Understand 802.11r/11k/11v Fast Roams on 9800 WLCs

Contents

Introduction

This document describes the different outcomes when fast roam methods are enabled/disabled on the wireless clients.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- IEEE 802.11 WLAN Fundamentals.
- IEEE 802.11 WLAN Security.
- IEEE 802.1X/EAP Basics.
- IEEE 802.11r BSS Fast Transition.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Wireless 9800-L Controller IOS® XE 17.9.4
- Cisco Catalyst 9130AXI Series Access Point.

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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This document helps you understand the difference when you have the protocols 802.11r, 802.11v, and 802.11k enabled on a 9800 wireless controller. It also explains what the impact is on the clients when you have them disabled.

802.11r, 802.11v, and 802.11k are all different standards or amendments within the 802.11 family of wireless network protocols.

802.11r: Is the Fast Transition across basic service sets which introduces a new concept where the initial handshake with a new AP is done even before the client roams to the target access point. It is particularly useful in environments where uninterrupted connectivity is crucial, such as in voice-over-IP or real-time stream applications with video or constant stream monitor. With a tuned 802.11r network, devices can roam between access points without the significant experience disruptions or drops in network connectivity.

802.11k: Neighbor List and Assisted Roam (Radio Resource Measurement) leverages the features of radio resource management to improve the overall performance and reliability of wireless networks. It optimizes available radio resources where access points collect and share information about their radio environment. This information includes channel usage, signal strength, and interference levels. It can then be used by client devices to make more informed decisions about which AP to connect to; which results in better load balance, reduced interference, and improved network efficiency.

802.11v: Is a Network assisted Power Save which helps clients to improve the battery life which allows them to sleep longer. It also focuses on how to enhance the efficiency and management of wireless networks. This in turn, enables a better control and coordination between the network infrastructure and client devices when clients roam. The primary features are neighbor reports, service set transitions, load balance, and network-assisted power save. These features enhance client network discovery, selection, and monitoring. It also allows the access points to encourage client devices to roam instead of waiting for the device to make a roam decision.

While 802.11r focuses on seamless transition between APs, 802.11v aims to enhance network management capabilities. The 802.11k is designed to optimize radio resource utilization for better performance and reliability.

Some statements in this document are from book **Understanding and Troubleshooting Cisco Catalyst 9800 Series Wireless Controllers** Chapter 6, 802.11 Roam section.

Higher-Level Security Roams

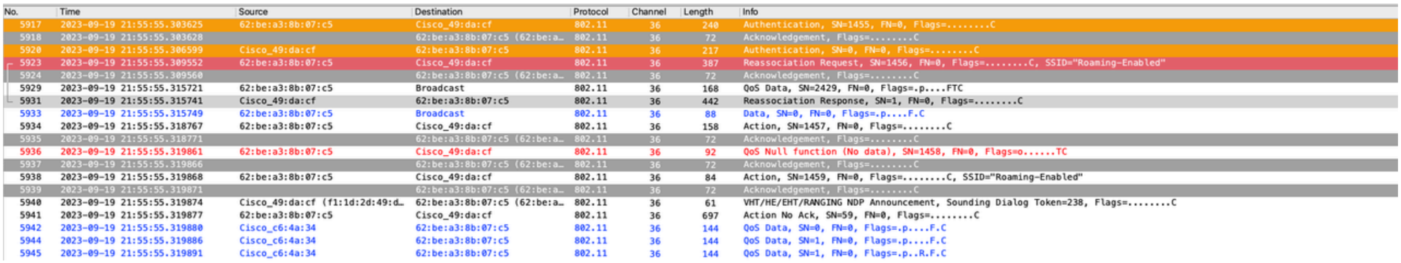
When the SSID is configured with L2 higher-level security on top of basic 802.11 Open System authentication, then more frames are required for the initial association and when clients roam. The two most-common security methods standardized and implemented for 802.11 WLANs are:

- WPA/WPA2/WPA3 Personal: A PSK is used to authenticate the clients.
- WPA/WPA2/WPA3 Enterprise: The Extensible Authentication Protocol (EAP) method and 802.1x is used to authenticate the wireless clients, which is to validate the user credentials (username and password), certificates, or tokens via a AAA server.

In this document, WPA2 Enterprise WLAN can be used with EAP-PEAP to show the difference in the use of the IEEE protocols (802.11r, 802.11k, and 802.11v) and how it could affect the wireless roam attempts.

SSID with Fast Roam Protocols Enabled (802.11r, 802.11k, and 802.11v)

The default WLAN configuration has every protocol enabled by default. In the lab, the wireless client attempts to roam between 9130 access points. Since you have the default configuration of the WLAN, in other words, fast roam is enabled addition to 802.11v and 802.11k, you would expect a seamless roam. Here is an example of an over-the-air OTA capture for a roam even:

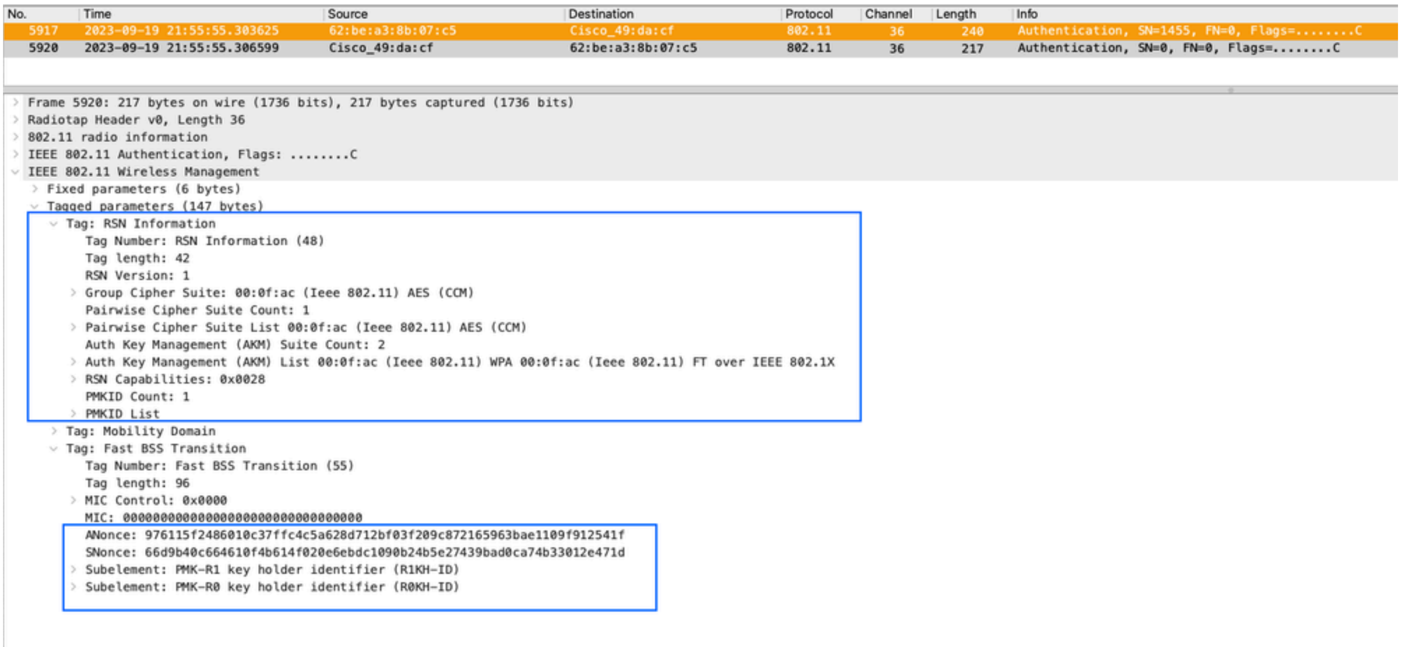


No.	Time	Source	Destination	Protocol	Channel	Length	Info
5917	2023-09-19 21:55:55.303625	62:be:a3:8b:07:c5	Cisco_49:da:cf	802.11	36	240	Authentication, SN=1455, FN=0, Flags=........C
5918	2023-09-19 21:55:55.303628		62:be:a3:8b:07:c5 (62:be:a…	802.11	36	72	Acknowledgement, Flags=........C
5920	2023-09-19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

Here is the RA traces for this roam event:

```
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
```

As 802.11r is enabled, the initial handshake with a new AP is done even before the client roams to the target access point. This concept is called Fast Transition. The initial handshake allows a client and the access points to do the Pairwise Transient Key (PTK) calculation in advance. These PTK keys are applied to the client and the access points after the client responds to the reassociation request or responds to the exchange with the new target AP:



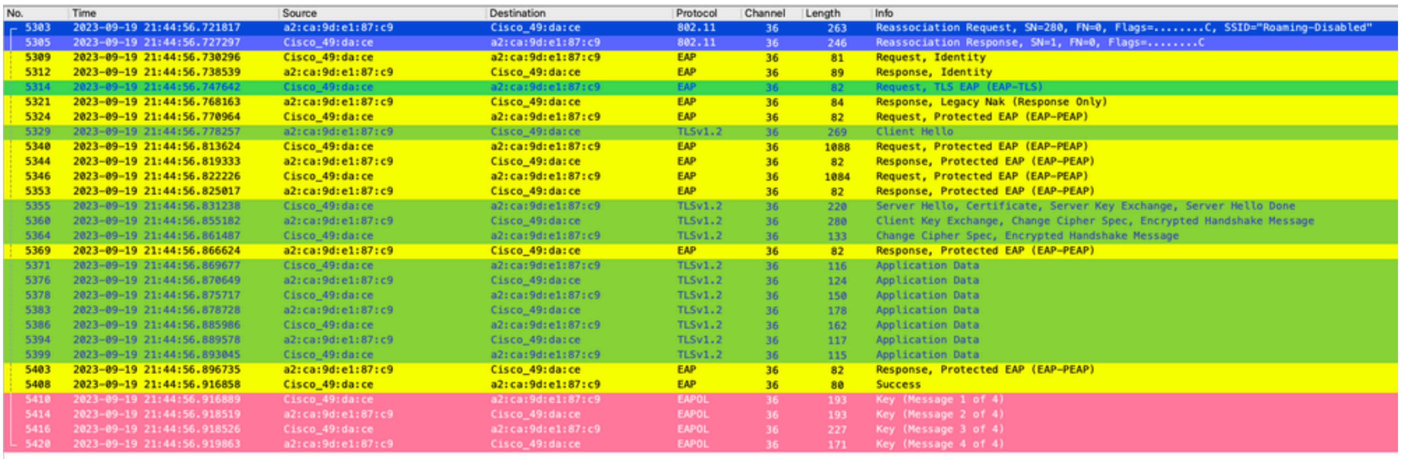
No.	Time	Source	Destination	Protocol	Channel	Length	Info
5917	2023-09-19 21:55:55.303625	62:be:a3:8b:07:c5	Cisco_49:da:cf	802.11	36	240	Authentication, SN=1455, FN=0, Flags=........C
5920	2023-09-19 21:55:55.306599	Cisco_49:da:cf	62:be:a3:8b:07:c5	802.11	36	217	Authentication, SN=0, FN=0, Flags=........C

```
> 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
v IEEE 802.11 Wireless Management
   > Fixed parameters (6 bytes)
   v Tagged parameters (147 bytes)
      v 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
      v 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 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 with Fast Roam Protocols Disabled (802.11r, 802.11k, and 802.11v)

In this scenario, all of the protocols are disabled on a 802.1x SSID, in this case, the client experiences a full authentication each time the wireless client roams between the access points, next figure shows an example of an over-the-air exchange where you can see the client could not skip the EAP exchange. Therefore, a full re-authentication took place because none of the fast roam methods are enabled:



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)

Over-The-Air Protocols Disabled

Here is a summary of the controller RA traces for this roam event:

```
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 E
```

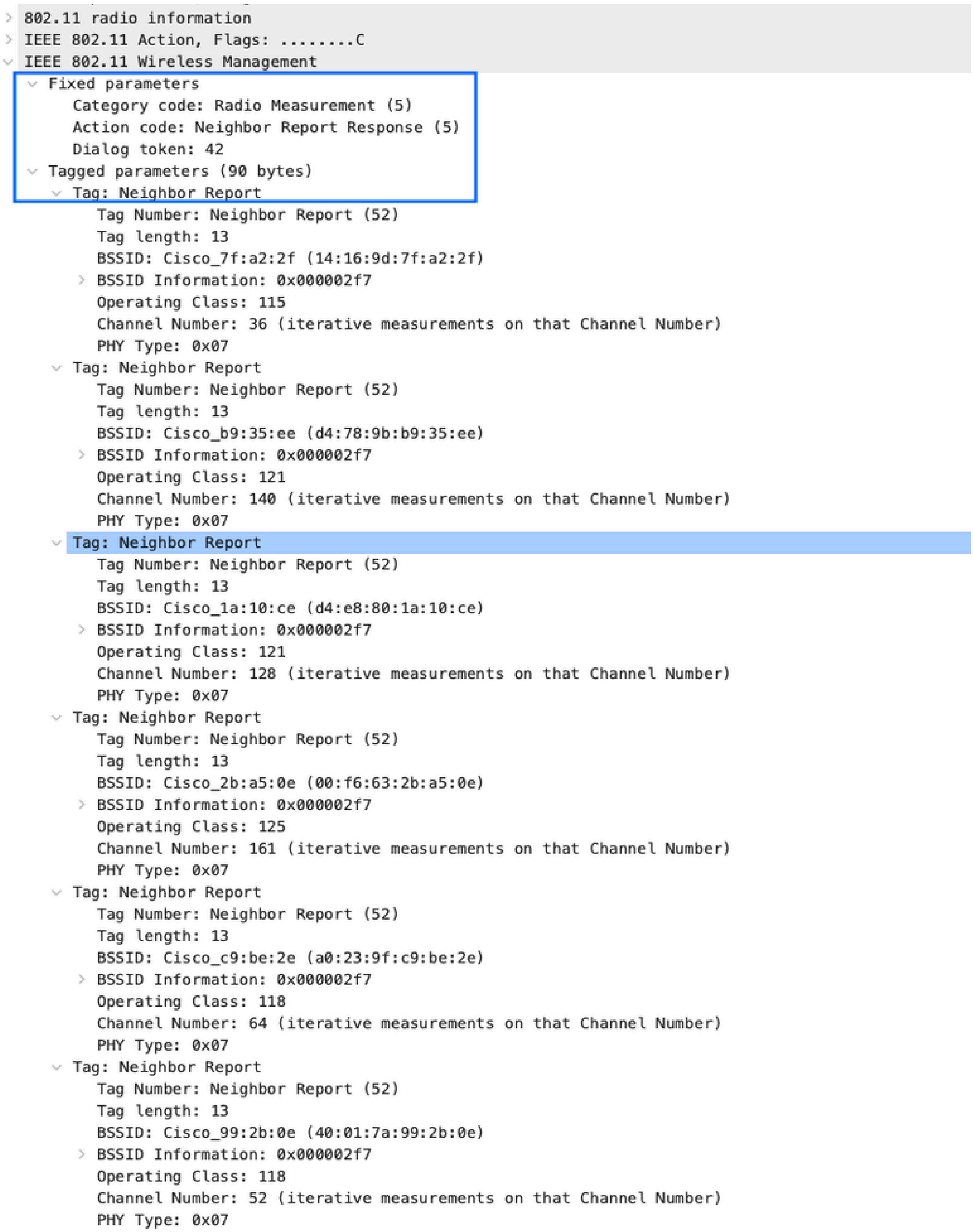
```
2023/09/19 21:44:47.662831295 {wncd_x_R0-0}{1}: [client-keymgmt] [15403]: (info): MAC: a2ca.9de1.87c9 M

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.
```

SSID with 802.11k Enabled

The 802.11k standard allows clients to request a neighbor report that contains information about APs that are good candidates for a roam within the service set. This enables clients to avoid passive or active RF scan before the client decides to move to a different access point. The C9800 supports a feature called 11k assisted roami, which creates and delivers an optimized neighbor list to the 802.11k clients. The 802.11k neighbor list is generated on demand and can be different for two clients on different APs because the WLC would consider the individual client RF relationship with the surrounded APs.

Clients that do not support 82.11k protocol, do not send neighbor list requests. This enables prediction optimization that helps those clients. As a result, a neighbor list is stored in the mobile station software data structure on C9800.

Clientssend requests for neighbor lists only after they associate with the access points that advertise the RM capability Information Element (IE) in the beacon. This next figure is an example of 802.11k action frames after the client got associated with the access point:



```
> 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
```

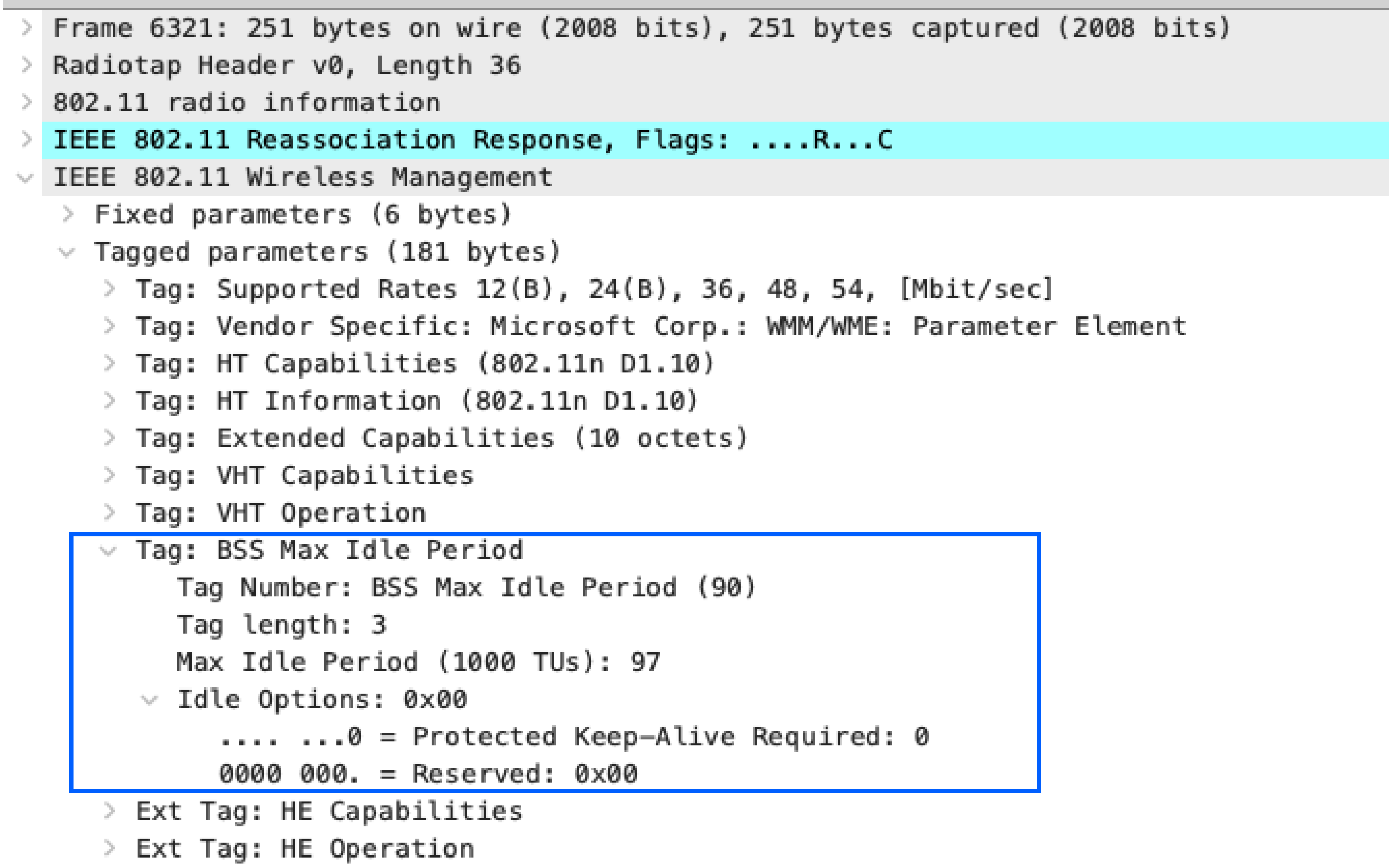
Over-The-Air Neighbor Report

SSID with 802.11v Enabled

With the 802.11v standard, the two main enhancements to the wireless network management include:

- **Network-assisted power save feature**: Enhances the client battery performance with a maximum idle period, which indicates the duration where a client can remain in a sleep mode without any data frames sent. The client is notified about this maximum idle period through association and disassociation frames.

If an access point does not receive frames from a wireless client for a certain period of time, it assumes the client left the network and disassociates it. The BSS Max idle period is the amount of time an AP can keep a client associated without having to receive any frame (client can remain asleep, this saves battery). This value is sent to the wireless client through the association and re-association response frame. The next figure shows the value in the re-association response from the access point, where the BSS Max Idle Period is specified in time units. Every time the unit is equal to 1.024 milliseconds:



```
> 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
```

Over-The-Air BSS Period Value

- **Network-assisted roam:** Enables the wireless infrastructure to suggest that the client roam away from its current access point. This provides the client the list of access points that it can roam to in the same extended service set (ESS).

802.11v BSS transition management frames are exchanged in three scenarios:

1. Solicited Request: Before the transition to a new access point, the client has the ability to send an 802.11v BSS Transition Management Query to find out better options of access points to reassociate with, and the current AP where the client is connected, respond with a BSS transition management request which provides the list of candidate access points to roam to.

2. Unsolicited load-balance request: A feature that allows the AP to load balance clients across access points

on the same controller to avoid AP overload. When the client counts exceed the configured load balance threshold for an AP, any new client that tries to associate with the AP is denied with an association response with status 17 (AP busy). Typically, the denied clients tries to associate to the same loaded AP even after the client gets an association reject, that is if from the RSSI perspective, that AP is their best option. For example, consider 40 users in a conference room serviced by one AP. With an 802.11v BSS Transition Management query, a load balance failure can be handled more smoothly where the AP sends a list of candidate APs to roam to instead.

3. Unsolicited optimized roam request: The wireless clients are expected to scan RF and roam to AP with the highest signal. However, some clients have displayed a sticky behavior where they stay with the AP to which they are associated, even when a neighbor AP provides a stronger signal. This is referred to as a sticky client problem. To address this problem, the 9800 controller supports a feature called optimized roam where the RSSI of the client data packets and data rate are monitored, and the client is proactively disassociated. The 802.11v BSS Transition Management Request enhances optimized roam which tells the client of an imminent disassociation and provides a list of APs to roam to.

Note: From TAC experience, Optimized Roam is not suitable for all networks. Make sure the coverage is good enough between access points to make this work as expected, otherwise more problems could come up if you enable it.

An 802.11v BSS Transition Management Request which when sent by an AP to a client is only a suggestion. The client can honor the suggestion or discard it. The 9800 wireless controller provides a configuration option called Imminent Disassociation for you to force the clients to disassociate if the client does not reassociate with another AP within a defined window of time. You can configure it only from CLI via command **bss-transition disassociation-imminent** under a specific WLAN profile.

Related Information

- 802.11r BSS Fast Transition
- 802.11k Neighbor List and Assisted Roaming
- 802.11v BSS
- Cisco Technical Support & Downloads