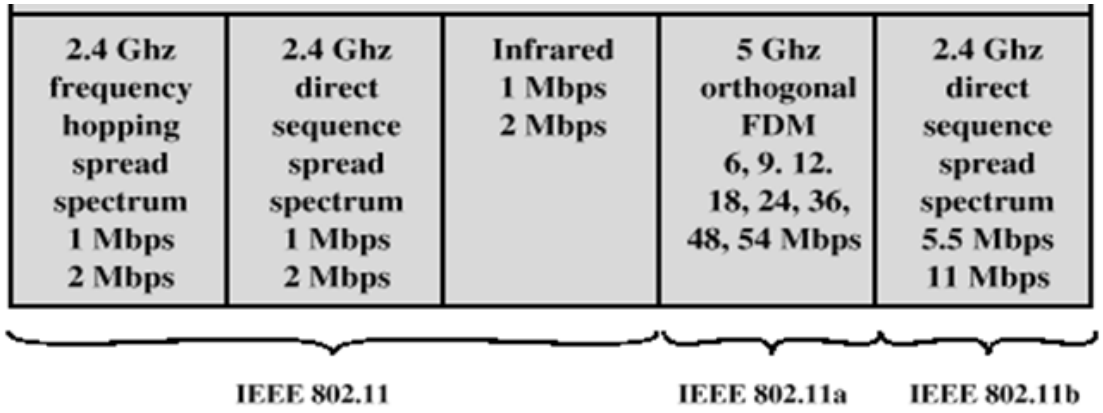
IEEE 802.11 Wireless LAN Standard

Updated: 5/10/2011

IEEE 802.11 History and Enhancements

- 802.11 is dedicated to WLAN
- The group started in 1990
- First standard that received industry support was 802.11b
  - Accepted in 1999
  - Focusing on 2.4 GHz unlicensed band
  - Initially 2 Mbit BW – relatively slow (802.11)



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	Ongoing	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	Ongoing	MAC: Enhance security and authentication mechanisms
IEEE 802.11j	Ongoing	Physical: Enhance IEEE 802.11a to conform to Japanese requirements
IEEE 802.11k	Ongoing	Radio Resource Measurement enhancements to provide interface to higher layers for radio and network measurements
IEEE 802.11m	Ongoing	Maintenance of IEEE 802.11-1999 standard with technical and editorial corrections
IEEE 802.11n	Ongoing	Physical/MAC: Enhancements to enable higher throughput

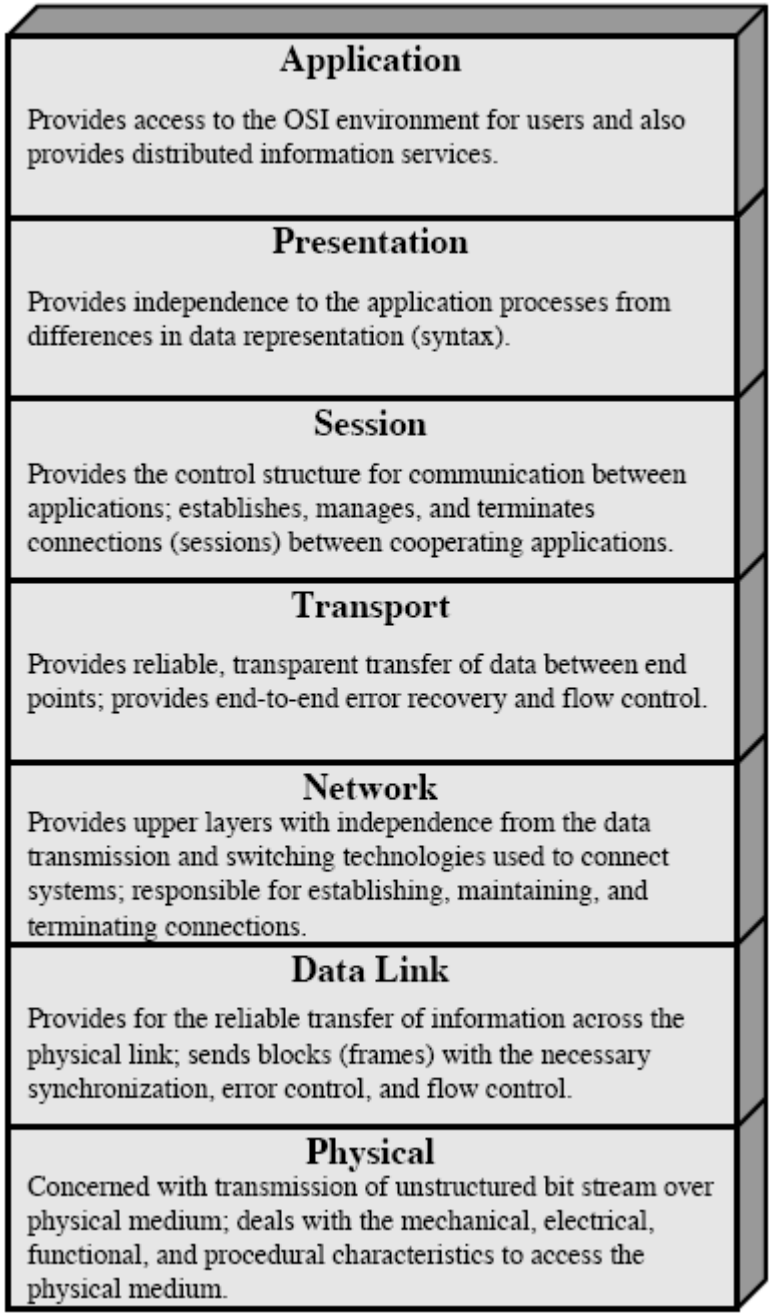
WiFi Alliance http://www.wi-fi.org/
Read the handout!

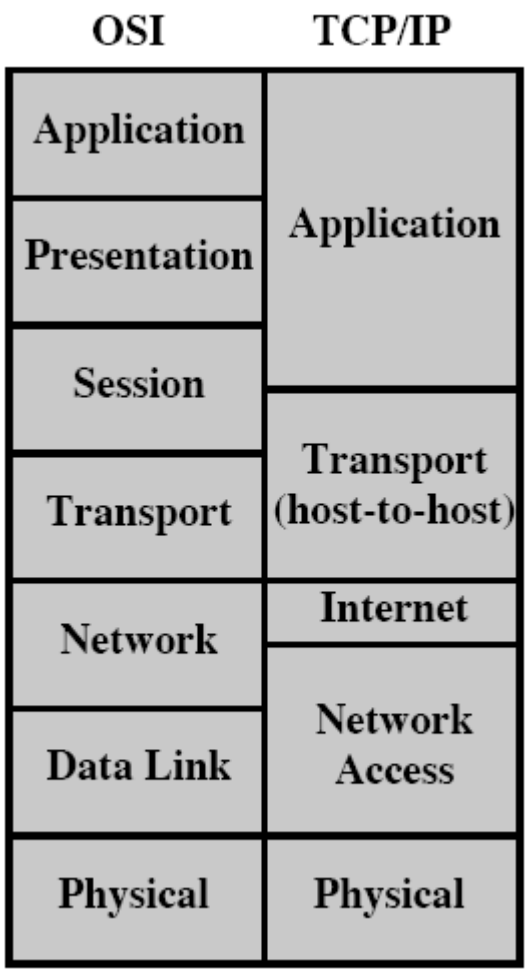
802.11 Standards

Protocol	Release Date	Op. Frequency	Throughput (Typ)	Data Rate (Max)	Modulation Technique	Range (Radius Indoor) Depends, # and type of walls	Range (Radius Outdoor) Loss includes one wall
Legacy	1997	2.4 GHz	0.9 Mbit/s	2 Mbit/s		~20 Meters	~100 Meters
802.11a	1999	5 GHz	23 Mbit/s	54 Mbit/s	OFDM	~35 Meters	~120 Meters
802.11b	1999	2.4 GHz	4.3 Mbit/s	11 Mbit/s	DSSS	~38 Meters	~140 Meters
802.11g	2003	2.4 GHz	19 Mbit/s	54 Mbit/s	OFDM	~38 Meters	~140 Meters
802.11n	June 2009[4] (est.)	2.4 GHz 5 GHz	74 Mbit/s	248 Mbit/s	MIMO	~70 Meters	~250 Meters
802.11y	June 2008[4] (est.)	3.7 GHz	23 Mbit/s	54 Mbit/s		~50 Meters	~5000 Meters

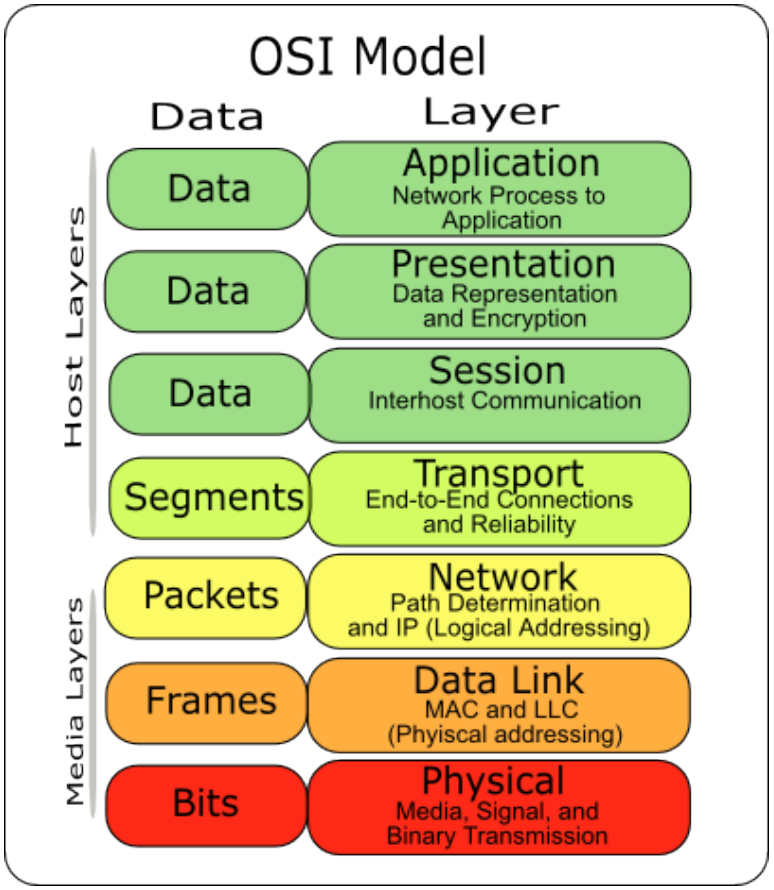
802.11ac @5GHz with 1.3Gbps Max. Data Rate!

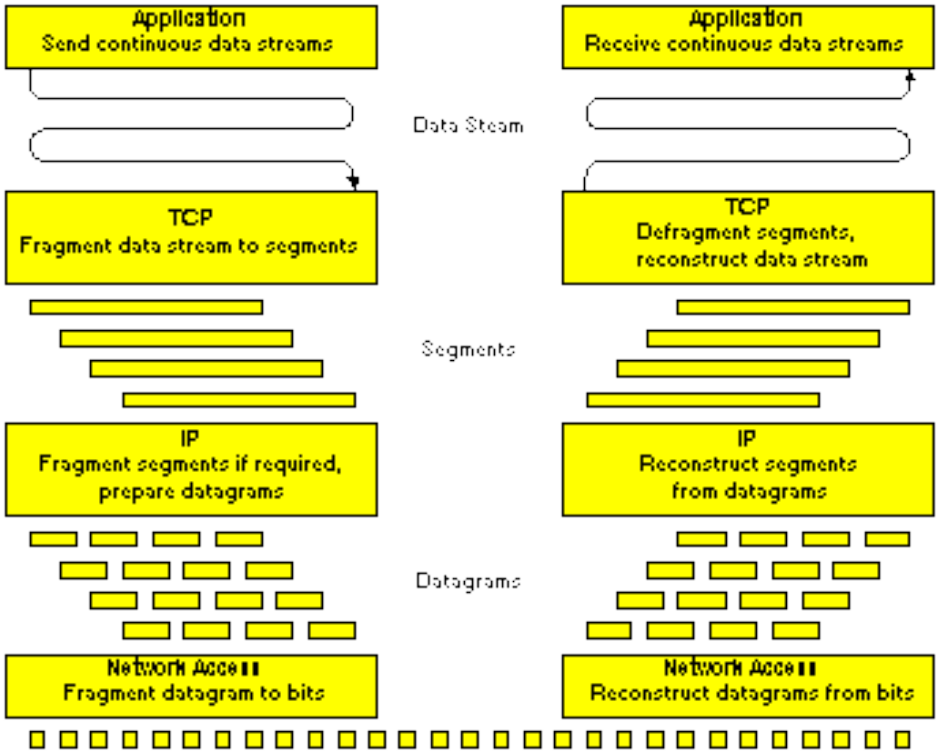
http://en.wikipedia.org/wiki/IEEE_802.11
http://www.wi-fi.org/discover-and-learn

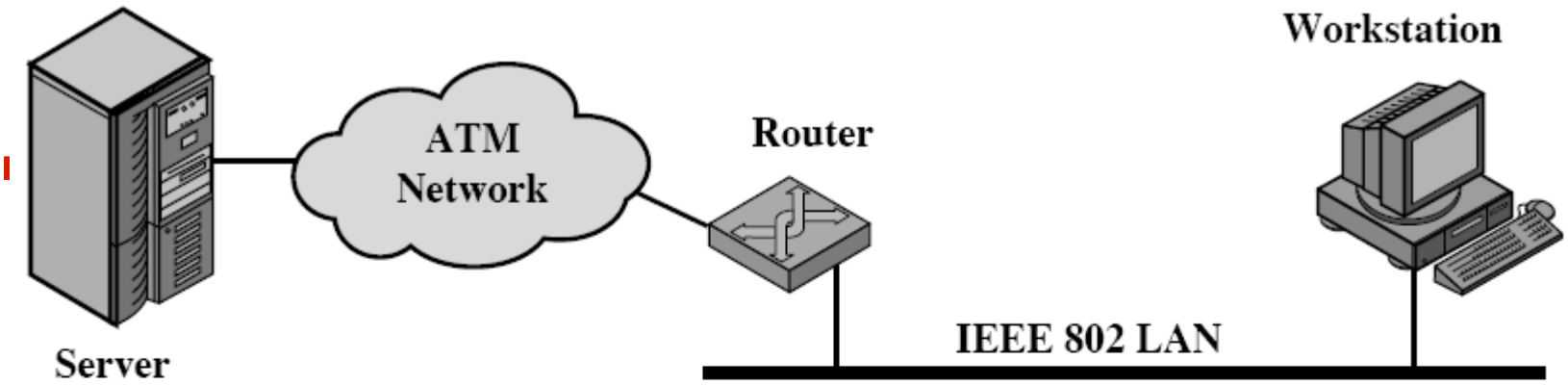

Application
Provides access to the OSI environment for users and also provides distributed information services.
Presentation
Provides independence to the application processes from differences in data representation (syntax).
Session
Provides the control structure for communication between applications; establishes, manages, and terminates connections (sessions) between cooperating applications.
Transport
Provides reliable, transparent transfer of data between end points; provides end-to-end error recovery and flow control.
Network
Provides upper layers with independence from the data transmission and switching technologies used to connect systems; responsible for establishing, maintaining, and terminating connections.
Data Link
Provides for the reliable transfer of information across the physical link; sends blocks (frames) with the necessary synchronization, error control, and flow control.
Physical
Concerned with transmission of unstructured bit stream over physical medium; deals with the mechanical, electrical, functional, and procedural characteristics to access the physical medium.

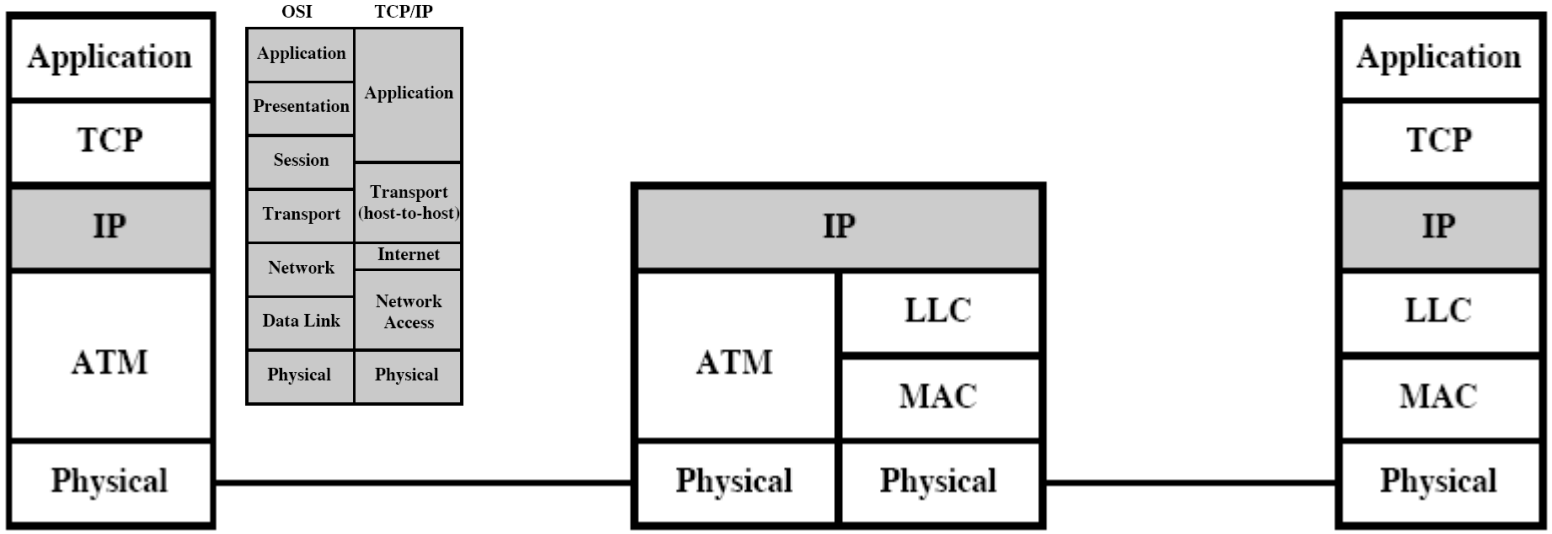

OSI
TCP/IP
Application
Presentation
Session
Transport
Network
Data Link
Physical
Application
Transport (host-to-host)
Internet
Network Access
Physical

OSI Model


OSI Model
Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation and Encryption
Data
Session
Interhost Communication
Segments
Transport
End-to-End Connections and Reliability
Packets
Network
Path Determination and IP (Logical Addressing)
Frames
Data Link
MAC and LLC (Phyiscal addressing)
Bits
Physical
Media, Signal, and Binary Transmission


Application
Send continuous data streams
Application
Receive continuous data streams
Data Steam
TCP
Fragment data stream to segments
TCP
Defragment segments, reconstruct data stream
Segments
IP
Fragment segments if required, prepare datagrams
IP
Reconstruct segments from datagrams
Datagrams
Network Acce
Fragment datagram to bits
Network Acce
Reconstruct datagrams from bits


Workstation
ATM
Network
Router
Server
IEEE 802 LAN


Application
TCP
IP
ATM
Physical
OSI
TCP/IP
Application
Presentation
Session
Transport
Network
Data Link
Physical
Application
Transport
(host-to-host)
Internet
Network
Access
Physical
IP
ATM
LLC
MAC
Physical
Physical
Application
TCP
IP
LLC
MAC
Physical

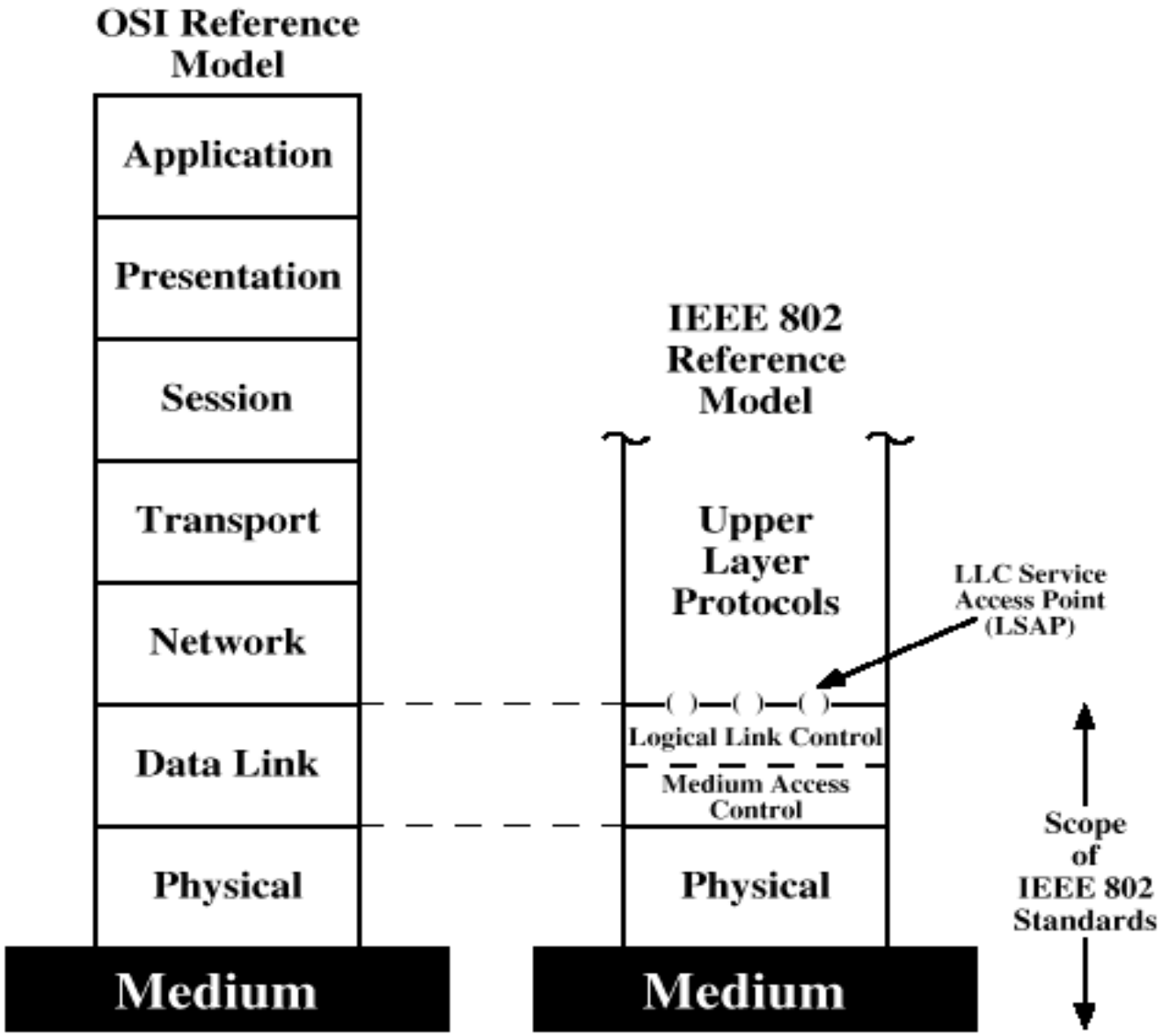


Figure 14.1 IEEE 802 Protocol Layers Compared to OSI Model

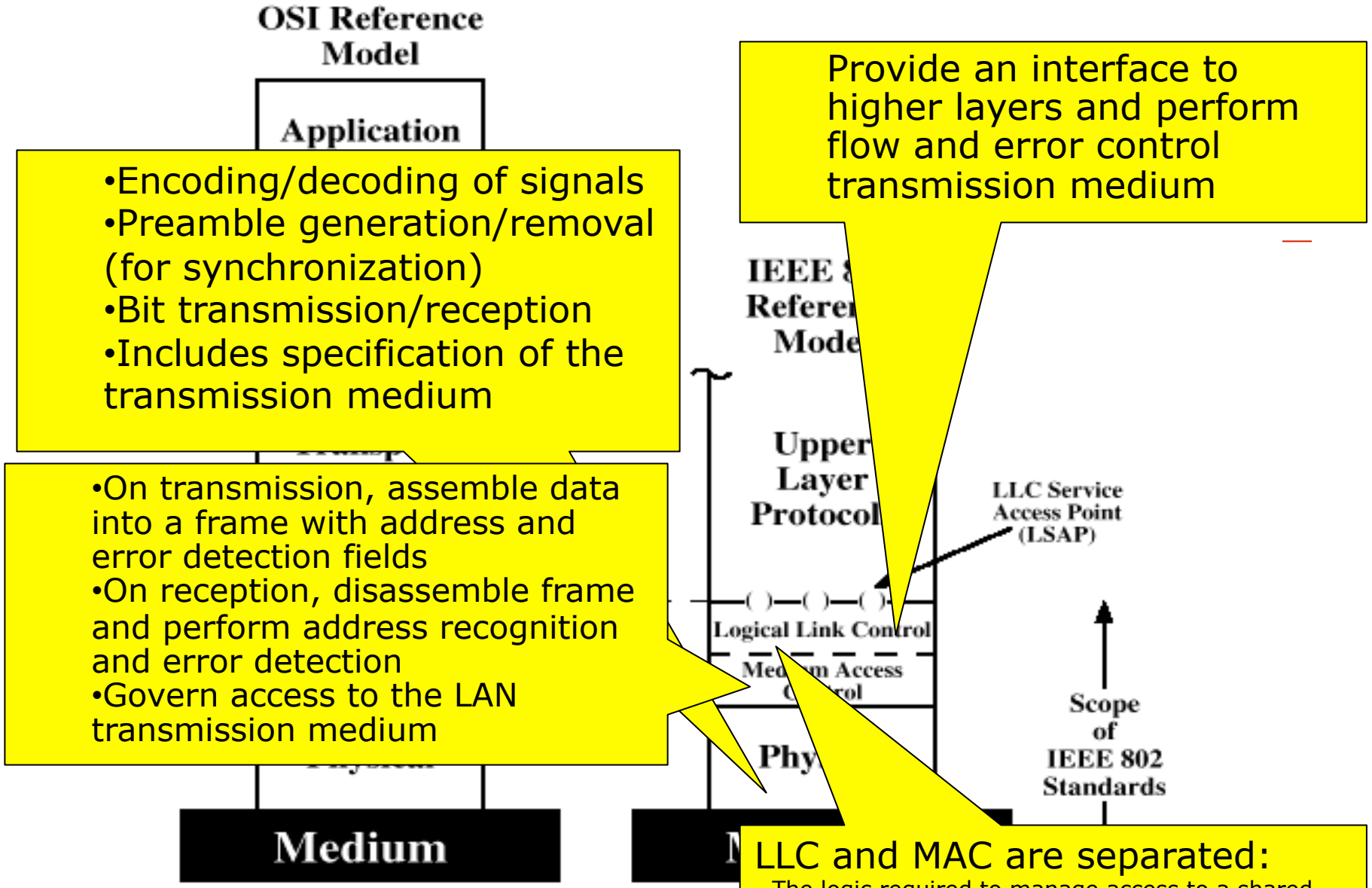


Figure 14.1 IEEE 802 Protocol Laye

Protocol Architecture

- Functions of physical layer:
  - Encoding/decoding of signals
  - Preamble generation/removal (for synchronization)
  - Bit transmission/reception
  - Includes specification of the transmission medium

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 - PRIORITY
- Destination MAC address
  - Destination physical attachment point
- Source MAC address
  - Source physical attachment point
- CRC
  - Cyclic redundancy check
  - Error-detecting code

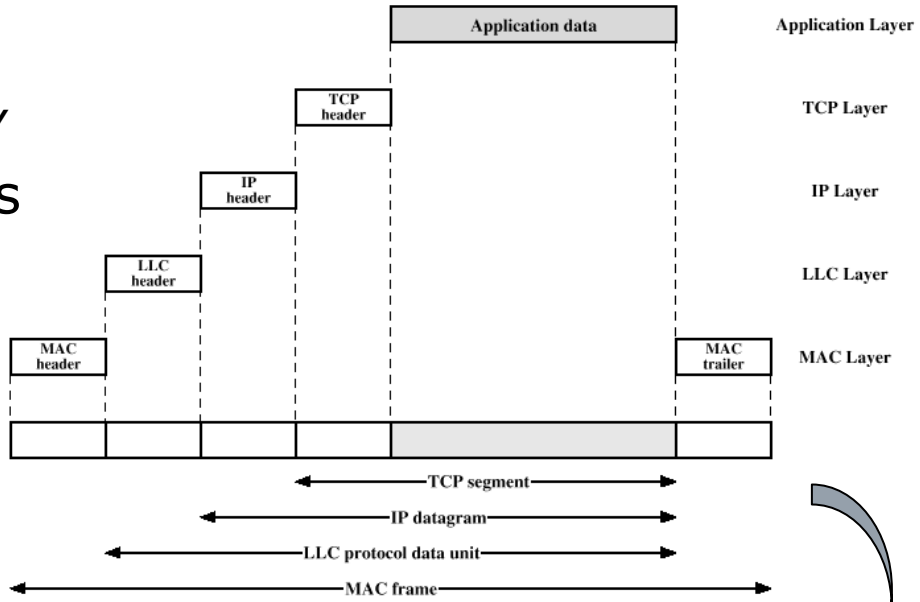
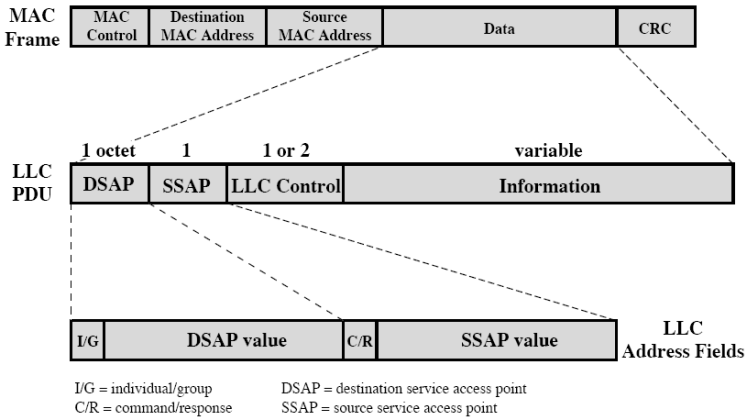


Figure 14.2 IEEE 802 Protocols in Context

MAC is responsible for detecting errors and discarding frames with errors – Frames with no errors are sent to the LLC layer

Logical Link Control

- LLC is in charge of ensuring transmission of a link-level PDU (Protocol Data Unit) between end-to-end stations
  - No intermediate node in between
- Characteristics of LLC **not** shared by other link control protocols:
  - Must support multiaccess, shared-medium nature of the link
  - Relieved of some details of link access by MAC layer



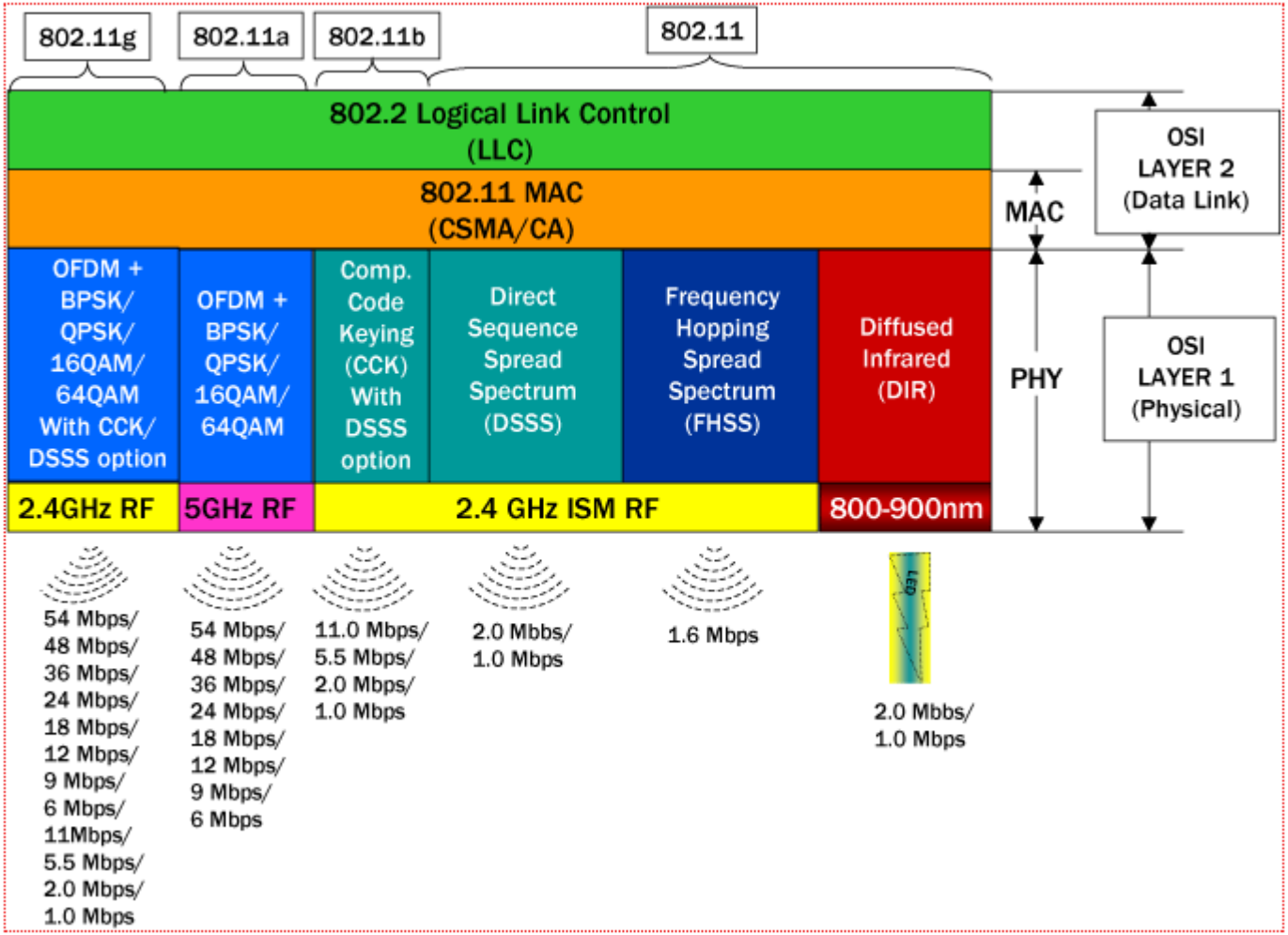
Note: SAP is the user address (service access point) / OSI terminology

LLC Services

- Basic services:
  - Provide mechanisms for addressing stations across the medium
- Services types:
  - Unacknowledged connectionless service
    - Datagram-style 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

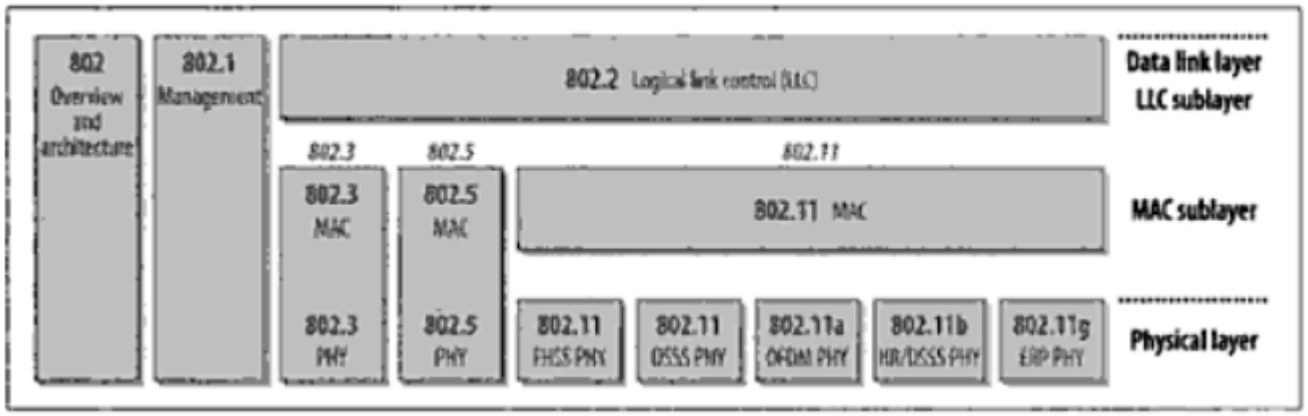
Skip LLC Protocol Section!

802.11 Architecture



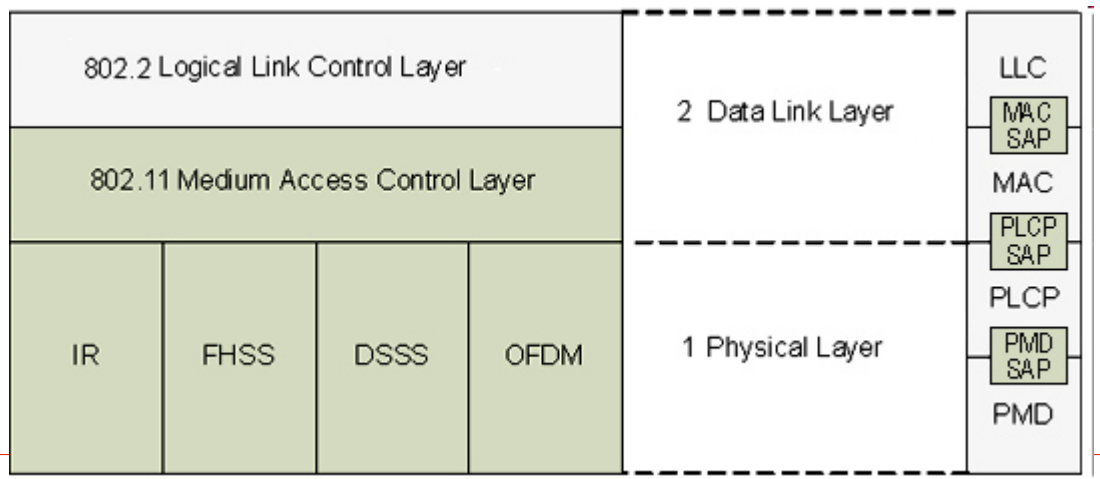
Related Sub-layers

- 802.3 CSMA/CS related to Ethernet (star specification)
- 802.5 Token Ring specifications LAN
- 802.1 Management (Virtual LAN – 802.1q / Bridging 802.1d)



802.11 Sub-layers

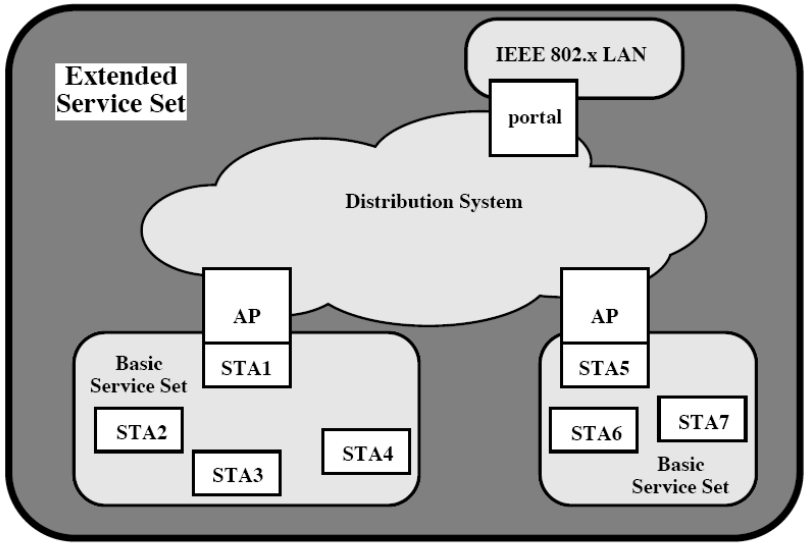
- The physical layer is divided into two sub layers:
  - PLCP: Physical Layer Convergence Protocol – glues between MAC and Radio transmission; maps the MAC frame and prepares it for transmission by adding appropriate and header
  - PMD: Physical Medium Dependent – transmits the mapped framed in the air through the antenna



Service Access Point

Basic Terminologies – Four Physical Components

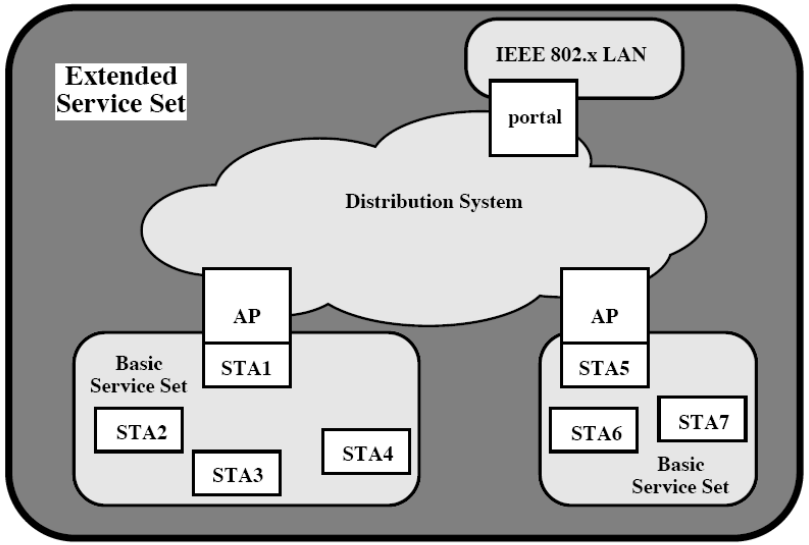
- Distribution system: backbone system used to relay frames between AP or between the AP and the backbone
- Access Point: Performs bridging function (wireless-to-wired)
- Medium: IR or RF physical medium
- Stations: End users



Figure

IEEE 802.11 Architecture

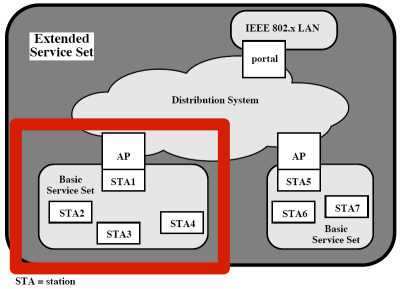
- Distribution system (DS)
- Access point (AP)
- Basic service set (BSS)
  - Stations competing for access to shared wireless medium
  - Isolated or connected to backbone DS through AP
  - Smallest building block
- Extended service set



STA = station

- Two or more basic service sets interconnected by DS
- Requires a backbone (Ethernet or VLAN)

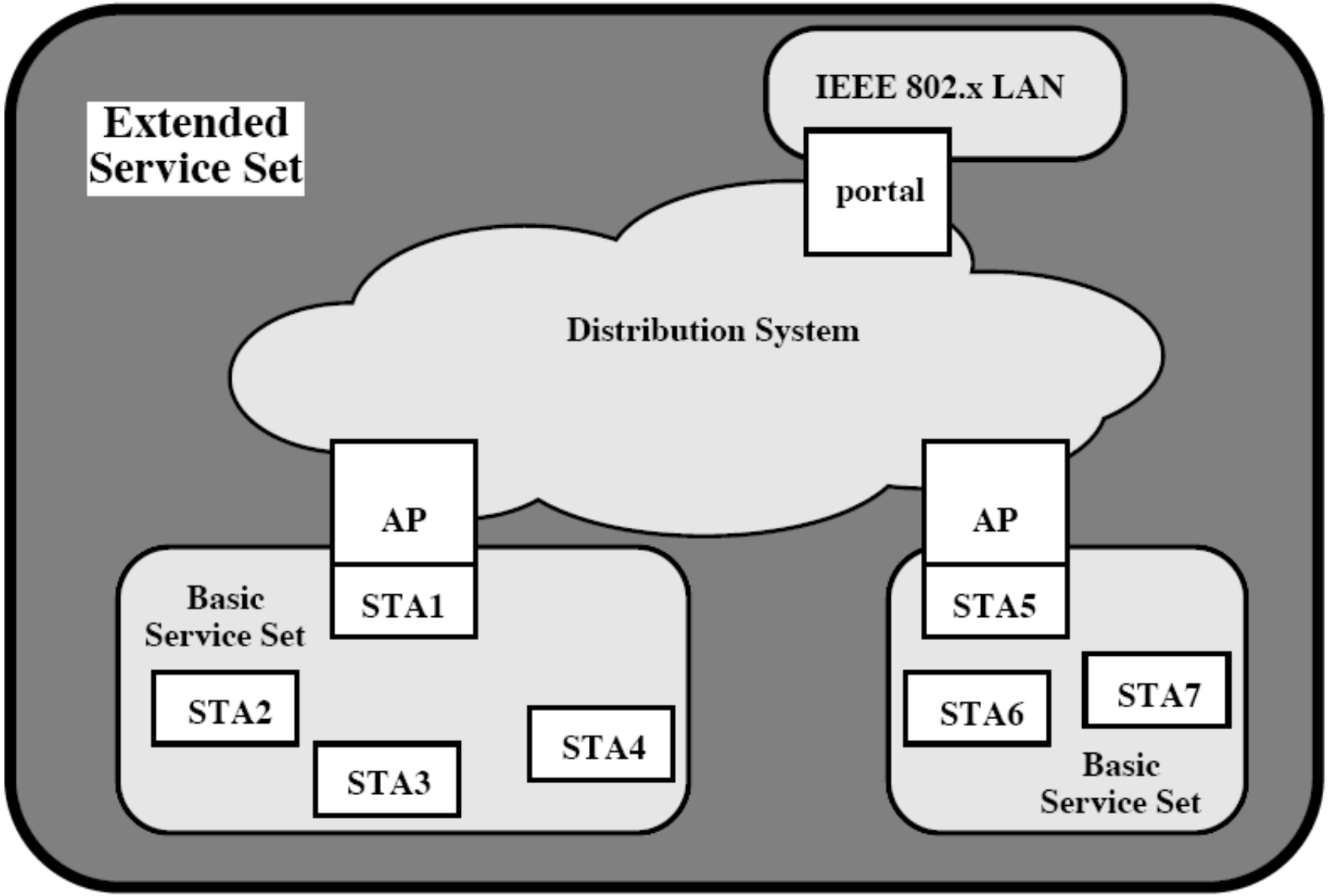
IEEE 802.11 Architecture IBSS Structure



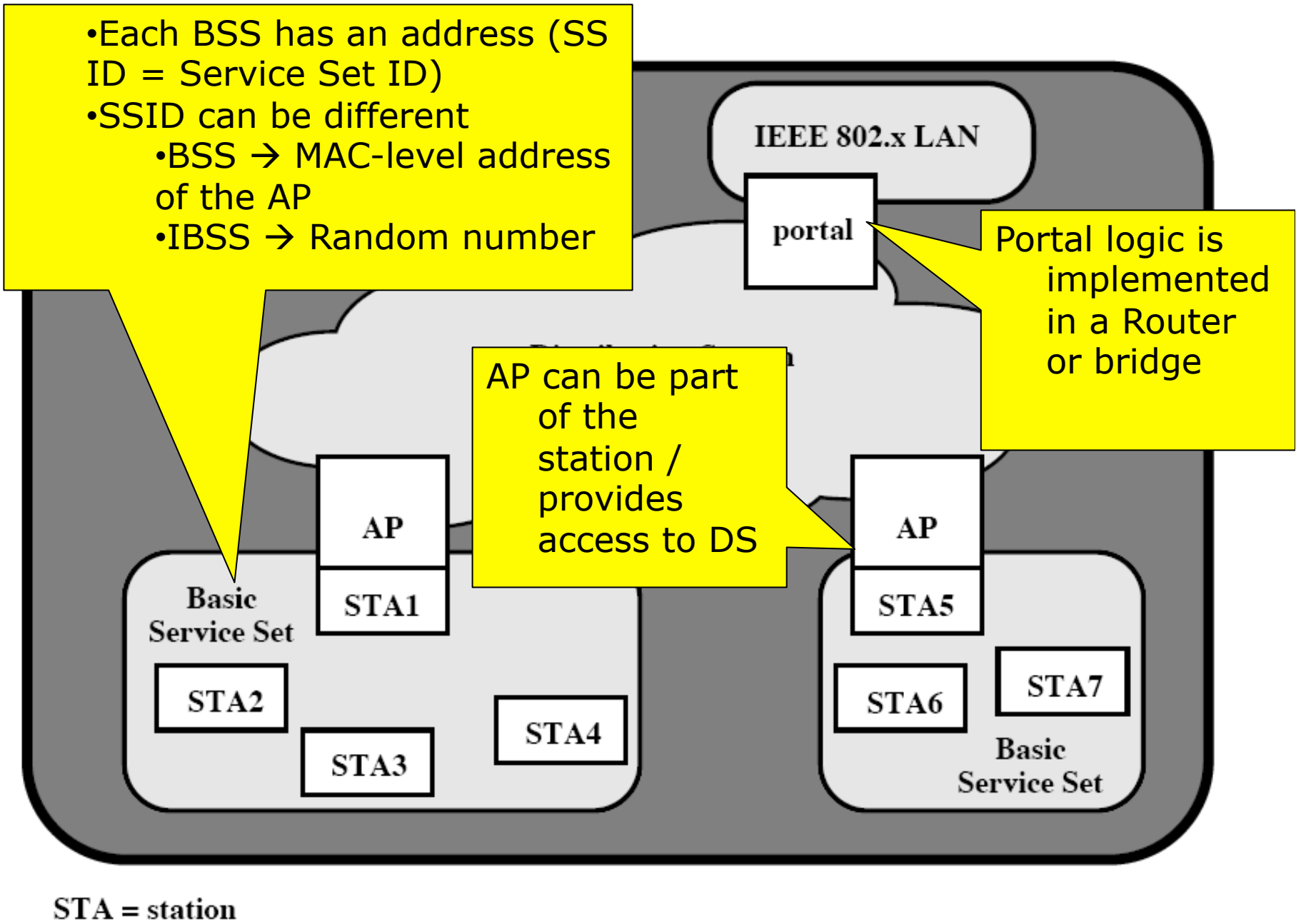
- Independent Basic Service Set (IBSS)
  - Multiple independent stations (STA) can communicate within the boundary of a cell
  - We refer to the cell as Basic Service Set
  - Often P2P
  - Used in single meetings with short duration
- In a geographical area we can have multiple IBSS
- Within IBSS the relation between STA and BSS is dynamic
  - STA moves / dies (temporary associating)
- We refer to IBSS structure as a peer-to-peer or ad-hoc wireless network

IEEE 802.11 Architecture - Networks

- Infrastructure Networks
  - All connections go through the AP
  - Nodes have to associate themselves to the AP
- Independent Networks
  - No access points (P2P)


Extended
Service Set
IEEE 802.x LAN
portal
Distribution System
AP
AP
Basic
Service Set
STA1
STA5
STA2
STA3
STA4
STA6
STA7
Basic
Service Set

STA = station


•Each BSS has an address (SS ID = Service Set ID)
•SSID can be different
•BSS → MAC-level address of the AP
•IBSS → Random number
IEEE 802.x LAN
portal
Portal logic is implemented in a Router or bridge
AP can be part of the station / provides access to DS
AP
AP
STA1
STA5
Basic Service Set
STA2
STA3
STA4
STA6
STA7
Basic Service Set
STA = station

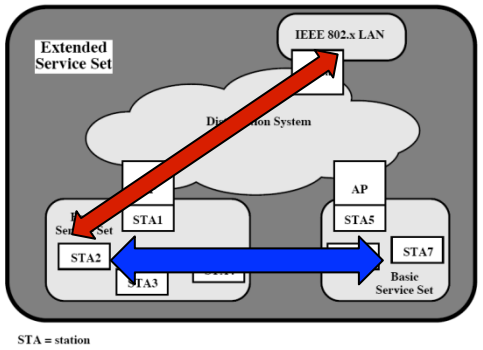
Distribution System Issues

- How AP communicates with one another to tell about their associated stations
  - Passing association information (using Inter-access Point Protocol – IAPP)
  - No real standard
- How to manage overlapping BSS in an ESS
  - Multiple 802.11 networks can coexist
- How to manage moving user from one BSS to another
- How to distinguish between overlapping BSS and an IBSS

802.11 Network Operation

- The network operation can be defined by the services it provides
  - Nine different services
- Services can be defined from STA or DS point of view
  - STA: Station and AP connections
  - **DS Services**: Connecting AP to DS

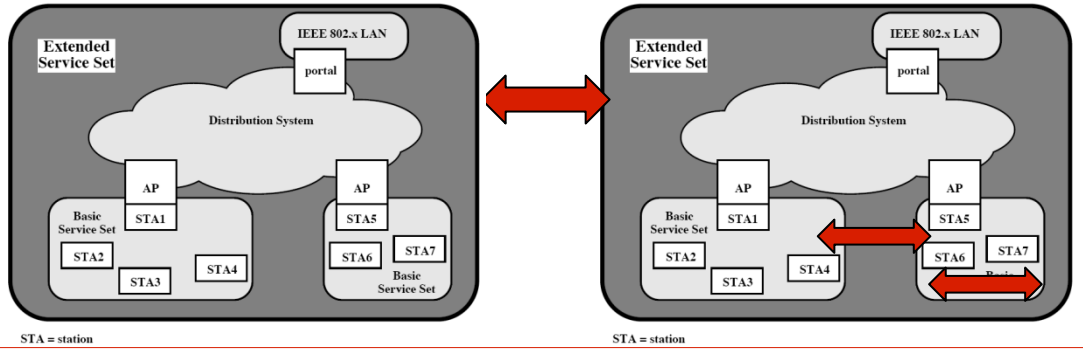
802.11 Services



- Typically divided into two types (in terms of distribution of messages within a DS)
  - Distribution service
    - Used to exchange MAC frames from station in one BSS to station in another BSS
    - E.g., Keeping track of mobile nodes and delivering to right node
  - Integration service
    - Transfer of data between station on IEEE 802.11 LAN and station on integrated IEEE 802.x LAN

What If Stations Are Moving?

- 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
      - Through association and re-association
  - ESS transition
    - Station moving from BSS in one ESS to BSS within another ESS
      - This seamless transition is often provided by Mobile IP



Service Types

- Distribution service (exchange between BSS)
  - **Association**
  - **Re-association**
  - **Disassociation**
  - **Authentication**
  - **De-authentication**
  - **Privacy**
- Integration service (Between Gateways)
  - Distribution
  - Integration
  - MSDU (MAC Service Data Units)

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 / updates location
  - Of due to temporary disconnection
- Disassociation
  - Association termination notice from station or AP

Access and Privacy Services

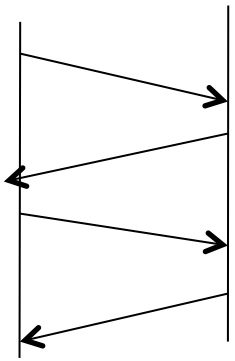
- Authentication
  - Establishes identity of stations to each other
  - Use name or public key
  - Not mandatory by standards
- Deathentication
  - Invoked when existing authentication is terminated
- Privacy
  - Prevents message contents from being read by unintended recipient
- MSDU Delivery
  - MAC Service Data Unit Delivery
  - Responsible to ensure delivery of data to the STA

IEEE 802.11 Medium Access Control

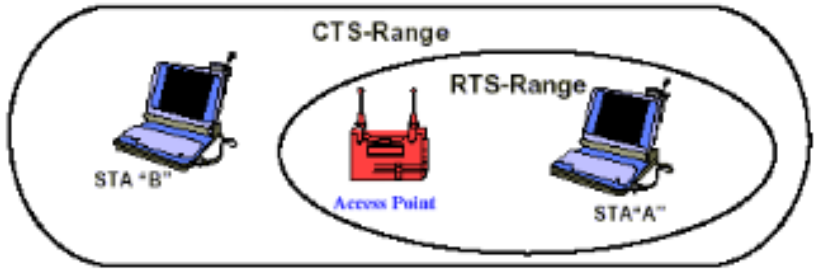
- The key to 802.11 is understanding the MAC
  - Ethernet style
  - CSMA/CA – not so much /CD which takes too much overhead)
  - Supporting different media
  - Typically half-duplex connection
- MAC challenges
  - Link quality (unpredictable in wireless)
  - Hidden node problem (not seeing unreachable nodes)
  - Simultaneous transmission of hidden nodes→ collision
- MAC layer covers three functional areas:
  - Reliable data delivery
  - Access control
  - Security

Reliable Data Delivery

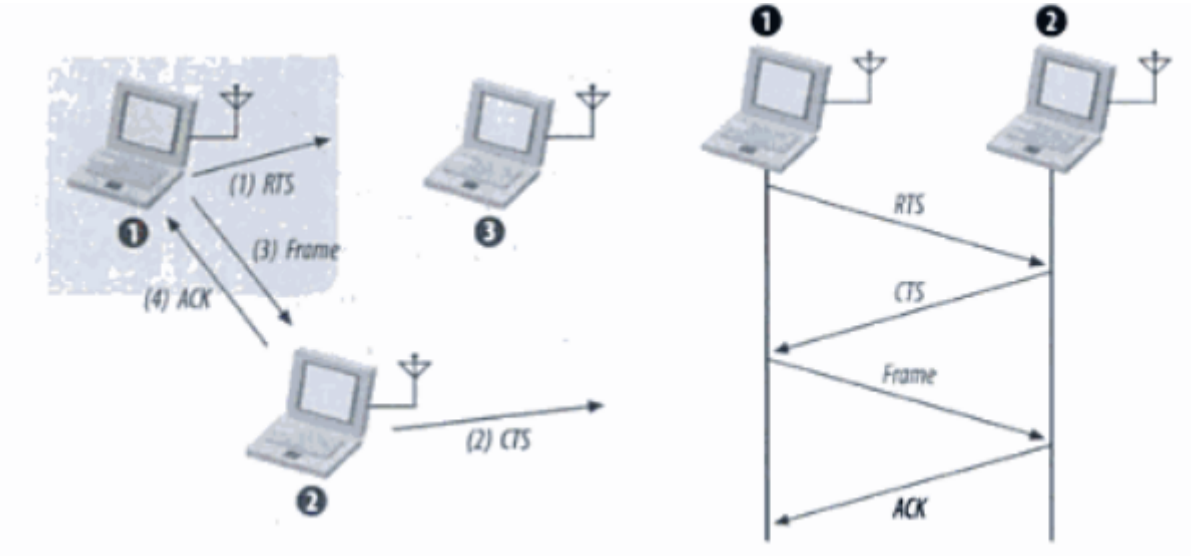
- More efficient to deal with errors at the MAC level than higher layer (such as TCP – but it is too slow)
- (Two) Frame exchange protocol
  - Source station transmits data
  - Destination responds with acknowledgment (ACK)
  - If source doesn't receive ACK, it retransmits frame
- Four frame exchange
  - Source issues request to send (RTS)
  - Destination responds with clear to send (CTS)
  - Source transmits data
  - Destination responds with ACK



Four Frame Exchange (RTS/CTS



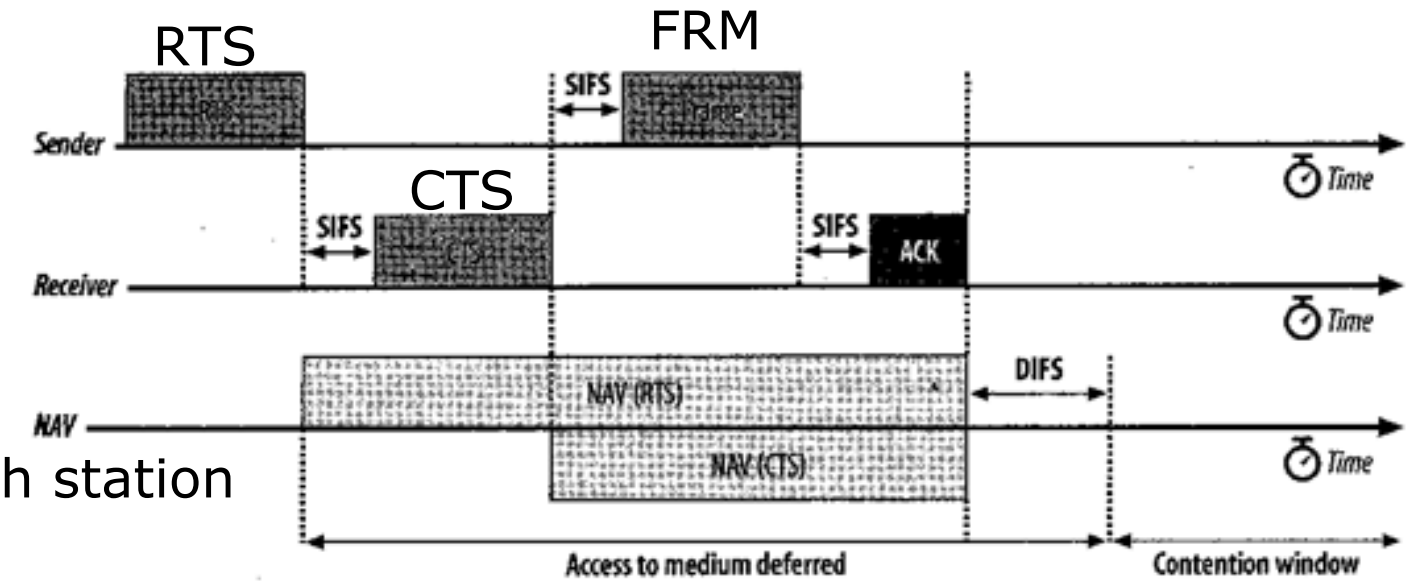
- Four frame exchange can resolve the hidden node problem by silencing them via CTS
- Often is required for high capacity networks with high collision



Medium Access

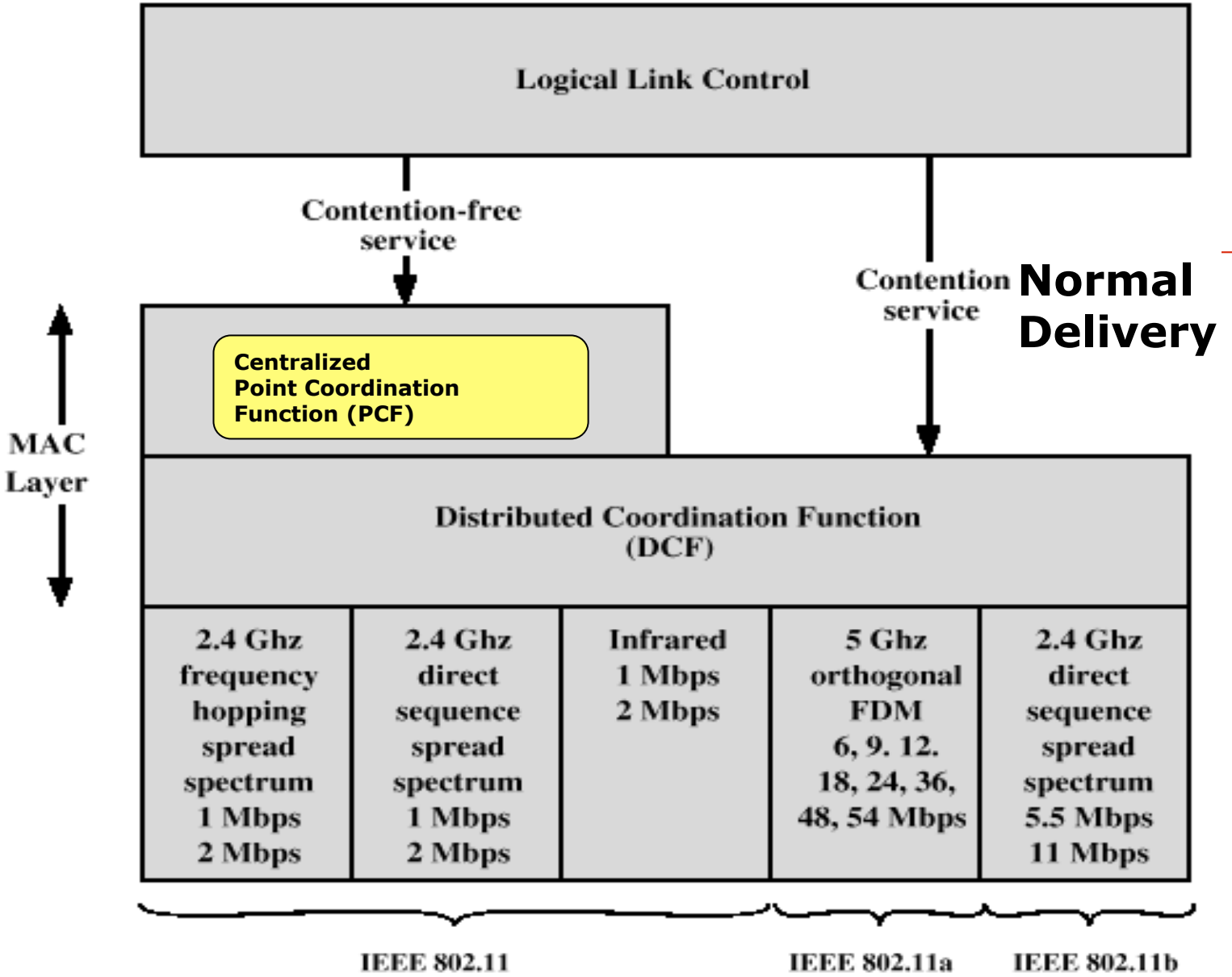
- Access to the wireless medium controlled by coordination functions
  - DCF (distributed coordination function)
    - Check the link before transmission
    - Ethernet-like - Based on CSMA with backoff
    - Used in IBSS
  - PCF (central coordination function)
    - Not widely used
    - A point of coordination is assumed – central station is assigned to coordinate access)
    - Ensures contention-free transmission
- 802.11 provides two ways to avoid collision
  - Physical detection of the medium – hardware-based sensing)
  - Virtual – using network allocation vetor (NAV) / basically use of various timers

Network allocation network (virtual) (NAV)



At each station

SIFS=Short interframe space
PIFS=Point Coordination Function IFS
DIFS=Distributed Coordinated Function IFS



802.11 Protocol Architecture

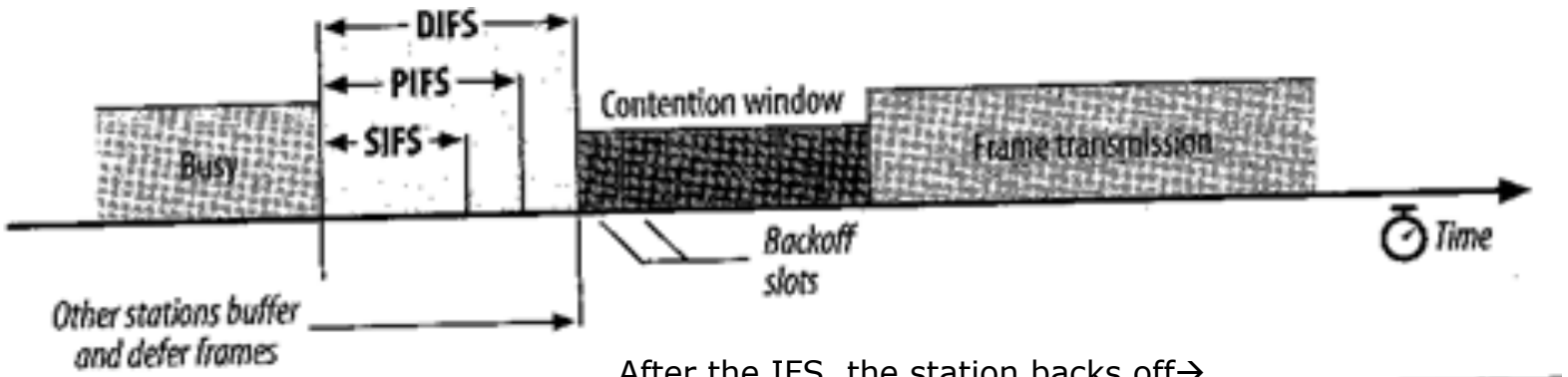
Carrier Sense Multiple Access / Collision Avoidance or Detection

- CSMA/CA belongs to a class of protocols called multiple access methods
- In CSMA, a station wishing to transmit has to first listen to the channel for a predetermined amount of time so as to check for any activity on the channel
- If the channel is sensed "idle" then the station is permitted to transmit
- If the channel is sensed as "busy" the station has to defer its transmission
- This is the essence of both CSMA/CA and CSMA/CD
- In CSMA/CA once the channel is clear, a station sends a signal telling all other stations not to transmit

See reference: http://sss-mag.com/pdf/802_11tut.pdf

Contention Window

Channel busy →
defer the transmission; keep monitoring



After the IFS, the station backs off→
If the medium still idle → transmit

IFS=interframe space

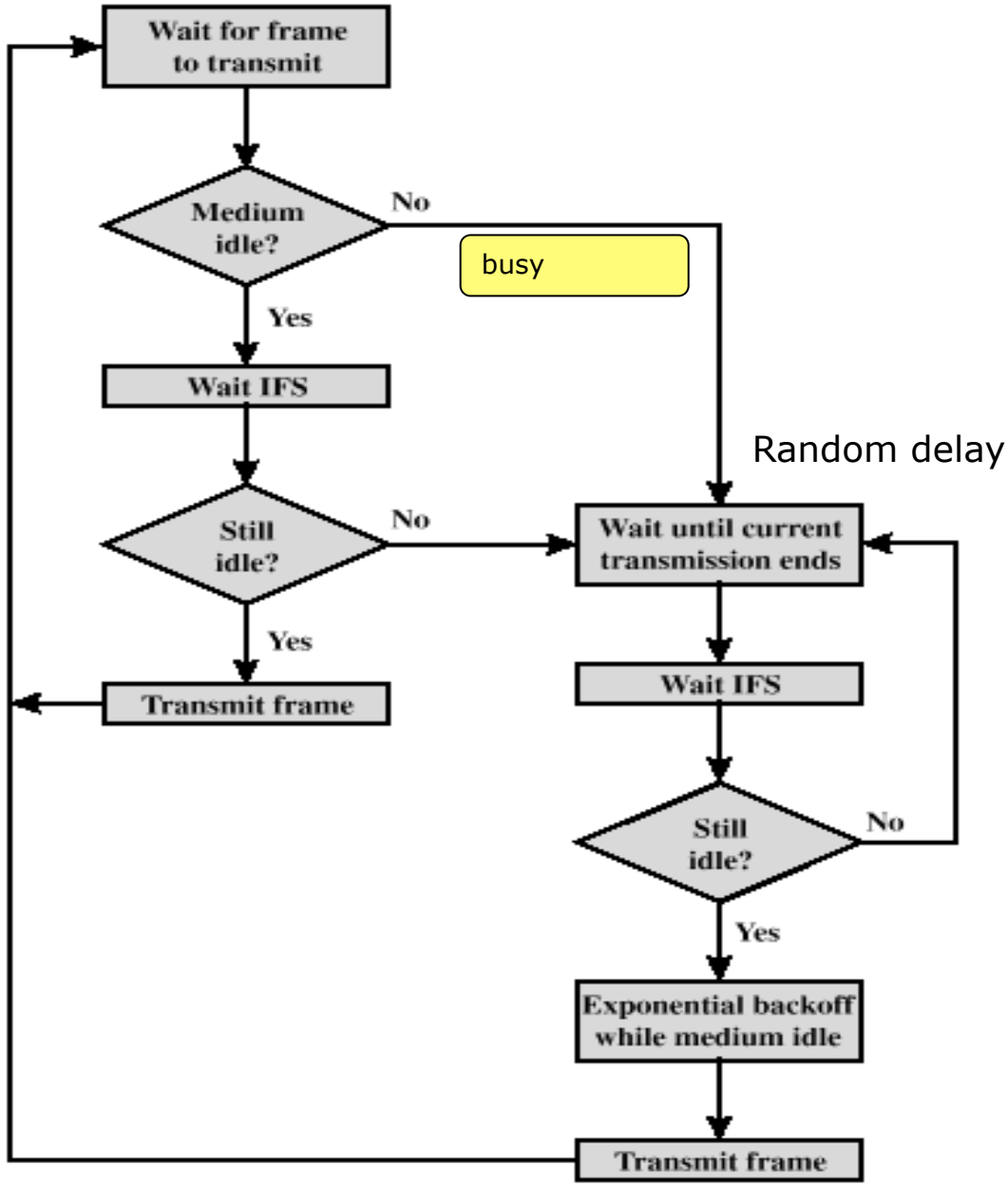


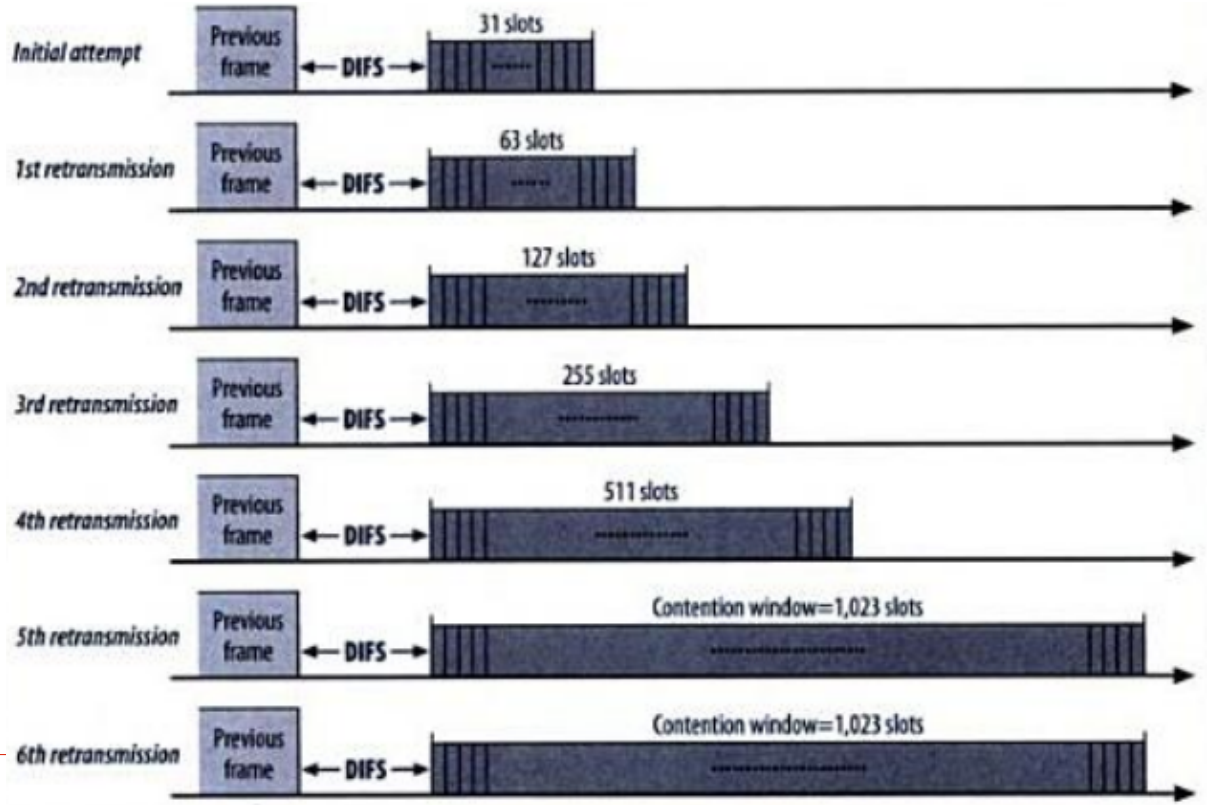
Figure 14.6 IEEE 802.11 Medium Access Control Logic

Applications of Different Waiting Times (Priority)

- SIFS
  - Between Data and its ACK (PDU is divided into multiple MAC frames)
  - Between RTS and CTS
  - Between a POLL request and transmitted data
- PIFS
  - Between poll requests to different stations
- DIFS
  - Others

Binary Backoff for DSSS

-A station attempts to transmit repeatedly
-When collision occurs (absence of ACK)→
-the mean average delay is doubled



Management Operation

- Mainly to solve power, reliability, and security
- Composed of three components
  - MLME : MAC layer management entity
  - PLME : Physical layer management entity
  - SME : system management entity
- Basic Functionalities
  - Scanning
  - Authentication
  - Power conservation
  - Timing shynchronization

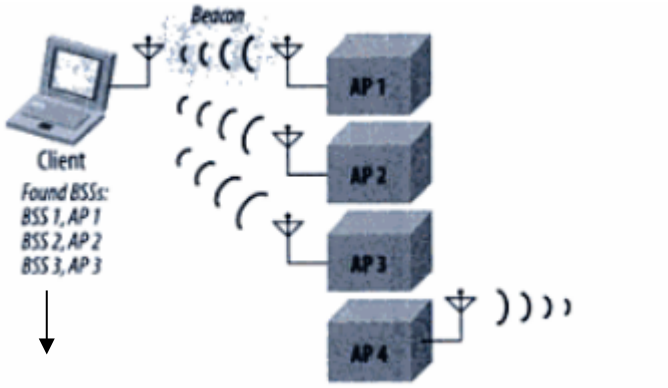
Figure

Scanning

- The process of finding the network
- Requires multiple parameters
  - BSSType – independent / infrastructure / both
  - BSSID - - individual / broadcast (anynetwork)
  - SSID – specific network name or broadcast
  - ScanType – active (transmit a Probe Request) or passive (listen)
  - ChanList – list of channel to perform scanning

Passive / Active Scanning

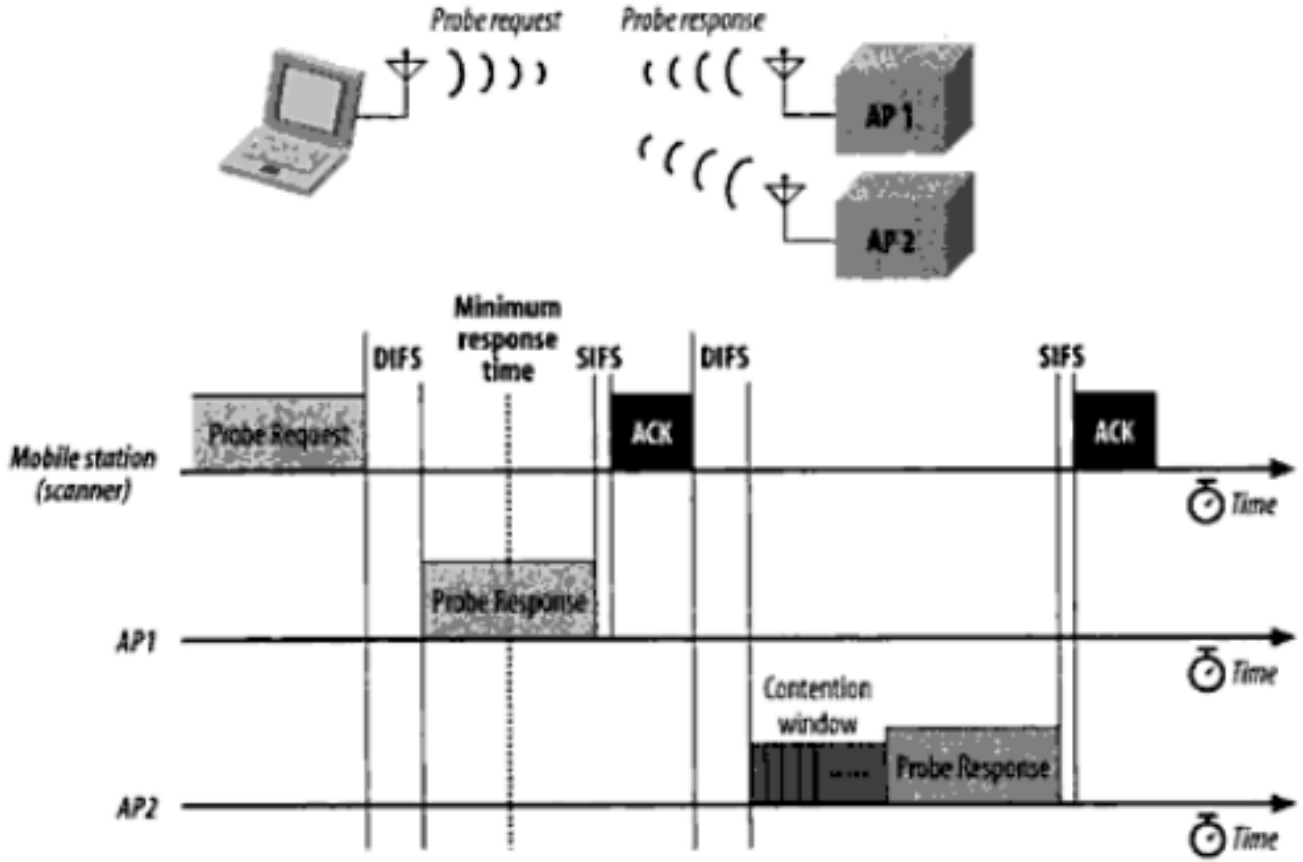
- Passive Scanning
  - Save power (not transmitting anything)
  - Typically has a ChanList to listen for transmitted BEACONs



1- Wait for beacon frame
2- check BSS information
3-Sweep from chan to chan

- Active Scanning
  - On Each designated channel a Probe Request is sent → soliciting service (like Calling FIRE!) – everyone responses
  - Search for a specific SSID by broadcasting its name

Active Scanning



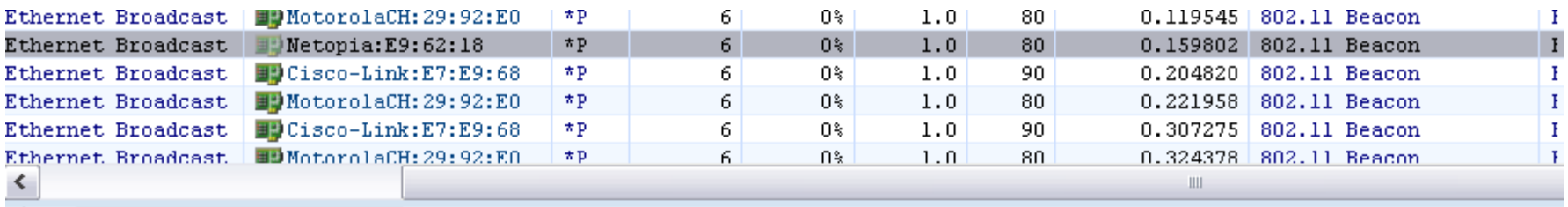
Gaining access to the channel is performed via DCF access process

Note how medium access control is implemented!

Scan Report

- Following each scan a report is generated
- The following information is acquired
  - Beacon interval (how often the BSS is sending its beacon)
  - DTIM – Delivery traffic indication map (frames indicating power management mechanism)
  - Timing Parameters - used for synchronization
  - PHY Parameter –
  - BSS Basic Rate

Example



Ethernet Broadcast	MotorolaCH:29:92:E0	*P	6	0%	1.0	80	0.119545	802.11 Beacon
Ethernet Broadcast	Netopia:E9:62:18	*P	6	0%	1.0	80	0.159802	802.11 Beacon
Ethernet Broadcast	Cisco-Link:E7:E9:68	*P	6	0%	1.0	90	0.204820	802.11 Beacon
Ethernet Broadcast	MotorolaCH:29:92:E0	*P	6	0%	1.0	80	0.221958	802.11 Beacon
Ethernet Broadcast	Cisco-Link:E7:E9:68	*P	6	0%	1.0	90	0.307275	802.11 Beacon
Ethernet Broadcast	MotorolaCH:29:92:E0	*P	6	0%	1.0	80	0.324378	802.11 Beacon

```
802.11 Management - Beacon
    Timestamp:              2538840883662  Microseconds [24-31]
    Beacon Interval:        100 [32-33]
    Capability Info:        %0000010000010001 [34-35]
                              0....... ........ Immediate Block Ack Not Allowed
                              .0...... ........ Delayed Block Ack Not Allowed
                              ..0..... ........ DSSS-OFDM is Not Allowed
                              ...0.... ........ Reserved
                              ....0... ........ APSD is not supported
                              .....1.. ........ G Mode Short Slot Time [9 microseconds]
                              ......0. ........ QoS is Not Supported
                              .......0 ........ Spectrum Mgmt Disabled
                              ........ 0....... Channel Agility Not Used
                              ........ .0...... PBCC Not Allowed
                              ........ ..0..... Short Preamble Not Allowed
                              ........ ...1.... Privacy Enabled
                              ........ ....0... CF Poll Not Requested
                              ........ .....0.. CF Not Pollable
                              ........ ......0. Not an IBSS Type Network
                              ........ .......1 ESS Type Network
    SSID
```

HOMEWORK : Read Chapter 4
Use OmniPeeK Demo Software and examine The following frames:
-Management frame in a beacon
-Probe Request Frame
-Beacon Frame
-Probe Response
-ACK frame

Joining

- STA decide on which BSS to join based on the scan report
- Joining is required to gain access to the medium
  - Before access association and authenticating is required
- Joining a BSS will be based on several parameters
  - Matching PHY
  - WEP
  - Negotiating timers, beacon interval, and power saving mechanism

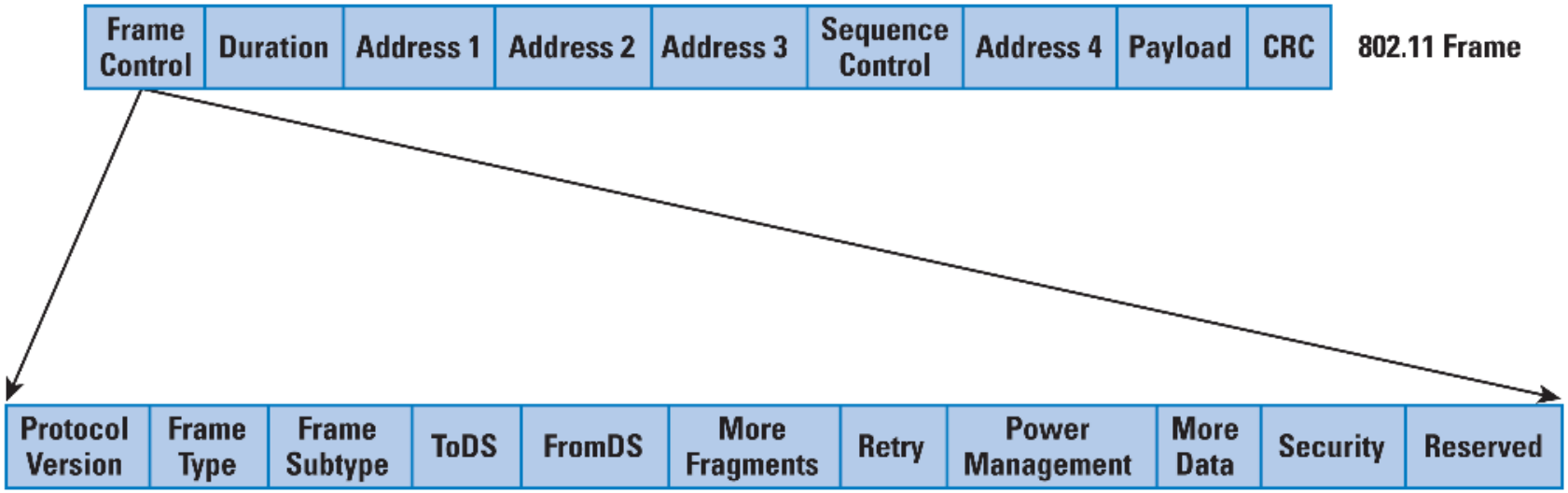
Authentication

- Authentication is initiated by the STA
- 802.11 Authentication
  - Open System
    - No identify verification (Going to bank with no id!)
  - Shared-Key
    - WEP between both stations
      - One way authentication
      - The AP is not authenticated by the station → a rogue AP can attack the station
    - Public Key authentication - 802.1x

Framing

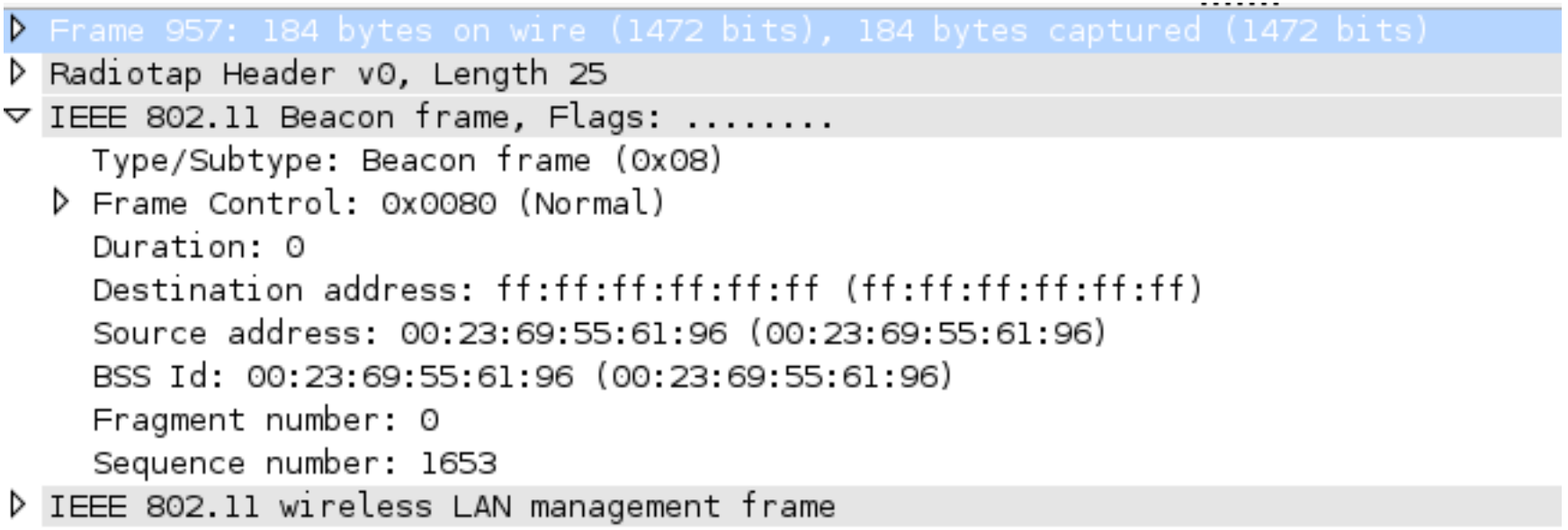
- MAC Frame Types
  - Date Frame
  - Control Frame
  - Management Frame
- Examples
  - IBSS data frame
  - Data Frame from AP
  - Data Frame to AP
  - RTS Frame
  - CTS Frame
  - ACK Frame
  - Management Frame
  - Etc.

Frame


Frame Control
Duration
Address 1
Address 2
Address 3
Sequence Control
Address 4
Payload
CRC
802.11 Frame
Protocol Version
Frame Type
Frame Subtype
ToDS
FromDS
More Fragments
Retry
Power Management
More Data
Security
Reserved

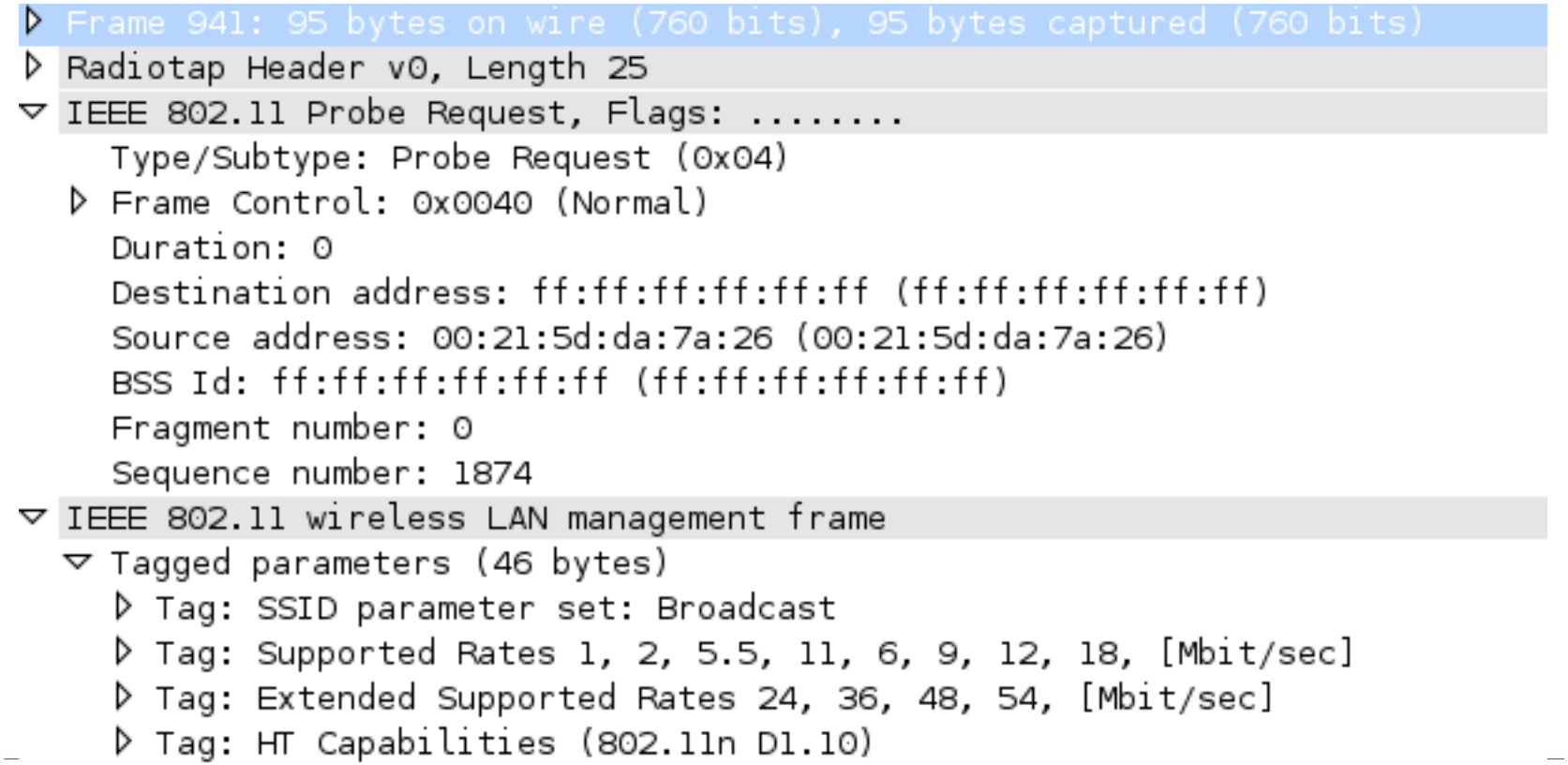
Frame Examples (Beacon Frame)

Transmitted periodically to identify and locate a BSS



Frame Example – Probe Request

Used by the station to obtain information about another stations or AP



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	Ongoing	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	Ongoing	MAC: Enhance security and authentication mechanisms
IEEE 802.11j	Ongoing	Physical: Enhance IEEE 802.11a to conform to Japanese requirements
IEEE 802.11k	Ongoing	Radio Resource Measurement enhancements to provide interface to higher layers for radio and network measurements
IEEE 802.11m	Ongoing	Maintenance of IEEE 802.11-1999 standard with technical and editorial corrections
IEEE 802.11n	Ongoing	Physical/MAC: Enhancements to enable higher throughput

WiFi Alliance http://www.wi-fi.org/

References

- Good tutorials about Spread Spectrum and MAC In 802.11
  - http://grouper.ieee.org/groups/802/11/Tutorial/index.html
- Google Book on 802.11:
  - http://books.google.com/books?id=TLUVG9yoGx4C&dq=802.11+Wireless+Gast&printsec=frontcover&source=bn&hl=en&ei=_a7ZS5HFDZD-sgPJm7yVAQ&sa=X&oi=book_result&ct=result&resnum=4&ved=0CBsQ6AEwAw#v=onepage&q&f=false