WLCでの802.11w管理フレーム保護の設定

内容

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。

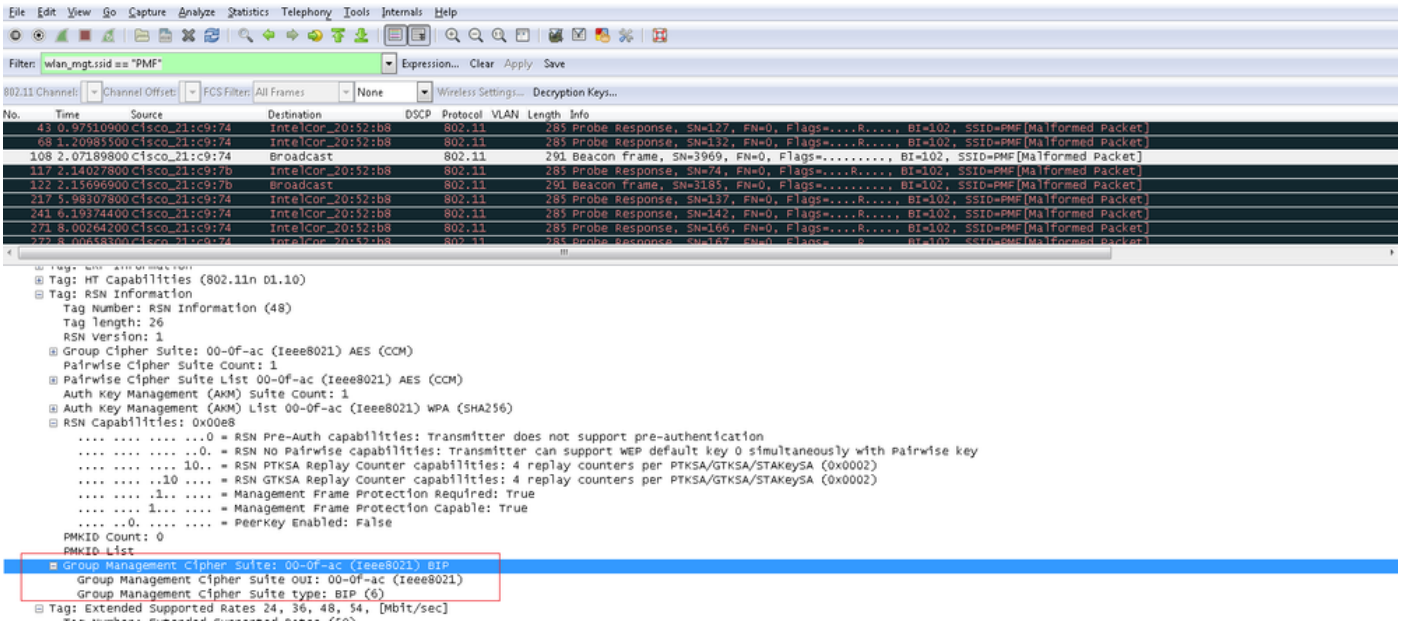
1	1	2	6	8
Element ID	Length	KeyID	IPN	MIC

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。

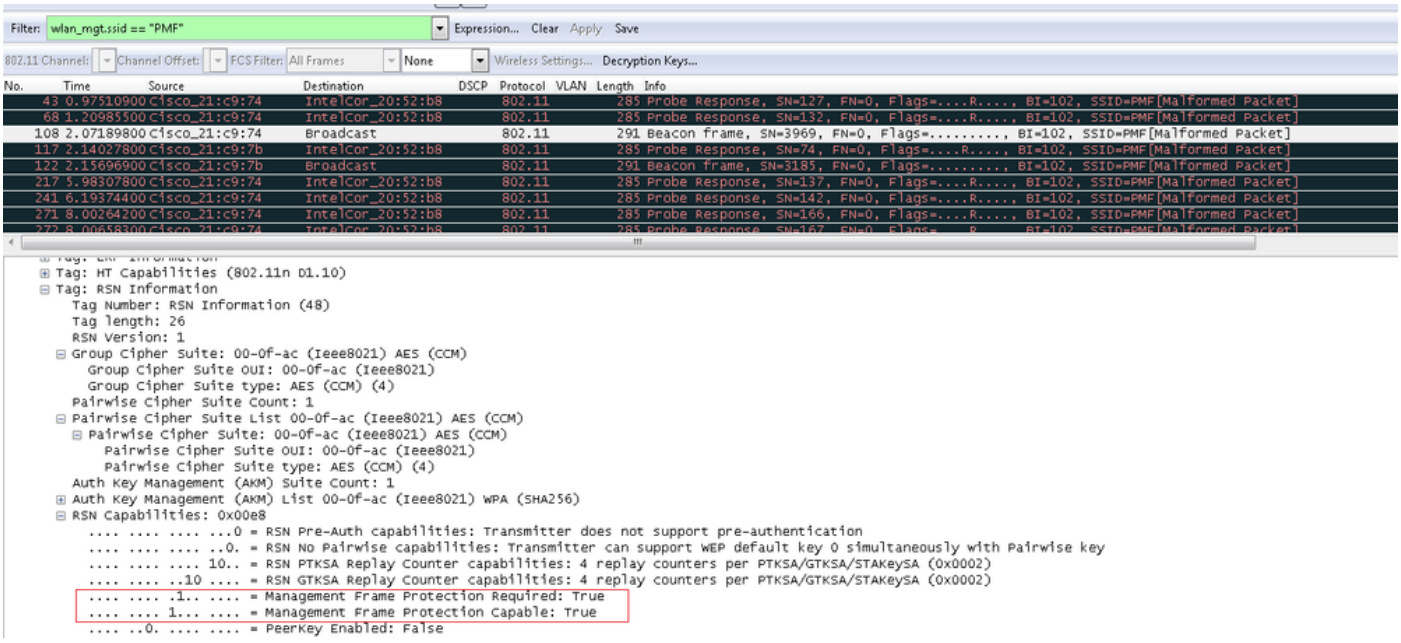


ここでは、802.11wが使用されていることを示すgroup management cipher suiteフィールドがあります。

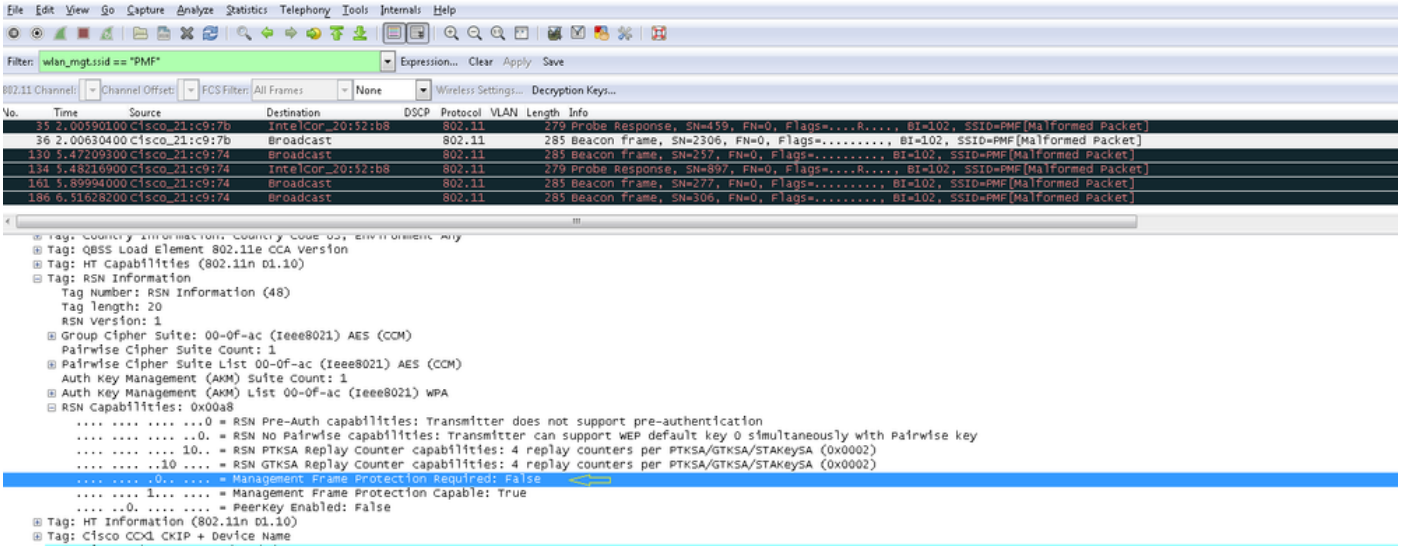
RSN機能にも変更が加えられています。ビット6と7は、802.11wの異なるパラメータを示すために使用されます。

- 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。



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。

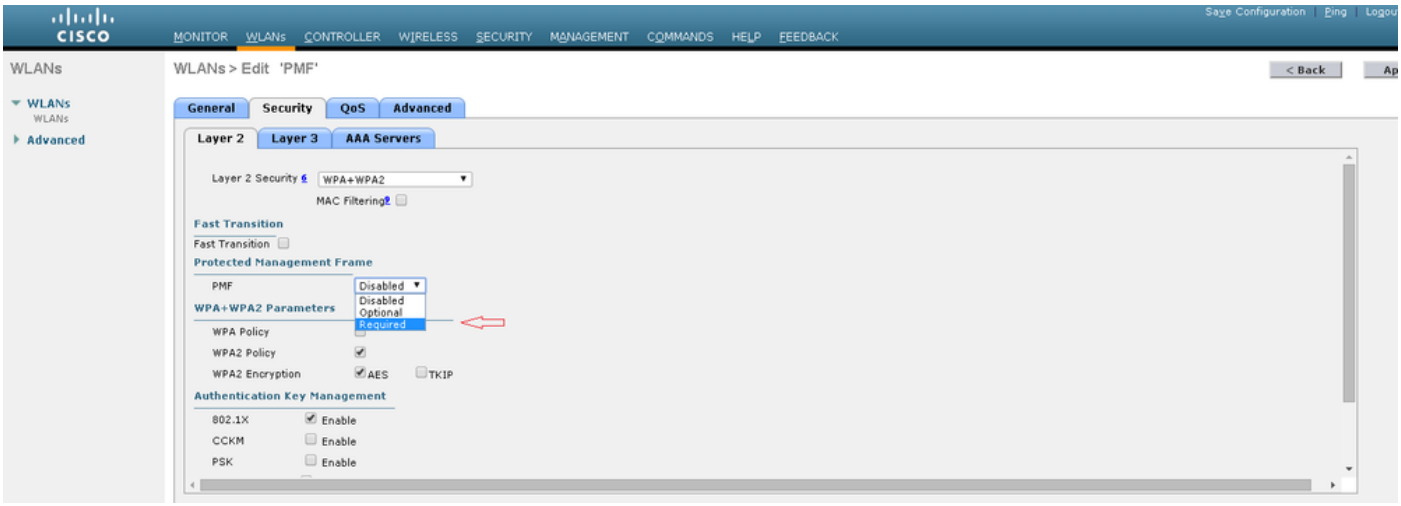
802.11wを有効にするための要件

- 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

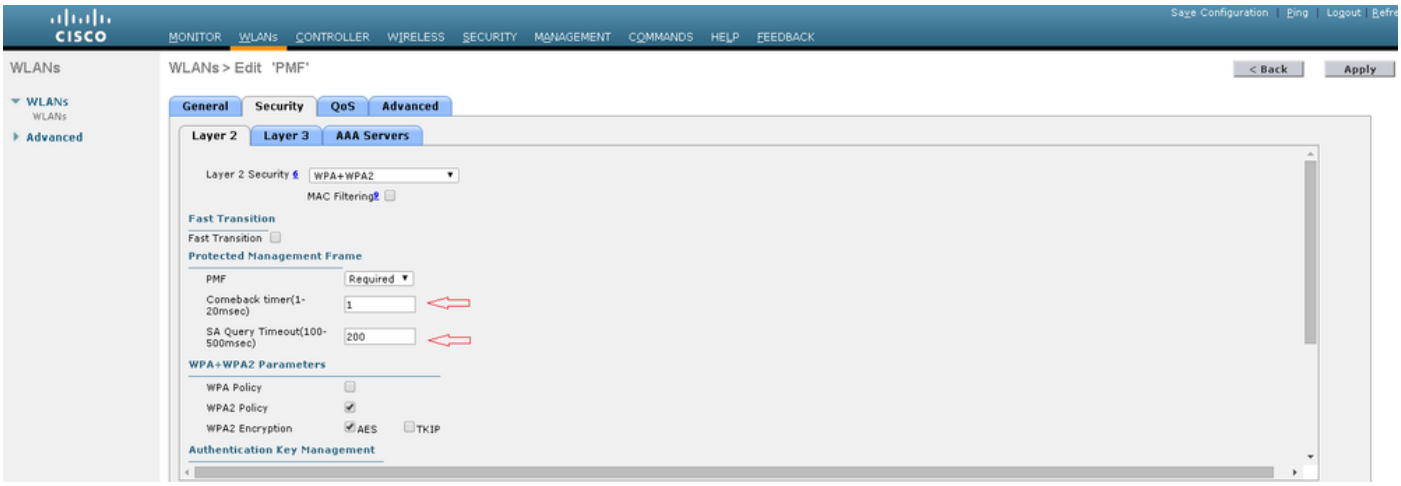
GUI

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。

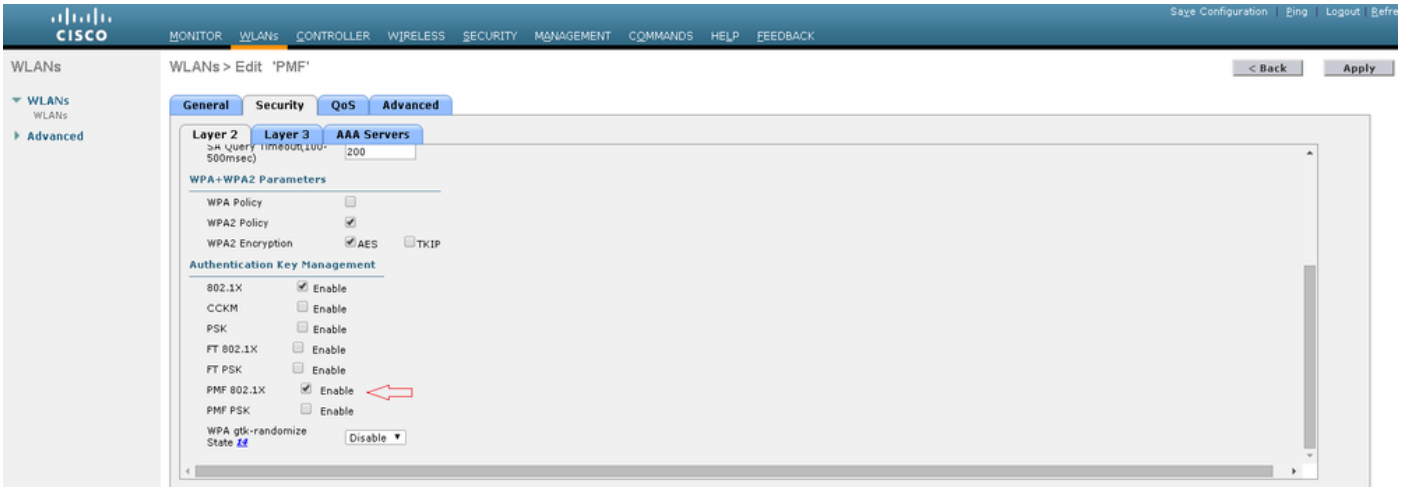


[必須]は、802.11wをサポートしていないクライアントが接続を許可されないように指定します。'Optional'は、802.11wをサポートしていないクライアントでも接続を許可することを指定します。

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。



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。



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：

config wlan security pmf 11w-association-comeback

- 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>
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
```

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。