IEEE 802.11 is a family of specifications for WLANs developed by a working group of IEEE.

802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients.

802.11 provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).

IEEE accepted the specification in 1997.
IEEE 802.11 Family (2)

- Infrastructure Mode
- Ad Hoc Mode

IEEE 802.11 Family (3)

<table>
<thead>
<tr>
<th>Standard</th>
<th>Capability</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.11</td>
<td>Initial standard (1.2 Mbps - 2.4 GHz)</td>
<td>1997 - 1999</td>
</tr>
<tr>
<td>IEEE 802.11b</td>
<td>New PHY layer (11 Mbps)</td>
<td>1999</td>
</tr>
<tr>
<td>IEEE 802.11a</td>
<td>New PHY Layer (54 Mbps, 5GHz support)</td>
<td>1999</td>
</tr>
<tr>
<td>IEEE 802.11g</td>
<td>New PHY Layer (54 Mbps)</td>
<td>2003</td>
</tr>
<tr>
<td>IEEE 802.11i</td>
<td>Security Enhancement (WPA)</td>
<td>2004</td>
</tr>
<tr>
<td>IEEE 802.11e</td>
<td>QoS Support</td>
<td>2005</td>
</tr>
<tr>
<td>IEEE 802.11n</td>
<td>New PHY Layer (540 Mbps, MIMO Support)</td>
<td>2009</td>
</tr>
<tr>
<td>IEEE 802.11s</td>
<td>Mesh Support</td>
<td>Expected 2010</td>
</tr>
<tr>
<td>IEEE 802.11aa</td>
<td>Robust streaming of audio/video transport streams</td>
<td>Active</td>
</tr>
</tbody>
</table>

IEEE 802.11 Family (4)

IEEE 802.11 (1997 - 1999)

- Operating frequency : 2.4 GHz
- Max. Data rates : 2 / 0.9 Mbps (Raw/Typical)
- 14 operating channels (3 non-overlapping)
- Three PHY layers
  - Frequency Hopping Spread Spectrum (FHSS)
  - Direct Sequence Spread Spectrum (DSSS)
  - Infrared (IrDA) (Not commonly used)
- Operating range (theoretical)
  - 20m (indoors)
  - 100m (outdoors)

IEEE 802.11 Family (5)

IEEE 802.11b (1999)

- Allows higher data rates
- Operating frequency : 2.4 GHz
- Max. Data rates : 11 / 4.5 Mbps (Raw/Typical)
- One NEW PHY layer
  - High Rate - Direct Sequence Spread Spectrum (HR - DSSS)
- Operating range (theoretical)
  - 35m (indoors)
  - 140m (outdoors)
IEEE 802.11 Family (6)

• IEEE 802.11a (1999)
  - Allows higher data rates at new frequency
  - Operating frequency: 5 GHz
  - Max. Data rates: 54 / 23 Mbps (Raw/Typical)
  - One NEW PHY layer
    • Orthogonal Frequency-Division Multiplexing (OFDM)
  - NEW Channels
    • 24 non-overlapping operating channels
    • Incompatible with 2.4 GHz family members
  - Operating range (theoretical)
    • 35m (indoors)
    • 120m (outdoors)

IEEE 802.11 Family (7)

• IEEE 802.11g (2003)
  - Allows higher data rates
  - Operating frequency: 2.4 GHz
  - Max. Data rates: 54 / 23 Mbps (Raw/Typical)
  - One NEW PHY layer
    • Orthogonal Frequency-Division Multiplexing (OFDM)
  - Operating range (theoretical)
    • 35m (indoors)
    • 140m (outdoors)

IEEE 802.11 Family (8)

• IEEE 802.11i (2004)
  - Improved Security
  - NEW Encryption Algorithm
    • WiFi Protected Access WPA2
  - NEW Authentication support (IEEE 802.1x)

IEEE 802.11 Family (9)

• IEEE 802.11e (2005)
  - Improved Quality of Service
  - NEW MAC layer medium sharing methods
    • Enhanced Distributed Channel Access (EDCA)
    • HCF Controlled Channel Access (HCCA)
  - Additional NEW MAC layer mechanisms
    • Block Acknowledgement
    • Direct Link Protocol (DLP)
IEEE 802.11 Family (10)

- IEEE 802.11y (2008)
  - Operating frequency: 3.65 - 3.75 GHz (lightly-licensed frequency)

- Additional NEW MAC layer mechanisms
  - Extended Channel Switch Announcement (ECSA)
    - Allows WLANs to switch frequencies and channel bandwidth so that noise and interference are minimized
  - Dependent Station Enablement (DSE)
    - Ability to use licensed frequencies for license-exempt devices
  - Operating range: 50-5000m

IEEE 802.11 Family (11)

- IEEE 802.11n (2009)
  - Allows higher data rates
  - Operating frequency: 2.4 GHz
  - Max. Data rates: 540 / 75 - 100 Mbps (Raw/Typical)

- One NEW PHY layer
  - Use of Multiple Input Multiple Output (MIMO) technique

- Additional NEW MAC layer mechanism
  - Frame Aggregation (improved Block Acknowledgement)

- Operating range (theoretical)
  - 70m (indoors)
  - 250m (outdoors)

IEEE 802.11 Family (12)

- IEEE 802.11s (Expected 2010)
  - Allows use of Mesh connectivity in the network.
  - Network includes Mesh Points (MP), Mesh Access Points (MAP), and Mesh Portal Points (MPP)

IEEE 802.11 Family (13)

- IEEE 802.11s (Expected 2010)
  - Additional NEW MAC layer mechanism
    - For intra-network routing, Hybrid Wireless Mesh Protocol (HWMP) is defined.
    - Efficient Mesh Security Association (EMSA) is developed to handle mesh topology specific security problems.
    - A congestion control mechanism has been developed.
IEEE 802.11 Family (14)

- IEEE 802.11aa  (Active)
  - Robust streaming of Audio Video Transport Streams
    - Agreed on a constrained definition of OBSS (overlapping basic service set), for which TGaa will specify a solution.
    - Adopt reliable multicast proposals into the draft
    - Review and converge on OBSS definition/solution
    - Incorporate changes and adopt Intra-AC, Intra-Stream prioritization proposal(s) into TGaa draft 0.01
    - Complete Draft 0.01

IEEE 802.11 Family (15)

- IEEE 802.11-2007
  - Current standard documentation
    - Includes 11a, 11b, 11d, 11e, 11g, 11h, 11i, and 11j

MAC Layer (DCF) (1)

- Available in all standards

- Most widely used MAC layer
  - WiFi Alliance approved

- Contention-based

- Very easy to implement

MAC Layer (DCF) (2)

- Nodes (STAs and the AP) contend to access the medium
  - Each node senses the medium
  - If the medium is busy, wait until transmission ends
  - When the medium is idle, wait for a brief amount of time - interframe space (IFS)
  - If the medium is idle, wait for an additional period calculated using a binary backoff algorithm
  - After this backoff time, if the medium is still idle send the packet
  - When waiting for this backoff duration, if the medium becomes busy, freeze backoff timer
  - Different packets use different IFS values
MAC Layer (DCF) (3)

- IFS Types
  - Distributed IFS (DIFS), used for:
    - Normal frames
  - Short IFS (SIFS), used for:
    - MAC layer ACK frames
    - CTS frames
    - Second and subsequent frames in a fragment burst
  - PCF IFS (PIFS), used for:
    - Beacon frames in PCF

MAC Layer (DCF) (4)

- STA₁ → AP
- STA₂ → AP
- STA₃ → AP

MAC Layer (DCF) (5)

- STA₁ → AP
- STA₂ → AP
- STA₃ → AP

MAC Layer (DCF) (6)

- When a node wants to send a frame and the channel has been idle for a period of time longer than DIFS (counted from the moment the node first probed the channel), it can send immediately (without waiting for the backoff period).

  - If there is a collision after the backoff, each node increases its contention window and enters contention with a longer contention window.

  - When a node successfully transmits a frame, its contention window returns to its initial value.
MAC Layer (DCF) (7)

- The duration of a transmission is written inside the frame using the "duration" field.

- Nodes sensing the busy channel extract this information and defer from using the channel for a time equal to the "duration" field.

- This information is stored in a node’s Network Allocation Vector (NAV).

MAC Layer (PCF) (1)

- Available in all standards

- Not widely used
  - PCF support is optional in WiFi Alliance approved devices

- Contention-free

- Increases MAC overhead

MAC Layer (PCF) (2)

- Time is divided into superframes
- Each superframe consists of two periods
  - Contention-free period
  - Contention period
- At the start of each superframe, the AP broadcasts a beacon frame to the STAs.
- Upon receiving this beacon frame, STAs set their NAV values to the maximum value (as stated inside the beacon frame).
- Until the end of this period, all traffic is managed by the AP.

MAC Layer (PCF) (3)

- First, the AP sends frames to the STAs (waiting for only a SIFS amount of time between the frames).
- After sending its frames, AP polls every STA by sending a Contention Free (CF) Poll frame.
- The STA to which the CF Poll frame is destined can send one frame to the AP after receiving the poll frame.
- Polling ends at the end of the CF period.
- At the end of the CF period, the contention period starts.
- Contention period is the same as DCF.
MAC Layer (PCF)

(4)

- STA\textsubscript{1} \rightarrow AP
- STA\textsubscript{2} \rightarrow AP
- AP \rightarrow STA\textsubscript{1}

(5)

- STA\textsubscript{1} \rightarrow AP
- STA\textsubscript{2} \rightarrow AP
- AP \rightarrow STA\textsubscript{1}

(6)

- STA\textsubscript{1} \rightarrow AP
- STA\textsubscript{2} \rightarrow AP
- AP \rightarrow STA\textsubscript{1}

(7)

- PCF is developed for QoS support.
- However, it increases the MAC overhead with the polling frames.
- Most importantly, it is generally not implemented in AP and STAs.
MAC Layer (Problems)  (1)

• Hidden Node Problem
  • Cause: Two STAs both in range of the same AP but not in range of each other
  • Problem: When one STA sends a frame to the AP, the other thinks that the medium is idle and sends its frame to the AP. Thus, these frames collide.
  • Solution: RTS/CTS mechanism

MAC Layer (Problems)  (2)

• RTS/CTS
  • Assume there is a Hidden Node in the network.
  • One node tries to send a frame to the AP.
  • Instead of sending the data frame, the node sends a Request to Send (RTS) frame to the AP.
  • The AP will respond with a Clear to Send (CTS) frame to inform the hidden nodes of the transmission.

MAC Layer (Problems)  (3)

• STA₁ → AP
• STA₂ → AP

   AP  ← DIFS  RTST  SIFS  CTS  SIFS  ACK  DIFS
   STA₁  ← RTST  Frame  DIFS
   STA₂

• NAV of RTS : CTS + Data frame + ACK + 3*SIFS
• NAV of CTS : Data frame + ACK + 2*SIFS

MAC Layer (Problems)  (4)

• Exposed Terminal Problem (Ad Hoc)

   STA₁  STA₂  STA₃  STA₄

   • Cause: STA₂ sends frames to STA₁, and STA₃ wants to send frames to STA₄.
   • STA₁ and STA₃ are in the range of STA₂.
   • STA₂ and STA₄ are in the range of STA₃.
   • Problem: STA₃ cannot send its frames since it thinks this will collide with the other traffic and STA₄ will not receive anything (although that is not the case).
**PHY Layer (Types) (1)**

- IrDA (Infrared)
- FHSS (Frequency Hopping Spread Spectrum)
- DSSS (Direct Sequence Spread Spectrum)
- OFDM (Orthogonal Frequency Division Multiplexing)

**PHY Layer (Types) (2)**

- Common Modulation Techniques
  - ASK: Modulation by amplitude
  - PSK: Modulation by phase
  - FSK: Modulation by frequency
  - QAM: Modulation by amplitude & phase
  - CCK: Complementary Code Keying

**PHY Layer (Types) (3)**

- QPSK symbols in the complex plane:

  - $\pi/2$
  - $\pi$
  - $3\pi/2$

  - Im
  - Re

<table>
<thead>
<tr>
<th>00</th>
<th>01</th>
<th>11</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>0010</td>
<td>0110</td>
<td>1110</td>
<td>1010</td>
</tr>
<tr>
<td>0011</td>
<td>0111</td>
<td>1111</td>
<td>1011</td>
</tr>
<tr>
<td>0001</td>
<td>0101</td>
<td>1101</td>
<td>1001</td>
</tr>
<tr>
<td>0000</td>
<td>0100</td>
<td>1100</td>
<td>1000</td>
</tr>
</tbody>
</table>

**Example for 16-QAM**

**PHY Layer (Types) – FHSS (1)**

- Used only by legacy 802.11
- Instead of sending the symbol using a fixed frequency, transmitter sends consecutive symbols using different frequencies
- In effect, the transmission hops between frequencies
PHY Layer (Types) – FHSS (2)

- **Advantages**
  - Resilient against jamming
  - Resilient against narrowband interference
  - Does not affect transmissions using the same frequency band

- **Disadvantages**
  - The channel is not utilized effectively
  - Transmitter and receiver must be fully synchronized with respect to time and frequency

PHY Layer (Types) – DSSS (1)

- **Used in legacy 802.11 and 802.11b**
- **The narrowband base transmission is spread upon a much wider bandwidth**
- **The signal appears like white noise to other receivers**

PHY Layer (Types) – DSSS (2)

- **Advantages**
  - Resilient against jamming
  - Resilient against narrowband interference
  - Does not affect transmissions using the same frequency band

- **Disadvantages**
  - The channel is not utilized effectively

PHY Layer (Types) – OFDM (1)

- **11 Mbps is not enough compared to LAN protocols (Eg. Ethernet supports 100/1000 even 10,000 Mbps)**

- **In order to increase the data rate, we can**
  - increase the channel bandwidth
  - use less robust modulation techniques

- **Single carrier systems with high channel bandwidth are significantly affected by multipath propagation.**

- **The air interface is not as stable as the wire interface. Thus, using less robust techniques results in performance that varies significantly with environmental conditions.**
**PHY Layer (Types) – OFDM (2)**

- **Advantages**
  - Since robust modulation techniques are used, adaptability to severe channel conditions is high.
  - Channels are orthogonal to each other.
    - Robust against narrowband co-channel interference
    - Robust against fading caused by multipath propagation and high ISI values
  - High spectral efficiency
  - Allows single-frequency network capability

**PHY Layer (Types) – OFDM (3)**

- **Disadvantages**
  - Sensitive to frequency synchronization problems
  - Sensitive to Doppler shift (effect of the movement)
  - Requires expensive circuitry

**PHY Layer (Types) – OFDM (4)**

- **Multipath propagation**

  - Signals generated by the transmitter are received by the receiver traversing different paths
  - Signals coming from different paths are received at the receiver at different times

**PHY Layer (Types) – OFDM (5)**

- **Inter Symbol Interference (ISI)**
  - $T$: the duration of the shortest transmission path (will be the LOS path, if there is any)
  - $T_{\text{max}}$: the duration of the longest transmission path

  - Since $T_{\text{max}} \geq T$, the multipath property adds an interference to all transmissions, symbols, during its duration.
  - The ratio between these two values is called the Inter Symbol Interference (ISI).
  - In order to correct ISI related problems, there should be an equalizer in the receiver.
  - To combat larger ISI values, more powerful equalizers are needed.
PHY Layer (Types) – OFDM (6)

- Inter Symbol Interference (ISI)
  - If a transmission is sent through a single carrier
    \[ ISI = \frac{T_{\text{max}}}{T} \]
  - If the same transmission is sent through \( N \) carriers
    \[ ISI = \frac{T_{\text{max}}}{N \times T} \]
  - This reduced ISI effect can be attained with the use of guard intervals

PHY Layer (Types) – OFDM (7)

- Guard Interval
  - The single carrier signal is transmitted in multiple subcarriers that are orthogonal to each other.
  - Each subcarrier uses a low symbol rate modulation scheme.
  - A guard interval is inserted between symbols.
    - Guard intervals reduce the ISI.
    - Guard intervals also reduce the signals susceptibility to time synchronization problems.

PHY Layer (Types) – OFDM (8)

Orthogonality between subcarriers

Orthogonality over this interval

Guard time for preventing intersymbol interference

In the receiver, FFT is calculated only during this time

0.8 \( \mu \)s

3.2 \( \mu \)s

4.0 \( \mu \)s

Symbol duration

Time

Next symbol

Orthogonality over the internal Subcarrier

Subcarrier +1

Previous symbol

Guard time

Symbol part that is used for FFT calculation at receiver

Next symbol
**PHY Layer (Types) – OFDM (10)**

- **Orthogonality**
  - The single carrier signal is transmitted over multiple subcarriers that are orthogonal to each other.
  - Being orthogonal to each other, there is nearly no cross-talk between subcarriers.

**PHY Layer (Types) – OFDM (11)**

- How to calculate raw bit rates in OFDM?
  - Symbol duration = 4 µs
  - Data-carrying subcarriers = 48
  - Coded bits / subcarrier = 6 (64 QAM)
  - Coded bits / symbol = 6 × 48 = 288
  - Data bits / symbol = 3/4 × 288 = 216
  - Bit rate = 216 bits / 4 µs = 54 Mbps

**PHY Layer (Types) – OFDM (12)**

- Data rates in OFDM

<table>
<thead>
<tr>
<th>Modulation</th>
<th>Bit rate</th>
<th>Coding Rate</th>
<th>Coded bits / symbol</th>
<th>Data bits / symbol</th>
</tr>
</thead>
<tbody>
<tr>
<td>BPSK</td>
<td>6 Mbit/sec</td>
<td>1/2</td>
<td>48</td>
<td>24</td>
</tr>
<tr>
<td>BPSK</td>
<td>9 Mbit/sec</td>
<td>3/4</td>
<td>48</td>
<td>36</td>
</tr>
<tr>
<td>QPSK</td>
<td>12 Mbit/sec</td>
<td>1/2</td>
<td>96</td>
<td>48</td>
</tr>
<tr>
<td>QPSK</td>
<td>18 Mbit/sec</td>
<td>3/4</td>
<td>96</td>
<td>72</td>
</tr>
<tr>
<td>16-QAM</td>
<td>24 Mbit/sec</td>
<td>1/2</td>
<td>192</td>
<td>96</td>
</tr>
<tr>
<td>16-QAM</td>
<td>36 Mbit/sec</td>
<td>3/4</td>
<td>192</td>
<td>144</td>
</tr>
<tr>
<td>64-QAM</td>
<td>48 Mbit/sec</td>
<td>1/2</td>
<td>288</td>
<td>192</td>
</tr>
<tr>
<td>64-QAM</td>
<td>54 Mbit/sec</td>
<td>3/4</td>
<td>288</td>
<td>216</td>
</tr>
</tbody>
</table>

**PHY Layer (Channels)**

- Interchannel Interference
  - Even though there are 14 channels
  - Only 3 of them can operate without causing serious interference to each other
MAC Layer (EDCA – 11e) (1)

- Introduced in 802.11e
- Basically an enhanced version of DCF
- Adds QoS support to DCF
- 4 types of traffic (called Access Category (AC)) is defined
  - Best effort
  - Video probe
  - Video
  - Voice
- STAs with QoS support are called QSTA
- APs with QoS support are called QAP

MAC Layer (EDCA – 11e) (2)

- In each QSTA, there are 4 different queues, one for each AC.
- Each queue contends for medium access as if a separate STA.
- Queues from different ACs have different medium access parameters.
  - IFS
  - Minimum Contention Window size (CWmin)
  - Maximum Contention Window size (CWmax)

MAC Layer (EDCA – 11e) (3)

- These parameters are defined and broadcasted by the AP
  - IFS
    - Each AC has a separate IFS value called AIFSD
    - AIFSD[AC] = SIFS + AIFS[AC]
  - CWmin and CWmax
    - Each queue starts with a different CWmin value, CWmin[AC] to calculate the backoff duration
    - The maximum size of backoff, CWmax, is also different, CWmax[AC]

MAC Layer (EDCA – 11e) (4)

- There is a virtual collision handler in each QSTA.
- If there is a collision among multiple ACs, the frame from the highest priority level is chosen and transmitted.
MAC Layer (EDCA – 11e)  (5)

- QSTA1[3] -> AP
- QSTA2[1] -> AP
- QSTA2[2] -> AP

MAC Layer (EDCA – 11e)  (6)

- QSTA1[3] -> AP
- QSTA2[1] -> AP
- QSTA2[2] -> AP

MAC Layer (EDCA – 11e)  (7)

- QSTA2[1] -> AP
- QSTA2[2] -> AP

MAC Layer (TXOP – 11e)

- 802.11e also defines a Transmission Opportunity (TXOP)
- The QAP broadcasts TXOP length for each AC.
- When a QSTA wins the contention for an AC class, it can send frames belonging to that AC class as the length of the TXOP of the same AC.
- Inside a TXOP, the QSTA only waits for SIFS before sending frames.
MAC Layer (HCCA – 11e)  (1)

- Hybrid Controller Function (HCF) Controlled Channel Access (HCCA)
- Introduced in 802.11e.
- An enhanced version of PCF.
- Similar to the ACs in EDCA, there are Traffic Classes (TC) in HCCA.
- Different TCs belong to different Traffic Streams (TS).

MAC Layer (HCCA – 11e)  (2)

- Similar to CP and CFP in PCF, there are two periods:
  - CP : Collision Period (This period is an EDCA period)
  - CAP : Controlled Access Phase
- CAPs do not have fixed durations and fixed places in the superframe.
- QAP initiates CAPs to send a number of frames to a QSTA.
- QAP can also initiate CAPs to poll a QSTA to send frames to the QAP.

MAC Layer (HCCA – 11e)  (3)

- HCCA can poll QSTA’s on a TC basis.
- Each QSTA has a maximum of 8 TCs.
- The traffic and QoS parameters of each TC is sent to the QAP in TC establishment.
- QAP enables CAPs using these parameters.
- How these CAPs are scheduled is left undefined in the standard.

MAC Layer (HCCA – 11e)  (4)

- TXOPs can also be used in an HCCA.
- In this case, when a QAP sends frames to a QSTA or polls a QSTA for frames, the sender can send as many frames as fits in the TXOP of the selected TC.
- Again similar to PCF, implementation of HCCA is not mandatory in 802.11e.
MAC Layer (DLP – 11e) (1)

- **Direct Link Protocol (DLP)**
  - If two STAs in a single WLAN cell try to communicate with each other, all traffic must be routed through the AP.
  - If these STAs are in range with each other, this will result in a waste of link resource equal to the size of the communication.
  - Using DLP, these two QSTAs can communicate directly with each other.

MAC Layer (DLP – 11e) (2)

- **Direct Link Protocol (DLP)**
  - The sender QSTA sends a request frame to the QAP.
  - QAP forwards this message to the receiver QSTA.
  - If the QSTA allows this transmission, it sends a response frame to the QAP.
  - QAP forwards this message to the transmitter QSTA.
  - The two QSTAs communicate with each other using a direct connection with each other.

MAC Layer (DLP – 11e) (3)

- **Block Acknowledgement**
  - Instead of sending one ACK frame for each data frame, the receiver sends one ACK frame for one TXOP.
- **No Acknowledgement**
  - Each frame can enable this mechanism.
  - No ACK frame will be sent from the receiver for the data frame.

IEEE 802.11 WLAN Architecture

- 802.11 defines two BSS (Basic Service Set) options:
  - **Infrastructure BSS**
  - **Independent BSS** (Ad-Hoc network)
**Infrastructure BSS**

- This is by far the most common way of implementing WLANs.
- Before stations can use the BSS, they perform an Association process.

**Independent BSS**

- Mainly of interest for military applications.
- No access point is required, stations can communicate directly.
- Efficient routing of packets is not a trivial problem (routing is not a task of 802.11).

**Extended Services Set (ESS)**

- This is a larger WLAN network consisting of a number of BSS networks interconnected via a common backbone.
- 802.11 supports link-layer mobility within an ESS (but not outside the ESS).

**Distribution System**

- This is the mechanism by which APs and other nodes in the wired IP subnetwork communicate with each other.
- This communication, using the Inter-Access Point Protocol (IAPP), is essential for link-layer mobility (stations can seamlessly move between different BSS networks).
For instance, when a wireless station moves from one BSS to another, all nodes must update their databases so that the DS can distribute packets via the correct AP.

When WS associates with AP2, the router in charge of the IP subnet addressing obtains an IP address from the DHCP server.

The router must maintain binding between this IP address and the MAC address of the wireless station.

The globally unique MAC address of the wireless station is used for routing the packets within the IP subnetwork (DS + attached BSS networks).
The dynamic and local IP address of the wireless station is only valid for the duration of attachment to the WLAN and is used for communicating with the outside world.

The router must also know (and use) the MAC address of the access point via which the packets must be routed. For this purpose, a special protocol (IAPP) is needed.

IAPP (Inter-Access Point Protocol)

- IAPP (defined in IEEE 802.11f) offers mobility in the Data Link layer (within an ESS).

In Addition to IAPP

- IAPP alone is not sufficient to enable seamless handovers in a WLAN. The stations must be able to measure the signal strengths from surrounding APs and decide when and to which AP a handover should be performed (no 802.11 standardized solutions are available for this operation).

- In 802.11 networks, a handover means reassociating with the new AP. There may be two kinds of problems:
  - Will handover work when APs are from different vendors?
  - Will handover work together with security solutions?