Comprendre les itinéraires rapides 802.11r/11k/11v sur les WLC 9800

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Itinéraires de sécurité de niveau supérieur

SSID avec protocoles d'itinérance rapide activés (802.11r, 802.11k et 802.11v)

SSID avec protocoles d'itinérance rapide désactivés (802.11r, 802.11k et 802.11v)

SSID avec 802.11k activé

SSID avec 802.11v activé

Informations connexes

Introduction

Ce document décrit les différents résultats lorsque les méthodes d'itinérance rapide sont activées/désactivées sur les clients sans fil.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Principes fondamentaux du WLAN IEEE 802.11.
- Sécurité WLAN IEEE 802.11.
- Notions de base sur IEEE 802.1X/EAP.
- Transition rapide BSS IEEE 802.11r.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleur Cisco Wireless 9800-L IOS® XE 17.9.4
- Point d'accès Cisco Catalyst 9130AXI.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Ce document vous aide à comprendre la différence lorsque les protocoles 802.11r, 802.11v et 802.11k sont activés sur un contrôleur sans fil 9800. Il explique également l'impact sur les clients lorsque vous les désactivez.

Les normes 802.11r, 802.11v et 802.11k sont toutes des normes ou des modifications différentes au sein de la famille de protocoles réseau sans fil 802.11.

- 802.11r : La transition rapide entre les ensembles de services de base introduit un nouveau concept où la connexion initiale avec un nouveau point d'accès est effectuée avant même que le client ne se déplace vers le point d'accès cible. Elle est particulièrement utile dans les environnements où la connectivité ininterrompue est essentielle, par exemple dans les applications de voix sur IP ou de flux en temps réel avec vidéo ou contrôle de flux constant. Avec un réseau 802.11r réglé, les périphériques peuvent se déplacer entre les points d'accès sans subir de perturbations ou de pertes importantes de connectivité réseau.
- 802.11k : Neighbor List and Assisted Roam (Radio Resource Measurement) tire parti des fonctions de gestion des ressources radio pour améliorer les performances et la fiabilité globales des réseaux sans fil. Il optimise les ressources radio disponibles où les points d'accès collectent et partagent des informations sur leur environnement radio. Ces informations incluent l'utilisation du canal, l'intensité du signal et les niveaux d'interférence. Il peut ensuite être utilisé par les périphériques clients pour prendre des décisions plus éclairées sur le point d'accès auquel se connecter ; ce qui permet un meilleur équilibrage de charge, une réduction des interférences et une meilleure efficacité du réseau.
- 802.11v : est une économie d'énergie assistée par réseau qui aide les clients à améliorer l'autonomie de la batterie, ce qui leur permet de dormir plus longtemps. Elle se concentre

également sur la manière d'améliorer l'efficacité et la gestion des réseaux sans fil. Ceci permet à son tour un meilleur contrôle et une meilleure coordination entre l'infrastructure réseau et les périphériques clients lorsque les clients sont en itinérance.

Les principales fonctionnalités sont les rapports de voisinage, les transitions de service, l'équilibrage de charge et l'économie d'énergie assistée par réseau. Ces fonctions améliorent la détection, la sélection et la surveillance du réseau client.

Il permet également aux points d'accès d'encourager les périphériques clients à se déplacer au lieu d'attendre que le périphérique prenne une décision d'itinérance.

Alors que la norme 802.11r se concentre sur la transition transparente entre les points d'accès, la norme 802.11v vise à améliorer les capacités de gestion du réseau.La norme 802.11k est conçue pour optimiser l'utilisation des ressources radio afin d'améliorer les performances et la fiabilité.

Certaines instructions de ce document sont tirées du livre Understanding and Troubleshooting Cisco Catalyst 9800 Series Wireless Controllers du Chapitre 6, section 802.11 Roam.

Itinéraires de sécurité de niveau supérieur

Lorsque le SSID est configuré avec une sécurité de niveau supérieur de couche 2 en plus de l'authentification 802.11 Open System de base, davantage de trames sont nécessaires pour l'association initiale et lorsque les clients sont en itinérance.

Les deux méthodes de sécurité les plus courantes normalisées et mises en oeuvre pour les réseaux locaux sans fil 802.11 sont les suivantes :

- WPA/WPA2/WPA3 personnel : Une clé prépartagée est utilisée pour authentifier les clients.
- WPA/WPA2/WPA3 Entreprise : La méthode EAP (Extensible Authentication Protocol) et la norme 802.1x sont utilisées pour authentifier les clients sans fil, c'est-à-dire pour valider les informations d'identification de l'utilisateur (nom d'utilisateur et mot de passe), les certificats ou les jetons via un serveur AAA.

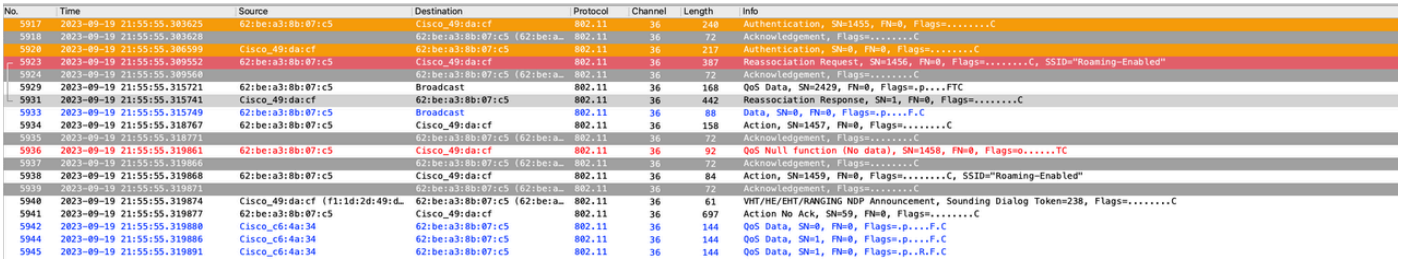
Dans ce document, le WLAN d'entreprise WPA2 peut être utilisé avec EAP-PEAP pour montrer la différence dans l'utilisation des protocoles IEEE (802.11r, 802.11k et 802.11v) et comment il pourrait affecter les tentatives d'itinérance sans fil.

SSID avec protocoles d'itinérance rapide activés (802.11r, 802.11k et 802.11v)

Chaque protocole est activé par défaut dans la configuration WLAN par défaut. Au cours des travaux pratiques, le client sans fil tente de se déplacer entre les points d'accès 9130.

Comme vous disposez de la configuration par défaut du WLAN (l'itinérance rapide est activée en plus des normes 802.11v et 802.11k), vous attendez une itinérance transparente.

Voici un exemple de capture OTA en direct pour un événement d'itinérance :



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

Voici les traces d'annonce de routeur pour cet événement d'itinérance :

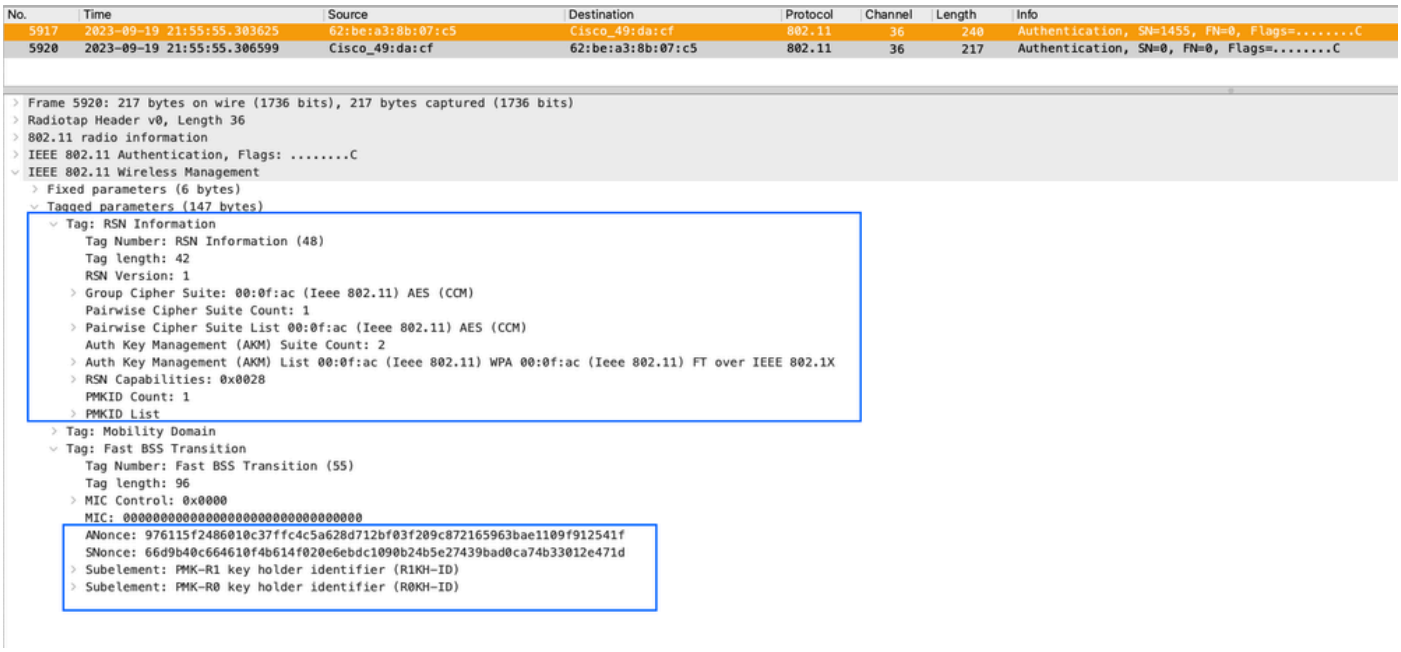
```
2023/09/19 21:54:25.912523930 {wncd_x_R0-0}{1}: [client-orch-sm] [15403]: (note): MAC: 62be.a38b.07c5 R
!--- Reassociation Request is received from the client.

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
```

Comme 802.11r est activé, la connexion initiale avec un nouveau point d'accès est effectuée avant même que le client ne se déplace vers le point d'accès cible. Ce concept est appelé Transition rapide.

La connexion initiale permet à un client et aux points d'accès d'effectuer le calcul PTK (Pairwise Transient Key) à l'avance.

Ces clés PTK sont appliquées au client et aux points d'accès une fois que le client répond à la demande de réassociation ou répond à l'échange avec le nouveau point d'accès cible :



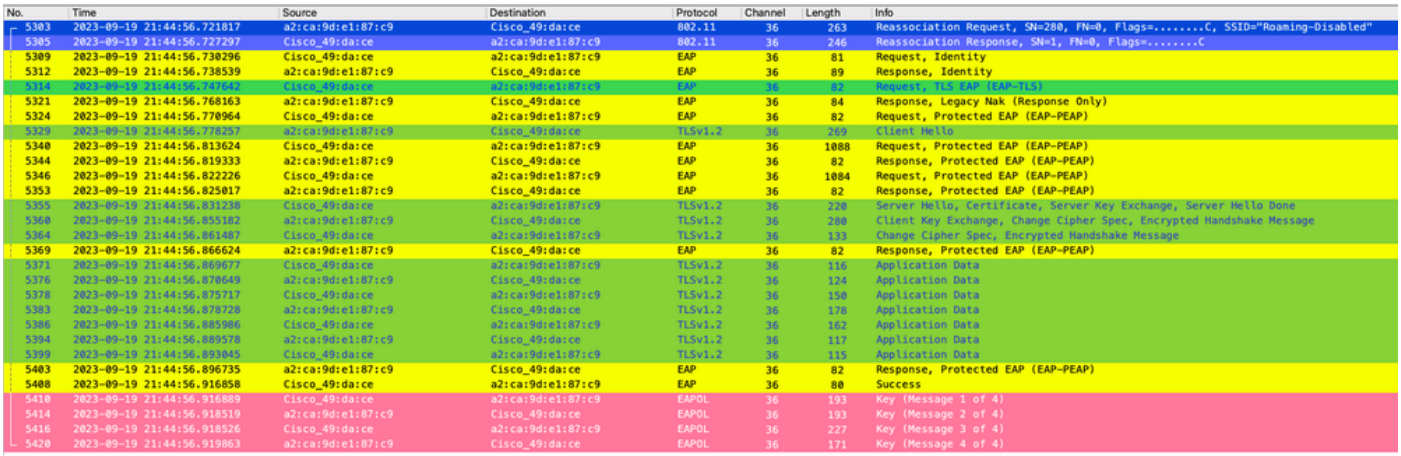

```
2023/09/19 21:54:25.913247615 {wncd_x_R0-0}{1}: [dot11] [15403]: (note): MAC: 62be.a38b.07c5 Associatio
!--- Reassociation Response is sent to the client.

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 avec protocoles d'itinérance rapide désactivés (802.11r, 802.11k et 802.11v)

Dans ce scénario, tous les protocoles sont désactivés sur un SSID 802.1x. Dans ce cas, le client fait l'expérience d'une authentification complète chaque fois que le client sans fil se déplace entre les points d'accès. La figure suivante montre un exemple d'échange sans fil où vous pouvez voir que le client n'a pas pu ignorer l'échange EAP.

Par conséquent, une nouvelle authentification complète a eu lieu car aucune des méthodes d'itinérance rapide n'est activée :



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)

Protocoles de communication radio désactivés

Voici un résumé des traces RA du contrôleur pour cet événement d'itinérance :

```
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 avec 802.11k activé

La norme 802.11k permet aux clients de demander un rapport de voisinage qui contient des informations sur les points d'accès qui sont de bons candidats pour une itinérance dans l'ensemble de services. Cela permet aux clients d'éviter un balayage RF passif ou actif avant qu'ils ne décident de se déplacer vers un autre point d'accès.

Le C9800 prend en charge une fonction appelée 11k assist. Il crée et fournit une liste de voisins optimisée aux clients 802.11k. La liste de voisins 802.11k est générée à la demande et peut être différente pour deux clients sur des AP différents parce que le WLC considérerait la relation RF de client individuel avec les AP entourés.

Les clients qui ne prennent pas en charge le protocole 82.11k n'envoient pas de demandes de liste de voisins. Cela permet une optimisation des prédictions qui aide ces clients.

Par conséquent, une liste de voisins est stockée dans la structure de données du logiciel de station mobile sur C9800.

Les clients envoient des demandes de listes de voisins uniquement après s'être associés aux points d'accès qui annoncent la fonctionnalité RM Information Element (IE) dans la balise.

La figure suivante est un exemple de trames d'action 802.11k après que le client a été associé au point d'accès :

```
> 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
```

Rapport De Voisinage En Direct

SSID avec 802.11v activé

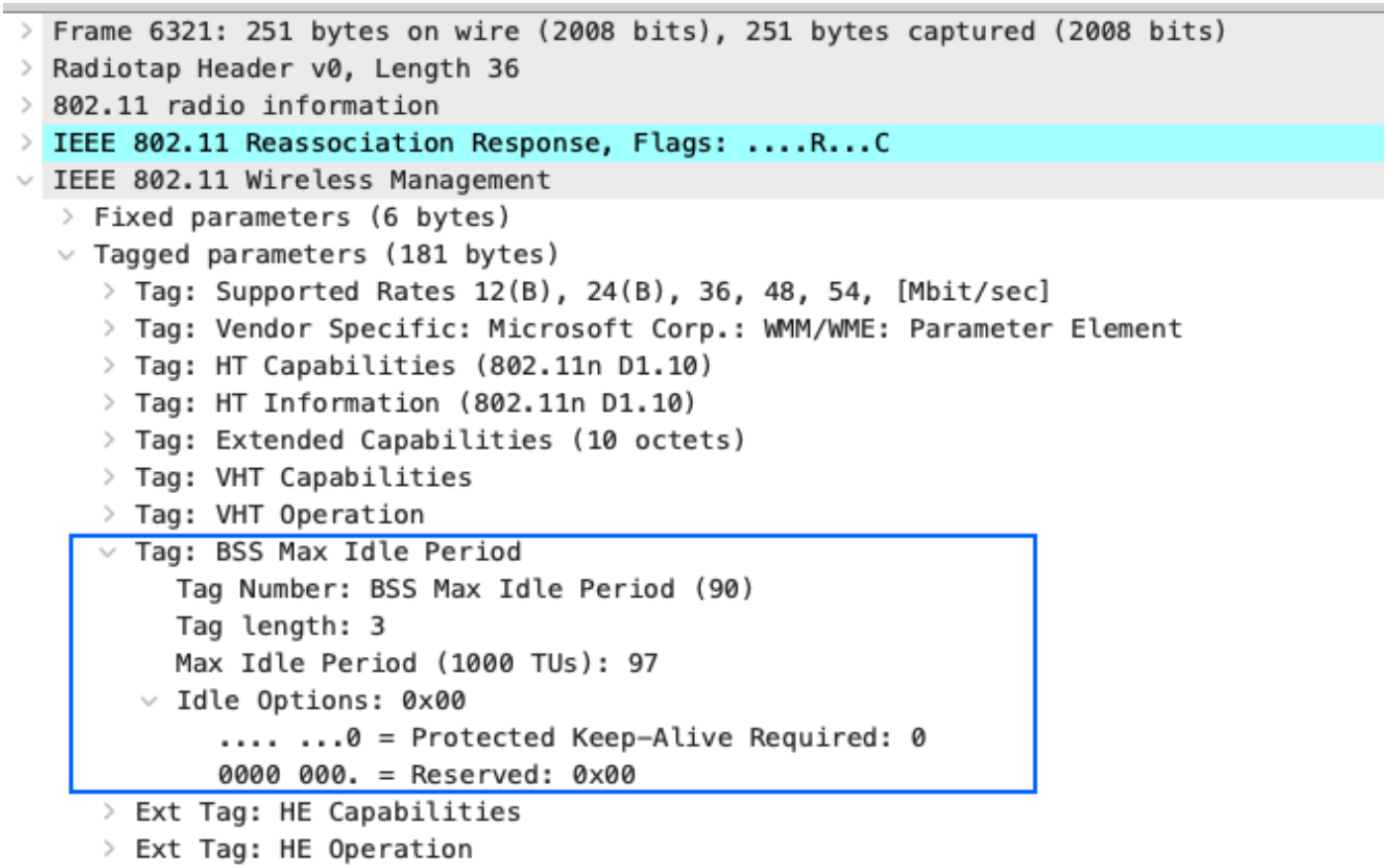
Avec la norme 802.11v, les deux principales améliorations apportées à la gestion du réseau sans fil incluent une fonction d'économie d'énergie assistée par réseau qui améliore les performances de la batterie du client avec une période d'inactivité maximale, qui indique la durée pendant laquelle un client peut rester en mode veille sans qu'aucune trame de données ne soit envoyée. Le client est averti de cette période d'inactivité maximale par le biais de trames d'association et de dissociation.

Si un point d’accès ne reçoit pas de trames d’un client sans fil pendant un certain temps, il suppose que le client a quitté le réseau et le dissocie.

La période d'inactivité BSS Max est la durée pendant laquelle un point d'accès peut maintenir un client associé sans avoir à recevoir de trame (le client peut rester en veille, ce qui économise la batterie).

Cette valeur est envoyée au client sans fil via la trame de réponse d'association et de réassociation.

La figure suivante montre la valeur de la réponse de réassociation du point d'accès, où la période d'inactivité maximale BSS est spécifiée en unités de temps. Chaque fois que l'unité est égale à 1,024 millisecondes :



Valeur de la période BSS en direct

L'itinérance assistée par réseau permet à l'infrastructure sans fil de suggérer au client de s'éloigner de son point d'accès actuel. Cela fournit au client la liste des points d'accès vers lesquels il peut se déplacer dans le même ensemble de services étendus (ESS).

Les trames de gestion de la transition BSS 802.11v sont échangées dans trois scénarios :

1. Demande sollicitée : Avant la transition vers un nouveau point d'accès, le client a la possibilité d'envoyer une requête de gestion de transition BSS 802.11v pour trouver de meilleures options de points d'accès auxquels se réassocier, et le point d'accès actuel auquel le client est connecté répond par une requête de gestion de transition BSS qui fournit la liste des points d'accès candidats vers lesquels se déplacer.

2. Unsolicited load-balance request : Cette fonctionnalité permet au point d'accès d'équilibrer la charge des clients entre les points d'accès sur le même contrôleur pour éviter la surcharge du point d'accès. Lorsque le nombre de clients dépasse le seuil d'équilibrage de charge configuré pour un point d'accès, tout nouveau client qui tente de s'associer au point d'accès est refusé avec une réponse d'association avec l'état 17 (AP occupé). En général, les clients refusés essaient de s'associer au même AP chargé même après que le client a reçu un rejet d'association, c'est-à-dire si du point de vue RSSI, cet AP est leur meilleure option. Prenons l'exemple de 40 utilisateurs dans une salle de conférence desservie par un point d'accès. Avec une requête de gestion de la

transition BSS 802.11v, une panne d'équilibrage de charge peut être gérée plus facilement lorsque le point d'accès envoie une liste de points d'accès candidats vers lesquels se déplacer à la place.

3. Requête d'itinérance optimisée non sollicitée : les clients sans fil sont censés analyser les radiofréquences et se déplacer vers le point d'accès avec le signal le plus élevé. Cependant, certains clients ont affiché un comportement rémanent où ils restent avec le point d'accès auquel ils sont associés, même lorsqu'un point d'accès voisin fournit un signal plus fort. C'est ce qu'on appelle un problème de client rémanent. Pour résoudre ce problème, le contrôleur 9800 prend en charge une fonctionnalité appelée « itinérance optimisée », dans laquelle les RSSI des paquets de données et du débit de données du client sont surveillés et le client est dissocié de manière proactive. La demande de gestion de la transition BSS 802.11v améliore l'itinérance optimisée qui informe le client d'une désassociation imminente et fournit une liste des points d'accès vers lesquels se déplacer.

Remarque : D'après l'expérience du TAC, l'itinérance optimisée ne convient pas à tous les réseaux. Assurez-vous que la couverture est suffisamment bonne entre les points d'accès pour que cela fonctionne comme prévu, sinon d'autres problèmes pourraient survenir si vous l'activez.

Une demande de gestion de transition BSS 802.11v qui, lorsqu'elle est envoyée par un AP à un client, n'est qu'une suggestion. Le client peut honorer la suggestion ou l'ignorer. Le contrôleur sans fil 9800 fournit une option de configuration appelée Désassociation imminente pour vous forcer les clients à se dissocier si le client ne se réassocie pas à un autre AP dans une fenêtre de temps définie. Vous pouvez le configurer uniquement à partir de l'interface de ligne de commande via la commande bss-transition disassociation-imminent sous un profil WLAN spécifique.

Informations connexes

- Transition rapide BSS 802.11r
- Liste de voisins 802.11k et itinérance assistée
- BSS 802.11v
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.