



Soluzioni WiFi e applicazioni real time



Chi sono :

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

Argomenti :

- INTRODUZIONE: I PARAMETRI DI PROGETTO
- CENNI DI TEORIA : QOS e ROAMING
- IL PROGETTO DI UNA RETE VOIP
- DEMO SURVEY VALIDAZIONE

I PARAMETRI DI PROGETTO: VOIP

Prendiamo come esempio i parametri suggeriti dal CWDP:

- **LATENZA** → Minore di 150 ms (unidirectional)
- AIRTIME UTILIZATION → Deve essere minore del 50%
- SEGNALE MOLTO BUONO → -67 dbm e un SNR di almeno 25 db
- PERDITA' DI PACCHETTI → Deve essere minore del 1%.
- REQUISITI DI BANDA → 30-128 Kbps
- **ROAMING**

Per capire il QOS nelle reti 802.11 bisogna avere chiaro come avviene l'accesso al canale :

- IL CANALE WIFI è HALF DUPLEX .
- L' ACCESSO AL CANALE è di tipo CSMA/CA (Carrier Sense Multiple Access, Collision Avoidance). Non esiste un meccanismo che coordina l'accesso. L'accesso è tipo probabilistico.
- L' Accesso del canale è governato da due meccanismi :
 1. Tiro un dado.
 2. Ascolto il canale.

- **Contentation Window (CW)** : Un range di numeri nel quale le STA scelgono randomicamente un numero . (**è il nostro dado**). Per esempio per 802.11ag da 0 a 15 e per 802.11b è da 0 a 31. Il valore Cwmax puo variare anche in funzione se la tramissione è il primo tentativo o è una ritrasmissione.
- **Random Backoff** : E' il valore randomicamente scelto. Questo numero determina quanti slot il WM deve essere libero prima che STA possa trasmettere. (es : 802.11ac 9 microsecondi ; 802.11b 20 microsecondi).

- **Physical carrier Sense:** E' composto da **Carrier sense**, misura della potenza ricevuta di frame 802.11 e **Energy detect** che mi misura la potenza ricevuta sul canale . Entrambi devono essere sotto una determinata soglia per considerare il canale libero. (es : 802.11a 82 dBm Carriese sense , 62 dbm Energy Detect)
- **Virtual carrier Sense :** Esiste un campo nei pacchetti chiamato **Duranton** che indica quando il WM sarà occupato per completare lo scambio della frame. In questo modo il client può risparmiare energia .

```

802.11 MAC Header
  Version: 0
  Type: 410 Data
  Subtype: 40000 Data Only
  Frame Control Flags=400000010
  Duration: 213 _Microseconds
  Destination: 00:02:8D:74:67:2A Agere Sys:74:67:2A
  BSSID: 00:0C:85:62:D2:1D Cisco:62:D2:1D
  Source: 00:0C:85:62:D2:1D Cisco:62:D2:1D
  Seq Number: 1653
  Frag Number: 0
  
```



Duration/ID field indicates how long it will take to complete the present frame exchange. This value is processed by all stations in a BSA except the station to which the frame is directed.

The series of events are as follows:

1. When a STA has a frame to transmit, it randomly picks a value from the CW.
2. STAs begin to countdown that value, which is called the back off time.
3. When the WM is idle (as determined by carrier sense mechanisms) for a slot time, the back off timer decrements by one.
4. When the WM is busy, the STAs must wait and start the process over (carrier sense, interframe space, back off countdown)
5. When the back off timer reaches zero and the WM is idle, STAs may transmit.

WMM (WI-FI Multimedia) è un certificazione della WI-fi alliance derivata da 802.11e . Definisce 4 code che hanno diversi CW a seconda delle categorie VOCE , VIDEO, BEST EFFORT , BACKGROUND.

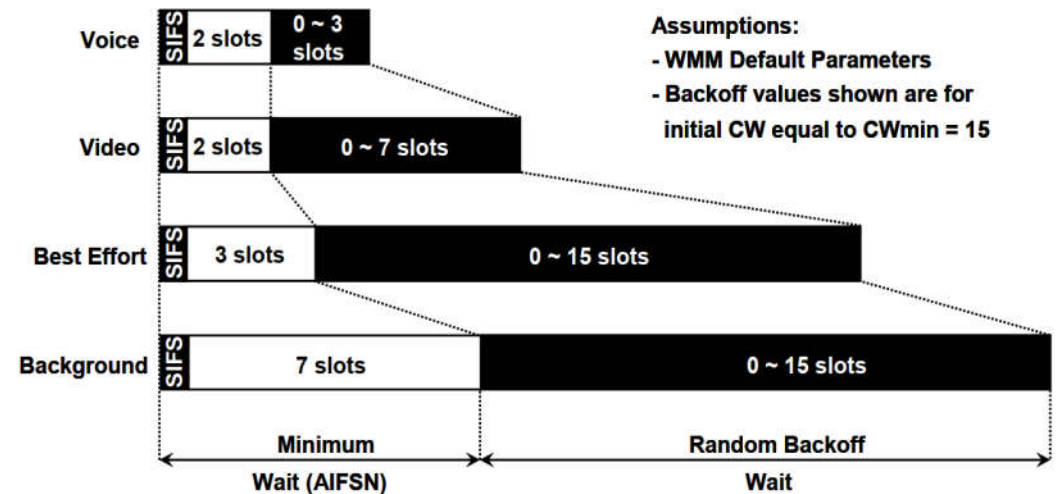
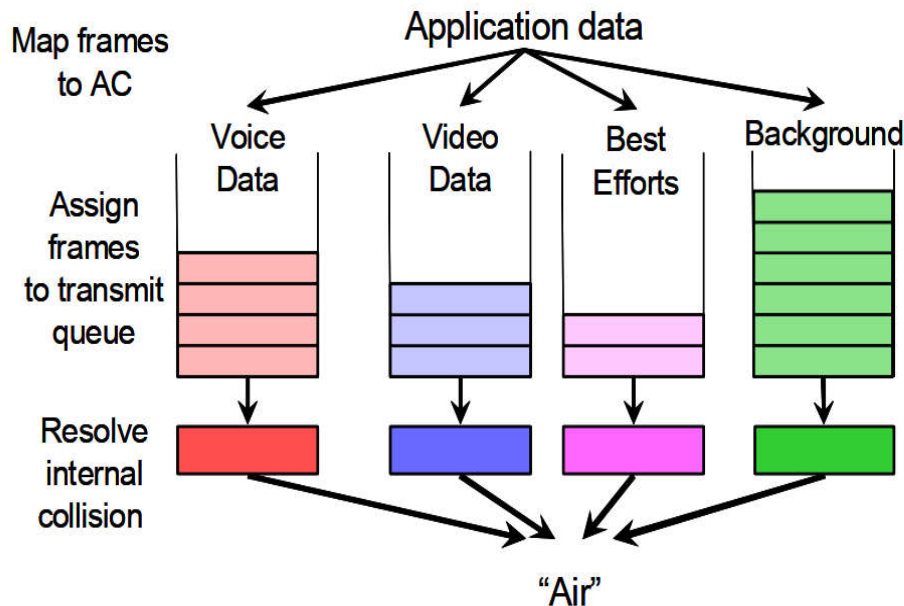
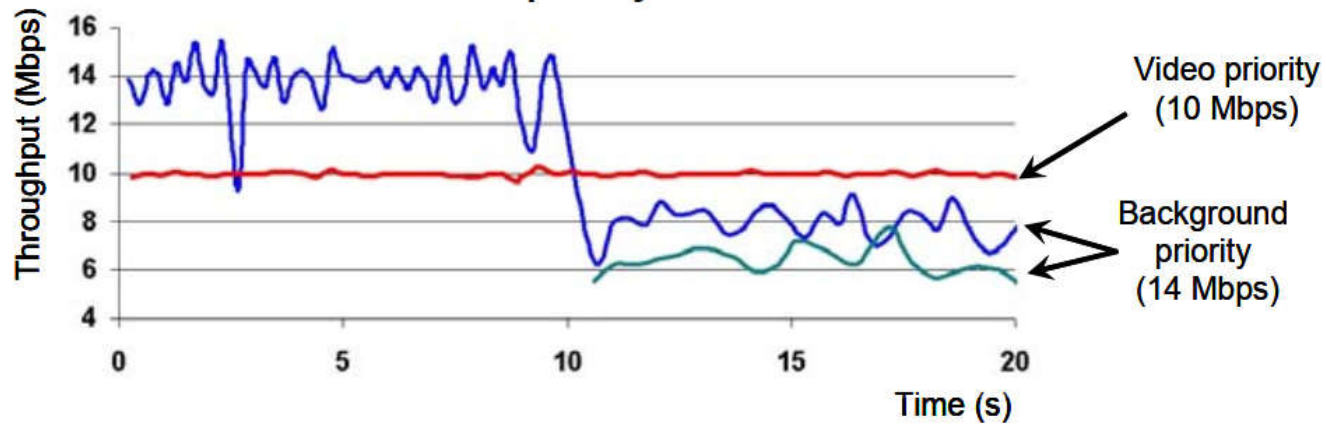


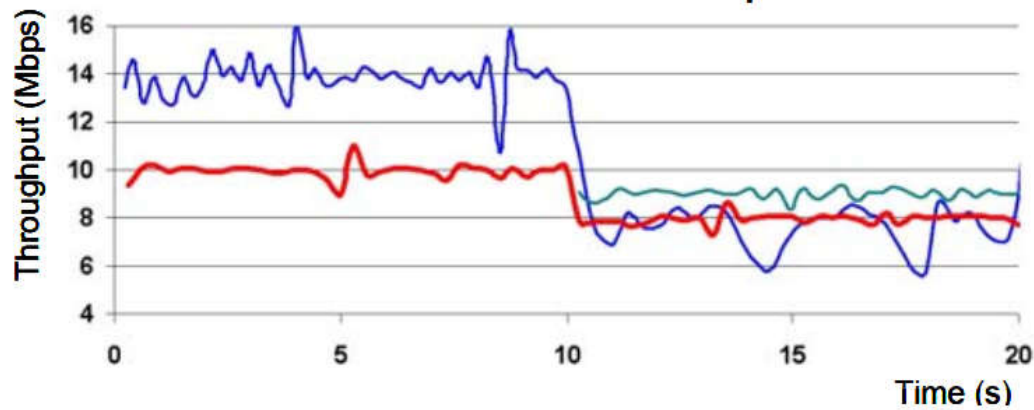
Figure 4. WMM AC Timing

QOS

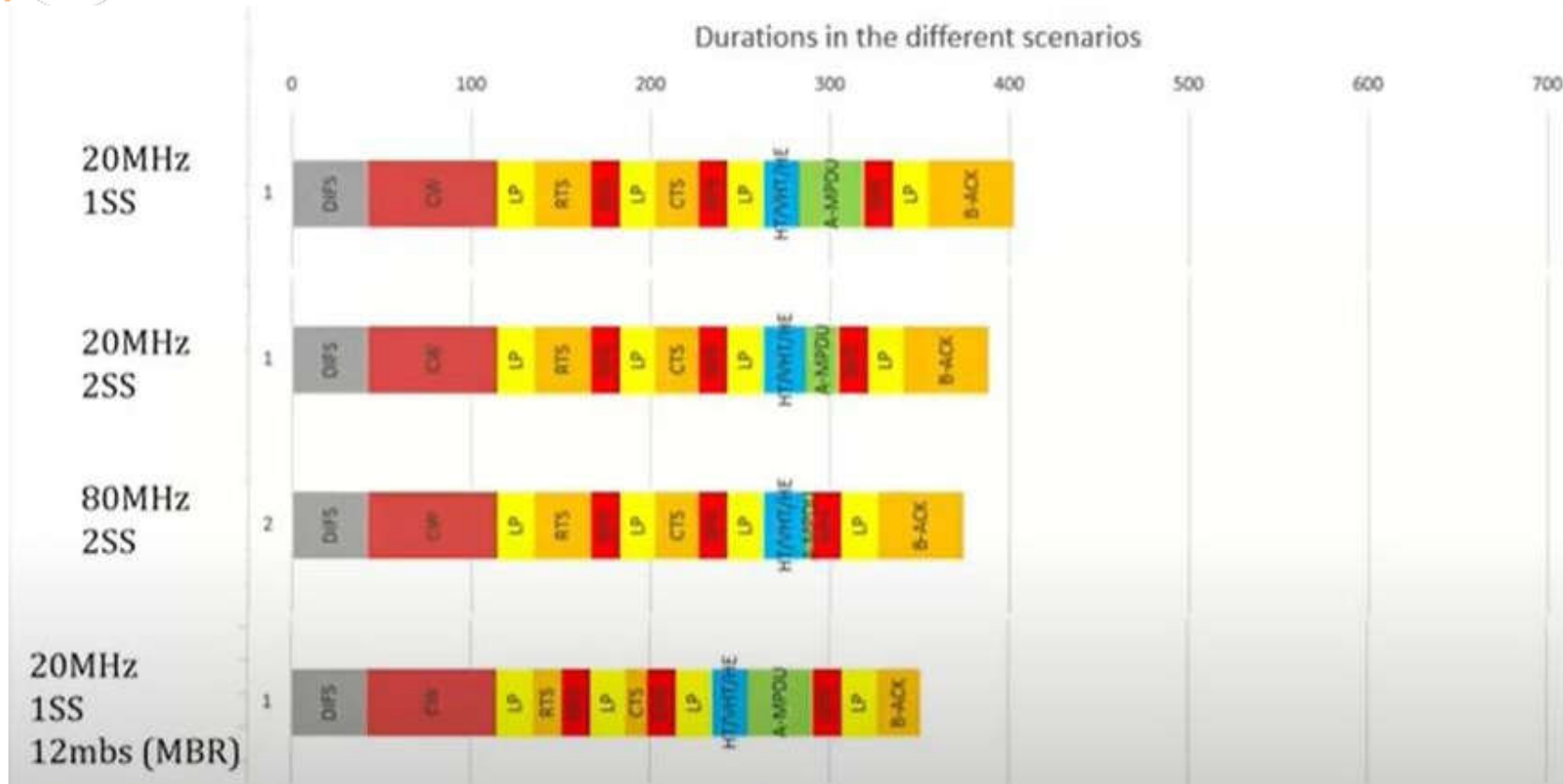
With WMM: video has priority over data



Without WMM: new data stream impacts video



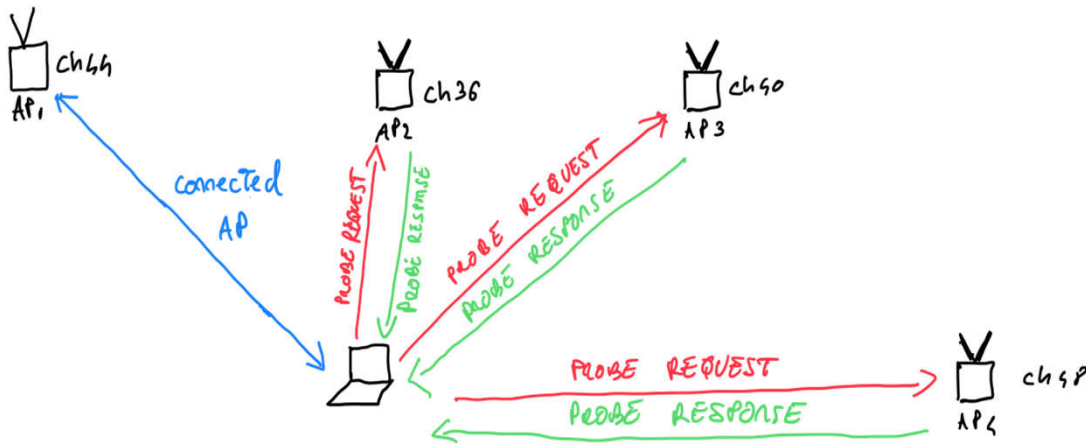
QOS



Il 38 % dell'intero tempo di invio di una frame è dedicato al meccanismo di contesa del canale!

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 su cui fare roaming

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.

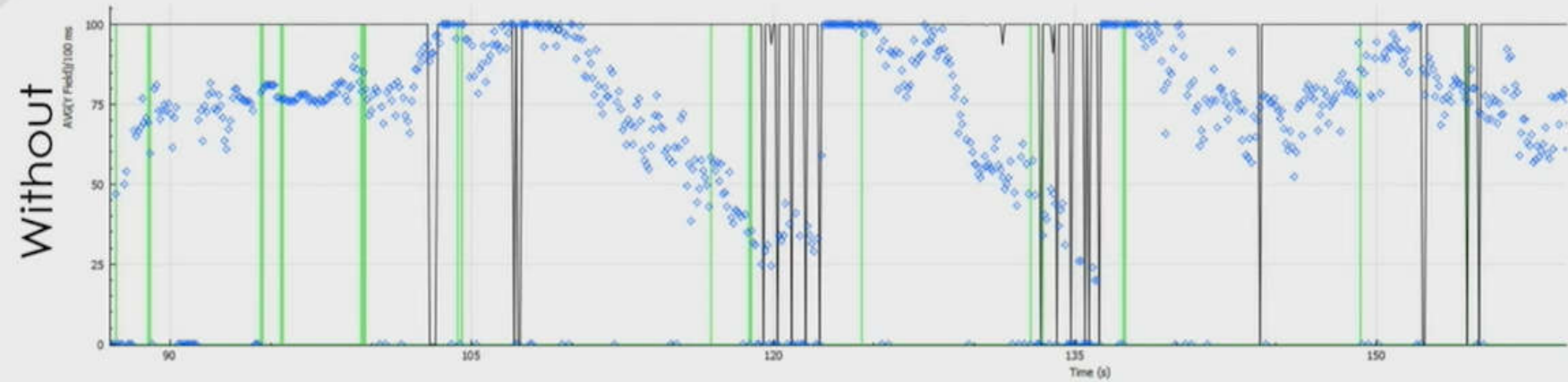
<https://support.apple.com/it-it/HT202628>

Come un device identifica l'AP su cui fare roaming

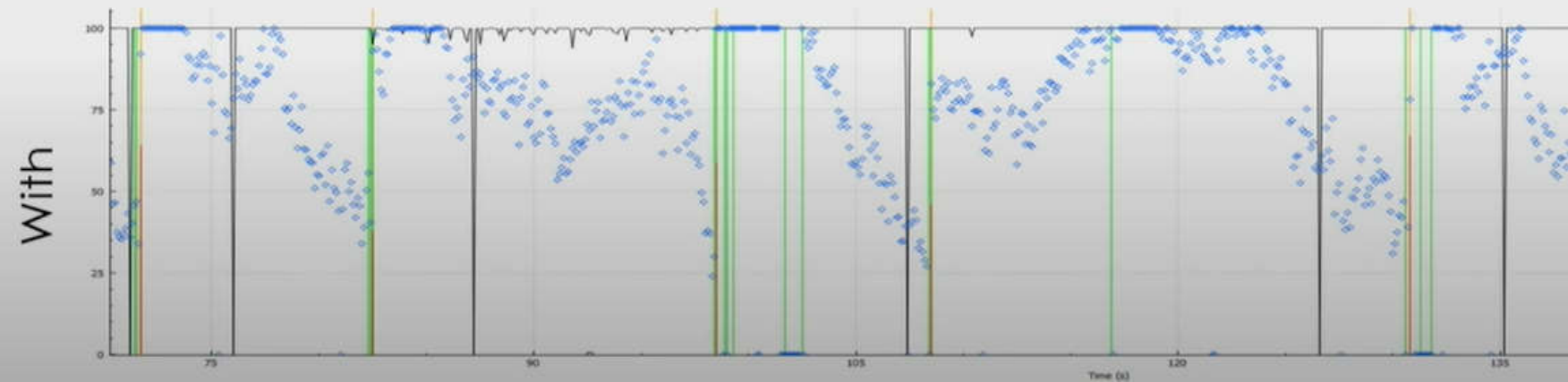
```
> 802.11 radio information
> IEEE 802.11 Action, Flags: .....C
v IEEE 802.11 Wireless Management
  > Fixed parameters
  v Tagged parameters (230 bytes)
    > Tag: Neighbor Report
    > Tag: Neighbor Report
    > Tag: Neighbor Report
    > Tag: Neighbor Report
    v Tag: Neighbor Report
      Tag Number: Neighbor Report (52)
      Tag length: 21
      BSSID: ExtremeN_db:d9:11 (d8:84:66:db:d9:11)
    > BSSID Information: 0x000018a7
      Operating Class: 0
      Channel Number: 44 (iterative measurements on that Channel Number)
      PHY Type: 0x09
    > Subelement: Wide Bandwidth Channel
    > Subelement: BSS Transition Candidate Preference
  v Tag: Neighbor Report
    Tag Number: Neighbor Report (52)
    Tag length: 21
    BSSID: ExtremeN_db:d6:81 (d8:84:66:db:d6:81)
  > BSSID Information: 0x000018a7
    Operating Class: 0
    Channel Number: 48 (iterative measurements on that Channel Number)
    PHY Type: 0x09
  > Subelement: Wide Bandwidth Channel
  > Subelement: BSS Transition Candidate Preference
  v Tag: Neighbor Report
    Tag Number: Neighbor Report (52)
    Tag length: 21
    BSSID: ExtremeN_86:60:71 (d8:84:66:86:60:71)
  > BSSID Information: 0x000018a7
```


Come un device identifica l'AP su cui fare roaming

iPhone 802.11k Comparison



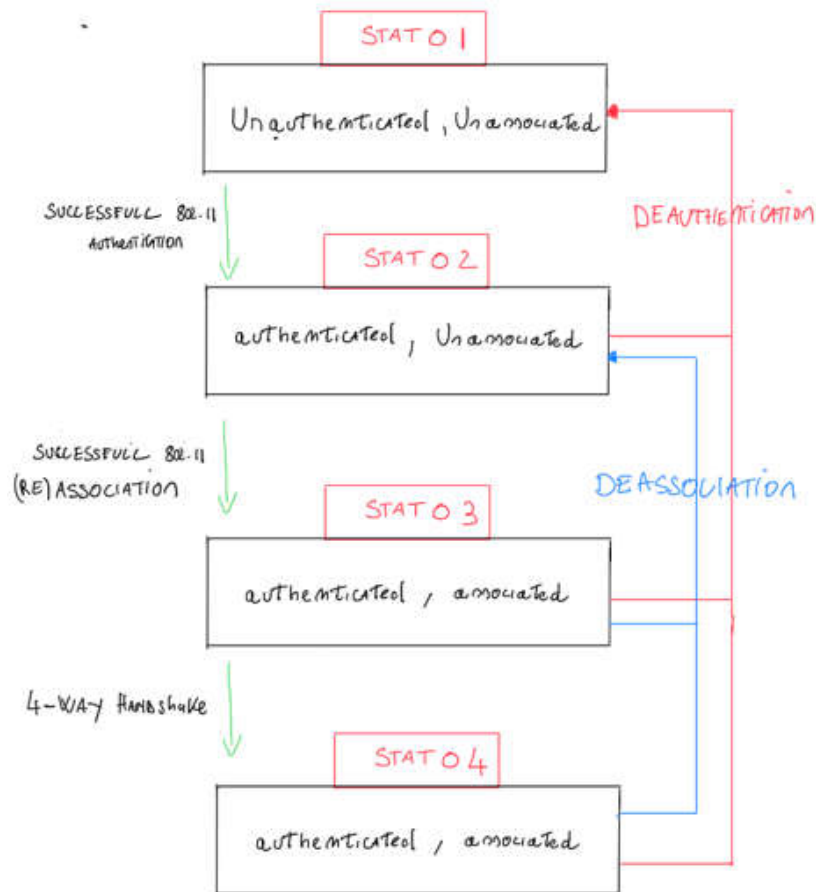
Without 11k
3.046 secs



With 11k
0.178 secs

Tipologie di Roaming

Prerequisiti per capire meglio le slide successive:



- Dallo stato 3 , se non c'è autenticazione , il client può trasmettere.
- 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 :

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

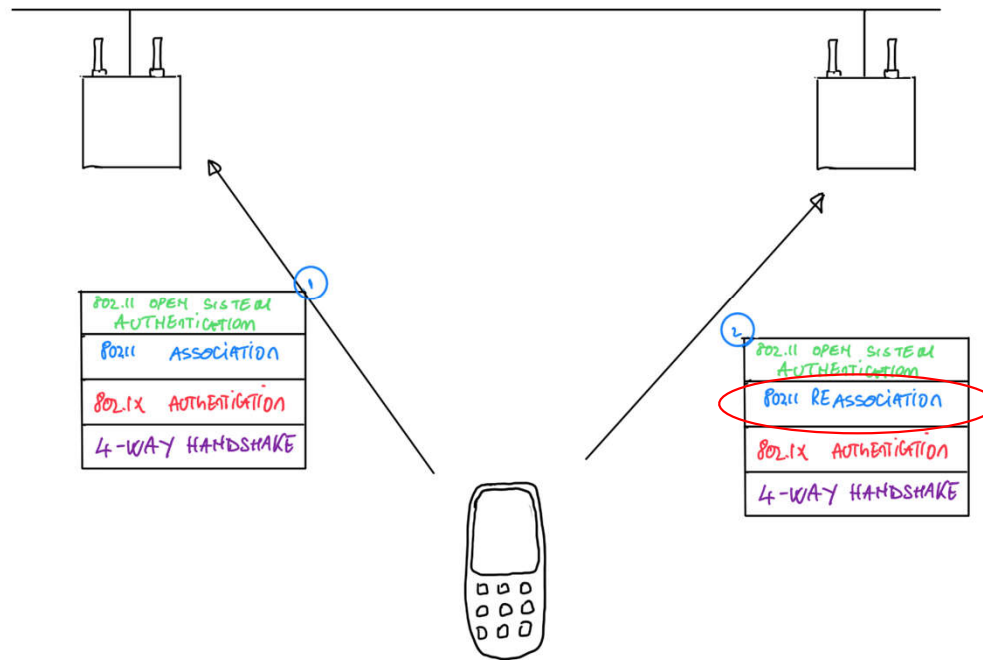
che però non analizzo in questo articolo.

- 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.**

Roaming Lento

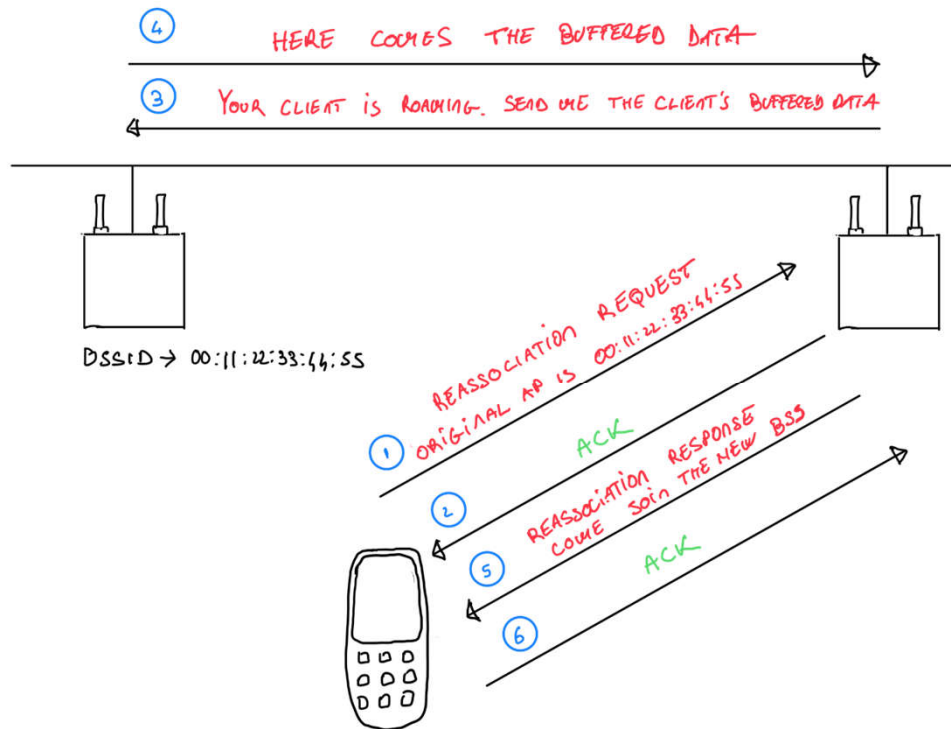
Tipologie di Roaming

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).

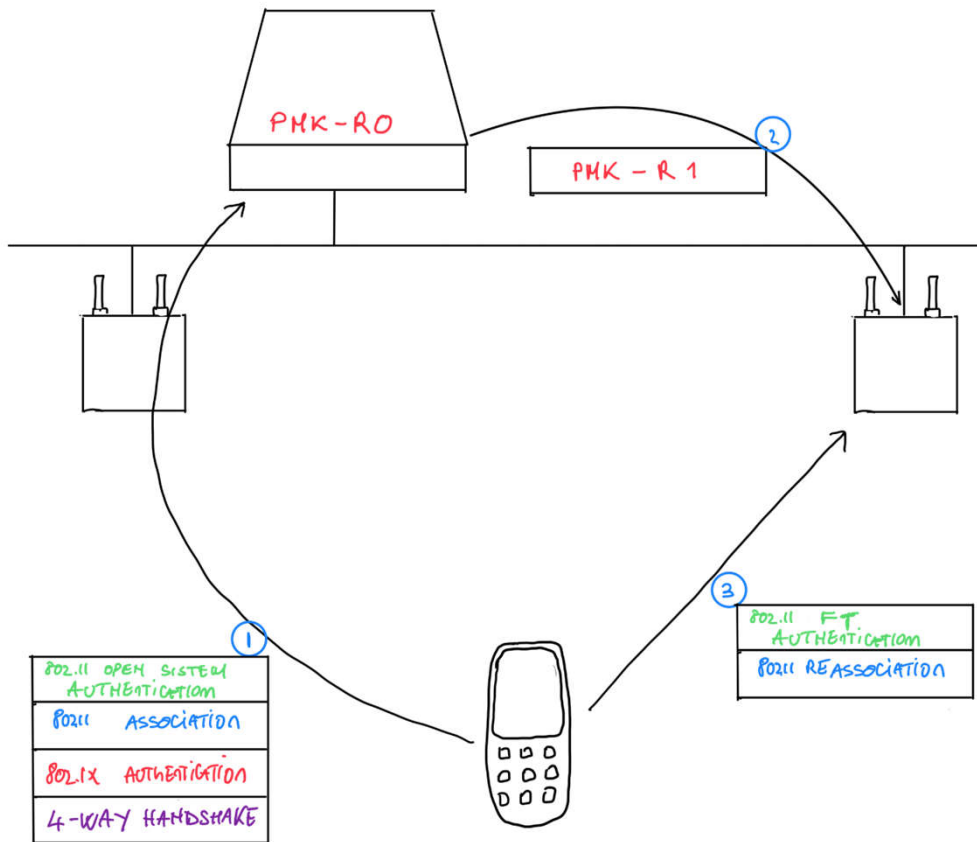


Tipologie di Roaming

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 così che quest'ultimo possa recuperare eventuali dati nel buffer. Nella figura successiva una spiegazione del meccanismo di reassociazione:



Tipologie di Roaming

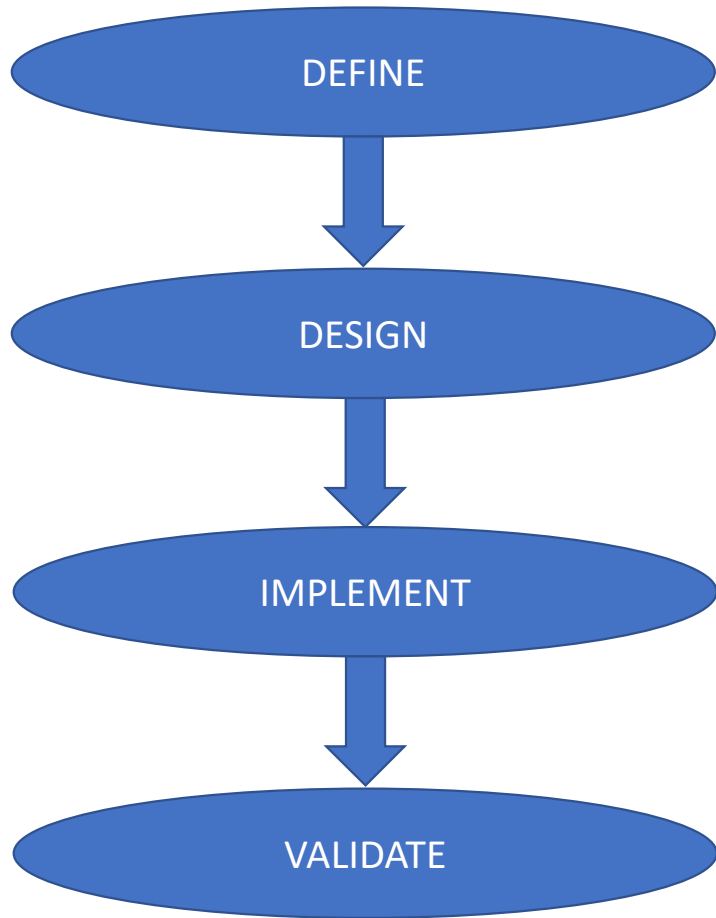


Fast Roaming Over-the-air (802.11r)

Siamo giunti al fast roaming che è lo standard per il roaming veloce. E molto simile a OKC a parte due aspetti , il primo è che esiste un architettura delle chiavi dove il controller detiene la PMK-R0 e gli AP le PMK-R1 ma la differenza maggiore è la fase 3 , come si vede in figura non c'è più il 4-way handshake .

Ma come è possibile visto che il 4-way handshake bisogna farlo con tutti gli AP a cui ci si connette ?
Nella fase 3 sparisce perchè viene inglobato nel 802.11 FT authentication e 802.11 Reassociation.

PROGETTO DI UNA RETE VOIP



1. STORICO MODIFICHE	2
2. INDICE	3
3. INFORMAZIONI SUL DOCUMENTO.....	4
4. OBIETTIVI E PARAMETRI.....	5
5. SURVEY PRE-DESIGN.....	6
5.1. SITE SURVEY	6
5.2. TEST LEAST CAPABLE DEVICE.....	7
6. ARCHITETTURA, CONFIGURAZIONI E MAPPE.....	9
6.1. MAPPE	9
6.2. PORTE RJ45 E INDIRIZZI IP.....	14
6.3. SCHEMA LOGICO.....	17
6.4. SSID E VLAN.....	18
6.5. SICUREZZA	18
6.6. QoS DESIGN.....	20
6.7. CONFIGURAZIONE RADIO	21
6.8. MODELLI E VERSIONI DI FIRMWARE	23
7. SURVEY DI VALIDAZIONE	24
7.1. ANALISI DELLE INTERFERENZE.....	40
7.2. ANALISI DEL THROUGHPUT	42
7.3. MODIFICHE DELLE POTENZE	43
8. REFERENCES.....	43



PROGETTO DI UNA RETE VOIP

OBIETTIVO:

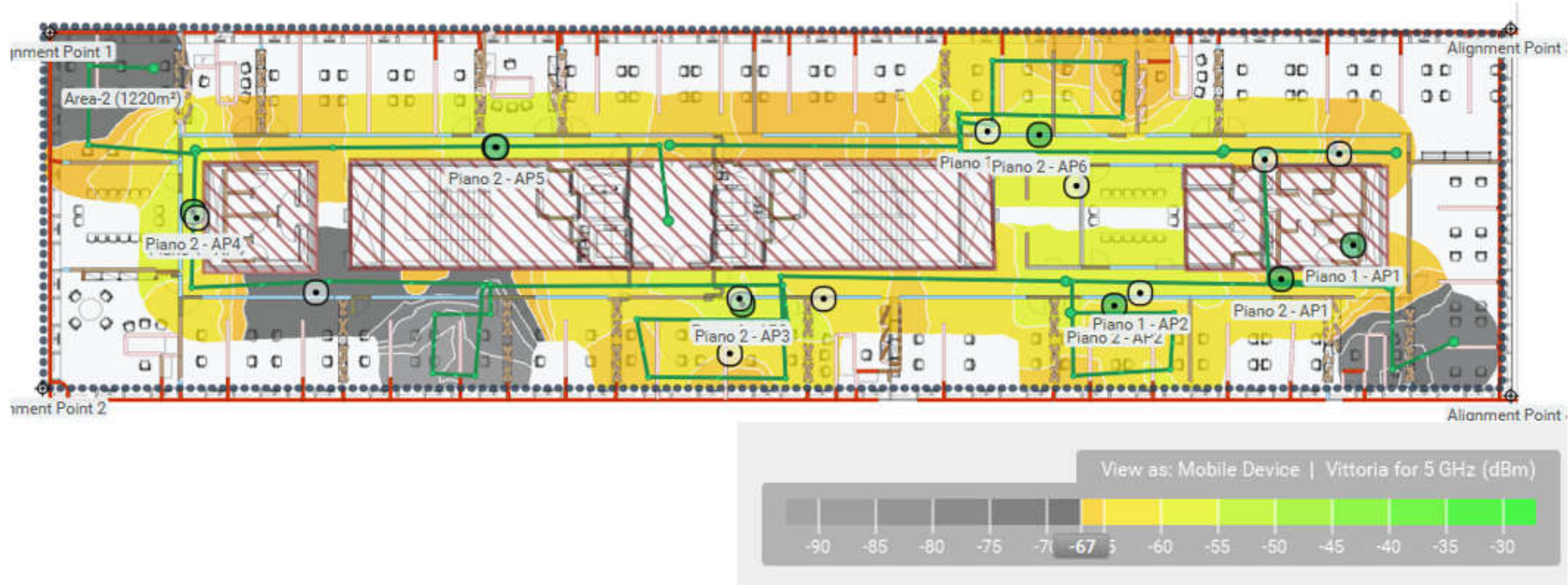
L'obiettivo del progetto è quello di aggiornare la rete Wireless esistente alle più moderne tecnologie (WIFI 6), un miglioramento della copertura della rete Wireless e l'introduzione del servizio VOIP.

Il primo step è un Survey per controllare il grado di copertura attuale e se la rete possa correttamente supportare del Roaming . Si fissano i parametri di progetto e si addatta lo strumento di misura Sidekick alla least capable device (samsung A51)

		2.4GHz	5GHz	
Signal Strength	Min	-67	-67	dBm
Secondary Signal Strength	Min	-75	-75	dBm
Tertiary Signal Strength	Min	OFF	OFF	dBm
Signal-to-Noise Ratio	Min	25	25	dB
Data Rate	Min	11	11	Mbps
Channel Interference	Max	4	2	
at minimum Signal Strength		-80	-80	dBm
Number of Access Points	Min	OFF	OFF	
at min.		OFF	OFF	dBm
Round Trip Time (RTT)	Max	200	200	ms
Packet Loss	Max	2	2	%

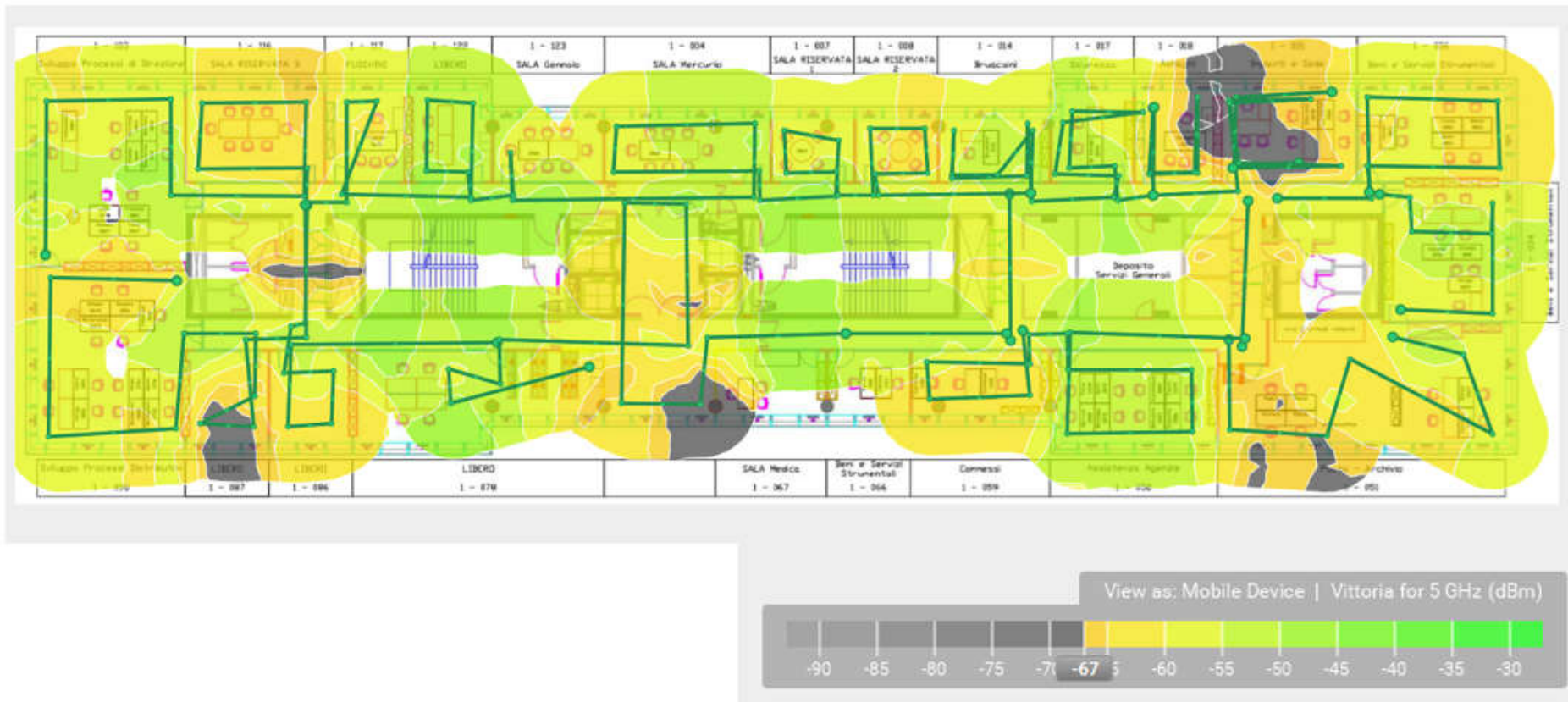
PROGETTO DI UNA RETE VOIP

Di seguito potete vedere l'immagine della potenza del segnale misurata a 5 GHz con strumento di Misura Ekahau Sidekick :



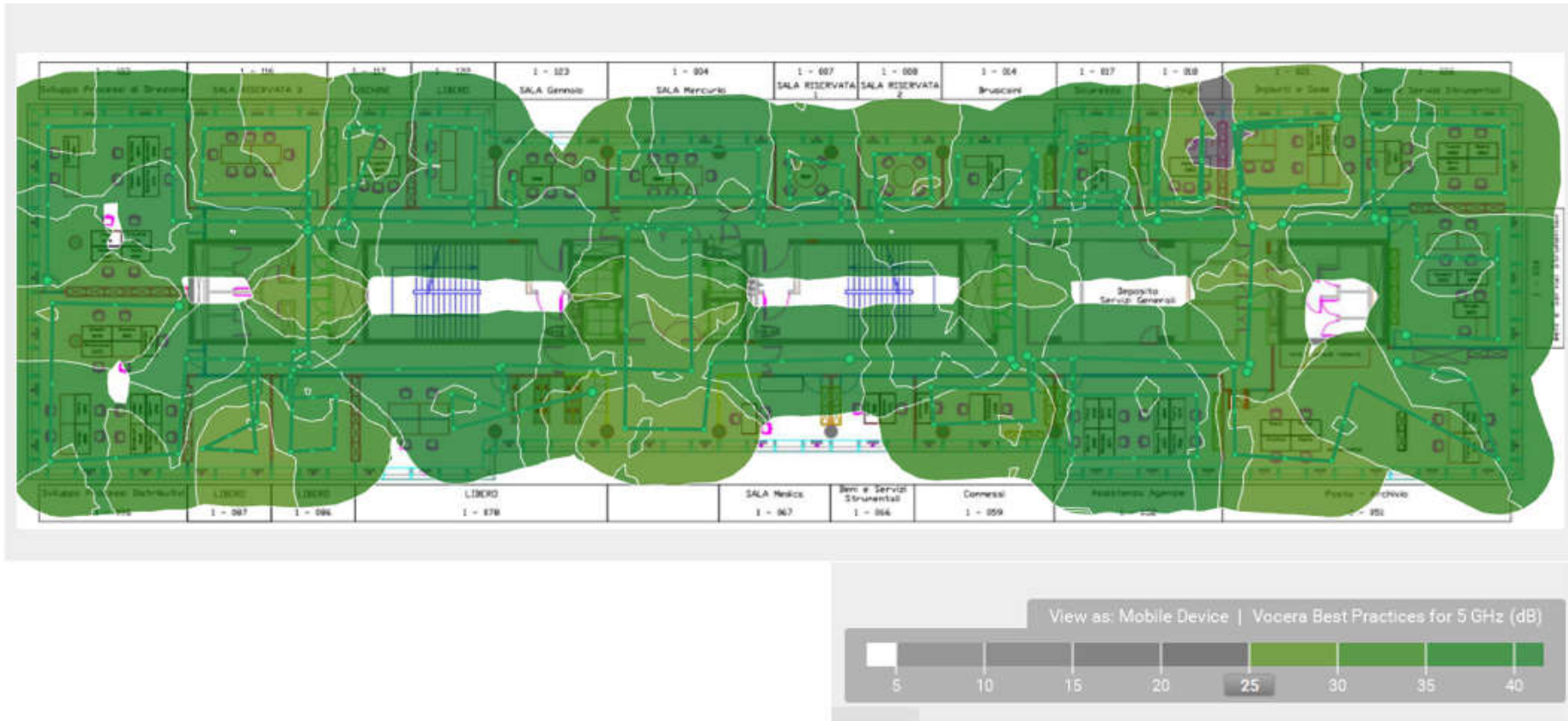
PROGETTO DI UNA RETE VOIP

Nella figura successiva mostriamo, invece, la misura di potenza di segnale a 5 GHz con strumento di Misura Ekahau Sidekick al Primo Piano con i nuovi AP410i installati fuori dal controsoffitto:



PROGETTO DI UNA RETE VOIP

I punti in grigio sono leggermente sotto i -67 dBm che abbiamo settato come parametro di progetto, quindi abbiamo deciso di analizzare anche il rapporto segnale/rumore del piano in quanto è il parametro più importante che influenza MCS (Modulation Coding Scheme) utilizzati dai dispositivi wireless (25 dBm parametro di progetto):





PROGETTO DI UNA RETE VOIP

Test Least Capable Device

Tra i dispositivi in dotazione in [REDACTED] il telefono con le peggiori caratteristiche è il Samsung Galaxy A51 e, buona prassi di progetto, è adattare la Rete al Least Capable Device.

Si sono, quindi, analizzate le caratteristiche radio del dispositivo, e di seguito riportiamo le più significative:

Antenna : **1x1**

Tecnologia : **802.11ac (WIFI 5)**

Roaming : Supporta roaming veloce 802.11r ma non i protocolli di roaming assistito 80211k, quindi è più lento a trovare l'AP su cui fare roaming.

E' stato necessario disabilitare il protocollo 802.11w Management Frame Protection in quanto il device si scollegava se quest'ultimo veniva attivato.

PROGETTO DI UNA RETE VOIP

Questi obiettivi sono stati affrontati tramite:

- Introduzione dei nuovi AP AP410i e AP460i (WIFI6)
- Il miglioramento della copertura della rete è stato ottenuto mediante l'aggiunta di nr. 2 AP nei piani 1-8 (rispetto ai nr. 6 esistenti) e con l'introduzione di altri AP nelle aree sprovviste della copertura Wireless originale. Inoltre, i nuovi AP sono stati posizionati all'esterno del controsoffitto.
- L'introduzione del servizio VOIP è il parametro di progetto più stringente in quanto il Voip ha la necessità di una buona copertura, avere sempre a disposizione 2 o 3 AP per ogni posizione e necessità di un roaming veloce tra di essi ed è molto sensibile ai ritardi.

Per rispondere a queste esigenze si sono aggiunti degli AP in specifiche posizioni e introdotti i protocolli di roaming veloce (802.11r) e di assistenza al roaming (802.11k).

Si segnala che non tutti i dispositivi supportano quest'ultimo protocollo (nello specifico il Samsung A51).

Per affrontare la questione ritardi lato wireless verranno introdotte politiche di QOS (vedere punto 6.6).

Si è deciso di utilizzare in maniera distinta le due frequenze WiFi disponibili a seconda delle due tipologie di utenti (PC e Cellulari).

In questo modo eventuali aggiornamenti pesanti legati ai PC (Windows, Backup, etc. etc.) non possono andare ad interferire con le latenze per i Cellulari che devono rimanere molto basse onde evitare ritardi sulla voce.

In particolare, si utilizzerà la frequenza a 5 GHz per i Cellulari e la frequenza 2,4 GHz per i PC.

Si è deciso di utilizzare la frequenza a 5 GHz per i Cellulari in quanto è più libera da possibili interferenze.

PROGETTO DI UNA RETE VOIP

Per la Quality of Service si sono utilizzate le stesse impostazioni che utilizza il client Cisco Jabber.

Nello specifico, da un'analisi del traffico radio si è dedotto che il client Jabber marca il traffico lato wireless con il CODE 6 :

```

0000 0010 0011 .... = Sequence Number: 33
▼ Qos Control: 0x0006
  .... 0110 = TID: 6
  [... 0110 = Priority: Voice (Voice) (6)]
  .... 0000 .... = QoS bit 4: Bits 8-15 of QoS Control field are TXOP Duration Requested
  .... 0000 .... = Ack Policy: Normal Ack (0x0)
  .... 0000 .... = Payload Type: MSDU
  0000 0000 .... = TXOP Duration Requested: 0 (no TXOP requested)
  
```

e lato IP con il DSCP CODE 46 :

```



..... = .....
▼ Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
  1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
  .... 0000 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  
```

Di conseguenza si è taggato il traffico lato wireless con lo stesso codice .

Si nota che lato Rete, ovvero dal centralino al telefono Voip, il pacchetto che riceve il telefono è sprovvisto di code DSCP.

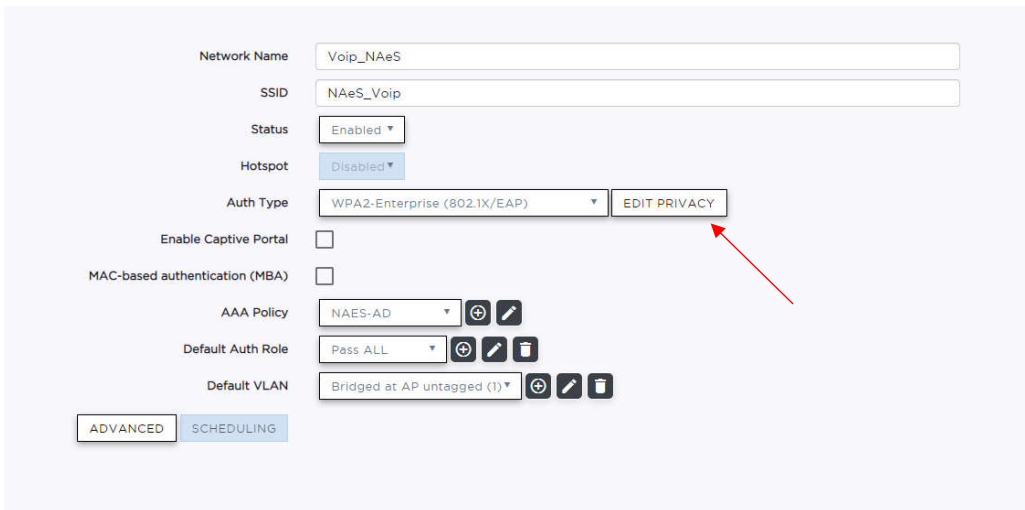
PROGETTO DI UNA RETE VOIP

Advanced (Radio 2) ? ×

OCS Channels	NONE SELECTED ▾
OCS Interval (DTIMs)	20
LDPC	Enabled ▾
STBC	Disabled ▾
Guard Interval Mode	Auto ▾
Airtime Fairness Mode	Off ▾
Maximum Distance	100
Tx Beam Forming	Disabled ▾
Radio Share Mode	Inline ▾
ADDBA support	Enabled ▾
Aggregate MSDU	Disabled ▾
Minimum Basic Rate	24 ▾ 
Aggregate MPDU	Enabled ▾
Aggregate MPDU max # of subframes	30
DTIM	2
OFDMA	Both ▾ 
BSS Color	0
Target Wake Time	Enabled ▾

Configurare il Fast Roaming

Configurare 802.11r su Extreme Cloud Controller (XCC)



Network Name: Voip_NAeS
SSID: NAeS_Voip
Status: Enabled
Hotspot: Disabled
Auth Type: WPA2-Enterprise (802.1X/EAP) **EDIT PRIVACY**
Enable Captive Portal:
MAC-based authentication (MBA):
AAA Policy: NAeS-AD
Default Auth Role: Pass ALL
Default VLAN: Bridged at AP untagged (1)

ADVANCED SCHEDULING

Configure → Networks → WLAN e selezionare la rete WPA2 Enterprise su cui si vuole abilitare 802.11r.

Privacy Settings



TKIP-CCMP

Protected Management Frames Disabled

Fast Transition

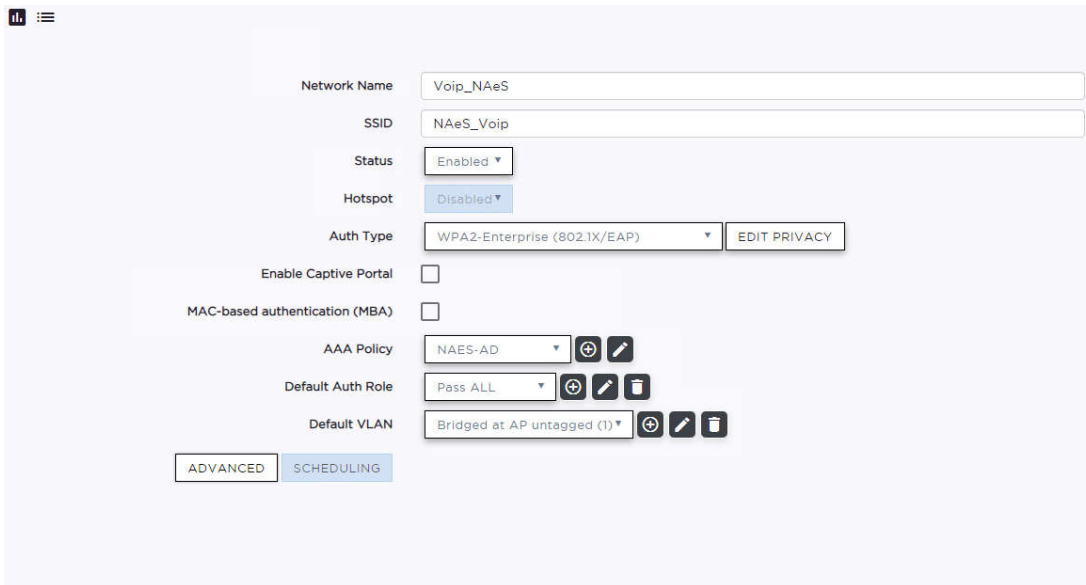
Mobility Domain ID: 8011

Close

Cliccare su edit privacy e selezionare il flag Fast Transition.

Configurare il 802.1k

Configurare 802.11k su XCC



Network Name: Voip_NAeS

SSID: NAeS_Voip

Status: Enabled

Hotspot: Disabled

Auth Type: WPA2-Enterprise (802.1X/EAP) EDIT PRIVACY

Enable Captive Portal:

MAC-based authentication (MBA):

AAA Policy: NAES-AD + ✎

Default Auth Role: Pass ALL + ✎ 🗑

Default VLAN: Bridged at AP untagged (1) + ✎ 🗑

ADVANCED SCHEDULING

Advanced Settings

- Agile Multiband i
- RADIUS Accounting
- Hide SSID
- Include Hostname
- Radio Management (11k) support i
- Beacon Report

Per abilitarlo su XCC andare su Configure → Networks e selezionare la wlan che ci interessa e poi cliccare su advanced.

E abilitare il flag del 802.11k.



DEMO SURVEY VALIDAZIONE



FINE! GRAZIE!