Configurar a proteção de quadros de gerenciamento 802.11w no WLC

Contents

Introduction

Este documento descreve detalhes sobre a proteção de quadros de gerenciamento IEEE 802.11w e sua configuração no Cisco Wireless LAN Controller (WLC).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento do Cisco WLC que executa o código 7.6 ou posterior.

Componentes Utilizados

As informações neste documento são baseadas no WLC 5508 que executa o código 7.6.

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

O padrão 802.11w tem como objetivo proteger os quadros de controle e gerenciamento e um conjunto de quadros de gerenciamento robustos contra falsificações e ataques de repetição. Os tipos de quadro protegidos incluem quadros de Desassociação, Desautenticação e Ação Robusta, como:

- Gerenciamento de espectro
- Quality of Service (QoS)
- Bloquear confirmação

- Medição de rádio
- Transição do Conjunto de Serviços Básicos (BSS)

O 802.11w não criptografa os quadros, mas protege os quadros de gerenciamento. Ele garante que as mensagens venham de fontes legítimas. Para fazer isso, você precisa adicionar um elemento Message Integrity Check (MIC). O 802.11w introduziu uma nova chave chamada IGTK (Integrity Group Temporal Key), usada para proteger quadros de gerenciamento robustos de broadcast/multicast. Isso é derivado como parte do processo de handshake de chave de quatro vias usado com o Wireless Protected Access (WPA). Isso torna o dot1x/Chave pré-compartilhada (PSK) um requisito quando você precisa usar 802.11w. Ele não pode ser usado com open/webauth Service Set Identifier (SSID).

Quando a Proteção de Quadro de Gerenciamento é negociada, o Ponto de Acesso (AP) criptografa os valores GTK e IGTK no quadro EAPOL-Key que é entregue na Mensagem 3 do handshake de 4 vias. Se o AP alterar posteriormente o GTK, ele enviará o novo GTK e o IGTK para o cliente com o uso do Handshake de Chave de Grupo. Adiciona um MIC que é calculado com o uso da chave IGTK.

Elemento de Informações MIC de Gerenciamento (MMIE)

802.11w introduz um novo elemento de informação chamado elemento de informação MIC de gerenciamento. Ele tem o formato de cabeçalho como mostrado na imagem.

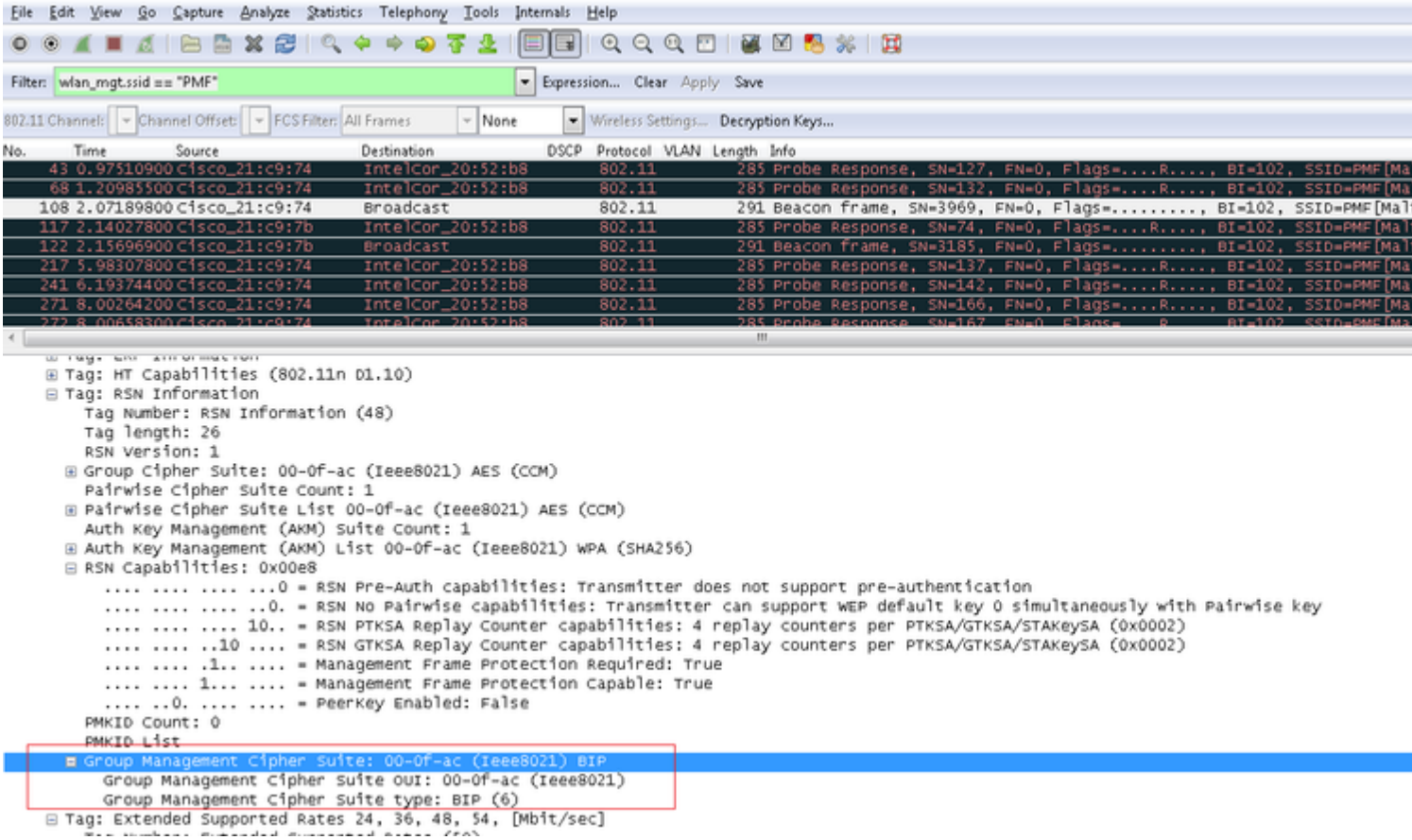
1	1	2	6	8
Element ID	Length	KeyID	IPN	MIC

Os principais campos de preocupação aqui são **ID de elemento** e **MIC**. A ID do elemento para MMIE é 0x4c e serve como uma identificação útil quando você analisa as capturas sem fio.

> **Observação**: MIC - Contém o código de integridade da mensagem calculado sobre o quadro de Gerenciamento. É importante observar que isso é adicionado no AP. O cliente de destino então recalcula o MIC para o quadro e o compara com o que foi enviado pelo AP. Se os valores forem diferentes, isso será rejeitado como um quadro inválido.

Alterações no IE RSN

O RSN IE (Elemento de Informações de Rede de Segurança Robusto) especifica os parâmetros de segurança suportados pelo AP. O 802.11w introduz um seletor de conjunto de cifras de gerenciamento de grupo no RSN IE que contém o seletor de conjunto de cifras usado pelo AP para proteger quadros de gerenciamento robustos de broadcast/multicast. Esta é a melhor maneira de saber se um AP faz 802.11w ou não. Isso também pode ser verificado como mostrado na imagem.

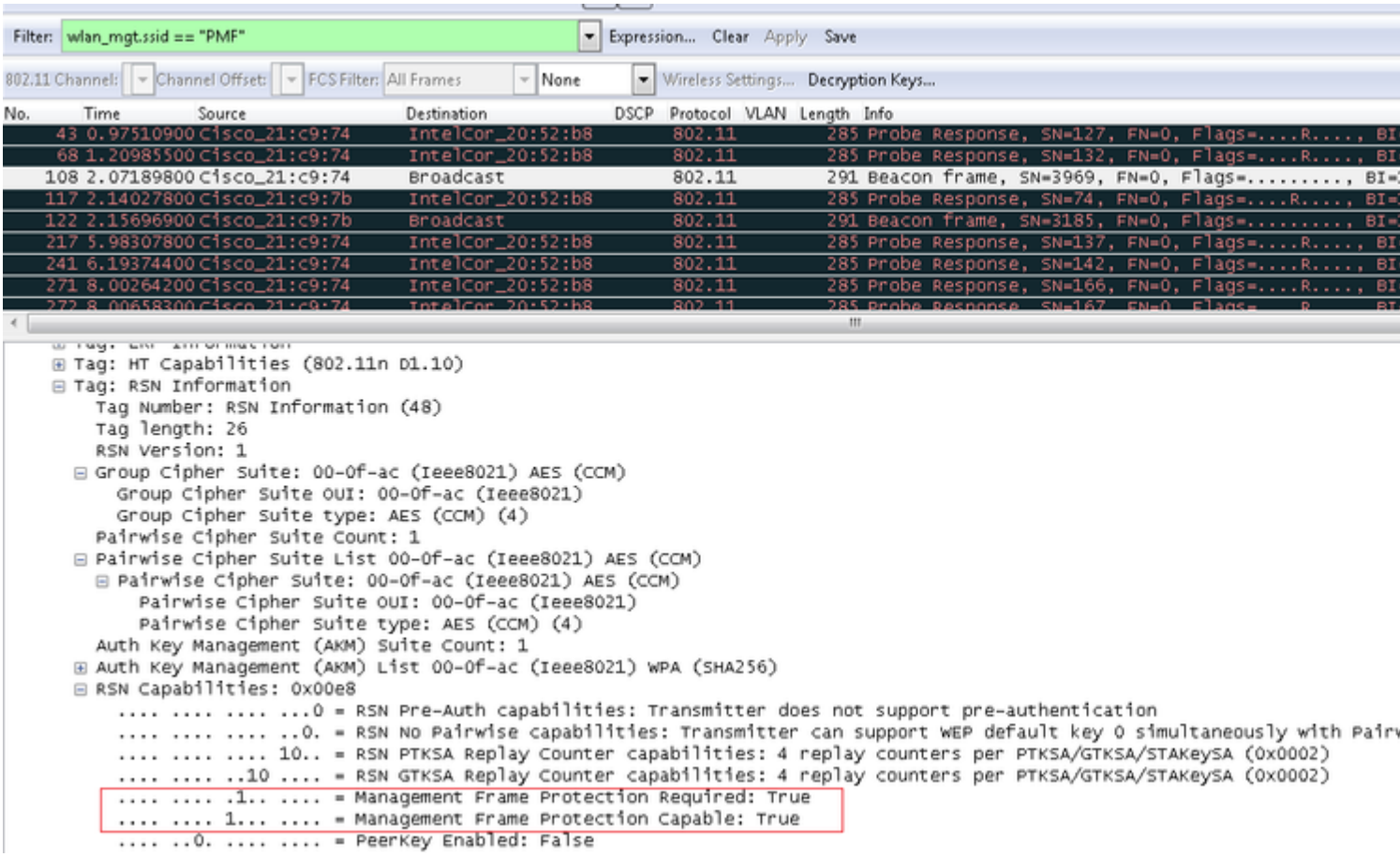


Aqui, você encontra o campo **group management cipher suite** que mostra que 802.11w é usado.

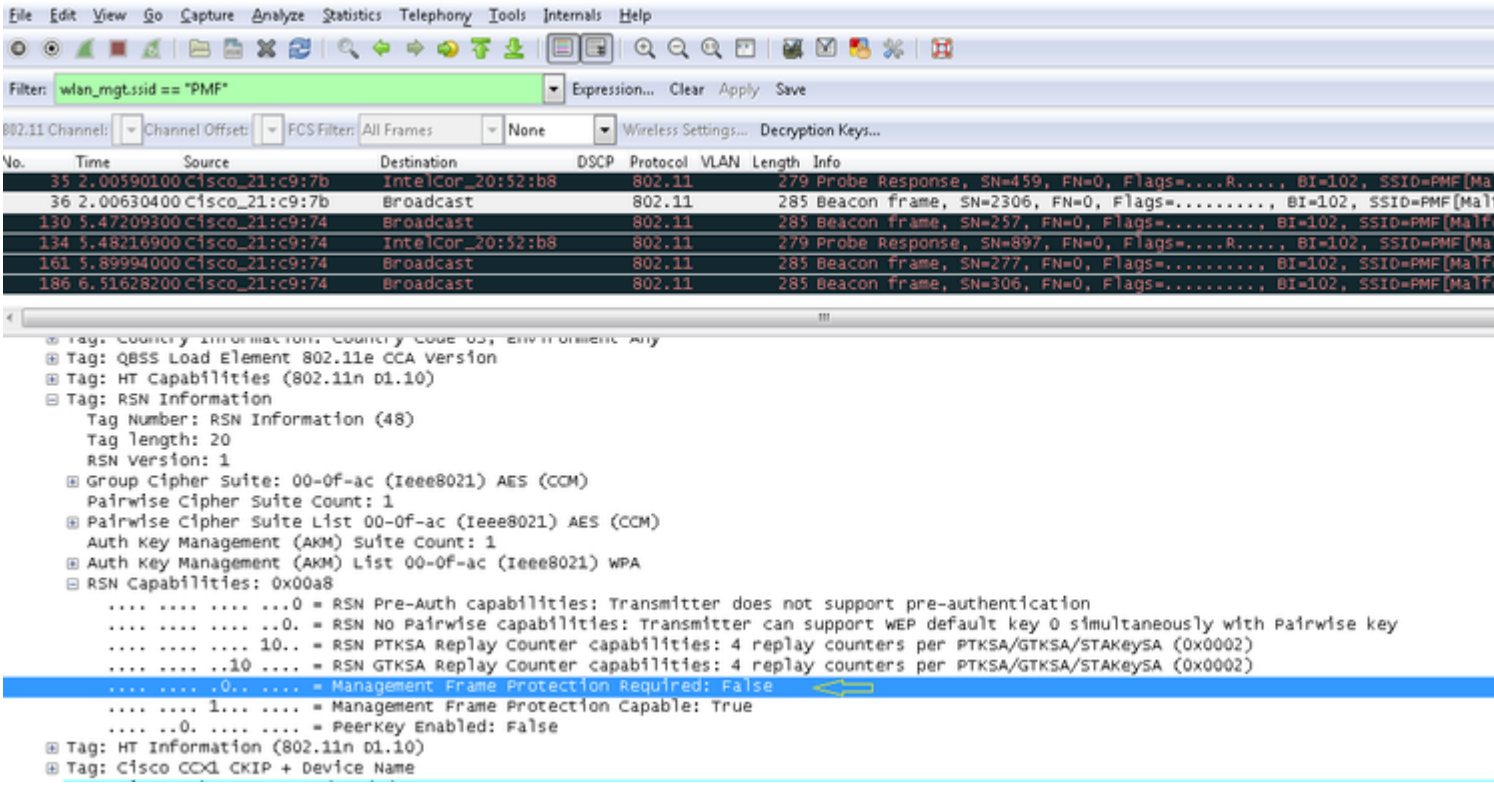
Também foram feitas alterações nos recursos de RSN. Os bits 6 e 7 agora são usados para indicar parâmetros diferentes para 802.11w.

- Bit 6: Proteção de Quadro de Gerenciamento Necessária (MFPR - Management Frame Protection Required) - Um STA define esse bit como 1 para anunciar que a proteção de Quadros de Gerenciamento Robustos é obrigatória.
- Bit 7: Management Frame Protection Capable (MFPC) - Um STA define esse bit como 1 para anunciar que a proteção de Quadros de Gerenciamento Robustos está habilitada. Quando o AP define isso, ele informa que suporta a proteção do quadro de gerenciamento.

Se você definir a proteção do quadro de gerenciamento conforme exigido nas opções de configuração, os bits 6 e 7 serão definidos. Isso é como mostrado na imagem de captura de pacotes aqui.



No entanto, se você definir isso como opcional, apenas o bit 7 será definido, como mostrado na imagem.



Observação: a WLC adiciona esse IE de RSN modificado em respostas de associação/reassociação e o AP adiciona esse IE de RSN modificado em beacons e respostas de sondagem.

Benefícios da proteção de quadros de gerenciamento 802.11w

- Proteção do cliente

Isso é obtido pela adição de proteção criptográfica aos quadros de desautenticação e desassociação. Isso evita que um usuário não autorizado inicie um ataque de negação de serviço (DOS) falsificando o endereço MAC de usuários legítimos e enviando os quadros de não-associação/desassociação.

- Proteção de AP

A proteção do lado da infraestrutura é adicionada com a adição de um mecanismo de proteção contra destruição de SA (Security Association, associação de segurança), que consiste em um tempo de retorno de associação e um procedimento SA-Query. Antes do 802.11w, se um AP recebeu uma solicitação de Associação ou Autenticação de um cliente já associado, o AP encerra a conexão atual e inicia uma nova conexão. Quando você usa o MFP 802.11w, se o STA estiver associado e tiver negociado a Proteção de Quadro de Gerenciamento, o AP rejeitará a Solicitação de Associação com o código de status de retorno 30 Association request rejected temporarily; Try again later ao cliente.

Incluído na Resposta de Associação está um elemento de informação de Tempo de Retorno de Associação que especifica um tempo de retorno quando o AP está pronto para aceitar uma associação com este STA. Dessa forma, você pode garantir que os clientes legítimos não sejam desassociados devido a uma solicitação de associação falsificada.

> **Observação**: a WLC (AireOS ou 9800) ignora os quadros de desassociação ou de desautenticação enviados pelos clientes se eles não usarem o PMF 802.11w. A entrada do cliente só será excluída imediatamente após o recebimento de tal quadro se o cliente usar o PMF. Isso serve para evitar a negação de serviço por dispositivos mal-intencionados, já que não há segurança nesses quadros sem PMF.

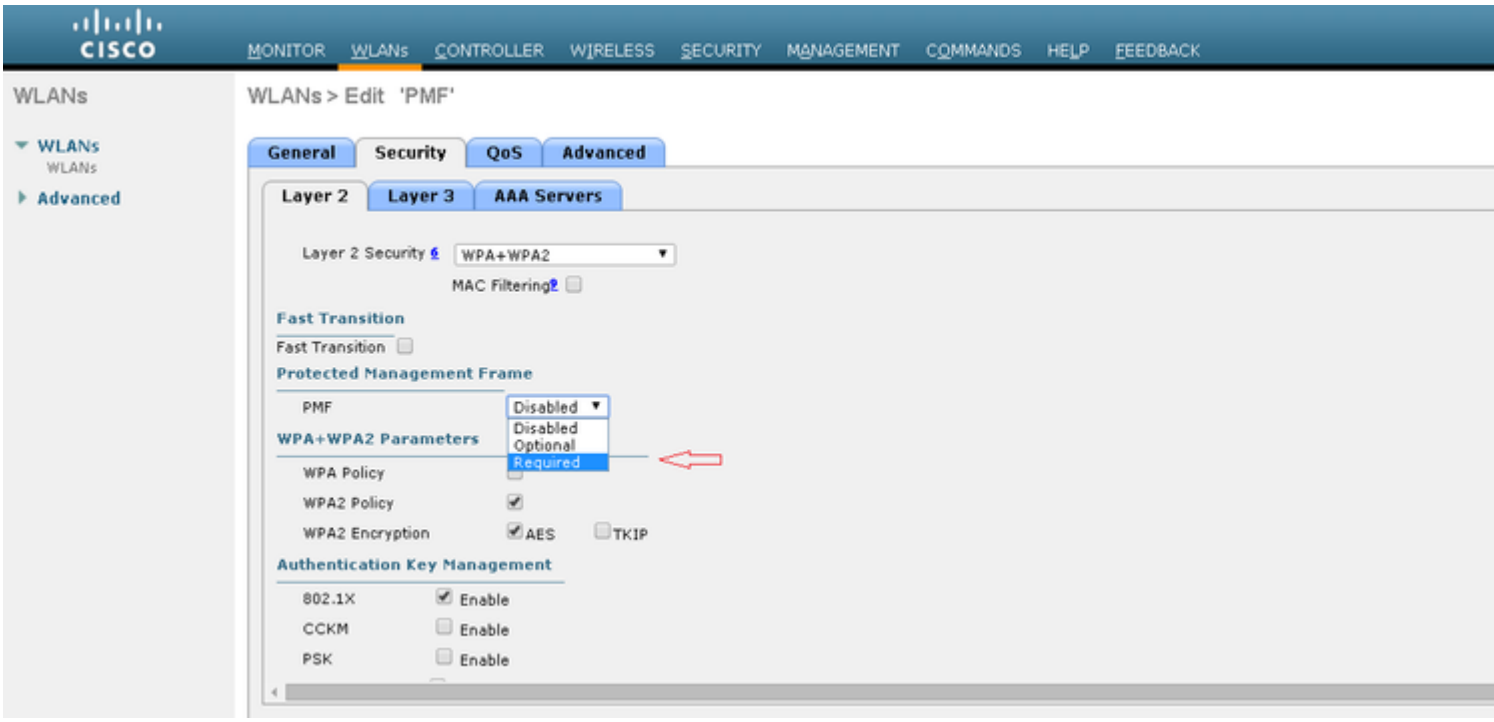
Requisitos para ativar 802.11w

- 802.11w exige que o SSID seja configurado com dot1x ou PSK.
- 802.11w é suportado em todos os AP compatíveis com 802.11n. Isso significa que AP 1130 e 1240 não suportam 802.11w.
- O 802.11w não é suportado no AP flexconnect e no 7510 WLC na versão 7.4. O suporte foi adicionado desde a versão 7.5.

Configurar

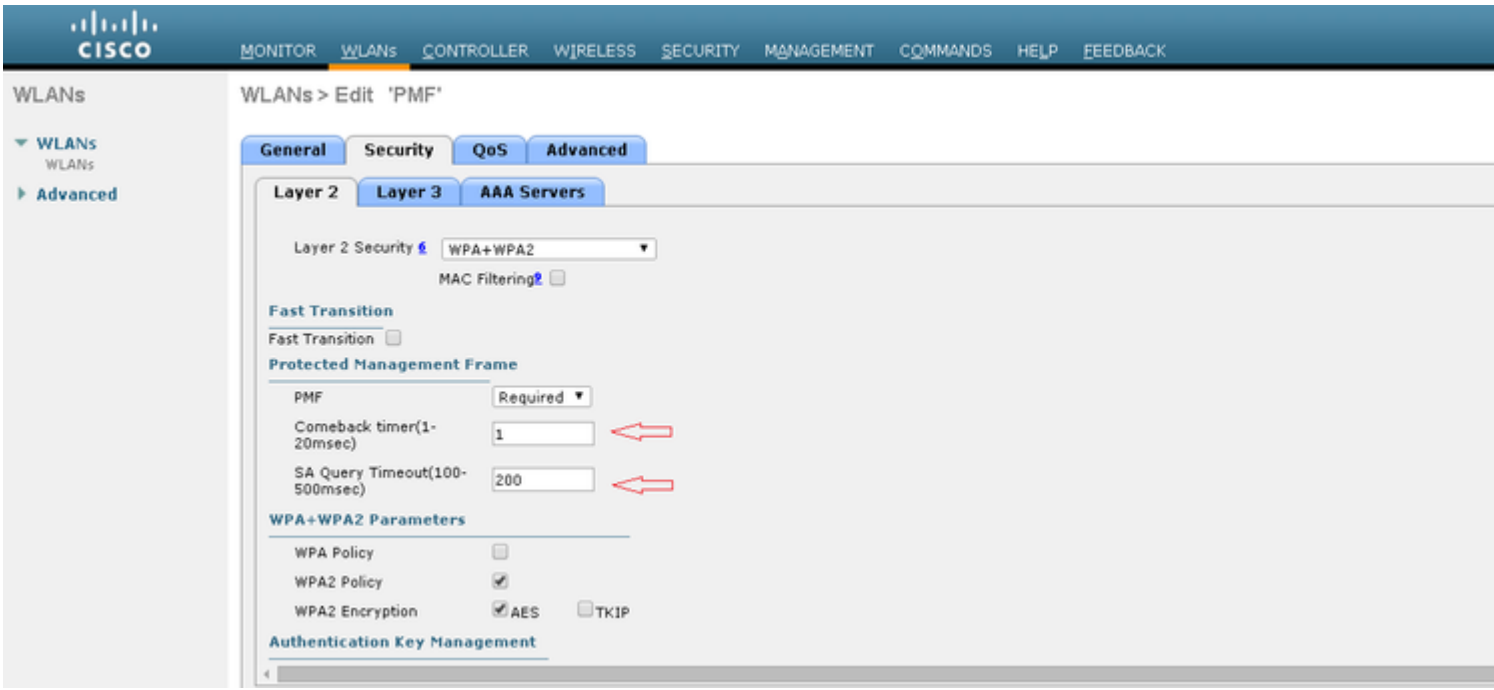
GUI

Etapa 1. Você precisa habilitar o quadro de gerenciamento protegido no SSID configurado com 802.1x/PSK. Você tem três opções, conforme mostrado na imagem.

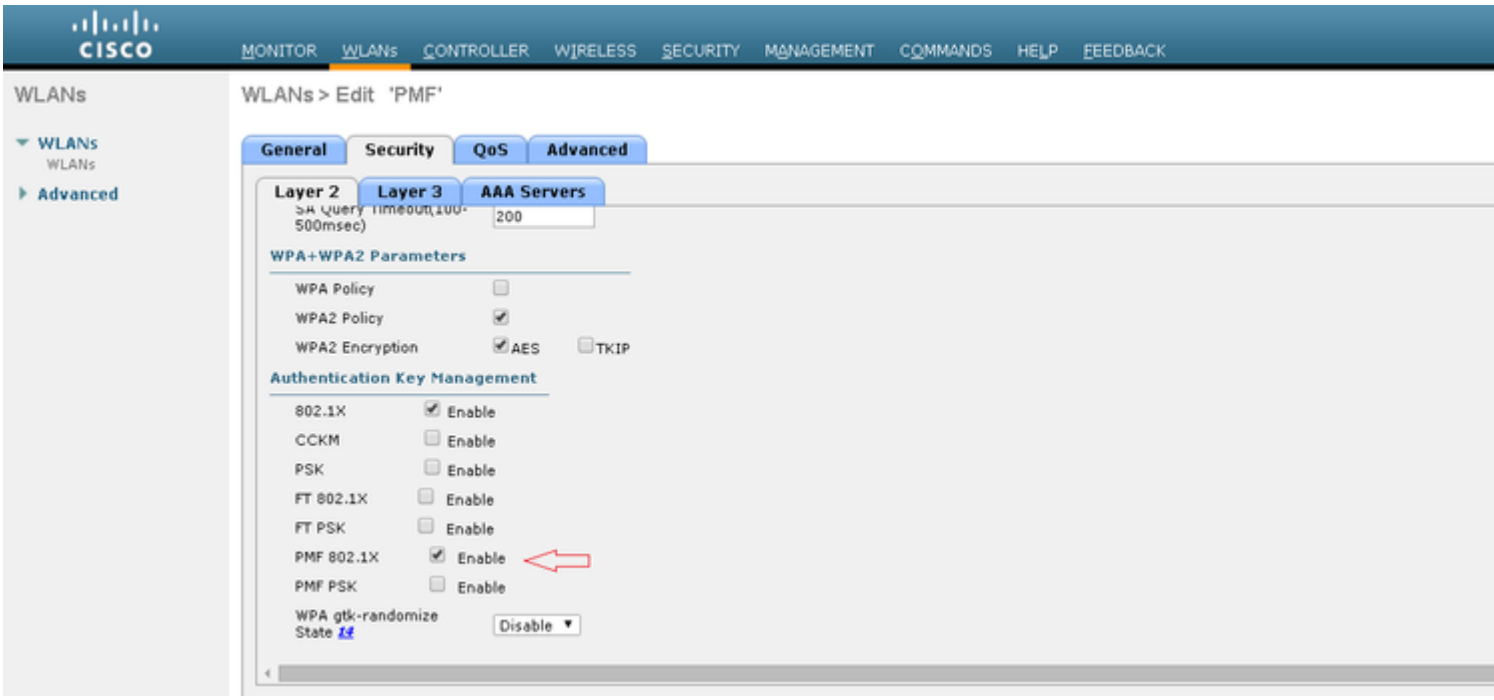


'Obrigatório' especifica que um cliente que não suporta 802.11w não tem permissão para se conectar. 'Opcional' especifica que até mesmo os clientes que não suportam 802.11w têm permissão para se conectar.

Etapa 2. Em seguida, você precisa especificar o temporizador de retorno e o tempo limite de consulta SA. O temporizador de retorno especifica o tempo que um cliente associado deve aguardar antes que a associação possa ser tentada novamente quando negada pela primeira vez com um código de status 30. O tempo limite de consulta SA especifica o tempo que a WLC espera por uma resposta do cliente para o processo de consulta. Se não houver resposta do cliente, sua associação será excluída da controladora. Isso é feito conforme mostrado na imagem.



Etapa 3. Você deve habilitar o 'PMF 802.1x' se usar 802.1x como o método de gerenciamento de chave de autenticação. Caso use a PSK, você deve marcar a caixa de seleção **PMF PSK** como mostrado na imagem.



CLI

- Para habilitar ou desabilitar o recurso 11w, execute o comando:

config wlan security wpa akm pmf 802.1x enable/disable

config wlan security wpa akm pmf psk enable/disable

- Para habilitar ou desabilitar Quadros de Gerenciamento Protegidos, execute o comando:

config wlan security pmf optional/required/disable

- Configurações de Tempo de Retorno de Associação:

config wlan security pmf 11w-association-comeback

- Configurações de Tempo Limite de Repetição de Consulta SA:

config wlan security pmf saquery-retry-time

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A configuração 802.11w pode ser verificada. Verifique a configuração da 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 seção fornece as informações que você pode usar para solucionar problemas da sua configuração.

Estes comandos de depuração estão disponíveis para solucionar problemas do 802.11w no WLC:

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

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.