Entender os Fast Roams 802.11r/11k/11v em WLCs 9800

Contents

Introdução

Este documento descreve os diferentes resultados quando os métodos de roaming rápido estão ativados/desativados nos clientes sem fio.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Fundamentos de WLAN do IEEE 802.11.
- IEEE 802.11 Segurança de WLAN.
- Conceitos básicos de IEEE 802.1X/EAP.
- IEEE 802.11r Transição rápida de BSS.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Controlador Cisco Wireless 9800-L IOS® XE 17.9.4
- Ponto de acesso Cisco Catalyst 9130AXI Series.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto

potencial de qualquer comando.

Informações de Apoio

Este documento ajuda você a entender a diferença quando os protocolos 802.11r, 802.11v e 802.11k estão habilitados em um controlador sem fio 9800. Ele também explica o impacto nos clientes quando eles estão desativados.

802.11r, 802.11v e 802.11k são padrões ou emendas diferentes dentro da família 802.11 de protocolos de rede sem fio.

802.11r: É a Transição Rápida em conjuntos de serviços básicos que introduz um novo conceito em que o handshake inicial com um novo AP é feito antes mesmo do cliente fazer roaming para o access point de destino.

Ele é particularmente útil em ambientes onde a conectividade ininterrupta é crucial, como em aplicações de voz sobre IP ou aplicações de fluxo em tempo real com vídeo ou monitor de fluxo constante.

Com uma rede 802.11r ajustada, os dispositivos podem fazer roaming entre pontos de acesso sem a experiência significativa de interrupções ou quedas na conectividade de rede.

802.11k: A Lista de vizinhos e o Roam Assistido (Medição de Recursos de Rádio) aproveitam os recursos de gerenciamento de recursos de rádio para melhorar o desempenho geral e a confiabilidade das redes sem fio.

Ele otimiza os recursos de rádio disponíveis, onde os access points coletam e compartilham informações sobre seu ambiente de rádio. Essas informações incluem o uso do canal, a intensidade do sinal e os níveis de interferência.

Ele pode ser usado por dispositivos clientes para tomar decisões mais informadas sobre a qual AP se conectar; o que resulta em melhor balanceamento de carga, interferência reduzida e eficiência de rede melhorada.

802.11v: é uma economia de energia assistida pela rede que ajuda os clientes a melhorar a vida útil da bateria, o que permite que eles durmam mais.

Também se concentra em como melhorar a eficiência e o gerenciamento de redes sem fio. Isso, por sua vez, permite um melhor controle e coordenação entre a infraestrutura de rede e os dispositivos do cliente quando os clientes fazem roaming.

Os principais recursos são relatórios de vizinhos, transições de conjuntos de serviços, balanceamento de carga e economia de energia assistida pela rede. Esses recursos aprimoram a descoberta, a seleção e o monitoramento da rede do cliente.

Ele também permite que os pontos de acesso incentivem os dispositivos cliente a fazerem roaming, em vez de esperar que o dispositivo tome uma decisão de roaming.

Enquanto o 802.11r se concentra na transição transparente entre APs, o 802.11v tem como

objetivo aprimorar os recursos de gerenciamento de rede.

O 802.11k foi projetado para otimizar a utilização de recursos de rádio para melhorar o desempenho e a confiabilidade.

Algumas instruções neste documento são da seção Compreensão e Troubleshooting de Cisco Catalyst 9800 Series Wireless Controllers Capítulo 6, 802.11 Roam.

Roaming de segurança de nível superior

Quando o SSID é configurado com segurança de nível superior L2 na parte superior da autenticação 802.11 básica do sistema aberto, mais quadros são necessários para a associação inicial e quando os clientes se deslocam.

Os dois métodos de segurança mais comuns padronizados e implementados para as WLANs 802.11 são:

- WPA/WPA2/WPA3 Pessoal: Uma PSK é usada para autenticar os clientes.
- Empresa WPA/WPA2/WPA3: O método EAP (Extensible Authentication Protocol) e o 802.1x são usados para autenticar os clientes sem fio, que é para validar as credenciais do usuário (nome de usuário e senha), certificados ou tokens através de um servidor AAA.

Neste documento, a WPA2 Enterprise WLAN pode ser usada com EAP-PEAP para mostrar a diferença no uso dos protocolos IEEE (802.11r, 802.11k e 802.11v) e como isso poderia afetar as tentativas de roaming sem fio.

SSID com protocolos Fast Roam ativados (802.11r, 802.11k e 802.11v)

A configuração padrão da WLAN tem todos os protocolos habilitados por padrão. No laboratório, o cliente sem fio tenta fazer roaming entre 9.130 pontos de acesso.

Como você tem a configuração padrão da WLAN (o roam rápido é habilitado além do 802.11v e 802.11k), espera-se um roam contínuo.

Aqui está um exemplo de uma captura OTA over-the-air para um 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

Aqui estão os rastreamentos de RA para este evento de roam:

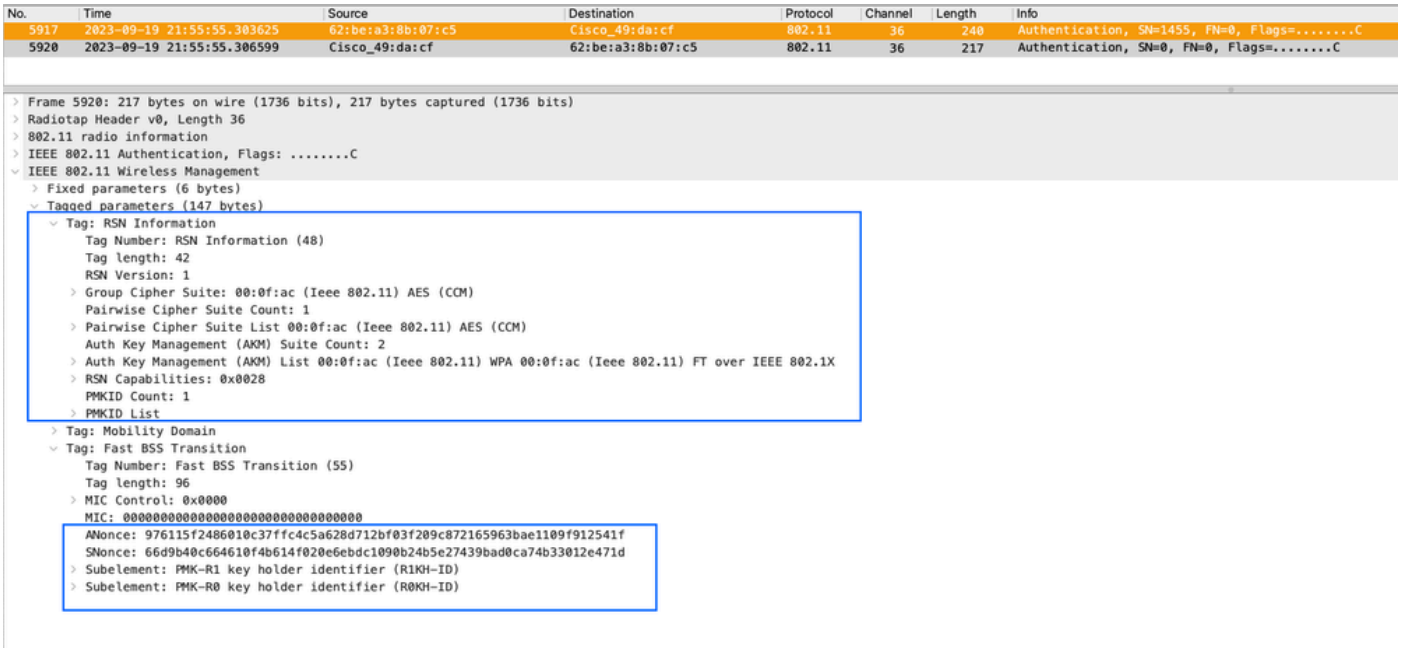
```
2023/09/19 21:54:25.912523930 {wncd_x_R0-0}{1}: [client-orch-sm] [15403]: (note): MAC: 62be.a38b.07c5 R
!--- Reassociation Request is received from the client.

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
```

Como o 802.11r está habilitado, o handshake inicial com um novo AP é feito antes mesmo do cliente fazer roaming para o access point de destino. Esse conceito é chamado de transição rápida.

O handshake inicial permite que um cliente e os access points façam o cálculo da PTK (Pairwise Transient Key) com antecedência.

Essas chaves PTK são aplicadas ao cliente e aos pontos de acesso depois que o cliente responde à solicitação de reassociação ou responde à troca com o novo AP de destino:




```
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 com protocolos Fast Roam desativados (802.11r, 802.11k e 802.11v)

Neste cenário, todos os protocolos são desativados em um SSID 802.1x. Nesse caso, o cliente passa por uma autenticação completa cada vez que o cliente sem fio faz roaming entre os pontos de acesso, a próxima figura mostra um exemplo de uma troca pelo ar, onde você pode ver que o

cliente não pode ignorar a troca EAP. Portanto, ocorreu uma reautenticação completa porque nenhum dos 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 Over-The-Air Desativados

Aqui está um resumo dos rastreamentos RA do controlador para este evento de roam:

```
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 com 802.11k ativado

O padrão 802.11k permite que os clientes solicitem um relatório de vizinho que contenha informações sobre APs que são bons candidatos para um roam dentro do conjunto de serviços.

Isso permite que os clientes evitem a verificação de RF passiva ou ativa antes que o cliente decida se mover para um ponto de acesso diferente.

O C9800 suporta um recurso chamado roami assistido por 11k, que cria e fornece uma lista de vizinhos otimizada para os clientes 802.11k.

A lista de vizinhos 802.11k é gerada sob demanda e pode ser diferente para dois clientes em APs diferentes, pois a WLC consideraria o relacionamento individual de RF do cliente com os APs cercados.

Os clientes que não suportam o protocolo 82.11k não enviam solicitações de lista de vizinhos. Isso permite a otimização da previsão que ajuda esses clientes.

Como resultado, uma lista de vizinhos é armazenada na estrutura de dados do software da estação móvel no C9800.

Os clientes enviam solicitações para listas de vizinhos somente depois de se associarem aos pontos de acesso que anunciam o IE (Elemento de Informação) da capacidade do RM no beacon.

A próxima figura é um exemplo de quadros de ação 802.11k depois que o cliente foi associado ao ponto de acesso:

```
> 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
```

Relatório De Vizinhos Over-The-Air

SSID com 802.11v ativado

Com o padrão 802.11v, os dois principais aprimoramentos do gerenciamento de rede sem fio incluem:

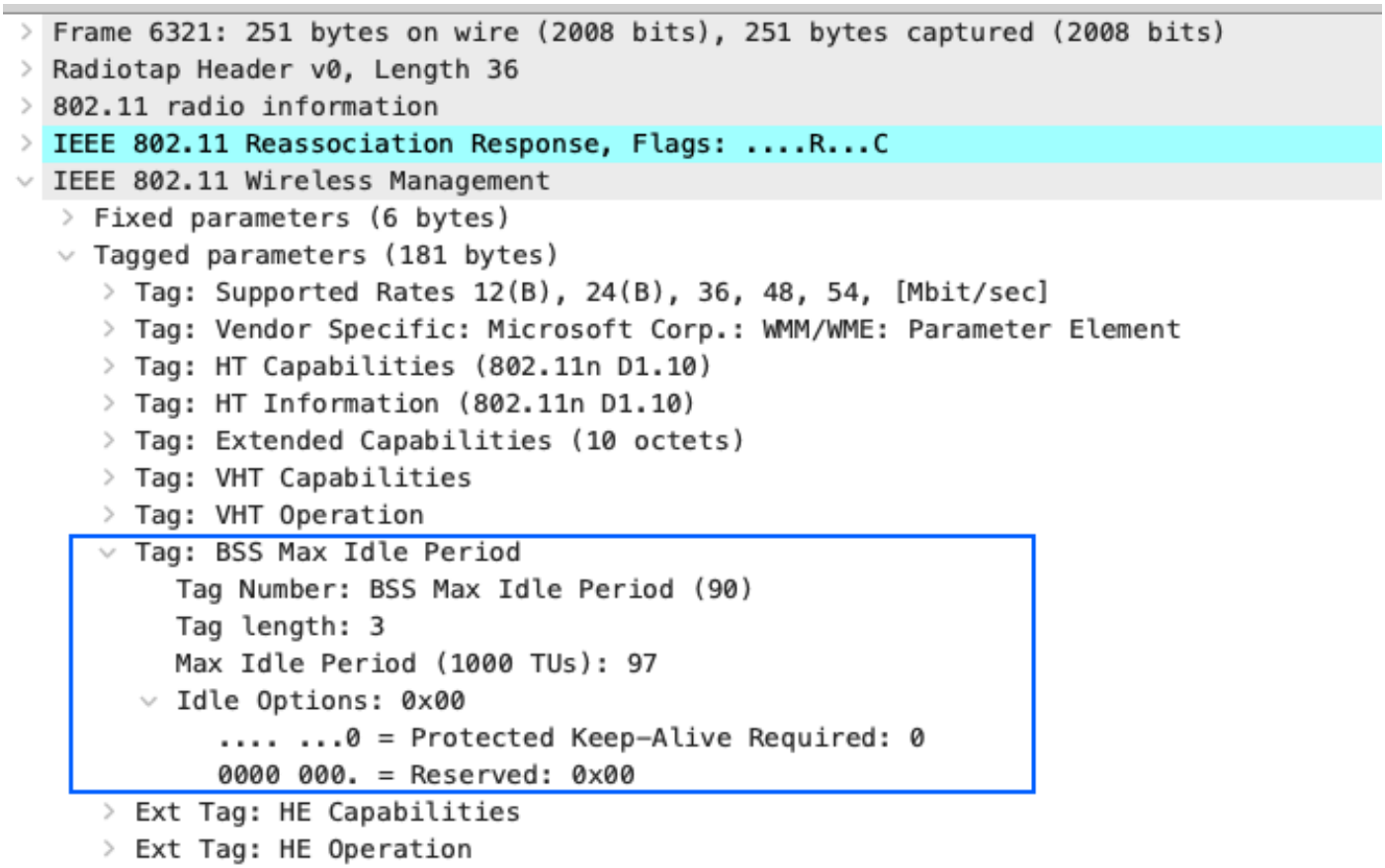
- Recurso de economia de energia assistida por rede: Melhora o desempenho da bateria do cliente com um período ocioso máximo, que indica a duração em que um cliente pode permanecer em modo de espera sem nenhum quadro de dados enviado. O cliente é notificado sobre esse período ocioso máximo por meio de quadros de associação e desassociação.

Se um ponto de acesso não receber quadros de um cliente sem fio por um certo período de tempo, ele supõe que o cliente deixou a rede e o desassocia.

O período ocioso máximo do BSS é a quantidade de tempo que um AP pode manter um cliente associado sem ter que receber qualquer quadro (o cliente pode permanecer em repouso, isso economiza bateria).

Esse valor é enviado ao cliente sem fio por meio do quadro de resposta de associação e reassociação.

A próxima figura mostra o valor na resposta de reassociação do ponto de acesso, onde o Período ocioso máximo do BSS é especificado em unidades de tempo. Toda vez que a unidade for igual a 1,024 milissegundos:



Valor do Período BSS Over-The-Air

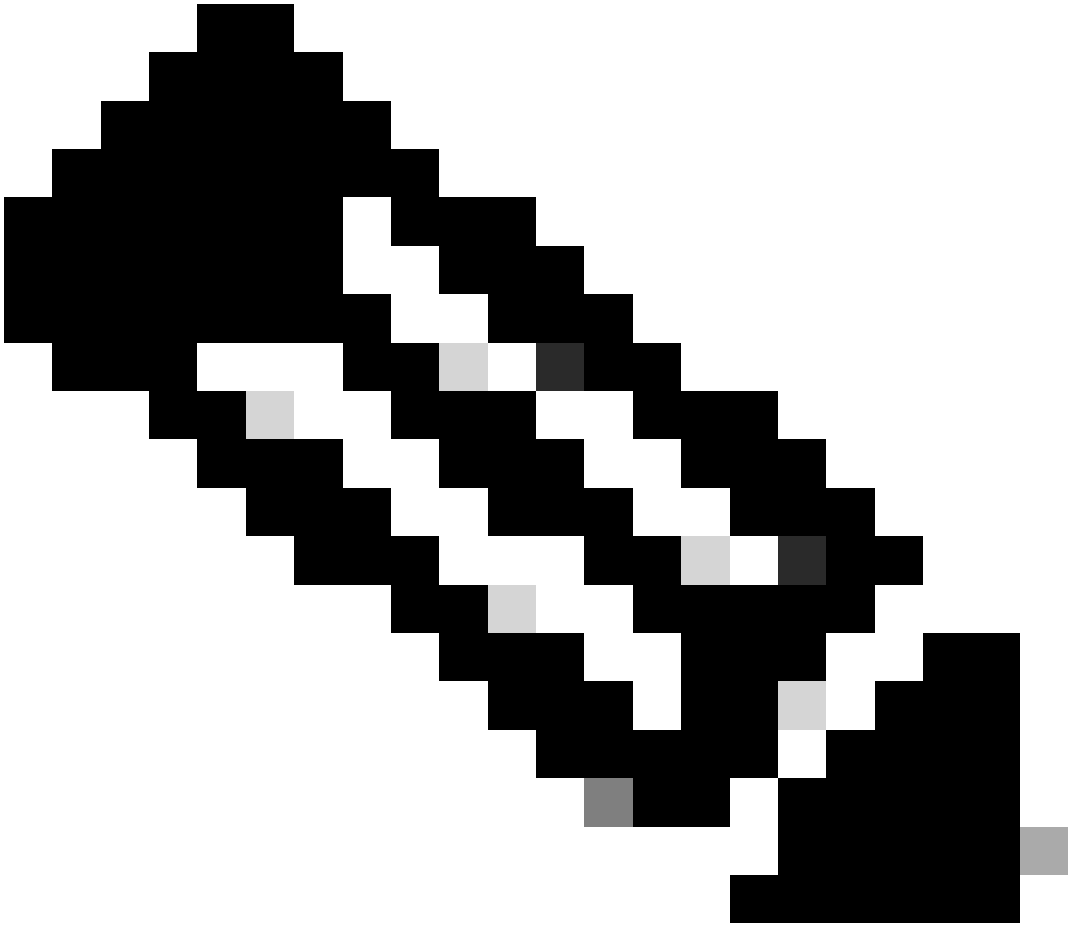
- Roam assistido por rede: permite que a infraestrutura sem fio sugira que o cliente faça roaming longe de seu ponto de acesso atual. Isso fornece ao cliente a lista de pontos de acesso para os quais ele pode fazer roaming no mesmo conjunto de serviços estendidos (ESS).

Os quadros de gerenciamento de transição BSS 802.11v são trocados em três cenários:

1. Solicitação Solicitada: Antes da transição para um novo access point, o cliente tem a capacidade de enviar uma consulta de gerenciamento de transição BSS 802.11v para descobrir melhores opções de access points a serem reassociados e o AP atual ao qual o cliente está conectado responde com uma solicitação de gerenciamento de transição BSS que fornece a lista de access points candidatos para roaming.

2. Solicitação de balanceamento de carga não solicitado: Este é um recurso que permite que o AP faça o balanceamento de carga de clientes entre pontos de acesso no mesmo controlador para evitar a sobrecarga do AP. Quando as contagens de clientes excedem o limite de balanceamento de carga configurado para um AP, qualquer novo cliente que tente se associar ao AP é negado com uma resposta de associação com o status 17 (AP ocupado). Normalmente, os clientes negados tentam associar-se ao mesmo AP carregado mesmo depois que o cliente recebe uma rejeição de associação, ou seja, se da perspectiva do RSSI, esse AP é sua melhor opção. Por exemplo, considere 40 usuários em uma sala de conferência atendida por um AP. Com uma consulta de gerenciamento de transição BSS 802.11v, uma falha de balanceamento de carga pode ser tratada mais suavemente, onde o AP envia uma lista de APs candidatos para fazer roaming.

3. Solicitação de roam otimizada não solicitada: Espera-se que os clientes sem fio examinem RF e façam roam para AP com o sinal mais alto. No entanto, alguns clientes exibiram um comportamento difícil onde permanecem com o AP ao qual estão associados, mesmo quando um AP vizinho fornece um sinal mais forte. Isso é conhecido como um problema difícil do cliente. Para resolver esse problema, o controlador 9800 suporta um recurso chamado roam otimizado, no qual o RSSI dos pacotes de dados do cliente e a taxa de dados são monitorados, e o cliente é desassociado proativamente. A solicitação de gerenciamento de transição BSS 802.11v melhora o roam otimizado, informando ao cliente sobre uma desassociação iminente e fornecendo uma lista de APs para o roam.



Note: Com base na experiência do TAC, o roaming otimizado não é adequado para todas as redes. Verifique se a cobertura é boa o suficiente entre os pontos de acesso para fazer com que isso funcione conforme o esperado, caso contrário, mais problemas podem surgir se você ativá-la.

Uma solicitação de gerenciamento de transição BSS 802.11v que, quando enviada por um AP a um cliente, é apenas uma sugestão. O cliente pode aceitar a sugestão ou descartá-la. O controlador sem fio 9800 fornece uma opção de configuração chamada Desassociação Iminente para que você force os clientes a se desassociarem se o cliente não reassociar com outro AP dentro de uma janela de tempo definida. Você pode configurá-lo somente a partir da CLI através do comando bss-transition disassociation-iminent em um perfil de WLAN específico.

Informações Relacionadas

- Transição rápida de BSS 802.11r
- Lista de vizinhos e roaming assistido 802.11k

- BSS 802.11v
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.