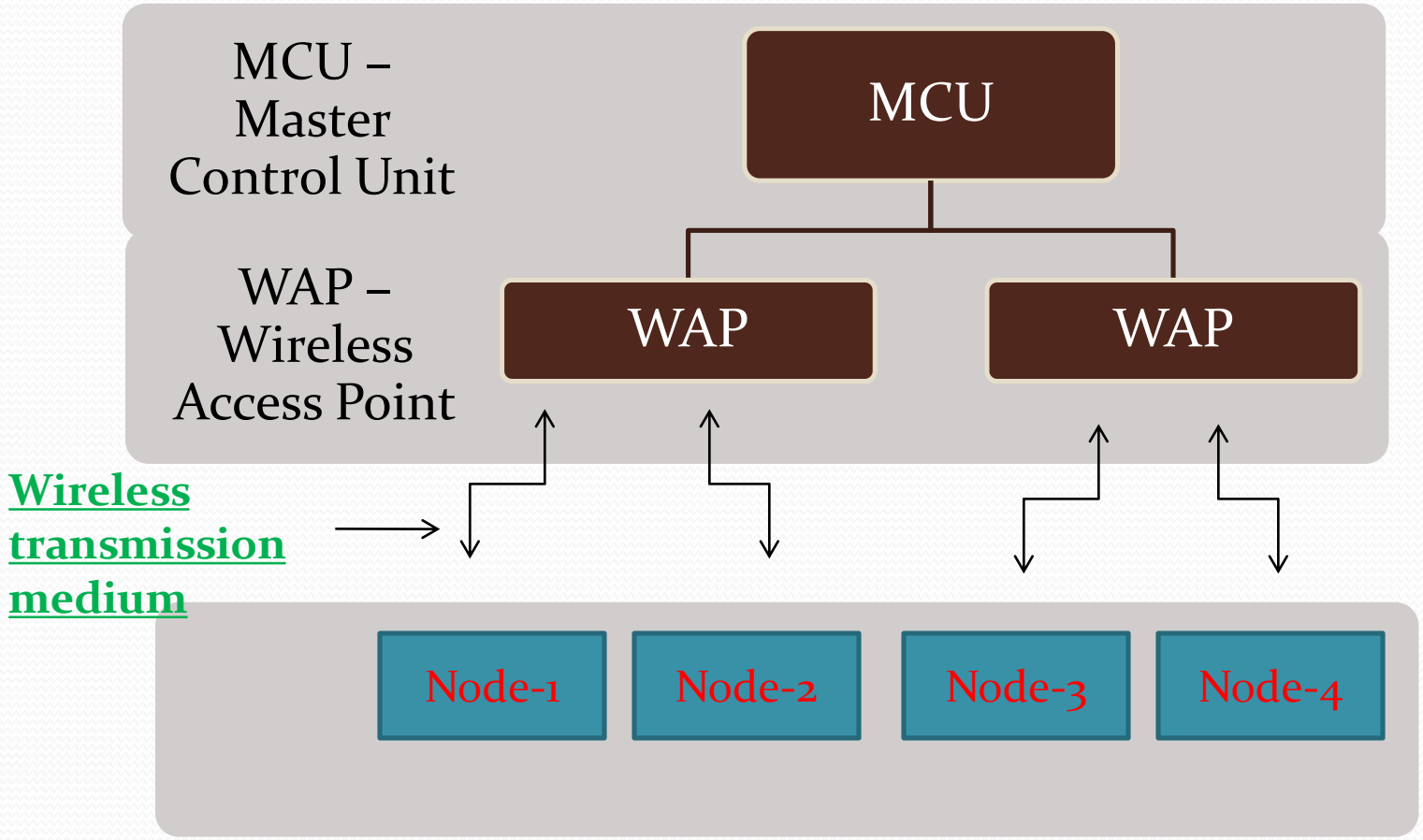
WIRELESS LAN

LAN(local area network)

- It is a communication network that interconnects variety of devices and provides means of information exchange among these devices
- Its scope may be a small room, a building or a cluster of buildings

WLAN(Wireless LAN)

- LAN that makes use of wireless transmission media is called as wireless LAN i.e. WLAN
- Instead of being an alternate it may be called as extension to LAN
- It is used to provide final connectivity of few meters between backbone wired network and end mobile users
- Used to have high prices, low data rates, occupational safety concerns, and licensing requirements
- Popularity of wireless LANs has grown rapidly


MCU – Master Control Unit
MCU
WAP – Wireless Access Point
WAP
WAP
Wireless transmission medium
Node-1
Node-2
Node-3
Node-4

- Access point : Should have NIC (Network Interface Card)
- Hub antenna : located at center or corner
- Line of sight : not necessary but desirable
- Frequency used may be
  - Licensed (require high length of paper work from FCC)
  - Unlicensed (does not require paper work but suffers inference from barcode , scanners etc)
- Standards used may be
  - de-facto (approved by individuals or organizations that don't have national international recognition)
  - De-jure(approved by nationally internationally approved organizations)

Advantages

- Flexibility
- Planning
- Installations
- Robustness
- Scalability
- Cost
- Improved productivity and service

Disadvantages

- Quality of service
- Proprietary solutions
- Restrictions
- Safety and security

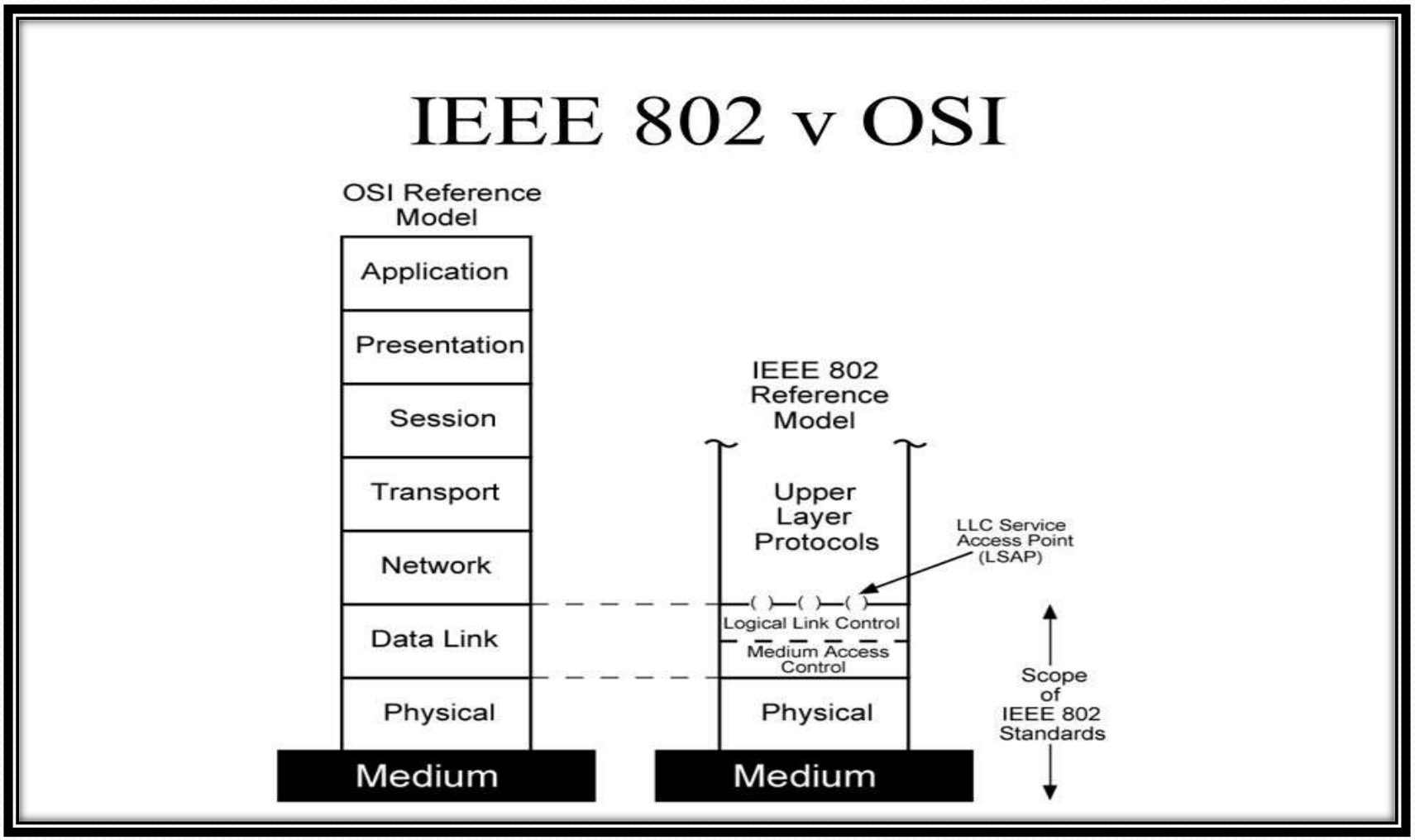
Applications

- LAN extensions
- Cross building interconnect
- Nomadic access
- Adhoc networking

WLAN requirements

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

IEEE 802 Architecture



- Physical layer
  - Encoding/decoding of signals
  - Preamble generation/removal (for synchronization)
  - Bit transmission/reception
  - Specification of transmission medium and topology (considered below lowest layer of OSI model)
  - For some standards physical layer is subdivided into sub-layers
    - **physical layer convergence procedure** : define method of mapping MPDU into framing format suitable for sending and receiving user data and management information between two or more stations
    - **Physical medium dependent sub-layer** : defines the characteristics of and methods of transmitting and receiving user data trough a wireless medium between two or more stations

Layer two is separated into two parts

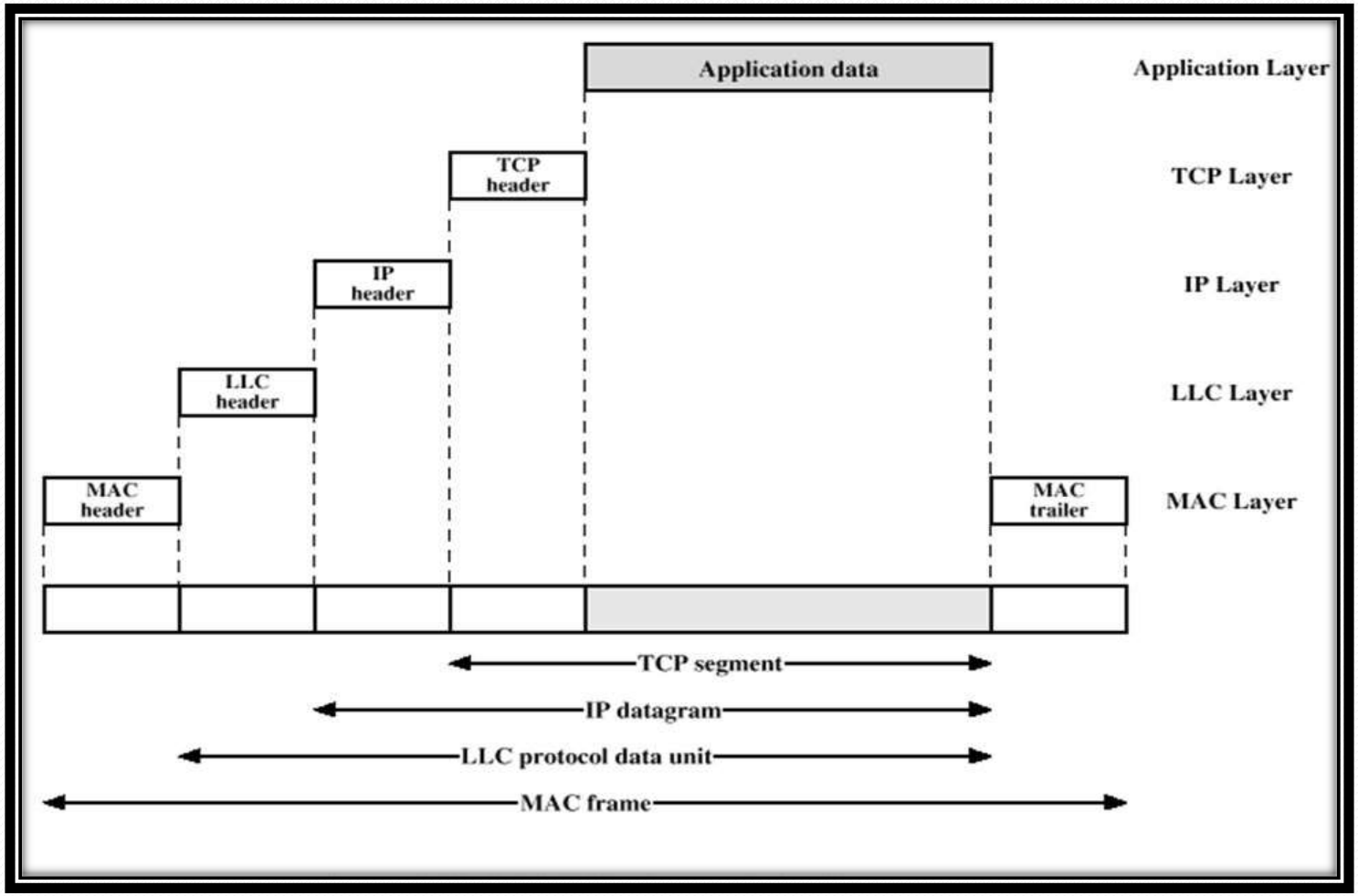
1) Medium Access control
2) logic link control

- Medium Access Control layer (MAC)
  - 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

- Logic link control layer (LLC)
  - Provide an interface to higher layer and perform flow and error control

- This separation is second layer is done for following reasons
  - Logic required to manage access to a shared-access medium is not found in traditional layer 2 data link control
  - For the same LLC, several MAC options may be provided

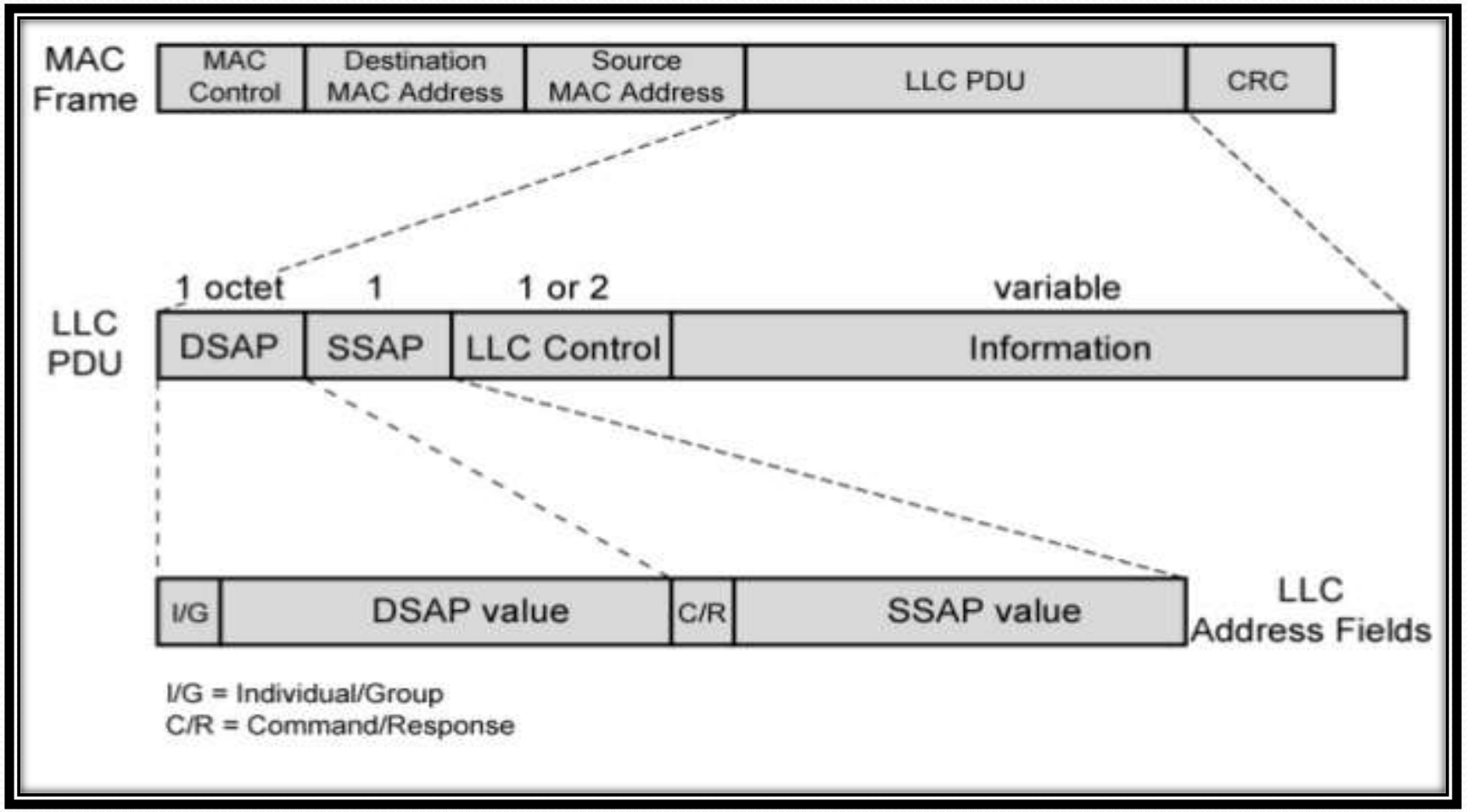
IEEE 802 protocols in context



- Higher level data are passed to LLC which appends control information as a header, creating an LLC protocol data unit
- This LLC PDU is then passed down to the MAC layer which appends control information at the back and front of the packet forming a MAC frame
- For context the figure also shows the use of TCP/IP and application layer above LAN protocol

- MAC frame format
  - MAC control: protocol control information needed for functioning of MAC protocol
  - Destination MAC address: destination physical attachment point on LAN
  - Source MAC address: source physical attachment point on LAN
  - Data: body of MAC frame
  - CRC: cyclic redundancy check field (error detecting code)

MAC Frame format

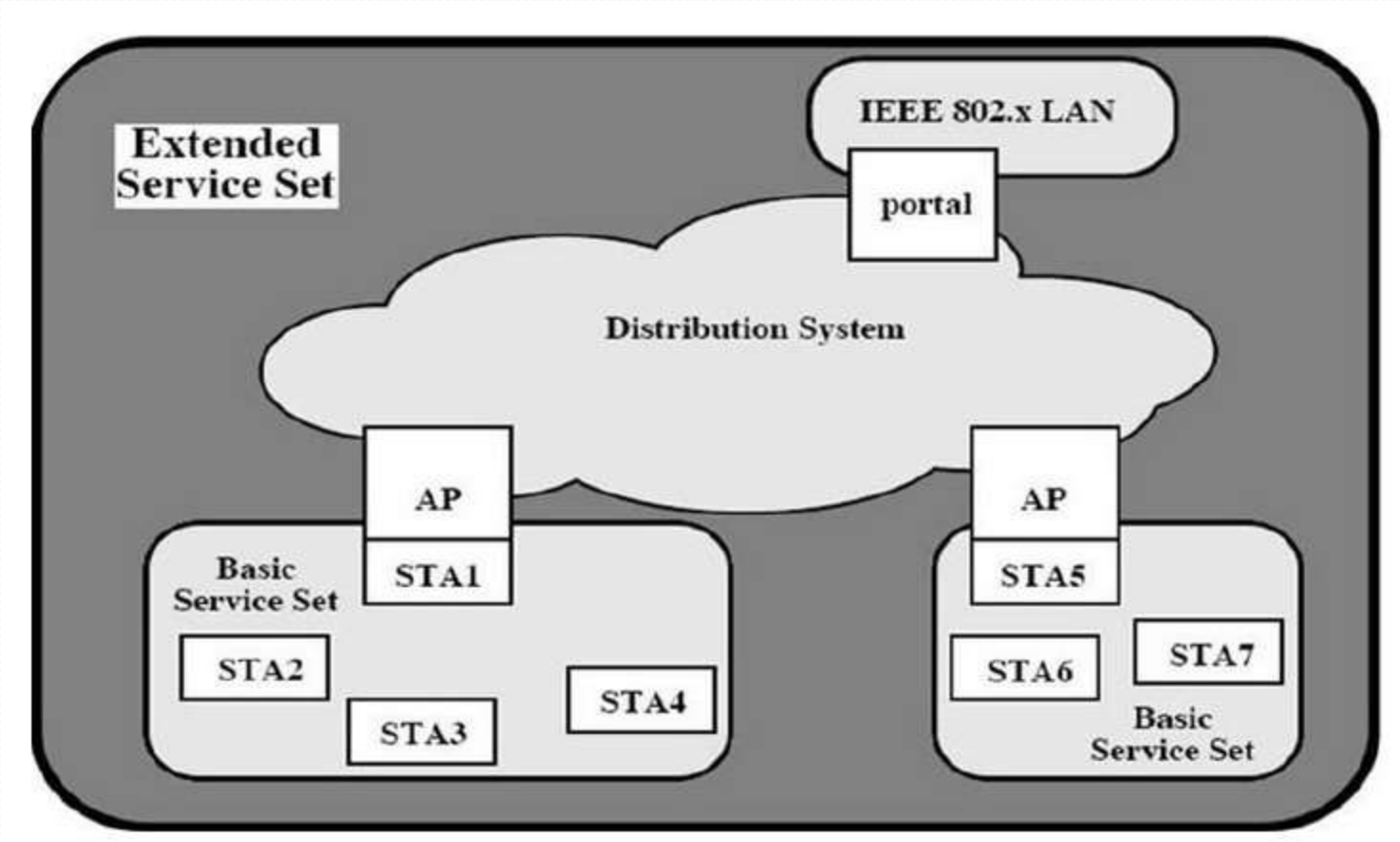


- MAC layer is responsible for detecting errors and discarding any frames that are in error
- LLC layer optionally keeps track of which frames have been successfully received and retransmits unsuccessful frames
- Previous 2 tasks normally responsibility of data link protocol
- LLC specifies mechanisms for addressing stations across the medium and for controlling the exchange of data between users

- LLC services
  - **Unacknowledged connectionless service**: datagram-style service. No flow or error control mechanisms (delivery of data not guaranteed). However in most devices there are some higher level software that deals with the reliability issues
  - **Connection-mode service**: logic connection set up between 2 users, providing flow-control and error control
  - **Acknowledged connectionless service**: datagrams to be acknowledged, but no prior logical connection is set up
- MAC layer is responsible for detecting errors and discarding any frames that are in error

IEEE 802.11 Architecture

This model was developed by 802.11 working group



- Basic service set (BSS)
  - it is the smallest building block of WLAN
  - Made of stationary or mobile wireless stations executing the same MAC protocol and competing for access to wireless medium
  - BSS may be isolated or it may connect to a backbone distribution system (DS) through central base station (Access Point AP)
  - AP functions as bridge or relay point, since stations that want to communicate with each other, weather is same of different BSS, will always do so through AP
  - DS can be switch wired network or wireless network
  - When all stations are mobile stations with no connections to other BSS , the BSS is called independent BSS(IBSS) which is typically an adhoc network .No AP is involved here

- Extended service set (ESS)
  - Two or more BSSs with Aps, connected through a distribution system (usually a wired LAN)
  - Similar to a cellular network (a BSS is a cell and each AP a base station)
  - MH can belong to more than one BSS at the same time
  - ESS appears as a single LAN to LLC level

IEEE 802.11 services

IEEE 802.11 defines nine services need to be provided by WLAN to provide functionality equivalent to that which is inherent to LAN

Following table list services and indicate two ways of categorizing them

Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Disassociation	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

Following we discuss services in order designed to clarify the operation of IEEE 802.11 ESSS network

- Distribution of message within DS
  - Distribution service
    - This service is used by stations to exchange MAC frames when frames must traverse the DS to go from station in one BSS to station in another BSS.
    - If two stations are within same BSS then distribution service logically goes through the single AP of same BSS
  - Integration service
    - Enables the transfer of data between stations on an IEEE 802.11 LAN(wireless-lan) and stations on integrated IEEE 802.x LAN(wired-lan)
  - MSDU delivery

- Association related services : before the distribution service can deliver data to or accept data from a station that station must be associated. Three services relate to this requirement
  - Association
    - Before station can transmit or receive frames its identity and address must be known. So station must establish a association with AP within particular BSS
  - Re-association
    - Enables established association to be transferred from one AP to another , allowing mobile station to move from one BSS to another
  - Disassociation
    - A notification from either a station or an AP that existing association is terminated

- Access and privacy services:
  - Authentication
    - Used to establish identity of stations to each other
  - De-authentication
    - This service is invoked when existing authentication is terminated
  - Privacy
    - Used to prevent content of message being read by other than the intended recepient

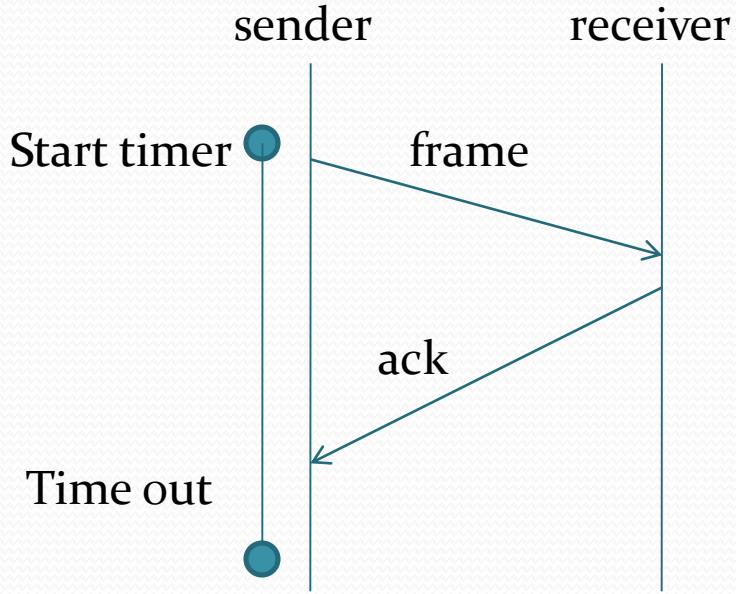
IEEE 802.11 Medium Access Control

- Covers 3 functional areas:
  - reliable data delivery
  - access control
  - security

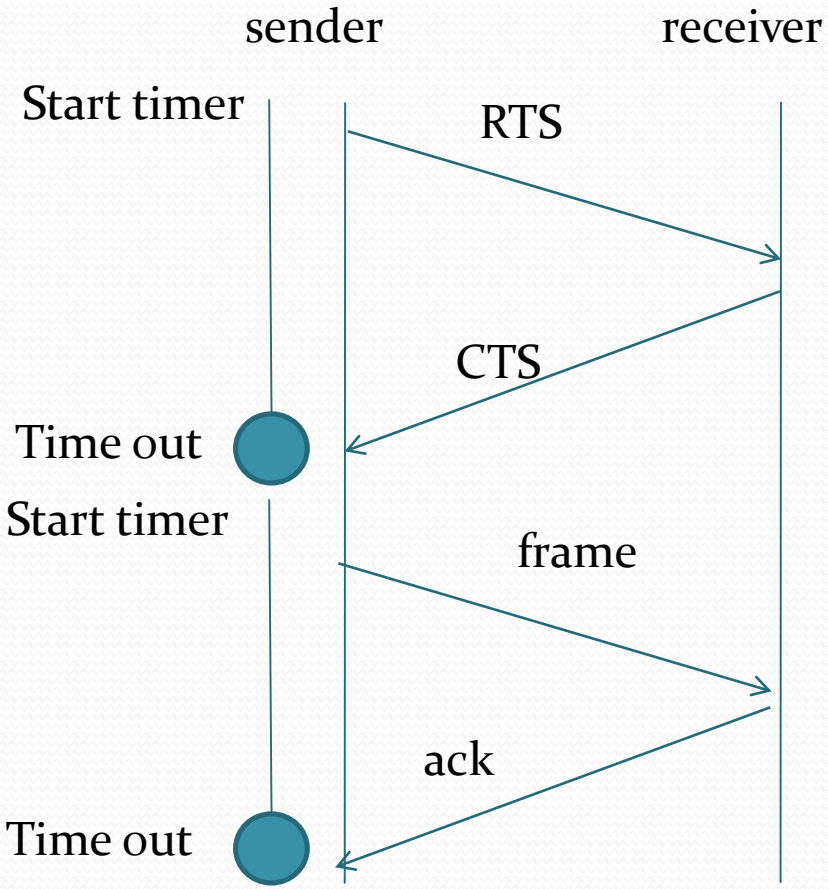
Reliable Data Delivery

- Due to noise, interference and other propagation effects a number of MAC frames are lost. Even with error correcting codes a number of MAC frames cannot be successfully received
- This situation is dealt by use of reliability mechanism at higher layers. However timers used at higher layers for retransmission are of the order of seconds
- Hence it is more efficient to deal with errors at MAC layer
- For this purpose Frame exchange protocols are implemented
  - two frame exchange:
  - four frame exchange:

- Two frame exchange : for every transmitted frame a acknowledgement is sent. If acknowledgement is not received before time out then frame is resent



- Four frame exchange protocol : source first sends request to send (RTS) to destination which responds with clear to send (CTS). After receiving CTS source transmits data frame and destination responds with acknowledgement

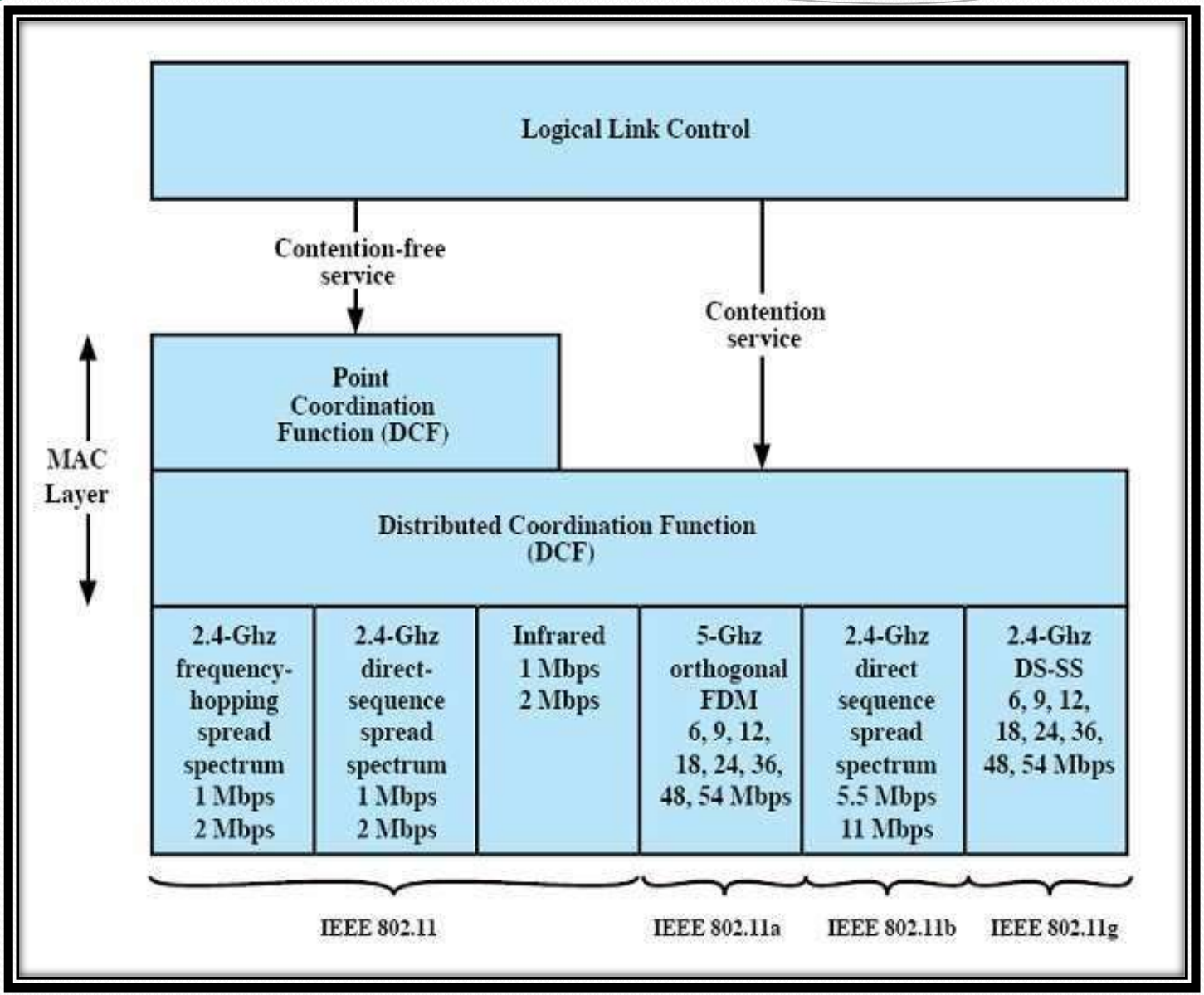


Medium Access control

- 802.11 group considered two proposals for MAC algorithm
  - Distributed access protocol : it will distribute the decision to transmit over all nodes using carrier sense algorithm
  - Centralized access protocol : which involve regulation of transmission by a centralized decision maker

- So the end result for 802.11 is a MAC algorithm called DFWMAC (distributed foundation wireless MAC)

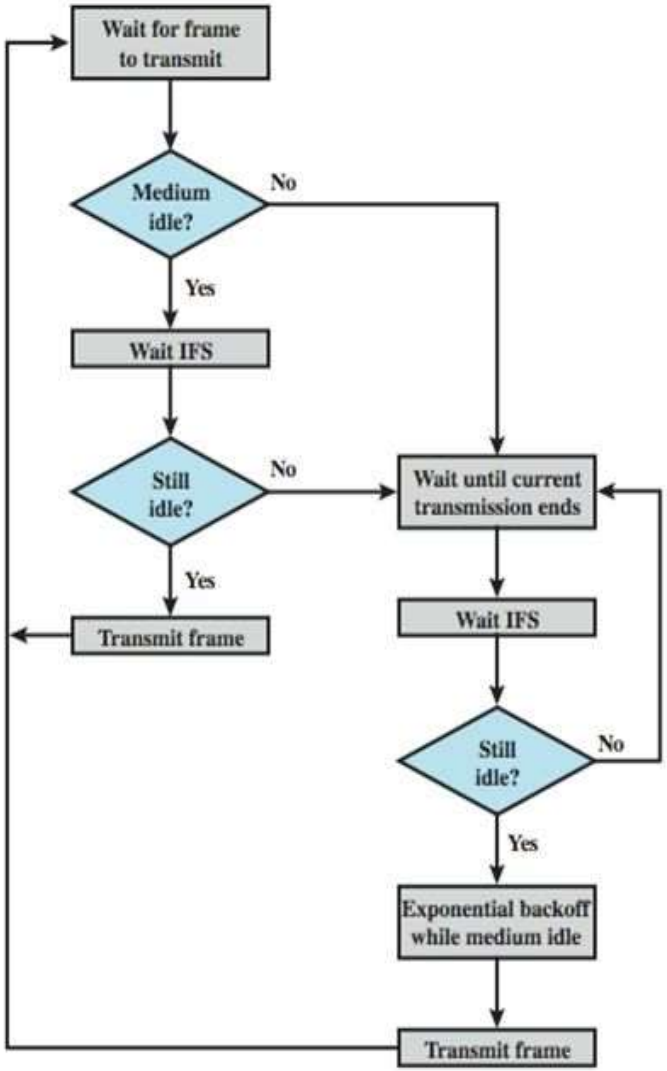
- DFMWAC provides distributed access control mechanism with an optional centralized control built on top of it.
- Lower sub-layer of MAC layer is distributed coordinate function (DCF) which uses a contention algorithm to provide access to all traffic
- Point Coordinate function (PCF) is centralized MAC algorithm used to provide contention free service.
- PCF is built on the top of DCF and exploits the feature of DCF to assure access for its users


Logical Link Control
Contention-free service
Contention service
Point Coordination Function (DCF)
MAC Layer
Distributed Coordination Function (DCF)
2.4-Ghz frequency-hopping spread spectrum 1 Mbps 2 Mbps
2.4-Ghz direct-sequence spread spectrum 1 Mbps 2 Mbps
Infrared 1 Mbps 2 Mbps
5-Ghz orthogonal FDM 6, 9, 12, 18, 24, 36, 48, 54 Mbps
2.4-Ghz direct sequence spread spectrum 5.5 Mbps 11 Mbps
2.4-Ghz DS-SS 6, 9, 12, 18, 24, 36, 48, 54 Mbps
IEEE 802.11
IEEE 802.11a
IEEE 802.11b
IEEE 802.11g

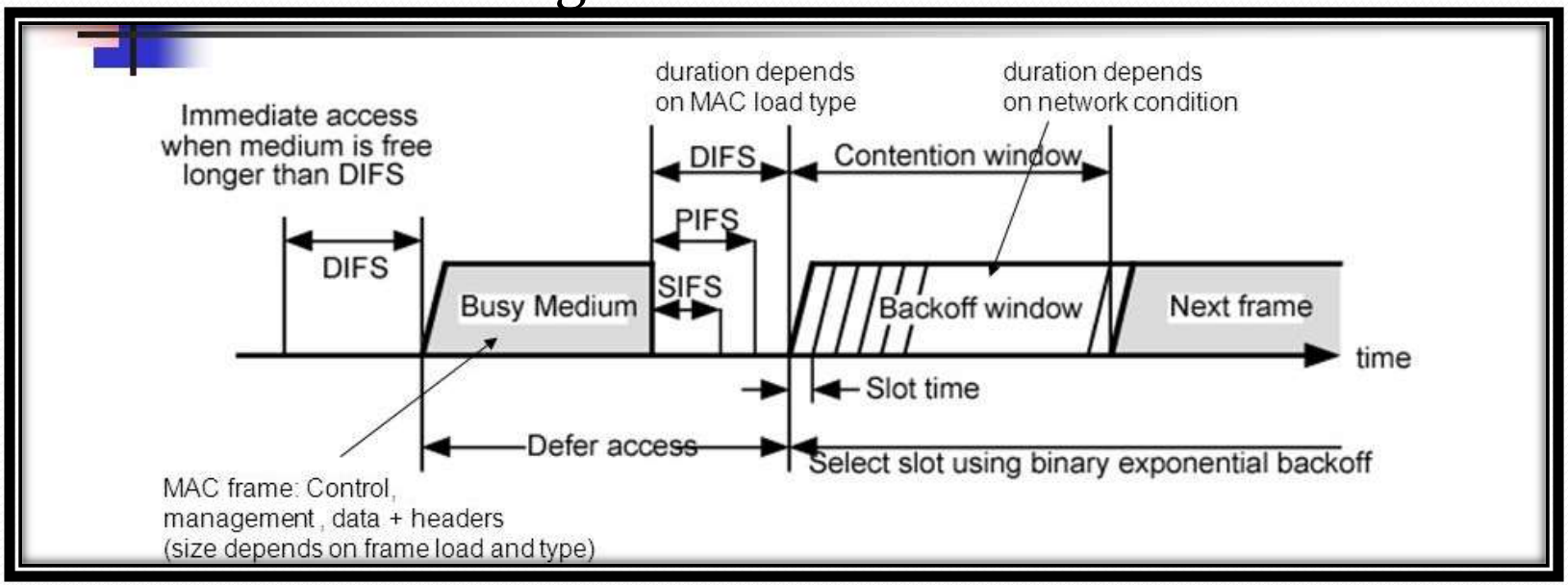
Let us consider the two sub-layers in turn

- Distributed coordinate function
  - Uses CSMA(carrier sense multiple access) algorithm which operates as follows
    - A station with a frame to transmit senses the medium, which if idle, station then waits to see if medium remains idle for the time equal to IFS (inter frame space). If so station may transmit immediately.
    - If the medium is busy , the station defers transmission and continues to monitor the medium until the current transmission is over
    - once the current transmission is over , the station delays another IFS. If the medium remains idle for this period, then the station backoff a random amount of time and again senses the medium. If the medium is still idle the station may transmit. During backoff time, if the medium becomes busy, the backoff timer is halted and resumes when the medium becomes idle
    - If the transmission is unsuccessful which is determined by the absence of an acknowledgement then it is assumed that collision has occurred

IEEE 802.11 Medium Access Control Logic

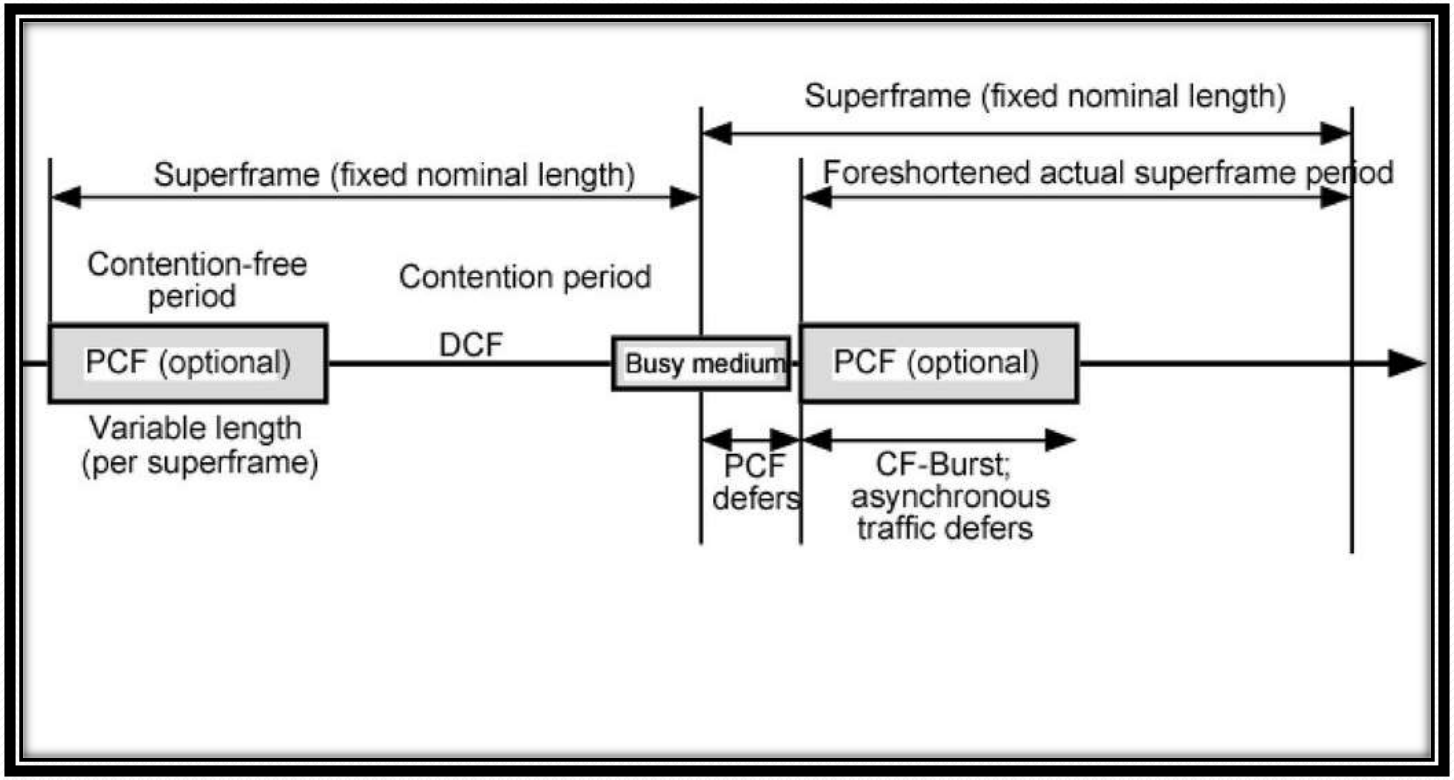


- Three values of IFS are used
  - SIFS(short IFS) : shortest IFS used for all immediate responses
  - PIFS (Point Coordinate Function IFS) : a midlength IFS, used by the centralized controller in the PCF scheme when issuing polls
  - DIFS (distributed coordination function IFS) : the longest IFS, used as a minimum delay for asynchronous frames contending for access



- Point Coordinate function
  - Alternative access method implemented on the top of DCF
  - The operation consist of polling by a centralized polling master (point coordinator), which make of PIFS when issuing polls.
  - Because PIFS is smaller than DIFS, the point coordinator can seize the medium and lock out all asynchronous traffic while it issues polls and receives responses
  - Eg :
    - a wireless network is configured so that number of stations with time sensitive are controlled by point coordinator while remaining traffic contends for access using CSMA .
    - The point coordinator could issue polls in round robin fashion to all stations configured for polling
    - When a poll is issued, the polled station may respond using SIFS.
    - If point coordinator receives a response, it issues another poll using PIFS.
    - If no response is received during the expected turnaround time, the coordinator issues a poll

- If the discipline of the preceding paragraph were implemented, the point coordinator would lock all asynchronous traffic by repeatedly issuing poll
- To prevent this an interval an interval known as super frame is defined
- Following figure illustrates the use of super-frame



MAC Frame format

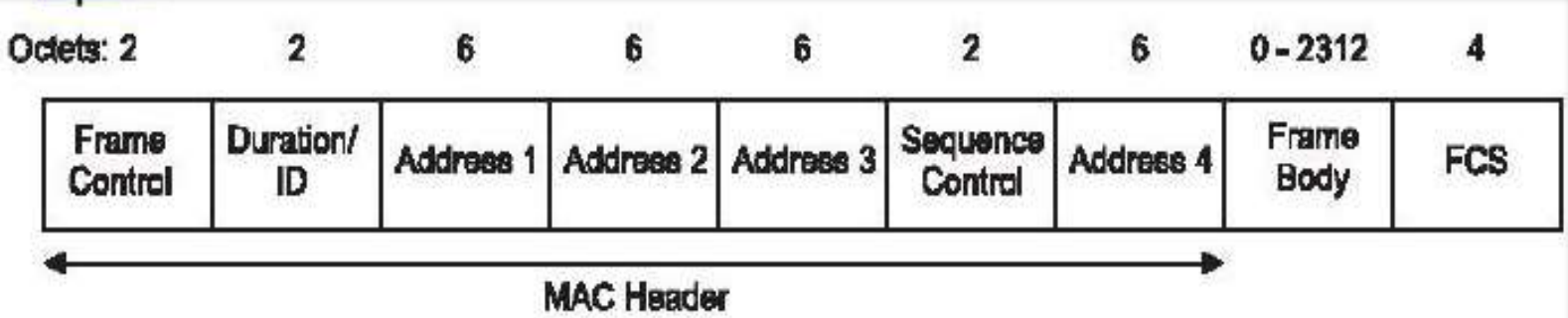


Figure 12—MAC frame format

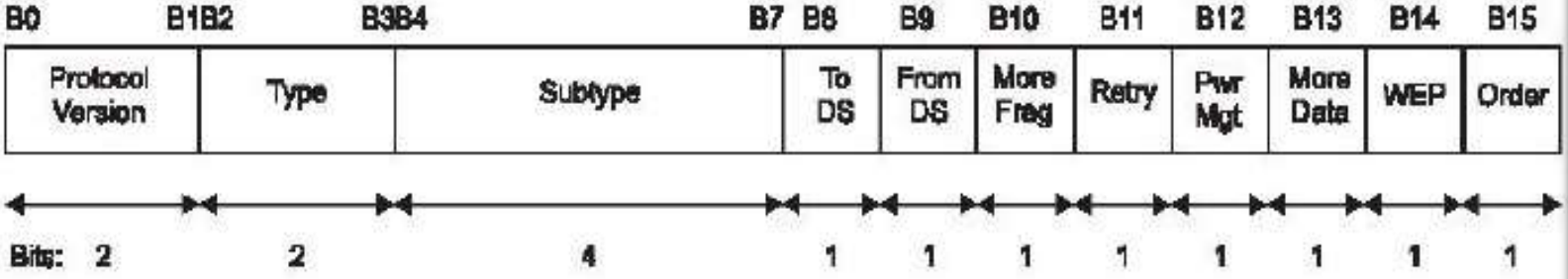


Figure 13—Frame Control field

- Frame control :
  - Indicates type of frame and provides control information
- Duration/connection ID :
  - If used as duration field, indicates time the channel will be allocated for successful transmission of frame
  - In some control frames , the field contains an association, or connection, identifier
- Address :
  - The number and meaning of 48 bit address field depends on context
  - Transmitter and receiver address are the MAC addresses of the stations joined to the BSS that are transmitting and receiving frames over WLAN
  - Service set ID(SSID) identifies WLAN over which frame is transmitted
  - Source and destination address are the MAC address of the stations, wireless or otherwise, that are ultimate source or destination of this frame

- Sequence control :
  - Contains a 4-bit fragment number subfield used for fragmentation and reassembly
  - And a 12-bit sequence number used to number sent between given transmitter and receiver
- Frame body
  - Contains MSDU or fragment of MSDU
- Frame check sequence
  - 32 bit cyclic redundancy check
- Protocol version
  - Shows 802.11 version
- Type
  - Identifies frame as control management or data

- Subtype
  - Further identifies function of frame
- To DS
  - This bit is set to 1 in a frame destined to DS
- From DS
  - This bit is set to 1 in frame leaving the DS
- More fragment
  - Set to 1 if more fragment follow this
- Retry
  - Set to 1 if this is retransmission of previous frame

- Power management
  - Set to 1 if transmitting station is in sleep mode
- More data
  - Indicates station has additional data to send
- WEP
  - Set to 1 if optional wired equivalent protocol is implemented
- Order
  - Set to 1 if any data sent using strictly ordered services

IEEE 802.11 physical layer

- Physical layer of IEEE 802.11 has been issued in four stages
  - First part called simply IEEE 802.11, includes the MAC layer and three physical layer specification
    - Direct sequence spread spectrum(DSSS) :
      - Operates in 2.4 GHz unlicensed band
      - Up to three non overlapping channels each with data rates are 1 or 2 Mbps can be used, each channel having BW of 5 MHz
      - Encoding scheme used is Differential binary phase sift keying (DBPSK) and Differential quadrature phase sift keying (DQPSK) for 1 and 2 Mbps data rate respectively
      - Uses 11 chip barker sequence where each binary 1 is mapped into sequence {+-++-+++---} and each binary 0 is mapped into the sequence {-+--+---+++}

- Frequency hopping spread spectrum(FHSS):
  - Make use of multiple 1 MHz channel with signal hopping from one channel to another at a hop rate of 2.5 hops per second
  - Hopping is done based on pn sequence
  - Modulation scheme used is 2-level and 4-level gaussian FSK for 1 and 2 Mbps data rates respectively
- Infrared
  - This scheme is omni-directional
  - Range : 20m
  - Modulation scheme used is 16-PPM (pulse position modulation)

- Second part called IEEE 802.11a

  - operates in the 5 GHz UNNI (universal national information infrastructure band) at data rates up to 54 Mbps.
  - UNNI band is divided into three parts
    - UNNI 1 band : for indoor use
    - UNNI 2 band : for either indoor or outdoor use
    - UNNI 3 band : for outdoor
  - Uses OFDM (orthogonal frequency division multiplexing)
  - System can use up to 48 subcarriers each with a spacing 0.3125 MHz that are modulated using BPSK, QPSK, 16-QAM OR 64-QAM
  - A convolution code at a rate of ½, 2/3, ¾ is used to provide forward error correction

- Third part is IEEE 802.11b
  - operates in 2.4 GHz band at 5.5 and 11 Mbps.
  - It is extension to IEEE 802.11 DSSS scheme
  - Chipping rate is 11 MHz
  - Modulation scheme used is complementary code keying
- Fort part is IEEE 802.11g
  - operates in 2.4GHz band at 54 Mbps
  - It is extension to IEEE 802.11b
  - Compatible to IEEE 802.11b
  - It provides a wide array of data rates and modulation schemes options

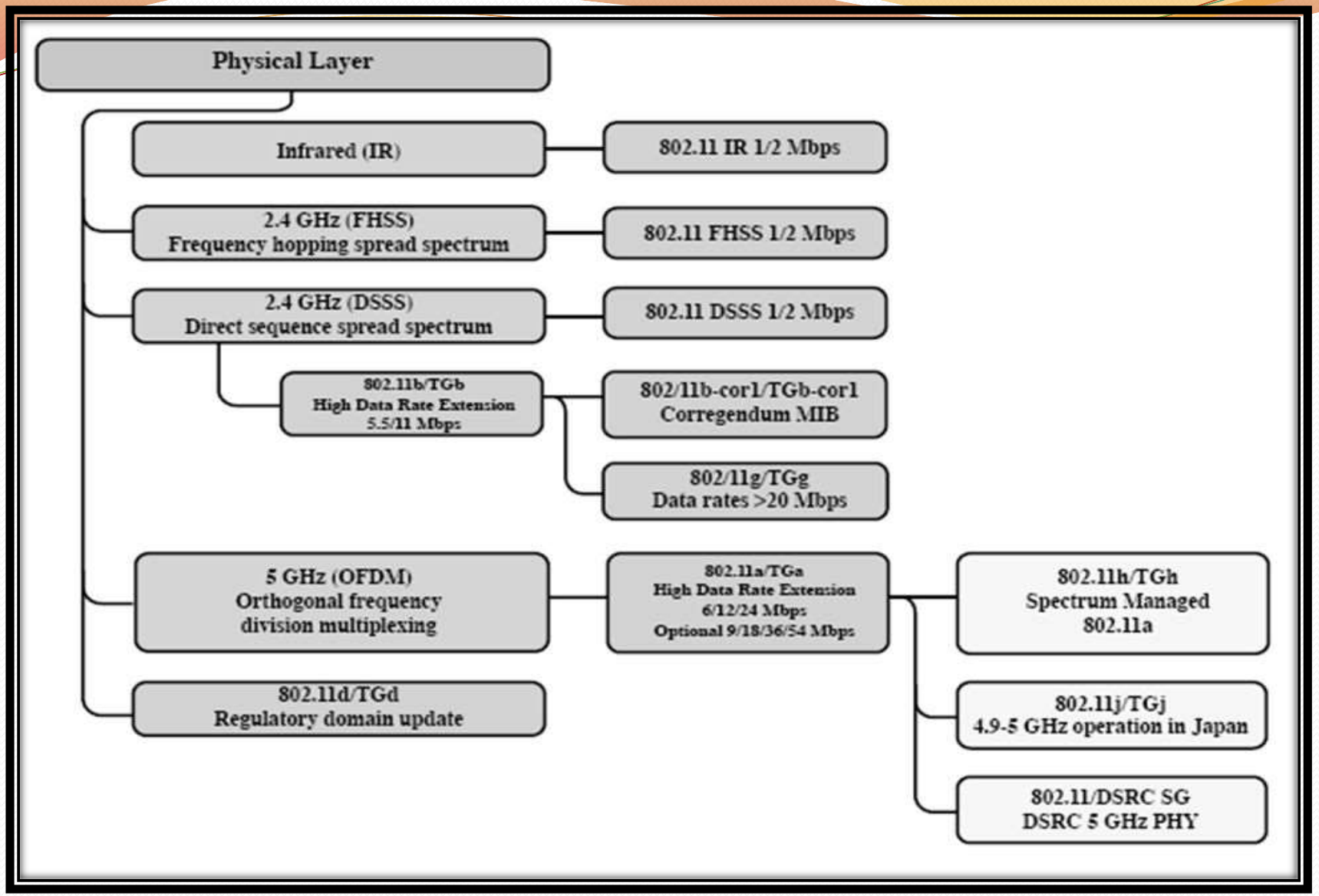


Fig : IEEE 802.11 activities- physical layer

IEEE 802.11 Physical layer standards

Standard	Date issued	Available bandwidth (MHz)	Unlicensed frequency of operation (MHz)	No. of nonoverlapping channels *	Data rate per channel (Mbps)	Compatibility
802.11	1997	83.5	2.4 to 2.4835 DSSS, FHSS	3 indoor or outdoor	1, 2	802.11
802.11a	1999	300	5.15 to 5.35 OFDM (orthogonal frequency division multiplexing) 5.725 to 5.825 OFDM	4 indoor 4 indoor or outdoor 4 outdoor	6, 9, 12, 18, 24, 36, 48, and 54	Wi-Fi5
802.11b	1999	83.5	2.4 to 2.4835 DSSS	3 indoor or outdoor	1, 2, 5.5, and 11	Wi-Fi
802.11g	2003	83.5	2. 4 to 2.4835 DSSS, OFDM	3 indoor or outdoor	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54	Wi-Fi at 11 Mbps and below

IEEE 802.11 standards

- In addition to IEEE 802.11a , 802.11b, 802.11g some other standards which are in function are as follows
  - IEEE 802.11 c
    - Concerned with bridge operations
  - IEEE 802.11 d
    - Deals with issues related to regulatory differences in various countries
  - IEEE 802.11 e
    - Makes revision to MAC layer to improve quality of service and address some security issues
  - IEEE 802.11 f
    - Addresses issues of interoperability among access points from multiple vendors

IEEE 802.11 standards

- IEEE 802.11 h
  - Deals with spectrum and power management issues
- IEEE 802.11 i
  - Defines security and authentication mechanism at the MAC layer
- IEEE 802.11 k
  - Defines radio resource measurement enhancements to provide mechanisms to higher layer for radio and network measurements.
- IEEE 802.11 m
  - Concerned with correction of editorial and technical issues in the standards
- IEEE 802.11 n
  - Concerned to both the physical and MAC layer to improve throughput