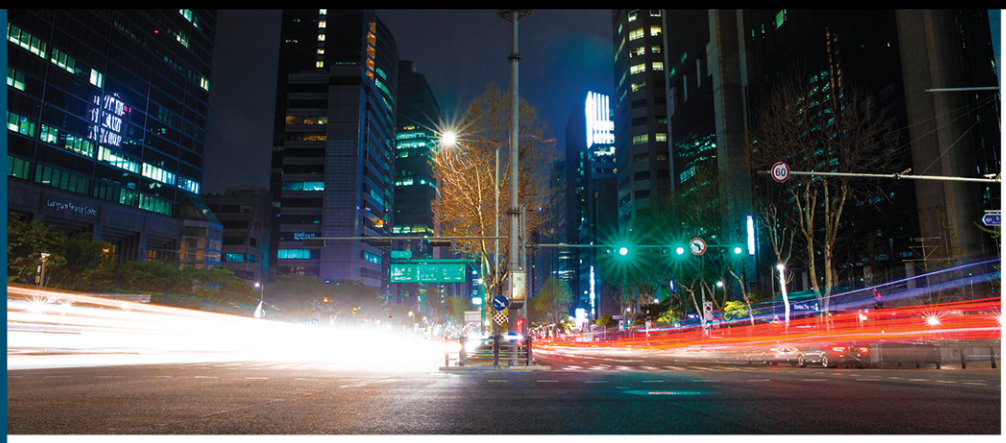

Understanding and Troubleshooting Cisco Catalyst 9800 Series Wireless Controllers

SIMONE ARENA
FRANCISCO SEDANO CRIPPA, CCIE® NO. 14859
NICOLAS DARCHIS, CCIE® NO. 25344
SUDHA KATGERI, CCIE® NO. 45857

ciscopress.com

Understanding and Troubleshooting Cisco Catalyst 9800 Series Wireless Controllers

Simone Arena
Francisco Sedano Crippa, CCIE No. 14859
Nicolas Darchis, CCIE No. 25344
Sudha Katgeri, CCIE No. 45857

Cisco Press

```
> IEEE 802.11 Reassociation Request, Flags: ........C
v IEEE 802.11 Wireless Management
   > Fixed parameters (10 bytes)
   v Tagged parameters (271 bytes)
      > Tag: SSID parameter set: OKC
      > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
      > Tag: Power Capability Min: -9, Max: 17
      > Tag: Supported Channels
      v Tag: RSN Information
           Tag Number: RSN Information (48)
           Tag length: 38
           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: 1
         > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) WPA
         > RSN Capabilities: 0x008c
           PMKID Count: 1
         v PMKID List
             PMKID: efdd9cb1ef752e98d80db8433376cbab
      > Tag: RM Enabled Capabilities (5 octets)
      > Tag: Supported Operating Classes
      > Tag: HT Capabilities (802.11n D1.10)
```

Figure 6-5 *OKC fast roam RSN IE*

OKC is enabled by default on the C9800 and cannot be disabled for central authentication either for local or FlexConnect deployment. It can only be disabled for FlexConnect local authentication. To do this, on the C9800 GUI, navigate to **Configuration > Tags and Profiles > WLANs > Advanced** and uncheck **OKC**, as shown in Figure 6-6.

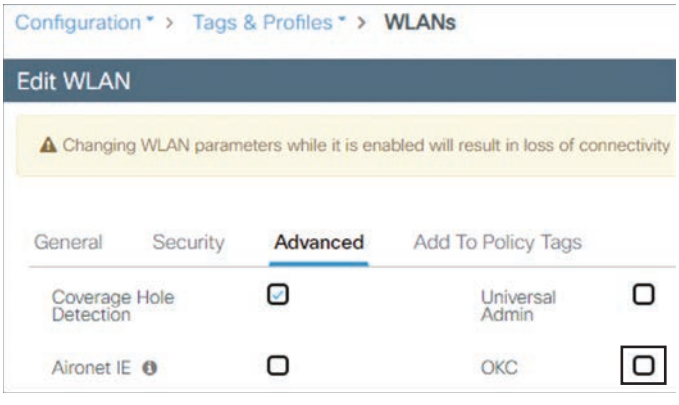

Figure 6-6 *Disabling OKC for FlexConnect local authorization*

The type of client that roams using OKC is reflected as 802.11i. On the C9800 GUI, navigate to **Monitoring > Wireless > Clients > Mobility History**, as shown in Figure 6-7.

The equivalent command-line interface (CLI) is **#show wireless client mac-address <mac-address> mobility history.**

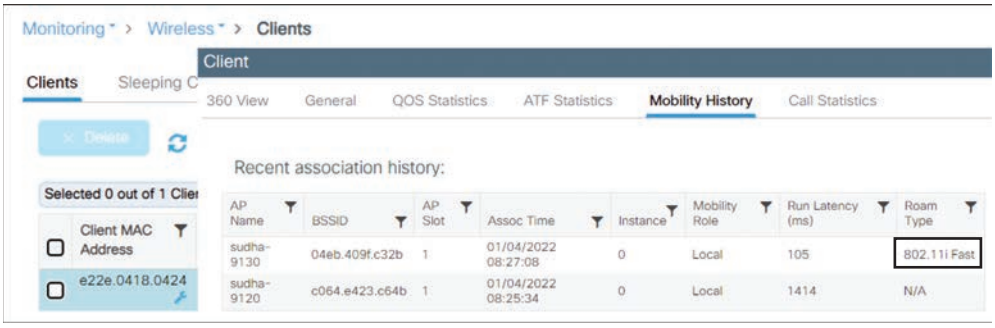

Figure 6-7 *Monitoring the client roam type on the C9800*

- **Pros with OKC:** The client requires only one full 802.1X/EAP authentication and can fast-secure roam to APs that it has not previously associated to. Also, the wireless client and infrastructure don't need to store multiple PMKIDs but only the original PMK from the initial 802.1X/EAP authentication, making this a scalable method.
- **Cons with OKC:** This method is not an 802.11 standard, so client support may not be there. However, this is one of the popular alternatives to 802.11r or Fast Transition (FT) method.

CCKM

Cisco Centralized Key Management (CCKM) is a Cisco proprietary fast-secure roaming method only supported by Cisco wireless infrastructure devices and wireless clients from different vendors that are Cisco Compatible Extension (CCX)-compatible. Support for CCKM is indicated in the Auth Key Management (AKM) Suite of RSN IE sent in beacon, probe response, and association request frames.

With CCKM, like regular WPA/WPA2, an MSK (also known as the Network Session Key, or NSK) is mutually derived between the client and the AAA server. This master key is sent from the AAA server to the WLC after a successful authentication. The WLC and the client derive the seed information from NSK and go through a four-way handshake like WPA/WPA2, to derive the unicast (PTK) and multicast/broadcast (GTK) encryption keys with the first AP.

When the CCKM client roams, it sends a single reassociation request frame to the AP/WLC, including a message integrity check (MIC) and a sequentially incrementing random number. This information, combined with BSSID of the roam-to AP, is used to derive PTK by the client as well as the wireless infrastructure. Because PTK can be derived with reassociation request itself, a four-way handshake, in addition to EAP authentication, is skipped. AP responds with a reassociation response, and the client can continue to forward data.

CCKM is supported with central authentication for local mode and FlexConnect deployments. With FlexConnect local authentication, in connected mode, the cache is distributed from the AP to the C9800 and then to other APs in the FlexConnect site tag. In standalone mode, only cached entries work; new authentications do not work. Enabling CCKM requires you to explicitly disable the Fast Transition setting, as shown in Figure 6-8.

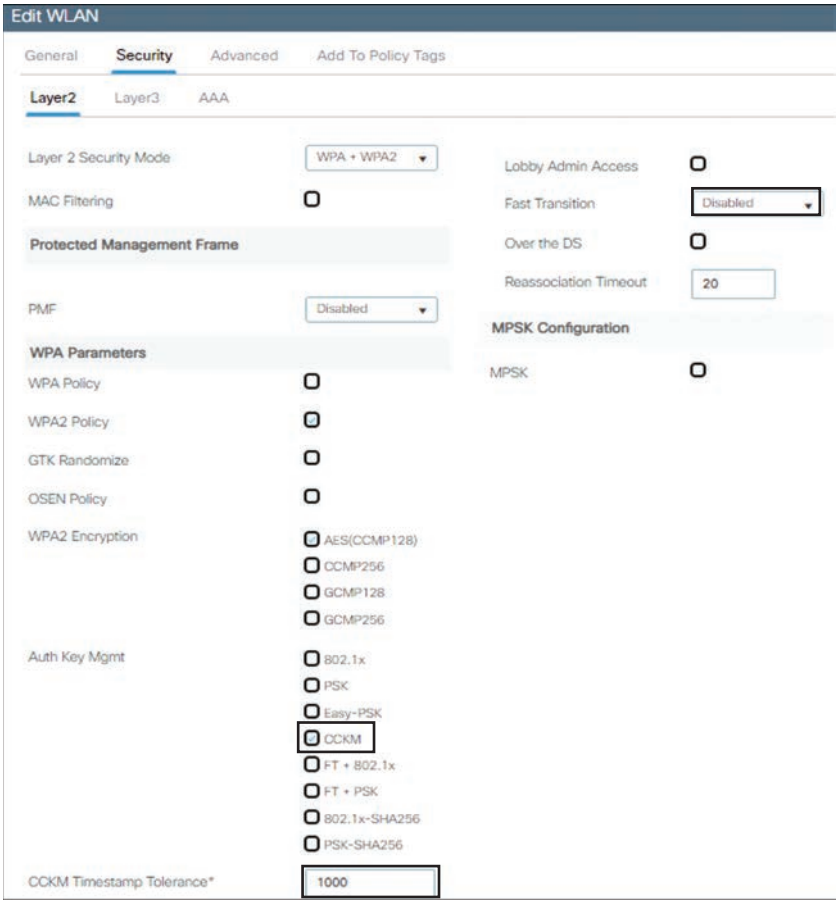

Figure 6-8 *Configuring CCKM on the C9800*

- **Pros with CCKM:** CCKM is faster than SKC and OKC because a four-way handshake and an EAP/802.1X exchange are avoided. It supports all the encryption methods within the 802.11 standard: Wired Equivalent Privacy (WEP), Temporal Key Integrity Protocol (TKIP), and Advanced Encryption Standard (AES).
- **Cons with CCKM:** Because CCKM is proprietary, it is supported only on Cisco wireless infrastructure and CCX wireless clients. Lack of adoption means CCKM is essentially obsolete and is only relevant in Cisco work group bridge (WGB) deployments, which only support CCKM.

Fast Transition (802.11r)

The 802.11r Fast Transition (FT) or Fast Basic Service Set (BSS) Transition is the IEEE standard for fast secure roaming. In Fast BSS Transition, the initial handshake with the new AP occurs before the client roams to it, thus reducing the roam time. During this initial handshake itself, PTK is derived both by client and wireless infrastructure, and data forwarding begins immediately after reassociation completes. The 802.11r adds a new Authentication Key Management (AKM) suite under WLAN profile configuration called FT.

In FT deployment, the first client association to a wireless network goes through the normal full authentication process, including 802.11 open authentication, association, EAP exchange, and four-way key handshake to let the client forward data. Beyond that, the 802.11 management frames all carry additional 802.11r information to complete FT negotiation as described next.

Beacon and Probe Responses

The 802.11r information carried in the 802.11 beacons and probe responses sent from the AP is shown in Figure 6-9 and Figure 6-10. The 802.11r fields contained within these 802.11 management frames are as follows:

1. Mobility Domain Information Element (MDIE), which includes
   - Element ID 54.
   - A Mobility Domain Identifier (MDID) that identifies groups of APs capable of FT. This MDID can be verified from the C9800 CLI with **#show wireless mobility summary**.
   - The FT capability set to 1.
   - The FT Over-the-DS field, which indicates how the client exchanges messages with the target AP to complete the FT roam.
     - If it is set to 1, the client does FT roaming to target the AP via the current AP over the wired network, referred to as FT over the distribution system (DS).
     - If it is set to 0, the client does FT roaming to target the AP directly over 802.11. On C9800, all WLANs perform FT key exchange over-the-air by default.
2. The Robust Security Network Information Element (RSN IE) in the beacon is determined by the FT mode in use.
   - **FT only**: Includes the FT AKM suite.
   - **FT Mixed Mode**: Includes two AKM suites: PSK/802.1X and PSK/802.1X FT over IEEE.
- **FT Adaptive**: Includes one AKM suite: PSK or 802.1X.

The difference between these modes is discussed further in the next subsection.

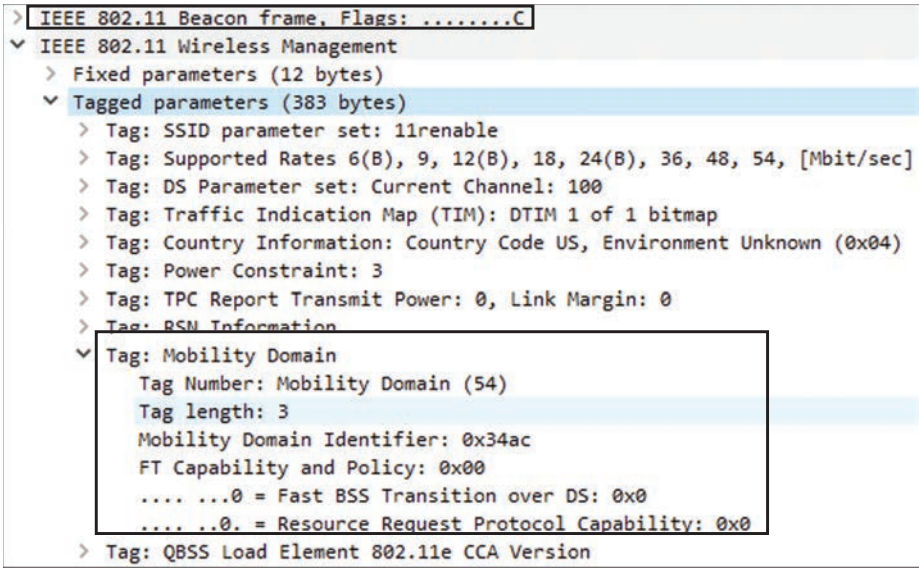

Figure 6-9 *802.11r FT Beacon MDIE*

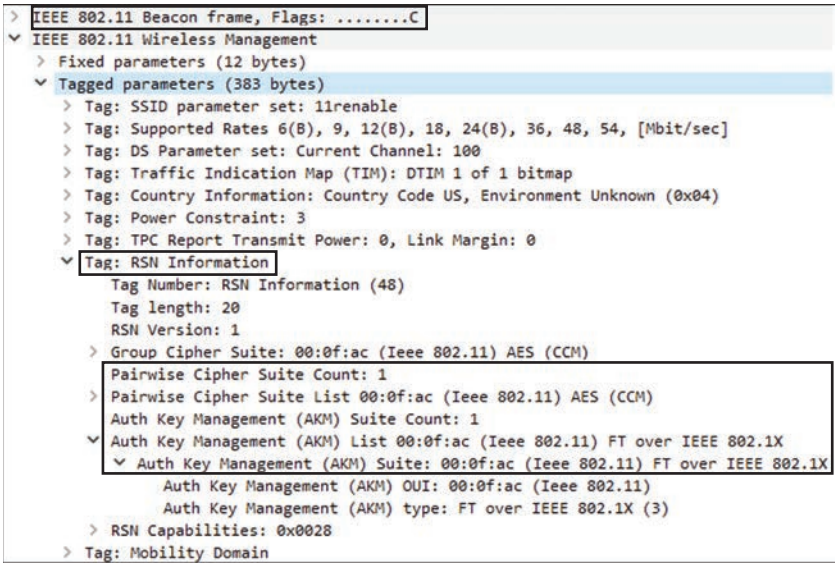

Figure 6-10 *802.11r FT Beacon RSN IE AKM*

Association Request

The association request is sourced from a wireless client and includes MDIE and FT over IEEE 802.1X AKM suite in RSN IE.

Association Response

The association response from the C9800/AP shown in Figure 6-11 includes the Fast BSS Transition Information Element (FTIE) in addition to MDIE. The FTIE includes information such as the MIC, nonces, PMK-R0 key holder identifier (R0KH-ID), and PMK-R1 key holder identifier (R1KH-ID), which are needed to perform the FT authentication sequence during a Fast BSS Transition.

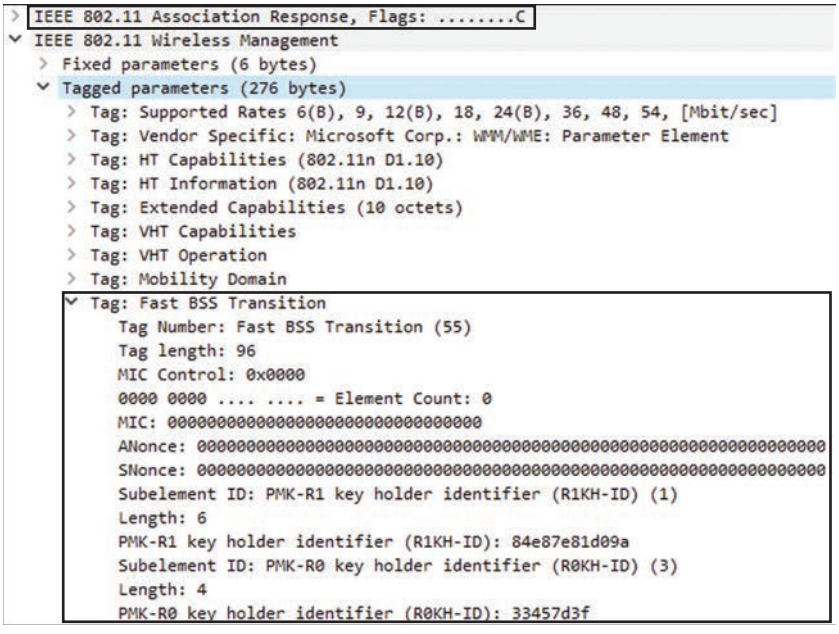

Figure 6-11 *802.11r FT association response*

Authentication

After association, PSK or 802.1X authentication kicks off. As with the other methods, MSK is derived from PSK or 802.1X/EAP authentication, both by the client and the AAA server. The MSK is used as a seed for the FT key hierarchy.

After authentication, an FT four-way handshake occurs. FT specifies three layers of key hierarchy that are cached:

1. **PMK-R0**: The Pairwise Master Key (PMK-R0) is the first level PMK and is derived from the MSK. The key holders for this PMK are the WLC (R0KH) and the client (S0KH).
2. **PMK-R1**: The Pairwise Master Key (PMK-R1) is the second level PMK and is derived from the PMK-R0 by the WLC. The WLC uses a secure channel to transmit unique PMK-R1 to each AP in the mobility domain. The key holders of PMK-R1 are the APs (R1KH) managed by the WLC and the client (S1KH).