Network+ | 10. Wireless Networks Cheat Sheet

by Aelphi (Aelphi) via cheatography.com/179727/cs/37877/

Wireless Network

WIFI standard	IEEE 802.11
	AdHoc (p2p) or Infrastructure mode (star topo)
WAP	*Wireless Access Point*
	extend wired LAN into wireless domain, devices are in the same subnet, single collision domain.
Wireless Router	gateway device, routing capacity added.

Wireless Service Sets

IBSS	adHoc mod only, no AP, no internet
BSS	one single AP connected to network
ESS	Several AP to extend coverage
Mesh Topology	combination of several types (WIFI, MW, cellular, etc)
AP Placement	Enough coverage but limit ovelapping
2.4GHz	10-15% overlapping, but with diff. channels. Channels shall not overlap
5 GHz	2 cells separation minimum
Sites survey	heatmaps to dertemine coverage gaps
Range extender	wireless repeater

Antennas

Effectiveness factors	distance, pattern, environment
Omnidirec-tional	radiates equally in all directions
Unidirectional	focus power in one direction, covers long distances (Yagi antenna)

802.11 standards

802.11b	2.4GHz	11Mbps
802.11g	"	56Mbps
802.11a	5GHz	56Mbps
802.11ac (WIFI5)	"	3Gbps (MU-MIMO)
802.11n (Wifi 4)	2.4 and 5GHz	150-600 Mbps (MIMO)
802.11ax (Wifi 6)	2.4, 5GHz & 6GHz	9.6Gbps (MU-MIMO)

Frequencies

DSSS	Spread spectrum modulation, reliable, inefficent use of bandwith
FHSS	Spread spectrum modulation, increased security, limited bandwith, latency & complexity (syncro)
OFDM	Multi carrier modulation (52 streams)
--------	----------
Channel	virtual medium to exchange data
2.4GHz	11-14 channels (US, World, Japan)
	1, 6 & 11 non-overlapping channels
5GHz	24 non-overlapping channels, 20MHz size
Channel Bonding	wider channel created with merging neighboring channels
--------	----------
RFI	Interferences due to similar fq on several devices
CSMA/CA	Collision avoidance principle
	Request to Send <> Clear to Send

Wireless Security	
PSK	Pre-Shared Key = WIFI Key
WEP	802.11 original security standard
unsecure	Initialization Vector (**IV**)
WPA	**TKIP** (IV+RC4)
replace WEP	MIC (integrity check)
WPA2	802.11i standard
strong	**CCMP** integrity check
	AES encryption
Authentication	Entreprise vs Personnal mode
	credentials vs PSK
802.1x	network authentication for each user
EAP	secured tunneling using 802.1x
MAC Filtering	listing of permitted MAC adresses
NAC	permission on devices' characteristics like OS or antivirus version
Captive Portals	web page with credential login or certificate
Geofencing	GPS or RFID real-world boundaries
Disable SSID broadcast	but can be detected with sniffing tools
Rogue AP	Malicious AP setup to capture packets
Wardriving	reconnaissance looking for unsecured Wless NW
War chalking	symbols on a wall to notify AP charac.