レイヤ 2 セキュリティの設定

レイヤ 2 セキュリティの前提条件

同じ SSID を持つ WLAN は、ビーコン応答とプローブ応答でアドバタイズされる情報に基づいてクライアントが WLAN を選択できるように、一意のレイヤ 2 セキュリティ ポリシーを使用している必要があります。 使用可能なレイヤ 2 セキュリティ ポリシーは、次のとおりです。

- なし（オープン WLAN）
- Static WEP または 802.1X

（注） Static WEP と 802.1X は両方とも、ビーコン応答とプローブ応答で同じビットによってアドバタイズされるので、クライアントはこれらを区別できません。したがって、同じ SSID を持つ複数の WLAN では、Static WEP と 802.1X の両方を使用できません。

- CKIP
- WPA/WPA2

（注） 同じ SSID を持つ複数の WLAN で WPA と WPA2 を使用することはできませんが、同じ SSID を持つ 2 つの WLAN は、PSK を使用する WPA/TKIP と 802.1X を使用する Wi-Fi Protected Access（WPA）/Temporal Key Integrity Protocol（WPA）で設定するか、802.1X を使用する WPA/TKIP または 802.1X を使用する WPA/AES で設定することができます。

Static WEP キーの設定（CLI）

コントローラでは、アクセス ポイント上で Static WEP キーを制御できます。 WLAN の Static WEP を設定するには、次のコマンドを使用します。

- 次のコマンドを入力して、802.1X 暗号化を無効にします。

  config wlan security 802.1X *disable wlan_id*

- 次のコマンドを入力して、40/64 ビットまたは 104/128 ビット WEP キーを設定します。

  config wlan security static-wep-key encryption *wlan_id* {**40** | **104**} {**hex** | **ascii**} **key** *key_index*

  - 40/64 ビットまたは 104/128 ビット暗号化を指定するには、**40** または **104** オプションを使用します。 デフォルトの設定は、104/128 です。
  - WEP キーの文字形式を指定するには、**hex** または **ascii** オプションを使用します。
  - 40 ビット/64 ビット WEP キーの場合は 10 桁の 16 進数（0 ～ 9、a ～ f、または A ～ F の組み合わせ）または印刷可能な 5 つの ASCII 文字を入力します。または、104 ビット/128 ビット キーの場合は 26 桁の 16 進数または 13 の ASCII 文字を入力します。
  - キー インデックス（キー スロットとも呼ばれます）を入力します。 デフォルト値は 0 で、これはキー インデックス 1 に相当します。有効な値は 0 ～ 3（キー インデックス 1 ～ 4）です。

802.1X 動的キーおよび許可の設定（CLI）

コントローラでは、アクセス ポイント上で Extensible Authentication Protocol（EAP; 拡張認証プロトコル）を使用する 802.1X Dynamic WEP キーを制御できます。また、WLAN の 802.1X ダイナミック キー設定をサポートしています。

（注） Lightweight アクセス ポイントとワイヤレス クライアントで LEAP を使用するには、CiscoSecure Access Control Server（ACS）を設定する際に RADIUS サーバ タイプとして [Cisco-Aironet] を選択することを確認します。

- 各無線 LAN のセキュリティ設定を確認するには、次のコマンドを入力します。

  show wlan *wlan_id*

  新しい WLAN のデフォルトのセキュリティ設定は、ダイナミック キーが有効な 802.1X です。 レイヤ 2 の堅牢なポリシーを維持するには、802.1X を WLAN 上で設定したままにします。

- 次のコマンドを入力して、802.1X 暗号化を無効または有効にします。

  config wlan security 802.1X {**enable** | **disable**} *wlan_id*

  802.1X認証を有効にした後、コントローラから、ワイヤレスクライアントと認証サーバとの間で EAP 認証パケットが送信されます。 このコマンドにより、すべての EAP タイプのパケットは、コントローラとの送受信が可能になります。

  （注） コントローラは、同じ WLAN で Web 認証と 802.1X 認証の両方を実行します。 クライアントは、最初に 802.1x で認証されます。 認証が成功すると、クライアントは、Web 認証クレデンシャルを提供する必要があります。 Web 認証が成功すると、クライアントは RUN 状態に移行します。

- 次のコマンドを入力して、WLAN の 802.1X 暗号化レベルを変更します。

  config wlan security 802.1X encryption *wlan_id* **[0 | 40 | 104]**

  - 802.1X 暗号化なしを指定するには、**0** オプションを使用します。
  - 40/64 ビット暗号化を指定するには、**40** オプションを使用します。
  - 104/128 ビット暗号化を指定するには、**104** オプションを使用します （これは、デフォルトの暗号化設定です）。

802.11r BSS の高速移行の設定

802.11r 高速移行の制約事項

- この機能はメッシュ アクセス ポイントでサポートされません。
- FlexConnect モードのアクセス ポイントの場合、
  - 802.11r 高速移行は、中央でスイッチされる WLAN とローカルにスイッチされる WLAN でのみサポートされます。
  - この機能は、ローカル認証が有効になっている WLAN ではサポートされません。
- この機能は、Cisco 600 シリーズ OfficeExtend アクセス ポイントなどの Linux ベースの AP ではサポートされません。

- 802.11r クライアント アソシエーションは、スタンドアロン モードのアクセス ポイントではサポートされません。
- 802.11r 高速ローミングは、スタンドアロン モードのアクセス ポイントではサポートされません。
- ローカル認証 WLAN と中央認証 WLAN 間の 802.11r 高速ローミングはサポートされていません。
- クライアントがスタンドアロン モードの Over-the-DS 事前認証を使用する場合、802.11r 高速ローミングはサポートされません。
- EAP LEAP 方式はサポートされません。 WAN リンク遅延は、最大 2 秒間にアソシエーション時間を抑制します。
- スタンドアロン AP からクライアントへのサービスは、セッション タイマーが切れるまでサポートされます。
- TSpec は 802.11r 高速ローミングではサポートされません。 したがって、RIC IE の処理はサポートされません。
- WAN リンク遅延がある場合、高速ローミングも遅延します。 音声またはデータの最大遅延を確認する必要があります。 コントローラは、Over-the-Air および Over-the-DS の両方の方式をローミングする間、802.11r 高速移行の認証要求を処理します。
- この機能は、オープンで WPA2 設定の WLAN でのみサポートされます。
- レガシー クライアントは、Robust Security Network Information Exchange（RSN IE）の解析を担当するサプリカントのドライバが古く、IE 内の追加 AKM を認識しない場合、802.11r が有効にされている WLAN にアソシエートできません。 この制限のため、クライアントは、WLAN にアソシエーション要求を送信できません。 ただし、これらのクライアントは、非 802.11r WLAN とアソシエートできます。 802.11r 対応クライアントは、802.11r と 802.11i の両方の認証キー管理スイートが有効にされている WLAN の 802.11i クライアントとしてアソシエートできます。

  回避策は、レガシー クライアントのドライバを新しい 802.11r AKM で動作するようにするか、またはアップグレードすることです。そうすることで、レガシークライアントは、802.11r 対応 WLAN と正常にアソシエートできます。

  もう 1 つの回避策は、同じ名前で異なるセキュリティ設定（FT および非 FT）の 2 つの SSID を持つことです。
- 高速移行のリソース要求プロトコルは、クライアントがこのプロトコルをサポートしていないため、サポートされません。 また、リソース要求プロトコルはオプションのプロトコルです。
- サービス不能（DoS）攻撃を回避するため、各コントローラでは、異なる AP と最大 3 つの高速移行ハンドシェイクが可能です。

802.11r の高速移行について

高速ローミングの IEEE 標準である 802.11r は、クライアントがターゲット AP にローミングする前でも、新しい AP との最初のハンドシェイクが実行される、高速移行（FT）と呼ばれるローミングの新しい概念が導入されています。 初期ハンドシェイクによって、クライアントと AP が事前に Pairwise Transient Key（PTK）計算をできるようになります。 これらの PTK キーは、クライアントが新しいターゲット AP の再アソシエーション要求または応答の交換をした後で、クライアントと AP に適用されます。

802.11r は、次の 2 通りのローミングを提供します。

- 無線
- Over-the-DS（分散システム）

FT キー階層は、クライアントが各 AP での再認証なしで、AP 間の高速 BSS 移行ができるように設計されています。 WLAN設定には、FT（高速移行）と呼ばれる、新しい認証キー管理（AKM）タイプが含まれています。

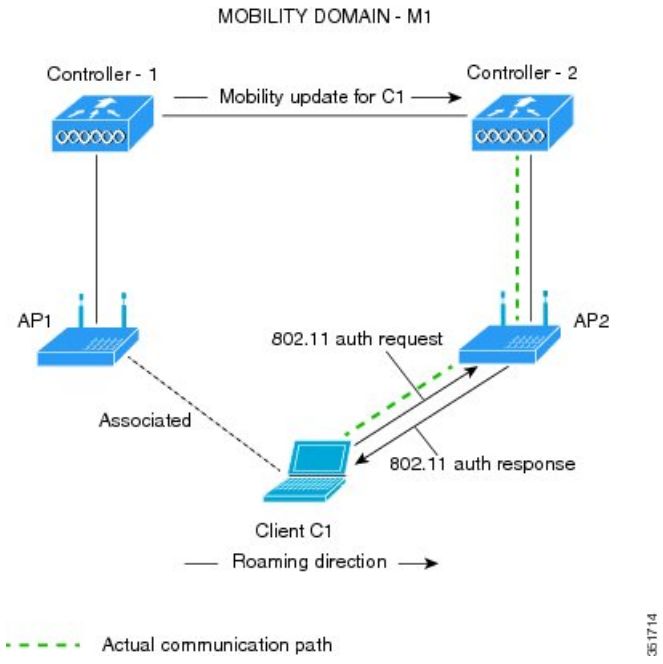
クライアントのローミング方法

FT プロトコルを使用して現在の AP からターゲット AP に移動するクライアントでは、メッセージ交換は次の 2 つの方法のいずれかを使用して行われます。

- 無線：クライアントは、FT 認証アルゴリズムを使用する IEEE 802.11 認証を使用して、ターゲット AP と直接通信を行います。
- Over-the-DS：クライアントは、現在の AP を介してターゲット AP と通信します。 クライアントとターゲット AP との間の通信は、クライアントと現在の AP 間の FT アクション フレームで実行されてから、コントローラによって送信されます。

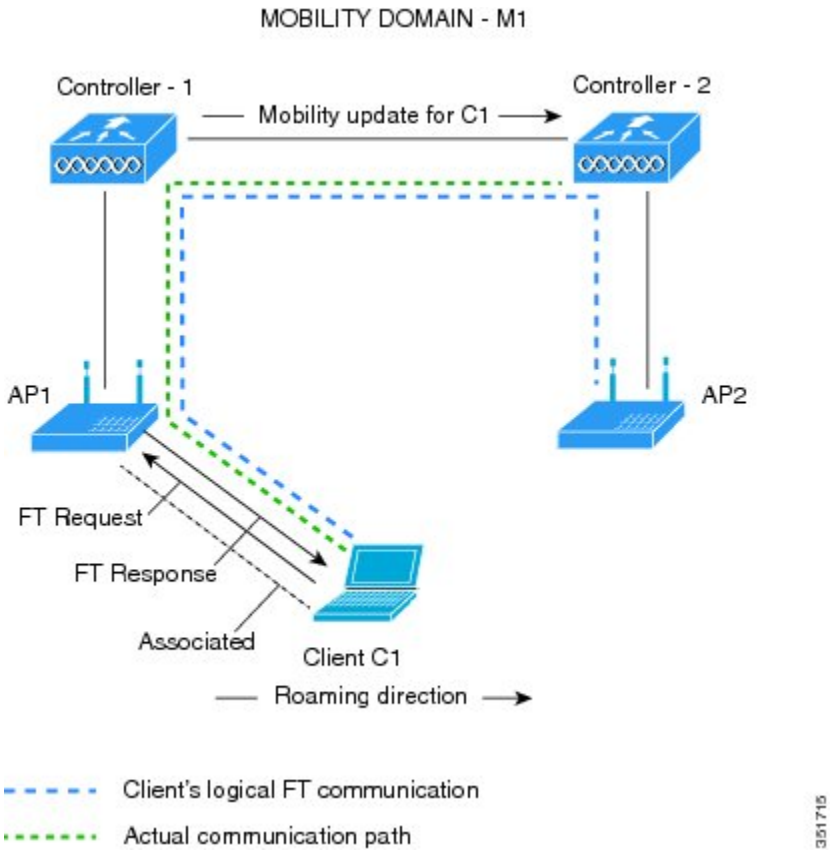
この図は、Over the Air クライアントのローミングを設定するときに実行されるメッセージ交換のシーケンスを示します。

図 1 : *Over the Air* クライアント ローミング設定時のメッセージ交換



この図は、Over the DS クライアントのローミングを設定するときに実行されるメッセージ交換のシーケンスを示します。

図 2：***Over the DS*** **クライアント ローミング設定時のメッセージ交換**



802.11r の高速移行の設定（GUI）

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 WLAN ID をクリックして、[WLANs > Edit] ページを開きます。

ステップ 3 [Security] > [Layer 2] タブを選択します。

ステップ 4 [Layer 2 Security] ドロップダウン リストから、[WPA+WPA2] を選択します。
高速移行の認証キーの管理パラメータが表示されます。

ステップ 5 [Fast Transition] チェックボックスを選択または選択解除して、WLAN の高速移行を有効または無効にします。

ステップ 6 [Over the DS] チェックボックスを選択または選択解除して、分散システム経由の高速移行を有効または無効にします。
このオプションは、高速移行を有効にした場合だけ使用できます。

ステップ 7 [Reassociation Timeout] ボックスに、AP へのクライアントの再アソシエーション試行がタイムアウトになる秒数を入力します。
有効範囲は 1 ～ 100 秒です。

このオプションは、高速移行を有効にした場合だけ使用できます。

ステップ 8 認証キー管理の場合は、[FT 802.1X] 、または [FT PSK] を選択します。 対応するチェックボックスを選択するかまたは選択解除して、キーを有効または無効にします。 [FT PSK] チェックボックスを選択する場合、[PSK Format] ドロップダウン リストから [ASCII] または [Hex] を選択して、キー値を入力します。

ステップ 9 [WPA gtk-randomize State] ドロップダウン リストで [Enable] または [Disable] を選択して、WPA グループの一時的なキー（GTK）randomize state を設定します。

ステップ 10 [Apply] をクリックして設定値を保存します。

802.11r の高速移行の設定（CLI）

ステップ 1 802.11r 高速移行パラメータを有効または無効にするには、**config wlan security ft** {**enable** | **disable**} *wlan-id* コマンドを使用します。
デフォルトで、高速移行は無効です。

ステップ 2 分散システム上の 802.11r 高速移行パラメータを有効または無効にするには、**config wlan security ft over-the-ds** {**enable** | **disable**} *wlan-id* コマンドを使用します。
デフォルトで、分散システム上の高速移行は無効です。

ステップ 3 事前共有キー（PSK）を使用した高速移行の認証キー管理を有効または無効にするには、**config wlan security wpa akm ft-psk** {**enable** | **disable**} *wlan-id* コマンドを使用します。
デフォルトで、PSK を使用した認証キー管理は無効です。

ステップ 4 802.1X を使用した高速移行の認証キー管理を有効または無効にするには、**config wlan security wpa akm ft-802.1X** {**enable** | **disable**} *wlan-id* コマンドを使用します。
デフォルトで、802.1X を使用した認証キー管理は無効です。

ステップ 5 802.11r 高速移行の再アソシエーション タイムアウトを有効または無効にするには、**config wlan security ft reassociation-timeout***timeout-in-seconds wlan-id* コマンドを使用します。
有効範囲は 1 ～ 100 秒です。 再アソシエーション タイムアウトのデフォルト値は 20 秒です。

ステップ 6 分散システム上の高速移行の認証キー管理を有効または無効にするには、**config wlan security wpa akm ft over-the-ds** {**enable** | **disable**} *wlan-id* コマンドを使用します。
デフォルトで、分散システム上の高速移行の認証キー管理は無効です。

ステップ 7 クライアントの高速移行の設定を表示するには、**show client detailed** *client-mac* コマンドを使用します。

ステップ 8 WLAN の高速移行の設定を表示するには、**show wlan** *wlan-id* コマンドを使用します。

ステップ 9 高速移行イベントのデバッグを有効または無効にするには、**debug ft events** {**enable** | **disable**} コマンドを使用します。

ステップ 10 高速移行のキー生成のデバッグを有効または無効にするには、**debug ft keys** {**enable** | **disable**} コマンドを使用します。

802.11r BSS の高速移行のトラブルシューティング

症状	解決策
非 802.11r レガシー クライアントはすでに接続していません。	WLAN で FT が有効であるかどうかを確認します。 その場合、非 FT WLAN が作成される必要があります。
WLAN を設定する場合、FT 設定オプションは表示されません。	WPA2 を使用されているかどうかを確認します（802.1x/PSK）。 FT は WPA2 SSID およびオープン SSID だけでサポートされます。
802.11r クライアントは、新しいコントローラにレイヤ 2 のローミングを実行するときに、再認証するとおもわれます。	コントローラの GUI で、[WLANs] > [WLAN Name] > [Security] > [Layer 2] と移動して、再認証タイムアウトがデフォルトの 20 よりも小さくなっているかどうか確認します。

802.1X 認証への MAC 認証フェールオーバーの設定

クライアントに対する Static WEP による MAC 認証が失敗したときに、802.1X 認証を開始するようにコントローラを設定できます。 RADIUS サーバが、クライアントを認証解除する代わりにクライアントからのアクセス要求を拒否した場合、コントローラは802.1X認証を受けることをクライアントに強制できます。 クライアントが 802.1X 認証にも失敗した場合、クライアントは認証解除されます。

MAC 認証が成功し、クライアントが 802.1X 認証を要求する場合、クライアントがデータ トラフィックの送信を許可されるには、802.1X 認証をパスする必要があります。 クライアントが 802.1X 認証を選択しない場合、クライアントが MAC 認証にパスすれば、クライアントは認証を宣言されます。

802.1X 認証への MAC 認証フェールオーバーの設定（GUI）

ステップ 1 [WLANs] > [WLAN ID]を選択して、[WLANs > Edit] ページを開きます。

ステップ 2 [Security] タブで、[Layer 2] タブをクリックします。

ステップ 3 [MAC Filtering] チェックボックスを選択します。

ステップ 4 [Mac Auth or Dot1x] チェックボックスをオンにします。

802.1X 認証への MAC 認証フェールオーバーの設定（CLI）

802.1X 認証への MAC 認証フェールオーバーを設定するには、次のコマンドを入力します。
config wlan security 802.1X on-macfilter-failure {**enable** | **disable**} *wlan-id*

802.11w の設定

802.11w の制約事項

- Cisco の従来の管理フレーム保護は 7.4 リリースで実装されている 802.11w 標準には関連しません。
- 802.11w 標準は FlexConnect の動作が設定されたものを除くすべての 802.11n 対応 AP でサポートされます。
- 802.11w 標準は、Cisco ワイヤレス LAN コントローラのモデル シリーズ、2500、5500、8500、および WiSM2 でサポートされています。

  802.11w 標準は、Cisco ワイヤレス LAN コントローラのモデル、Flex 7500 と仮想 Wireless LAN Controller でサポートされていません。
- 802.11w がオプションに設定され、キーが設定されている場合、AKM スイートには依然として、802.11w が無効として示されます。これは、Wi-Fi の制限です。
- 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。

- 802.11w が設定された WLAN では、WPA2-PSK または WPA2-802.1x セキュリティを設定する必要があります。

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/ディスアソシエーション、ビーコンおよびプローブなどの制御/管理フレームは、無線クライアントによって、AP を選択し、ネットワーク サービスのセッションを開始するために使用されます。

機密保持レベルを提供する暗号化可能なデータ 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解釈されることが必要であり、したがって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、攻撃者はクライアントと AP の間のセッションを切断するために、AP から管理フレームをスプーフィングする可能性があります。

管理フレーム保護のための 802.11w 標準が 7.4 リリースに実装されています。

802.11w プロトコルは、管理フレーム保護（PMF）サービスによって保護された一連の強力な管理フレームにのみ適用されます。 これらには、ディスアソシエーション、認証解除、ロバストアクション フレームが含まれます。

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。

- スペクトラム管理
- QoS
- DLS
- ブロック ACK
- 無線測定
- 高速 BSS 移行
- SA クエリー
- 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。

- ディスアソシエーション フレームと認証解除フレームに対して、（MIC 情報要素を含めることにより）AP の暗号保護によるクライアント保護が追加されます。これによって、DoS 攻撃でのスプーフが防止されます。
- アソシエーションの復帰期間と SA クエリーの手順から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を追加することによって、インフラストラクチャ

の保護が追加され、スプーフィングされた要求によるすでに接続済みのクライアントの切断が防止されます。

802.11w の設定（GUI）

ステップ 1 [WLANs] > [WLAN ID] の順に選択して、[WLANs > Edit] ページを開きます。

ステップ 2 [Security] タブで、[Layer 2] セキュリティ タブを選択します。

ステップ 3 [Layer 2 Security] ドロップダウン リストから、[WPA+WPA2] を選択します。
802.11w IGTK キーはフォーウェイ ハンドシェークを使用して生成されます。つまり、レイヤ 2 で WPA2 セキュリティ用に設定された WLAN でのみ使用できます。

（注） WPA2 は必須であり、暗号化タイプは AES である必要があります。 TKIP は無効です。

ステップ 4 ドロップダウン リストから PMF 状態を選択します。
次のオプションを使用できます。

- [Disabled]：WLAN での 802.11w MFP 保護を無効にします。
- [Optional]：クライアントが 802.11w をサポートしている場合に使用します。
- [Required]：802.11w をサポートしていないクライアントが WLAN とアソシエートできないようにします。

ステップ 5 PMF 状態を [Optional] または [Required] のいずれかとして選択する場合、次を行います。

a) [Comeback Timer] ボックスに、Association Comeback の間隔をミリ秒単位で入力します。 これは、有効なセキュリティ アソシエーションの後に、アクセス ポイントがクライアントと再度アソシエーションする期間です。

b) [SA Query Timeout] ボックスに、Security Association（SA）クエリーがタイム アウトするまでの最大時間を入力します。

ステップ 6 [Authentication Key Management] セクションで、次の手順を実行します。

a) [PMF 802.1X] チェックボックスをオンまたはオフにして、管理フレームを保護するために 802.1X 認証を設定します。

b) [PMF PSK] チェックボックスをオンまたはオフにして、PMF 用に事前共有されているキーを設定します。 PSK フォーマットには ASCII または 16 進数のいずれかを選択し、PSK を入力します。

ステップ 7 [Apply] をクリックします。

ステップ 8 [Save Configuration] をクリックします。

802.11w の設定（CLI）

- 次のコマンドを入力して、PMF の 802.1X 認証を設定します。
  config wlan security wpa akm pmf 802.1x {**enable** | **disable**} *wlan-id*
- 次のコマンドを入力して、PMF の事前共有キーのサポートを設定します。
  config wlan security wpa akm pmf psk {**enable** | **disable**} *wlan-id*
- 完了しない場合、次のコマンドを入力して、WLAN の事前共有キーを設定します。
  config wlan security wpa akm psk set-key {*ascii* | *hex*} *psk wlan-id*
- 次のコマンドを入力して、保護された管理フレームを設定します。
  config wlan security pmf {**disable** | **optional** | **required**} *wlan-id*
- 次のコマンドを入力して、Association Comeback の時間設定を構成します。
  config wlan security pmf association-comeback *timeout-in-seconds wlan-id*
- 次のコマンドを入力して、SA クエリー リトライ タイムアウト設定を構成します。
  config wlan security pmf saquery-retrytimeout *timeout-in-milliseconds wlan-id*
- 次のコマンドを入力して、WLAN の 802.11w 設定ステータスを表示します。
  show wlan *wlan-id*
- 次のコマンドを入力して、PMF のデバッグを設定します。
  debug pmf events {**enable** | **disable**}