CHAPTER 13

インターフェイス コンフィギュレーションの実行（ルーテッド モード）

この章では、ルーテッド ファイアウォール モードで、すべてのモデルのインターフェイス コンフィギュレーションを実行するためのタスクについて説明します。この章は、次の項で構成されています。

（注） マルチ コンテキスト モードでは、この項のタスクをコンテキスト実行スペースで実行してください。[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

ルーテッド モードでのインターフェイス コンフィギュレーションの実行の概要

この項は、次の内容で構成されています。

セキュリティ レベル

各インターフェイスには、0（最下位）～ 100（最上位）のセキュリティ レベルを設定する必要があります。たとえば、内部ホスト ネットワークなど、最もセキュアなネットワークにはレベル 100 を割り当てる必要があります。一方、インターネットなどに接続する外部ネットワークにはレベル 0 が割り当てられる場合があります。DMZ など、その他のネットワークはその中間に設定できます。複数のイン

ターフェイスを同じセキュリティ レベルに割り当てることができます。詳細については、「同じセキュリティ レベルの通信の許可」（P.13-20）を参照してください。

レベルによって、次の動作が制御されます。

- ネットワーク アクセス：デフォルトで、高いセキュリティ レベルのインターフェイスから低いセキュリティ レベルのインターフェイスへの通信（発信）は暗黙的に許可されます。高いセキュリティ レベルのインターフェイス上のホストは、低いセキュリティ レベルのインターフェイス上の任意のホストにアクセスできます。インターフェイスにアクセス リストを適用することによって、アクセスを制限できます。

  同じセキュリティ レベルのインターフェイスの通信をイネーブルにすると（「同じセキュリティ レベルの通信の許可」（P.13-20）を参照）、同じセキュリティ レベルまたはそれより低いセキュリティ レベルの他のインターフェイスにアクセスするインターフェイスは、暗黙的に許可されます。

- インスペクション エンジン：一部のアプリケーション インスペクション エンジンはセキュリティ レベルに依存します。同じセキュリティ レベルのインターフェイス間では、インスペクション エンジンは発信と着信のいずれのトラフィックに対しても適用されます。
  - NetBIOS インスペクション エンジン：発信接続に対してのみ適用されます。
  - SQL*Net インスペクション エンジン：SQL*Net（旧称 OraServ）ポートとの制御接続が一対のホスト間に存在する場合、着信データ接続だけが ASA を通過することが許可されます。

- フィルタリング：HTTP(S) および FTP フィルタリングは、（高いレベルから低いレベルへの）発信接続にのみ適用されます。

  同じセキュリティ レベルのインターフェイス間の通信をイネーブルにすると、どちらの方向のトラフィックにもフィルタリングが適用できます。

- **established** コマンド：このコマンドを使用すると、高いレベルのホストから低いレベルのホストへの接続がすでに確立されている場合、低いセキュリティ レベルのホストから高いセキュリティ レベルのホストへの戻り接続が許可されます。

  セキュリティ レベルが同じインターフェイス間の通信をイネーブルにすると、両方向に対して **established** コマンドを設定できます。

デュアル IP スタック（IPv4 および IPv6）

ASA は、1 つのインターフェイス上で IPv6 と IPv4 の両方のコンフィギュレーションをサポートします。そのために特別なコマンドを入力する必要はありません。単純に、IPv4 コンフィギュレーション コマンドと IPv6 コンフィギュレーション コマンドを通常と同じように入力します。IPv4 と IPv6 の両方で、デフォルト ルートを設定してください。

ルーテッド モードのインターフェイス コンフィギュレーションを実行するためのライセンス要件

モデル	ライセンス要件
ASA 5505	VLAN： 基本ライセンス：3（2 つの正規ゾーンともう 1 つの制限ゾーンだけが他の 1 つのゾーンと通信可能） Security Plus ライセンス：20 VLAN トランク： 基本ライセンス：なし。 Security Plus ライセンス：8 すべての種類のインターフェイス[1]： 基本ライセンス：52。 Security Plus ライセンス：120。

1. VLAN、物理、冗長、およびブリッジ グループ インターフェイスなど、すべてを合わせたインターフェイスの最大数。

モデル	ライセンス要件
ASA 5510	VLAN： 基本ライセンス：50 Security Plus ライセンス：100 インターフェイス速度： 基本ライセンス：すべてのインターフェイスがファスト イーサネット。 Security Plus ライセンス：Ethernet 0/0 および 0/1：ギガビット イーサネット、その他すべてはファスト イーサネット。 すべての種類のインターフェイス[1]： 基本ライセンス：52 Security Plus ライセンス：120
ASA 5520	VLAN： 基本ライセンス：150 すべての種類のインターフェイス[1]： 基本ライセンス：640
ASA 5540	VLAN： 基本ライセンス：200 すべての種類のインターフェイス[1]： 基本ライセンス：840
ASA 5550	VLAN： 基本ライセンス：400 すべての種類のインターフェイス[1]： 基本ライセンス：1640

モデル	ライセンス要件
ASA 5580	VLAN： 基本ライセンス：1024 すべての種類のインターフェイス[1]： 基本ライセンス：4176
ASA 5512-X	VLAN： 基本ライセンス：50 すべての種類のインターフェイス[1]： 基本ライセンス：328
ASA 5515-X	VLAN： 基本ライセンス：100 すべての種類のインターフェイス[1]： 基本ライセンス：528
ASA 5525-X	VLAN： 基本ライセンス：200 すべての種類のインターフェイス[1]： 基本ライセンス：928
ASA 5545-X	VLAN： 基本ライセンス：300 すべての種類のインターフェイス[1]： 基本ライセンス：1328
ASA 5555-X	VLAN： 基本ライセンス：500 すべての種類のインターフェイス[1]： 基本ライセンス：2128
ASA 5585-X	VLAN： 基本ライセンス：1024 SSP-10 および SSP-20 のインターフェイス速度： 基本ライセンス：ファイバ インターフェイスの場合 1 ギガビット イーサネット 10 GE I/O ライセンス（Security Plus）：ファイバ インターフェイスの場合 10 ギガビット イーサネット （SSP-40 および SSP-60 は 10 ギガビット イーサネットをデフォルトでサポートします）。 すべての種類のインターフェイス[1]： 基本ライセンス：4176

1. VLAN、物理、冗長、ブリッジ グループ、および EtherChannel インターフェイスなど、すべてを合わせたインターフェイスの最大数。

モデル	ライセンス要件
ASASM	VLAN： 基本ライセンス：1000

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

- マルチ コンテキスト モードでの ASA 5510 以降の場合、第 11 章「インターフェイス コンフィギュレーションの開始（ASA 5510 以降）」に従って、システム実行スペースで物理インターフェイスを設定します。次に、この章に従って、コンテキスト実行スペースで論理インターフェイス パラメータを設定します。マルチ コンテキスト モードの ASASM の場合は、スイッチのスイッチポートおよび VLAN を設定し、第 2 章「ASA サービス モジュール を使用するためのスイッチの設定」に従って VLAN を ASASM に割り当てます。

  ASA 5505 はマルチ コンテキスト モードをサポートしません。

- マルチ コンテキスト モードで設定できるのは、「マルチ コンテキストの設定」（P.8-15）に従ってシステム コンフィギュレーションでコンテキストにすでに割り当てられているコンテキスト インターフェイスだけです。

- PPPoE は、マルチ コンテキスト モードではサポートされていません。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードでサポートされています。トランスペアレント モードの場合は、第 14 章「インターフェイス コンフィギュレーションの実行（トランスペアレント モード、8.4 以降）」を参照してください。

フェールオーバーのガイドライン

フェールオーバー インターフェイスの設定は、この章の手順では完了しません。フェールオーバーおよびステート リンクの設定については、第 9 章「フェールオーバーの設定」を参照してください。マルチ コンテキスト モードでは、フェールオーバー インターフェイスがシステム コンフィギュレーションに設定されます。

IPv6 のガイドライン

IPv6 をサポートします。

ASASM の VLAN ID に関するガイドライン

コンフィギュレーションにはあらゆる VLAN ID を追加できますが、トラフィックを転送できるのはスイッチによって ASA に割り当てられた VLAN だけです。ASA に割り当てられたすべての VLAN を表示するには、**show vlan** コマンドを使用します。

スイッチによって ASA にまだ割り当てられていない VLAN にインターフェイスを追加した場合、そのインターフェイスはダウン ステートになります。ASA に VLAN を割り当てた時点で、インターフェイスはアップ ステートに変化します。インターフェイス ステートの詳細については、**show interface** コマンドを参照してください。

デフォルト設定

この項では、工場出荷時のデフォルト コンフィギュレーションが設定されていない場合のインターフェイスのデフォルト設定を示します。工場出荷時のデフォルト コンフィギュレーションについては、「工場出荷時のデフォルト コンフィギュレーション」（P.3-19）を参照してください。

デフォルトのセキュリティ レベル

デフォルトのセキュリティ レベルは 0 です。インターフェイスに名前「inside」を付けて、明示的にセキュリティ レベルを設定しないと、ASA はセキュリティ レベルを 100 に設定します。

（注）　インターフェイスのセキュリティ レベルを変更したときに、既存の接続がタイムアウトするまで待機せずに新しいセキュリティ情報を使用する必要がある場合は、**clear local-host** コマンドを使用して接続をクリアできます。

ASASM のインターフェイスのデフォルトの状態

- シングル モードまたはシステム実行スペースでは、VLAN インターフェイスがデフォルトでイネーブルになります。
- マルチ コンテキスト モードでは、システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。

ジャンボ フレーム サポート

デフォルトでは、ASASM はジャンボ フレームをサポートしています。「MAC アドレス、MTU、TCP MSS の設定」（P.13-13）に従って、目的のパケット サイズの MTU を設定します。

ルーテッド モードでのインターフェイス コンフィギュレーションの実行

この項は、次の内容で構成されています。

- 「IPv6 アドレッシングの設定」（P.13-16）
- 「同じセキュリティ レベルの通信の許可」（P.13-20）

インターフェイス コンフィギュレーションを実行するためのタスク フロー

ステップ 1　モデルに応じてインターフェイスを設定します。

- ASA 5510 以降：第 11 章「インターフェイス コンフィギュレーションの開始（ASA 5510 以降）」
- ASA 5505：第 12 章「インターフェイス コンフィギュレーションの開始（ASA 5505）」
- ASASM：第 2 章「ASA サービス モジュール を使用するためのスイッチの設定」

ステップ 2　（マルチ コンテキスト モード）「マルチ コンテキストの設定」（P.8-15）に従って、コンテキストにインターフェイスを割り当てます。

ステップ 3　（マルチ コンテキスト モード）[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

ステップ 4　インターフェイス名、セキュリティ レベル、IPv4 アドレスなどの一般的なインターフェイス パラメータを設定します。「一般的なインターフェイス パラメータの設定」（P.13-7）を参照してください。

ステップ 5　（任意）MAC アドレスと MTU を設定します。「MAC アドレス、MTU、TCP MSS の設定」（P.13-13）を参照してください。

ステップ 6　（任意）IPv6 アドレッシングを設定します。「IPv6 アドレッシングの設定」（P.13-16）を参照してください。

ステップ 7　（任意）2 つのインターフェイス間の通信を許可するか、またはトラフィックが同じインターフェイスに入って同じインターフェイスから出ることを許可することで、同じセキュリティ レベルの通信を許可します。「同じセキュリティ レベルの通信の許可」（P.13-20）を参照してください。

一般的なインターフェイス パラメータの設定

この手順では、名前、セキュリティ レベル、IPv4 アドレス、およびその他のオプションを設定する方法について説明します。

ASA 5510 以降では、次のインターフェイス タイプのインターフェイス パラメータを設定する必要があります。

- 物理インターフェイス
- VLAN サブインターフェイス
- 冗長インターフェイス
- EtherChannel インターフェイス

ASA 5505 および ASASM では、次のインターフェイス タイプのインターフェイス パラメータを設定する必要があります。

- VLAN インターフェイス

ガイドラインと制限事項

- ASA 5550 では、スループットを最大にするために、トラフィックを 2 つのインターフェイス スロットに分散してください。たとえば、内部インターフェイスをスロット 1 に、外部インターフェイスをスロット 0 に割り当てます。
- フェールオーバーを使用している場合は、フェールオーバー通信およびステートフル フェールオーバー通信に予約されているインターフェイスには、この方法で名前を付けないでください。フェールオーバーおよびステート リンクの設定については、第 9 章「フェールオーバーの設定」を参照してください。

制限事項

- PPPoE は、マルチ コンテキスト モードではサポートされていません。
- ASASM では、PPPoE および DHCP はサポートされません。

前提条件

- モデルに応じてインターフェイスを設定します。
  - ASA 5510 以降：第 11 章「インターフェイス コンフィギュレーションの開始（ASA 5510 以降）」
  - ASA 5505：第 12 章「インターフェイス コンフィギュレーションの開始（ASA 5505）」
  - ASASM：第 2 章「ASA サービス モジュール を使用するためのスイッチの設定」
- マルチ コンテキスト モードで設定できるのは、「マルチ コンテキストの設定」（P.8-15）に従ってシステム コンフィギュレーションでコンテキストにすでに割り当てられているコンテキスト インターフェイスだけです。
- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システムからコンテキスト コンフィギュレーションに変更するには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

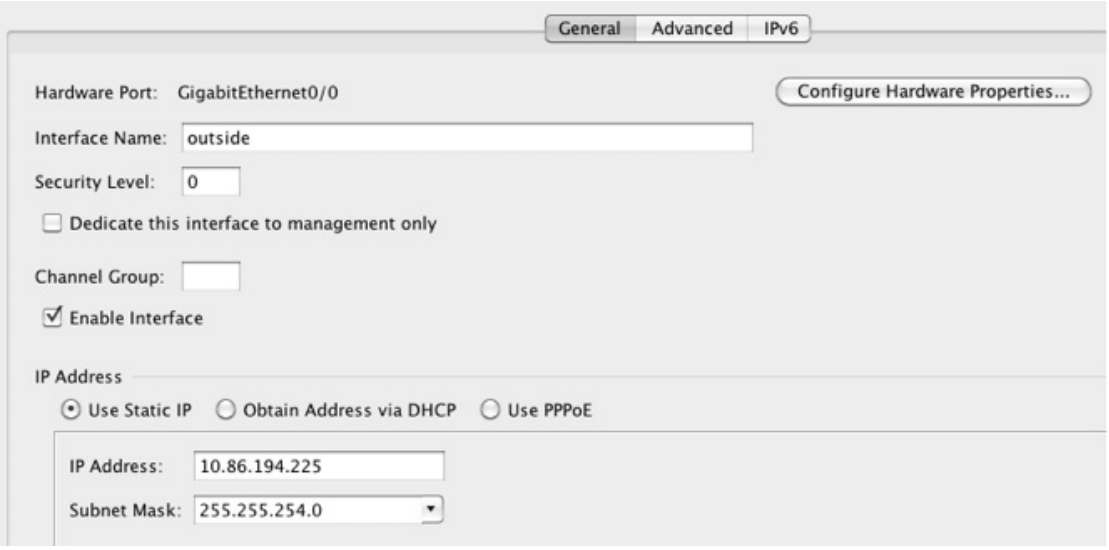
手順の詳細

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。

ASA 5505 では、[Interfaces] タブがデフォルトで表示されます。

ステップ 2　インターフェイス行を選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。



ステップ 3　[Interface Name] フィールドに、名前を 48 文字以内で入力します。

ステップ 4　[Security level] フィールドに、0（最低）～ 100（最高）のレベルを入力します。

詳細については、「セキュリティ レベル」（P.13-1）を参照してください。

ステップ 5　（任意。冗長インターフェイスではサポートされていません）このインターフェイスを管理専用インターフェイスとして設定するには、[Dedicate this interface to management-only] チェックボックスをオンにします。

管理専用インターフェイスでは、通過トラフィックは受け入れられません。ASA 5510 以降の場合、詳細については、「前提条件」（P.13-8）を参照してください。

（ASA 5512-X ～ ASA 5555-X）Management 0/0 インターフェイスではこのオプションをディセーブルにできません。

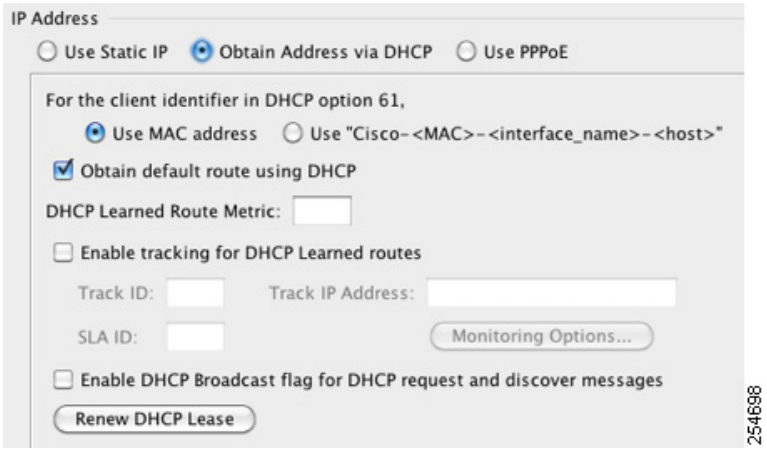
（注）　[Channel Group] フィールドは読み取り専用で、インターフェイスが EtherChannel の一部であるかどうかを示します。

ステップ 6　インターフェイスがまだイネーブルでない場合は、[Enable Interface] チェックボックスをオンにします。

ステップ 7　IP アドレスを設定するには、次のいずれかのオプションを使用します。

（注）　フェールオーバーで使用する場合、IP アドレスとスタンバイ アドレスを手動で設定する必要があります。DHCP および PPPoE はサポートされません。[Configuration] > [Device Management] > [High Availability] > [Failover] > [Interfaces] タブのスタンバイ IP アドレスを設定します。

- IP アドレスを手動で設定するには、[Use Static IP] オプション ボタンをクリックして IP アドレスとマスクを入力します。
- DHCP サーバから IP アドレスを取得するには、[Obtain Address via DHCP] オプション ボタンをクリックします。



a. MAC アドレスがオプション 61 の DHCP 要求パケット内に保存されるようにするには、[Use MAC Address] オプション ボタンをクリックします。

いくつかの ISP はインターフェイスの MAC アドレスにオプション 61 が必要です。MAC アドレスが DHCP 要求パケットに含まれていない場合、IP アドレスは割り当てられません。

b. オプション 61 用に生成された文字列を使用するには、[Use "Cisco-<MAC>-<interface_name>-<host>"] をクリックします。

c. （任意）DHCP サーバからデフォルト ルートを取得するには、[Obtain Default Route Using DHCP] をオンにします。

d. （任意）アドミニストレーティブ ディスタンスを既知のルートに割り当てるには、[DHCP Learned Route Metric] フィールドに 1 ～ 255 の値を入力します。このフィールドを空白のままにすると、既知のルートのアドミニストレーティブ ディスタンスは 1 になります。

e. （任意）DHCP の既知のルートのトラッキングをイネーブルにするには、[Enable Tracking for DHCP Learned Routes] をオンにします。次の値を設定します。

[Track ID] : ルート トラッキング プロセスに使用される一意の識別子。有効な値は、1 ～ 500 です。

[Track IP Address] : トラッキングの対象 IP アドレスを入力します。通常、ルートのネクストホップはゲートウェイ IP アドレスです。ただし、そのインターフェイスの先にネットワーク オブジェクトがあれば表示されます。

（注） ルート トラッキングは、シングル ルーテッド モードでだけ使用できます。

[SLA ID] : SLA モニタリング プロセスの一意の ID です。有効な値は 1 ～ 2147483647 です。

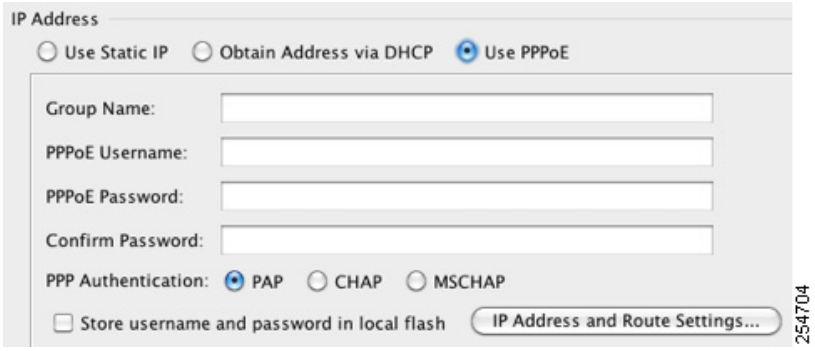
[Monitor Options] : このボタンをクリックすると [Route Monitoring Options] ダイアログボックスが開きます。[Route Monitoring Options] ダイアログボックスで、トラッキング対象オブジェクトのモニタリング プロセスのパラメータを設定できます。

f. （任意）DHCP クライアントが IP アドレス要求の探索を送信する場合に、DHCP パケット ヘッダーでブロードキャスト フラグを 1 に設定するには、[Enable DHCP Broadcast flag for DHCP request and discover messages] をオンにします。

DHCP サーバはこのブロードキャスト フラグをリッスンし、フラグが 1 に設定されている場合は応答パケットをブロードキャストします。

g. （任意）リースを更新するには、[Renew DHCP Lease] をクリックします。

- （シングル モードのみ）PPPoE を使用して IP アドレスを取得するには、[Use PPPoE] をオンにします。



  a. [Group Name] フィールドで、グループ名を指定します。
  b. [PPPoE Username] フィールドで、ISP から提供されたユーザ名を指定します。
  c. [PPPoE Password] フィールドで、ISP から提供されたパスワードを指定します。
  d. [Confirm Password] フィールドに、パスワードを再入力します。
  e. PPP 認証の場合、[PAP]、[CHAP]、または [MSCHAP] のいずれかのオプション ボタンをクリックします。

     PAP は認証時にクリアテキストのユーザ名とパスワードを渡すため、セキュアではありません。CHAP では、サーバのチャレンジに対して、クライアントは暗号化された「チャレンジとパスワード」およびクリアテキストのユーザ名を返します。CHAP は PAP よりセキュアですが、データを暗号化しません。MSCHAP は CHAP に似ていますが、サーバが CHAP のようにクリア テキスト パスワードを扱わず、暗号化されたパスワードだけを保存、比較するため、CHAP よりセキュアです。また、MSCHAP では MPPE によるデータの暗号化のためのキーを生成します。

  f. （任意）フラッシュ メモリにユーザ名とパスワードを保存するには、[Store Username and Password in Local Flash] チェックボックスをオンにします。

     ASA は、NVRAM の特定の場所にユーザ名とパスワードを保存します。Auto Update Server が **clear config** コマンドを ASA に送信して、接続が中断されると、ASA は NVRAM からユーザ名とパスワードを読み取り、アクセス コンセントレータに対して再度認証できます。

  g. （任意）[PPPoE IP Address and Route Settings] ダイアログボックスを表示し、アドレッシングおよびトラッキングのオプションを選択するには、[IP Address and Route Settings] をクリックします。詳細については、「PPPoE IP Address and Route Settings」（P.13-12）を参照してください。

ステップ 8　（任意）[Description] フィールドに、このインターフェイスの説明を入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。フェールオーバーまたはステート リンクの場合、説明は、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」などの固定の値になります。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

（注）　（ASA 5510 以降）[Configure Hardware Properties] ボタンに関する情報については、「物理インターフェイスのイネーブル化およびイーサネット パラメータの設定」（P.11-26）を参照してください。

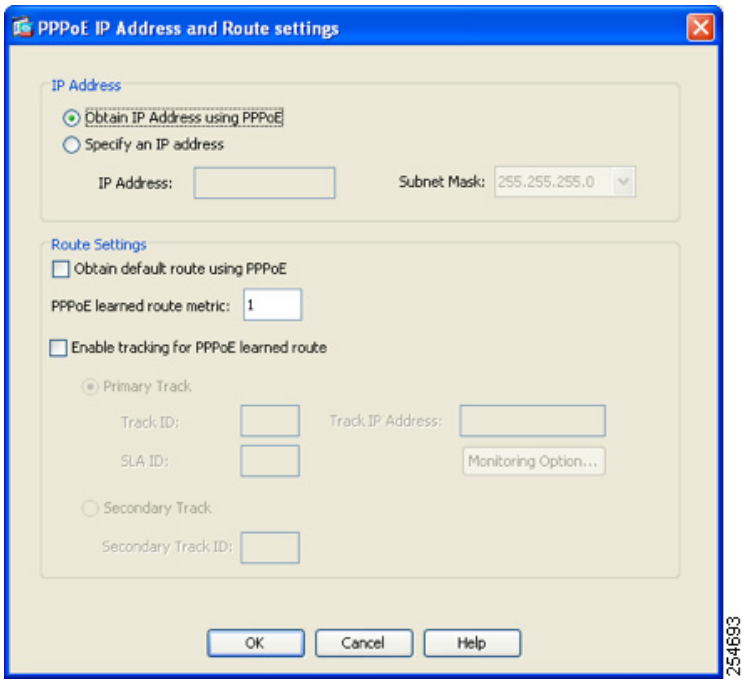
ステップ 9　[OK] をクリックします。

次の作業

- （任意）MAC アドレスと MTU を設定します。「MAC アドレス、MTU、TCP MSS の設定」（P.13-13）を参照してください。
- （任意）IPv6 アドレッシングを設定します。「IPv6 アドレッシングの設定」（P.13-16）を参照してください。

PPPoE IP Address and Route Settings

[Configuration] > [Interfaces] > [Add/Edit Interface] > [General] > [PPPoE IP Address and Route Settings] > [PPPoE IP Address and Route Settings] ダイアログボックスで、PPPoE 接続のアドレッシング オプションとトラッキング オプションを選択できます。



フィールド

- [IP Address] エリア：IP アドレスを PPP から取得する方法または IP アドレスを指定する方法を選択します。次のフィールドがあります。
  - [Obtain IP Address using PPP]：ASA を選択してイネーブルにし、PPP を使用して IP アドレスを取得します。
  - [Specify an IP Address]：ASA は、PPPoE サーバとネゴシエートするのではなく、IP アドレスとマスクを指定してアドレスを動的に割り当てます。
- [Route Settings] エリア：ルートおよびトラッキングの設定を行います。次のフィールドがあります。

- [Obtain default route using PPPoE]：PPPoE クライアントがまだ接続を確立していない場合に、デフォルト ルートを設定します。このオプションを使用する場合は、スタティックに定義されたルートを設定に含めることができません。

  [PPPoE learned route metric]：アドミニストレーティブ ディスタンスを既知のルートに割り当てます。有効な値は、1 ～ 255 です。このフィールドを空白のままにすると、既知のルートのアドミニストレーティブ ディスタンスは 1 になります。

- [Enable tracking]：PPPoE の既知のルートのトラッキングをイネーブルにします。

  （注）　ルート トラッキングは、シングル ルーテッド モードでだけ使用できます。

- [Primary Track]：プライマリ PPPoE ルート トラッキングを設定するには、このオプションを選択します。
- [Track ID]：ルート トラッキング プロセスに使用される一意の識別子。有効な値は、1 ～ 500 です。
- [Track IP Address]：トラッキングの対象 IP アドレスを入力します。通常、ルートのネクストホップはゲートウェイ IP アドレスです。ただし、そのインターフェイスの先にネットワーク オブジェクトがあれば表示されます。
- [SLA ID]：SLA モニタリング プロセスの一意の ID です。有効な値は 1 ～ 2147483647 です。
- [Monitor Options]：このボタンをクリックすると [Route Monitoring Options] ダイアログボックスが開きます。[Route Monitoring Options] ダイアログボックスで、トラッキング対象オブジェクトのモニタリング プロセスのパラメータを設定できます。
- [Secondary Track]：セカンダリ PPPoE ルート トラッキングを設定するには、このオプションを選択します。
- [Secondary Track ID]：ルート トラッキング プロセスに使用される一意の識別子。有効な値は、1 ～ 500 です。

MAC アドレス、MTU、TCP MSS の設定

ここでは、インターフェイスの MAC アドレスの設定方法、MTU の設定方法、TCP MSS の設定方法を説明します。

MAC アドレスに関する情報

デフォルトでは、物理インターフェイスはバーンドイン MAC アドレスを使用し、物理インターフェイスのすべてのサブインターフェイスは同じバーンドイン MAC アドレスを使用します。

ASASM では、すべての VLAN がバックプレーンから提供される同じ MAC アドレスを使用します。

冗長インターフェイスは、追加した最初の物理インターフェイスの MAC アドレスを使用します。コンフィギュレーションでメンバ インターフェイスの順序を変更すると、MAC アドレスは、リストの最初になったインターフェイスの MAC アドレスと一致するように変更されます。このコマンドを使用して冗長インターフェイスに MAC アドレスを割り当てると、メンバ インターフェイスの MAC アドレスに関係なく、割り当てた MAC アドレスが使用されます。

EtherChannel の場合は、そのチャネル グループに含まれるすべてのインターフェイスが同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワーク アプリケーションとユーザに対してトランスペアレントになります。ネットワーク アプリケーションやユーザから見えるのは 1 つの論理接続のみであり、個々のリンクのことは認識しないからです。ポート チャネル インターフェイスは、最も小さいチャネル グループ インターフェイスの MAC アドレスをポート チャネル MAC アド

レスとして使用します。または、ポートチャネル インターフェイスの MAC アドレスを手動で設定することもできます。マルチ コンテキスト モードでは、EtherChannel ポート インターフェイスを含め、固有の MAC アドレスをインターフェイスに自動的に割り当てることができます。グループ チャネル インターフェイスのメンバーシップを変更する場合は、固有の MAC アドレスを手動で設定するか、またはマルチ コンテキスト モードで自動的に設定することを推奨します。ポートチャネル MAC アドレスを提供していたインターフェイスを削除すると、そのポートチャネルの MAC アドレスは次に番号が小さいインターフェイスに変わるため、トラフィックが分断されます。

マルチ コンテキスト モードでは、コンテキスト間でインターフェイスを共有している場合、固有の MAC アドレスをそれぞれのコンテキストのインターフェイスに割り当てることができます。この機能を使用すると、ASA はパケットを適切なコンテキストに容易に分類できます。固有の MAC アドレスがなくても共有インターフェイスを使用できますが、制限があります。詳細については、「ASA によるパケットの分類方法」（P.8-3）を参照してください。コンテキストの共有インターフェイスには、手動で各 MAC アドレスを割り当てることも、自動生成することもできます。MAC アドレスの自動生成については、「コンテキスト インターフェイスへの MAC アドレスの自動割り当て」（P.8-24）を参照してください。MAC アドレスを自動生成する場合、この手順を使用して生成されたアドレスを上書きできます。

シングル コンテキスト モード、またはマルチ コンテキスト モードで共有されないインターフェイスの場合は、固有の MAC アドレスをサブインターフェイスに割り当てることを推奨します。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス コントロールを実行する場合があります。

MTU および TCP MSS に関する情報

「最大伝送単位および TCP 最大セグメント サイズのフラグメンテーションの制御」（P.11-8）を参照してください。

前提条件

- モデルに応じてインターフェイスを設定します。
  - ASA 5510 以降：第 11 章「インターフェイス コンフィギュレーションの開始（ASA 5510 以降）」
  - ASA 5505：第 12 章「インターフェイス コンフィギュレーションの開始（ASA 5505）」
  - ASASM：第 2 章「ASA サービス モジュール を使用するためのスイッチの設定」
- マルチ コンテキスト モードで設定できるのは、「マルチ コンテキストの設定」（P.8-15）に従ってシステム コンフィギュレーションでコンテキストにすでに割り当てられているコンテキスト インターフェイスだけです。
- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システムからコンテキスト コンフィギュレーションに変更するには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順の詳細

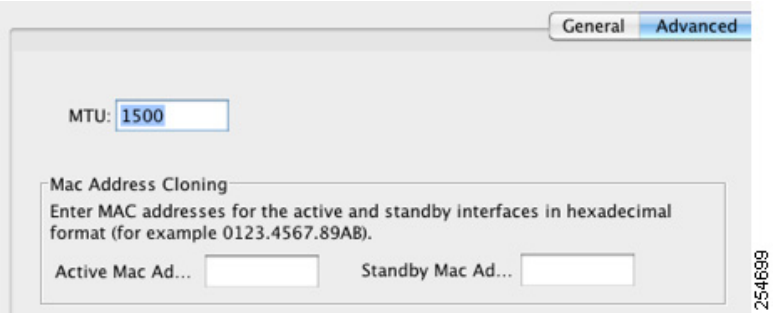
ステップ 1　[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。

ASA 5505 では、[Interfaces] タブがデフォルトで表示されます。

ステップ 2　インターフェイス行を選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

ステップ 3　[Advanced] タブをクリックします。



ステップ 4　MTU を設定する、またはジャンボ フレームのサポート（サポート対象モジュールのみ）をイネーブルにするには、[MTU] フィールドに 300 ～ 65,535 バイトの範囲の値を入力します。

デフォルトは 1500 バイトです。

（注）　冗長インターフェイスまたはポートチャネル インターフェイスに MTU を設定すると、ASA は、この設定をすべてのメンバ インターフェイスに適用します。

- ジャンボ フレームをサポートする、シングル モードのモデルの場合：いずれかのインターフェイスに 1500 を超える値を入力すると、ジャンボ フレーム サポートがすべてのインターフェイスに対して自動的にイネーブルになります。すべてのインターフェイスの MTU の設定を 1500 未満に戻すと、ジャンボ フレーム サポートがディセーブルになります。
- ジャンボ フレームをサポートしているモジュールの場合：いずれかのインターフェイスに 1500 を超える値を入力する場合は、必ずシステム コンフィギュレーションのジャンボ フレーム サポートをイネーブルにしてください。「ジャンボ フレーム サポートのイネーブル化（サポート対象のモデル）」（P.11-41）を参照してください。

（注）　ジャンボ フレーム サポートをイネーブルまたはディセーブルにするには、ASA をリロードする必要があります。

ステップ 5　MAC アドレスをこのインターフェイスに手動で割り当てるには、[Active Mac Address] フィールドに MAC アドレスを H.H.H 形式（H は 16 ビットの 16 進数）で入力します。

たとえば、MAC アドレスが 00-0C-F1-42-4C-DE であれば、000C.F142.4CDE と入力します。自動生成された MAC アドレスも使用する場合、手動で割り当てる MAC アドレスの最初の 2 バイトには A2 を使用できません。

ステップ 6　フェールオーバーを使用する場合、[Standby Mac Address] フィールドにスタンバイ MAC アドレスを入力します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

ステップ 7　TCP MSS を設定するには、[Configuration] > [Firewall] > [Advanced] > [TCP Options] の順に選択します。次のオプションを設定します。

- [Force Maximum Segment Size for TCP]：最大 TCP セグメント サイズを 48 から最大数の範囲のバイト数で設定します。デフォルト値は 1380 バイトです。この機能は、0 バイトに設定することによってディセーブルにできます。

- [Force Minimum Segment Size for TCP] : 48 から最大数の間で、ユーザが設定したバイト数未満にならないように最大セグメント サイズを上書きします。この機能は、デフォルトでディセーブルです（0 に設定）。

次の作業

（任意）IPv6 アドレッシングを設定します。「IPv6 アドレッシングの設定」（P.13-16）を参照してください。

IPv6 アドレッシングの設定

この項では、IPv6 アドレッシングを設定する方法について説明します。IPv6 の詳細については、「IPv6 アドレス」（P.48-5）を参照してください。

この項は、次の内容で構成されています。

IPv6 に関する情報

ここでは、IPv6 を設定する手順について説明します。内容は次のとおりです。

IPv6 アドレス指定

次の 2 種類の IPv6 のユニキャスト アドレスを設定できます。

- グローバル：グローバル アドレスは、パブリック ネットワークで使用可能なパブリック アドレスです。
- リンクローカル：リンクローカル アドレスは、直接接続されたネットワークだけで使用できるプライベート アドレスです。ルータは、リンクローカル アドレスを使用してパケットを転送するのではなく、特定の物理ネットワーク セグメント上で通信だけを行います。ルータは、アドレス設定またはアドレス解決およびネイバー探索などの ND 機能に使用できます。

最低限、IPv6 が動作するようにリンクローカル アドレスを設定する必要があります。グローバル アドレスを設定すると、リンクローカル アドレスがインターフェイスに自動的に設定されるため、リンクローカル アドレスを個別に設定する必要はありません。グローバル アドレスを設定しない場合は、リンクローカル アドレスを自動的にするか、手動で設定する必要があります。

Modified EUI-64 インターフェイス ID

RFC 3513「Internet Protocol Version 6 (IPv6) Addressing Architecture」（インターネット プロトコル バージョン 6 アドレッシング アーキテクチャ）では、バイナリ値 000 で始まるものを除き、すべてのユニキャスト IPv6 アドレスのインターフェイス識別子部分は長さが 64 ビットで、Modified EUI-64 形式で組み立てることが要求されています。ASA では、ローカル リンクに接続されたホストにこの要件を適用できます。

この機能がインターフェイスでイネーブルになっていると、そのインターフェイス ID が Modified EUI-64 形式を採用していることを確認するために、インターフェイスで受信した IPv6 パケットの送信元アドレスが送信元 MAC アドレスに照らして確認されます。IPv6 パケットがインターフェイス ID に Modified EUI-64 形式を採用していない場合、パケットはドロップされ、次のシステム ログ メッセージが生成されます。

```
%ASA-3-325003: EUI-64 source address check failed.
```

アドレス形式の確認は、フローが作成される場合にのみ実行されます。既存のフローからのパケットは確認されません。また、アドレスの確認はローカル リンク上のホストに対してのみ実行できます。ルータの背後にあるホストから受信したパケットは、アドレス形式の検証に失敗してドロップされます。これは、その送信元 MAC アドレスがルータの MAC アドレスであり、ホストの MAC アドレスではないためです。

グローバル IPv6 アドレスの設定

グローバル IPv6 アドレスを設定するには、次の手順を実行します。

（注） グローバル アドレスを設定すると、リンクローカル アドレスは自動的に設定されるため、別々に設定する必要はありません。

制限事項

ASA は、IPv6 エニーキャスト アドレスはサポートしません。

前提条件

- モデルに応じてインターフェイスを設定します。
  - ASA 5510 以降：第 11 章「インターフェイス コンフィギュレーションの開始（ASA 5510 以降）」
  - ASA 5505：第 12 章「インターフェイス コンフィギュレーションの開始（ASA 5505）」
  - ASASM：第 2 章「ASA サービス モジュール を使用するためのスイッチの設定」
- マルチ コンテキスト モードで設定できるのは、「マルチ コンテキストの設定」（P.8-15）に従ってシステム コンフィギュレーションでコンテキストにすでに割り当てられているコンテキスト インターフェイスだけです。
- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システムからコンテキスト コンフィギュレーションに変更するには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

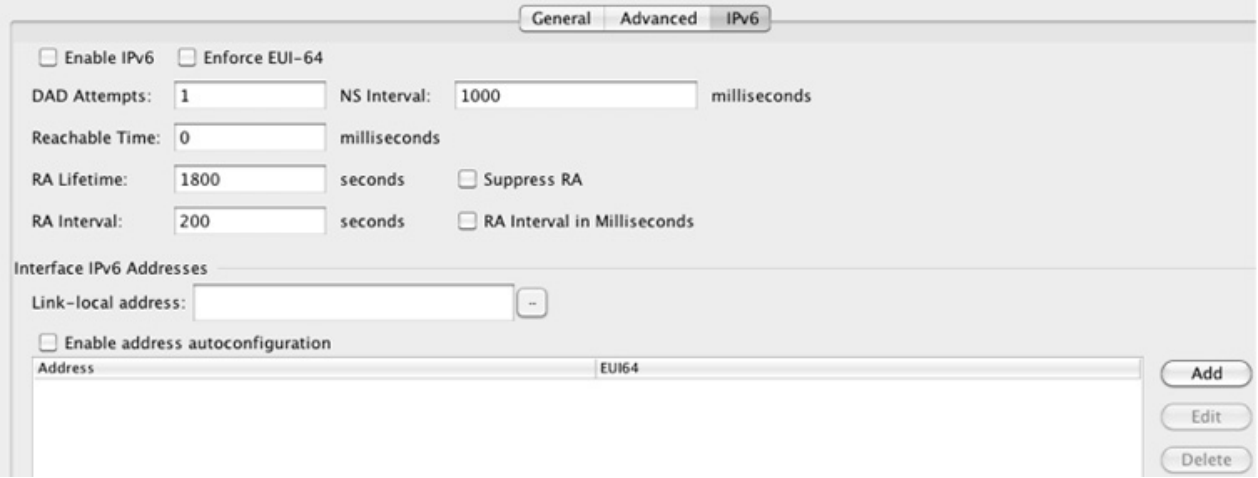
手順の詳細

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。

ステップ 2　インターフェイスを選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

ステップ 3　[IPv6] タブをクリックします。



ステップ 4　[Enable IPv6] チェックボックスをオンにします。

ステップ 5　（任意）ローカル リンクの IPv6 アドレスに Modified EUI-64 形式のインターフェイス識別子の使用を適用するには、[Enforce EUI-64] チェックボックスをオンにします。

詳細については、「Modified EUI-64 インターフェイス ID」（P.13-16）を参照してください。

ステップ 6　（任意）上部で、第 31 章「IPv6 ネイバー探索の設定」を参照して IPv6 設定をカスタマイズします。

ステップ 7　グローバル IPv6 アドレスを次のいずれかの方法で設定します。

- ステートレス自動設定：[Interface IPv6 Addresses] エリアで、[Enable address autoconfiguration] チェックボックスをオンにします。

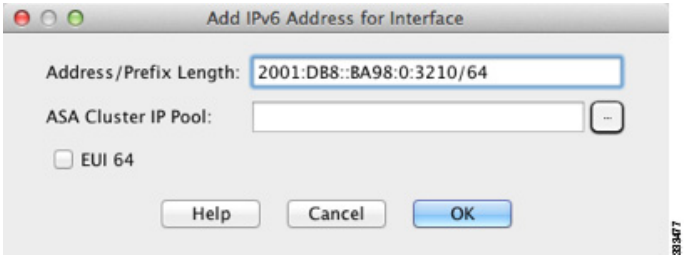
  インターフェイス上でステートレス自動設定をイネーブルにすると、受信したルータ アドバタイズメント メッセージのプレフィックスに基づいて IPv6 アドレスを設定します。ステートレスな自動設定がイネーブルになっている場合、インターフェイスのリンクローカル アドレスは、Modified EUI-64 インターフェイス ID に基づいて自動的に生成されます。

  （注）　RFC 4862 では、ステートレス自動設定に設定されたホストは、ルータ アドバタイズメント メッセージを送信しないと規定されていますが、この場合、ASA はルータ アドバタイズメント メッセージを送信します。メッセージを非表示にする場合は、[Suppress RA] チェックボックスを参照してください。

- 手動設定：グローバル IPv6 アドレスを手動で設定するには、次の手順を実行します。

  a.　[Interface IPv6 Addresses] エリアで、[Add] をクリックします。

  [Add IPv6 Address for Interface] ダイアログボックスが表示されます。



b. [Address/Prefix Length] フィールドに、インターフェイス ID を含む完全なグローバル IPv6 アドレス、または IPv6 プレフィックス長と IPv6 プレフィックスのいずれかを入力します。プレフィックスだけを入力した場合は、必ず [EUI 64] チェックボックスをオンにして、Modified EUI-64 形式を使用してインターフェイス ID を生成するようにしてください。たとえば、2001:0DB8::BA98:0:3210/48（完全なアドレス）または 2001:0DB8::/48（プレフィックス、[EUI 64] はオン）。IPv6 アドレッシングの詳細については、「IPv6 アドレス」（P.48-5）を参照してください。

（注） ASA クラスタ IP プールについては、「個別インターフェイスの設定（管理インターフェイスの場合に推奨）」（P.10-35）を参照してください。

c. [OK] をクリックします。

ステップ 8　（任意）IPv6 ルータ アドバタイズメントに含める IPv6 プレフィックスを設定するには、「ルータ アドバタイズメントの IPv6 プレフィックスの設定」（P.31-11）を参照してください。

ステップ 9　[OK] をクリックします。

[Configuration] > [Device Setup] > [Interfaces] ペインに戻ります。

IPv6 ネイバー探索の設定

IPv6 ネイバー探索を設定するには、第 31 章「IPv6 ネイバー探索の設定」を参照してください。

（任意）リンクローカル アドレスの自動設定

グローバル アドレスを設定する必要がなく、リンクローカル アドレスだけを設定する必要がある場合は、リンクローカル アドレスをインターフェイスの MAC アドレス（Modified EUI-64 形式。MAC アドレスで使用するビット数は 48 ビットであるため、インターフェイス ID に必要な 64 ビットを埋めるために追加ビットを挿入する必要があります。

リンクローカル アドレスを手動で割り当てる場合（非推奨）については、「（任意）リンクローカル アドレスの手動設定」（P.13-20）を参照します。

Modified EUI-64 形式の適用および DAD 設定を含むその他の IPv6 オプションについては、「グローバル IPv6 アドレスの設定」（P.13-17）を参照してください。

リンクローカル アドレスをインターフェイスに自動的に設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。

ステップ 2　インターフェイスを選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

ステップ 3　[IPv6] タブをクリックします。

ステップ 4　[IPv6 configuration] 領域で、[Enable IPv6] チェックボックスをオンにします。

このオプションでは、IPv6 をイネーブルにし、インターフェイスの MAC アドレスに基づく Modified EUI-64 インターフェイス ID を使用してリンクローカル アドレスを自動的に生成します。

ステップ 5　[OK] をクリックします。

（任意）リンクローカル アドレスの手動設定

グローバル アドレスを設定する必要がなく、リンクローカル アドレスだけを設定する必要がある場合は、リンクローカル アドレスを手動で定義できます。Modified EUI-64 形式に基づくリンクローカル アドレスを自動的に割り当てることを推奨します。たとえば、他のデバイスが Modified EUI-64 形式の使用を必要とする場合、手動で割り当てたリンクローカル アドレスのパケットはドロップされる可能性があります。

リンクローカル アドレスを自動的に割り当てる場合（推奨）については、「（任意）リンクローカル アドレスの自動設定」（P.13-19）を参照してください。

Modified EUI-64 形式の適用および DAD 設定を含むその他の IPv6 オプションについては、「グローバル IPv6 アドレスの設定」（P.13-17）を参照してください。

インターフェイスにリンクローカル アドレスを割り当てるには、次の手順を実行します。

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。

ステップ 2　インターフェイスを選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

ステップ 3　[IPv6] タブをクリックします。

ステップ 4　リンクローカル アドレスを設定するには、[Link-local address] フィールドにアドレスを入力します。

リンクローカル アドレスは、FE8、FE9、FEA、または FEB で始まっている必要があります。たとえば fe80::20d:88ff:feee:6a82 のようになります。IPv6 アドレッシングの詳細については、「IPv6 アドレス」（P.48-5）を参照してください。

ステップ 5　[OK] をクリックします。

同じセキュリティ レベルの通信の許可

デフォルトでは、同じセキュリティ レベルのインターフェイスは相互に通信することができません。また、パケットは同じインターフェイスを出入りすることができません。この項では、複数のインターフェイスが同じセキュリティ レベルの場合にインターフェイス間通信をイネーブルにする方法と、インターフェイス内通信をイネーブルにする方法について説明します。

インターフェイス間通信に関する情報

同じセキュリティ レベルのインターフェイスで相互通信を許可する利点としては、次のものがあります。

- 101 より多い数の通信インターフェイスを設定できます。

各インターフェイスで異なるセキュリティ レベルを使用したときに、同一のセキュリティ レベルにインターフェイスを割り当てないと、各レベル（0 ～ 100）に 1 つのインターフェイスしか設定できません。

- アクセス リストがなくても同じセキュリティ レベルのインターフェイスすべての間で自由にトラフィックが流れるようにできます。

同じセキュリティ インターフェイス通信をイネーブルにした場合でも、異なるセキュリティ レベルで通常どおりインターフェイスを設定できます。

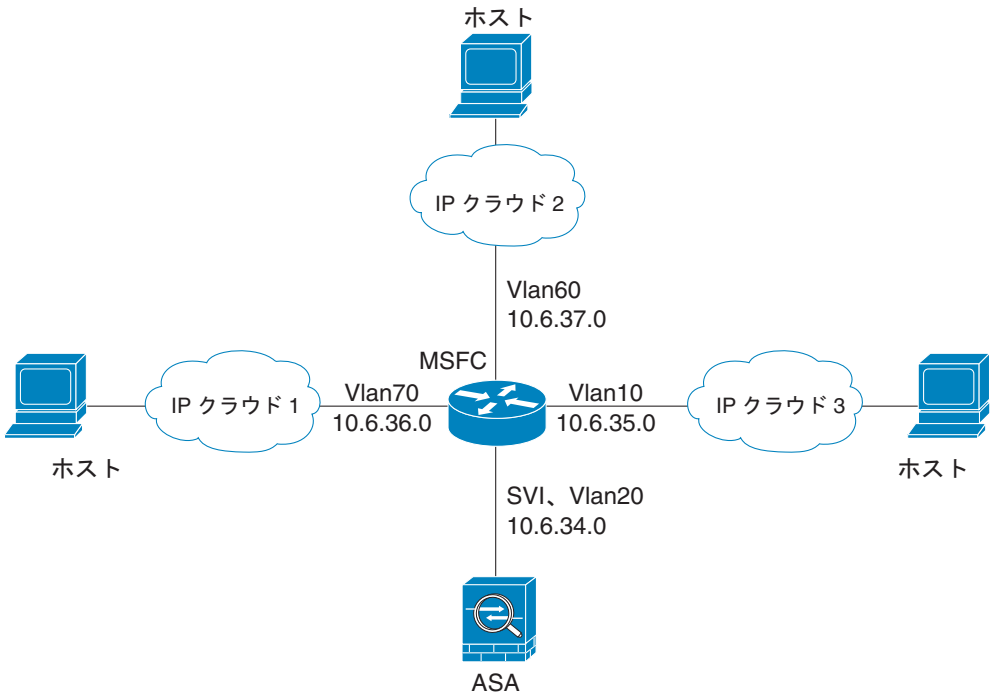
インターフェイス内通信に関する情報

インターフェイス内通信は、インターフェイスに入ってくる VPN トラフィックに対して使用できますが、その場合は同じインターフェイスのルートから外されます。この場合、VPN トラフィックは暗号化解除されたり、別の VPN 接続のために再度暗号化されたりする場合があります。たとえば、ハブ アンド スポーク VPN ネットワークがあり、ASA がハブ、リモート VPN ネットワークがスポークの場合、あるスポークが別のスポークと通信するためには、トラフィックは ASA に入ってから他のスポークに再度ルーティングされる必要があります。

（注） この機能で許可されたすべてのトラフィックは、引き続きファイアウォール規則に従います。リターン トラフィックが ASA を通過できない原因となるため、非対称なルーティング状態にしないよう注意してください。

ASASM の場合、この機能をイネーブルにするには、まず、パケットがスイッチ経由で宛先ホストに直接送信されるのではなく、ASA MAC アドレスに送信されるように、MSFC を正しく設定する必要があります。図 13-1 に、同一インターフェイス上のホストが通信する必要があるネットワークを示します。

図 13-1　同一インターフェイス上のホスト間の通信



次の設定例では、図 13-1 に示すネットワークのポリシー ルーティングをイネーブルにするために使用される Cisco IOS **route-map** コマンドを示します。

```
route-map intra-inter3 permit 0
    match ip address 103
    set interface Vlan20
    set ip next-hop 10.6.34.7
!
route-map intra-inter2 permit 20
    match ip address 102
    set interface Vlan20
    set ip next-hop 10.6.34.7
!
route-map intra-inter1 permit 10
    match ip address 101
    set interface Vlan20
    set ip next-hop 10.6.34.7
```

手順の詳細

- 同じセキュリティ レベルのインターフェイス間の通信をイネーブルにするには、[Configuration] > [Interfaces] ペインで、[Enable traffic between two or more interfaces which are configured with same security level] をオンにします。
- 同じインターフェイスに接続されているホスト間の通信をイネーブルにするには、[Enable traffic between two or more hosts connected to the same interface] をオンにします。

インターフェイスのオン/オフ

ここでは、インターフェイスのオン/オフの方法について説明します。

デフォルトでは、すべてのインターフェイスがイネーブルです。マルチ コンテキスト モードでは、コンテキスト内でインターフェイスをディセーブルにした場合、または再度イネーブルにした場合は、そのコンテキスト インターフェイスだけが影響を受けます。ただし、システム実行スペースでインターフェイスをディセーブルにした場合、または再度イネーブルにした場合は、全コンテキストに対応するそのインターフェイスに影響します。

手順の詳細

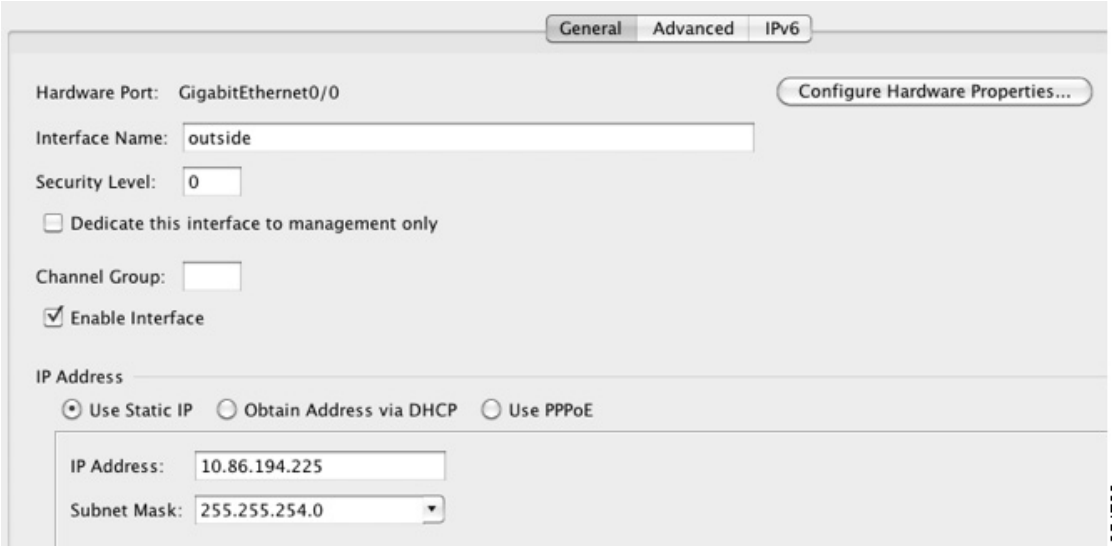
ステップ 1　コンテキスト モードによって次のように異なります。

- シングル モードの場合、[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。
- マルチ モードの場合、システム実行スペースで、[Configuration] > [Context Management] > [Interfaces] ペインを選択します。

デフォルトでは、すべての物理インターフェイスが一覧表示されます。

ステップ 2　設定する VLAN インターフェイスをクリックし、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが表示されます。



ステップ 3　インターフェイスをイネーブルまたはディセーブルにするには、[Enable Interface] チェックボックスをオンまたはオフにします。

インターフェイスのモニタリング

この項では、次のトピックについて取り上げます。

- 「ARP Table」（P.13-23）
- 「DHCP」（P.13-24）
- 「MAC Address Table」（P.13-26）
- 「Dynamic ACLs」（P.13-27）
- 「Interface Graphs」（P.13-27）
- 「PPPoE Client」（P.13-29）
- 「Interface Connection」（P.13-30）

ARP Table

[Monitoring] > [Interfaces] > [ARP Table] ペインには、スタティックとダイナミック エントリを含む ARP テーブルが表示されます。ARP テーブルには、MAC アドレスを所定のインターフェイスの IP アドレスにマッピングするエントリが含まれます。

フィールド

- [Interface]：マッピングに関連付けられているインターフェイス名を一覧表示します。
- [IP Address]：IP アドレスを表示します。
- [MAC Address]：MAC アドレスを表示します。

- [Proxy ARP]：インターフェイスでプロキシ ARP がイネーブルになっている場合は Yes と表示します。インターフェイスでプロキシ ARP がイネーブルになっていない場合は No と表示します。
- [Clear]：ダイナミック ARP テーブルのエントリをクリアします。スタティック エントリはクリアされません。
- [Refresh]：ASA の現在の情報でテーブルをリフレッシュし、[Last Updated] の日付と時刻を更新します。
- [Last Updated]：*表示専用*。表示が更新された日付と時刻を示します。

DHCP

ASA では、クライアントに割り当てられているアドレス、ASA インターフェイスのリース情報、および DHCP 統計情報を含む DHCP ステータスをモニタできます。

DHCP Server Table

[Monitoring] > [Interfaces] > [DHCP] > [DHCP Server Table] には、DHCP クライアントに割り当てられている IP アドレスが一覧表示されます。

フィールド

- [IP Address]：クライアントに割り当てられている IP アドレスを表示します。
- [Client-ID]：クライアントの MAC アドレスまたは ID を表示します。
- [Lease Expiration]：DHCP リースの期限が満了する日付を表示します。リースは、クライアントが割り当てられている IP アドレスを使用できる期間を示します。また、残り時間は、[Last Updated] 表示専用フィールドのタイムスタンプを基準に秒数で表示されます。
- [Number of Active Leases]：DHCP リースの合計数を表示します。
- [Refresh]：ASA の情報をリフレッシュします。
- [Last Updated]：テーブルのデータが最後に更新された日付を表示します。

DHCP Client Lease Information

DHCP サーバから ASA インターフェイスの IP アドレスを取得すると、[Monitoring] > [Interfaces] > [DHCP] > [DHCP Server Table] > [DHCP Client Lease Information] ペインには、DHCP リースに関する情報が表示されます。

フィールド

- [Select an interface]：ASA のインターフェイスを一覧表示します。DHCP リースを表示するインターフェイスを選択します。インターフェイスに DHCP リースが複数ある場合、表示するインターフェイスと IP アドレスのペアを選択します。
- [Attribute and Value]：インターフェイス DHCP リースの属性と値を一覧表示します。
  - [Temp IP addr]：*表示専用*。インターフェイスに割り当てられている IP アドレス。
  - [Temp sub net mask]：*表示専用*。インターフェイスに割り当てられているサブネット マスク。
  - [DHCP lease server]：*表示専用*。DHCP サーバ アドレス。
  - [state]：*表示専用*。DHCP リースの状態で、次のとおりです。

[Initial]：初期化状態で、ASA がリースを取得するプロセスを開始します。この状態は、リースが終了したか、リースのネゴシエーションに失敗したときにも表示されます。

[Selecting]：ASA は 1 つ以上の DHCP サーバから DHCPOFFER メッセージを受信することを待機しており、メッセージを選択できます。

[Requesting]：ASA は、要求を送信した送信先サーバからの応答を待機しています。

[Purging]：ASA は、エラーが発生したためリースを削除しています。

[Bound]：ASA は有効なリースを保持し、正常に動作しています。

[Renewing]：ASA はリースを更新しようとしています。DHCPREQUEST メッセージを現在の DHCP サーバに定期的に送信し、応答を待機します。

[Rebinding]：ASA は元のサーバのリースを更新することに失敗したため、いずれかのサーバから応答を受け取るかリースが終了するまで DHCPREQUEST メッセージを送信します。

[Holddown]：ASA はリースを削除するプロセスを開始しました。

[Releasing]：ASA は IP アドレスが不要になったことを示すリリース メッセージをサーバに送信します。

- [Lease]：*表示専用*。DHCP サーバによって指定される、インターフェイスがこの IP アドレスを使用できる時間の長さ。
- [Renewal]：*表示専用*。インターフェイスがこのリースを自動的に更新しようとするまでの時間の長さ。
- [Rebind]：*表示専用*。ASA が DHCP サーバに再バインドしようとするまでの時間の長さ。再バインドが発生するのは、ASA が元の DHCP サーバと通信できず、リース期間の 87.5% を経過した場合です。ASA は、DHCP 要求をブロードキャストすることによって、使用可能な任意の DHCP サーバに接続を試みます。
- [Next timer fires after]：*表示専用*。内部タイマーがトリガーするまでの秒数。
- [Retry count]：*表示専用*。ASA がリースを設定しようとしているとき、このフィールドは、ASA が DHCP メッセージの送信を試行した回数を示します。たとえば、ASA が Selecting 状態の場合、この値は ASA が探索メッセージを送信した回数を示します。ASA が Requesting 状態の場合、この値は ASA が要求メッセージを送信した回数を示します。
- [Client-ID]：*表示専用*。サーバとのすべての通信に使用したクライアント ID。
- [Proxy]：*表示専用*。このインターフェイスが VPN クライアント用のプロキシ DHCP クライアントかどうかを True または False で指定します。
- [Hostname]：*表示専用*。クライアントのホスト名。

DHCP Statistics

[Monitoring] > [Interfaces] > [DHCP] > [DHCP Statistics] ペインは、DHCP サーバ機能の統計情報が表示されます。

フィールド

- [Message Type]：送受信された DHCP メッセージのタイプを一覧表示します。
  - BOOTREQUEST
  - DHCPDISCOVER
  - DHCPREQUEST
  - DHCPDECLINE

  - DHCPRELEASE
  - DHCPINFORM
  - BOOTREPLY
  - DHCPOFFER
  - DHCPACK
  - DHCPNAK
- [Count]：特定のメッセージが処理された回数を表示します。
- [Direction]：メッセージ タイプが Sent か Received かを示します。
- [Total Messages Received]：ASA で受信したメッセージの合計数を表示します。
- [Total Messages Sent]：ASA で送信したメッセージの合計数を表示します。
- [Counter]：次のような DHCP の全般的な統計データを表示します。
  - DHCP UDP Unreachable Errors
  - DHCP Other UDP Errors
  - Address Pools
  - Automatic Bindings
  - Expired Bindings
  - Malformed Messages
- [Value]：各カウンタ項目の数を表示します。
- [Refresh]：DHCP テーブルのリストを更新します。
- [Last Updated]：テーブルのデータが最後に更新された日付を表示します。

MAC Address Table

[Monitoring] > [Interfaces] > [MAC Address Table] ペインには、スタティックおよびダイナミック MAC アドレス エントリが表示されます。MAC アドレス テーブルおよび追加のスタティック エントリに関する詳細情報については、「MAC Address Table」（P.13-26）を参照してください。

フィールド

- [Interface]：エントリに関連付けられているインターフェイス名を表示します。
- [MAC Address]：MAC アドレスを表示します。
- [Type]：エントリがスタティックかダイナミックかを表示します。
- [Age]：エントリの経過時間を分数で表示します。タイムアウトを設定するには、「MAC Address Table」（P.13-26）を参照してください。
- [Refresh]：ASA の現在の情報でテーブルをリフレッシュします。

Dynamic ACLs

[Monitoring] > [Interfaces] > [Dynamic ACLs] ペインには、ダイナミック ACL のテーブルが表示されます。ダイナミック ACL は、ASA によって自動的に作成、アクティブ化、削除される点を除いて、ユーザ設定の ACL と機能上同じです。これらの ACL はコンフィギュレーションには表示されず、このテーブルだけに表示されます。ダイナミック ACL は、ACL ヘッダーの「(dynamic)」キーワードで区別されます。

このテーブルで ACL を選択すると、その ACL の内容が下部のテキスト フィールドに表示されます。

フィールド

- [ACL]：ダイナミック ACL の名前を表示します。
- [Element Count]：ACL の要素の数を表示します。
- [Hit Count]：ACL のすべての要素に対する合計ヒット数を表示します。

Interface Graphs

[Monitoring] > [Interfaces] > [Interface Graphs] ペインには、インターフェイス統計情報をグラフ形式またはテーブル形式で表示できます。インターフェイスをコンテキスト間で共有している場合、ASA には現在のコンテキストの統計情報だけが表示されます。サブインターフェイスに表示される統計情報の数は、物理インターフェイスに表示される統計情報の数のサブセットです。

フィールド

- [Available Graphs for]：モニタリングに使用可能な統計情報のタイプを一覧表示します。1 つのグラフ ウィンドウに表示する統計情報のタイプは 4 つまで選択できます。複数のグラフ ウィンドウを同時に開くことができます。
  - [Byte Counts]：インターフェイスのバイト入力およびバイト出力の数を表示します。
  - [Packet Counts]：インターフェイスのパケット入力およびパケット出力の数を表示します。
  - [Packet Rates]：インターフェイスのパケット入力およびパケット出力のレートを表示します。
  - [Bit Rates]：インターフェイスの入出力のビット レートを表示します。
  - [Drop Packet Count]：インターフェイスでドロップされたパケットの数を表示します。

  物理インターフェイスに追加して表示できる統計情報は次のとおりです。
  - [Buffer Resources]：次の統計情報を表示します。

    [Overruns]：入力速度が、ASA のデータ処理能力を超えたため、ASA がハードウェア バッファに受信したデータを処理できなかった回数。

    [Underruns]：ASA で処理できる速度より速くトランスミッタが動作した回数。

    [No Buffer]：メイン システムにバッファ スペースがなかったために廃棄された受信パケットの数。この数を、無視された数と比較してください。イーサネット ネットワーク上のブロードキャスト ストームは、多くの場合、入力バッファ イベントがないことに原因があります。
  - [Packet Errors]：次の統計情報を表示します。

    [CRC]：巡回冗長検査エラーの数。ステーションがフレームを送信すると、フレームの末尾に CRC を付加します。この CRC は、フレーム内のデータに基づくアルゴリズムから生成されます。送信元と宛先の間でフレームが変更された場合、ASA は CRC が一致しないことを通知します。CRC の数値が高いことは、通常、コリジョンの結果であるか、ステーションが不良データを送信することが原因です。

[Frame]：フレーム エラーの数。不良フレームには、長さが正しくないパケットや、フレーム チェックサムが正しくないパケットがあります。このエラーは通常、コリジョンまたはイーサネット デバイスの誤動作が原因です。

[Input Errors]：ここにリストされている他のタイプのものも含めた入力エラーの合計数。また、その他の入力関連のエラーによって入力エラー数が増えたり、一部のデータグラムに複数のエラーが存在していたりする可能性があります。したがって、この合計は、他のタイプにリストされているエラーの数を超えることがあります。

[Runts]：最小パケット サイズの 64 バイトよりも小さかったために廃棄されたパケットの数。ラントは通常、コリジョンによって発生します。不適切な配線や電気干渉によって発生することもあります。

[Giants]：最大パケット サイズを超えたために廃棄されたパケットの数。たとえば、1518 バイトよりも大きいイーサネット パケットはジャイアントと見なされます。

[Deferred]：FastEthernet インターフェイスだけ。リンク上のアクティビティが原因で送信前に保留されたフレームの数。

- [Miscellaneous]：受信したブロードキャストの統計情報を表示します。
- [Collision Counts]：FastEthernet インターフェイスだけ。次の統計情報を表示します。

  [Output Errors]：設定されている衝突の最大数を超えたために伝送されなかったフレームの数。このカウンタは、ネットワーク トラフィックが多い場合にのみ増加します。

  [Collisions]：イーサネット衝突（1 つまたは複数の衝突）が原因で、再度伝送されたメッセージ数。これは通常、過渡に延長した LAN で発生します（イーサネット ケーブルまたはトランシーバ ケーブルが長すぎる、ステーション間のリピータが 2 つよりも多い、またはマルチポート トランシーバのカスケードが多すぎる場合）。衝突するパケットは、出力パケットによって 1 回だけカウントされます。

  [Late Collisions]：通常の衝突ウィンドウの外で衝突が発生したために伝送されなかったフレームの数。レイト コリジョンは、パケットの送信中に遅れて検出されるコリジョンです。これは通常発生しません。2 つのイーサネット ホストが同時に通信しようとした場合、早期にパケットが衝突して両者がバックオフするか、2 番目のホストが 1 番目のホストの通信状態を確認して待機します。レイト コリジョンが発生すると、デバイスは割り込みを行ってイーサネット上にパケットを送信しようとしますが、ASA はパケットの送信を部分的に完了しています。ASA は、パケットの最初の部分を保持するバッファを解放した可能性があるため、パケットを再送しません。このことはあまり問題になりません。その理由は、ネットワーキング プロトコルはパケットを再送することでコリジョンを処理する設計になっているためです。ただし、レイト コリジョンはネットワークに問題が存在することを示しています。一般的な問題は、リピータで接続された大規模ネットワーク、および仕様の範囲を超えて動作しているイーサネット ネットワークです。

- [Input Queue]：入力キューの現在のパケット数および最大パケット数を表示します。次の統計情報が含まれます。

  [Hardware Input Queue]：ハードウェア キューのパケット数。

  [Software Input Queue]：ソフトウェア キューのパケット数。

- [Output Queue]：出力キューの現在のパケット数および最大パケット数を表示します。次の統計情報が含まれます。

  [Hardware Output Queue]：ハードウェア キューのパケット数。

  [Software Output Queue]：ソフトウェア キューのパケット数。

- [Add]：選択した統計タイプを、選択したグラフ ウィンドウに追加します。

- [Remove]：選択したグラフ ウィンドウから、選択した統計タイプを削除します。削除している項目が他のパネルから追加され、[Available Graphs] ペインに戻されていない場合、このボタン名は [Delete] に変わります。
- [Show Graphs]：統計タイプを追加するグラフ ウィンドウ名を表示します。すでにグラフ ウィンドウを開いている場合は、デフォルトで新しいグラフ ウィンドウがリストされます。すでに開いているグラフに統計タイプを追加する場合は、開いているグラフ ウィンドウの名前を選択します。すでにグラフに含まれている統計情報が [Selected Graphs] ペインに表示され、タイプを追加できます。グラフ ウィンドウには ASDM、インターフェイスの IP アドレス、および「Graph」という順番で名前が付けられます。後続のグラフは、「Graph (2)」のように名前が付けられます。
- [Selected Graphs]：選択したグラフ ウィンドウに表示する統計タイプを表示します。タイプを 4 つまで含めることができます。
  - [Show Graphs]：グラフ ウィンドウを表示するか、または、追加した場合は追加の統計タイプでグラフを更新します。

Graph/Table

[Monitoring] > [Interfaces] > [Interface Graphs] > [Graph/Table] ウィンドウには、選択した統計情報のグラフが表示されます。[Graph] ウィンドウには、最大 4 つのグラフおよびテーブルを同時に表示することができます。デフォルトで、グラフまたはテーブルにリアルタイムな統計情報が表示されます。履歴メトリック（「履歴メトリックのイネーブル化」（P.4-35）を参照）をイネーブルにすると、過去の期間の統計情報を表示できます。

フィールド

- [View]：グラフまたはテーブルを表示する期間を設定します。リアルタイム以外の期間を表示するには、[History Metrics]（「履歴メトリックのイネーブル化」（P.4-35）を参照）をイネーブルにします。次のオプションの指定に従ってデータが更新されます。
  - Real-time, data every 10 sec
  - Last 10 minutes, data every 10 sec
  - Last 60 minutes, data every 1 min
  - Last 12 hours, data every 12 min
  - Last 5 days, data every 2 hours
- [Export]：グラフをカンマ区切り形式でエクスポートします。[Graph] ウィンドウに複数のグラフまたはテーブルがある場合、[Export Graph Data] ダイアログボックスが表示されます。名前の横のチェックボックスを選択して、リストされているグラフおよびテーブルを 1 つ以上選択します。
- [Print]：グラフまたはテーブルを印刷します。[Graph] ウィンドウに複数のグラフまたはテーブルがある場合、[Print Graph] ダイアログボックスが表示されます。[Graph/Table Name] リストから印刷するグラフまたはテーブルを選択します。
- [Bookmark]：ブラウザ ウィンドウに、[Graph] ウィンドウ上のすべてのグラフおよびテーブルへのリンク 1 つと、各グラフまたはテーブルへの個別のリンクが表示されます。ブラウザでこれらの URL をブックマークとしてコピーできますグラフの URL を開くときに、ASDM を実行している必要はありません。ブラウザによって ASDM が起動され、グラフが表示されます。

PPPoE Client

[Monitoring] > [Interfaces] > [PPPoE Client] > /PPPoE Client Lease Information] ペインには、現在の PPPoE 接続に関する情報が表示されます。

フィールド

[Select a PPPoE interface]：PPPoE クライアントのリース情報を表示するインターフェイスを選択します。

[Refresh]：ASA から最新の PPPoE 接続情報をロードして表示します。

Interface Connection

[Monitoring] > [Interfaces] ツリーの [Monitoring] > [Interfaces] > *インターフェイス*接続ノードは、スタティック ルート トラッキングが設定されている場合にだけ表示されます。複数のルートを追跡している場合、追跡されるルートが含まれている各インターフェイスにノードがあります。

ルート トラッキングに関する詳細については、次の項を参照してください。

- 「Track Status for」（P.13-30）
- 「Monitoring Statistics for」（P.13-30）

Track Status for

[Monitoring] > [Interfaces] > インターフェイス接続 > [Track Status for] ペインには、トラッキング対象オブジェクトに関する情報が表示されます。

フィールド

- [Tracked Route]：*表示専用*。トラッキング プロセスに関連付けられているルートを表示します。
- [Route Statistics]：*表示専用*。オブジェクトの到達性情報を表示します。到達性情報で最後に変更があった場合は、オペレーションのリターンコード、およびトラッキングを実行するプロセスを表示します。

Monitoring Statistics for

[Monitoring] > [Interfaces] > インターフェイス接続 > [Monitoring Statistics for] ペインには、SLA モニタリング プロセスの統計情報が表示されます。

フィールド

- [SLA Monitor ID]：*表示専用*。SLA モニタリング プロセスの ID を表示します。
- [SLA statistics]：*表示専用*。プロセスが変更された最後の時刻、試行されたオペレーション回数、スキップされたオペレーション回数などの SLA モニタリング統計情報を表示します。

ルーテッド モードのインターフェイスの機能履歴

表 13-1 に、この機能のリリース履歴の一覧を示します。

表 13-1　インターフェイスの機能履歴

機能名	リリース	機能情報
VLAN 数の増加	7.0(5)	次の制限値が増加されました。 • ASA 5510 基本ライセンスの VLAN 数が 0 から 10 に増えました。 • ASA 5510 Security Plus ライセンスの VLAN 数が 10 から 25 に増えました。 • ASA 5520 の VLAN 数が 25 から 100 に増えました。 • ASA 5540 の VLAN 数が 100 から 200 に増えました。
VLAN 数の増加	7.2(2)	ASA 5505 上の Security Plus ライセンスに対する VLAN 最大数が、5（3 つのフル機能インターフェイス、1 つのフェールオーバー インターフェイス、1 つのバックアップ インターフェイスに制限されるインターフェイス）から 20 のフル機能インターフェイスに増加されました。また、トランク ポート数も 1 から 8 に増加されました。フル機能のインターフェイスの数が 20 になり、バックアップ ISP インターフェイスを停止するために backup interface コマンドを使用する必要がなくなりました。つまり、バックアップ ISP インターフェイス用にフル機能のインターフェイスを使用できるようになりました。backup interface コマンドは、これまでどおり Easy VPN 設定用に使用できます。 VLAN の制限値も変更されました。ASA 5510 の基本ライセンスでは 10 から 50 に、Security Plus ライセンスでは 25 から 100 に、ASA 5520 では 100 から 150 に、ASA 5550 では 200 から 250 に増えています。
ASA 5510 Security Plus ライセンスに対するギガビット イーサネット サポート	7.2(3)	ASA 5510 は、GE（ギガビット イーサネット）を Security Plus ライセンスのあるポート 0 および 1 でサポートするようになりました。ライセンスを Base から Security Plus にアップグレードした場合、外部 Ethernet 0/0 および Ethernet 0/1 ポートの容量は、元の Fast Ethernet（FE; ファスト イーサネット）の 100 Mbps から GE の 1000 Mbps に増加します。インターフェイス名は Ethernet 0/0 および Ethernet 0/1 のままです。
ASA 5505 に対するネイティブ VLAN サポート	7.2(4)/8.0(4)	ネイティブ VLAN を ASA 5505 トランク ポートに割り当てることができるようになりました。 次の画面が変更されました。[Configuration] > [Device Setup] > [Interfaces] > [Switch Ports] > [Edit Switch Port]。

表 13-1　インターフェイスの機能履歴 （続き）

機能名	リリース	機能情報
ASA 5580 に対するジャンボ パケット サポート	8.1(1)	Cisco ASA 5580 はジャンボ フレームをサポートしています。ジャンボ フレームとは、標準的な最大値 1518 バイト（レイヤ 2 ヘッダーおよび FCS を含む）より大きく、9216 バイトまでのイーサネット パケットのことです。イーサネット フレームを処理するためのメモリ容量を増やすことにより、すべてのインターフェイスに対してジャンボ フレームのサポートをイネーブルにできます。ジャンボ フレームに割り当てるメモリを増やすと、他の機能（アクセス リストなど）の最大使用量が制限される場合があります。 次の画面が変更されました。[Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Interface] > [Advanced]。
ASA 5580 の VLAN 数の増加	8.1(2)	ASA 5580 上でサポートされる VLAN 数が 100 から 250 に増加されました。
トランスペアレント モードの IPv6 のサポート	8.2(1)	トランスペアレント ファイアウォール モードの IPv6 サポートが導入されました。
ASA 5580 10 ギガビット イーサネット インターフェイスでのフロー制御のポーズ フレームのサポート	8.2(2)	フロー制御のポーズ（XOFF）フレームをイネーブルにできるようになりました。 次の画面が変更されました。 （シングル モード）[Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Interface] > [Advanced] （マルチ モード、システム）[Configuration] > [Interfaces] > [Add/Edit Interface]