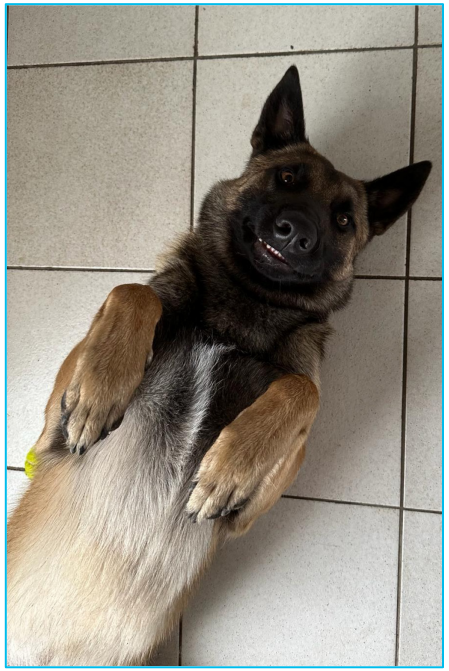
Roaming with Cisco Catalyst Wireless: how we do it

March 21st 2024

Hafida Barhoun – Technical Solutions Architect at Cisco
CCIE Routing &Switching #65298

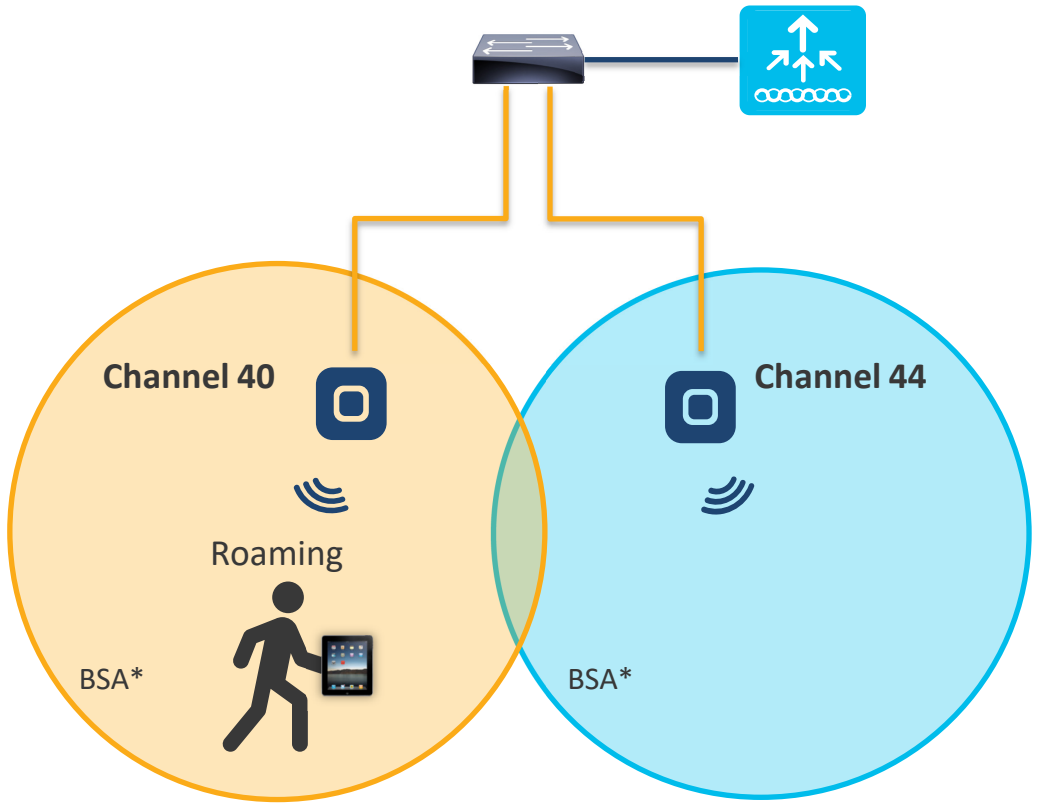
A little bit about myself

- Joined Cisco in 2018
- Technical solutions Architect focused on wireless since January 2021
- Cisco Live NoC Member (Barcelona 2020 & Amsterdam 2023)
- Freshly mom of two kids



Roaming Definition

- In a Wi-Fi network, roaming occurs when a station moves, or leaves the coverage area (BSA*) of the AP to which it was originally connected, and arrives at the BSA of another AP.
- It's the ability to maintain client's association seamlessly from one access point to another, securely and with as little latency as possible.

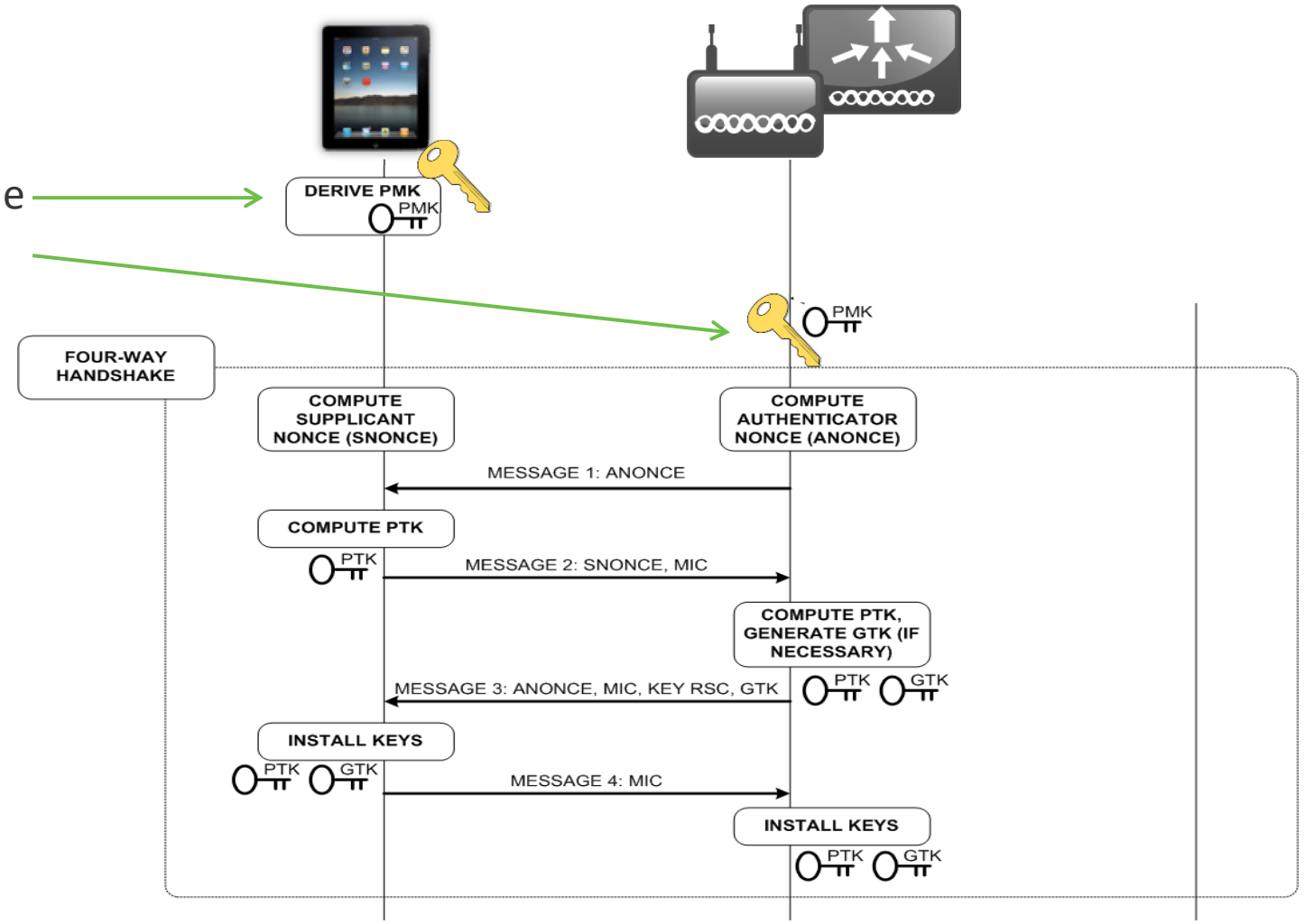


* Basic Service Area

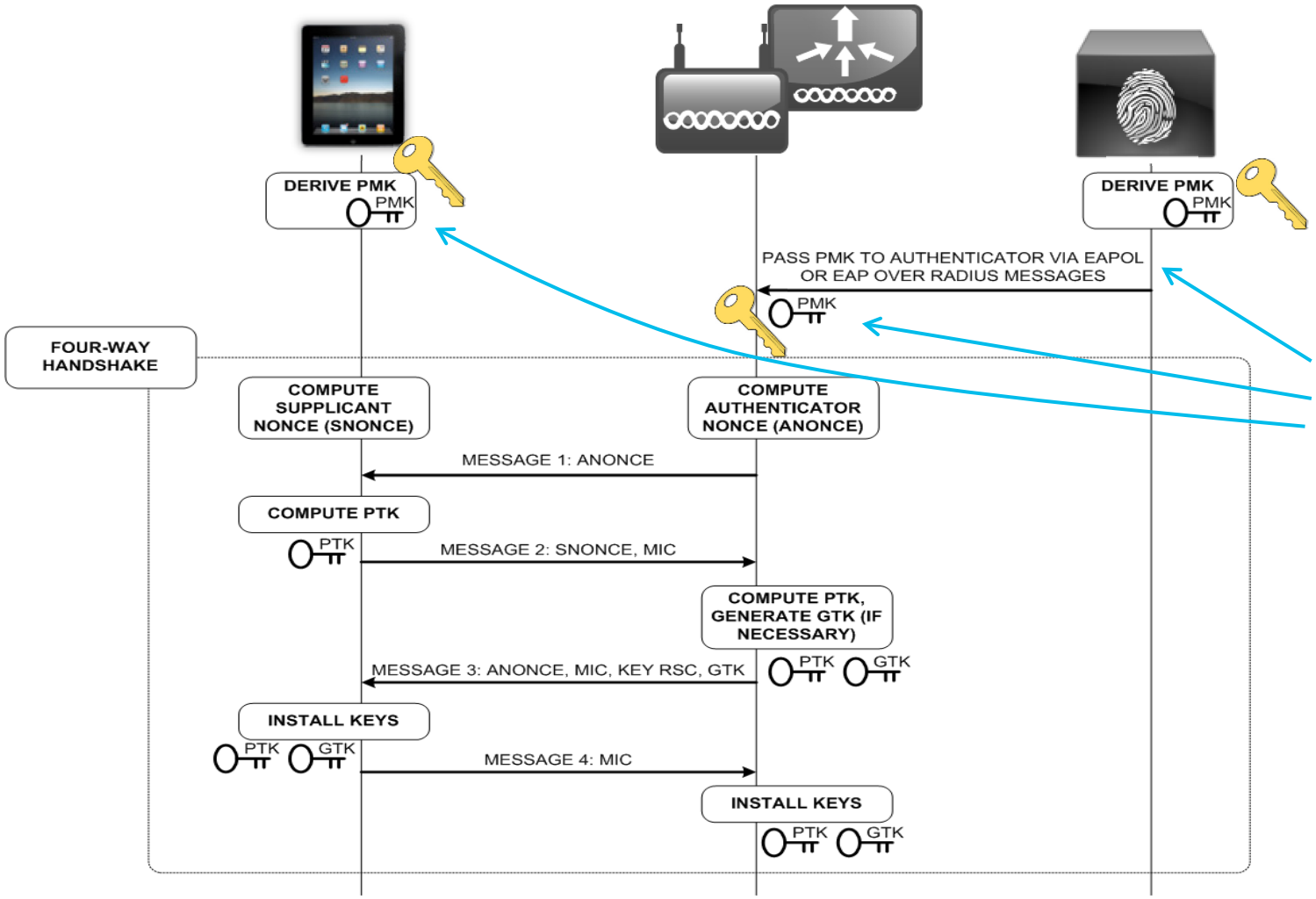
Roaming Techniques

PSK/static key management with WPA2

- Pairwise Master Key (PMK) derived from the Pre-Shared Key (PSK)

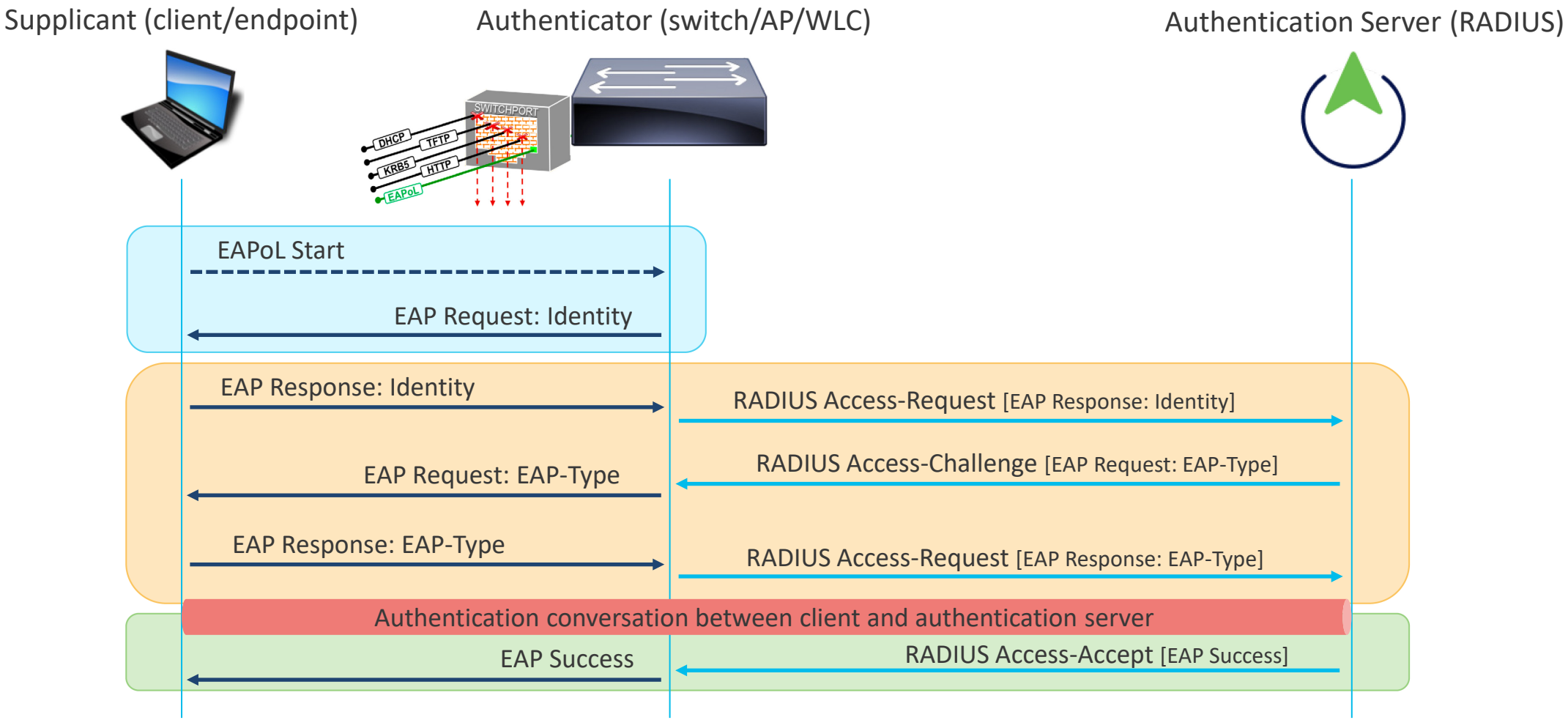


802.1X/dynamic of key management with WPA2



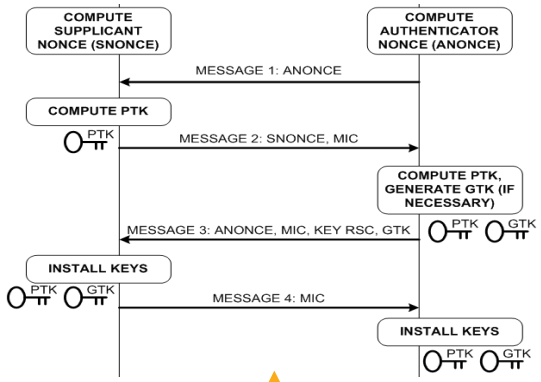
- PMK derived from 802.1X

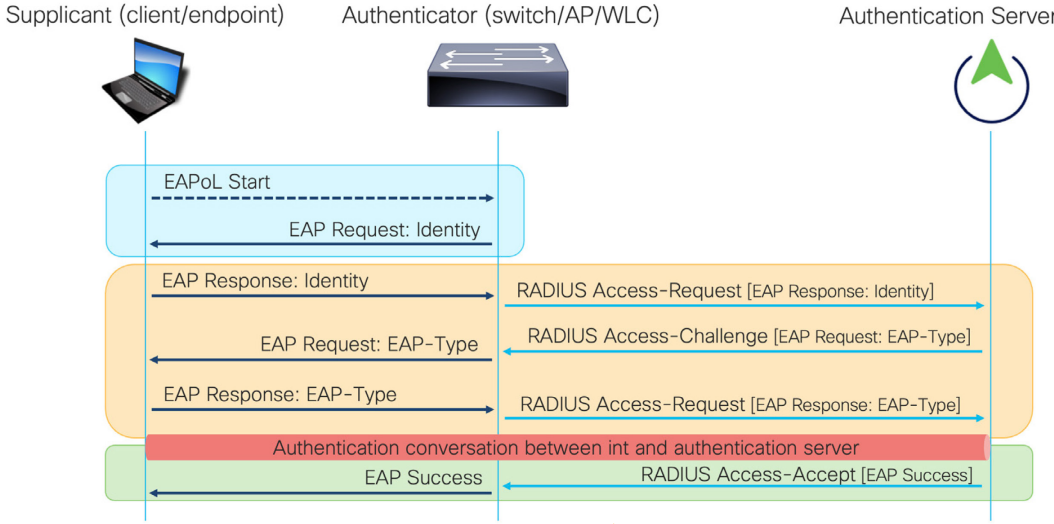
EAP/802.1X Call Flow

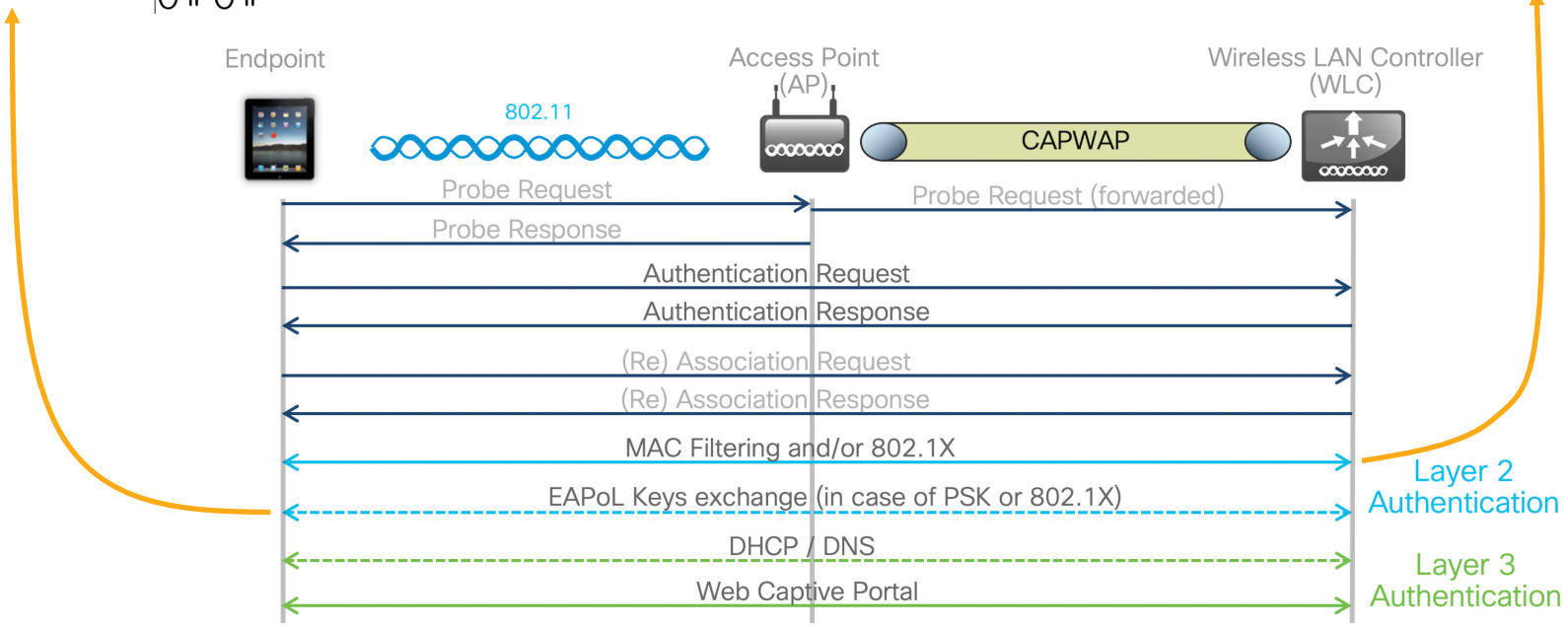


L2 and authentication keys reuse

The 4-way handshake doesn't take long and doesn't "break" L2 connectivity



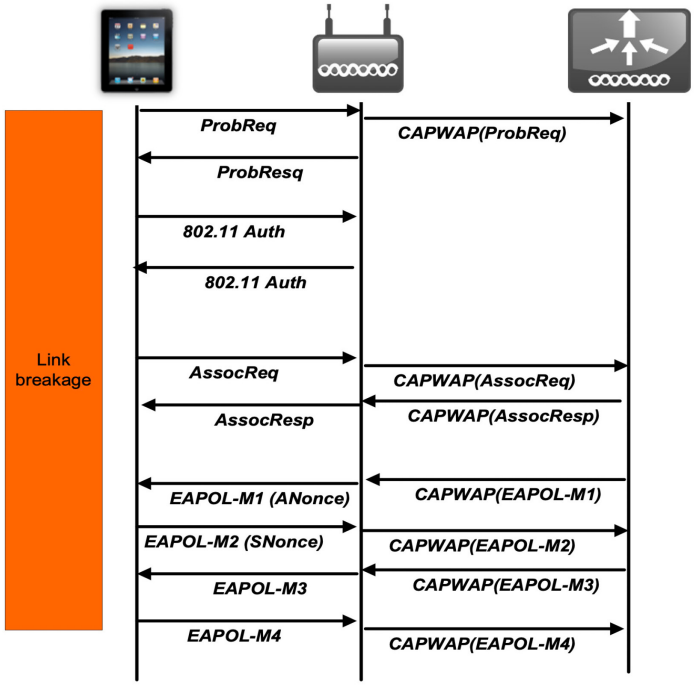




A full 802.1X (re)authentication takes too long, "breaks" L2 connectivity and even causes the client to go through DHCP again

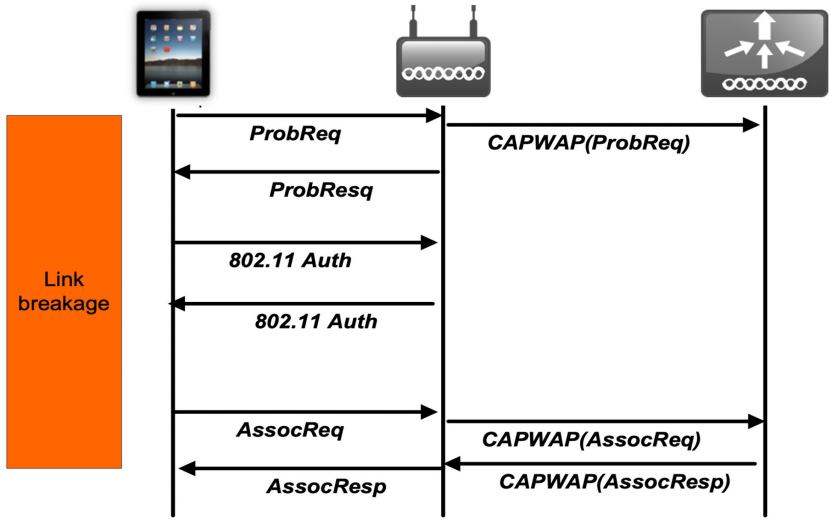
The different roaming techniques

Opportunistic Key Caching (OKC)



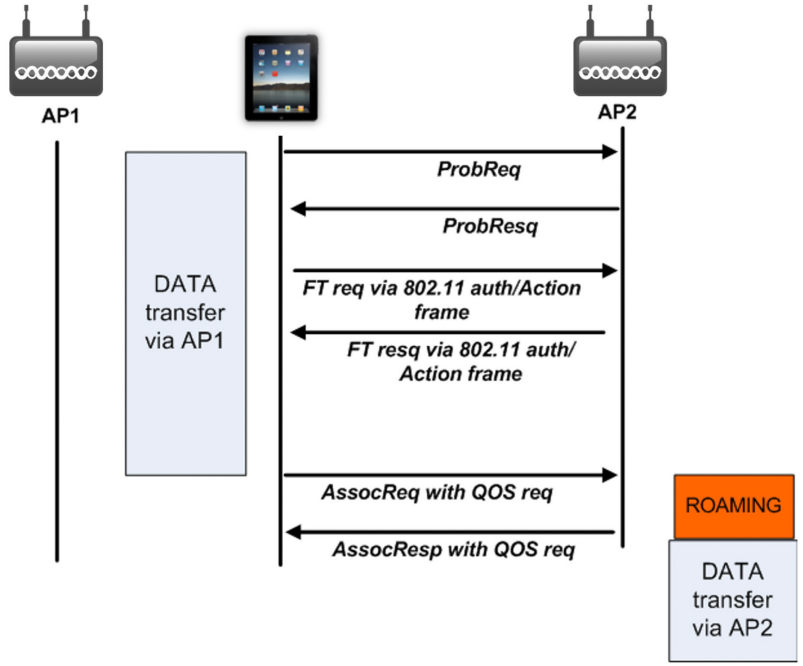
Not an official standard, but widely agreed between different vendors since many years.
~8-100 ms

Cisco Centralized Key Management (CCKM)



A Cisco proprietary technique, open to 3rd party endpoints too (to be checked).
~4-50 ms

802.11r / Fast Transition (FT)

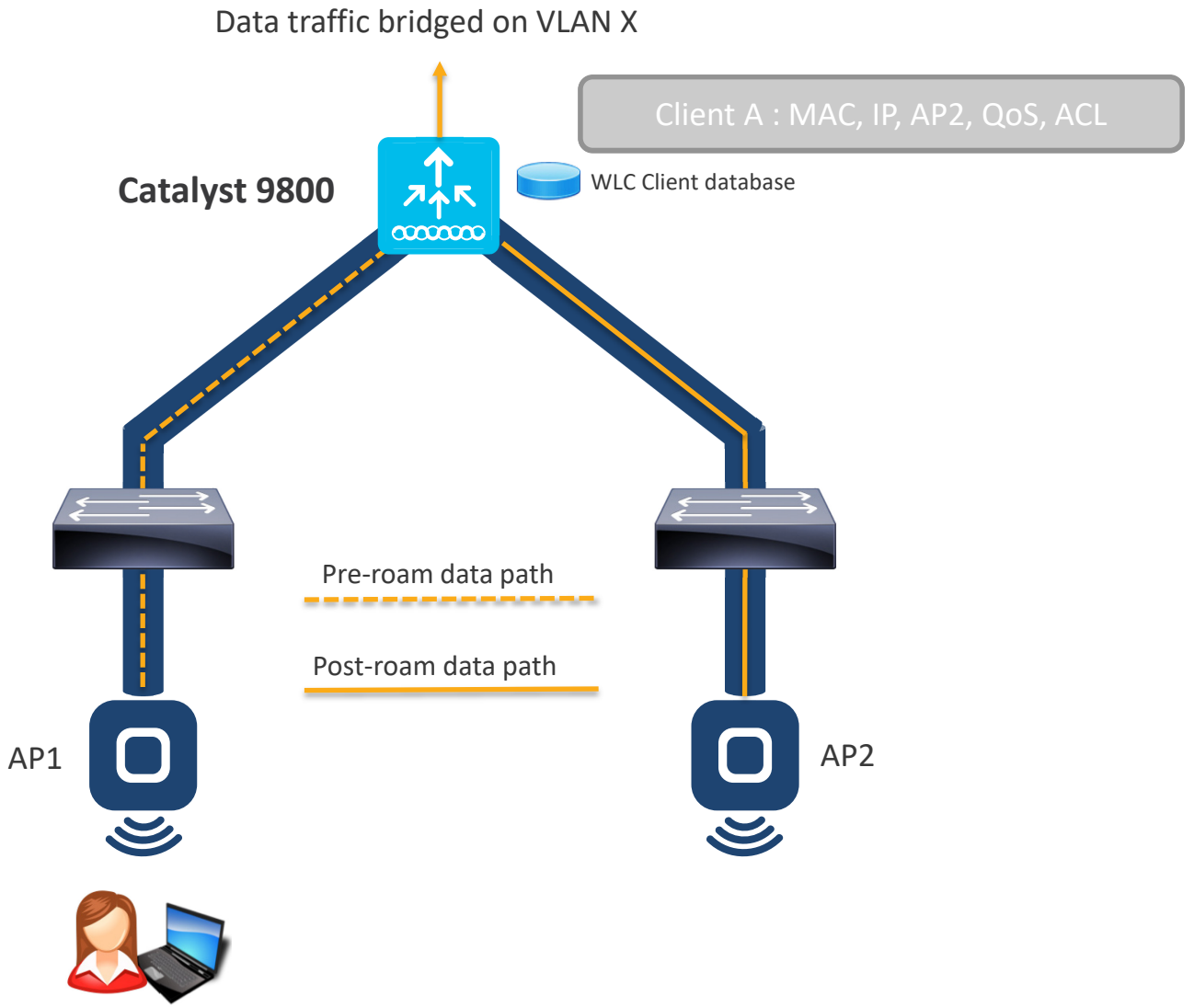


The real standard, today widely supported by the vast majority of endpoints.
~< 10 ms

https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/116493-technote-technology-00.html

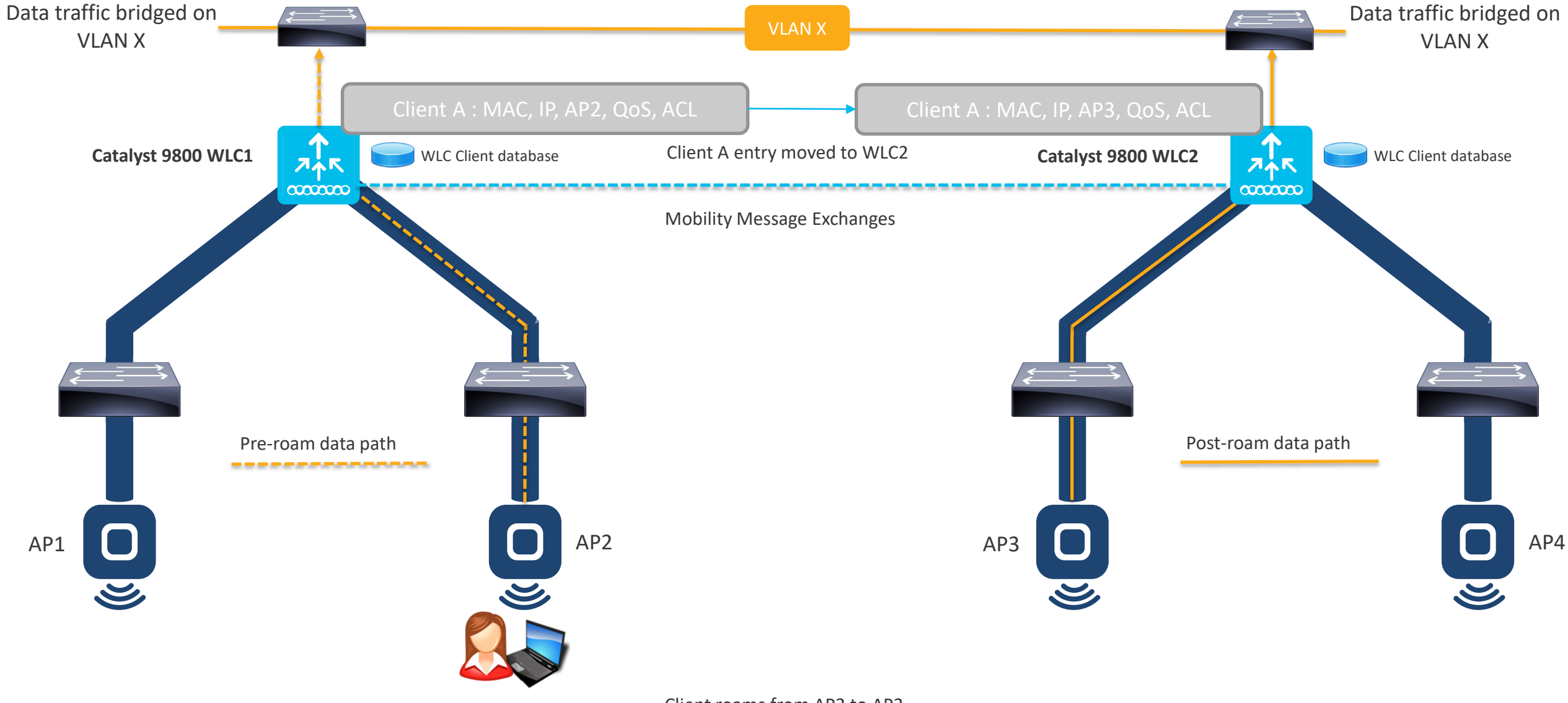
Different types of roaming

Intra-controller roaming



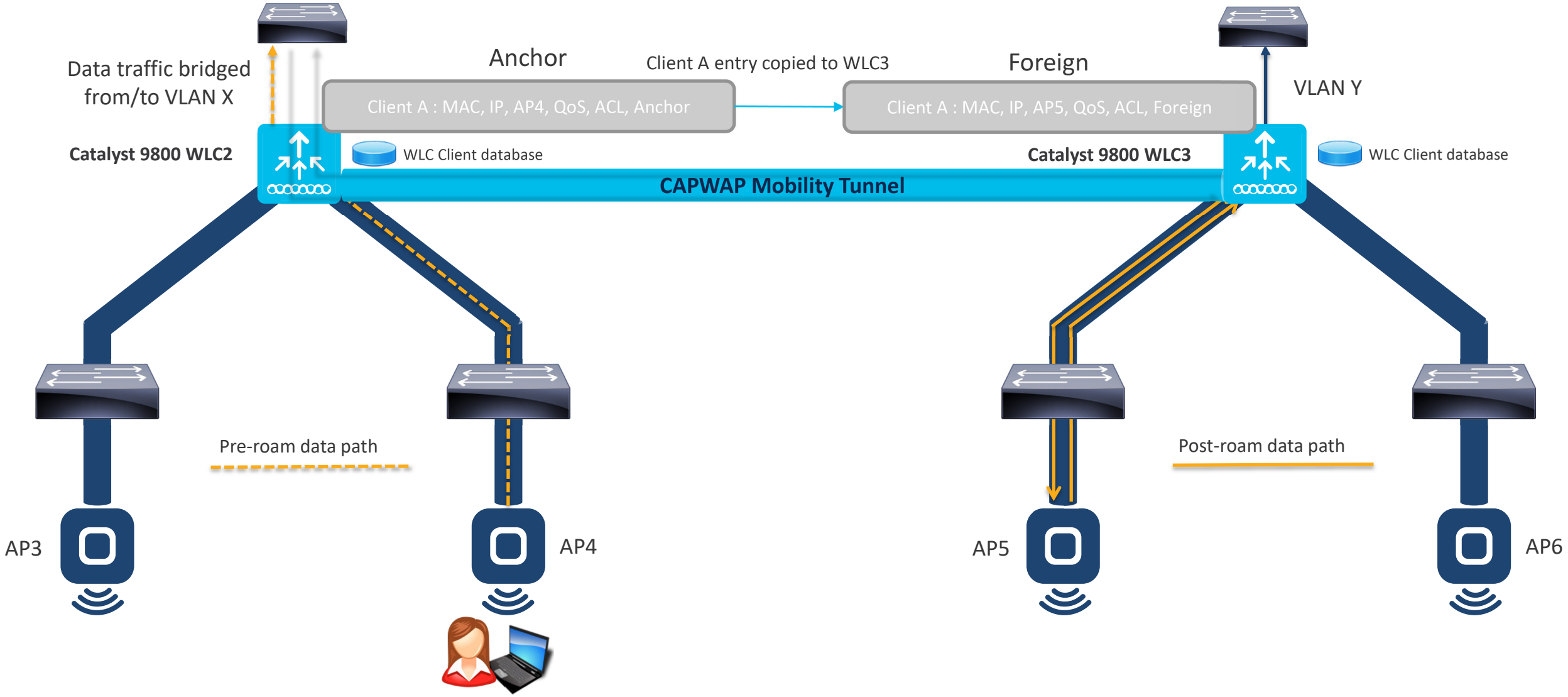
Client roams from AP1 to AP2

Inter-controller roaming (L2)



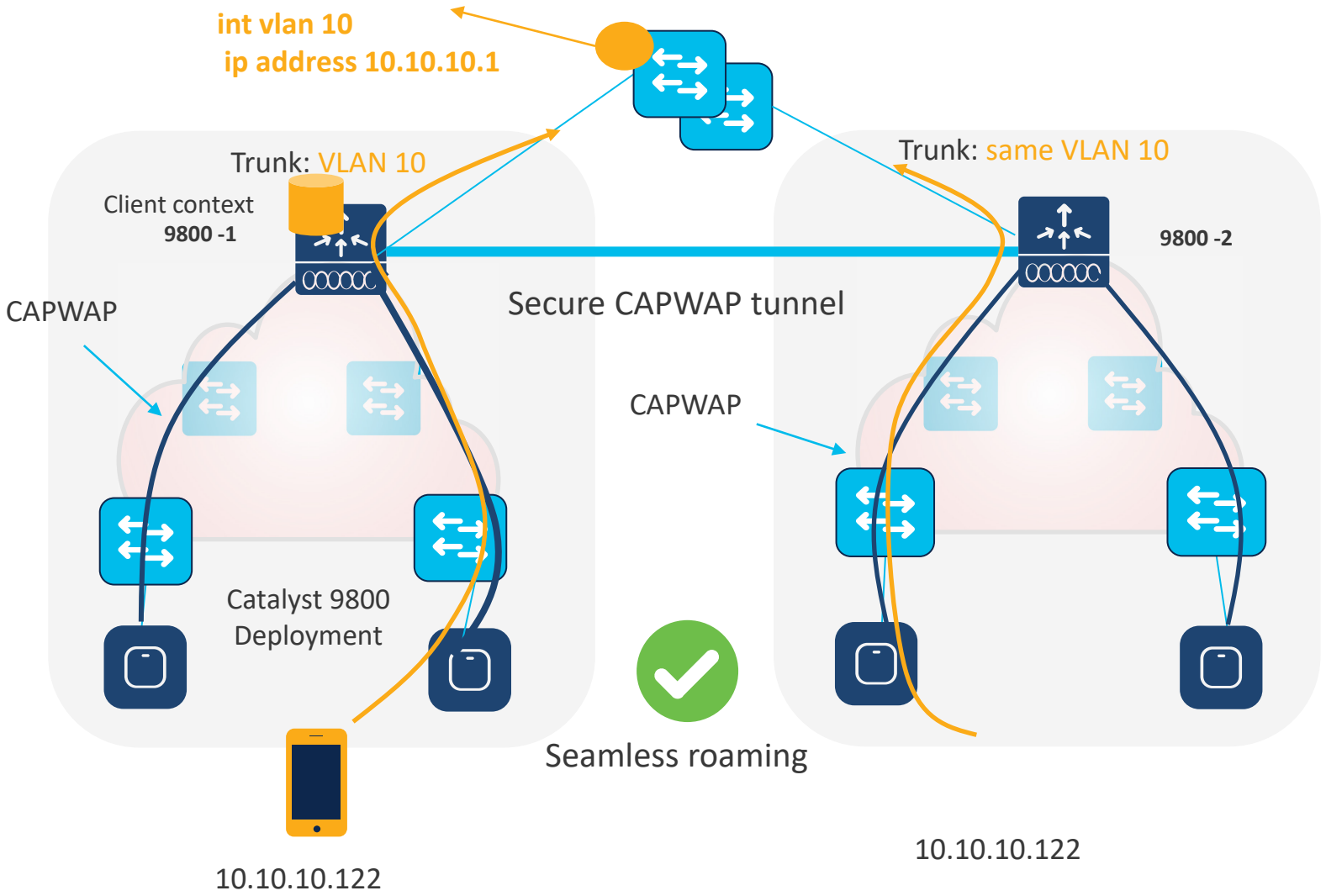
Client roams from AP2 to AP3

Inter-controller roaming (L3)



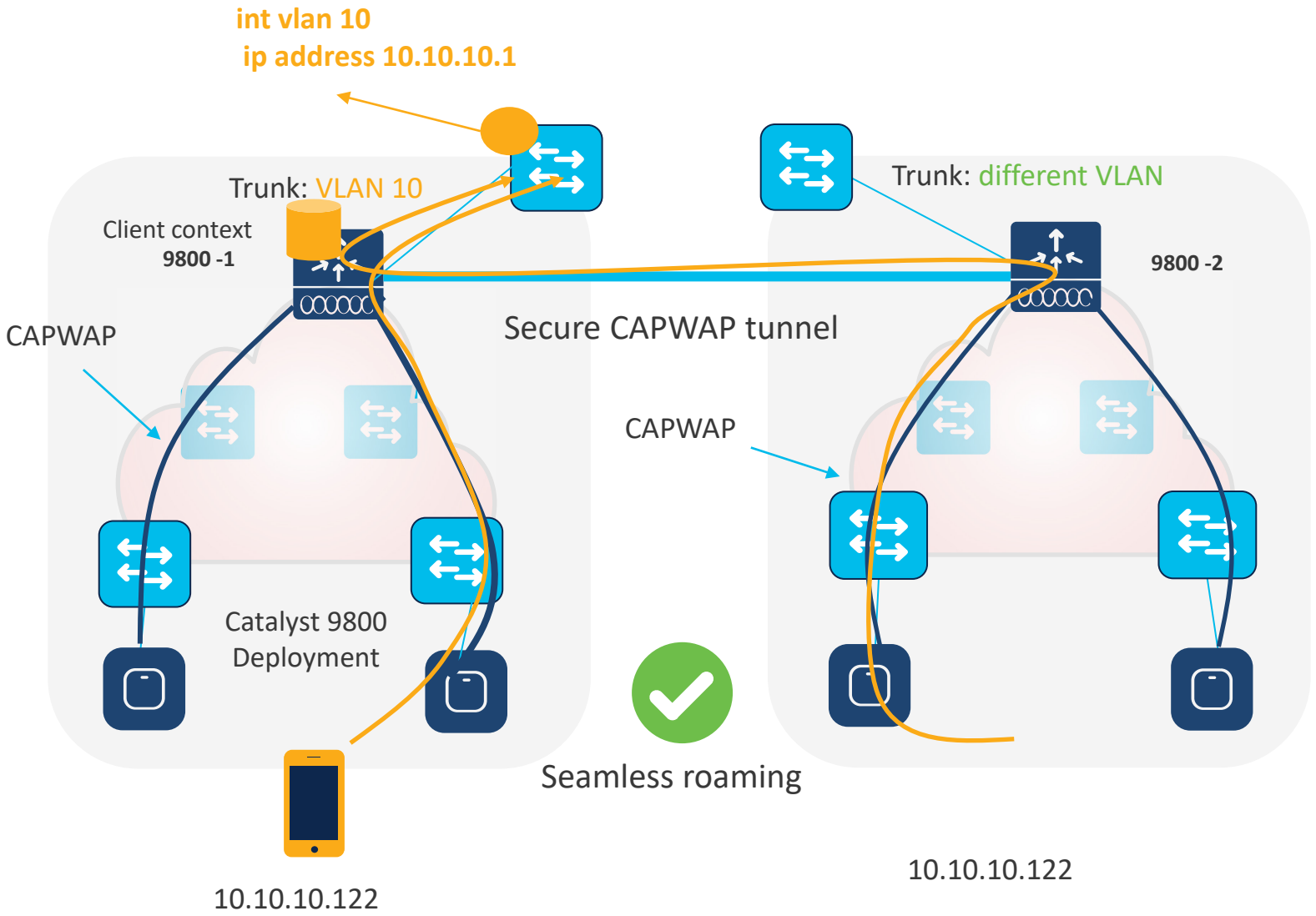
Client roams from AP4 to AP5

L2 vs. L3 seamless roaming – what's different?



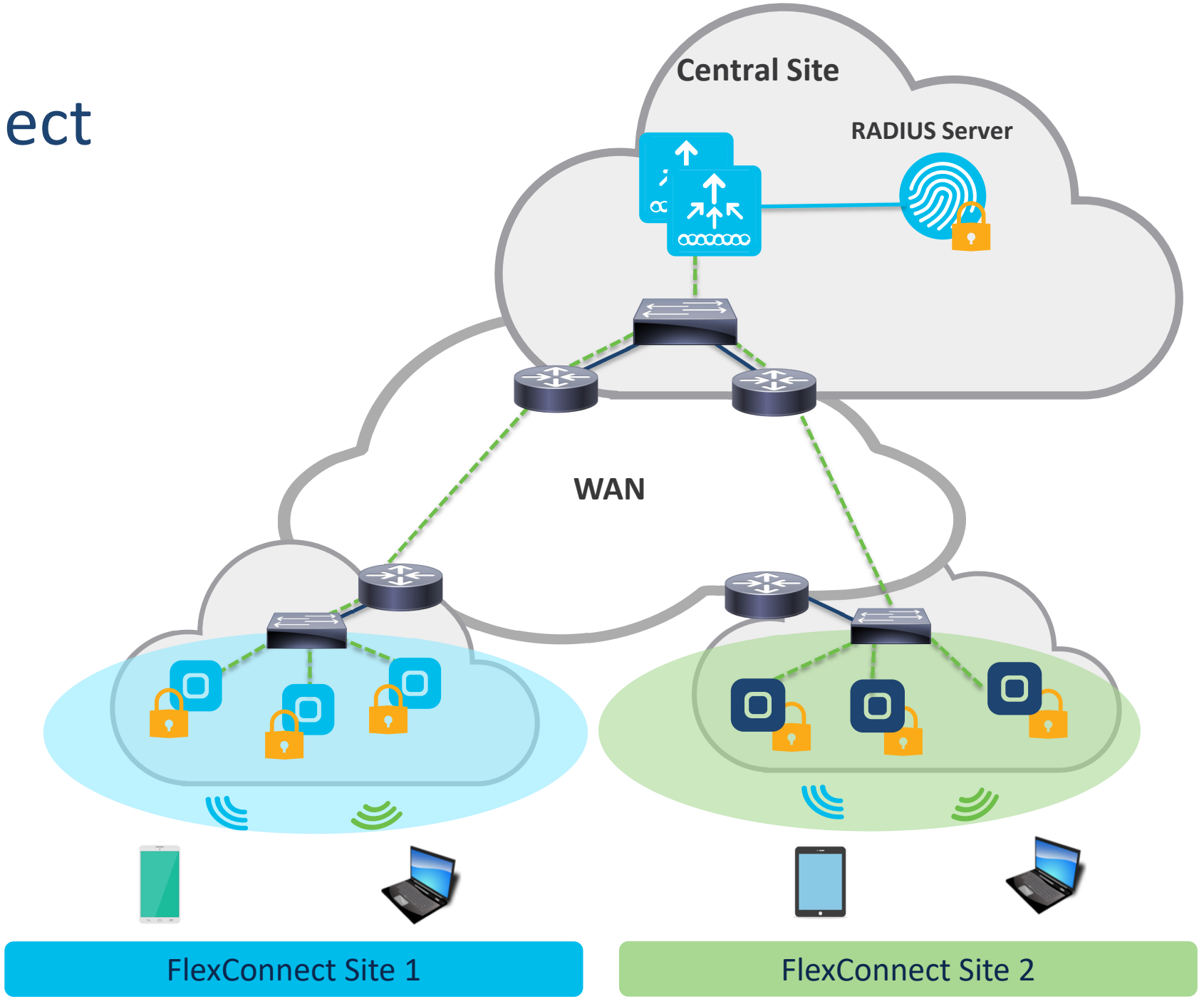
- **Seamless roaming** needs the two controllers in the **same Mobility Group**
- What differentiates **L2 vs. L3 roaming**?
- In C9800, it's only **the vlan number (ID),** not the vlan name AND not the subnet
- **Same VLAN ID > L2 roaming**

L2 vs. L3 seamless roaming – what's different?



- **Seamless roaming** needs the two controllers in the **same Mobility Group**
- What differentiates **L2 vs. L3 roaming**?
- In C9800, its only the vlan number
- **Same VLAN ID > L2 roaming**
- **Different VLAN ID > L3 roaming**
- This is independent of SVI being present and the subnet specified
- Why? C9800 doesn't mandate an IP address for the client VLAN (like dynamic interface for AireOS)
- Note: if you configure the same VLAN ID on both c9800 but then map it to a different subnet, you will break roaming

FlexConnect



Client Roaming & Best practices

Roaming is the endpoint decision

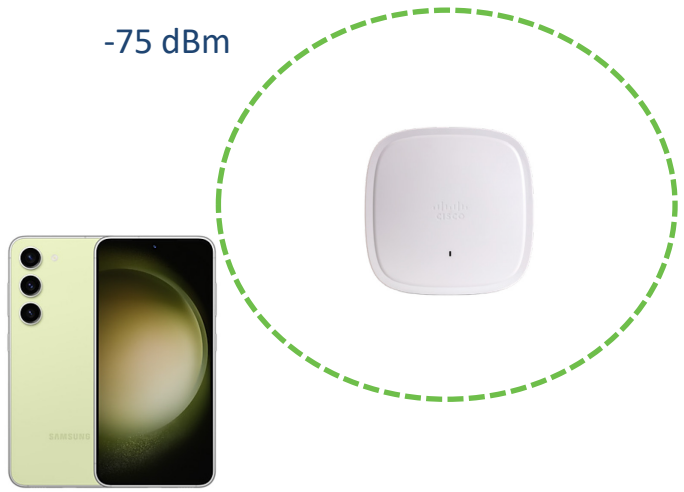
- Phones do not scan ‘because you move’ (no accelerometer trigger)
- Common client roam triggers:
  - Low RSSI
  - Max retry count is exceeded
  - Low SNR
  - Proprietary algorithm

Apple (IOS)

- If current AP signal is below -70 dBm OR beacon loss > 2 seconds:
  - Scan, join AP with 8 dB better than current AP
  - if client is not sending data, only join if new AP is 12 dB better than current AP
  - If 2 APs or more are better than -65 dBm, prefer the 5GHz AP

https://support.apple.com/en-us/HT203068

Samsung (Android)



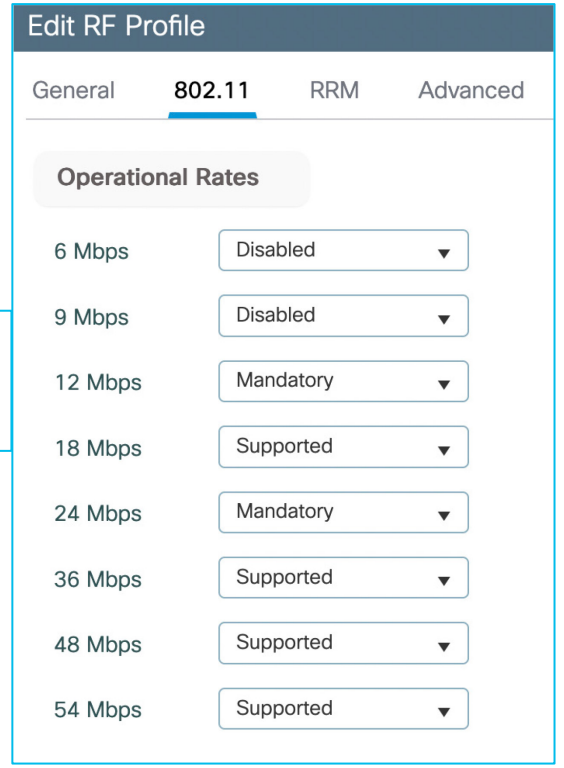
Android behavior depends on vendor, above is Samsung S8 and later

- If current AP signal is below -75 dBm OR if beacon loss > 2 seconds, OR if (RSSI lower than -65 dBm and CU > 70%) :
  - Scan, join AP with signal 10 dBm better than current AP
  - Samsung uses the ‘short scan’ (remembered channels first)

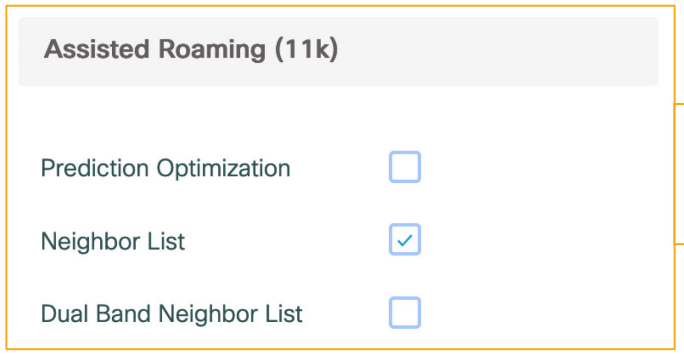
https://docs.samsungknox.com/admin/knox-platform-for-enterprise/kbas/kba-115013403768.htm

Helping the endpoint with coverage

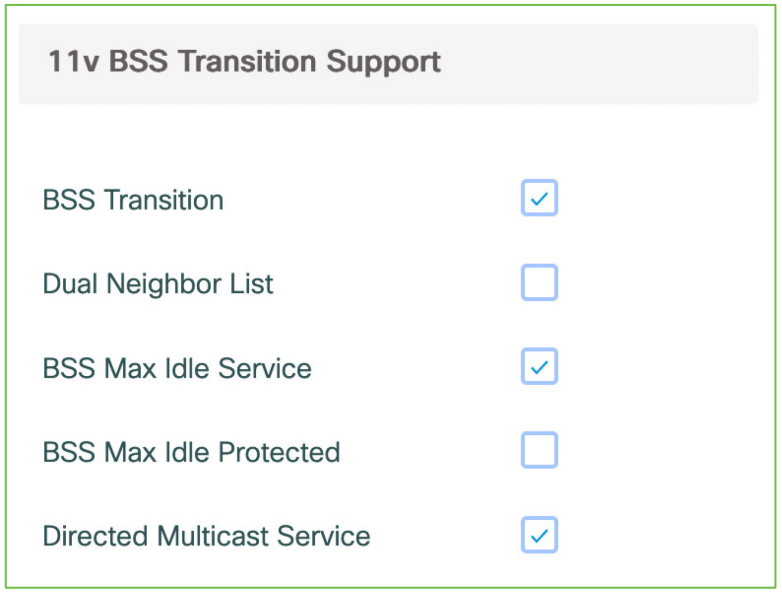
Mandatory data rates “encourage” the endpoint looking for APs



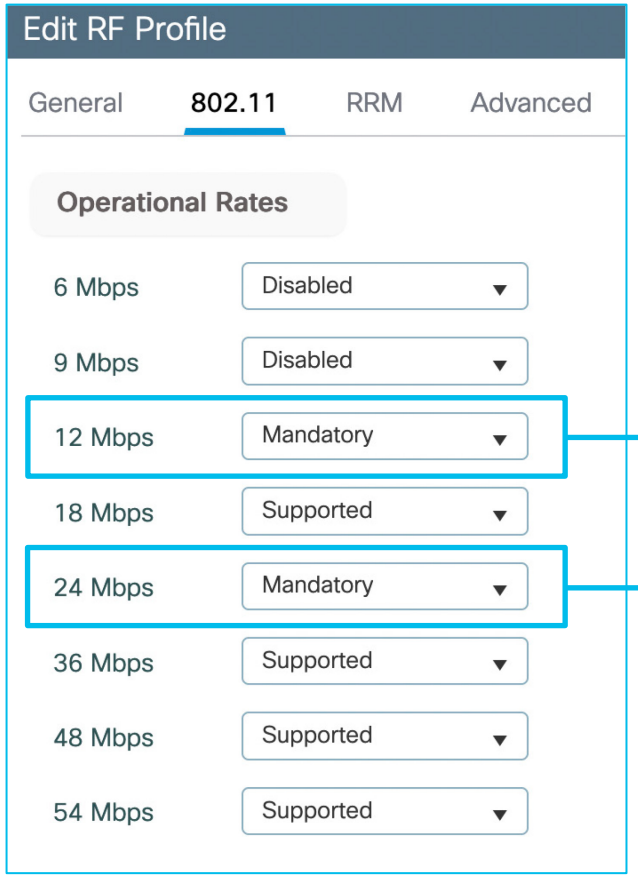
802.11k helps the endpoint build a list of surrounding APs



802.11v helps the endpoint choose the next “candidate” AP



Data rates



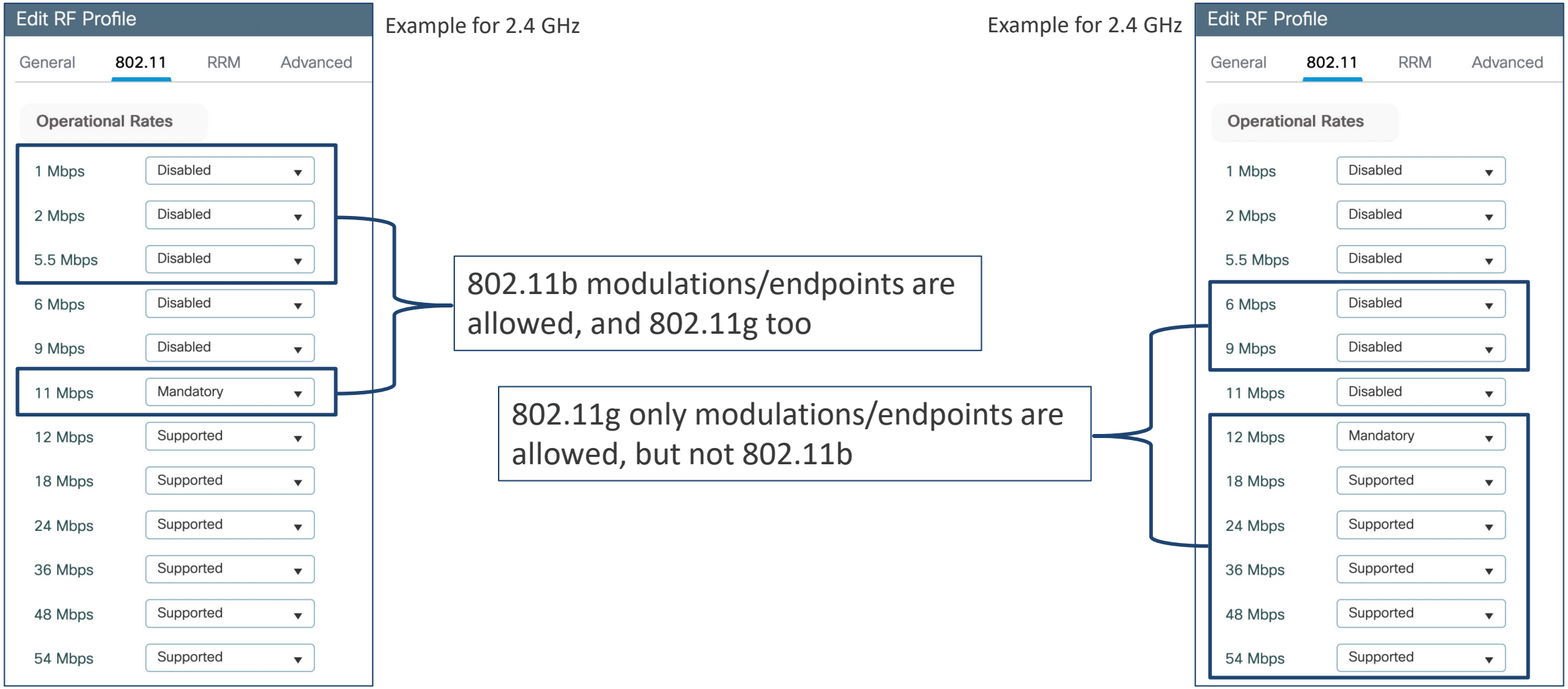
Example for 5 GHz

Lowest mandatory: the data rate at which the endpoint must be able to decode management frames to associate.
If we don't support this, we cannot associate.

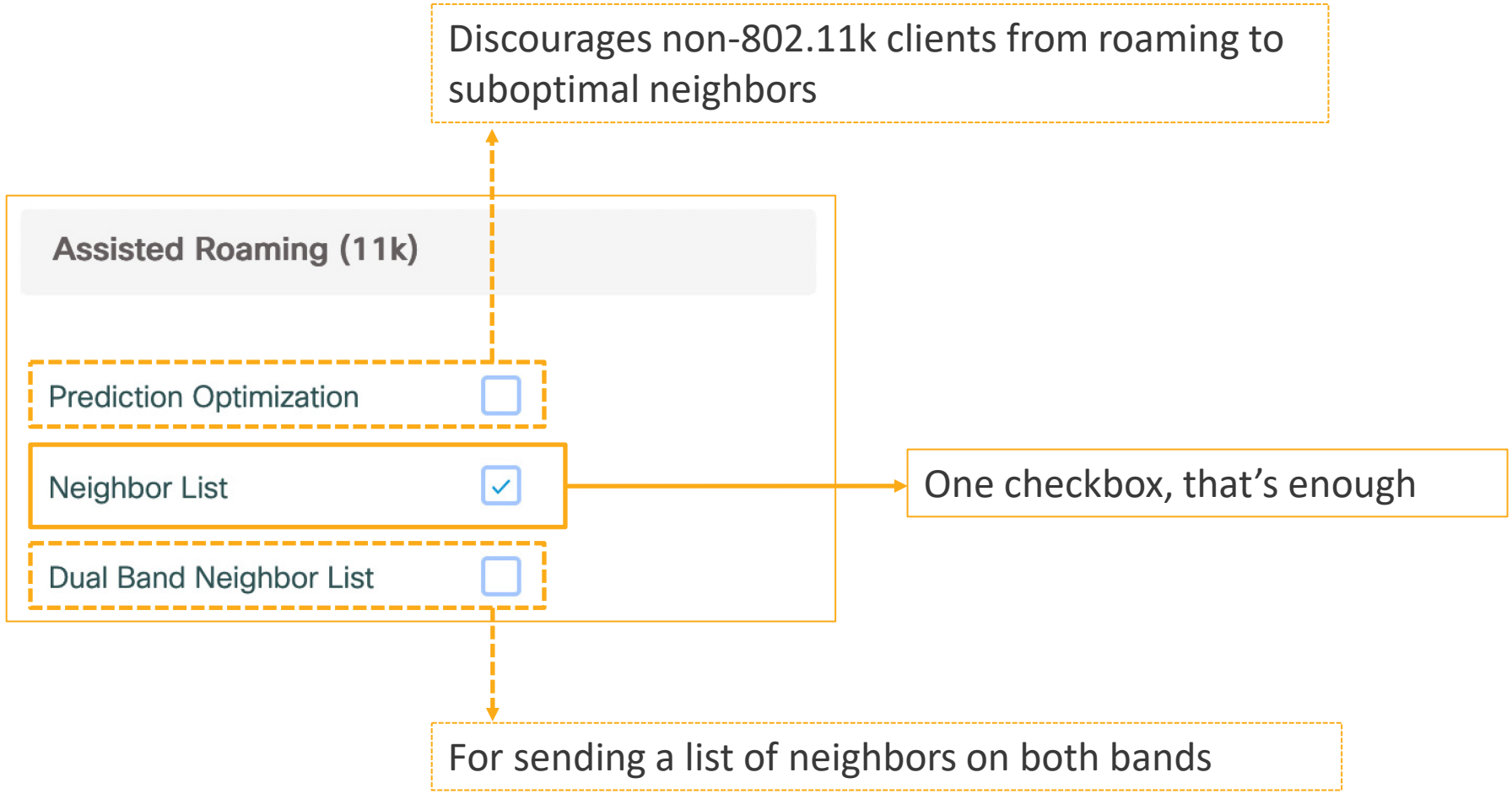
Highest mandatory: the data rate at which multicast frames will be sent.

Higher data rate ➔ Better modulation ➔ Better signal ➔ Closer to the AP ➔ Smaller cell size

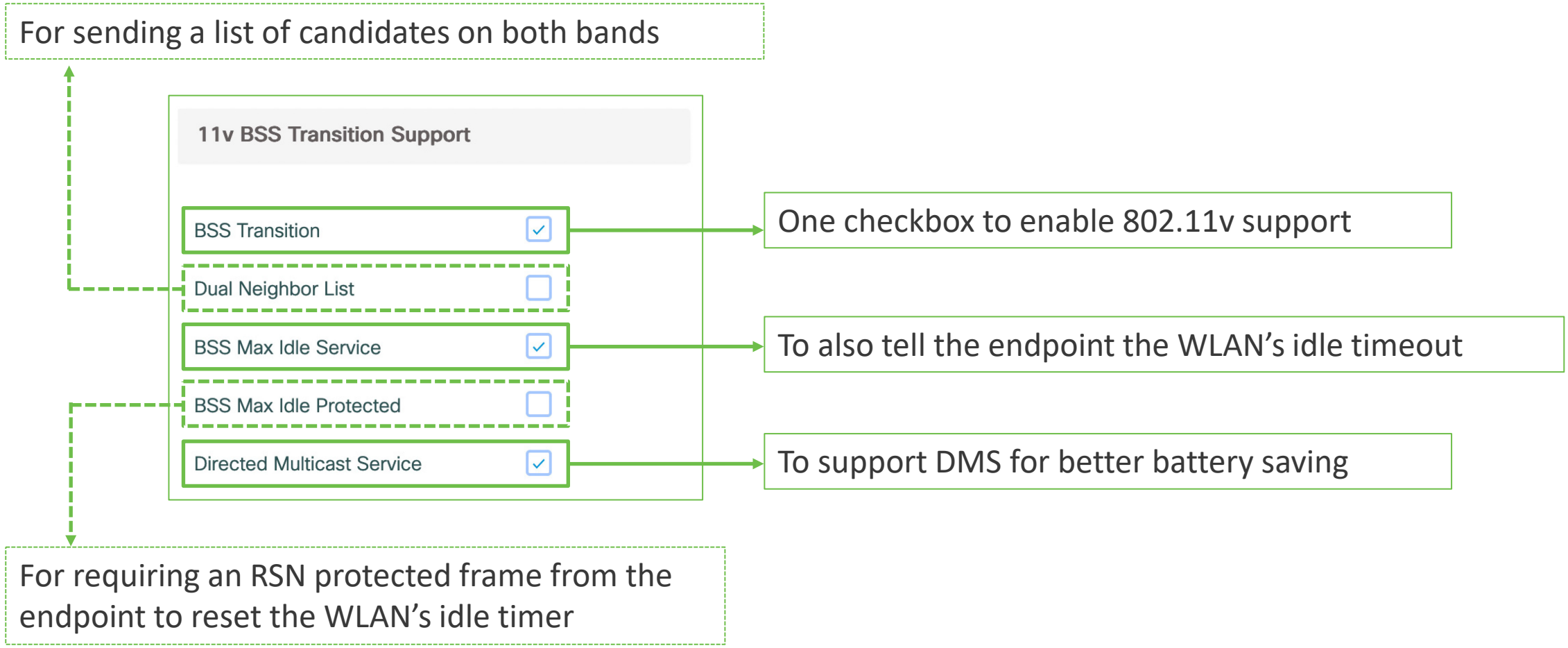
Data rates can exclude modulations/endpoints



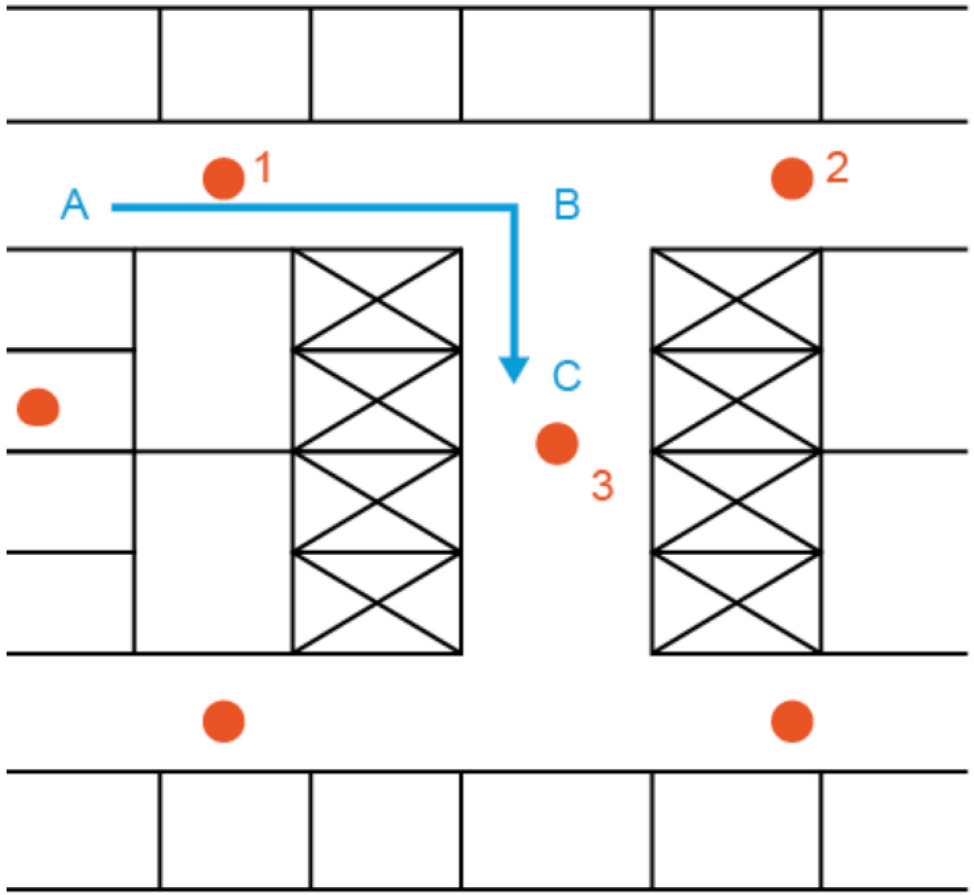
802.11k


Discourages non-802.11k clients from roaming to suboptimal neighbors
Assisted Roaming (11k)
Prediction Optimization
Neighbor List
Dual Band Neighbor List
One checkbox, that’s enough
For sending a list of neighbors on both bands

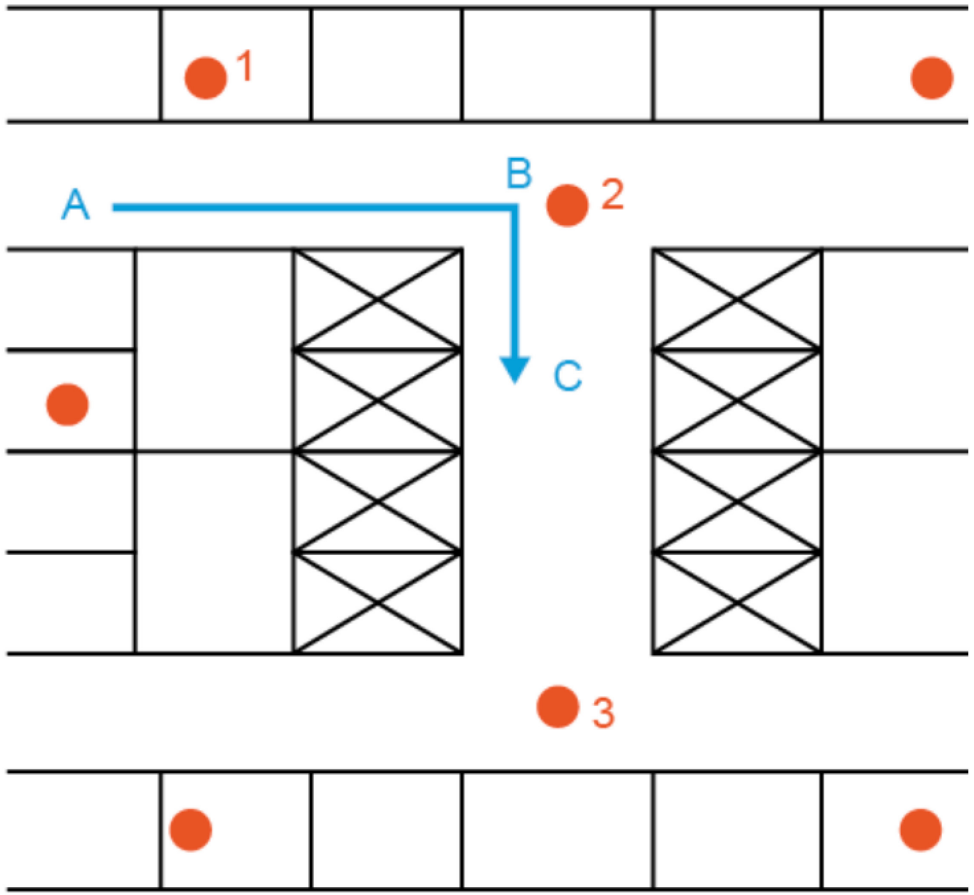
802.11v


For sending a list of candidates on both bands
11v BSS Transition Support
BSS Transition
Dual Neighbor List
BSS Max Idle Service
BSS Max Idle Protected
Directed Multicast Service
One checkbox to enable 802.11v support
To also tell the endpoint the WLAN's idle timeout
To support DMS for better battery saving
For requiring an RSN protected frame from the endpoint to reset the WLAN's idle timer

Designing the roaming path



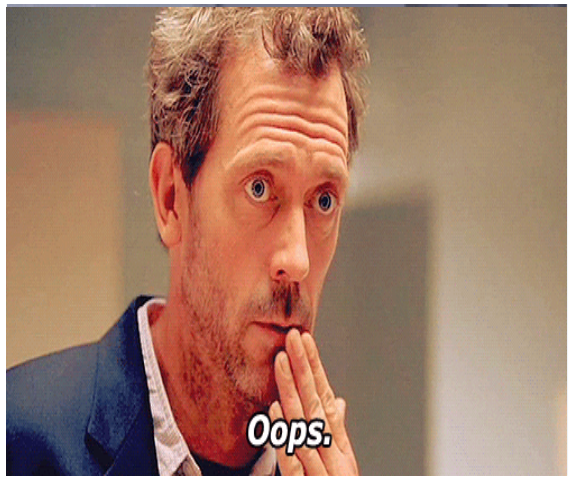
Example 1

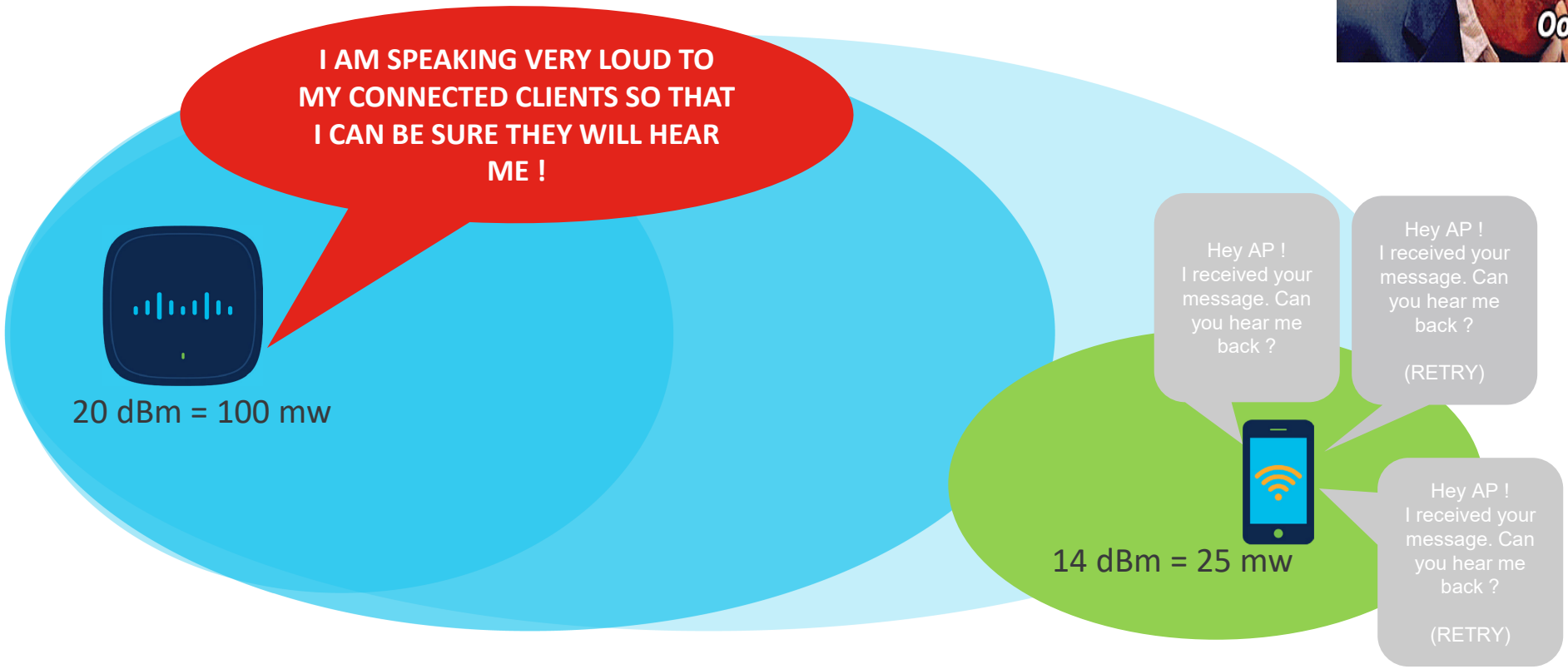


Example 2

AP Power Level

- Do not use maximum power level
- The AP power level should match the client power level.
- Use TPC





Optimized roaming and RX-SOP

Optimized roaming

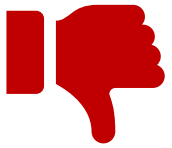
- Addresses the sticky client challenge
- Proactively disconnect clients
- Disassociates client when the RSSI is lower than the set threshold

RX-SOP

- Determine if the AP should demodulate the signal or not
- Set a value below which an AP will ignore the client
- Fine tuning

Do…and Don’t !

- Keep intra-controller roaming as possible
- Use video call, facetime, ping to test roaming
- Activate 11r/k/v
- Influence the roaming with data rates
- Design an optimized roaming path
- Design your network with sufficient number of AP



- Don’t use maximum power level
- Don’t test roaming with web browsing
- Be careful with what you activate
- Do not put all your controller in a same mobility group, because it is so simple ☺
- Don’t forget that site survey is your friend (Before & After)


CISCO