UNIVERSIDAD
COMPLUTENSE
MADRID

Networks and Protocols 1

Security/Wifi 6/Wifi Mesh/Wifi HaLow

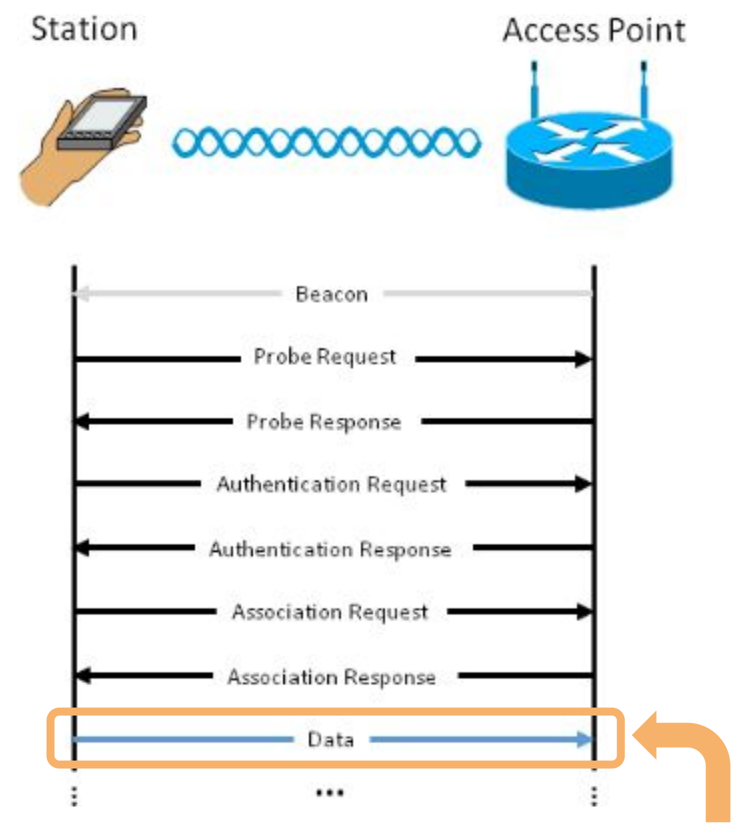
Facultad de Informática

Security in Wifi networks

Authentication modes

- Open Authentication
  - For open networks
  - Used for WPA/WPA2/WPA3, the authentication and key generation comes after open authentication
- Shared Key Authentication:
  - Encryption key shared among all users (WEP)
  - It is used both for authentication and for encryption
  - **OBSOLETE**, very insecure, easy to break

Open Authentication

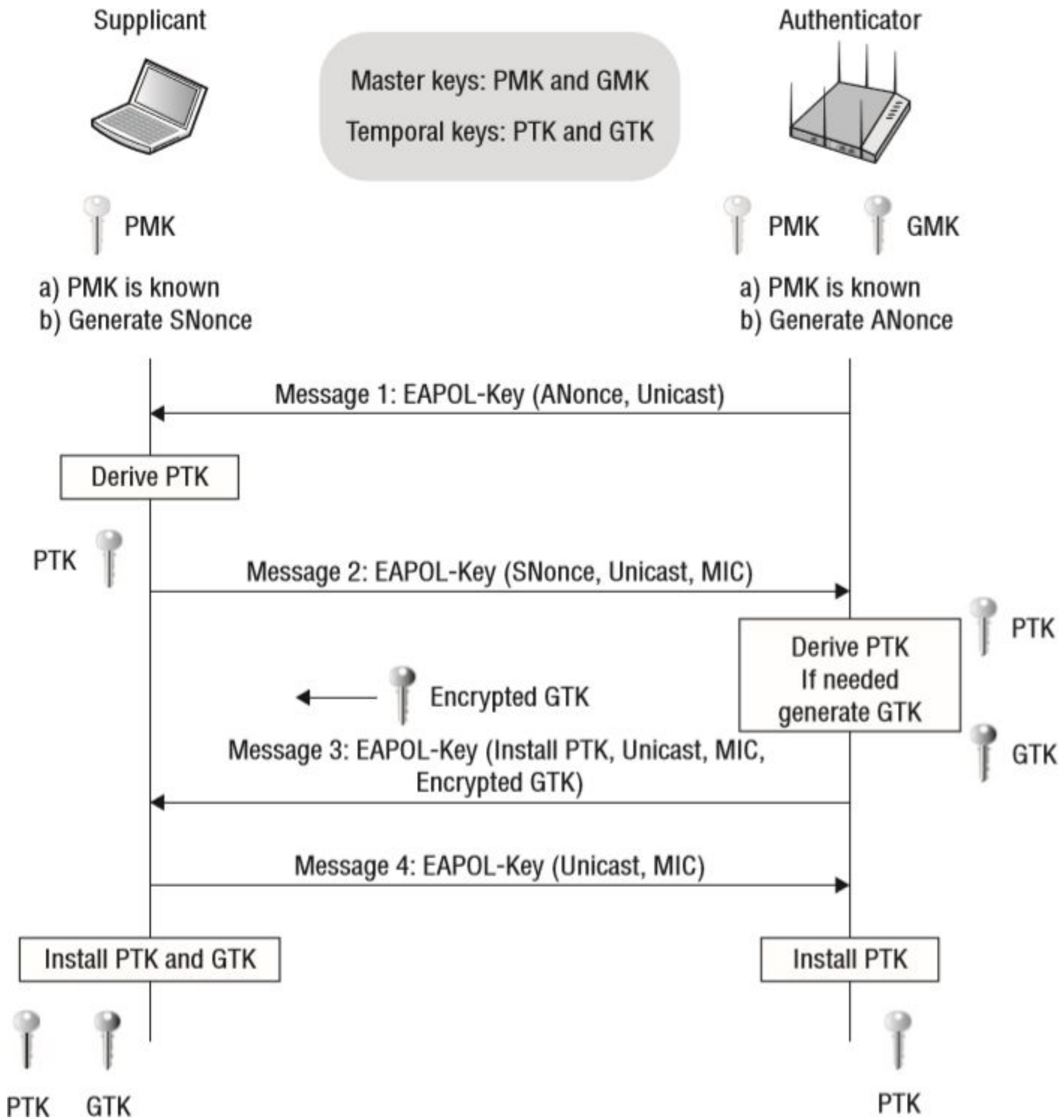


Authentication with WPA/WPA2/WPA3

802.11i Authentication options

	WEP	WPA	WPA2	WPA3
Year	1997	2003	2004	2018
Encryption	RC4	TKIP with RC4	AES-CCMP	AES-CCMP and AES-GCMP
Key size	64 and 128 bits	128 bits	128 bits	128 and 256 bits
Authentication	Open system and shared key	Pre Shared Key (PSK) and 802.1x with EAP	Pre Shared Key (PSK) and 802.1x with EAP	Simultaneous Authentication of Equals (SAE) and 802.x with EAP

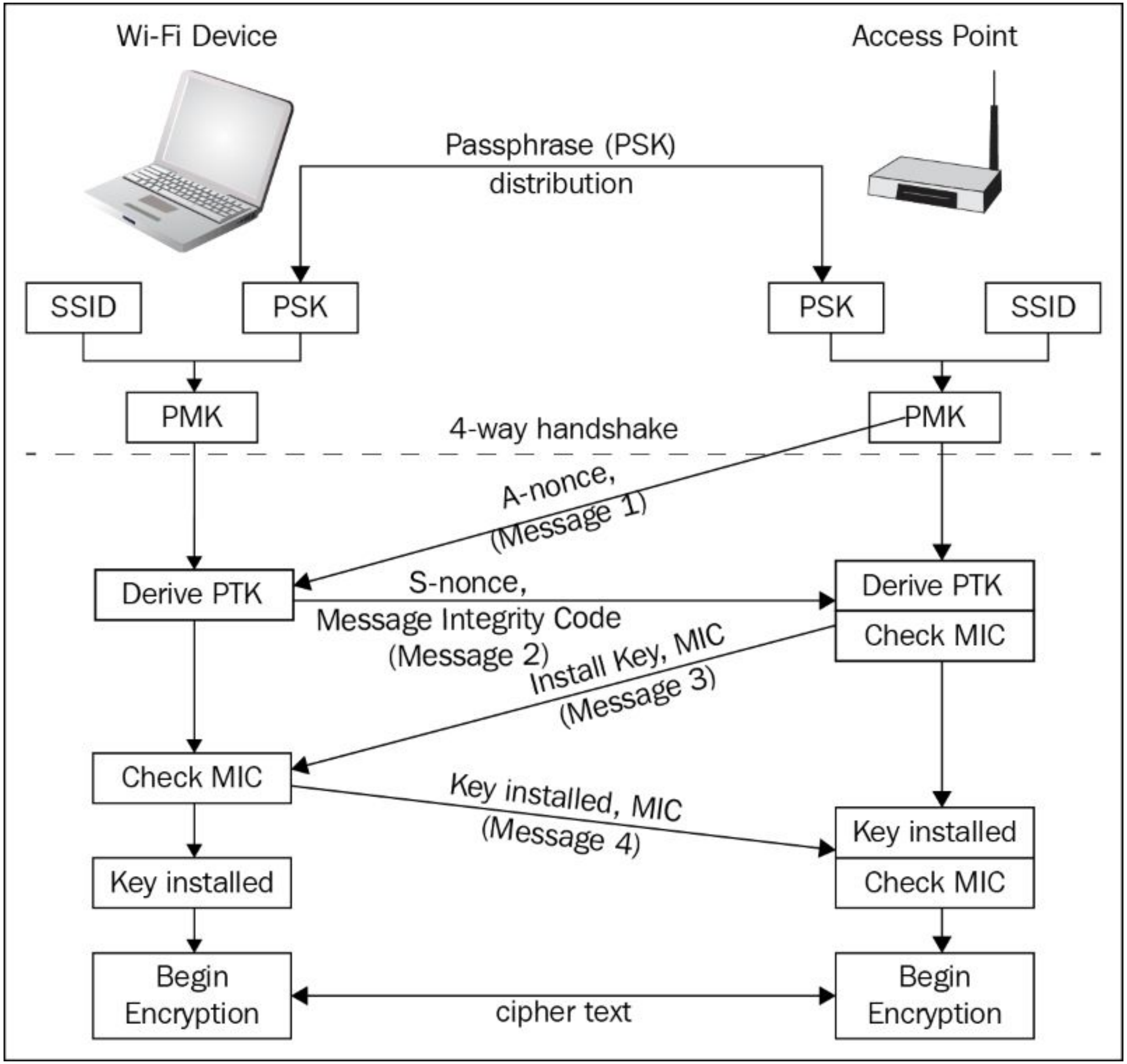
WPA2 4-way handshake



MSK (Master Session Key)
PMK (Pairwise Master Key)
GMK (Group Master Key)
PTK (Pairwise Transit Key)
GTK (Group Temporal Key)
ANonce
SNonce
MIC (Message Integrity Code)
PRF (Pseudo Random Function)

PTK = PRF (PMK + Anonce + SNonce + Mac (AA)+ Mac (SA))

PMK from the PSK (personal)



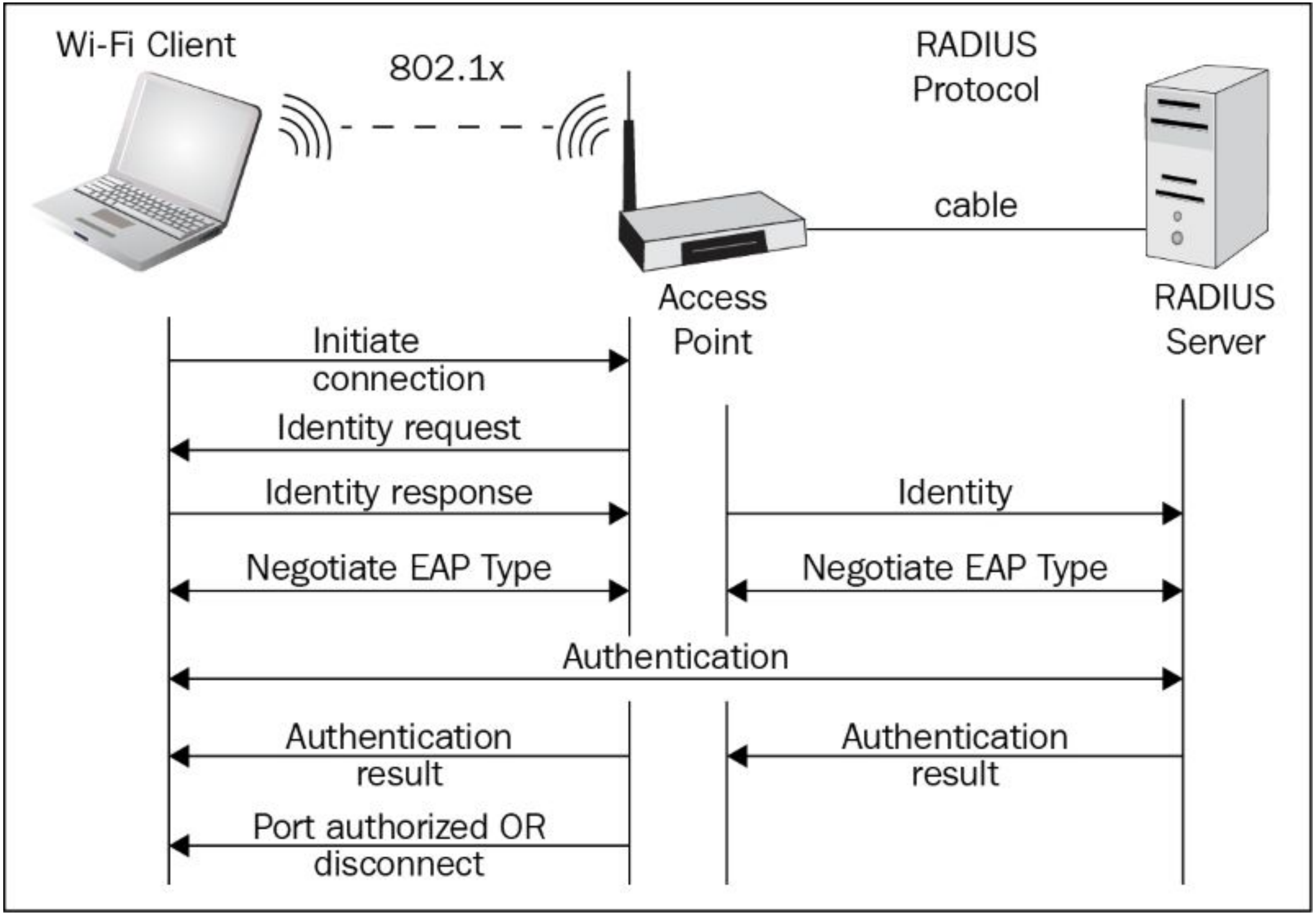
PSK: Pre-Shared Key

The *password* that comes in the sticker behind the router at home

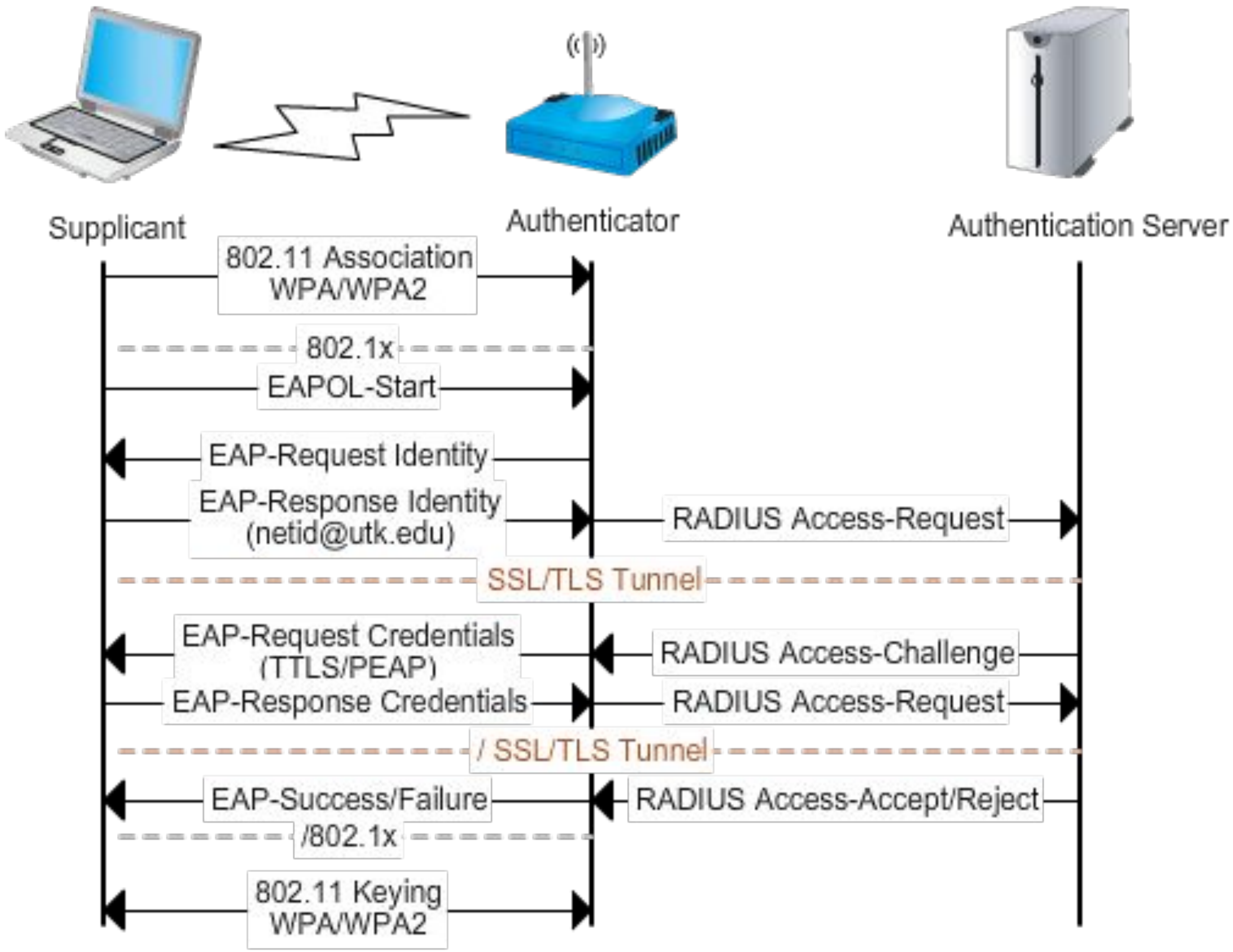
Knowing the PSK you can obtain the PTK if you can sniff the 4-way handshake.

WPA3 avoid this by the SAE that uses Elliptic Curve Diffie-Hellman key exchange

PMK with 802.1X EAP (enterprise)



PMK with 802.1X EAP TTLS + PAP



802.11ax - Wifi6

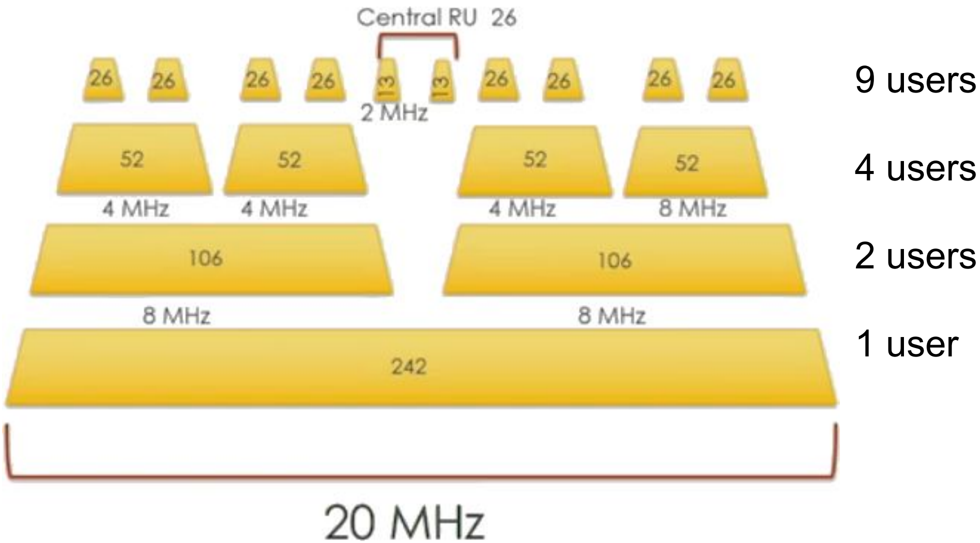
	802.11n	802.11ac	802.11ax
Channel Size (MHz)	20, 40	20, 40, 80, 80 + 80 and 160	20, 40, 80, 80 + 80 and 160
Subcarrier (KHz)	312.5	312.5	**78.125**
Symbol time (µs)	3.2	3.2	**12.8**
Frequency multiplexing	OFDM	OFDM	OFDM & **OFDMA**
Modulation	BPSK, QPSK, 16-QAM, 64-QAM	BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM	BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM **1024-QAM**
Multi User Operation	N/A	Downlink MU-MIMO	**OFDMA UL/DL** MU-MIMO **UL**/DL
Spectrum Bands	2.4GHz & 5GHZ	5GHZ	**2.4GHz** & 5GHZ

802.11ax - OFDMA

312.5 kHz 802.11a/n/ac subcarrier spacing

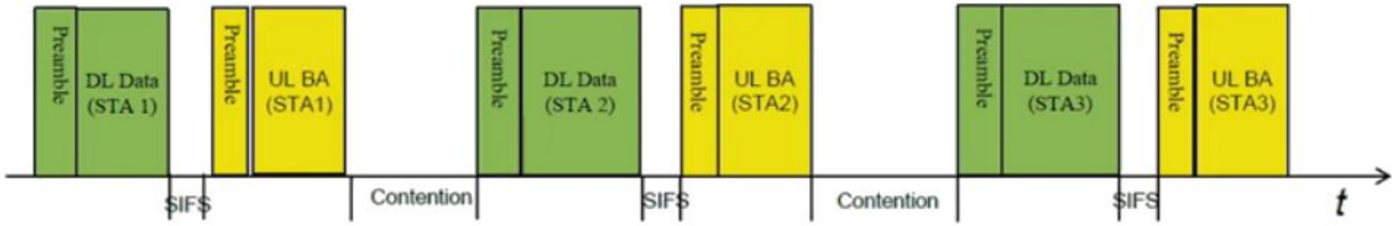
78.125 kHz 802.11ax subcarrier spacing

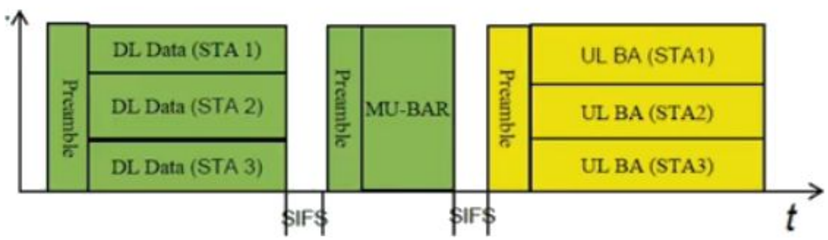
- 256 subcarriers in 20 MHz (40 MHz/512, 80 MHz/1024, 160 MHz/2048)
  - data subcarriers: 234 / 468 /980 / 1960
  - pilots: 8 / 16 /16 /32

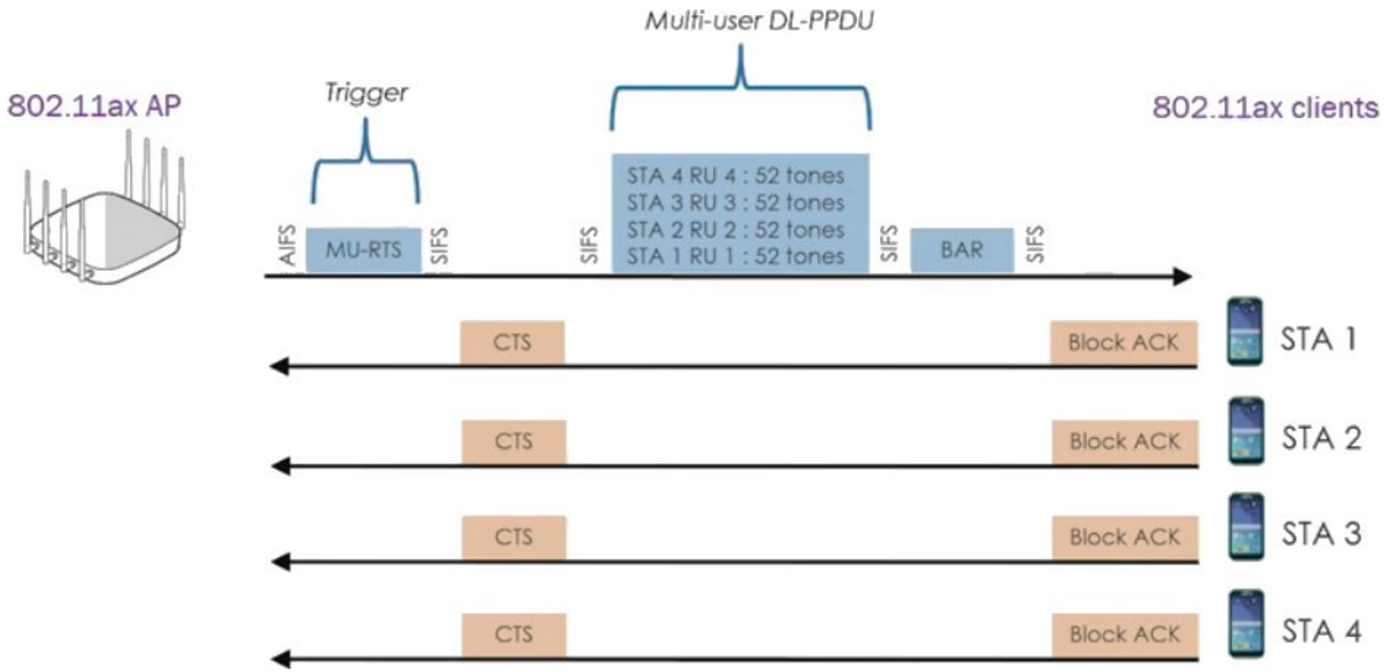


Resource Units (RU) reserved for uplink and downlink

802.11ax - OFDMA







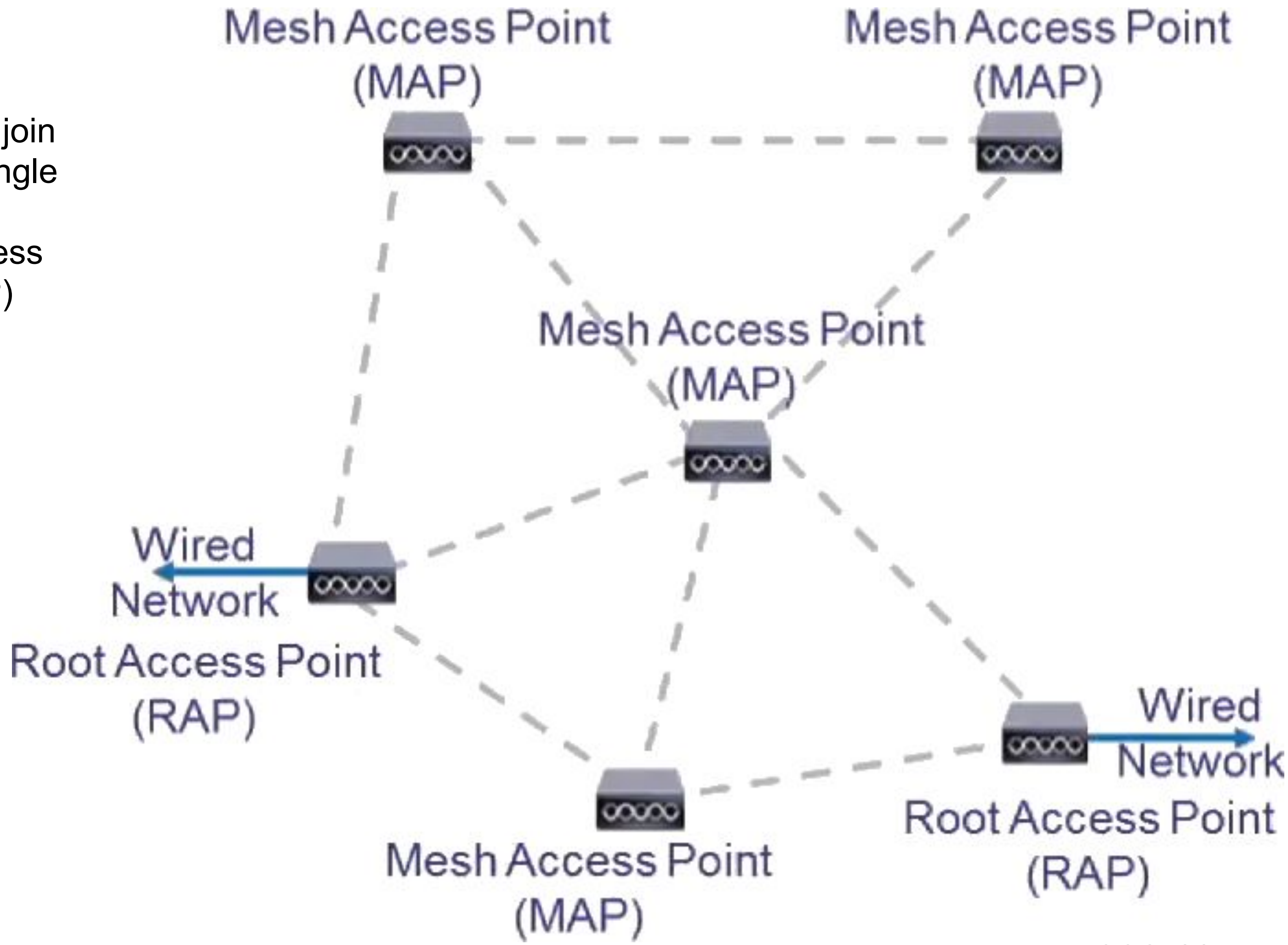
Wifi Mesh

Protocols that enable us to join several WLAN forming a single WAN:

- Cisco Adaptive Wireless Path Protocol (AWPP)
- IEEE 802.11s

Uses:

- Town or campus wifi
- Emargency solutions
- Shared wifi



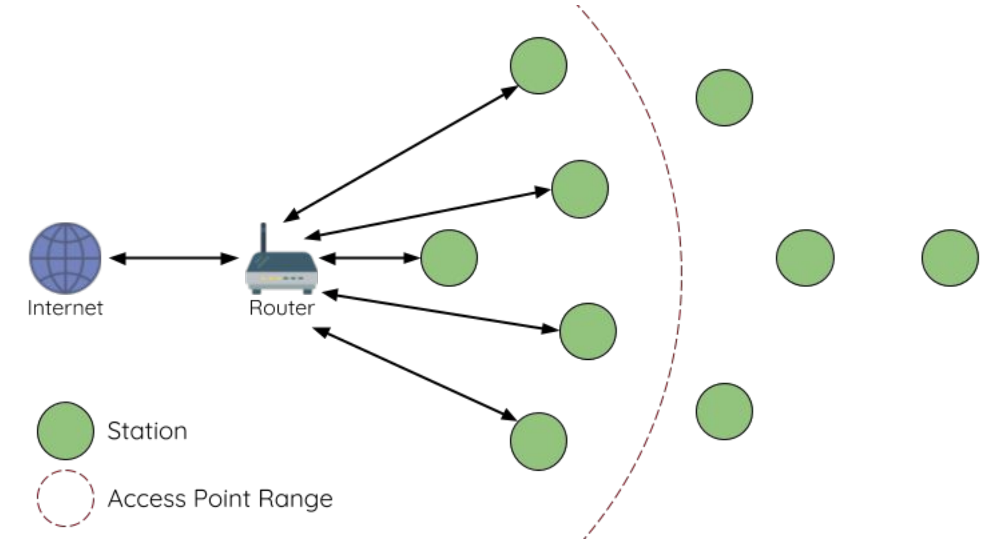
MPP en 802.11s

802.11s Hybrid Wireless Mesh Protocol

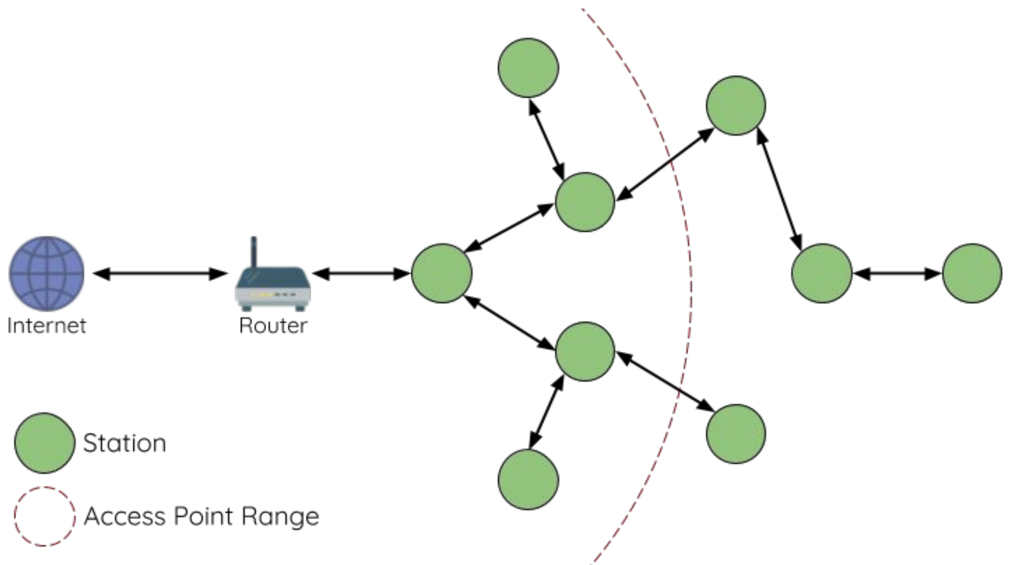
Two configurations:

- With root portal: organized as a tree
  - Rooting based on the distance to the root
- Without root portal: organized as a mesh
  - Distance vector routing algorithms like Radio Metric AODV
    - Cost: time consumed transmitting a packet
  - Link state algorithms like Radio Aware OSLR Path Selection Protocol

ESP Wifi Mesh



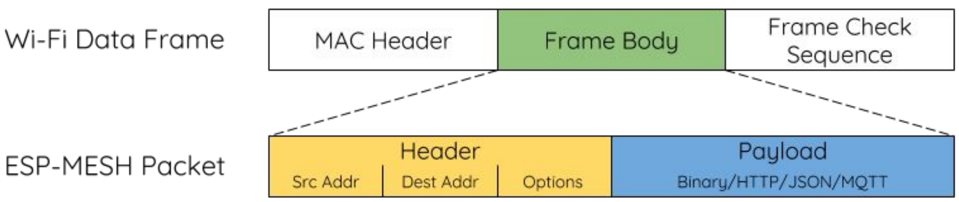
Traditional WLAN

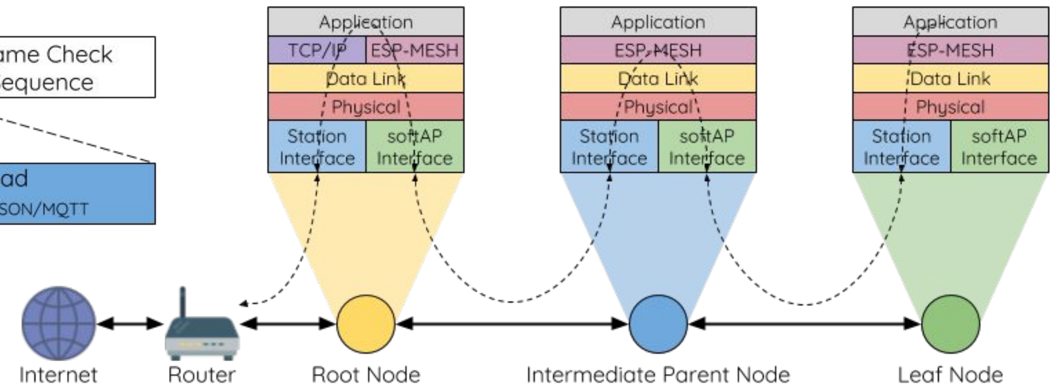


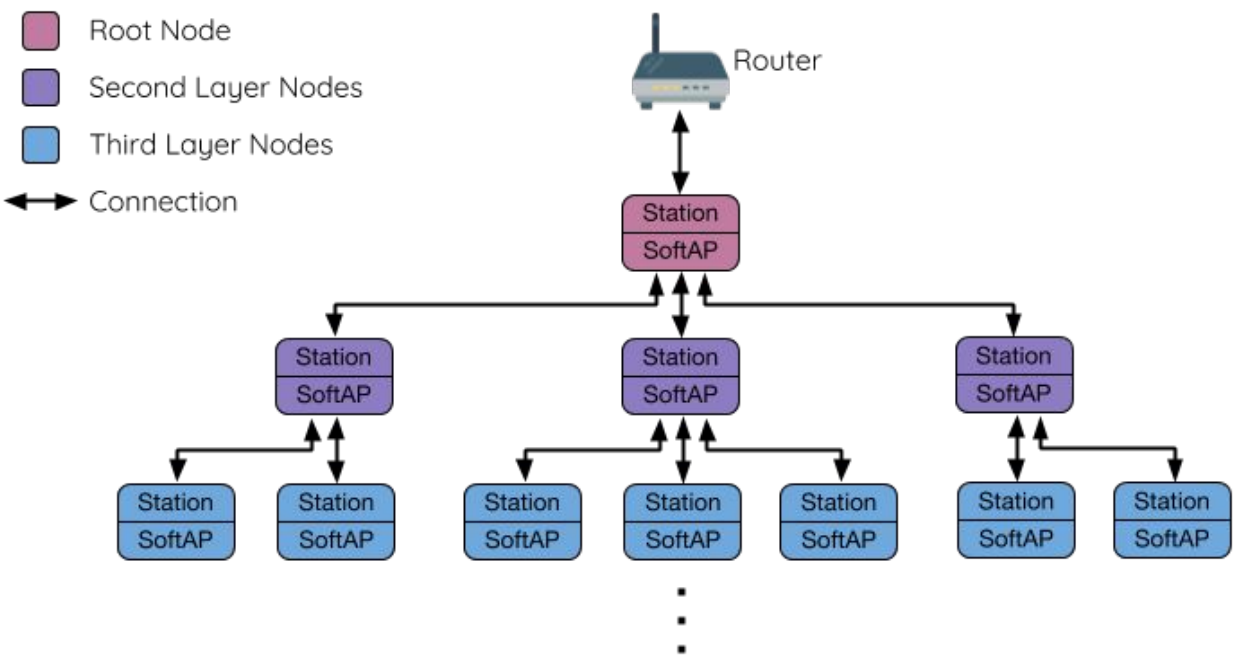
ESP Wifi Mesh

ESP - Wifi Mesh

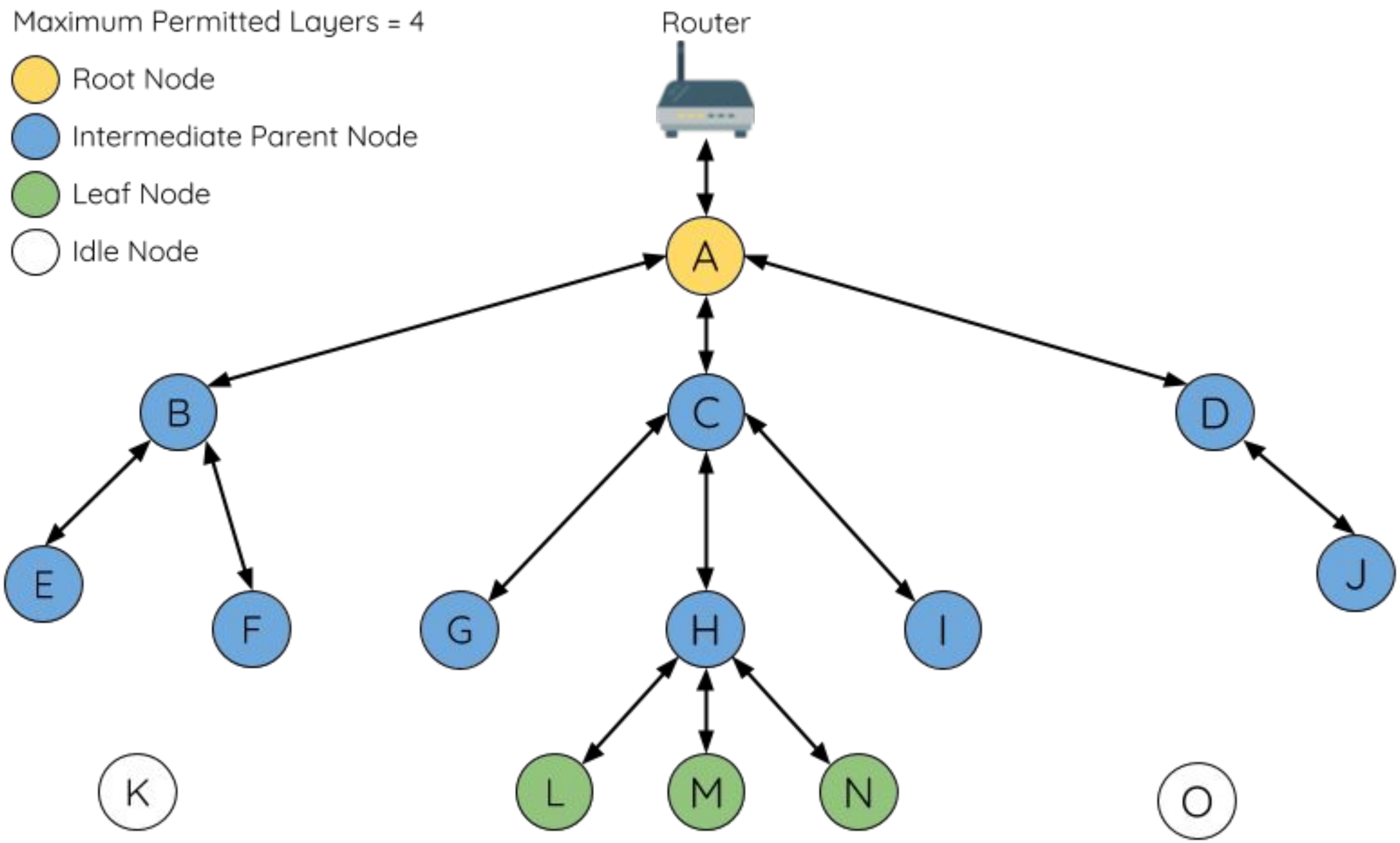
https://docs.espressif.com/projects/esp-idf/en/latest/esp32/api-guides/mesh.html







ESP - Wifi Mesh: types of nodes

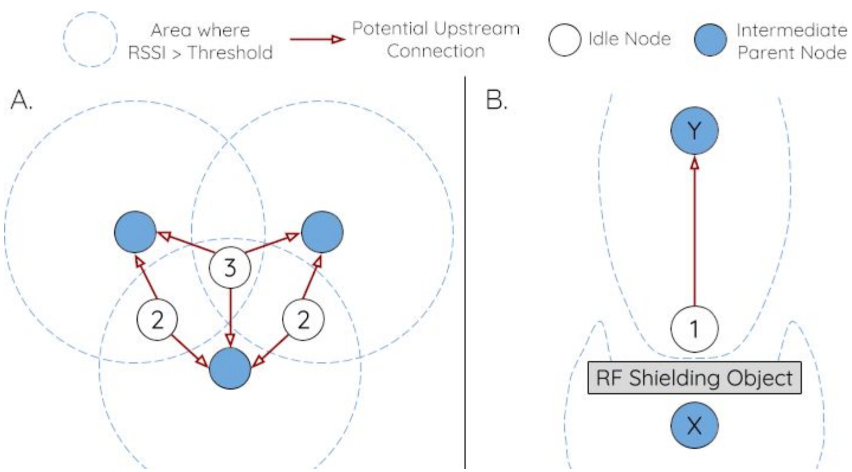


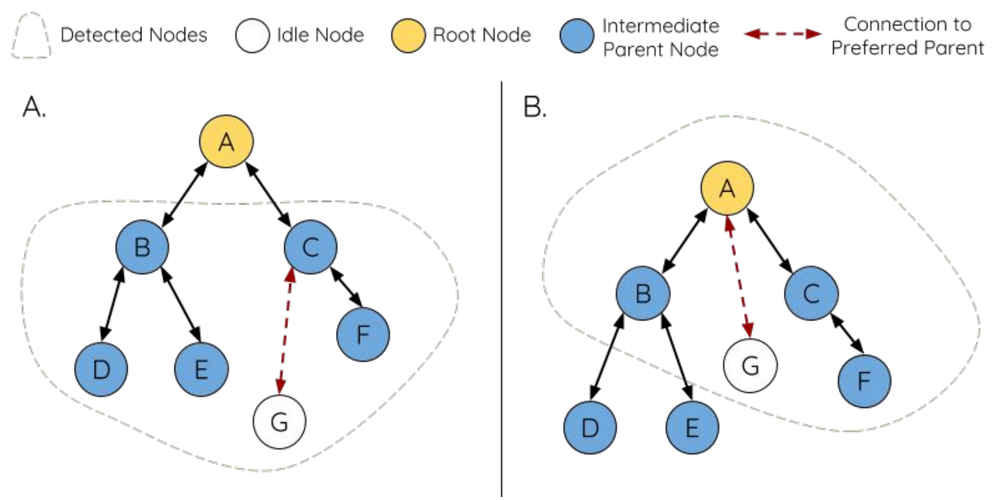
UNIVERSIDAD COMPLUTENSE MADRID

ESP - Wifi Mesh: preferred parent node

The upstream (parent) node is selected based on:

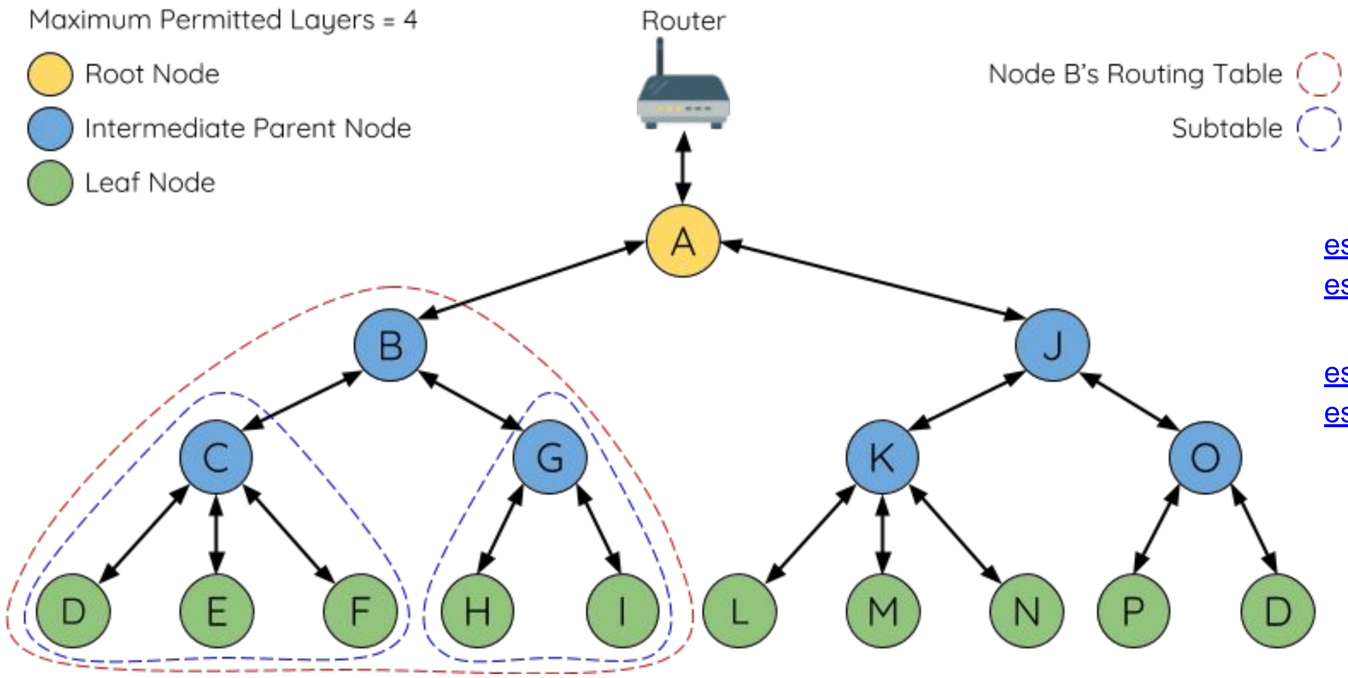
- The Received Signal Strength Indication (RSSI) of the received beacon
  - If the RSSI < threshold -> the node is discarded as parent
- The distance to the root node
- The number of child nodes (in case of tie)





ESP-Mesh allows the programmer to select an alternative procedure to choose an alternative parent node (Mesh Manual Networking Example)

ESP Wifi Mesh: routing



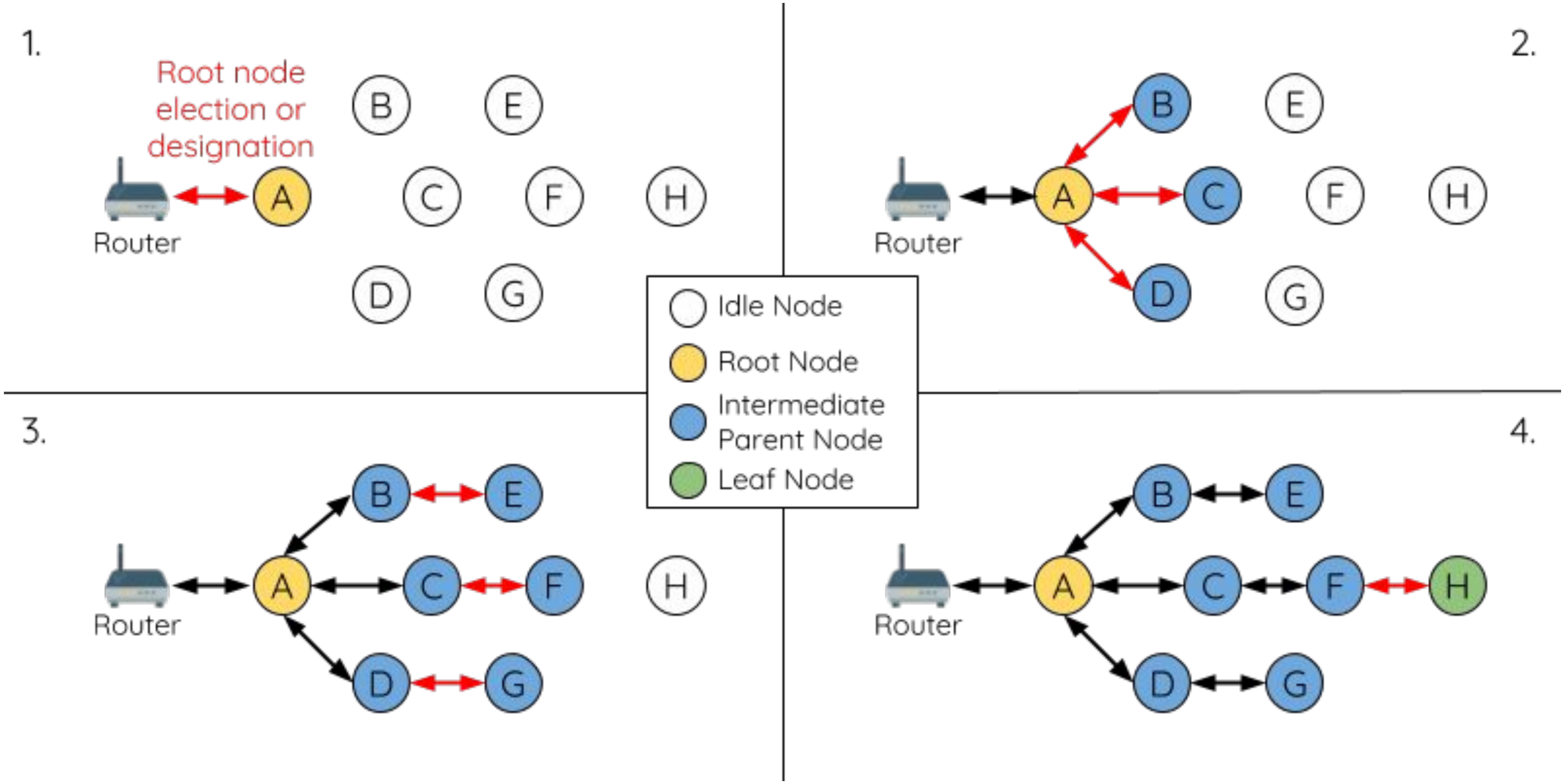
esp_mesh_get_routing_table()
esp_mesh_get_routing_table_size()

esp_mesh_get_subnet_nodes_list()
esp_mesh_get_subnet_nodes_num()

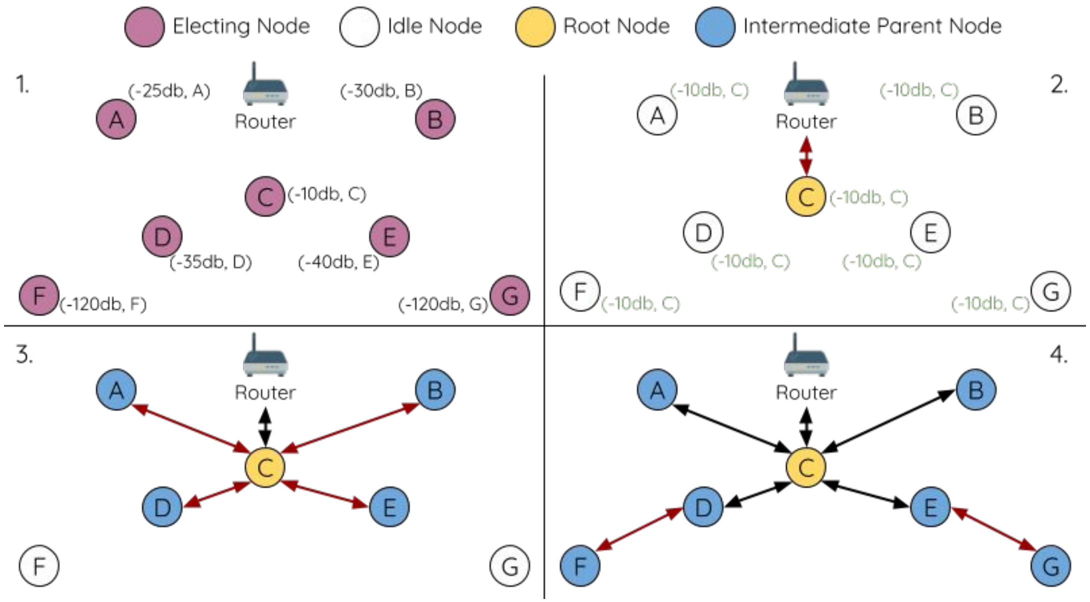
Each node maintains a routing table with the MAC addresses of all the nodes in its subtree

- Partitioned in subtables for each of its child subtrees

ESP Wifi Mesh: network formation



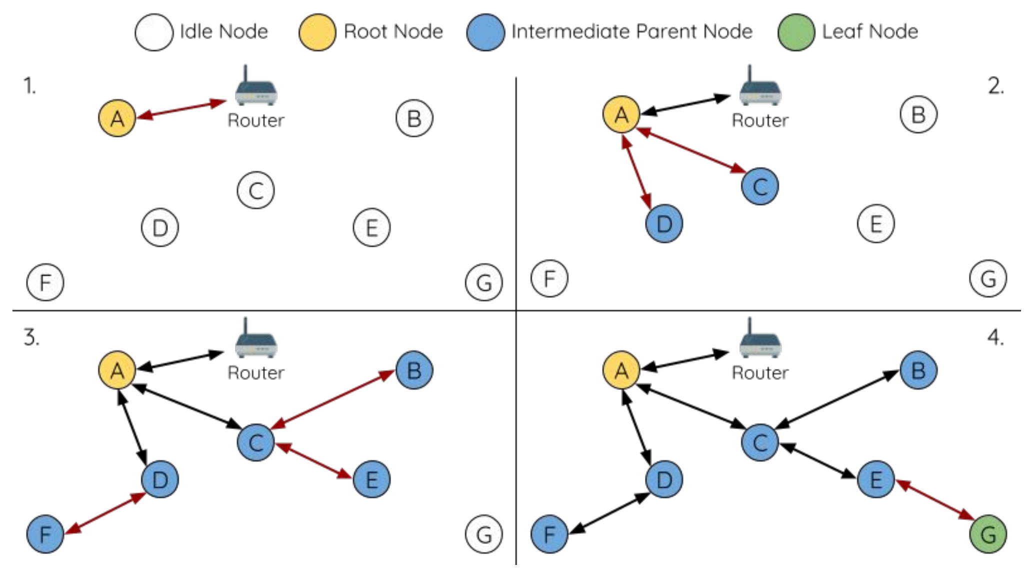
ESP Wifi Mesh: selection of the root node



By election, a distributed process where the RSSI of the beacon frames dominates

esp_mesh_set_attempts()

[esp_mesh_set_vote_percentage()]

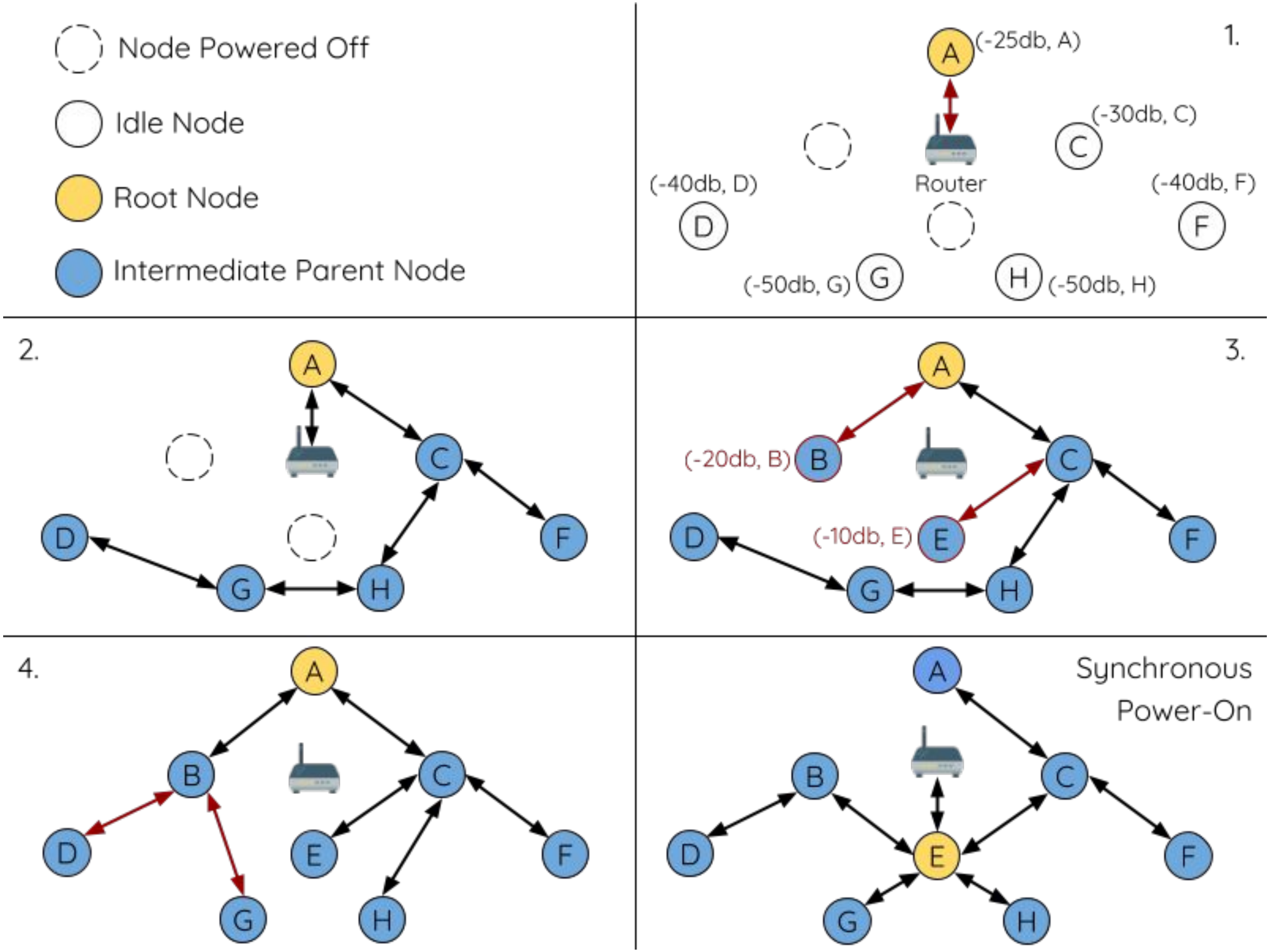


By designation of the programmer

[esp_mesh_set_parent()]

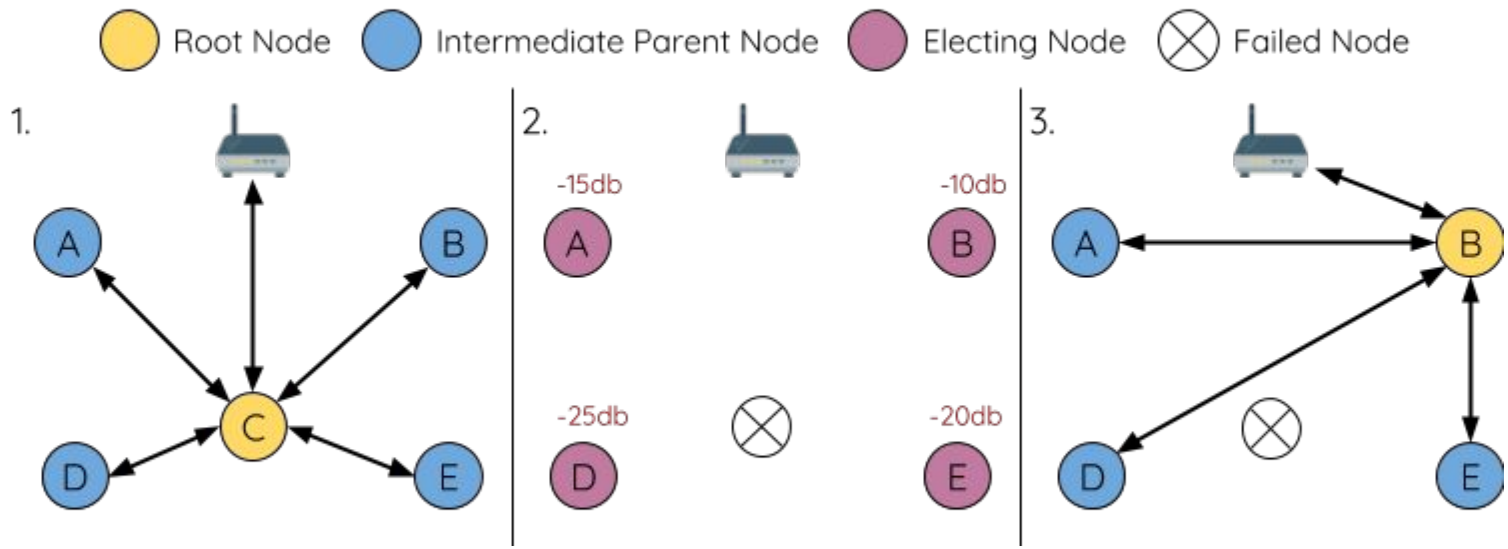
[esp_mesh_fix_root()]

ESP Wifi Mesh: asynchronous power on reset

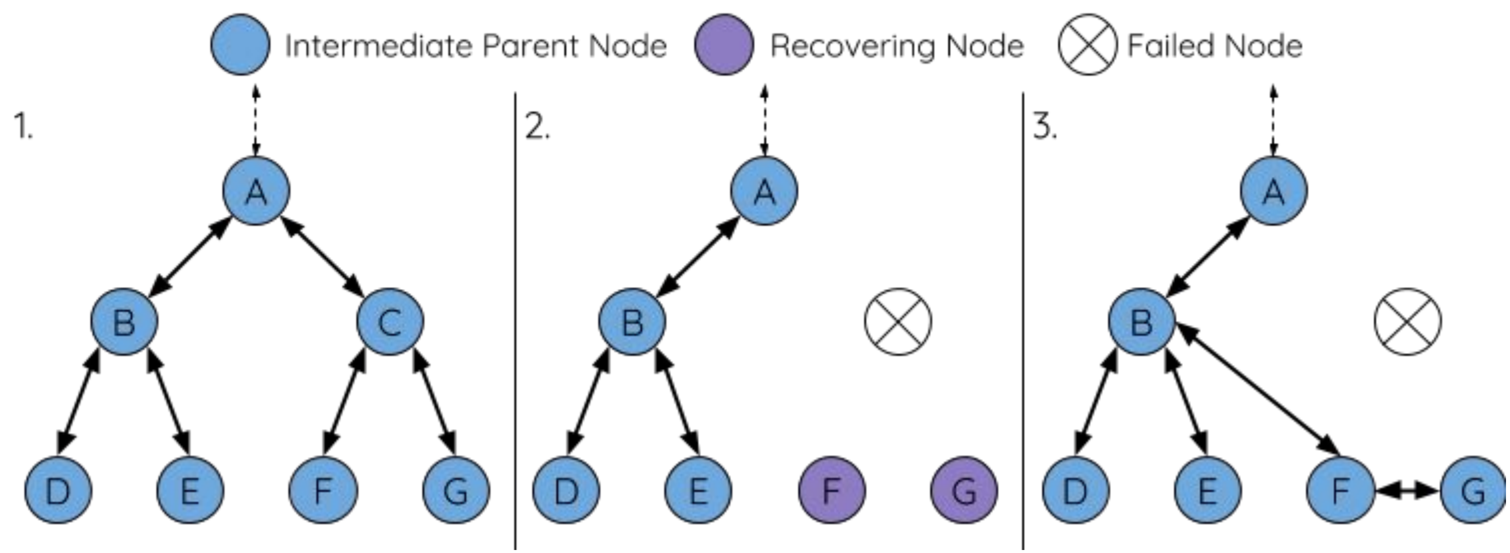


ESP Wifi Mesh: node failure

Root node

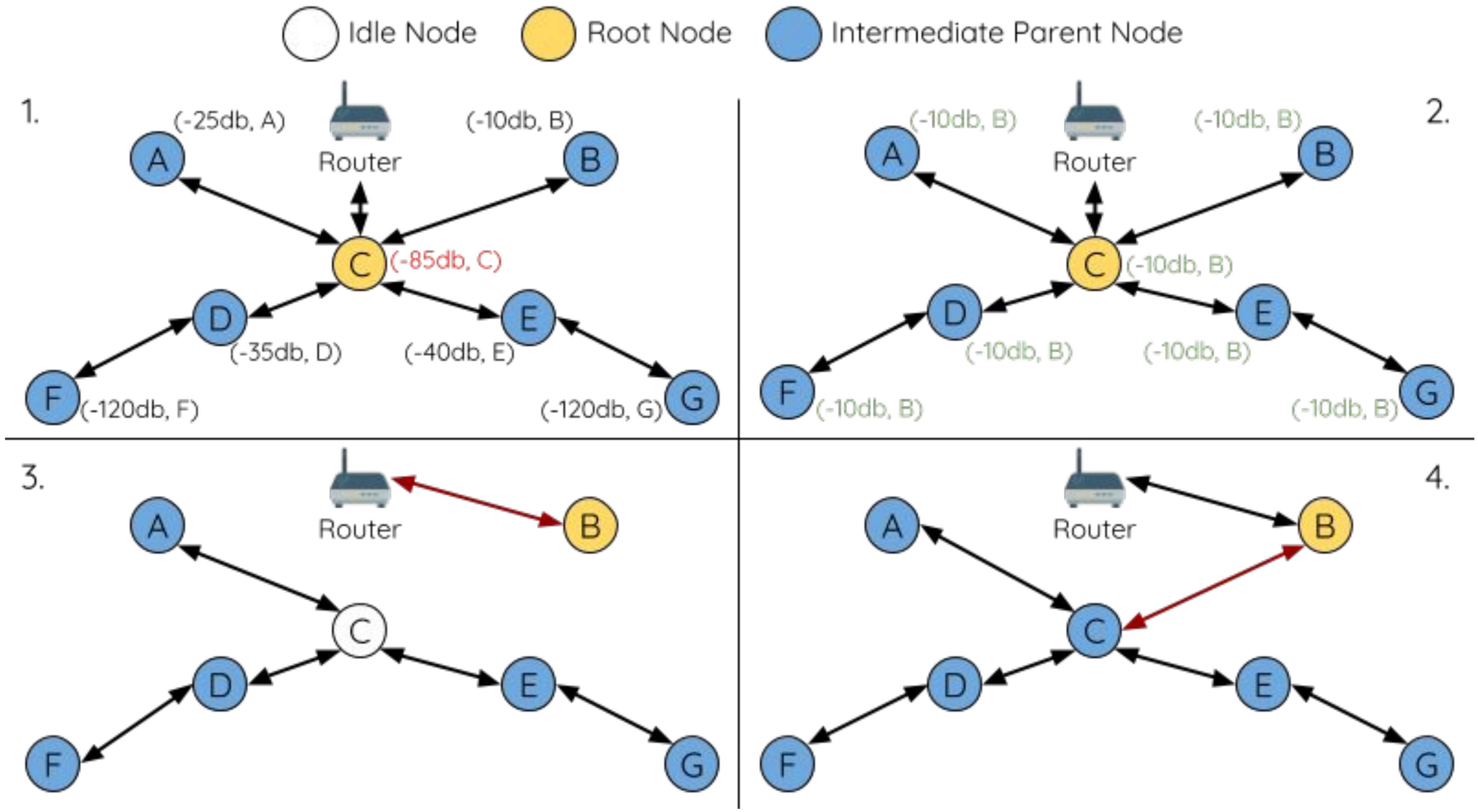


Intermediate parent node



ESP Wifi Mesh: change of root node

[esp_mesh_waive_root()]



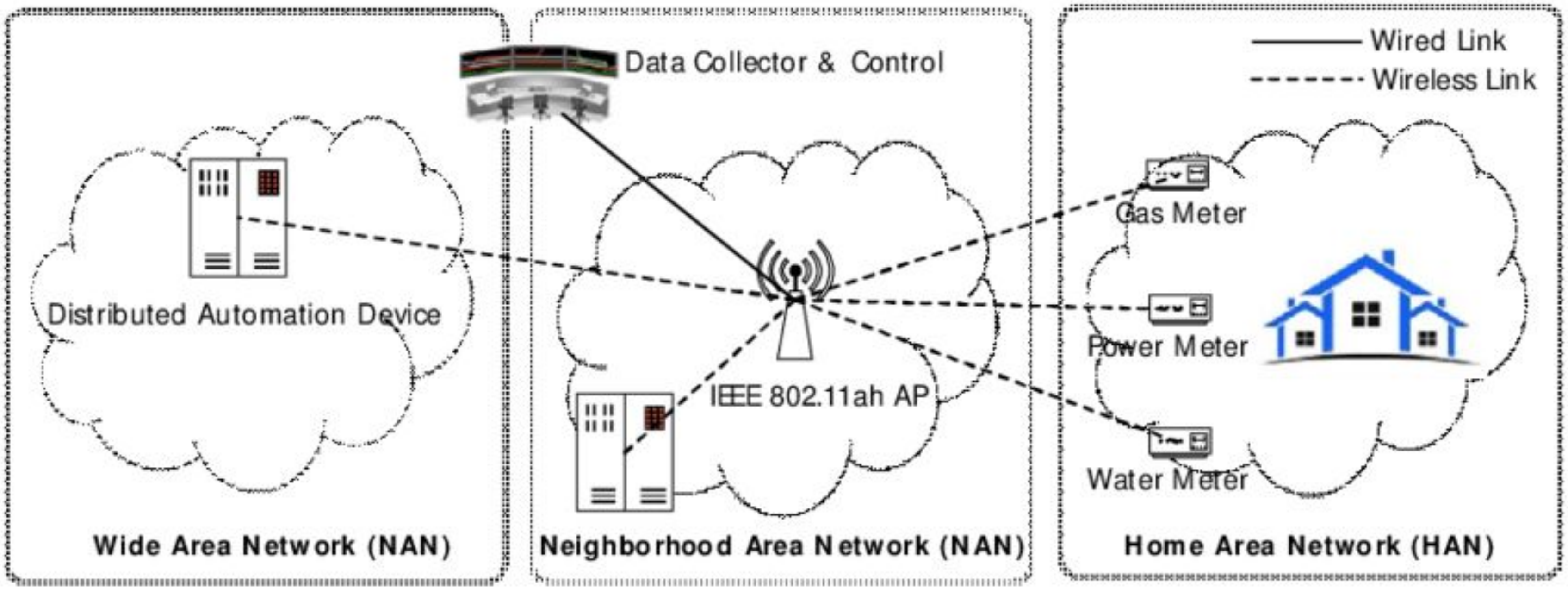
ESP Wifi Mesh: other characteristics

- Multicast
  - By list: Set the packet's destination address to the Multicast-Group Address (01:00:5E:xx:xx:xx).
    - The ESP-WIFI-MESH packet is a multicast packet with a group of addresses
    - The address should be obtained from the header options.
    - Users must then list the MAC addresses of the target nodes as options
  - By group: nodes can be adhered to a multicast group
    - esp_mesh_set_group_id()
- Broadcast
- Upstream flow control
  - Nodes request a reception window to send upstream
  - Parents can control the upstream flow by the size of the window offered

802.11ah - Wifi HaLow

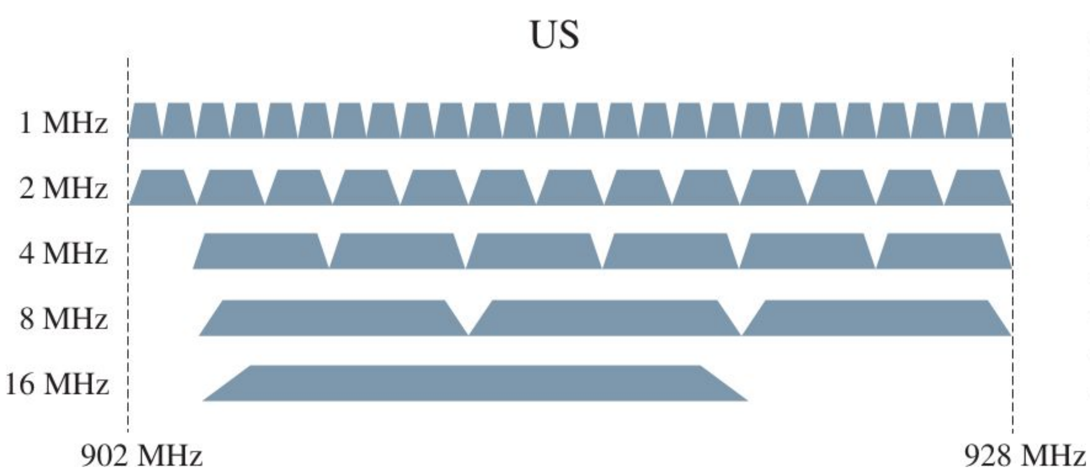
- 802.11 standard for IoT
- Uses Sub GHz band
  - 902 - 928 MHz in USA
  - 863 - 868 MHz in Europe
  - Greater distances ~ 1 km (Neighbour Area Network, NAN)
  - Less congestion, greater penetration
- Lower transmission/data rate
  - Each bit last longer
  - More tolerance to multipath distortions
- Reduced frame formats
  - Better use of the bandwidth
  - Less power consumption
- Low power modes, less communication with the AP
- 4x devices per AP

802.11ah use cases



802.11ah PHY

- 802.11ac clock is divided by 10
  - Channels of 2/4/8/16 MHz
  - OFDM, FFT with 64 points: 52 data subcarriers + 4 pilots
    - 10x symbol duration (40μs) -> 10x tolerance to multipath interference
    - 10x all times (SIFS, DIFS, …)
  - 1 MHz Channels
    - FFT with 32 points: 24 data subcarriers + 2 pilots
    - New Modulation Coding Schemes (MCS) for 1 MHz channels, 9x range



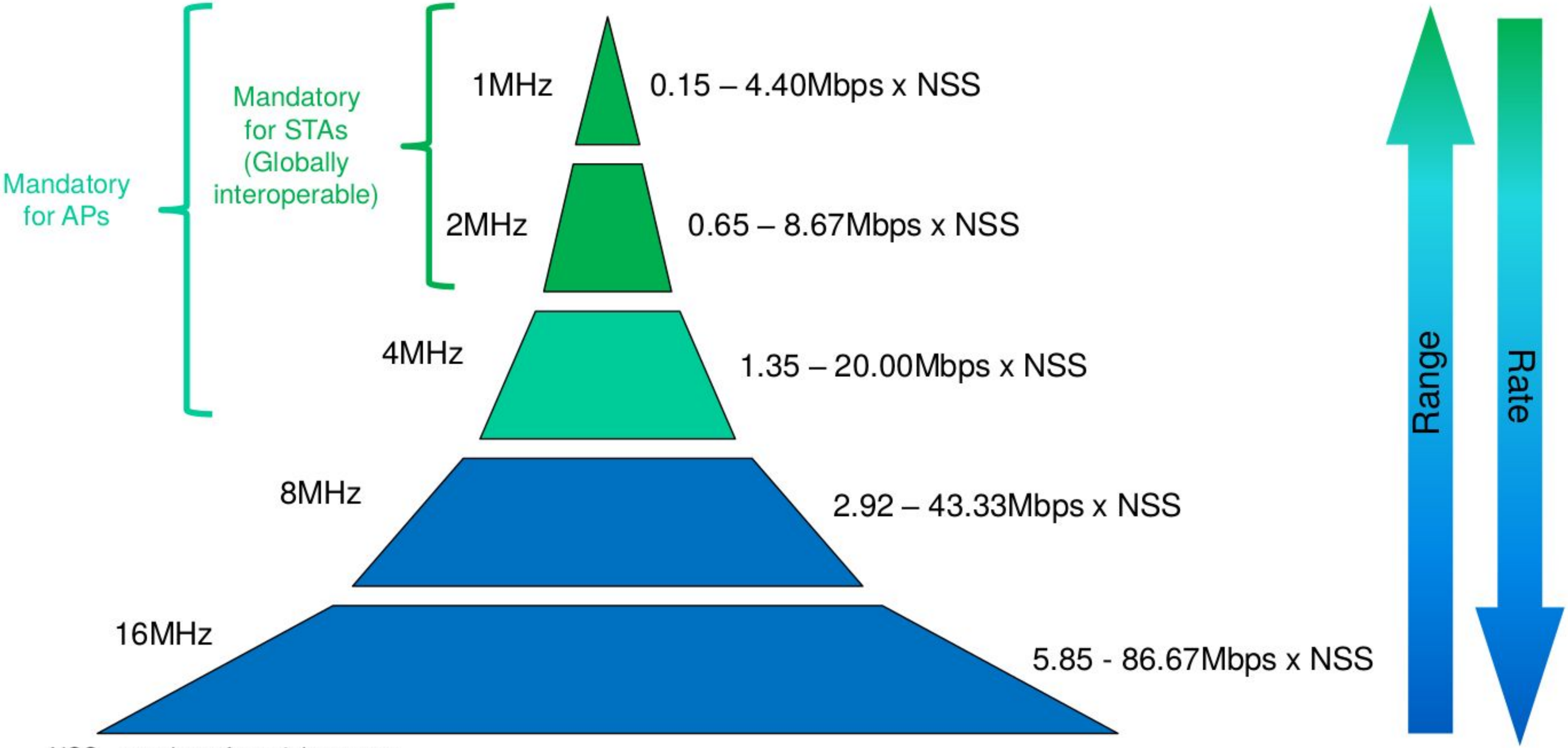
All stations must support 1MHz and 2MHz channels

STREAM

	Modul.	Code Rate	1MHz (Mbps)	2MHz (Mbps)	16MHz (Mbps)
MCS0	BPSK	1/2	0.30	0.65	6.5
MCS1	QPSK	1/2	0.60	1.3	13
MCS2	QPSK	3/4	0.90	1.95	19.5
MCS3	16QAM	1/2	1.2	2.6	26
MCS4	16QAM	3/4	1.8	3.9	39
MCS5	64QAM	2/3	2.4	5.2	52
MCS6	64QAM	3/4	2.7	5.85	58.5
MCS7	64QAM	5/6	3	6.5	65
MCS8	256QAM	3/4	3.6	7.8	78
MCS9	256QAM	5/6	4	N/A for 1 spat. stream	86.67
*MCS10	BPSK	1/2	0.15		

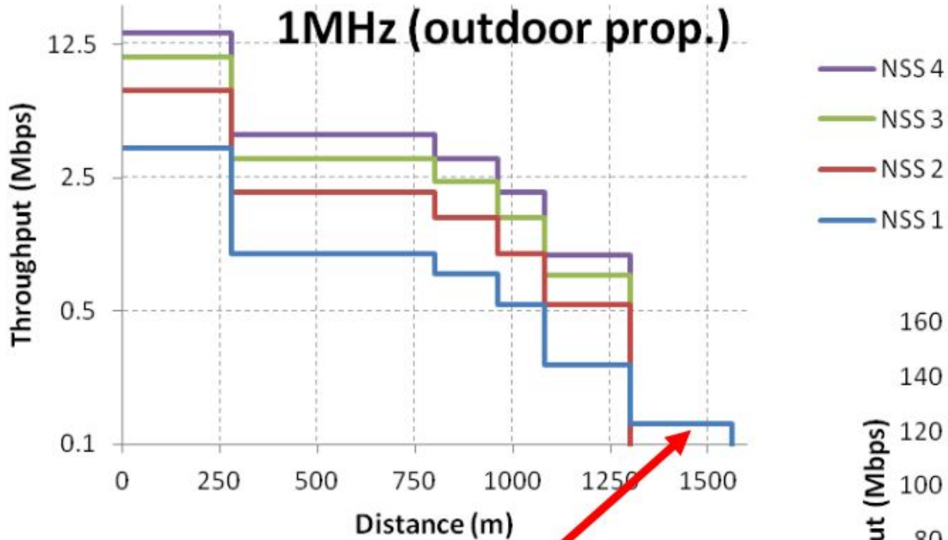
*includes 2x repetition mode to increase range

802.11ah PHY distance vs data rate

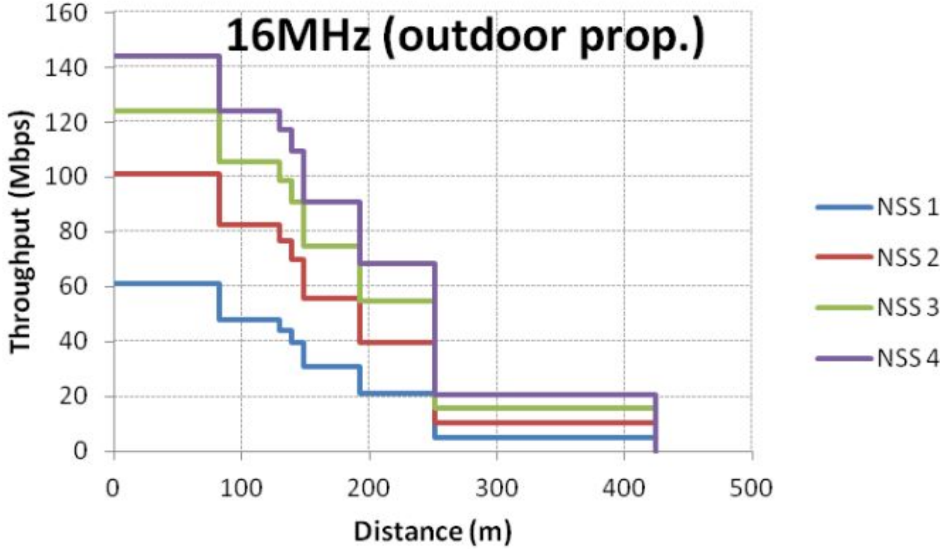


NSS = number of spatial streams

802.11ah PHY distance vs data rate



Additional step thanks to MCS10 (only available with 1MHz and NSS 1)



NSS = number of spatial streams

802.11ah MAC

- New frame format, with reduced size
  - Some fields are removed (Duration, QoS control, HT control, Sequence control)
  - Option to use only two addresses
    - Option to use 2B AID instead of 6B MAC addresses

Bytes	2	2	6	6	6	2	2	4
	FC	Duration /ID	A1	A2	A3	Sequence Control	QoS Control	HT Control

(a) Legacy 802.11 MAC header format.

Bytes	2	2	6	2	6
Downlink:	FC	A1 (AID)	A2 (BSSID)	Sequence Control	A3 (Optionally present)
Bytes	2	6	2	2	6
Uplink:	FC	A1 (BSSID/RA)	A2 (AID)	Sequence Control	A3 (Optionally present)

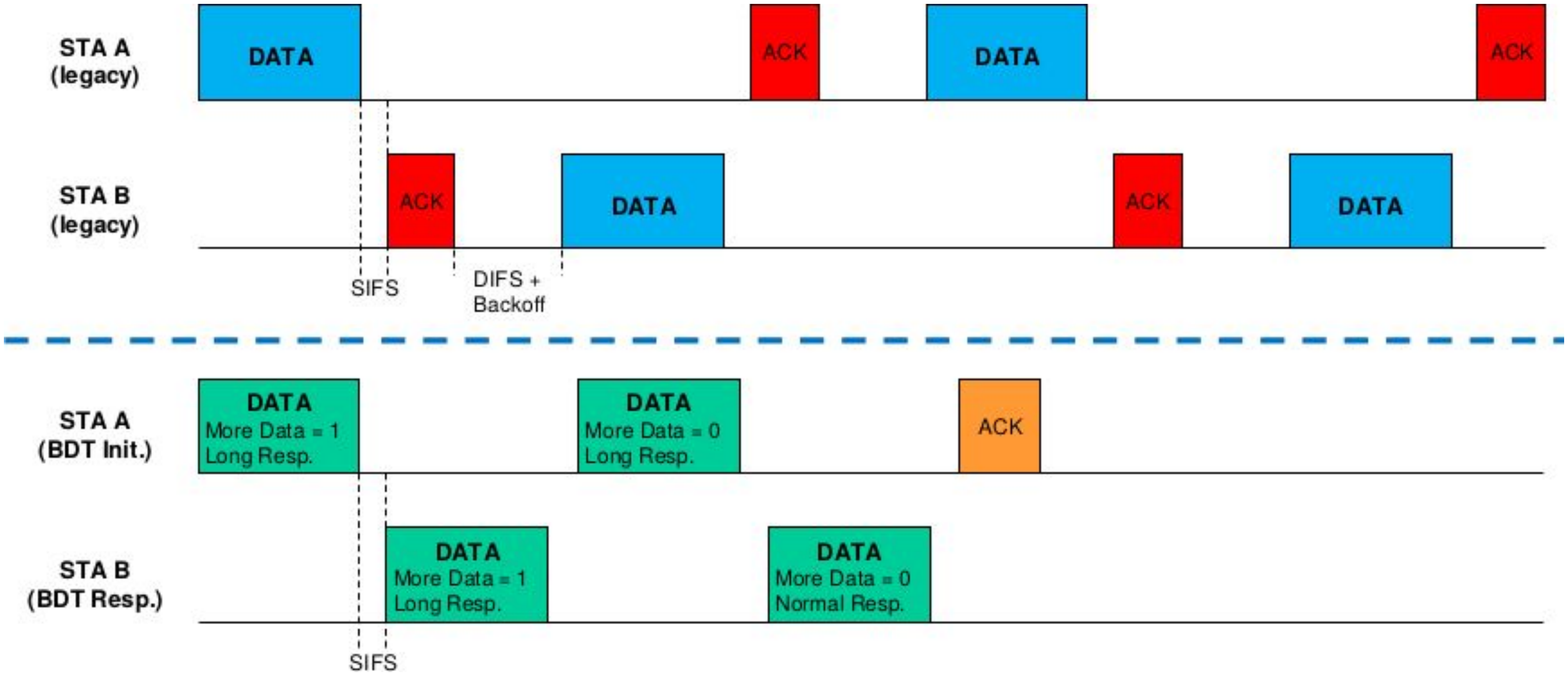
(b) 802.11ah short MAC header format.

802.11ah MAC

- Null Data Packet: only PHY bits
  - Only the PHY preamble is sent (no MAC header or payload)
  - The function is identified by the MCS, adding MCS codes not used for regular data frames (ACK, block ACK, …)
- Short Beacon Frames
  - Sent frequently at the lowest data rate
  - The complete beacons are sent with less frequency

802.11ah MAC

- Bi Directional Transmit (BDT): fast frame interchange
  - The sender sets the response indicator to *long response*
  - The receiver can then send data instead of an ACK after the SIFS, avoiding a contention process
    - This implies an ACK on the received data
  - Frames are sent until no more data needs to be sent during a transmission opportunity (TXOP).



802.11ah MAC

- 802.11 allows the stations to keep inactive for a maximum period indicated by a 16 bit number in 1024 ms units (> 18h)
- 802.11ah: the two most significant bits are used as a scaling factor $(1,10,10^3$ o $10^4) \rightarrow 10^4(2^{14} - 1) > 5$ years!!
- Each station negotiates a Target Wake Time (TWT) with the AP
  - Null Data Packet with information on the stored packets for the node
- Segmented Traffic Indication Map (TIM), organized in pages
  - Stations wake only to receive the beacon with their portion of the TIM

802.11 ah MAC

- Tree types of stations
  - High traffic stations (TIM stations):
    - Listen to the beacon frames with Traffic Indication Map (TIM) and transmit in their Restricted Access Window (RAW, a time slot negotiated with the AP for a group of stations)
    - The contention access (DCF) limited to the RAW, only other nodes in the same group can send in that RAW
    - TIM information segmented to reduce the size of the beacons
  - Low periodic traffic (Non-Tim stations)
    - Negotiate a RAW
    - They do not monitor beacons
  - Very low traffic (Unscheduled stations)
    - Contention when they need to send