

# 瞭解9800 WLC上的802.11r/11k/11v快速漫遊

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[更高級別的安全漫遊](#)

[啟用了快速漫遊協定的SSID \( 802.11r、802.11k和802.11v \)](#)

[停用快速漫遊協定的SSID \( 802.11r、802.11k和802.11v \)](#)

[啟用802.11k的SSID](#)

[啟用802.11v的SSID](#)

[相關資訊](#)

---

## 簡介

本文檔介紹在無線客戶端上啟用/停用快速漫遊方法時的不同結果。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- IEEE 802.11 WLAN基礎。
- IEEE 802.11 WLAN安全性。
- IEEE 802.1X/EAP基礎知識。
- IEEE 802.11r BSS快速轉換。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco無線9800-L控制器IOS® XE 17.9.4
- Cisco Catalyst 9130AXI系列存取點。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

在9800無線控制器上啟用802.11r、802.11v和802.11k通訊協定時，本檔案可協助您瞭解不同之處。同時說明停用使用者端後對使用者端的影響。

802.11r、802.11v和802.11k都是802.11系列無線網路通訊協定中的不同標準或修訂。

802.11r：是跨基本服務集的快速過渡，引入一個新概念，即在客戶端漫遊到目標存取點之前，與新AP的初始握手已經完成。它特別適用於不間斷連線至關重要的環境，例如在IP語音或即時流應用中，使用影片或恆定流監控器。使用經過調整的802.11r網路，裝置可以在存取點之間漫遊，而不會出現網路連線中斷或中斷的情況。

802.11k：鄰居清單和輔助漫遊（Radio Resource Measurement，無線電資源測量）利用無線電資源管理功能，提高無線網路的整體效能和可靠性。它可以最佳化存取點收集和共用其無線電環境資訊的可用無線電資源。此資訊包括通道使用情況、訊號強度和干擾水準。然後，客戶端裝置可以使用它來更明智地決定連線到哪個AP；這將實現更好的負載平衡、減少干擾和提高網路效率。

802.11v：是網路輔助省電，可協助使用者端改善電池續航力，讓他們有更長的睡眠時間。本章還著重介紹如何提高無線網路的效率和管理水準。反過來，當客戶端漫遊時，這可以更好地控制和協調網路基礎設施與客戶端裝置。主要功能包括鄰居報告、服務集轉換、負載均衡和網路輔助節能。這些功能增強了客戶端網路發現、選擇和監控。它還允許存取點鼓勵客戶端裝置漫遊，而不是等待裝置做出漫遊決定。

802.11r專注於AP之間的無縫過渡，而802.11v則旨在增強網路管理功能。802.11k旨在最佳化無線電資源利用率，以實現更好的效能和可靠性。

本文檔中的一些語句摘自瞭解Cisco Catalyst 9800系列無線控制器和對其進行故障排除第6章「802.11漫遊」部分。

## 更高級別的安全漫遊

在基本的802.11開放系統身份驗證基礎上配置SSID的L2更高層安全時，初始關聯和客戶端漫遊時需要更多幀。針對802.11 WLAN標準化和實施的兩種最常見安全方法為：

- WPA/WPA2/WPA3個人：PSK用於驗證客戶端。
- WPA/WPA2/WPA3企業：可擴展身份驗證協定(EAP)方法和802.1x用於驗證無線客戶端，即透過AAA伺服器驗證使用者憑證（使用者名稱和密碼）、證書或令牌。

在本文中，WPA2企業WLAN可以與EAP-PEAP一起使用，以顯示IEEE協定（802.11r、802.11k和802.11v）在使用上的差異，以及它如何影響無線漫遊嘗試。

## 啟用了快速漫遊協定的SSID（802.11r、802.11k和802.11v）

預設情況下，預設的WLAN配置啟用了每個協定。在實驗中，無線客戶端嘗試在9130個存取點之間漫遊。換句話說，由於您擁有WLAN的預設配置，因此除了802.11v和802.11k外，還啟用了快速漫遊，因此您會期望實現無縫漫遊。以下是漫遊時的空中OTA捕獲示例：

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	Cisco_49:da:cf (62:be:a3:8b:07:c5)	802.11	36	72	Acknowledgment, 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:a3:8b:07:c5 (62:be:a3:8b:07:c5)	802.11	36	72	Acknowledgment, 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....FC
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:a3:8b:07:c5 (62:be:a3:8b:07:c5)	802.11	36	72	Acknowledgment, 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=.....TC
5937	2023-09-19 21:55:55.319863	62:be:a3:8b:07:c5	62:be:a3:8b:07:c5 (62:be:a3:8b:07:c5)	802.11	36	72	Acknowledgment, 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:a3:8b:07:c5 (62:be:a3:8b:07:c5)	802.11	36	72	Acknowledgment, Flags=.....C
5940	2023-09-19 21:55:55.319874	Cisco_49:da:cf (f1:1d:2d:49:d1)	62:be:a3:8b:07:c5 (62:be:a3:8b:07:c5)	802.11	36	61	VHT/VHE/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....FC
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....FC
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....FC

以下是此漫遊事件的RA跟蹤：

2023/09/19 21:54:25.912523930 {wncd\_x\_R0-0}{1}: [client-orch-sm] [15403]: (note): MAC: 62be.a38b.07c5 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 Since 802.11r is enabled, WLC/AP were able to validate/use the PMKID

啟用802.11r後，即使客戶端漫遊到目標存取點，也會與新AP進行初始握手。這個概念稱為「快速轉換」。初始握手允許客戶端和存取點提前執行成對臨時金鑰(PTK)計算。在客戶端響應重新關聯請求或響應與新目標AP的交換之後，這些PTK金鑰將應用到客戶端和存取點：

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
> IEEE 802.11 Wireless Management
  > Fixed parameters (6 bytes)
  > Tagged parameters (147 bytes)
    > 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
    > 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 Association 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.07c5 Client took an IP address and moved to run state.

停用快速漫遊協定的SSID ( 802.11r、802.11k和802.11v )

在此案例中，所有通訊協定在802.1x SSID上皆已停用，在這種情況下，每次無線使用者端在存取點之間漫遊時，使用者端都會經歷完整驗證，下圖顯示無線交換的範例，您可以在其中看到使用者端無法略過EAP交換。因此，由於未啟用任何快速漫遊方法，因此進行了完全重新身份驗證：

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
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)
5327	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	228	Server Hello, Certificate, Server Key Exchange, Server Hello Done
5360	2023-09-19 21:44:56.835182	a2:ca:9d:e1:87:c9	Cisco_49:da:ce	TLSv1.2	36	288	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
5364	2023-09-19 21:44:56.861407	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 21:44:56.879728	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	182	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 21:44:56.893845	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)

已停用無線協定

以下是此漫遊事件的控制器RA跟蹤的摘要：

```

2023/09/19 21:44:47.425575500 {wncd_x_R0-0}{1}: [client-orch-sm] [15403]: (note): MAC: a2ca.9de1.87c9 R
!--- Reassociation 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
!--- Reassociation Response is sent to the client.

2023/09/19 21:44:47.4444466744 {wncd_x_R0-0}{1}: [dot1x] [15403]: (info): [a2ca.9de1.87c9:capwap_9000000
2023/09/19 21:44:47.4444469338 {wncd_x_R0-0}{1}: [dot1x] [15403]: (info): [a2ca.9de1.87c9:capwap_9000000

2023/09/19 21:44:47.4444481064 {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 E
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 E

```

```
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.
```

## 啟用802.11k的SSID

802.11k標準允許客戶端請求鄰居報告，其中包含適合在服務集中漫遊的AP的相關資訊。這樣，在客戶端決定移動到不同存取點之前，客戶端就可以避免被動或主動RF掃描。C9800支援11k輔助漫遊功能，該功能可建立並向802.11k客戶端提供最佳化的鄰居清單。802.11k鄰居清單按需生成，對於不同AP上的兩個客戶端可以不同，因為WLC會考慮與被包圍的AP的單個客戶端RF關係。

不支援82.11k協定的客戶端不傳送鄰居清單請求。這樣可以啟用預測最佳化，從而幫助這些客戶端。結果，鄰居清單儲存在C9800上的移動台軟體資料結構中。

客戶端僅在與通告信標中的RM功能資訊元素(IE)的存取點關聯之後才傳送鄰居清單請求。下圖是客戶端與存取點關聯後802.11k操作幀的示例：

```

> 802.11 radio information
> IEEE 802.11 Action, Flags: .....C
> IEEE 802.11 Wireless Management
  > Fixed parameters
    Category code: Radio Measurement (5)
    Action code: Neighbor Report Response (5)
    Dialog token: 42
  > Tagged parameters (90 bytes)
    > Tag: Neighbor Report
      Tag Number: Neighbor Report (52)
      Tag length: 13
      BSSID: Cisco_7f:a2:2f (14:16:9d:7f:a2:2f)
    > BSSID Information: 0x00002f7
      Operating Class: 115
      Channel Number: 36 (iterative measurements on that Channel Number)
      PHY Type: 0x07
    > Tag: Neighbor Report
      Tag Number: Neighbor Report (52)
      Tag length: 13
      BSSID: Cisco_b9:35:ee (d4:78:9b:b9:35:ee)
    > BSSID Information: 0x00002f7
      Operating Class: 121
      Channel Number: 140 (iterative measurements on that Channel Number)
      PHY Type: 0x07
    > Tag: Neighbor Report
      Tag Number: Neighbor Report (52)
      Tag length: 13
      BSSID: Cisco_1a:10:ce (d4:e8:80:1a:10:ce)
    > BSSID Information: 0x00002f7
      Operating Class: 121
      Channel Number: 128 (iterative measurements on that Channel Number)
      PHY Type: 0x07
    > Tag: Neighbor Report
      Tag Number: Neighbor Report (52)
      Tag length: 13
      BSSID: Cisco_2b:a5:0e (00:f6:63:2b:a5:0e)
    > BSSID Information: 0x00002f7
      Operating Class: 125
      Channel Number: 161 (iterative measurements on that Channel Number)
      PHY Type: 0x07
    > Tag: Neighbor Report
      Tag Number: Neighbor Report (52)
      Tag length: 13
      BSSID: Cisco_c9:be:2e (a0:23:9f:c9:be:2e)
    > BSSID Information: 0x00002f7
      Operating Class: 118
      Channel Number: 64 (iterative measurements on that Channel Number)
      PHY Type: 0x07
    > Tag: Neighbor Report
      Tag Number: Neighbor Report (52)
      Tag length: 13
      BSSID: Cisco_99:2b:0e (40:01:7a:99:2b:0e)
    > BSSID Information: 0x00002f7
      Operating Class: 118
      Channel Number: 52 (iterative measurements on that Channel Number)
      PHY Type: 0x07

```

使用802.11v標準時，無線網路管理的兩個主要增強功能包括：

- 網路輔助省電功能：利用最大空閒時間增強客戶端電池效能，該空閒時間指示客戶端在不傳送任何資料幀的情況下可以保持休眠模式的持續時間。透過關聯幀和分離幀，客戶端會收到有關此最長空閒時間的通知。

如果存取點在一段時間內未收到來自無線使用者端的訊框，它會假設使用者端已離開網路並取消關聯。BSS Max idle period是AP在不接收任何幀（客戶端可以保持休眠，從而節省電池）的情況下保持客戶端關聯的時間量。該值透過關聯和重新關聯響應幀傳送到無線客戶端。下圖顯示來自存取點的重新關聯響應中的值，其中BSS最大空閒週期以時間單位指定。每次單位等於1.024毫秒時：

```
> Frame 6321: 251 bytes on wire (2008 bits), 251 bytes captured (2008 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 Reassociation Response, Flags: ....R...C
v IEEE 802.11 Wireless Management
  > Fixed parameters (6 bytes)
  v Tagged parameters (181 bytes)
    > Tag: Supported Rates 12(B), 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: HT Information (802.11n D1.10)
    > Tag: Extended Capabilities (10 octets)
    > Tag: VHT Capabilities
    > Tag: VHT Operation
    v Tag: BSS Max Idle Period
      Tag Number: BSS Max Idle Period (90)
      Tag length: 3
      Max Idle Period (1000 TUs): 97
      v Idle Options: 0x00
        .... ...0 = Protected Keep-Alive Required: 0
        0000 000. = Reserved: 0x00
    > Ext Tag: HE Capabilities
    > Ext Tag: HE Operation
```

空中BSS期間值

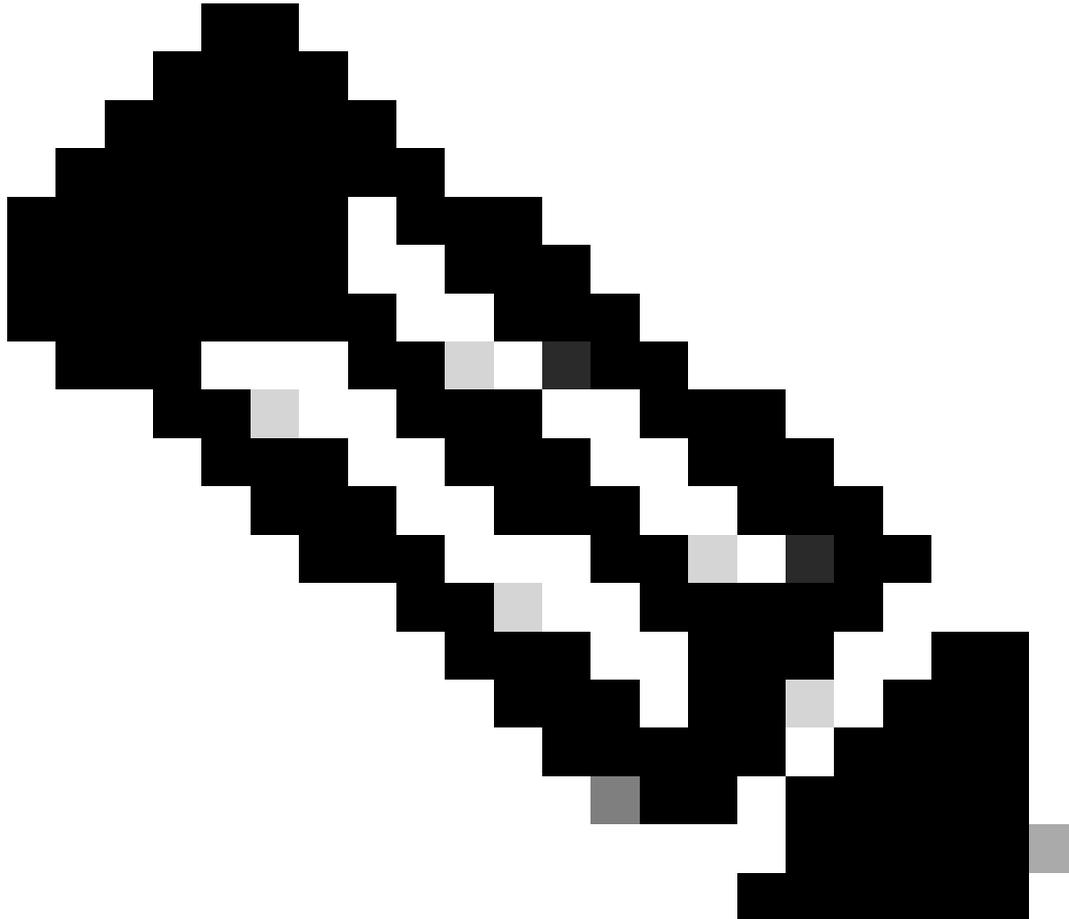
- 網路輔助漫遊：使無線基礎設施能夠建議客戶端遠離其當前存取點漫遊。這會向客戶端提供可在同一擴展服務集(ESS)中漫遊的存取點清單。

802.11v BSS過渡管理幀在以下三種情況下交換：

1. 請求的請求：在轉換到新的存取點之前，客戶端可以傳送802.11v BSS轉換管理查詢來查詢要重新關聯的存取點的更好選項，以及客戶端所連線的當前AP，以BSS轉換管理請求作出響應，該請求提供要漫遊的候選存取點清單。
2. 未經請求的負載平衡請求：允許AP在同一控制器上的存取點之間對客戶端進行負載平衡以避免AP過載的功能。當客戶端計數超過為AP配置的負載平衡閾值時，任何嘗試與AP關聯的新客戶端都將遭到拒絕，且關聯響應的狀態為17（AP忙碌）。通常，被拒絕的客戶端會嘗試關聯到同一已載入AP，即使客戶端獲得了關聯拒絕（即從RSSI角度看，該AP是其最佳選項）。例如，假設會議室

中由1個AP提供服務的40名使用者。使用802.11v BSS Transition Management查詢時，可以更順利地處理負載平衡故障，AP會向其中傳送要漫遊的候選AP清單。

3. 未經請求的最佳化漫遊請求：無線客戶端應掃描RF並漫遊到訊號最高的AP。但是，某些客戶端顯示了一種粘滯行為，即使AP鄰居提供較強的訊號，這些客戶端仍會與它們關聯的AP保持連線。這稱為粘性客戶端問題。為了解決此問題，9800控制器支援一種稱為最佳化漫遊的功能，在該功能中，客戶端資料包的RSSI和資料速率受到監控，並且客戶端主動取消關聯。802.11v BSS轉換管理請求增強了最佳化漫遊，它告知客戶端即將取消關聯，並提供要漫遊到的AP清單。



注意：從TAC經驗來看，最佳化漫遊不適用於所有網路。請確保存取點之間的覆蓋足夠好，以使此操作按預期工作，否則，如果啟用該功能，可能會出現更多問題。

802.11v BSS轉換管理請求，當由AP傳送到客戶端時只是一個建議。客戶可以遵循建議或放棄建議。9800無線控制器提供了一個名為「立即解除關聯」的配置選項，如果客戶端在定義的時間窗口內未與另一個AP重新關聯，則可以強制客戶端解除關聯。您只能透過CLI在特定的WLAN配置檔案下發出命令**bss-transition disassociation-importing**進行配置。

## 相關資訊

- [802.11r BSS快速轉換](#)
- [802.11k鄰居清單和輔助漫遊](#)
- [802.11伏BSS](#)
- [思科技術支援與下載](#)

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。