

Wi-Fi 802.11

11	2.4 GHz	2Mbps	
11b wifi 1	2.4	10mbps	11
11a wifi 2	5	50mbps	11
11g wifi 3, native and mixed mode ji	2.4	50mbps	11b
11n wifi 4, legacy(b), mixed(a,g) n greenfield(n)	2.4/5	500mbps	b, a, g
11ac wifi 5	5	3Gbps	a, g, n
11ax wifi 6	2.4,5,6	10gbps	a, g, n, ac

Wifi Standards

The first standard was 802.11 and several wireless standards were defined under this,

Hardware	To connect wireless to wired, WAP(Wireless Access Point) is required
Software	
Driver	Which talks to NIC
Configuration	Setting up the connectivity and status
Wireless Network Modes	
Ad Hoc Mode(P2P)	Independent Basic Service Set(IBSS) , note here that two devices will be connecting to each other and there is no central device. In this case, a random SSID(32 Characters) is generated for the Network

Infrastructure Mode	Can be termed as WLAN(Wireless LAN) , also called Basic Service Set(BSS) , BSSID is used. For extended network, ESS(Extended Service Set)
	Roaming happens in an ESS, when a connected device switches to another WAP
Transmission Frequency	Half-Duplex connections with frequencies running in either 2.4GHz or 5GHz
Transmission Methods	
Direct-Sequence Spread-Spectrum(DSSS)	Sending different frequencies at the same time
Frequency-Hopping Spread-Spectrum(FHSS)	Hopping between multiple frequencies instantly of sending
Orthogonal Frequency-Division Multiplexing(OFDM)	FHSS but more Bandwidth
Channel	Wifis operate on channels, the 2.4GHz band has 14 different channels
CSMA/CA	
Interframe Gap(IFG)	A certain period for which a frame has to wait before sending signal
Backoff Period	A waiting time if a collision is detected
DCF(Distributed Coordination Function)	If collision is detected, IFG + Backoff for the next frames, also, every sending node should be receiving a ACK packet along with wait-times

We had WPS after 802.11ax which was working in PIN and WPS button mode for devices which had

no interface to configure Wireless networks and instead use these two methods for configuration

Wifi-Security

WEP(Wired Equivalent Privacy)	Low encryption with only 64-bit or 128-bit
WPA(Wifi Protected Access)	EAP(Extensible Authentication Protocol) Authentication - It was a wrapper that would allow around seven PPP authentication methods for the device interconnection. It can be used with 7 different types of authentications
PSK(Pre-Shared Key)	Secret encrypted code on two devices which enable authentication of devices
TLS	Radius with certificate on both the sides
TTLS	Certificate on server-side only
MSCHAPv2 or PEAP(Protected EAP)	Password in the method of MSCHAP and then TLS above it
MD5	Only hashing the shared authentication credentials, very weak
LEAP(Lightweight EAP)	Mixture of Radius and MSCHAP used by Cisco
FAST(Flexible Auth with Secure Tunnel)	Similar to LEAP but used by every OS
	802.1X - Not relying on any PPP Framed Containers but using Ethernet Frames as EAP. It is a port-based authentication where the devices go through a complete AAA process
	TKIP(Temporal Key Integrity Protocol) -

	In WEP, encryption was done using keys which were permanent and posses an attack but in TKIP, the keys are temporarily assigned for scrambling and de-scrambling data. It was used with WPA. Also, the encryption was RC4, hence TKIP-RC4
WPA2	Full-fledged version of 802.11i. The encryption type is AES
WPA3	Uses an encryption key generated based on SAE(Simultaneous Authentication or Equals) rather than relying on using passwords as a form of encryption
Additional Security Measures	
Disable SSID Broadcast	
MAC Filtering	Using ACL
Isolation	Only allowing internet
Geofencing	Authentication based on location, device, network etc.

Enterprise Wireless

Device Construction	
Wireless Administration	Thin Client - Wireless Switches, Thick Client - Wired Management, LWAPP(Lightweight Access Point Protocol), Meraki by Cisco
VLAN Pooling	Pool of same VLANs
POE	Standard 802.3af, 802.3at, 802.3bt, POE/

Implementing Wifi