MACsec の設定

この章では、Cisco NX-OS デバイスに MACsec を設定する手順について説明します。

MACsec の設定

この章では、Cisco NX-OS デバイスに MACsec を設定する手順について説明します。

MACsec について

Media Access Control Security（MACsec）である IEEE 802.1AE と MACsec Key Agreement（MKA）プロトコルは、イーサネットリンク上でセキュアな通信を提供します。次の機能があります。

- ライン レート暗号化機能を提供します。
- レイヤ 2 で強力な暗号化を提供することで、データの機密性を確保します。
- 整合性チェックを行い、転送中にデータを変更できないことを保証します。
- 中央集中型ポリシーを使用して選択的に有効にでき、MACsec 非対応コンポーネントがネットワークにアクセスできるようにしながら、必要に応じて適用することができます。
- レイヤ 2 ではホップバイホップ ベースでパケットを暗号化します。これにより、ネットワークは、既存のポリシーに従って、トラフィックを検査、モニター、マーク、転送できます。その点で、パケットの内容をネットワーク デバイスから隠すエンドツーエンド レイヤ 3 暗号化技術とは異なっています。

キー ライフタイムおよびヒットレス キー ロールオーバー

MACsec キー チェーンには、キー ID とオプションのライフタイムが設定された複数の事前共有キー（PSK）を含めることができます。キーのライフタイムでは、キーがいつ有効になり、いつ期限切れになるかが指定されます。ライフタイム設定が存在しない場合は、無期限のデフォルト ライフタイムが使用されます。ライフタイムが構成されている場合に、ライフタイムの期限が切れると、MKA はキー チェーン内で次に構成された事前共有キーにロール オーバー

します。キーのタイム ゾーンは、ローカルまたは UTC を指定できます。デフォルトの時間帯は UTC です。

MACsec キーチェーンを設定するには、MACsec キーチェーンとキーの設定 （6 ページ）を参照してください。

どのキーも、同じキーチェーンの中の 2 番目のキーにロールオーバーできます。 それには 2 番目のキーを構成し、最初のキーではライフタイムを構成します。最初のキーのライフタイムが期限切れになると、リスト内の次のキーに自動的にロールオーバーします。同一のキーがリンクの両側で同時に構成されていた場合、キーのロールオーバーはノーヒットになります。つまり、キーはトラフィックを中断せずにロールオーバーされます。

フォールバック キー

MACsec セッションは、キー/キー名（CKN）のミスマッチで、またはスイッチとピア間のキーの期限が切れて、失敗する可能性があります。MACsec セッションが失敗した場合、フォールバック キーが設定されていれば、フォールバック セッションが引き継ぐことができます。フォールバック セッションは、プライマリ セッションの障害によるダウンタイムを防止し、ユーザが障害の原因となっている主要な問題を修正できるようにします。フォールバック キーは、プライマリ セッションの開始に失敗した場合のバックアップ セッションも提供します。この機能はオプションです。

MACsec フォールバックキーを設定するには、MACsec フォールバック キーの設定 （8 ページ）を参照してください。

MACSec の注意事項と制約事項

MACsec に関する注意事項と制約事項は次のとおりです。

- MACsec は、次のインターフェイス タイプでサポートされます。
  - レイヤ 2 スイッチポート（アクセスとトランク）access and trunk)
  - レイヤ 3 ルーテッド インターフェイス（サブインターフェイスなし）

（注） レイヤ 3 ルーテッド インターフェイスで MACsec を有効にすると、そのインターフェイスで定義されているすべてのサブインターフェイスでも暗号化が有効になります。ただし、同じレイヤ 3 ルーテッド インターフェイスのサブインターフェイスのサブセットで MACsec を選択的に有効にすることはサポートされていません。

  - 個々のレイヤ 2 およびレイヤ 3 ポート チャネル メンバー（サブインターフェイスなし）

- Secure Channel Identified（SCI）エンコーディングは、Cisco Nexus 3600 シリーズ スイッチでは無効にできません。

- リリース 10.x からダウングレードする場合、MACsec のサポートは Cisco Nexus ToR スイッチでは使用できません。
- MKA は、MACsec でサポートされている唯一のキー交換プロトコルです。Security Association Protocol（SAP）はサポートされていません。
- リンクレベルフロー制御（LLFC）およびプライオリティフロー制御（PFC）は、MACsec ではサポートされません。
- 同じインターフェイスに対する複数の MACsec ピア（異なる SCI 値）はサポートされません。
- **macsec shutdown** コマンドを使用して MACsec を無効にすると、MACsec 設定を保持できます。
- MACsec セッションは、最新の Rx および最新の Tx フラグが Tx SA のインストール後に最初に廃止されたキーサーバからのパケットを受け入れるのに寛容です。MACsec セッションは、セキュアな状態に収束します。
- Cisco NX-OS リリース 10.1(1) 以降では、ポリシーがインターフェイスによって参照されている間に MACSec ポリシーを変更できます。
- Cisco Nexus リリース 10.1(1) 以降では、MACsec は Cisco Nexus N3KC3636C-R プラットフォーム スイッチでサポートされます。
- N3K-C3636C-R：MACsec は、緑色でマークされた N3K-C3636C-R の次の 8 つのポートでサポートされます [ポート 29 ～ 36]。

（注） Cisco Nexus N3K-C3636C-R プラットフォーム スイッチでは、MACsec がポートで構成済みまたは未構成の場合のどちらでも、MACsec セキュリティポリシー タイプに関係なく、ポートフラップが発生します。

- Cisco Nexus 3600 シリーズ スイッチは、QSA が使用されている場合、MACsec 対応ポートで MACsec をサポートしません。
- MACsec はブレークアウト ポートではサポートされません。また、MACsec が構成されている場合、N3K-C3636C-R のポート 29 からポート 36 までの 8 つのポートではブレークアウトがサポートされません。
- MACsec ポリシーの conf-offset パラメータが動的に変更された場合、パケットは短期間ドロップされます。ポリシーがポートでアクティブでない場合は、静的構成でのみ conf-offset パラメータを変更してください。
- Cisco Nexus リリース 10.3(3)F 以降、MACsec は Cisco N3K-C36180YC-R スイッチでサポートされますが、次の制限があります：
  - MACsec は、Eth1/49、Eth1/51、Eth1/52、Eth1/53、および Eth1/54 ポートでのみサポートされます。

- Eth1/50 ポートでは MACsec がリンクをダウンさせるため、構成しないでください。

キーチェーンの制限：

- MACsec キーのオクテット文字列は上書きできません。代わりに、新しいキーまたは新しいキーチェーンを作成する必要があります。
- end または exit を入力すると、キーチェーンの新しいキーが設定されます。エディタ モードのデフォルトのタイムアウト値は 6 秒です。キーがキー オクテット文字列または 6 秒間の送信ライフタイムで設定されていない場合、MACsec セッションを起動するために不完全な情報が使用され、セッションが承認保留状態のままになる可能性があります。設定の完了後に MACsec セッションがコンバージされない場合は、ポートをシャットダウン/非シャットダウンすることをお勧めします。
- 指定したキーチェーンでは、キーの有効期間を重複させて、有効なキーの不在期間を避ける必要があります。キーがアクティブ化されない期間が発生すると、セッション ネゴシエーションが失敗し、トラフィックがドロップされる可能性があります。MACsec キー ロールオーバーでは、現在アクティブなキーの中で最も遅い開始時刻のキーが優先されます。

フォールバックの制限：

- MACsecセッションが古いプライマリキーで保護されている場合、最新のアクティブなプライマリ キーが一致しない場合、フォールバック セッションには進みません。そのため、セッションは古いプライマリ キーで保護されたままになり、ステータスが古いCA のキー再生成として表示されます。プライマリ PSK の新しいキーの MACsec セッションは init 状態になります。
- フォールバック キーチェーンでは、無期限のキーを 1 つだけ使用します。複数のキーはサポートされていません。
- フォールバック キー チェーンで使用されるキー ID（CKN）は、プライマリ キー チェーンで使用されるキー ID（CKN）のいずれとも一致しないようにしてください。
- 一度設定すると、インターフェイスのすべての MACsec 設定が削除されない限り、インターフェイスのフォールバック設定は削除できません。

MACsec ポリシーの制限：

- MACsec セッションがセキュアになる前に、BPDU パケットを送信できます。

レイヤ 2 トンネリング プロトコル（L2TP）の制限：

- MACsec は、dot1q トンネリングまたは L2TP 用に設定されたポートではサポートされません。

- 非ネイティブ VLAN のトランク ポートで STP が有効になっている場合、L2TP は機能しません。

統計の制限：

- MACsec モードと非 MACsec モード（通常のポート シャットダウン/非シャットダウン）の間の移行中に発生する CRC エラーはほとんどありません。
- IEEE8021-SECY-MIB OID secyRxSAStatsOKPkts、secyTxSAStatsProtectedPkts、および secyTxSAStatsEncryptedPkts は最大 32 ビットのカウンタ値しか伝送できませんが、トラフィックは 32 ビットを超える可能性があります。

MACsec の有効化

MACsec および MKA コマンドにアクセスする前に、MACsec 機能を有効に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：
	`switch# configure terminal`
	`switch(config)#`
		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	**feature macsec** **例**： `switch(config)# feature macsec`	デバイスで MACsec および MKA を有効にします。
ステップ 3	（任意） copy running-config startup-config **例**： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MACsec の無効化

Cisco NX-OS リリース 10.1(1) 以降では、MACsec 機能を無効にしても、この機能が非アクティブ化されるだけで、関連する MACsec 設定は削除されません。

MACsec の無効化には、次の条件があります。

- MACsec shutdown はグローバルコマンドであり、インターフェイス レベルでは使用できません。

- macsec shutdown、show macsec mka session/summary、show macsec mka session detail、およびshow macsec mka/secy statisticsコマンドは、「Macsec is shutdown」メッセージを表示します。ただし、show macsec policy および show key chain コマンドは出力を表示します。
- 連続する MACsec ステータスが macsec shutdown から no macsec shutdown に変更された場合、またはその逆の場合は、ステータス変更の間に 30 秒の間隔が必要です。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	**macsec shutdown** 例： `switch(config)# macsec shutdown`	デバイスの MACsec 設定を無効にします。**no** オプションは、MACsec 機能を復元します。
ステップ 3	（任意） copy running-config startup-config 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。この手順は、スイッチのリロード後に MACsec をシャットダウン状態に維持する場合にのみ必要です。 （注） **no feature macsec** コマンドを使用して MACsec 機能を無効にすることもできます。

MACsec キーチェーンとキーの設定

デバイスに MACsec キーチェーンとキーを作成できます。

（注） MACsec キーチェーンのみが MKA セッションをコンバージします。

始める前に

MACsec が有効であることを確認します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

ステップ 2	（任意）[**no**] **key-chain macsec-psk no-show** 例： `switch(config)# key-chain macsec-psk no-show`	**show running-config** および **show startup-config** コマンドの出力で、暗号化されたキーオクテット文字列をワイルドカード文字に置き換えて非表示にします。デフォルトでは、PSK キーは暗号化形式で表示され、簡単に復号化できます。このコマンドは、MACsec キーチェーンにのみ適用されます。 （注） オクテット文字列は、設定をファイルに保存するときにも非表示になります。

ステップ 3	**key chain** *name***macsec**
	例：
	`switch(config)# key chain 1 macsec`
	`switch(config-macseckeychain)#`
		MACSec キーチェーンを作成して MACSec キーのセットを保持し、MACSec キーチェーン設定モードを開始します。

ステップ 4	**key** *key-id*
	例：
	`switch(config-macseckeychain)# key 1000`
	`switch(config-macseckeychain-macseckey)#`
		MAC secキーを作成し、MACsec キー設定モードを開始します。範囲は 1ー32 オクテットで、最大サイズは 64 です。
		（注）
		キーの文字数は偶数でなければなりません。

ステップ 5	**key-octet-string** *octet-string* **cryptographic-algorithm** {**AES_128_CMAC** | **AES_256_CMAC**}
	例：
	`switch(config-macseckeychain-macseckey)#`
	`key-octet-string`
	`abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789`
	`cryptographic-algorithm AES_256_CMAC`
		そのキーの octet ストリングを設定します。octet-string 引数には、最大 64 文字の 16 進数文字を含めることができます。octet キーは内部でエンコードされるため、クリア テキストのキーは **show running-config macsec** コマンドの出力に表示されません。
		キーオクテット文字列には、次のものが含まれます。
		• 0 暗号化タイプ - 暗号化なし（デフォルト）
		• 6 暗号化タイプ - 独自仕様（タイプ 6 暗号化）。詳細については、 *MACsec* キーでタイプ *6* 暗号化を有効にするを参照してください。
		• 7 暗号化タイプ - 最大 64 文字の、独自仕様 WORD キー オクテット文列

	コマンドまたはアクション	目的
		（注） AES_128_CMAC 暗号化アルゴリズムを使用するためには、MACsec ピアは同じ Cisco NX-OS リリースを実行する必要があります。以前のリリースと、Cisco NX-OS リリース 7.0(3)I7(2) 以降のリリース間で相互運用できるようにするには、キーを AES_256_CMAC 暗号化アルゴリズムで使用する必要があります。
ステップ 6	**send-lifetime** *start-time* **duration** *duration* 例： `switch(config-macseckeychain-macseckey)# send-lifetime 00:00:00 Oct 04 2016 duration 100000`	キーの送信ライフタイムを設定します。デフォルトでは、デバイスは開始時間を UTC として扱います。 *start-time* 引数は、キーがアクティブになる日時です。*duration* 引数はライフタイムの長さ（秒）です。最大値は 2147483646 秒（約 68 年）です。
ステップ 7	（任意） **show key chain** *name* 例： `switch(config-macseckeychain-macseckey)# show key chain 1`	キーチェーンの設定を表示します。
ステップ 8	（任意） copy running-config startup-config 例： `switch(config-macseckeychain-macseckey)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MACsec フォールバック キーの設定

Cisco NX-OS リリース 10.1(1) 以降では、プライマリ セッションがスイッチとピア間のキー/キー名（CKN）のミスマッチまたはキーの有効期限の結果として失敗した場合にバックアップ セッションを開始するよう、デバイスのフォールバック キーを設定できます。

始める前に

MACsec が有効になっており、プライマリおよびフォールバック キーチェーンとキー ID が設定されていることを確認します。「MACsec キーチェーンとキーの設定 （6 ページ）」を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	グローバル構成モードを開始します。

	コマンドまたはアクション	目的
	switch# **configure terminal** switch(config)#	
ステップ 2	**interface** *name* 例： switch(config)# **interface ethernet 1/29** switch(config-if)#	設定するインターフェイスを指定します。インターフェイス タイプと ID を指定できます。イーサネット ポートの場合は、「ethernet slot / port」を使用します。
ステップ 3	**macsec keychain** *keychain-name* **policy** *policy-name* **fallback-keychain** *keychain-name* 例： switch(config-if)# **macsec keychain kc2 policy abc fallback-keychain fb_kc2**	キー/キー ID のミスマッチまたはキーの期限切れによる MACsec セッションの失敗後に使用するフォールバック キーチェーンを指定します。フォールバック キー ID は、プライマリ キーチェーンのキー ID と一致してはなりません。 フォールバック キーチェーン名を変更して同じコマンドを再発行することで、MACsec 設定を削除せずに、各インターフェイスのフォールバック キーチェーン設定を対応するインターフェイスで変更できます。 （注） コマンドは、フォールバック キーチェーン名を除き、インターフェイスの既存のコンフィギュレーション コマンドとまったく同じように入力する必要があります。 「MACsec キーチェーンとキーの設定 （6 ページ）」を参照してください。
ステップ 4	（任意） **copy running-config startup-config** 例： switch(config-if)# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MACsec ポリシーの設定

異なるパラメータを使用して複数の MACSec ポリシーを作成できます。しかし、1 つのインターフェイスでアクティブにできるポリシーは 1 つのみです。

始める前に

MACsec が有効であることを確認します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	**macsec policy** *name*
	例：
	`switch(config)# macsec policy abc`
	`switch(config-macsec-policy)#`
		MACsec ポリシーを作成します。

ステップ 3	**cipher-suite** *name* 例： `switch(config-macsec-policy)# cipher-suite GCM-AES-256`	次のいずれかの暗号方式を構成します。 GCM-AES-128、GCM-AES-256、GCM-AES-XPN-128、または GCM-AES-XPN-256。
ステップ 4	**key-server-priority** *number* 例： `switch(config-macsec-policy)# key-server-priority 0`	キー交換中はピア間の接続が解除されるように、キー サーバのプライオリティを設定します。範囲は0（最高）ー 255（最低）で、デフォルト値は 16 です。
ステップ 5	**security-policy** *name* 例： `switch(config-macsec-policy)# security-policy should-secure`	次のいずれかのセキュリティ ポリシーを設定して、データおよび制御パケットの処理を定義します。 • **must-secure**：MACsec ヘッダーを持たないパケットはドロップされます。 • **should-secure**：MACsec ヘッダーを持たないパケットも許可されます。これはデフォルト値です。
ステップ 6	**window-size** *number* 例： `switch(config-macsec-policy)# window-size 512`	インターフェイスが、設定されたウィンドウ サイズ未満のパケットを受け入れないように、再生保護ウィンドウを設定します。範囲は 0 ～ 596000000 です。
ステップ 7	**sak-expiry-time** *time* 例： `switch(config-macsec-policy)# sak-expiry-time 100`	SAK キー再生成を強制する時間を秒単位で設定します。このコマンドを使用して、セッション キーを予測可能な時間間隔に変更できます。デフォルトは 0 です。
ステップ 8	**conf-offset** *name* 例：	暗号化を開始するレイヤ 2 フレームの機密性オフセットの 1 つとして、CONF-OFFSET-0、

	コマンドまたはアクション	目的
	`switch(config-macsec-policy)# conf-offset CONF-OFFSET-0`	CONF-OFFSET-30、またはCONF-OFFSET-50 のいずれかを設定します。 このコマンドは、中間スイッチがパケットヘッダー {dmac、smac、etype} を MPLS タグのように使用するために必要です。
ステップ 9	（任意） **show macsec policy** 例： `switch(config-macsec-policy)# show macsec policy`	MACSec ポリシー設定を表示します。
ステップ 10	（任意） **copy running-config startup-config** 例： `switch(config-macsec-policy)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

PSK のローテーション

SAK の有効期限が MACsec ポリシーで 60 秒に設定されている場合は、次の手順に従って PSK を切り替えます。

手順

ステップ 1 **no sak-expiry-time** コマンドを使用して、MACsec ポリシーから SAK 期限切れタイマーを削除します。

設定内のポリシーの数だけ、SAK の有効期限タイマーを削除する必要があります。インターフェイスごとに削除する必要はありません。ポリシーを 1 つだけ定義してすべてのインターフェイスに適用した場合は、このポリシーからのみ SAK の有効期限タイマーを削除する必要があります。

ステップ 2 2 分間待機します。

ステップ 3 **key** *key-id* コマンドを使用して、キーチェーンの下に新しいキーをプログラムします。

ステップ 4 新しいキーとのセッションがセキュア化されたら、**no key** *key-id* コマンドを使用して古いキーを削除します。

ステップ 5 2 分間待機します。

ステップ 6 **sak-expiry-timer 60** コマンドを使用して、SAK キー再生成タイマーを MACsec ポリシーに追加します。

MACsec 設定の確認

MACsec 設定情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
show key chain *name*	キーチェーンの設定を表示します。
show macsec mka session [**interface** *type slot/port*] [**detail**]	特定のインターフェイスまたはすべてのインターフェイスの MACsec MKA セッションに関する情報を表示します。
show macsec mka session details	MAC アドレスに関する情報を表示します。
show macsec mka summary	MACsec MKA 設定を表示します。
show macsec policy [*policy-name*]	特定の MACsec ポリシーまたはすべての MACsec ポリシーの設定を表示します。
show running-config macsec	MACsec の実行コンフィギュレーション情報を表示します。

次に、すべてのインターフェイスの MACsec MKA セッションに関する情報を表示する例を示します。

```
switch(config)# show macsec mka session
Interface          Local-TxSCI                     # Peers            Status
   Key-Server         Auth Mode
------------------ ------------------------------- ------------------ ------------------
 ------------------ ------------------
Ethernet1/29       6c8b.d3db.e968/0001             1                  Secured
   No                 PRIMARY-PSK
Ethernet1/30       6c8b.d3db.e96c/0001             1                  Secured
   No                 PRIMARY-PSK
Ethernet1/31       6c8b.d3db.e970/0001             1                  Secured
   Yes                PRIMARY-PSK
Ethernet1/32       6c8b.d3db.e974/0001             1                  Secured
   Yes                PRIMARY-PSK
Ethernet1/33       6c8b.d3db.e978/0001             1                  Secured
   Yes                PRIMARY-PSK
Ethernet1/34       6c8b.d3db.e97c/0001             1                  Secured
   Yes                PRIMARY-PSK
Ethernet1/35       6c8b.d3db.e980/0001             1                  Secured
   Yes                PRIMARY-PSK
Ethernet1/36       6c8b.d3db.e984/0001             1                  Secured
   No                 PRIMARY-PSK
------------------ ------------------------------- ------------------ ------------------
 ------------------ ------------------
Total Number of Sessions : 8
        Secured Sessions : 8
        Pending Sessions : 0
switch(config)#
```

次に、特定のインターフェイスの MACsec MKA セッションに関する情報を表示する例を示します。前の例で説明したテーブルの一般的な要素に加えて、現在の MACsec セッション タイプを定義する認証モードも示します。

```
switch(config)# show macsec mka session interface e1/35
Interface          Local-TxSCI                     # Peers            Status
   Key-Server         Auth Mode
------------------ ------------------------------- ------------------ ------------------
 ------------------ ------------------
```

```
Ethernet1/35       6c8b.d3db.e980/0001             1                  Secured
   Yes               PRIMARY-PSK
switch(config)#
```

次に、特定のイーサネット インターフェイスの MACsec MKA セッションに関する詳細情報を表示する例を示します。

```
switch(config)# show macsec mka session interface e1/35 details
Detailed Status for MKA Session
-----------------------------------
Interface Name                          : Ethernet1/35
    Session Status                      : SECURED - Secured MKA Session with MACsec
    Local Tx-SCI                        : 6c8b.d3db.e980/0001
    Local Tx-SSCI                       : 2
    MKA Port Identifier                 : 2
    CAK Name (CKN)                      : 2006
    CA Authentication Mode              : PRIMARY-PSK
    Member Identifier (MI)              : 50BE8367F1C6D0AB1C442229
    Message Number (MN)                 : 1048
    MKA Policy Name                     : mpsr1
    Key Server Priority                 : 1
    Key Server                          : Yes
    Include ICV                         : Yes
    SAK Cipher Suite                    : GCM-AES-128
    SAK Cipher Suite (Operational)      : GCM-AES-128
    Replay Window Size                  : 148809600
    Confidentiality Offset              : CONF-OFFSET-30
    Confidentiality Offset (Operational): CONF-OFFSET-30
    Latest SAK Status                   : Rx & TX
    Latest SAK AN                       : 0
    Latest SAK KI                       : 50BE8367F1C6D0AB1C44222900000021
    Latest SAK KN                       : 33
    Last SAK key time                   : 11:23:53 pst Tue Dec 15 2020
    CA Peer Count                       : 1
    Eapol dest mac                      : 0180.c200.0003
    Ether-type                          : 0x888e
Peer Status:
    Peer MI                             : 37AFE73EC8617FD32F70E21A
    RxSCI                               : 6c8b.d3db.e984/0001
    Peer CAK                            : Match
    Latest Rx MKPDU                     : 11:24:52 pst Tue Dec 15 2020
Fallback Data:
    Fallback CKN                        : FB2004
    Fallback MI                         : 849D72D5F6A900F5B0718C78
    Fallback MN                         : 0x3d6
Fallback Peer:
    Peer MI                             : 8DCE8CBE67B474D2C2955F58
    RxSCI                               : 6c8b.d3db.e984/0001
    Peer CAK                            : Match
    Latest Rx MKPDU                     : 11:24:52 pst Tue Dec 15 2020
switch(config)#
```

次に、MACsec MKA 設定を表示する例を示します。

```
switch# show macsec mka summary
Interface          MACSEC-policy                   Keychain
------------------ ------------------------------- ------------------------
Ethernet2/13       1                               1/10000000000000000
Ethernet2/14       1                               1/10000000000000000
switch#
```

次に、すべての MACsec ポリシーの設定を表示する例を示します。

```
switch# show macsec policy
MACSec Policy Cipher Pri Window Offset Security SAK Rekey time ICV Indicator
```

```
------------------------------- ---------------- ---- ------------ -------- --------------
-------------- --------------
system-default-macsec-policy GCM-AES-XPN-256 16 148809600 0 should-secure
pn-rollover FALSE
tests1 GCM-AES-XPN-256 16 148809600 0 should-secure
pn-rollover FALSE
tests2 GCM-AES-XPN-256 16 148809600 0 should-secure
pn-rollover FALSE
tests3 GCM-AES-256 16 148809600 0 should-secure
pn-rollover FALSE
```

次の例では、**key-chain macsec-psk no-show** コマンドが構成されていない場合に **show running-config** および **show startup-config** コマンドの出力のキー オクテット文字列を表示します：

```
key chain KC256-1 macsec
    key 2000
      key-octet-string 7
075e701e1c5a4a5143475e5a527d7c7c706a6c724306170103555a5c57510b051e47080
a05000101005e0e50510f005c4b5f5d0b5b070e234e4d0a1d0112175b5e cryptographic-algorithm
AES_256_CMAC
```

次の例では、**key-chain macsec-psk no-show** コマンドが構成されている場合に **show running-config** および **show startup-config** コマンドの出力のキー オクテット文字列を表示します：

```
key chain KC256-1 macsec
    key 2000
      key-octet-string 7 ****** cryptographic-algorithm AES_256_CMAC
```

MACsec 統計の表示

次のコマンドを使用して、MACsec 統計情報を表示できます。

コマンド	目的
show macsec mka statistics [**interface** *type slot/port*]	MACsec MKA 統計情報を表示します。
show macsec secy statistics [**interface** *type slot/port*]	MACsecセキュリティ統計情報を表示します。

次に、特定のイーサネット インターフェイスの MACsec MKA 統計情報の例を示します。

```
switch# show macsec mka statistics interface ethernet 1/29
MKA Statistics for Session on interface (Ethernet1/29)
============================================================
CA Statistics
   Pairwise CAK Rekeys..... 0

SA Statistics
   SAKs Generated.......... 0
   SAKs Rekeyed............ 0
   SAKs Received........... 0
   SAK Responses Received.. 0

MKPDU Statistics
   MKPDUs Transmitted...... 41
      "Distributed SAK".. 0
   MKPDUs Validated & Rx... 41
      "Distributed SAK".. 0
```

```
MKA IDB Statistics
   MKPDUs Tx Success.......... 82
   MKPDUs Tx Fail............. 0
   MKPDUS Tx Pkt build fail... 0
   MKPDUS No Tx on intf down.. 0
   MKPDUS No Rx on intf down.. 0
   MKPDUs Rx CA Not found..... 0
   MKPDUs Rx Error............ 0
   MKPDUs Rx Success.......... 82

MKPDU Failures
   MKPDU Rx Validation ..................... 0
   MKPDU Rx Bad Peer MN..................... 0
   MKPDU Rx Non-recent Peerlist MN.......... 0
   MKPDU Rx Drop SAKUSE, KN mismatch........ 0
   MKPDU Rx Drop SAKUSE, Rx Not Set......... 0
   MKPDU Rx Drop SAKUSE, Key MI mismatch.... 0
   MKPDU Rx Drop SAKUSE, AN Not in Use...... 0
   MKPDU Rx Drop SAKUSE, KS Rx/Tx Not Set... 0
   MKPDU Rx Drop Packet, Ethertype Mismatch. 0
   MKPDU Rx Drop Packet, DestMAC Mismatch... 0

SAK Failures
   SAK Generation................... 0
   Hash Key Generation.............. 0
   SAK Encryption/Wrap.............. 0
   SAK Decryption/Unwrap............ 0

CA Failures
   ICK Derivation................... 0
   KEK Derivation................... 0
   Invalid Peer MACsec Capability... 0

MACsec Failures
   Rx SA Installation............... 0
   Tx SA Installation............... 0

switch(config)#
```

次に、特定のイーサネット インターフェイスの MACsec セキュリティ統計情報を表示する例を示します。

（注） Rx および Tx 統計情報の非制御パケットと制御パケットには、次の違いがあります。

- Rx 統計
  - 非制御=暗号化および非暗号化
  - 制御 = 非暗号化
- TX 統計情報：
  - 非制御 = 非暗号化
  - 制御 = 暗号化
  - 共通 = 暗号化および非暗号化

```
switch(config)# show macsec secy statistics interface e1/29
Interface Ethernet1/29 MACSEC SecY Statistics:
-------------------------------------------
Interface Rx Statistics:
   Unicast Uncontrolled Pkts: 8067779
   Multicast Uncontrolled Pkts: 14
   Broadcast Uncontrolled Pkts: 0
   Uncontrolled Pkts - Rx Drop: 0
   Uncontrolled Pkts - Rx Error: 0
   Unicast Controlled Pkts: N/A (N3K-C3636C-R not supported)
   Multicast Controlled Pkts: N/A (N3K-C3636C-R not supported)
   Broadcast Controlled Pkts: N/A (N3K-C3636C-R not supported)
   Controlled Pkts: 8056748
   Controlled Pkts - Rx Drop: N/A (N3K-C3636C-R not supported)
   Controlled Pkts - Rx Error: N/A (N3K-C3636C-R not supported)
   In-Octets Uncontrolled: 37641828280 bytes
   In-Octets Controlled: 37324295914 bytes
   Input rate for Uncontrolled Pkts: N/A (N3K-C3636C-R not supported)
   Input rate for Uncontrolled Pkts: N/A (N3K-C3636C-R not supported)
   Input rate for Controlled Pkts: N/A (N3K-C3636C-R not supported)
   Input rate for Controlled Pkts: N/A (N3K-C3636C-R not supported)

Interface Tx Statistics:
   Unicast Uncontrolled Pkts: N/A (N3K-C3636C-R not supported)
   Multicast Uncontrolled Pkts: N/A (N3K-C3636C-R not supported)
   Broadcast Uncontrolled Pkts: N/A (N3K-C3636C-R not supported)
   Uncontrolled Pkts - Rx Drop: N/A (N3K-C3636C-R not supported)
   Uncontrolled Pkts - Rx Error: N/A (N3K-C3636C-R not supported)
   Unicast Controlled Pkts: N/A (N3K-C3636C-R not supported)
   Multicast Controlled Pkts: N/A (N3K-C3636C-R not supported)
   Broadcast Controlled Pkts: N/A (N3K-C3636C-R not supported)
   Controlled Pkts: 8049279
   Controlled Pkts - Rx Drop: N/A (N3K-C3636C-R not supported)
   Controlled Pkts - Rx Error: N/A (N3K-C3636C-R not supported)
   Out-Octets Uncontrolled: N/A (N3K-C3636C-R not supported)
   Out-Octets Controlled: 37262189352 bytes
   Out-Octets Common: 37699748491 bytes
   Output rate for Uncontrolled Pkts: N/A (N3K-C3636C-R not supported)
   Output rate for Uncontrolled Pkts: N/A (N3K-C3636C-R not supported)
   Output rate for Controlled Pkts: N/A (N3K-C3636C-R not supported)
   Output rate for Controlled Pkts: N/A (N3K-C3636C-R not supported)

SECY Rx Statistics:
   Transform Error Pkts: N/A (N3K-C3636C-R not supported)
   Control Pkts: 0
   Untagged Pkts: N/A (N3K-C3636C-R not supported)
   No Tag Pkts: 0
   Bad Tag Pkts: 0
   No SCI Pkts: 0
   Unknown SCI Pkts: 0
   Tagged Control Pkts: N/A (N3K-C3636C-R not supported)

SECY Tx Statistics:
   Transform Error Pkts: N/A (N3K-C3636C-R not supported)
   Control Pkts: 0
   Untagged Pkts: N/A (N3K-C3636C-R not supported)

SAK Rx Statistics for AN [0]:
   Unchecked Pkts: 0
   Delayed Pkts: 0
   Late Pkts: 0
   OK Pkts: 8056748
   Invalid Pkts: 0
   Not Valid Pkts: 0
```

```
   Not-Using-SA Pkts: 0
   Unused-SA Pkts: 0
   Decrypted In-Octets: 36952542946 bytes
   Validated In-Octets: 0 bytes

SAK Tx Statistics for AN [0]:
   Encrypted Protected Pkts: 8049279
   Too Long Pkts: N/A (N3K-C3636C-R not supported)
   SA-not-in-use Pkts: N/A (N3K-C3636C-R not supported)
   Encrypted Protected Out-Octets: 36909704659 bytes

switch(config)#
```

MACsec の設定例

次に、ユーザ定義のMACsecポリシーを設定し、そのポリシーをインターフェイスに適用する例を示します。

```
switch(config)# macsec policy mpsr1
switch(config-macsec-policy)# cipher-suite GCM-AES-128
switch(config-macsec-policy)# key-server-priority 1
switch(config-macsec-policy)# window-size 1000
switch(config-macsec-policy)# conf-offset CONF-OFFSET-30
switch(config-macsec-policy)# security-policy must-secure
switch(config-macsec-policy)# sak-expiry-time 60
switch(config-macsec-policy)# include-icv-indicator

switch(config-macsec-policy)# interface e1/35-36
switch(config-if-range)# macsec keychain ksr policy mpsr1
switch(config-if-range)# show macsec mka session
Interface          Local-TxSCI                       # Peers            Status
   Key-Server         Auth Mode
------------------ --------------------------------- ------------------ ------------------
 ------------------ ------------------
Ethernet1/35       6c8b.d3db.e980/0001               1                  Secured
   Yes                PRIMARY-PSK
Ethernet1/36       6c8b.d3db.e984/0001               1                  Secured
   No                 PRIMARY-PSK
------------------ --------------------------------- ------------------ ------------------
 ------------------ ------------------

switch(config-if-range)# show macsec mka summary
Interface          Status   Cipher (Operational)   Key-Server   MACSEC-policy
          Keychain                          Fallback-keychain
------------------ -------- ---------------------- ------------
-------------------------------- ---------------------------------
--------------------------------
Ethernet1/35       Secured  GCM-AES-128            Yes          mpsr1
          ksr                               no keychain
Ethernet1/36       Secured  GCM-AES-128            No           mpsr1
          ksr                               no keychain

switch(config-if-range)# show running-config macsec
!Command: show running-config macsec
!Running configuration last done at: Tue Dec 15 11:41:53 2020
!Time: Tue Dec 15 11:45:06 2020

version 10.1(1) Bios:version 01.14
feature macsec

macsec policy mpsr1
   cipher-suite GCM-AES-128
   key-server-priority 1
```

```
   window-size 1000
   conf-offset CONF-OFFSET-30
   sak-expiry-time 60
   include-icv-indicator

interface Ethernet1/35
   macsec keychain ksr policy mpsr1

interface Ethernet1/36
   macsec keychain ksr policy mpsr1
```

次に、MACsec キーチェーンを設定し、インターフェイスにシステムデフォルトの MACsecポリシーを追加する例を示します。

```
switch(config)# key chain ksr macsec
switch(config-macseckeychain)# key 2006
switch(config-macseckeychain-macseckey)# key-octet-string
1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef cryptographic-algorithm
 AES_256_CMAC
switch(config-macseckeychain-macseckey)# interface e1/35-36
switch(config-if-range)# macsec keychain ksr

switch(config-if-range)# show running-config macsec
!Command: show running-config macsec
!Running configuration last done at: Tue Dec 15 11:53:10 2020
!Time: Tue Dec 15 11:54:40 2020

version 10.1(1) Bios:version 01.14
feature macsec

interface Ethernet1/35
   macsec keychain ksr policy system-default-macsec-policy

interface Ethernet1/36
   macsec keychain ksr policy system-default-macsec-policy

switch(config-if-range)# show macsec mka summary
Interface          Status   Cipher (Operational)   Key-Server   MACSEC-policy
          Keychain                          Fallback-keychain
------------------ -------- ---------------------- ------------
--------------------------------- ---------------------------------
---------------------------------
Ethernet1/35       Secured  GCM-AES-XPN-256        Yes
system-default-macsec-policy     ksr                              no keychain

Ethernet1/36       Secured  GCM-AES-XPN-256        No
system-default-macsec-policy     ksr                              no keychain


switch(config-if-range)# show macsec mka session
Interface          Local-TxSCI                       # Peers            Status
   Key-Server         Auth Mode
------------------ --------------------------------- ------------------ ------------------
 ------------------ ------------------
Ethernet1/35       6c8b.d3db.e980/0001               1                  Secured
   Yes                PRIMARY-PSK
Ethernet1/36       6c8b.d3db.e984/0001               1                  Secured
   No                 PRIMARY-PSK
------------------ --------------------------------- ------------------ ------------------
 ------------------ ------------------

Total Number of Sessions : 2
   Secured Sessions : 2
   Pending Sessions : 0
```

```
switch(config-if-range)#
```

XML の例

MACsec は、| **xml** を使用したスクリプト用に次の **show** コマンドの XML 出力をサポートします。

- **show key chain** *name* | **xml**
- **show macsec mka session** *interface interface slot/port* **details** |**xml**
- **show macsec mka statistics interface** *interface slot/port* |**xml**
- **show macsec mka summary** |**xml**
- **show macsec policy** *name* |**xml**
- **show macsec secy statistics interface** *interface slot/port* |**xml**
- **show running-config macsec** |**xml**

次に、上記の各 **show** コマンドの出力例を示します。

例 1：キーチェーンの構成を表示します

```
switch(config)# show key chain "ksr" | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns="http://www.cisco.com/nxos:1.0:rpm"
xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0">
<nf:data>
  <show>
   <key>
    <chain>
     <__XML__OPT_Cmd_rpm_show_keychain_cmd_keychain>
      <keychain>ksr</keychain>
      <__XML__OPT_Cmd_rpm_show_keychain_cmd___readonly__>
       <__readonly__>
        <TABLE_keychain>
         <ROW_keychain>
          <chain_name>ksr</chain_name>
          <TABLE_key>
           <ROW_key>
            <key_id>2006</key_id>

<key_string>075e731f1a5c4f524f4d5b0d0629f212e62677147524054590f09595170a061e470d0d030604020c520b07055b5301155756085f535976141759180714160e0a</key_string>

            <crypto_algo>AES_256_CMAC</crypto_algo>
            <send_valid>true</send_valid>
           </ROW_key>
          </TABLE_key>
         </ROW_keychain>
        </TABLE_keychain>
       </__readonly__>
      </__XML__OPT_Cmd_rpm_show_keychain_cmd___readonly__>
     </__XML__OPT_Cmd_rpm_show_keychain_cmd_keychain>
    </chain>
   </key>
  </show>
</nf:data>
</nf:rpc-reply>
```

```
]]>]]>
switch(config)#
```

例 2：特定のインターフェイスの MACsec MKA セッションに関する情報を表示します

```
switch(config)# show macsec mka session interface e1/35 details | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns="http://www.cisco.com/nxos:1.0:cts"
xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0">
<nf:data>
  <show>
   <macsec>
    <mka>
     <session>
      <__XML__OPT_Cmd_show_macsec_mka_session_interface>
       <interface>
        <__XML__INTF_ifname>
         <__XML__PARAM_value>
          <__XML__INTF_output>Ethernet1/35</__XML__INTF_output>
         </__XML__PARAM_value>
        </__XML__INTF_ifname>
       </interface>
       <__XML__OPT_Cmd_show_macsec_mka_session_details>
        <details/>
        <__XML__OPT_Cmd_show_macsec_mka_session___readonly__>
         <__readonly__>
          <TABLE_mka_session_details>
           <ROW_mka_session_details>
            <ifname>Ethernet1/35</ifname>
            <status>SECURED - Secured MKA Session with MACsec</status>
            <sci>6c8b.d3db.e980/0001</sci>
            <ssci>2</ssci>
            <port_id>2</port_id>
            <ckn>2006</ckn>
            <ca_auth_mode>PRIMARY-PSK</ca_auth_mode>
            <mi>5AABE0AB9CC867AB0FF40F7D</mi>
            <mn>3550</mn>
            <policy>system-default-macsec-policy</policy>
            <ks_prio>16</ks_prio>
            <keyserver>Yes</keyserver>
            <include_icv_indicator>No</include_icv_indicator>
            <cipher>GCM-AES-XPN-256</cipher>
            <cipher_operational>GCM-AES-XPN-256</cipher_operational>
            <window>148809600</window>
            <conf_offset>CONF-OFFSET-0</conf_offset>
            <conf_offset_operational>CONF-OFFSET-0</conf_offset_operational>
            <sak_status>Rx & TX</sak_status>
            <sak_an>0</sak_an>
            <sak_ki>5AABE0AB9CC867AB0FF40F7D00000001</sak_ki>
            <sak_kn>1</sak_kn>
            <last_sak_rekey_time>11:53:25 pst Tue Dec 15 2020</last_sak_rekey_time>
            <peer_count>1</peer_count>
            <mac_addr>0180.c200.0003</mac_addr>
            <ether_type>0x888e</ether_type>
            <TABLE_mka_peer_status>
             <ROW_mka_peer_status>
              <peer_mi>27FC36C2BFAFBDBC65419A40</peer_mi>
              <rxsci>6c8b.d3db.e984/0001</rxsci>
              <icv_status>Match</icv_status>
              <last_rx_time>13:51:39 pst Tue Dec 15 2020</last_rx_time>
             </ROW_mka_peer_status>
            </TABLE_mka_peer_status>
           </ROW_mka_session_details>
          </TABLE_mka_session_details>
```

```
        </__readonly__>
       </__XML__OPT_Cmd_show_macsec_mka_session___readonly__>
      </__XML__OPT_Cmd_show_macsec_mka_session_details>
     </__XML__OPT_Cmd_show_macsec_mka_session_interface>
    </session>
   </mka>
  </macsec>
 </show>
</nf:data>
</nf:rpc-reply>
]]>]]>
switch(config)#
```

例 3：MACsec MKA 統計を表示します

```
switch(config)# show macsec mka statistics interface e1/29 | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns="http://www.cisco.com/nxos:1.0:cts"
xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0">
<nf:data>
 <show>
  <macsec>
   <mka>
    <statistics>
     <__XML__OPT_Cmd_some_macsec_mka_statistics_interface>
      <interface>
       <__XML__INTF_ifname>
        <__XML__PARAM_value>
         <__XML__INTF_output>Ethernet1/29</__XML__INTF_output>
        </__XML__PARAM_value>
       </__XML__INTF_ifname>
      </interface>
      <__XML__OPT_Cmd_some_macsec_mka_statistics___readonly__>
       <__readonly__>
        <TABLE_mka_intf_stats>
         <ROW_mka_intf_stats>
          <ifname2>Ethernet1/29</ifname2>
          <TABLE_ca_stats>
           <ROW_ca_stats>
            <ca_stat_ckn>2002</ca_stat_ckn>
            <ca_stat_pairwise_cak_rekey>0</ca_stat_pairwise_cak_rekey>
            <sa_stat_sak_generated>0</sa_stat_sak_generated>
            <sa_stat_sak_rekey>0</sa_stat_sak_rekey>
            <sa_stat_sak_received>2</sa_stat_sak_received>
            <sa_stat_sak_response_rx>0</sa_stat_sak_response_rx>
            <mkpdu_stat_mkpdu_tx>4335</mkpdu_stat_mkpdu_tx>
            <mkpdu_stat_mkpdu_tx_distsak>0</mkpdu_stat_mkpdu_tx_distsak>
            <mkpdu_stat_mkpdu_rx>4335</mkpdu_stat_mkpdu_rx>
            <mkpdu_stat_mkpdu_rx_distsak>2</mkpdu_stat_mkpdu_rx_distsak>
           </ROW_ca_stats>
          </TABLE_ca_stats>
          <TABLE_idb_stats>
           <ROW_idb_stats>
            <ca_stat_pairwise_cak_rekey>0</ca_stat_pairwise_cak_rekey>
            <sa_stat_sak_generated>0</sa_stat_sak_generated>
            <sa_stat_sak_rekey>0</sa_stat_sak_rekey>
            <sa_stat_sak_received>2</sa_stat_sak_received>
            <sa_stat_sak_response_rx>0</sa_stat_sak_response_rx>
            <mkpdu_stat_mkpdu_tx>4335</mkpdu_stat_mkpdu_tx>
            <mkpdu_stat_mkpdu_tx_distsak>0</mkpdu_stat_mkpdu_tx_distsak>
            <mkpdu_stat_mkpdu_rx>4335</mkpdu_stat_mkpdu_rx>
            <mkpdu_stat_mkpdu_rx_distsak>2</mkpdu_stat_mkpdu_rx_distsak>
            <idb_stat_mkpdu_tx_success>8666</idb_stat_mkpdu_tx_success>
            <idb_stat_mkpdu_tx_fail>0</idb_stat_mkpdu_tx_fail>
```

```
                <idb_stat_mkpdu_tx_pkt_build_fail>0</idb_stat_mkpdu_tx_pkt_build_fail>
                <idb_stat_mkpdu_no_tx_on_intf_down>0</idb_stat_mkpdu_no_tx_on_intf_down>
                <idb_stat_mkpdu_no_rx_on_intf_down>0</idb_stat_mkpdu_no_rx_on_intf_down>
                <idb_stat_mkpdu_rx_ca_notfound>0</idb_stat_mkpdu_rx_ca_notfound>
                <idb_stat_mkpdu_rx_error>0</idb_stat_mkpdu_rx_error>
                <idb_stat_mkpdu_rx_success>8666</idb_stat_mkpdu_rx_success>
<idb_stat_mkpdu_failure_rx_integrity_check_error>0</idb_stat_mkpdu_failure_rx_integrity_check_error>
<idb_stat_mkpdu_failure_invalid_peer_mn_error>0</idb_stat_mkpdu_failure_invalid_peer_mn_error>
<idb_stat_mkpdu_failure_nonrecent_peerlist_mn_error>0</idb_stat_mkpdu_failure_nonrecent_peerlist_mn_error>
<idb_stat_mkpdu_failure_sakuse_kn_mismatch_error>0</idb_stat_mkpdu_failure_sakuse_kn_mismatch_error>
<idb_stat_mkpdu_failure_sakuse_rx_not_set_error>0</idb_stat_mkpdu_failure_sakuse_rx_not_set_error>
<idb_stat_mkpdu_failure_sakuse_key_mi_mismatch_error>0</idb_stat_mkpdu_failure_sakuse_key_mi_mismatch_error>
<idb_stat_mkpdu_failure_sakuse_an_not_in_use_error>0</idb_stat_mkpdu_failure_sakuse_an_not_in_use_error>
<idb_stat_mkpdu_failure_sakuse_ks_rx_tx_not_set_error>0</idb_stat_mkpdu_failure_sakuse_ks_rx_tx_not_set_error>
<idb_stat_mkpdu_failure_sakuse_eapol_ethertype_mismatch_error>0</idb_stat_mkpdu_failure_sakuse_eapol_ethertype_mismatch_error>
<idb_stat_mkpdu_failure_sakuse_eapol_destmac_mismatch_error>0</idb_stat_mkpdu_failure_sakuse_eapol_destmac_mismatch_error>
<idb_stat_sak_failure_sak_generate_error>0</idb_stat_sak_failure_sak_generate_error>
<idb_stat_sak_failure_hash_generate_error>0</idb_stat_sak_failure_hash_generate_error>
<idb_stat_sak_failure_sak_encryption_error>0</idb_stat_sak_failure_sak_encryption_error>
<idb_stat_sak_failure_sak_decryption_error>0</idb_stat_sak_failure_sak_decryption_error>
<idb_stat_sak_failure_ick_derivation_error>0</idb_stat_sak_failure_ick_derivation_error>
<idb_stat_sak_failure_kek_derivation_error>0</idb_stat_sak_failure_kek_derivation_error>
<idb_stat_sak_failure_invalid_macsec_capability_error>0</idb_stat_sak_failure_invalid_macsec_capability_error>
<idb_stat_macsec_failure_rx_sa_create_error>0</idb_stat_macsec_failure_rx_sa_create_error>
<idb_stat_macsec_failure_tx_sa_create_error>0</idb_stat_macsec_failure_tx_sa_create_error>
            </ROW_idb_stats>
          </TABLE_idb_stats>
        </ROW_mka_intf_stats>
```

```
        </TABLE_mka_intf_stats>
       </__readonly__>
      </__XML__OPT_Cmd_some_macsec_mka_statistics___readonly__>
     </__XML__OPT_Cmd_some_macsec_mka_statistics_interface>
    </statistics>
   </mka>
  </macsec>
 </show>
</nf:data>
</nf:rpc-reply>
]]>]]>
switch(config)#
```

例 4：MACsec MKA 構成を表示します

```
switch(config)# show macsec mka summary | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns="http://www.cisco.com/nxos:1.0:cts"
xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0">
<nf:data>
  <show>
   <macsec>
    <mka>
     <__XML__OPT_Cmd_some_macsec_summary>
      <__XML__OPT_Cmd_some_macsec___readonly__>
       <__readonly__>
        <TABLE_mka_summary>
         <ROW_mka_summary>
          <ifname>Ethernet1/29</ifname>
          <status>Secured</status>
          <cipher>GCM-AES-128</cipher>
          <keyserver>No</keyserver>
          <policy>mpd1</policy>
          <keychain>kd</keychain>
          <fallback_keychain>fbkd</fallback_keychain>
         </ROW_mka_summary>
         <ROW_mka_summary>
          <ifname>Ethernet1/30</ifname>
          <status>Secured</status>
          <cipher>GCM-AES-128</cipher>
          <keyserver>No</keyserver>
          <policy>mpd2</policy>
          <keychain>kd</keychain>
          <fallback_keychain>fbkd</fallback_keychain>
         </ROW_mka_summary>
         <ROW_mka_summary>
          <ifname>Ethernet1/31</ifname>
          <status>Secured</status>
          <cipher>GCM-AES-128</cipher>
          <keyserver>Yes</keyserver>
          <policy>mps1</policy>
          <keychain>ks</keychain>
          <fallback_keychain>fbks</fallback_keychain>
         </ROW_mka_summary>
         <ROW_mka_summary>
          <ifname>Ethernet1/32</ifname>
          <status>Secured</status>
          <cipher>GCM-AES-128</cipher>
          <keyserver>Yes</keyserver>
          <policy>mps2</policy>
          <keychain>ks</keychain>
          <fallback_keychain>fbks</fallback_keychain>
         </ROW_mka_summary>
         <ROW_mka_summary>
```

```
          <ifname>Ethernet1/33</ifname>
          <status>Secured</status>
          <cipher>GCM-AES-128</cipher>
          <keyserver>Yes</keyserver>
          <policy>mpsr1</policy>
          <keychain>ksr</keychain>
          <fallback_keychain>fbksr</fallback_keychain>
         </ROW_mka_summary>
         <ROW_mka_summary>
          <ifname>Ethernet1/34</ifname>
          <status>Secured</status>
          <cipher>GCM-AES-128</cipher>
          <keyserver>Yes</keyserver>
          <policy>mpsr2</policy>
          <keychain>ksr</keychain>
          <fallback_keychain>fbksr</fallback_keychain>
         </ROW_mka_summary>
         <ROW_mka_summary>
          <ifname>Ethernet1/35</ifname>
          <status>Secured</status>
          <cipher>GCM-AES-XPN-256</cipher>
          <keyserver>Yes</keyserver>
          <policy>system-default-macsec-policy</policy>
          <keychain>ksr</keychain>
          <fallback_keychain>no keychain</fallback_keychain>
         </ROW_mka_summary>
         <ROW_mka_summary>
          <ifname>Ethernet1/36</ifname>
          <status>Secured</status>
          <cipher>GCM-AES-XPN-256</cipher>
          <keyserver>No</keyserver>
          <policy>system-default-macsec-policy</policy>
          <keychain>ksr</keychain>
          <fallback_keychain>no keychain</fallback_keychain>
         </ROW_mka_summary>
        </TABLE_mka_summary>
       </__readonly__>
      </__XML__OPT_Cmd_some_macsec___readonly__>
     </__XML__OPT_Cmd_some_macsec_summary>
    </mka>
   </macsec>
  </show>
</nf:data>
</nf:rpc-reply>
]]>]]>
switch(config)#
```

例 5：特定の MACsec ポリシーの構成を表示します

```
switch(config)# show macsec policy mpsr1 | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns="http://www.cisco.com/nxos:1.0:cts"
xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0">
<nf:data>
  <show>
   <macsec>
    <policy>
     <__XML__OPT_Cmd_show_macsec_policy_policy_name>
      <policy_name>mpsr1</policy_name>
      <__XML__OPT_Cmd_show_macsec_policy___readonly__>
       <__readonly__>
        <TABLE_macsec_policy>
         <ROW_macsec_policy>
          <name>mpsr1</name>
```

```
          <cipher_suite>GCM-AES-128</cipher_suite>
          <keyserver_priority>1</keyserver_priority>
          <window_size>1000</window_size>
          <conf_offset>30</conf_offset>
          <security_policy>should-secure</security_policy>
          <sak-expiry-time>60</sak-expiry-time>
          <include_icv_indicator>TRUE</include_icv_indicator>
         </ROW_macsec_policy>
        </TABLE_macsec_policy>
       </__readonly__>
      </__XML__OPT_Cmd_show_macsec_policy___readonly__>
     </__XML__OPT_Cmd_show_macsec_policy_policy_name>
    </policy>
   </macsec>
  </show>
</nf:data>
</nf:rpc-reply>
]]>]]>
switch(config)#
```

例 6：MACsec セキュリティ統計を表示します

```
switch(config)# show macsec secy statistics interface e1/29 | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns="http://www.cisco.com/nxos:1.0:cts"
xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0">
<nf:data>
  <show>
   <macsec>
    <secy>
     <statistics>
      <__XML__OPT_Cmd_some_macsec_secy_statistics_interface>
       <interface>
        <__XML__INTF_ifname>
         <__XML__PARAM_value>
          <__XML__INTF_output>Ethernet1/29</__XML__INTF_output>
         </__XML__PARAM_value>
        </__XML__INTF_ifname>
       </interface>
       <__XML__OPT_Cmd_some_macsec_secy_statistics___readonly__>
        <__readonly__>
         <TABLE_statistics>
          <ROW_statistics>
           <ifname2>Ethernet1/29</ifname2>
           <in_pkts_unicast_uncontrolled>6536205587</in_pkts_unicast_uncontrolled>
           <in_pkts_multicast_uncontrolled>10775</in_pkts_multicast_uncontrolled>
           <in_pkts_broadcast_uncontrolled>0</in_pkts_broadcast_uncontrolled>
           <in_rx_drop_pkts_uncontrolled>0</in_rx_drop_pkts_uncontrolled>
           <in_rx_err_pkts_uncontrolled>0</in_rx_err_pkts_uncontrolled>
           <in_pkts_unicast_controlled>N/A (N3K-C3636C-R not
supported)</in_pkts_unicast_controlled>
           <in_pkts_multicast_controlled>N/A (N3K-C3636C-R not
supported)</in_pkts_multicast_controlled>
           <in_pkts_broadcast_controlled>N/A (N3K-C3636C-R not
supported)</in_pkts_broadcast_controlled>
           <in_pkts_controlled>5173107800</in_pkts_controlled>
           <in_rx_drop_pkts_controlled>N/A (N3K-C3636C-R not
supported)</in_rx_drop_pkts_controlled>
           <in_rx_err_pkts_controlled>N/A (N3K-C3636C-R not
supported)</in_rx_err_pkts_controlled>
           <in_octets_uncontrolled>30491280431357</in_octets_uncontrolled>
           <in_octets_controlled>23935220809548</in_octets_controlled>
           <input_rate_uncontrolled_pps>N/A (N3K-C3636C-R not
supported)</input_rate_uncontrolled_pps>
```

```
            <input_rate_uncontrolled_bps>N/A (N3K-C3636C-R not
supported)</input_rate_uncontrolled_bps>
            <input_rate_controlled_pps>N/A (N3K-C3636C-R not
supported)</input_rate_controlled_pps>
            <input_rate_controlled_bps>N/A (N3K-C3636C-R not
supported)</input_rate_controlled_bps>
            <out_pkts_unicast_uncontrolled>N/A (N3K-C3636C-R not
supported)</out_pkts_unicast_uncontrolled>
            <out_pkts_multicast_uncontrolled>N/A (N3K-C3636C-R not
supported)</out_pkts_multicast_uncontrolled>
            <out_pkts_broadcast_uncontrolled>N/A (N3K-C3636C-R not
supported)</out_pkts_broadcast_uncontrolled>
            <out_rx_drop_pkts_uncontrolled>N/A (N3K-C3636C-R not
supported)</out_rx_drop_pkts_uncontrolled>
            <out_rx_err_pkts_uncontrolled>N/A (N3K-C3636C-R not
supported)</out_rx_err_pkts_uncontrolled>
            <out_pkts_unicast_controlled>N/A (N3K-C3636C-R not
supported)</out_pkts_unicast_controlled>
            <out_pkts_multicast_controlled>N/A (N3K-C3636C-R not
supported)</out_pkts_multicast_controlled>
            <out_pkts_broadcast_controlled>N/A (N3K-C3636C-R not
supported)</out_pkts_broadcast_controlled>
            <out_pkts_controlled>5173113173</out_pkts_controlled>
            <out_rx_drop_pkts_controlled>N/A (N3K-C3636C-R not
supported)</out_rx_drop_pkts_controlled>
            <out_rx_err_pkts_controlled>N/A (N3K-C3636C-R not
supported)</out_rx_err_pkts_controlled>
            <out_octets_uncontrolled>N/A (N3K-C3636C-R not
supported)</out_octets_uncontrolled>
            <out_octets_controlled>23946219872208</out_octets_controlled>
            <out_octets_common>30664229104600</out_octets_common>
            <output_rate_uncontrolled_pps>N/A (N3K-C3636C-R not
supported)</output_rate_uncontrolled_pps>
            <output_rate_uncontrolled_bps>N/A (N3K-C3636C-R not
supported)</output_rate_uncontrolled_bps>
            <output_rate_controlled_pps>N/A (N3K-C3636C-R not
supported)</output_rate_controlled_pps>
            <output_rate_controlled_bps>N/A (N3K-C3636C-R not
supported)</output_rate_controlled_bps>
            <in_pkts_transform_error>N/A (N3K-C3636C-R not
supported)</in_pkts_transform_error>
            <in_pkts_control>0</in_pkts_control>
            <in_pkts_untagged>N/A (N3K-C3636C-R not supported)</in_pkts_untagged>
            <in_pkts_no_tag>0</in_pkts_no_tag>
            <in_pkts_badtag>0</in_pkts_badtag>
            <in_pkts_no_sci>0</in_pkts_no_sci>
            <in_pkts_unknown_sci>0</in_pkts_unknown_sci>
            <in_pkts_tagged_ctrl>N/A (N3K-C3636C-R not supported)</in_pkts_tagged_ctrl>
            <out_pkts_transform_error>N/A (N3K-C3636C-R not
supported)</out_pkts_transform_error>
            <out_pkts_control>0</out_pkts_control>
            <out_pkts_untagged>N/A (N3K-C3636C-R not supported)</out_pkts_untagged>
            <TABLE_rx_sa_an>
             <ROW_rx_sa_an>
              <rx_sa_an>2</rx_sa_an>
              <in_pkts_unchecked>0</in_pkts_unchecked>
              <in_pkts_delayed>0</in_pkts_delayed>
              <in_pkts_late>0</in_pkts_late>
              <in_pkts_ok>1951781408</in_pkts_ok>
              <in_pkts_invalid>0</in_pkts_invalid>
              <in_pkts_not_valid>0</in_pkts_not_valid>
              <in_pkts_not_using_sa>0</in_pkts_not_using_sa>
              <in_pkts_unused_sa>0</in_pkts_unused_sa>
              <in_octets_decrypted>8952613134278</in_octets_decrypted>
```

```
            <in_octets_validated>0</in_octets_validated>
           </ROW_rx_sa_an>
          </TABLE_rx_sa_an>
          <TABLE_tx_sa_an>
           <ROW_tx_sa_an>
            <tx_sa_an>2</tx_sa_an>
            <out_pkts_encrypted_protected>1951773387</out_pkts_encrypted_protected>
            <out_pkts_too_long>N/A (N3K-C3636C-R not supported)</out_pkts_too_long>
            <out_pkts_sa_not_inuse>N/A (N3K-C3636C-R not
supported)</out_pkts_sa_not_inuse>
           <out_octets_encrypted_protected>8952606203313</out_octets_encrypted_protected>

           </ROW_tx_sa_an>
          </TABLE_tx_sa_an>
         </ROW_statistics>
        </TABLE_statistics>
       </__readonly__>
      </__XML__OPT_Cmd_some_macsec_secy_statistics___readonly__>
     </__XML__OPT_Cmd_some_macsec_secy_statistics_interface>
    </statistics>
   </secy>
  </macsec>
 </show>
</nf:data>
</nf:rpc-reply>
]]>]]>
switch(config)#
```

例 7：MACsec の実行構成情報を表示します

```
switch(config)# show running-config macsec | xml

!Command: show running-config macsec
!Running configuration last done at: Tue Dec 15 11:53:10 2020
!Time: Tue Dec 15 13:58:58 2020

version 10.1(1) Bios:version 01.14
****************************************
This may take time. Please be patient.
****************************************
<?xml version="1.0"?>
<nf:rpc xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="http://www.cisco.com/nxos:10.1.1.:configure_"
xmlns:m="http://www.cisco.com/nxos:10.1.1.:_exec"
xmlns:m1="http://www.cisco.com/nxos:10.1.1.:configure__macsec-policy"
xmlns:m2="http://www.cisco.com/nxos:10.1.1.:configure__if-ethernet-all" message-id="1">
  <nf:get-config>
    <nf:source>
      <nf:running/>
    </nf:source>
    <nf:filter>
      <m:configure>
        <m:terminal>
          <feature>
            <macsec/>
          </feature>
          <macsec>
            <policy>
              <__XML__PARAM__policy_name>
                <__XML__value>mpd1</__XML__value>
                <m1:cipher-suite>
                  <m1:__XML__PARAM__suite>
                    <m1:__XML__value>GCM-AES-128</m1:__XML__value>
                  </m1:__XML__PARAM__suite>
```

```
      </m1:cipher-suite>
      <m1:conf-offset>
        <m1:__XML__PARAM__offset>
          <m1:__XML__value>CONF-OFFSET-30</m1:__XML__value>
        </m1:__XML__PARAM__offset>
      </m1:conf-offset>
    </__XML__PARAM__policy_name>
  </policy>
</macsec>
<macsec>
  <policy>
    <__XML__PARAM__policy_name>
      <__XML__value>mpd2</__XML__value>
      <m1:cipher-suite>
        <m1:__XML__PARAM__suite>
          <m1:__XML__value>GCM-AES-128</m1:__XML__value>
        </m1:__XML__PARAM__suite>
      </m1:cipher-suite>
      <m1:conf-offset>
        <m1:__XML__PARAM__offset>
          <m1:__XML__value>CONF-OFFSET-30</m1:__XML__value>
        </m1:__XML__PARAM__offset>
      </m1:conf-offset>
      <m1:security-policy>
        <m1:__XML__PARAM__policy>
          <m1:__XML__value>must-secure</m1:__XML__value>
        </m1:__XML__PARAM__policy>
      </m1:security-policy>
    </__XML__PARAM__policy_name>
  </policy>
</macsec>
<macsec>
  <policy>
    <__XML__PARAM__policy_name>
      <__XML__value>mps1</__XML__value>
      <m1:cipher-suite>
        <m1:__XML__PARAM__suite>
          <m1:__XML__value>GCM-AES-128</m1:__XML__value>
       </m1:__XML__PARAM__suite>
      </m1:cipher-suite>
      <m1:key-server-priority>
        <m1:__XML__PARAM__pri>
          <m1:__XML__value>1</m1:__XML__value>
        </m1:__XML__PARAM__pri>
      </m1:key-server-priority>
      <m1:conf-offset>
        <m1:__XML__PARAM__offset>
          <m1:__XML__value>CONF-OFFSET-30</m1:__XML__value>
        </m1:__XML__PARAM__offset>
      </m1:conf-offset>
      <m1:sak-expiry-time>
        <m1:__XML__PARAM__ts>
          <m1:__XML__value>60</m1:__XML__value>
        </m1:__XML__PARAM__ts>
      </m1:sak-expiry-time>
      <m1:include-icv-indicator/>
    </__XML__PARAM__policy_name>
  </policy>
</macsec>
<macsec>
  <policy>
    <__XML__PARAM__policy_name>
      <__XML__value>mps2</__XML__value>
      <m1:cipher-suite>
```

```
            <m1:__XML__PARAM__suite>
              <m1:__XML__value>GCM-AES-128</m1:__XML__value>
            </m1:__XML__PARAM__suite>
          </m1:cipher-suite>
          <m1:key-server-priority>
            <m1:__XML__PARAM__pri>
              <m1:__XML__value>1</m1:__XML__value>
            </m1:__XML__PARAM__pri>
          </m1:key-server-priority>
          <m1:window-size>
            <m1:__XML__PARAM__size>
              <m1:__XML__value>1000</m1:__XML__value>
            </m1:__XML__PARAM__size>
          </m1:window-size>
          <m1:conf-offset>
            <m1:__XML__PARAM__offset>
              <m1:__XML__value>CONF-OFFSET-30</m1:__XML__value>
            </m1:__XML__PARAM__offset>
          </m1:conf-offset>
          <m1:security-policy>
            <m1:__XML__PARAM__policy>
              <m1:__XML__value>must-secure</m1:__XML__value>
            </m1:__XML__PARAM__policy>
          </m1:security-policy>
          <m1:sak-expiry-time>
            <m1:__XML__PARAM__ts>
              <m1:__XML__value>60</m1:__XML__value>
            </m1:__XML__PARAM__ts>
          </m1:sak-expiry-time>
          <m1:include-icv-indicator/>
        </__XML__PARAM__policy_name>
      </policy>
    </macsec>
    <macsec>
      <policy>
        <__XML__PARAM__policy_name>
          <__XML__value>mpsr1</__XML__value>
          <m1:cipher-suite>
            <m1:__XML__PARAM__suite>
              <m1:__XML__value>GCM-AES-128</m1:__XML__value>
            </m1:__XML__PARAM__suite>
          </m1:cipher-suite>
          <m1:key-server-priority>
            <m1:__XML__PARAM__pri>
              <m1:__XML__value>1</m1:__XML__value>
            </m1:__XML__PARAM__pri>
          </m1:key-server-priority>
          <m1:window-size>
            <m1:__XML__PARAM__size>
              <m1:__XML__value>1000</m1:__XML__value>
            </m1:__XML__PARAM__size>
          </m1:window-size>
          <m1:conf-offset>
            <m1:__XML__PARAM__offset>
              <m1:__XML__value>CONF-OFFSET-30</m1:__XML__value>
            </m1:__XML__PARAM__offset>
          </m1:conf-offset>
          <m1:sak-expiry-time>
            <m1:__XML__PARAM__ts>
              <m1:__XML__value>60</m1:__XML__value>
            </m1:__XML__PARAM__ts>
          </m1:sak-expiry-time>
          <m1:include-icv-indicator/>
        </__XML__PARAM__policy_name>
```

```
  </policy>
</macsec>
<macsec>
  <policy>
    <__XML__PARAM__policy_name>
      <__XML__value>mpsr2</__XML__value>
      <m1:cipher-suite>
        <m1:__XML__PARAM__suite>
          <m1:__XML__value>GCM-AES-128</m1:__XML__value>
        </m1:__XML__PARAM__suite>
      </m1:cipher-suite>
      <m1:key-server-priority>
        <m1:__XML__PARAM__pri>
          <m1:__XML__value>1</m1:__XML__value>
        </m1:__XML__PARAM__pri>
      </m1:key-server-priority>
      <m1:window-size>
        <m1:__XML__PARAM__size>
          <m1:__XML__value>1000</m1:__XML__value>
        </m1:__XML__PARAM__size>
      </m1:window-size>
      <m1:conf-offset>
        <m1:__XML__PARAM__offset>
          <m1:__XML__value>CONF-OFFSET-30</m1:__XML__value>
        </m1:__XML__PARAM__offset>
      </m1:conf-offset>
      <m1:security-policy>
        <m1:__XML__PARAM__policy>
          <m1:__XML__value>must-secure</m1:__XML__value>
        </m1:__XML__PARAM__policy>
      </m1:security-policy>
      <m1:sak-expiry-time>
        <m1:__XML__PARAM__ts>
          <m1:__XML__value>60</m1:__XML__value>
        </m1:__XML__PARAM__ts>
      </m1:sak-expiry-time>
      <m1:include-icv-indicator/>
    </__XML__PARAM__policy_name>
  </policy>
</macsec>
<interface>
  <__XML__PARAM__interface>
    <__XML__value>Ethernet1/29</__XML__value>
    <m2:macsec>
      <m2:keychain>
        <m2:__XML__PARAM__keychain_name>
          <m2:__XML__value>kd</m2:__XML__value>
          <m2:policy>
            <m2:__XML__PARAM__policy_name>
              <m2:__XML__value>mpd1</m2:__XML__value>
              <m2:fallback-keychain>
                <m2:__XML__PARAM__fallback_kc_name>
                  <m2:__XML__value>fbkd</m2:__XML__value>
                </m2:__XML__PARAM__fallback_kc_name>
              </m2:fallback-keychain>
            </m2:__XML__PARAM__policy_name>
          </m2:policy>
        </m2:__XML__PARAM__keychain_name>
      </m2:keychain>
    </m2:macsec>
  </__XML__PARAM__interface>
</interface>
<interface>
  <__XML__PARAM__interface>
```

```
    <__XML__value>Ethernet1/30</__XML__value>
    <m2:macsec>
      <m2:keychain>
        <m2:__XML__PARAM__keychain_name>
          <m2:__XML__value>kd</m2:__XML__value>
          <m2:policy>
            <m2:__XML__PARAM__policy_name>
              <m2:__XML__value>mpd2</m2:__XML__value>
              <m2:fallback-keychain>
                <m2:__XML__PARAM__fallback_kc_name>
                  <m2:__XML__value>fbkd</m2:__XML__value>
                </m2:__XML__PARAM__fallback_kc_name>
              </m2:fallback-keychain>
            </m2:__XML__PARAM__policy_name>
          </m2:policy>
        </m2:__XML__PARAM__keychain_name>
      </m2:keychain>
    </m2:macsec>
  </__XML__PARAM__interface>
</interface>
<interface>
  <__XML__PARAM__interface>
    <__XML__value>Ethernet1/31</__XML__value>
    <m2:macsec>
      <m2:keychain>
        <m2:__XML__PARAM__keychain_name>
          <m2:__XML__value>ks</m2:__XML__value>
          <m2:policy>
            <m2:__XML__PARAM__policy_name>
              <m2:__XML__value>mps1</m2:__XML__value>
              <m2:fallback-keychain>
                <m2:__XML__PARAM__fallback_kc_name>
                  <m2:__XML__value>fbks</m2:__XML__value>
                </m2:__XML__PARAM__fallback_kc_name>
              </m2:fallback-keychain>
            </m2:__XML__PARAM__policy_name>
          </m2:policy>
        </m2:__XML__PARAM__keychain_name>
      </m2:keychain>
    </m2:macsec>
  </__XML__PARAM__interface>
</interface>
<interface>
  <__XML__PARAM__interface>
    <__XML__value>Ethernet1/32</__XML__value>
    <m2:macsec>
      <m2:keychain>
        <m2:__XML__PARAM__keychain_name>
          <m2:__XML__value>ks</m2:__XML__value>
          <m2:policy>
            <m2:__XML__PARAM__policy_name>
              <m2:__XML__value>mps2</m2:__XML__value>
              <m2:fallback-keychain>
                <m2:__XML__PARAM__fallback_kc_name>
                  <m2:__XML__value>fbks</m2:__XML__value>
                </m2:__XML__PARAM__fallback_kc_name>
              </m2:fallback-keychain>
            </m2:__XML__PARAM__policy_name>
          </m2:policy>
        </m2:__XML__PARAM__keychain_name>
      </m2:keychain>
    </m2:macsec>
  </__XML__PARAM__interface>
</interface>
```

```
<interface>
  <__XML__PARAM__interface>
    <__XML__value>Ethernet1/33</__XML__value>
    <m2:macsec>
      <m2:keychain>
        <m2:__XML__PARAM__keychain_name>
          <m2:__XML__value>ksr</m2:__XML__value>
          <m2:policy>
            <m2:__XML__PARAM__policy_name>
              <m2:__XML__value>mpsr1</m2:__XML__value>
              <m2:fallback-keychain>
                <m2:__XML__PARAM__fallback_kc_name>
                  <m2:__XML__value>fbksr</m2:__XML__value>
                </m2:__XML__PARAM__fallback_kc_name>
              </m2:fallback-keychain>
            </m2:__XML__PARAM__policy_name>
          </m2:policy>
        </m2:__XML__PARAM__keychain_name>
      </m2:keychain>
    </m2:macsec>
  </__XML__PARAM__interface>
</interface>
<interface>
  <__XML__PARAM__interface>
    <__XML__value>Ethernet1/34</__XML__value>
    <m2:macsec>
      <m2:keychain>
        <m2:__XML__PARAM__keychain_name>
          <m2:__XML__value>ksr</m2:__XML__value>
          <m2:policy>
            <m2:__XML__PARAM__policy_name>
              <m2:__XML__value>mpsr2</m2:__XML__value>
              <m2:fallback-keychain>
                <m2:__XML__PARAM__fallback_kc_name>
                  <m2:__XML__value>fbksr</m2:__XML__value>
                </m2:__XML__PARAM__fallback_kc_name>
              </m2:fallback-keychain>
            </m2:__XML__PARAM__policy_name>
          </m2:policy>
        </m2:__XML__PARAM__keychain_name>
      </m2:keychain>
    </m2:macsec>
  </__XML__PARAM__interface>
</interface>
<interface>
  <__XML__PARAM__interface>
    <__XML__value>Ethernet1/35</__XML__value>
    <m2:macsec>
      <m2:keychain>
        <m2:__XML__PARAM__keychain_name>
          <m2:__XML__value>ksr</m2:__XML__value>
          <m2:policy>
            <m2:__XML__PARAM__policy_name>
              <m2:__XML__value>system-default-macsec-policy</m2:__XML__value>
            </m2:__XML__PARAM__policy_name>
          </m2:policy>
        </m2:__XML__PARAM__keychain_name>
      </m2:keychain>
    </m2:macsec>
  </__XML__PARAM__interface>
</interface>
<interface>
  <__XML__PARAM__interface>
    <__XML__value>Ethernet1/36</__XML__value>
```

```
                <m2:macsec>
                  <m2:keychain>
                    <m2:__XML__PARAM__keychain_name>
                      <m2:__XML__value>ksr</m2:__XML__value>
                      <m2:policy>
                        <m2:__XML__PARAM__policy_name>
                          <m2:__XML__value>system-default-macsec-policy</m2:__XML__value>
                        </m2:__XML__PARAM__policy_name>
                      </m2:policy>
                    </m2:__XML__PARAM__keychain_name>
                  </m2:keychain>
                </m2:macsec>
              </__XML__PARAM__interface>
            </interface>
          </m:terminal>
        </m:configure>
      </nf:filter>
    </nf:get-config>
</nf:rpc>
]]>]]>

switch(config)#
```

MIB

MACsec は次の MIB をサポートします。

- IEEE8021-SECY-MIB
- CISCO-SECY-EXT-MIB

関連資料

関連項目	マニュアル タイトル
キーチェーン管理	『Cisco Nexus 3600 Series NX-OS Security Configuration Guide』
システム メッセージ	Cisco Nexus 3600 シリーズ NX-OS システム メッセージ リファレンス

関連資料

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。