

IEEE Standards				
	802.11a	802.11b	802.11g	802.11n (Draft)
<b>Maximum Throughput</b>	54 Mbps	11 Mbps	54 Mbps	300 Mbps
<b>Frequency</b>	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz
<b>Modulation</b>	OFDM	DSSS	DSSS/OFDM	OFDM
<b>Channels (FCC/ETSI)</b>	21/19	11/13	11/13	32/32
<b>Ratified</b>	1999	1999	2003	N/A

## WLAN Types

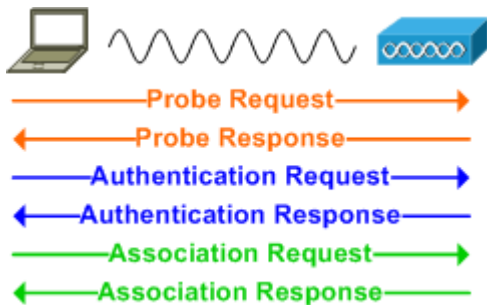
**Ad Hoc** · A WLAN between isolated stations with no central point of control; an IBSS

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

## Frame Types

Type	Class
Association	Management
Authentication	Management
Probe	Management
Beacon	Management
Request To Send (RTS)	Control
Clear To Send (CTS)	Control
Acknowledgment (ACK)	Control
Data	Data

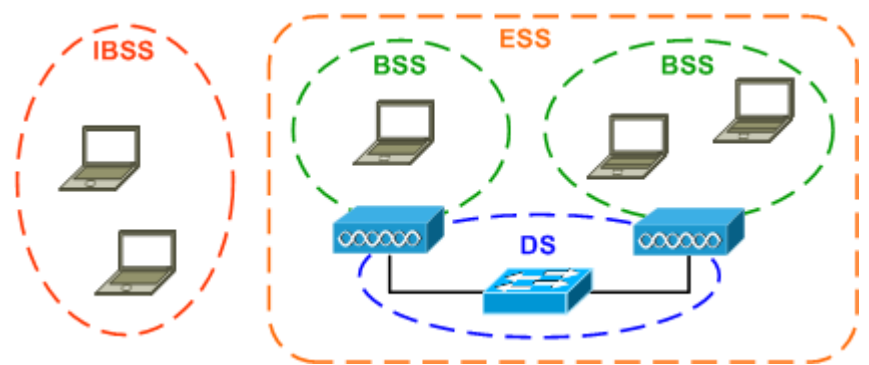
## Client Association



## Modulations

Scheme	Modulation	Throughput
DSSS	DBPSK	1 Mbps
	DQPSK	2 Mbps
	CCK	5.5, 11 Mbps
OFDM	BPSK	6, 9 Mbps
	QPSK	12, 18 Mbps
	16-QAM	24, 36 Mbps
	64-QAM	48, 54 Mbps

## WLAN Components



**Basic Service Area (BSA)** · The physical area covered by the wireless signal of a BSS

**Basic Service Set (BSS)** · A set of stations and/or access points which can directly communicate via a wireless medium

**Distribution System (DS)** · The wired infrastructure connecting multiple BSSs to form an ESS

**Extended Service Set (ESS)** · A set of multiple BSSs connected by a DS which appear to wireless stations as a single BSS

**Independent BSS (IBSS)** · An isolated BSS with no connection to a DS; an *ad hoc* WLAN

## Measuring RF Signal Strength

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

**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

## Terminology

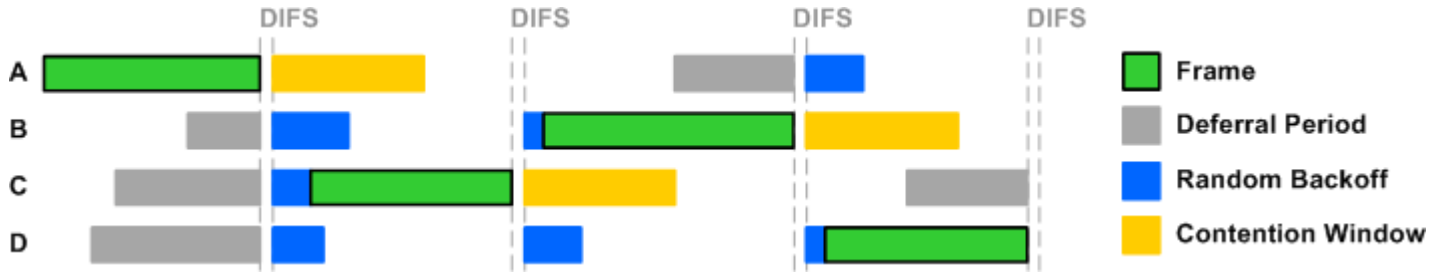
**Basic Service Set Identifier (BSSID)** · A MAC address (typically belonging to an AP) which serves to uniquely identify a BSS

**Service Set Identifier (SSID)** · A human-friendly text string which identifies a BSS (up to 32 characters in length)

**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)** · An expression of net signal strength (transmitter power + antenna gain - cable loss)

## Distributed Coordination Function



### 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 nonfragment data frames

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

**Extended IFS (EIFS)** · Extended delay imposed after detecting errors in a received frame

### Encryption Schemes

**Wired Equivalent Privacy (WEP)** · Deprecated encryption mechanism which employs a flawed RC4 implementation and a 40- or 104-bit preshared encryption key

**Wi-Fi Protected Access (WPA)** · A temporary fix for the flaws in WEP; implements an improved RC4-based encryption called 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

### Client Authentication

**Open** · No authentication is used

**Preshared Encryption Keys** · Keys must be manually entered into clients and access points before a secure connection can be established

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

**EAP-TLS** · Employs Transport Layer Security (TLS); PKI certificates are required on the AP and clients to provide mutual authentication

**EAP-TTLS** · Clients authenticate the AP with its cert, then form a secure tunnel inside which the client authentication takes place; removes the requirement for a PKI cert on the client

**Protected EAP (PEAP)** · A proposal by Cisco, Microsoft, and RSA which forms a secure tunnel like EAP-TTLS and does not require a cert on the client

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

### Quality of Service Markings

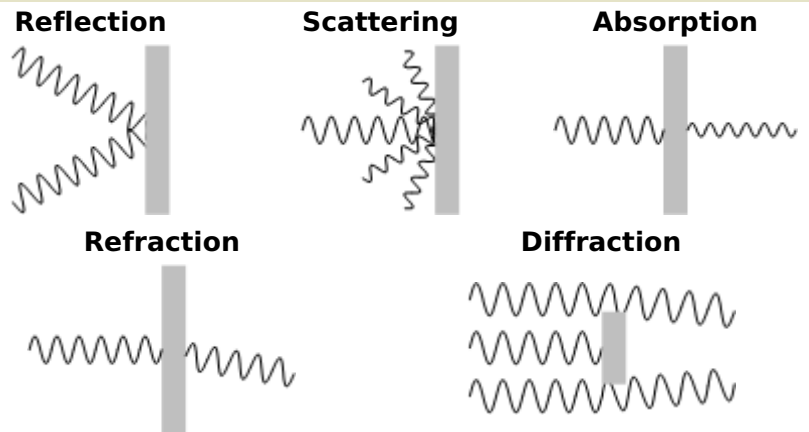
WMM	802.11e	802.1p
Platinum	7	6
	6	5
Gold	5	4
	4	3
Silver	3	0
	0	0
Bronze	2	2
	1	1

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

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

**802.1p** · QoS markings in the 802.1Q header on wired Ethernet LANs shown for comparison

### RF Signal Interference



### Antenna Types

**Directional** · Radiates power in one or several focused directions

**Omnidirectional** · Radiates power uniformly across a plane

**Isotropic** · A theoretical antenna referenced when measuring effective radiated power