Comprensión de Fast Roams 802.11r/11k/11v en WLC 9800

Contenido

Introducción

Este documento describe los diferentes resultados cuando los métodos de roaming rápido están habilitados/inhabilitados en los clientes inalámbricos.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Fundamentos de WLAN IEEE 802.11.
- Seguridad WLAN IEEE 802.11.
- Aspectos básicos de IEEE 802.1X/EAP.
- IEEE 802.11r: BSS Fast Transition.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Controlador Cisco Wireless 9800-L IOS® XE 17.9.4
- Punto de acceso Cisco Catalyst serie 9130AXI.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Este documento le ayuda a comprender la diferencia cuando tiene los protocolos 802.11r, 802.11v y 802.11k habilitados en un controlador inalámbrico 9800. También explica cuál es el impacto en los clientes cuando los tiene inhabilitados.

802.11r, 802.11v y 802.11k son estándares o enmiendas diferentes dentro de la familia 802.11 de protocolos de red inalámbrica.

802.11r: Es la transición rápida entre los conjuntos de servicios básicos que introduce un nuevo concepto en el que el intercambio de señales inicial con un nuevo punto de acceso se realiza incluso antes de que el cliente se traslade al punto de acceso de destino.

Resulta especialmente útil en entornos en los que la conectividad ininterrumpida es crucial, como en aplicaciones de transmisión de voz sobre IP o en tiempo real con vídeo o con un monitor de transmisión constante.

Con una red 802.11r optimizada, los dispositivos pueden desplazarse entre los puntos de acceso sin experimentar interrupciones o caídas significativas en la conectividad de red.

802.11k: Neighbor List and Assisted Roam (Medición de recursos de radio) aprovecha las funciones de la gestión de recursos de radio para mejorar el rendimiento y la fiabilidad generales de las redes inalámbricas.

Optimiza los recursos de radio disponibles en los que los puntos de acceso recopilan y comparten información sobre su entorno de radio. Esta información incluye el uso del canal, la potencia de la señal y los niveles de interferencia.

Luego, los dispositivos cliente pueden utilizarlo para tomar decisiones más informadas sobre a qué AP conectarse; lo que se traduce en un mejor equilibrio de carga, una reducción de las interferencias y una mayor eficacia de la red.

802.11v: es un ahorro de energía asistido por red que ayuda a los clientes a mejorar la duración de la batería, lo que les permite dormir más tiempo.

También se centra en cómo mejorar la eficiencia y la gestión de las redes inalámbricas. Esto, a su vez, permite un mejor control y coordinación entre la infraestructura de la red y los dispositivos del cliente cuando los clientes se desplazan.

Las funciones principales son los informes de vecinos, las transiciones de conjuntos de servicios, el equilibrio de carga y el ahorro de energía con ayuda de la red. Estas funciones mejoran la detección, selección y supervisión de la red del cliente.

También permite que los puntos de acceso animen a los dispositivos cliente a desplazarse en

lugar de esperar a que el dispositivo tome una decisión sobre la itinerancia.

Mientras que 802.11r se centra en la transición fluida entre los puntos de acceso, 802.11v pretende mejorar las capacidades de gestión de la red.

El estándar 802.11k está diseñado para optimizar la utilización de los recursos de radio para mejorar el rendimiento y la fiabilidad.

Algunas de las afirmaciones de este documento provienen del libro Comprensión y solución de problemas de los controladores de red inalámbrica de Cisco Catalyst serie 9800, capítulo 6, sección Itinerancia de 802.11.

Roams de seguridad de nivel superior

Cuando el SSID se configura con una seguridad de nivel superior L2 sobre la autenticación básica de sistema abierto 802.11, se requieren más tramas para la asociación inicial y cuando los clientes se desplazan.

Los dos métodos de seguridad más comunes estandarizados e implementados para WLAN 802.11 son:

- WPA/WPA2/WPA3 Personal: Se utiliza una PSK para autenticar los clientes.
- WPA/WPA2/WPA3 Enterprise: El método de protocolo de autenticación extensible (EAP) y 802.1x se utiliza para autenticar los clientes inalámbricos, que es validar las credenciales del usuario (nombre de usuario y contraseña), certificados o tokens a través de un servidor AAA.

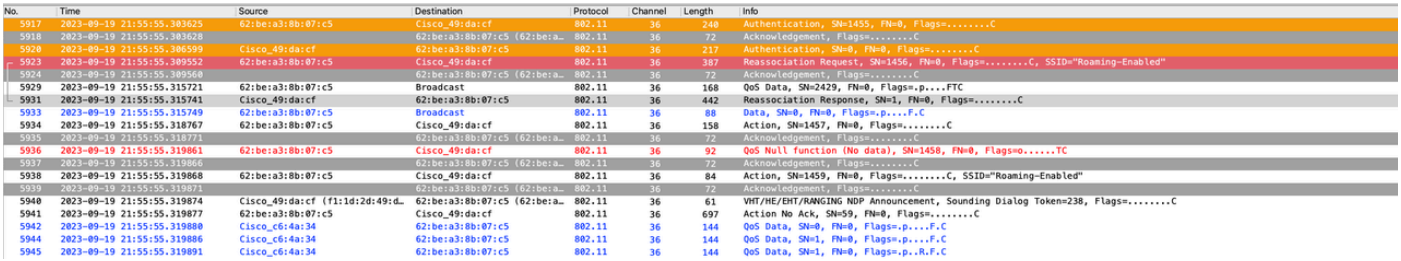
En este documento, se puede utilizar WPA2 Enterprise WLAN con EAP-PEAP para mostrar la diferencia en el uso de los protocolos IEEE (802.11r, 802.11k y 802.11v) y cómo podría afectar a los intentos de roaming inalámbrico.

SSID con protocolos de itinerancia rápida habilitados (802.11r, 802.11k y 802.11v)

La configuración WLAN predeterminada tiene cada protocolo habilitado de forma predeterminada. En el laboratorio, el cliente inalámbrico intenta desplazarse entre 9130 puntos de acceso.

Dado que tiene la configuración predeterminada de la WLAN (se habilita la itinerancia rápida además de 802.11v y 802.11k), espera una itinerancia perfecta.

A continuación se muestra un ejemplo de una captura OTA inalámbrica para un evento de 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 21:55:55.319861	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 21:55:55.319866		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

Estos son los rastros de RA para este evento de itinerancia:

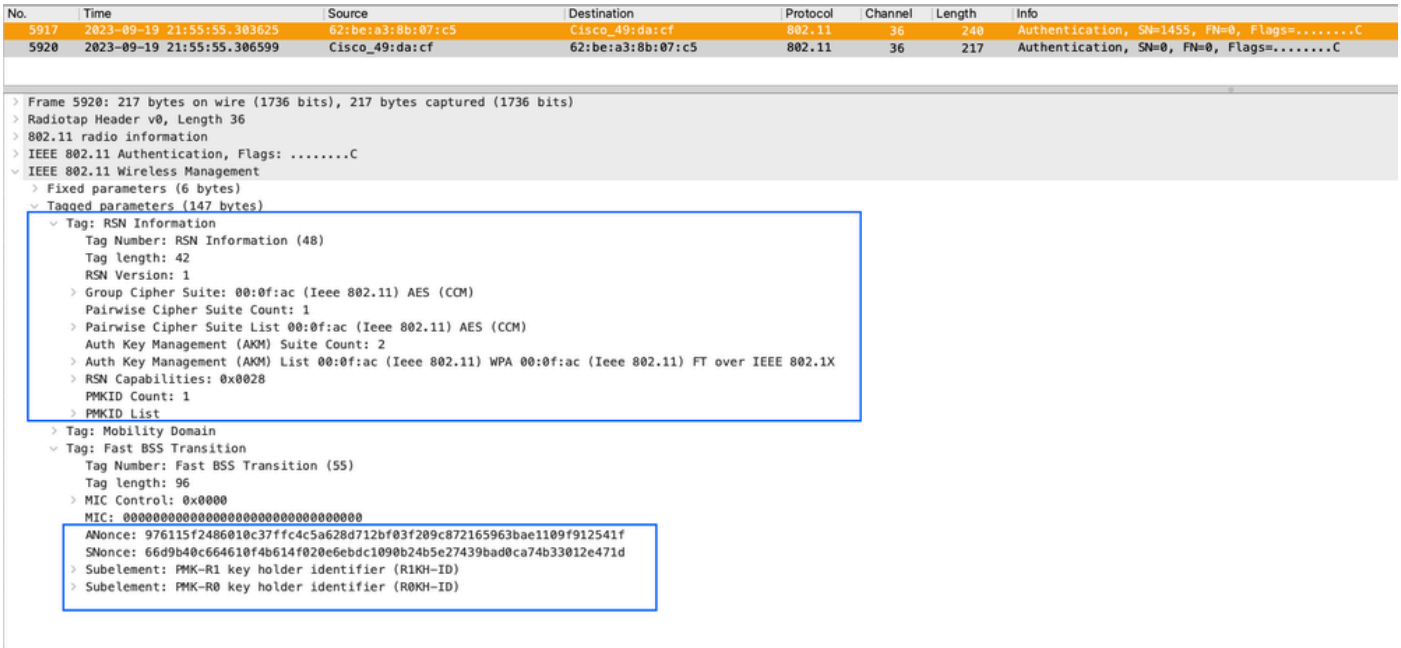
```
2023/09/19 21:54:25.912523930 {wncd_x_R0-0}{1}: [client-orch-sm] [15403]: (note): MAC: 62be.a38b.07c5 R
!--- Reassociation Request is received from the client.

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
```

A medida que se habilita 802.11r, el protocolo de enlace inicial con un nuevo punto de acceso se realiza incluso antes de que el cliente se traslade al punto de acceso de destino. Este concepto se denomina transición rápida.

El protocolo de enlace inicial permite al cliente y a los puntos de acceso realizar el cálculo de clave transitoria en pares (PTK) por adelantado.

Estas claves PTK se aplican al cliente y a los puntos de acceso después de que el cliente responda a la solicitud de reasociación o responda al intercambio con el nuevo AP de destino:



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
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

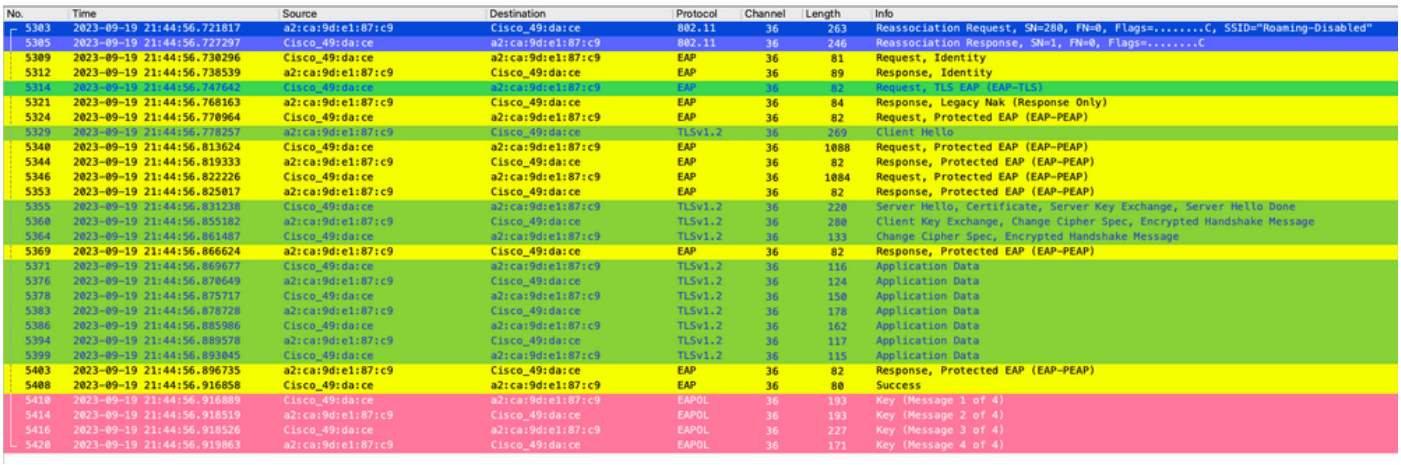
```
> Frame 5920: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 Authentication, Flags: ........C
v IEEE 802.11 Wireless Management
  > Fixed parameters (6 bytes)
  v Tagged parameters (147 bytes)
    v Tag: RSN Information
        Tag Number: RSN Information (48)
        Tag length: 42
        RSN Version: 1
      > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
        Pairwise Cipher Suite Count: 1
      > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
        Auth Key Management (AKM) Suite Count: 2
      > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) WPA 00:0f:ac (Ieee 802.11) FT over IEEE 802.1X
      > RSN Capabilities: 0x0028
        PMKID Count: 1
      > PMKID List
    > Tag: Mobility Domain
    v Tag: Fast BSS Transition
        Tag Number: Fast BSS Transition (55)
        Tag length: 96
      > MIC Control: 0x0000
        MIC: 00000000000000000000000000000000
        ANonce: 976115f2486010c37ffc4c5a628d712bf03f209c872165963bae1109f912541f
        SNonce: 66d9b40c664610f4b614f020e6ebdc1090b24b5e27439bad0ca74b33012e471d
      > Subelement: PMK-R1 key holder identifier (R1KH-ID)
      > Subelement: PMK-R0 key holder identifier (R0KH-ID)
```

```
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 protocolos de itinerancia rápida desactivados (802.11r, 802.11k y 802.11v)

En esta situación, todos los protocolos están desactivados en un SSID 802.1x. En este caso, el cliente experimenta una autenticación completa cada vez que el cliente inalámbrico se traslada entre los puntos de acceso; la siguiente figura muestra un ejemplo de un intercambio por aire donde puede ver que el cliente no pudo omitir el intercambio EAP. Por lo tanto, se realizó una reautenticación completa porque ninguno de los métodos de roaming rápido está habilitado:



No.	Time	Source	Destination	Protocol	Channel	Length	Info
5303	2023-09-19 21:44:56.721817	a2:ca:9d:e1:87:c9	Cisco_49:da:ce	802.11	36	263	Reassociation Request, SN=280, FN=0, Flags=.....C, SSID="Roaming-Disabled"
5305	2023-09-19 21:44:56.727297	Cisco_49:da:ce	a2:ca:9d:e1:87:c9	802.11	36	246	Reassociation Response, SN=1, FN=0, Flags=.....C
5309	2023-09-19 21:44:56.730296	Cisco_49:da:ce	a2:ca:9d:e1:87:c9	EAP	36	81	Request, Identity
5312	2023-09-19 21:44:56.738539	a2:ca:9d:e1:87:c9	Cisco_49:da:ce	EAP	36	89	Response, Identity
5314	2023-09-19 21:44:56.747642	Cisco_49:da:ce	a2:ca:9d:e1:87:c9	EAP	36	82	Request, TLS EAP (EAP-TLS)
5321	2023-09-19 21:44:56.768163	a2:ca:9d:e1:87:c9	Cisco_49:da:ce	EAP	36	84	Response, Legacy Nak (Response Only)
5324	2023-09-19 21:44:56.770964	Cisco_49:da:ce	a2:ca:9d:e1:87:c9	EAP	36	82	Request, Protected EAP (EAP-PEAP)
5329	2023-09-19 21:44:56.778257	a2:ca:9d:e1:87:c9	Cisco_49:da:ce	TLSv1.2	36	269	Client Hello
5340	2023-09-19 21:44:56.813624	Cisco_49:da:ce	a2:ca:9d:e1:87:c9	EAP	36	1088	Request, Protected EAP (EAP-PEAP)
5344	2023-09-19 21:44:56.819333	a2:ca:9d:e1:87:c9	Cisco_49:da:ce	EAP	36	82	Response, Protected EAP (EAP-PEAP)
5346	2023-09-19 21:44:56.822226	Cisco_49:da:ce	a2:ca:9d:e1:87:c9	EAP	36	1084	Request, Protected EAP (EAP-PEAP)
5353	2023-09-19 21:44:56.825017	a2:ca:9d:e1:87:c9	Cisco_49:da:ce	EAP	36	82	Response, Protected EAP (EAP-PEAP)
5355	2023-09-19 21:44:56.831238	Cisco_49:da:ce	a2:ca:9d:e1:87:c9	TLSv1.2	36	220	Server Hello, Certificate, Server Key Exchange, Server Hello Done
5360	2023-09-19 21:44:56.855182	a2:ca:9d:e1:87:c9	Cisco_49:da:ce	TLSv1.2	36	280	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
5364	2023-09-19 21:44:56.861487	Cisco_49:da:ce	a2:ca:9d:e1:87:c9	TLSv1.2	36	133	Change Cipher Spec, Encrypted Handshake Message
5369	2023-09-19 21:44:56.866624	a2:ca:9d:e1:87:c9	Cisco_49:da:ce	EAP	36	82	Response, Protected EAP (EAP-PEAP)
5371	2023-09-19 21:44:56.869677	Cisco_49:da:ce	a2:ca:9d:e1:87:c9	TLSv1.2	36	116	Application Data
5376	2023-09-19 21:44:56.870649	a2:ca:9d:e1:87:c9	Cisco_49:da:ce	TLSv1.2	36	124	Application Data
5378	2023-09-19 21:44:56.875717	Cisco_49:da:ce	a2:ca:9d:e1:87:c9	TLSv1.2	36	150	Application Data
5383	2023-09-19 21:44:56.878728	a2:ca:9d:e1:87:c9	Cisco_49:da:ce	TLSv1.2	36	178	Application Data
5386	2023-09-19 21:44:56.885986	Cisco_49:da:ce	a2:ca:9d:e1:87:c9	TLSv1.2	36	162	Application Data
5394	2023-09-19 21:44:56.889578	a2:ca:9d:e1:87:c9	Cisco_49:da:ce	TLSv1.2	36	117	Application Data
5399	2023-09-19 21:44:56.893045	Cisco_49:da:ce	a2:ca:9d:e1:87:c9	TLSv1.2	36	115	Application Data
5403	2023-09-19 21:44:56.896735	a2:ca:9d:e1:87:c9	Cisco_49:da:ce	EAP	36	82	Response, Protected EAP (EAP-PEAP)
5408	2023-09-19 21:44:56.916858	Cisco_49:da:ce	a2:ca:9d:e1:87:c9	EAP	36	80	Success
5410	2023-09-19 21:44:56.916889	Cisco_49:da:ce	a2:ca:9d:e1:87:c9	EAPOL	36	193	Key (Message 1 of 4)
5414	2023-09-19 21:44:56.918519	a2:ca:9d:e1:87:c9	Cisco_49:da:ce	EAPOL	36	193	Key (Message 2 of 4)
5416	2023-09-19 21:44:56.918526	Cisco_49:da:ce	a2:ca:9d:e1:87:c9	EAPOL	36	227	Key (Message 3 of 4)
5420	2023-09-19 21:44:56.919863	a2:ca:9d:e1:87:c9	Cisco_49:da:ce	EAPOL	36	171	Key (Message 4 of 4)

Protocolos de transmisión por aire desactivados

A continuación se muestra un resumen de los seguimientos RA del controlador para este evento de 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 activado

El estándar 802.11k permite a los clientes solicitar un informe de vecino que contenga información sobre los AP que son buenos candidatos para una itinerancia dentro del conjunto de servicios.

Esto permite a los clientes evitar el escaneo de RF pasivo o activo antes de que el cliente decida trasladarse a un punto de acceso diferente.

El C9800 admite una función denominada itinerancia asistida de 11k, que crea y ofrece una lista de vecinos optimizada para los clientes 802.11k.

La lista de vecinos 802.11k se genera a demanda y puede ser diferente para dos clientes en AP diferentes porque el WLC consideraría la relación de RF individual del cliente con los AP rodeados.

Los clientes que no admiten el protocolo 82.11k, no envían solicitudes de lista de vecinos. Esto permite optimizar la predicción para ayudar a esos clientes.

Como resultado, una lista de vecinos se almacena en la estructura de datos del software de la estación móvil en C9800.

Los clientes envían solicitudes de listas de vecinos solo después de asociarse con los puntos de acceso que anuncian el elemento de información de capacidad (IE) de RM en la baliza.

La siguiente figura es un ejemplo de tramas de acción 802.11k después de que el cliente se asociara con el punto de acceso:

```
> 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
```

Informe de vecino por aire

SSID con 802.11v activado

Con el estándar 802.11v, las dos mejoras principales en la gestión de redes inalámbricas incluyen:

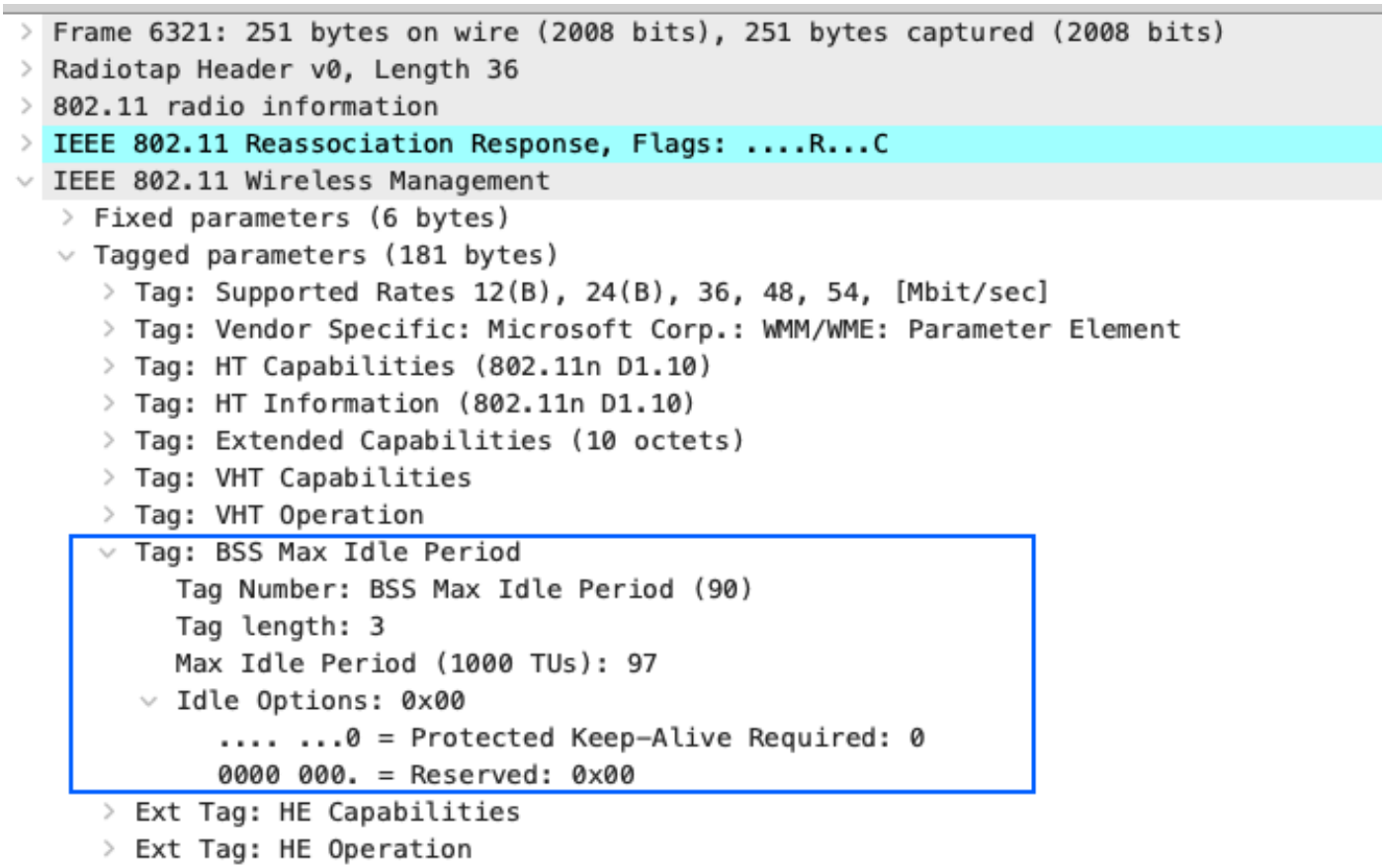
- Función de ahorro de energía asistido por red: Mejora el rendimiento de la batería del cliente con un período de inactividad máximo, que indica la duración en la que un cliente puede permanecer en modo de suspensión sin enviar ninguna trama de datos. Se notifica al cliente acerca de este período de inactividad máximo a través de tramas de asociación y desasociación.

Si un punto de acceso no recibe tramas de un cliente inalámbrico durante un determinado período de tiempo, asume que el cliente abandonó la red y la desasocia.

El período de inactividad máximo de BSS es la cantidad de tiempo que un AP puede mantener a un cliente asociado sin tener que recibir ninguna trama (el cliente puede permanecer dormido, esto ahorra batería).

Este valor se envía al cliente inalámbrico a través de la trama de respuesta de asociación y reasociación.

La siguiente figura muestra el valor de la respuesta de reasociación del punto de acceso, donde el período máximo de inactividad de BSS se especifica en unidades de tiempo. Cada vez que la unidad es igual a 1,024 milisegundos:



Valor del período de BSS aéreo

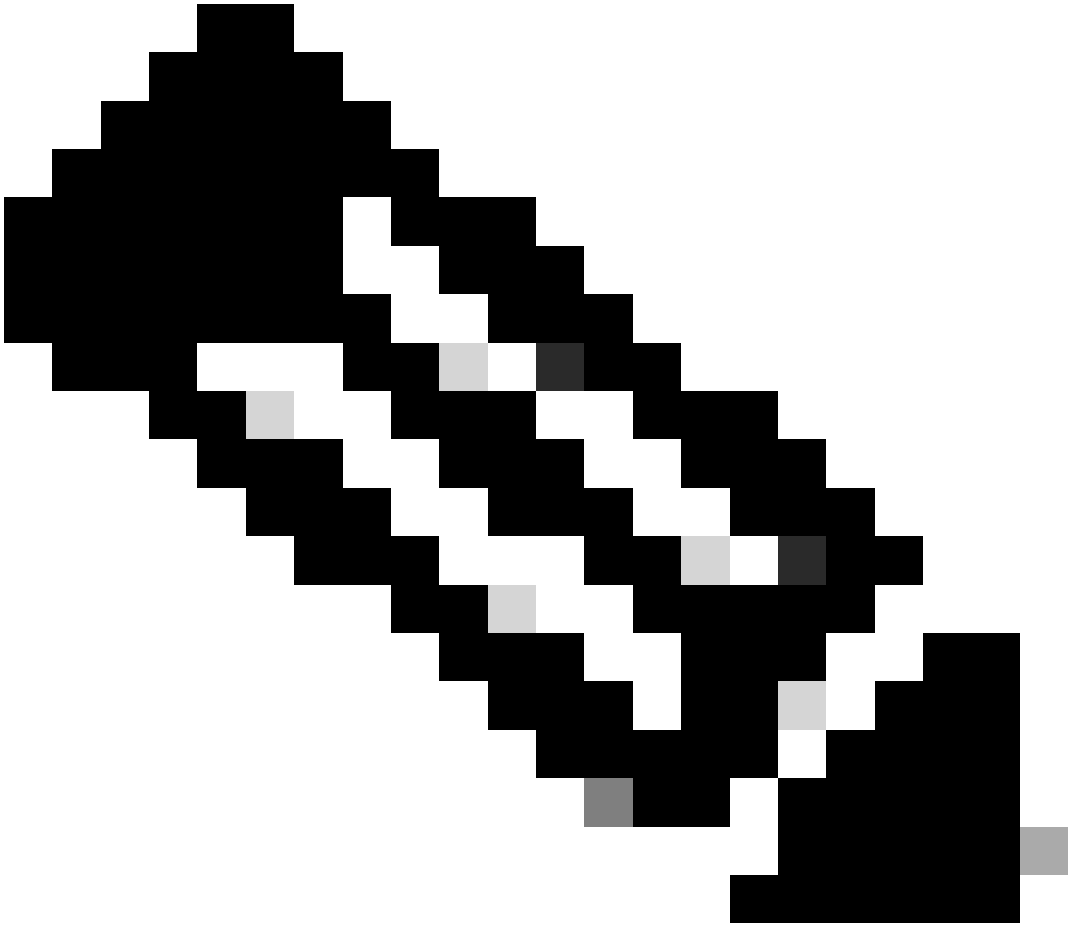
- Itinerancia asistida por la red: habilita la infraestructura inalámbrica para sugerir que el cliente se aleje de su punto de acceso actual. Esto proporciona al cliente la lista de puntos de acceso a los que puede desplazarse en el mismo conjunto de servicios ampliados (ESS).

Las tramas de administración de transición de 802.11v BSS se intercambian en tres escenarios:

1. Solicitud solicitada: Antes de la transición a un nuevo punto de acceso, el cliente tiene la capacidad de enviar una consulta de administración de transición de BSS 802.11v para encontrar mejores opciones de puntos de acceso con los que reasociarse, y el AP actual donde el cliente está conectado, responder con una solicitud de administración de transición de BSS que proporciona la lista de puntos de acceso candidatos a los que vagar.

2. Solicitud de balanceo de carga no solicitada: Esta es una función que permite al AP balancear la carga de los clientes entre los puntos de acceso en el mismo controlador para evitar la sobrecarga de AP. Cuando los recuentos de clientes exceden el umbral de equilibrio de carga configurado para un AP, cualquier cliente nuevo que intente asociarse con el AP es denegado con una respuesta de asociación con el estado 17 (AP ocupado). Normalmente, los clientes denegados intentan asociarse al mismo AP cargado incluso después de que el cliente obtiene un rechazo de asociación, es decir, si desde la perspectiva RSSI, ese AP es su mejor opción. Por ejemplo, considere 40 usuarios en una sala de conferencias atendida por un AP. Con una consulta de administración de transición de BSS 802.11v, un error de equilibrio de carga se puede manejar más fácilmente donde el AP envía una lista de AP candidatos a los cuales se debe trasladar en su lugar.

3. Solicitud de roaming optimizada no solicitada: se espera que los clientes inalámbricos escaneen RF y se trasladen al AP con la señal más alta. Sin embargo, algunos clientes han mostrado un comportamiento pegajoso donde permanecen con el AP al cual están asociados, incluso cuando un AP vecino proporciona una señal más fuerte. Esto se conoce como un problema de cliente persistente. Para resolver este problema, el controlador 9800 admite una función llamada roaming optimizada donde se monitorea el RSSI de los paquetes de datos del cliente y la velocidad de datos, y el cliente se desasocia proactivamente. La petición de administración de transición de BSS 802.11v mejora la itinerancia optimizada, que indica al cliente una desasociación inminente y proporciona una lista de AP a los que vagar.



Nota: Según la experiencia del TAC, la itinerancia optimizada no es adecuada para todas las redes. Asegúrese de que la cobertura sea lo suficientemente buena entre los puntos de acceso para que funcione como se espera; de lo contrario, podrían surgir más problemas si lo habilita.

Una petición de administración de transición BSS 802.11v que cuando es enviada por un AP a un cliente es solamente una sugerencia. El cliente puede aceptar la sugerencia o descartarla. El controlador inalámbrico 9800 proporciona una opción de configuración llamada Inminent Disassociation para que usted obligue a los clientes a desasociarse si el cliente no se vuelve a asociar con otro AP dentro de una ventana de tiempo definida. Puede configurarlo solamente desde CLI mediante el comando bss-transaction disassociation-imminent bajo un perfil WLAN específico.

Información Relacionada

- Transición rápida a 802.11r BSS

- Lista de vecinos 802.11k e itinerancia asistida
- 802.11v BSS
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).