IEEE 802.11 WLAN · PART 1

IEEE Standards

<table>
<thead>
<tr>
<th></th>
<th>802.11a</th>
<th>802.11b</th>
<th>802.11g</th>
<th>802.11n</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Maximum Throughput</strong></td>
<td>54 Mbps</td>
<td>11 Mbps</td>
<td>54 Mbps</td>
<td>300 Mbps</td>
</tr>
<tr>
<td><strong>Frequency</strong></td>
<td>5 GHz</td>
<td>2.4 GHz</td>
<td>2.4 GHz</td>
<td>2.4/5 GHz</td>
</tr>
<tr>
<td><strong>Modulation</strong></td>
<td>OFDM</td>
<td>DSSS</td>
<td>DSSS/OFDM</td>
<td>OFDM</td>
</tr>
<tr>
<td><strong>Channels (FCC/ETSI)</strong></td>
<td>21/19</td>
<td>11/13</td>
<td>11/13</td>
<td>32/32</td>
</tr>
</tbody>
</table>

WLAN Types

**Ad Hoc**
A WLAN between isolated stations with no central point of control; an IBSS

**Infrastructure**
A WLAN attached to a wired network via an access point; a BSS or ESS

WLAN Components

- **IBSS**
- **BSS**
- **ESS**
- **DS**

Frame Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Association</td>
<td>Management</td>
</tr>
<tr>
<td>Authentication</td>
<td>Management</td>
</tr>
<tr>
<td>Probe</td>
<td>Management</td>
</tr>
<tr>
<td>Request to Send (RTS)</td>
<td>Control</td>
</tr>
<tr>
<td>Clear to Send (CTS)</td>
<td>Control</td>
</tr>
<tr>
<td>Acknowledgment (ACK)</td>
<td>Control</td>
</tr>
<tr>
<td>Data</td>
<td>Data</td>
</tr>
</tbody>
</table>

Client Association

- **Probe Request**
- **Probe Response**
- **Authentication Request**
- **Authentication Response**
- **Association Request**
- **Association Response**

Modulations

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Modulation</th>
<th>Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSSS</td>
<td>DBPSK</td>
<td>1 Mbps</td>
</tr>
<tr>
<td></td>
<td>DQPSK</td>
<td>2 Mbps</td>
</tr>
<tr>
<td></td>
<td>CCK</td>
<td>5.5/11 Mbps</td>
</tr>
<tr>
<td></td>
<td>BPSK</td>
<td>6/9 Mbps</td>
</tr>
<tr>
<td></td>
<td>QPSK</td>
<td>12/18 Mbps</td>
</tr>
<tr>
<td></td>
<td>16-QAM</td>
<td>24/36 Mbps</td>
</tr>
<tr>
<td></td>
<td>64-QAM</td>
<td>48/54 Mbps</td>
</tr>
<tr>
<td>OFDM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Terminology

- **Basic Service Set Identifier (BSSID)**
  A MAC address which serves to uniquely identify a BSS

- **Service Set Identifier (SSID)**
  A human-friendly text string which identifies a BSS; 1-32 characters

- **Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)**
  The mechanism which facilitates efficient communication across a shared wireless medium (provided by DCF or PCF)

- **Effective Isotropic Radiated Power (EIRP)**
  Net signal strength (transmitter power + antenna gain - cable loss)

Measuring RF Signal Strength

**Decibel (dB)**
An expression of signal strength as compared to a reference signal; calculated as $10\log_{10}(\text{signal/reference})$

- **dBm** · Signal strength compared to a 1 milliwatt signal
- **dBw** · Signal strength compared to a 1 watt signal
- **dBi** · Compares forward antenna gain to that of an isotropic antenna

In 1999, the 802.11 standards were ratified, with 802.11b offering a maximum throughput of 11 Mbps at 2.4 GHz. In 2003, 802.11g was ratified, providing 54 Mbps at 2.4 GHz, utilizing DSSS/OFDM modulation. In 2009, 802.11n was ratified, offering 300 Mbps at 2.4/5 GHz using OFDM modulation. The Basic Service Set (BSS) is a set of stations and/or access points which can directly communicate via a wireless medium. The Distribution System (DS) is the wired infrastructure connecting multiple BSSs to form an ESS. An Independent BSS (IBSS) is an isolated BSS with no connection to a DS; an ad hoc WLAN. The Basic Service Area (BSA) is the physical area covered by the wireless signal of a BSS. The Effective Isotropic Radiated Power (EIRP) is the net signal strength (transmitter power + antenna gain - cable loss).
Distributed Coordination Function (DCF)

Interframe Spacing

Short IFS (SIFS)
Used to provide minimal spacing delay between control frames or data fragments

DCF IFS (DIFS)
Normal spacing enforced under DCF for management and non-fragment data frames

Arbitrated IFS (AIFS)
Variable spacing calculated to accommodate differing qualities of service (QoS)

Extended IFS (EIFS)
Extended delay imposed after errors are detected in a received frame

Encryption Schemes

Wired Equivalent Privacy (WEP)
Flawed RC4 implementation using a 40- or 104-bit pre-shared encryption key (deprecated)

Wi-Fi Protected Access (WPA)
Implements the improved RC4-based encryption Temporal Key Integrity Protocol (TKIP) which can operate on WEP-capable hardware

IEEE 802.11i (WPA2)
IEEE standard developed to replace WPA; requires a new generation of hardware to implement significantly stronger AES-based CCMP encryption

Quality of Service Markings

<table>
<thead>
<tr>
<th>WMM</th>
<th>802.11e</th>
<th>802.1p</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platinum</td>
<td>7/6</td>
<td>6/5</td>
</tr>
<tr>
<td>Gold</td>
<td>5/4</td>
<td>4/3</td>
</tr>
<tr>
<td>Silver</td>
<td>3/0</td>
<td>0</td>
</tr>
<tr>
<td>Gold</td>
<td>2/1</td>
<td>2/1</td>
</tr>
</tbody>
</table>

Wi-Fi Multimedia (WMM)
A Wi-Fi Alliance certification for QoS; a subset of 802.11e QoS

IEEE 802.11e
Official IEEE WLAN QoS standard ratified in 2005; replaces WMM

IEEE 802.1p
QoS markings in the 802.1Q header on wired Ethernet

Client Authentication

Open
No authentication is used

Pre-shared Encryption Keys
Keys are manually distributed among clients and APs

Lightweight EAP (LEAP)
Cisco-proprietary EAP method introduced to provide dynamic keying for WEP (deprecated)

EAP-TLS
Employs Transport Layer Security (TLS); PKI certificates are required on the AP and clients

EAP-TTLS
Clients authenticate the AP via PKI, then form a secure tunnel inside which the client authentication takes place (clients do not need PKI certificates)

Protected EAP (PEAP)
A proposal by Cisco, Microsoft, and RSA which employs a secure tunnel for client authentication like EAP-TTLS

EAP-FAST
Developed by Cisco to replace LEAP; establishes a secure tunnel using a Protected Access Credential (PAC) in the absence of PKI certificates

RF Signal Interference

Reflection
Scattering
Absorption

Refraction
Diffraction

Antenna Types

Directional
Radiates power in one focused direction

Omnidirectional
Radiates power uniformly across a plane

Isotropic
A theoretical antenna referenced when measuring effective radiated power