Determinar métodos para WLAN 802.11 e roaming rápido seguro no CUWN

Contents

Introduction

Este documento descreve os tipos de roaming sem fio e rápido-seguro disponíveis para LANs sem fio IEEE 802.11 (WLANs) em Unified Wireless Network (CUWN).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Fundamentos de WLAN do IEEE 802.11
- Segurança de WLAN IEEE 802.11
- Conceitos básicos de IEEE 802.1X/EAP

Componentes Utilizados

As informações neste documento são baseadas no software Cisco WLAN Controller versão 7.4.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

As informações neste documento são baseadas no Cisco WLAN Controller Software Versão 7.4, mas a maioria das saídas e comportamentos de depuração descritos podem ser aplicados a qualquer versão de software que suporte os métodos discutidos. As especificações de todos os métodos explicados aqui permanecem as mesmas nos códigos posteriores da Cisco WLAN Controller (até a versão 8.3 quando este artigo foi atualizado).

Este documento descreve os diferentes tipos de roaming sem fio e métodos de roaming rápido-seguro disponíveis para LANs sem fio (WLANs) IEEE 802.11 suportadas no Cisco Unified Wireless Network (CUWN).

O documento não fornece todos os detalhes sobre como cada método funciona ou como eles são configurados. O objetivo principal deste documento é descrever as diferenças entre as várias técnicas disponíveis, suas vantagens e limitações e a troca de quadros em cada método. São fornecidos exemplos de depurações de controladoras de WLAN (WLC) e imagens de pacotes sem fio são usadas para analisar e explicar os eventos que ocorrem para cada método de roaming descrito.

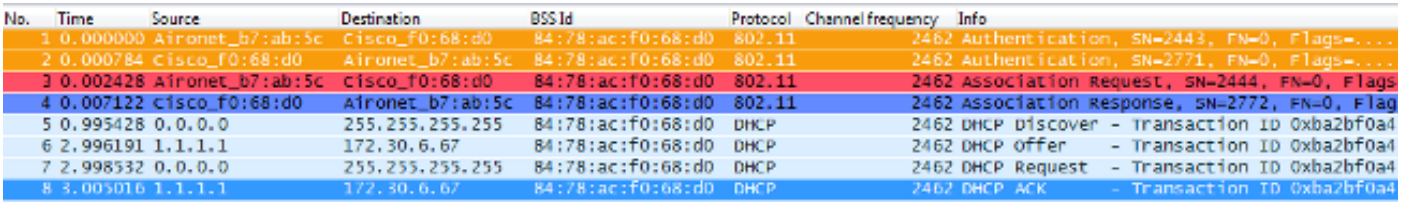
Antes de fornecer uma descrição dos diferentes métodos de roaming rápido disponíveis para as WLANs, é importante entender como o processo de associação da WLAN funciona e como um evento de roaming regular ocorre quando não há segurança configurada no Identificador do Conjunto de Serviços (SSID).

Quando um cliente sem fio 802.11 se conecta a um ponto de acesso (AP), antes de começar a passar o tráfego (quadros de dados sem fio), ele primeiro deve passar o processo básico de autenticação do sistema aberto 802.11. Em seguida, o processo de associação deve ser concluído. O processo de autenticação Open System é como uma conexão a cabo no AP que o cliente seleciona. Esse é um ponto muito importante, pois é sempre o cliente sem fio que seleciona qual AP é o preferido e baseia a decisão em vários fatores que variam entre os fornecedores. É por isso que o cliente começa esse processo enviando o quadro de Autenticação para o AP selecionado, como mostrado mais adiante neste documento. O AP não pode solicitar

que você estabeleça uma conexão.

Uma vez que o processo de autenticação do sistema aberto é concluído com êxito com uma resposta do AP ("cabo conectado"), o processo de associação essencialmente termina a negociação da camada 2 (L2) 802.11 que estabelece o link entre o cliente e o AP. O AP atribui um ID de associação ao cliente se a conexão for bem-sucedida e o prepara para passar tráfego ou executar um método de segurança de nível superior se configurado no SSID. O processo de autenticação Sistema aberto consiste em dois quadros de gerenciamento, bem como o processo de associação. Os quadros de autenticação e associação são **quadros de gerenciamento** sem fio, não quadros de dados, que são basicamente aqueles usados para o processo de conexão com o AP.

Esta é uma imagem dos quadros sem fio no ar para este processo:



No.	Time	Source	Destination	BSS Id	Protocol	Channel frequency	Info
1	0.000000	Aironet_b7:ab:5c	Cisco_f0:68:d0	84:78:ac:f0:68:d0	802.11	2462	Authentication, SN=2443, FN=0, Flags=....
2	0.000784	Cisco_f0:68:d0	Aironet_b7:ab:5c	84:78:ac:f0:68:d0	802.11	2462	Authentication, SN=2771, FN=0, Flags=....
3	0.002428	Aironet_b7:ab:5c	Cisco_f0:68:d0	84:78:ac:f0:68:d0	802.11	2462	Association Request, SN=2444, FN=0, Flags
4	0.007122	Cisco_f0:68:d0	Aironet_b7:ab:5c	84:78:ac:f0:68:d0	802.11	2462	Association Response, SN=2772, FN=0, Flag
5	0.995428	0.0.0.0	255.255.255.255	84:78:ac:f0:68:d0	DHCP	2462	DHCP Discover - Transaction ID 0xba2bf0a4
6	2.996191	1.1.1.1	172.30.6.67	84:78:ac:f0:68:d0	DHCP	2462	DHCP Offer - Transaction ID 0xba2bf0a4
7	2.998532	0.0.0.0	255.255.255.255	84:78:ac:f0:68:d0	DHCP	2462	DHCP Request - Transaction ID 0xba2bf0a4
8	3.005016	1.1.1.1	172.30.6.67	84:78:ac:f0:68:d0	DHCP	2462	DHCP ACK - Transaction ID 0xba2bf0a4

> **Observação**: se você deseja aprender sobre farejamento sem fio 802.11 e sobre os filtros/cores usados no Wireshark para as imagens que aparecem neste documento, visite a publicação da Comunidade de Suporte da Cisco chamada Análise de Imagem do Sniffer 802.11.

O cliente sem fio começa com o quadro de autenticação e o AP responde com outro quadro de autenticação. Em seguida, o cliente envia o quadro de solicitação de associação e o AP termina em uma resposta com o quadro de resposta de associação. Como mostrado nos pacotes DHCP, depois que os processos de autenticação e associação do 802.11 Open System são passados, o cliente começa a passar quadros de dados. Nesse caso, não há nenhum método de segurança configurado no SSID, portanto o cliente começa imediatamente a enviar quadros de dados (nesse caso, DHCP) que não estão criptografados.

Como mostrado mais adiante neste documento, se a segurança estiver habilitada no SSID, haverá quadros de handshake de autenticação e criptografia de nível superior para o método de segurança específico, logo após a Resposta de associação e antes do envio dos quadros de dados de tráfego do cliente, como DHCP, Address Resolution Protocol (ARP) e pacotes de aplicativos, que são criptografados. Os quadros de dados só podem ser enviados até que o cliente seja totalmente autenticado e as chaves de criptografia sejam negociadas, com base no método de segurança configurado.

Com base na imagem anterior, estas são as mensagens que você vê nas saídas do comando **debug client** da WLC quando o cliente sem fio inicia uma nova associação com a WLAN:

```
*apfMsConnTask_0: Jun 21 18:55:14.221: 00:40:96:b7:ab:5c
  Association received from mobile on BSSID 84:78:ac:f0:68:d0
!--- This is the Association Request from the wireless client
     to the selected AP.
```

```
*apfMsConnTask_0: Jun 21 18:55:14.222: 00:40:96:b7:ab:5c
  Sending Assoc Response to station on BSSID 84:78:ac:f0:68:d0
  (status 0) ApVapId 1 Slot 0
!--- This is the Association Response from the AP to the client.
```

> **Observação**: a depuração da WLC usada para as saídas mostradas neste documento é o comando **debug client**, e os exemplos mostram apenas algumas mensagens relevantes, não a saída inteira. Para obter mais detalhes sobre esse comando de depuração, consulte o documento Understand the Debug Client on Wireless LAN Controllers (WLCs).

Essas mensagens mostram os quadros de solicitação e resposta de associação; os quadros de autenticação iniciais não são registrados no WLC porque esse handshake acontece rapidamente no nível AP no CUWN.

Que informações aparecem quando o cliente faz roaming? O cliente sempre troca quatro quadros de gerenciamento no estabelecimento de uma conexão com um AP, que é devido ao estabelecimento de associação do cliente ou a um evento de roaming. O cliente tem apenas uma conexão estabelecida para apenas um AP por vez. A única diferença na troca de quadros entre uma nova conexão à infraestrutura da WLAN e um evento de roaming é que os quadros de associação de um evento de roaming são chamados de quadros de **reassociação**, que indicam que o cliente está realmente em roaming de outro AP sem tentativas de estabelecer uma nova associação à WLAN. Esses quadros podem conter diferentes elementos usados para negociar o evento de roaming; isso depende da configuração, mas esses detalhes estão fora do escopo deste documento.

Aqui está um exemplo de troca de quadros:

No.	Time	Source	Destination	BSS Id	Protocol	Channel frequency	Info
1	0.000000	Aironet_b7:ab:5c	Cisco_f0:2a:90	84:78:ac:f0:2a:90	802.11	2437	Authentication, SN=2611, FN=0, Flags=.....
2	0.001608	Cisco_f0:2a:90	Aironet_b7:ab:5c	84:78:ac:f0:2a:90	802.11	2437	Authentication, SN=3010, FN=0, Flags=.....
3	0.003248	Aironet_b7:ab:5c	Cisco_f0:2a:90	84:78:ac:f0:2a:90	802.11	2437	Reassociation Request, SN=2612, FN=0, Flags
4	0.008122	Cisco_f0:2a:90	Aironet_b7:ab:5c	84:78:ac:f0:2a:90	802.11	2437	Reassociation Response, SN=3011, FN=0, Flag
5	4.291764	Aironet_b7:ab:5c	Broadcast	84:78:ac:f0:2a:90	ARP	2437	Who has 172.30.6.254? Tell 172.30.6.67
6	4.293918	Cisco_f5:4a:4d	Aironet_b7:ab:5c	84:78:ac:f0:2a:90	ARP	2437	172.30.6.254 is at 00:1e:f7:f5:4a:4d

Estas mensagens aparecem na saída da depuração:

```
*apfMsConnTask_2: Jun 21 19:02:19.709: 00:40:96:b7:ab:5c
  Reassociation received from mobile on BSSID 84:78:ac:f0:2a:90
!--- This is the Reassociation Request from the wireless client
     to the selected AP.

*apfMsConnTask_2: Jun 21 19:02:19.710: 00:40:96:b7:ab:5c
  Sending Assoc Response to station on BSSID 84:78:ac:f0:2a:90
  (status 0) ApVapId 1 Slot 0
!--- This is the Reassociation Response from the AP to the client.
```

Como mostrado, o cliente executa com êxito um evento de roaming depois que a Solicitação de reassociação para o novo AP é enviada e recebe a Resposta de reassociação do AP. Como o cliente já tem um endereço IP, os primeiros quadros de dados são para pacotes ARP.

Se você espera um evento de roaming, mas o cliente envia uma Solicitação de Associação em vez de uma Solicitação de Reassociação (que você pode confirmar a partir de algumas imagens e depurações semelhantes às explicadas anteriormente neste documento), o cliente não está realmente em roaming. O cliente inicia uma nova associação com a WLAN como se uma desconexão tivesse ocorrido e tenta reconectar do zero. Isso pode acontecer por várias razões, como quando um cliente se afasta das áreas de cobertura e, em seguida, encontra um AP com

qualidade de sinal suficiente para iniciar uma associação, mas normalmente indica um problema de cliente em que o cliente não inicia um evento de roaming devido a problemas de drivers, firmware ou software.

> **Observação**: você pode consultar o fornecedor do cliente sem fio para determinar a causa do problema.

Roaming com segurança de nível superior

Quando o SSID é configurado com segurança de nível superior L2 na parte superior da autenticação 802.11 básica do sistema aberto, mais quadros são necessários para a associação inicial e quando em roaming. Os dois métodos de segurança mais comuns padronizados e implementados para as WLANs 802.11 são descritos neste documento:

- **WPA/WPA2-PSK (Pre-Shared Key)** - autenticação de clientes com uma chave pré-compartilhada.
- **WPA/WPA2-EAP (Extensible Authentication Protocol)** - autenticação de clientes com um método 802.1X/EAP para validar credenciais mais seguras por meio do uso de um Servidor de Autenticação, como certificados, nome de usuário e senha, e tokens.

Éimportante saber que, embora esses dois métodos (PSK e EAP) autentiquem/validem os clientes de maneiras diferentes, ambos usam basicamente as mesmas regras WPA/WPA2 para o processo de gerenciamento de chaves. Se a segurança for WPA/WPA2-PSK ou WPA/WPA2-EAP, o processo conhecido como handshake de 4 vias WPA/WPA2 inicia a negociação de chave entre o WLC/AP e o cliente com uma chave de sessão mestra (MSK) como material de chave original depois que o cliente é validado com o método de autenticação específico usado.

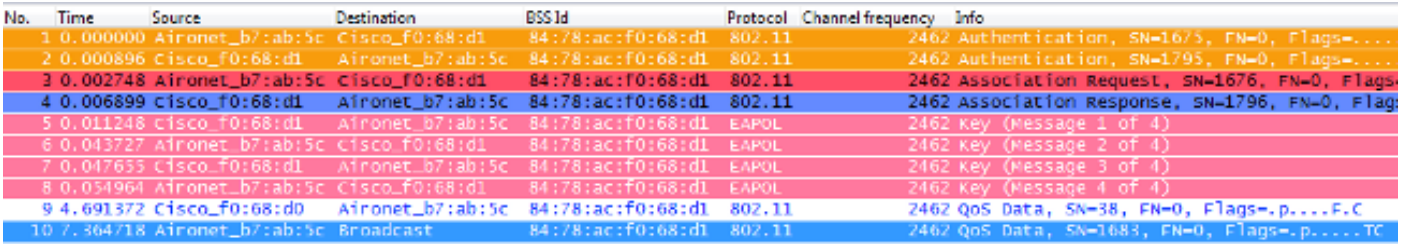
Aqui está um resumo do processo:

1. Um MSK é derivado da fase de autenticação EAP quando a segurança 802.1X/EAP é usada, ou da PSK quando a WPA/WPA2-PSK é usada como o método de segurança.
2. A partir desse MSK, o cliente e a WLC/AP derivam a PMK (Pairwise Master Key), e a WLC/AP gera uma GMK (Group Master Key).
3. Quando essas duas chaves mestras estiverem prontas, o cliente e o WLC/AP iniciam o handshake de 4 vias WPA/WPA2 (que é ilustrado mais adiante neste documento com algumas imagens de tela e depurações) com as chaves mestras como sementes para a negociação das chaves de criptografia reais.
4. Essas chaves de criptografia finais são conhecidas como PTK (Pairwise Transient Key) e GTK (Group Transient Key). O PTK é derivado do PMK e usado para criptografar quadros unicast com o cliente. A GTK (Group Transient Key) é derivada do GMK e é usada para criptografar multicast/broadcast nesse SSID/AP específico.

WPA/WPA2-PSK

Quando o WPA-PSK ou o WPA2-PSK é executado via TKIP (Temporal Key Integrity Protocol) ou AES (Advanced Encryption Standard) para a criptografia, o cliente deve passar pelo processo conhecido como handshake WPA de 4 vias para a associação inicial e também quando em roaming. Como explicado anteriormente, esse é basicamente o processo de gerenciamento de chaves usado para que a WPA/WPA2 derive as chaves de criptografia. No entanto, quando a

PSK é executada, ela também é usada para verificar se o cliente tem uma chave pré-compartilhada válida para ingressar na WLAN. Esta imagem mostra o processo de associação inicial quando a WPA ou a WPA2 com PSK é executada:



No.	Time	Source	Destination	BSS Id	Protocol	Channel frequency	Info
1	0.000000	Aironet_b7:ab:5c	Cisco_f0:68:d1	84:78:ac:f0:68:d1	802.11	2462	Authentication, SN=1675, FN=0, Flags=....
2	0.000896	Cisco_f0:68:d1	Aironet_b7:ab:5c	84:78:ac:f0:68:d1	802.11	2462	Authentication, SN=1795, FN=0, Flags=....
3	0.002748	Aironet_b7:ab:5c	Cisco_f0:68:d1	84:78:ac:f0:68:d1	802.11	2462	Association Request, SN=1676, FN=0, Flags
4	0.006899	Cisco_f0:68:d1	Aironet_b7:ab:5c	84:78:ac:f0:68:d1	802.11	2462	Association Response, SN=1796, FN=0, Flag
5	0.011248	Cisco_f0:68:d1	Aironet_b7:ab:5c	84:78:ac:f0:68:d1	EAPOL	2462	Key (Message 1 of 4)
6	0.043727	Aironet_b7:ab:5c	Cisco_f0:68:d1	84:78:ac:f0:68:d1	EAPOL	2462	Key (Message 2 of 4)
7	0.047655	Cisco_f0:68:d1	Aironet_b7:ab:5c	84:78:ac:f0:68:d1	EAPOL	2462	Key (Message 3 of 4)
8	0.054964	Aironet_b7:ab:5c	Cisco_f0:68:d1	84:78:ac:f0:68:d1	EAPOL	2462	Key (Message 4 of 4)
9	4.691372	Cisco_f0:68:d0	Aironet_b7:ab:5c	84:78:ac:f0:68:d1	802.11	2462	QoS Data, SN=38, FN=0, Flags=.p....F.C
10	7.364718	Aironet_b7:ab:5c	Broadcast	84:78:ac:f0:68:d1	802.11	2462	QoS Data, SN=1683, FN=0, Flags=.p.....TC

Como mostrado, após o processo de autenticação e associação do sistema aberto 802.11, há quatro quadros EAPOL do handshake de 4 vias WPA, que são iniciados pelo AP com **message-1** e terminados pelo cliente com **message-4**. Após um handshake bem-sucedido, o cliente começa a passar quadros de dados (como DHCP), que, nesse caso, são criptografados com as chaves derivadas do handshake de 4 vias (é por isso que você não pode ver o conteúdo real e o tipo de tráfego das imagens sem fio).

> **Observação**: os quadros EAPOL são usados para transportar todos os quadros de gerenciamento de chaves e os quadros de autenticação 802.1X/EAP pelo ar entre o AP e o cliente; eles são transmitidos como quadros de dados sem fio.

Essas mensagens aparecem nas saídas de depuração:

```
*apfMsConnTask_0: Jun 21 19:30:05.172: 00:40:96:b7:ab:5c
  Association received from mobile on BSSID 84:78:ac:f0:68:d1
*apfMsConnTask_0: Jun 21 19:30:05.173: 00:40:96:b7:ab:5c
  Sending Assoc Response to station on BSSID 84:78:ac:f0:68:d1
  (status 0) ApVapId 2 Slot 0
!--- The Association handshake is finished.

*dot1xMsgTask: Jun 21 19:30:05.178: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c
  state INITPMK (message 1), replay counter
  00.00.00.00.00.00.00.00
!--- Message-1 of the WPA/WPA2 4-Way handshake is sent
     from the WLC/AP to the client.

*Dot1x_NW_MsgTask_4: Jun 21 19:30:05.289: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c
*Dot1x_NW_MsgTask_4: Jun 21 19:30:05.289: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTK_START state (message 2)
  from mobile 00:40:96:b7:ab:5c
!--- Message-2 of the WPA/WPA2 4-Way handshake is successfully
     received from the client.

*Dot1x_NW_MsgTask_4: Jun 21 19:30:05.290: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c
  state PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01
!--- Message-3 of the WPA/WPA2 4-Way handshake is sent
     from the WLC/AP to the client.

*Dot1x_NW_MsgTask_4: Jun 21 19:30:05.309: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c
*Dot1x_NW_MsgTask_4: Jun 21 19:30:05.310: 00:40:96:b7:ab:5c
```

```
  Received EAPOL-key in PTKINITNEGOTIATING state (message 4)
  from mobile 00:40:96:b7:ab:5c
!--- Message-4 (final message) of the WPA/WPA2 4-Way handshake
      is successfully received from the client, which confirms
      the installation of the derived keys. They can now be used in
      order to encrypt data frames with current AP.
```

Em roaming, o cliente basicamente rastreia a mesma troca de quadros, onde o handshake de 4 vias WPA é necessário para derivar novas chaves de criptografia com o novo AP. Isso se deve a razões de segurança estabelecidas pelo padrão e ao fato de que o novo AP não conhece as chaves originais. A única diferença é que existem quadros de Reassociação em vez de quadros de Associação, como mostrado nesta imagem:

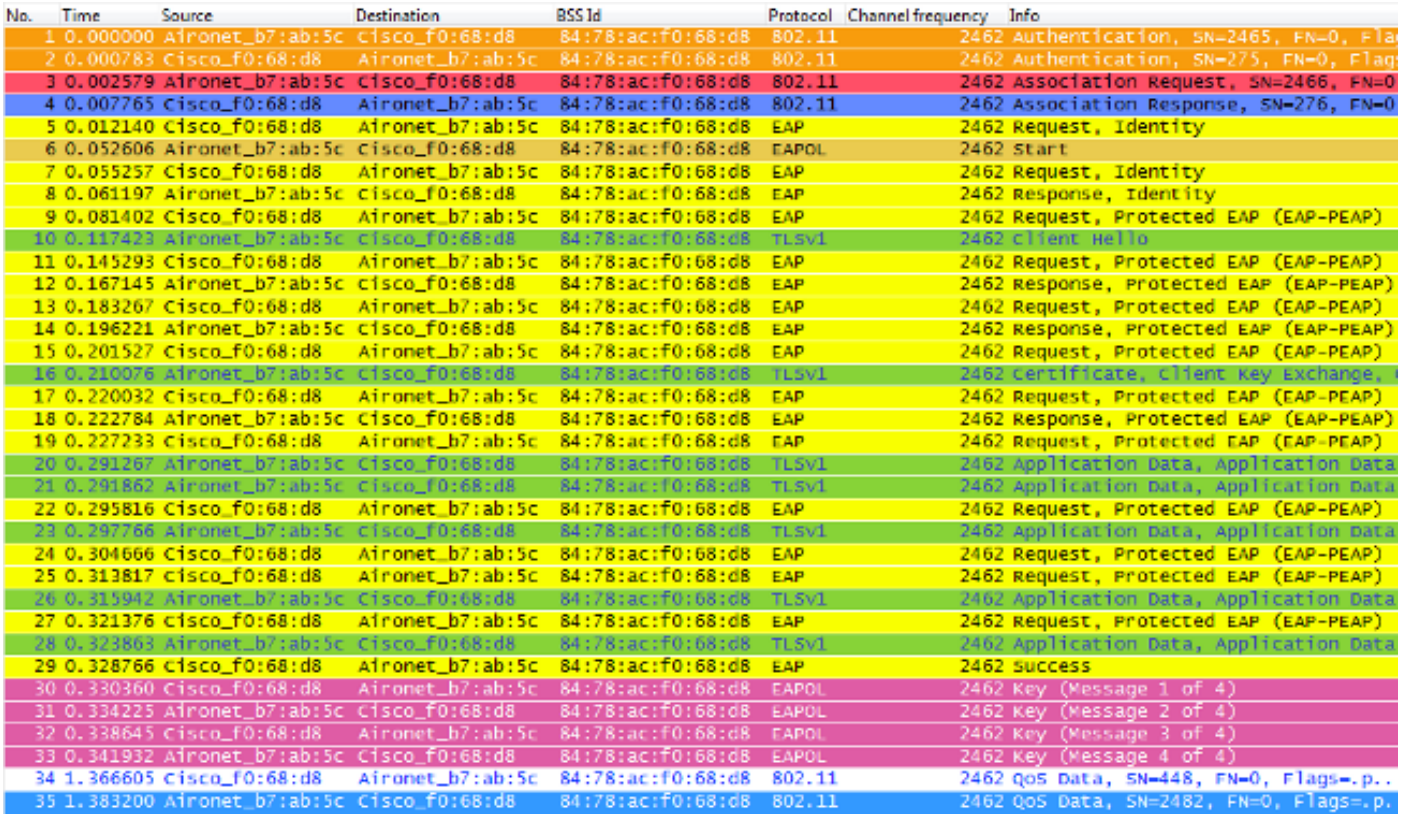
No.	Time	Source	Destination	BSS Id	Protocol	Channel frequency	Info
1	0.000000	Aironet_b7:ab:5c	Cisco_f0:2a:91	84:78:ac:f0:2a:91	802.11	2437	Authentication, SN=2356, FN=0, Flags=.....
2	0.000846	Cisco_f0:2a:91	Aironet_b7:ab:5c	84:78:ac:f0:2a:91	802.11	2437	Authentication, SN=3694, FN=0, Flags=.....
3	0.004296	Aironet_b7:ab:5c	Cisco_f0:2a:91	84:78:ac:f0:2a:91	802.11	2437	Reassociation Request, SN=2357, FN=0, Flags
4	0.010867	Cisco_f0:2a:91	Aironet_b7:ab:5c	84:78:ac:f0:2a:91	802.11	2437	Reassociation Response, SN=3695, FN=0, Flag
5	0.013109	Cisco_f0:2a:91	Aironet_b7:ab:5c	84:78:ac:f0:2a:91	EAPOL	2437	Key (Message 1 of 4)
6	0.034339	Aironet_b7:ab:5c	Cisco_f0:2a:91	84:78:ac:f0:2a:91	EAPOL	2437	Key (Message 2 of 4)
7	0.041124	Cisco_f0:2a:91	Aironet_b7:ab:5c	84:78:ac:f0:2a:91	EAPOL	2437	Key (Message 3 of 4)
8	0.056241	Aironet_b7:ab:5c	Cisco_f0:2a:91	84:78:ac:f0:2a:91	EAPOL	2437	Key (Message 4 of 4)
9	0.695758	Aironet_b7:ab:5c	Broadcast	84:78:ac:f0:2a:91	802.11	2437	QoS Data, SN=2360, FN=0, Flags=.p..R..TC
10	0.698357	Cisco_f5:4a:40	Aironet_b7:ab:5c	84:78:ac:f0:2a:91	802.11	2437	QoS Data, SN=42, FN=0, Flags=.p....F.C

Você vê as mesmas mensagens nas saídas de depuração, mas o primeiro pacote do cliente é uma reassociação em vez de uma associação, como mostrado e explicado anteriormente.

WPA/WPA2-EAP

Quando um método 802.1X/EAP é usado para autenticar os clientes em um SSID seguro, há ainda mais quadros necessários antes que o cliente comece a transmitir tráfego. Esses quadros extras são usados para autenticar as credenciais do cliente e, dependendo do método EAP, pode haver entre quatro e vinte quadros. Eles vêm após a Associação/Reassociação, mas antes do handshake de 4 vias WPA/WPA2, pois a fase de autenticação deriva o MSK usado como a semente para a geração final da chave de criptografia no processo de gerenciamento de chaves (handshake de 4 vias).

Esta imagem mostra um exemplo dos quadros trocados no ar entre o AP e o cliente sem fio na associação inicial quando o WPA com PEAPv0/EAP-MSCHAPv2 é executado:



No.	Time	Source	Destination	BSS Id	Protocol	Channel frequency	Info
1	0.000000	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	802.11	2462	Authentication, SN=2465, FN=0, Fla
2	0.000783	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	802.11	2462	Authentication, SN=275, FN=0, Flag
3	0.002579	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	802.11	2462	Association Request, SN=2466, FN=0
4	0.007765	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	802.11	2462	Association Response, SN=276, FN=0
5	0.012140	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAP	2462	Request, Identity
6	0.052606	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	EAPOL	2462	Start
7	0.055257	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAP	2462	Request, Identity
8	0.061197	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	EAP	2462	Response, Identity
9	0.081402	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAP	2462	Request, Protected EAP (EAP-PEAP)
10	0.117423	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	TLSv1	2462	Client Hello
11	0.145293	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAP	2462	Request, Protected EAP (EAP-PEAP)
12	0.167145	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	EAP	2462	Response, Protected EAP (EAP-PEAP)
13	0.183267	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAP	2462	Request, Protected EAP (EAP-PEAP)
14	0.196221	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	EAP	2462	Response, Protected EAP (EAP-PEAP)
15	0.201527	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAP	2462	Request, Protected EAP (EAP-PEAP)
16	0.210076	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	TLSv1	2462	Certificate, Client Key Exchange,
17	0.220032	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAP	2462	Request, Protected EAP (EAP-PEAP)
18	0.222784	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	EAP	2462	Response, Protected EAP (EAP-PEAP)
19	0.227233	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAP	2462	Request, Protected EAP (EAP-PEAP)
20	0.291267	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	TLSv1	2462	Application Data, Application Data
21	0.291862	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	TLSv1	2462	Application Data, Application Data
22	0.295816	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAP	2462	Request, Protected EAP (EAP-PEAP)
23	0.297766	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	TLSv1	2462	Application Data, Application Data
24	0.304666	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAP	2462	Request, Protected EAP (EAP-PEAP)
25	0.313817	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAP	2462	Request, Protected EAP (EAP-PEAP)
26	0.315942	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	TLSv1	2462	Application Data, Application Data
27	0.321376	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAP	2462	Request, Protected EAP (EAP-PEAP)
28	0.323863	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	TLSv1	2462	Application Data, Application Data
29	0.328766	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAP	2462	Success
30	0.330360	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAPOL	2462	Key (Message 1 of 4)
31	0.334225	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	EAPOL	2462	Key (Message 2 of 4)
32	0.338645	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAPOL	2462	Key (Message 3 of 4)
33	0.341932	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	EAPOL	2462	Key (Message 4 of 4)
34	1.366605	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	802.11	2462	QoS Data, SN=448, FN=0, Flags=.p..
35	1.383200	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	802.11	2462	QoS Data, SN=2482, FN=0, Flags=.p.

Às vezes, essa troca mostra mais ou menos quadros, o que depende de vários fatores, como o método EAP, retransmissões devido a problemas, comportamento do cliente (como as duas Solicitações de identidade neste exemplo, porque o cliente envia um **EAPOL START** depois que o AP envia a primeira Solicitação de identidade) ou se o cliente já trocou o certificado com o servidor. Sempre que o SSID é configurado para um método 802.1X/EAP, há mais quadros (para a autenticação) e, portanto, ele requer mais tempo antes que o cliente comece a enviar quadros de dados.

Aqui está um resumo das mensagens de depuração:

```
*apfMsConnTask_0: Jun 21 23:41:19.092: 00:40:96:b7:ab:5c
  Association received from mobile on BSSID 84:78:ac:f0:68:d8
*apfMsConnTask_0: Jun 21 23:41:19.094: 00:40:96:b7:ab:5c
  Sending Assoc Response to station on BSSID 84:78:ac:f0:68:d8
  (status 0) ApVapId 9 Slot 0
!--- The Association handshake is finished.

*dot1xMsgTask: Jun 21 23:41:19.098: 00:40:96:b7:ab:5c
  Sending EAP-Request/Identity to mobile 00:40:96:b7:ab:5c
  (EAP Id 1)
!--- The EAP Identity Request is sent to the client once it is
     associated in order to begin the higher-level authentication
     process. This informs the client that an identity to start
     this type of 802.1X/EAP authentication must be provided.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.226: 00:40:96:b7:ab:5c
  Received EAPOL START from mobile 00:40:96:b7:ab:5c
!--- The wireless client decides to start the EAP authentication
     process, and informs the AP with an EAPOL START data frame.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.227: 00:40:96:b7:ab:5c
  Sending EAP-Request/Identity to mobile 00:40:96:b7:ab:5c
  (EAP Id 2)
!--- WLC/AP sends another EAP Identity Request to the client.
```

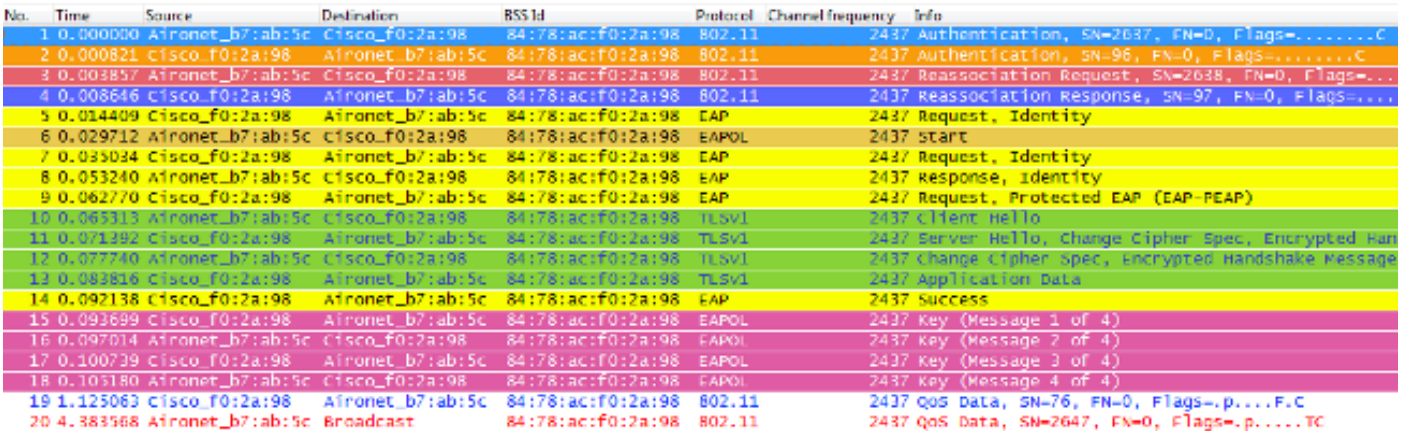
```
*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.235: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c
*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.235: 00:40:96:b7:ab:5c
  Received Identity Response (count=2) from mobile 00:40:96:b7:ab:5c
!--- The client responds with an EAP Identity Response on an EAPOL
      frame.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.301: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c
*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.301: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 3)
!--- Once the WLC/AP sends the client response to the Authentication
      Server on a RADIUS Access-Request packet, the server responds
      with a RADIUS Access-Challenge in order to officially start the
      EAP negotiation, handshake, and authentication with the client
      (sometimes with mutual authentication, dependent upon the EAP
      method). This response received by the WLC/AP is sent to the client.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.344: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c
*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.344: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 3, EAP Type 25)
!--- The client responds with an EAP Response on an EAPOL frame, which
      is sent to the Authentication Server on a RADIUS Access-Request
      packet. The server responds with another RADIUS Access-Challenge.
      This process continues, dependent upon the EAP method (the exchange
      of certificates when used, the building of TLS tunnels, validation
      of client credentials, client validation of server identity when
      applicable). Hence, the next few messages are basically the same on
      the WLC/AP side, as this acts as a "proxy" between the client and
      the Authentication Server exchanges.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.347: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.347: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 4)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.375: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.375: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 4, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.377: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.377: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 5)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.403: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.403: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 5, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.404: 00:40:96:b7:ab:5c
```

```
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.404: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 6)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.414: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.414: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 6, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.421: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.421: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 7)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.425: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.425: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 7, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.427: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.427: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 8)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.434: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.434: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 8, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.436: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.436: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 9)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.440: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.440: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 9, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.442: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.442: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 10)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.449: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c
```

```
*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.449: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 10, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.452: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.452: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 11)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.457: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.457: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 11, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.459: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.459: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 13)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.469: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.469: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 13, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.472: 00:40:96:b7:ab:5c
  Processing Access-Accept for mobile 00:40:96:b7:ab:5c
!--- The authentication finishes and is successful for this client,
     so the RADIUS Server sends a RADIUS Access-Accept to the WLC/AP.
     This RADIUS Access-Accept comes with the special attributes
     that are assigned to this client (if any are configured on the
     Authentication Server for this client). This Access-Accept also
     comes with the MSK derived with the client in the EAP
     authentication process, so the WLC/AP installs it in order to
     initiate the WPA/WPA2 4-Way handshake with the wireless client.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.473: 00:40:96:b7:ab:5c
  Sending EAP-Success to mobile 00:40:96:b7:ab:5c
  (EAP Id 13)
!--- The accept/pass of the authentication is sent to the client as
     an EAP-Success message.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.473: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c
  state INITPMK (message 1), replay counter
  00.00.00.00.00.00.00.00
!--- Message-1 of the WPA/WPA2 4-Way handshake is sent from the
     WLC/AP to the client.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.481: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c
*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.481: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTK_START state (message 2)
  from mobile 00:40:96:b7:ab:5c
!--- Message-2 of the WPA/WPA-2 4-Way handshake is successfully
     received from the client.
```

```
*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.481: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c
  state PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01
!--- Message-3 of the WPA/WPA2 4-Way handshake is sent from the
     WLC/AP to the client.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.487: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c
*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.487: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTKINITNEGOTIATING state (message 4)
  from mobile 00:40:96:b7:ab:5c
!--- Message-4 (final message) of the WPA/WPA2 4-Way handshake
     is successfully received from the client, which confirms the
     installation of the derived keys. They can now be used in
     order to encrypt data frames with the current AP.
```

Quando o cliente sem fio executa um roaming regular aqui (o comportamento normal, sem a implementação de um método de roaming rápido e seguro), o cliente deve passar exatamente pelo mesmo processo e executar uma autenticação completa no Servidor de autenticação, como mostrado nas imagens. A única diferença é que o cliente usa uma Solicitação de Reassociação para informar ao novo AP que ele está realmente em roaming de outro AP, mas o cliente ainda tem que passar pela validação completa e pela nova geração de chave:



No.	Time	Source	Destination	BSSId	Protocol	Channel frequency	Info
1	0.000000	Aironet_b7:ab:5c	Cisco_f0:2a:98	84:78:ac:f0:2a:98	802.11	2437	Authentication, SN=2037, FN=0, Flags=.....C
2	0.000821	Cisco_f0:2a:98	Aironet_b7:ab:5c	84:78:ac:f0:2a:98	802.11	2437	Authentication, SN=96, FN=0, Flags=.....C
3	0.003857	Aironet_b7:ab:5c	Cisco_f0:2a:98	84:78:ac:f0:2a:98	802.11	2437	Reassociation Request, SN=2038, FN=0, Flags=...
4	0.008646	Cisco_f0:2a:98	Aironet_b7:ab:5c	84:78:ac:f0:2a:98	802.11	2437	Reassociation Response, SN=97, FN=0, Flags=...
5	0.014409	Cisco_f0:2a:98	Aironet_b7:ab:5c	84:78:ac:f0:2a:98	EAP	2437	Request, Identity
6	0.029712	Aironet_b7:ab:5c	Cisco_f0:2a:98	84:78:ac:f0:2a:98	EAPOL	2437	Start
7	0.033084	Cisco_f0:2a:98	Aironet_b7:ab:5c	84:78:ac:f0:2a:98	EAP	2437	Request, Identity
8	0.053240	Aironet_b7:ab:5c	Cisco_f0:2a:98	84:78:ac:f0:2a:98	EAP	2437	Response, Identity
9	0.062770	Cisco_f0:2a:98	Aironet_b7:ab:5c	84:78:ac:f0:2a:98	EAP	2437	Request, Protected EAP (EAP-PEAP)
10	0.065313	Aironet_b7:ab:5c	Cisco_f0:2a:98	84:78:ac:f0:2a:98	TLSv1	2437	Client Hello
11	0.071292	Cisco_f0:2a:98	Aironet_b7:ab:5c	84:78:ac:f0:2a:98	TLSv1	2437	Server Hello, Change Cipher Spec, Encrypted Han
12	0.077740	Aironet_b7:ab:5c	Cisco_f0:2a:98	84:78:ac:f0:2a:98	TLSv1	2437	Change Cipher Spec, Encrypted Handshake Message
13	0.083816	Cisco_f0:2a:98	Aironet_b7:ab:5c	84:78:ac:f0:2a:98	TLSv1	2437	Application Data
14	0.092138	Cisco_f0:2a:98	Aironet_b7:ab:5c	84:78:ac:f0:2a:98	EAP	2437	Success
15	0.093699	Cisco_f0:2a:98	Aironet_b7:ab:5c	84:78:ac:f0:2a:98	EAPOL	2437	Key (Message 1 of 4)
16	0.097014	Aironet_b7:ab:5c	Cisco_f0:2a:98	84:78:ac:f0:2a:98	EAPOL	2437	Key (Message 2 of 4)
17	0.100739	Cisco_f0:2a:98	Aironet_b7:ab:5c	84:78:ac:f0:2a:98	EAPOL	2437	Key (Message 3 of 4)
18	0.105180	Aironet_b7:ab:5c	Cisco_f0:2a:98	84:78:ac:f0:2a:98	EAPOL	2437	Key (Message 4 of 4)
19	1.125063	Cisco_f0:2a:98	Aironet_b7:ab:5c	84:78:ac:f0:2a:98	802.11	2437	QoS Data, SN=76, FN=0, Flags=.p....F.C
20	4.383568	Aironet_b7:ab:5c	Broadcast	84:78:ac:f0:2a:98	802.11	2437	QoS Data, SN=2647, FN=0, Flags=.p.....TC

Como mostrado, mesmo quando há menos quadros do que na autenticação inicial (que é causada por vários fatores, como mencionado anteriormente), quando o cliente faz roaming para um novo AP, a autenticação EAP e os processos de gerenciamento de chave WPA ainda devem ser concluídos para continuar a transmitir quadros de dados (mesmo se o tráfego tiver sido enviado ativamente antes do roaming). Portanto, se o cliente tiver um aplicativo ativo que seja sensível a atrasos (como aplicativos de tráfego de voz ou aplicativos que sejam sensíveis a timeouts), o usuário poderá perceber problemas quando estiver em roaming, como falhas de áudio ou desconexões de aplicativos. Isso depende do tempo que o processo leva para que o cliente continue a enviar/receber quadros de dados. Esse atraso pode ser maior, dependendo do ambiente de RF, da quantidade de clientes, do tempo de ida e volta entre a WLC e os LAPs e com o Servidor de Autenticação e de outros motivos.

Aqui está um resumo das mensagens de depuração para esse evento de roaming (basicamente as mesmas que as anteriores, portanto essas mensagens não são descritas mais detalhadamente):

```
*apfMsConnTask_2: Jun 21 23:47:54.872: 00:40:96:b7:ab:5c
  Reassociation received from mobile on BSSID 84:78:ac:f0:2a:98
```

```
*apfMsConnTask_2: Jun 21 23:47:54.874: 00:40:96:b7:ab:5c
  Sending Assoc Response to station on BSSID 84:78:ac:f0:2a:98
  (status 0) ApVapId 9 Slot 0

*dot1xMsgTask: Jun 21 23:47:54.879: 00:40:96:b7:ab:5c
  Sending EAP-Request/Identity to mobile 00:40:96:b7:ab:5c
  (EAP Id 1)

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.895: 00:40:96:b7:ab:5c
  Received EAPOL START from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.895: 00:40:96:b7:ab:5c
  dot1x - moving mobile 00:40:96:b7:ab:5c into Connecting state

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.895: 00:40:96:b7:ab:5c
  Sending EAP-Request/Identity to mobile 00:40:96:b7:ab:5c
  (EAP Id 2)

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.922: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.922: 00:40:96:b7:ab:5c
  Received Identity Response (count=2) from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.929: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.929: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 3)

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.941: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.941: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 3, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.943: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.943: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 4)

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.954: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.954: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 4, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.956: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.957: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 7)

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.976: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.976: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
```

```
  (EAP Id 7, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.978: 00:40:96:b7:ab:5c
  Processing Access-Accept for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.978: 00:40:96:b7:ab:5c
  Sending EAP-Success to mobile 00:40:96:b7:ab:5c
  (EAP Id 7)

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.978: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c
  state INITPMK (message 1), replay counter
  00.00.00.00.00.00.00.00

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.995: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.995: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTK_START state (message 2)
  from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.995: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c
  state PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01

*Dot1x_NW_MsgTask_4: Jun 21 23:47:55.005: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:55.005: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTKINITNEGOTIATING state (message 4)
  from mobile 00:40:96:b7:ab:5c
```

Éassim que o 802.1X/EAP e a estrutura de segurança WPA/WPA2 funcionam. Para evitar o impacto do aplicativo/serviço nos atrasos de um evento regular de roaming, vários métodos de roaming rápido e seguro são desenvolvidos e implementados pelo setor de WiFi para acelerar o processo de roaming quando a segurança for usada na WLAN/SSID. Os clientes enfrentam alguma latência quando continuam a passar tráfego enquanto fazem roaming entre APs através da implantação de segurança de alto nível na WLAN. Isso se deve à autenticação EAP e às trocas de quadros de gerenciamento de chaves exigidas pela configuração de segurança, conforme explicado anteriormente.

Éimportante entender que o roaming rápido e seguro é apenas o termo usado pelo setor em referência à implementação de um método/esquema que acelera o processo de roaming quando a segurança é configurada na WLAN. Os diferentes métodos/esquemas de roaming rápido que estão disponíveis para WLANs e são suportados pelo CUWN são explicados na próxima seção.

Roaming rápido e seguro com CCKM

O Cisco Centralized Key Management (CCKM) é o primeiro método de roaming rápido e seguro desenvolvido e implementado em WLANs corporativas, criado pela Cisco como a solução usada para reduzir os atrasos explicados até agora, quando a segurança 802.1X/EAP é usada na WLAN. Como este é um protocolo proprietário da Cisco, ele é suportado apenas pelos dispositivos de infraestrutura de WLAN da Cisco e clientes sem fio (de vários fornecedores) que são compatíveis com o Cisco Compatible Extension (CCX) para CCKM.

O CCKM pode ser implementado com todos os diferentes métodos de criptografia disponíveis para as WLANs, incluindo: WEP, TKIP e AES. Ele também é suportado pela maioria dos métodos

de autenticação 802.1X/EAP usados para WLANs, dependendo da versão CCX suportada pelos dispositivos.

> **Observação**: para obter uma visão geral do conteúdo do recurso suportado pelas diferentes versões da especificação CCX (que inclui os métodos EAP suportados), consulte o documento Versões e recursos do CCX e verifique a versão exata do CCX suportada pelos seus clientes sem fio (se eles forem compatíveis com CCX), para que você possa confirmar se o método de segurança que deseja usar com o CCKM pode ser implementado.

Essa imagem sem fio fornece um exemplo dos quadros trocados na associação inicial quando você executa o CCKM com TKIP como a criptografia e PEAPv0/EAP-MSCHAPv2 como o método 802.1X/EAP. Essa é basicamente a mesma troca como se WPA/TKIP com PEAPv0/EAP-MSCHAPv2 fosse executada, mas dessa vez o CCKM entre o cliente e a infraestrutura é negociado para que eles usem hierarquia de chave e métodos de cache diferentes para executar roaming rápido seguro quando o cliente precisa fazer roaming:

No.	Time	Source	Destination	BSS Id	Protocol	Channel frequency	Info
1	0.000000	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	802.11	2462	Authentication, SN=2518, FN=0, Flag
2	0.000906	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	802.11	2462	Authentication, SN=3096, FN=0, Flag
3	0.002675	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	802.11	2462	Association Request, SN=2519, FN=0,
4	0.007562	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	802.11	2462	Association Response, SN=3097, FN=0
5	0.013614	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	EAP	2462	Request, Identity
6	0.032754	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	EAPOL	2462	Start
7	0.042974	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	EAP	2462	Response, Identity
8	0.046855	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	EAP	2462	Response, Identity
9	0.054287	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	EAP	2462	Request, Protected EAP (EAP-PEAP)
10	0.090265	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	TLSv1	2462	Client Hello
11	0.107247	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	EAP	2462	Request, Protected EAP (EAP-PEAP)
12	0.124080	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	EAP	2462	Response, Protected EAP (EAP-PEAP)
13	0.140385	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	EAP	2462	Request, Protected EAP (EAP-PEAP)
14	0.154095	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	EAP	2462	Response, Protected EAP (EAP-PEAP)
15	0.158341	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	EAP	2462	Request, Protected EAP (EAP-PEAP)
16	0.176346	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	TLSv1	2462	Certificate, Client Key Exchange, C
17	0.186458	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	EAP	2462	Request, Protected EAP (EAP-PEAP)
18	0.195391	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	EAP	2462	Response, Protected EAP (EAP-PEAP)
19	0.201648	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	EAP	2462	Request, Protected EAP (EAP-PEAP)
20	0.298860	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	TLSv1	2462	Application Data, Application Data
21	0.310941	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	TLSv1	2462	Application Data, Application Data
22	0.315574	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	EAP	2462	Request, Protected EAP (EAP-PEAP)
23	0.318255	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	TLSv1	2462	Application Data, Application Data
24	0.324589	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	EAP	2462	Request, Protected EAP (EAP-PEAP)
25	0.332059	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	EAP	2462	Request, Protected EAP (EAP-PEAP)
26	0.339778	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	EAP	2462	Success
27	0.341365	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	EAPOL	2462	Key (Message 1 of 4)
28	0.354695	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	EAPOL	2462	Key (Message 2 of 4)
29	0.358951	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	EAPOL	2462	Key (Message 3 of 4)
30	0.362866	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	EAPOL	2462	Key (Message 4 of 4)

Aqui está um resumo das mensagens de depuração (com algumas trocas de EAP removidas para reduzir a saída):

```
*apfMsConnTask_0: Jun 25 15:41:41.507: 00:40:96:b7:ab:5c
  Association received from mobile on BSSID 84:78:ac:f0:68:d3
!--- This is the Association Request from the client.

*apfMsConnTask_0: Jun 25 15:41:41.507: 00:40:96:b7:ab:5c
  Processing WPA IE type 221, length 22 for mobile
  00:40:96:b7:ab:5c
*apfMsConnTask_0: Jun 25 15:41:41.507: 00:40:96:b7:ab:5c
  CCKM: Mobile is using CCKM
!--- The WLC/AP finds an Information Element that claims CCKM
    support on the Association request that is sent from the client.
```

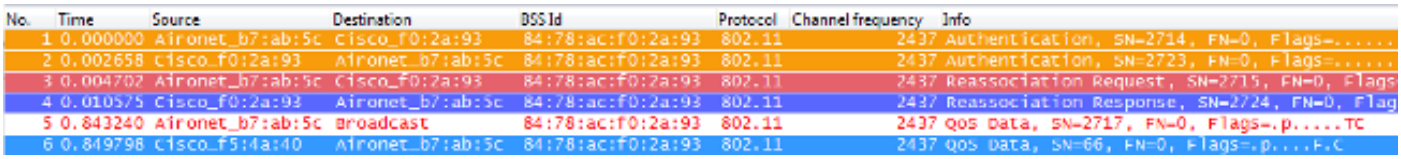
```
*apfMsConnTask_0: Jun 25 15:41:41.507: 00:40:96:b7:ab:5c
  Setting active key cache index 8 ---> 8
!--- This is the key cache index for this client, which is set temporally.

*apfMsConnTask_0: Jun 25 15:41:41.508: 00:40:96:b7:ab:5c
  Sending Assoc Response to station on BSSID 84:78:ac:f0:68:d3
  (status 0) ApVapId 4 Slot 0
!--- The Association Response is sent to the client.

*dot1xMsgTask: Jun 25 15:41:41.513: 00:40:96:b7:ab:5c
  Sending EAP-Request/Identity to mobile 00:40:96:b7:ab:5c
  (EAP Id 1)
!--- An EAP Identity Request is sent to the client once it is
     associated in order to begin the higher-level authentication
     process. This informs the client that an identity to start
     this type of 802.1X/EAP authentication must be provided.
     Further EAP messages are not described, as they are basically
     the same as the ones previously-explained.

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.536: 00:40:96:b7:ab:5c
  Received EAPOL START from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.536: 00:40:96:b7:ab:5c
  Sending EAP-Request/Identity to mobile 00:40:96:b7:ab:5c
  (EAP Id 2)

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.546: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.546: 00:40:96:b7:ab:5c
  Received EAP Response packet with mismatching id
  (currentid=2, eapid=1) from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.550: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.550: 00:40:96:b7:ab:5c
  Received Identity Response (count=2) from mobile
  00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.555: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.555: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 3)

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.594: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.594: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 3, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.840: 00:40:96:b7:ab:5c
  Processing Access-Accept for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.841: 00:40:96:b7:ab:5c
  Creating a PKC PMKID Cache entry for station 00:40:96:b7:ab:5c
  (RSN 0)<br/ >
*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.841: 00:40:96:b7:ab:5c
  Setting active key cache index 8 ---> 8
*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.841: 00:40:96:b7:ab:5c
```

```
  Setting active key cache index 8 ---> 0
*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.841: 00:40:96:b7:ab:5c
  CCKM: Create a global PMK cache entry
!--- WLC creates a global PMK cache entry for this client,
      which is for CCKM in this case.

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.841: 00:40:96:b7:ab:5c
  Sending EAP-Success to mobile 00:40:96:b7:ab:5c
  (EAP Id 13)
!--- The client is informed of the successful EAP authentication.

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.841: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c state
  INITPMK(message 1),replay counter 00.00.00.00.00.00.00.00
!--- Message-1 of the initial 4-Way handshake is sent from the
      WLC/AP to the client.

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.858: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c
*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.858: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTK_START state (message 2) from mobile
  00:40:96:b7:ab:5c
!--- Message-2 of the initial 4-Way handshake is received
      successfully from the client.

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.858: 00:40:96:b7:ab:5c
  CCKM: Sending cache add
*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.858: CCKM: Sending CCKM PMK
  (Version_1) information to mobility group
*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.858: CCKM: Sending CCKM PMK
  (Version_2) information to mobility group
!--- The CCKM PMK cache entry for this client is shared with
      the WLCs on the mobility group.

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.858: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c
  state PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01
!--- Message-3 of the initial 4-Way handshake is sent from the
      WLC/AP to the client.

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.866: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c
*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.866: 00:40:96:b7:ab:5c Received
  EAPOL-key in PTKINITNEGOTIATING state (message 4) from mobile
  00:40:96:b7:ab:5c
!--- Message-4 (final message) of this initial 4-Way handshake
      is received successfully from the client, which confirms the
      installation of the derived keys. They can now be used in order
      to encrypt data frames with the current AP.
```

Com o CCKM, a associação inicial à WLAN é semelhante à WPA/WPA2 normal, onde um MSK (também conhecido aqui como Network Session Key (NSK)) é mutuamente derivado com o cliente e o servidor RADIUS. Essa chave primária é enviada do servidor para a WLC após uma autenticação bem-sucedida e é armazenada em cache como a base para derivação de todas as chaves subsequentes durante a vida útil da associação do cliente com essa WLAN. A partir daqui, a WLC e o cliente derivam as informações semente que são usadas para roaming rápido e seguro com base no CCKM, isso passa por um handshake de 4 vias semelhante ao da WPA/WPA2, a fim de derivar as chaves de criptografia unicast (PTK) e multicast/broadcast (GTK) com o primeiro AP.

A grande diferença é percebida quando se está em roaming. Nesse caso, o cliente CCKM envia

um único quadro de solicitação de reassociação ao AP/WLC (que inclui um MIC e um número aleatório de incremento sequencial) e fornece informações suficientes (que inclui o novo endereço MAC do AP **-BSSID-**) para derivar o novo PTK. Com essa Solicitação de Reassociação, a WLC e o novo AP também têm informações suficientes para derivar o novo PTK, portanto eles simplesmente respondem com uma Resposta de Reassociação. O cliente agora pode continuar a transmitir tráfego, como mostrado nesta imagem:



No.	Time	Source	Destination	BSS Id	Protocol	Channel frequency	Info
1	0.000000	Aironet_b7:ab:5c	Cisco_f0:2a:93	84:78:ac:f0:2a:93	802.11	2437	Authentication, SN=2714, FN=0, Flags=.....
2	0.002658	Cisco_f0:2a:93	Aironet_b7:ab:5c	84:78:ac:f0:2a:93	802.11	2437	Authentication, SN=2723, FN=0, Flags=.....
3	0.004702	Aironet_b7:ab:5c	Cisco_f0:2a:93	84:78:ac:f0:2a:93	802.11	2437	Reassociation Request, SN=2715, FN=0, Flags
4	0.010575	Cisco_f0:2a:93	Aironet_b7:ab:5c	84:78:ac:f0:2a:93	802.11	2437	Reassociation Response, SN=2724, FN=0, Flag
5	0.843240	Aironet_b7:ab:5c	Broadcast	84:78:ac:f0:2a:93	802.11	2437	QoS Data, SN=2717, FN=0, Flags=.p.....TC
6	0.849798	Cisco_f5:4a:40	Aironet_b7:ab:5c	84:78:ac:f0:2a:93	802.11	2437	QoS Data, SN=66, FN=0, Flags=.p....F.C

Aqui está um resumo das depurações de WLC para este evento de roaming:

```
*apfMsConnTask_2: Jun 25 15:43:33.749: 00:40:96:b7:ab:5c
  CCKM: Received REASSOC REQ IE
*apfMsConnTask_2: Jun 25 15:43:33.749: 00:40:96:b7:ab:5c
  Reassociation received from mobile on BSSID
  84:78:ac:f0:2a:93
*apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c
  Processing WPA IE type 221, length 22 for mobile
  00:40:96:b7:ab:5c
*apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c
  CCKM: Mobile is using CCKM
!--- The Reassociation Request is received from the client,
     which provides the CCKM information needed in order to
     derive the new keys with a fast-secure roam.

*apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c
  Setting active key cache index 0 ---> 8

*apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c
  CCKM: Processing REASSOC REQ IE

*apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c
  CCKM: using HMAC MD5 to compute MIC
!--- WLC computes the MIC used for this CCKM fast-roaming
     exchange.

*apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c
  CCKM: Received a valid REASSOC REQ IE

*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c
  CCKM: Initializing PMK cache entry with a new PTK
!--- The new PTK is derived.

*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c
  Setting active key cache index 8 ---> 8

*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c
  Setting active key cache index 8 ---> 8

*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c
  Setting active key cache index 8 ---> 0

*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c
  Creating a PKC PMKID Cache entry for station
  00:40:96:b7:ab:5c (RSN 0) on BSSID 84:78:ac:f0:2a:93
!--- The new PMKID cache entry is created for this new
```

```
     AP-to-client association.

*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c
  CCKM: using HMAC MD5 to compute MIC
*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c
  Including CCKM Response IE (length 62) in Assoc Resp to mobile
*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c
  Sending Assoc Response to station on BSSID 84:78:ac:f0:2a:93
  (status 0) ApVapId 4 Slot 0
!--- The Reassociation Response is sent from the WLC/AP to
     the client, which includes the CCKM information required
     in order to confirm the new fast-roam and key derivation.

*dot1xMsgTask: Jun 25 15:43:33.757: 00:40:96:b7:ab:5c
  Skipping EAP-Success to mobile 00:40:96:b7:ab:5c
!--- EAP is skipped due to the fast roaming, and CCKM does not
     require further key handshakes. The client is now ready to
     pass encrypted data frames on the new AP.
```

Como mostrado, o roaming rápido e seguro é executado enquanto os quadros de autenticação EAP são evitados e ainda mais handshakes 4-Way, porque as novas chaves de criptografia ainda são derivadas, mas com base no esquema de negociação CCKM. Isso é concluído com os quadros de reassociação de roaming e as informações previamente armazenadas em cache pelo cliente e pelo WLC.

FlexConnect com CCKM

- Há suporte para a Autenticação Central. Isso inclui a troca de dados local e central. Os APs devem fazer parte do mesmo grupo FlexConnect.
- Há suporte para a Autenticação Local Flex. No modo conectado, o cache pode ser distribuído do AP para o controlador e, em seguida, para o restante dos APs no grupo FlexConnect.
- Há suporte para o modo autônomo. Se o cache já estiver presente no AP (devido à distribuição anterior), o roam rápido funcionará. A nova autenticação no modo autônomo não oferece suporte ao roaming rápido e seguro.

Prós com CCKM

- O CCKM é o método de roaming mais rápido e seguro, implantado principalmente em WLANs corporativas. Os clientes não precisam passar por um handshake de gerenciamento de chaves para derivar novas chaves quando ocorre uma mudança entre APs, e nunca mais precisam executar uma autenticação 802.1X/EAP completa com novos APs durante a vida útil do cliente nesta WLAN.
- O CCKM suporta todos os métodos de criptografia disponíveis dentro do padrão 802.11 (WEP, TKIP e AES), além de alguns métodos proprietários legados da Cisco ainda usados em clientes legados.

Contras com CCKM

- O CCKM é um método proprietário da Cisco, que limita a implementação e o suporte à infraestrutura de WLAN da Cisco e aos clientes sem fio CCX.
- O CCX Versão 5 não é amplamente adotado, portanto o CCKM com WPA2/AES não é suportado por muitos clientes sem fio CCX (principalmente porque a maioria deles já suporta o CCKM com WPA/TKIP, que ainda é muito seguro).

Roaming rápido e seguro com cache PMKID / Sticky Key

O cache de ID de chave (PMKID - Key ID), ou **Sticky Key Caching (SKC)**, é o primeiro método de roaming rápido sugerido pelo padrão IEEE 802.11 dentro da emenda de segurança 802.11i, onde o objetivo principal é padronizar um alto nível de segurança para as WLANs. Essa técnica de roaming rápido e seguro foi adicionada como um método opcional para dispositivos WPA2 a fim de melhorar o roaming quando essa segurança foi implementada.

Isso é possível porque, sempre que um cliente é totalmente autenticado por EAP, o cliente e o Servidor de autenticação derivam um MSK, que é usado para derivar o PMK. Isso é usado como semente para o handshake de 4 vias WPA2 para derivar a chave de criptografia unicast (PTK) final que é usada para a sessão (até que o cliente faça roaming para outro AP ou a sessão expire); portanto, esse método impede a fase de autenticação EAP quando em roaming porque reutiliza o PMK original armazenado em cache pelo cliente e o AP. O cliente só precisa passar pelo handshake de 4 vias WPA2 para obter novas chaves de criptografia.

Este método não é amplamente implantado como o método roaming rápido seguro padrão 802.11 recomendado, principalmente por estes motivos:

- Este método é opcional e não é suportado por todos os dispositivos WPA2, porque a finalidade da emenda 802.11i não diz respeito ao roaming rápido seguro, e o IEEE já trabalhou em outra emenda para padronizar o roaming rápido seguro para WLANs (802.11r, que é abordado mais adiante neste documento).
- Esse método tem uma grande limitação em sua implementação: os clientes sem fio podem executar roaming rápido e seguro apenas quando em roaming de volta para um AP onde eles já tenham se autenticado/conectado anteriormente.

Com esse método, a associação inicial a qualquer AP é como uma autenticação de primeira vez regular para a WLAN, onde toda a autenticação 802.1X/EAP contra o servidor de autenticação e o handshake de 4 vias para geração de chave deve acontecer antes que o cliente possa enviar quadros de dados, como mostrado nesta imagem da tela:

No.	Time	Source	Destination	BSS Id	Protocol	Channel frequency	Info
1	0.000000	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	802.11	2462	Authentication, SN=2, FN=0, Flags=.....
2	0.000814	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	802.11	2462	Authentication, SN=4052, FN=0, Flags=...
3	0.002747	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	802.11	2462	Association Request, SN=3, FN=0, Flags=.
4	0.007357	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	802.11	2462	Association Response, SN=4053, FN=0, Fla
5	0.011957	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAP	2462	Request, Identity
6	0.022896	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	EAP	2462	Response, Identity
7	0.044470	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
8	0.069885	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	TLSv1	2462	Client Hello
9	0.093349	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
10	0.095916	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	EAP	2462	Response, Protected EAP (EAP-PEAP)
11	0.112358	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
12	0.116114	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	EAP	2462	Response, Protected EAP (EAP-PEAP)
13	0.120221	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
14	0.129519	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	TLSv1	2462	Certificate, Client Key Exchange, Change
15	0.139156	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
16	0.162262	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	EAP	2462	Response, Protected EAP (EAP-PEAP)
17	0.166459	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
18	0.171454	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	TLSv1	2462	Application Data
19	0.175710	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
20	0.178181	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	TLSv1	2462	Application Data
21	0.182858	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
22	0.187006	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	TLSv1	2462	Application Data
23	0.192835	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
24	0.197049	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	TLSv1	2462	Application Data
25	0.202860	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
26	0.205372	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	TLSv1	2462	Application Data
27	0.210763	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAP	2462	Success
28	0.212505	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAPOL	2462	Key (Message 1 of 4)
29	0.215434	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	EAPOL	2462	Key (Message 2 of 4)
30	0.219023	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAPOL	2462	Key (Message 3 of 4)
31	0.221930	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	EAPOL	2462	Key (Message 4 of 4)
32	0.224559	Apple_15:39:32	Cisco_f5:4a:40	84:78:ac:f0:68:d2	802.11	2462	QoS Data, SN=0, FN=0, Flags=.p.....TC

As depurações revelam a mesma troca de quadros de autenticação EAP que o restante dos

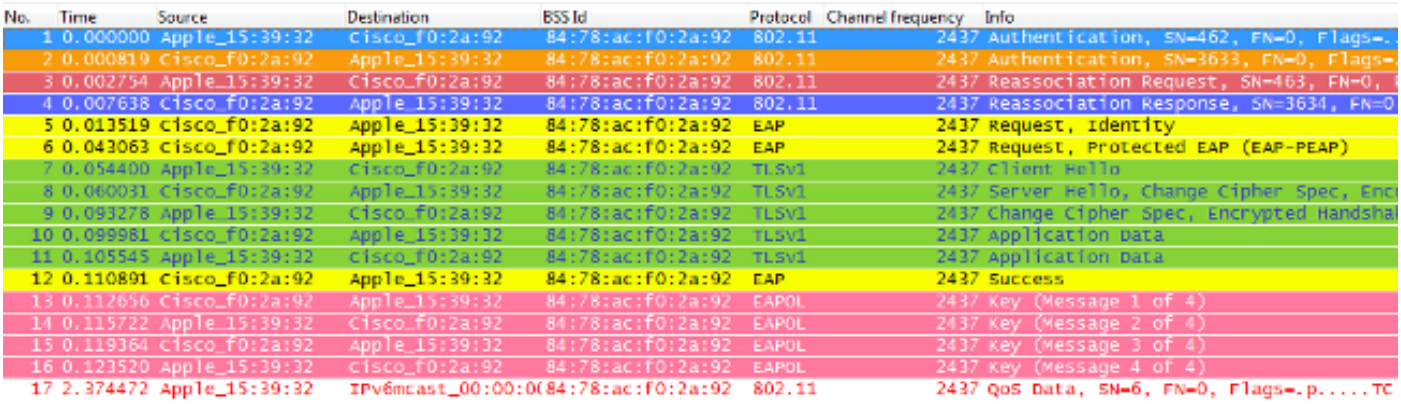
métodos na autenticação inicial para a WLAN, com algumas saídas adicionadas em relação às técnicas de cache de chave usadas aqui. Essas saídas de depuração são cortadas para mostrar principalmente as novas informações, e não toda a troca de quadros EAP, porque basicamente as mesmas informações são trocadas todas as vezes para autenticação do cliente no Servidor de autenticação. Isso é demonstrado até o momento e correlacionado com os quadros de autenticação EAP mostrados nas imagens do pacote, portanto, a maioria das mensagens EAP é removida das saídas de depuração para simplificar:

```
*apfMsConnTask_0: Jun 22 00:23:15.097: ec:85:2f:15:39:32
  Association received from mobile on BSSID 84:78:ac:f0:68:d2
!--- This is the Association Request from the client.

*apfMsConnTask_0: Jun 22 00:23:15.098: ec:85:2f:15:39:32
  Processing RSN IE type 48, length 20 for mobile ec:85:2f:15:39:32
!--- The WLC/AP finds an Information Element that claims PMKID
     Caching support on the Association request that is sent
     from the client.

*apfMsConnTask_0: Jun 22 00:23:15.098: ec:85:2f:15:39:32
  Received RSN IE with 0 PMKIDs from mobile ec:85:2f:15:39:32
!--- Since this is an initial association, the Association
     Request comes without any PMKID.

*apfMsConnTask_0: Jun 22 00:23:15.098: ec:85:2f:15:39:32
  Setting active key cache index 8 ---> 8

*apfMsConnTask_0: Jun 22 00:23:15.099: ec:85:2f:15:39:32
  Sending Assoc Response to station on BSSID 84:78:ac:f0:68:d2
  (status 0) ApVapId 3 Slot 0
!--- The Association Response is sent to the client.

*dot1xMsgTask: Jun 22 00:23:15.103: ec:85:2f:15:39:32
  Sending EAP-Request/Identity to mobile ec:85:2f:15:39:32
  (EAP Id 1)

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.118: ec:85:2f:15:39:32
  Received EAPOL EAPPKT from mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.118: ec:85:2f:15:39:32
  Received Identity Response (count=1) from mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.126: ec:85:2f:15:39:32
  Processing Access-Challenge for mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.126: ec:85:2f:15:39:32
  Sending EAP Request from AAA to mobile ec:85:2f:15:39:32
  (EAP Id 2)

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.146: ec:85:2f:15:39:32
  Received EAPOL EAPPKT from mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.146: ec:85:2f:15:39:32
  Received EAP Response from mobile ec:85:2f:15:39:32
  (EAP Id 2, EAP Type 25)

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.274: ec:85:2f:15:39:32
  Processing Access-Accept for mobile ec:85:2f:15:39:32
```

```
*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.274: ec:85:2f:15:39:32
  Creating a PKC PMKID Cache entry for station ec:85:2f:15:39:32
  (RSN 2)
*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.274: ec:85:2f:15:39:32
  Setting active key cache index 8 ---> 8
*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.274: ec:85:2f:15:39:32
  Setting active key cache index 8 ---> 0
*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.274: ec:85:2f:15:39:32
  Adding BSSID 84:78:ac:f0:68:d2 to PMKID cache at index 0
  for station ec:85:2f:15:39:32
*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.274:
  New PMKID: (16)
*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.274:
  [0000] c9 4d 0d 97 03 aa a9 0f 1b c8 33 73 01 f1 18 f5
!--- WLC creates a PMK cache entry for this client, which is
     used for SKC in this case, so the PMKID is computed with
     the AP MAC address (BSSID 84:78:ac:f0:68:d2).

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.274: ec:85:2f:15:39:32
  Sending EAP-Success to mobile ec:85:2f:15:39:32
  (EAP Id 12)

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.275:
  Including PMKID in M1  (16)
!--- The hashed PMKID is included on the Message-1 of the
     WPA/WPA2 4-Way handshake.

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.275:
  [0000] c9 4d 0d 97 03 aa a9 0f 1b c8 33 73 01 f1 18 f5
!--- This is the hashed PMKID.

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.275: ec:85:2f:15:39:32
  Sending EAPOL-Key Message to mobile ec:85:2f:15:39:32
  state INITPMK (message 1), replay counter
  00.00.00.00.00.00.00.00
!--- Message-1 of the WPA/WPA2 4-Way handshake is sent from
     the WLC/AP to the client.

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.284: ec:85:2f:15:39:32
  Received EAPOL-Key from mobile ec:85:2f:15:39:32
*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.284: ec:85:2f:15:39:32
  Received EAPOL-key in PTK_START state (message 2) from mobile
  ec:85:2f:15:39:32
!--- Message-2 of the WPA/WPA-2 4-Way handshake is successfully
     received from the client.

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.284: ec:85:2f:15:39:32
  PMK: Sending cache add

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.285: ec:85:2f:15:39:32
  Sending EAPOL-Key Message to mobile ec:85:2f:15:39:32
  state PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01
!--- Message-3 of the WPA/WPA2 4-Way handshake is sent from
     the WLC/AP to the client.

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.291: ec:85:2f:15:39:32
  Received EAPOL-Key from mobile ec:85:2f:15:39:32
*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.291: ec:85:2f:15:39:32
  Received EAPOL-key in PTKINITNEGOTIATING state (message 4)
  from mobile ec:85:2f:15:39:32
!--- Message-4 (final message) of this initial WPA/WPA2 4-Way
     handshake is successfully received from the client, which
     confirms the installation of the derived keys. They can
```

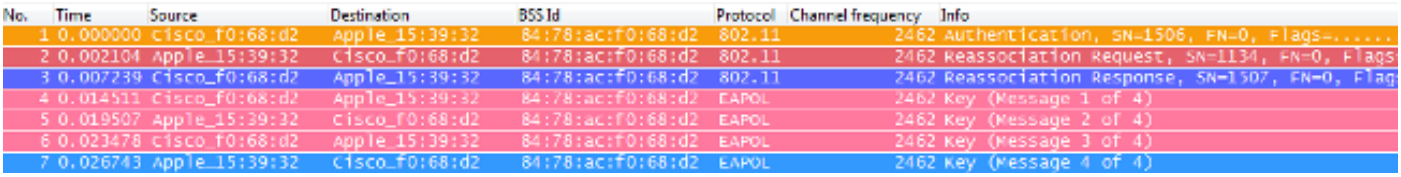
now be used in order to encrypt data frames with the current AP.

Com esse método, o AP e o cliente sem fio armazenam em cache as PMKs das associações seguras já estabelecidas. Portanto, se o cliente sem fio faz roaming para um novo AP ao qual nunca foi associado, o cliente deve executar uma autenticação EAP completa novamente, como mostrado nesta imagem, onde o cliente faz roaming para um novo AP:



No.	Time	Source	Destination	BSS Id	Protocol	Channel frequency	Info
1	0.000000	Apple_15:39:32	Cisco_f0:2a:92	84:78:ac:f0:2a:92	802.11	2437	Authentication, SN=462, FN=0, Flags=.
2	0.000819	Cisco_f0:2a:92	Apple_15:39:32	84:78:ac:f0:2a:92	802.11	2437	Authentication, SN=3633, FN=0, Flags=
3	0.002754	Apple_15:39:32	Cisco_f0:2a:92	84:78:ac:f0:2a:92	802.11	2437	Reassociation Request, SN=463, FN=0,
4	0.007638	Cisco_f0:2a:92	Apple_15:39:32	84:78:ac:f0:2a:92	802.11	2437	Reassociation Response, SN=3634, FN=0
5	0.013519	Cisco_f0:2a:92	Apple_15:39:32	84:78:ac:f0:2a:92	EAP	2437	Request, Identity
6	0.043063	Cisco_f0:2a:92	Apple_15:39:32	84:78:ac:f0:2a:92	EAP	2437	Request, Protected EAP (EAP-PEAP)
7	0.054400	Apple_15:39:32	Cisco_f0:2a:92	84:78:ac:f0:2a:92	TLSv1	2437	Client Hello
8	0.060031	Cisco_f0:2a:92	Apple_15:39:32	84:78:ac:f0:2a:92	TLSv1	2437	Server Hello, Change Cipher Spec, Enc
9	0.093278	Apple_15:39:32	Cisco_f0:2a:92	84:78:ac:f0:2a:92	TLSv1	2437	Change Cipher Spec, Encrypted Handsha
10	0.099981	Cisco_f0:2a:92	Apple_15:39:32	84:78:ac:f0:2a:92	TLSv1	2437	Application Data
11	0.105545	Apple_15:39:32	Cisco_f0:2a:92	84:78:ac:f0:2a:92	TLSv1	2437	Application Data
12	0.110891	Cisco_f0:2a:92	Apple_15:39:32	84:78:ac:f0:2a:92	EAP	2437	Success
13	0.112656	Cisco_f0:2a:92	Apple_15:39:32	84:78:ac:f0:2a:92	EAPOL	2437	Key (Message 1 of 4)
14	0.115722	Apple_15:39:32	Cisco_f0:2a:92	84:78:ac:f0:2a:92	EAPOL	2437	Key (Message 2 of 4)
15	0.119364	Cisco_f0:2a:92	Apple_15:39:32	84:78:ac:f0:2a:92	EAPOL	2437	Key (Message 3 of 4)
16	0.123520	Apple_15:39:32	Cisco_f0:2a:92	84:78:ac:f0:2a:92	EAPOL	2437	Key (Message 4 of 4)
17	2.374472	Apple_15:39:32	IPv6mcast_00:00:0(	84:78:ac:f0:2a:92	802.11	2437	QoS Data, SN=6, FN=0, Flags=.p.....TC

No entanto, se o cliente sem fio retornar a um AP em que uma associação/autenticação anterior ocorreu, o cliente enviará um quadro de Solicitação de Reassociação que lista vários PMKIDs, que informa o AP dos PMKs armazenados em cache de todos os APs em que o cliente foi autenticado anteriormente. Portanto, como o cliente está fazendo roaming de volta para um AP que também tem um PMK em cache para esse cliente, o cliente não precisa reautenticar por meio do EAP para derivar um novo PMK. O cliente simplesmente passa pelo handshake de 4 vias WPA2 para derivar as novas chaves de criptografia transitórias:



No.	Time	Source	Destination	BSS Id	Protocol	Channel frequency	Info
1	0.000000	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	802.11	2462	Authentication, SN=1506, FN=0, Flags=.....
2	0.002104	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	802.11	2462	Reassociation Request, SN=1134, FN=0, Flags
3	0.007239	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	802.11	2462	Reassociation Response, SN=1507, FN=0, Flag
4	0.014511	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAPOL	2462	Key (Message 1 of 4)
5	0.019507	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	EAPOL	2462	Key (Message 2 of 4)
6	0.023478	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAPOL	2462	Key (Message 3 of 4)
7	0.026743	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	EAPOL	2462	Key (Message 4 of 4)

> **Observação**: essa imagem não mostra o primeiro quadro de autenticação de Sistema Aberto 802.11 do cliente, mas isso não ocorre devido ao método implementado, pois esse quadro é sempre necessário. O motivo é que esse quadro específico não é criado pelo adaptador ou pelo software de imagem de pacote sem fio usado para farejar os quadros no ar para esse exemplo, mas é deixado dessa forma no exemplo para fins educacionais. Esteja ciente de que há uma possibilidade de que isso possa acontecer quando você executa imagens de pacote no ar; alguns quadros podem ser perdidos pela imagem, mas são realmente trocados entre o cliente e o AP. Caso contrário, o roaming nunca será iniciado neste exemplo.

Aqui está um resumo das depurações de WLC para este método de roaming rápido e seguro:

```
*apfMsConnTask_0: Jun 22 00:26:40.787: ec:85:2f:15:39:32
  Reassociation received from mobile on BSSID
  84:78:ac:f0:68:d2
!--- This is the Reassociation Request from the client.
```

```
*apfMsConnTask_0: Jun 22 00:26:40.787: ec:85:2f:15:39:32
  Processing RSN IE type 48, length 38 for mobile
  ec:85:2f:15:39:32
!--- The WLC/AP finds an Information Element that claims PMKID
     Caching support on the Association request that is sent
     from the client.

*apfMsConnTask_0: Jun 22 00:26:40.787: ec:85:2f:15:39:32
  Received RSN IE with 1 PMKIDs from mobile
  ec:85:2f:15:39:32
!--- The Reassociation Request from the client comes with
     one PMKID.

*apfMsConnTask_0: Jun 22 00:26:40.787:
  Received PMKID:  (16)
*apfMsConnTask_0: Jun 22 00:26:40.788:
  [0000] c9 4d 0d 97 03 aa a9 0f 1b c8 33 73 01 f1 18 f5
!--- This is the PMKID that is received.

*apfMsConnTask_0: Jun 22 00:26:40.788: ec:85:2f:15:39:32
  Searching for PMKID in MSCB PMKID cache for mobile
  ec:85:2f:15:39:32
!--- WLC searches for a matching PMKID on the database.

*apfMsConnTask_0: Jun 22 00:26:40.788: ec:85:2f:15:39:32
  Found an cache entry for BSSID 84:78:ac:f0:68:d2 in
  PMKID cache at index 0 of station ec:85:2f:15:39:32

*apfMsConnTask_0: Jun 22 00:26:40.788: ec:85:2f:15:39:32
  Found a valid PMKID in the MSCB PMKID cache for mobile
  ec:85:2f:15:39:32
!--- The WLC validates the PMKID provided by the client,
     and confirms that it has a valid PMK cache for this
     client-and-AP pair.

*apfMsConnTask_0: Jun 22 00:26:40.788: ec:85:2f:15:39:32
  Setting active key cache index 1 ---> 0

*apfMsConnTask_0: Jun 22 00:26:40.788: ec:85:2f:15:39:32
  Sending Assoc Response to station on BSSID
  84:78:ac:f0:68:d2(status 0) ApVapId 3 Slot 0
!--- The Reassociation Response is sent to the client, which
     validates the fast-roam with SKC.

*dot1xMsgTask: Jun 22 00:26:40.795: ec:85:2f:15:39:32
  Initiating RSN with existing PMK to mobile
  ec:85:2f:15:39:32
!--- WLC initiates a Robust Secure Network association with
     this client-and-AP pair based on the cached PMK found.
Hence, EAP is avoided as per the next message.

*dot1xMsgTask: Jun 22 00:26:40.795: ec:85:2f:15:39:32
  Skipping EAP-Success to mobile ec:85:2f:15:39:32

*dot1xMsgTask: Jun 22 00:26:40.795: ec:85:2f:15:39:32
  Found an cache entry for BSSID 84:78:ac:f0:68:d2 in
  PMKID cache at index 0 of station ec:85:2f:15:39:32

*dot1xMsgTask: Jun 22 00:26:40.795: Including PMKID in M1(16)
!--- The hashed PMKID is included on the Message-1 of the
     WPA/WPA2 4-Way handshake.

*dot1xMsgTask: Jun 22 00:26:40.795:
  [0000] c9 4d 0d 97 03 aa a9 0f 1b c8 33 73 01 f1 18 f5
```

```
!--- The PMKID is hashed. The next messages are the same
     WPA/WPA2 4-Way handshake messages described thus far
     that are used in order to finish the encryption keys
     generation/installation.

*dot1xMsgTask: Jun 22 00:26:40.795: ec:85:2f:15:39:32
  Sending EAPOL-Key Message to mobile ec:85:2f:15:39:32 state
  INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00

*Dot1x_NW_MsgTask_2: Jun 22 00:26:40.811: ec:85:2f:15:39:32
  Received EAPOL-Key from mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 22 00:26:40.812: ec:85:2f:15:39:32
  Received EAPOL-key in PTK_START state (message 2) from mobile
  ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 22 00:26:40.812: ec:85:2f:15:39:32
  PMK: Sending cache add

*Dot1x_NW_MsgTask_2: Jun 22 00:26:40.812: ec:85:2f:15:39:32
  Sending EAPOL-Key Message to mobile ec:85:2f:15:39:32 state
  PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01

*Dot1x_NW_MsgTask_2: Jun 22 00:26:40.820: ec:85:2f:15:39:32
  Received EAPOL-Key from mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 22 00:26:40.820: ec:85:2f:15:39:32
  Received EAPOL-key in PTKINITNEGOTIATING state (message 4)
  from mobile ec:85:2f:15:39:32
```

FlexConnect com cache PMKID / cache de chave sticky

- Quando você usa esse método em uma configuração do FlexConnect, ele pode funcionar e o comportamento pode parecer semelhante ao que foi explicado anteriormente se você usar a Autenticação central de volta para a WLC (com switching central ou local); no entanto, esse método de SKC não é suportado no FlexConnect.
- Esse método é oficialmente suportado apenas no CUWN com APs no modo Local, não no FlexConnect ou em outros modos.

Prós com cache PMKID / Sticky Key Caching

Esse método pode ser implementado localmente por APs autônomos independentes, sem a necessidade de um dispositivo centralizado para gerenciar as chaves em cache.

Contras com Cache PMKID / Sticky Key Caching

- Como mencionado anteriormente neste documento, a principal limitação desse método é que o cliente pode executar roaming rápido e seguro somente quando estiver em roaming de volta para um AP ao qual tenha sido previamente associado/autenticado. Se estiver em roaming para um novo AP, o cliente deverá concluir a autenticação EAP completa novamente.
- O cliente sem fio e os APs devem se lembrar de todas as PMKs derivadas em cada nova autenticação, portanto, esse recurso é normalmente limitado a uma determinada quantidade de PMKs que estão em cache. Como esse limite não é claramente definido pelo padrão, os fornecedores podem definir limites diferentes em suas implementações de SKC. Por

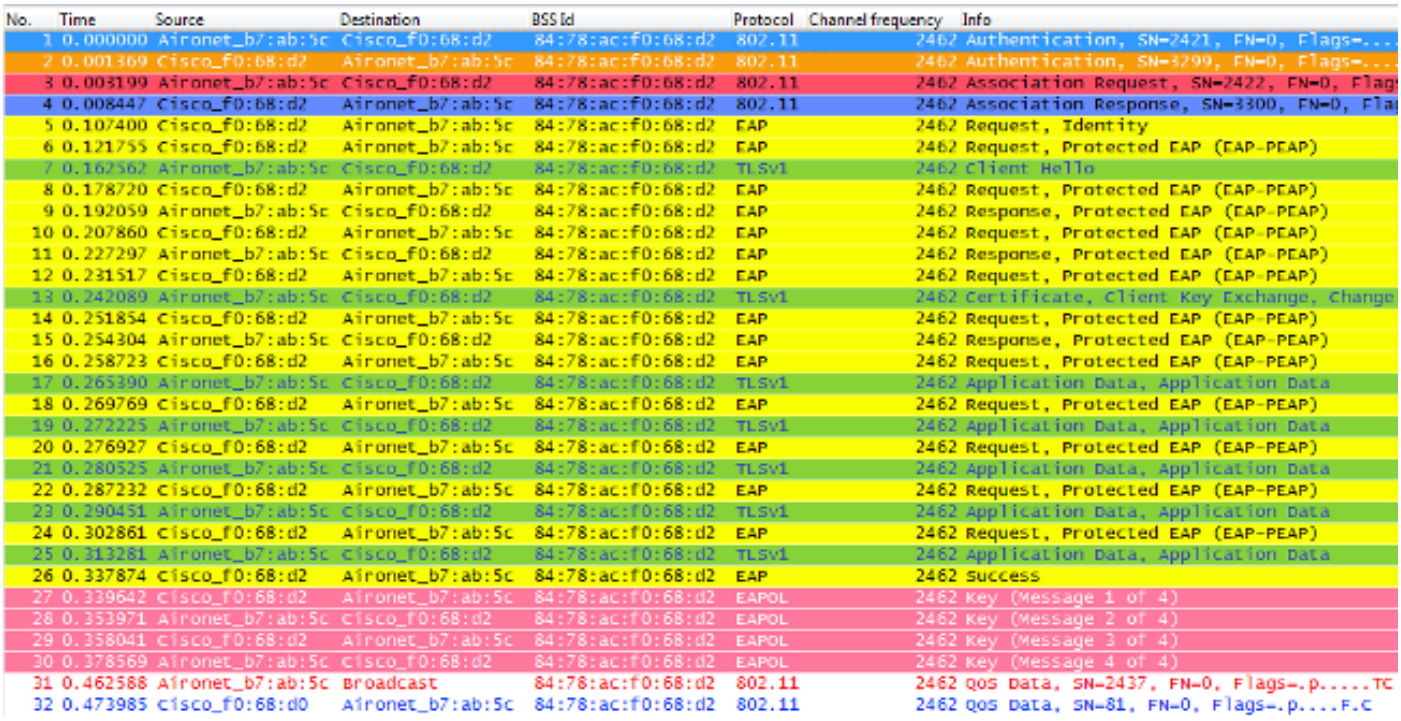
exemplo, os Cisco WLAN Controllers podem atualmente armazenar em cache os PMKs de um cliente para até oito APs. Se um cliente faz roaming para mais de oito APs por sessão, os APs mais antigos são removidos da lista de cache para armazenar as entradas recém-armazenadas em cache.
- Esse método é opcional e ainda não é suportado por muitos dispositivos WPA2; portanto, esse método não é amplamente adotado e implantado.
- O SKC não é suportado quando você executa roaming entre controladores, o que ocorre quando você se move entre APs gerenciados por WLCs diferentes, mesmo que eles estejam no mesmo grupo de mobilidade.

Roaming rápido e seguro com cache de chave oportunista

O OKC (Opportunistic Key Caching), também conhecido como PKC (Proactive Key Caching) (este termo é explicado em maiores detalhes em uma nota a seguir), é basicamente um aprimoramento do método de cache de PMKID WPA2 descrito anteriormente, e é por isso que ele também é chamado de Cache de PMKID Proativo/Oportunista. Portanto, é importante observar que esse não é um método de roaming rápido-seguro definido pelo padrão 802.11 e não é suportado por muitos dispositivos, mas funciona com WPA2-EAP, assim como o cache PMKID.

Essa técnica permite que o cliente sem fio e a infraestrutura da WLAN armazenem em cache apenas um PMK durante o tempo de vida da associação do cliente com essa WLAN (derivado do MSK após a autenticação 802.1X/EAP inicial com o Servidor de autenticação), mesmo quando em roaming entre vários APs, pois todos eles compartilham o PMK original que é usado como a semente em todos os handshakes de 4 vias WPA2. Isso ainda é necessário, assim como no SKC, para gerar novas chaves de criptografia toda vez que o cliente se reassocia aos APs. Para que os APs compartilhem esse PMK original da sessão do cliente, todos devem estar sob algum tipo de controle administrativo, com um dispositivo centralizado que armazena em cache e distribui o PMK original para todos os APs. Isso é semelhante ao CUWN, onde a WLC executa esse trabalho para todos os LAPs sob seu controle e usa os grupos de mobilidade para lidar com esse PMK entre várias WLCs; portanto, essa é uma limitação em ambientes de AP autônomos.

Com esse método, assim como no PMKID Caching (SKC), a associação inicial a qualquer AP é uma autenticação de primeira vez regular para a WLAN, onde você deve completar toda a autenticação 802.1X/EAP no Servidor de autenticação e o handshake de 4 vias para geração de chave antes de enviar quadros de dados. Aqui está uma imagem de tela que ilustra isso:



No.	Time	Source	Destination	BSS Id	Protocol	Channel frequency	Info
1	0.000000	Aironet_b7:ab:5c	Cisco_f0:68:d2	84:78:ac:f0:68:d2	802.11	2462	Authentication, SN=2421, FN=0, Flags=...
2	0.001369	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	802.11	2462	Authentication, SN=3299, FN=0, Flags=...
3	0.003199	Aironet_b7:ab:5c	Cisco_f0:68:d2	84:78:ac:f0:68:d2	802.11	2462	Association Request, SN=2422, FN=0, Flag
4	0.008447	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	802.11	2462	Association Response, SN=3300, FN=0, Fla
5	0.107400	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	EAP	2462	Request, Identity
6	0.121755	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
7	0.162562	Aironet_b7:ab:5c	Cisco_f0:68:d2	84:78:ac:f0:68:d2	TLSv1	2462	Client Hello
8	0.178720	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
9	0.192059	Aironet_b7:ab:5c	Cisco_f0:68:d2	84:78:ac:f0:68:d2	EAP	2462	Response, Protected EAP (EAP-PEAP)
10	0.207860	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
11	0.227297	Aironet_b7:ab:5c	Cisco_f0:68:d2	84:78:ac:f0:68:d2	EAP	2462	Response, Protected EAP (EAP-PEAP)
12	0.231517	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
13	0.242089	Aironet_b7:ab:5c	Cisco_f0:68:d2	84:78:ac:f0:68:d2	TLSv1	2462	Certificate, Client Key Exchange, Change
14	0.251854	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
15	0.254304	Aironet_b7:ab:5c	Cisco_f0:68:d2	84:78:ac:f0:68:d2	EAP	2462	Response, Protected EAP (EAP-PEAP)
16	0.258723	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
17	0.265390	Aironet_b7:ab:5c	Cisco_f0:68:d2	84:78:ac:f0:68:d2	TLSv1	2462	Application Data, Application Data
18	0.269769	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
19	0.272225	Aironet_b7:ab:5c	Cisco_f0:68:d2	84:78:ac:f0:68:d2	TLSv1	2462	Application Data, Application Data
20	0.276927	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
21	0.280525	Aironet_b7:ab:5c	Cisco_f0:68:d2	84:78:ac:f0:68:d2	TLSv1	2462	Application Data, Application Data
22	0.287232	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
23	0.290451	Aironet_b7:ab:5c	Cisco_f0:68:d2	84:78:ac:f0:68:d2	TLSv1	2462	Application Data, Application Data
24	0.302861	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
25	0.313281	Aironet_b7:ab:5c	Cisco_f0:68:d2	84:78:ac:f0:68:d2	TLSv1	2462	Application Data, Application Data
26	0.337874	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	EAP	2462	Success
27	0.339642	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	EAPOL	2462	Key (Message 1 of 4)
28	0.353971	Aironet_b7:ab:5c	Cisco_f0:68:d2	84:78:ac:f0:68:d2	EAPOL	2462	Key (Message 2 of 4)
29	0.358041	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	EAPOL	2462	Key (Message 3 of 4)
30	0.378569	Aironet_b7:ab:5c	Cisco_f0:68:d2	84:78:ac:f0:68:d2	EAPOL	2462	Key (Message 4 of 4)
31	0.462588	Aironet_b7:ab:5c	Broadcast	84:78:ac:f0:68:d2	802.11	2462	QoS Data, SN=2437, FN=0, Flags=.p.....TC
32	0.473985	Cisco_f0:68:d0	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	802.11	2462	QoS Data, SN=81, FN=0, Flags=.p....F.C

As saídas de depuração mostram basicamente a mesma troca de quadros de autenticação EAP que o resto dos métodos descritos neste documento na autenticação inicial para a WLAN (como mostrado nas imagens), juntamente com a adição de algumas saídas que dizem respeito às técnicas de cache de chave usadas pela WLC aqui. Esta saída de depuração também é cortada para mostrar apenas as informações relevantes:

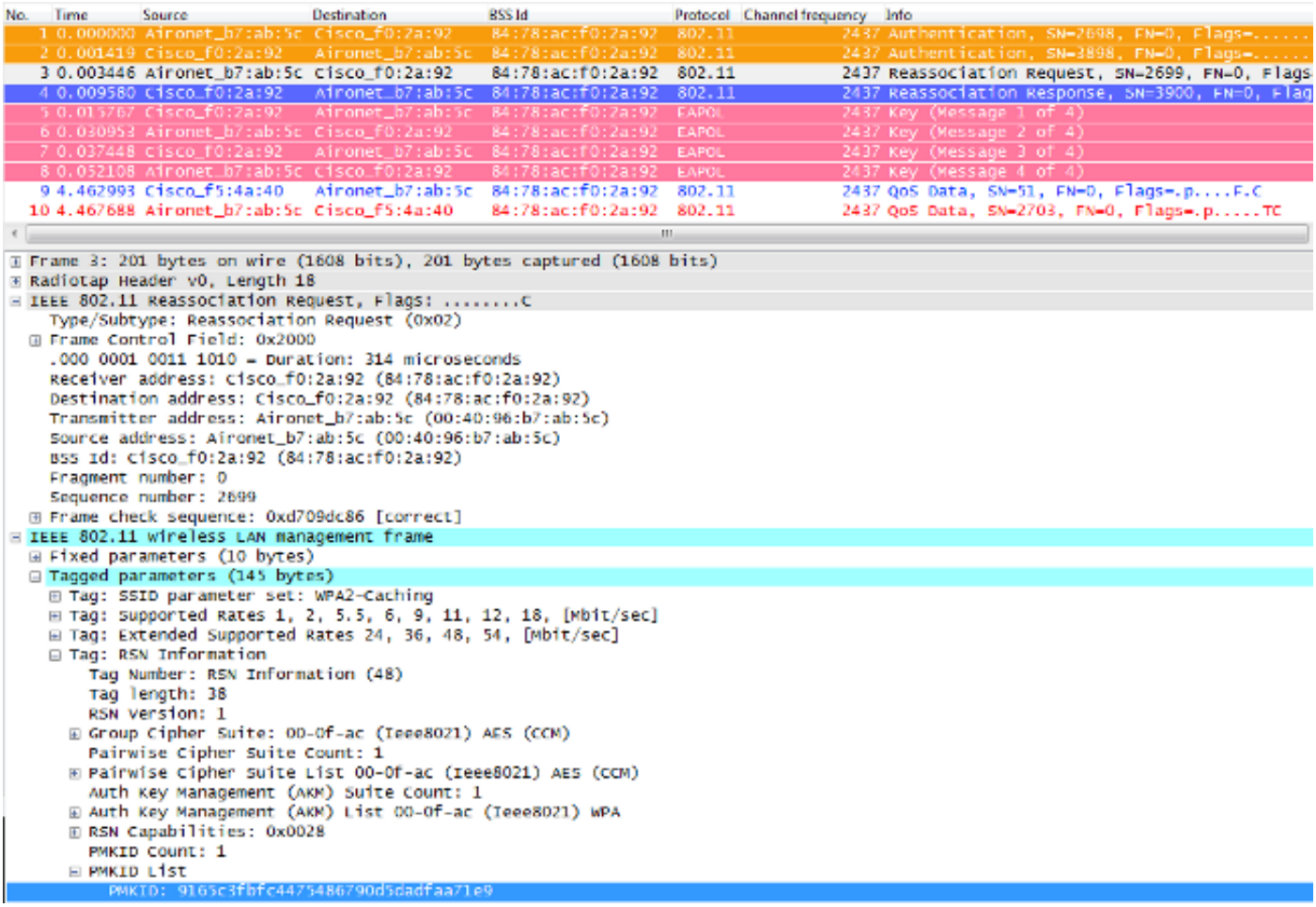
```
*apfMsConnTask_0: Jun 21 21:46:06.515: 00:40:96:b7:ab:5c
  Association received from mobile on BSSID
  84:78:ac:f0:68:d2
!--- This is the Association Request from the client.

*apfMsConnTask_0: Jun 21 21:46:06.516: 00:40:96:b7:ab:5c
  Processing RSN IE type 48, length 20 for mobile
  00:40:96:b7:ab:5c
!--- The WLC/AP finds an Information Element that claims
     PMKID Caching support on the Association request that
     is sent from the client.

*apfMsConnTask_0: Jun 21 21:46:06.516: 00:40:96:b7:ab:5c
  Received RSN IE with 0 PMKIDs from mobile
  00:40:96:b7:ab:5c
!--- Since this is an initial association, the Association
     Request comes without any PMKID.

*apfMsConnTask_0: Jun 21 21:46:06.516: 00:40:96:b7:ab:5c
  Setting active key cache index 0 ---> 8

*apfMsConnTask_0: Jun 21 21:46:06.516: 00:40:96:b7:ab:5c
  Sending Assoc Response to station on BSSID
  84:78:ac:f0:68:d2 (status 0) ApVapId 3 Slot
!--- The Association Response is sent to the client.

*dot1xMsgTask: Jun 21 21:46:06.522: 00:40:96:b7:ab:5
  Sending EAP-Request/Identity to mobile 00:40:96:b7:ab:5c
  (EAP Id 1)

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.614: 00:40:96:b7:ab:5c
  Received EAPOL START from mobile 00:40:96:b7:ab:5c
```

```
*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.614: 00:40:96:b7:ab:5c
  Sending EAP-Request/Identity to mobile 00:40:96:b7:ab:5c
  (EAP Id 2)

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.623: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.623: 00:40:96:b7:ab:5c
  Received Identity Response (count=2) from mobile
  00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.630: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.630: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 3)

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.673: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.673: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 3, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.843: 00:40:96:b7:ab:5c
  Processing Access-Accept for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: 00:40:96:b7:ab:5c
  Creating a PKC PMKID Cache entry for station
  00:40:96:b7:ab:5c (RSN 2)
*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: 00:40:96:b7:ab:5c
  Setting active key cache index 8 ---> 8
*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: 00:40:96:b7:ab:5c
  Setting active key cache index 8 ---> 0
*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: 00:40:96:b7:ab:5c
  Adding BSSID 84:78:ac:f0:68:d2 to PMKID cache at index 0
  for station 00:40:96:b7:ab:5
*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: New PMKID: (16)
*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844:
  [0000] 4e a1 7f 5a 75 48 9c f9 96 e3 a8 71 25 6f 11 d0
!--- WLC creates a PMK cache entry for this client, which is
      used for OKC in this case, so the PMKID is computed
      with the AP MAC address (BSSID 84:78:ac:f0:68:d2).

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: 00:40:96:b7:ab:5c
  PMK sent to mobility group
!--- The PMK cache entry for this client is shared with the
      WLCs on the mobility group.

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: 00:40:96:b7:ab:5c
  Sending EAP-Success to mobile 00:40:96:b7:ab:5c (EAP Id 13)

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: 00:40:96:b7:ab:5c
  Found an cache entry for BSSID 84:78:ac:f0:68:d2 in PMKID
  cache at index 0 of station 00:40:96:b7:ab:5

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: Including PMKID
  in M1  (16)
!--- The hashed PMKID is included on the Message-1 of the
      WPA/WPA2 4-Way handshake.

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844:
```

```
  [0000] 4e a1 7f 5a 75 48 9c f9 96 e3 a8 71 25 6f 11 d0
!--- This is the hashed PMKID. The next messages are the same
     WPA/WPA2 4-Way handshake messages described thus far that
     are used in order to finish the encryption keys
     generation/installation.

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c state
  INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.865: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.865: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTK_START state (message 2)
  from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.865: 00:40:96:b7:ab:5c
  PMK: Sending cache add

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.865: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c state
  PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.889: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.890: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTKINITNEGOTIATING state (message 4)
  from mobile 00:40:96:b7:ab:5c
```

Com esse método, o cliente sem fio e a WLC (para todos os APs gerenciados) armazenam em cache um PMK original da associação segura que é inicialmente estabelecida. Basicamente, toda vez que o cliente sem fio se conecta a um AP específico, um PMKID é dividido em: o endereço MAC do cliente, o endereço MAC do AP (BSSID da WLAN) e o PMK derivado com esse AP. Portanto, como o OKC armazena em cache o mesmo PMK original para todos os APs e para o cliente específico, quando esse cliente (re)associa-se a outro AP, o único valor que muda para fazer o hash do novo PMKID é o novo endereço MAC do AP.

Quando o cliente inicia o roaming para um novo AP e envia o quadro de Solicitação de Reassociação, ele adiciona o PMKID no Elemento de Informações RSN WPA2 se quiser informar ao AP que um PMK em cache é usado para o roaming rápido e seguro. Ele já sabe o endereço MAC do BSSID (AP) para onde ele faz roaming, em seguida, o cliente simplesmente mistura o novo PMKID que é usado nesta Solicitação de Reassociação. Quando o AP recebe essa solicitação do cliente, ele também mistura o PMKID com os valores que já tem (o PMK armazenado em cache, o endereço MAC do cliente e seu próprio endereço MAC do AP) e responde com a Resposta de Reassociação bem-sucedida que confirma a correspondência dos PMKIDs. A PMK armazenada em cache pode ser usada como a semente que inicia um handshake de 4 vias WPA2 para derivar as novas chaves de criptografia (e ignorar EAP):



Nesta imagem, o quadro Solicitação de reassociação do cliente é selecionado e expandido para que você possa ver mais detalhes do quadro. As informações de endereço MAC e também o Elemento de Informação de Rede de Segurança Robusta (RSN, conforme 802.11i - WPA2), onde são mostradas as informações sobre as configurações WPA2 usadas para esta associação (destacado é o PMKID obtido da fórmula com hash).

Aqui está um resumo das depurações de WLC para este método de roaming rápido e seguro com OKC:

```
*apfMsConnTask_2: Jun 21 21:48:50.562: 00:40:96:b7:ab:5c
  Reassociation received from mobile on BSSID
  84:78:ac:f0:2a:92
!--- This is the Reassociation Request from the client.

*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c
  Processing RSN IE type 48, length 38 for mobile
  00:40:96:b7:ab:5c
!--- The WLC/AP finds and Information Element that claims
     PMKID Caching support on the Association request that
     is sent from the client.

*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c
  Received RSN IE with 1 PMKIDs from mobile
  00:40:96:b7:ab:5c
!--- The Reassociation Request from the client comes with
     one PMKID.

*apfMsConnTask_2: Jun 21 21:48:50.563:
  Received PMKID:  (16)
```

```
*apfMsConnTask_2: Jun 21 21:48:50.563:
  [0000] 91 65 c3 fb fc 44 75 48 67 90 d5 da df aa 71 e9

*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c
  Searching for PMKID in MSCB PMKID cache for mobile
  00:40:96:b7:ab:5c
*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c
  No valid PMKID found in the MSCB PMKID cache for mobile
  00:40:96:b7:ab:5
!--- As the client has never authenticated with this new AP,
      the WLC cannot find a valid PMKID to match the one provided
      by the client. However, since the client performs OKC
      and not SKC (as per the following messages), the WLC computes
      a new PMKID based on the information gathered (the cached PMK,
      the client MAC address, and the new AP MAC address).

*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c
  Trying to compute a PMKID from MSCB PMK cache for mobile
  00:40:96:b7:ab:5c

*apfMsConnTask_2: Jun 21 21:48:50.563:
  CCKM: Find PMK in cache: BSSID =  (6)
*apfMsConnTask_2: Jun 21 21:48:50.563:
  [0000] 84 78 ac f0 2a 90
*apfMsConnTask_2: Jun 21 21:48:50.563:
  CCKM: Find PMK in cache: realAA =  (6)
*apfMsConnTask_2: Jun 21 21:48:50.563:
  [0000] 84 78 ac f0 2a 92
*apfMsConnTask_2: Jun 21 21:48:50.563:
  CCKM: Find PMK in cache: PMKID =  (16)
*apfMsConnTask_2: Jun 21 21:48:50.563:
  [0000] 91 65 c3 fb fc 44 75 48 67 90 d5 da df aa 71 e9
*apfMsConnTask_2: Jun 21 21:48:50.563:
  CCKM: AA (6)
*apfMsConnTask_2: Jun 21 21:48:50.563:
  [0000] 84 78 ac f0 2a 92
*apfMsConnTask_2: Jun 21 21:48:50.563:
  CCKM: SPA (6)
*apfMsConnTask_2: Jun 21 21:48:50.563:
  [0000] 00 40 96 b7 ab 5c
*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c
  Adding BSSID 84:78:ac:f0:2a:92 to PMKID cache at
  index 0 for station 00:40:96:b7:ab:5c
*apfMsConnTask_2: Jun 21 21:48:50.563:
  New PMKID: (16)
*apfMsConnTask_2: Jun 21 21:48:50.563:
  [0000] 91 65 c3 fb fc 44 75 48 67 90 d5 da df aa 71 e9
*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c
  Computed a valid PMKID from MSCB PMK cache for mobile
  00:40:96:b7:ab:5c
!--- The new PMKID is computed and validated to match the
      one provided by the client, which is also computed with
      the same information. Hence, the fast-secure roam is
      possible.

*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c
  Setting active key cache index 0 ---> 0

*apfMsConnTask_2: Jun 21 21:48:50.564: 00:40:96:b7:ab:5c
  Sending Assoc Response to station on BSSID 84:78:ac:f0:2a:92
  (status 0) ApVapId 3 Slot
!--- The Reassociation response is sent to the client, which
      validates the fast-roam with OKC.
```

```
*dot1xMsgTask: Jun 21 21:48:50.570: 00:40:96:b7:ab:5c
  Initiating RSN with existing PMK to mobile
  00:40:96:b7:ab:5c
!--- WLC initiates a Robust Secure Network association with
     this client-and AP pair with the cached PMK found.
Hence, EAP is avoided, as per the the next message.

*dot1xMsgTask: Jun 21 21:48:50.570: 00:40:96:b7:ab:5c
  Skipping EAP-Success to mobile 00:40:96:b7:ab:5c

*dot1xMsgTask: Jun 21 21:48:50.570: 00:40:96:b7:ab:5c
  Found an cache entry for BSSID 84:78:ac:f0:2a:92 in
  PMKID cache at index 0 of station 00:40:96:b7:ab:5c

*dot1xMsgTask: Jun 21 21:48:50.570:
  Including PMKID in M1  (16)
!--- The hashed PMKID is included on the Message-1 of the
     WPA/WPA2 4-Way handshake.

*dot1xMsgTask: Jun 21 21:48:50.570:
  [0000] 91 65 c3 fb fc 44 75 48 67 90 d5 da df aa 71 e9
!--- The PMKID is hashed. The next messages are the same
     WPA/WPA2 4-Way handshake messages described thus far,
     which are used in order to finish the encryption keys
     generation/installation.

*dot1xMsgTask: Jun 21 21:48:50.570: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c state
  INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00

*Dot1x_NW_MsgTask_4: Jun 21 21:48:50.589: 00:40:96:b7:ab:5
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:48:50.589: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTK_START state (message 2) from mobile
  00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:48:50.589: 00:40:96:b7:ab:5c
  PMK: Sending cache add

*Dot1x_NW_MsgTask_4: Jun 21 21:48:50.590: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c state
  PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01

*Dot1x_NW_MsgTask_4: Jun 21 21:48:50.610: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:48:50.610: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTKINITNEGOTIATING state (message 4)
  from mobile 00:40:96:b7:ab:5c
```

Como mostrado no início das depurações, o PMKID deve ser computado depois que a Solicitação de Reassociação do cliente for recebida. Isso é necessário para validar o PMKID e confirmar se o PMK em cache é usado com o handshake de 4 vias WPA2 para derivar as chaves de criptografia e concluir o roaming rápido e seguro. Não confunda as entradas CCKM nas depurações; isso não é usado para executar o CCKM, mas o OKC, como explicado anteriormente. CCKM aqui é simplesmente um nome usado pela WLC para essas saídas, como o nome de uma função que manipula os valores para computar o PMKID.

FlexConnect com cache de chave oportunista

- Há suporte para a Autenticação Central. Isso inclui switching de dados local e central. Se o AP fizer parte do mesmo grupo FlexConnect, o roam com segurança rápida será substituído pelo AP, caso contrário, o roam com segurança rápida será substituído pelo controlador. **Observação**: essa configuração pode funcionar se os APs não estiverem no mesmo Grupo FlexConnect, mas essa não é uma configuração recomendada ou suportada.
- Há suporte para a Autenticação Local Flex. No modo conectado, o cache pode ser distribuído do AP para o controlador e, em seguida, para o restante dos APs no grupo FlexConnect.
- Há suporte para o modo autônomo. Se o cache já estiver presente no AP (devido à distribuição anterior), o roam rápido e seguro deverá funcionar. A nova autenticação no modo autônomo não oferece suporte ao roaming rápido e seguro.

Prós com Cache de Chave Oportunista

- O cliente sem fio e a infraestrutura da WLAN não precisam lembrar de vários PMKIDs, mas simplesmente armazenar em cache um PMK original da autenticação inicial para a WLAN. Em seguida, você deve criar um novo hash da PMKID apropriada (usada na Solicitação de reassociação) necessária com cada associação segura de AP para validar o roaming rápido e seguro.
- Aqui, o cliente sem fio executa roaming rápido e seguro para um novo AP na mesma WLAN/SSID, mesmo que nunca esteja associado a esse AP (não o caso em SKC). Desde que o cliente execute a autenticação 802.1X/EAP inicial com um AP gerenciado pela implantação centralizada que manipula o cache PMK para todos os APs para onde o cliente faz roaming, não serão necessárias mais autenticações completas para o resto da vida do cliente nesta WLAN.

Contras com Cache de Chave Oportunista

- Esse método é implantado apenas em um ambiente centralizado onde todos os APs estão sob algum tipo de controle administrativo (como um controlador de WLAN) que é responsável pelo cache e compartilhamento de um PMK original da sessão do cliente. Portanto, essa é uma limitação em ambientes AP autônomos.
- As técnicas que são aplicadas neste método não são sugeridas ou descritas no padrão 802.11, portanto, o suporte varia muito de um dispositivo para outro. No entanto, esse ainda é o método que foi mais adotado enquanto aguardava o 802.11r.

Observação sobre o termo "Cache de chave pró-ativo"

O Cache de chave pró-ativo (ou PKC) é conhecido como OKC (Cache de chave oportunista) e os dois termos são usados de forma intercambiável quando descrevem o mesmo método explicado aqui. No entanto, este foi apenas um termo que foi usado pelo espaço aéreo em 2001 para um antigo método de cache de chaves, que foi então usado pelo padrão 802.11i como base para "Pré-autenticação" (outro método de roaming rápido e seguro explicado brevemente abaixo). PKC não é Pré-autenticação ou OKC (Opportunistic Key Caching), mas quando você ouve ou lê sobre PKC, a referência é basicamente para OKC, e não para Pré-autenticação.

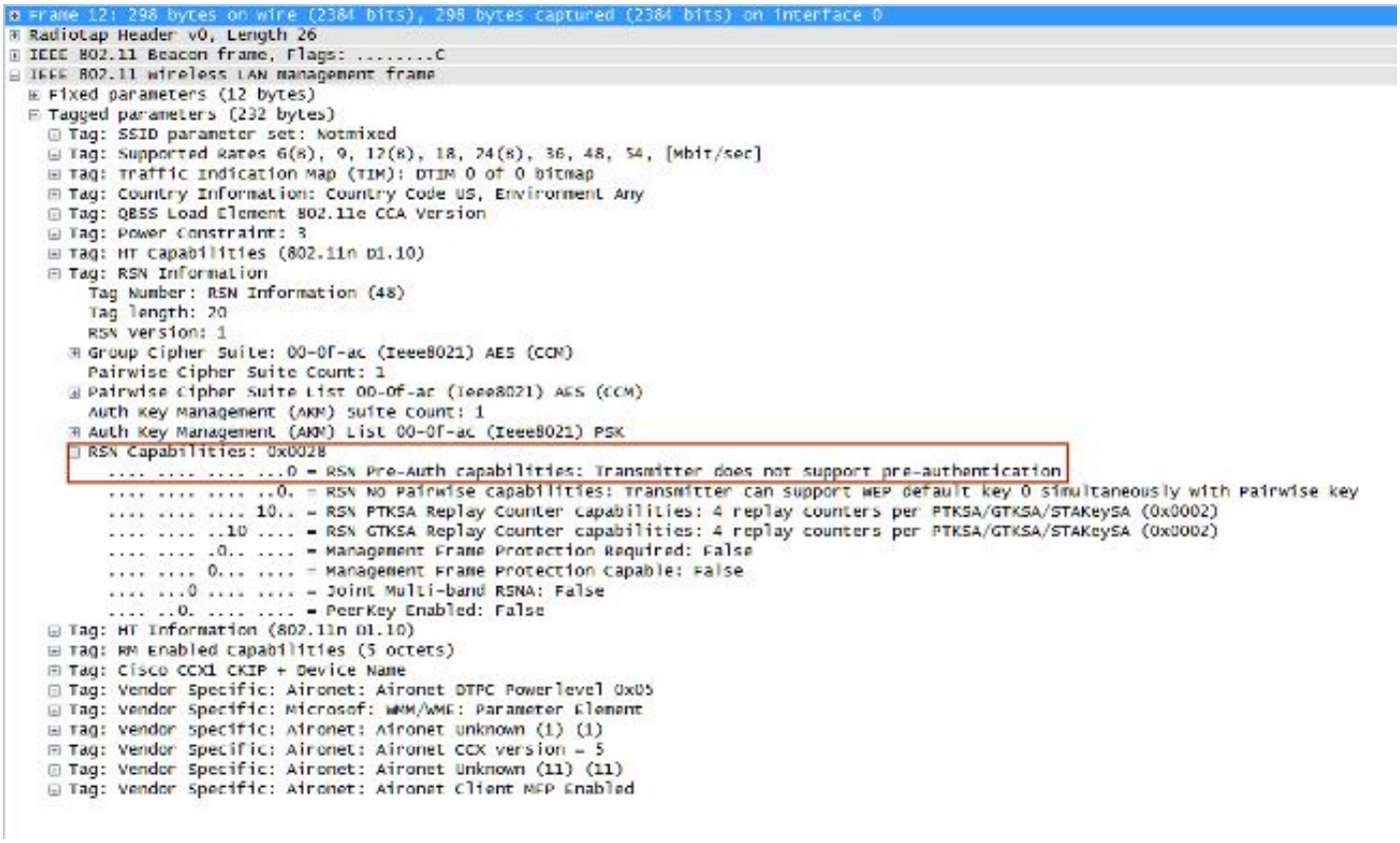
Roaming rápido e seguro com pré-autenticação

Esse método também é sugerido pelo padrão IEEE 802.11 dentro da emenda de segurança 802.11i, portanto, ele também funciona com WPA2, mas é o único método Fast Secure Roaming que não é suportado pela infraestrutura WLAN da Cisco. Por esta razão, é explicado apenas brevemente aqui e sem resultados.

Com a pré-autenticação, os clientes sem fio podem autenticar com vários APs de uma vez enquanto estão associados ao AP atual. Quando isso ocorre, o cliente envia os quadros de autenticação EAP para o AP atual onde está conectado, mas é destinado para o outro AP onde o cliente deseja executar a pré-autenticação (APs vizinhos que são possíveis candidatos para roaming). O AP atual envia esses quadros para o(s) AP(s) de destino pelo sistema de distribuição. O novo AP executa a autenticação completa contra o servidor RADIUS para este cliente, de modo que um handshake de autenticação EAP inteiro é concluído, e este novo AP atua como o Autenticador.

A ideia é executar a autenticação e derivar o PMK com os APs vizinhos antes que o cliente realmente faça roaming para eles, de modo que, quando for o momento de fazer roaming, o cliente já esteja autenticado e com um PMK já armazenado em cache para essa nova associação segura de AP para cliente, então eles só precisam executar o Handshake de 4 Vias e experimentar um roam rápido depois que o cliente enviar sua solicitação de reassociação inicial.

Aqui está uma imagem de um beacon AP que mostra o campo IE RSN que anuncia suporte para Pré-autenticação (este é de um AP Cisco, onde é confirmado que a Pré-autenticação não é suportada):



Prós com pré-autenticação

Há um PMK para cada associação segura AP-cliente, que pode ser considerado uma vantagem de segurança caso um AP seja comprometido e as chaves sejam roubadas (não pode ser usado com outros APs). No entanto, essa vantagem de segurança é tratada pela infraestrutura da WLAN de diferentes maneiras em outros métodos.

Contras com pré-autenticação

- Como há um PMK por AP, os clientes têm um limite na quantidade de APs que podem ser pré-autenticados.
- Cada vez que um cliente executa a pré-autenticação com um novo AP, há uma troca de autenticação EAP completa, o que significa mais carga na rede e no Servidor de autenticação.
- A maioria dos clientes sem fio não suporta esse método, pois ele nunca foi altamente adotado (o OKC foi mais adotado).

Roaming rápido e seguro com 802.11r

A técnica de roaming rápido-seguro baseada na emenda 802.11r (oficialmente denominada **Transição Fast BSS** pelo padrão 802.11 e conhecida como **FT**) é o primeiro método oficialmente ratificado (em 2008) pelo IEEE para o padrão 802.11 como a solução para realizar transições rápidas entre APs (Conjuntos de serviços básicos ou BSSs), que define claramente a hierarquia de chaves usada quando você manipula e armazena em cache chaves em uma WLAN. No entanto, sua adoção tem sido lenta, principalmente devido às outras soluções já disponíveis quando transições rápidas eram realmente necessárias, como com implementações de VoWLAN quando usadas com um dos métodos anteriormente explicados neste documento. Existem apenas alguns dispositivos que atualmente suportam algumas das opções de FT (até 2013).

Essa técnica é mais complexa de explicar do que os outros métodos, pois introduz novos conceitos e várias camadas de PMKs que são armazenadas em cache em dispositivos diferentes (cada dispositivo com uma função diferente) e fornece ainda mais opções para roaming rápido e seguro. Portanto, um breve resumo é fornecido sobre esse método e a forma como ele é implementado com cada opção disponível.

O 802.11r é diferente do SKC e OKC, principalmente por estes motivos:

- A mensagem de handshake (troca de PMKID, ANonce e SNonce, por exemplo) acontece nos quadros de autenticação 802.11 ou nos quadros de ação em vez dos quadros de reassociação. Diferentemente dos métodos de cache PMKID, a fase separada de handshake de 4 vias, que é levada após a troca de mensagens de (re)associação, é evitada. O handshake de chave com o novo AP começa antes que o cliente faça roaming/reassocie-se totalmente a esse novo AP.
- Ele fornece dois métodos para o handshake de roaming rápido: pelo AIR e pelo Sistema de Distribuição (DS).
- O 802.11r tem mais camadas de hierarquia de chave.
- Como esse protocolo evita o handshake de 4 vias para o gerenciamento de chaves quando um cliente faz roaming (gera novas chaves de criptografia - PTK e GTK - sem a necessidade desse handshake), ele também pode ser aplicado para configurações WPA2 com uma PSK, e não apenas quando 802.1X/EAP é usado para a autenticação. Isso acelera ainda mais o roaming nessas configurações, em que não ocorrem trocas de handshake de 4 vias ou EAP.

Com esse método, o cliente sem fio executa apenas uma autenticação inicial na infraestrutura da WLAN quando uma conexão é estabelecida com o primeiro AP e executa roaming rápido e seguro enquanto faz roaming entre APs do mesmo domínio de mobilidade FT.

Esse é um dos novos conceitos, que basicamente se refere aos APs que usam o mesmo SSID

(conhecido como Conjunto de serviços estendidos ou ESS) e manipulam as mesmas teclas FT. Isto é semelhante aos outros métodos explicados até agora. A maneira como os APs lidam com as chaves de domínio de mobilidade FT normalmente se baseia em uma configuração centralizada, como a WLC ou os grupos de mobilidade; no entanto, esse método também pode ser implementado em ambientes de AP autônomos.

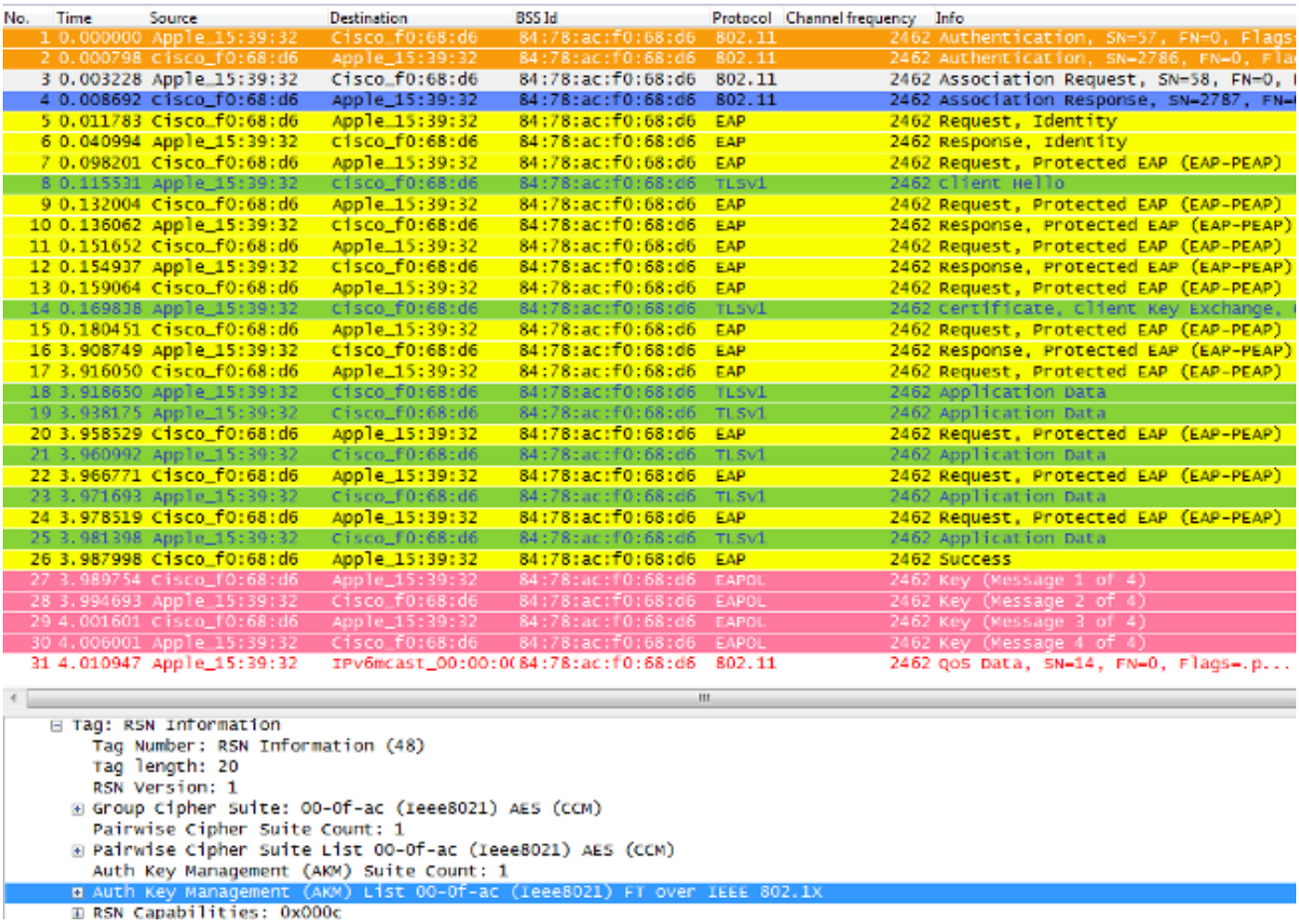
Aqui está um resumo da hierarquia principal:

- Um MSK ainda é derivado no solicitante do cliente e no Servidor de autenticação da fase de autenticação 802.1X/EAP inicial (transferido do Servidor de autenticação para o Autenticador (WLC) depois que a autenticação for bem-sucedida). Esta MSK, como nos outros métodos, é usada como semente para a hierarquia de chave FT. Quando você usa o WPA2-PSK em vez de um método de autenticação EAP, o PSK é basicamente esse MSK.
- Uma PMK-R0 (Pairwise Master Key R0) é derivada do MSK, que é a chave de primeiro nível da hierarquia de chave FT. Os detentores de chave para este PMK-R0 são o WLC e o cliente.
- Uma chave de segundo nível, chamada PMK-R1 (Pairwise Master Key R1), é derivada do PMK-R0, e os detentores de chave são o cliente e os APs gerenciados pelo WLC que contém o PMK-R0.
- A chave de terceiro e último nível da hierarquia de chaves FT é a PTK, que é a chave final usada para criptografar os quadros de dados unicast 802.11 (semelhante aos outros métodos que usam WPA/TKIP ou WPA2/AES). Esse PTK é derivado no FT do PMK-R1, e os detentores de chave são o cliente e os APs gerenciados pelo WLC.

  Observação: dependendo do fornecedor da WLAN e das configurações de implementação (como APs autônomos, FlexConnect ou Mesh), a infraestrutura da WLAN pode transferir e manipular as chaves de maneira diferente. Ele pode até mudar as funções dos detentores de chaves, mas como isso está fora do escopo deste documento, os exemplos baseados no resumo da hierarquia de chaves fornecido anteriormente são o próximo foco. Na verdade, as diferenças não são relevantes para entender o processo, a menos que você precise analisar os dispositivos de infraestrutura (e seu código) para descobrir um problema de software.

Transição rápida de BSS pelo ar

Com esse método, a primeira associação a qualquer AP é uma autenticação de primeira vez regular para a WLAN, onde toda a autenticação 802.1X/EAP contra o Servidor de Autenticação e o handshake de 4 vias para geração de chave deve ocorrer antes que os quadros de dados sejam enviados, como mostrado nesta imagem da tela:



As principais diferenças são:

- A negociação do gerenciamento de chave de autenticação é ligeiramente diferente da WPA/WPA2 normal, portanto, algumas informações adicionais são usadas para executar essa negociação quando ocorre a associação a uma infraestrutura de WLAN que suporta a FT. Como mostrado na imagem, o quadro Solicitação de associação do cliente é selecionado e o campo AKM do Elemento de informação RNS é realçado para mostrar que esse cliente deseja executar FT sobre 802.1X/EAP.
- Também é mostrado o Mobility Domain Information Element (parte do FT), onde o campo **FT Capability and Policy** indica se a transição do Fast BSS foi concluída pelo ar ou pelo DS quando o roaming rápido (isso indica Over-the-Air nesta imagem).
- Outro elemento de informação também é adicionado (Transição rápida de BSS ou FT IE, que é descrito mais adiante neste documento) com a informação que é necessária para executar a sequência de autenticação FT quando FT roaming.
- A geração de chave é diferente devido à hierarquia de chave, portanto, mesmo que o handshake de 4 vias FT pareça semelhante ao handshake de 4 vias WPA/WPA2, ele é, na verdade, ligeiramente diferente em conteúdo.

As depurações mostram basicamente a mesma troca de quadros de autenticação EAP que o resto dos métodos na autenticação inicial para a WLAN (como observado nas imagens), mas algumas saídas que dizem respeito às técnicas de cache de chave usadas pela WLC são adicionadas; assim, essa saída de depuração é cortada para mostrar apenas as informações relevantes:

```
*apfMsConnTask_0: Jun 27 19:25:23.426: ec:85:2f:15:39:32
```

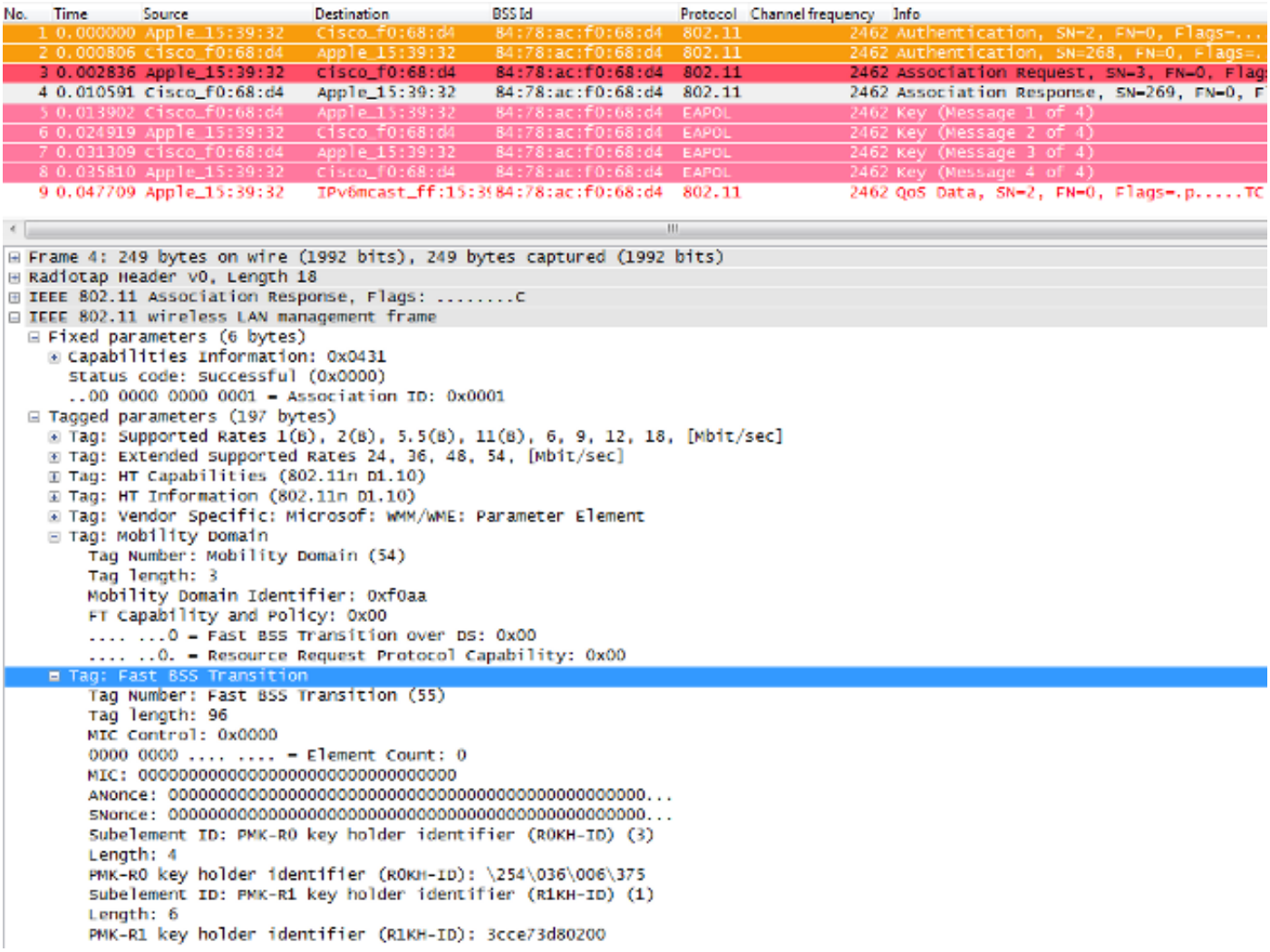
```
  Association received from mobile on BSSID
  84:78:ac:f0:68:d6
!--- This is the Association request from the client.

*apfMsConnTask_0: Jun 27 19:25:23.427: ec:85:2f:15:39:32
  Marking this mobile as TGr capable.
!--- WLC recognizes that the client is 802.11r-capable.

*apfMsConnTask_0: Jun 27 19:25:23.427: ec:85:2f:15:39:32
  Processing RSN IE type 48, length 20 for mobile
  ec:85:2f:15:39:32
!--- The WLC/AP finds an Information Element that claims FT
     support on the Association request that is sent from the client.

*apfMsConnTask_0: Jun 27 19:25:23.427:
  Sending assoc-resp station:ec:85:2f:15:39:32
  AP:84:78:ac:f0:68:d0-00 thread:144be808
*apfMsConnTask_0: Jun 27 19:25:23.427:
  Adding MDIE, ID is:0xaaf0
*apfMsConnTask_0: Jun 27 19:25:23.427: ec:85:2f:15:39:32
  Including FT Mobility Domain IE (length 5) in Initial
  assoc Resp to mobile
*apfMsConnTask_0: Jun 27 19:25:23.427: ec:85:2f:15:39:32
  Sending R0KH-ID as:-84.30.6.-3
*apfMsConnTask_0: Jun 27 19:25:23.427: ec:85:2f:15:39:32
  Sending R1KH-ID as 3c:ce:73:d8:02:00
*apfMsConnTask_0: Jun 27 19:25:23.427: ec:85:2f:15:39:32
  Including FT IE (length 98) in Initial Assoc Resp to mobile
*apfMsConnTask_0: Jun 27 19:25:23.427: ec:85:2f:15:39:32
  Sending Assoc Response to station on BSSID 84:78:ac:f0:68:d6
  (status 0) ApVapId 7 Slot 0
!--- The Association Response is sent to the client once the
     FT information is computed (as per the previous messages),
     so this is included in the response.

*dot1xMsgTask: Jun 27 19:25:23.432: ec:85:2f:15:39:32
  Sending EAP-Request/Identity to mobile ec:85:2f:15:39:32
  (EAP Id 1)
!--- EAP begins, and follows the same exchange explained so far.

*apfMsConnTask_0: Jun 27 19:25:23.436: ec:85:2f:15:39:32
  Got action frame from this client.

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.449: ec:85:2f:15:39:32
  Received EAPOL EAPPKT from mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.449: ec:85:2f:15:39:32
  Received Identity Response (count=1) from mobile
  ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.456: ec:85:2f:15:39:32
  Processing Access-Challenge for mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.456: ec:85:2f:15:39:32
  Sending EAP Request from AAA to mobile ec:85:2f:15:39:32
  (EAP Id 2)

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.479: ec:85:2f:15:39:32
  Received EAPOL EAPPKT from mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.479: ec:85:2f:15:39:32
  Received EAP Response from mobile ec:85:2f:15:39:32
  (EAP Id 2, EAP Type 25)
```

```
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.627: ec:85:2f:15:39:32
  Processing Access-Accept for mobile ec:85:2f:15:39:32
!--- The client is validated/authenticated by the RADIUS Server.

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.627: ec:85:2f:15:39:32
  Creating a PKC PMKID Cache entry for station
  ec:85:2f:15:39:32 (RSN 2)
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.627: ec:85:2f:15:39:32
  Resetting MSCB PMK Cache Entry 0 for station
  ec:85:2f:15:39:32
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.627: ec:85:2f:15:39:32
  Setting active key cache index 8 ---> 8
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.628: ec:85:2f:15:39:32
  Setting active key cache index 8 ---> 0
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.628: ec:85:2f:15:39:32
  Adding BSSID 84:78:ac:f0:68:d6 to PMKID cache at index 0
  for station ec:85:2f:15:39:32
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.628: New PMKID: (16)
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.628:
  [0000] 52 b8 8f cf 50 a7 90 98 2b ba d6 20 79 e4 cd f9
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.629: ec:85:2f:15:39:32
  Created PMK Cache Entry for TGr AKM:802.1x ec:85:2f:15:39:32
!--- WLC creates a PMK cache entry for this client, which is
     used for FT with 802.1X in this case, so the PMKID is
     computed with the AP MAC address (BSSID 84:78:ac:f0:68:d6).

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.629:
  ec:85:2f:15:39:32   R0KH-ID:172.30.6.253
  R1KH-ID:3c:ce:73:d8:02:00  MSK Len:48 pmkValidTime:1807
!--- The R0KH-ID and R1KH-ID are defined, as well as the PMK
     cache validity period.

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.630: ec:85:2f:15:39:32
  PMK sent to mobility group
!--- The FT PMK cache entry for this client is shared with the
     WLCs on the mobility group.

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.630: ec:85:2f:15:39:32
  Sending EAP-Success to mobile ec:85:2f:15:39:32 (EAP Id 12)

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.630: ec:85:2f:15:39:32
  Found an cache entry for BSSID 84:78:ac:f0:68:d6 in PMKID
  cache at index 0 of station ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.630: Including PMKID in
  M1  (16)
!--- The hashed PMKID is included on the Message-1 of the
     initial FT 4-Way handshake.

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.630:
  [0000] 52 b8 8f cf 50 a7 90 98 2b ba d6 20 79 e4 cd f9

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.630: ec:85:2f:15:39:32
  Sending EAPOL-Key Message to mobile ec:85:2f:15:39:32 state
  INITPMK (message 1), replay counter 00.00.00.00.00.00.00.0
!--- Message-1 of the FT 4-Way handshake is sent from the
     WLC/AP to the client.

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.639: ec:85:2f:15:39:32
  Received EAPOL-Key from mobile ec:85:2f:15:39:32
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.639: ec:85:2f:15:39:32
  Received EAPOL-key in PTK_START state (message 2) from
  mobile ec:85:2f:15:39:32
!--- Message-2 of the FT 4-Way handshake is received
```

```
     successfully from the client.

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.639: ec:85:2f:15:39:32
  Calculating PMKR0Name
!--- The PMKR0Name is calculated.

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.639: ec:85:2f:15:39:32
  DOT11R: Sending cache add

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.639: Adding MDIE,
  ID is:0xaaf0
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.639: ec:85:2f:15:39:32
  Adding TIE for reassociation deadtime:20000 milliseconds
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.639: ec:85:2f:15:39:32
  Adding TIE for R0Key-Data valid time :1807
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.640: ec:85:2f:15:39:32
  Sending EAPOL-Key Message to mobile ec:85:2f:15:39:32 state
  PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01
!--- After the MDIE, TIE for reassociation deadtime, and TIE
     for R0Key-Data valid time are calculated, the Message-3
     of this FT 4-Way handshake is sent from the WLC/AP to the
     client with this information.

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.651: ec:85:2f:15:39:32
  Received EAPOL-Key from mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.651: ec:85:2f:15:39:32
  Received EAPOL-key in PTKINITNEGOTIATING state (message 4)
  from mobile ec:85:2f:15:39:32
!--- Message-4 (final message) of this initial FT 4-Way handshake
     is received successfully from the client, which confirms the
     installation of the derived keys. They can now be used in order
     to encrypt data frames with the current AP.
```

Observação: para depurar esse método e atingir as saídas 802.11r/FT extras mostradas aqui, uma depuração adicional é habilitada junto com o cliente de depuração, que é o debug ft events enable.

Aqui estão as imagens e depurações de uma associação inicial à WLAN quando você executa FT com WPA2-PSK (em vez de um método 802.1X/EAP), onde o quadro Resposta de associação do AP é selecionado para mostrar o Elemento de informação de transição BSS rápido (realçado). Algumas das principais informações necessárias para executar o handshake de 4 vias da FT também são mostradas:



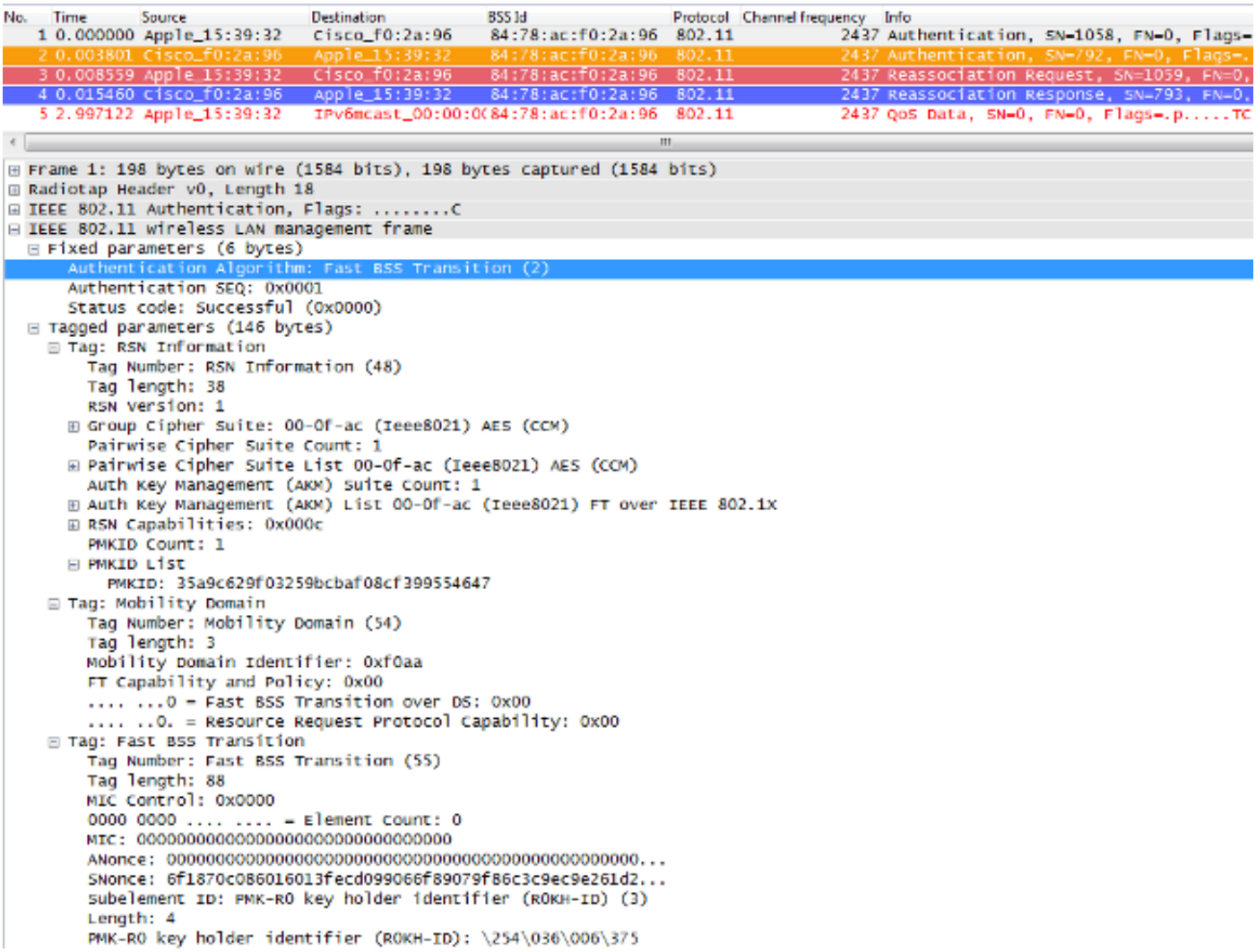

```
*apfMsConnTask_0: Jun 27 19:29:09.136: ec:85:2f:15:39:32
  Association received from mobile on BSSID
  84:78:ac:f0:68:d4

*apfMsConnTask_0: Jun 27 19:29:09.137: ec:85:2f:15:39:32
  Marking this mobile as TGr capable.

*apfMsConnTask_0: Jun 27 19:29:09.137: ec:85:2f:15:39:32
  Processing RSN IE type 48, length 20 for mobile
  ec:85:2f:15:39:32

*apfMsConnTask_0: Jun 27 19:29:09.137: Sending assoc-resp
  station:ec:85:2f:15:39:32 AP:84:78:ac:f0:68:d0-00
  thread:144be808

*apfMsConnTask_0: Jun 27 19:29:09.137: Adding MDIE,
  ID is:0xaaf0

*apfMsConnTask_0: Jun 27 19:29:09.137: ec:85:2f:15:39:32
  Including FT Mobility Domain IE (length 5) in Initial
  assoc Resp to mobile

*apfMsConnTask_0: Jun 27 19:29:09.137: ec:85:2f:15:39:32
  Sending R0KH-ID as:-84.30.6.-3

*apfMsConnTask_0: Jun 27 19:29:09.137: ec:85:2f:15:39:32
  Sending R1KH-ID as 3c:ce:73:d8:02:00

*apfMsConnTask_0: Jun 27 19:29:09.137: ec:85:2f:15:39:32
```

```
  Including FT IE (length 98) in Initial Assoc Resp to mobile

*apfMsConnTask_0: Jun 27 19:29:09.138: ec:85:2f:15:39:32
  Sending Assoc Response to station on BSSID 84:78:ac:f0:68:d4
  (status 0) ApVapId 5 Slot 0

*dot1xMsgTask: Jun 27 19:29:09.141: ec:85:2f:15:39:32
  Creating a PKC PMKID Cache entry for station
  ec:85:2f:15:39:32 (RSN 2)

*dot1xMsgTask: Jun 27 19:29:09.141: ec:85:2f:15:39:32
  Resetting MSCB PMK Cache Entry 0 for station
  ec:85:2f:15:39:32

*dot1xMsgTask: Jun 27 19:29:09.141: ec:85:2f:15:39:32
  Setting active key cache index 8 ---> 8

*dot1xMsgTask: Jun 27 19:29:09.141: ec:85:2f:15:39:32
  Setting active key cache index 8 ---> 0

*dot1xMsgTask: Jun 27 19:29:09.141: ec:85:2f:15:39:32
  Adding BSSID 84:78:ac:f0:68:d4 to PMKID cache at
  index 0 for station ec:85:2f:15:39:32

*dot1xMsgTask: Jun 27 19:29:09.142: New PMKID: (16)

*dot1xMsgTask: Jun 27 19:29:09.142:
  [0000] 17 4b 17 5c ed 5f c7 1d 66 39 e9 5d 3a 63 69 e7

*dot1xMsgTask: Jun 27 19:29:09.142: ec:85:2f:15:39:32
  Creating global PMK cache for this TGr client

*dot1xMsgTask: Jun 27 19:29:09.142: ec:85:2f:15:39:32
  Created PMK Cache Entry for TGr AKM:PSK
  ec:85:2f:15:39:32

*dot1xMsgTask: Jun 27 19:29:09.142: ec:85:2f:15:39:32
  R0KH-ID:172.30.6.253   R1KH-ID:3c:ce:73:d8:02:00
  MSK Len:48 pmkValidTime:1813

*dot1xMsgTask: Jun 27 19:29:09.142: ec:85:2f:15:39:32
  Initiating RSN PSK to mobile ec:85:2f:15:39:32

*dot1xMsgTask: Jun 27 19:29:09.142: ec:85:2f:15:39:32
  Found an cache entry for BSSID 84:78:ac:f0:68:d4 in
  PMKID cache at index 0 of station ec:85:2f:15:39:32

*dot1xMsgTask: Jun 27 19:29:09.142: Including PMKID
  in M1  (16)

*dot1xMsgTask: Jun 27 19:29:09.142:
  [0000] 17 4b 17 5c ed 5f c7 1d 66 39 e9 5d 3a 63 69 e7

*dot1xMsgTask: Jun 27 19:29:09.143: ec:85:2f:15:39:32
  Sending EAPOL-Key Message to mobile ec:85:2f:15:39:32
  state INITPMK (message 1), replay counter
  00.00.00.00.00.00.00.00

*apfMsConnTask_0: Jun 27 19:29:09.144: ec:85:2f:15:39:32
  Got action frame from this client.

*Dot1x_NW_MsgTask_2: Jun 27 19:29:09.152: ec:85:2f:15:39:32
  Received EAPOL-Key from mobile ec:85:2f:15:39:32
```

```
*Dot1x_NW_MsgTask_2: Jun 27 19:29:09.153: ec:85:2f:15:39:32
  Received EAPOL-key in PTK_START state (message 2) from
  mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 27 19:29:09.153: ec:85:2f:15:39:32
  Calculating PMKR0Name

*Dot1x_NW_MsgTask_2: Jun 27 19:29:09.153: Adding MDIE,
  ID is:0xaaf0

*Dot1x_NW_MsgTask_2: Jun 27 19:29:09.153: ec:85:2f:15:39:32
  Adding TIE for reassociation deadtime:20000 milliseconds

*Dot1x_NW_MsgTask_2: Jun 27 19:29:09.153: ec:85:2f:15:39:32
  Adding TIE for R0Key-Data valid time :1813

*Dot1x_NW_MsgTask_2: Jun 27 19:29:09.154: ec:85:2f:15:39:32
  Sending EAPOL-Key Message to mobile ec:85:2f:15:39:32 state
  PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01

*Dot1x_NW_MsgTask_2: Jun 27 19:29:09.163: ec:85:2f:15:39:32
  Received EAPOL-Key from mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 27 19:29:09.163: ec:85:2f:15:39:32
  Received EAPOL-key in PTKINITNEGOTIATING state (message 4)
  from mobile ec:85:2f:15:39:32
```

Com o 802.11r, a associação inicial à WLAN é a base usada para derivar as chaves base usadas por essa técnica, assim como nos outros métodos de roaming rápido e seguro. As principais diferenças ocorrem quando o cliente começa a fazer roaming; a FT não apenas evita 802.1X/EAP quando isso é usado, mas na verdade executa um método de roaming mais eficiente que combina os quadros iniciais 802.11 Open System Authentication e Reassociation (que são sempre usados e exigidos quando em roaming entre APs) para trocar informações de FT e derivar novas chaves de criptografia dinâmicas no lugar do handshake de 4 vias.

A imagem a seguir mostra os quadros trocados quando uma transição via satélite Fast BSS com segurança 802.1X/EAP é executada. O quadro Open System Authentication do cliente para o AP é selecionado para ver os elementos de informação do protocolo FT que são necessários para iniciar a negociação de chave FT. Isso é usado para derivar o novo PTK com o novo AP (com base no PMK-R1). O campo que mostra o algoritmo de autenticação é destacado para mostrar que este cliente não executa uma Autenticação de Sistema Aberto simples, mas uma Transição BSS Rápida:

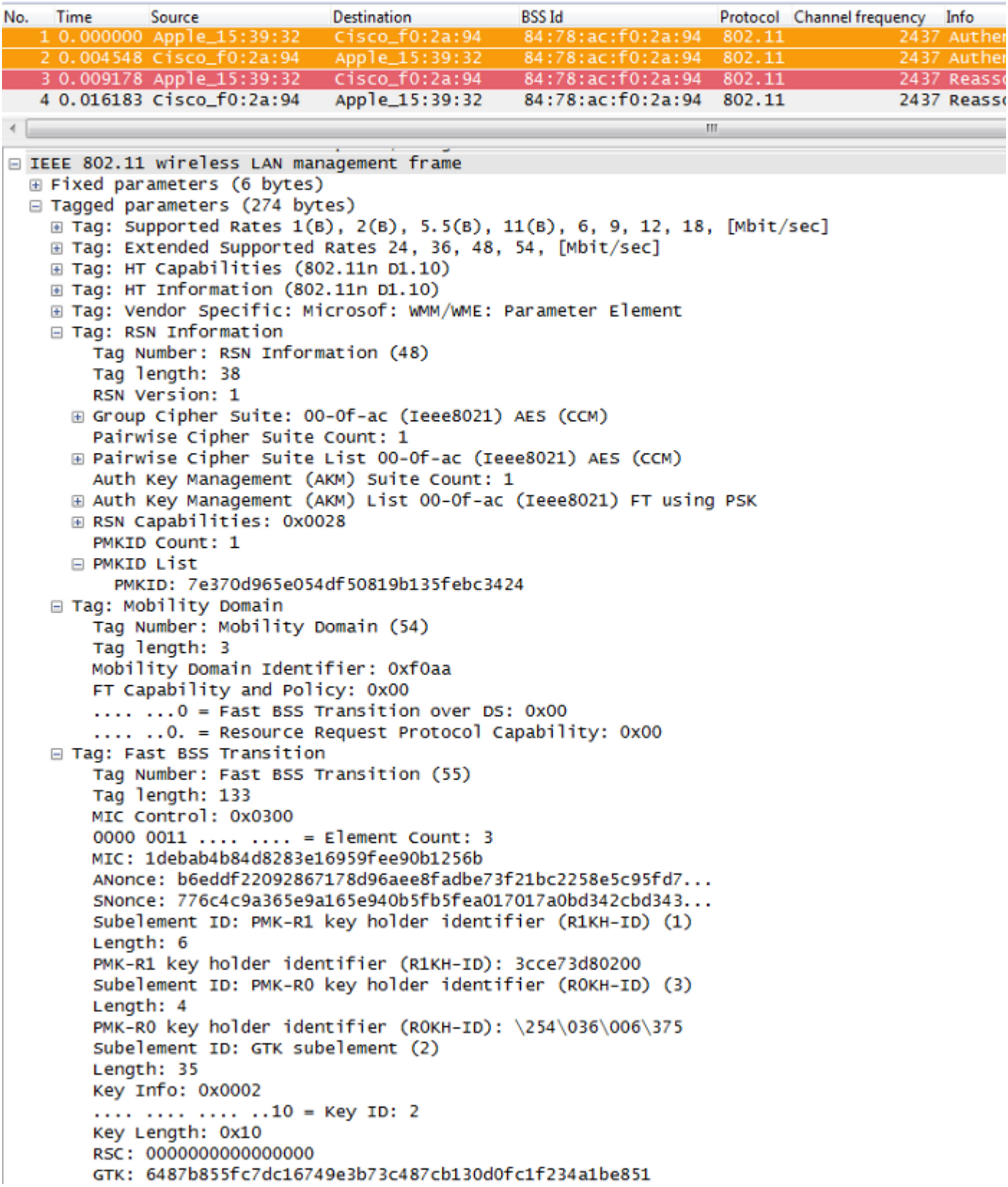


Estas são as saídas de depuração do WLC quando este evento de roaming FT ocorre com 802.1X/EAP:

```
*apfMsConnTask_2: Jun 27 19:25:48.751: ec:85:2f:15:39:32
  Doing preauth for this client over the Air
!--- WLC begins FT fast-secure roaming over-the-Air with
      this client and performs a type of preauthentication,
      because the client asks for this with FT on the Authentication
      frame that is sent to the new AP over-the-Air
      (before the Reassociation Request).

*apfMsConnTask_2: Jun 27 19:25:48.751: ec:85:2f:15:39:32
  Doing local roaming for destination address
  84:78:ac:f0:2a:96
!--- WLC performs the local roaming event with the new AP to
      which the client roams.

*apfMsConnTask_2: Jun 27 19:25:48.751: ec:85:2f:15:39:32
  Got 1 AKMs in RSNIE
*apfMsConnTask_2: Jun 27 19:25:48.751: ec:85:2f:15:39:32
  RSNIE AKM matches with PMK cache entry :0x3
!--- WLC receives one PMK from this client (known as AKM here),
      which matches the PMK cache entry hold for this client.

*apfMsConnTask_2: Jun 27 19:25:48.751: ec:85:2f:15:39:32
  Created a new preauth entry for AP:84:78:ac:f0:2a:96
*apfMsConnTask_2: Jun 27 19:25:48.751: Adding MDIE,
  ID is:0xaaf0
```

```
!--- WLC creates a new preauth entry for this AP-and-Client pair,
      and adds the MDIE information.

*apfMsConnTask_2: Jun 27 19:25:48.763: Processing assoc-req
  station:ec:85:2f:15:39:32 AP:84:78:ac:f0:2a:90-00
  thread:144bef38
*apfMsConnTask_2: Jun 27 19:25:48.763: ec:85:2f:15:39:32
  Reassociation received from mobile on BSSID
  84:78:ac:f0:2a:96
!--- Once the client receives the Authentication frame reply from the
      WLC/AP, the Reassociation request is sent, which is received at
      the new AP to which the client roams.

*apfMsConnTask_2: Jun 27 19:25:48.764: ec:85:2f:15:39:32
  Marking this mobile as TGr capable.

*apfMsConnTask_2: Jun 27 19:25:48.764: ec:85:2f:15:39:32
  Processing RSN IE type 48, length 38 for mobile
  ec:85:2f:15:39:32

*apfMsConnTask_2: Jun 27 19:25:48.765: ec:85:2f:15:39:32
  Roaming succeed for this client.
!--- WLC confirms that the FT fast-secure roaming is successful
      for this client.

*apfMsConnTask_2: Jun 27 19:25:48.765: Sending assoc-resp
  station:ec:85:2f:15:39:32 AP:84:78:ac:f0:2a:90-00
  thread:144bef38
*apfMsConnTask_2: Jun 27 19:25:48.766: Adding MDIE,
  ID is:0xaaf0
*apfMsConnTask_2: Jun 27 19:25:48.766: ec:85:2f:15:39:32
  Including FT Mobility Domain IE (length 5) in
  reassociation assoc Resp to mobile
*apfMsConnTask_2: Jun 27 19:25:48.766: ec:85:2f:15:39:32
  Sending Assoc Response to station on BSSID 84:78:ac:f0:2a:96
  (status 0) ApVapId 7 Slot 0
!--- The Reassociation response is sent to the client, which
      includes the FT Mobility Domain IE.

*dot1xMsgTask: Jun 27 19:25:48.769: ec:85:2f:15:39:32
  Finishing FT roaming for mobile ec:85:2f:15:39:32
!--- FT roaming finishes and EAP is skipped (as well as any
      other key management handshake), so the client is ready
      to pass encrypted data frames with the current AP.

*dot1xMsgTask: Jun 27 19:25:48.769: ec:85:2f:15:39:32
  Skipping EAP-Success to mobile ec:85:2f:15:39:32
```

Esta é uma imagem que mostra uma transição via satélite Fast BSS com segurança WPA2-PSK, onde o quadro de resposta de reassociação final do AP para o cliente é selecionado para mostrar mais detalhes sobre esta troca de FT:



Estas são as saídas de depuração quando este evento de roaming FT ocorre com PSK, que são semelhantes àquelas quando 802.1X/EAP é usado:

```
*apfMsConnTask_2: Jun 27 19:29:29.854: ec:85:2f:15:39:32
  Doing preauth for this client over the Air

*apfMsConnTask_2: Jun 27 19:29:29.854: ec:85:2f:15:39:32
  Doing local roaming for destination address
```

```
  84:78:ac:f0:2a:94

*apfMsConnTask_2: Jun 27 19:29:29.854: ec:85:2f:15:39:32
  Got 1 AKMs in RSNIE

*apfMsConnTask_2: Jun 27 19:29:29.854: ec:85:2f:15:39:32
  RSNIE AKM matches with PMK cache entry :0x4

*apfMsConnTask_2: Jun 27 19:29:29.854: ec:85:2f:15:39:32
  Created a new preauth entry for AP:84:78:ac:f0:2a:94

*apfMsConnTask_2: Jun 27 19:29:29.854: Adding MDIE,
  ID is:0xaaf0

*apfMsConnTask_2: Jun 27 19:29:29.867: Processing assoc-req
  station:ec:85:2f:15:39:32 AP:84:78:ac:f0:2a:90-00
  thread:144bef38

*apfMsConnTask_2: Jun 27 19:29:29.867: ec:85:2f:15:39:32
  Reassociation received from mobile on BSSID
  84:78:ac:f0:2a:94

*apfMsConnTask_2: Jun 27 19:29:29.868: ec:85:2f:15:39:32
  Marking this mobile as TGr capable.

*apfMsConnTask_2: Jun 27 19:29:29.868: ec:85:2f:15:39:32
  Processing RSN IE type 48, length 38 for mobile
  ec:85:2f:15:39:32

*apfMsConnTask_2: Jun 27 19:29:29.869: ec:85:2f:15:39:32
  Roaming succeed for this client.

*apfMsConnTask_2: Jun 27 19:29:29.869: Sending assoc-resp
  station:ec:85:2f:15:39:32 AP:84:78:ac:f0:2a:90-00
  thread:144bef38

*apfMsConnTask_2: Jun 27 19:29:29.869: Adding MDIE,
  ID is:0xaaf0

*apfMsConnTask_2: Jun 27 19:29:29.869: ec:85:2f:15:39:32
  Including FT Mobility Domain IE (length 5) in
  reassociation assoc Resp to mobile

*apfMsConnTask_2: Jun 27 19:29:29.870: ec:85:2f:15:39:32
  Sending Assoc Response to station on BSSID
  84:78:ac:f0:2a:94 (status 0) ApVapId 5 Slot 0

*dot1xMsgTask: Jun 27 19:29:29.874: ec:85:2f:15:39:32
  Finishing FT roaming for mobile ec:85:2f:15:39:32
```

Como mostrado na imagem, uma vez que a transição rápida de BSS é negociada na associação inicial à WLAN, os quatro quadros que são usados e necessários para roaming (Autenticação de sistema aberto do cliente, Autenticação de sistema aberto do AP, Solicitação de reassociação e Resposta de reassociação) são basicamente usados como um handshake de 4 vias FT para derivar o novo PTK (chave de criptografia unicast) e GTK (chave de criptografia multicast/broadcast).

Isso substitui o handshake de 4 vias que normalmente ocorre depois que esses quadros são trocados, e o conteúdo de FT e a negociação de chave nesses quadros é basicamente o mesmo se você usar 802.1X/EAP ou PSK como o método de segurança. Como mostrado na imagem, o campo AKM é a principal diferença, que confirma se o cliente executa FT com PSK ou 802.1X. Portanto, é importante observar que esses quatro quadros normalmente não têm esse tipo de

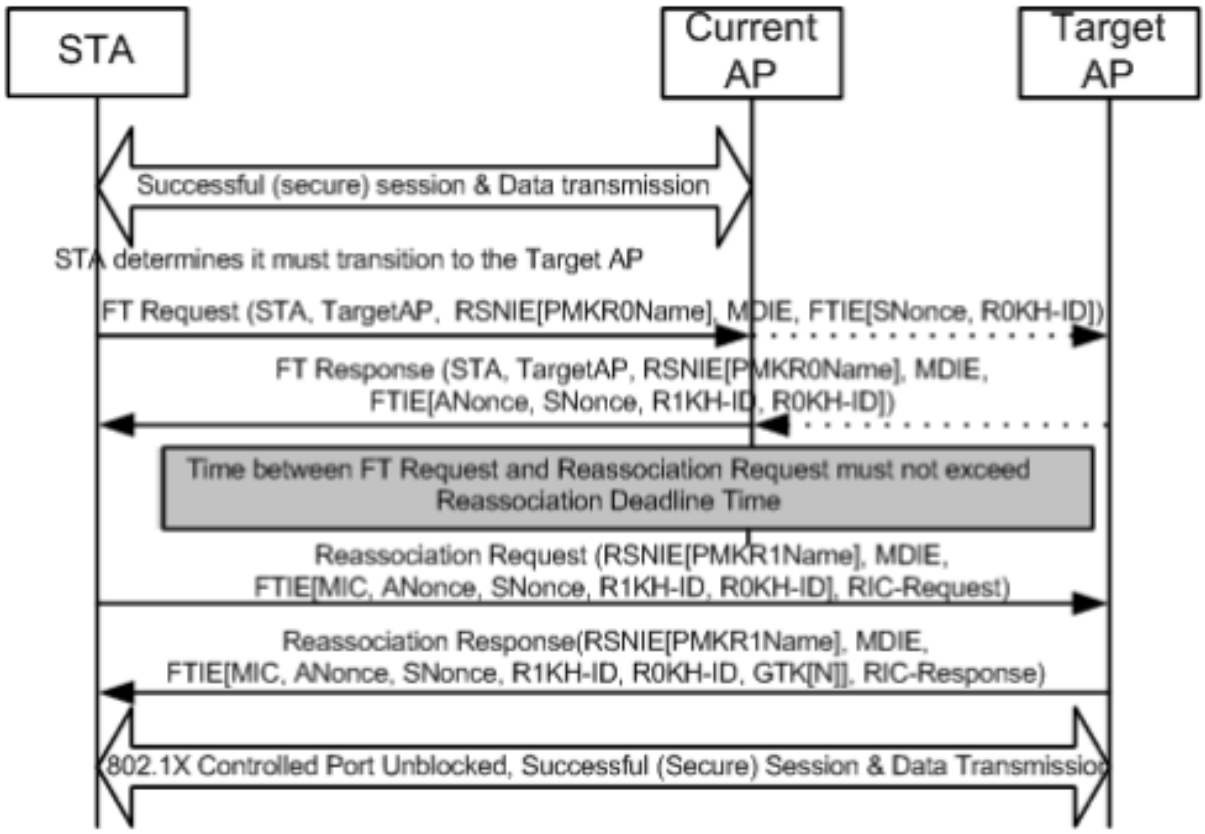
informação de segurança para a negociação principal, mas somente quando a FT do cliente faz roaming se 802.11r for implementado e negociado entre o cliente e a infraestrutura da WLAN na associação inicial.

Transição rápida de BSS pelo DS

O 802.11r permite outra implementação da Transição rápida de BSS, onde o roaming de FT é iniciado pelo cliente com o novo AP para o qual o cliente faz roaming pelo DS (Sistema de distribuição), e não pelo ar. Nesse caso, os quadros de ação FT são usados para iniciar a negociação de chave em vez dos quadros de autenticação de sistema aberto.

Basicamente, uma vez que o cliente decide que pode fazer roaming para um AP melhor, ele envia um quadro de solicitação de ação FT para o AP original, onde ele está conectado atualmente antes do roaming. O cliente indica o BSSID (endereço MAC) do AP de destino onde deseja fazer roaming de FT. O AP original encaminha esse quadro de solicitação de ação FT para o AP de destino pelo sistema de distribuição (normalmente a infraestrutura com fio) e o AP de destino responde ao cliente com um quadro de resposta de ação FT (também pelo DS, para que ele possa finalmente enviá-lo pelo ar ao cliente). Uma vez que esta troca de quadro de Ação FT é bem-sucedida, o cliente termina o roaming FT; o cliente envia a Solicitação de Reassociação para o AP de destino (desta vez no ar), e recebe uma Resposta de Reassociação do novo AP para confirmar o roaming e a derivação final das chaves.

Em resumo, há quatro quadros para negociar a transição rápida de BSS e derivar novas chaves de criptografia, mas aqui os quadros de autenticação de sistema aberto são substituídos pelos quadros de solicitação/resposta de ação de FT, que são trocados com o AP de destino pelo sistema de distribuição com o AP atual. Este método também é válido para os métodos de segurança 802.1X/EAP e PSK, todos suportados pelos Cisco Wireless LAN Controllers; no entanto, como essa transição Over-the-DS não é suportada e implementada pela maioria dos clientes sem fio no setor de WiFi (e como a troca de quadros e as saídas de depuração são basicamente as mesmas), exemplos não são fornecidos neste documento. Em vez disso, esta imagem é usada para visualizar a Transição rápida de BSS pelo DS:



FlexConnect com 802.11r

- Há suporte para a Autenticação Central. Isso inclui switching de dados local e central. Os APs devem fazer parte do mesmo grupo FlexConnect.
- Não há suporte para Autenticação Local.
- Não há suporte para o modo autônomo.

Prós com 802.11r

- Este método é o primeiro que usa uma hierarquia-chave claramente definida pelo IEEE no padrão 802.11 como uma emenda (802.11r), de modo que a implementação dessas técnicas FT são mais compatíveis entre os fornecedores e sem interpretações diferentes.
- O 802.11r permite várias técnicas úteis, dependendo das suas necessidades (Over-the-Air e Over-the-DS, para segurança 802.1x/EAP e para segurança PSK).
- O cliente sem fio executa roaming rápido e seguro para um novo AP na mesma WLAN/SSID, mesmo que nunca esteja associado a esse AP, e sem a necessidade de salvar vários PMKIDs.
- Esse é o primeiro método de roaming rápido que permite roaming mais rápido, mesmo com a segurança PSK, e evita o handshake de 4 vias necessário ao roaming entre APs com WPA/WPA2 PSK. O principal objetivo dos métodos de roaming rápido e seguro é evitar o handshake 802.1X/EAP quando esse método de segurança é implementado; no entanto, para a segurança PSK, o evento de roaming é acelerado ainda mais com o 802.11r quando o handshake de 4 vias é evitado.

Contras com 802.11r

- Há alguns dispositivos de cliente sem fio que realmente suportam as transições rápidas de BSS e, na maioria dos casos, eles não suportam todas as técnicas disponíveis no 802.11r.
- Devido ao fato de que essas implementações são muito novas, não há resultados de teste suficientes em ambientes de produção real ou resultados de depuração suficientes para lidar com possíveis advertências que podem aparecer.
- Quando você configura uma WLAN/SSID para usar qualquer um dos métodos FT, somente os clientes sem fio que suportam 802.11r podem se conectar a essa WLAN/SSID. As configurações de FT não são opcionais para os clientes, de modo que os clientes sem fio que não suportam 802.11r devem se conectar com uma WLAN/SSID separada onde FT não está configurada de forma alguma.

Adaptável 802.11r

- Alguns clientes antigos não podem se associar a uma WLAN/SSID que tenha 802.11r ativado, mesmo para o "modo misto" (que você espera que possa ter nos mesmos clientes SSID que suportam e que não suportam 802.11r). Isso ocorre quando o driver do solicitante cliente que é responsável pela análise do Elemento de Informações de Rede de Segurança Robusta (RSN IE) é antigo e não conhece os conjuntos AKM adicionais no IE. Devido a essa limitação, os clientes não podem enviar solicitações de associação a WLANs que anunciam suporte a 802.11r e, portanto, você precisa configurar uma WLAN/SSID para clientes 802.11r e uma WLAN/SSID separada para clientes que não suportam 802.11r.
- Para superar isso, a infraestrutura de LAN sem fio da Cisco introduziu o recurso Adaptive 802.11r. Quando o modo FT está definido como Adaptativo no nível da WLAN, a WLAN anuncia o ID do domínio de mobilidade 802.11r em uma WLAN habilitada para 802.11i. Alguns dispositivos clientes Apple iOS10 identificam a presença de MDIE em uma WLAN 80211i/WPA2 e fazem um handshake proprietário para estabelecer a associação com 802.11r. Quando o cliente concluir a associação 802.11r com êxito, ele poderá fazer roaming de FT como em uma WLAN habilitada para 802.11r normal. O Adaptador FT é aplicável somente a dispositivos Apple iOS10 (e posteriores) selecionados. Todos os outros clientes podem continuar a ter associação 802.11i/WPA2 na WLAN e executar o método FSR aplicável conforme suportado.
- Mais documentação sobre este novo recurso introduzido para dispositivos iOS10 para executar 802.11r em uma WLAN/SSID onde 802.11r não é verdadeiramente habilitado (para que outros clientes não 802.11r possam se conectar com êxito), pode ser encontrada em Melhores Práticas Corporativas para Dispositivos IOS Cisco em Cisco Wireless LAN.

Conclusões

- Tenha em mente que o cliente é sempre aquele que decide fazer roaming para um AP específico, e o WLC/AP não pode decidir isso para o cliente. O evento de roaming é iniciado pelo cliente sem fio quando ele considera que deve fazer roaming.
- A WLC suporta uma combinação da maioria ou de todos os métodos FSR (Fast-Secure Roaming) juntos na mesma WLAN/SSID. No entanto, lembre-se de que isso normalmente não funciona, pois depende muito do comportamento do cliente (muito diferente em diferentes dispositivos móveis) para suportar ou mesmo entender o que a WLC tenta anunciar como suportado. Em vez de obter interoperabilidade em apenas um SSID, normalmente há mais problemas do que os que se espera corrigir, portanto isso não é

recomendado. Se isso for realmente necessário, é necessário realizar testes aprofundados com todos os clientes possíveis a serem usados nessa WLAN.

- Émuito importante entender que os métodos de roaming rápido e seguro são desenvolvidos para acelerar o processo de roaming da WLAN quando você se move entre APs se a WLAN/SSID tiver a segurança habilitada. Quando não há segurança, não há nada para acelerar, pois o AP cliente simplesmente troca os quadros de gerenciamento sem fio que são sempre exigidos quando em roaming entre APs antes que os quadros de dados sejam enviados (Autenticação de Sistema Aberto do cliente, Autenticação de Sistema Aberto do AP, Solicitação de Reassociação e Resposta de Reassociação). Portanto, isso não pode avançar mais rápido. Se você encontrar problemas de roaming sem segurança, então não há métodos de roaming rápido para melhorar o roaming, apenas métodos para confirmar se a configuração e o design da WLAN/SSID são apropriados para que as estações clientes sem fio façam roaming de acordo entre as células de cobertura do AP.
- O 802.11r/FT é implementado com WPA2-PSK para acelerar eventos de roaming com essa segurança e evitar o handshake de 4 vias, como explicado na seção 802.11r.
- Todos os métodos têm suas vantagens e desvantagens, mas no final, você deve sempre verificar se as estações cliente sem fio suportam o método específico que você deseja implementar e se a infraestrutura de WLAN da Cisco suporta todos os métodos disponíveis. Assim, você deve selecionar o melhor método que é realmente suportado pelos clientes sem fio que se conectam à WLAN/SSID específica. Por exemplo, em algumas implantações, você pode criar uma WLAN/SSID com CCKM para telefones IP sem fio da Cisco (que suportam WPA2/AES com CCKM, mas não 802.11r) e depois outra WLAN/SSID com WPA2/AES via 802.11r/FT para clientes sem fio que suportam esse método de roaming rápido seguro (ou usar OKC, se for o que é suportado).
- Se os clientes sem fio não oferecerem suporte a nenhum dos métodos de roaming rápido-seguro disponíveis, você poderá aceitar o fato de que esses clientes sempre podem experimentar os atrasos explicados neste documento quando em roaming entre APs em uma WLAN/SSID com segurança 802.1X/EAP (o que pode causar interrupções nos aplicativos/serviços do cliente).
- Todos os métodos, exceto SKC (WPA2 PMKID Caching), são suportados para roaming rápido-seguro entre APs gerenciados por WLCs diferentes (roaming intercontrolador), desde que estejam no mesmo grupo de mobilidade.
- O CUWN oferece suporte total a todos os métodos de roaming rápido-seguro cobertos neste artigo quando a autenticação 802.1X/EAP é usada para WPA/WPA2. O CUWN não suporta o roaming rápido e seguro em métodos que funcionam com o WPA2-RSN (CCKM, PMKID Caching/SKC, OKC/PKC) quando o PSK (WPA2-Personal) é usado, onde os métodos de roaming rápido não são necessários. No entanto, o CUWN suporta o roaming rápido e seguro no caso do WPA2-FT (802.11r) com PSK, como também explicado neste artigo.

Informações Relacionadas

- Guia de implantação de transição rápida 802.11r BSS
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.