IEEE 802.11n WIFI 4

Pablo Brenner
BreezeCom Wireless Communications 1

Date 31 Mar 2025

Wonseok

Table of Contents

Basic Operations

- Scanning, Joining
- Authentication, Association
- Power Saving
- Timer Synchronization

Scanning

- **Scanning**
  - **Wired:** easy; look for the cable or a jack on the wall
  - **Wireless**: stations must identify a compatible network before **joining** it

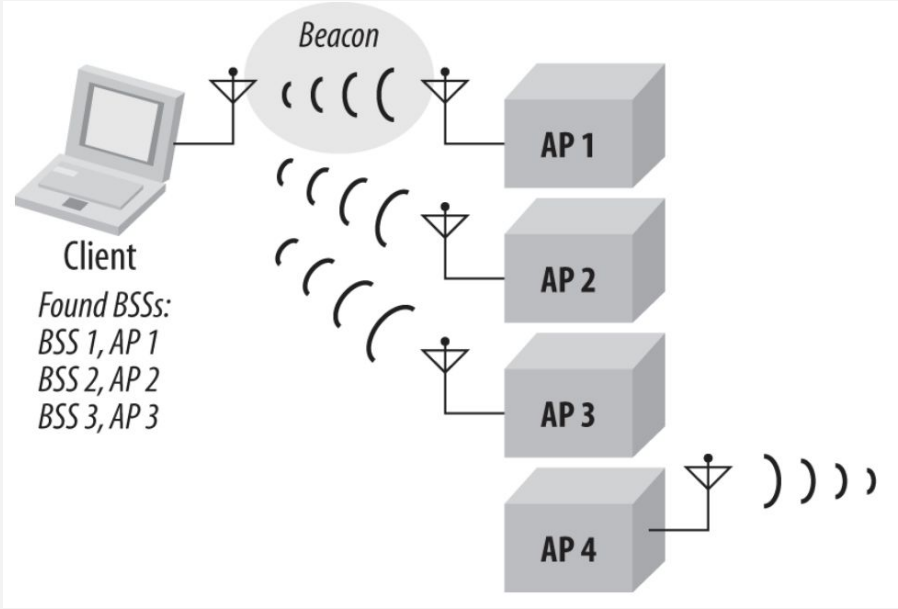
- **Parameters**

BSSType	BSSID	SSID	ScanType	ChannelList	ProbeDelay	ChannelTime

- **Scan Type**
  - **active:**
  - **passive**: moves to each channel on the channel list and waits for Beacon frames

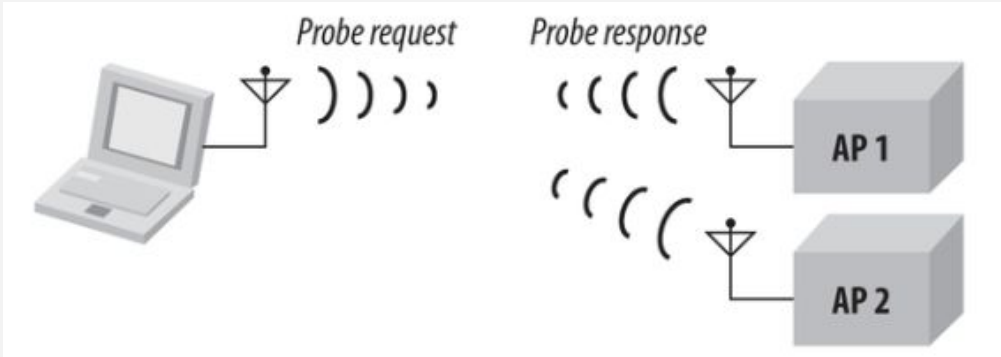
Scanning

- **Passive**
  - any Beacons received are buffered
  - extract information about the BSS
  - saves battery power for not transmitting

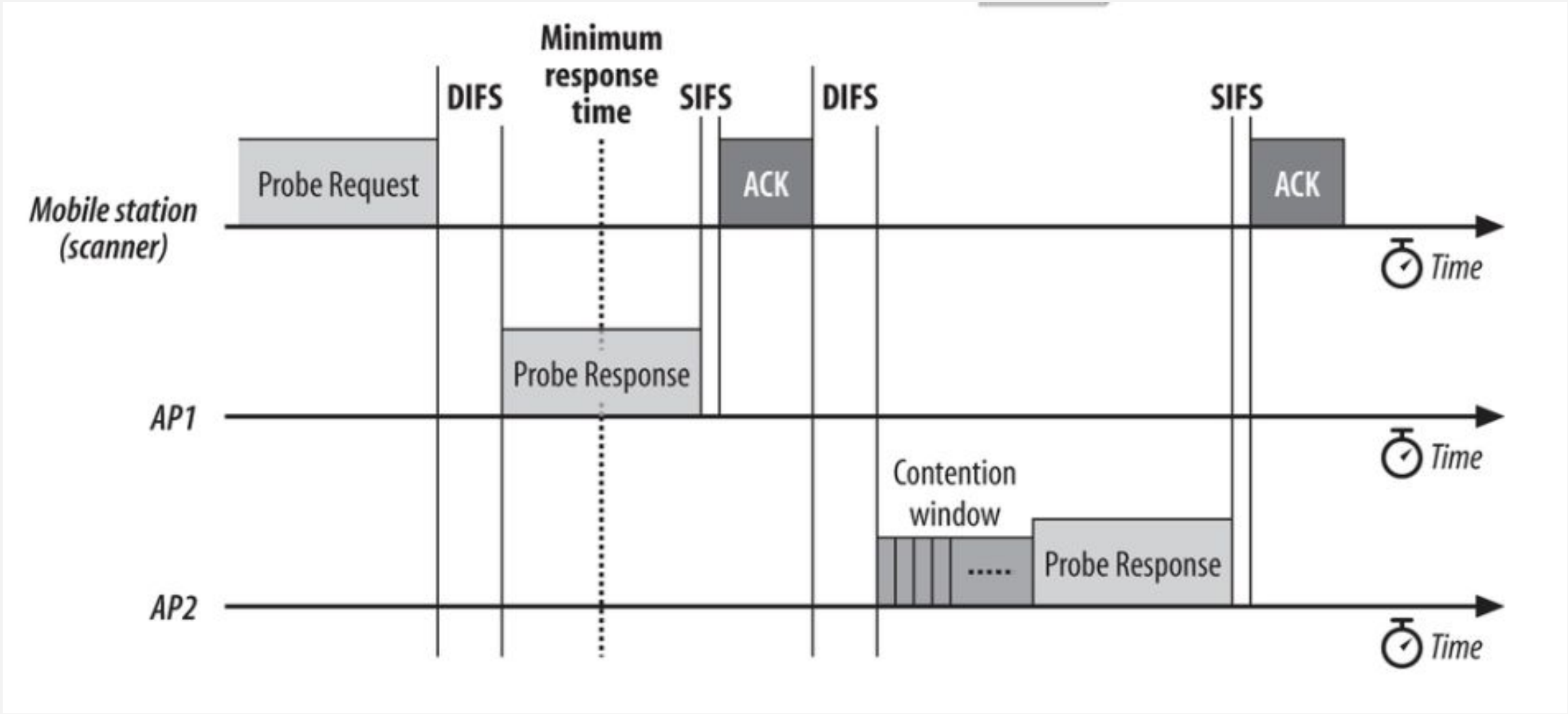


- **Active**

1. Moves to a channel and wait for an incoming frame
2. sends a Probe Request frame and listens for response
3. Wait for the minimum channel time,
   - if the channel is never busy, move to the next channel
   - if the channel is busy, wait for response frame



Scanning

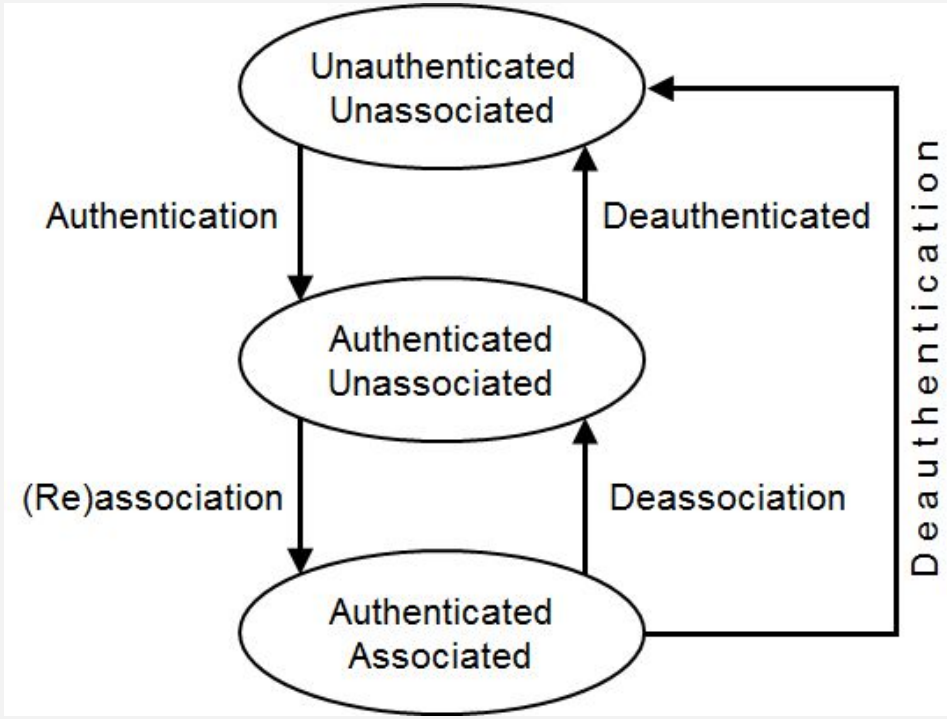

Minimum response time
DIFS
SIFS
DIFS
SIFS
Probe Request
ACK
ACK
Mobile station (scanner)
Time
Probe Response
AP1
Time
Contention window
.....
Probe Response
AP2
Time

Joining

- choose which BSS to join before begin authentication
- synchronize local timer based on beacon frame
- examine MAC, PHY parameters (not adopt yet)
  - BSSID
  - Frequency Hopping pattern
  - DTIM period
  - data rates
  - Beacon interval
  - …

Joining

- **Authentication**
  - a station establish its identity before sending frames
  - functionally a handshake, not a real identity check



- **Algorithms**
  - **Open-system** (merely a handshake, 2 frames)
    - STA requests to join with its MAC address
    - AP returns response (“OK”)
  - **WEP** (shared key, 4 frames)
    - STA requests to join -> AP gives challenge text to STA
    - STA encrypts the challenge text -> AP decrypts it

Association

- **Association**
  - a three-step exchange after authentication
    - Association Request -> Association Response -> Traffic
  - AP issues AID(Association ID) to logically identify the STA
    - buffer frames and notify in power saving mode

- **Reassociation**
  - association to a new AP in ESS without authentication
  - new AP verifies STA’s status on the old AP
  - buffered frames on the old AP may be transferred
  - agree on parameters, capability
    - data rates, listen interval, security, …

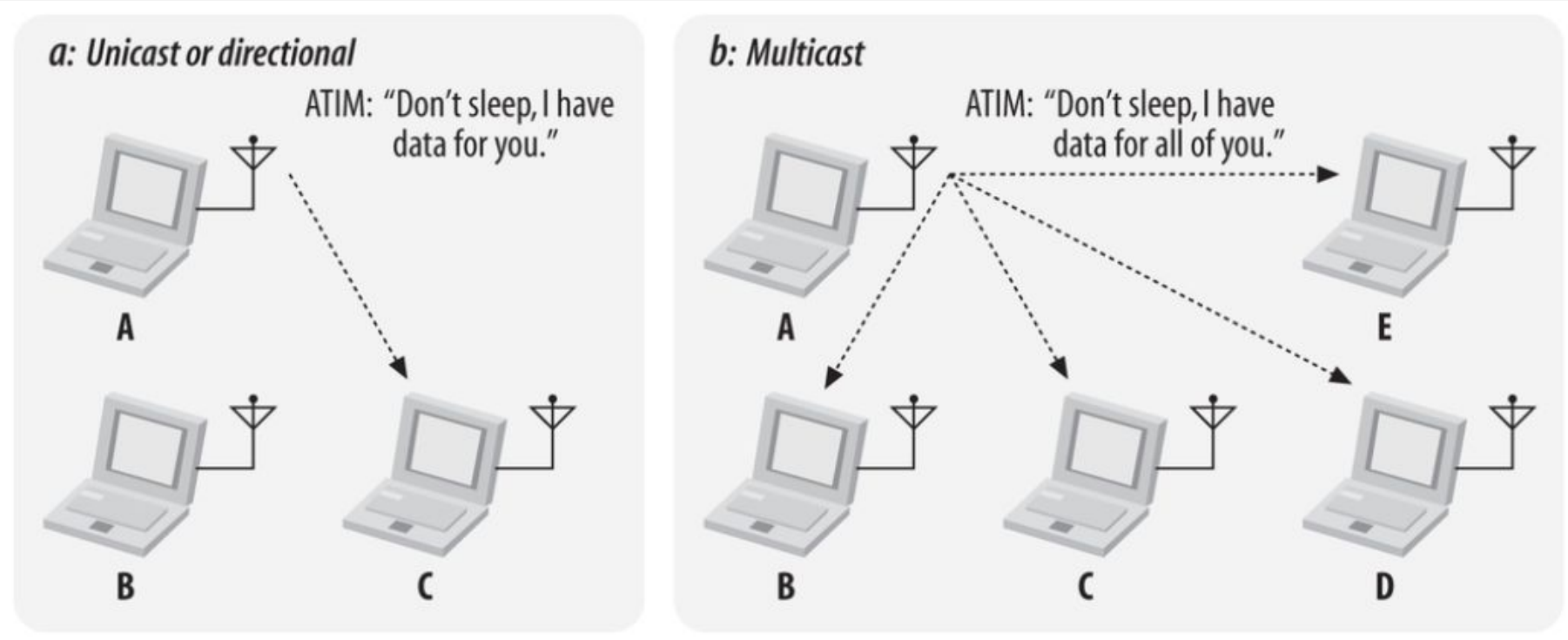
Power Saving

- powering down the transceiver => PS mode/sleeping

- **Infrastructure Networks (AP)**
  - AP agrees on STA's beacon interval, and STA on DTIM period
  - stations must wake up at every DTIM to check buffered frames
    - DTIM (Delivery Traffic Indication Map)
  - buffered frames may be discarded if STA fails to check until listen interval

Power Saving

- **Independent Networks (Ad Hoc)**
  - All stations should listen for ATIM at fixed intervals (ATIM window)
    - ATIM (Announcement Traffic Indication Map)
  - during ATIM window, only Beacons, RTS, CTS and ACK are allowed
    - may transmit data after ATIM window is concluded

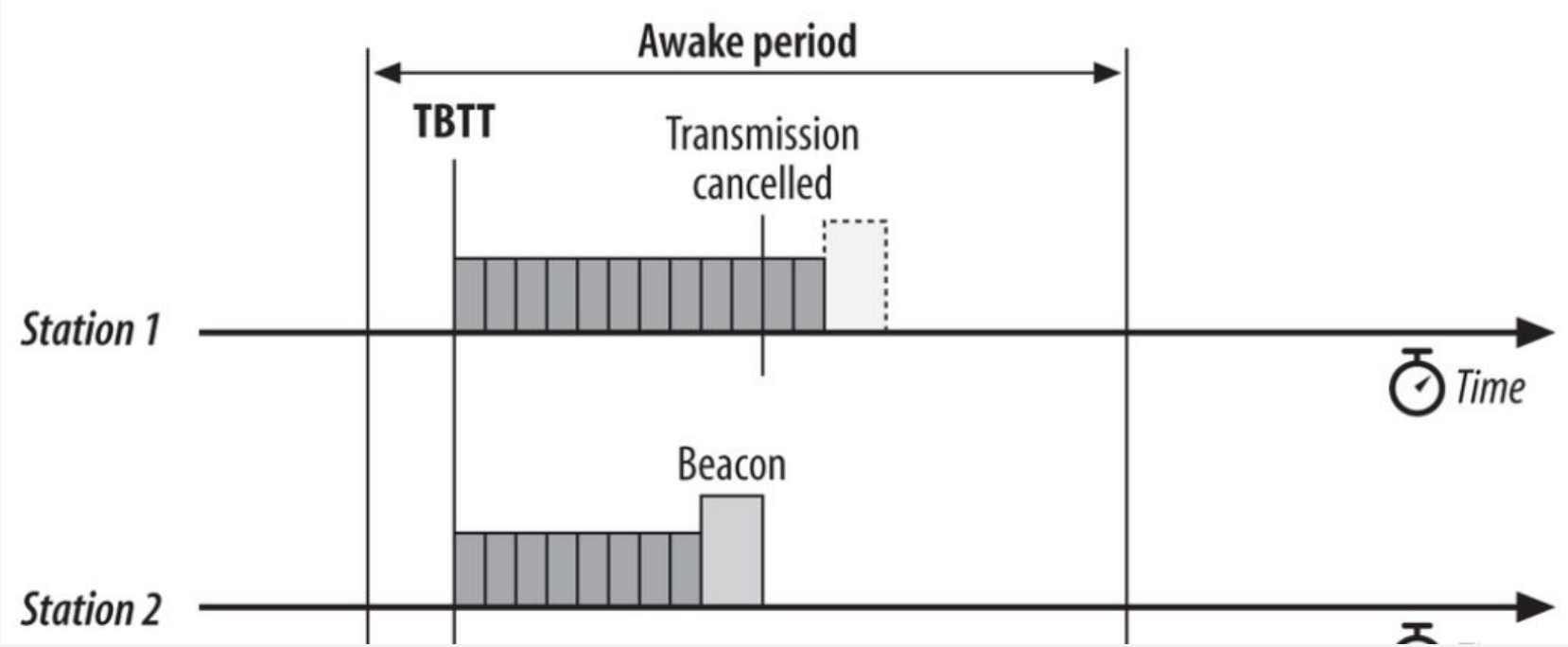


Timer Synchronization

- **Infrastructure Networks (AP)**
  - All stations have identical Timer Synchronization Function (TSF)
    - 1 Mhz clock and ticks in microseconds
  - All stations associated with AP simply adopt AP's TSF
    - maintains local TSF timer in case of occasional loss of beacons
  - Propagation/Processing delay is negligible
    - TSF granularity is in microseconds, so the delay is well within margin

Timer Synchronization

- **Independent Networks (Ad Hoc)**
  - All stations prepare to transmit a Beacon frame at a target time
    - At TBTT(Target Beacon Transmission Time) all stations start begin backoff timer
  - The sender remains awake and reply to Probe Request
  - synchronize the timer to the fastest running clock
    - do not update if TSF value of beacon is smaller than local TSF

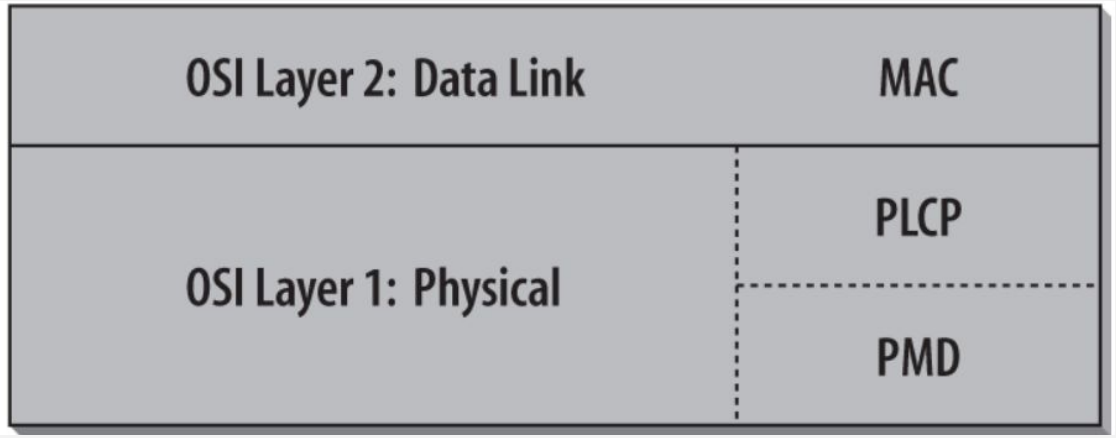


Physical Layer

- Architecture
- FHSS
- DSSS
- OFDM

Architecture

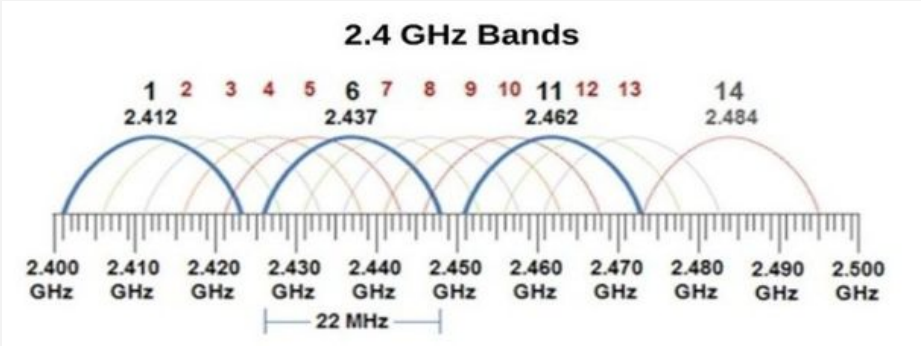
- **Physical Layer Convergence Procedure (PLCP)**
  - adds PHY header to MAC frame
- **Physical Medium Dependent (PMD)**
  - transmits frames received from the PLCP
  - manages antena and carrier sensing

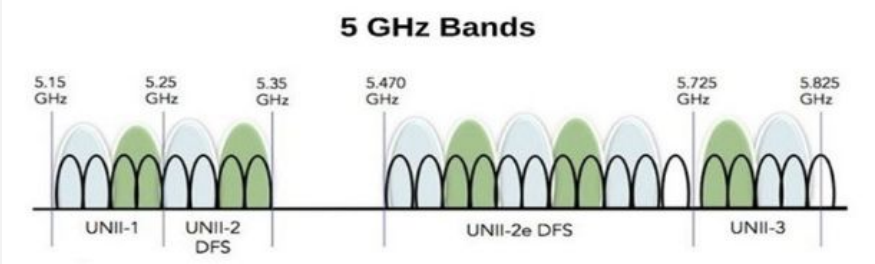


- **Clear Channel Assessment function (CCA)**
  - Energy Detection (is any signal present?)
  - Preamble Detection (is there a valid 802.11 frame?)

Architecture

- **Frequency Band (ISM Band)**
  - 2.4 GHz: 14 channels and 3 non-overlappings
  - 5.0 GHz: up to 24 channels and 24 non-overlappings
    - 20/40/80/160 MHz channel width

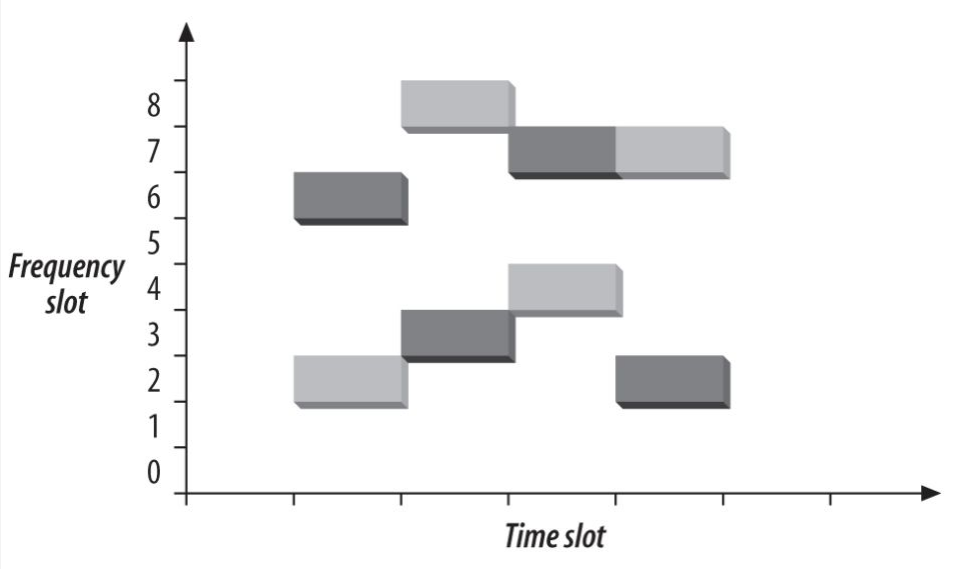


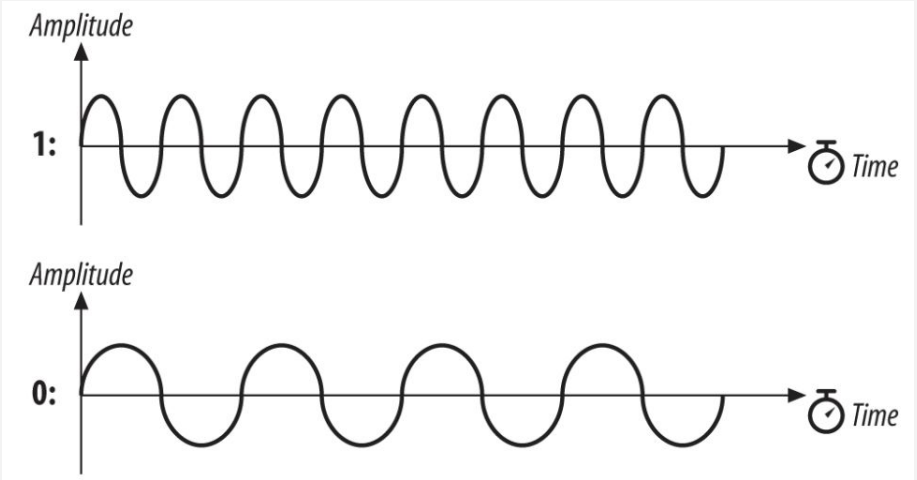


- **Spread Spectrum**
  - spreads signal power over wide frequencies
  - communicating stations should agree on spreading techniques
    - frequency hopping for hopping pattern
    - direct sequence for encoding/decoding function

FHSS

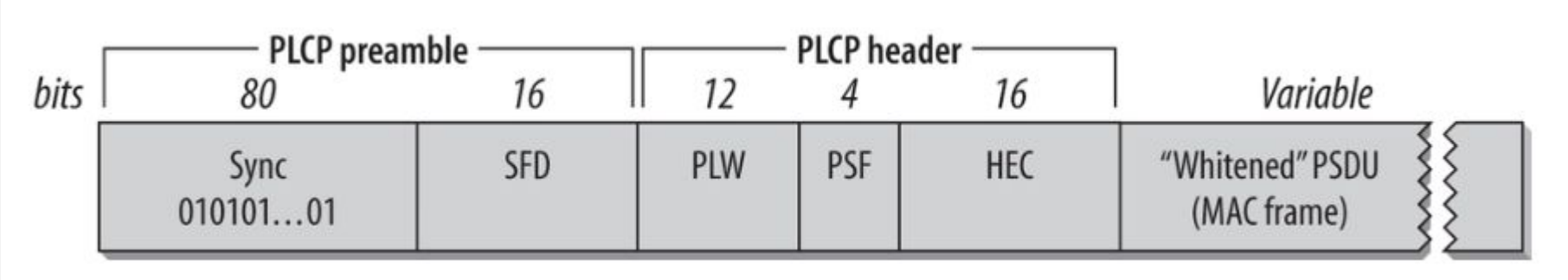
- **Technique**
  - divides ISM band into a series of 1 MHz channels
    - at n bit per cycle, n Mbps is the maximum speed
  - transmits based on hopping pattern
    - uses pre-defined orthogonal hop sequence set
    - agreed upon joining by examining beacon frame
  - supports 1Mbps and 2Mbps (GFSK)
- **Gaussian Frequency Shift Keying (GFSK)**
  - assigns 1/0 bit on different center frequency
  - 2 levels (2GFSK) / 4 levels (4GFSK) encoding





FHSS

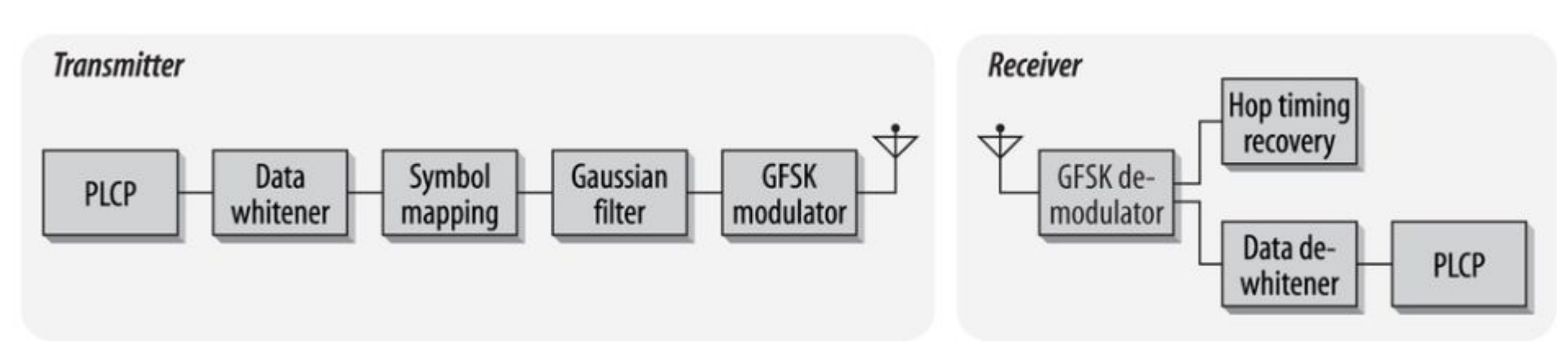
- **FH PLCP Layer**

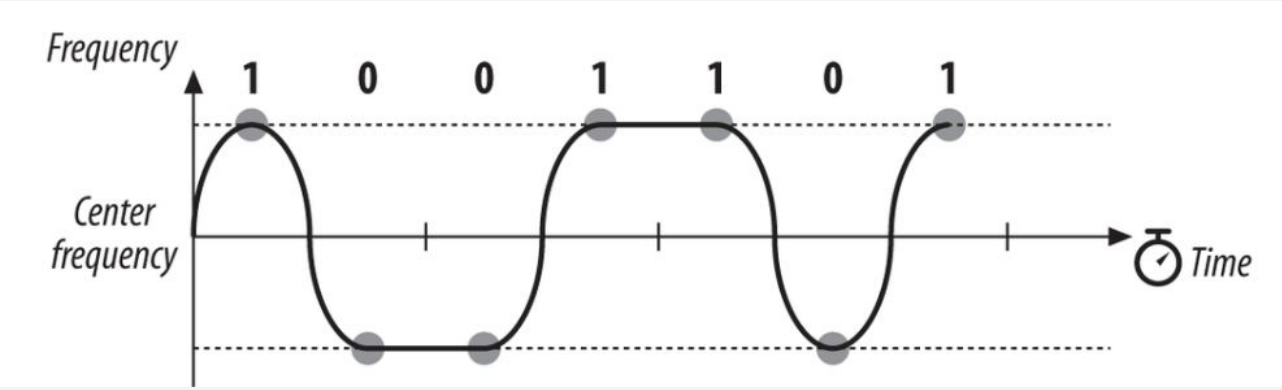


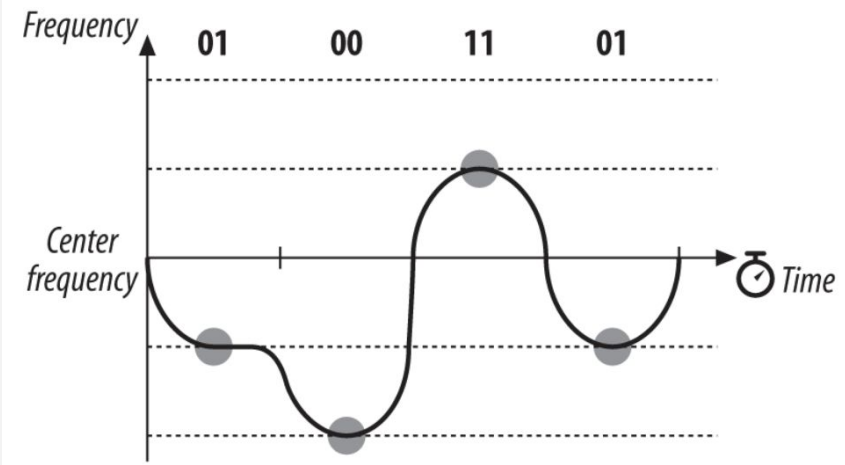
  - **preamble**: a fixed pattern to serve
    - sync the signal indicating a frame is imminent
    - measure the frequency relative to its nominal value (+ correction)
  - **header**: FHSS specific parameters
    - **PSDU** Length: the size of payload
    - **PSF**: data rates at which the PSDU(Mac Frame) is encoded
      - 000 for 1.0 Mbps, 010 for 2.0 Mbps

FHSS

- **FH PMD Layer**

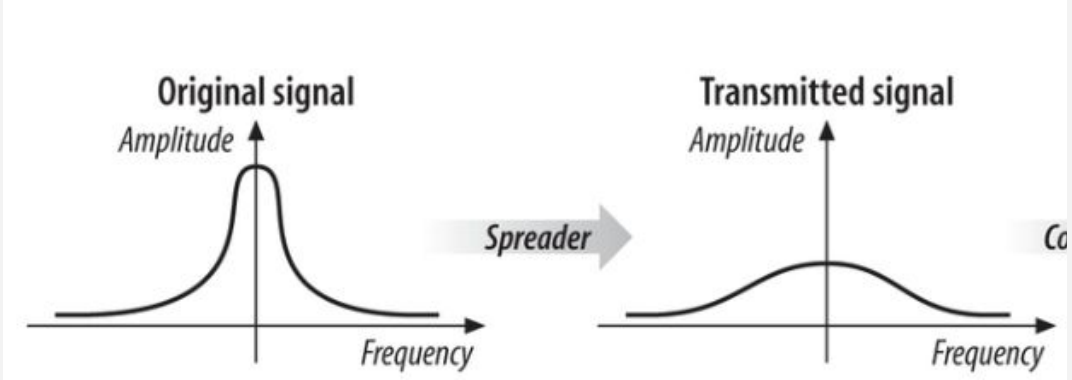




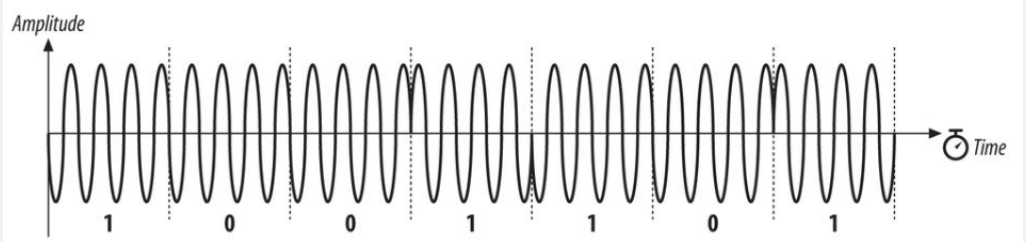


DSSS

- **Technique**
  - applies a chipping sequence to spread narrowband
    - the original signal is recovered with ***correlator***
    - uses barker sequence(11 chips) to encode data
  - tolerant to noise since the long spreading code
  - supports 1Mbps and 2Mbps
    - 5.5Mbps and 11Mbps at 802.11b (1999)

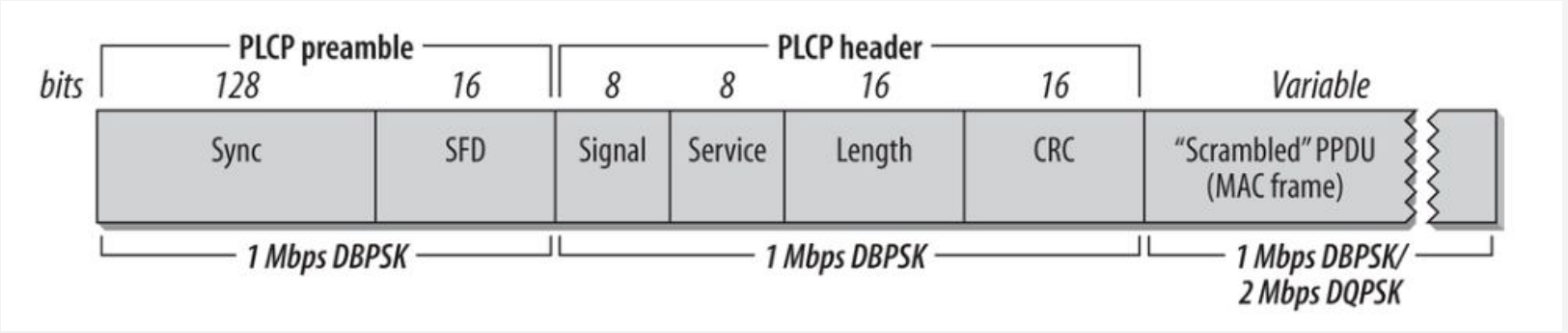


- **Differential Phase Shift Keying (DPSK)**
  - bit representation by shifting the phase
  - cannot be used in severe multipath interference



DSSS

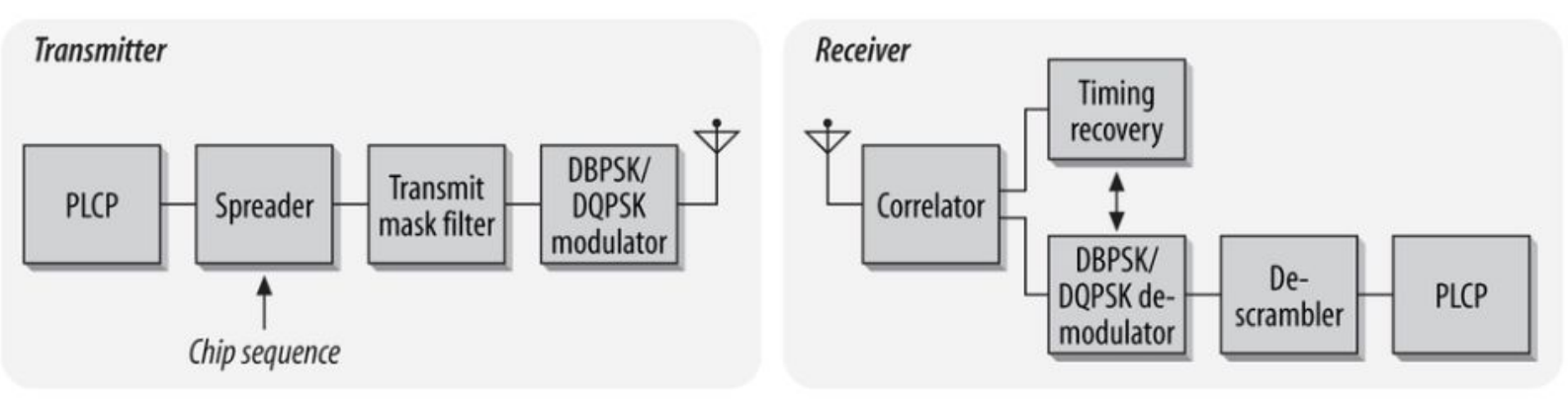
- **DSSS PLCP Layer**

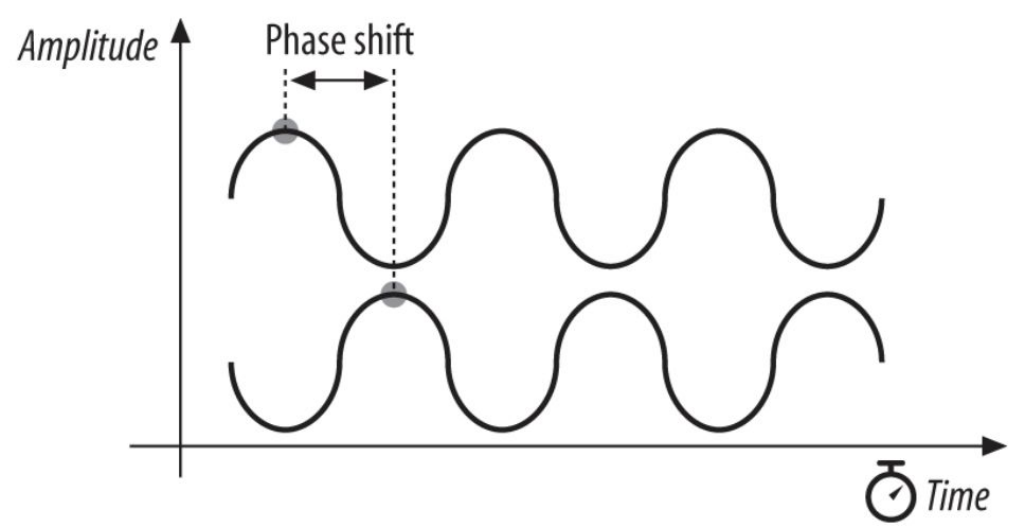


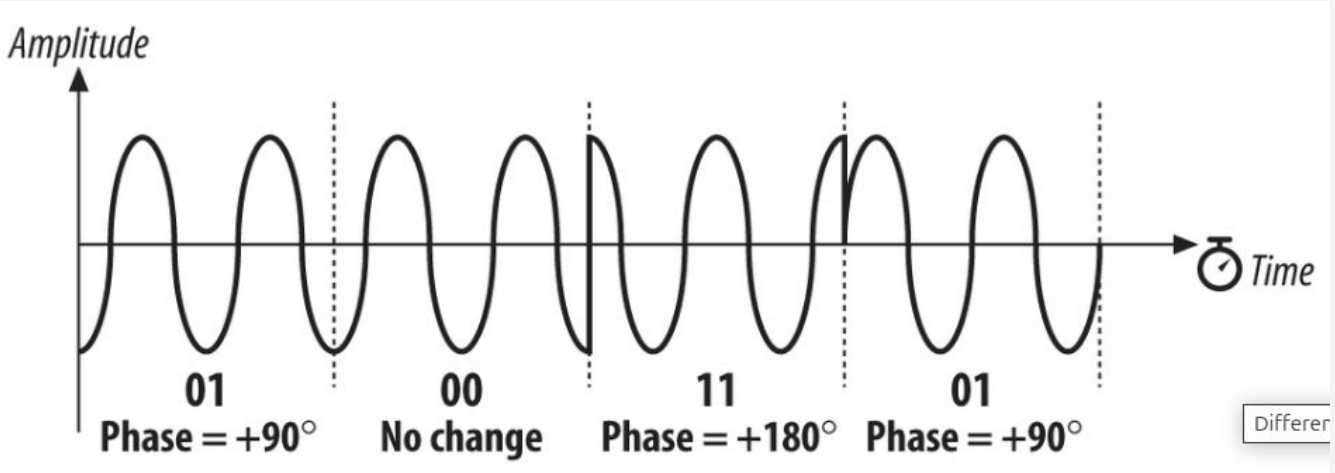
  - **preamble**: same functionality as FHSS's, but scrambled
  - **header**: DSSS specific parameters
    - **Signal**: data rate of DPSK (1Mbps / 2Mbps)
    - **Service**: reserved for future use (all 0s)

DSSS

- **DSSS PMD Layer**

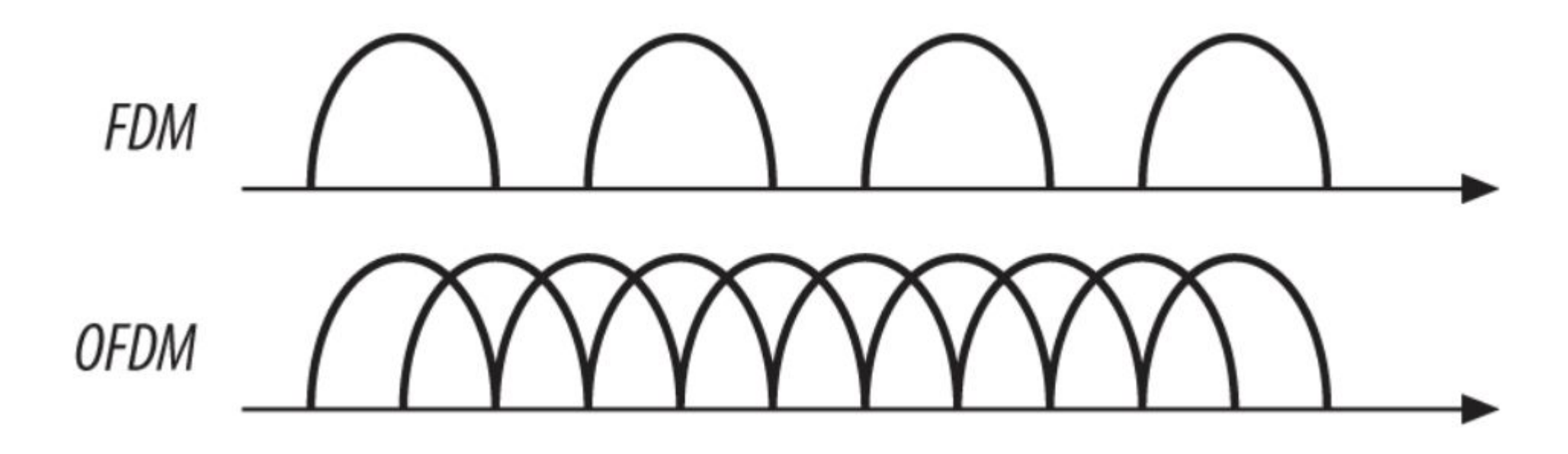






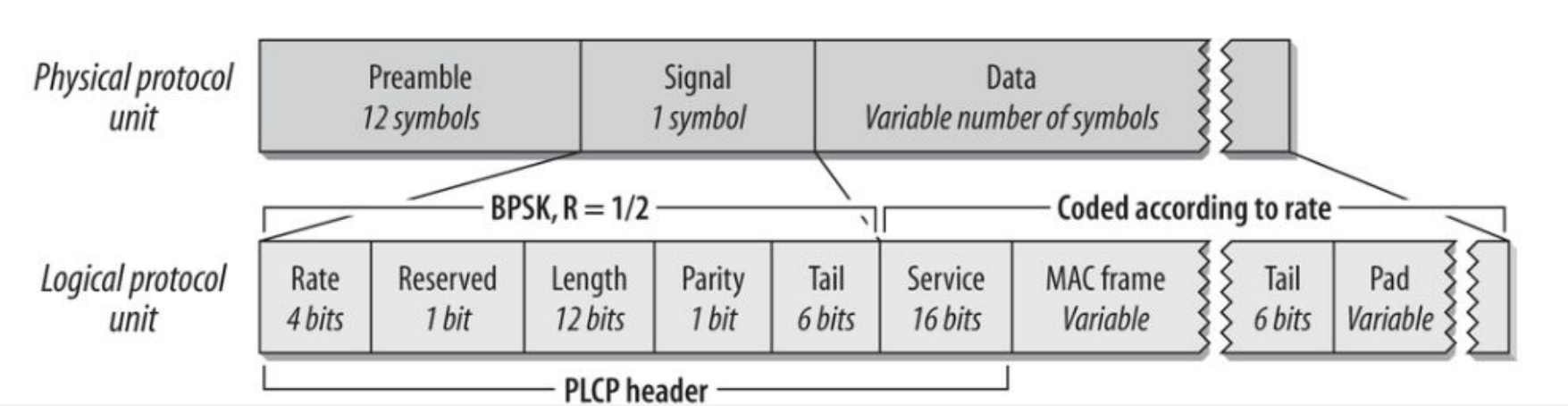
OFDM

- **Orthogonal Frequency Division Multiplexing (OFDM)**
  - multiplexing technique for parallel transmission
    - slow subchannels are combined into large fast channel
  - uses Inverse Fast Fourier Transform(IFFT) to create a composite waveform



OFDM

- **OFDM PLCP Layer**



- **preamble**: composed of 12 OFDM symbols
  - 10 symbols: timing synchronization to lock on to the signal
  - 2 symbols: fine-tune the timing
- **header**:
  - rate : 4bits, 6Mbps to 54Mbps
  - length : 12bits, the size of MAC frame
  - tail: 6 zero bits, unwind the convolutional code

OFDM

- **OFDM PMD Layer**

Speed (Mbps)	Modulation and coding rate (R)	Coded bits per carrier[a]	Coded bits per symbol	Data bits per symbol[b]
6	BPSK, R=1/2	1	48	24
9	BPSK, R=3/4	1	48	36
12	QPSK, R=1/2	2	96	48
18	QPSK, R=3/4	2	96	72
24	16-QAM, R=1/2	4	192	96
36	16-QAM, R=3/4	4	192	144
48	64-QAM, R=2/3	6	288	192
54	64-QAM, R=3/4	6	288	216
72[c]	64-QAM	6	288	288