Wireless terminology

Essid: Name of the wireless network and is broadcast in beacon probes.

Bssid: Mac address of the accesspoint

Client or Station: The client using the wireless network

Gain: A positive Amplitude between two RF signals.

Two Types

Active done with an inline amp. Amplifies everything including noise

Passive done with antennas. Directs the waves in the direction you need them to go

Loss

Intentional :Done with an attenuation to stay with in FCC spec or for other reason

Natural: Loss due to natural process of RF though either reflection, refraction scattering diffraction and absorption.

Watt :Basic unit of power

Milli watt: Wireless does not need alot of power to tx
average home router 50mw aprox
average enterprise 1-200mw

dB: measure of change between one signal and another

Basic dB math:

A gain of 3dB doubles the power output
A loss of 3dB halves the power output
A gain of 10dB multiplies power by 10
A loss of 10dB divides power by 10
dB gains and losses are cumulative

Basic FCC rules

max of 1W active in 2.4ghz Note: its .1W or 100mW in europe
4W passive in 2.4 ghz

Charts

Azimuth chart: top down view of the signal
Elevation chart: side view of the signal

dBm:

the relation of dB to the mW power output

See chart pm dB to Mw

dBi: measurement of directional gain in power based on isotropic radiator (perfect antenna, doesn't exist)

dBd: measurement of a dipole antenna which is 2.14 over a isotropic radiator IE a 7dBd has a gain of 9.14 dBi

SNR: Noise floor, the amount of noise that a signal must overcome to be heard on the other end

Receive sensitivity: the lowest signal that a card can receive and still maintain a link

FHSS
2.400 Ghz - 2.4835 Ghz
Bluetooth
79 Channels 1Mhz wide

DSSS
802.11
2.401 Ghz - 2.473 Ghz
1,2 Mbps

HR/DSSS
802.11b
14 Channels (only 11 in the US)
1,2,5.5 11 Mbps
22mhz wide channels

OFDM
802.11a / 802.11g
20mhz wide channels
Both 2.4 Ghz and 5 Ghz
Channels
6,9,12,18,24,36,48,54

Dwell Time: Time spent on channel

Hop Seq: list of channels that will be hopped based on the Dwell time

Pcap / cap: A file containing recorded network traffic

Comma Separated Value (CSV): A common file format where data is separated by commas

Antenna Types

Omnidirectional: Rubber Ducks aka diepoles: higher dBi means that the lobes are compressed

Highly Directional: Parabolic or grid with a very narrow beam width

Sectorized antennas: normally used in groups with a single processor to form an omnidirectional antennae.

Semi Directional: Semi Directional antennas offer good long range transmission and decent reception in some cases.
Some types are:
- yagi
- Cantenna
- patch

Multi Input Multi Output (MIMO): multiple antennas in use at the time time allowing a system to make use for antennae diversity and signal multi-path.

Polarization: direction of the antennas

Antenna Diversity : picks the best signal of two antennas

802.11A

First 54mb 5ghz band
36,40,44,48,52,56,60,64 149,153,157,161,165 US channels
Short range
20mhz wide
No Channel overlap
Channel Range 5.14-5.320
Actual throughput is 3-29 Mbps
Range 50/100 ft aprox

802.11B

First 11mb 2.4ghz Band
22mhz wide channels
Actual Thoughput is 3-6Mbps
Range 200/300 ft aprox

802.11G

First 54mb in 2.4ghz Band
20mhz wide channels
Actual throughput is 3-29 Mbps
Range 150/300 ft aprox

802.11N

Comes in several forms, is described by number of antennas on each side.
Example, 2x2, 3x3
20mhz and 40mhz Wide
Actual Throughput is 144Mbps for 2x2
Range 300/600 ft aprox

Encryption types

WEP, Wired Equivalency privacy: Broken since 2000 due to weak IV's, based on RC4

WPA, **TKIP** : Replacement for wep still based on RC4 but cycles keys fast enough to prevent cracking. There are parts of tkip that are broken allowing injection of certain types of packets but there is not a full public break of it yet.

WPA, **AES**: Complete and total replacement for TKIP and RC4/wep

WPA2: Designed to meet all of 802.11i and completely replace WPA

Management Frames

Beacons: Broadcast several times a second and contains the name of the network as well as all encryption and connection information needed.

Probe requests: Used to request information from a station and determine what access-points are in range

Probe responses: Stations will respond to a client with a probe response frame, containing capability information, supported data rates, etc., after the station receives a probe request frame

Disassoication frames: A station sends a disassociation frame to another station if it wishes to

terminate the association.

Deauthentication frames: A station sends a deauthentication frame to another station if it wishes to terminate secure communications.

5.8 GHZ freq Chart

Frequency Band	Channel ID	FCC (GHz)	ETSI (GHz)	MKK (GHz)	SG (GHz)	ASIA (GHz)	TW (GHz)
Lower Band (36 = default)	34	—	—	5.170 [1]	—	—	—
	36	5.180	5.180	—	5.180	—	—
	38	—	—	5.190	—	—	—
	40	5.200	5.200	—	5.200	—	—
	42	—	—	5.210	—	—	—
	44	5.220	5.220	—	5.220	—	—
	46	—	—	5.230	—	—	—
	48	5.240	5.240	—	5.240	—	—
Middle Band (52 = default)	52	5.260	5.260	—	—	—	5.260
	56	5.280	5.280	—	—	—	5.280
	58	5.300	5.300	—	—	—	5.300
	60	5.320	5.320	—	—	—	5.320
H Band	100	—	5.500	—	—	—	—
	104	—	5.520	—	—	—	—
	108	—	5.540	—	—	—	—
	112	—	5.560	—	—	—	—
	116	—	5.580	—	—	—	—
	120	—	5.600	—	—	—	—
	124	—	5.620	—	—	—	—
	128	—	5.640	—	—	—	—
	132	—	5.660	—	—	—	—
	136	—	5.680	—	—	—	—
	140	—	5.700	—	—	—	—
Upper Band (149 = default)	149	5.745	—	—	5.745	5.745	5.745
	153	5.675	—	—	5.675	5.675	5.675
	157	5.785	—	—	5.785	5.785	5.785
	161	5.805	—	—	5.805	5.805	5.805
ISM Band	165	5.825	—	—	5.825	—	5.825

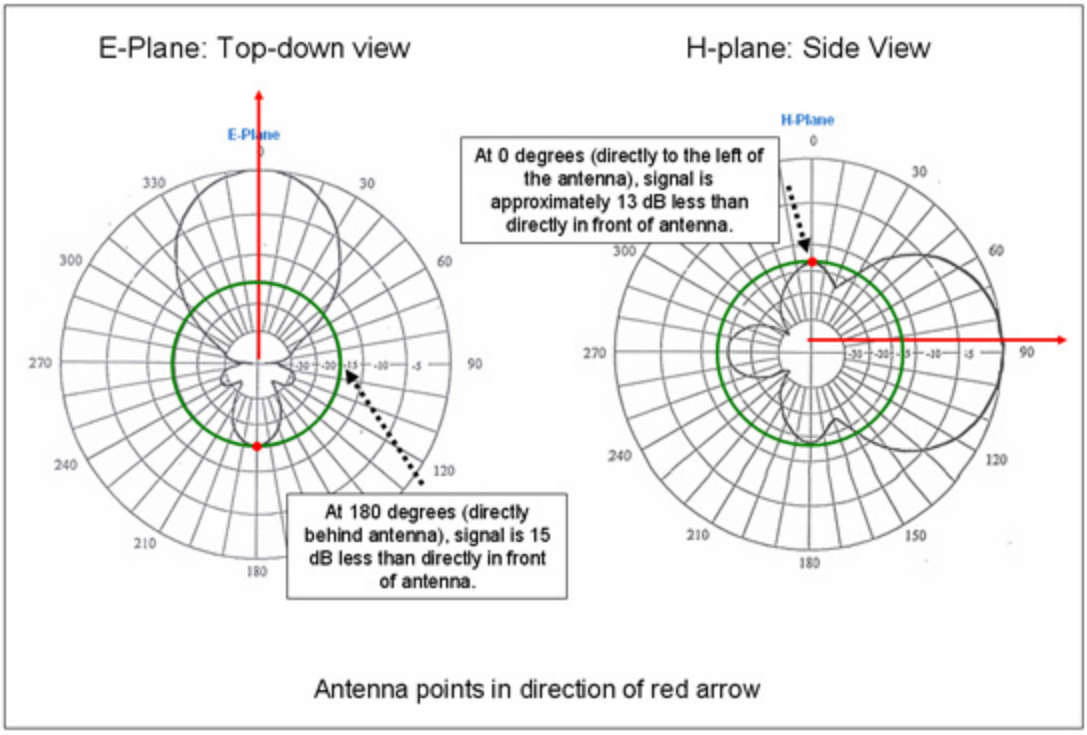
Note 1: Channel 34 is the default channel for Japan

2.4 Ghz Channel list

Kanal	Trägerfrequenz	Frequenzbereich	DE	ES	FR	USA	JP
1	2412 MHz	2399,5 MHz - 2424,5 MHz	×			×	×
2	2417 MHz	2404,5 MHz - 2429,5 MHz	×			×	×
3	2422 MHz	2409,5 MHz - 2434,5 MHz	×			×	×
4	2427 MHz	2414,5 MHz - 2439,5 MHz	×			×	×
5	2432 MHz	2419,5 MHz - 2444,5 MHz	×			×	×
6	2437 MHz	2424,5 MHz - 2449,5 MHz	×			×	×
7	2442 MHz	2429,5 MHz - 2454,5 MHz	×			×	×
8	2447 MHz	2434,5 MHz - 2459,5 MHz	×			×	×
9	2452 MHz	2439,5 MHz - 2464,5 MHz	×			×	×
10	2457 MHz	2444,5 MHz - 2469,5 MHz	×	×	×	×	×
11	2462 MHz	2449,5 MHz - 2474,5 MHz	×	×	×	×	×
12	2467 MHz	2454,5 MHz - 2479,5 MHz	×		×		×
13	2472 MHz	2459,5 MHz - 2484,5 MHz	×		×		×
14	2477 MHz	2464,5 MHz - 2489,5 MHz					×

DE = Deutschland / ES = Spanien / FR = Frankreich / JP = Japan

Azimuth and Elevation charts


E-Plane: Top-down view
H-plane: Side View
E-Plane
H-Plane
At 0 degrees (directly to the left of the antenna), signal is approximately 13 dB less than directly in front of antenna.
At 180 degrees (directly behind antenna), signal is 15 dB less than directly in front of antenna.
Antenna points in direction of red arrow