WORKSHOP GARR 2023

NET MAKERS

# Il Roaming e la scoperta delle reti WIFI

Jacopo Saladini

NAeS Consulting SRL

# Chi sono :

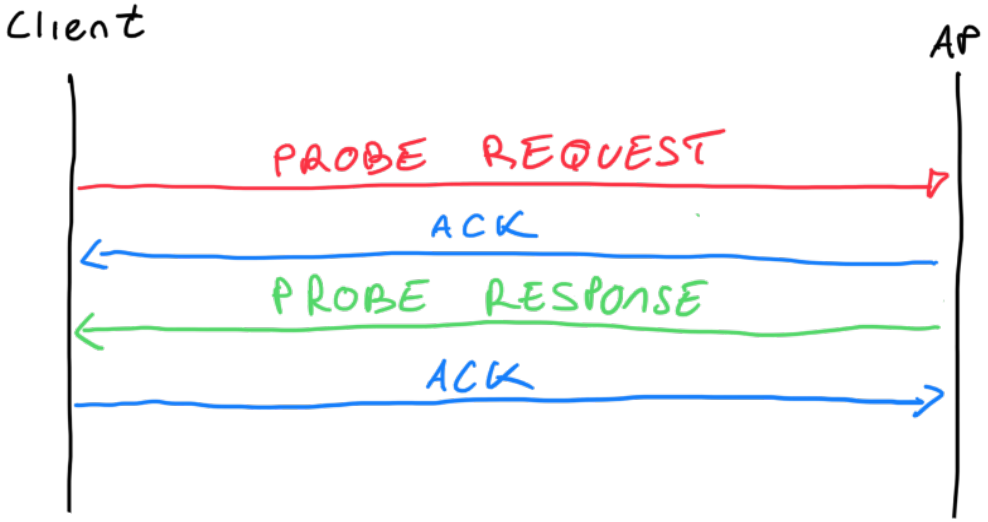
- Ing. JACOPO SALADINI (www.jacoposaladini.it)
- Consulente per NAeS Consulting da oltre 10 anni.
- Black Belt n.188
- Certificato CWNA, CWSP, CWDP.

# Argomenti :

- Come un device identifica l'AP su cui fare roaming.
- Tipologie di Roaming.
- Dal mondo reale.

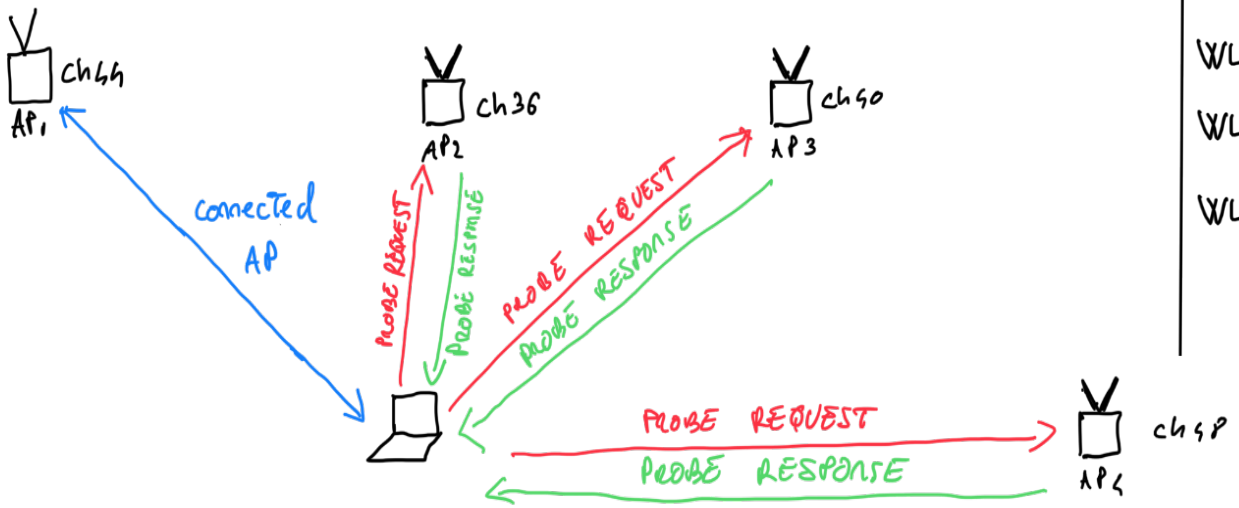
# Come un device identifica l'AP su cui fare roaming

I device wifi "scoprono" le reti wireless presenti nelle vicinanze tramite **l'active e il passive scanning** ovvero ascoltando i pacchetti beacon e attraverso il meccanismo di **probe request e probe response.** Per il roaming, è l'active scanning quello che ricopre il ruolo più importante:



# Come un device identifica l'AP su cui fare roaming

Il **risultato del meccanismo di probing è una tabella** di AP che il device tiene sempre aggiornata per trovare il **miglior candidato** su cui fare roaming :




| SSID | AP | ch | RSSI |
|---|---|---|---|
| WLANTEST | AP2 | 36 | -57 dBm |
| WLANTEST | AP3 | 40 | -70 dBm |
| WLANTEST | AP4 | 48 | -83 dBm |

**Nota bene: Non solo la potenza ricevuta è il parametro utilizzato per scegliere AP a cui fare roaming e vi sono dei protocolli come 802.11k e 802.11v che influenzano le decisioni del client.**

# Come un device identifica l'AP su cui fare roaming

La questione è ora capire quando il device decide di fare roaming ?

**La risposta è che dipende dai driver del dispositivo!!!!**

There are 3 factors that trigger roaming on a Samsung mobile device:

1. **Weak signal —** Mobile devices trigger a roaming scan to avoid frequent retransmissions from lost packets. When the current AP's Received Signal Strength Indicator (RSSI) value is weak (below -75dBm), the device searches for an AP with a stronger signal.
2. **Beacon loss** — When beacon packets from a connected AP isn't received after 2 seconds (6 second if the display is OFF), the mobile device considers it a lost beacon and triggers a roaming scan.
3. **Channel Utilization (CU)** — When multiple clients are connected to the same AP, connectivity may be hindered despite having a strong radio signal due to limited resources. In which case, the AP will notify the clients of its current traffic through the CU factor in its beacon. The mobile device will then trigger a roaming scan if the received CU value is greater than 70 percent and the current RSSI value is between -65dBM and -75dBm.

Currently, CU roaming is supported on Galaxy S and Note series devices released since the Galaxy S8. The mobile devices will choose to connect to a new AP with 10dBm higher RSSI value than the current AP from the result of its roaming scan triggered by the aforementioned cases.

il "roaming scan" ovvero l'invio di probe request deve dare come risultato un valore di potenza ricevuta della probe response **10 dbm più alto rispetto all'AP a cui si è connessi**, solo in quel caso si inizierà il processo di roaming.

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

# Come un device identifica l'AP su cui fare roaming

Un altro aspetto fondamentale è che quando si è in fase di probing ( invio e ricezione di probe request e probe response) non si trasmettono più dati perché **la radio è off-channel rispetto** all'ap a cui si è collegati.**Più canali** vengono interrogati per trovare un ap con una potenza migliore ,**più si perde tempo**, questo aspetto è fondamentale quando il servizio che si vuole garantire sul WIFI è il voip.

Come affrontano questo problema i client?

**Save Roaming Channels**

The purpose of roaming is to provide a seamless data experience. However, data may be muted while performing roaming scans. To remedy this, Samsung mobile devices support partial scanning for a more efficient roaming performance.

For a partial scan, a mobile device maintains a list of channels containing the same SSID at every scan. During roaming, the device will only scan for the channels in this list instead of a full-channel scan. This helps the device to update the scan list at a much faster rate.

For example, on Galaxy S series, an active scan takes 40ms and a passive scan (on DFS channels) takes 130ms. With this, a legacy full-scan takes about 2800ms to complete while a partial scan with 7 saved channels will only take about 280ms — a 90% improvement.

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

# Come un device identifica l'AP sulla banda dei 6 GHZ

Nella frequenza dei 6 ghz uno scan completo **impiegherebbe circa 6** secondi visto l'elevato numero dei canali 59 e sarebbe anche **molto inefficiente** dal punto di vista del risparmio energetico . Quindi sono stati **introdotti altri meccanismi** rispetto la ricerca degli AP:

1- **Out of Band Discovery (RNR)** : Si utilizzano le bande 2,4/5 ghz per trovare l'ap con i metodo visiti prima . Il device legge RNR dai beacon e si connette successivamente a 6 ghz. Sarà il metodo preferito da molti vendor sia di client che di AP , per esempio **l'unico supportato da apple ad oggi.**

2. **In-Band Discovery:** Sone metodi direttamente implementati nella frequenza dei 6 ghz e sono tre:

**a.** Preferred Scan Channel (PSC): Il device è autorizzato a fare probing su 15 dei 59 canali.

**b.** Fast Initial Link Setup (FILS) : Sono dei beacon compressi che ed inviati ogni 20 msec.

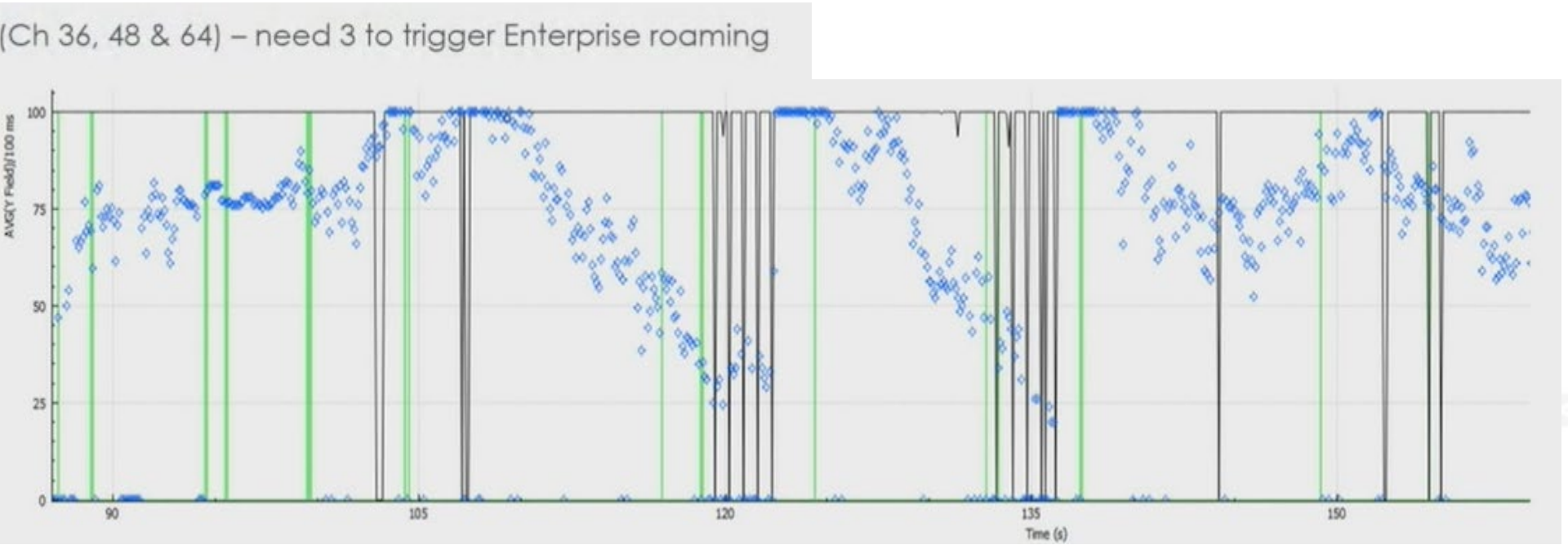
**c**. Unsolicited Probe Responses (UPR) : Molto simile al precedente , ma meno efficiente,si inviano delle probe response ogni 20 msec.

https://mrncciew.com/2023/09/20/6ghz-ap-discovery-part-1/

# Come un device identifica l'AP su cui fare roaming

Alcuni dati dal mondo reale:

Iphone .



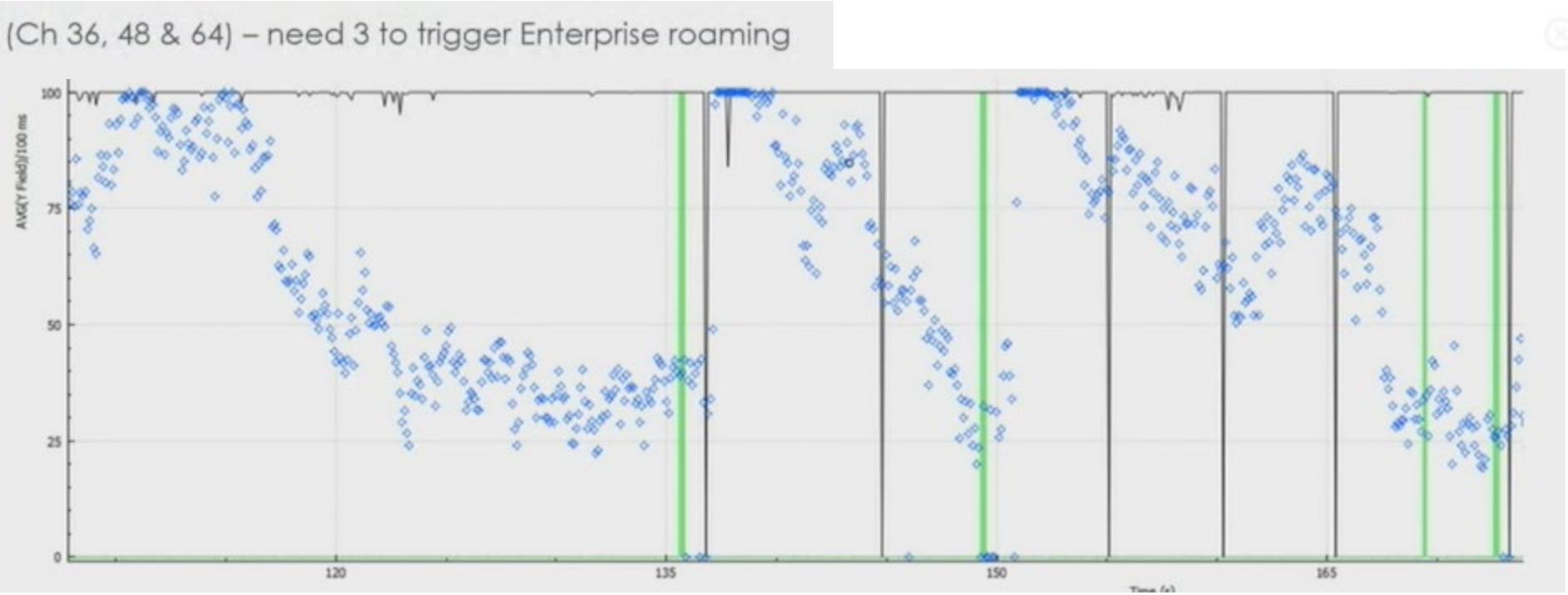

Without 11k
3.046 secs

Effects of 802.11k/r/v | Andrew McHale | WLPC Prague 2019

# Come un device identifica l'AP su cui fare roaming

Alcuni dati dal mondo reale:

Telefono VOIP




Without 11k
1.712 secs

Effects of 802.11k/r/v | Andrew McHale | WLPC Prague 2019

# Protocolli di supporto al roaming 802.11k

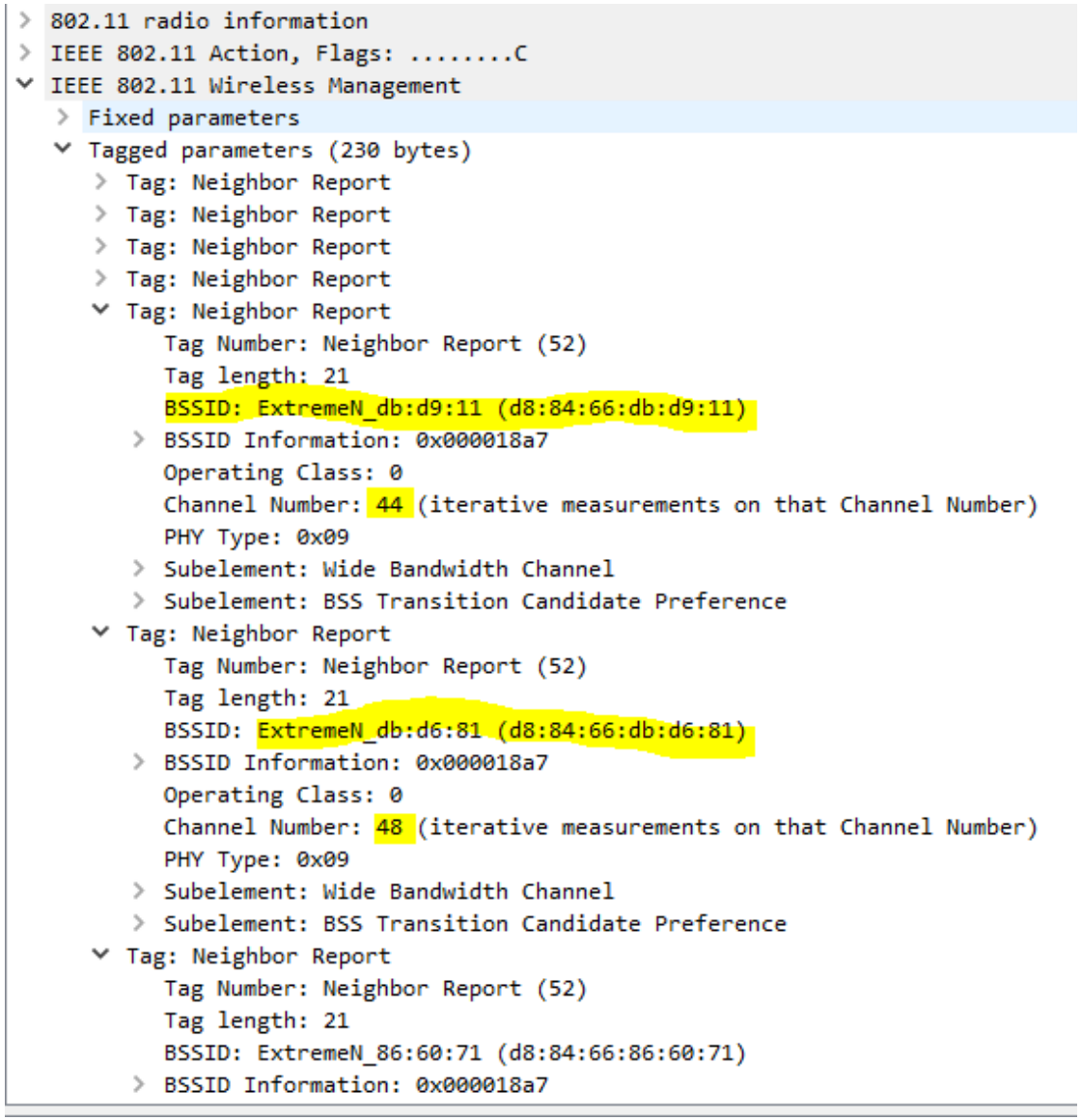
Nella prima parte ho parlato di come un device identifica i vari candidati per fare roaming, per aiutarlo in questa operazione esistono due protocolli che opzionalmente possono essere abilitati 802.11k e 802.11v.

## 802.11k

Grazie allo standard 802.11k, la ricerca sui dispositivi dei punti di accesso vicini disponibili come destinazioni per il roaming viene velocizzata mediante la creazione di un elenco di canali ottimizzato. Quando la potenza del segnale del punto di accesso corrente si indebolisce, il dispositivo esegue la scansione dei punti di accesso di destinazione inclusi in tale elenco.

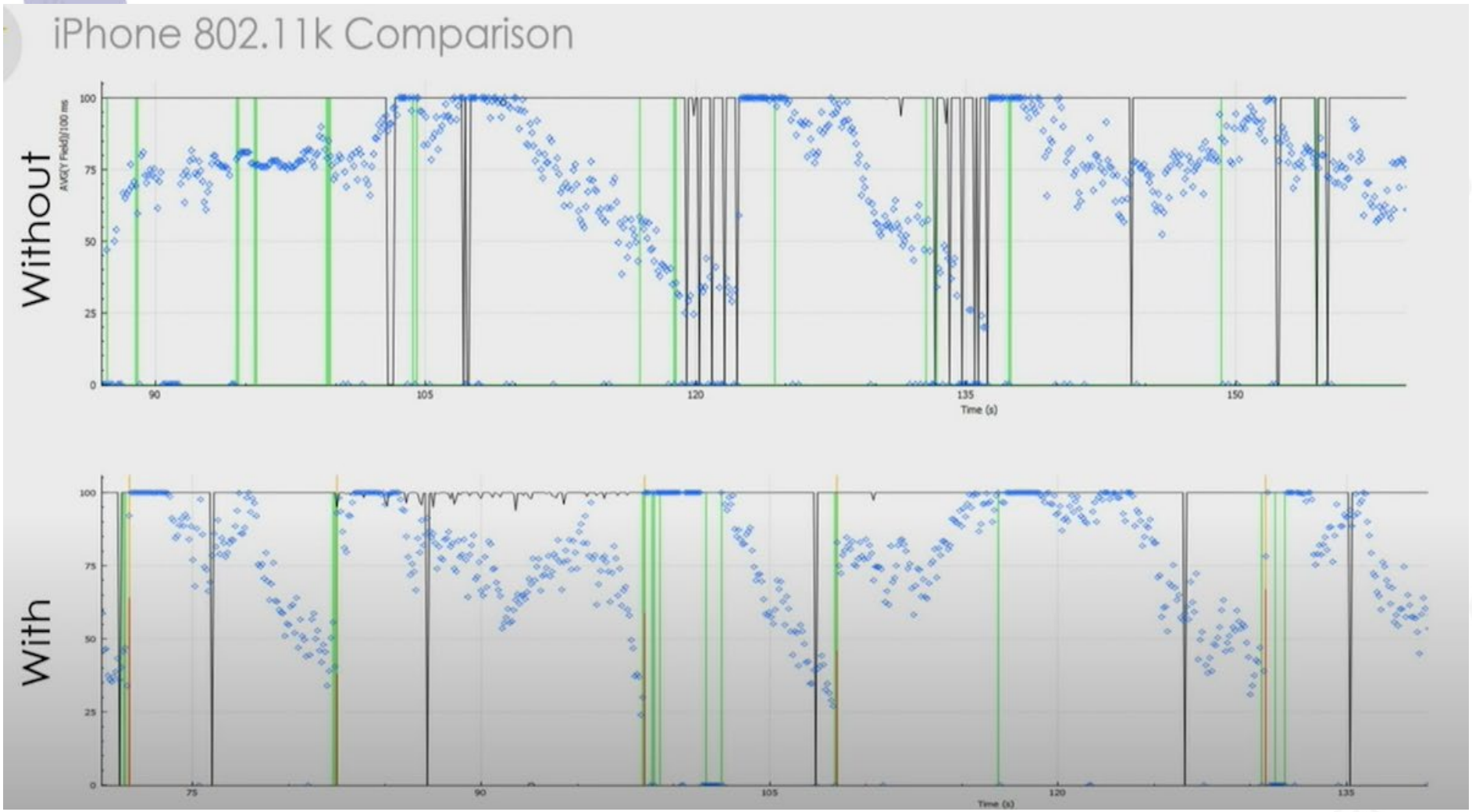
https://support.apple.com/it-it/HT202628

# Configurare il Fast Roaming




https://support.apple.com/it-it/HT202628

# Configurare il Fast Roaming




Without 11k
3.046 secs

With 11k
0.178 secs

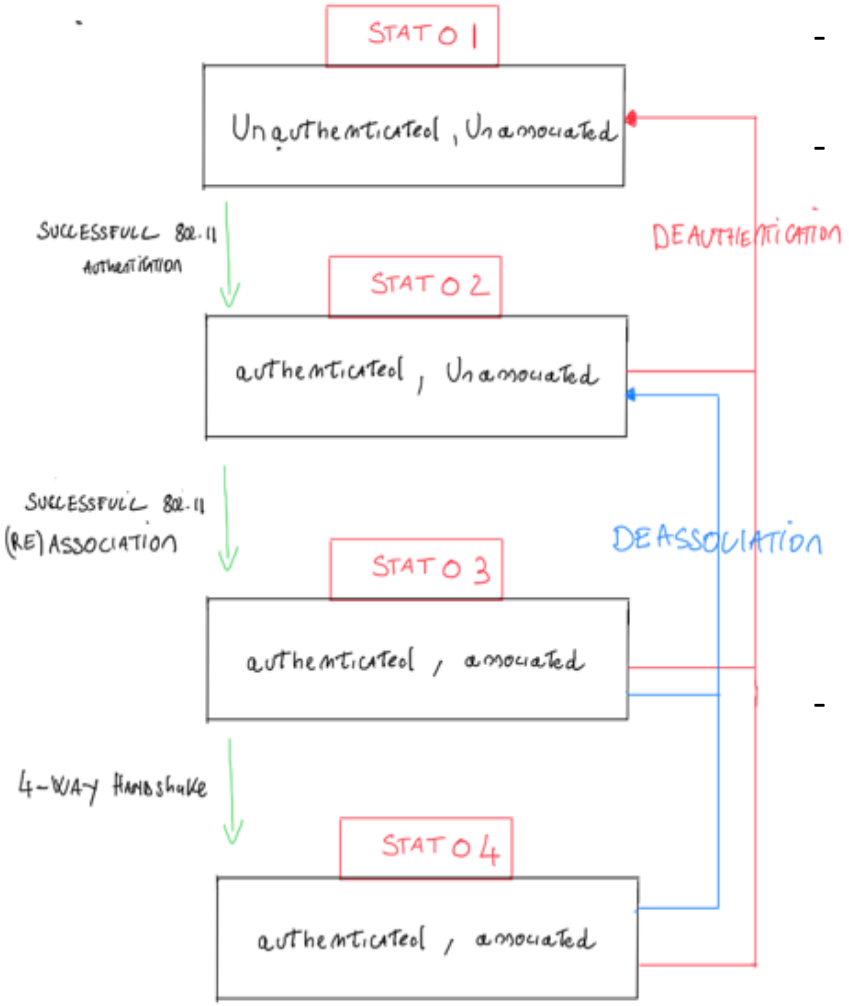
# Tipologie di Roaming

- Roaming Lento
- PMK Caching
- Fast Roaming (802.11r)

Peter MacKenzie | Analysing Roaming Protocols Wifi Design Day Ekahau 8 Novembre 2019

# Tipologie di Roaming

Prerequisiti per capire meglio le slide successive:




- Dallo stato 3 , se non c'è autenticazione , il client può trasmette.
- Tra lo stato 3 e lo stato 4 sia per autenticazione WPA Personale (PSK) o WPA Enterprise (802.1x) si creano le chiavi di criptazione temporanee PTK tra client e AP. **Nota bene quindi ogni volta che si fa roaming bisogna ricreare queste chiavi** . La differenza tra PSK e 802.1x è come viene creata la PMK che uno dei componenti per creare le PTK con i vari AP, di seguito la formula :

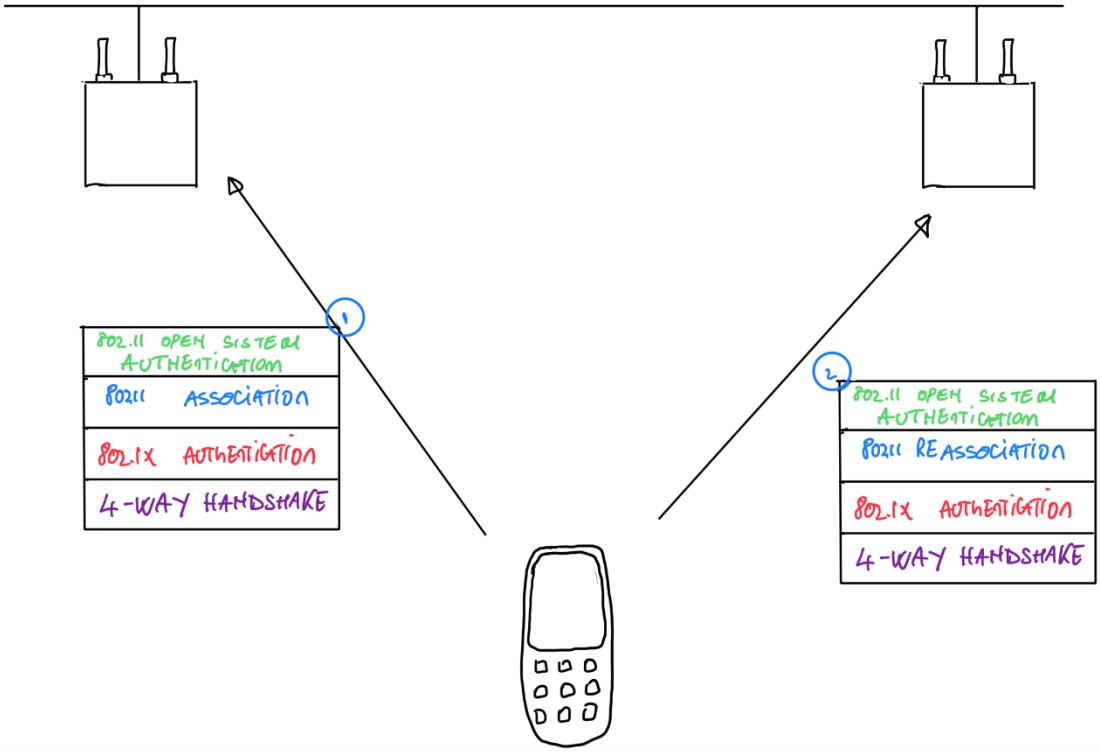
  **PTK=PRF(PMK+ANonce+SNonce+AA+SPA)**

  che però non analizzo in questo articolo.
- Se l'autenticazione è 802.1x ,nello stato 3, è coinvolto un componente esterno chiamato Radius , è il responsabile di verificare le credenziali inviate dal cliente che possono essere login/password o un certificato. **Essendo un componente esterno questa fase può essere molto lenta.**

# Tipologie di Roaming

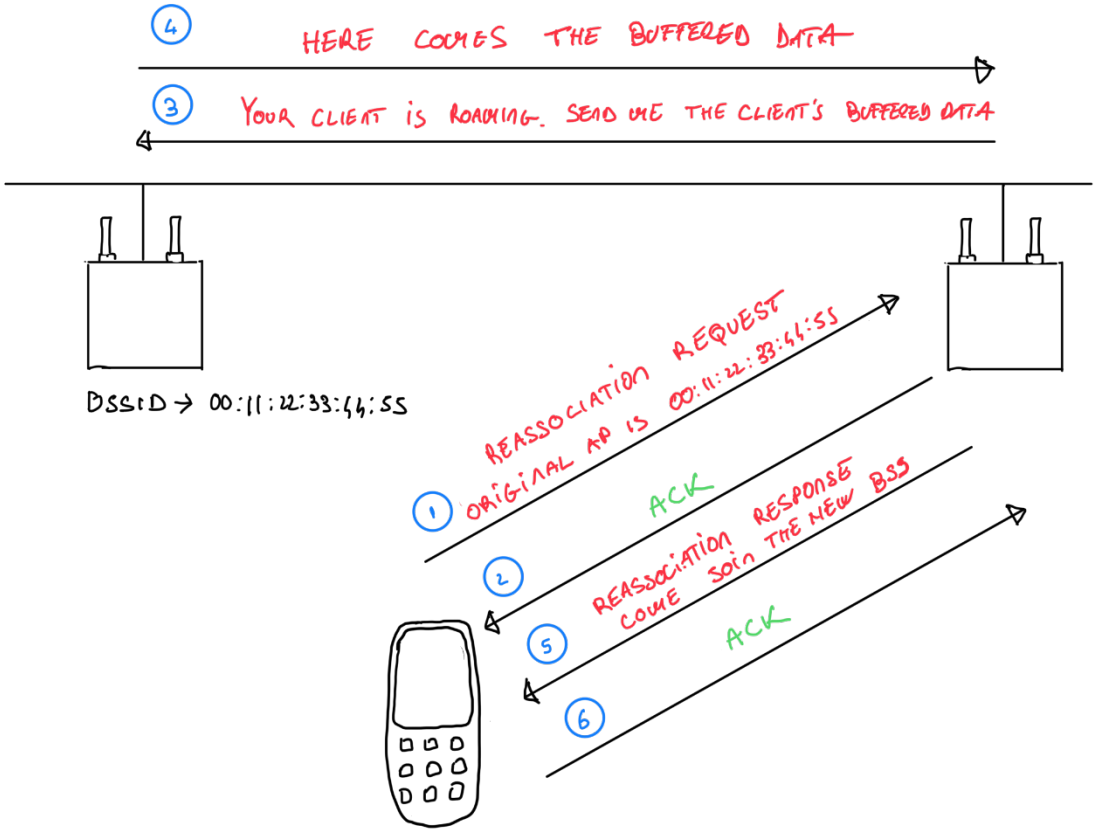
**Roaming Lento**

Intendo per roaming lento il roaming in cui la rete wireless ha autenticazione 802.1x e non c'è nessun tipo di meccanismo che possa velocizzare il roaming . In questo caso ogni volta che si fa roaming con un nuovo AP è come una nuova connessione alla rete wireless e quindi si passa da tutte le fasi , compresa quella con il radius che è la più lenta (**anche più di 200ms**).



# Tipologie di Roaming

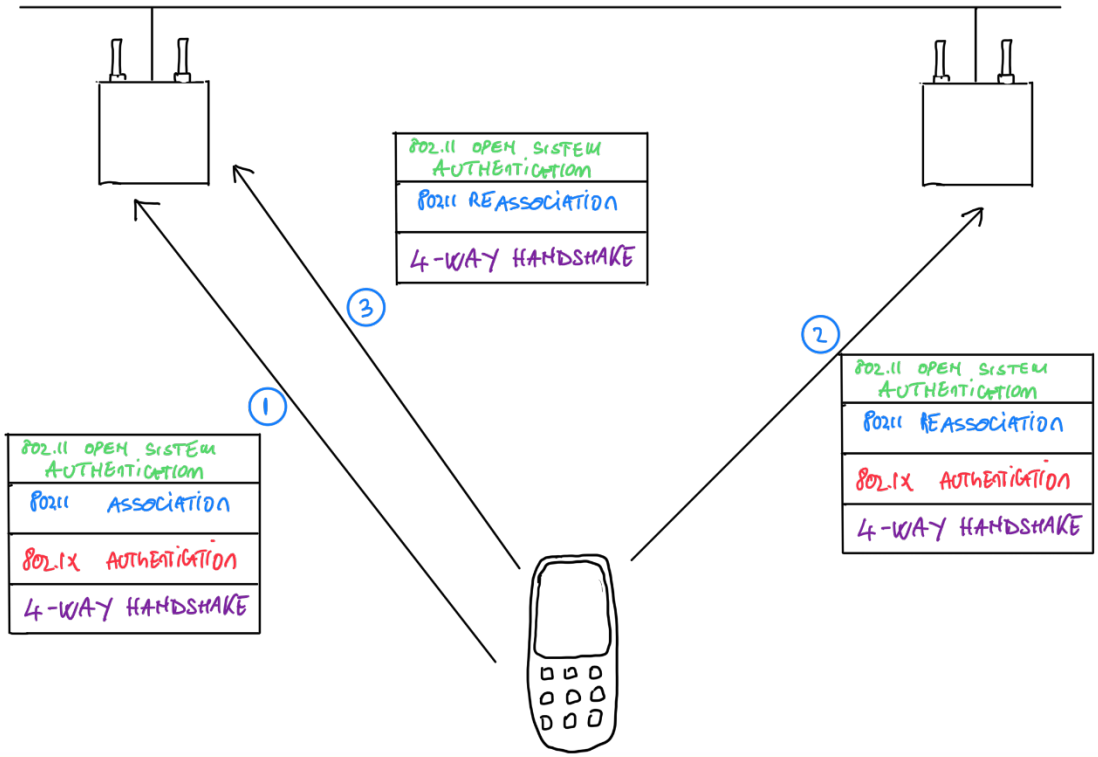
L’unica differenza fra la prima connessione alla rete wifi e i successivi roaming è il pacchetto di associazione che cambia in re-associazione , in questo pacchetto il client segnala il mac address dell’ AP a cui è connesso cosi che quest’ultimo possa recuperare eventuali dati nel buffer.  Nella figura successiva una spiegazione del meccanismo di reassociazione:



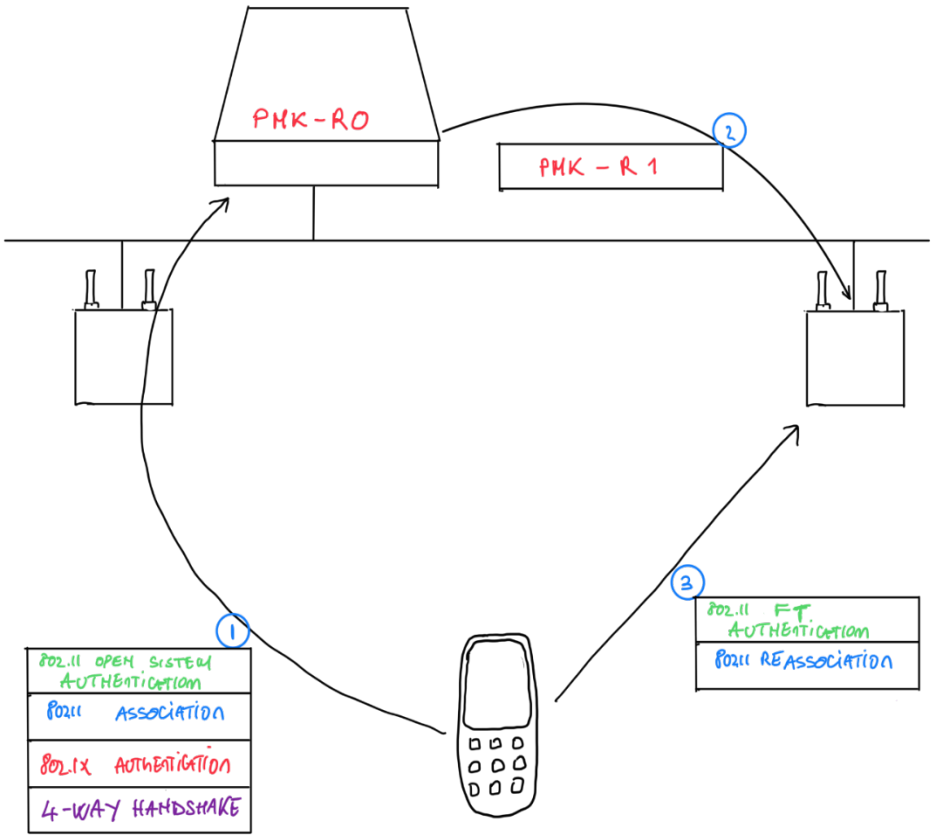
# Tipologie di Roaming

## PMK Caching

Con il pmk caching c'è una prima ottimizzazione del roaming , infatti quando si fa roaming su un AP su cui si è già precedentemente fatto roaming il client invia nella reassociation request anche nuovo parametro che è  il PMKID che può essere utilizzato per non eseguire la lenta autenticazione verso il radius. Nella figura sottostante un esempio di pmk caching dove il client non fa l'autenticazione 802.1x nella terza fase perché nella prima fase ha già fatto "caching" di una pmk valida per quel AP.



# Tipologie di Roaming




## Fast Roaming Over-the-air (802.11r )

Con il Fast Roaming diventa fondamentale la **presenza di un wireless controller** perché **l'associazione avviene con il controller** e non con l'AP. Questo meccanismo permette di distribuire a tutti gli AP la PMK ,che serve come input al meccanismo di 4-way handshake che bisogna fare ad ogni roaming ,per creare le chiavi di criptazione temporanea PTK . Il 4-way handshake è inglobato nel 802.11 FT authentication e 802.11 Reassociation.

Without 11r
0.472 secs

With 11r OTA
0.002 secs

# Dal mondo reale.

- Se si abilita 802.11r è difficile poter controllare che tutti i device lo supportino correttamente, quando c'è qualche device che ha dei problemi di solito l'autenticazione radius si chiude correttamente ma in aria la segnalazione si blocca. Nel wireless controller il device sembra connesso ma privo di indirizzo ip. Riscontrato in alcuni modelli di huawei e su pc di fascia bassa.
- Se si abilita 802.11r insieme al 802.11w (Protected Management Frame) in alcuni device per esempio (Galaxy A51) l'aggancio alla rete funziona ma i successivi roaming falliscono e il device si scollega.
- Se si abilita 802.11k è opportuno fare un giro per controllare i Neighbour Report inviati dagli AP , è successo che per un baco dell'infrastruttura, gli AP informassero il client solamente degli AP che erano sullo stesso canale dell'AP che inviava il Neighbour Report. Il client quindi invece di fare roaming sull'AP migliore cercava di fare roaming con AP molto lontani e il più delle volte la connessione cadeva.

WORKSHOP GARR 2023

NET MAKERS

GRAZIE