Wireless and Wi-Fi cheat sheet

Every term in CompTIA Network+ N10-009 objective 2.3 (channels, frequencies, SSIDs, network types, encryption, authentication, antennas and AP types), Bluetooth, NFC and RFID from A+ 2.2, the 802.11 standards from a to be, and the wireless security around them.

Core 28 is every term in CompTIA Network+ N10-009 objective 2.3, plus Bluetooth, NFC and RFID from CompTIA A+ 220-1201 objective 2.2. A+ lists 802.11 standards only as a topic, so Standards 7 matches each one to its band, speed or Wi-Fi name. Ext. 20 adds the wireless security, tools and attacks around them. Speeds are the maximums in each standard. The short descriptions are ours.

TERM	WHAT IT IS
CORE 28	
Frequencies	
2.4 GHz	**Longest range, most crowded** Goes through walls best, but has only 3 non-overlapping channels and shares the air with Bluetooth and microwaves
5 GHz	**Middle band, more channels, less reach** Many more channels and faster speeds than 2.4 GHz, but weaker through walls
6 GHz	**Newest band, Wi-Fi 6E and 7 only** Wide open spectrum with no older devices on it. Shortest range of the three
Band steering	**Shifts capable clients to faster radio** The AP pushes devices that can use the faster band onto it, leaving 2.4 GHz for the rest
Channels	
Channel width	**20, 40, 80, 160 or 320 MHz** Wider channels carry more data but there are fewer of them, so they overlap more easily. 320 MHz is new in Wi-Fi 7
Non-overlapping channels	**1, 6 and 11 on 2.4 GHz** The only three 2.4 GHz channels in the US that don't interfere with each other
Regulatory impacts	**Country rules on channels and power** Each country decides which channels can be used and how much power an AP may transmit
802.11h	**Avoids radar on 5 GHz (DFS, TPC)** Adds Dynamic Frequency Selection and Transmit Power Control so 5 GHz Wi-Fi stays clear of radar
Network names	
SSID	**The network name clients see** Service set identifier: the name of the wireless network
BSSID	**An AP radio's MAC address** Basic service set identifier: identifies one AP radio, so it's unique even when the SSID is shared

TERM	WHAT IT IS
`ESSID`	**One name across many APs** Extended service set identifier: several APs share one SSID so clients can roam between them
Network types	
`Infrastructure`	**Clients join through an access point** The normal setup: every device talks to an access point, which connects to the wired network
`Ad hoc`	**Devices link directly, no AP** Devices connect straight to each other, often for a quick setup or file share
`Mesh network`	**APs relay traffic to each other** Access points pass traffic between themselves, so only one needs a cable back to the network
`Point to point`	**A dedicated link between two sites** Two directional antennas aimed at each other connect two buildings or sites
Security	
`WPA2`	**AES-CCMP with a 4-way handshake** Wi-Fi Protected Access 2: AES encryption. Still common, but weaker passwords can be cracked offline
`WPA3`	**SAE login that resists guessing** Uses Simultaneous Authentication of Equals, which stops offline password guessing and adds forward secrecy
`PSK`	**One password shared by everyone** Pre-shared key: home and small office Wi-Fi where every device uses the same passphrase
`Enterprise`	**Each user logs in via RADIUS** Each person signs in with their own account through 802.1X and a RADIUS server, so access can be removed per user
`Guest network`	**Visitors kept off the internal LAN** A separate wireless network that gives visitors internet access but no way into company systems
`Captive portal`	**Sign-in page before you get online** The web page a guest network shows first, to accept terms or log in. Common in hotels and cafes
Antennas and APs	
`Omnidirectional`	**Covers a full circle around it** Sends signal evenly in every direction. The usual antenna on an AP in the middle of a room
`Directional`	**Aims the signal at one spot** Concentrates signal in one direction for long range, like a link between buildings
`Autonomous AP`	**Configured one by one, no controller** A standalone AP that holds its own settings. Fine for a few APs, slow to manage at scale
`Lightweight AP`	**Managed by a central controller** The AP takes its settings from a wireless LAN controller, so hundreds can be managed in one place
Other wireless (A+)	
`Bluetooth`	**Short-range link for headsets, mice** Pairs nearby devices on 2.4 GHz, usually within about 10 meters
`NFC`	**Works within about 4 cm, tap to pay** Near-field communication: a very short-range link for tap to pay and pairing

TERM	WHAT IT IS
RFID	**Tags read by radio, like badges** Radio-frequency identification: a reader picks up small tags in badges, inventory labels and toll passes
STANDARDS 7 · 802.11	
802.11a	**5 GHz, 54 Mbps** The first 5 GHz standard, from 1999
802.11b	**2.4 GHz, 11 Mbps** The first popular Wi-Fi, also from 1999
802.11g	**2.4 GHz, 54 Mbps** Brought 54 Mbps to 2.4 GHz in 2003
802.11n	**Wi-Fi 4** 2.4 and 5 GHz, up to 600 Mbps with MIMO
802.11ac	**Wi-Fi 5** 5 GHz only, up to about 6.9 Gbps
802.11ax	**Wi-Fi 6 and 6E** 2.4 and 5 GHz, plus 6 GHz as Wi-Fi 6E. Up to 9.6 Gbps
802.11be	**Wi-Fi 7** 2.4, 5 and 6 GHz with 320 MHz channels. Up to about 46 Gbps
EXT. 20 · SECURITY, TOOLS AND ATTACKS	
WEP	**First Wi-Fi security, long broken** Wired Equivalent Privacy. Can be cracked in minutes, so never use it
WPA	**Stopgap after WEP, used TKIP** The first Wi-Fi Protected Access, a quick fix for WEP until WPA2 arrived
TKIP	**WPA's cipher, now deprecated** Temporal Key Integrity Protocol, used by the first WPA. Replaced by AES-CCMP in WPA2
WPS	**PIN or button setup, easy to crack** Wi-Fi Protected Setup. The 8-digit PIN can be brute-forced, so turn it off
SAE	**WPA3's password handshake** Simultaneous Authentication of Equals, also called Dragonfly
802.1X	**Port-based login before access** The standard behind Enterprise Wi-Fi: no network access until the user is authenticated
RADIUS	**Server that checks Enterprise logins** The authentication server that 802.1X asks whether a user may connect
EAP-TLS	**Certificates on client and server** The strongest common Enterprise method. Each device needs its own certificate
PEAP	**Password login in a TLS tunnel** The server has a certificate; users sign in with a username and password inside the tunnel
DFS	**Leaves a channel when it hears radar** Dynamic Frequency Selection, part of 802.11h
TPC	**Turns transmit power down** Transmit Power Control, the other half of 802.11h
MU-MIMO	**Sends to several clients at once** Multi-user MIMO: separate streams to different devices at the same time, using multiple antennas
OFDMA	**Splits a channel among clients** Wi-Fi 6 divides each channel into small pieces so many devices share it with less waiting

TERM	WHAT IT IS
`Channel bonding`	**Joins 20 MHz slices into one wider** Combines neighboring channels into 40, 80, 160 or (in Wi-Fi 7) 320 MHz for more speed
`802.11r`	**Fast handoff between APs** Fast roaming, so calls and video don't drop when you walk to the next AP
`Evil twin`	**Fake AP copying a real network** An attacker's AP with the same SSID, used to catch logins and traffic
`Rogue AP`	**Unapproved AP plugged into the LAN** An access point nobody authorized, opening a back door into the network
`Wi-Fi analyzer`	**Shows channels, signal and overlap** An app or device that lists nearby networks, their channels and signal strength
`Heat map`	**Coverage drawn over a floor plan** A site survey drawn over a floor plan, showing where coverage is strong or weak
`Zigbee`	**Low-power mesh for smart homes** A slow, low-power wireless mesh for sensors, plugs and lights