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

# Contenido

Introducción Prerequisites Requirements Componentes Utilizados Antecedentes Elemento de información de MIC de administración (MMIE) Cambios en RSN IE Ventajas de la protección de tramas de administración 802.11w Requisitos para habilitar 802.11w Configurar GUI CLI Verificación Troubleshoot

# 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	KeylD	IPN	MIC

Los principales campos de interés aquí son **element ID** y **MIC**. El ID de elemento para MMIE es <sub>0x4c</sub> 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.

Eile	Edit View	Go Capture	Analyze Stati	istics Telephony	Tools Inte	mals <u>H</u> elp						
•	• ք 🔳	a i 🖻 🖨	X 2   9	( 🔶 🔶 🥥 🖥	F 🕹 I 🔳		🖸   👪 🗹 🥵 :	* 🛙 🛱				
Filter	wlan_mgt.s	sid == "PMF"			-	Expression Clear Ap	oply Save					
802.11	Channel:	Channel Offset	FCS Filter	All Frames	- None	Wireless Settings	Decryption Keys					
No.	Time	Source		Destination		DSCP Protocol VLAN	I Length Info					
	43 0.9751	0900 c1sco_	21:c9:74	IntelCor_2	0:52:b8	802.11	285 Probe R	esponse, SN=12	7, FN=0, F	lags=R	, BI=102,	, SSID=PMF[Ma
	68 1.2098	5500 C1sco_	21:c9:74	IntelCor_2	0:52:b8	802.11	285 Probe R	esponse, SN=13	2, FN=0, F	lags=R	, BI=102,	, SSID=PMF[Ma
	108 2.0718	9800 C1sco_	21:c9:74	Broadcast		802.11	291 Beacon	frame, SN=3969	, FN=0, Fla	ags=	., BI=102,	SSID=PMF[Ma]
	117 2.1402	7800 C1sco_	21:c9:7b	IntelCor_2	0:52:68	802.11	285 Probe R	esponse, SN=74	, FN=0, F1	ags=R	., BI=102,	SSID=PMF[Ma]
	122 2.1569	6900 C15C0_	21:09:70	Broadcast	A.53.60	802.11	291 Beacon	Trame, SN=3185	, FN=0, FI	ags=	., BI=102,	SSID=PMF[Mai
	241 6 1027	4400 C15C0_	21:09:74	IntelCor_2	0:52:08	802.11	285 Probe R	esponse, SN=13	7, FN=0, F	lags=R	BT-102	SSID=PMF[Ma
	271 8.0026	4200 C1sco	21:09:74	IntelCor 2	0:52:b8	802.11	285 Probe R	esponse, SN=16	6. FN=0. F	lags=R	BI=102.	SSID=PMF[Ma
	272 8 0065	8300 C1sco	21 9 . 74	IntelCor 2	0.52.h8	802 11	285 Probe 8	esnonse SN=16	7 EN=0 E	lags= R	BT=102	SSTD=PME Ma
<							III					
	Tag: RSI Tag N Tag N RSN V Group Pairw Auth I Auth I RSN C  PMKID PMKID	N Informati umber: RSN ength: 26 ersion: 1 Cipher Suf ise Cipher ise Cipher apabilities 	informatio Informatio Suite Coun Suite List intent (AKM) S: 0x00e8 0 = RS = RS = Ma = Ma = Pe	ac (Ieee8021) tt: 1 :00-0f-ac (Ie Suite Count: List 00-0f-ac N Pre-Auth ca N Pre-Auth ca N PTKSA Repla N GTKSA Repla N GTKSA Repla Inagement Fram reerKey Enabled	AES (CC) eee8021) . 1 : (Ieee80 epabiliti e capabil y Counte is Protec : False	M) AES (CCM) 21) WPA (SHA256) es: Transmitter ities: Transmitt r capabilities: r capabilities: t capabilities: Tri tion Required: Tri tion Capable: Tri	does not suppor er can support 4 replay counte 4 replay counte ue ue	t pre-authenti WEP default ke rs per PTKSA/G rs per PTKSA/G	cation y O simulta TKSA/STAKey TKSA/STAKey	aneously wit ySA (0x0002) ySA (0x0002)	h Pairwise	key
l	Gro Gro	up Manageme up Manageme tended Sunn	ant Cipher	Suite OUI: 00 Suite type: E	0-0f-ac ( BIP (6) 54. [Mb	it/sec]						
	- ragi ex	serioco popp	ren eco nace		241 040	1410003						

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.

Filter	wlan_mg	gt.ssid == "PMF"				Expression Clea	n Apply Sa	ve						
802.11	Channel:	- Channel Offs	et: 💌 FCS Filte	er: All Frames	- None	▼ Wireless Se	ttings Decr	yption Keys						
No.	Time	Source		Destination		DSCP Protocol	VLAN Lengt	h Info						
	43 0.97	510900 Cisco	_21:c9:74	IntelCor.	_20:52:b8	802.11	21	85 Probe	Response,	SN=127	, FN=0,	Flags=.	R	, BI
	68 1.20	985500 C1sco	_21:c9:74	IntelCor,	_20:52:b8	802.11	21	85 Probe	Response,	SN=132	, FN=0,	Flags=.	R	, BI
	LO8 2.07	189800 cisco	)_21:c9:74	Broadcas	t	802.11	29	91 Beacon	frame, S	N=3969,	FN=0,	Flags=		, BI=
	117 2.14	027800 Cisco	)_21:c9:7b	IntelCor.	_20:52:b8	802.11	2	85 Probe	Response,	SN=74,	FN=0,	Flags=	R	, BI=
	122 2.15	696900 C1sco	)_21:c9:7b	Broadcas	t	802.11	20	91 Beacon	frame, S	N=3185,	FN=0,	Flags=		, BI-
	217 5.98	307800 C1sco	)_21:c9:74	IntelCor.	_20:52:b8	802.11	2	85 Probe	Response,	SN=137	, FN=0,	Flags=.	R	, BI
	241 6.19	374400 C15C0	)_21:c9:74	IntelCor,	_20:52:68	802.11	2	85 Probe	Response,	SN=142	, FN=0,	Flags=.	R	, BI
	271 8.00	264200 C15C0	_21:c9:74	IntelCor.	20:52:68	802.11	21	85 Probe	Response,	SN=166	, FN=0,	Flags=.	R	, BI
<	/// 8 100	masulir 1scr	21-69-74	Intell or	2015 3 2 5 68	8412 11		111	vesninnse	SNELDY	k Nett	E Lanse		BI
	Tag: Tag: Tag: Tag Tag RSN Gro G Pai	HT Capabili RSN Informar Number: RSI length: 26 Version: 1 up Cipher Su roup Cipher roup Cipher rwise Cipher	ties (802.1) tion N Informati uite: 00-0f Suite OUI: Suite type r Suite Cou	<pre>1n D1.10) on (48) -ac (Ieee802:     00-0f-ac (I :: AES (CCM) nt: 1     00 of ac ()</pre>	1) AES (CC eee8021) (4)	EM)								
	■ P Aut ● Aut ■ RSN	airwise Cip Pairwise C Pairwise C h Key Manag h Key Manag Capabiliti	her Suite: ipher Suite ipher Suite ement (AKM) ement (AKM) es: 0x00e8 0 = R 0. = R 0. = R 10 = R	00-Of-ac (Ie OUI: 00-Of- type: AES ( Suite Count List 00-Of- SN Pre-Auth SN NO Pairwi SN PTKSA Rep SN GTKSA Rep anagement Fr	ee8021) AG ac (Ieee8( CCM) (4) : 1 ac (Ieee8( capabilit: se capabilit: lay Counta ame Protex	ES (CCM) D21) WPA (SHAZ ies: Transmitt lities: Transm er capabilitie er capabilitie tion Required	256) er does n nitter can es: 4 repl es: 4 repl 1: True	not suppor 1 support ay count ay count	rt pre-au WEP defa ers per P ers per P	thentica ult key TKSA/GTM TKSA/GTM	tion O simu (SA/STA (SA/STA	ltaneous KeySA (O KeySA (O	ly with ×0002) ×0002)	Pairs
	Ŀ	1.		anagement Fr eerKey Enabl	ame Protec ed: False	ction Capable:	True	]						

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

Eile Edit View Go Capt	ure Analyze Statistics	Telephony Tools Internals	Help					
0 0 🧉 🔳 🔬 🖻	🖹 🗶 🎜   🔍 🗢	+ 4 7 £ 🗐	] @ @ @ @	]   🍇 🗹 🥵 🎉	1			
Filter: wlan_mgt.ssid == "PM	F"	💌 Equ	ession Clear Appl	y Save				
802.11 Channel: 🔽 Channel O	ffset: FCS Filter: All Fr	rames v None	<ul> <li>Wireless Settings</li> </ul>	Decryption Keys				
No. Time Sour	ce De	estination DSG	Protocol VLAN	Length Info				
35 2.00590100 c1s	co_21:c9:7b In	ntelCor_20:52:b8	802.11	279 Probe Respo	nse, SN=459, FN	=0, Flags=R	, BI=102	, SSID=PMF[Ma
36 2.00630400 c1s	:co_21:c9:7b Br	roadcast	802.11	285 Beacon fram	e, SN=2306, FN=	0, Flags=	., BI=102,	SSID=PMF[Ma]
130 5.47209300 C1s	CO_21:C9:74 Br	roadcast	802.11	285 Beacon fram	e, SN=257, FN=0	, Flags=	, BI=102, S	SSID=PMF[Malf
134 5.48216900 C1s	CO_21:C9:74 In	ntelCor_20:52:68	802.11	279 Probe Respo	nse, SN=897, FN	=0, Flags=R	, BI=102	, SSID=PMF[Ma
101 3.89994000 C15	CO_21:C9:74 B	roadcast	802.11	285 Beacon fram	e, SN=277, FN=U	Flags=	97-102, 1	SSID=PMF[Mail]
100 0.01020200 C15	CO_21:C9:/4 Bi	roaucast	802.11	200 Beacon Tram	e, sn=300, FN=0	, Flays=	, 61=102, 3	SSID=PMP (Mail)
< [								
<ul> <li>              Taġ: HT Capabii          </li> <li>             Taġ: RSN Inform             Taġ Number: F             Taġ Number: F             Taġ Number: F             Sroup Cipher             Pairwise Ciph             Pairwise Ciph             Auth Key Mana             RSN Capabilit         </li> <li>             Auth Key Mana         </li> <li>             RSN Capabilit         </li> </ul>	<pre>lities (802.11n D1 mation RSN Information (4) 20 1 suite: 00-0f-ac () her Suite Count: 1 her Suite List 00-0 factor (AKM) suit agement (AKM) suit agement (AKM) List ties: 0x00a8 0 = RSN PT 0. = RSN PT 0. = RSN PT </pre>	.10) 8) Ieee8021) AES (CCM) 0f-ac (Ieee8021) AES e Count: 1 00-0f-ac (Ieee8021) e-Auth capabilities: Pairwise capabilities: KSA Replay Counter c ment Frame Protection ment Frame Protection	(CCM) WPA Transmitter do es: Transmitter apabilities: 4 apabilities: 4 n Required: Fal n Capable: True	es not support pr can support WEP replay counters p replay counters p	e-authenticatio default key 0 s' er PTKSA/GTKSA/S er PTKSA/GTKSA/S	n imultaneously wit stakeysa (0x0002) stakeysa (0x0002)	h Pairwise	key
	ation (802.11n D1.1 1 CKIP + Device Nam	10) me						

**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.

،،ا،،،ا،، cısco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK
WLANs	WLANs > Edit 'PMF'
WLANS	General Security QoS Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 2 Security 1 WPA+WPA2 MAC Filtering 2 Fast Transition Fast Transition Protected Management Frame PMF WPA+WPA2 Parameters WPA+WPA2 Parameters WPA Policy WPA2 Policy WPA2 Encryption AES TKIP Authentication Key Management 802.1X Enable CCKM Enable PSK Enable

'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.

،،۱،،۱۰، cısco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK								
WLANs	WLANs > Edit 'PMF'								
WLANS	General Security QoS Advanced								
▶ Advanced	Layer 2 Layer 3 AAA Servers								
	Layer 2 Security £ WPA+WPA2 🔻								
	Fast Transition								
	Fast Transition								
	Protected Management Frame								
	PMF Required T								
	Comeback timer(1- 20msee) 1								
	SA Query Timeout(100- 500msec) 200								
	WPA+WPA2 Parameters								
	WPA Policy								
	WPA2 Policy 🕑								
	WPA2 Encryption @AES TKIP								
	Authentication Key Management								
	4								

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.

սիսիս cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK
WLANs	WLANs > Edit 'PMF'
▼ WLANs WLANs	General Security QoS Advanced
WLANS Advanced	Layer 2       Layer 3       AAA Servers         Sh Query Timeout(100*       200         WPA+WPA2 Parameters         WPA Policy         WPA2 Policy         WPA2 Encryption         AES       TKIP         Authentication Key Management         802.1X       Enable         PSK       Enable         FT 802.1X       Enable         FT PSK       Enable         PMF 802.1X       Enable
	PMF PSK Enable WPA gtk-randomize State 14

#### 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></snip>	
802.1x Enable	ed
PSK Disabl	Led
CCKM Disabl	Led
FT-1X(802.11r) Disab]	Led
FT-PSK(802.11r) Disab]	Led
PMF-1X(802.11w) Enable	ed
PMF-PSK(802.11w) Disab]	Led
FT Reassociation Timeout	
FT Over-The-DS mode Ena	abled
GTK Randomization Dis	abled
<snip></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).