802.11r/11k/11v Fast-Roaming auf 9800 WLCs

Inhalt

Einleitung

In diesem Dokument werden die verschiedenen Ergebnisse beschrieben, wenn schnelle Roaming-Methoden auf den Wireless-Clients aktiviert/deaktiviert werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- IEEE 802.11 WLAN-Grundlagen
- IEEE 802.11: WLAN-Sicherheit
- IEEE 802.1x/EAP-Grundlagen
- Schneller Umstieg auf IEEE 802.11r BSS

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Wireless Controller 9800-L IOS® XE 17.9.4
- Cisco Catalyst Access Points der Serie 9130AXI

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Dieses Dokument hilft Ihnen, den Unterschied zu verstehen, wenn Sie die Protokolle 802.11r, 802.11v und 802.11k auf einem Wireless-Controller der Serie 9800 aktiviert haben. Außerdem wird erläutert, welche Auswirkungen die Deaktivierung auf die Clients hat.

802.11r, 802.11v und 802.11k sind verschiedene Standards oder Änderungen innerhalb der 802.11-Familie von Wireless-Netzwerkprotokollen.

802.11r: Ist der schnelle Übergang über grundlegende Service Sets, wodurch ein neues Konzept eingeführt wird, bei dem der erste Handshake mit einem neuen Access Point durchgeführt wird, noch bevor der Client zum Ziel-Access Point wechselt. Sie ist besonders in Umgebungen nützlich, in denen eine unterbrechungsfreie Anbindung von entscheidender Bedeutung ist, z. B. bei Voice-over-IP- oder Echtzeit-Stream-Anwendungen mit Video oder konstantem Stream-Monitor. Mit einem optimierten 802.11r-Netzwerk können Geräte zwischen Access Points wechseln, ohne dass es zu merklichen Unterbrechungen oder Ausfällen der Netzwerkverbindung kommt.

802.11k: Neighbor List and Assisted Roam (Radio Resource Measurement) nutzt die Funktionen der Funkressourcenverwaltung, um die Gesamtleistung und Zuverlässigkeit von Wireless-Netzwerken zu verbessern. Es optimiert die verfügbaren Funkressourcen, bei denen Access Points Informationen über ihre Funkumgebung sammeln und austauschen. Zu diesen Informationen gehören Kanalnutzung, Signalstärke und Interferenzpegel. Er kann dann von Client-Geräten verwendet werden, um fundiertere Entscheidungen darüber zu treffen, mit welchem Access Point eine Verbindung hergestellt werden soll. Dies führt zu einem besseren Lastenausgleich, geringeren Interferenzen und einer verbesserten Netzwerkeffizienz.

802.11v: Bietet netzwerkgestützten Energiesparmodus, mit dem die Akkulaufzeit verbessert und der Energiesparmodus verlängert werden kann. Ein weiterer Schwerpunkt ist die Verbesserung der Effizienz und Verwaltung von Wireless-Netzwerken. Dies wiederum ermöglicht eine bessere Kontrolle und Koordination zwischen der Netzwerkinfrastruktur und den Client-Geräten, wenn die Clients Roaming nutzen. Die Hauptfunktionen sind Berichte von Nachbarn, Änderungen von Service-Sets, Lastausgleich und netzwerkgestützte Energieeinsparungen. Diese Funktionen verbessern die Erkennung, Auswahl und Überwachung des Client-Netzwerks. Darüber hinaus können die Access Points Client-Geräte zum Roaming anregen, anstatt darauf zu warten, dass das Gerät eine Roaming-Entscheidung trifft.

Während bei 802.11r der nahtlose Übergang zwischen APs im Mittelpunkt steht, zielt 802.11v darauf ab, die Netzwerkverwaltungsfunktionen zu verbessern. Der 802.11k-Standard ist auf eine optimierte Nutzung von Funkressourcen für eine bessere Leistung und Zuverlässigkeit ausgelegt.

Einige Aussagen in diesem Dokument stammen aus dem Abschnitt Verständnis und Fehlerbehebung für Cisco Catalyst Wireless Controller der Serie 9800, Kapitel 6, 802.11 Roaming.

Höherstufige Sicherheits-Roams

Wenn die SSID zusätzlich zur grundlegenden 802.11-Open-System-Authentifizierung mit L2-

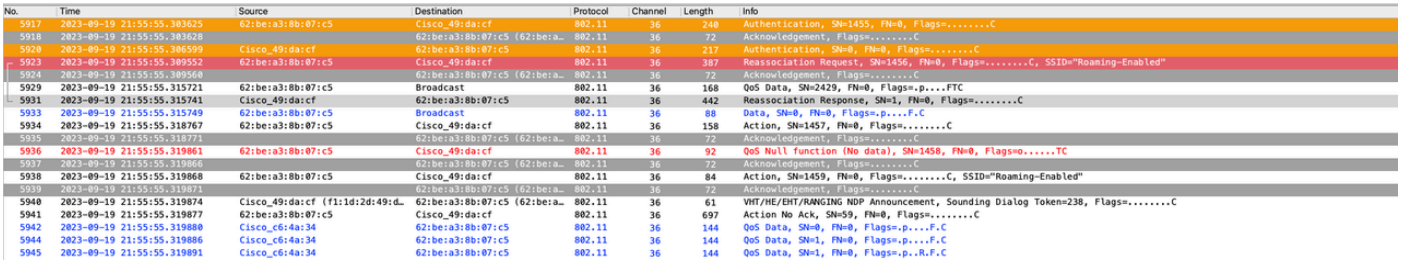
Sicherheit auf höherer Ebene konfiguriert ist, sind für die anfängliche Zuordnung und beim Roaming der Clients mehr Frames erforderlich. Die beiden gebräuchlichsten Sicherheitsmethoden, die für 802.11-WLANs standardisiert und implementiert werden, sind:

- WPA/WPA2/WPA3 Personal: Ein PSK wird verwendet, um die Clients zu authentifizieren.
- WPA/WPA2/WPA3 Enterprise: Das Extensible Authentication Protocol (EAP)-Verfahren und 802.1x werden zur Authentifizierung der Wireless-Clients verwendet. Dabei werden die Benutzeranmeldeinformationen (Benutzername und Kennwort), Zertifikate oder Token über einen AAA-Server validiert.

In diesem Dokument kann WPA2 Enterprise WLAN mit EAP-PEAP verwendet werden, um den Unterschied bei der Verwendung der IEEE-Protokolle (802.11r, 802.11k und 802.11v) und die möglichen Auswirkungen auf die Wireless-Roamingversuche aufzuzeigen.

SSID mit aktivierten Fast Roam-Protokollen (802.11r, 802.11k und 802.11v)

In der WLAN-Standardkonfiguration ist jedes Protokoll standardmäßig aktiviert. In der Übung versucht der Wireless-Client, zwischen 9.130 Access Points zu wechseln. Da Sie über die Standardkonfiguration des WLAN verfügen, d. h. zusätzlich zu 802.11v und 802.11k schnelles Roaming aktiviert ist, ist ein nahtloses Roaming zu erwarten. Hier ist ein Beispiel für eine OTA-Aufzeichnung auf Sendung für eine Roam-Veranstaltung:



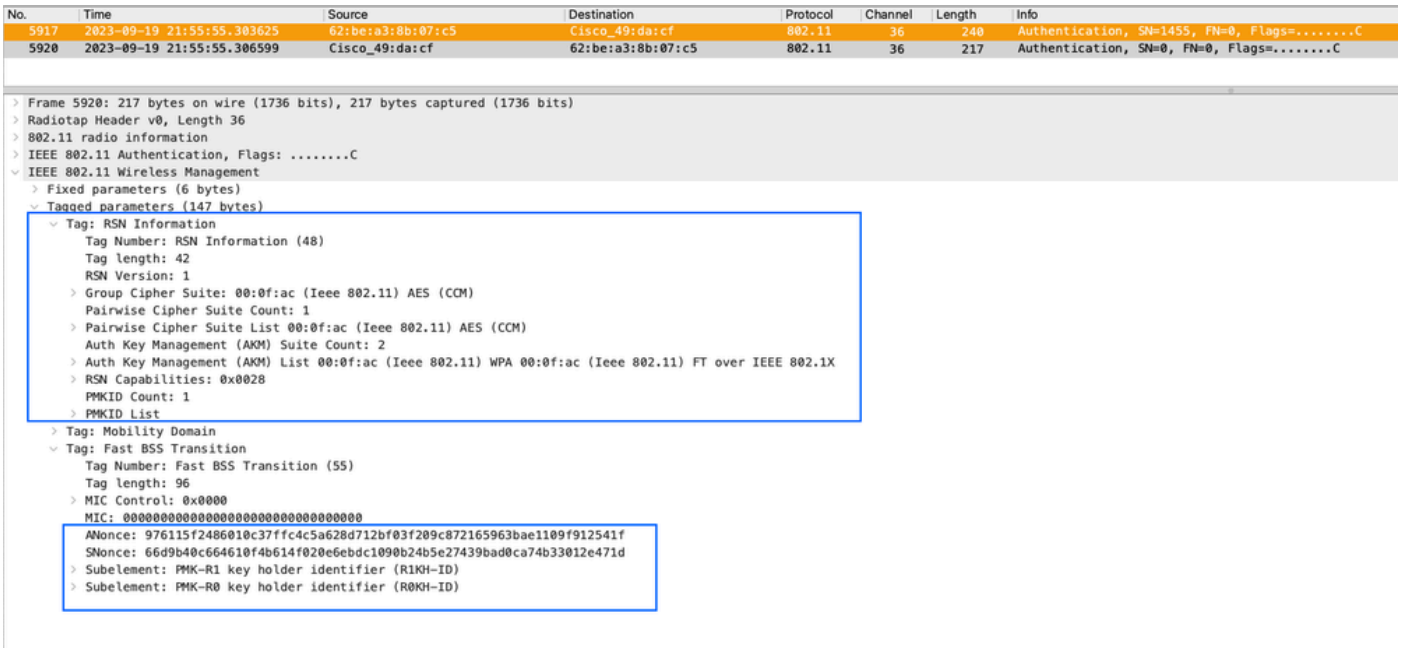
No.	Time	Source	Destination	Protocol	Channel	Length	Info
5917	2023-09-19 21:55:55.303625	62:be:a3:8b:07:c5	Cisco_49:da:cf	802.11	36	240	Authentication, SN=1455, FN=0, Flags=.....C
5918	2023-09-19 21:55:55.303628		62:be:a3:8b:07:c5 (62:be:a…	802.11	36	72	Acknowledgement, Flags=.....C
5920	2023-09-19 21:55:55.306599	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 21:55:55.319061	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 21:55:55.319066		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

Hier sind die RA-Spuren für diese Roam-Veranstaltung:

```
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
```

Wenn 802.11r aktiviert ist, erfolgt der erste Handshake mit einem neuen Access Point, noch bevor der Client zum Ziel-Access Point wechselt. Dieses Konzept nennt sich schneller Übergang. Der erste Handshake ermöglicht einem Client und den Access Points, die Pairwise Transient Key (PTK)-Berechnung im Voraus durchzuführen. Diese PTK-Schlüssel werden auf den Client und die Access Points angewendet, nachdem der Client auf die Neuzuordnungsanforderung oder auf den Austausch mit dem neuen Ziel-AP reagiert:

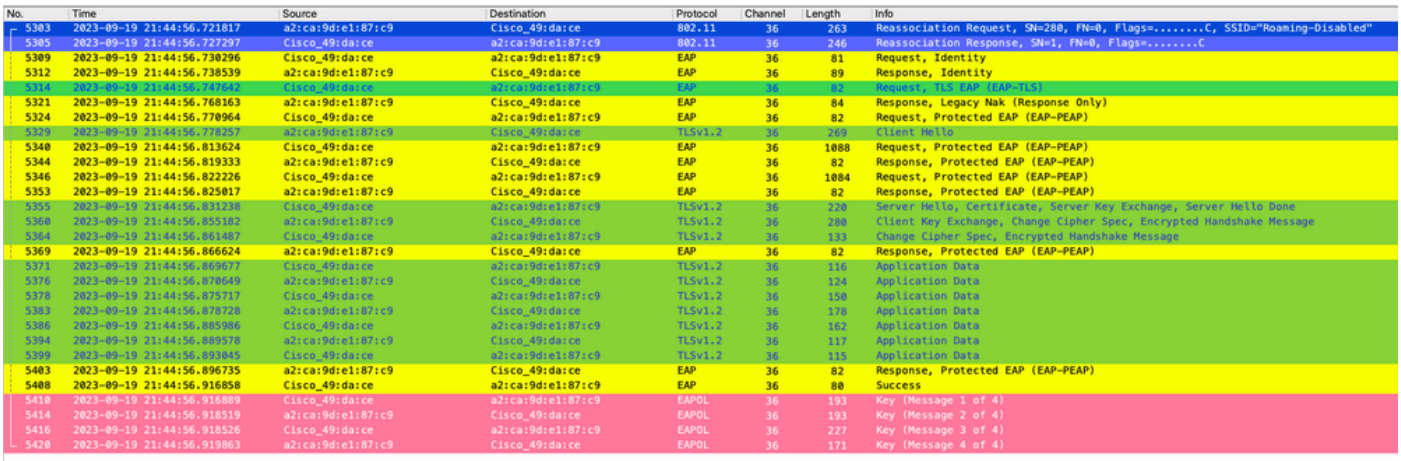



```
2023/09/19 21:54:25.913247615 {wncd_x_R0-0}{1}: [dot11] [15403]: (note): MAC: 62be.a38b.07c5 Associatio
!--- Reassociation Response is sent to the client.

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 mit deaktivierten Fast-Roam-Protokollen (802.11r, 802.11k und 802.11v)

In diesem Szenario sind alle Protokolle auf einer 802.1x-SSID deaktiviert. In diesem Fall erfährt der Client bei jedem Roaming des Wireless-Clients zwischen den Access Points eine vollständige Authentifizierung. Die nächste Abbildung zeigt ein Beispiel für einen drahtlosen Austausch, bei dem Sie sehen, dass der Client den EAP-Austausch nicht überspringen konnte. Daher wurde eine vollständige Neuauthentifizierung durchgeführt, da keine der schnellen Roamingmethoden aktiviert ist:



Nachfolgend finden Sie eine Zusammenfassung der RA-Ablaufverfolgungen des Controllers für dieses Roam-Ereignis:

```
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 mit aktivierter 802.11k-Funktion

Der 802.11k-Standard ermöglicht es Clients, einen Nachbarbericht anzufordern, der Informationen über APs enthält, die sich für ein Roaming innerhalb des Service Sets eignen. Auf diese Weise können Clients passiven oder aktiven RF-Scan vermeiden, bevor der Client beschließt, zu einem anderen Access Point zu wechseln. Der C9800 unterstützt eine Funktion namens 11k-unterstütztes Roaming, die eine optimierte Nachbarliste für 802.11k-Clients erstellt und bereitstellt. Die 802.11k-Nachbarliste wird bei Bedarf generiert und kann für zwei Clients an unterschiedlichen APs unterschiedlich sein, da der WLC die jeweilige Client-RF-Beziehung zu den umschlossenen

APs berücksichtigen würde.

Clients, die das 82.11k-Protokoll nicht unterstützen, senden keine Nachbar-Listenanforderungen. Dies ermöglicht eine Vorhersageoptimierung, die diesen Clients hilft. Dadurch wird eine Nachbarliste in der Mobilstationssoftware-Datenstruktur auf C9800 gespeichert.

Clients senden Anfragen für Nachbarlisten nur, nachdem sie eine Verbindung zu den Access Points hergestellt haben, die das RM-Funktionsinformationselement (IE) im Beacon ankündigen. Die folgende Abbildung zeigt ein Beispiel für 802.11k-Action-Frames, nachdem der Client dem Access Point zugeordnet wurde:

```
> 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
```

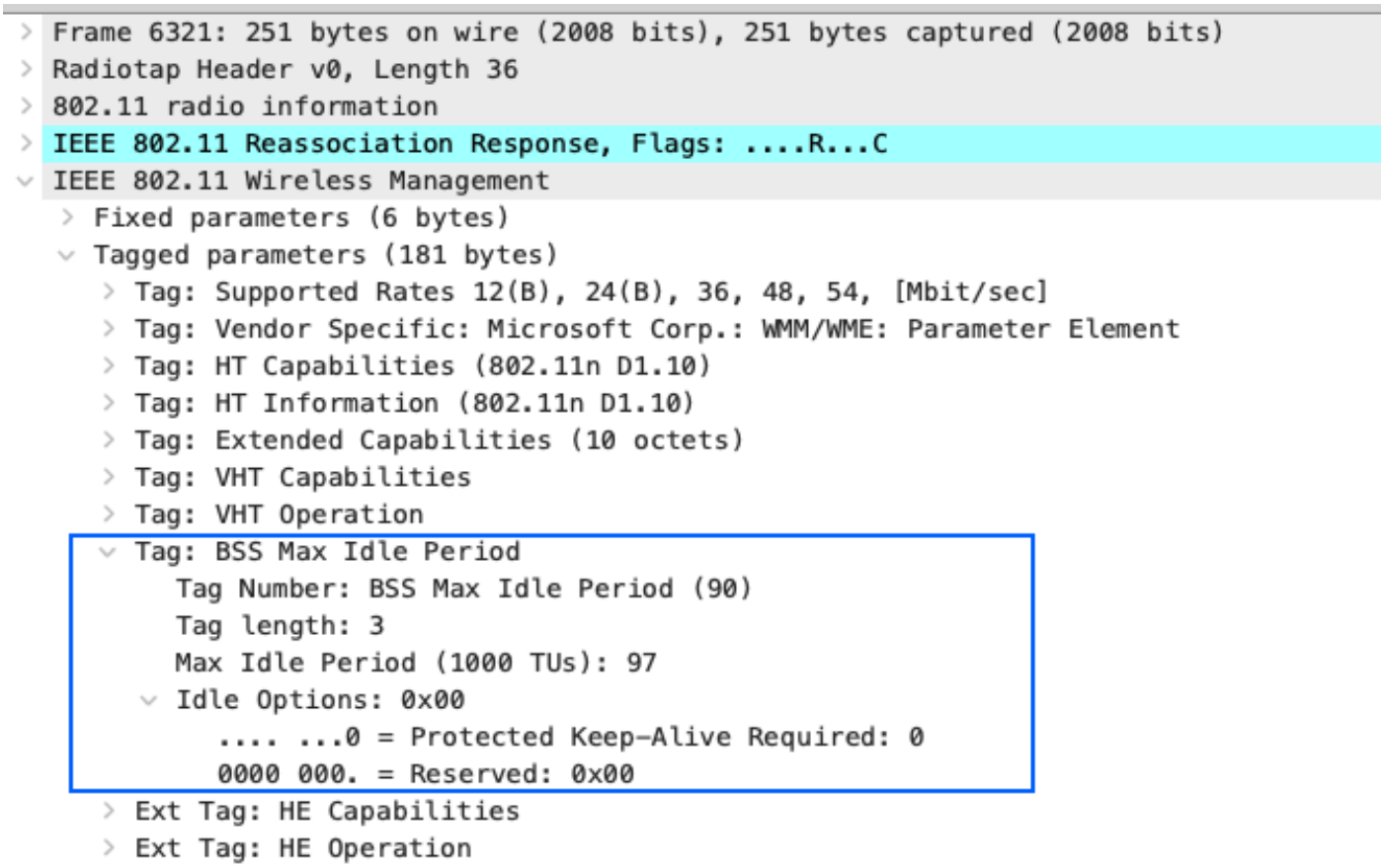
Over-the-Air Neighbor-Bericht

SSID mit aktivierter 802.11v-Technologie

Der 802.11v-Standard erweitert das Management des Wireless-Netzwerks um folgende Funktionen:

- Netzwerkgestützte Energiesparfunktion: Verbessert die Leistung des Client-Akkus bei maximaler Leerlaufzeit. Diese gibt die Dauer an, während der ein Client ohne gesendete Daten-Frames im Ruhemodus bleiben kann. Der Kunde wird über diese maximale Leerlaufzeit durch Zuordnungs- und Abtrennungs-Frames informiert.

Wenn ein Access Point für einen bestimmten Zeitraum keine Frames von einem Wireless-Client empfängt, geht er davon aus, dass der Client das Netzwerk verlassen hat, und trennt die Verbindung. Die maximale BSS-Leerlaufperiode gibt an, wie lange ein Access Point einen Client in Verbindung halten kann, ohne einen Frame empfangen zu müssen (der Client kann eingeschaltet bleiben, wodurch der Akku eingespart wird). Dieser Wert wird über den Antwortframe für die Zuordnung und die erneute Zuordnung an den Wireless-Client gesendet. Die nächste Abbildung zeigt den Wert in der Antwort auf die erneute Zuordnung vom Access Point, bei der die maximale BSS-Leerlaufperiode in Zeiteinheiten angegeben wird. Jedes Mal, wenn die Einheit 1,024 Millisekunden entspricht:



Wert des Over-the-Air BSS-Zeitraums

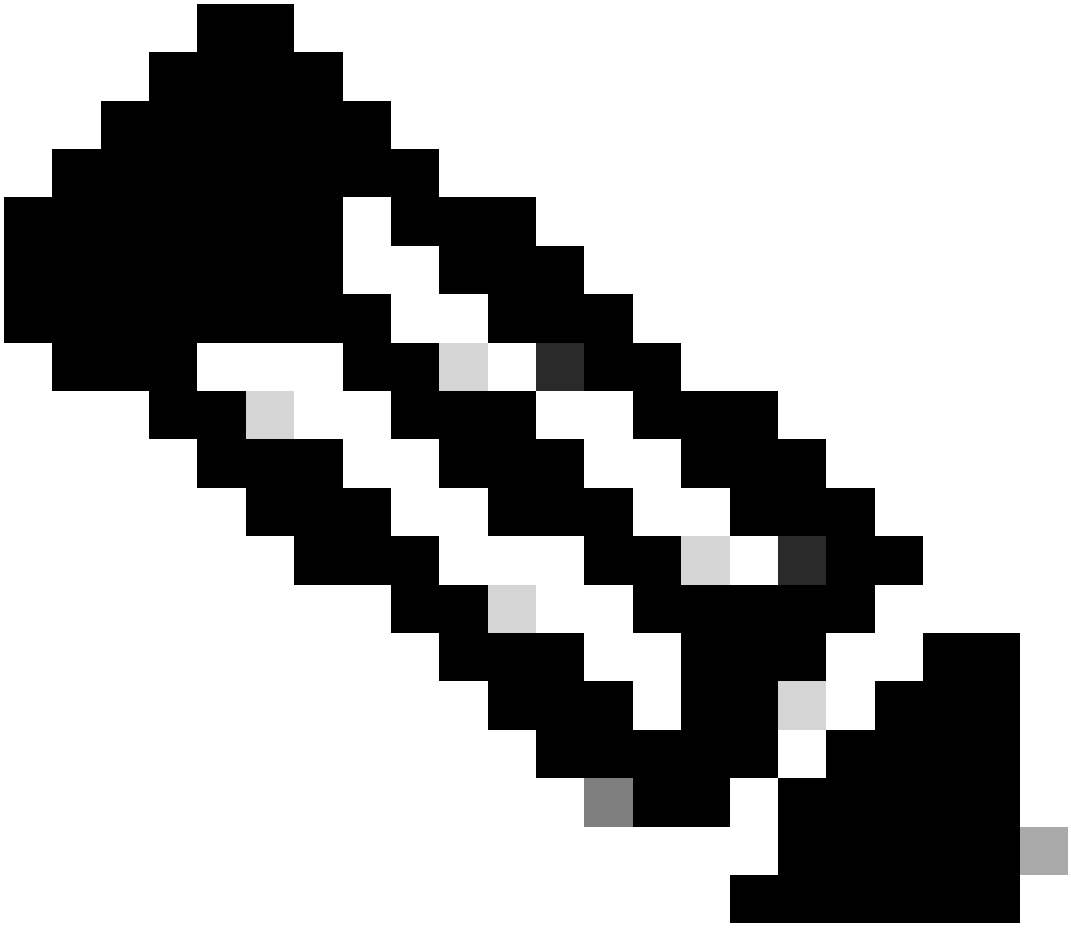
- Netzwerkunterstütztes Roaming: Ermöglicht der Wireless-Infrastruktur, dem Client das Roaming von seinem aktuellen Access Point aus vorzuschlagen. Dadurch erhält der Client eine Liste von Access Points, zu denen er im selben erweiterten Service Set (ESS) wechseln kann.

802.11v BSS Transition Management Frames werden in drei Szenarien ausgetauscht:

1. Angeforderte Anforderung: Vor dem Übergang zu einem neuen Access Point hat der Client die Möglichkeit, eine 802.11v BSS Transition Management Query zu senden, um bessere Optionen für Access Points zu ermitteln, denen neu zugeordnet werden kann. Der aktuelle AP, mit dem der Client verbunden ist, antwortet mit einer BSS Transition Management Request, die eine Liste der möglichen Access Points bereitstellt, zu denen Roaming übertragen werden kann.

2. Unerwünschte Lastenausgleichsanforderung: Eine Funktion, mit der der Access Point Clients an Access Points auf demselben Controller lastenausgleichen kann, um eine Überlastung des Access Points zu vermeiden. Wenn die Client-Anzahl den konfigurierten Lastenausgleichschwellenwert für einen Access Point überschreitet, wird jedem neuen Client, der versucht, eine Verbindung zum Access Point herzustellen, eine Zuordnungsantwort mit dem Status 17 (AP besetzt) verweigert. In der Regel versuchen die abgelehnten Clients, eine Verbindung mit demselben geladenen Access Point herzustellen, auch nachdem der Client eine Ablehnung der Zuordnung erhalten hat, d. h. wenn dieser Access Point aus RSSI-Sicht die beste Option ist. Nehmen wir als Beispiel 40 Benutzer in einem Konferenzraum, der von einem AP bedient wird. Mit einer 802.11v BSS Transition Management-Abfrage kann ein Lastenausgleichsfehler reibungsloser gehandhabt werden, wenn der Access Point stattdessen eine Liste potenzieller Access Points zum Roaming sendet.

3. Unerwünschte optimierte Roam-Anforderung: Von den Wireless-Clients wird erwartet, dass sie RF scannen und mit dem höchsten Signal zu AP roamen. Einige Clients zeigen jedoch ein klebriges Verhalten, wenn sie beim AP verbleiben, dem sie zugeordnet sind, selbst wenn ein Nachbar-AP ein stärkeres Signal liefert. Dies wird als klebriges Client-Problem bezeichnet. Um dieses Problem zu beheben, unterstützt der Controller 9800 eine Funktion namens optimiertes Roaming, bei der das RSSI der Client-Datenpakete und die Datenrate überwacht werden und der Client proaktiv getrennt wird. Die 802.11v BSS Transition Management Request verbessert das optimierte Roaming, wodurch der Client von einer drohenden Trennung in Kenntnis gesetzt wird und eine Liste der APs bereitgestellt wird, zu denen das Roaming erfolgen kann.



Hinweis: Aus TAC-Erfahrung ist Optimized Roam nicht für alle Netzwerke geeignet. Vergewissern Sie sich, dass die Abdeckung zwischen den Access Points ausreichend ist, damit dies wie erwartet funktioniert, da andernfalls weitere Probleme auftreten könnten, wenn Sie die Funktion aktivieren.

Eine 802.11v BSS Transition Management Request, die, wenn sie von einem Access Point an einen Client gesendet wird, nur einen Vorschlag darstellt. Der Kunde kann den Vorschlag honorieren oder verwerfen. Der Wireless-Controller 9800 bietet eine Konfigurationsoption mit der Bezeichnung "Imminent Disassociation" (unmittelbare Trennung), mit der Sie die Clients zwingen können, die Verbindung zu trennen, wenn der Client innerhalb eines festgelegten Zeitfensters keine Neuzuweisung zu einem anderen Access Point vornimmt. Sie können sie nur über den CLI-Befehl bss-sition disassociation-imminent unter einem bestimmten WLAN-Profil konfigurieren.

Zugehörige Informationen

- Schneller Umstieg auf 802.11r BSS

- 802.11k: Nachbarliste und unterstütztes Roaming
- 802.11v BSS
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.