Comprensione dei roaming veloci 802.11r/11k/11v su 9800 WLC

Sommario

Introduzione

In questo documento vengono descritti i diversi risultati dei metodi di roaming veloce attivati/disattivati sui client wireless.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Nozioni fondamentali sulle WLAN IEEE 802.11.
- Sicurezza WLAN IEEE 802.11.
- Nozioni di base di IEEE 802.1X/EAP
- Transizione rapida BSS IEEE 802.11r.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Wireless 9800-L Controller IOS® XE 17.9.4
- Access point Cisco Catalyst serie 9130AXI.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Questo documento aiuta a comprendere la differenza quando si attivano i protocolli 802.11r, 802.11v e 802.11k su un controller wireless 9800. Viene inoltre illustrato l'impatto sui client quando vengono disattivati.

802.11r, 802.11v e 802.11k sono tutti standard o modifiche differenti della famiglia di protocolli di rete wireless 802.11.

802.11r: è la transizione rapida tra set di servizi di base che introduce un nuovo concetto in cui l'handshake iniziale con un nuovo access point viene eseguito prima che il client esegua il roaming verso il punto di accesso di destinazione. È particolarmente utile in ambienti in cui la connettività ininterrotta è fondamentale, come ad esempio nelle applicazioni di streaming voce su IP o in tempo reale con monitor video o a flusso costante. Con una rete 802.11r ottimizzata, i dispositivi possono spostarsi tra i punti di accesso senza subire interruzioni significative o cali nella connettività di rete.

802.11k: Neighbor List and Assisted Roam (Radio Resource Measurement) sfrutta le funzionalità di gestione delle risorse radio per migliorare le prestazioni complessive e l'affidabilità delle reti wireless. Ottimizza le risorse radio disponibili dove i punti di accesso raccolgono e condividono informazioni sul proprio ambiente radio. Queste informazioni includono l'utilizzo dei canali, la potenza del segnale e i livelli di interferenza. Può quindi essere utilizzato dai dispositivi client per prendere decisioni più informate su quale punto di accesso connettersi, il che si traduce in un migliore bilanciamento del carico, minori interferenze e una maggiore efficienza della rete.

802.11v: Risparmio energia basato su rete che aiuta i client a migliorare la durata della batteria, consentendo loro di dormire più a lungo. Si concentra inoltre su come migliorare l'efficienza e la gestione delle reti wireless. Ciò a sua volta consente un migliore controllo e coordinamento tra l'infrastruttura di rete e i dispositivi client quando i client sono in roaming. Le caratteristiche principali sono i report sui router adiacenti, le transizioni dei set di servizi, il bilanciamento del carico e il risparmio energia basato sulla rete. Queste funzionalità migliorano l'individuazione, la selezione e il monitoraggio della rete client. Consente inoltre ai punti di accesso di incoraggiare i dispositivi client a effettuare il roaming invece di attendere che il dispositivo prenda una decisione di roaming.

Mentre lo standard 802.11r è incentrato sulla transizione senza interruzioni tra i punti di accesso, lo standard 802.11v mira a migliorare le funzionalità di gestione della rete. Lo standard 802.11k è progettato per ottimizzare l'utilizzo delle risorse radio al fine di migliorare le prestazioni e l'affidabilità.

Alcune affermazioni di questo documento sono tratte dal libro Comprensione e risoluzione dei problemi dei Cisco Catalyst serie 9800 Wireless Controller Capitolo 6, sezione roaming 802.11.

Roam di sicurezza di livello superiore

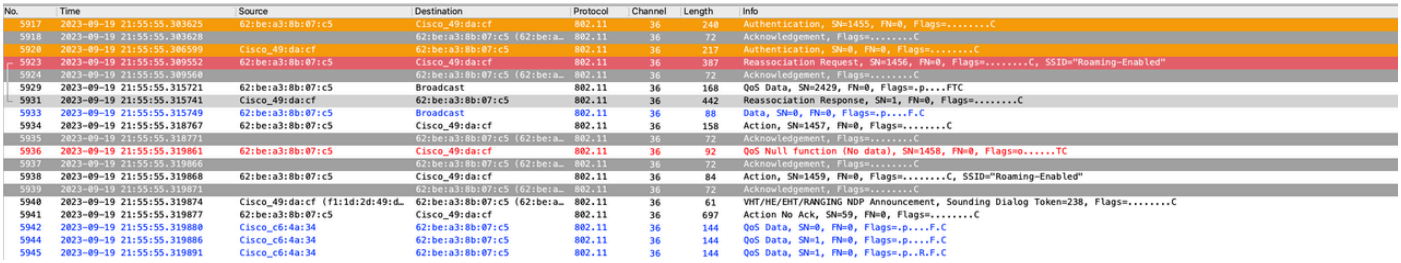
Quando il SSID è configurato con la protezione di livello superiore L2 oltre all'autenticazione di base 802.11 Open System, sono necessari più frame per l'associazione iniziale e quando i client eseguono il roaming. I due metodi di sicurezza più comuni standardizzati e implementati per le WLAN 802.11 sono:

- WPA/WPA2/WPA3 Personale: PSK utilizzato per autenticare i client.
- WPA/WPA2/WPA3 Enterprise: il metodo EAP (Extensible Authentication Protocol) e 802.1x vengono utilizzati per autenticare i client wireless, ovvero per convalidare le credenziali utente (nome utente e password), i certificati o i token tramite un server AAA.

In questo documento, WPA2 Enterprise WLAN può essere usato con EAP-PEAP per mostrare la differenza nell'uso dei protocolli IEEE (802.11r, 802.11k e 802.11v) e come potrebbe influenzare i tentativi di roaming wireless.

SSID con protocolli di roaming veloce abilitati (802.11r, 802.11k e 802.11v)

Per impostazione predefinita, nella configurazione WLAN predefinita tutti i protocolli sono abilitati. In laboratorio, il client wireless tenta di effettuare il roaming tra punti di accesso 9130. Poiché si dispone della configurazione predefinita della WLAN, in altre parole, il roaming veloce è abilitato oltre agli switch 802.11v e 802.11k, il roaming dovrebbe essere uniforme. Di seguito è riportato un esempio di un'acquisizione OTA over-the-air per un evento di roaming:



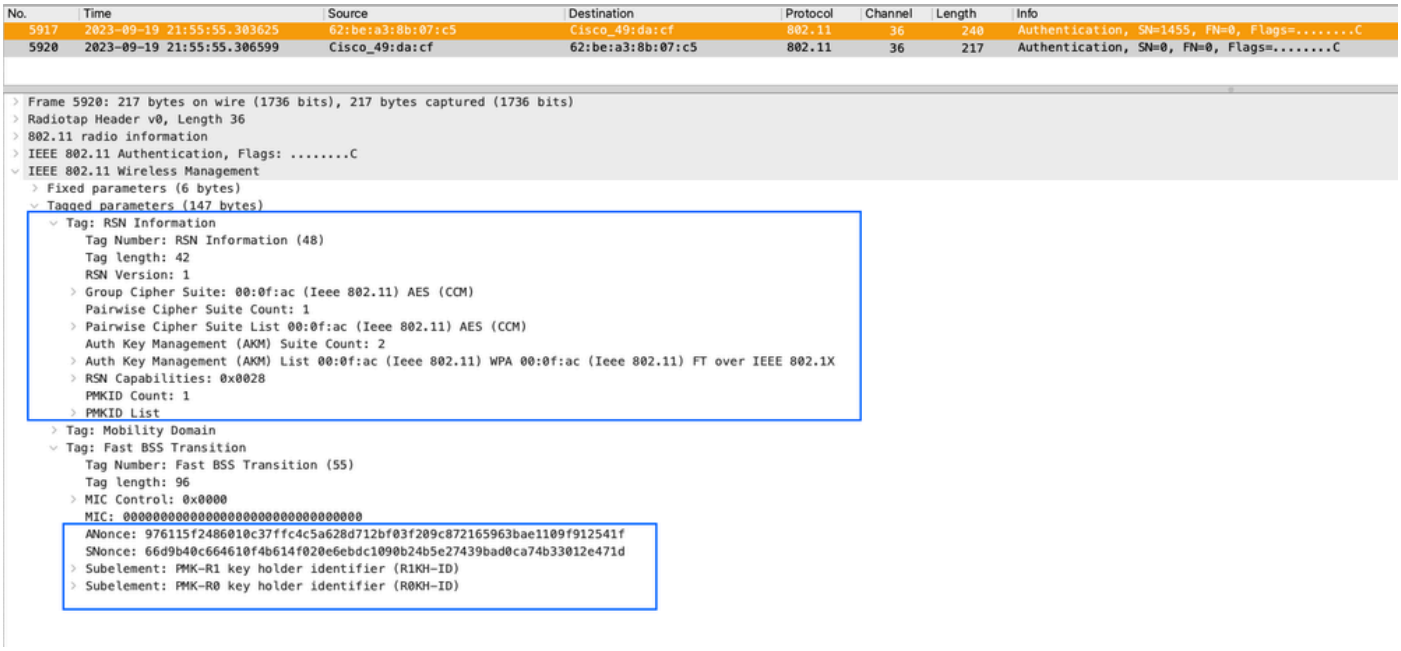
No.	Time	Source	Destination	Protocol	Channel	Length	Info
5917	2023-09-19 21:55:55.303625	62:be:a3:8b:07:c5	Cisco_49:da:cf	802.11	36	240	Authentication, SN=1455, FN=0, Flags=.....C
5918	2023-09-19 21:55:55.303628		62:be:a3:8b:07:c5 (62:be:a…	802.11	36	72	Acknowledgement, Flags=.....C
5920	2023-09-19 21:55:55.306599	Cisco_49:da:cf	62:be:a3:8b:07:c5	802.11	36	217	Authentication, SN=0, FN=0, Flags=.....C
5923	2023-09-19 21:55:55.309552	62:be:a3:8b:07:c5	Cisco_49:da:cf	802.11	36	387	Reassociation Request, SN=1456, FN=0, Flags=.....C, SSID="Roaming-Enabled"
5924	2023-09-19 21:55:55.309560		62:be:a3:8b:07:c5 (62:be:a…	802.11	36	72	Acknowledgement, Flags=.....C
5929	2023-09-19 21:55:55.315721	62:be:a3:8b:07:c5	Broadcast	802.11	36	168	QoS Data, SN=2429, FN=0, Flags=.p....FTC
5931	2023-09-19 21:55:55.315741	Cisco_49:da:cf	62:be:a3:8b:07:c5	802.11	36	442	Reassociation Response, SN=1, FN=0, Flags=.....C
5933	2023-09-19 21:55:55.315749	62:be:a3:8b:07:c5	Broadcast	802.11	36	88	Data, SN=0, FN=0, Flags=.p....F.C
5934	2023-09-19 21:55:55.318767	62:be:a3:8b:07:c5	Cisco_49:da:cf	802.11	36	158	Action, SN=1457, FN=0, Flags=.....C
5935	2023-09-19 21:55:55.318771		62:be:a3:8b:07:c5 (62:be:a…	802.11	36	72	Acknowledgement, Flags=.....C
5936	2023-09-19 21:55:55.319061	62:be:a3:8b:07:c5	Cisco_49:da:cf	802.11	36	92	QoS Null function (No data), SN=1458, FN=0, Flags=o.....TC
5937	2023-09-19 21:55:55.319066		62:be:a3:8b:07:c5 (62:be:a…	802.11	36	72	Acknowledgement, Flags=.....C
5938	2023-09-19 21:55:55.319868	62:be:a3:8b:07:c5	Cisco_49:da:cf	802.11	36	84	Action, SN=1459, FN=0, Flags=.....C, SSID="Roaming-Enabled"
5939	2023-09-19 21:55:55.319871		62:be:a3:8b:07:c5 (62:be:a…	802.11	36	72	Acknowledgement, Flags=.....C
5940	2023-09-19 21:55:55.319874	Cisco_49:da:cf (f1:1d:2d:49:d…	62:be:a3:8b:07:c5 (62:be:a…	802.11	36	61	VHT/HE/EHT/RANGING NDP Announcement, Sounding Dialog Token=238, Flags=.....C
5941	2023-09-19 21:55:55.319877	62:be:a3:8b:07:c5	Cisco_49:da:cf	802.11	36	697	Action No Ack, SN=59, FN=0, Flags=.....C
5942	2023-09-19 21:55:55.319880	Cisco_c6:4a:34	62:be:a3:8b:07:c5	802.11	36	144	QoS Data, SN=0, FN=0, Flags=.p....F.C
5944	2023-09-19 21:55:55.319886	Cisco_c6:4a:34	62:be:a3:8b:07:c5	802.11	36	144	QoS Data, SN=1, FN=0, Flags=.p....F.C
5945	2023-09-19 21:55:55.319891	Cisco_c6:4a:34	62:be:a3:8b:07:c5	802.11	36	144	QoS Data, SN=1, FN=0, Flags=.p..R.F.C

Tracce RA per questo evento di roaming:

```
2023/09/19 21:54:25.912523930 {wncd_x_R0-0}{1}: [client-orch-sm] [15403]: (note): MAC: 62be.a38b.07c5 R
!--- Reassociation Request is received from the client.

2023/09/19 21:54:25.912882280 {wncd_x_R0-0}{1}: [dot11-validate] [15403]: (info): MAC: 62be.a38b.07c5 D
!--- Since 802.11r is enabled, WLC/AP were able to validate/use the PMKID
```

Quando lo standard 802.11r è abilitato, l'handshake iniziale con un nuovo access point viene eseguito prima che il client esegua il roaming al punto di accesso di destinazione. Questo concetto è denominato Fast Transition. L'handshake iniziale consente a un client e ai punti di accesso di eseguire in anticipo il calcolo Pairwise Transient Key (PTK). Le seguenti chiavi PTK vengono applicate al client e ai punti di accesso dopo che il client ha risposto alla richiesta di riassociazione o allo scambio con il nuovo access point di destinazione:

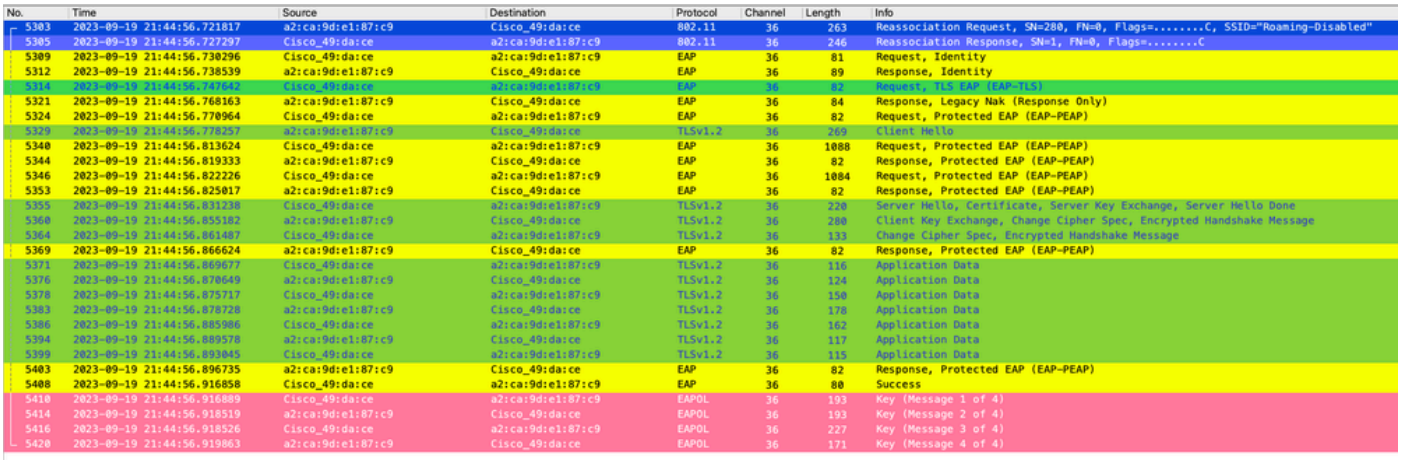



```
2023/09/19 21:54:25.913247615 {wncd_x_R0-0}{1}: [dot11] [15403]: (note): MAC: 62be.a38b.07c5 Associatio
!--- Reassociation Response is sent to the client.

2023/09/19 21:53:59.692212232 {wncd_x_R0-0}{1}: [client-orch-state] [15403]: (note): MAC: 62be.a38b.07c
!--- Client took an IP address and moved to run state.
```

SSID con protocolli di roaming veloce disabilitati (802.11r, 802.11k e 802.11v)

In questo scenario, tutti i protocolli sono disabilitati su un SSID 802.1x; in questo caso, il client usa un'autenticazione completa ogni volta che il client wireless passa da un punto di accesso all'altro. La figura seguente mostra un esempio di scambio over-the-air in cui è possibile vedere che il client non può ignorare lo scambio EAP. Pertanto, è stata eseguita una riautenticazione completa perché nessuno dei metodi di roaming veloce è abilitato:



Protocolli Over-The-Air Disabilitati

Di seguito è riportato un riepilogo delle tracce RA del controller per questo evento di roaming:

```
2023/09/19 21:44:47.425575500 {wncd_x_R0-0}{1}: [client-orch-sm] [15403]: (note): MAC: a2ca.9de1.87c9 R
!--- Reasscoiation Request is received from the client.

2023/09/19 21:44:47.425980179 {wncd_x_R0-0}{1}: [dot11-validate] [15403]: (ERR): MAC: a2ca.9de1.87c9 Fa
!--- Since none of the roam methods are enabled, WLC/AP could not find any PMKID available.

2023/09/19 21:44:47.426252733 {wncd_x_R0-0}{1}: [dot11] [15403]: (note): MAC: a2ca.9de1.87c9 Associatio
!--- Reasscoiation Response is sent to the client.

2023/09/19 21:44:47.444466744 {wncd_x_R0-0}{1}: [dot1x] [15403]: (info): [a2ca.9de1.87c9:capwap_9000000
2023/09/19 21:44:47.444469338 {wncd_x_R0-0}{1}: [dot1x] [15403]: (info): [a2ca.9de1.87c9:capwap_9000000

2023/09/19 21:44:47.444481064 {wncd_x_R0-0}{1}: [dot1x] [15403]: (info): [a2ca.9de1.87c9:capwap_9000000
2023/09/19 21:44:47.471913767 {wncd_x_R0-0}{1}: [dot1x] [15403]: (info): [a2ca.9de1.87c9:capwap_9000000
2023/09/19 21:44:47.471916029 {wncd_x_R0-0}{1}: [dot1x] [15403]: (info): [a2ca.9de1.87c9:capwap_9000000

2023/09/19 21:44:47.475646582 {wncd_x_R0-0}{1}: [radius] [15403]: (info): RADIUS: Received from id 1812

2023/09/19 21:44:47.627108647 {wncd_x_R0-0}{1}: [dot1x] [15403]: (info): [a2ca.9de1.87c9:capwap_9000000

2023/09/19 21:44:47.627110791 {wncd_x_R0-0}{1}: [dot1x] [15403]: (info): [a2ca.9de1.87c9:capwap_9000000

2023/09/19 21:44:47.631319121 {wncd_x_R0-0}{1}: [dot1x] [15403]: (info): [a2ca.9de1.87c9:capwap_9000000

2023/09/19 21:44:47.657492378 {wncd_x_R0-0}{1}: [radius] [15403]: (info): RADIUS: Received from id 1812

2023/09/19 21:44:47.657840708 {wncd_x_R0-0}{1}: [dot1x] [15403]: (info): [a2ca.9de1.87c9:capwap_9000000
!--- Full Reauthentication EAP exchange packets.

2023/09/19 21:44:47.658787303 {wncd_x_R0-0}{1}: [client-keymgmt] [15403]: (info): MAC: a2ca.9de1.87c9 EA

2023/09/19 21:44:47.662831295 {wncd_x_R0-0}{1}: [client-keymgmt] [15403]: (info): MAC: a2ca.9de1.87c9 M

2023/09/19 21:44:47.662931971 {wncd_x_R0-0}{1}: [client-keymgmt] [15403]: (info): MAC: a2ca.9de1.87c9 EA

2023/09/19 21:44:47.665864464 {wncd_x_R0-0}{1}: [client-keymgmt] [15403]: (info): MAC: a2ca.9de1.87c9 M
!--- 4-way handshake in order to compute the PTK/GTK keys.
```

SSID con 802.11k abilitato

Lo standard 802.11k consente ai client di richiedere un report sui router adiacenti contenente informazioni sugli access point idonei per un roaming all'interno del set di servizi. In questo modo i client possono evitare la scansione RF passiva o attiva prima che decidano di passare a un punto di accesso diverso. Il modello C9800 supporta una funzione denominata roami assistito da 11k, che consente di creare e distribuire ai client 802.11k un elenco ottimizzato di router adiacenti. L'elenco di router adiacenti 802.11k viene generato su richiesta e può essere diverso per due client su access point diversi, in quanto il WLC considererebbe la relazione di RF tra il singolo client e gli access point circondati.

I client che non supportano il protocollo 82.11k non inviano richieste di elenco dei router adiacenti.

In questo modo è possibile ottimizzare la previsione per tali client. Di conseguenza, un elenco di router adiacenti viene archiviato nella struttura di dati del software della stazione mobile su C9800.

I client inviano le richieste per gli elenchi di router adiacenti solo dopo l'associazione ai punti di accesso che annunciano l'elemento di informazioni sulle funzionalità RM (IE) nel beacon. La figura seguente mostra un esempio di frame in azione 802.11k dopo che il client è stato associato al punto di accesso:

```
> 802.11 radio information
> IEEE 802.11 Action, Flags: ........C
v IEEE 802.11 Wireless Management
  v Fixed parameters
      Category code: Radio Measurement (5)
      Action code: Neighbor Report Response (5)
      Dialog token: 42
  v Tagged parameters (90 bytes)
    v Tag: Neighbor Report
        Tag Number: Neighbor Report (52)
        Tag length: 13
        BSSID: Cisco_7f:a2:2f (14:16:9d:7f:a2:2f)
      > BSSID Information: 0x000002f7
        Operating Class: 115
        Channel Number: 36 (iterative measurements on that Channel Number)
        PHY Type: 0x07
    v Tag: Neighbor Report
        Tag Number: Neighbor Report (52)
        Tag length: 13
        BSSID: Cisco_b9:35:ee (d4:78:9b:b9:35:ee)
      > BSSID Information: 0x000002f7
        Operating Class: 121
        Channel Number: 140 (iterative measurements on that Channel Number)
        PHY Type: 0x07
    v Tag: Neighbor Report
        Tag Number: Neighbor Report (52)
        Tag length: 13
        BSSID: Cisco_1a:10:ce (d4:e8:80:1a:10:ce)
      > BSSID Information: 0x000002f7
        Operating Class: 121
        Channel Number: 128 (iterative measurements on that Channel Number)
        PHY Type: 0x07
    v Tag: Neighbor Report
        Tag Number: Neighbor Report (52)
        Tag length: 13
        BSSID: Cisco_2b:a5:0e (00:f6:63:2b:a5:0e)
      > BSSID Information: 0x000002f7
        Operating Class: 125
        Channel Number: 161 (iterative measurements on that Channel Number)
        PHY Type: 0x07
    v Tag: Neighbor Report
        Tag Number: Neighbor Report (52)
        Tag length: 13
        BSSID: Cisco_c9:be:2e (a0:23:9f:c9:be:2e)
      > BSSID Information: 0x000002f7
        Operating Class: 118
        Channel Number: 64 (iterative measurements on that Channel Number)
        PHY Type: 0x07
    v Tag: Neighbor Report
        Tag Number: Neighbor Report (52)
        Tag length: 13
        BSSID: Cisco_99:2b:0e (40:01:7a:99:2b:0e)
      > BSSID Information: 0x000002f7
        Operating Class: 118
        Channel Number: 52 (iterative measurements on that Channel Number)
        PHY Type: 0x07
```

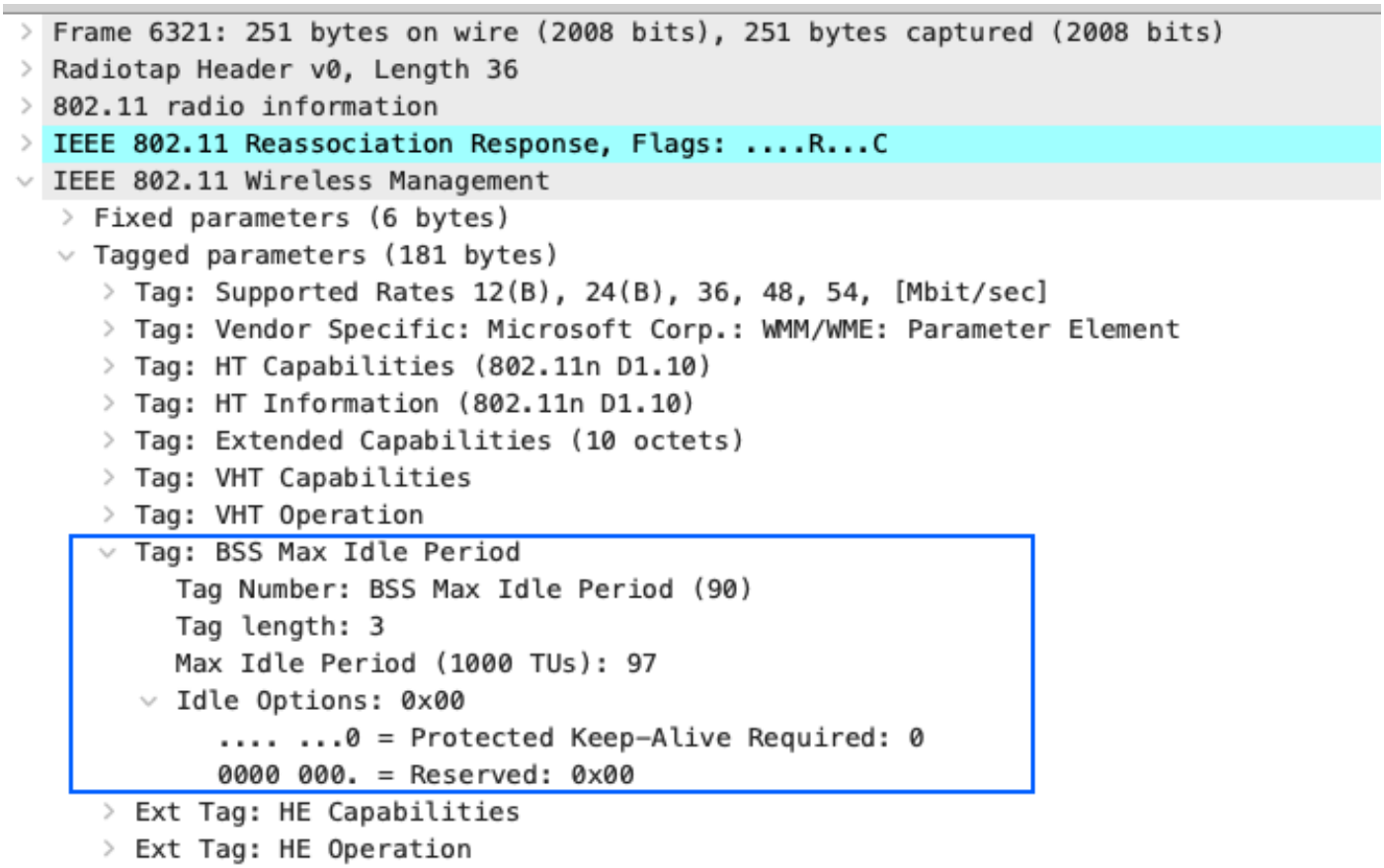
Rapporto Over-The-Air Neighbor

SSID con 802.11v abilitato

Con lo standard 802.11v, i due principali miglioramenti apportati alla gestione delle reti wireless includono:

- Funzione di risparmio energia assistita dalla rete: migliora le prestazioni della batteria del client con un periodo di inattività massimo, che indica la durata in cui il client può rimanere in modalità di sospensione senza alcun frame di dati inviato. Il client riceve una notifica relativa al periodo di inattività massimo tramite frame di associazione e disassociazione.

Se un punto di accesso non riceve i frame da un client wireless per un determinato periodo di tempo, presuppone che il client abbia lasciato la rete e lo dissocia. Il periodo di inattività massimo BSS indica il periodo di tempo durante il quale un punto di accesso può mantenere un client associato senza dover ricevere alcun frame (il client può rimanere in modalità di sospensione, risparmiando così la batteria). Questo valore viene inviato al client wireless tramite il frame di risposta di associazione e riassociazione. La figura seguente mostra il valore nella risposta di riassociazione dal punto di accesso, dove il periodo di inattività massimo BSS è specificato in unità di tempo. Ogni volta che l'unità è uguale a 1.024 millisecondi:



Valore periodo BSS over-the-air

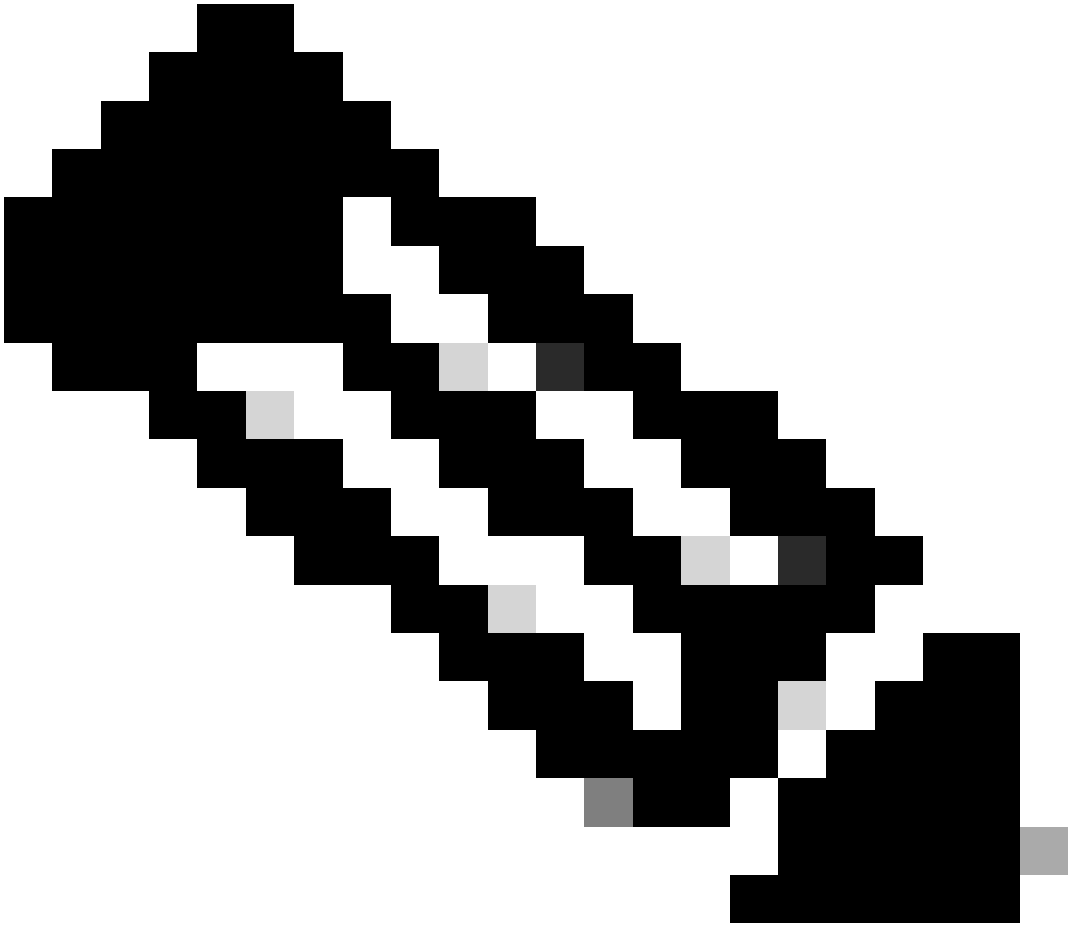
- Roam basato sulla rete: consente all'infrastruttura wireless di suggerire che il client si allontani dal punto di accesso corrente. In questo modo, il client ottiene l'elenco dei punti di accesso ai quali può eseguire il roaming nello stesso set di servizi estesi (ESS, Extended Service Set).

I frame di gestione della transizione BSS 802.11v vengono scambiati in tre scenari:

1. Richiesta sollecitata: prima della transizione a un nuovo punto di accesso, il client è in grado di inviare una query di gestione della transizione BSS 802.11v per individuare le migliori opzioni dei punti di accesso a cui riassociarsi e l'access point corrente a cui il client è connesso, rispondere con una richiesta di gestione della transizione BSS che fornisce l'elenco dei punti di accesso candidati a cui effettuare il roaming.

2. Richiesta di bilanciamento del carico non richiesta: funzionalità che consente all'access point di bilanciare il carico tra i client sullo stesso controller per evitare il sovraccarico dell'access point. Quando il numero di client supera la soglia di bilanciamento del carico configurata per un punto di accesso, qualsiasi nuovo client che tenti di associarsi all'punto di accesso viene rifiutato con una risposta di associazione con stato 17 (punto di accesso occupato). In genere, i client non autorizzati tentano di associarsi allo stesso access point caricato anche dopo che il client ha ricevuto un rifiuto di associazione, ovvero se dal punto di vista RSSI l'access point è l'opzione migliore. Si considerino, ad esempio, 40 utenti in una sala conferenze servita da un unico punto di accesso. Con una query 802.11v BSS Transition Management, un errore di bilanciamento del carico può essere gestito in modo più efficiente quando l'access point invia un elenco di access point candidati a cui effettuare il roaming.

3. Richiesta di roaming ottimizzata non richiesta: i client wireless devono eseguire la scansione di RF e il roaming verso l'access point con il segnale più alto. Tuttavia, alcuni client hanno un comportamento permanente quando rimangono con l'access point a cui sono associati, anche quando un access point vicino fornisce un segnale più forte. Questo problema è noto come problema del client permanente. Per risolvere questo problema, il controller 9800 supporta una funzione denominata roaming ottimizzato in cui vengono monitorati gli RSSI dei pacchetti di dati e della velocità dei dati del client e il client viene disassociato in modo proattivo. La richiesta di gestione della transizione BSS 802.11v migliora il roaming ottimizzato che comunica al client l'imminente dissociazione e fornisce un elenco di access point a cui effettuare il roaming.



Nota: dall'esperienza TAC, il roaming ottimizzato non è adatto a tutte le reti. Assicurati che la copertura tra i punti di accesso sia sufficiente per far funzionare il sistema come previsto, altrimenti potrebbero sorgere altri problemi se lo abiliti.

Una richiesta di gestione della transizione BSS 802.11v che, quando inviata da un punto di accesso a un client, è solo un suggerimento. Il cliente può accettare il suggerimento o ignorarlo. Il controller wireless 9800 fornisce un'opzione di configurazione denominata Imminent Disassociation che consente di forzare i client a dissociarsi se il client non si riassocia a un altro access point entro un intervallo di tempo definito. è possibile configurarla solo dalla CLI con il comando bss-transition disassociation-imminent in uno specifico profilo WLAN.

Informazioni correlate

- Transizione rapida BSS 802.11r
- Elenco router adiacenti e roaming assistito 802.11k
- 802.11v BSS

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).