Configuración de la protección de tramas de administración 802.11w en WLC

Contenido

Introducción

Este documento describe los detalles sobre la protección de trama de administración IEEE 802.11w y su configuración en el Cisco Wireless LAN Controller (WLC).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de Cisco WLC que ejecuta el código 7.6 o posterior.

Componentes Utilizados

La información en este documento se basa en el WLC 5508 que ejecuta el código 7.6.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El estándar 802.11w tiene como objetivo proteger las tramas de control y administración, así como un conjunto de tramas de administración robustas contra ataques de falsificación y reproducción. Los tipos de tramas protegidas incluyen tramas de desasociación, desautenticación y acción robusta como:

- Gestión del espectro
- Quality of Service (QoS)

- Bloquear confirmación
- Medición de radio
- Transición a Fast Basic Service Set (BSS)

802.11w no cifra las tramas; sin embargo, protege las tramas de administración. Garantiza que los mensajes procedan de fuentes legítimas. Para ello, debe agregar un elemento de comprobación de integridad del mensaje (MIC). 802.11w ha introducido una nueva clave llamada Integrity Group Temporal Key (IGTK), que se utiliza para proteger las tramas de administración robustas de difusión/multidifusión. Se deriva como parte del proceso de protocolo de enlace de cuatro vías que se utiliza con el acceso inalámbrico protegido (WPA). Esto hace que dot1x/Pre-Shared Key (PSK) sea un requisito cuando necesite utilizar 802.11w. No se puede utilizar con el identificador del conjunto de servicios (SSID) open/webauth.

Cuando se negocia la protección de tramas de administración, el punto de acceso (AP) cifra los valores GTK e IGTK en la trama EAPOL-Key que se entrega en el mensaje 3 del protocolo de enlace de 4 vías. Si el AP cambia más tarde el GTK, envía el nuevo GTK e IGTK al cliente con el uso del intercambio de señales de clave de grupo. Agrega un MIC que se calcula con el uso de la clave IGTK.

Elemento de información de MIC de administración (MMIE)

802.11w introduce un nuevo elemento de información denominado elemento de información Management MIC. Tiene el formato de encabezado como se muestra en la imagen.

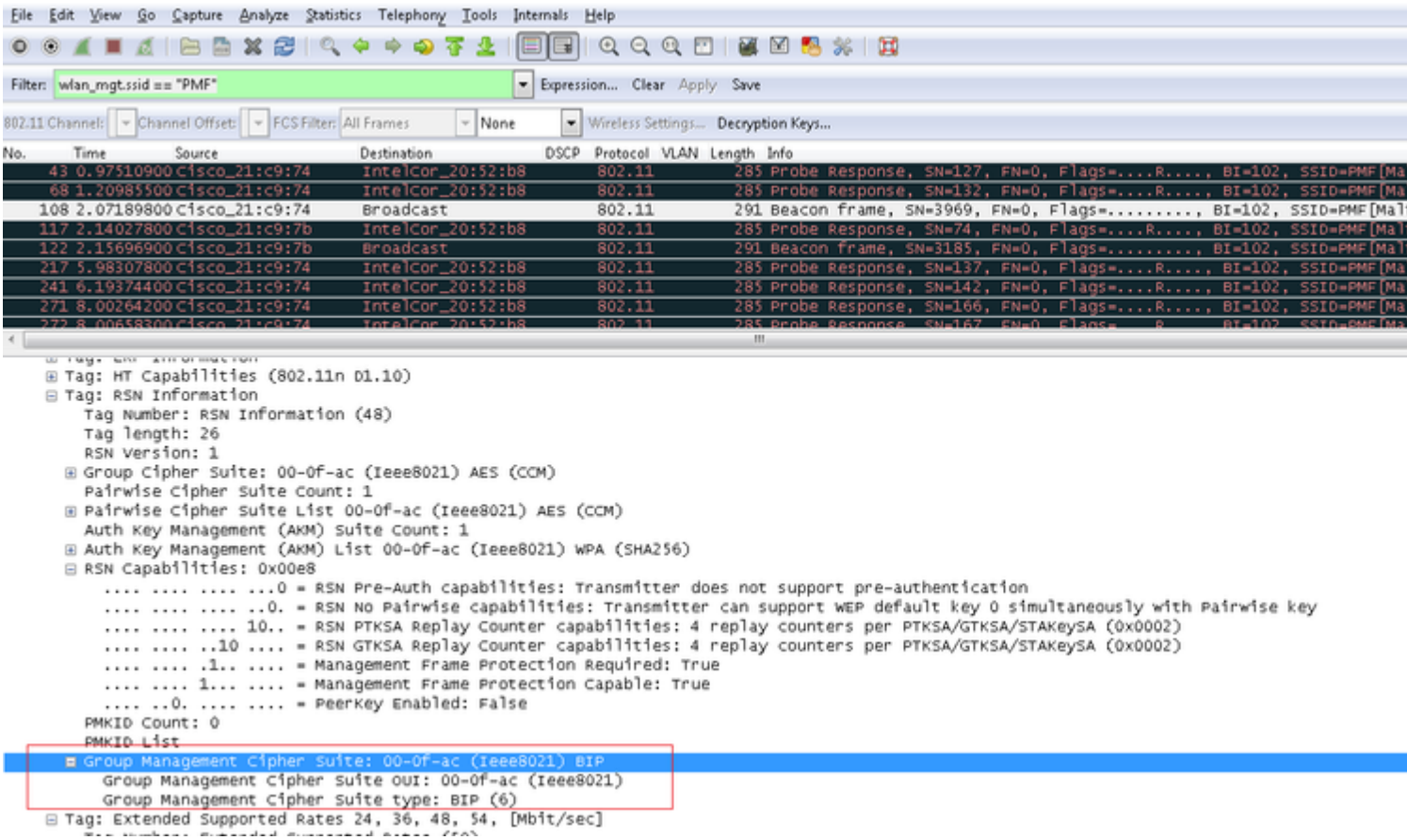
1	1	2	6	8
Element ID	Length	KeyID	IPN	MIC

Los principales campos de interés aquí son **element ID** y **MIC**. El ID de elemento para MMIE es 0x4c y sirve como identificación útil cuando analiza las capturas inalámbricas.

Nota: MIC: contiene el código de integridad del mensaje calculado sobre la trama de administración. Es importante tener en cuenta que esto se agrega en el AP. El cliente de destino luego vuelve a calcular el MIC para la trama y lo compara con lo que fue enviado por el AP. Si los valores son diferentes, se rechaza como una trama no válida.

Cambios en RSN IE

Robust Security Network Information Element (RSN IE) especifica los parámetros de seguridad admitidos por el punto de acceso. 802.11w introduce un selector de conjunto de cifrado de administración de grupo en RSN IE que contiene el selector de conjunto de cifrado utilizado por el AP para proteger tramas de administración robustas de difusión/multidifusión. Esta es la mejor manera de saber si un AP hace 802.11w o no. Esto también se puede verificar como se muestra en la imagen.

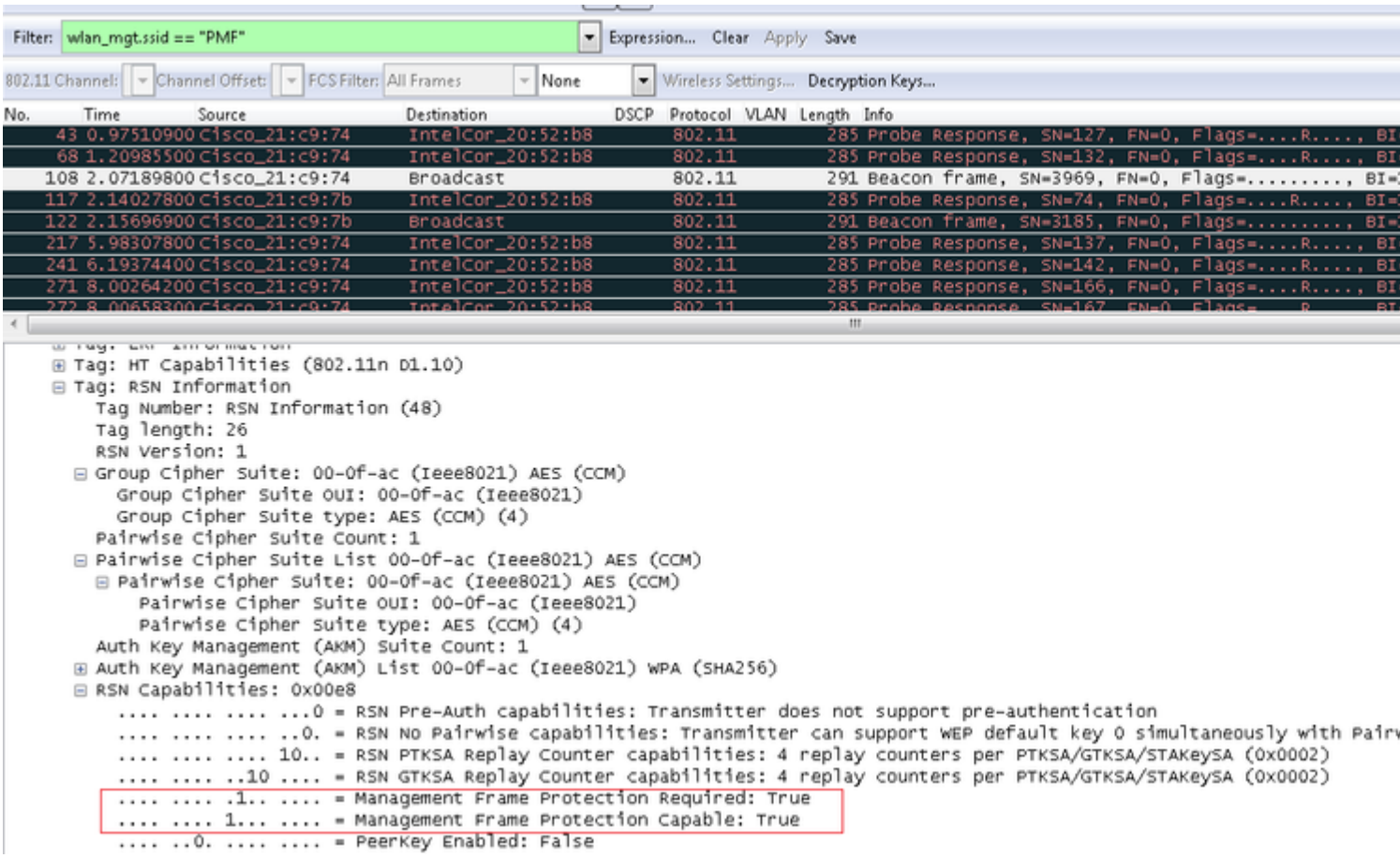


Aquí encontrará el campo **group management cipher suite** que muestra que se utiliza 802.11w.

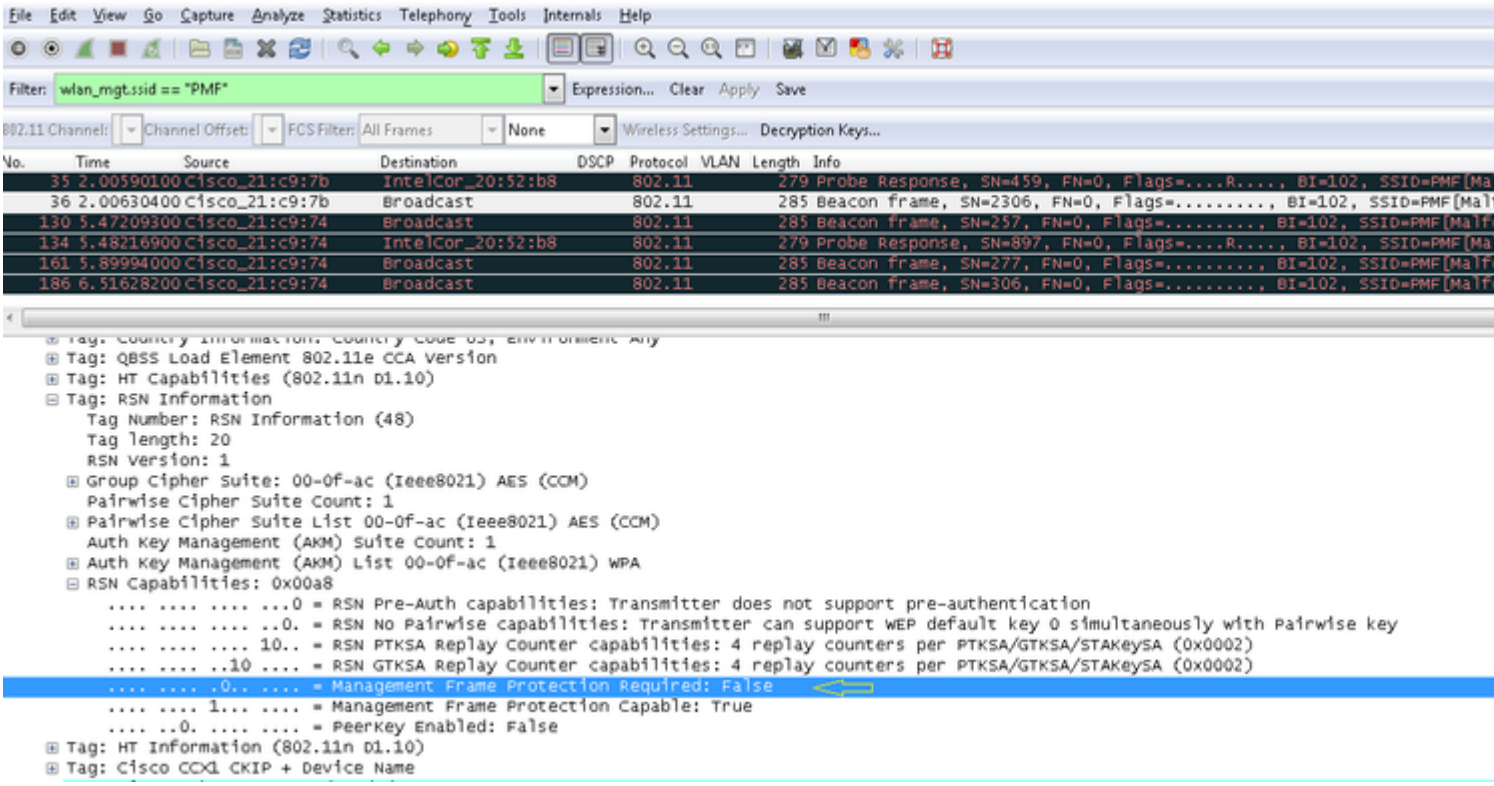
También se realizaron cambios en las capacidades de RSN. Los bits 6 y 7 se utilizan ahora para indicar diferentes parámetros para 802.11w.

- Bit 6: Management Frame Protection Required (MFPR) (Se requiere protección de tramas de administración [MFPR]): una STA establece este bit en 1 para anunciar que la protección de las tramas de administración robustas es obligatoria.
- Bit 7: Capacidad de protección de tramas de administración (MFPC): un STA establece este bit en 1 para anunciar que la protección de tramas de administración robustas está habilitada. Cuando el AP establece esto, informa que soporta la protección de trama de administración.

Si configura la protección de tramas de administración según lo requerido en las opciones de configuración, se configuran los bits 6 y 7. Esto es como se muestra en la imagen de captura de paquetes aquí.



Sin embargo, si establece esto como opcional, sólo se establece el bit 7, como se muestra en la imagen.



Nota: El WLC agrega este IE de RSN modificado en las respuestas de asociación/re-asociación y el AP agrega este IE de RSN modificado en las respuestas de sondeo e indicadores.

Ventajas de la protección de tramas de administración 802.11w

- Protección del cliente

Esto se logra mediante la adición de protección criptográfica a las tramas de desautenticación y desasociación. Esto evita que un usuario no autorizado lance un ataque de denegación de servicio (DOS) mediante la suplantación de la dirección MAC de usuarios legítimos y el envío de tramas de deauth/disassociation.

- Protección de PA

La protección del lado de la infraestructura se añade mediante la adición de un mecanismo de protección de eliminación de asociaciones de seguridad (SA) que consiste en un tiempo de reaparición de la asociación y un procedimiento de consulta SA. Antes de 802.11w, si un AP recibía una solicitud de asociación o autenticación de un cliente ya asociado, el AP termina la conexión actual y luego inicia una nueva conexión. Cuando utiliza la MFP 802.11w, si el STA está asociado y ha negociado la protección de tramas de administración, el AP rechaza la solicitud de asociación con el código de estado de devolución 30 Association request rejected temporarily; Try again later al cliente.

En la respuesta de asociación se incluye un elemento de información del tiempo de reaparición de la asociación que especifica un tiempo de reaparición cuando el AP está listo para aceptar una asociación con este STA. De esta manera, puede asegurarse de que los clientes legítimos no se desasocien debido a una solicitud de asociación simulada.

> **Nota**: El WLC (AireOS o 9800) ignora las tramas de desasociación o desautenticación enviadas por los clientes si no utilizan 802.11w PMF. La entrada de cliente sólo se elimina inmediatamente después de recibir dicha trama si el cliente utiliza PMF. Esto es para evitar la denegación de servicio por parte de dispositivos maliciosos, ya que no hay seguridad en esas tramas sin PMF.

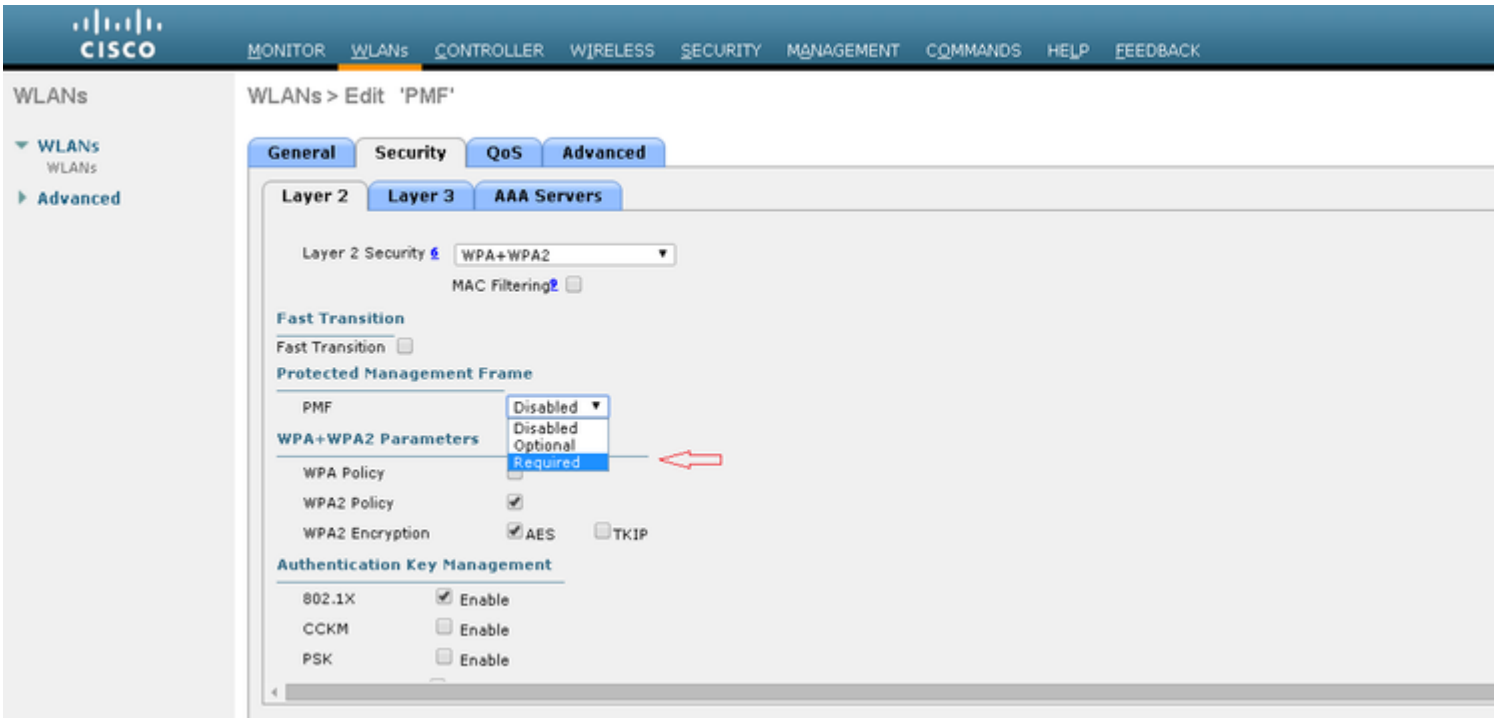
Requisitos para habilitar 802.11w

- 802.11w requiere que el SSID se configure con dot1x o PSK.
- 802.11w es compatible con todos los PA compatibles con 802.11n. Esto significa que los puntos de acceso 1130 y 1240 no admiten 802.11w.
- 802.11w no es compatible con flexconnect AP y 7510 WLC en la versión 7.4. Se ha añadido soporte desde la versión 7.5.

Configurar

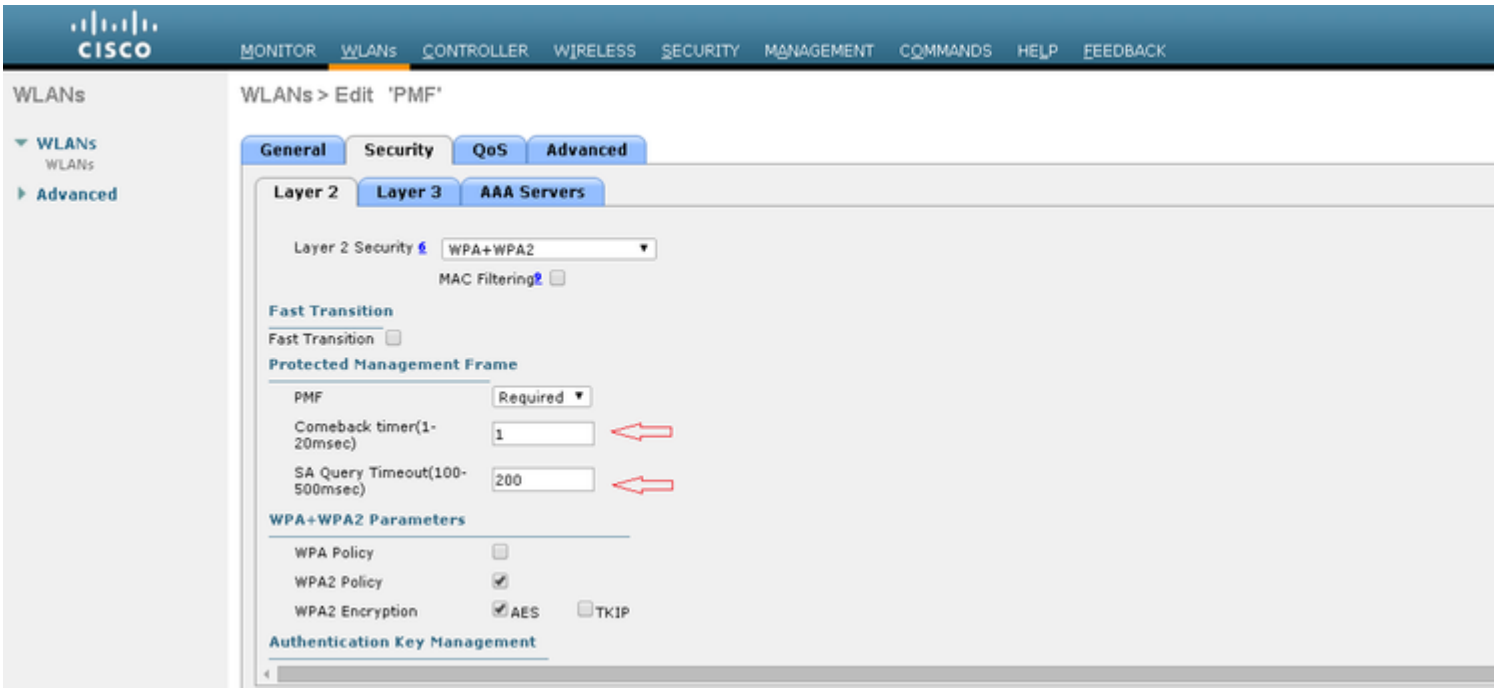
GUI

Paso 1. Debe habilitar la trama de administración protegida en el SSID configurado con 802.1x/PSK. Tiene tres opciones, como se muestra en la imagen.

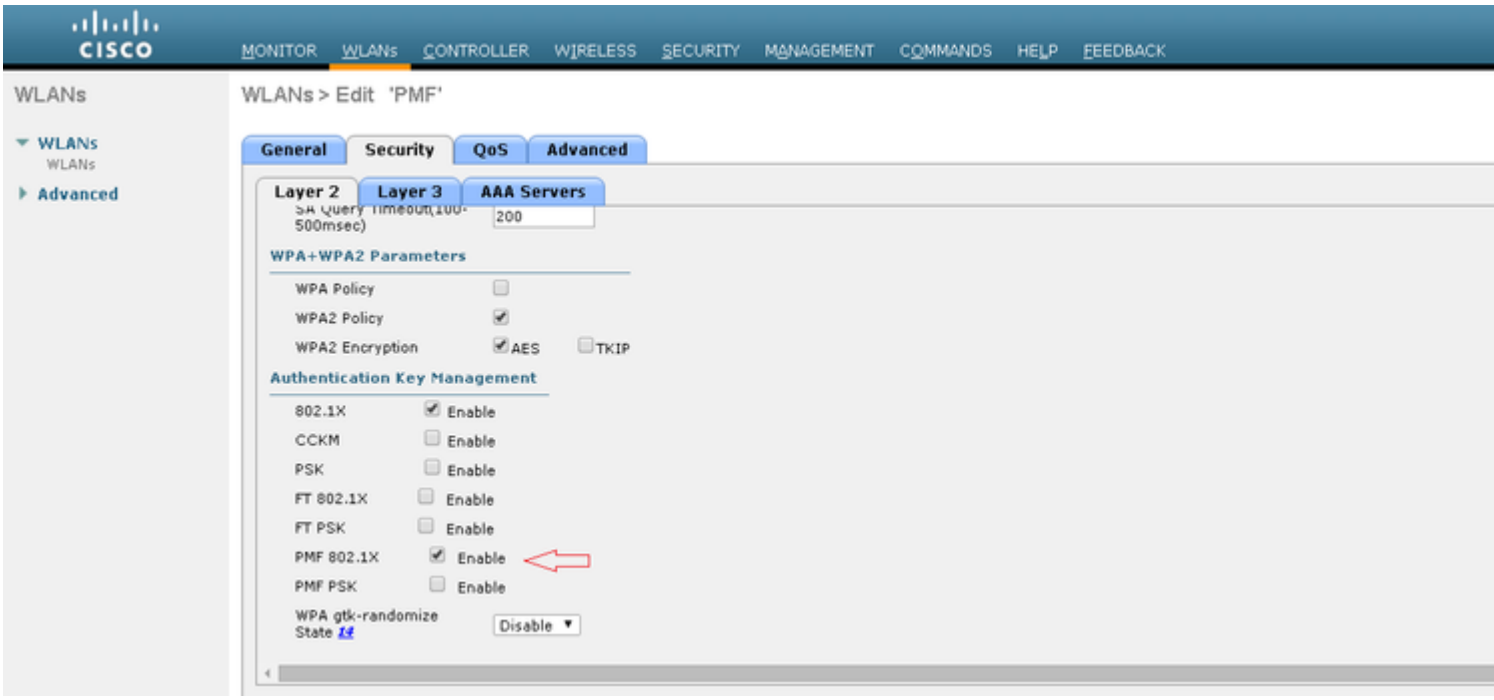


'Requerido' especifica que un cliente que no admite 802.11w no puede conectarse. 'Opcional' especifica que incluso los clientes que no admiten 802.11w pueden conectarse.

Paso 2. A continuación, debe especificar el temporizador de reaparición y el tiempo de espera de la consulta SA. El temporizador de reaparición especifica el tiempo que debe esperar un cliente asociado antes de que se pueda volver a intentar la asociación cuando se deniegue por primera vez con un código de estado 30. El tiempo de espera de la consulta SA especifica la cantidad de tiempo que el WLC espera una respuesta del cliente para el proceso de la consulta. Si no hay respuesta del cliente, su asociación se elimina del controlador. Esto se hace como se muestra en la imagen.



Paso 3. Debe habilitar 'PMF 802.1x' si utiliza 802.1x como método de administración de claves de autenticación. En caso de que utilice PSK, debe seleccionar la casilla de verificación **PMF PSK**, como se muestra en la imagen.



CLI

- Para habilitar o inhabilitar la función 11w, ejecute el comando:

config wlan security wpa akm pmf 802.1x enable/disable

config wlan security wpa akm pmf psk enable/disable

- Para habilitar o inhabilitar los marcos de administración protegidos, ejecute el comando:

config wlan security pmf optional/required/disable

- Configuración de hora de reaparición de asociación:

config wlan security pmf 11w-association-comeback

- Configuración de tiempo de espera de reintento de consulta SA:

config wlan security pmf saquery-retry-time

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Se puede verificar la configuración de 802.11w. Compruebe la configuración de WLAN:

```
(wlc)>show wlan 1
Wi-Fi Protected Access (WPA/WPA2)............ Enabled
<snip>
802.1x.................................. Enabled
PSK..................................... Disabled
CCKM.................................... Disabled
FT-1X(802.11r)......................... Disabled
FT-PSK(802.11r)........................ Disabled
PMF-1X(802.11w)........................ Enabled
PMF-PSK(802.11w)....................... Disabled
FT Reassociation Timeout................... 20
FT Over-The-DS mode....................... Enabled
GTK Randomization......................... Disabled
<snip>
PMF.......................................... Required
PMF Association Comeback Time................. 1
PMF SA Query RetryTimeout..................... 200
```

Troubleshoot

Esta sección proporciona la información que puede utilizar para resolver problemas de su configuración.

Estos comandos debug están disponibles para resolver problemas de 802.11w en el WLC:

- **debug 11w-pmf events enable/disable**
- debug 11w-pmf keys enable/disable
- debug 11w-pmf all enable

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).