インターフェイス コンフィギュレーションの開始（ASA 5505）

この章では、VLAN インターフェイスを作成してスイッチ ポートに割り当てる方法など、ASA 5505 のインターフェイス コンフィギュレーションを開始するためのタスクについて説明します。

ASA 5510 以降のコンフィギュレーションについては、「ASA 5505 インターフェイスの機能履歴」（P.12-16）を参照してください。

この章は、次の項で構成されています。

ASA 5505 インターフェイスについて

この項では、ASA 5505 のポートおよびインターフェイスについて説明します。次の項目を取り上げます。

ASA 5505 のポートおよびインターフェイスについて

ASA 5505 は組み込みスイッチをサポートしています。次の 2 種類のポートおよびインターフェイスを設定する必要があります。

- 物理スイッチ ポート：ASA には 8 個のファスト イーサネット スイッチ ポートがあり、これらはハードウェアのスイッチ機能を使用して、レイヤ 2 でトラフィックを転送します。これらのポートのうちの 2 つは PoE ポートです。詳細については、「Power Over Ethernet」（P.12-4）を参照してください。これらのインターフェイスを、PC、IP 電話、DSL モデムなどのユーザ機器に直接接続できます。または、別のスイッチに接続できます。
- 論理 VLAN インターフェイス：ルーテッド モードでは、これらのインターフェイスは、設定済みのセキュリティ ポリシーを使用してファイアウォールと VPN サービスを適用することによって、レイヤ 3 の VLAN ネットワーク間でトラフィックを転送します。トランスペアレント モードでは、これらのインターフェイスは、設定済みのセキュリティ ポリシーを使用してファイアウォール サービスを適用することによって、レイヤ 2 の同じネットワーク上の VLAN 間でトラフィックを転送します。最大 VLAN インターフェイス数の詳細については、「ライセンスで使用できる最大アクティブ VLAN インターフェイス数」を参照してください。VLAN インターフェイスを使用することにより、別々の VLAN、たとえばホーム VLAN、ビジネス VLAN、インターネット VLAN などに装置を分けることができます。

スイッチ ポートを別々の VLAN に分離するには、各スイッチ ポートを VLAN インターフェイスに割り当てます。同じ VLAN 上のスイッチ ポートは、ハードウェア スイッチングを使用して相互に通信できます。ただし、VLAN 1 のスイッチ ポートが VLAN 2 のスイッチ ポートと通信する場合、ASA は、セキュリティ ポリシーを 2 つの VLAN 間のトラフィックとルートまたはブリッジに適用します。

ライセンスで使用できる最大アクティブ VLAN インターフェイス数

ルーテッド モードでは、ライセンスに応じて次の VLAN を設定できます。

- 基本ライセンス：3 つのアクティブ VLAN。3 つ目の VLAN は、別の VLAN へのトラフィックを開始する目的に限り設定できます。詳細については、「図 12-1」を参照してください。
- Security Plus ライセンス：20 個のアクティブ VLAN。

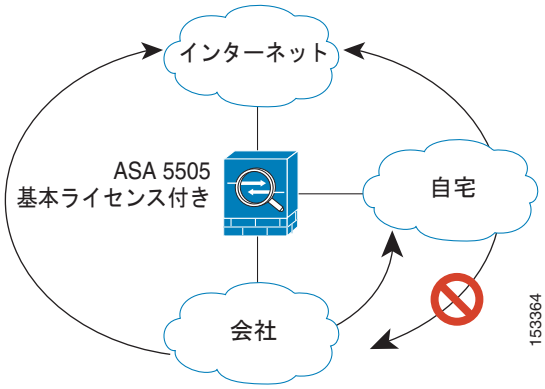
トランスペアレント ファイアウォール モードでは、ライセンスに応じて次の VLAN を設定できます。

- 基本ライセンス：1 つのブリッジ グループ内の 2 つのアクティブ VLAN。
- Security Plus ライセンス：3 つのアクティブ VLAN、1 つのブリッジ グループ内の 2 つのアクティブ VLAN、およびフェールオーバー リンクの 1 つのアクティブ VLAN。

（注）　*アクティブ VLAN* とは、**nameif** コマンドが設定された VLAN のことです。

ルーテッド モードの基本ライセンスの場合、3 つ目の VLAN は、別の VLAN へのトラフィックを開始する目的に限り設定できます。図 12-1 のネットワークの例では、ホーム VLAN はインターネットと通信できますが、ビジネス VLAN とは接続を開始できません。

図 12-1　基本ライセンスでの ASA 5505

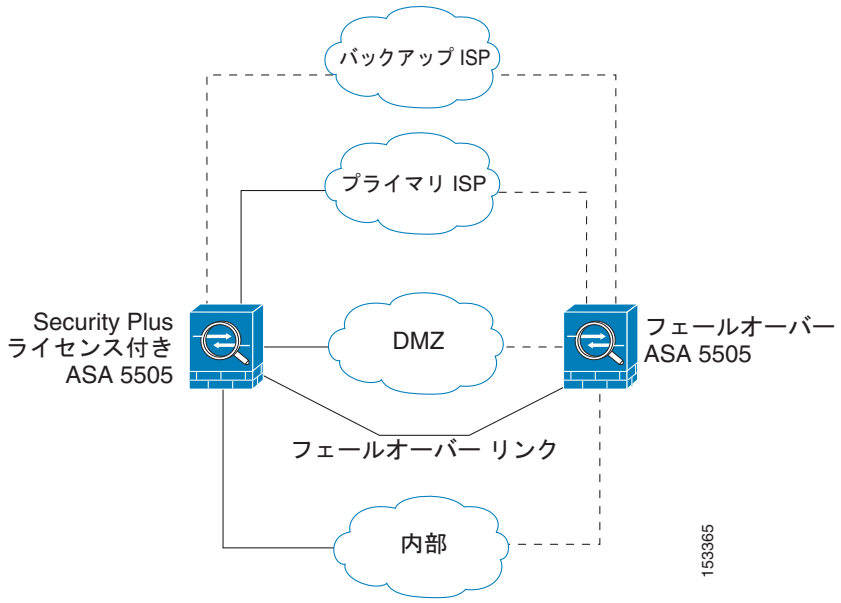


Security Plus ライセンスでは、ルーテッド モードの 20 個の VLAN インターフェイスを設定できます。これには、フェールオーバー用の VLAN インターフェイスと、ISP へのバックアップ リンクとしての VLAN インターフェイスも含まれます。バックアップ インターフェイスは、プライマリ インターフェイス経由のルートで障害が発生しない限り、トラフィックを通過させないように設定できます。トランク ポートを設定して、1 つのポートで複数の VLAN を使用できます。

（注） ASA 5505 は、アクティブ/スタンバイ フェールオーバーをサポートしていますが、ステートフル フェールオーバーはサポートしていません。

ネットワークの例については、図 12-2 を参照してください。

図 12-2　Security Plus ライセンスでの ASA 5505



VLAN MAC アドレス

- ルーテッド ファイアウォール モード：すべての VLAN インターフェイスが MAC アドレスを共有します。接続スイッチがどれもこのシナリオをサポートできるようにします。接続スイッチに固有の MAC アドレスが必要な場合、手動で MAC アドレスを割り当てることができます。「MAC アドレス、MTU、TCP MSS の設定」（P.13-13）を参照してください。
- トランスペアレント ファイアウォール モード：各 VLAN に固有の MAC アドレスが割り当てられます。必要に応じて、手動で MAC アドレスを割り当てて、生成された MAC アドレスを上書きできます。「MAC アドレス、MTU、TCP MSS の設定」（P.14-15）を参照してください。

Power Over Ethernet

Ethernet 0/6 および Ethernet 0/7 は、IP 電話や無線アクセス ポイントなどのデバイス用に PoE をサポートしています。非 PoE デバイスをインストールした場合やこれらのスイッチ ポートに接続しない場合、ASA はスイッチ ポートに電源を供給しません。

スイッチ ポートをシャットダウンすると、デバイスへの電源がディセーブルになります。portd をイネーブルにすると、電源が回復します。スイッチ ポートのシャットダウンの詳細については、「スイッチ ポートのアクセス ポートとしての設定とイネーブル化」（P.12-8）を参照してください。

SPAN を使用したトラフィックのモニタリング

1 つまたは複数のスイッチ ポートを出入りするトラフィックをモニタするには、スイッチ ポート モニタリングとも呼ばれる SPAN をイネーブルにします。SPAN をイネーブルにしたポート（宛先ポートと呼ばれる）は、特定の送信元ポートで送受信するすべてのパケットのコピーを受信します。SPAN 機能を使用すれば、スニファを宛先ポートに添付して、すべてのトラフィックをモニタできます。SPAN を使用しないと、モニタするポートごとにスニファを添付しなければなりません。SPAN をイネーブルにすることができるのは、1 つの宛先ポートのみです。

SPAN 監視をイネーブルにするには、Command Line Interface ツールを使用し、**switchport monitor** コマンドを入力する必要があります。詳細については、コマンド リファレンスの **switchport monitor** コマンドを参照してください。

Auto-MDI/MDIX 機能

すべての ASA 5505 インターフェイスには、Auto-MDI/MDIX 機能が含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。Auto-MDI/MDIX はディセーブルにできません。

ASA 5505 インターフェイスのライセンス要件

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

注意事項と制約事項

コンテキスト モードのガイドライン

ASA 5505 はマルチ コンテキスト モードをサポートしません。

ファイアウォール モードのガイドライン

- トランスペアレント モードでは、最大 8 個のブリッジ グループを設定できます。少なくとも 1 つのブリッジ グループを使用しなければならないことに注意してください。データ インターフェイスはブリッジ グループに属している必要があります。
- 各ブリッジ グループには、最大 4 個の VLAN インターフェイスをライセンス制限まで含めることができます。

フェールオーバーのガイドライン

アクティブ/スタンバイ フェールオーバーは、Security Plus ライセンスでのみサポートされます。アクティブ/アクティブ フェールオーバーはサポートされません。

IPv6 のガイドライン

IPv6 をサポートします。

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。

インターフェイスのデフォルトの状態

インターフェイスには、次のデフォルト状態があります。

- スイッチ ポート：ディセーブル。
- VLAN：イネーブル。ただし、トラフィックが VLAN を通過するためには、スイッチ ポートもイネーブルになっている必要があります。

デフォルトの速度および二重通信

デフォルトでは、速度と二重通信はオートネゴシエーションに設定されています。

ASA 5505 インターフェイス コンフィギュレーションの開始

この項では、次のトピックについて取り上げます。

インターフェイス コンフィギュレーションを開始するためのタスク フロー

シングル モードでインターフェイスを設定するには、次の手順を実行します。

ステップ 1　VLAN インターフェイスを設定します。「VLAN インターフェイスの設定」（P.12-6）を参照してください。

ステップ 2　スイッチ ポートをアクセス ポートとして設定し、イネーブルにします。「スイッチ ポートのアクセス ポートとしての設定とイネーブル化」（P.12-8）を参照してください。

ステップ 3　（Security Plus ライセンスのオプション）スイッチ ポートをトランク ポートとして設定し、イネーブルにします。「スイッチ ポートのトランク ポートとしての設定とイネーブル化」（P.12-10）を参照してください。

ステップ 4　第 13 章「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）」または第 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）」に従って、インターフェイス コンフィギュレーションを実行します。

VLAN インターフェイスの設定

この項では、VLAN インターフェイスを設定する方法について説明します。ASA 5505 のインターフェイスの詳細については、「ASA 5505 インターフェイスについて」（P.12-1）を参照してください。

ガイドライン

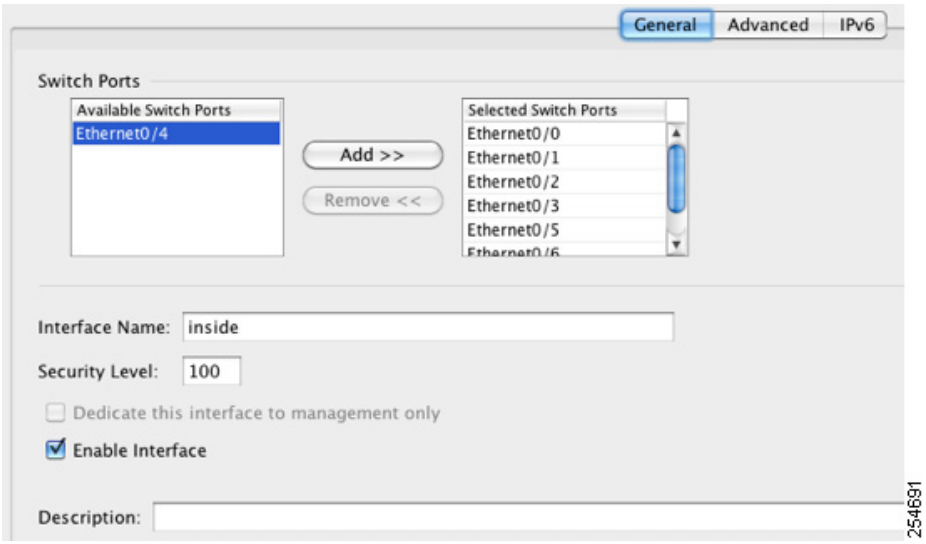
インターフェイスをすべて設定してから Easy VPN をイネーブルにすることをお勧めします。Easy VPN をイネーブルにすると、VLAN インターフェイスを追加または削除できません。また、セキュリティ レベルまたはインターフェイス名の変更もできません。

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　[Interfaces] タブで、[Add] をクリックします。

[Add 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　[Available Switch Ports] ペインでスイッチ ポートを選択し、[Add] をクリックします。

次のメッセージが表示されます。

"switchport" is associated with *name* interface.Adding it to this interface, will remove it from *name* interface.Do you want to continue?」

[OK] をクリックして、スイッチ ポートを追加します。

スイッチ ポートをインターフェイスに追加する場合、このメッセージは常に表示されます。コンフィギュレーションがない場合でも、スイッチ ポートは VLAN 1 インターフェイスにデフォルトで割り当てられています。

この VLAN に所属する他のスイッチ ポートにも繰り返します。

（注）　スイッチ ポートのデフォルト VLAN インターフェイスは VLAN 1 なので、インターフェイスからスイッチ ポートを削除すると、基本的にそのスイッチ ポートは VLAN 1 に再度割り当てられます。

ステップ 4　[Advanced] タブをクリックします。

（注）　IP アドレスの設定に関するエラー メッセージが表示されます。この時点で、IP アドレスとその他のパラメータを設定するか、[Yes] クリックして VLAN およびスイッチ ポートの設定を終了し、後で IP アドレスとその他のパラメータを第 13 章「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）」または第 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）」に従って設定します。

ステップ 5　[VLAN ID] フィールドに、このインターフェイスの VLAN ID を 1 ～ 4090 の範囲で入力します。

VLAN ID を割り当てない場合、ASDM により ID がランダムに割り当てられます。

ステップ 6　（基本ライセンスの場合はオプション）別の VLAN への接続開始を制限して、このインターフェイスが 3 番目の VLAN になるように、[Block Traffic From this Interface to] ドロップダウン リストで、この VLAN インターフェイスがトラフィックを開始できない VLAN を選択してください。

基本ライセンスでは、このコマンドを使用して制限した場合だけ、3 つ目の VLAN を設定できます。

たとえば、1 つの VLAN をインターネット アクセスの外部に、もう 1 つを内部ビジネス ネットワーク内に、そして 3 つ目をホーム ネットワークにそれぞれ割り当てます。自宅のネットワークはビジネス ネットワークにアクセスする必要がないので、自宅の VLAN でこのオプションを使用できます。ビジネス ネットワークは自宅のネットワークにアクセスできますが、その反対はできません。

2 つの VLAN インターフェイスに名前をすでに設定している場合、必ずこの設定を行ってから 3 番目のインターフェイスに名前を設定してください。ASA 5505 の基本ライセンスでは、ASA の 3 つの VLAN インターフェイスがフル機能で動作できません。

（注） Security Plus ライセンスにアップグレードすれば、このオプションを削除して、このインターフェイスのフル機能を取得できます。このオプションをイネーブルにしたままにすると、アップグレード後もインターフェイスの制限はそのまま残ります。

MAC アドレスおよび MTU を設定するには、「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 7　[OK] をクリックします。

次の作業

スイッチ ポートを設定します。「スイッチ ポートのアクセス ポートとしての設定とイネーブル化」（P.12-8）および「スイッチ ポートのトランク ポートとしての設定とイネーブル化」（P.12-10）を参照してください。

スイッチ ポートのアクセス ポートとしての設定とイネーブル化

デフォルト（コンフィギュレーションなし）では、すべてのスイッチ ポートがシャットダウンされ、VLAN 1 に割り当てられます。1 つの VLAN にスイッチ ポートを割り当てるには、アクセス ポートとして設定します。複数の VLAN を伝送するトランク ポートを作成するには、「スイッチ ポートのトランク ポートとしての設定とイネーブル化」（P.12-10）を参照してください。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る場合に、次の手順に従ってデフォルトのインターフェイス設定を変更する必要があるかどうかを確認するには、「ASA 5505 のデフォルト コンフィギュレーション」（P.3-22）を参照してください。

ASA 5505 のインターフェイスの詳細については、「ASA 5505 インターフェイスについて」（P.12-1）を参照してください。

注意　ASA 5505 は、ネットワーク内のループ検出用のスパニングツリー プロトコルをサポートしていません。したがって、ASA とのすべての接続は、ネットワーク ループ内で終わらないようにする必要があります。

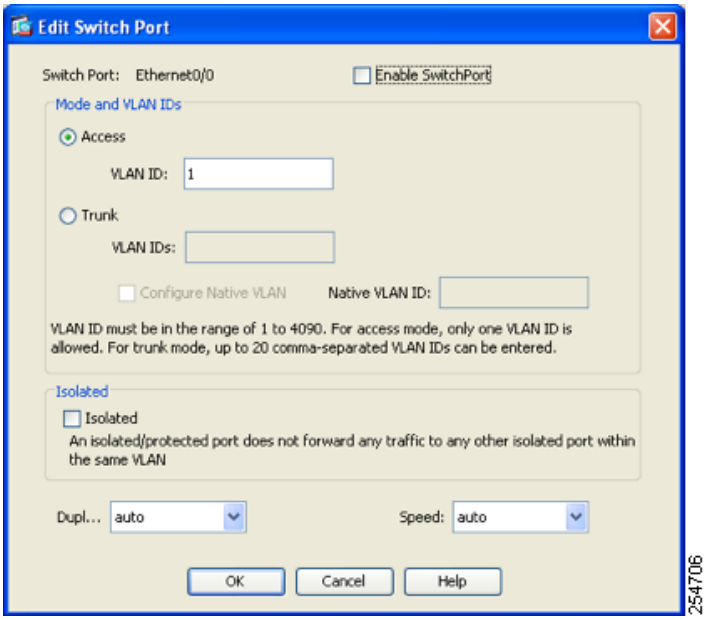
手順の詳細

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

ステップ 2　[Switch Ports] タブをクリックします。

ステップ 3　編集するスイッチ ポートをクリックします。

[Edit Switch Port] ダイアログボックスが表示されます。



ステップ 4　スイッチ ポートをイネーブルにするには、[Enable SwitchPort] チェックボックスをオンにします。

ステップ 5　[Mode and VLAN IDs] エリアで、[Access] オプション ボタンをクリックします。

ステップ 6　[VLAN ID] フィールドに、このスイッチ ポートに関連付けられている VLAN ID を入力します。VLAN ID は、1 ～ 4090 の範囲で入力できます。

デフォルトでは、VLAN ID を、「VLAN インターフェイスの設定」（P.12-6）で（[Configuration] > [Device Setup] > [Interfaces] > [Interfaces] > [Add/Edit Interface] ダイアログボックスで）設定を完了した VLAN インターフェイスから取得します。VLAN の割り当てはこのダイアログボックスで変更できます。変更を適用する場合、必ず VLAN コンフィギュレーションを新しい情報で更新してください。まだ追加していない VLAN を指定する場合、このダイアログボックスで指定するのではなく、「VLAN インターフェイスの設定」（P.12-6）に従って、VLAN を追加することをお勧めします。いずれの場合でも、「VLAN インターフェイスの設定」（P.12-6）に従って VLAN を追加してからスイッチ ポートを割り当てる必要があります。

ステップ 7　（任意）スイッチ ポートが同じ VLAN 上の他の保護されたスイッチ ポートと通信しないようにするには、[Isolated] チェックボックスをオンにします。

このオプションによって、スイッチ ポートは同じ VLAN 上の他の保護されたスイッチ ポートと通信できなくなります。スイッチ ポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互に分離する場合に、スイッチ ポートが相互に通信しないようにします。たとえば、3 つの Web サーバをホストする DMZ がある場合、各スイッチ ポートに [Protected] オプションを適用すると、Web サーバを相互に分離できます。内部ネットワークと外部ネットワークはいずれも 3 つの Web サーバすべてと通信でき、その逆も可能ですが、Web サーバは相互に通信できません。

ステップ 8　（任意）[Duplex] ドロップダウン リストから、[Full]、[Half]、または [Auto] を選択します。

デフォルトの設定は Auto です。PoE ポート Ethernet 0/6 または 0/7 でデュプレックスを [Auto] 以外に設定した場合、IEEE 802.3af をサポートしない Cisco IP Phone および Cisco ワイヤレス アクセス ポイントは検出されず、電力は供給されません。

ステップ 9　（任意）[Speed] ドロップダウン リストから、[10]、[100]、または [Auto] を選択します。

デフォルトの設定は Auto です。PoE ポート Ethernet 0/6 または 0/7 で速度を [Auto] 以外に設定した場合、IEEE 802.3af をサポートしない Cisco IP Phone および Cisco ワイヤレス アクセス ポイントは検出されず、電力は供給されません。

ステップ 10　[OK] をクリックします。

次の作業

- スイッチ ポートをトランク ポートとして設定する場合は、「スイッチ ポートのトランク ポートとしての設定とイネーブル化」（P.12-10）を参照してください。
- インターフェイス コンフィギュレーションを実行する場合は、第 13 章「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）」または第 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。

スイッチ ポートのトランク ポートとしての設定とイネーブル化

この手順では、802.1Q タグ付けを使用して複数の VLAN を伝送するトランク ポートの作成方法について説明します。トランク モードが使用できるのは Security Plus ライセンスだけです。

インターフェイスが 1 つの VLAN にだけ割り当てられるアクセス ポートを作成するには、「スイッチ ポートのアクセス ポートとしての設定とイネーブル化」（P.12-8）を参照してください。

ガイドライン

ネイティブまたは非ネイティブにかかわらず、少なくとも 1 つの VLAN が割り当てられないと、このスイッチ ポートはトラフィックを通過させることができません。

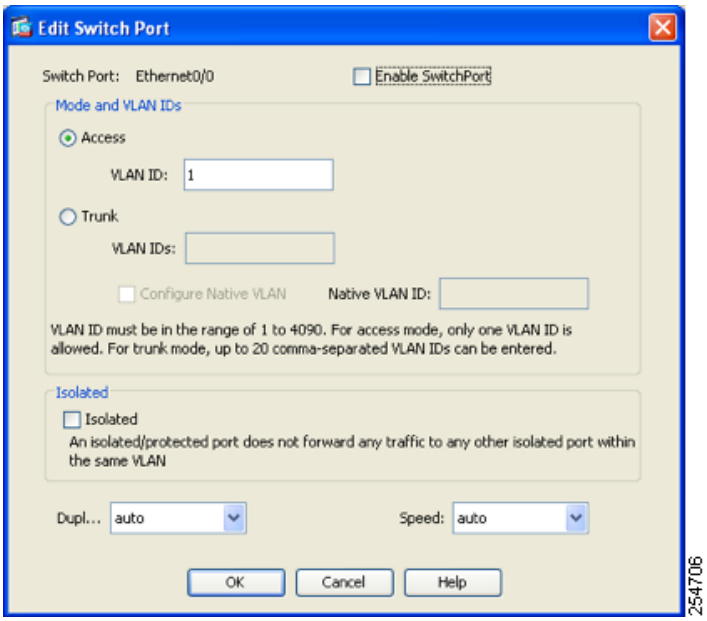
手順の詳細

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

ステップ 2　[Switch Ports] タブをクリックします。

ステップ 3　編集するスイッチ ポートをクリックします。

[Edit Switch Port] ダイアログボックスが表示されます。



ステップ 4　スイッチ ポートをイネーブルにするには、[Enable SwitchPort] チェックボックスをオンにします。

ステップ 5　[Mode and VLAN IDs] エリアで、[Trunk] オプション ボタンをクリックします。

ステップ 6　[VLAN IDs] フィールドに、このスイッチ ポートに関連付けられている VLAN ID をカンマで区切って入力します。VLAN ID は、1 ～ 4090 の範囲で入力できます。

このフィールドには、ネイティブ VLAN を含めることができますが、ネイティブ VLAN は必須ではありません。ネイティブ VLAN がこのフィールドに含まれているかどうかにかかわらず、トラフィックはネイティブ VLAN を通過します。

ネイティブまたは非ネイティブにかかわらず、少なくとも 1 つの VLAN が割り当てられないと、このスイッチ ポートはトラフィックを通過させることができません。

VLAN を設定済みの場合は、変更を適用すると、[Configuration] > [Device Setup] > [Interfaces] > [Interfaces] タブでそれぞれの VLAN に追加されたこのスイッチ ポートを確認できます。まだ追加していない VLAN を指定する場合、このダイアログボックスで指定するのではなく、「VLAN インターフェイスの設定」（P.12-6）に従って、VLAN を追加することをお勧めします。いずれの場合でも、「VLAN インターフェイスの設定」（P.12-6）に従って VLAN を追加してからスイッチ ポートを割り当てる必要があります。

ステップ 7　ネイティブ VLAN を設定するには、[Configure Native VLAN] チェックボックスをオンにし、[Native VLAN ID] フィールドに VLAN ID を入力します。VLAN ID は、1 ～ 4090 の範囲で入力できます。

ネイティブ VLAN 上のパケットは、トランク経由で送信されるときに変更されません。たとえば、ポートに VLAN 2、3、および 4 が割り当てられており、VLAN 2 がネイティブ VLAN である場合、ポートを出る VLAN 2 上のパケットは 802.1Q ヘッダーによって変更されません。このポートに入ってくるフレームは、802.1Q ヘッダーが付いていない場合は VLAN 2 に割り当てられます。

各ポートのネイティブ VLAN は 1 つのみですが、すべてのポートに同じネイティブ VLAN または異なるネイティブ VLAN を使用できます。

ステップ 8　（任意）スイッチ ポートが同じ VLAN 上の他の保護されたスイッチ ポートと通信しないようにするには、[Isolated] チェックボックスをオンにします。

このオプションによって、スイッチ ポートは同じ VLAN 上の他の保護されたスイッチ ポートと通信できなくなります。スイッチ ポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互

に分離する場合に、スイッチ ポートが相互に通信しないようにします。たとえば、3 つの Web サーバをホスティングする DMZ の場合、[Protected] オプションを各スイッチ ポートに適用すると、Web サーバを相互に孤立させることができます。内部ネットワークと外部ネットワークはいずれも 3 つの Web サーバすべてと通信でき、その逆も可能ですが、Web サーバは相互に通信できません。

ステップ 9　（任意）[Duplex] ドロップダウン リストから、[Full]、[Half]、または [Auto] を選択します。

デフォルトの設定は Auto です。PoE ポート Ethernet 0/6 または 0/7 でデュプレックスを [Auto] 以外に設定した場合、IEEE 802.3af をサポートしない Cisco IP Phone および Cisco ワイヤレス アクセス ポイントは検出されず、電力は供給されません。

ステップ 10　（任意）[Speed] ドロップダウン リストから、[10]、[100]、または [Auto] を選択します。

デフォルトの設定は Auto です。PoE ポート Ethernet 0/6 または 0/7 で速度を [Auto] 以外に設定した場合、IEEE 802.3af をサポートしない Cisco IP Phone および Cisco ワイヤレス アクセス ポイントは検出されず、電力は供給されません。

ステップ 11　[OK] をクリックします。

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

[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。

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.12-13）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.12-13）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。

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。

次の作業

第 13 章「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）」または第 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）」に従って、インターフェイス コンフィギュレーションを実行します。

ASA 5505 インターフェイスの機能履歴

表 12-1 に、この機能のリリース履歴を示します。

表 12-1　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	7.2(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。
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]。