了解9800 WLC上的802.11r/11k/11v快速漫游

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

更高级别的安全漫游

启用快速漫游协议的SSID（802.11r、802.11k和802.11v）

禁用快速漫游协议的SSID（802.11r、802.11k和802.11v）

启用802.11k的SSID

启用802.11v的SSID

相关信息

简介

本文档介绍在无线客户端上启用/禁用快速漫游方法时的不同结果。

先决条件

要求

Cisco 建议您了解以下主题：

- IEEE 802.11 WLAN基础知识。
- IEEE 802.11 WLAN安全。
- IEEE 802.1X/EAP基础知识。
- IEEE 802.11r BSS快速过渡。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科无线9800-L控制器®17.9.4
- Cisco Catalyst 9130AXI系列接入点。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文档可帮助您了解在9800无线控制器上启用协议802.11r、802.11v和802.11k时的区别。它还解释了禁用客户端后对客户端的影响。

802.11r、802.11v和802.11k都是802.11系列无线网络协议中的不同标准或修正案。

- 802.11r:是跨基本服务集的快速过渡，它引入了一个新概念，即甚至在客户端漫游到目标接入点之前，即与新AP进行初始握手。它特别适用于不间断连接至关重要的环境，例如在IP语音或实时流应用程序中具有视频或持续流监控的情况。借助经过调整的802.11r网络，设备可以在接入点之间漫游，而不会出现重大网络连接中断或中断的情况。
- 802.11k:邻居列表和辅助漫游(Radio Resource Measurement)利用无线电资源管理功能来改善无线网络的整体性能和可靠性。它优化了可用的无线电资源，供接入点收集和共享有关其无线电环境的信息。这些信息包括信道使用情况、信号强度和干扰水平。然后，客户端设备可以使用它来做出更明智的决策，确定连接到哪个AP;从而实现更好的负载平衡、减少干扰并提高网络效率。
- 802.11v：是网络辅助节电，帮助客户端延长电池寿命，从而延长睡眠时间。本章还重点介绍如何提高无线网络的效率和管理水平。反过来，当客户端漫游时，这又可以在网络基础设施和客户端设备之间实现更好的控制和协调。

主要功能包括邻居报告、服务集转换、负载均衡和网络辅助节能。这些功能增强了客户端网络发现、选择和监控。

它还允许接入点鼓励客户端设备漫游，而不是等待设备做出漫游决策。

802.11r侧重于无线接入点之间的无缝过渡，而802.11v则旨在增强网络管理功能。802.11k旨在优化无线电资源利用率，从而提高性能和可靠性。

本文档中的部分陈述摘自Cisco Catalyst 9800系列无线控制器的了解和故障排除第6章802.11漫游部分中的书籍。

更高级别的安全漫游

在基本802.11开放系统身份验证的基础上为SSID配置L2更高级别的安全时，初始关联和客户端漫游时需要更多帧。

为802.11 WLAN标准化和实施的两种最常见安全方法是：

- WPA/WPA2/WPA3个人：PSK用于对客户端进行身份验证。
- WPA/WPA2/WPA3企业版：可扩展身份验证协议(EAP)方法和802.1x用于对无线客户端进行身份验证，即通过AAA服务器验证用户凭证（用户名和密码）、证书或令牌。

在本文档中，WPA2企业WLAN可以与EAP-PEAP配合使用，以展示IEEE协议（802.11r、802.11k和802.11v）在使用上的差异，以及它如何影响无线漫游尝试。

启用快速漫游协议的SSID（802.11r、802.11k和802.11v）

默认WLAN配置默认启用每个协议。在实验中，无线客户端尝试在9130个接入点之间漫游。

由于您拥有WLAN的默认配置（除802.11v和802.11k外，还启用了快速漫游），因此您期望无缝漫游。

以下是用于漫游的空中OTA捕获示例：

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

以下是此漫游事件的RA跟踪：

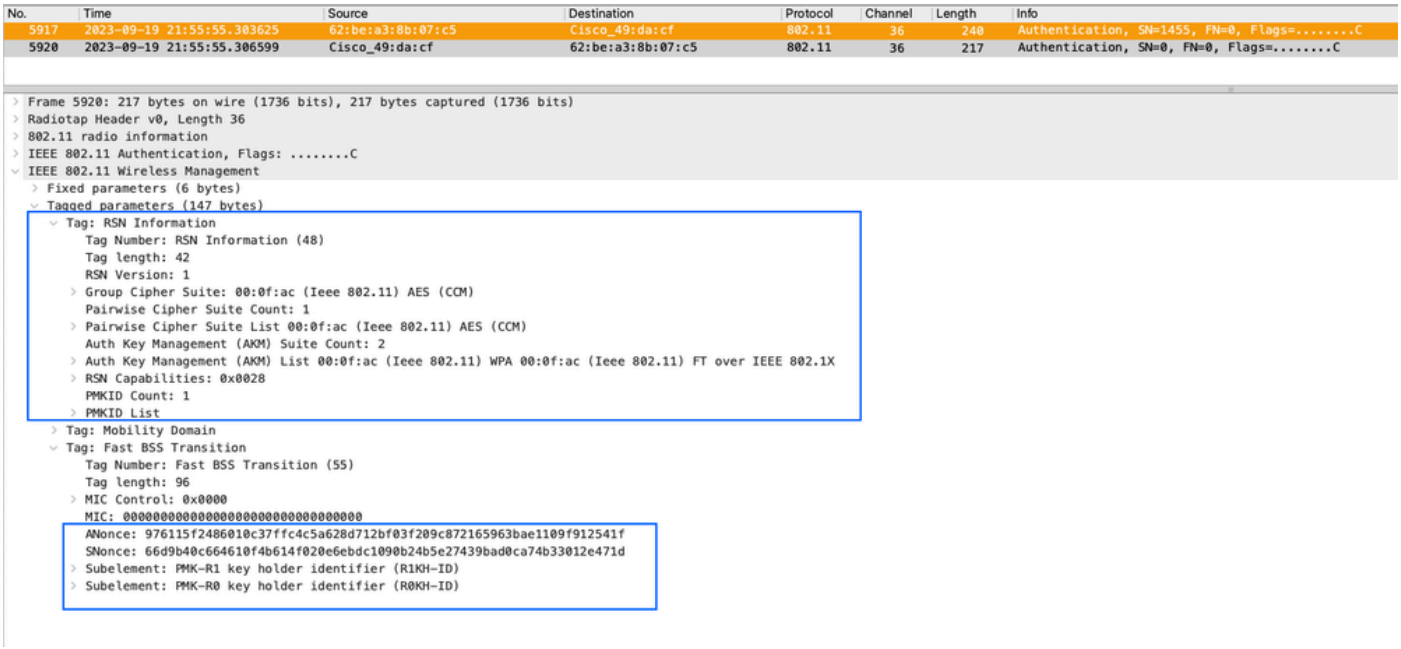
```
2023/09/19 21:54:25.912523930 {wncd_x_R0-0}{1}: [client-orch-sm] [15403]: (note): MAC: 62be.a38b.07c5 R
!--- Reassociation Request is received from the client.

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
```

启用802.11r后，即使在客户端漫游到目标接入点之前，也会与新的AP进行初始握手。此概念称为快速过渡。

初始握手允许客户端和接入点提前执行成对瞬时密钥(PTK)计算。

在客户端响应重新关联请求或响应与新目标AP的交换后，这些PTK密钥将应用于客户端和接入点：



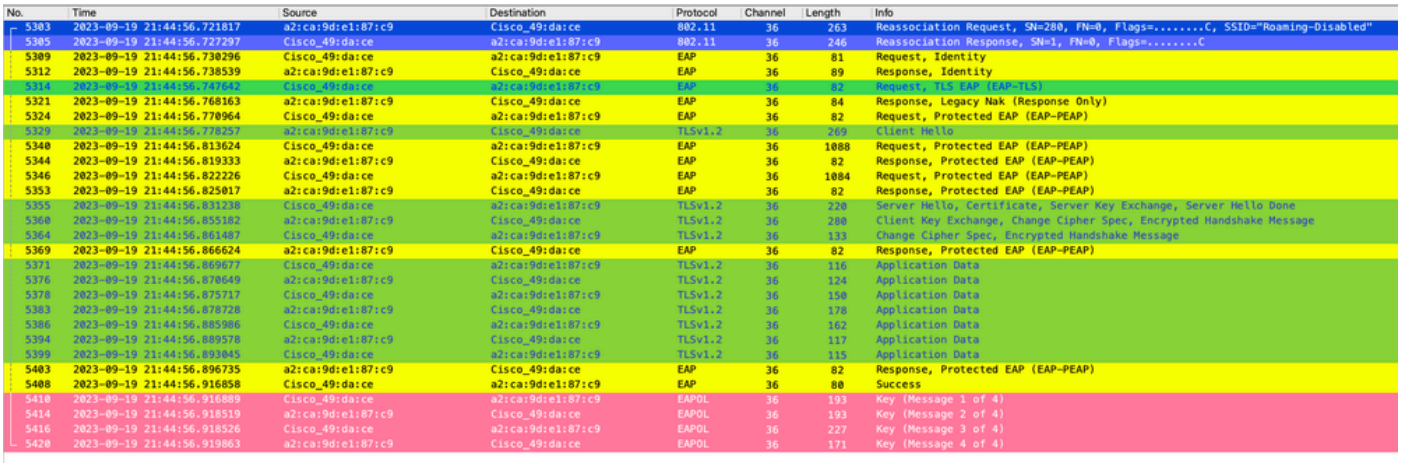

```
2023/09/19 21:54:25.913247615 {wncd_x_R0-0}{1}: [dot11] [15403]: (note): MAC: 62be.a38b.07c5 Associatio
!--- Reassociation Response is sent to the client.

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.
```

禁用快速漫游协议的SSID（802.11r、802.11k和802.11v）

在此场景中，所有协议在802.1x SSID上均被禁用。在这种情况下，每次无线客户端在接入点之间漫游时，客户端都会经历完全身份验证，下图显示空中交换的示例，在该示例中，您可以看到客户端无法跳过EAP交换。

因此，由于未启用任何快速漫游方法，因此发生了完全重新身份验证：



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)

禁用无线协议

以下是此漫游事件的控制器RA跟踪的摘要：

```
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.
```

启用802.11k的SSID

802.11k标准允许客户端请求邻居报告，其中包含有关适合在服务集中进行漫游的AP的信息。这样，客户端在决定移动到其他接入点之前，就可以避免被动或主动RF扫描。

C9800支持称为11k辅助漫游的功能，该功能可创建并向802.11k客户端提供优化的邻居列表。802.11k邻居列表按需生成，对于不同AP上的两个客户端可以不同，因为WLC会考虑与被包围的AP的单个客户端RF关系。

不支持82.11k协议的客户端不发送邻居列表请求。这可实现预测优化，从而帮助这些客户端。

因此，邻居列表存储在C9800上的移动台软件数据结构中。

客户端仅在与信标中通告RM功能信息元素(IE)的接入点关联之后才会发送邻居列表请求。

下图是客户端与接入点关联后802.11k操作帧的示例：

```
> 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
```

空中邻居报告

启用802.11v的SSID

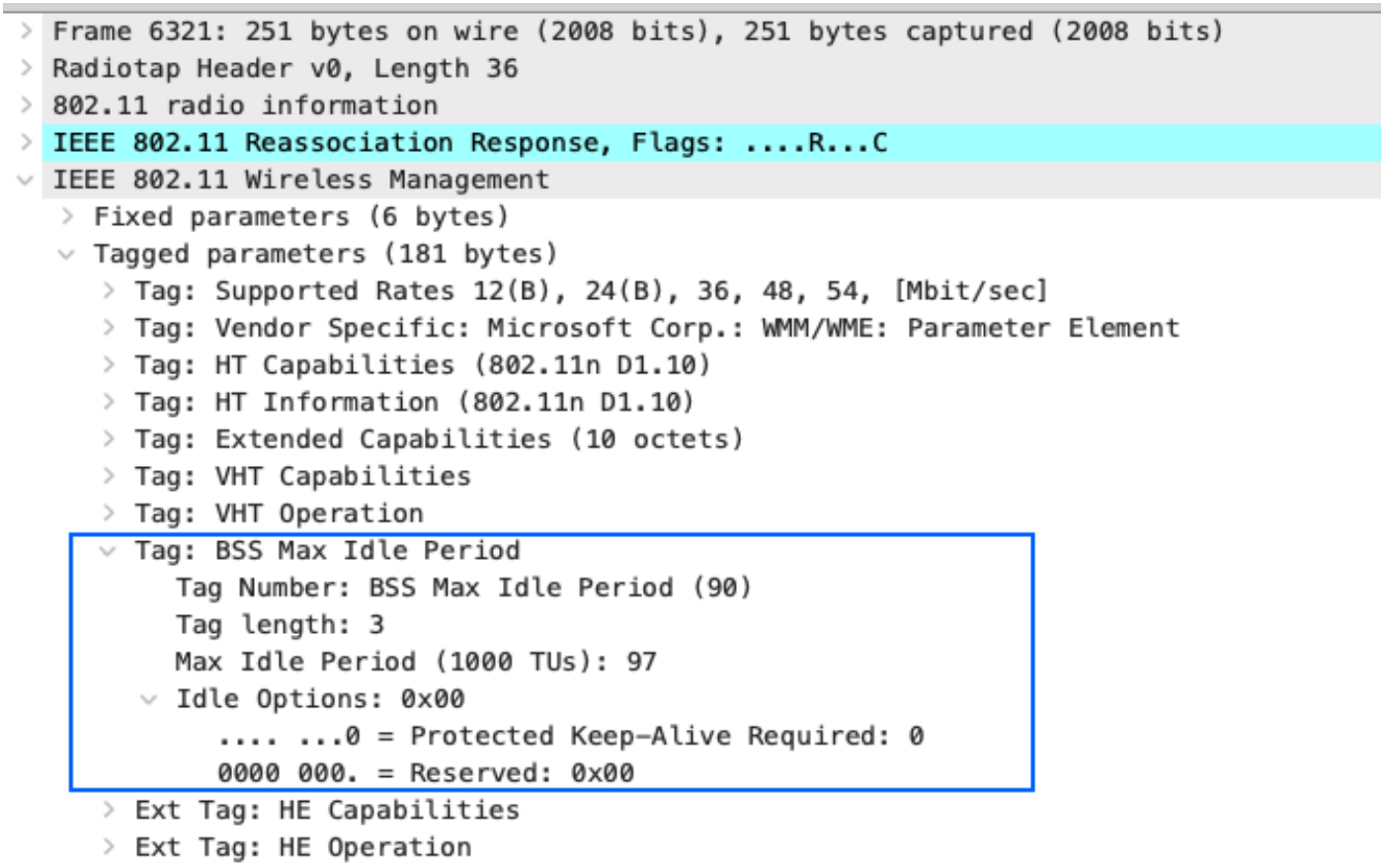
在802.11v标准下，无线网络管理的两项主要增强功能包括网络辅助省电功能，该功能以最大空闲周期增强客户端电池性能，该空闲周期表示客户端可以在不发送任何数据帧的情况下保持休眠模式的持续时间。客户端通过关联帧和取消关联帧收到有关此最大空闲时段的通知。

如果接入点在一定时间段内未收到来自无线客户端的帧，它会假定该客户端已离开网络并取消关联。

BSS Max idle period是AP无需接收任何帧（客户端可以保持休眠，从而节省电池）即可保持客户端关联的时间量。

该值通过关联和重新关联响应帧发送到无线客户端。

下图显示来自接入点的重新关联响应中的值，其中BSS最大空闲周期以时间单位指定。每次单位等于1.024毫秒时：



空中BSS周期值

网络辅助漫游使无线基础设施能够建议客户端漫游远离其当前接入点。这为客户端提供了可在同一扩展服务集(ESS)中漫游的接入点列表。

802.11v BSS过渡管理帧在以下三个场景中进行交换：

1.请求请求:在向新接入点过渡之前，客户端能够发送802.11v BSS过渡管理查询，以找出重新关联的接入点的更好选项，以及客户端所连接的当前AP，并响应BSS过渡管理请求，该请求提供要漫游的候选接入点列表。

2.未请求的负载平衡请求：此功能允许AP在同一控制器上的接入点之间对客户端进行负载均衡，以避免AP过载。当客户端计数超过AP的已配置负载均衡阈值时，任何尝试与AP关联的新客户端都会被拒绝，并显示状态为17（AP忙）的关联响应。 通常，被拒绝的客户端会尝试关联到同一已加载的AP，即使客户端收到关联拒绝后也是如此，即从RSSI角度而言，如果AP是其最佳选项。例如，假设一个AP为会议室提供服务，但会有40个用户。使用802.11v BSS过渡管理查询，可以更顺畅地处理负载均衡故障，其中AP会将候选的AP列表发送到漫游目的地。

3.未经请求的优化漫游请求：无线客户端应扫描RF并漫游到信号最高的AP。但是，有些客户端显示粘滞行为，即它们停留在与其关联的AP上，即使邻居AP提供较强信号时也是如此。这称为粘性客户端问题。为了解决此问题，9800控制器支持称为优化漫游的功能，其中监控客户端数据包的RSSI和数据速率，并主动取消关联客户端。802.11v BSS过渡管理请求增强了优化的漫游，它告知客户端即将取消关联，并提供要漫游到的AP列表。

注意：根据TAC经验，优化漫游并不适用于所有网络。确保接入点之间的覆盖足够好，使此功能达到预期效果，否则，如果启用此功能，可能会出现更多问题。

由AP发送到客户端的802.11v BSS过渡管理请求只是一个建议。客户可以遵循建议或放弃建议。9800无线控制器提供了一个名为“即将取消关联”的配置选项，如果客户端在定义的时间窗口内未与另一个AP重新关联，则您可以强制客户端取消关联。您只能从CLI通过特定WLAN配置文件下的bss-transition disassociation-imming命令进行配置。

相关信息

- 802.11r BSS快速过渡
- 802.11k邻居列表和辅助漫游
- 802.11v BSS
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。