

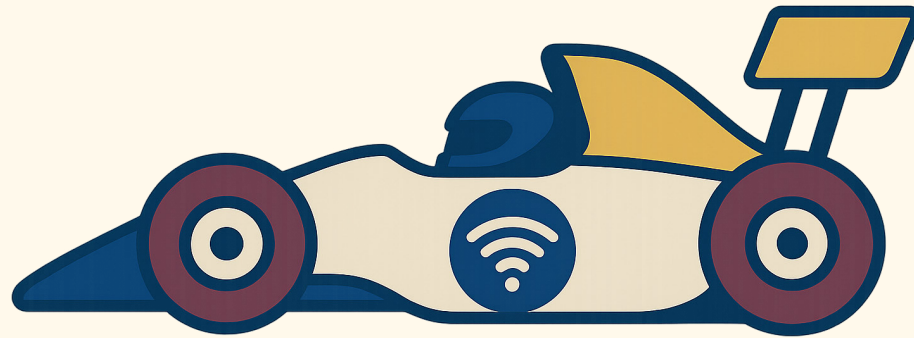
Differentiate These Roaming Technologies: Part 3

802.11r

"802.11rrrrrrr
I'm a wireless
pirate!"



802.11r is BSS Fast Transition



- It shortens the time it takes for when re-association could take 5s+.
- 11r does this by separating the PMK into levels.
- 11r is critical for environments that both value security and voice services.

What types of 802.11r are there?

- Adaptive mode: Cisco and Apple only. Allows iOS devices to use 11r when not enabled in network.

- Otherwise 802.11r has two submodes:

 - Over the Air - Auth. request sent to APs OTA

 - Over the DS - Auth. request sent to APs via LAN

When should I use 802.11r?



- Use it for "secure" SSID types
- For example: WPA3-Personal or WPA2/3-Enterprise
- Do not use it for open or WPA2-Personal SSIDs.
- WPA2-Personal specifically vulnerable to the KRACK attack.

How do I know if my SSID uses 802.11r ?

Check for "Mobility Domain" Tag in Beacons

```

  Tag: Mobility Domain
    Tag Number: Mobility Domain (54)
    Tag length: 3
    Mobility Domain Identifier: 0x667a
  FT Capability and Policy: 0x00
    .... 0 = Fast BSS Transition over DS: 0x0
    .... 0. = Resource Request Protocol Capability: 0x0
    0000 00.. = Reserved: 0x00

```

Filter for Mobility Domain tag in Beacons :
(wlan.tag.number == 54) && (wlan.fc.subtype == 8)

How does 802.11r work?



- The PMK is split into two levels:
 - R0 - Same for every AP in ESS
 - R1 - Unique for each AP
- Key Holder values for these are sent in the Fast BSS Transition tag in association responses
- PMKR1 used to calculate PTK for each client connection

Bonus

The examples shown are for checking AP support of 802.11r.

Clients may not consistently advertise the MD tag.

It's best to check with the manufacturer.

Recap

802.11r improves roaming times for secure SSIDs.

It accomplishes this with separate PMK levels.

APs advertise support with the Mobility Domain Tag.

Sources/Credits

-Understand 802.11r/11k/11v Fast Roams on
9800 WLCs (Cisco Technotes Document
ID:221671)

-802.11r BSS Fast Transition

<https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/technotes/80211r-ft/b-80211r-dg.html>

-iOS Compatibility with Cisco QoS Fastlane &
Adaptive 802.11r

<https://support.apple.com/en-us/101917>

-IEEE 802.11r-2008

<https://ieeexplore.ieee.org/document/4573292>