802.11W

802.11w に関する情報

Wi-Fi は、正規のデバイスまたは不法なデバイスのいずれであっても、あらゆるデバイスで傍受または参加が可能なブロードキャストメディアです。認証、認証解除、アソシエーション、アソシエーション解除、ビーコン、プローブなどの管理フレームは、ワイヤレスクライアントがネットワーク サービスのセッションを開始および切断するために使用します。暗号化により、一定レベルの機密保持を実現できるデータ トラフィックとは異なり、これらのフレームはすべてのクライアントによって受信および解釈される必要があるため、オープンまたは非暗号化形式で送信されます。これらのフレームは暗号化できませんが、攻撃から無線メディアを保護するために偽造を防止することが必要になります。たとえば、攻撃者は AP にアソシエートされたクライアントを攻撃するために、AP からの管理フレームをスプーフィングする可能性があります。

802.11w プロトコルは、保護管理フレーム（PMF）サービスによって保護された一連の堅牢な管理フレームにのみ適用されます。これには、アソシエーション解除フレーム、認証解除フレーム、ロバスト アクション フレームなどが含まれます。

したがって、ロバストアクションであり、保護されているものと見なされる管理フレームは次のとおりです。

- スペクトル管理
- QoS
- DLS
- ブロック ACK

- 無線測定
- 高速 BSS 移行
- SA クエリ
- 保護されたデュアル パブリック アクション
- ベンダー固有保護

802.11w が無線メディアで実行されると、次のことが行われます。

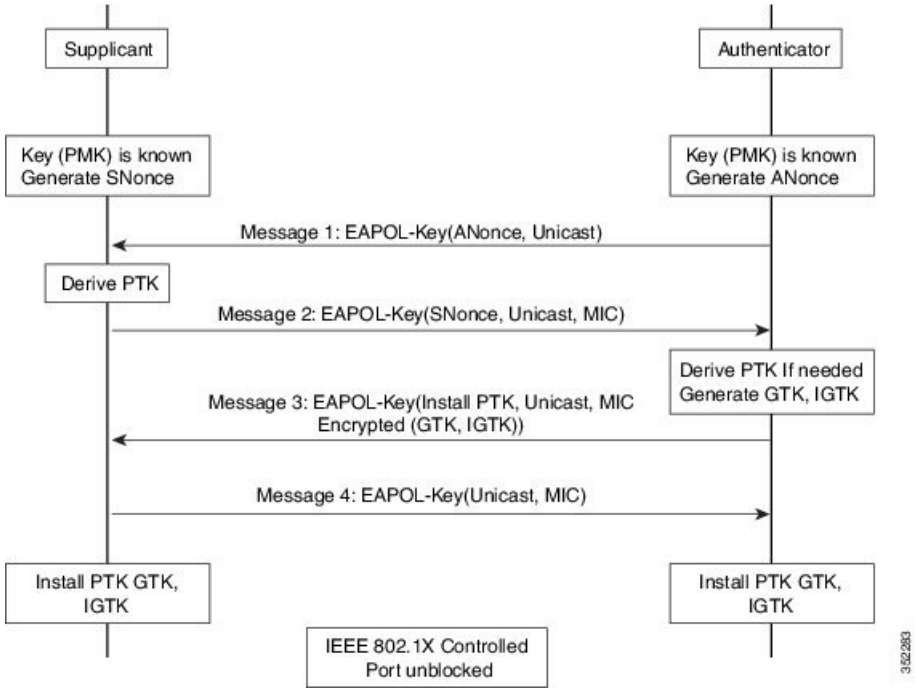
- AP が認証解除フレームと関連付け解除フレームに暗号保護を追加することでクライアント保護が追加され、DoS 攻撃でのスプーフィングを阻止します。
- アソシエーション復帰期間とセキュリティ アソシエーション（SA）クエリの手順で構成される SA ティアダウン保護メカニズムを追加することでインフラストラクチャ保護が追加され、スプーフィングされたアソシエーション要求によって接続済みのクライアントが切断されることを阻止します。

802.11w で新たに導入された IGTK 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。

- IGTK はオーセンティケータ STA（WLC）によって割り当てられるランダムな値で、ソース STA からの MAC 管理プロトコル データ ユニット（MMPDU）を保護するために使用されます。

管理フレーム保護のネゴシエーション時に、AP は 4 ウェイ ハンドシェイクのメッセージ 3 で送信される EAPOL キー フレーム内の GTK 値と IGTK 値を暗号化します。

図 *1 : 4* ウェイ ハンドシェイクでの *IGTK* 交換

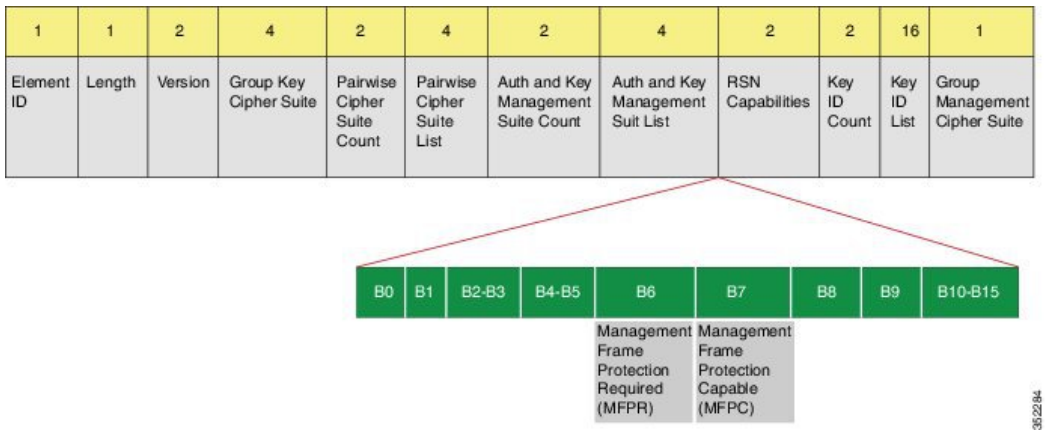


- AP は後で GTK を変更した場合には、グループ キー ハンドシェイクを使用して新しい GTK と IGTK をクライアントに送信します。

802.11w では、新たに Broadcast/Multicast Integrity Protocol（BIP）が定義されています。このプロトコルは、IGTKSA が正常に確立された後、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におけるデータの整合性、およびリプレイ保護を提供し、共有 IGTK キーを使用して計算される MIC を追加します。

802.11w の情報要素（IE）

図 *2 : 802.11w* の情報要素



1. RSNIE の RSN 機能フィールドに変更が加えられています。

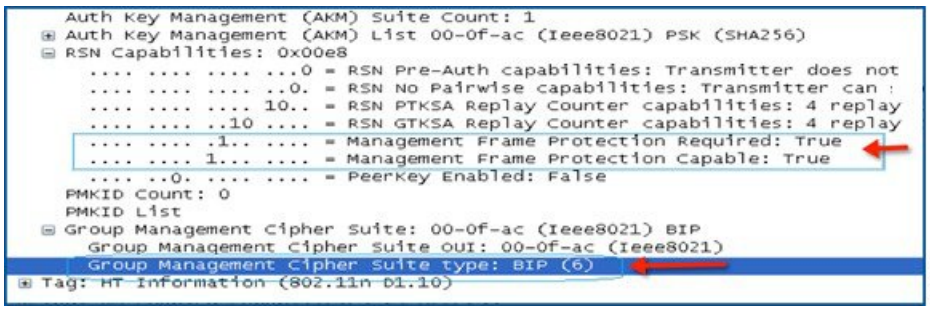
1. ビット 6：Management Frame Protection Required（MFPR）
2. ビット 7：Management Frame Protection Capable（MFPC）

2. 2 つの新しい AKM スイート 5 および 6 が AKM スイート セレクタ用に追加されています。
3. BIP に対応するため、タイプ 6 の新たな暗号スイートが追加されました。

この変更された RSNIE を WLC はアソシエーション応答と再アソシエーション応答に追加し、AP はビーコン応答とプローブ応答に追加します。

次の Wireshark キャプチャ画面は、RSNIE 機能とグループ管理暗号スイートの要素を示します。

図 *3 : 802.11w* の情報要素



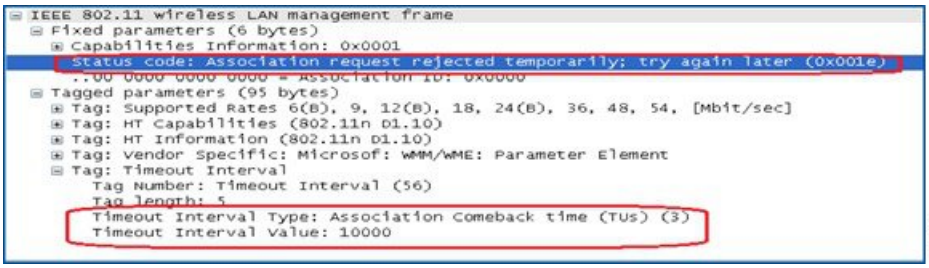
セキュリティ アソシエーション（SA）ティアダウン保護

SA ティアダウン保護は、リプレイ攻撃によって既存のクライアントのセッションが切断されるのを防止するメカニズムです。アソシエーションの復帰期間と SA クエリの手順を組み合わせることで、スプーフィングされたアソシエーション要求により、接続済みのクライアントが切断されることを防止します。

クライアントが有効なセキュリティ アソシエーションを有し、802.11w をネゴシエートしている場合は、AP はステータス コード 30 を使用して、新たなアソシエーション要求を拒否します。このステータス コードは、「アソシエーション要求が一時的に拒否されました。後でやり直してください」ということを意味します。AP は、SA クエリ手順によって元の SA が無効であると判断されない限り、既存アソシエーションを切断したり、その状態を変更したりすることはできません。また、APのアソシエーション応答には、APがこのクライアントとのアソシエーションを受け入れる準備が整うまでの時間を指定したアソシエーション復帰期間の情報要素が含められます。

次の図は、ステータス コード 0x1e（30）のアソシエーション拒否メッセージと、10 秒に設定されたアソシエーション復帰期間を示しています。

図 *4:* アソシエーション拒否と復帰期間



クライアントとの SA クエリがまだ実行されていない場合、AP は一致する SA クエリ応答を受信するか、アソシエーション復帰期間が経過するまで、SA クエリを発行します。AP は有効な保護フレームを受信すると、SA クエリが正常に完了したと解釈します。

一致するトランザクション識別子を含む SA クエリ応答が期間内に行われると、AP は追加の SA クエリ手順を開始せずに、アソシエーション プロセスの開始を許可します。

802.11w の前提条件

- 任意および必須の 802.11w 機能を設定するには、WPA および AKM を設定する必要があります。

> 注 Robust Secure Network（RNS）IE は AES 暗号化とともにイネーブルにする必要があります。

- 必須として 802.11w を設定するには、WPA AKM に加えて PMF AKM を有効にします。

802.11w の制約事項

- 802.11w はオープン WLAN、 WEP 暗号化 WLAN、または TKIP 暗号化 WLAN に適用されていません。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ Apple 以外のクライアントに対しては、802.11w + PMF の組み合わせがサポートされています。ただし、Apple iOS バージョン 11 以前で関連付けの問題を解決するには、Apple iOS 側からの修正が必要です。
- クライアントで802.11wPMFが使用されていない場合、コントローラは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を無視します。クライアントで PMF が使用されている場合、クライアントエントリは該当フレームを受信した場合のみすぐに削除されます。これは、PMFのないフレームは安全ではないため、悪意のあるデバイスによるサービス妨害を回避するためです。

802.11w の設定方法

802.11w の設定（GUI）

始める前に

WPA および AKM を設定する必要があります。

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。

ステップ 2 [Add] をクリックして WLAN を作成します。

[Add WLAN] ページが表示されます。

ステップ 3 **[Security]** > **[Layer2]** タブで、[Protected Management Frame] セクションに移動します。

ステップ 4 [PMF] で [Disabled]、[Optional]、または [Required] を選択します。デフォルトでは、PMF は無効になっています。

[PMF] で [Optional]、または [Required] を選択した場合は、次のフィールドが表示されます。

- [Association Comeback Timer]：1 ～ 10 秒の値を入力して、802.11w のアソシエーション復帰期間を設定します。
- [SA Query Time]：100 ～ 500（ミリ秒）の値を入力します。これは、クライアントが WLAN の 802.11w PMF 保護をネゴシエートするために必要です。

ステップ 5 [Save & Apply to Device] をクリックします。

802.11w の設定（CLI）

始める前に

WPA および AKM を設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**wlan** *profile-name wlan-id ssid* 例： `Device(config)# wlan wlan-test 12 alpha`	WLANを設定し、コンフィギュレーション モードを開始します。
ステップ 3	**security wpa akm pmf dot1x** 例： `Device(config-wlan)#security wpa akm pmf dot1x`	802.1x のサポートを設定します。
ステップ 4	**security pmf association-comeback** *comeback-interval* 例： `Device(config-wlan)# security pmf association-comeback 10`	802.11wアソシエーション復帰時間を設定します。
ステップ 5	**security pmf mandatory** 例： `Device(config-wlan)# security pmf mandatory`	クライアントが WLAN の 802.11w PMF 保護をネゴシエートすることを要求します。
ステップ 6	**security pmf saquery-retry-time** *timeout* 例： `Device(config-wlan)# security pmf saquery-retry-time 100`	SA クエリ応答を受け取るまでの時間（ミリ秒単位）です。デバイスが応答を受け取らなかった場合、別の SQ クエリが試行されます。

802.11w の無効化

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name wlan-id ssid* 例： `Device(config)# wlan wlan-test 12 alpha`	WLANを設定し、コンフィギュレーション モードを開始します。
ステップ 3	**no security wpa akm pmf dot1x** 例： `Device(config-wlan)# no security wpa akm pmf dot1x`	802.1x サポートを無効にします。

	コマンドまたはアクション	目的
ステップ 4	**no security pmf association-comeback** *comeback-interval* 例： `Device(config-wlan)# no security pmf association-comeback 10`	802.11wのアソシエーション復帰期間を無効にします。
ステップ 5	**no security pmf mandatory** 例： `Device(config-wlan)# no security pmf mandatory`	クライアントによる WLAN の 802.11w PMF 保護のネゴシエートを無効にします。
ステップ 6	**no security pmf saquery-retry-time** *timeout* 例： `Device(config-wlan)# no security pmf saquery-retry-time 100`	SQ クエリの再試行を無効にします。

802.11w のモニターリング

802.11w をモニターリングするには、次のコマンドを使用します。

手順

ステップ 1 **show wlan name** *wlan-name*

WLAN の WLAN パラメータを表示します。PMF パラメータが表示されます。

```
. . . .
. . . .
Auth Key Management
            802.1x                              : Disabled
            PSK                                 : Disabled
            CCKM                                : Disabled
            FT dot1x                            : Disabled
            FT PSK                              : Disabled
            FT SAE                              : Disabled
            Dot1x-SHA256                        : Enabled
            PSK-SHA256                          : Disabled
            SAE                                 : Disabled
            OWE                                 : Disabled
            SUITEB-1X                           : Disabled
            SUITEB192-1X                        : Disabled
    CCKM TSF Tolerance                          : 1000
    FT Support                                  : Adaptive
        FT Reassociation Timeout                : 20
        FT Over-The-DS mode                     : Enabled
    PMF Support                                 : Required
        PMF Association Comeback Timeout        : 1
        PMF SA Query Time                       : 500
```

```
. . . .
. . . .
```

ステップ 2 **show wireless client mac-address** *mac-address***detail**

クライアントの 802.11w 認証キー管理設定の概要を表示します。

```
. . . .
. . . .
Policy Manager State: Run
NPU Fast Fast Notified : No
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 497 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : 802.1x-SHA256
Encrypted Traffic Analytics : No
Management Frame Protection : No
Protected Management Frame - 802.11w : Yes
EAP Type : LEAP
VLAN : 39
Multicast VLAN : 0
Access VLAN : 39
Anchor VLAN : 0
WFD capable : No
Manged WFD capable : No
. . . .
. . . .
```