# WLCでの802.11w管理フレーム保護の設定

内容
はじめに
前提条件
要件
使用するコンポーネント
背景説明
管理MIC情報要素(MMIE)
RSNIEの変更
802.11w管理フレーム保護の利点
802.11wを有効にするための要件
設定
GUI
CLIを使う場合:
確認
トラブルシュート

## はじめに

このドキュメントでは、IEEE 802.11w管理フレーム保護と、Cisco Wireless LAN Controller(WLC)での設定について詳しく説明します。

### 前提条件

要件

コード7.6以降が稼働するCisco WLCに関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、コード7.6を実行するWLC 5508に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

### 背景説明

802.11w標準の目的は、制御フレームと管理フレーム、および一連の堅牢な管理フレームを偽造 およびリプレイ攻撃から保護することです。保護されるフレームタイプには、次のような関連付 け解除、認証解除、および堅牢なアクションフレームがあります。

- スペクトラム管理
- Quality of Service ( QoS )
- ・ブロックAck
- 無線測定
- Fast Basic Service Set(BSS)への移行

802.11wはフレームを暗号化しませんが、管理フレームを保護します。メッセージが正当な送信 元から送信されることが保証されるそのためには、メッセージ整合性チェック(MIC)要素を追加す る必要があります。802.11wでは、Integrity Group Temporal Key(IGTK)と呼ばれる新しいキーが 導入されました。このキーは、ブロードキャスト/マルチキャストの堅牢な管理フレームを保護す るために使用されます。これは、Wireless Protected Access(WPA)で使用される4方向キーハンド シェイクプロセスの一部として導出されます。このため、802.11wを使用する必要がある場合は 、dot1x/事前共有キー(PSK)が必要になります。オープン/webauthのService Set Identifier(SSID)では使用できません。

管理フレーム保護(MFP)がネゴシエートされると、アクセスポイント(AP)は4ウェイハンドシェイ クのメッセージ3で配信されるEAPOLキーフレームのGTK値とIGTK値を暗号化します。APは後 でGTKを変更すると、Group Key Handshakeを使用して新しいGTKとIGTKをクライアントに送信 します。IGTKキーを使用して計算されたMICを追加します。

管理MIC情報要素(MMIE)

802.11wでは、管理MIC情報要素と呼ばれる新しい情報要素が導入されています。図に示すよう に、ヘッダー形式があります。

1	1	2	6	8
Element ID	Length	KeylD	IPN	MIC

ここで問題となる主なフィールドは、要素IDとMICです。MMIEのエレメントIDは 0x4c また、ワ イヤレスキャプチャを分析する際に役立つ識別情報として使用できます。

◆ 注:MIC:管理フレームで計算されたメッセージ整合性コードが含まれます。これはAPで追加されることに注意してください。次に、宛先クライアントはフレームのMICを再計算し、APから送信されたものと比較します。値が異なる場合、無効なフレームとして拒否されます。

### RSN IEの変更

Robust Security Network Information Element(RSN IE)は、APでサポートされるセキュリティパラ メータを指定します。802.11wでは、ブロードキャスト/マルチキャストの堅牢な管理フレームを 保護するためにAPで使用される暗号スイートセレクタを含むGroup Management Cipher Suite(GMS)セレクタがRSN IEに導入されています。これは、APが802.11wを実行するかどうか を確認する最良の方法です。これは、図に示すように確認することもできます。

Ele Edit View So Sapture Analyze Statistics Telephony Iools Internals Help				
● ● 🗶 🔳 🔬 📄 🗎 🗶 😂   🔍 4	> + • • 7 ½ 🗐 🗐 Q Q Q	🔟   🎆 🗹 🥵 茶   🎇		
Filter: wlan_mgt.ssid == "PMF"	💌 Expression Clear A	lipply Save		
802.11 Channel: 👻 Channel Offset: 👻 FCS Filter: All	Frames Vireless Setting	gs Decryption Keys		
No. Time Source	Destination DSCP Protocol VLA	W Length Info		
68 1.20985500 c1sco_21:c9:74	IntelCor_20:52:68 802.11	285 Probe Response, SM=127, FN=0, Flags=, BI=102, SSID=PMF[Malformed Packet]		
108 2.07189800 cisco_21:c9:74	Broadcast 802.11	291 Beacon frame, SN=3969, FN=0, Flags=, BI=102, SSID=PMF[Malformed Packet]		
117 2.14027800 Cisco_21:c9:7b	IntelCor_20:52:b8 802.11	285 Probe Response, SN=74, FN=0, Flags=R, BI=102, SSID=PMF[Malformed Packet]		
122 2.15696900 C15C0_21:C9:70	Broadcast 802.11 Totalcon 20:52:68 802.11	291 BEACON TRAME, SN#5185, FNHU, Flags=, BI=102, SSID=PMF[MaiTormed Packet] 295 Prohe Resonnes SNH27 ENHO Elace- P RI402 SSID=PMF[MaiTormed Packet]		
241 6.19374400 C1sco_21:c9:74	IntelCor_20:52:58 802.11	285 Probe Response, SN-142, FN-0, Flags, BI=102, SSID=PMF[Malformed Packet]		
271 8.00264200 Cisco_21:c9:74	IntelCor_20:52:b8 802.11	285 Probe Response, SN=166, FN=0, Flags=R, BI=102, SSID=PMF[Malformed Packet]		
272 8 00658300 C1sco 21 c9 74	TotelCor 20:52:68 802 11	285 Brohe Seconce SN=167 EN=0 Elance & RT=107 SST0=BME[Malfnormed Backet]		
<pre>ing: Ext An Origination B Tag: Ext Information Tag: Ext Information Tag length: 26 Ext Information B Group Cipher Suite: 00-0f-ac (Ieee8021) AES (CCM) Pairwise Cipher Suite count: 1 B Pairwise Cipher Suite Count: 1 B Pairwise Cipher Suite Count: 1 B Alth Key Management (AMM) Suite Count: 1 D Alth Key Management (AMM) Suite Count: 1 B Alth Key Management (AMM) Suite Count: 1 D Alth Key Management (AMM) Suite Capabilities: Transmitter does not support pre-authentication D = RSN No Pairwise Capabilities: Transmitter does not support wEP default key 0 simultaneously with Pairwise key D = RSN Capabilities: DNODe8 D = RSN No Pairwise Capabilities: I replay counter sper PTKSA/GTKSA/STAKeySA (0x002) D = RSN GTKSA Replay Counter capabilities: True D = RSN Capabilities: 00000 Management Frame Protection Capable: True D = RSN Capabilities: 00000 Management Frame Protection Capable: True D = RSN Capabilities: 00000 Management Frame Protection Capable: True D = RSN Capabilities: 00000 Management Frame Protection Capable: True D = RSN Capabilities: 00000 Management Frame Protection Capable: True D = RSN Capabilities: 00000 Management Frame Protection Capable: True D = RSN Capabilities: 00000 Management Frame Protection Capabilities: True D = RSN Capabilities: 00000 Management Frame Protection Capabilities: True D = RSN Capabilities: 00000 Mitter Capabilities: 0000000 Mitt</pre>				
Group Management Cipher Sui Tag: Extended Supported Rates 2	ite type: BIP (6) 24, 36, 48, 54, [Mbit/sec]			

ここでは、802.11wが使用されていることを示すgroup management cipher suiteフィールドがあります。

RSN機能にも変更が加えられています。ビット6と7は、802.11wの異なるパラメータを示すため に使用されます。

- ビット6:Management Frame Protection Required(MFPR):STAは、このビットを1に設定して、堅牢な管理フレームの保護が必須であることをアドバタイズします。
- ビット7:Management Frame Protection Capable(MFPC):STAは、このビットを1に設定して、 、堅牢な管理フレームの保護が有効であることをアドバタイズします。APはこれを設定すると、管理フレーム保護をサポートしていることを通知します。

設定オプションで必要に応じて管理フレーム保護を設定すると、ビット6と7の両方が設定されま す。これは、次のパケットキャプチャの図に示すとおりです。

Filter:	wlan_mgt.ssid == "PMF"		Expression Clear Apply	ly Save		
802.11	Channel: 💌 Channel Offset:	▼ FCS Filter: All Frames ▼	None 💌 Wireless Settings	. Decryption Keys		
No.	Time Source	Destination	DSCP Protocol VLAN L	Length Info		
	43 0.97510900 cisco_2	1:c9:74 IntelCor_20:	i2:b8 802.11	285 Probe Response, SN=127, FN=0, Flags=, RI=102, SSID=PMF[Malformed Packet]		
	58 1.20985500 cisco_2	1:c9:74 IntelCor_20:	2:b8 802.11	285 Probe Response, SN=132, FN=0, Flags=R, BI=102, SSID=PMF[Malformed Packet]		
1	08 2.07189800 ⊂is⊂o_2	1:c9:74 Broadcast	802.11	291 Beacon frame, SN=3969, FN=0, Flags=, BI=102, SSID=PMF[Malformed Packet]		
1	L7 2.14027800 Cisco_2	1:c9:7b IntelCor_20:	12:58 802.11	285 Probe Response, SN=74, FN=0, Flags=, BI=102, SSID=PMF[Malformed Packet]		
	22 2.15696900 C1sco_2	1:C9:/D Broadcast	802.11	291 Beacon Trame, SN=3185, FN=U, Flags=, BI=102, SSID=FMF[Mailtormed Packet]		
4	L/ 5.9850/800 C15C0_2	1:c9:74 IntelCor_20:	2:08 802.11	285 Probe Response, SN=157, FN=0, Flags=, BI=102, SSL0=PMF[Malformed Packet]		
	71 8 00264200 Cisco 2	1:c9:74 IntelCor_20:	2.56 602.11	205 FLODE RESPONSE, SWEIME, FNEU, FLAGSE, BIELVZ, SSIDEFME[Mail/onmed Facket]		
2	72 8 00658300 cisco 2	1:c9:74 IntelCor 20:	12.b0 002.11	285 Probe Response, SN=167, EN=0, Flags, BI=102, SSID=PMP[Malformed Packet]		
٠ 📃				III		
	B Tag: HT Capabilities (802.11n DL.10) B Tag: RSN Information Tag Number: RSN Information (48) Tag length: 26 RSN Version: 1 B Group Cipher Suite: 00-0F-ac (Ieee8021) AES (CCM) Group Cipher Suite type: AES (CCM) (4) Pairwise Cipher Suite type: AES (CCM) (4) Pairwise Cipher Suite List 00-0F-ac (Ieee8021) AES (CCM) B Pairwise Cipher Suite List 00-0F-ac (Ieee8021) AES (CCM) Pairwise Cipher Suite List 00-0F-ac (Ieee8021) AES (CCM) Pairwise Cipher Suite List 00-0F-ac (Ieee8021) AES (CCM) Pairwise Cipher Suite toul: 00-0F-ac (Ieee8021) WPA (SHA256) B RSN Capabilities: 0x0008					

ただし、これをオプションに設定すると、図に示すようにビット7だけが設定されます。



✤ 注:WLCはこの変更されたRSN IEを関連付け/再関連付け応答に追加し、APはこの変更され たRSN IEをビーコンとプローブ応答に追加します。

#### 802.11w管理フレーム保護の利点

クライアント保護

これは、認証解除フレームと関連付け解除フレームに暗号化保護を追加することで実現されます 。これにより、正当なユーザのMACアドレスをスプーフィングして認証/関連付け解除フレームを 送信することで、権限のないユーザがサービス拒否(DOS)攻撃を開始することを防止できます。

AP保護

インフラストラクチャ側の保護は、関連付け復帰時間とSA-Query手順で構成されるセキュリティ アソシエーション(SA)ティアダウン保護メカニズムの追加によって追加されます。802.11wより も前のバージョンでは、APがすでに関連付けられているクライアントから関連付けまたは認証要 求を受信した場合、APは現在の接続を終了してから新しい接続を開始します。802.11w MFPを使 用する場合、STAが関連付けられており、管理フレーム保護(MFP)をネゴシエートすると、APは リターンステータスコード30で関連付け要求を拒否します Association request rejected temporarily; Try again later クライアントに送信します。

アソシエーション応答には、APがこのSTAとのアソシエーションを受け入れる準備ができている ときのカムバック時間を指定するアソシエーションのカムバック時間情報要素が含まれています 。このようにして、スプーフィングされた関連付け要求が原因で正当なクライアントの関連付け が解除されないようにすることができます。

◆ 注:WLC(AireOSまたは9800)では、クライアントが802.11w PMFを使用しない場合、ク ライアントから送信された関連付け解除または認証解除フレームは無視されます。クライア ントエントリは、クライアントがPMFを使用する場合に、このようなフレームを受信した 直後にのみ削除されます。これは、PMFのないフレームにはセキュリティがないため、悪 意のあるデバイスによるサービス拒否を回避するためです。

### 802.11wを有効にするための要件

- ・ 802.11wでは、SSIDをdot1xまたはPSKのいずれかで設定する必要があります。
- 802.11wは、すべての802.11n対応APでサポートされます。これは、AP 1130および1240が 802.11wをサポートしないことを意味します。
- ・ 802.11wは、7.4リリースのflexconnect APおよび7510 WLCではサポートされません。7.5リ リースからサポートが追加されています。

## 設定

GUI

ステップ1:802.1x/PSKで設定されたSSIDで、保護された管理フレームを有効にする必要があり ます。次の図に示すように、3つのオプションがあります。

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK	Sa <u>v</u> e Configuration Ping Logou
WLANs	WLANs > Edit 'PMF'	< Back Ap
▼ WLANs WLANs	General Security QoS Advanced	
Advanced	Layer 2 Layer 3 AAA Servers	
	Layer 2 Security f WPA+WPA2  MAC Filtering	Î
	Fast Transition Fast Transition	
	Protected Management Frame PMF Disabled Y	
	WPA+WPA2 Parameters Optional Optional Required	
	WPA Policy  WPA2 Policy	
	WFA2 Endrypoon CAES TKIP Authentication Key Management	
	802.1X C Enable	
	PSK Enable	

[必須]は、802.11wをサポートしていないクライアントが接続を許可されないように指定します。 'Optional'は、802.11wをサポートしていないクライアントでも接続を許可することを指定します 。

ステップ2:次に、復帰タイマーとSAクエリーのタイムアウトを指定する必要があります。復帰 タイマーは、関連付けられたクライアントがステータスコード30で最初に拒否されたときに、関 連付けを再試行できるようになるまで待機する時間を指定します。SAクエリタイムアウトは、 WLCがクエリプロセスのためにクライアントからの応答を待機する時間を指定します。クライア ントから応答がない場合、その関連付けはコントローラから削除されます。これは、図に示すよ うに行われます。

ululu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	Sa⊻e Configuration   £ing	Logout   <u>R</u> e
WLANs	WLANs > Edit 'PMF'	< Back	Apply
VLANS	General Security QoS Advanced		
Advanced	Layer 2 Layer 3 AAA Servers		
	Layer 2 Security & WPA+WPA2 MAC Filtering & Fast Transition Fast Transition Protected Nanagement Frame PMF Required • Comeback timer(1- 20msec) SA Query Timeout(100- S00msec) WPA+WPA2 Parameters WPA Policy WPA Policy WPA2 Policy WPA2 Encryption Mags TKIP		
			ł.

ステップ 3:認証キー管理方式として802.1xを使用する場合は、「PMF 802.1x」を有効にする必要があります。PSKを使用する場合は、図に示すようにPMF PSKチェックボックスを選択する必要があります。

	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK	Sa⊻e Configuration   <u>P</u> ing	Logout   <u>B</u> efre
WLANs	WLANs > Edit 'PMF'	< Back	Apply
WLANS WLANS	General Security QoS Advanced		
P Autoliceu	SA Quer' I Imbout 100-         200           S00msec)         WPA+WPA2 Parameters           WPA Policy	•	
	WPA2 Policy     Image: Constraint of the second secon		
	802.1X     Imable       CCKM     Enable       PSK     Enable       FT 002.1X     Enable       FT PSK     Enable		
	PMF 802.1X  Enable PMF PSK Enable WPA gik-randomize State &		

### CLI を使う場合:

### • 11w機能を有効または無効にするには、次のコマンドを実行します。

config wlan security wpa akm pmf 802.1x enable/disable

config wlan security wpa akm pmf psk enable/disable

#### • 保護された管理フレームを有効または無効にするには、次のコマンドを実行します。

config wlan security pmf optional/required/disable

・ 関連付け復帰時間の設定:

#### • SAクエリ再試行タイムアウト設定:

config wlan security pmf saquery-retry-time

## 確認

ここでは、設定が正常に機能しているかどうかを確認します。

802.11wの設定は確認できます。WLAN設定をチェックします。

(wlc)>show wlan 1	
Wi-Fi Protected Access (WPA/WPA2)	Enabled
<snip></snip>	
802.1x Enable	ed
PSK Disab	led
CCKM Disab	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 20	
FT Over-The-DS mode Ena	abled
GTK Randomization Dis	sabled
<snip></snip>	
PMF	Required
PMF Association Comeback Time	1
PMF SA Query RetryTimeout	200

# トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

WLCの802.11wの問題をトラブルシューティングするには、次のdebugコマンドを使用できます。

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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。