Wireless Local Area Networks (WLANs) based on IEEE 802.11 Standard
aka
Wi-Fi
Wireless Local Area Networks (WLANs)

• Offers clear benefits over wired LANs:
  – Avoid the inconvenience and cost of running cables
  – Flexible network connectivity: get connectivity where desired instead of having to connect at locations wired network allows

• IEEE 802.11 has become the de facto standard for WLANs
  – Survived the competition from other proposed WLAN technologies and standards (e.g., HiperLAN)

• Now WLANs are synonymous with 802.11 based WLANs (also called Wi-Fi)
  – Wi-Fi is to wireless LANs as Ethernet is to wired LANs
The Success of Wi-Fi

- Contributing factors:
  - **Operation in license exempt (unlicensed) spectrum bands** ➔ no barrier to deployment
  - Continually evolving **standards** aimed at higher data rates and enhanced functionality
  - **Low cost commodity hardware** from reaching economies of scale
## (Partial) History of 802.11 WLANs

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1985</td>
<td>US Federal Communications Commission (FCC) allowed unlicensed use of ISM bands</td>
</tr>
<tr>
<td>1997</td>
<td>First version of 802.11 standard published</td>
</tr>
</tbody>
</table>
| 1999   | - 802.11b and 802.11a amendments supporting higher data rates up to 54Mbps  
        - Wi-Fi Alliance formed to certify interoperability between IEEE 802.11 devices from different manufacturers |
| 2003   | - 802.11g amendment using 802.11a OFDM PHY and supporting up to 54Mbps data rates |
| 2007   | - 802.11-2007 (a new release of the standard) that includes amendments a, b, d, e, g, h, i & j |
| 2009   | - 802.11n amendment with high throughput improvements via MIMO, channel bonding and frame aggregation |
| 2012   | - 802.11-2012 (a new release of the standard) that includes amendments k, n, p, r, s, u, v, w, y and z  
        - 802.11ad amendment to enable very high throughput operation in frequencies around 60GHz ➔ 802.11ay |
| 2013 - | - 2013: 802.11ac amendment with very high throughput enhancements including multi-user MIMO ➔ 802.11ax  
        - 2014: 802.11af amendment supporting operation in Television White Spaces (TVWS)  
        - 2016: 802.11ah for sub 1GHz operation in license-exempt bands  
        - 802.11-2016 (a new release of the standard) that includes amendments ac, ad, af, aa and ae |
Useful 802.11 Links

• Get latest 802.11 standards via:
  – http://ieeexplore.ieee.org/browse/standards/get-program/page/series?id=68

• Official IEEE 802.11 working group project timelines:
  – http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm
IEEE 802.11 Standard Overview

• Defines multiple physical layers (PHYs) and a common medium access control (MAC) layer for WLANs

• Member of IEEE 802 family of local area networking (LAN) and metropolitan area networking (MAN) standards
  – Inherits the 802 reference model and 48-bit universal addressing scheme
802.11 in the TCP/IP Internet Protocol Stack
A Typical Implementation of 802.11 Network Interface

- Frequency conversion
- Amplifier
- Shielding
- (De)modulation
- Physical carrier sensing
802.11 Medium Access Control (MAC) Overview

- 802.11 adopted the distributed MAC protocol based on carrier sense multiple access (CSMA) from Ethernet (the wired counterpart of 802.11)
  - listen/sense medium (carrier) and transmit if idle

- Ethernet uses a CSMA variant called *CSMA with collision detection (CSMA/CD)*
  - Each Ethernet device can receive its own transmission and detect collisions
  - Upon collision detection: stop transmission ➔ random backoff ➔ retry
802.11 Medium Access Control (MAC) Overview

- 802.11 uses a different variant called *CSMA with collision avoidance (CSMA/CA)*
  - Coz half-duplex wireless interfaces do not allow receiving one’s own transmission
  - Moreover, collisions occur on receiver side

- Idea: be conservative in attempting a transmission
  - 802.11 devices on finding a busy medium defer by different randomly chosen periods (counting down only when medium is idle)
# Overview of 802.11 Physical Layers (PHYs)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PHY technology</td>
<td>IR, FHSS and DSSS in 2.4 GHz</td>
<td>DSSS/CCK</td>
<td>OFDM</td>
<td>OFDM &amp; DSSS/CC K</td>
<td>SDM/OFDM</td>
<td>SDM/OFDM and MU-MIMO</td>
</tr>
<tr>
<td>Data rates (Mbps)</td>
<td>1, 2</td>
<td>1, 2, 5.5, 11</td>
<td>6-54</td>
<td>1-54</td>
<td>6.5-600</td>
<td>6.5-6933.3</td>
</tr>
<tr>
<td>Frequency band (GHz)</td>
<td>2.4</td>
<td>2.4</td>
<td>5</td>
<td>2.4</td>
<td>2.4 and 5</td>
<td>5</td>
</tr>
<tr>
<td>Channel widths (MHz)</td>
<td>25</td>
<td>25</td>
<td>20</td>
<td>25</td>
<td>20 and 40</td>
<td>20, 40, 80 and 160</td>
</tr>
</tbody>
</table>

**Key**

- IR: Infrared
- FHSS: Frequency Hopping Spread Spectrum
- DSSS: Direct Sequence Spread Spectrum
- CCK: Complementary Code Keying
- OFDM: Orthogonal Frequency Division Multiplexing
- SDM: Spatial Division Multiplexing
- MU-MIMO: Multi-User MIMO
Exponentially Increasing 802.11 PHY Data Rates

Note that the y-axis is in log-scale
802.11 Network Architecture

- Individual 802.11 devices referred to as stations

- Basic building block: basic service set (BSS)
  - Essentially, a set of stations
Infrastructure BSS

- Special station called **access point (AP)** manages the BSS and connects with other infrastructure BSSs and network infrastructure via a **distributed system (DS)**

- **Extended service set (ESS)**: a set of infrastructure BSSs interconnected by DS
  - Stations within an ESS can address directly at the MAC layer
802.11 WLAN Deployment Scenarios (1)

- **Home** scenario
  - Single BSS, but there can be several other nearby similar BSSs that can cause interference
802.11 WLAN Deployment Scenarios (2)

- Enterprise wireless access scenario
  - ESS with multiple BSSs
802.11 WLAN Deployment Scenarios (3)

- **Hotspots**: airports, coffee shops, hotels, libraries, WLAN deployments in public areas of cities by municipalities
  - Can be indoor or outdoor
802.11 WLAN Deployment Scenarios (4)

• City-wide / Community / neighbourhood mesh networks
  – Essentially, *multihop* version of infrastructure WLAN

• Long-distance Wi-Fi for enabling low cost Internet access in rural and developing regions
Independent BSS (IBSS)

- Stand-alone BSS in which stations form an ad-hoc network, independent of any network infrastructure
Wi-Fi Direct (1)

• Developed by the Wi-Fi alliance for direct communication between Wi-Fi devices
  – Could be achieved via IBSS in 802.11 standard
  – But Wi-Fi direct aims to achieve this in a form that is similar to that of commonly used infrastructure BSS

• Wi-Fi Direct operation:
  – One device takes the role of group owner (GO), similar to that of AP
  – Rest of the devices associate with GO as they would with an AP
Wi-Fi Direct (2)

• Differences with infrastructure BSS in vanilla 802.11:
  – GO does not provide access to a distribution system
  – GO can be mobile, battery operated device and can enter a low power sleep state when idle

• Wi-Fi Direct standard
  – Builds on the 802.11 specification
  – Additional protocols for:
    ➢ device discovery
    ➢ group owner election
    ➢ protocol for absence from session channel (to save power, for example)
802.11a/b/g Channels (UK)

- Both 2.4GHz and 5GHz bands used by 802.11 are unlicensed (license-exempt)
  - 2.4GHz band used for 802.11b/g relatively more crowded whereas shorter range in 5GHz 802.11a bands (recall: increase in free-space loss by 6dB when frequency is doubled)

Source: Kawade-Hodgkinson'07
Transmit Spectrum Mask

- To limit power leakage into adjacent channels

Transmit spectrum mask for 802.11a
802.11b

- Based on Direct Sequence Spread Spectrum (DSSS)
- Like CDMA but with common chipping sequence (spreading code) for all users

<table>
<thead>
<tr>
<th>Bit-rate (Mbps)</th>
<th>Modulation and coding rate (R)</th>
<th>Data bits per symbol&lt;sup&gt;b&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>BPSK, R=1/11</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>QPSK, R=1/11</td>
<td>2</td>
</tr>
<tr>
<td>5.5</td>
<td>CCK&lt;sup&gt;a&lt;/sup&gt;, R=4/8</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>CCK, R=4/8</td>
<td>2</td>
</tr>
</tbody>
</table>

<sup>a</sup> Complementary Code Keying

<sup>b</sup> Symbol (chipping) rate is 1 Mega symbols (11 Mega chips) per second
802.11a/g

- Based on OFDM (Orthogonal Frequency Division Multiplexing), which is more spectrally efficient and robust to multipath fading
- Total 52 subcarriers for a 20MHz channel
  - 48 subcarriers used for data and the remaining 4 are pilot subcarriers for synchronization
### 802.11a/g Bit-Rates

<table>
<thead>
<tr>
<th>Bit-rate (Mbps)</th>
<th>Modulation and coding rate (R)</th>
<th>Coded bits per sub-carrier&lt;sup&gt;a&lt;/sup&gt;</th>
<th>Coded bits per symbol</th>
<th>Data bits per symbol&lt;sup&gt;b&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>BPSK, R=1/2</td>
<td>1</td>
<td>48</td>
<td>24</td>
</tr>
<tr>
<td>9</td>
<td>BPSK, R=3/4</td>
<td>1</td>
<td>48</td>
<td>36</td>
</tr>
<tr>
<td>12</td>
<td>QPSK, R=1/2</td>
<td>2</td>
<td>96</td>
<td>48</td>
</tr>
<tr>
<td>18</td>
<td>QPSK, R=3/4</td>
<td>2</td>
<td>96</td>
<td>72</td>
</tr>
<tr>
<td>24</td>
<td>16-QAM, R=1/2</td>
<td>4</td>
<td>192</td>
<td>96</td>
</tr>
<tr>
<td>36</td>
<td>16-QAM, R=3/4</td>
<td>4</td>
<td>192</td>
<td>144</td>
</tr>
<tr>
<td>48</td>
<td>64-QAM, R=2/3</td>
<td>6</td>
<td>288</td>
<td>192</td>
</tr>
<tr>
<td>54</td>
<td>64-QAM, R=3/4</td>
<td>6</td>
<td>288</td>
<td>216</td>
</tr>
</tbody>
</table>

<sup>a</sup> Coded bits per sub-carrier is dependent on the modulation scheme used (BPSK, QPSK, 16-QAM, or 64-QAM).

<sup>b</sup> The data bits per symbol is determined by the rate of the convolutional code.

250,000 symbols per second across 48 subcarriers (that together make up a symbol)
Role of Bit-Rate and Frame Length Selection for Efficient and Reliable Transmission

• Recall:
  – Throughput = bit-rate \times (1 - \text{FER}) = \text{bit-rate} \times (1 - \text{BER})^L, where L is the frame length
  – Higher bit-rates require higher SNR to keep BER under a desirable threshold (e.g., 10^{-5})

• But channel (and hence, channel quality metrics such as SNR) are time varying

• So need to adapt bit-rate with SNR (or other easily measurable channel quality metrics at transmitter side such as FER)
Adaptive Bit-Rate Selection (or simply, Rate Adaptation)

- Mechanism not specified in standard, instead left to vendor/user discretion
- Issues:
  - Channel quality measurement
  - Responsiveness in dynamic environments
  - Separating channel induced losses from collision/interference losses
    - Because rate adaptation appropriate only for channel losses

1. SNR decreases (e.g., as node moves away from AP), BER increases
2. When BER becomes too high, switch to lower bit-rate with lower BER
802.11 Multiple Access Overview

• Core mechanism is distributed and based on contention based random access
  – Called Distributed Coordination Function (DCF)

• Collision detection (CD) at transmitter as in Ethernet (or 802.3) not possible due to half-duplex radios and receiver-side interference
  – Need acknowledgement (ACK) from receiver; missing ACK used to infer collisions and other types of frame losses (e.g., channel induced bit errors)
  – Need to transmit collided frames in entirety

• So adopt a collision avoidance approach
  – Specifically, carrier sense multiple access with collision avoidance (CSMA/CA)
  – Still bears similarity with Ethernet’s CSMA/CD approach due to use of CSMA and exponential backoff (upon frame transmission failure)
802.11 Multiple Access Ingredients

• **CSMA**
  - Sense if medium idle (e.g., via signal energy detection)
    - This physical carrier sensing referred to as Clear Channel Assessment (CCA) in 802.11

• **Collision avoidance via:**
  - Random backoffs
  - Inter frame spaces (IFSs)
  - Virtual carrier sensing using Network Allocation Vector (NAV) to complement physical carrier sensing (CCA)
  - (Optional) RTS/CTS mechanism to mitigate hidden terminal problem

• **Loss recovery / reliability via:**
  - Receiver ACKs for successful frame transmissions
  - Failed frames retransmitted with exponential backoffs
  - Multiple physical layer bit-rates, each using different modulation and coding scheme (MCS)
  - Option of frame fragmentation for shorter sized frames
Inter Frame Spaces for Prioritised Channel Access

- Short inter-frame space (SIFS) = \( a_{SIFS} \text{Time} = 16\mu s \) with 802.11a/g/n/ac PHYs
- Slot time = \( a_{Slot} \text{Time} = 9\mu s \) with 802.11a/g/n/ac PHYs
- PCF IFS (PIFS) = \( a_{SIFS} \text{Time} + a_{Slot} \text{Time} \)
- DCF IFS (DIFS) = \( a_{SIFS} \text{Time} + 2 \times a_{Slot} \text{Time} \)
802.11 CSMA/CA Protocol

I. When a station has a frame to transmit:
   1. If medium busy, then choose a random backoff counter between 0 and CW (initially, \( CW_{\text{min}} \)) slots; \( CW_{\text{min}} = 15 \) with 802.11a/g/n/ac PHYs
      a. Random backoff counter counts down to zero only during idle slots (i.e., medium idle for DIFS period); pauses otherwise. When counter reaches 0, then transmit frame
   2. Else: if medium stays idle for another DIFS period and backoff counter is 0, then transmit frame

II. On the receiver side:
   – If frame received correctly then transmit ACK after SIFS period

III. If no ACK received at transmitter then:
   a. Double the backoff interval \( CW \) unless \( CW = CW_{\text{max}} \) (1023 with 802.11a/g/n/ac PHYs) \( \Rightarrow \) exponential backoff
   b. Attempt a retransmission by following step 1.a until frame transmission successful or max. retransmission limit reached

IV. If ACK received at transmitter and has another frame to transmit, then follow step 1 regardless of medium busy or idle (i.e., random backoff, countdown and transmit)

Note that ACK frames use a lower PHY data rate compared to the corresponding data frame for extra reliability
802.11 CSMA/CA Protocol Illustrated

Station A sends to D

D acks A

B ready to send

Wait for idle

Backoff

C ready to send

Wait for idle

Backoff

B sends to D

D acks B

C sends to D

D acks C

Rest of backoff

Data

Ack

Data

Ack

Time
Virtual Carrier Sensing

• Via a “virtual medium busy timer” variable called Network Allocation Vector (NAV) maintained independently and internally at each node (AP or station)

• Every node’s NAV keeps track its notion of medium usage by looking at the value of duration field in overheard frames (even those not destined to it)

• Non-zero NAV is taken to mean medium is busy regardless of what physical carrier sensing (CCA) sees
  – Can be seen as MAC level carrier sensing

• E.g.,
  – Upon hearing a DATA frame, NAV extended (at least) till the time required for completion of ACK transmission corresponding to the DATA frame
  – As a result, each hearing node (not just the intended receiver) considers the medium to be busy even if it does not hear the following ACK frame
RTS/CTS Mechanism

- Optional, to mitigate hidden terminal problem
- Leverages NAVs

Idea: use short control frames, request-to-send (RTS) and clear to send (CTS), upfront to reserve the medium around transmitter and receiver for the ensuing data frame transmission

Example in above figure:
- A wants to transmit frame to B; C within range of A (and possibly B) but D only within range of B
RTS/CTS frames can also experience collisions; dealt the same way as with DATA frames.
RTS/CTS Mechanism: Discussion

• Not found to be very useful in practice
  – Not helpful for shorter frames or AP frames
  – Does not help with exposed terminals
• Physical/virtual carrier sensing can largely prevent potential hidden terminal collisions; besides, unsuccessful transmitters are automatically slowed down with basic CSMA/CA because of stop-and-wait ARQ mechanism with exponential backoffs
• So additional benefit from using RTS/CTS for hidden terminals marginal, especially when considering the extra delay and handshake overhead
• This changes with newer high throughput 802.11 standards (e.g., 802.11n/ac) with very large aggregated frames
Extended Inter-Frame Space (EIFS)

- Another mechanism to protect against hidden nodes
- EIFS = aSIFSTime + ACKTxTime + DIFS

where ACKTxTime is the time required to transmit an ACK at the lowest mandatory PHY data rate
Finding, joining and leaving a BSS

• **Scanning** for a station to discover a BSS and its attributes
  1. Passive
  2. Active

• **(Re-/Dis-)Association**
  – By associating with an AP, a station becomes a member of the BSS represented by the AP
  – By disassociating, it leaves the BSS
  – In an ESS with multiple BSSs, a station can move from one BSS and reassociate with another BSS
Beacons

• Each AP periodically broadcasts beacon frames, typically every 100ms
• Each beacon carries regulatory info, capability info, and info for managing the BSS:
  – Network/ESS identifier (SSID)
  – AP/BSS identifier (BSSID)
  – Country code info
  – Maximum allowable transmit power
  – Allowed channels
  – time reference
  – time till next beacon
  – bit-rates supported
  – security settings
  – power-saving capabilities
  – QoS support
  – ...

Target Beacon Transmission Time (TBTT)

- Beacons scheduled every TBTT
- Actual transmission time of beacons depends on whether channel is idle at scheduled time
AP and Station Channel Assignment

- Each AP operates on a channel in a band (e.g., 2.4GHz, 5GHz)
- The channel used by an AP depends on its hardware capability and channel assignment procedure in use (default setting, manual configuration, automatic and adaptive channel selection)
- Channel used by a station implicitly chosen depending on the AP it associates with
- Neighboring APs (and their associated stations) could interfere with each other depending on their channels of operation
Passive Scanning

• A station looks for beacon transmissions in all channels, by repeating the following process:
  – dwelling for some time in each channel, then switching to another channel

• Passive (receive only) operation

• Compatible with all regulatory domains

• May need to follow it up with active scanning if additional info required
Active Scanning

• Actively probe for a BSS using **Probe Request and Probe Response messages**

• **A station transmits** **Probe Request frames on each of the channels it is seeking a BSS**, including the following addresses in the request:
  – SSID: specific or wild card
  – BSSID: specific or wild card
  – Destination Address (DA): broadcast MAC address (FF:FF:FF:FF:FF:FF)

• **AP receiving a Probe Request responds with a Probe Response if its SSID and BSSID match with that in request**

• **Multiple APs may respond to a Probe Request**
802.11 Association

• Note that scanning (passive or active) may lead to discovery of one or more APs (BSSs)

• AP selection problem: selecting an AP if more than one discovered
  – AP selection mechanism left unspecified in the standard
  – Could be based on signal strength, load, etc.

• Before a station can send/receive data, it must:
  – Associate with the selected AP
  – Then get an IP address (in the associated AP’s subnet), typically via DHCP
Scanning + Association Illustrated

Passive Scanning:
1. Beacon frames sent periodically from APs
2. Association Request frame sent from H1 to selected AP
3. Association Response frame sent from Selected AP to H1

Active Scanning:
1. Probe Request frame broadcast from H1
2. Probe Response frames sent from APs
3. Association Request frame sent from H1 to selected AP
4. Association Response frame sent from Selected AP to H1
Reassociation and Disassociation

• Reassociation
  – Happens when:
    ➢ Station moves to a new BSS served by an AP different from the one it is associated with
    ➢ To change attributes of station association such as station capability info
  – Initiated by station (Reassociation Request to AP seeking a Reassociation Response)

• Disassociation
  – When leaving the network or loss of communication
  – Explicitly performed (by either AP or station) by sending Disassociation frame and seeking acknowledgement
  – Implicitly via timeout at AP
802.11 Mobility Support

**BSS Transition**

**ESS Transition**
802.11 Mobility Within Same Subnet (Intra-ESS)

- H1 remains in same IP subnet: IP address can remain same
- Switch: H1 associated with which AP?
  - self-learning: switch will see incoming frames from H1 and “remember” which switch port can be used to reach H1
802.11 Authentication

- Establish the identity of the station before it is allowed to communicate
- Broadly speaking, two authentication methods:
  1. Open system authentication (*prior* to Association)
     - Station joining the BSS sends an Authentication frame requesting open system authentication
     - AP responds with an Authentication frame with status “success”
  2. Shared key authentication
     - Initially, Wired Equivalent Privacy (WEP) which was found to be insecure in 2001
     - Currently used approach from the 802.11i (WPA2) amendment from 2004
       - Authentication *after* Association
Authentication and Association Process Illustrated

802.11 open system authentication

Security parameter exchange: STA determines whether PSK or 802.1X authentication applies

802.1X authentication, if needed

4-Way Handshake, if needed

Authentication

Authentication

Association Request

Association Response

EAP-Request/Identity

EAP-Response/Identity

Mutual authentication

EAP-Success

Key Message 1

Key Message 2

Key Message 3

Key Message 4

Data transfer

Request

Accept
802.1X Authentication

• Station to access a BSS authenticates with an authentication server (AS) using extensible authentication protocol (EAP)
  – AS may be co-located with AP or on a separately located server

• Multiple options for the authentication method:
  – EAP-Transport Layer Security (EAP-TLS) often used
  – Lightweight Extensible Authentication Protocol (LEAP)
  – EAP-MD5
802.11i Operation

Following Association Request/Response exchange:
- AP sends an EAP Request challenging the station to identify itself
- Station responds with an EAP Response that is forwarded to the AS
- EAP authentication exchange between station and AS via AP to mutually authenticate each other and derive a Master Key (MK) known to both
  - A second key called Pairwise Master Key (PMK) is generated from MK
- On successful authentication of station:
  - AS informs this to AP along with PMK
  - AP then forwards EAP−Success to station → AP and station mutually authenticated and have a shared key
- If authentication fails:
  - AS informs the AP which sends an EAP−Failure message to station followed by Disassociation frame
Transient Keys

• Data frames are encrypted using transient keys, regenerated using PMK periodically (typically, every 24 hours)

• **Pairwise transient key (PTK)** to protect traffic between AP and station

• **Group transient key (GTK)** to protect broadcast and multicast traffic from AP
Transient Key Generation

• Four/two-way handshake for station and AP to derive PTK/GTK
  
  - **Key Message 1 (AP to station):** station derives PTK using ANonce from AP + locally generated SNonce + knowledge of PMK
  
  - **Key Message 2 (station to AP):**
    - AP derives PTK using SNonce from station + previously locally generated ANonce + knowledge of PMK
    - AP confirms that station knows PTK using the message integrity check (MIC) in message generated using PTK by station
  
  - **Key Message 3 (AP to station):** GTK encrypted using PTK + MIC sent to station
  
  - **Key Message 4 (station to AP):** confirms receipt of GTK and authentication of AP
MAC and PHY Data Units

• Service Data Unit (SDU) refers to data transferred between layers
  – MAC SDU (MSDU)
  – PHY SDU (PSDU)

• Protocol Data Unit (PDU) refers to data exchanged by peer entities of the same layer
  – MAC PDU (MPDU) = MAC header + MSDU + trailer (frame check sequence) = PSDU
  – PHY PDU (PPDU) = Preamble + PHY header + PSDU
MAC Frame Format

- Protocol Version subfield always set to 00
<table>
<thead>
<tr>
<th>Type</th>
<th>Type description</th>
<th>Subtype</th>
<th>Subtype description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>Management</td>
<td>0000</td>
<td>Association Request</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0001</td>
<td>Association Response</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0010</td>
<td>Reassociation Request</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0011</td>
<td>Reassociation Response</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0100</td>
<td>Probe Request</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0101</td>
<td>Probe Response</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0110-0111</td>
<td>Reserved</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1000</td>
<td>Beacon</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1001</td>
<td>ATIM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1010</td>
<td>Disassociation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1011</td>
<td>Authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1100</td>
<td>Deauthentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1101</td>
<td>Action</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1110</td>
<td>Action No Ack</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1111</td>
<td>Reserved</td>
</tr>
<tr>
<td>01</td>
<td>Control</td>
<td>0100</td>
<td>Beamforming Report Poll</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0101</td>
<td>VHT NDP Announcement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0111</td>
<td>Control Wrapper</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1000</td>
<td>Block Ack Request</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1001</td>
<td>Block Ack</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1010</td>
<td>PS-Poll</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1011</td>
<td>RTS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1100</td>
<td>CTS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1101</td>
<td>ACK</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1110</td>
<td>CF-End</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1111</td>
<td>CF-End + CF-Ack</td>
</tr>
<tr>
<td>10</td>
<td>Data</td>
<td>0000</td>
<td>Data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0001</td>
<td>Data + CF-Ack</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0010</td>
<td>Data + CF-Poll</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0011</td>
<td>Data + CF-Ack + CF-Poll</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0100</td>
<td>Null (no data)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0101</td>
<td>CF-Ack (no data)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0110</td>
<td>CF-Poll (no data)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0111</td>
<td>CF-Ack + CF-Poll (no data)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1000</td>
<td>QoS Data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1001</td>
<td>QoS Data + CF-Ack</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1010</td>
<td>QoS Data + CF-Poll</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1011</td>
<td>QoS Data + CF-Ack + CF-Poll</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1100</td>
<td>QoS Null (no data)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1101</td>
<td>Reserved</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1110</td>
<td>QoS CF-Poll (no data)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1111</td>
<td>QoS CF-Ack + CF-Poll (no data)</td>
</tr>
</tbody>
</table>
# To/From DS

<table>
<thead>
<tr>
<th>From DS</th>
<th>To DS</th>
<th>Meaning</th>
</tr>
</thead>
</table>
| 0       | 0     | Indicates:  
- a data frame direct from one station to another within the same IBSS  
- a data frame direct from one non-AP station to another non-AP station within the same BSS  
- all management and control frames |
| 0       | 1     | A data frame destined for the distribution system (DS) or being sent by a station associated with an AP to the Port Access Entity in that AP |
| 1       | 0     | A data frame exiting the DS or being sent by the Port Access Entity in an AP |
| 1       | 1     | A data frame using the four-address format (not defined in the standard) |
Duration and Address Fields

- **Duration/ID:**
  - If less than 32,768 then interpreted as a duration in $\mu$s to update NAV
  - If the two high order bits are set in PS-Poll frame then low order 14 bits are interpreted as association identifier (AID)

- **Address 1:** receiver address, present in all frames

- **Address 2:** transmitter address, present in all frames except CTS and ACK

- **Address 3:** present in data and management frames
  - In data frame, dependent on To/From DS settings and MSDU/A-MSDU
  - In management frame, address 3 contains BSSID

- **Address 4:** present only in data frames and only when both From/To DS bits are set

![MAC Header Diagram]
A Use of “Address 3”

Internet

router

AP

H1

R1

AP MAC addr  H1 MAC addr  R1 MAC addr

address 1  address 2  address 3

802.11/Wi-Fi frame

802.3/Ethernet frame
Fragmentation

- Allows a large MSDU to be divided into smaller data fragments, each encapsulated in a MPDU.
- Individual MPDUs containing the fragments of a MSDU can be sent separately, or in a burst upon gaining access to channel as shown here.
- MSDU is fragmented if it is longer than `dot11FragmentationThreshold`.
Sequence Control Field

• Duplicate detection via:
  – Sequence numbers for duplicate detection
    - Start from 0 and are assigned from a modulo-4096 counter
  – Retry subfield
    - Set to 1 in any data or management frame that is a retransmission
    - Set to 0 in all other frames
    - Receiver uses this bit while eliminating duplicate frames

• When a MSDU is fragmented, MPDUs with fragments are given different fragment numbers in sequence starting from 0 but share the same sequence number
  – More Fragments subfield set to 1 in all data or management frames if another fragment to follow, otherwise set to 0
Power Management

• 802.11 radio interface that is idle and listening consumes nearly as much power as when receiving and marginally lower than when it is transmitting
• Turning off the radio altogether leads to greater power savings
  – Which is essentially how stations can save power using 802.11 power management features
• Broadly speaking, a station can be in one of two modes:
  – Power Save (PS) mode: in this mode, a station alternates between Awake state and Doze (Sleep) state
  – Active mode (i.e., always awake)
• AP always in active mode
• A station indicates its mode to its AP via the “Pwr Mgt” bit in Frame Control field
Unicast Traffic and Traffic Indication Map (TIM)

- AP buffers frames addressed to stations in PS mode
- Traffic indication map (TIM) in every beacon frame used to indicate buffered traffic to a station in PS mode
  - TIM is a partial virtual bitmap: each bit represents a station on the BSS
  - A station identified in the TIM by the bit position indexed by its association ID (AID)
  - First bit (AID = 0) used for group addressed (broadcast/multicast traffic)
- All stations in PS mode wake up periodically to receive beacon frames
- If a station has buffered frames waiting at the AP as indicated via TIM then
  - It remains awake and polls AP to receive one or more buffered frames (“More Data” bit in Frame Control field), then go back to doze state
Group Addressed Traffic and Delivery TIM (DTIM)

- AP also delivers group addressed (broadcast/multicast) traffic at predictable intervals to allow stations in PS mode to receive
- Delivery TIM (DTIM) in every $n$th beacon frame
  - Indicates group addressed traffic will be delivered immediately following the beacon with DTIM
- DTIM Count in a beacon frame indicates #beacons until next DTIM
  - DTIM Count = 0 in beacon frame with DTIM
  - All non-DTIM beacons have non-zero DTIM Count
- DTIM interval is the interval between beacons carrying DTIM
- Multiple buffered group addressed frames are delivered one after another using the “More Data” bit in a similar way to delivery of multiple buffered unicast frames
• In this example:
  - DTIM Count = 0 in 1\textsuperscript{st} Beacon
  - DTIM Count = 2 in 2\textsuperscript{nd} Beacon
  - DTIM Count = 1 in 3\textsuperscript{rd} Beacon
  - DTIM Count = 0 in 4\textsuperscript{th} Beacon
Automatic Power Save Delivery (APSD)

- Introduced in 802.11e amendment (2005)

- AP buffers frames until the station wakes up when it needs to send frames to the AP

- Allows more flexible and fine-grained sleep schedule
  - Works well for interactive applications like VoIP with bidirectional traffic pattern
  - A VoIP phone can send and receive frames every 20ms and sleep in between (instead of having to wake up at beacon frame arrival times, which are typically every 100ms)
WNM-Sleep Mode

• Introduced in 802.11u amendment (2011)

• Allows a station to miss DTIMs without missing associated group addressed traffic

• To support a station using this mode (indicated to AP via TFS request frame), AP converts group addressed frames to equivalent unicast frame addressed to that station
802.11 Power Management: Discussion

- Even if a station wakes up to receive every beacon, significant energy savings possible, especially when at times of no buffered traffic
  - E.g., ~250 microseconds (=0.25ms) wakeup period to receive beacon frames every beacon interval (typically 100ms) ➔ sleep more than 99% of the time!

- Standard does not define which beacon frames a station should receive ➔ even greater power savings can be achieved at the expense of increased latency
Enhanced Distributed Channel Access (EDCA)

- Introduced in 802.11e amendment (2005) to support prioritised Quality of Service (QoS)
- Defines four access categories (ACs) representing four different traffic types: background, best effort, video and voice traffic
- Other key new features introduced in 802.11e:
  - Transmit opportunity (TXOP) concept
  - QoS Data frame = regular Data frame + QoS Control field
  - Block acknowledgements
• Each AC has:
  – a logically separate queue at MAC layer
  – different settings for access parameters (contention window, inter-frame space, etc.)

<table>
<thead>
<tr>
<th>Priority</th>
<th>802.ID user priority</th>
<th>802.ID Designation</th>
<th>AC</th>
<th>Designation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lowest</td>
<td>1</td>
<td>BK</td>
<td>AC_BK</td>
<td>Background</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td></td>
<td>AC_BE</td>
<td>Best effort</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>BE</td>
<td>AC_BE</td>
<td>Best effort</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>EE</td>
<td>AC_BE</td>
<td>Best effort</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>CL</td>
<td>AC_VI</td>
<td>Video</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>VI</td>
<td>AC_VI</td>
<td>Video</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>VO</td>
<td>AC_VO</td>
<td>Voice</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>NC</td>
<td>AC_VO</td>
<td>Voice</td>
</tr>
</tbody>
</table>
Transmit Opportunity (TXOP)

• A bounded period during which a station may transfer data of a particular traffic class (AC)

• Obtained using the access parameters of the traffic class (AC) that will use it

• Once obtained, station may continue to transmit and receive frames provided frame sequence duration does not exceed TXOP limit for that AC

• **TXOP = 0** (the default prior to 802.11e) ➔ after a transmission of MSDU or management frame, a station needs to compete again for channel access

• Collision detect via a short frame exchange (e.g., RTS/CTS) required at the beginning of TXOP
• TXOP promotes resource (air time) fairness
• Note that vanilla 802.11 fair in terms of transmission opportunities (throughput) even when links use multiple different PHY data rates
EDCA Access Parameters

- DIFS in the vanilla DCF protocol replaced by arbitration inter-frame space (AIFS):

\[
\text{AIFS } [\text{AC}] = a\text{SIFS} + \text{AIFSN } [\text{AC}] \times a\text{SlotTime}
\]

Default parameters for 802.11a/g/n PHYs
Block Acknowledgements

- Allows transfer of a block of frames that are together acknowledged with a single Block Acknowledgement (BA) frame instead of ACK for each individual frame
- Two options:
  1. **Immediate block ACK**: After sending a block of frames, possibly spanning multiple TXOPs, sender sends a block acknowledgement request (BAR) frame soliciting a block ack (BA) from receiver
  2. **Delayed block ACK**: BAR sent in one TXOP and BA can come back in a separate, later TXOP
802.11n

- Goal: achieving **100Mbps+ throughput above data link layer**
- Key features:
  - Higher PHY data rates via:
    - Spatial division multiplexing (SDM) using MIMO
    - 40MHz operation
  - MAC efficiency improvement via:
    - Frame aggregation
    - Block acknowledgement enhancement
MIMO and SDM

• Multiple input, multiple output (MIMO) system: transmitter with multiple antennas transmitting to a receiver with multiple receive antennas
  – Contrast with single input single output (SISO) system in which both transmitter and receiver have only one antenna

• Spatial division multiplexing (SDM): A MIMO system used to transmit independent data streams (or spatial streams) on different antennas
  – Spatial streams: streams of bits transmitted over separate spatial dimensions
  – \( k \) spatial streams require \( k \) antennas
  – \( N \times N \) MIMO system has \( N \) Tx antennas and \( N \) Rx antennas
Other Enhancements in 802.11n

• Robustness improvements via:
  – Spatial diversity through the use of multiple antennas
  – Space-time block coding (STBC)
  – Fast link adaptation
  – Low density parity check (LDPC) codes
  – Transmit beamforming (TxBF)

• Other enhancements:
  – Shorter guard interval (GI)
  – Greenfield preamble
  – Reverse direction MAC protocol (subleasing TXOP)
  – Reduced inter-frame space (RIFS)
802.11n PHY Features

- 1, 2* spatial streams
- 20 MHz; rate 5/6; 56 sub-carriers
- Mixed format
- Basic MIMO/SDM
- Convolution code
- Throughput Enhancement
- Interoperability w/Legacy
- Robustness Enhancement
- 2*, 3, 4 spatial streams
- 40 MHz
- Short GI
- Greenfield format
- TxBF
- STBC
- LDPC code

* 2 spatial streams mandatory for AP only
# 802.11n PHY Data Rates

<table>
<thead>
<tr>
<th>MCS Index</th>
<th>Spatial Streams</th>
<th>Modulation Scheme</th>
<th>Coding Rate</th>
<th>20MHz w/ LGI</th>
<th>40MHz w/ LGI</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>BPSK</td>
<td>1/2</td>
<td>6.50</td>
<td>13.50</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>QPSK</td>
<td>1/2</td>
<td>13.00</td>
<td>27.00</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>QPSK</td>
<td>3/4</td>
<td>19.50</td>
<td>40.50</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>16-QAM</td>
<td>1/2</td>
<td>26.00</td>
<td>54.00</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>16-QAM</td>
<td>3/4</td>
<td>39.00</td>
<td>81.00</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>64-QAM</td>
<td>2/3</td>
<td>52.00</td>
<td>108.00</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>64-QAM</td>
<td>3/4</td>
<td>58.50</td>
<td>121.50</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>64-QAM</td>
<td>5/6</td>
<td>65.00</td>
<td>135.00</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>BPSK</td>
<td>1/2</td>
<td>13.00</td>
<td>27.00</td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>QPSK</td>
<td>1/2</td>
<td>26.00</td>
<td>54.00</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>QPSK</td>
<td>3/4</td>
<td>39.00</td>
<td>81.00</td>
</tr>
<tr>
<td>11</td>
<td>2</td>
<td>16-QAM</td>
<td>1/2</td>
<td>52.00</td>
<td>108.00</td>
</tr>
<tr>
<td>12</td>
<td>2</td>
<td>16-QAM</td>
<td>3/4</td>
<td>78.00</td>
<td>162.00</td>
</tr>
<tr>
<td>13</td>
<td>2</td>
<td>64-QAM</td>
<td>2/3</td>
<td>104.00</td>
<td>216.00</td>
</tr>
<tr>
<td>14</td>
<td>2</td>
<td>64-QAM</td>
<td>3/4</td>
<td>117.00</td>
<td>243.00</td>
</tr>
<tr>
<td>15</td>
<td>2</td>
<td>64-QAM</td>
<td>5/6</td>
<td>130.00</td>
<td>270.00</td>
</tr>
</tbody>
</table>
802.11ac PHY Features

- 802.11ac Goals:
  - Single link throughput at least 500Mbps
  - Multi-station throughput of at least 1Gbps
802.11n and 802.11ac MAC Enhancements
802.11n Throughput without MAC Changes

- 3ms TXOP limit, block ack, 10% PER
Overhead Increase at Higher PHY Data Rates

- Relative preamble overhead for a 1500 byte frame at different PHY data rates
802.11n MAC Efficiency without MAC Changes

- 3ms TXOP limit, block ack, 10% PER
MAC Throughput Enhancements
802.11 Throughput with MAC Enhancements

- 3ms TXOP limit, block ack, 10% PER
MAC Efficiency with MAC Enhancements

- 3ms TXOP limit, block ack, 10% PER
802.11n Frame Aggregation

- Two types:
  - MSDU aggregation (A-MSDU) at the top of the MAC
  - MPDU aggregation (A-MPDU) at the bottom of the MAC

- In both cases, subframes must be destined to the same receiver and should belong to the same service category
Aggregate MSDU (A-MSDU)

- Multiple MSDUs from LLC aggregated and encapsulated within a single MPDU
- Maximum length = 3839/7935 bytes depending on receiver buffer size (4KB/8KB)
Aggregate MPDU (A-MPDU)

- Multiple MPDUs are aggregated together and encapsulated within a single PSDU (A-MPDU)
- Maximum A-MPDU length with 802.11n can be 8191; 16383; 32, 767, or 65,535 bytes
Need both A-MSDU and A-MPDU with 802.11ac
HT Control Field

- To carry .11n and .11ac specific information in MAC header