WLAN - IEEE802.11

- **Architecture (WS:14.1+PK:11.2)**
- **Protocol Structure (WS:14.2+PK:11.2)**
- **PHY Layer (WS:14.4+PK:11.3)**
- **MAC Layer (WS:14.3+PK:11.4)**

Review

- CDMA System Architecture(IS95)
- CDMA System Characteristics
- CDMA Handoff
- IS-95 Logical Channels
- Forward and Reverse Channel Processing

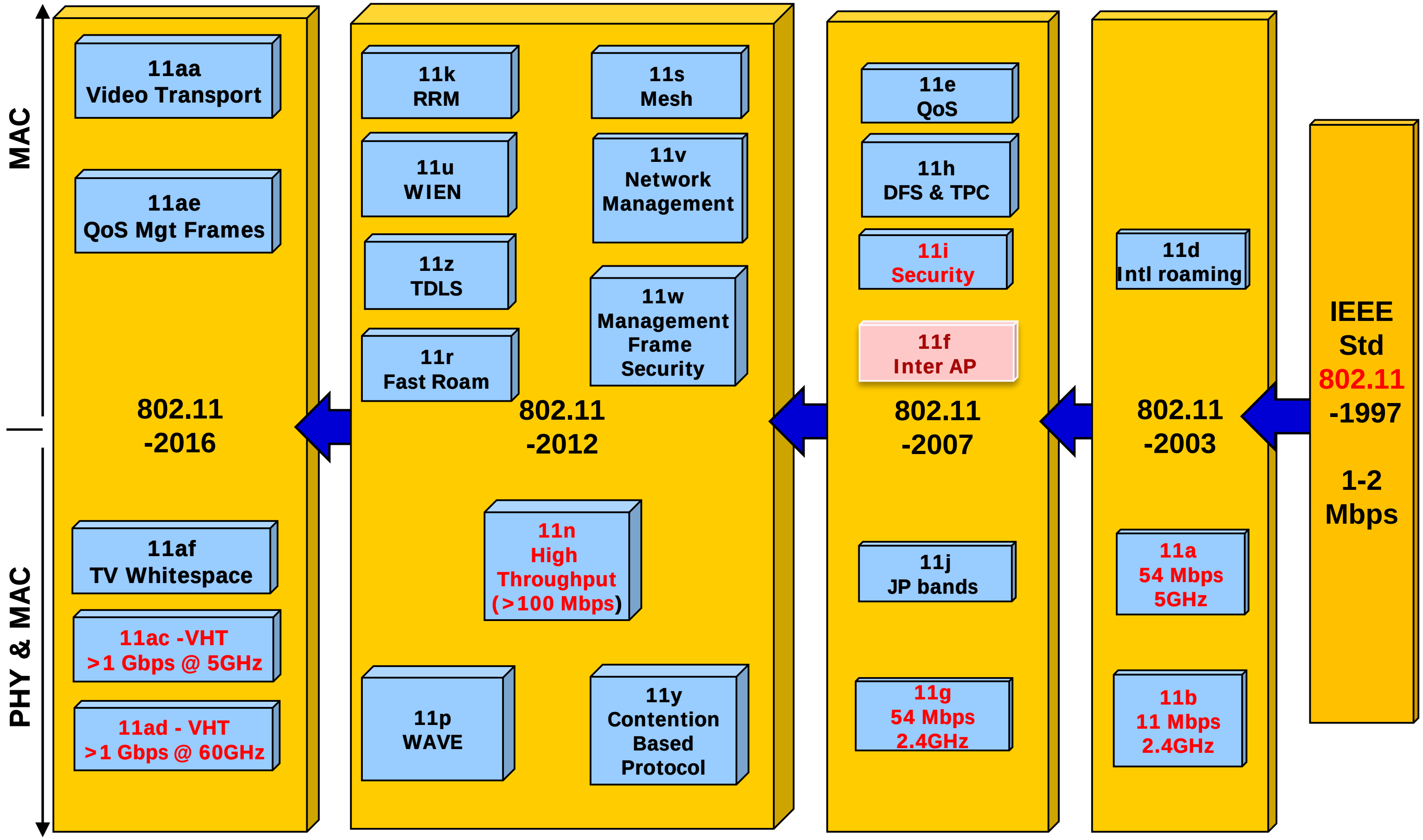
History of IEEE802.11

- 1987: Started as 802.4L
- 1989: Moved to 802.11
- 1997: MAC & PHY for 1&2Mbps at 2.4GHz
- 1999 (a,b): PHY for 11Mbps at 2.4GHz (3 Ch) and 54Mbps at 5GHz (12 ch)
- 2000 (c,d): Supplement to 802.1d bridges. Dynamic regulatory domain update
- Current (e,g,h,i,j,k,m,n,p,r,s, ac,ad,ax)

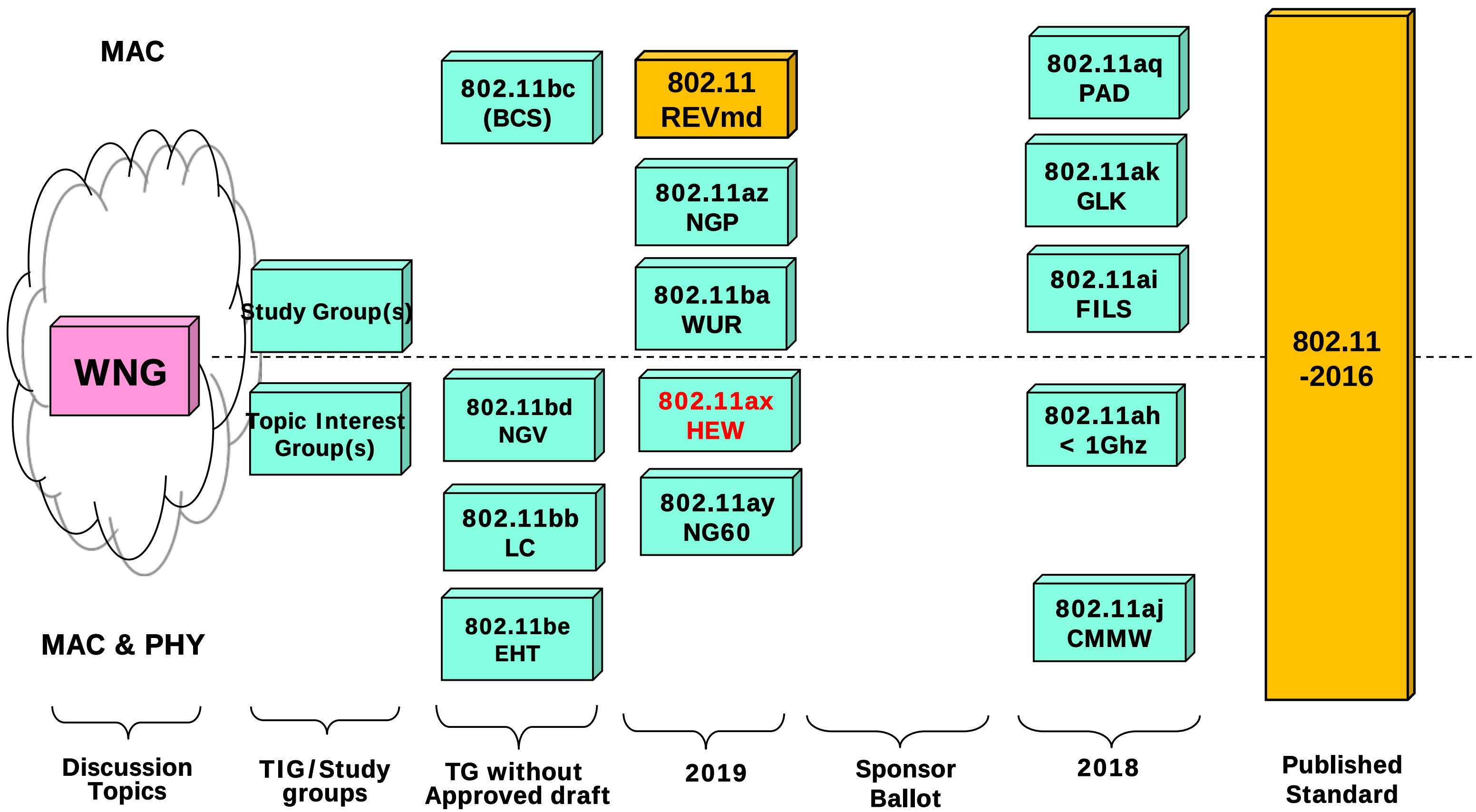
IEEE 802.11 WLAN Standards

- 802.11a: 5 GHz, 54 Mbps
- 802.11b: 2.4 GHz, 11 Mbps
- 802.11d: Multiple regulatory domains
- 802.11e: Quality of Service (QoS)
- 802.11f: Inter-Access Point Protocol (IAPP)
- 802.11g: 2.4 GHz, 54 Mbps
- 802.11h: Dynamic Frequency Selection (DFS) and Tran Power
- 802.11i: Security – Ratified | WPAv2 – Draft 9
- 802.11j: Japan 5 GHz Channels (4.9-5.1 GHz)
- 802.11k: Measurement
- 802.11m: Maintenance
- 802.11n: High Throughput
- 802.11p: Wireless Access for Vehicular Environment
- 802.11r: Public WLAN Fast Roaming
- 802.11s: Mesh Networking

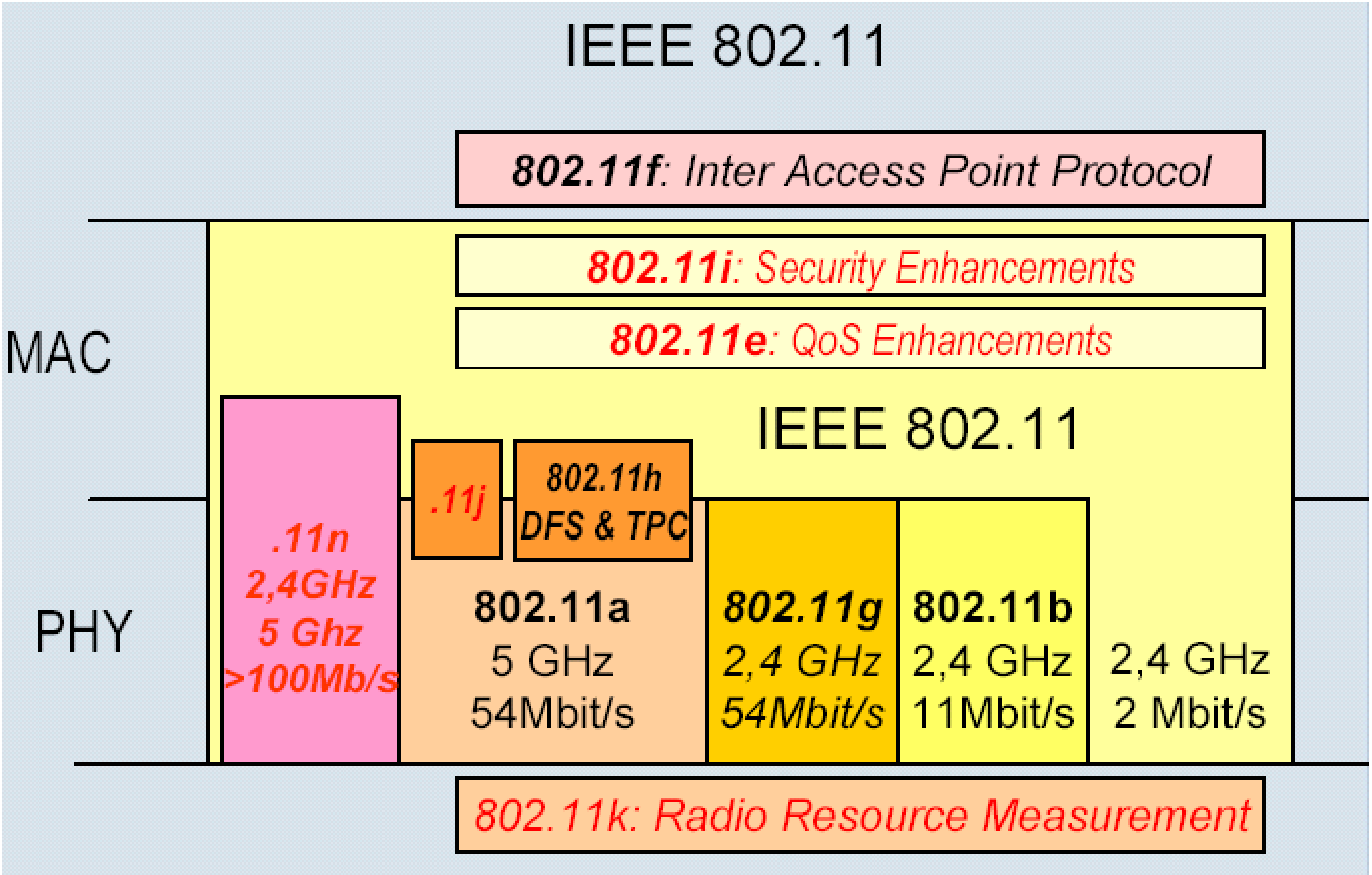
Development of the IEEE 802.11 Standard



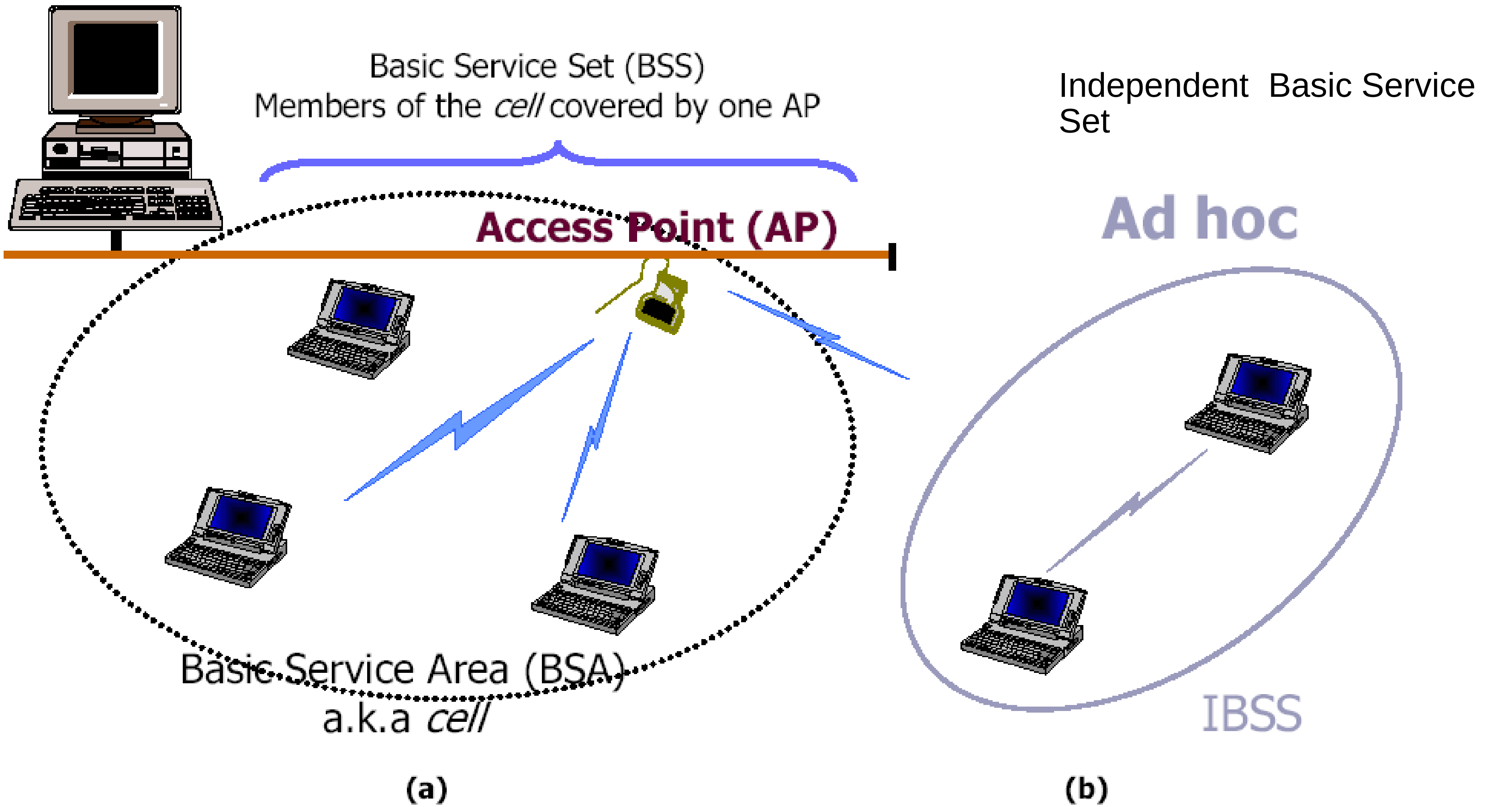
IEEE 802.11 Standards Pipeline



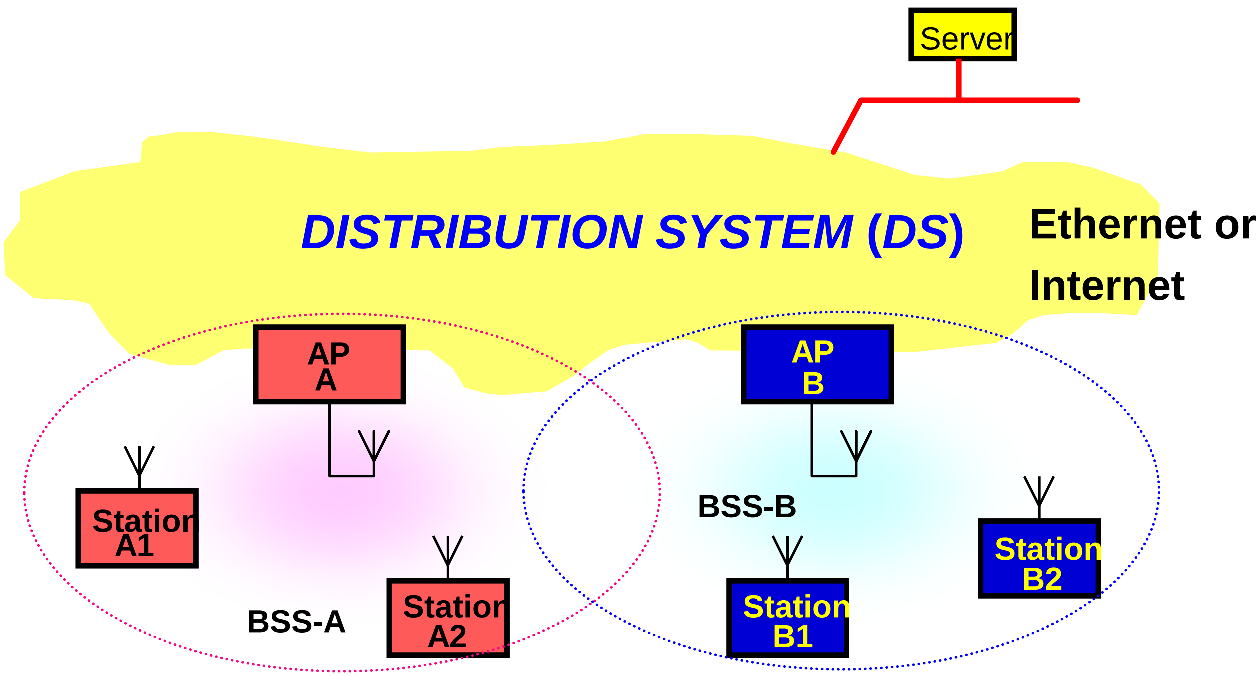
Overview of IEEE802.11 Standards



Architecture/Reference Model



802.11 Configurations - ESS

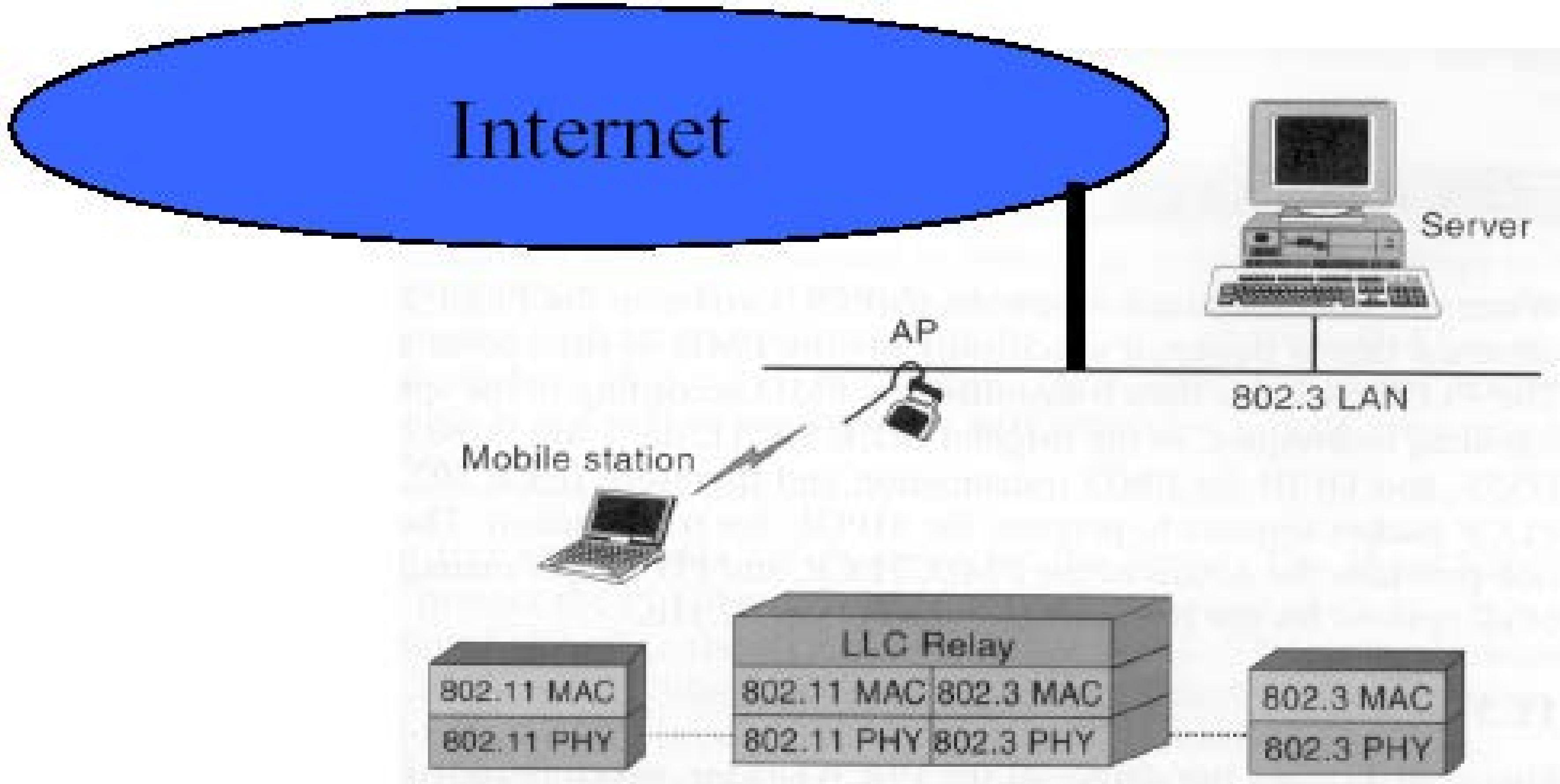


- **Extended Service Set**
  - **Access Points (AP) and stations (STA)**
- **Distribution System interconnects Multiple Cells via Access Points to form a single Network.**
  - **extends wireless coverage area**

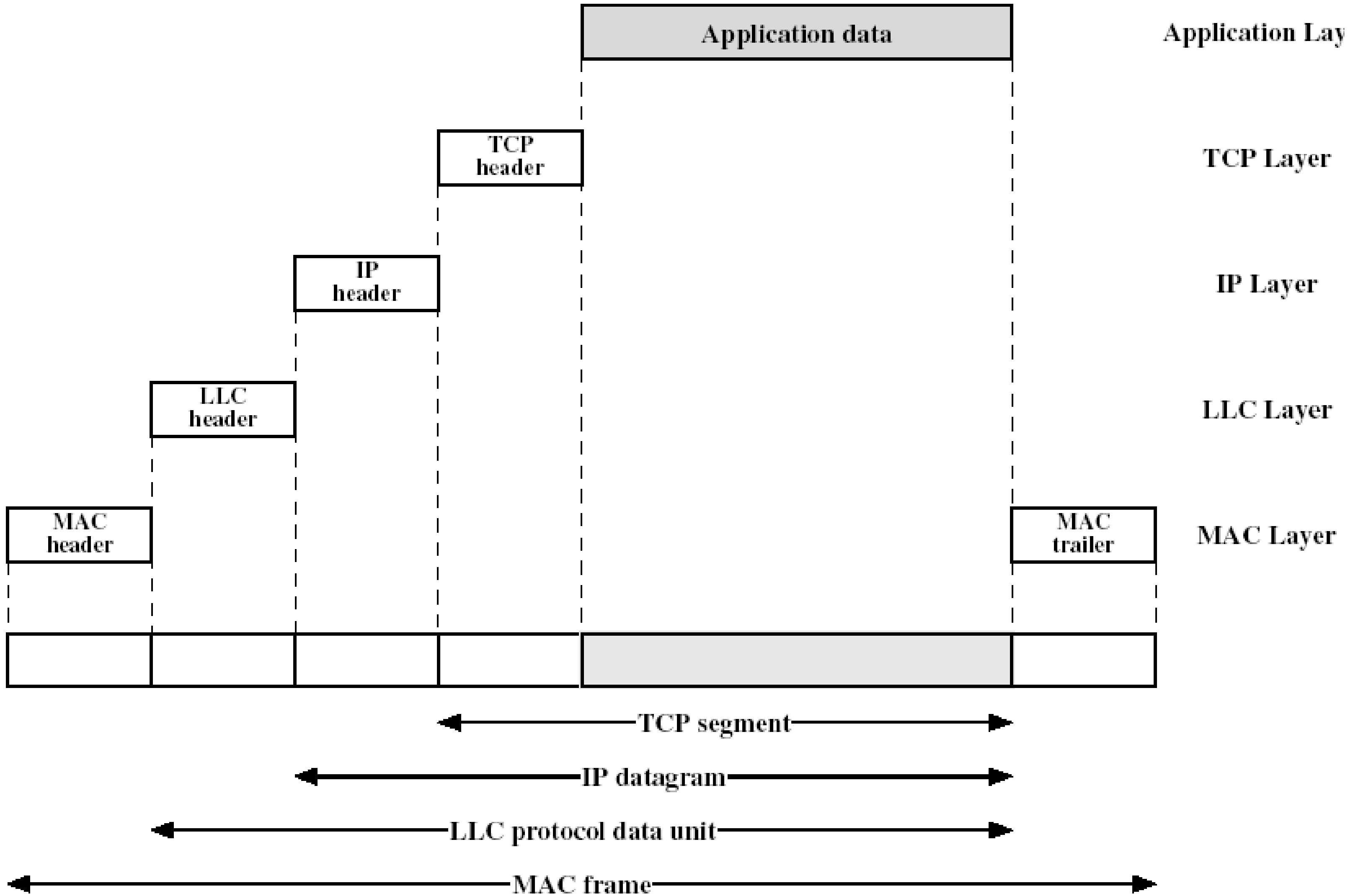
Terminology

- **Access Point (AP)**
  - Provides access to distribution services via the wireless medium
- **Basic Service Area**
  - The coverage area of one access point
- **Basic Service Set (BSS)**
  - A set of stations controlled by one access point
- **Distribution System (DS)**
  - The fixed (wired) infrastructure used to connect a set of BSS to create an **extended service set (ESS)**
- **Portal(s)**
  - The logical point(s) at which non-802.11 packets enter an ESS
- **MAC Protocol Data Unit (MPDU)**
- **MAC Service Data Unit (MSDU)**

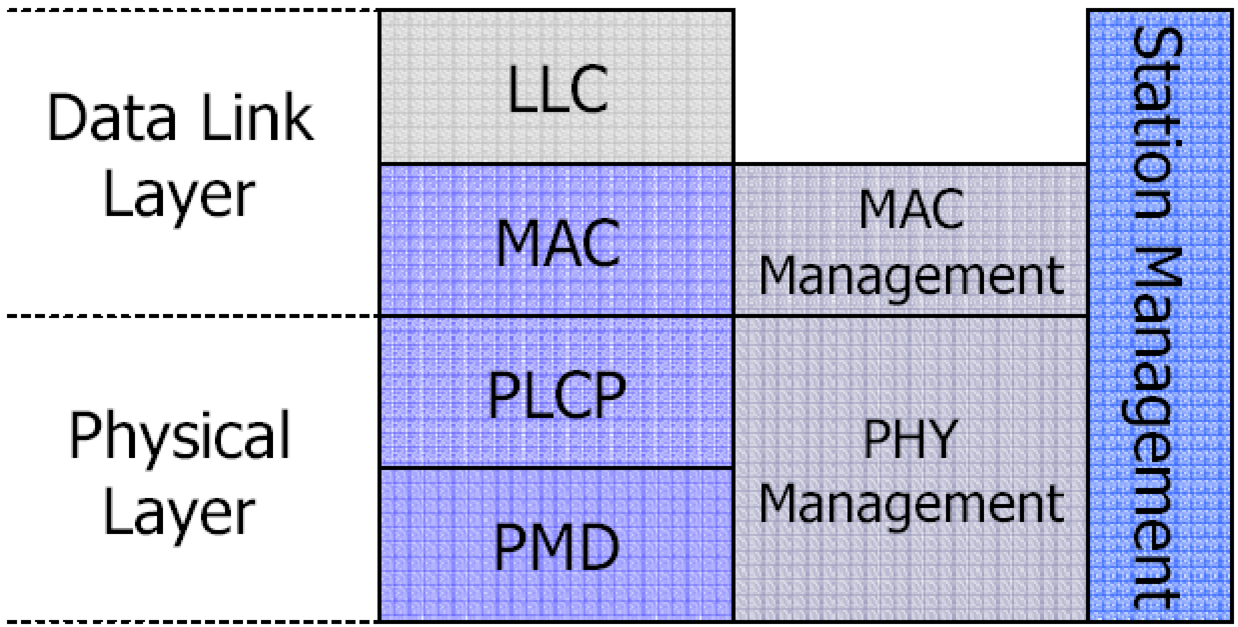
Practical Implementation



IEEE802.11 Protocols in Context



IEEE 802.11 Protocol Layers



PLCP: Physical Layer Convergence Protocol
PMD: Physical Medium Dependent

Sub-layer Responsibilities

- LLC: Provide an interface to higher layers and perform flow and error control
- MAC Sublayer: access mechanism, data format
- MAC Management: roaming in ESS, power management, and security.
- PLCP: carrier sensing assessment, forming packets for PHYs
- PMD: modulation and coding
- PHY Layer Management: channel tuning
- Station Management: interacts with MAC and PHY

Detailed View of Protocol Architecture

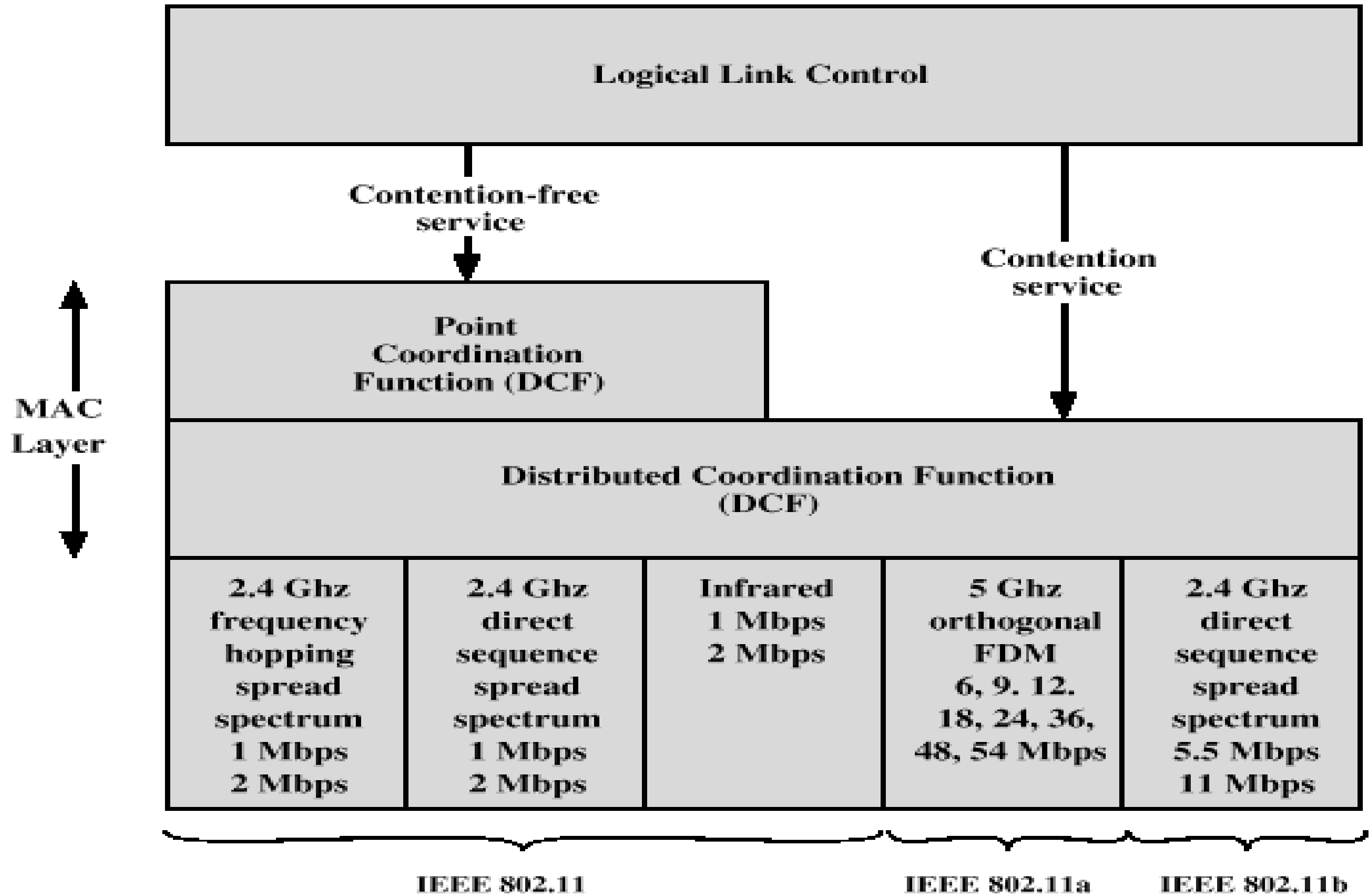


Figure 14.5 IEEE 802.11 Protocol Architecture

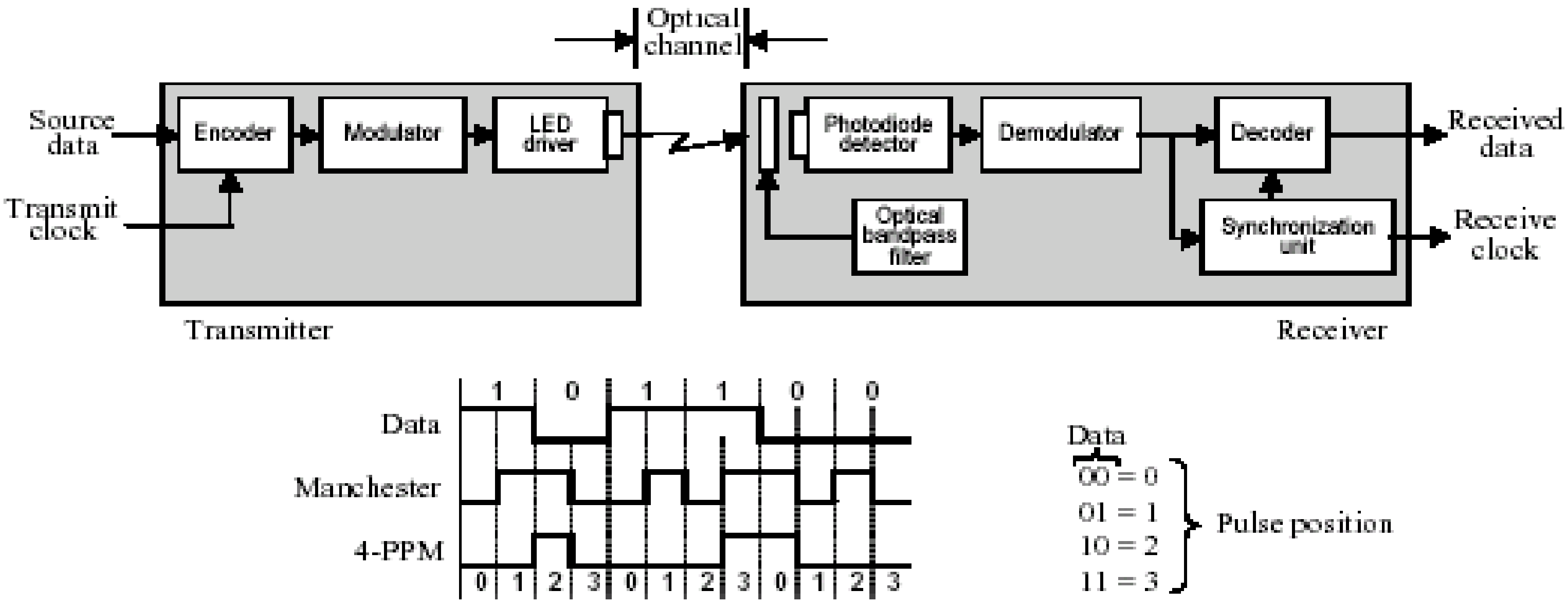
Physical Layer in 802.11

- Three options
  - Frequency Hopping Spread Spectrum (FHSS)
  - Direct Sequence Spread Spectrum (DSSS)
  - Diffused Infra Red (DFIR) – not widely used.

- Note, same MAC layer but all 802.11, 802.11 a and 802.11 b all are incompatible at the physical layer!

Infrared -PPM Modulation

- OOK (On-Off-Keying) PPM (Pulse Position Modulation) :
  - Reduce the optical power

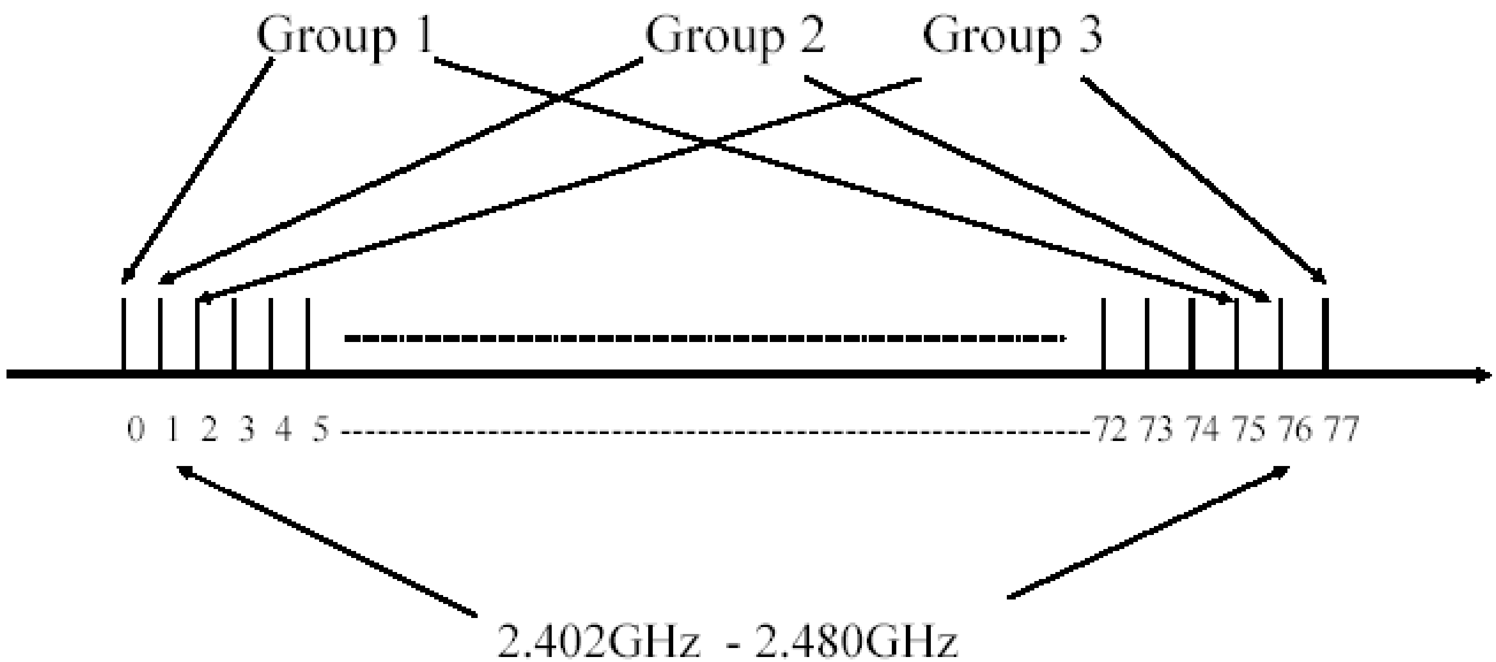


FHSS

- Fast and slow hoppers
- Each packet is transmitted using a different frequency or across a number of hops (F3, F6, F7, F1, F8, F2, F7)
- The hopping mitigates frequency selective fading for example
- IEEE 802.11 uses 78 hops, hops are 1 MHz apart
- 3 patterns of 26 hops corresponding to channel numbers (0, 3, 6, 9 …75), (1,4, 7, 10,…., 76), (2, 5, 8, 11, …., 77)
- Allows 3 different systems to co-exist without hop collision or “hit”.
- In IEEE 802.11 this technique allows the installation of three APs in the same area in an overlapping format that results in a three fold increase in the capacity of a cell

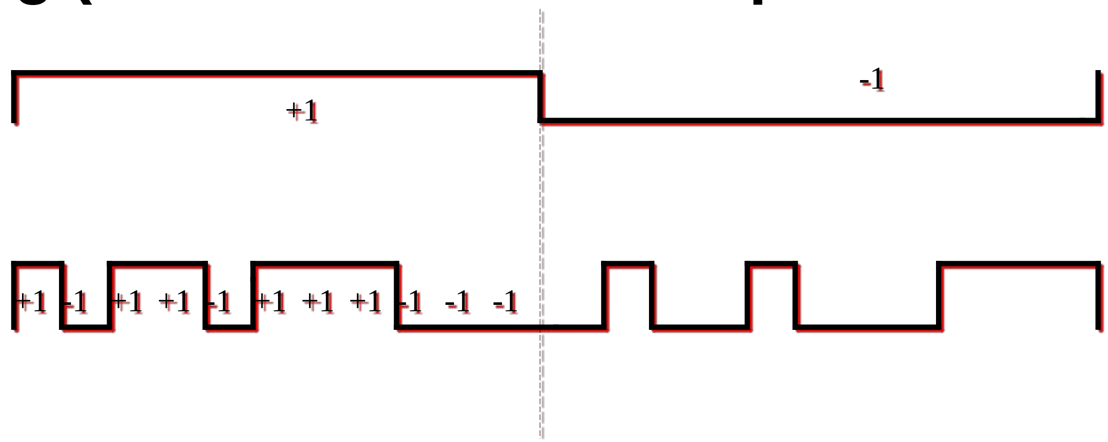
Three Frequency Groups for the FHSS

(0, 3, 6, 9 …75) (1,4, 7, 10,…., 76) (2, 5, 8, 11, …., 77)



DSSS -1

- Uses a Baker code of length 11 as the spreading signal for DSSS at the physical layer
  - –[1,1,1,-1,-1,-1,1,-1,-1,1,-1]
- “1” is coded using the Baker code and “spread”
- N * the bandwidth of a traditional system without spreading (N is the bandwidth expansion factor)



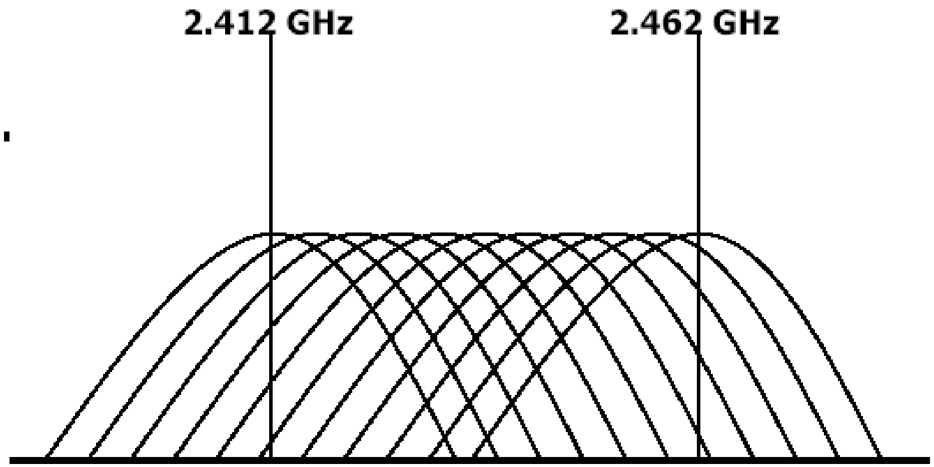
Coding gain 10.4 dB

DSSS-2

- **Overlapping bands in IEEE802.**

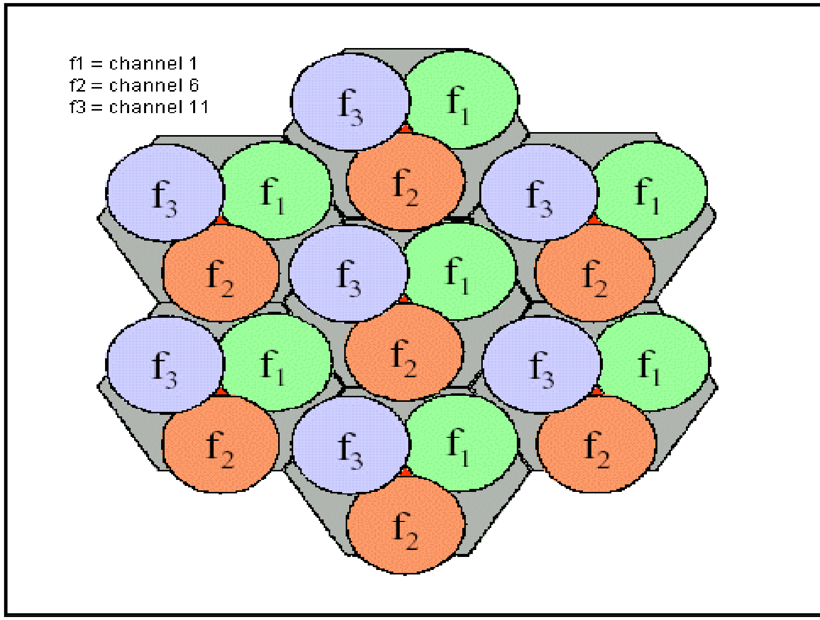
  11 channels
  (shifting 5MHz);
  3 non-overlapping ones
  (1,6,11);

  Chip rate: 11 Mcps -> 22MHz



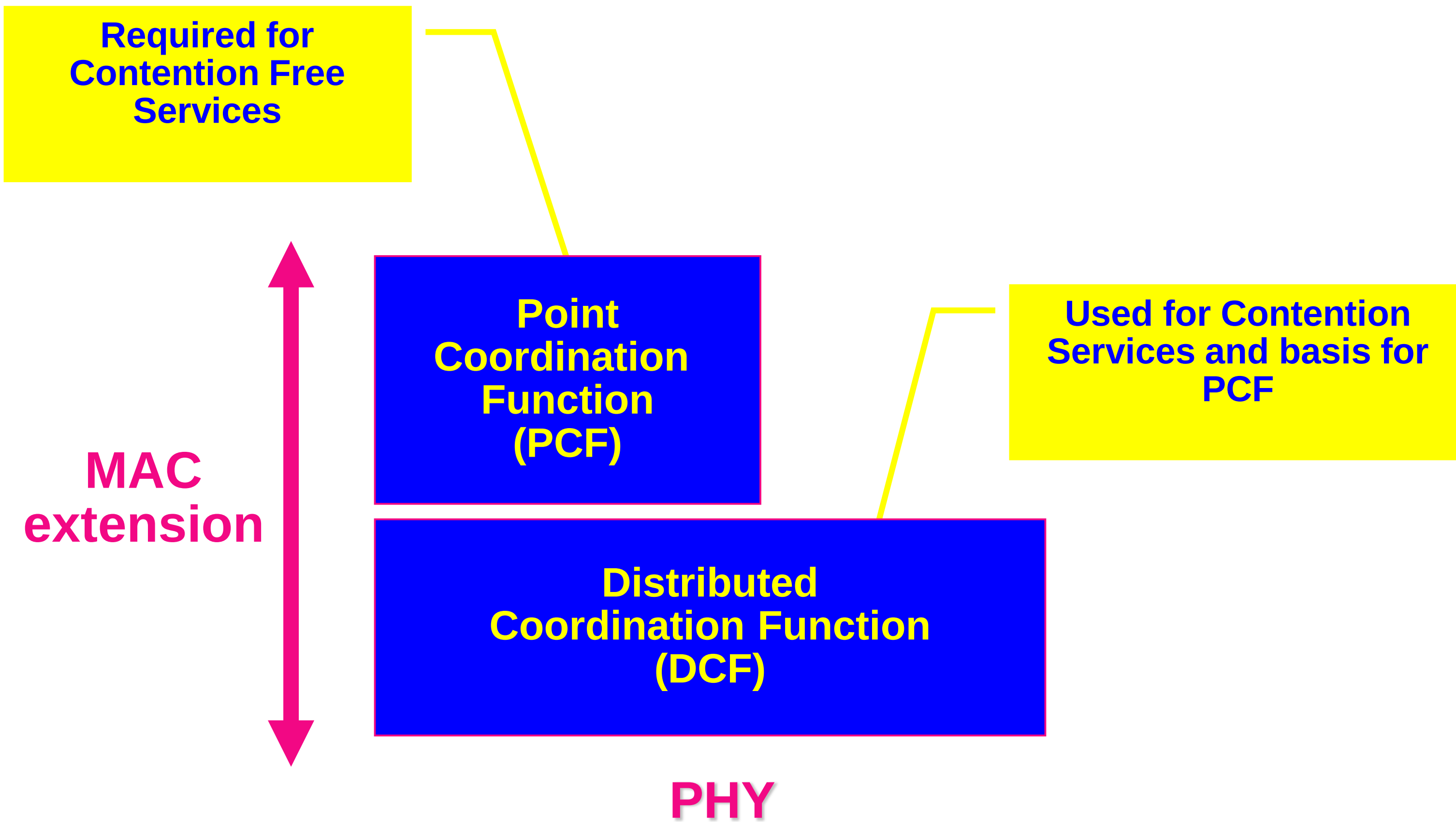
CHNL_ID	Frequencies	FCC Channel Frequencies	ETSI Channel Frequencies	Japan Frequency (MKK)	Japan Frequency (New MKK)
1	2412 MHz	X	X	-	X
2	2417 MHz	X	X	-	X
3	2422 MHz	X	X	-	X
4	2427 MHz	X	X	-	X
5	2432 MHz	X	X	-	X
6	2437 MHz	X	X	-	X
7	2442 MHz	X	X	-	X
8	2447 MHz	X	X	-	X
9	2452 MHz	X	X	-	X
10	2457 MHz	X	X	-	X
11	2462 MHz	X	X	-	X
12	2467 MHz	-	X	-	X
13	2472 MHz	-	X	-	X
14	2484 MHz	-	-	X	X

Table 1, DSSS PHY Frequency Channel Plan



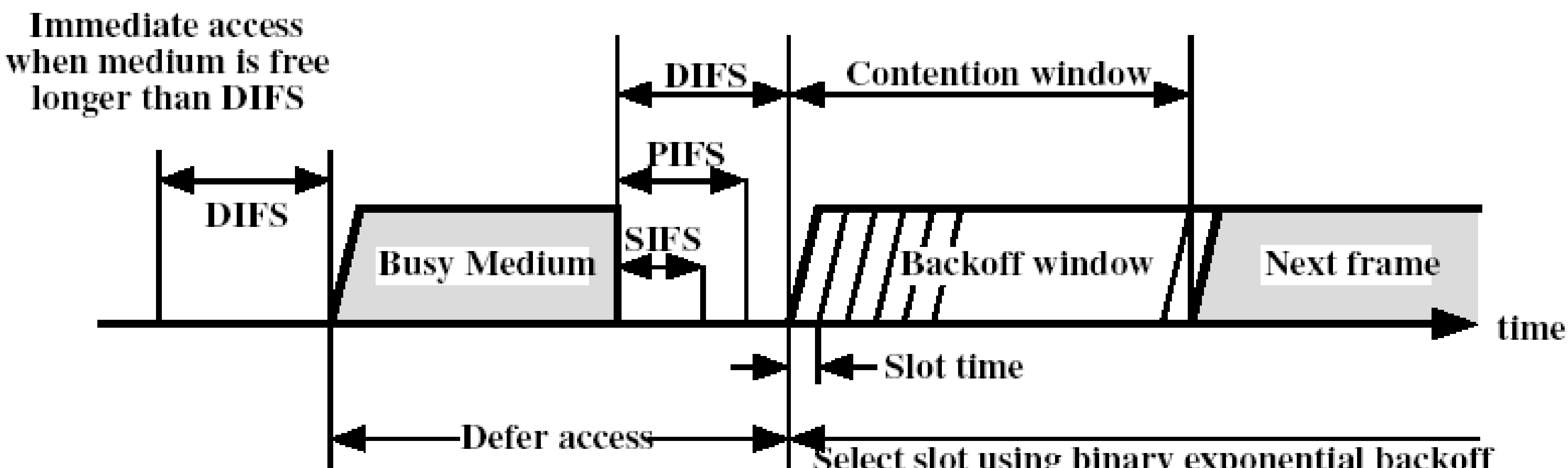
Frequency planning

MAC Architecture



MAC Timing: Basic Access Method

- After transmission of a packet all mobiles wait for one of three devices IFS (inter-frame spacings) according to the level of priority of their packet
  - DCF-IFS (DIFS) used for contention, lowest priority, longest delay
  - Short-IFS (SIFS) used for high priority such as ACKs, CTS, etc. has the lowest duration time
  - PCF-IFS (PCF) has second priority rate with duration between DIFS and SIFS



Distributed Coordination Function (DCF)

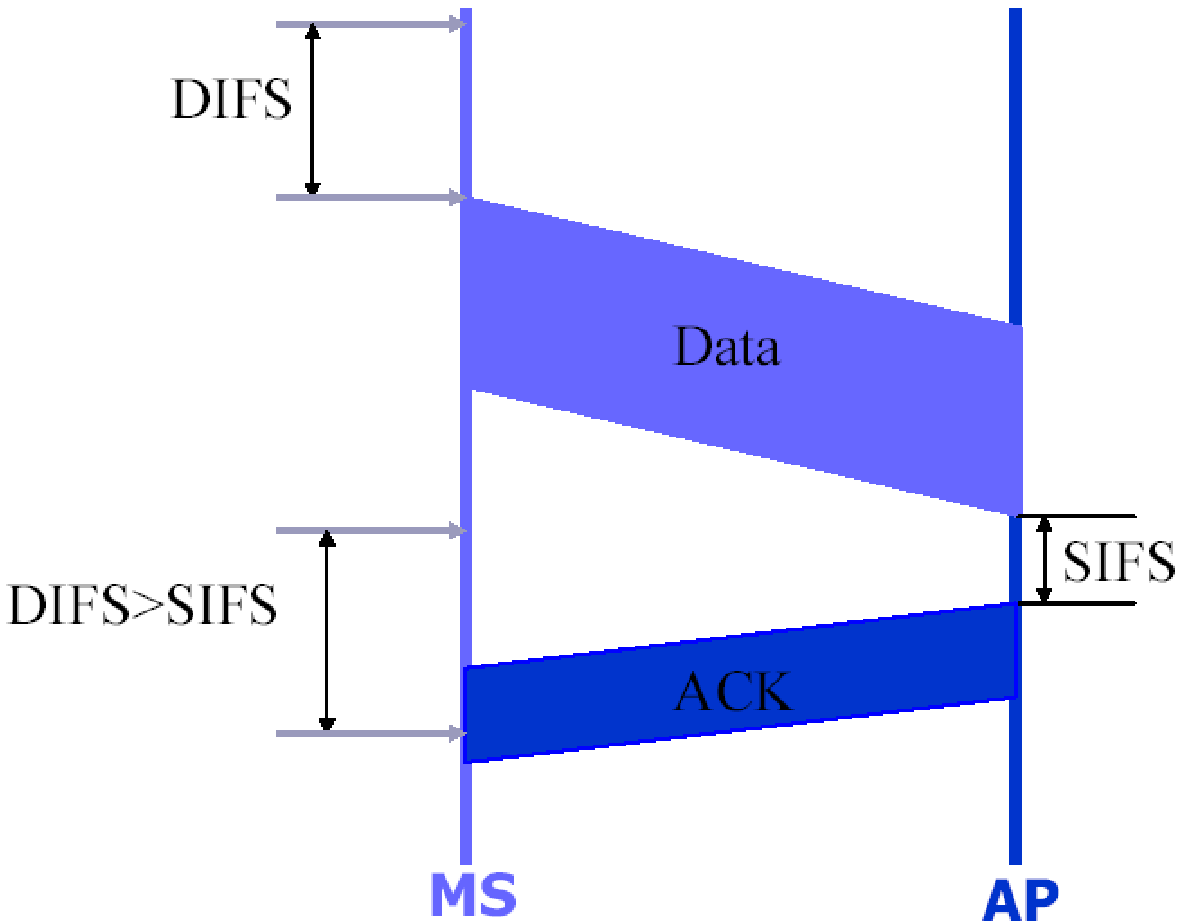
Use CSMA/CA Algorithm based on Interframe Space (IFS):

1) If the medium is idle, the station waits to see if the medium is idle for a time equal to IFS. If so, it may transmit immediately.

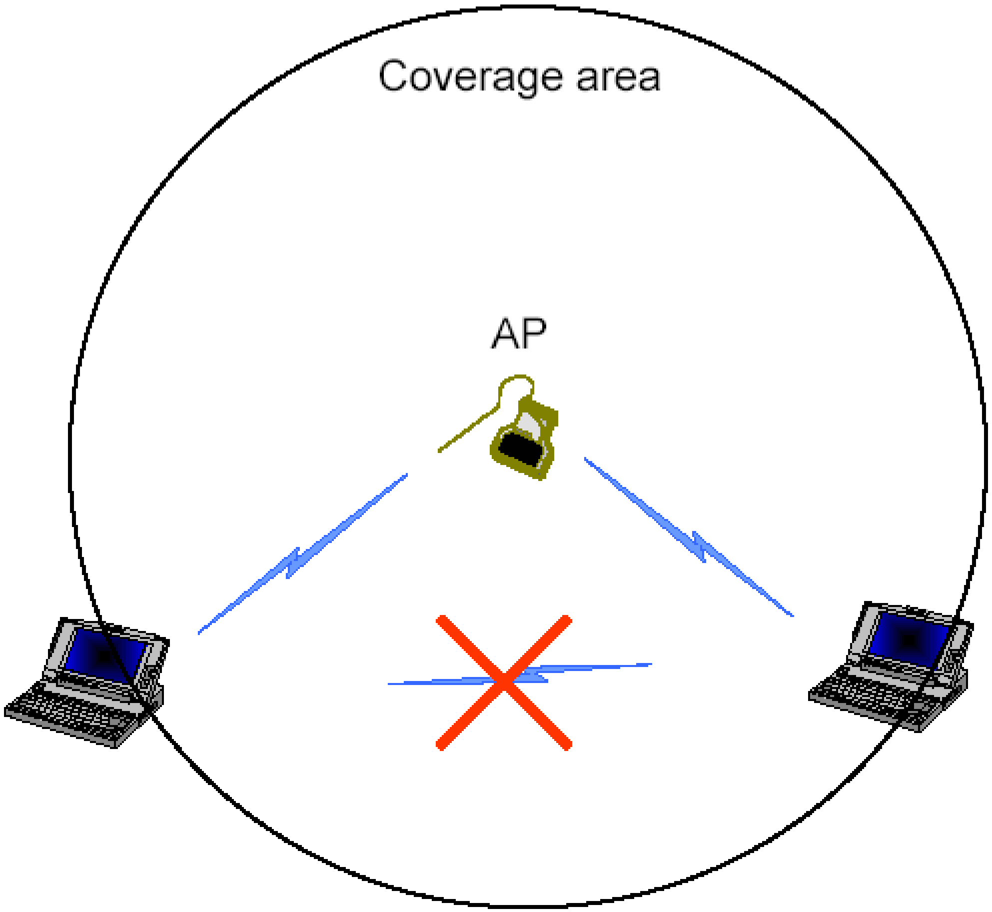
2) If the medium is busy, the station defers transmission and continues to monitor the medium.

3) Once the current transmission is over, the station delays another IFS. If the medium remains idle for this period, then it back off the random amount of time and again sense the medium. If the medium is still idle, it may transmit. During the backoff time, if the medium becomes busy, the backoff timer is halted and resumes when the medium is idle.

CSMA/CA with ACK in an Infrastructure Network



Hidden Terminals



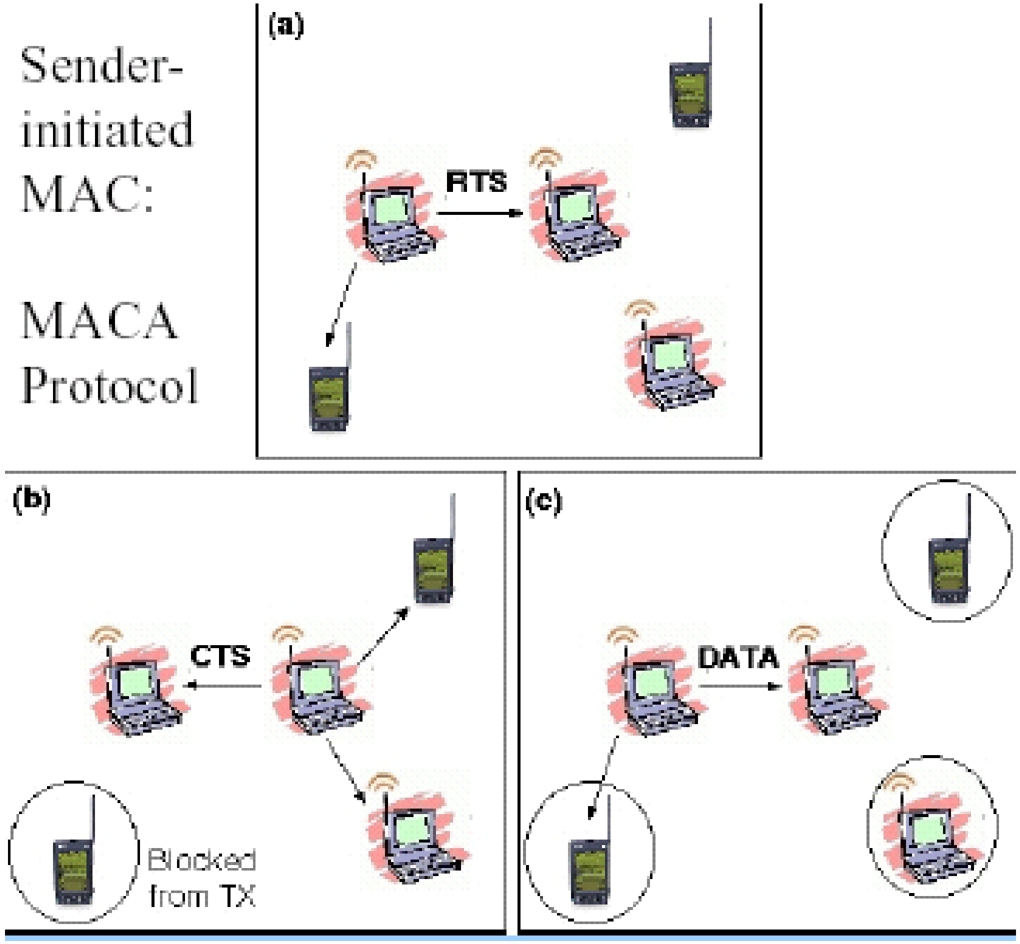
The two terminals contending to communicate with the AP are both in the coverage area of the AP, but they are out of the coverage area of each other (distance or shadowing).

It has no effect on ALOHA protocols, but degrades the performance of CSMA protocols.

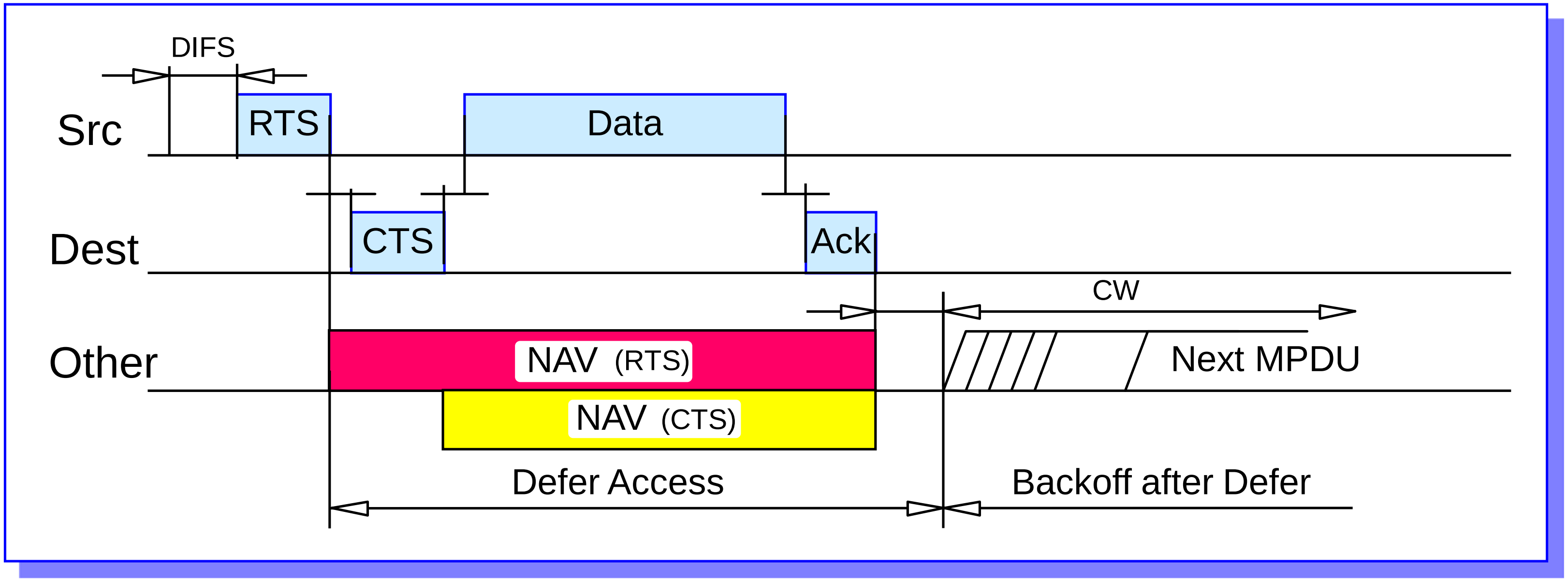
RTS/CTS Protocol

Sender-initiated MAC:

MACA Protocol



CTS/RTS Mechanism

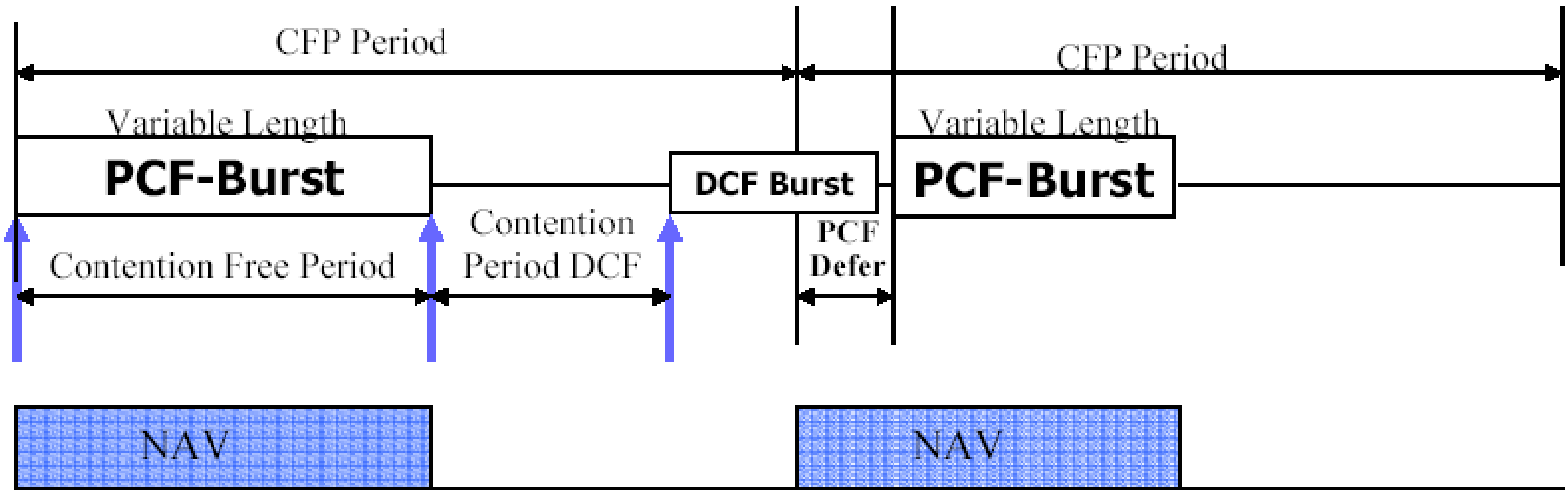


- *Duration* field in RTS and CTS frames distribute *Medium Reservation* information which is stored in a *Net Allocation Vector (NAV)*.
- Defer on either NAV or "CCA (Clear Channel Assessment)" indicating *Medium Busy*.
- Use of RTS / CTS is optional but must be implemented.
- Use is controlled by a *RTS_Threshold* parameter per station.
  - To limit overhead for short frames. (200 bytes)

PCF (Point Coordination Function) Mode

- Built of top of DCF
- Supports contention-free, time bounded and asynchronous transmission operations
- Optional MAC function/feature – not widely available in products
- Mostly available as part of infrastructure mode with an AP, which can be set up to be a central coordinator like in cellular systems
- Operation in PCF mode
  - – AP polls devices periodically
  - – Sets up contention-free period (CFP)
  - – Coordinates time bounded data to be transmitted in each CFP
  - – During that period when a device is transmitting data PCF sets all the NAV signals ON at all other stations
  - – Length of PCF period is variable and only occupies a potion of the CFP
  - – The remainder of the CFP is used for contention and DCF packets
  - – If DCF has not completed before the start of the next CFP period, the starting time of the CFP is deferred but NAV is turned ON

MAC Timing: PCF Operation



PCF (Point Coordination Function) Mode

MAC Frame and Control Field

octets	2	2	6	6	6	2	6	0 to 2312	4
	FC	D/I	Address	Address	Address	SC	Address	Frame body	CRC

FC = Frame control
D/I = Duration/Connection ID
SC = Sequence control

(a) MAC frame

Addresses: receiver, transmitter (physical), BSS identifier, sender (logical)

12-34-56-78-9A-BC

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

Figure 14.8 IEEE 802.11 MAC Frame Format

Type/Subtype

- Management Type (00)
  - Assoc. request/response(0000/0001)
  - Reassoc. request/response
  - Probe-request/response
  - Beacon
  - Announcement traffic indication (used for sleep mode operations
  - Authentication/Deauthentication
- Control Type (01)
  - Power save poll
  - RTS/CTS
  - Ack
  - CF end and CF end with ACK (CF: Contention Free)
- Data Type (10)
  - Data/ Data with CF ACK
  - Data Poll with CF/ Data Poll with CF and ACK
  - CF poll/ CF poll CK

Control Message Format

RTS

octets:	2	2	6	6	4
	Frame Control	Duration	RA	TA	CRC

MAC Header

CTS

octets:	2	2	6	4
	Frame Control	Duration	RA	CRC

MAC Header

ACK

octets:	2	2	6	4
	Frame Control	Duration	RA	CRC

MAC Header

RA – Receiver Address; TA – Transmitter Address

MAC Management Layer

- Synchronization
  - finding and staying with a WLAN
  - Synchronization functions
    - » TSF Timer, Beacon Generation
- Power Management
  - sleeping without missing any messages
  - Power Management functions
    - » periodic sleep, frame buffering, Traffic Indication Map
- Association and Reassociation
  - Joining a network
  - Roaming, moving from one AP to another
  - Scanning
- Security

Synchronization in 802.11

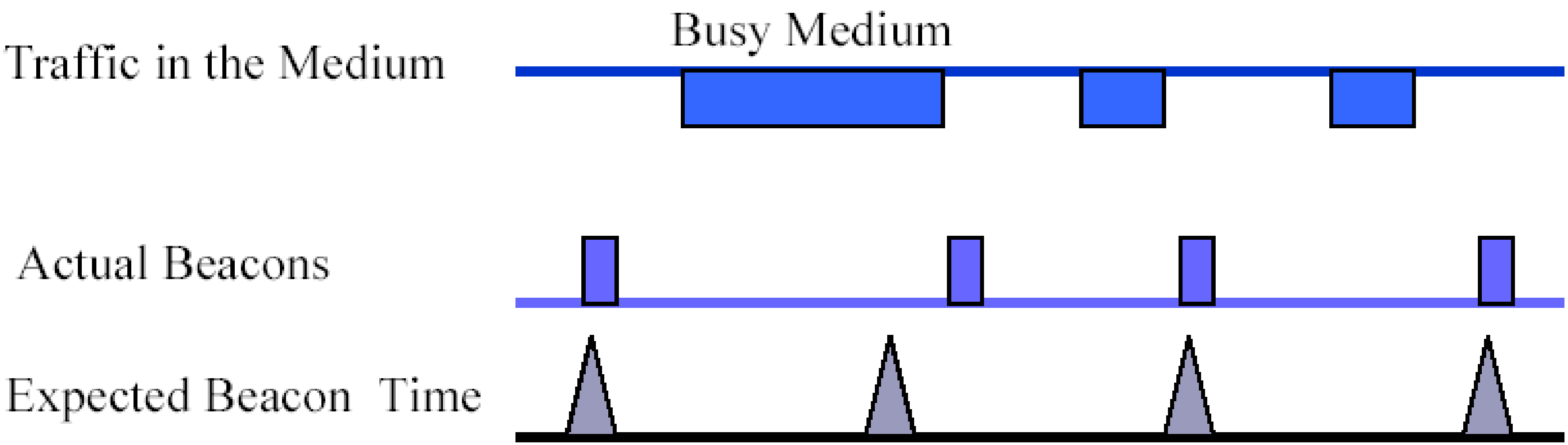
- Timing Synchronization Function (TSF)
- Used for Power Management
  - Beacons sent at well known intervals
  - All station timers in BSS are synchronized
- Used for Point Coordination Timing
  - TSF Timer used to predict start of Contention Free burst
- Used for Hop Timing for FH PHY
  - TSF Timer used to time Dwell Interval
  - All Stations are synchronized, so they hop at same time.

Synchronization Approach

- All stations maintain a local timer.
- Timing Synchronization Function
  - keeps timers from all stations in synch
  - AP controls timing in infrastructure networks
  - distributed function for Independent BSS
- Timing conveyed by periodic Beacon transmissions
  - Beacons contain Timestamp for the entire BSS
  - Timestamp from Beacons used to calibrate local clocks
  - not required to hear every Beacon to stay in synch
  - Beacons contain other management information
    - » also used for Power Management, Roaming

Beacon Generation

- **In Infrastructure**
  - **AP defines the *aBeaconPeriod* for transmitting beacons**
  - ***aBeaconPeriod* is broadcast by beacon and probe response**
  - **may delayed by CSMA/CA**



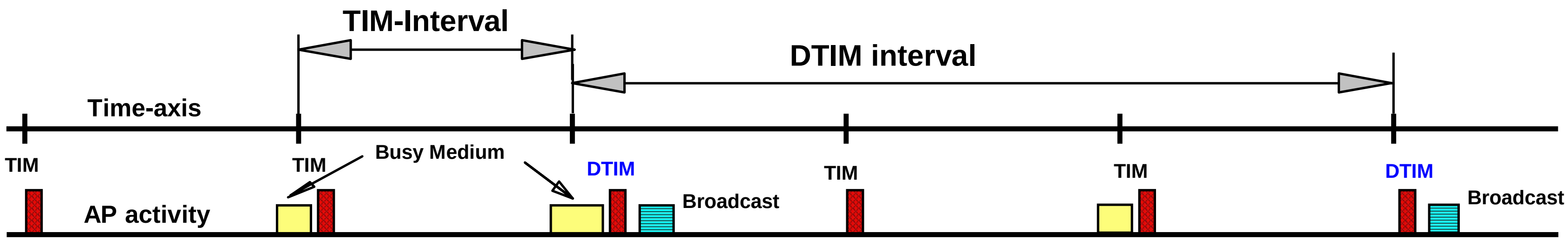
Power Management

- **Mobile devices are battery powered.**
  - ***Power Management*** **is important for mobility.**
- **Current LAN protocols assume stations are always ready to receive.**
  - **Idle receive state dominates LAN adapter power consumption over time.**
- **How can we power off during idle periods, yet maintain an active session?**
- **802.11 Power Management Protocol:**
  - **allows transceiver to be off as much as possible**
  - **is transparent to existing protocols**
  - **is flexible to support different applications**
    - » **possible to trade off throughput for battery life**

Power Management Approach

- Allow idle stations to go to sleep
  - station power save mode stored in AP
- APs buffer packets for sleeping stations.
  - AP announces which stations have frames buffered
  - Traffic Indication Map (TIM) sent with every Beacon
- Power Saving stations wake up periodically
  - listen for Beacons
- TSF assures AP and Power Save stations are synchronized
  - stations will wake up to hear a Beacon
  - TSF timer keeps running when stations are sleeping
  - synchronization allows extreme low power operation
- Independent BSS also have Power Management
  - similar in concept, distributed approach

Infrastructure Power Management



- Broadcast frames are also buffered in AP.
  - all broadcasts/multicasts are buffered
  - broadcasts/multicasts are only sent after DTIM
    - DTIM : Delivery Traffic Indication Message
  - DTIM interval is a multiple of TIM interval

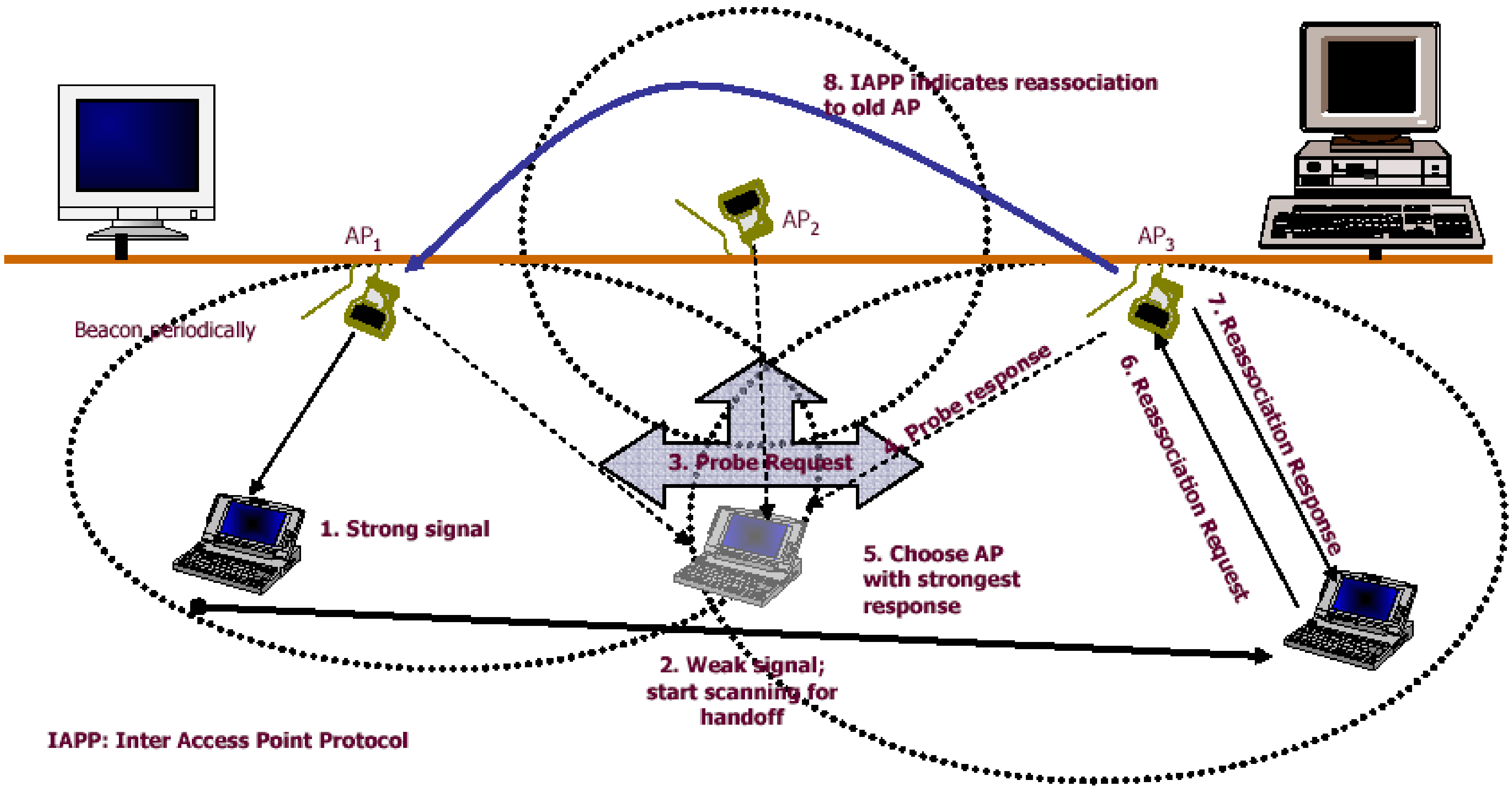
Association

- **Beacons sent periodically (every 100ms) by AP to establish time sync. (TSF) and maintain connectivity or associations**
  - **contains BSS-ID used to identify the AP and network,**
  - **traffic indication map (for sleep mode),**
  - **power management,**
  - **roaming**
- **RSS (Radio Signal Strength) measurements are based on the beacon message**
- **AP and mobile devices form "associations", mobile device "registers" with AP.**
- **Mobiles send "requests" and APs "responses"**
- **Only after registering can mobiles send/receive DATA**

Scanning

- **Scanning required for many functions.**
  - finding and joining a network
  - finding a new AP while roaming
  - initializing an Independent BSS (ad hoc) network
- **802.11 MAC uses a common mechanism for all PHY.**
  - single or multi channel
  - passive or active scanning
- **Passive Scanning**
  - Find networks simply by listening for Beacons
- **Active Scanning**
  - On each channel
    - Send a Probe, Wait for a Probe Response
- **Beacon or Probe Response contains information necessary to join new network.**

Roaming



8. IAPP indicates reassociation to old AP
AP$_1$
AP$_2$
AP$_3$
Beacon periodically
1. Strong signal
3. Probe Request
4. Probe response
5. Choose AP with strongest response
6. Reassociation Request
7. Reassociation Response
2. Weak signal; start scanning for handoff
IAPP: Inter Access Point Protocol

Roaming Approach

- Station decides that link to its current AP is poor
- Station uses scanning function to find another AP
  - or uses information from previous scans
- Station sends Reassociation Request to new AP
- If Reassociation Response is successful
  - then station has roamed to the new AP
  - else station scans for another AP
- If AP accepts Reassociation Request
  - AP indicates Reassociation to the Distribution System
  - Distribution System information is updated
  - normally old AP is notified through Distribution System

Security

- **Open system authentication (default):**
  - SSID (Service Set ID) as a request / response
- **Shared key authentication:**
  - AP and mobile use a shared key that they exchange as a request/response
  - Sends the “key” using a 40-bit secret code that is shared by the AP and mobile
- **Wired Equivalent Privacy (WEP)**
  - Pseudo random generator is used along with a 40-bit secret key to create a key sequence that is simply XOR-ed with the message

- **Susceptible to attacks in IEEE80.2.11b (static 40-bit key)**

Authentication Service

- Examples of a C/R exchange are:

- An open system example:
  (a) Assertion: I'm station 4.
  (b) Challenge: Null.
  (c) Response: Null.
  (d) Result: Station becomes Authenticated.

- A password based example:
  (a) Assertion: I'm station 4.
  (b) Challenge: Prove your identity.
  (c) Response: Here is my password.
  (d) Result: If password OK, station becomes Authenticated.

Wired Equivalent Privacy

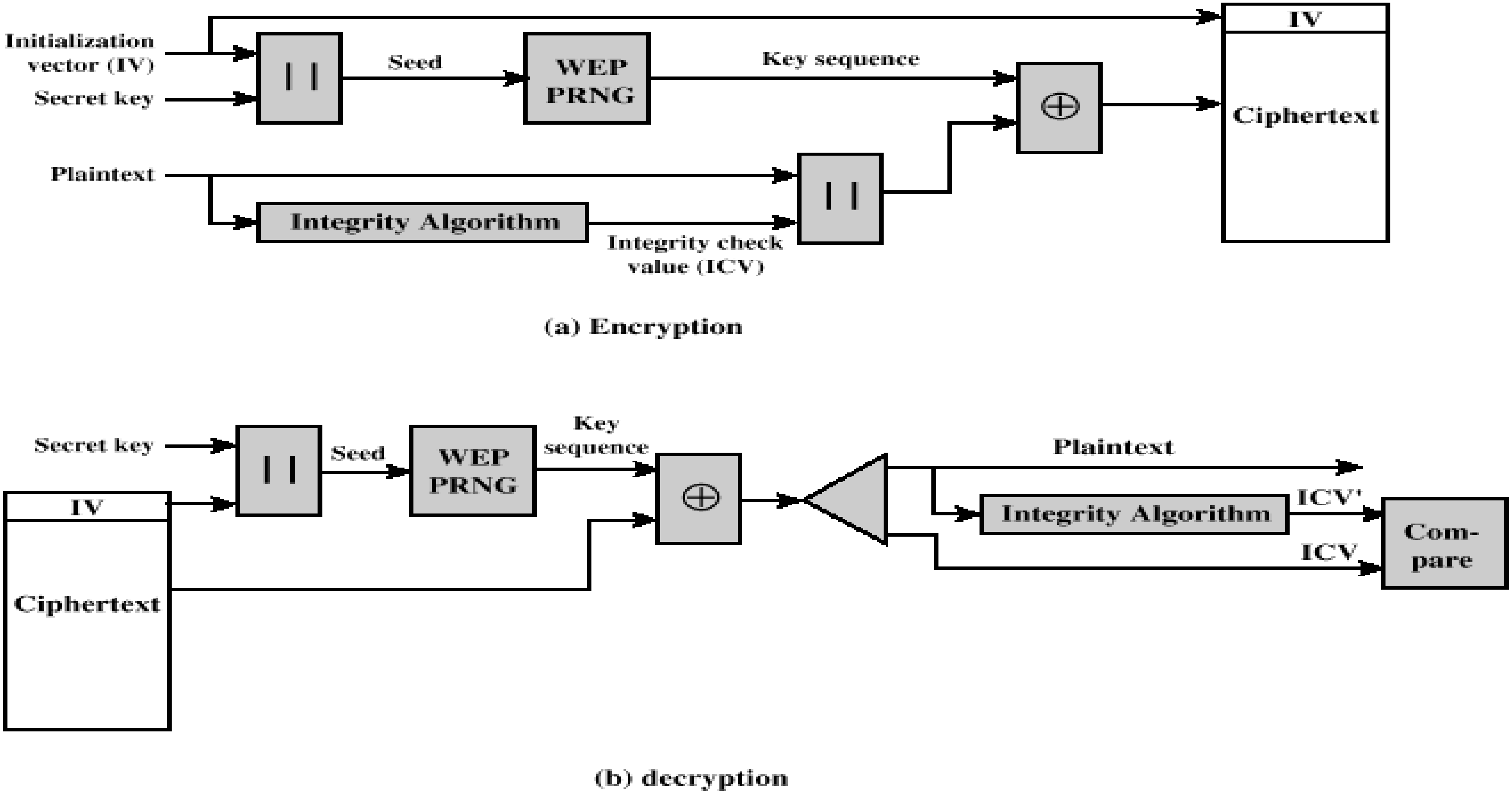


Figure 14.9 WEP Block Diagram

Class Quiz

- What is the IEEE802.11 architecture?
- How is the channel impairments dealt with in IEEE802.11 Phy Layer?
- How is the wireless channel being shared in WLAN?
- What is CTS/RTS protocol?
- How is the roaming arranged?