ルータインターフェイスの設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、バグの修正や拡張機能はサポートしていません。

この章は次のトピックで構成されています。

Cisco IOS ルータでの基本的なインターフェイス設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

一般に、Security Manager にインターフェイスを追加するには、ポリシーの検出の説明に従って検出を実行します。インターフェイスを検出したあと、各インターフェイスのプロパティを変更できます。

また、Security Manager を使用して、物理インターフェイスおよび仮想インターフェイスを手動で設定することもできます。これは既存のデバイスのインターフェイス設定を変更するときに便利であり、ネットワークにデバイスを物理的に追加する前にデバイスのすべてのインターフェイスを設定できるようになります。

関連項目

- 使用可能なインターフェイス タイプ （2 ページ）
- 基本的なルータ インターフェイス設定の定義 （5 ページ）
- Cisco IOS ルータ インターフェイスの削除 （7 ページ）

使用可能なインターフェイス タイプ

表 1 : ルータ インターフェイス タイプ （2 ページ）では、Cisco IOS ルータで設定できるインターフェイスのタイプについて説明します。

表 *1:* ルータ インターフェイス タイプ

タイプ	説明
Null	ヌル インターフェイス。
Analysis-module	Network Analysis Module（NAM; ネットワーク分析モジュール）の内部インターフェイスに接続するファスト イーサネット インターフェイス。 （注） このタイプのインターフェイスには、速度やデュプレックス モードなどのパラメータを設定できません。
Async	非同期インターフェイスとして使用されるポート回線。
ATM	ATM インターフェイス。

タイプ	説明
BRI	ISDN BRI インターフェイス。このインターフェイス設定は、各 B チャネルに伝播します。B チャネルは個別に設定できません。 （注） BRI インターフェイスでコールを発信するには、ダイヤラ インターフェイス ポリシーを設定する必要があります。詳細については、Cisco IOS ルータ上のダイヤラ インターフェイス （36 ページ）を参照してください。
BVI	ブリッジ グループ仮想インターフェイス。BVI インターフェイスは、レイヤ3でトラフィックをブリッジグループのインターフェイスにルーティングする場合に使用します。
Content-engine	Content Engine（CE; コンテンツ エンジン）ネットワーク モジュール インターフェイス。 （注） このタイプのインターフェイスには、速度やデュプレックス モードなどのパラメータを設定できません。このタイプのインターフェイスのサブインターフェイスは作成できません。
Dialer	ダイヤラ インターフェイス。
Ethernet	イーサネット IEEE 802.3 インターフェイスです。
Fast Ethernet	100 Mbps イーサネット インターフェイスです。
FDDI	ファイバ分散データ インターフェイス。
Gigabit Ethernet	1000 Mbps イーサネット インターフェイス。
Group-Async	メイン非同期インターフェイス。このインターフェイス タイプは、1 つの非同期インターフェイスに他のインターフェイスを関連付けるためのものです。このように 1 対多の設定にすると、メインインターフェイスを設定することにより、関連付けられたすべてのメンバーインターフェイスを設定できるようになります。
HSSI	High-Speed Serial Interface（高速シリアル インターフェイス）の略。
Loopback	常時稼働しているインターフェイスをエミュレートする論理インターフェイス。たとえば、ルータにループバック インターフェイスがあると、ネイバーOSPFルータの物理インターフェイスがダウンしても、そのルータとの隣接が失われません。 ループバック インターフェイスの名前は、0 ～ 2147483647 の数値で終了する必要があります。 （注） このインターフェイス タイプは、すべてのプラットフォームでサポートされます。作成できるループバック インターフェイスの数に制限はありません。

タイプ	説明
Multilink	マルチリンク インターフェイス。Multilink PPP（MLP; マルチリンク PPP）に使用される論理インターフェイスです。
Port channel	ポート チャネル インターフェイス。このインターフェイス タイプを使用すると、複数のポイントツーポイント ファスト イーサネット リンクを 1 つの論理リンクにバンドルできます。その結果、最大 800 Mbps の双方向の帯域幅を実現できます。
POS	Packet-over-SONET（POS）インターフェイス プロセッサ上のパケット OC-3 インターフェイス。
PRI	ISDN PRI インターフェイス。23/30 個の B チャネルと 1 個の D チャネルが含まれています。
Serial	シリアル インターフェイス。
Switch	スイッチ インターフェイス。
Ten Gigabit Ethernet	10000 Mbps イーサネット インターフェイス。
Token Ring	トークン リング インターフェイス。
Tunnel	トンネル インターフェイス。 （注） 作成できる仮想トンネル インターフェイスの数に制限はありません。有効値の範囲は 0 ～ 2147483647 です。
VG-AnyLAN	100VG-AnyLAN ポート アダプタ。
VLAN	仮想 LAN サブインターフェイス。
Virtual Template	仮想テンプレート インターフェイス。ユーザがダイヤルインすると、定義済みの設定テンプレートにより、仮想アクセス インターフェイスが設定されます。ユーザがダイヤルアウトすると、仮想アクセスインターフェイスがダウンし、他のダイヤルインに使用できるようにリソースが解放されます。

関連項目

- 基本的なルータ インターフェイス設定の定義 （5 ページ）
- Cisco IOS ルータ インターフェイスの削除 （7 ページ）
- Cisco IOS ルータでの基本的なインターフェイス設定 （2 ページ）

基本的なルータ インターフェイス設定の定義

Cisco IOS ルータのインターフェイスまたはサブインターフェイスを定義するときは、インターフェイスに名前を付け、インターフェイスに IP アドレスを割り当てる方法を指定します。また任意で、速度、最大伝送単位（MTU）、カプセル化のタイプなど他のプロパティを定義することもできます。

（注） 基本的なインターフェイス設定は、常に設定先のデバイスにローカルなものとなります。このポリシーは他のデバイスと共有できません。ただし、高度なインターフェイス設定は共有できます。詳細については、Cisco IOS ルータでの高度なインターフェイス設定（17 ページ）を参照してください。

関連項目

- Cisco IOS ルータ インターフェイスの削除 （7 ページ）

ステップ 1 デバイスビューで、ポリシーセレクタから [インターフェイス（Interfaces）] > [インターフェイス（Interfaces）] を選択します。

[Router Interfaces] ページ （8 ページ）が表示されます。

ステップ 2 新規インターフェイスまたはサブインターフェイスを追加するには、[Add Row] ボタンをクリックして [Create Router Interface] ダイアログボックスを開きます。

既存のインターフェイスまたはサブインターフェイスを編集するには、[Interfaces] テーブルでそのインターフェイスを選択し、[Edit Row] ボタンをクリックして [Edit Router Interface] ダイアログボックスを開きます。これらのダイアログボックスのフィールドについては、[Create Router Interface] ダイアログボックス （10 ページ）を参照してください。

ステップ 3 Security Manager でこのインターフェイスまたはサブインターフェイスをアクティブに管理するには、[有効（Enabled）] を選択します。このオプションを選択しないと、インターフェイス/サブインターフェイス定義は保持されますが、インターフェイス/サブインターフェイス自体は無効になります（または「シャットダウン」されます）。

ステップ 4 [タイプ（Type）] リストから [インターフェイス（Interface）] または [サブインターフェイス（Subinterface）] を選択します。

ステップ 5 インターフェイスを作成している場合は、インターフェイスの名前を入力します。[選択（Select）] をクリックするとダイアログボックスが開き、インターフェイスタイプ、およびインターフェイスの位置情報（カード、スロット、サブインターフェイスなど）に基づいて、標準の名前を生成できます。ダイアログボックスを使用してインターフェイス名を生成する方法については、[Interface Auto Name Generator] ダイアログボックス （16 ページ）を参照してください。

（注） BVI インターフェイスに名前を付けるときには、カード番号としてブリッジ グループ番号を使用します。対応するブリッジ グループを設定せずに BVI インターフェイスを設定すると、展開が失敗します。

ステップ 6 サブインターフェイスを作成している場合は、次の項目を設定します。

a) [親（Parent）]：このサブインターフェイスの親インターフェイスを選択します。

b) [サブインターフェイス ID（Subinterface ID）]：サブインターフェイスを識別するための数値を入力します。

（注） Security Manager は、シリアル サブインターフェイスをマルチポイントではなくポイントツーポイントとして設定します。

ステップ 7 [レイヤタイプ（Layer Type）] を指定するには、このリストから [レベル 2（Level 2）]（データリンク）または [レベル 3（Level 3）]（ネットワーク）オプションを選択します。

ステップ 8 このインターフェイス/サブインターフェイスに **IP** アドレスを割り当てる方法を選択し、必要に応じて他にも情報を指定します。

- [スタティック IP（Static IP）]：[IP アドレス（IP Address）] および [サブネットマスク（Subnet Mask）] を指定します。
- [DHCP]：他に情報は必要ありません。
- [PPPoE]：他に情報は必要ありません。
- [アンナンバード（Unnumbered）]：IP アドレスを「借用する」インターフェイスの名前を指定します。

（注） レイヤ 2 インターフェイスでは IP アドレスはサポートされません。

ステップ 9 このほかに、インターフェイス/サブインターフェイスのプロパティをいくつか定義します。

- [ネゴシエーション（Negotiation）] チェックボックスを使用して、インターフェイスのオートネゴシエーションをイネーブルまたはディセーブルにします。

オートネゴシエーションでは、リモート デバイスの機能が検出され、2 つのデバイス間で可能な最大のパフォーマンスがネゴシエーションされます。ネゴシエーションがイネーブルであると、[Fast Ethernet Duplex] オプションおよび [Speed] オプションはディセーブルになります。

（注） オートネゴシエーションは、ASR デバイス上のファストイーサネットインターフェイスおよびギガビット イーサネット インターフェイスに対してだけ使用可能になります。

- [デュプレックス（Duplex）] リストから伝送モードを選択します。[Auto] を選択した場合は、伝送モードを自動的に検出するように、このインターフェイスの接続先となるネットワーク デバイスを設定してください（ASR では [Auto] を使用できません。代わりにオートネゴシエーションを使用してください）。

（注） デュプレックス値を定義するには、固定速度を設定する必要があります。トンネルインターフェイスおよびループバック インターフェイスは、この設定値をサポートしません。

- [速度（Speed）] リストから伝送速度を選択します。[Auto] を選択した場合は、伝送速度を自動的に検出するように、このインターフェイスの接続先となるネットワーク デバイスを設定してください（ASR では [Auto] を使用できません。代わりにオートネゴシエーションを使用してください）。

- 最大伝送単位（**MTU**）を入力して、このインターフェイスがサポートできる最大パケットサイズをバイト単位で定義します。

（注） インターフェイスプロパティには自動的に設定されるものもあれば、使用できないものもあり、インターフェイスタイプおよび基礎となるポートタイプによって決まります。たとえば、[Speed] オプションはファストイーサネットインターフェイスおよびギガビットイーサネットインターフェイスにだけ使用できます。

ステップ 10 [カプセル化（Encapsulation）] リストからカプセル化方法を選択します。

- [なし（None）]：カプセル化なし。他にパラメータは必要ありません。
- （イーサネット サブインターフェイス専用）[DOT1Q]：VLAN カプセル化。IEEE 802.1Q 標準の定義に従います。このサブインターフェイスには、次の VLAN パラメータを指定します。
  - このサブインターフェイスに関連付ける VLAN ID を入力します。

（注） 同じ物理インターフェイスに設定されたすべてのサブインターフェイスでは、VLAN ID がすべて一意である必要があります。

- 802.1Q トランク インターフェイスを定義している場合は、[Native VLAN] を選択します。

ヒント VLAN をサブインターフェイスに関連付けずに、イーサネット インターフェイスで DOT1Q カプセル化を設定するには、CLI コマンドまたは FlexConfig を使用して **vlan-id dot1q** コマンドを入力します。FlexConfig ポリシーとポリシー オブジェクトについてを参照してください。メインインターフェイスに VLAN を設定すると、ルータに設定できる VLAN の数が多くなります。

- （シリアルインターフェイス専用）[フレームリレー（Frame Relay）]：IETF フレームリレーのカプセル化。サブインターフェイスの Data-Link Connection Identifier（DLCI; データリンク接続識別子）を指定します。

（注） フレーム リレーは、親インターフェイスに設定する必要があります。

（注） IETF フレーム リレー カプセル化によって、Cisco IOS ルータと他のベンダーの機器との間に相互運用性が実現されます。Cisco フレーム リレー カプセル化を設定するには、CLI コマンドまたは FlexConfig を使用します。

ステップ 11 （任意）インターフェイスの説明を最大 1024 文字で入力します。

ステップ 12 [OK] をクリックして、インターフェイス/サブインターフェイス定義を保存し、ダイアログボックスを閉じます。新規インターフェイスが [Router Interfaces] ページに表示されます。サブインターフェイスが親インターフェイスの下に表示されます。

Cisco IOS ルータ インターフェイスの削除

仮想インターフェイスの定義をいつでも削除できますが、このオプションの使用には最大限の注意を払ってください。インターフェイスがこのルータ向けのポリシー定義に含まれている場

合は、インターフェイスを削除すると、そのポリシー定義をデバイスに展開しようとしたときに失敗します。

（注） 基本的なインターフェイス定義を削除しても、**[インターフェイス（Interface）] > [設定（Settings）] > [詳細設定（Advanced Settings）]** に設定されている高度な設定は削除されません。このような高度な設定は個別に削除する必要があります。そうしないと、展開が失敗します。

（注） [Router Interfaces] ページから物理インターフェイスの定義を削除しても、そのインターフェイスはデバイスから削除されません。誤ってこの操作を実行した場合は、再検出を実行して Security Manager に定義を復元できます。詳細については、Security Manager にすでに存在するデバイス上のポリシーの検出を参照してください。

関連項目

- 基本的なルータ インターフェイス設定の定義 （5 ページ）
- Cisco IOS ルータでの基本的なインターフェイス設定 （2 ページ）

ステップ 1 ツールバーの [デバイスビュー（Device View）] ボタンをクリックします。

ステップ 2 デバイス セレクタからルータを選択します。

ステップ 3 ポリシーセレクタから **[インターフェイス（Interfaces）] > [インターフェイス（Interfaces）]** を選択します。[Router Interfaces] ページが表示されます。このページのフィールドの説明については、表 2 : [Router Interfaces] ページ （9 ページ）を参照してください。

ステップ 4 テーブルからインターフェイスを選択し、[削除（Delete）] をクリックします。インターフェイスが削除されます。

[Router Interfaces] ページ

[Router Interfaces] ページは、選択した Cisco IOS ルータでインターフェイス定義（物理および仮想）を表示、作成、編集、および削除する場合に使用します。[Router Interfaces] ページには、Security Manager が検出したインターフェイスだけでなく、デバイスをシステムに追加したあとに手動で追加したインターフェイスも表示されます。

（注） [Interfaces] ポリシーは、他のルータ ポリシーと異なり、複数のデバイス間で共有できません。一方、[Advanced Settings] ポリシーは共有できます。ローカルポリシーと共有ポリシーを参照してください。

詳細については、 Cisco IOS ルータでの基本的なインターフェイス設定 （2 ページ）を参照してください。

ナビゲーション パス

デバイスセレクタから Cisco IOS ルータを選択し、ポリシーセレクタから **[インターフェイス（Interfaces）] > [インターフェイス（Interfaces）]** を選択します。

関連項目

- 使用可能なインターフェイス タイプ （2 ページ）
- Cisco IOS ルータ インターフェイスの削除 （7 ページ）
- テーブル カラムおよびカラム見出しの機能
- テーブルのフィルタリング

フィールド リファレンス

表 2 : [Router Interfaces] ページ

要素	説明
Interface Type	インターフェイス タイプ。サブインターフェイスが、親インターフェイスの下にインデントされて表示されます。
インターフェイス名	インターフェイスの名前。
[有効（Enabled）]	インターフェイスが現在イネーブルである（Security Manager で管理されている）のか、ディセーブルである（シャットダウン状態である）のかを示します。
IPアドレス	スタティック アドレスで定義されたインターフェイスの IP アドレス。
IP アドレス タイプ	インターフェイスに割り当てられた IP アドレスのタイプ。スタティック、DHCP、PPPoE、アンナンバードのいずれかになります（IP アドレスは、選択したインターフェイス ロールによって定義されます）。
インターフェイス ロール	選択したインターフェイスに割り当てられるインターフェイス ロール。
[追加（Add）] ボタン	[Create Router Interface] ダイアログボックス （10 ページ）が開きます。ここから、選択したルータにインターフェイスを作成できます。
[編集（Edit）] ボタン	[Create Router Interface] ダイアログボックス （10 ページ）が開きます。ここから、選択したインターフェイスを編集できます。

要素	説明
[削除（Delete）] ボタン	選択したインターフェイスをテーブルから削除します。インターフェイスを削除する前に、他のポリシーでそのインターフェイスが使用されていないことを確認してください。

[Create Router Interface] ダイアログボックス

[Create Router Interface] ダイアログボックスは、選択した Cisco IOS ルータで物理インターフェイスおよび仮想インターフェイスを作成または編集する場合に使用します。

ヒント　インターフェイス設定は、デバイスのタイプに固有のものです。デバイス タイプまたはインターフェイス タイプによっては、このページのオプションの多くがグレーになります。そのオプションが適用されないか、または設定できないためです。

ナビゲーション パス

[Router Interfaces] ページ （8 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- Cisco IOS ルータでの基本的なインターフェイス設定 （2 ページ）
- Cisco IOS ルータ インターフェイスの削除 （7 ページ）
- Cisco IOS ルータでの高度なインターフェイス設定 （17 ページ）

フィールド リファレンス

表 3 : [Create Router Interface] ダイアログボックス

要素	説明
有効	インターフェイスはイネーブルである（シャットダウン状態でない）かどうかを指定します。このオプションを選択しないと、インターフェイスは設定には作成されますが、シャットダウンされます。
タイプ（Type）	インターフェイスまたはサブインターフェイスを定義しているかどうかを指定します。

要素	説明
名前	インターフェイスにだけ適用されます。 インターフェイスの名前。名前を手動で入力するか、または [選択（Select）] をクリックして名前を自動的に生成するためのダイアログボックスを表示します。[Interface Auto Name Generator] ダイアログボックス （16 ページ）を参照してください。 論理インターフェイスには、名前のあとに数値が必要です。 • ダイヤラ インターフェイスの範囲は 0 ～ 799 です。 • ループバック インターフェイスの範囲は 0 ～ 2147483647 です。 • BVI インターフェイスの範囲は 1 ～ 255 です。 • ヌル インターフェイスに唯一許可されている値は 0 です。
親	サブインターフェイスだけに適用されます。 サブインターフェイスの親インターフェイス。このリストから親インターフェイスを選択します。
Subinterface ID	サブインターフェイスだけに適用されます。 サブインターフェイスの ID 番号。

要素	説明
IP	インターフェイスに IP アドレスを割り当てる方法。 • [Static IP]：インターフェイスのスタティック IP アドレスおよびサブネットマスクを定義します。オプションの下に表示されるフィールドにこの情報を入力します。 （注） ドット付き 10 進（たとえば、255.255.255.255）または CIDR 表記（/32）を使用して、マスクを定義できます。連続および不連続ネットワークマスク（IPv4 アドレスに対応）を参照してください。 • [DHCP]：インターフェイスは、DHCP サーバからダイナミックに IP アドレスを取得します。 • [PPPoE]：ルータは、（PPP/IPCP 経由で）中央のサーバから自身の登録済み IP アドレスを自動的にネゴシエートします。次のインターフェイス タイプが PPPoE をサポートしています。 • Async • シリアル • HSSI（High-Speed Serial Interface） • ダイヤラ • [BRI]、[PRI]（ISDN） • Virtual template • マルチリンク • [Unnumbered]：インターフェイスは、デバイス上の別のインターフェイスから IP アドレスを取得します。[Interface] リストからインターフェイスを選択します。このオプションは、ポイントツーポイント インターフェイスでだけ使用できます。 （注） レイヤ 2 インターフェイスでは IP アドレスはサポートされません。レイヤ 2 インターフェイスに IP アドレスを定義した場合には、展開が失敗します。

要素	説明
レイヤタイプ（Layer Type）	インターフェイスが定義されている OSI レイヤ。 • [Unknown]：レイヤは不明です。 • [Layer 2]：データ リンク層。物理層（レイヤ 1）を制御するプロトコルと、メディアに送信するデータを事前にフレーム化する方法が含まれています。レイヤ 2 は、ブリッジングおよびスイッチングに使用されます。レイヤ 2 インターフェイスには IP アドレスがありません。 • [Layer 3]：ネットワーク層。主として論理インターネットワーク パスでデータをパケット単位でルーティングします。このルーティングは、IP アドレスを使用して実現されます。
Negotiation	ASR で使用可能で、ファスト イーサネット インターフェイスおよびギガビット イーサネット インターフェイスにだけ適用されます。 オートネゴシエーションでは、リモート デバイスの機能が検出され、2 つのデバイス間で可能な最大のパフォーマンスがネゴシエーションされます。ネゴシエーションがイネーブルであると、[Duplex] オプションおよび [Speed] オプションはディセーブルになります。
デュプレックス	インターフェイス伝送モード。 • [None]：伝送モードが、デバイス固有のデフォルト設定に戻ります。 • [Full]：インターフェイスは同時に送受信します（全二重）。 • [Half]：インターフェイスは送信または受信できますが、送受信を同時に行うことはできません（半二重）。これがデフォルトです。 • [Auto]：ルータは、適切な伝送モード（全二重または半二重）を自動的に検出して設定します。ASR では使用できません。代わりにオートネゴシエーションを使用してください。 （注） [Auto] モードを使用している場合は、このインターフェイスの接続先となるアクティブなネットワーク デバイス上のポートも、伝送モードを自動的にネゴシエートするように設定されていることを確認してください。それ以外の場合は、適切な固定モードを選択します。 （注） デュプレックス値を設定できるのは、[Speed] を [Auto] ではなく固定速度に設定する場合だけです。 （注） この設定値は、シリアル、HSSI、ATM、PRI、DSL、トンネル、ループバックの各インターフェイスには適用されません。

要素	説明
速度	ファスト イーサネット インターフェイスおよびギガビット イーサネット インターフェイスにだけ適用されます。 インターフェイスの速度。 • [None]：設定はデバイスに設定できません。 • [10]：10 メガビット/秒（10Base-T ネットワーク）。 • [100]：100 メガビット/秒（100Base-T ネットワーク）。これは、ファスト イーサネット インターフェイスのデフォルトです。 • [1000]：1000 メガビット/秒（ギガビット イーサネット ネットワーク）。これは、ギガビット イーサネット インターフェイスのデフォルトです。 • [Auto]：ルータは適切なインターフェイス速度を自動的に検出して設定します。ASR では使用できません。オートネゴシエーションを使用してください。 （注） [Auto] モードを使用している場合は、このインターフェイスの接続先となるアクティブなネットワーク デバイス上のポートも、伝送速度を自動的にネゴシエートするように設定されていることを確認してください。それ以外の場合は、適切な固定速度を選択します。
[MTU]	最大伝送単位。このインターフェイスが処理できる最大パケット サイズ（バイト単位）です。 シリアル、イーサネット、ファスト イーサネットの各インターフェイスの有効値の範囲は、64 ～ 17940 バイトです。 ギガビット イーサネット インターフェイスの有効値の範囲は、1500 ～ 9216 バイトです。
カプセル化	インターフェイスによって実行されたカプセル化のタイプ。 • [None]：カプセル化なし。 • [DOT1Q]：VLAN カプセル化。IEEE 802.1Q 標準の定義に従います。イーサネット サブインターフェイスだけに適用されます。 • [Frame Relay]：IETF フレーム リレーのカプセル化。（シリアル サブインターフェイスではなく）シリアル インターフェイスにだけ適用されます。 （注） IETF フレーム リレー カプセル化によって、Cisco IOS ルータと他のベンダーの機器との間に相互運用性が実現されます。Cisco フレーム リレー カプセル化を設定するには、CLI コマンドまたは FlexConfig を使用します。

要素	説明
VLAN ID（Admin. VLAN ID）	カプセル化のタイプが DOT1Q であるサブインターフェイスにだけ適用されます。 このサブインターフェイスに関連付けられた VLAN ID。VLAN ID は、このサブインターフェイスで 802.1Q タグ付きパケットを送受信する場所を示します。VLAN ID が指定されていない場合は、サブインターフェイスでトラフィックを送受信できません。有効値の範囲は 1 ～ 4094 です。 （注） 同じ物理インターフェイスに設定されたすべてのサブインターフェイスでは、VLAN ID がすべて一意である必要があります。 ヒント VLAN をサブインターフェイスに関連付けずに、イーサネット インターフェイスで DOT1Q カプセル化を設定するには、CLI コマンドまたは FlexConfig を使用して **vlan-id dot1q** コマンドを使用します。FlexConfig ポリシーとポリシー オブジェクトについてを参照してください。メイン インターフェイスに VLAN を設定すると、ルータに設定できる VLAN の数が多くなります。
ネイティブ VLAN	カプセル化のタイプが DOT1Q で、802.1Q トランク インターフェイスとして機能する物理インターフェイスを設定しているときにだけ適用します。トランキングは、2 つのデバイスをつなぐポイントツーポイント リンクに複数の VLAN を定義してトラフィックを伝送する方法です。 選択されている場合、[VLAN ID] フィールドで指定された ID を使用して、このインターフェイスにネイティブ VLAN が関連付けられます（ネイティブ VLAN に VLAN ID が指定されていない場合、デフォルト値は 1 です）。ネイティブ VLAN は、タグ付けされていないすべての VLAN パケットがデフォルトで論理的に割り当てられる VLAN です。これには、VLAN に関連付けられた管理トラフィックが含まれます。VLAN ID が定義されていない場合、デフォルトは 1 です。 たとえば、このインターフェイスの VLAN ID が 1 である場合、すべての着信非タグ付きパケットと VLAN ID が 1 であるパケットが、サブインターフェイスではなくメイン インターフェイスで受信されます。メインインターフェイスから送信されるパケットは、802.1Q タグが付与されずに送信されます。 オフにすると、ネイティブ VLAN はこのインターフェイスに関連付けられません。 （注） トランク インターフェイスのサブインターフェイスには、ネイティブ VLAN を設定できません。リンクの両端には必ず同じ [Native VLAN] 値を設定してください。同じ値を設定しないと、トラフィックが失われたり、間違った VLAN に送信される場合があります。

要素	説明
DLCI	フレーム リレーがカプセル化されるシリアル サブインターフェイスにだけ適用されます。 サブインターフェイスに関連付けるデータリンク接続識別子を入力します。有効値の範囲は 16 ～ 1007 です。 （注） Security Manager は、シリアル サブインターフェイスをマルチポイントではなくポイントツーポイントとして設定します。
説明	インターフェイスに関する追加の情報（最大 1024 文字）。
ロール（Roles）	このインターフェイスに割り当てられたインターフェイス ロール。ロールがまだ割り当てられていない場合は、メッセージが表示されます。

[Interface Auto Name Generator] ダイアログボックス

[Interface Auto Name Generator] ダイアログボックスは、インターフェイスのタイプとルータやスイッチでのインターフェイスの場所に基づいて、Security Manager でインターフェイスの名前を生成する場合に使用します。

ナビゲーション パス

[Create Router Interface] ダイアログボックス （10 ページ）に移動し、[タイプ（Type）] リストから [インターフェイス（Interface）] を選択し、[名前（Name）] フィールドで [選択（Select）] をクリックします。

フィールド リファレンス

表 4 : [Interface Auto Name Generator] ダイアログボックス

要素	説明
タイプ	インターフェイスのタイプ。このリストで選択した内容が、生成した名前の先頭部分となり、[Result] フィールドに表示されます。詳細については、使用可能なインターフェイス タイプ （2 ページ）を参照してください。
カード	インターフェイスに関連するカード。 （注） BVI インターフェイスを定義している場合は、対応するブリッジ グループの番号を入力します。
スロット	インターフェイスに関連するスロット。
[ポート（Port）]	インターフェイスに関連するポート。 （注） これらのフィールドに入力した情報によって、[Result] フィールドに表示される、生成される名前の残りの部分が形成されます。

要素	説明
結果	入力したインターフェイス タイプおよび場所の情報を基に Security Manager が生成した名前。このフィールドに表示される名前は読み取り専用です。 ヒント　このダイアログボックスを閉じたあと、必要に応じて [Create Router Interface] ダイアログボックスで生成した名前を編集できます。

Cisco IOS ルータでの高度なインターフェイス設定

Security Manager では、[Interfaces] ページに定義できる基本的なインターフェイス定義に加えて、高度な設定も、インターフェイスでサポートされていれば定義できます。

[Interfaces] ページに定義されている基本的なインターフェイス設定と異なり、[Advanced Settings] ポリシーは複数のデバイスで共有できます。これにより、同じ設定の複数のデバイスを簡単に設定できます。デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用を参照してください。

選択したインターフェイス、サブインターフェイス、またはインターフェイス ロールに関して、次に挙げるように、さまざまな高度な設定を定義できます。

- Cisco Discovery Protocol（CDP）設定。
- インターネット制御メッセージ プロトコル（ICMP）設定。
- ダイレクト ブロードキャスト設定。
- 平均負荷を求めるための負荷間隔。
- ルーティング プロトコルに使用するスループット遅延。
- TCP 最大セグメント サイズの設定。
- UDP ブロードキャストを転送するためのヘルパー アドレス。ヘルパー アドレスを入力する方法の詳細については、ヘルパー アドレスについて （18 ページ）を参照してください。
- Maintenance Operation Protocol（MOP; メンテナンス オペレーション プロトコル）のイネーブル化。
- Virtual Fragmentation Reassembly（VFR; 仮想フラグメンテーション再構成）のイネーブル化。
- プロキシ ARP のイネーブル化。
- NBAR プロトコル検出のイネーブル化。
- Unicast Reverse Path Forwarding（uRPF; ユニキャスト リバース パス転送）のイネーブル化および設定。

ヒント　特定のインターフェイスではなくインターフェイス ロールを選択すると、デバイス上の複数のインターフェイスに対してこれらの設定を一度にまとめて定義できます。たとえば、All-Ethernets インターフェイス ロールを定義した場合は、1 つの定義だけでデバイス上のあらゆるイーサネット インターフェイスに対して同じ高度な設定を定義できます。インターフェイス ロール オブジェクトについてを参照してください。

はじめる前に

- 基本的なインターフェイス設定を定義します。Cisco IOS ルータでの基本的なインターフェイス設定　（2 ページ）を参照してください。

ステップ 1　次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[インターフェイス（Interfaces）] > [設定（Settings）] > [詳細設定（Advanced Settings）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータインターフェイス（Router Interfaces）] > [設定（Settings）] > [詳細設定（Advanced Settings）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Advanced Interface Settings] ページが表示されます（[Advanced Interface Settings] ダイアログボックス　（21 ページ）を参照）。

ステップ 2　次のいずれかを実行します。

- [追加（Add）] ボタンをクリックして、インターフェイスまたはインターフェイスロールをテーブルに追加します。[詳細インターフェイス設定（Advanced Interface Settings）] ダイアログボックスで、インターフェイスまたはインターフェイスロールの名前を入力します。あるいは、[選択（Select）] をクリックして既存のロールを選択するか、または新しいロールを作成します。
- テーブル内の既存エントリを選択し、[編集（Edit）] ボタンをクリックしてそのエントリの設定を変更します。

ステップ 3　選択したインターフェイスに必要な高度な設定を設定します。各設定の詳細については、[Advanced Interface Settings] ダイアログボックス　（21 ページ）を参照してください。

ステップ 4　[OK] をクリックして定義を保存します。定義が、[Advanced Interface Settings] テーブルに表示されます。

ヘルパー アドレスについて

ネットワーク ホストが、ユーザ データグラム プロトコル（UDP）ブロードキャストを使用して、アドレス、設定、名前の情報を確認することがあります。これは、そのホストが存在するネットワーク セグメントに必要なサーバが配置されていない場合には問題となります。ルータは、デフォルトでは自身が属しているサブネットを越えて UDP ブロードキャストを転送しな

いためです。特定のクラスのブロードキャストをヘルパーアドレスに転送するようにインターフェイスを設定すると、この状況を改善できます。

ヘルパー アドレスがよく使用されるのは、ルータが DHCP クライアントのリレー エージェントとして機能しており、そのクライアントが別のサブネットにある DHCP サーバに問い合わせる必要がある場合です。ヘルパー アドレスは、特定の DHCP サーバであるか、または複数の DHCP サーバが含まれているセグメントのネットワーク アドレスとなります。また、DHCP サーバごとにヘルパー アドレスを設定することもできます。

図 1 : Helper Addresses （19 ページ）では、ネットワーク 192.168.1.0 にあるホストは、10.44.23.7 をヘルパー アドレスとして使用して、UDP ブロードキャストを他のネットワークに転送できます。一方、ネットワーク 10.44.0.0 にあるホストは、192.168.1.19 をヘルパー アドレスとして使用できます。

図 *1 : Helper Addresses*

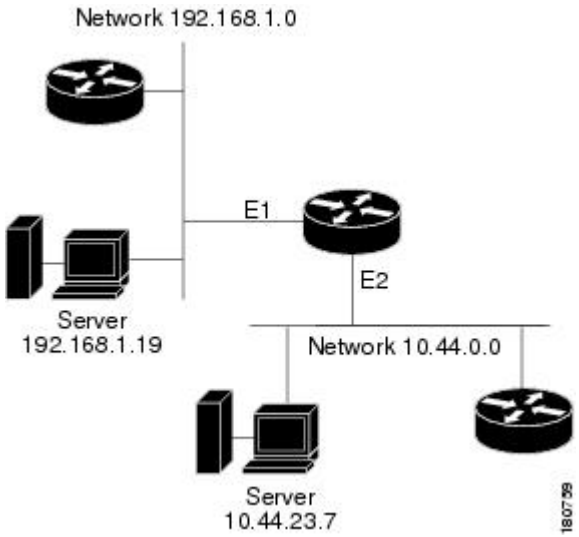


表 5 : ヘルパー アドレスに転送されるデフォルトの UDP サービス （19 ページ）に、ヘルパー アドレスに転送できるデフォルトの UDP サービスを示します。

表 *5 :* ヘルパー アドレスに転送されるデフォルトの *UDP* サービス

Service	ポート
BOOTP/DHCP クライアント	68
BOOTP/DHCP サーバ	67
DNS	53
NetBIOS データグラム サービス	138
NetBIOS ネーム サービス	137

Service	ポート
TACACS	49
TFTP	69
Time	37

ヒント　他の UDP サービスを転送するには、CLI または FlexConfig を使用して、ip forward-protocol コマンドを設定します。表 5 : ヘルパー アドレスに転送されるデフォルトの UDP サービス （19 ページ）に記載されているデフォルト サービスのいずれも転送できないようにするには、このコマンドの no 形式を使用します。

UDP パケットまたは IP パケットがヘルパー アドレスを使用するためには、次に挙げるすべての条件を満たす必要があります。

- 受信したフレームの MAC アドレスは、すべてが 1 のブロードキャスト アドレス（ffff.ffff.ffff）である必要があります。
- IP の宛先アドレスは、すべてが 1 のブロードキャスト（255.255.255.255）または受信インターフェイスのサブネット ブロードキャストであるか、あるいは no ip classless コマンドも設定されている場合には受信インターフェイスのメジャーネットブロードキャストである必要があります。
- IP の存続可能時間（TTL）値は 2 以上である必要があります。
- IP プロトコルは UDP（17）である必要があります。

関連項目

- [Advanced Interface Settings] ページ （20 ページ）
- Cisco IOS ルータでの基本的なインターフェイス設定 （2 ページ）

[Advanced Interface Settings] ページ

[Advanced Interface Settings] ページは、ルータに高度なインターフェイス定義（物理および仮想）を設定する場合に使用します。高度な設定の例としては、Cisco Discovery Protocol（CDP）設定、ICMP メッセージ設定、仮想フラグメント再構成設定などがあります。特定のインターフェイスまたはインターフェイス ロールの設定値を設定できます。テーブルの各カラムはエントリの高度な設定の概要であり、それぞれの説明については [Advanced Interface Settings] ダイアログボックス （21 ページ）を参照してください。

高度な設定を設定するには、次の手順を実行します。

- [追加（Add）] ボタンをクリックして、インターフェイスまたはインターフェイスロールをテーブルに追加し、[高度なインターフェイスの設定（Advanced Interface Settings）] ダイアログボックスに入力します。
- エントリを選択し、[編集（Edit）] ボタンをクリックして、既存のエントリを編集します。
- エントリを選択し、[削除（Delete）] ボタンをクリックして削除します。

詳細については、Cisco IOS ルータでの高度なインターフェイス設定 （17 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [インターフェイス（Interfaces）] > [設定（Settings）] > [Advanced Settings] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータインターフェイス（Router Interfaces）] > [設定（Settings）] > [詳細設定（Advanced Settings）] を選択します。[高度な設定（Advanced Settings）] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- [Router Interfaces] ページ （8 ページ）
- 使用可能なインターフェイス タイプ （2 ページ）
- Cisco IOS ルータ インターフェイスの削除 （7 ページ）
- テーブル カラムおよびカラム見出しの機能
- テーブルのフィルタリング

[Advanced Interface Settings] ダイアログボックス

[Advanced Interface Settings] ダイアログボックスは、次の表の説明に従って、選択したインターフェイスのさまざまな高度な設定を定義する場合に使用します。

ナビゲーション パス

[Advanced Interface Settings] ページ （20 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- Cisco IOS ルータでの基本的なインターフェイス設定 （2 ページ）
- Cisco IOS ルータでの高度なインターフェイス設定 （17 ページ）
- Cisco IOS ルータ インターフェイスの削除 （7 ページ）

• 使用可能なインターフェイス タイプ （2 ページ）

フィールド リファレンス

表 *6 : [Advanced Interface Settings]* ダイアログボックス

要素	説明
インターフェイス（Interface）	高度な設定を定義するインターフェイス。インターフェイスまたはインターフェイスロールの名前を入力するか、[選択（Select）] をクリックしてインターフェイスまたはインターフェイスロールを選択します。目的の項目が表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 （注） レイヤ 2 インターフェイスでサポートされている高度な設定は、[Max Bandwidth]、[Load Interval]、および [CDP] だけです。
最大帯域幅（Max Bandwidth）	上位のプロトコルとキロビット/秒（kbps）で通信するための帯域幅値。このフィールドに定義する値は情報パラメータにすぎず、物理インターフェイスには影響を与えません。
Load Interval	インターフェイスでの平均負荷の計算に使用される時間の長さ（秒単位）。有効値の範囲は 30 ～ 600 秒（30 秒の倍数単位）です。デフォルトは 300 秒（5 分）です。負荷間隔は、サブインターフェイスではサポートされません。 平均負荷の計算に使用する時間を短くするには、デフォルト値を変更します。時間を短くすると、負荷計算に短いトラフィック バーストが強く反映されるようになります。 負荷データは 5 秒おきに収集されます。このデータは、秒あたりのビット数およびパケット数単位で表される入出力速度、負荷、信頼性など、負荷統計を算出するために使用されます。負荷データは加重平均計算を使用して算出され、新しい負荷データの方が古い負荷データよりも加重が大きくなります。 ヒント このオプションを使用すると、バックアップインターフェイスをアクティブにする可能性を増減できます。たとえば、アクティブインターフェイスで負荷が突然急増して、バックアップ ダイヤル インターフェイスがトリガーされる場合があります。

要素	説明
TCP 最大セグメントサイズ（TCP Maximum Segment Size）	このインターフェイスを通過する TCP SYN パケットの Maximum Segment Size（MSS; 最大セグメント サイズ）。有効値の範囲は 500 ～ 1460 バイトです。値を指定しない場合、MSS は発信元ホストによって設定されます。 このオプションは、TCP セッションがルータを通過する際にドロップされるのを防ぐのに役立ちます。このオプションは、TCP フレーム サイズのオートネゴシエーションを実行する ICMP メッセージが（ファイアウォールなどによって）ブロックされるときに使用します。DMVPN ネットワークのトンネル インターフェイスには、このオプションを使用することを強く推奨します。 （注） 一般に、最適な MSS は 1452 バイトです。この値に、20 バイトの IP ヘッダー、20 バイトの TCP ヘッダー、および 8 バイトの PPPoE ヘッダーが追加されて、イーサネット リンクの MTU サイズと同じ 1500 バイトのパケットになります。
Helper Addresses	このインターフェイスで受信されるユーザ データグラム プロトコル（UDP）ブロードキャストを転送するために使用されるヘルパー アドレス。ネットワーク/ホスト オブジェクトのアドレスまたは名前を 1 つ以上入力します。あるいは、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新規オブジェクトを作成します。 ルータは、デフォルトでは自身のサブネットの外部にブロードキャストを転送しません。ヘルパー アドレスを使用すると、ルータは特定のタイプの UDP ブロードキャストをユニキャストとして宛先サブネット上のアドレスに転送できるようになります。詳細については、ヘルパー アドレスについて （18 ページ）を参照してください。
Interface Throughput Delay	インターフェイスで想定される遅延（数十マイクロ秒単位。たとえば、3000 は 30,000 マイクロ秒になります）。1 ～ 16777215 の値を入力でき、デフォルトはインターフェイスのタイプによって異なります。 上位のプロトコルが、遅延情報を使用して動作を決定することがあります。たとえば、IGRP では遅延情報を使用して衛星のリンクと地上のリンクを区別できます。この設定値は情報を提供するだけのものであり、インターフェイスの実際の遅延には影響を与えません。

要素	説明
Cisco Discovery Protocol settings	Cisco Discovery Protocol（CDP）に関連する設定。CDP は、メディアおよびプロトコルに依存しないデバイス検出プロトコルであり、すべてのシスコ製装置（ルータ、アクセス サーバ、ブリッジ、スイッチなど）上で動作します。主としてネイバーデバイスのプロトコルのアドレスを取得し、そのデバイスのプラットフォームを検出するのに使用されます。次のオプションがあります。 • [Enable CDP]：このインターフェイスで Cisco Discovery Protocol（CDP）をイネーブルにするかどうかを指定します。ATM インターフェイスでは CDP をイネーブルにできません。 • [Log CDP Messages]：イーサネット インターフェイスで、このインターフェイスのデュプレックスの不一致をログに記録するかどうかを指定します。
ICMP メッセージ設定	
Enable Redirect Messages	デバイスが受信時と同じインターフェイス経由でパケットを同じサブネット上の他のデバイスに再送信するようになっている場合には、インターネット制御メッセージ プロトコル（ICMP）リダイレクト メッセージの送信をイネーブルにするかどうかを指定します。リダイレクトメッセージは、デバイスがパケットの発信者に対して、宛先へのルートからそのデバイスを削除し、宛先までより直接的に到達できるパスを提供する別のデバイスに置き換えるように指示する場合に送信されます。
Enable Unreachable Messages	ICMP 到達不能メッセージの送信をイネーブルにするかどうかを指定します。到達不能メッセージは、次の 2 つの状況で送信されます。 • インターフェイスは、不明なプロトコルを使用する自身宛の非ブロードキャストパケットを受信した場合、ICMP 到達不能メッセージを送信元に送信します。 • デバイスは、最終宛先宛のパケットを受信したものの、その宛先アドレスへのルートがないためにパケットを配信できない場合、ICMP ホスト到達不能メッセージをパケットの発信者に送信します。 （注） これは、null0 インターフェイスでサポートされている唯一の高度な設定です。
Enable Mask Reply Messages	ICMP マスク応答メッセージの送信をイネーブルにするかどうかを指定します。マスク応答メッセージは、マスク要求メッセージに応えて送信されます。マスク要求メッセージは、デバイスが特定のサブネットワークのサブネット マスクを知る必要があるときに送信されます。
追加設定（Additional Settings）	
Enable Maintenance Operation Protocol (MOP)	インターフェイスで MOP をイネーブルにするかどうかを指定します。システム ソフトウェアのアップグレードとダウンロード、リモート テスト、問題診断など、ユーティリティ サービスの MOP を使用できます。

要素	説明
Enable Virtual Fragment Reassembly (VFR)	このインターフェイスで Virtual Fragmentation Reassembly（VFR; 仮想フラグメンテーション再構成）をイネーブルにするかどうかを指定します。VFR は、Cisco IOS ファイアウォールがダイナミック ACL を作成してさまざまなフラグメンテーション攻撃からネットワークを保護できるようにする機能です。
Enable Proxy ARP	インターフェイスでプロキシアドレス解決プロトコル（ARP）をイネーブルにするかどうかを指定します。RFC 1027 に規定されているプロキシ ARP は、あるホスト（通常はルータ）が他のマシン向けの ARP 要求に応答して、パケットを実際の宛先にルーティングするという手法です。プロキシ ARP を使用すると、ルーティングやデフォルト ゲートウェイを設定しなくても、サブネット上のマシンがリモートのサブネットに容易に到達できるようになります。
Enable NBAR Protocol Discovery	このインターフェイスで Network-Based Application Recognition（NBAR）をイネーブルにして、トラフィックを検出し、すべてのプロトコルのトラフィック統計情報が NBAR に認識されるようにするかどうかを指定します。プロトコル検出により、インターフェイスを通過するアプリケーション プロトコルを検出し、QoS ポリシーを策定してプロトコルに適用できます。詳細については、次の URL にアクセスしてください。 http://www.cisco.com/en/US/products/ps6616/products_qanda_item09186a00800a3ded.shtml

要素	説明
Enable Directed Broadcasts ACL	このインターフェイスが宛先サブネットに直接接続されているときに、ダイレクトブロードキャストパケットがリンクレイヤブロードキャストとして「展開」されるかどうかを指定します。選択解除されている場合、このインターフェイスが直接接続されているサブネット宛のダイレクトブロードキャストパケットはブロードキャストされず、ドロップされます。これがデフォルトです。 IP ダイレクト ブロードキャストは、宛先アドレスが発信元のノードとは別のサブネットで有効なブロードキャスト アドレスとなっている IP パケットです。このような場合、パケットは宛先サブネットに達するまでユニキャストパケットであるかのように転送されます。 このオプションは、宛先サブネットでのダイレクトブロードキャストの最終伝送にだけ影響を与えます。IP ダイレクトブロードキャストの送信ユニキャストルーティングには影響を与えません。 ダイレクトブロードキャストをイネーブルにした場合は、宛先サブネットでどのダイレクト ブロードキャストをブロードキャストできるかを ACL に基づいて決定できます。このインターフェイスが直接接続されているサブネット宛のそれ以外のダイレクト ブロードキャストはドロップされます。標準または拡張 ACL オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 **ヒント** ダイレクト ブロードキャストと特に ICMP ダイレクト ブロードキャストはこれまで悪意のある個人によって悪用されたことがあるため、ダイレクトブロードキャストが必要ないインターフェイスではこのオプションを選択しないことを推奨します。ダイレクトブロードキャストをイネーブルにするときは、その使用を制限する ACL を適用してください。
Unicast Reverse Path Forwarding（uRPF; ユニキャスト リバース パス転送）設定	
Enable Unicast RPF	インターフェイスで Unicast Reverse Path Forwarding（uRPF; ユニキャスト リバース パス転送）をイネーブルにするかどうかを指定します。インターフェイスでユニキャスト RPF をイネーブルにすると、ルータはそのインターフェイスで受信されるすべてのパケットを検査します。ルータは、送信元アドレスが FIB にあることを確認し、ユニキャスト RPF 設定に基づいて必要な対策を講じます。ユニキャスト RPF を使用すると、不正な形式の IP 送信元アドレスまたは偽装（スプーフィング）された IP 送信元アドレスがルータを通過したために発生する問題を軽減できます。不正な形式の送信元アドレスまたは偽装された送信元アドレスは、送信元 IP アドレスのスプーフィングに基づく DoS 攻撃である場合があります。ユニキャスト RPF の詳細については、『*Cisco IOS Interface and Hardware Component Command Reference*』で **ip verify unicast source reachable-via** コマンドの説明を参照してください。 ユニキャスト RPF をイネーブルにするには、Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）もグローバルにイネーブルにする必要があります。CEF の詳細については、Cisco IOS ルータでの CEF インターフェイス設定 （32 ページ）を参照してください。

要素	説明
[モード（Mode）]	ユニキャスト RPF の厳格さを示します。 • loose モード：デフォルト。着信パケットを調べて送信元アドレスが Forwarding Information Base（FIB; 転送情報ベース）にあるかどうかを判断し、ルータ上のいずれかのインターフェイスを経由して送信元に到達可能である場合にはパケットを許可します。 loose モードは、非対称パスが有効な送信元ネットワーク（FIB に含まれるネットワーク）からのパケットを許可するインターフェイスで使用します。たとえば、ISP ネットワークのコアに存在するルータでは、ルータから転送されるパケットに最適なパスが、ルータに戻ってくるパケットに対しても選択されるとはかぎりません。 • strict モード：着信パケットを調べて送信元アドレスが FIB にあるかどうかを判断し、パケットを受信したインターフェイスを経由して送信元に到達可能である場合にだけパケットを許可します。 strict モードは、1 つのパスだけが有効な送信元ネットワーク（FIB に含まれるネットワーク）からのパケットを許可するインターフェイスで使用します。このほか、有効なネットワークが着信インターフェイスで切り替えられる場合にかぎり、ルータに特定のネットワークへのパスが複数あるときにも strict モードを使用します。無効なネットワークのパケットはドロップされます。たとえば、ISP ネットワークのエッジにあるルータには、対称リバース パスが設定されている可能性があります。strict モードは、マルチホームにも適用できる場合があります。ただし、加重やローカル プリファレンスなど任意のボーダー ゲートウェイ プロトコル（BGP）属性を使用して対称ルーティングを実現する場合にかぎられます。
Allow Use Of Default Route for RPF Verification	パケットを通過させるかどうかを判断するときに、ユニキャスト RPF がデフォルト ルート経由で確認したプレフィックスに対して照合を正しく実行できるようにするかどうかを指定します。通常、FIB に存在する送信元であっても、デフォルト ルートを経由するだけであればドロップされます。
Allow Self Ping	ルータが自身のインターフェイスに対して ping を実行できるかどうかを指定します。デフォルトでは、ユニキャスト RPF をイネーブルにすると、ルータによって生成され、かつルータを宛先とするパケットがドロップされるため、トラブルシューティングと管理が困難になることがあります。 **注意** self-ping を許可すると、Denial of Service（DoS; サービス拒絶）ホールとなる可能性があります。
ACL（ユニキャスト RPF の場合）	ユニキャスト RPF をイネーブルにした場合は、ACL を適用して、リバース パスが見つからない場合のパケットの処理方法を改良できます。ACL を指定した場合は、パケットがユニキャスト RPF のチェックに失敗したときに、ACL の内容に基づいて、（ACL で拒否ステートメントを使用して）パケットをドロップするか、（ACL の許可ステートメントを使用して）転送するかが判断されます。標準または拡張 ACL オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。

Cisco IOS ルータでの IPS モジュール インターフェイス設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS および IOS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

ルータによっては、Cisco Intrusion Prevention System Advanced Integration Module や Network Module などの IPS モジュールをインストールできます。このようなモジュールをインストールし、アクティブにするときには、IPS モジュール インターフェイス設定ポリシーで次の情報を定義する必要があります。

- モジュールとルータ間のインターフェイスの名前。
- モジュールの障害モード。モジュールが失敗する場合は、すべてのトラフィックを許可するか、またはすべてのトラフィックを拒否するようにモジュールを設定できます。
- モニタするルータ インターフェイス。特定のインターフェイスに名前を付けたり、インターフェイス ロールを使用して複数のインターフェイスを一度に処理したりできます。たとえば、All-Ethernets インターフェイス ロールを定義した場合は、1 つの定義だけでデバイス上のあらゆるイーサネット インターフェイスに対して同じモニタリング設定を定義できます。インターフェイス ロール オブジェクトについてを参照してください。

ヒント IPS モジュール インターフェイス設定ポリシーを定義したあと、ポリシーを共有し、他のデバイスにポリシーを割り当てることができます。これにより、同じ設定の複数のデバイスを簡単に設定できます。デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用を参照してください。

はじめる前に

基本的なインターフェイス設定を定義します。 Cisco IOS ルータでの基本的なインターフェイス設定 （2 ページ）を参照してください。

ステップ 1 次のいずれかを実行します。

- （デバイス ビュー）ポリシー セレクタから [インターフェイス（Interfaces）] > [設定（Settings）] > [IPS モジュール（IPS Module）] を選択します。
- （ポリシー ビュー）ポリシー タイプ セレクタから [ルータ インターフェイス（Router Interfaces）] > [設定（Settings）] > [PVC] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[IPS Module Interface Settings] ページが表示されます。このページのフィールドの説明については、[IPS Module Interface Settings] ページ （29 ページ）を参照してください。

ステップ 2 [IPS Module Interface Settings] の各フィールドには、IPS インターフェイスの名前（IDS-Sensor1/0 など）を入力するか、または [Select] をクリックしてリストから名前を選択します。また、モジュールが失敗した場合にすべてのトラフィックを許可するのか（フェールオープン）、すべてのトラフィックを拒否するのか（フェールクローズ）を決定します。

ステップ 3 モジュールがモニタするルータ インターフェイスを特定します。[IPSモジュールサービスのモジュールモニタリング設定（IPS Module Service Module Monitoring Settings）] テーブルの下にある [追加（Add）] ボタンをクリックしてインターフェイスをリストに追加するか、またはインターフェイスを選択し、[編集（Edit）] ボタンをクリックして既存のインターフェイスの設定を変更します。[IPS Monitoring Information] ダイアログボックスを使用して、インターフェイス名またはインターフェイス ロール、モニタリング モード、およびアクセス リスト（ある場合）を定義します。詳細については、[IPS Monitoring Information] ダイアログボックス （31 ページ）を参照してください。

[IPS Module Interface Settings] ページ

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

[IPS Module Interface Settings] ページは、Cisco Intrusion Prevention System Advanced Integration Module または Network Module に関する設定を定義する場合に使用します。モジュールは、IPS 6.0 以降を実行している必要があります。IPS インターフェイスの障害モード、およびモジュールがモニタするインターフェイスを定義できます。ルータが IPS モジュールをホストしている場合にだけ、このポリシーを設定します。

注意 Cisco IOS IPS と Cisco IPS モジュールは併用できません。IPS モジュールがインストールされているときには、Cisco IOS IPS はディセーブルである必要があります。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [インターフェイス（Interfaces）] > [設定（Settings）] > [IPSモジュール（IPS Module）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータインターフェイス（Router Interfaces）] > [設定（Settings）] > [PVC] を選択します。新しいポリシーを作成するか、共有ポリシー セレクタから既存のポリシーを選択します。

関連項目

- Cisco IOS ルータでの IPS モジュール インターフェイス設定 （28 ページ）

- テーブル カラムおよびカラム見出しの機能
- テーブルのフィルタリング

フィールド リファレンス

表 *7 : [IPS Module Interface Settings]* ページ

要素	説明
Interface Name	IPS モジュール インターフェイスの名前。名前を入力するか、[選択（Select）] をクリックしてインターフェイスまたはインターフェイスロールを選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。
Fail Over Mode	モジュールの障害時にモジュールがトラフィック検査を処理する方法。フェール オープン（検査なしですべてのトラフィックを通過させる）か、またはフェール クローズ（すべてのトラフィックをドロップする）のいずれかになります。デフォルトはフェール オープンです。
[IPS Module Service Module Monitoring Settings] テーブル	IPS モジュールがモニタするルータ上のインターフェイスのリスト。 テーブルには、インターフェイスまたはインターフェイス ロールの名前、モニタリングがインラインか無差別か、およびインターフェイスでの検査のために ACL を使用してトラフィックをフィルタリングするかどうかが表示されます。インライン モードの場合、IPS モジュールが直接トラフィック フローに入り込むため、悪意のあるトラフィックを目的のターゲットに到達する前にドロップして、攻撃を阻止できます。無差別モードでは、パケットはセンサーを通過しません。センサーは、実際に転送されたパケットではなくモニタ対象トラフィックのコピーを分析します。ACL が一致した場合、一致したトラフィックは検査されません。 • インターフェイスをテーブルに追加するには、[Add] ボタンをクリックし、 [IPS Monitoring Information] ダイアログボックス （31 ページ）に入力します。 • インターフェイスの設定を編集するには、そのインターフェイスを選択し、[Edit] ボタンをクリックします。 • インターフェイスを削除するには、そのインターフェイスを選択し、[Delete] ボタンをクリックします。

[IPS Monitoring Information] ダイアログボックス

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしていますが、バグの修正や拡張機能はサポートしていません。

[IPS Monitoring Information] ダイアログボックスは、IPS モジュールがモニタするインターフェイスのプロパティを追加または編集する場合に使用します。

ナビゲーション パス

[IPS Module Interface Settings] ページ （29 ページ）に移動し、[IPSモジュールサービスのモジュールモニタリング設定（IPS Module Service Module Monitoring Settings）] テーブルの下にある [追加（Add）] ボタンまたは [編集（Edit）] ボタンをクリックします。

関連項目

- Cisco IOS ルータでの IPS モジュール インターフェイス設定 （28 ページ）
- Cisco IOS ルータでの基本的なインターフェイス設定 （2 ページ）

フィールド リファレンス

表 8 : [IPS Monitoring Information] ダイアログボックス

要素	説明
Interface Name	モジュールがモニタするインターフェイスまたはインターフェイス ロールの名前。名前を入力するか、[選択（Select）] をクリックしてインターフェイスまたはインターフェイスロールを選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。
Monitoring Mode	インターフェイスをモニタする方法。 • [Inline mode]：IPS モジュールが直接トラフィック フローに入り込むため、悪意のあるトラフィックを目的のターゲットに到達する前にドロップして、攻撃を阻止できます。 • [Promiscuous mode]：パケットはセンサーを通過しません。センサーは、実際に転送されたパケットではなくモニタ対象トラフィックのコピーを分析します。

要素	説明
アクセス リスト（Access List）	検査のためにこのインターフェイスでトラフィックをフィルタリングするのに使用する標準または拡張アクセス リスト ポリシー オブジェクトの名前（そのポリシー オブジェクトを適用する場合）。ACL が一致すると、その ACL に対してトラフィックは検査されません。[選択（Select）] をクリックして、ACL を選択するか、または新規 ACL を作成します。

Cisco IOS ルータでの CEF インターフェイス設定

Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）は高度なレイヤ 3 IP スイッチング テクノロジーで、Web 中心のアプリケーションまたは対話型セッションを特徴とするインターネットや各種ネットワークなど、少量のトラフィックを伝送するネットワークから複雑なパターンで大量のトラフィックを伝送するネットワークまで、あらゆる種類のネットワークのネットワーク パフォーマンスおよびスケーラビリティを最適化します。CEF は、ほとんどの Cisco IOS ルータでデフォルトでイネーブルになります。

一般に、ルータで **show ip cef** コマンドを使用して統計情報を表示できるように CEF アカウンティングをイネーブルにする場合を除き、CEF ポリシーを設定する必要はありません。このほか、CEF を無効にする場合や、送信元/宛先パケット ストリームではなくパケットに基づいてロード バランスを実施するなどデフォルト以外の CEF 動作を特定のインターフェイスに設定する場合にも、CEF ポリシーを設定します。

インターフェイスの代替 CEF 設定を設定する場合は、特定のインターフェイスに名前を付けたり、インターフェイス ロールを使用して複数のインターフェイスを一度に処理したりできます。たとえば、All-Ethernets インターフェイス ロールを定義した場合は、1 つの定義だけでデバイス上のあらゆるイーサネット インターフェイスに対して同じ CEF 設定を定義できます。インターフェイス ロール オブジェクトについてを参照してください。

ヒント CEF インターフェイス設定ポリシーを定義したあと、ポリシーを共有し、他のデバイスにポリシーを割り当てることができます。これにより、同じ設定の複数のデバイスを簡単に設定できます。デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用を参照してください。

はじめる前に

基本的なインターフェイス設定を定義します。 Cisco IOS ルータでの基本的なインターフェイス設定 （2 ページ）を参照してください。

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [インターフェイス（Interfaces）]>[設定（Settings）]>[CEF] を選択します。

- （ポリシービュー）ポリシータイプセレクタから [ルータインターフェイス（Router Interfaces）] > [設定（Settings）] > [CEF] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[CEF Interface Settings] ページが表示されます。このページのフィールドの説明については、[CEF Interface Settings] ページ （33 ページ）を参照してください。

ステップ 2 CEF をイネーブルにする場合は、目的に応じたアカウンティング オプションを選択します。

ステップ 3 特定のインターフェイスにデフォルト以外の動作を設定する場合は、そのインターフェイスを [CEF Interface Settings] テーブルに追加します。テーブルの下にある [追加（Add）] ボタンをクリックしてインターフェイスをリストに追加するか、またはインターフェイスを選択し、[編集（Edit）] ボタンをクリックして既存のインターフェイスの設定を変更します。これらのオプションの詳細については、[CEF Interface Settings] ダイアログボックス （35 ページ）を参照してください。

[CEF Interface Settings] ページ

[CEF Interface Settings] ページは、シスコ エクスプレス フォワーディングの設定を定義する場合に使用します。CEF は高度なレイヤ 3 IP スイッチング テクノロジーで、Web 中心のアプリケーションまたは対話型セッションを特徴とするインターネットや各種ネットワークなど、少量のトラフィックを伝送するネットワークから複雑なパターンで大量のトラフィックを伝送するネットワークまで、あらゆる種類のネットワークのネットワーク パフォーマンスおよびスケーラビリティを最適化します。CEF は、ほとんどの Cisco IOS ルータでデフォルトでイネーブルになります。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [インタフェイス（Interfaces）] > [設定（Settings）] > [CEF] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータインターフェイス（Router Interfaces）] > [設定（Settings）] > [CEF] を選択します。新しいポリシーを作成するか、共有ポリシー セレクタから既存のポリシーを選択します。

関連項目

- Cisco IOS ルータでの CEF インターフェイス設定 （32 ページ）
- テーブル カラムおよびカラム見出しの機能
- テーブルのフィルタリング

フィールド リファレンス

表 *9 : [CEF Interface Settings]* ページ

要素	説明
Enable Cisco Express Forwarding	デバイスでグローバルに CEF をイネーブルにするかどうかを指定します。デバイスで CEF をディセーブルにできない場合にはグレーになります。CEF をグローバルにイネーブルにする場合にだけ、ページの他の設定を設定できます。
CEF Network Accounting	CEFアカウンティングをグローバルに設定するためのオプションです。アカウンティング統計情報を収集すると、ルータで **show ip cef** コマンドを使用してその情報を表示できます。次のオプションを選択して、さまざまなタイプのアカウンティングをイネーブルにできます。 • [Enable Accounting for Traffic Through Non-Recursive Prefixes]：ネクストホップが直接接続されたネットワーク プレフィックスの場合、非再帰アカウンティングにより、プレフィックスを介したパケット収集のエクスプレスフォワーディングがイネーブルになります。 • [プレフィックス単位のアカウンティングの有効化（Enable Per-Prefix Accounting）]：パケットのネットワークプレフィックスに基づいたアカウンティング統計情報。 • [Enable Prefix Length Accounting]：ネットワーク プレフィックス長に基づいたアカウンティング統計情報。 • [Enable Load Balance Hash Accounting]：宛先単位のロード バランシング（デフォルト）を使用すると、CEF は 16 の一続きのハッシュ バケットを使用して、送信元アドレスおよび宛先アドレスに基づいて使用可能なパスを配布します。ロード バランス ハッシュ アカウンティングをイネーブル化すると、ハッシュ バケット単位のカウンタが用意されます。

要素	説明
CEF Interface Settings table	特殊な CEF 設定を定義しているルータ上のインターフェイス。CEF をグローバルにイネーブルにすると、デフォルトではルータ上のすべてのインターフェイスが CEF をイネーブルにし、宛先単位のロードバランシングを使用します。インターフェイスに別の動作を設定する場合にだけ、インターフェイスをこのテーブルに追加します。 テーブルには、インターフェイスまたはインターフェイス ロールの名前、CEF がイネーブルかディセーブルか、およびインターフェイスがロード バランシングを宛先またはパケット単位で実施しているかが表示されます。各フィールドの詳細については、[CEF Interface Settings] ダイアログボックス （35 ページ）を参照してください。 • テーブルにインターフェイスを追加するには、[Add] ボタンをクリックします。 • インターフェイスの設定を編集するには、そのインターフェイスを選択し、[Edit] ボタンをクリックします。 • インターフェイスを削除するには、そのインターフェイスを選択し、[Delete] ボタンをクリックします。

[CEF Interface Settings] ダイアログボックス

[CEF Interface Settings] ダイアログボックスは、グローバルなデフォルトとは異なる設定にするときに、インターフェイスの CEF プロパティを追加または編集する場合に使用します。

ナビゲーション パス

[CEF Interface Settings] ページ （33 ページ）に移動してから、[CEF インターフェイス設定（CEF Interface Settings）] テーブルの下にある [追加（Add）] ボタンまたは [編集（Edit）] ボタンをクリックします。

関連項目

• Cisco IOS ルータでの CEF インターフェイス設定 （32 ページ）
• Cisco IOS ルータでの基本的なインターフェイス設定 （2 ページ）

フィールド リファレンス

表 *10 : [CEF Interface Settings]* ダイアログボックス

要素	説明
Interface Name	CEF を設定しているインターフェイスまたはインターフェイス ロールの名前。名前を入力するか、[選択（Select）] をクリックしてインターフェイスまたはインターフェイスロールを選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。
Enable CEF on Interface	インターフェイスでCEFをイネーブルにするかどうかを指定します。CEFは、デフォルトでイネーブルになっています。
ロードバランシング	インターフェイスがトラフィックのロードバランシングを実施する方法。宛先単位またはパケット単位になります。 宛先単位のロードバランシングでは、特定の送信元/宛先ペアのすべてのパケットが同じパスを通ります。パケット単位ロードバランシングでは、特定の送信元/宛先ペアのパケットが常に同じ等コストルートを取るとはかぎらないため、宛先への到着順序がばらばらになることがあります。 デフォルトは、トラフィックの宛先に基づいたロードバランシングです。

Cisco IOS ルータ上のダイヤラ インターフェイス

サイト間 VPN（ダイヤル バックアップの設定を参照）のダイヤル バックアップ ポリシーを設定する場合は、事前に適切な Cisco IOS ルータにダイヤラ インターフェイス ポリシーを設定する必要があります。ダイヤラ インターフェイス ポリシーは、ダイヤラ プールを使用して、ダイヤル バックアップで使用されているダイヤラ インターフェイスをルータ上の物理 BRI インターフェイスに関連付けます。各ダイヤラ インターフェイスは、単一のダイヤラ プールに関連付けられます。ダイヤラ プールには、1 つ以上の物理インターフェイスを含めることができます。複数のダイヤラ インターフェイスが、同じダイヤラ プールを参照できます。

以降のトピックでは、Cisco IOS ルータでダイヤラ インターフェイス ポリシーを作成する方法について説明します。

- ダイヤラ プロファイルの定義 （36 ページ）
- BRI インターフェイス プロパティの定義 （38 ページ）

ダイヤラ プロファイルの定義

ダイヤラ プロファイルを設定するときには、ダイヤラ インターフェイスを表すインターフェイスまたはインターフェイス ロールを選択し、ダイヤルする番号を指定する必要があります。また、プール ID を割り当てる必要があります。プール ID は、物理ダイヤラ インターフェイ

スを設定するときに、このダイヤラインターフェイスを参照するために使用されます。また、回線のデフォルトのタイムアウト設定を変更することもできます。

（注） IP は、Security Manager がダイヤラ プロファイルに対してサポートする唯一のプロトコルです。

（注） ダイヤラ プロファイルの認証パラメータが、PPP ポリシーに定義されています。

はじめる前に

ルータに仮想および物理ダイヤラ インターフェイスを定義します。 Cisco IOS ルータでの基本的なインターフェイス設定 （2 ページ）を参照してください。

（注） また、オプションで仮想および物理ダイヤラ インターフェイスのインターフェイス ロールを定義できます。 ダイヤラ プロファイルの定義 （36 ページ） を参照してください。

関連項目

- BRI インターフェイス プロパティの定義 （38 ページ）
- Cisco IOS ルータ上のダイヤラ インターフェイス （36 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[インタフェース（Interfaces）] > [設定（Settings）] > [ダイヤラ（Dialer）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータインターフェイス（Router Interfaces）] > [設定（Settings）] > [ダイヤラ（Dialer）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Dialer] ページが表示されます。このページのフィールドの説明については、表 11 : [Dialer] ページ （40 ページ）を参照してください。

ステップ 2 [ダイヤラインターフェイス（Dialer Interfaces）]ページの上部にあるテーブルからダイヤラプロファイルを選択し、[編集（Edit）]をクリックします。あるいは、プロファイルを作成するときには[追加（Add）]をクリックします。[Dialer Profile] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、表 12 : [Dialer Profile] ダイアログボックス （42 ページ）を参照してください。

ステップ 3 仮想ダイヤラインターフェイスを表すインターフェイスまたはインターフェイスロールの名前を入力します。あるいは [選択（Select]） をクリックしてインターフェイス ロール オブジェクトを選択するか、または新しいインターフェイス ロール オブジェクトを作成します。詳細については、ポリシー定義中のインターフェイスの指定を参照してください。

ステップ 4 ダイヤラ プロファイルの名前を入力します。名前を付けると、適切なダイヤラ プールを物理インターフェイスに割り当てるのが容易になります。BRI インターフェイス プロパティの定義 （38 ページ）を参照してください。

ヒント ダイヤラ インターフェイスがバックアップとして機能するサイトに論理的に関連付けられた名前を定義することを推奨します。たとえば、ダイヤラ インターフェイスが London サイトのバックアップ接続として機能している場合は、ダイヤラ プロファイルに London という名前を定義します。

ステップ 5 このダイヤラ インターフェイスに関連付けるダイヤラ プールの ID 番号を入力します。各ダイヤラ インターフェイスは、単一のプールに関連付けられます。ただし、複数のインターフェイスを同じダイヤラ プールに関連付けることもできます。

ステップ 6 ダイヤラ インターフェイスに割り当てるダイヤラ グループの数を入力します。

ステップ 7 （任意）[インタレスティングトラフィック ACL（Interesting Traffic ACL）] フィールドに、このダイヤラ プロファイルを使用したコールの開始を許可するパケットを定義する拡張 ACL オブジェクトの名前を入力します。あるいは、[選択（Select）] をクリックしてリストから拡張 ACL オブジェクトを選択するか、または新しい拡張 ACL オブジェクトを作成します。このオプションは、ダイヤラを使用できる IP トラフィックを制限する場合に使用します。

ステップ 8 ダイヤラ インターフェイス接続のリモート側の電話番号となるダイヤラ文字列を入力します。

ステップ 9 （任意）必要に応じてデフォルトのタイムアウト値（[Idle Timeout] および [Fast Idle Timeout]）を変更します。

ステップ 10 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。ダイヤラ プロファイルは、[Dialer] ページの [Dialer Profile] テーブルに表示されます。

BRI インターフェイス プロパティの定義

適切なインターフェイスまたはインターフェイス ロールを選択し、インターフェイスが属するダイヤラ プールを定義し、ISDN スイッチ タイプを定義して、ダイヤラ インターフェイス ポリシーに使用される物理 BRI インターフェイスのプロパティを設定します。物理インターフェイスを仮想ダイヤラ インターフェイスに結び付けるのがダイヤラ プールです。

（注） ATM やイーサネットなど、物理ダイヤラ インターフェイスの他のタイプを定義するには、FlexConfig を使用します。詳細については、FlexConfig ポリシーとポリシー オブジェクトについてを参照してください。

はじめる前に

ルータに仮想および物理ダイヤラ インターフェイスを定義します。Cisco IOS ルータでの基本的なインターフェイス設定 （2 ページ）を参照してください。

（注） また、オプションで仮想および物理ダイヤラ インターフェイスのインターフェイス ロールを定義できます。インターフェイス ロール オブジェクトの作成 を参照してください。

関連項目

- ダイヤラ プロファイルの定義 （36 ページ）
- Cisco IOS ルータ上のダイヤラ インターフェイス （36 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[インタフェース（Interfaces）] > [設定（Settings）] > [ダイヤラ（Dialer）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータインターフェイス（Router Interfaces）] > [設定（Settings）] > [ダイヤラ（Dialer）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Dialer Interfaces] ページが表示されます。このページのフィールドの説明については、表 11 : [Dialer] ページ （40 ページ）を参照してください。

ステップ 2 [ダイヤラ物理インタフェース（Dialer Physical Interfaces）] テーブルから物理 BRI インターフェイスを選択し、[編集（Edit）] をクリックするか、または [追加（Add）] をクリックして物理 BRI インターフェイスを追加します。[Dialer Physical Interface] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、表 13 : [Dialer Physical Interface] ダイアログボックス （43 ページ）を参照してください。

ステップ 3 物理ダイヤラインターフェイスを表すインターフェイスまたはインターフェイスロールの名前を入力します。あるいは [選択（Select）] をクリックしてリストからインターフェイス ロール オブジェクトを選択するか、または新しいインターフェイス ロール オブジェクトを作成します。詳細については、ポリシー定義中のインターフェイスの指定を参照してください。

ステップ 4 物理インターフェイスに関連付けるダイヤラプールの名前を入力するか、または [選択（Select）] をクリックしてセレクタを表示します。複数のエントリを指定する場合は、カンマで区切ります。

ステップ 5 物理インターフェイスで使用する ISDN スイッチ タイプを選択します。 <Table> 使用可能なスイッチタイプについて説明します。

ステップ 6 （任意）スイッチ タイプとして Basic-DMS-100、Basic-NI、または Basic-5ess を選択した場合は、最大 2 つの Service Provider Identifier（SPID; サービス プロバイダー識別子）を入力します。

（注） Basic-5ess スイッチ タイプの場合は、SPID がサポートされていても入力しないことを推奨します。

ステップ 7 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。インターフェイス定義は、[Dialer Interfaces] ページの [Dialer Physical Interfaces] テーブルに表示されます。

[Dialer Policy] ページ

[Dialer] ページは、物理 Basic Rate Interface（BRI; 基本インターフェイス）と仮想ダイヤラ インターフェイスとの関係を定義する場合に使用します。これらのダイヤラインターフェイスは、サイト間 VPN のダイヤル バックアップ機能を設定したときに使用します。

詳細については、Cisco IOS ルータ上のダイヤラ インターフェイス （36 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[インタフェース（Interfaces）] > [設定（Settings）] > [ダイヤラ（Dialer）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータインターフェイス（Router Interfaces）] > [設定（Settings）] > [ダイヤラ（Dialer）]** を選択します。[ダイヤラ（Dialer）] を右クリックしてポリシーを作成するか、または共有ポリシー セレクタから既存のポリシーを選択します。

関連項目

- ダイヤル バックアップの設定
- テーブル カラムおよびカラム見出しの機能
- テーブルのフィルタリング

フィールド リファレンス

表 11 : [Dialer] ページ

要素	説明
Dialer Profiles table	ダイヤラ プールを定義するダイヤラ プロファイル。物理 BRI インターフェイスを追加する場合は、事前にプロファイルを追加する必要があります。テーブルには、ダイヤラ インターフェイスが使用するインターフェイスまたはインターフェイス ロールの名前、プロファイル名、プール、グループ、どのトラフィックがこのプロファイルを使用できるかを定義する ACL、ダイヤル文字列、およびアイドル時間が表示されます。 • プロファイルを追加するには、[行の追加（Add Row）] ボタンをクリックし、[Dialer Profile] ダイアログボックス （41 ページ）に入力します。 • プロファイルを編集するには、プロファイルを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • プロファイルを削除するには、プロファイルを選択し、[行の削除（Delete Row）] ボタンをクリックします。

要素	説明
Dialer Physical Interfaces (BRI) table	ダイヤラ プロファイルを使用する物理インターフェイス。テーブルには、インターフェイスまたはインターフェイス ロールの名前、ダイヤル プール、ISDN スイッチ タイプ、およびインターフェイスに関連する 1 つめおよび 2 つめの Service Provider Identifier（SPID; サービス プロバイダー識別子）が表示されます。 • インターフェイスを追加するには、[行の追加（Add Row）] ボタンをクリックし、[Dialer Physical Interface] ダイアログボックス （42 ページ）に入力します。 • インターフェイスを編集するには、インターフェイスを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • インターフェイスを削除するには、インターフェイスを選択し、[行を削除（Delete Row）] ボタンをクリックします。

[Dialer Profile] ダイアログボックス

[Dialer Profile] ダイアログボックスは、ダイヤラ プロファイルを追加または編集する場合に使用します。

ナビゲーション パス

[Dialer Policy] ページ （40 ページ）に移動してから、[ダイヤラプロファイル（Dialer Profile）] テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- [Dialer Physical Interface] ダイアログボックス （42 ページ）
- ダイヤラ プロファイルの定義 （36 ページ）
- Cisco IOS ルータ上のダイヤラ インターフェイス （36 ページ）
- Cisco IOS ルータでの基本的なインターフェイス設定 （2 ページ）
- インターフェイス ロール オブジェクトの作成

フィールド リファレンス

表 *12 : [Dialer Profile]* ダイアログボックス

要素	説明
名前	ダイヤラ プロファイルのわかりやすい名前。名前を付けると、適切なダイヤラプールを物理インターフェイスに割り当てることができます。プロファイル名は、このダイヤラ インターフェイスがバックアップとして機能するサイトへの参照として使用することもできます。
インターフェイス	ダイヤラ プロファイルに関連付ける仮想ダイヤラ インターフェイス。インターフェイスまたはインターフェイスロールの名前を入力するか、[選択（Select）] をクリックしてインターフェイスまたはインターフェイスロールを選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。
Pool ID	ダイヤラ プール ID。各プールは複数の物理インターフェイスを含めることができ、複数のダイヤラ インターフェイスに関連付けることができます。ただし、各ダイヤラインターフェイスは、1つのプールにだけ関連付けられます。
グループ	このダイヤラ インターフェイスが使用するダイヤラ グループを識別するグループ ID。
Interesting Traffic ACL	どのパケットにこのダイヤラ プロファイルを使用したコールの開始を許可するかを定義する拡張番号付き ACL。有効な ACL 番号は 100 ～ 199 です。 ACL オブジェクトの名前を入力するか、[選択（Select）] をクリックして選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。
Dialer String (Remote Phone Number)	ダイヤラが問い合わせる宛先の電話番号。
アイドル タイムアウト	デフォルトのアイドル時間。この時間を過ぎると、非コンテンション方式の回線が切断されます。デフォルトは 120 秒です。
Fast Idle Timeout	デフォルトのアイドル時間。この時間を過ぎると、コンテンション方式の回線が切断されます。デフォルトは 20 秒です。 別のパケットを異なる宛先に送信するためにビジー状態の回線が要求されると、回線コンテンションが発生します。

[Dialer Physical Interface] ダイアログボックス

[Dialer Physical Interface] ダイアログボックスは、物理 BRI インターフェイスをダイヤラ インターフェイスに関連付けるプロパティを追加または編集する場合に使用します。

（注） ATM やイーサネットなど、物理ダイヤラ インターフェイスの他のタイプを定義するには、FlexConfig を使用します。詳細については、FlexConfig ポリシーとポリシー オブジェクトについてを参照してください。

ナビゲーション パス

[Dialer Policy] ページ （40 ページ）に移動してから、[ダイヤラの物理インターフェイス（Dialer Physical Interfaces）] テーブルの下にある [追加（Add）] ボタンまたは [編集（Edit）] ボタンをクリックします。

関連項目

- [Dialer Profile] ダイアログボックス （41 ページ）
- BRI インターフェイス プロパティの定義 （38 ページ）
- Cisco IOS ルータ上のダイヤラ インターフェイス （36 ページ）
- Cisco IOS ルータでの基本的なインターフェイス設定 （2 ページ）
- インターフェイス ロール オブジェクトについて

フィールド リファレンス

表 *13 : [Dialer Physical Interface]* ダイアログボックス

要素	説明
ISDN BRI	ダイヤラ インターフェイスに関連付けられた物理 BRI インターフェイス。インターフェイスまたはインターフェイス ロール オブジェクトの名前を入力するか、[選択（Select）] をクリックしてインターフェイスまたはインターフェイス ロールを選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。
プール	ダイヤラ プールを物理インターフェイスに関連付けます。1 つ以上のプールの名前を（[Dialer Profile] ダイアログボックス （41 ページ）で定義されているように）入力するか、または[選択（Select）]をクリックしてセレクタを表示します。複数のエントリを指定する場合は、カンマで区切ります。

要素	説明
スイッチ タイプ	ISDN スイッチ タイプ。 北米の場合、オプションは次のとおりです。 • [basic-5ess]：Lucent（AT&T）基本速度 5ESS スイッチ • [basic-dms100]：Northern Telecom DMS-100 基本速度スイッチ • [basic-ni]：National ISDN スイッチ オーストラリア、ヨーロッパ、およびイギリスの場合、オプションは次のとおりです。 • [basic-1tr6]：ドイツ 1TR6 ISDN スイッチ • [basic-net3]：ノルウェー NET3、オーストラリア NET3、ニュージーランド NET3 の各スイッチ タイプの NET3 ISDN BRI。Euro-ISDN E-DSS1 シグナリング システムの ETSI 準拠のスイッチ タイプ • [vn3]：フランス VN3 スイッチおよび VN4 ISDN BRI スイッチ 日本の場合、オプションは次のとおりです。 • [ntt]：日本 NTT ISDN スイッチ 音声/PBX システムの場合、オプションは次のとおりです。 • [basic-qsig]：Q.931 準拠の QSIG シグナリングを搭載した PINX（PBX）スイッチ
SPID1	スイッチ タイプとして Basic-DMS-100、Basic-NI、Basic-5ess のいずれかを選択したときにだけ適用されます。 インターフェイスがサブスクライブする ISDN サービスの Service Provider Identifier（SPID; サービス プロバイダー識別子）。北米のサービス プロバイダーによっては、ISDN サービスを初めてサブスクライブしたときに、SPID が ISDN デバイスに割り当てられることがあります。SPID を必要とするサービス プロバイダーを使用している場合、ISDN デバイスはスイッチにアクセスして接続を初期化するときに、有効な割り当て済み SPID をサービス プロバイダーに送信するまで、コールを発信または受信できません。 有効な SPID は、スペースや特殊文字を含めて最大 20 文字です。 （注） AT&T 5ESS スイッチ タイプを使用するインターフェイスの場合、サポートされていても、SPID は入力しないことを推奨します。

要素	説明
SPID2	スイッチ タイプとして DMS-100 または NI を選択したときにだけ適用されます。 インターフェイスがサブスクライブする 2 つめの ISDN サービスの Service Provider Identifier（SPID; サービス プロバイダー識別子）。有効な SPID には、最大 20 文字の英数字を含めることができます（スペースは含めることができません）。

Cisco IOS ルータでの ADSL

Digital Subscriber Line（DSL; デジタル加入者線）は、既存のツイストペア銅線上でデータを転送するテクノロジーのファミリです。DSL では、POTS（単純な旧式の電話サービス）で使用される上位リストを超える周波数を使用して、電話会社の交換局をカスタマーサイトに接続するローカルループ（またはラストマイル）上でマルチメディアやビデオなどのブロードバンド アプリケーションを配信します。

Asymmetric Digital Subscriber Line（ADSL; 非対称デジタル加入者線）は、DSL の一形態で、カスタマー サイトへのデータ フロー ダウンストリームの方が、Central Office（CO; 交換局）へのデータ フロー アップストリームよりもはるかに大きくなっています。この非対称設定は、Web サーフィン、ビデオオンデマンド、リモート LAN アクセスなど、ダウンロードするときの方が送信するときよりも情報量が多い用途に適しています。ADSL の接続速度は、カスタマー サイトと、複数のカスタマー サイトの接続を 1 つの高速回線に集約する Digital Subscriber Line-Access Multiplexer（DSLAM; デジタル加入者線アクセス マルチプレクサ）との距離に関係があります。

ADSL のダウンストリームの帯域幅は 1.5 ～ 9 Mbps であり、アップストリームの帯域幅は 16 ～ 640 kbps です。ADSL では、単一の銅ツイスト ペアで最大 18,000 フィート（5,488 m）まで正常に伝送できます。ADSL2 や ADSL2+ など最新の ADSL テクノロジーでは、短距離でのデータ レートを高めるだけでなく、電源管理およびリアルタイム パフォーマンス モニタリングを実現しています。

ATM は、小さな固定長のセル サイズであることから数多くの ADSL 実装に使用されており、音声やビデオなど時間が重要となるトラフィックを、他のトラフィックとともに伝送するのに適しています。Security Manager では、Cisco IOS ルータに ATM over DSL を設定できます。Security Manager で ADSL ポリシーを設定する方法の詳細については、ADSL 設定の定義 （47 ページ）を参照してください。

Security Manager で ADSL を設定するには、次の手順を実行する必要があります。

1. ATM インターフェイスまたはサブインターフェイスを設定します。基本的なルータ インターフェイス設定の定義 （5 ページ）を参照してください。
2. ATM インターフェイスまたはサブインターフェイスに ADSL 設定を設定します。ADSL 設定の定義 （47 ページ）を参照してください。
3. ATM インターフェイスまたはサブインターフェイスに PVC を設定します。ATM PVC の定義 （67 ページ）を参照してください。

（注） デバイスで検出を実行した場合は、Security Manager が [Interfaces] ポリシーに ATM インターフェイスおよびサブインターフェイスを入力し、[ADSL] ポリシーにそのインターフェイスの ADSL 設定を入力します。検出された PVC は PVC ポリシーに追加されます。

関連項目

- サポートされる ADSL 動作モード （46 ページ）

サポートされる ADSL 動作モード

表 14 : ADSL カードとサポートされている DSL 動作モード （46 ページ）では、Security Manager で設定できる各 ADSL インターフェイス カードでどのような動作モードがサポートされているかを説明します。

表 *14 : ADSL* カードとサポートされている *DSL* 動作モード

ADSL インターフェイス カード	サポートされる DSL 動作モード
WIC-1ADSL	auto、ansi-dmt、itu-dmt、splitterless
WIC-1ADSL-I-DG	auto、etsi、itu-dmt
WIC-1ADSL-DG	auto、ansi-dmt、itu-dmt、splitterless
HWIC-1ADSL	auto、ansi-dmt、itu-dmt、adsl2、adsl2+
HWIC-1ADSLI	auto、etsi、itu-dmt、adsl2、adsl2+
HWIC-ADSL-B/ST	auto、ansi-dmt、itu-dmt、adsl2、adsl2+
HWIC-ADSLI-B/ST	auto、etsi、itu-dmt、adsl2、adsl2+

表 15 : 固定 ADSL デバイスとサポートされている DSL 動作モード （46 ページ）では、Security Manager で設定できる各 ADSL デバイスでどのような動作モードがサポートされているかを説明します。

表 *15 :* 固定 *ADSL* デバイスとサポートされている *DSL* 動作モード

デバイス	サポートされる DSL 動作モード
857 サービス統合型ルータ	auto、ansi-dmt、itu-dmt、adsl2、adsl2+
876 サービス統合型ルータ	auto、etsi、itu-dmt、adsl2、adsl2+
877 サービス統合型ルータ	auto、ansi-dmt、itu-dmt、adsl2、adsl2+
1801 サービス統合型ルータ	auto、ansi-dmt、itu-dmt、adsl2、adsl2+

デバイス	サポートされる DSL 動作モード
1802 サービス統合型ルータ	auto、etsi、itu-dmt、adsl2、adsl2+

関連項目

- ADSL 設定の定義 （47 ページ）
- Cisco IOS ルータでの ADSL （45 ページ）

ADSL 設定の定義

Security Manager で ADSL 定義を設定するときには、ADSL を定義する ATM インターフェイスを選択する必要があります。また、ルータ タイプまたはルータに組み込まれている WAN Interface Card（WIC; WAN インターフェイス カード）のタイプを指定することを強く推奨します。DSL ポリシー定義の有効性は、ハードウェアに大きく依存します。このポリシーで使用されているハードウェアを指定すると、Security Manager では定義した値が正しく検証されるため、展開の失敗を回避できます。

次のパラメータを任意で指定することもできます。

- DSL 動作モード。
- Inverse Multiplexing over ATM（IMA; ATM の逆多重化）を使用している場合に、VC 帯域幅の動的な調整をイネーブルにするかどうか。
- 特定のインターフェイス カードで特定のキャリア トーン セットを使用するかどうか。

モジュラ Cisco IOS ルータに複数のインターフェイス カードが含まれ、それぞれのカードに単一の ATM インターフェイスが含まれることがあります。インターフェイスごとに ADSL 定義を 1 つだけ定義することもできます。

はじめる前に

- デバイスに ADSL ATM インターフェイスが含まれていることを確認します。 Cisco IOS ルータでの基本的なインターフェイス設定 （2 ページ） を参照してください。

関連項目

- サポートされる ADSL 動作モード （46 ページ）
- Cisco IOS ルータでの ADSL （45 ページ）
- Cisco IOS ルータでの PVC （61 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[インターフェイス（Interfaces）] > [設定（Settings）] > [DSL] > [ADSL]** を選択します。

- （ポリシービュー）ポリシータイプセレクタから **[ルータインターフェイス（Router Interfaces）] > [設定（Settings）] > [DSL] > [ADSL]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[ADSL] ページが表示されます。このページのフィールドの説明については、表 16 : [ADSL] ページ （49 ページ）を参照してください。

ステップ 2 テーブルの下にある [追加（Add）] ボタンをクリックして、[ADSL設定（ADSL Settings）] ダイアログボックスを表示します。このダイアログボックスのフィールドの説明については、表 17 : [ADSL Settings] ダイアログボックス （51 ページ）を参照してください。

ステップ 3 [ATMインターフェイス（ATM Interface）] フィールドに、ADSL 設定を定義する ATM インターフェイスまたはインターフェイスロールの名前を入力します。あるいは、[選択（Select）] をクリックしてインターフェイスロールを選択するか、または新規にインターフェイスロールを作成します。詳細については、ポリシー定義中のインターフェイスの指定を参照してください。

（注） 選択するインターフェイスは、デバイスに物理的に存在する必要があります。存在しないと、展開が失敗します。

ステップ 4 （任意）ルータに組み込まれているインターフェイス カードのタイプを選択します。

（注） ライブ デバイスから検出したときは、正しいインターフェイス カード タイプがすでに表示されています。ライブデバイスで検出を実行しなかった場合、または Cisco Security Manager がデバイスに取り付けられているインターフェイスカードのタイプを検出できない場合、このフィールドに「Unknown」と表示されます。

ステップ 5 （任意）IMA グループを使用している場合は、[ATM PVCで帯域幅変更を許可（Allow bandwidth change on ATM PVCs）] チェックボックスをオンにして、グループ帯域幅の変更に応じて VC 帯域幅が動的に調整されるようにします。このチェックボックスをオフのままにした場合は、このような調整を手動で行う必要があります。

ステップ 6 （任意）この ATM インターフェイスの DSL 動作モードを指定します。各カード タイプでサポートされている動作モードのリストについては、表 14 : ADSL カードとサポートされている DSL 動作モード （46 ページ）を参照してください。

ステップ 7 （任意）インターフェイスカードでキャリアトーン 29 ～ 48 を使用するには、[低トーンセットを使用（Use low tone set）] チェックボックスをオンします。

ステップ 8 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。定義が、[ADSL] テーブルに表示されます。

（注） ADSL 定義を編集するには、テーブルから目的の PVC を選択し、[編集（Edit）] をクリックします。ADSL 定義を削除するには、そのエントリを選択し、[削除（Delete）] をクリックします。

ステップ 9 他の ATM インターフェイスについてもステップ 2 （48 ページ）～ステップ 8 （48 ページ）を繰り返して ADSL 設定を定義します。インターフェイスに定義できる ADSL 定義は 1 つだけです。

[ADSL] ポリシー ページ

[ADSL] ページは、ルータの ATM インターフェイスに関する ADSL 定義を作成、編集、および削除する場合に使用します。詳細については、ADSL 設定の定義 （47 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[インターフェイス（Interfaces）] > [設定（Settings）] > [DSL] > [ADSL]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルーターインターフェイス（Router Interfaces）] > [設定（Settings）] > [DSL] > [ADSL]** を選択します。[ADSL] を右クリックしてポリシーを作成するか、共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- [PVC] ポリシー ページ （71 ページ）
- [SHDSL] ポリシー ページ （55 ページ）
- Cisco IOS ルータでの ADSL （45 ページ）
- テーブル カラムおよびカラム見出しの機能
- テーブルのフィルタリング

フィールド リファレンス

表 16 : [ADSL] ページ

要素	説明
ATM インターフェイス	ADSL 設定が定義されている ATM インターフェイス。
インターフェイス カード	ATM インターフェイスが存在するデバイスまたは ADSL インターフェイス カードのタイプ。
Bandwidth Change	帯域幅全体の変更に応じてルータが VC 帯域幅を動的に調整するかどうかを示します（これは、IMA グループが ATM インターフェイスに設定されているときにだけ重要な意味を持ちます）。
DSL動作モード（DSL Operating Mode）	この ATM インターフェイスの DSL 動作モード。
Tone Low	インターフェイスが低トーン セット（キャリア トーン 29 ～ 48）を使用しているかどうかを示します。

要素	説明
[追加（Add）] ボタン	[ADSL Settings] ダイアログボックス （50 ページ）が開きます。ここから、選択した ATM インターフェイスの ADSL 設定を定義できます。
[編集（Edit）] ボタン	[ADSL Settings] ダイアログボックス （50 ページ）が開きます。ここから、選択した ADSL 定義を編集できます。
[削除（Delete）] ボタン	選択した ADSL 定義をテーブルから削除します。

[ADSL Settings] ダイアログボックス

[ADSL Settings] ダイアログボックスは、選択した ATM インターフェイスの ADSL 設定を設定する場合に使用します。

（注） ADSL 設定を設定した場合は、ATM インターフェイスが定義されているデバイスまたはインターフェイス カードのタイプを選択することを強く推奨します。ADSL 設定は、ハードウェアに大きく依存します。Security Manager でハードウェア タイプを定義すると、設定が適切に検証されるため、デバイスへの展開を正常に完了できます。

ナビゲーション パス

[ADSL] ポリシー ページ （49 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- ADSL 設定の定義 （47 ページ）
- [PVC] ポリシー ページ （71 ページ）

フィールド リファレンス

表 *17 : [ADSL Settings]* ダイアログボックス

要素	説明
ATM インターフェイス	ADSL 設定が定義されている ATM インターフェイス。インターフェイスまたはインターフェイスロールの名前を入力するか、[選択（Select）] をクリックしてインターフェイスまたはインターフェイスロールを選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 （注） インターフェイス ロールを定義するときには、同じインターフェイス カードからの ATM インターフェイスだけを含めることを推奨します。各カード タイプでサポートされている設定が異なると、展開に失敗することがあります。 （注） インターフェイスごとに ADSL 定義を 1 つだけ作成できます。
インターフェイス カード	ルータに組み込まれているデバイスまたはインターフェイス カードのタイプ。 • [blank]：インターフェイス カード タイプは定義されません。 • [WIC-1ADSL]：ADSL over POTS（通常の電話回線）を提供する 1 ポート ADSL WAN インターフェイス カード。 • [WIC-1ADSL-I-DG]：Dying Gasp サポートのある ADSL over ISDN を提供する 1 ポート ADSL WAN インターフェイス カード（Dying Gasp を使用すると、ルータは、ルータの電力が失われかけているときに、差し迫った回線ドロップを DSLAM に警告します）。 • [WIC-1ADSL-DG]：Dying Gasp サポートのある ADSL over POTS を提供する 1 ポート ADSL WAN インターフェイス カード。 • [HWIC-1ADSL]：ADSL over POTS を提供する 1 ポート高速 ADSL WAN インターフェイス カード。 • [HWIC-1ADSLI]：ADSL over ISDN を提供する 1 ポート高速 ADSL WAN インターフェイス カード。 • [HWIC-ADSL-B/ST]：バックアップのために ISDN BRI ポートに ADSL over POTS を提供する 2 ポート高速 ADSL WAN インターフェイス カード。 • [HWIC-ADSLI-B/ST]：バックアップのために ISDN BRI ポートに ADSL over ISDN を提供する 2 ポート高速 ADSL WAN インターフェイス カード。

要素	説明
Interface Card（続き）	• [857 ADSL]：ADSL インターフェイスがある Cisco 857 サービス統合型ルータ。 • [876 ADSL]：ADSL インターフェイスがある Cisco 876 サービス統合型ルータ。 • [877 ADSL]：ADSL インターフェイスがある Cisco 877 サービス統合型ルータ。 • [1801 ADSLoPOTS]：ADSL over POTS を提供する Cisco 1801 サービス統合型ルータ。 • [1802 ADSLoISDN]：ADSL over ISDN を提供する Cisco 1802 サービス統合型ルータ。 （注） ライブデバイスから検出したときは、正しいインターフェイスカードタイプがすでに表示されています。ライブデバイスで検出を実行しなかった場合、または Cisco Security Manager がデバイスに取り付けられているインターフェイスカードのタイプを検出できない場合、このフィールドに「Unknown」と表示されます。
Allow bandwidth change on ATM PVCs	選択されている場合、ATM インターフェイスに定義されている Inverse Multiplexing over ATM（IMA; ATM の逆多重化）グループの帯域幅全体の変更に応じて、ルータは VC 帯域幅を動的に調整します。 選択解除されている場合、IMA グループの個々の物理リンクがアップまたはダウンするたびに、PVC 帯域幅を（CLI を使用して）手動で調整する必要があります。
DSL動作モード（DSL Operating Mode）	この ADSL 回線に設定された動作モード。 • [auto]：Central Office（CO; 交換局）にある DSLAM とのオートネゴシエーションを実施します。これがデフォルトです。 • [ansi-dmt]：回線は、ANSI T1.413 Issue 2 モードでトレインします。 • [itu-dmt]：回線は、G.992.1 モードでトレインします。 • [splitterless]：回線は、G.992.2（G.Lite）モードでトレインします。 • [etsi]：回線は、European Telecommunications Standards Institute（ETSI）モードでトレインします。 • [adsl2]：回線は、G.992.3（adsl2）モードでトレインします。 • [adsl2+]：回線は、G.992.5（adsl2+）モードでトレインします。 （注） 各カードタイプでサポートされている動作モードについては、表 14 : ADSL カードとサポートされている DSL 動作モード （46 ページ）を参照してください。

要素	説明
Use low tone set	選択されている場合、インターフェイス カードはキャリア トーン 29 ～ 48 を使用します。 選択解除されている場合、インターフェイス カードはキャリア トーン 33 ～ 56 を使用します。 （注） Deutsche Telekom 仕様 U-R2 に従ってインターフェイス カードが動作しているときには、このオプションを選択しないでください。

Cisco IOS ルータでの SHDSL

Digital Subscriber Line（DSL; デジタル加入者線）は、既存のツイストペア銅線上でデータを転送するテクノロジーのファミリです。DSL では、POTS（単純な旧式の電話サービス）で使用される上位リストを超える周波数を使用して、電話会社の交換局をカスタマーサイトに接続するローカルループ（またはラストマイル）上でマルチメディアやビデオなどのブロードバンド アプリケーションを配信します。

Symmetric High-Speed Digital Subscriber Line（SHDSL; 対称高速デジタル加入者線）は、International Telecommunications Union（ITU; 国際電気通信連合）G.991.2 グローバル業界標準に基づいて、単一のワイヤ ペアで 192 kbps ～ 2.3 Mbps までの対称データ レートを実現します。T1、E1、ISDN、ATM、IP など多くの信号タイプを転送します。また、G.SHDSL 信号は、交換局からの到達距離が ADSL 接続および独自の SDSL 接続よりも長くなっています。

Security Manager で SHDSL を設定するには、次の手順を実行します。

1. SHDSL コントローラを設定します。SHDSL コントローラの定義 （54 ページ）を参照してください。
2. SHDSL ポリシーを展開します。ATM モードがアクティブである場合は、ルータは展開時にコントローラに対応する ATM インターフェイスを作成します。展開および Configuration Archive の使用を参照してください。
3. デバイスを再検出して、その新規 ATM インターフェイスを Security Manager に追加します。Security Manager にすでに存在するデバイス上のポリシーの検出を参照してください。
4. （任意）ATM インターフェイスに 1 つ以上のサブインターフェイスを作成します。基本的なルータ インターフェイス設定の定義 （5 ページ）を参照してください。
5. ATM インターフェイスまたはサブインターフェイスに PVC を設定します。ATM PVC の定義 （67 ページ）を参照してください。

（注） デバイスで検出を実行した場合、Security Manager は [SHDSL] ポリシーにコントローラの定義を読み込み、[Interfaces] ポリシーに ATM インターフェイスおよびサブインターフェイスを読み込みます。検出された PVC は PVC ポリシーに追加されます。

関連項目

- Cisco IOS ルータでの PVC （61 ページ）

SHDSL コントローラの定義

Security Manager で SHDSL コントローラを設定した場合、Cisco IOS ルータにインストールされているコントローラの名前を入力する必要があります。名前を入力すると、次の設定が自動的に適用されます。

- ATM モードがイネーブルになります。
- 回線終端が、Customer Premises Equipment（CPE; 宅内装置）に設定されます。
- 回線モードが、Auto に設定されます。

任意で回線終端を CO に変更し、DSL モードおよび回線モードを指定できます。また、信号対雑音比マージンを定義して、回線の安定性を高めることができます。

1 台の Cisco IOS ルータに、複数の SHDSL コントローラを含めることができます。その場合、SHDSL 定義はコントローラごとに 1 つだけ定義できます。

（注） ATM モードをイネーブルにして SHDSL ポリシーを展開すると、ルータに ATM インターフェイスが自動的に作成されます。再検出を実行して、インターフェイスを Security Manager に追加します。次に、必要に応じて ATM インターフェイスに PVC を定義できます。 ATM PVC の定義 （67 ページ）を参照してください。

はじめる前に

- SHDSL コントローラがデバイスにインストールされていることを確認します。

関連項目

- Cisco IOS ルータでの SHDSL （53 ページ）
- Cisco IOS ルータでの PVC （61 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[インターフェイス（Interfaces）] > [設定（Settings）] > [DSL] > [SHDSL]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータインターフェイス（Router Interfaces）] > [設定（Settings）] > [DSL] > [SHDSL]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[SHDSL] ページが表示されます。このページのフィールドの説明については、[SHDSL] ポリシー ページ（55 ページ）を参照してください。

ステップ 2 テーブルの下にある [追加（Add）] ボタンをクリックして、[SHDSL] ダイアログボックスを表示します。

ステップ 3 コントローラの名前を入力します。または[選択（Select）] をクリックしてコントローラ名を生成するためのユーティリティを表示します。[Controller Auto Name Generator] ダイアログボックス （60 ページ）を参照してください。

（注） 選択するコントローラは、デバイスに物理的に存在する必要があります。存在しないと、展開が失敗します。

ステップ 4 必要に応じて SHDSL コントローラを定義します。詳細については、表 19 : [SHDSL] ダイアログボックス（57 ページ）を参照してください。

ステップ 5 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。定義が、[SHDSL] テーブルに表示されます。

（注） SHDSL コントローラを編集するには、編集するコントローラをテーブルから選択し、[編集（Edit）] をクリックします。SHDSL コントローラを削除するには、削除するコントローラを選択し、[削除（Delete）] をクリックします。

ステップ 6 ステップ 2 （55 ページ）～ステップ 5 （55 ページ）を繰り返して、他の SHDSL コントローラを定義します。定義は、コントローラごとに 1 つだけ定義できます。

[SHDSL] ポリシー ページ

[SHDSL] ページは、ルータで DSL コントローラ定義を作成、編集、および削除する場合に使用します。詳細については、SHDSL コントローラの定義 （54 ページ）を参照してください。

ナビゲーション パス

- （デバイス ビュー）ポリシーセレクタから [インターフェイス（Interfaces）] > [設定（Settings）] > [DSL] > [SHDSL] を選択します。
- （ポリシー ビュー）ポリシータイプセレクタから [ルータインターフェイス（Router Interfaces）] > [設定（Settings）] > [DSL] > [SHDSL] を選択します。[SHDSL] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- [PVC] ポリシー ページ （71 ページ）
- [ADSL] ポリシー ページ （49 ページ）
- Cisco IOS ルータでの SHDSL （53 ページ）
- テーブル カラムおよびカラム見出しの機能

- テーブルのフィルタリング

フィールド リファレンス

表 *18 : [SHDSL]* ページ

要素	説明
名前	DSL コントローラの名前。
説明	（任意）コントローラの説明。
シャットダウン	DSL コントローラがシャットダウン モードであるかどうかを示します。
Configure ATM Mode	DSL コントローラが ATM モードに設定されているかどうかを示します。
Line Termination	ルータに設定されている回線終端（CPE または CO）。
DSL Mode	DSL コントローラに対して定義されている動作モード。
[回線モード（Line Mode）]	DSL コントローラに対して定義されている回線モード。
Line Rate	DSL コントローラに対して定義されている回線レート（kbps 単位）。 （注） 回線モードが Auto に設定されている場合にだけ、値がこの列に表示されます。
SNR Margin Current	コントローラの現在の信号対雑音比。
SNR Margin Snext	コントローラの Self Near-End Crosstalk（Snext; セルフ近端クロストーク）信号対雑音比。
[追加（Add）] ボタン	[SHDSL Controller] ダイアログボックス （56 ページ）が開きます。ここから、DSL コントローラの設定を定義できます。
[編集（Edit）] ボタン	[SHDSL Controller] ダイアログボックス （56 ページ）が開きます。ここから、選択した DSL コントローラ定義を編集できます。
[削除（Delete）] ボタン	選択した DSL コントローラ定義をテーブルから削除します。

[SHDSL Controller] ダイアログボックス

[SHDSL Controller] ダイアログボックスは、SHDSL コントローラを設定する場合に使用します。

ナビゲーション パス

[SHDSL] ポリシー ページ （55 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- SHDSL コントローラの定義 （54 ページ）
- [PVC] ポリシー ページ （71 ページ）
- Security Manager にすでに存在するデバイス上のポリシーの検出

フィールド リファレンス

表 *19 : [SHDSL]* ダイアログボックス

要素	説明
名前	コントローラの名前。名前を手動で入力するか、または[選択（Select）]をクリックして名前を生成するためのダイアログボックスを表示します。[Controller Auto Name Generator] ダイアログボックス （60 ページ）を参照してください。
説明	コントローラに関する追加の情報（最大 80 文字）。
シャットダウン	選択されている場合、DSL コントローラがシャットダウン状態になります。ただし、その定義は削除されません。 選択解除されている場合、DSL コントローラがイネーブルになります。これがデフォルトです。
Configure ATM mode	選択されている場合、コントローラを ATM モードに設定し、コントローラと同じ ID で ATM インターフェイスを作成します。これがデフォルトです。ATM モードをイネーブルにし、再検出を実行してデバイスに ATM または PVC を設定する必要があります。 選択解除されている場合、ATM モードがディセーブルになります。展開時に ATM インターフェイスが作成されません。 （注） いったん Security Manager に保存された ATM モードは、コントローラから削除できません。
Line Termination	ルータに設定されている回線終端。 • [CPE]：宅内装置。これがデフォルトです。 • [CO]：交換局。

要素	説明
DSL Mode	地域の動作パラメータなど、コントローラで使用されている DSL 動作モード。 • [blank]：動作モードは定義されません（展開時には、北米の Annex A 規格が使用されます）。 • A：北米の G.991.2 規格の Annex A をサポートします。 • AB：Annex A または Annex B をサポートします。Line Term が CPE に設定されている場合にのみ使用できます。回線トレイン時に適切なモードが選択されます。 • A-B-ANFP：Annex A または Annex B-ANFP をサポートします。[Line Term] が [CPE] に設定されている場合にだけ使用可能です。回線トレイン時に適切なモードが選択されます。 • B：ヨーロッパの G.991.2 規格の Annex B をサポートします。 • B-ANFP：Annex B-Access Network Frequency Plan（ANFP）をサポートします。 （注） 使用可能な DSL モードは、選択した回線終端によって異なります。
回線モード設定	
[回線モード（Line Mode）]	コントローラで使用されている回線モード。 • [Auto]：コントローラは、他の回線終端と同じモードで動作します（2 線式回線 0、2 線式回線 1、または 4 線式拡張）。これは CPE 回線終端のデフォルトです。 • [2-wire]：コントローラは、2 線式モードで動作します。これは CO 回線終端のデフォルトです。 • [4-wire]：コントローラは、4 線式モードで動作します。 （注） コントローラを CPE として設定したときにだけ、[Auto] を選択できます。
回線（Line）	[Line Mode] が [2-wire] に定義されているときにだけ適用されます。 使用するワイヤのペアは次のとおりです。 • [line-zero]：RJ-11 PIN 1 および PIN 2。これは CO 回線終端のデフォルトです。 • [line-one]：RJ-11 PIN 3 および PIN 4。

要素	説明
Exchange Handshake	回線モードが [4-wire] に定義されているときにだけ適用されます。 使用するハンドシェイク モードのタイプは次のとおりです。 • [blank]：ハンドシェイク モードは指定されません（展開時には、[拡張（enhanced）] オプションが使用されます）。これがデフォルトです。 • [enhanced]：両方のワイヤ ペアでハンドシェイク ステータスを交換します。 • [標準（standard）]：メインワイヤペアでのみハンドシェイクステータスを交換します。
Line Rate	[Line Mode] が [Auto] に定義されているときには適用されません。 SHDSL ポートが対応する DSL 回線レート（kbps 単位）。 • [auto]：コントローラは、回線レートを選択します。2 線式モードでだけ使用可能です。 • サポートされている回線レートは次のとおりです。 • 2 線式モードの場合：192、256、320、384、448、512、576、640、704、768、832、896、960、1024、1088、1152、1216、1280、1344、1408、1472、1536、1600、1664、1728、1792、1856、1920、1984、2048、2112、2176、2240、および 2304。 • 4 線式モードの場合：384、512、640、768、896、1024、1152、1280、1408、1536、1664、1792、1920、2048、2176、2304、2432、2560、2688、2816、2944、3072、3200、3328、3456、3584、3712、3840、3968、4096、4224、4352、4480、および 4608。 （注） サードパーティ機器によっては、2 線式モードで 8 kbps、4 線式モードで 16 kbps の SHDSL オーバーヘッドを考慮に入れた回線レートを使用できるものもあります。
SNR Margin の設定	
現在（Current）	コントローラの現在の Signal-To-Noise（SNR; 信号対雑音）比をデシベル単位（dB）で表した値。有効値の範囲は -10 ～ 10 dB です。 このオプションを選択すると、トレイン時に回線トレインが現在の雑音マージンに SNR 比しきい値を加えた値を上回るため、回線の安定性を高めることができます。設定された SNR マージンよりも外部のノイズが低いと、回線は安定します。 （注） 現在の SNR を無効にするには、[無効（disable）] を選択します。

要素	説明
Snext	コントローラの Self Near-End Crosstalk（Snext; セルフ近端クロストーク）信号対雑音比をデシベル単位で表した値。有効値の範囲は -10 ～ 10 dB です。 このオプションを選択すると、トレイン時に回線トレインが SNEXT しきい値を上回るため、回線の安定性を高めることができます。設定された SNEXT マージンよりも外部のノイズが低いと、回線は安定します。 （注） SNEXT SNR を無効にするには、[無効（disable）] を選択します。

[Controller Auto Name Generator] ダイアログボックス

[Controller Auto Name Generator] ダイアログボックスは、ルータ内での DSL コントローラの場所に基づいて DSL コントローラの名前を Security Manager で自動的に生成する場合に使用します。

ナビゲーション パス

[SHDSL Controller] ダイアログボックス （56 ページ）に移動し、[名前（Name）] フィールドの [選択（Select）] をクリックします。

関連項目

- SHDSL コントローラの定義 （54 ページ）
- [SHDSL] ポリシー ページ （55 ページ）
- [PVC] ポリシー ページ （71 ページ）

フィールド リファレンス

表 *20 : [Controller Auto Name Generator]* ダイアログボックス

要素	説明
タイプ	インターフェイスのタイプ。このフィールドにはDSL という値が表示され、読み取り専用となります。
カード	コントローラに関連するカード。
スロット	コントローラに関連するスロット。
[ポート（Port）]	コントローラに関連するポート。 （注） これらのフィールドに入力した情報によって、[Result] フィールドに表示される、生成される名前の残りの部分が形成されます。

要素	説明
結果	コントローラの場所に入力した情報を基に Security Manager が生成した名前。このフィールドに表示される名前は読み取り専用です。 **ヒント** このダイアログボックスを閉じたあと、必要に応じて [SHDSL] ダイアログボックスで生成した名前を編集できます。

Cisco IOS ルータでの PVC

非同期転送モード（ATM）は、セルリレー技術を使用したパブリック ネットワークおよびプライベート ネットワークで音声、ビデオ、およびデータを高速転送するために定められた International Telecommunication Union（ITU-T; 国際電気通信連合）規格です。ATM はセルの交換と多重化の技術により、回線交換の利点（一定した伝搬遅延、容量保証）とパケット交換の利点（断続的なトラフィックへの柔軟かつ効率的な対応）とを兼ね備えたものとなっています。ATM ネットワークは、Cisco IOS ルータなど、1 つ以上の ATM スイッチと ATM エンドポイントで構成されます。

ATM サービスには一般に 3 つのタイプがあります。Permanent Virtual Connection（PVC; 相手先固定接続）、Switched Virtual Connection（SVC; 相手先選択接続）、およびコネクションレス型サービスです。PVC では、リース回線に似たサービスを提供するためにサイト間に直接および永続的な接続を確立できます。PVC の利点は、接続の可用性が保証されていることと、スイッチ間でコール確立手順が不要であることです。発信元から宛先までの間にある各機器は、PVC に対応するように手動でプロビジョニングする必要があります。

ATM PVC の詳細については、次の項目を参照してください。

- 仮想パスおよび仮想チャネルについて （62 ページ）
- ATM サービス クラスについて （63 ページ）
- ATM 管理プロトコルについて （64 ページ）

Security Manager での PVC の定義の詳細については、次の項目を参照してください。

- ATM PVC の定義 （67 ページ）
- Cisco IOS ルータでの SHDSL （53 ページ）

関連項目

- Cisco IOS ルータでの ADSL （45 ページ）
- Cisco IOS ルータでの SHDSL （53 ページ）

仮想パスおよび仮想チャネルについて

ATM ネットワークは、基本的にはコネクション型です。つまり、データ転送を開始する前に ATM ネットワークに仮想接続を確立する必要があります。ATM 接続には、2 つのタイプがあります。

- Virtual Path Connection（VPC; 仮想パス接続）。Virtual Path Identifier（VPI; 仮想パス識別子）で識別されます。
- Virtual Channel Connection（VCC; 仮想チャネル接続）。VPI と Virtual Channel Identifier（VCI; 仮想チャネル識別子）の組み合わせで識別されます。PVC は、2 つのサイト間に永続的な接続が定義されているタイプの VCC です。

図 2 : ATM 仮想パスおよび仮想チャネル接続 （62 ページ）に示すように、仮想パスは仮想チャネルをいくつかバンドルしたもので、いずれのチャネルも共通の VPI に基づいて ATM ネットワークで透過的にスイッチングされます。VPC は、VPI 値が同じ VCC をいくつかバンドルしたものであると考えることができます。

図 *2 : ATM* 仮想パスおよび仮想チャネル接続

どのセル ヘッダーにも VPI フィールドおよび VCI フィールドが含まれており、両フィールドともセルを物理リンク上の特定の仮想チャネルに明示的に関連付ける働きをします。VPI および VCI については次の属性に留意することが重要です。

- VPI および VCI は、LAN スイッチングで使用される MAC アドレスのようなアドレスではありません。
- VPI および VCI は接続の各セグメントで明示的に割り当てられるため、有効範囲が特定のリンクにローカルになります。各スイッチング ポイントで必要に応じて再マッピングされます。

ATM レイヤで VPI/VCI 識別子を使用すると、セルの多重化（インターリーブ）や逆多重化を行ったり、複数の接続からセルを切り替えることができます。VPI/VCI 識別子によっては、Integrated Local Management Interface（ILMI; 統合ローカル管理インターフェイス）など、特定の用途に予約されているものもあります。

関連項目

- ATM サービス クラスについて （63 ページ）
- ATM 管理プロトコルについて （64 ページ）
- ATM PVC の定義 （67 ページ）
- Cisco IOS ルータでの PVC （61 ページ）

ATM サービス クラスについて

ATM フォーラムが公表したトラフィック管理仕様のバージョン 4.0 には、サービス クラスが 5 つ定義されています。各クラスには、ネットワークで送信されるユーザ トラフィックと、ネットワークがそのトラフィックで実現する必要があるサービスの品質が記述されています。Security Manager は、次の ATM サービス クラスをサポートします。

- 使用可能ビットレート（ABR、Available Bit Rate ）：ATM スイッチがセル配信を保証せず、最小ビットレートを保証し、フィードバックメカニズムを使用してセル損失をできるかぎり抑えるサービスクラス。ABR サービス カテゴリは、ファイル転送をはじめ、最小限の帯域幅を必要とするバーストで非リアルタイムなトラフィックを伝送する VC 向けに設計されています。この帯域幅は、VC が設定されてアクティブである場合に確保する必要がある最小セル レートで指定されます。詳細については、次の URL にある「Understanding the Available Bit Rate (ABR) Service Category for ATM VCs」を参照してください。
http://www.cisco.com/en/US/tech/tk39/tk51/technologies_tech_note09186a00800fbc76.shtm

- 固定ビットレート（CBR、Constant Bit Rate）：音声およびビデオの QoS ニーズを満たすように、セルが連続ビットストリームで送信されるサービスクラス。CBR サービス クラスは、接続がアクティブである間、固定量の帯域幅を継続して使用できることが求められる ATM 仮想回線（VC）向けに設計されています。CBR として設定された ATM VC は、Peak Cell Rate（PCR; ピーク セル レート）でいつでも好きな期間だけセルを送信できます。また、PCR を下回るレートでセルを送信したり、セルを送信しないようにしたりすることもできます。CBR に関する設定は、プラットフォームによって異なることがあります。詳細については、次の URL にある「Understanding the CBR Service Category for ATM VCs」を参照してください。
http://www.cisco.com/en/US/tech/tk39/tk51/technologies_tech_note09186a0080094e6a.shtml

- 未指定ビットレート（UBR、Unspecified Bit Rate）：ネットワーク管理で Quality of Service（QoS）が保証されないサービスクラス。インターネットが通常提供するベストエフォート型のサービスをモデル化したもので、リアルタイムの応答を必要とせず、遅延が発生しても問題ないアプリケーションに適しています。たとえば、電子メール、FAX 転送、ファイル転送、Telnet、LAN、リモート オフィスの相互接続などです。詳細については、次の URL にある「Understanding the UBR Service Category for ATM Virtual Circuits」を参照してください。
http://www.cisco.com/en/US/tech/tk39/tk51/technologies_tech_note09186a00800a4837.shtml

- 未指定ビットレート（UBR+、Unspecified Bit Rate）：シスコでは、UBR+ という UBR サービスクラスのバリアントを提供しています。UBR+ サービス クラスの主な利点は、ATM エンド システムが接続要求時に ATM スイッチまで最小セル レートを確保し、ATM ネットワークがエンドツーエンド保証としてこの最小セル レートを維持しようとすることです。詳細については、次の URL にある「Understanding the UBR+ Service Category for ATM VCs」を参照してください。
http://www.cisco.com/en/US/tech/tk39/tk51/technologies_tech_note09186a0080094b40.shtml

- 可変ビットレート - 非リアルタイム（VBR-nrt、Variable Bit Rate - Non-Real Time）：このサービスクラスは、バースト性の非リアルタイム アプリケーションを送信する場合に使用します。トラフィック特性は、Peak Cell Rate（PCR; ピーク セル レート）、平均セルレート (Sustained Cell Rate)、および Minimum Burst Size（MBS; 最小バースト サイズ）の観点

から定義されます。詳細については、次の URL にある「Understanding the VBR-nrt Service Category and Traffic Shaping for ATM VCs」を参照してください。
http://www.cisco.com/en/US/tech/tk39/tk51/technologies_tech_note09186a0080102a42.shtml

- 可変ビット レート - リアルタイム（VBR-rt、Variable Bit Rate - Real Time ）：このサービス クラスは、圧縮した Voice over IP やビデオ会議など、時間遅延が重要な要素となるリアルタイムデータを送信する場合に使用します。VBR-nrt と同じく、VBR-rt トラフィックは PCR、SCR、および MBS の観点から定義されます。詳細については、次の URL にある「Understanding the Variable Bit Rate Real Time (VBR-rt) Service Category for ATM VCs」を参照してください。
http://www.cisco.com/en/US/tech/tk39/tk51/technologies_tech_note09186a0080094cd0.shtml

このようなサービス クラスを使用すると、トラフィック シェーピングなど、ATM の Quality of Service（QoS）保証を定義できます。トラフィック シェーピングとは、トラフィック コントラクトによって定義されているエンベロープにトラフィックが収まるように、キューを使用してデータ バーストを抑制し、ピーク データ レートを制限し、ジッタを抑えることです。ATM デバイスは、トラフィック シェーピングを使用して、トラフィック コントラクトの条件に準拠します。

関連項目

- 仮想パスおよび仮想チャネルについて （62 ページ）
- ATM 管理プロトコルについて （64 ページ）
- ATM PVC の定義 （67 ページ）
- Cisco IOS ルータでの PVC （61 ページ）

ATM 管理プロトコルについて

ATM は、2 種類のシグナリングを使用して PVC のステータスを追跡します。

- Integrated Local Management Interface（ILMI; 統合ローカル管理インターフェイス）。詳細については、 ILMI について （65 ページ）を参照してください。
- フロー 4（F4）およびフロー 5（F5）の Operation, Administration, and Maintenance（OAM; 運用管理および保守）セル。詳細については、 OAM について （66 ページ）を参照してください。

Security Manager では、特定の PVC で ILMI をイネーブルまたはディセーブルにし、F5 OAM 機能を設定できます。

関連項目

- 仮想パスおよび仮想チャネルについて （62 ページ）
- ATM サービス クラスについて （63 ページ）

- ATM PVC の定義 （67 ページ）
- ATM PVC での OAM 管理の定義 （69 ページ）
- Cisco IOS ルータでの PVC （61 ページ）

ILMI について

Integrated Local Management Interface（ILMI; 統合ローカル管理インターフェイス）は、ATM インターフェイスで物理層、ATM レイヤ、仮想パス、および仮想回線パラメータを設定およびキャプチャするためのプロトコルとして、ATM フォーラムが定義したものです。ILMI を使用すると、デバイスが物理リンクの反対側にあるコンポーネントのステータスを判断し、動作パラメータの共通セットをネゴシエートして相互運用性を確保できるようになるため、ネットワーク全体での自動設定が容易になります。Private Network to Network Interface（PNNI; プライベート ネットワーク間インターフェイス）と IISP（Interim-Interswitch Signaling Protocol）という ATM ルーティング プロトコルは、この情報を使用して、ATM スイッチ ルータを検出し、それらを相互接続したネットワークを構築します。

2 つの ATM インターフェイスが ILMI プロトコルを実行すると、互いに物理的な接続で ILMI パケットを交換します。このようなパケットは、484 オクテットの大きさの SNMP メッセージで構成されています。ATM インターフェイスは、このようなメッセージを ATM アダプテーション レイヤ 5（AAL5）トレーラにカプセル化し、パケットをセルにセグメント化し、セル伝送をスケジューリングします。ATM インターフェイスは、相手先固定接続（PVC）自動検出などのネットワーク機能で SNMP オブジェクト ID を使用します。特に、Digital Subscriber Line（DSL; デジタル加入者線）アプリケーションで便利です。

ILMI は、管理対象オブジェクトを管理情報ベース（MIB）に編成します。リンク管理用のものなどがあります。この MIB には、各 ATM インターフェイスで使用される次のオブジェクト グループが含まれています。

- 物理層：ILMI 4.0 が、物理層 ILMI 値を中断または「廃止」し、標準のインターフェイス MIB（RFC 1213）を使用することを指定します。
- ATM レイヤ：ATM セル ヘッダーの VPI 値および VCI 値に使用可能なビット数、許可された Virtual Path Connection（VPC; 仮想パス接続）および Virtual Channel Connection（VCC; 仮想チャネル接続）の最大数、設定した PVC の数などを示します。
- 仮想パス接続：VPC のアップ/ダウン ステータスとその Quality of Service（QoS）パラメータを示します。
- 仮想チャネル接続：VCC のアップ/ダウン ステータスとその QoS パラメータを示します。

管理者は任意に ILMI をイネーブルまたはディセーブルにできますが、イネーブルにすることを強く推奨します。ILMI がイネーブルになっていないと、ATM デバイスを正しく動作させるために ILMI が管理するパラメータの多くを手動で設定しなければならなくなります。ILMI は、VPI=X、VCI=16 の予約済み PVC で動作します。

関連項目

- ATM 管理プロトコルについて （64 ページ）
- Cisco IOS ルータでの PVC （61 ページ）

OAM について

Operation, Administration, and Maintenance（OAM; 運用管理および保守）機能は、ATM の障害管理およびパフォーマンス管理を実現するもので、ITU 推奨事項 I.610 に定義されている規格に基づいています。OAM は、PVC でネットワーク接続障害を検出し、問題の PVC を停止することによって障害に対応します。OAM がないと、ネットワーク接続が失われても、PVC はアップのままとなります。そのような状況では、ルーティング テーブル エントリが引き続き PVC を指しているため、パケットが失われます。

Security Manager では、F5 OAM を使用できます。これは、仮想回線（VC）レベルで動作します。OAM は、Cisco IOS ルータなどのエンド デバイスで PVC パスに沿って障害を検出するため、次のセルを使用します。

- ループバック セル：OAM 対応のルータは、通常の間隔でループバック セルを送信します。ループバック セルは、ネットワークでループします。このループ ポイントは、PVC の終端にあるマシン（エンドツーエンド ループバック セル）か、またはパス上にあるデバイス（セグメント ループバック セル）とします。ループバック セルが失敗して発信元に戻ると、障害が発生します。
- Continuity Check（CC; 連続性チェック）セル：CC セルは、OAM 対応のルータによって定期的に送信されて、リンクの整合性がチェックされます。CC セルの送信先は、エンドツーエンドにすることも、PVC の特定のセグメントに限定することもできます。アクティベーション セルおよびディアクティベーション セルは、連続性チェックを開始する場合と、一時停止する場合に使用します。接続障害があれば、特殊な SNMP 通知で報告されます。
- Alarm Indication Signal（AIS; アラーム表示信号）セル：物理層で障害が発生したときには、AIS セルがダウンストリーム デバイスに送信されて、ATM レイヤでの仮想接続障害が報告されます。PVC は、定義した数だけ AIS セルを受信したあとでダウン状態に移行し、AIS セルを追加せずに定義済みの間隔が経過するまでアップしません。
- Remote Detection Indication（RDI; リモート検出表示）セル：ダウンストリーム デバイスに接続障害を警告するために AIS セルが送信されると、ネットワークの制御とフィードバックのメカニズムが働いてアップストリームに RDI セルが送信されます。

障害が解決されるまで、障害の影響を受ける PVC 上のユーザ セルと同じ VPI/VCI を使用して、AIS/RDI セルが送信されます。

関連項目

- ATM 管理プロトコルについて （64 ページ）
- Cisco IOS ルータでの PVC （61 ページ）
- ATM PVC での OAM 管理の定義 （69 ページ）

ATM PVC の定義

ATM 相手先固定接続（PVC）を定義するには、ATM インターフェイスを選択し、次の設定を定義します。

- PVC ID。
- 使用するカプセル化のタイプ。
- この PVC で ILMI 管理がイネーブルになるかどうか。
- Inverse ARP（InARP）を使用して宛先デバイスの IP アドレスを学習するかどうか。
- PPP over Ethernet（PPPoE）および PPP over ATM（PPPoA）に関連するオプション。
- トラフィック シェーピングなどの Quality of Service（QoS）設定。
- InARP の代わりとなるスタティック IP アドレス マッピング。

ループバックや連続性チェックなど、PVC での F5 Operation, Administration, and Maintenance（OAM; 運用管理および保守）管理の定義の詳細については、ATM PVC での OAM 管理の定義 （69 ページ）を参照してください。

はじめる前に

- ATM over DSL を設定する場合は、ADSL ポリシー（Cisco IOS ルータでの ADSL （45 ページ）を参照）または SHDSL ポリシー（Cisco IOS ルータでの SHDSL （53 ページ））をすでに設定していることを確認してください。
- デバイスに ATM インターフェイスおよびサブインターフェイスが含まれていることを確認します（PVC は一般に、ATM サブインターフェイスに設定されます）。Cisco IOS ルータでの基本的なインターフェイス設定 （2 ページ）を参照してください。

（注） ATM を SHDSL 対応に設定した場合、SHDSL コントローラを定義し、ATM モードをイネーブルにすると、ATM インターフェイスが作成されます。その場合、デバイスを再検出して、ATM インターフェイスを Security Manager に追加する必要があります。SHDSL コントローラの定義 （54 ページ） を参照してください。

関連項目

- ATM PVC での OAM 管理の定義 （69 ページ）
- ポリシング パラメータとシェーピング パラメータについて
- Cisco IOS ルータでの PVC （61 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [インターフェイス（Interfaces）] > [設定（Settings）] > [PVC] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータインターフェイス（Router Interfaces）] > [設定（Settings）] > [PVC] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[PVC] ページが表示されます。このページのフィールドの説明については、表 21 : [PVC] ページ （72 ページ）を参照してください。

ステップ 2 テーブルの下にある [追加（Add）] ボタンをクリックして、[PVC] ダイアログボックスを表示します。このダイアログボックスのフィールドの説明については、表 22 : [PVC] ダイアログボックス （74 ページ）を参照してください。

ステップ 3 [インターフェイス（Interface）] フィールドに、PVC を定義する ATM インターフェイス、ATM サブインターフェイス、またはインターフェイスロールの名前を入力します。あるいは、[選択（Select）] をクリックしてインターフェイスロールを選択するか、または新規にインターフェイスロールを作成します。

ステップ 4 ATM インターフェイスが組み込まれているデバイスまたは DSL WAN インターフェイス カードのタイプを選択します。

（注） この設定値を定義して、PVC ポリシーを適切に検証することを強く推奨します。このポリシーの設定は、ハードウェアに強く依存するためです。

ステップ 5 [PVC] ダイアログボックスの [Settings] タブで、PVC の基本的な設定を定義します。

a) VPI/VCI 識別子を入力します。任意でテキスト ハンドルを入力することもできます。管理 PVC を定義している場合は、[管理 PVC（ILMI）（Management PVC (ILMI)）] チェックボックスをオンにします。

（注） 2 人のユーザが同じ識別子で同時に PVC を定義しようとすると、エラーが発生します。

b) 使用する ATM カプセル化のタイプを選択します。aal5autoppp または aal5ciscoppp を選択した場合は、PPPoA に使用する仮想テンプレートを定義するか、または [Select] をクリックしてセレクタを表示する必要があります。カプセル化のタイプとして aal5mux を選択した場合は、PVC によって伝送されるプロトコルを選択する必要があります。

（注） 管理 PVC を定義するときには、カプセル化のタイプを選択しないでください。

（注） 既存の PVC の仮想テンプレート設定を修正する場合は、ATM サブインターフェイスで **shutdown** コマンドに続けて **no shutdown** コマンドを入力して、インターフェイスを再起動する必要があります。これにより、新規に設定したパラメータが有効になります。

c) ILMI でこの PVC を管理するには、[Enable ILMI] チェックボックスをオンにします。詳細については、ILMI について （65 ページ）を参照してください。

（注） サブインターフェイスには、管理 PVC を設定できません。

d) トラフィックをそのようなデバイスに転送するのに必要なレイヤ 3 アドレスを PVC で動的に学習するには、[Inverse ARP] チェックボックスをオンにします。

（注） このほか、ステップ 7 （69 ページ）の説明に従って、スタティック アドレス マッピングを作成する方法もあります。

e) [PPPoE Max Sessions] フィールドに、PVC で許可されている PPPoE セッションの最大数を定義します。

f) [VPN Service Name] フィールドに、PVC での PPPoA セッションに使用するスタティック ドメイン名を定義します。

[設定（Settings）] タブのフィールドの説明については、表 23 : [PVC] ダイアログボックス - [Settings] タブ （75 ページ）を参照してください。

ステップ 6 （任意）[PVC] ダイアログボックスの [QoS] タブで、この PVC によって伝送されるトラフィックで実行する ATM トラフィック シェーピングのタイプを定義します。トラフィック シェーピングは、定義されたビット レートを超えるトラフィックをキューに入れて、PVC によって伝送されるトラフィックのフローを規制します。[QoS] タブのフィールドの説明については、表 24 : [PVC] ダイアログボックス - [QoS] タブ （79 ページ）を参照してください。

ステップ 7 （任意）[PVC] ダイアログボックスの [Protocol] タブで、PVC の反対側にある IP アドレス用にスタティック マッピングを作成します。

a) [追加（Add）] をクリックして、[マッピングの定義（Define Mapping）] ダイアログボックスを表示します。このダイアログボックスのフィールドの説明については、表 26 : [Define Mapping] ダイアログボックス （84 ページ）を参照してください。

b) IP アドレスを選択し、マッピングするアドレスまたはネットワーク/ホストオブジェクトを入力します。あるいは、[選択（Select）] をクリックしてリストからネットワーク/ホストオブジェクトを選択するか、または新規のネットワーク/ホストオブジェクトを作成します。

c) [OK] をクリックスタティック マッピングが、[Protocol] タブに表示されます。

d) 7.a （69 ページ）～7.c （69 ページ）を繰り返して、他のスタティック マッピングを定義します。

（注） [Protocol] タブではこのほか、使用する InARP のタイプをブロードキャストまたは非ブロードキャストに変更することもできます。

ステップ 8 [詳細設定（Advanced）] をクリックして、PVC での OAM 管理を設定します。 ATM PVC での OAM 管理の定義 （69 ページ）を参照してください。

ステップ 9 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。定義が、[PVC] テーブルに表示されます。

（注） PVC を編集するには、テーブルから目的の PVC を選択し、[編集（Edit）] をクリックします。PVC を削除するには、目的の PVC を選択し、[削除（Delete）] をクリックします。

ステップ 10 ステップ 2 （68 ページ）～ステップ 9 （69 ページ）を繰り返して、他の PVC を定義します。

ATM PVC での OAM 管理の定義

Security Manager では、次の F5（VC レベル）の Operation, Administration, and Maintenance（OAM; 運用管理および保守）セルを設定して、Cisco IOS ルータで PVC 障害を検出できます。

- ループバック セル
- 連続性チェック（CC）セル

- アラーム表示信号（AIS）セル
- リモート検出表示（RDI）セル

このようなセルタイプを個別にイネーブルおよびディセーブルにできます。また、障害が検出されたときに、各セル タイプが PVC にどのように影響を与えるかを左右する設定を定義できます。

はじめる前に

- PVC が定義されている ATM インターフェイスを選択します。
- PVC の一般的な設定および QoS 設定を定義します。 ATM PVC の定義 （67 ページ） を参照してください。

関連項目

- ATM PVC の定義 （67 ページ）
- Cisco IOS ルータでの PVC （61 ページ）

ステップ 1 [PVC] ダイアログボックスで、[詳細設定（Advanced）] をクリックして [PVC の詳細設定（PVC Advanced Settings）] ダイアログボックスを表示します。このダイアログボックスのフィールドの説明については、表 27 : [PVC Advanced Settings] ダイアログボックス （85 ページ）を参照してください。

ステップ 2 選択した PVC で OAM ループバック セルをイネーブルにします。

a) [OAM-PVC] タブをクリックします。このタブのフィールドの説明については、表 29 : [PVC Advanced Settings] ダイアログボックス - [OAM-PVC] タブ （88 ページ）を参照してください。

b) [OAM 管理の有効化（Enable OAM Management）] チェックボックスをオンにします。

c) ループバック セル伝送の頻度を定義します。

ステップ 3 （任意）PVC でセグメント CC セルをイネーブルにします。

a) [セグメント連続性チェック（Segment Continuity Check）] で、[連続性チェックの設定（Configure Continuity Check）] を選択します。

b) ルータがシンク、ソース、あるいはその両方として機能するのかを選択します。これにより、CCセルの送信方向が決まります。

c) セグメント障害またはエンドツーエンド障害が検出されても、PVC はアップしたままとするかどうかを選択します。

（注） [アクティベーション要求を拒否（Deny Activation Requests）] を選択すると、ルータはピアから受信した CC アクティベーション要求を拒否します。

ステップ 4 （任意）セグメント CC セル向けにステップ 3 （70 ページ）で説明している手順に従って、PVC でエンドツーエンド CC セルをイネーブルにします。

ステップ 5 （任意）他のループバック セル パラメータを設定します。

a) [OAM] タブをクリックします。

b) [OAM 再試行の有効化（Enable OAM Retry）] チェックボックスをオンにし、ダウンカウント、アップカウント、および再試行頻度を定義します。使用可能なオプションの説明については、表 28 : [PVC Advanced Settings] ダイアログボックス - [OAM] タブ （86 ページ）を参照してください。

ステップ 6 （任意）他の CC セル パラメータを設定します。

a) セグメント CC セルの [有効化（Enable）] チェックボックスをオンにし、アクティベーションカウント、ディアクティベーション カウント、および再試行頻度を定義します。これらのフィールドによって、ピアに送信されるアクティベーション要求とディアクティベーション要求の数、およびルータの試行間隔が決まります。使用可能なオプションの説明については、表 28 : [PVC Advanced Settings] ダイアログボックス - [OAM] タブ （86 ページ）を参照してください。

b) エンドツーエンド CC セルについても6.a （71 ページ）を繰り返します。

ステップ 7 （任意）PVC で AIS/RDI セルを設定します。

a) [OAM] タブで、[AIS-RDI 検出の有効化（Enable AIS-RDI Detection）] チェックボックスをオンにします。

b) PVC がダウン状態に移行するために必要な AIS/RDI セルの数を定義します。

c) どのくらいの時間 AIS/RDI セルを受信しなければ PVC がアップ状態に移行できるかを秒単位で定義します。

ステップ 8 [OK] をクリックして、ダイアログボックスを閉じ、[PVC] ダイアログボックスに戻ります。

[PVC] ポリシー ページ

[PVC] ページは、ルータで Permanent Virtual Connection（PVC; 相手先固定接続）を作成、編集、および削除する場合に使用します。PVC では、リース回線に似たサービスを提供するためにサイト間に直接および永続的な接続を確立できます。このような PVC は、ADSL、SHDSL、または基本的な ATM 環境に使用できます。詳細については、ATM PVC の定義 （67 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [インターフェイス（Interfaces）] > [設定（Settings）] > [PVC] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータインターフェイス（Router Interfaces）] > [設定（Settings）] > [PVC] を選択します。[PVC] を右クリックしてポリシーを作成するか、共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- [ADSL] ポリシー ページ （49 ページ）
- [SHDSL] ポリシー ページ （55 ページ）
- Cisco IOS ルータでの PVC （61 ページ）
- テーブル カラムおよびカラム見出しの機能

- テーブルのフィルタリング

フィールド リファレンス

表 *21 : [PVC]* ページ

要素	説明
ATM インターフェイス	PVC が定義されている ATM インターフェイス。
インターフェイス カード	ATM インターフェイスが存在するデバイスまたは WAN インターフェイス カードのタイプ。
PVC ID	PVC の Virtual Path Identifier（VPI; 仮想パス識別子）および Virtual Channel Identifier（VCI; 仮想チャネル識別子）。
設定	カプセル化、PPPoE セッションの数、VPN サービス名など、PVC 用のその他の設定。
QoS	トラフィック シェーピングなど、PVC に対して定義する QoS 設定。
プロトコル	PVC 用に設定される IP プロトコル マッピング（スタティック マップまたは Inverse ARP）。
OAM	PVC 用に設定される F5 Operation, Administration, and Maintenance（OAM; 運用管理および保守）ループバック、連続性チェック、および AIS/RDI 定義。
OAM-PVC	PVC 用に設定される OAM 管理セル。
[追加（Add）] ボタン	[PVC] ダイアログボックス （72 ページ）が開きます。ここから、PVC を定義できます。
[編集（Edit）] ボタン	[PVC] ダイアログボックス （72 ページ）が開きます。ここから、選択した PVC を編集できます。
[削除（Delete）] ボタン	選択した PVC をテーブルから削除します。

[PVC] ダイアログボックス

[PVC] ダイアログボックスは、ATM Permanent Virtual Circuit（PVC; 相手先固定接続）を設定する場合に使用します

次のインターフェイス カード タイプを設定できます。

- [Unknown]：インターフェイス カード タイプは定義されません。

- [WIC-1ADSL]：ADSL over POTS（通常の電話回線）を提供する 1 ポート ADSL WAN インターフェイス カード。
- [WIC-1ADSL-I-DG]：Dying Gasp サポートのある ADSL over ISDN を提供する 1 ポート ADSL WAN インターフェイス カード（Dying Gasp を使用すると、ルータは、ルータの電力が失われかけているときに、差し迫った回線ドロップを DSLAM に警告します）。
- [WIC-1ADSL-DG]：Dying Gasp サポートのある ADSL over POTS を提供する 1 ポート ADSL WAN インターフェイス カード。
- [HWIC-1ADSL]：ADSL over POTS を提供する 1 ポート高速 ADSL WAN インターフェイス カード。
- [HWIC-1ADSLI]：ADSL over ISDN を提供する 1 ポート高速 ADSL WAN インターフェイス カード。
- [HWIC-ADSL-B/ST]：バックアップのために ISDN BRI ポートに ADSL over POTS を提供する 2 ポート高速 ADSL WAN インターフェイス カード。
- [HWIC-ADSLI-B/ST]：バックアップのために ISDN BRI ポートに ADSL over ISDN を提供する 2 ポート高速 ADSL WAN インターフェイス カード。
- [WIC-1-SHDSL-V2]：2 線式モードおよび拡張 4 線式モードに対応した、1 ポート複数回線 G.SHDSL WAN インターフェイス カード。
- [WIC-1-SHDSL-V3]：2 線式モードおよび 4 線式モード（標準および拡張）に対応した、1 ポート複数回線 G.SHDSL WAN インターフェイス カード。
- [NM-1A-T3]：T3 リンクを備えた 1 ポート ATM ネットワーク モジュール。
- [NM-1A-OC3-POM]：光信号レベル 3（OC-3）リンクおよび 3 つの動作モード（マルチモード、Single-Mode Intermediate Reach（SMIR; シングルモード中距離）、および Single-Mode Long-Reach（SMLR; シングルモード長距離））に対応した、1 ポート ATM ネットワーク モジュール。
- [NM-1A-E3]：E3 リンクを備えた 1 ポート ATM ネットワーク モジュール。
- [857 ADSL]：ADSL インターフェイスがある Cisco 857 サービス統合型ルータ。
- [876 ADSL]：ADSL インターフェイスがある Cisco 876 サービス統合型ルータ。
- [877 ADSL]：ADSL インターフェイスがある Cisco 877 サービス統合型ルータ。
- [878 888 G.SHDSL]：G.SHDSL インターフェイスがある Cisco 878 サービス統合型ルータ。
- [1801 ADSLoPOTS]：ADSL over POTS を提供する Cisco 1801 サービス統合型ルータ。
- [1802 ADSLoISDN]：ADSL over ISDN を提供する Cisco 1802 サービス統合型ルータ。
- [1803 G.SHDSL]：4 線式 G.SHDSL を提供する Cisco 1803 サービス統合型ルータ。

ナビゲーション パス

[PVC] ポリシー ページ （71 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- ATM PVC の定義 （67 ページ）

フィールド リファレンス

表 *22 : [PVC]* ダイアログボックス

要素	説明
ATMインターフェイス	PVCが定義されているATMインターフェイス。インターフェイス、サブインターフェイス、またはインターフェイスロールの名前を入力するか、[選択（Select）] をクリックしていずれかを選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 （注） インターフェイス ロールを定義するときには、同じインターフェイス カードからの ATM インターフェイスだけを含めることを強く推奨します。各カードタイプでサポートされている設定が異なると、展開に失敗することがあります。
インターフェイス カード	ルータに組み込まれている WAN インターフェイス カードのタイプ、またはルータ タイプ。サポートされるカード タイプは上記のとおりです。 （注） ポリシーを適切に検証するために、このフィールドに値を定義することを強く推奨します。ライブ デバイスを検出したときは、正しいインターフェイス カードタイプがすでに表示されています。ライブデバイスで検出を実行しなかった場合、またはCisco Security Managerがデバイスに取り付けられているインターフェイスカードのタイプを検出できない場合、このフィールドに「Unknown」と表示されます。
[設定（Settings）] タブ	VPI/VCI やカプセル化など、基本的な PVC 設定を定義します。 [PVC] ダイアログボックス - [Settings] タブ （75 ページ）を参照してください。
[QoS] タブ	ATM トラフィック シェーピングをはじめ、PVC のその他の QoS 設定を定義します。 [PVC] ダイアログボックス - [QoS] タブ （78 ページ）を参照してください。
[Protocol] タブ	PVC 用に設定される IP プロトコル マッピングを定義します（スタティック マップまたは Inverse ARP）。 [PVC] ダイアログボックス - [Protocol] タブ （82 ページ）を参照してください。

要素	説明
[Advanced] ボタン	PVC の F5 Operation, Administration, and Maintenance（OAM; 運用管理および保守）設定を定義します。[PVC Advanced Settings] ダイアログボックス - [OAM] タブ （85 ページ） を参照してください。

[PVC] ダイアログボックス - [Settings] タブ

[PVC] ダイアログボックスの [Settings] タブは、PVC の基本的な設定を設定する場合に使用します。

- ID 設定。
- カプセル化設定。
- ILMI および Inverse ARP が有効になるかどうか。
- PPPoE セッションの最大数。
- PPPoA に使用するスタティック ドメイン（VPN サービス）名。

ナビゲーション パス

[PVC] ダイアログボックス （72 ページ）に移動し、[設定（Settings）] タブをクリックします。

関連項目

- [PVC] ダイアログボックス - [QoS] タブ （78 ページ）
- [PVC] ダイアログボックス - [Protocol] タブ （82 ページ）
- [PVC Advanced Settings] ダイアログボックス （84 ページ）
- ATM PVC の定義 （67 ページ）

フィールド リファレンス

表 23 : [PVC] ダイアログボックス - [Settings] タブ

要素	説明
PVC ID 設定	

要素	説明
VPI	PVC の仮想パス識別子。VCI と組み合わせて、セルの次の宛先を特定します。この組み合わせは、宛先に至るまでに存在する一連の ATM スイッチを通過します。ほぼどのプラットフォームでも有効値の範囲は 0 ～ 255 です。 Inverse Multiplexing over ATM（IMA; ATM の逆多重化）を使用する Cisco 2600 および 3600 シリーズ ルータの場合、有効値の範囲は 0 ～ 15、64 ～ 79、128 ～ 143、および 192 ～ 207 です。 （注） VPI/VCI 値は、選択したインターフェイスに設定されているすべての PVC で一意である必要があります。VPI/VCI 値は、単一のリンクに対してだけ一意であり、セルが ATM ネットワークを通過するときに変化することがあります。
VCI	PVC の 16 ビット仮想チャネル識別子。VPI と組み合わせて、セルの次の宛先を特定します。この組み合わせは、宛先に至るまでに存在する一連の ATM スイッチを通過します。有効な値は、プラットフォームによって異なります。一般に、最大 31 までの値は、特殊なトラフィック（ILMI など）用に予約されているため、使用しないでください。3 および 4 は無効です。 （注） VPI/VCI 値は、選択したインターフェイスに設定されているすべての PVC で一意である必要があります。VPI/VCI 値は、単一のリンクに対してだけ一意であり、セルが ATM ネットワークを通過するときに変化することがあります。
ハンドル	PVC を識別するために任意で指定する名前。最大長は 15 文字です。
Management PVC (ILMI)	サブインターフェイスに PVC を設定する場合には適用されません。 選択されている場合、Interim Local Management Interface（ILMI; 暫定ローカル管理インターフェイス）との通信がイネーブルになって、この PVC はこの ATM インターフェイスの管理 PVC となります。ILMI は、ATM インターフェイスで物理層、ATM レイヤ、仮想パス、および仮想回線パラメータを設定およびキャプチャするためのプロトコルとして、ATM フォーラムが定義したものです。ILMI について （65 ページ）を参照してください。 選択解除されている場合、この PVC は管理 PVC として機能しません。これがデフォルトです。 （注） 管理 PVC の VPI/VCI は、一般に 0/16 に設定されます。
カプセル化設定	

要素	説明
タイプ（Type）	[Management PVC (ILMI)] チェックボックスがオンになっているときには適用されません。 PVC で使用する ATM Adaptation Layer（AAL; ATM アダプテーション レイヤ）およびカプセル化のタイプ。 • [blank]：カプセル化のタイプは定義されません（展開時に aal5snap が適用されます）。 • [aal2]：AAL2 Voice over ATM 専用の PVC。AAL2 は、Variable Bit Rate（VBR; 可変ビット レート）トラフィックに使用されます。リアルタイム（VBR-RT）とすることも、非リアルタイム（VBR-NRT）とすることもできます。 • [aal5autoppp]：ルータは、着信 PPP over ATM（PPPoA）と PPP over Ethernet（PPPoE）セッションとを区別し、要求に応じて両方の PPP タイプの仮想アクセスを確立します。 • [aal5ciscoppp]：Cisco 独自の PPP over ATM 用。 • [aal5mux]：[Protocol] フィールドでの定義に従って、PVC を単一のプロトコル専用にします。 • [aal5nlpid]：ATM インターフェイスは、ATM Data Service Unit（ADSU; ATM データ サービス ユニット）を使用し、かつ ATM-Data Exchange Interface（DXI; データ交換インターフェイス）を実行している High-Speed Serial Interface（HSSI）と連携して動作できるようになります。 • [aal5snap]：Inverse ARP をサポートし、プロトコル データグラムの前にある Logical Link Control/Subnetwork Access Protocol（LLC; 論理リンク制御/SNAP; サブネットワーク アクセス プロトコル）を組み込みます。これにより、複数のプロトコルが同じ PVC を通過できます。
Virtual Template	この PVC で PPP over ATM に使用される仮想テンプレート。仮想テンプレート インターフェイスまたはインターフェイスロールの名前を入力するか、[選択（Select）] をクリックして仮想テンプレート インターフェイスまたはインターフェイスロールを選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 ユーザがダイヤルインすると、仮想テンプレートを使用して仮想アクセス インターフェイスが設定されます。ユーザがダイヤルアウトすると、仮想アクセス インターフェイスがダウンし、他のダイヤルインユーザのためにリソースが解放されます。 （注） 既存の PVC の仮想テンプレート設定を修正する場合は、ATM サブインターフェイスで shutdown コマンドに続けて no shutdown コマンドを入力して、インターフェイスを再起動する必要があります。これにより、新規に設定したパラメータが有効になります。

要素	説明
プロトコル	aal5mux がカプセル化のタイプとして定義されたときにだけ適用されます。 MUX カプセル化 PVC によって伝送されるプロトコル。 • [frame-relay]：Cisco MC3810 上のフレーム リレー/ATM ネットワーク インターワーキング（FRF.5）。 • [fr-atm-srv]：Cisco MC3810 上のフレーム リレー/ATM サービス インターワーキング（FRF.8）。 • [ip]：IP プロトコル。 • [ppp]：IETF 準拠の PPP over ATM。このプロトコル タイプを使用するときには、仮想テンプレートを指定する必要があります。 • [voice]：Voice over ATM。
その他の設定	
Enable ILMI	選択されている場合、この PVC で ILMI 管理がイネーブルになります。 選択解除されている場合、この PVC で ILMI 管理がディセーブルになります。
Inverse ARP	選択されている場合、PVC で Inverse Address Resolution Protocol（Inverse ARP）がイネーブルになります。 選択解除されている場合、Inverse ARP がディセーブルになります。これがデフォルトです。 Inverse ARP は、確立済み接続のリモート エンドでレイヤ 3 アドレスを学習する場合に使用します。仮想回線を使用するには、事前にこのようなアドレスを学習する必要があります。 （注） [Protocol] タブは、Inverse ARP を使用してアドレスを動的に学習するのではなく、IP アドレスのスタティック マッピングを定義する場合に使用します。[PVC] ダイアログボックス - [Protocol] タブ （82 ページ）を参照してください。
PPPoE Max Sessions	PVC に許可されている PPP over Ethernet セッションの最大数。
VPN Service Name	この PVC で使用するスタティック ドメイン名。最大長は 128 文字です。 このオプションは、PPP を開始せずに、指定されたドメイン名に従って PVC の PPP over ATM（PPPoA）セッションを転送する場合に使用します。

[PVC] ダイアログボックス - [QoS] タブ

[PVC] ダイアログボックスの [QoS] タブは、ATM トラフィック シェーピングをはじめ、PVC のその他の QoS 設定を設定する場合に使用します。

- 伝送リングでパケットに課される制限。
- QoS サービス。
- ランダム検出がイネーブルになるかどうか。

これらの設定は、定義済みの許容可能なビット レートを超えるトラフィックをキューに入れて、PVC を経由するトラフィックのフローを規制します。

（注） QoS 値は、ハードウェアに強く依存します。デバイスに設定できる設定の詳細については、ルータのマニュアルを参照してください。

ナビゲーション パス

[PVC] ダイアログボックス （72 ページ）に移動し、[QoS] タブをクリックします。

関連項目

- [PVC] ダイアログボックス - [Settings] タブ （75 ページ）
- [PVC] ダイアログボックス - [Protocol] タブ （82 ページ）
- [PVC Advanced Settings] ダイアログボックス （84 ページ）
- ATM PVC の定義 （67 ページ）
- サービス品質ポリシーページ
- ポリシング パラメータとシェーピング パラメータについて

フィールド リファレンス

表 *24 : [PVC]* ダイアログボックス - *[QoS]* タブ

要素	説明
Tx Ring Limit	WAN Interface Card（WIC; WAN インターフェイス カード）またはインターフェイスで伝送リングに配置できる伝送パケットの最大数。 有効な値の範囲は、[Settings] タブで選択されているインターフェイス カードのタイプによって異なります。 [PVC] ダイアログボックス - [Settings] タブ （75 ページ）を参照してください。
トラフィック シェーピング設定	

要素	説明
Traffic Shaping	PVC に定義するサービスのタイプ。 • [null]：ビット レートは定義されません。 • [ABR]：使用可能ビット レート。セルの損失または遅延の保証が必要ないアプリケーションに適したベスト エフォート型のサービス。 • [CBR]：固定ビット レート サービス。音声やビデオなど遅延に影響されやすいデータを固定レートで送信して、専用線と同じようなサービスを提供します。 • [UBR]：未指定ビット レート サービス。遅延が問題にならず、リアルタイムの応答を必要としないアプリケーションに適したベスト エフォート型のサービス。 • [UBR+]：未指定ビット レート サービス。UBR と異なり、UBR+ は保証した最小レートを維持しようとしています。 • [VBR-NRT]：可変ビット レート - 非リアルタイム サービス。バースト性がある非リアルタイム アプリケーションに適したサービス。VBR は、CBR よりも効率的で、UBR よりも信頼性が高くなっています。 • [VBR-RT]：可変ビット レート - リアルタイム サービス。バースト性があるリアルタイム アプリケーションに適したサービス。 各サービス クラスの詳細については、ATM サービス クラスについて （63 ページ）を参照してください。
ABR	ビット レートとして [ABR] を選択すると、次のフィールドが表示されます。 • [PCR]：キロビット/秒（kbps）単位でのピーク セル レート。これが、ABR の最大値となります。 • [MCR]：キロビット/秒（kbps）単位での最小セル レート。これが、ABR の最小値となります。 ABR は、MCR と PCR の間で変化します。輻輳制御メカニズムによって動的に制御されます。
CBR	ビット レートとして [CBR] を選択すると、次のフィールドが表示されます。 • [Rate]：キロビット/秒（kbps）単位での PVC の固定ビット レート（平均セル レートとも呼ばれます）。CBR 用に設定された ATM VC は、必要とされるかぎり、このレートでセルを送信できます。
UBR	ビット レートとして [UBR] を選択すると、次のフィールドが表示されます。 • [PCR]：キロビット/秒（kbps）単位での出力のピーク セル レート。PCR を超えるセルは廃棄されることがあります。

要素	説明
UBR+	ビット レートとして [UBR+] を選択すると、次のフィールドが表示されます。 • [PCR]：キロビット/秒（kbps）単位での出力のピーク セル レート。PCR を超えるセルは廃棄されることがあります。 • [MCR]：キロビット/秒（kbps）単位での出力の最小保証セル レート。トラフィックは、常にこのレートで送信できます。 （注） UBR+ を使用するには、Cisco IOS ソフトウェア Release 12.4(2)XA 以降、またはバージョン 12.4(6)T 以降が必要です。
VBR-NRT	ビット レートとして [VBR-NRT] を選択すると、次のフィールドが表示されます。 • [PCR]：キロビット/秒（kbps）単位での出力のピーク セル レート。PCR を超えるセルは廃棄されることがあります。 • [SCR]：キロビット/秒（kbps）単位での出力の平均セル レート。この値は、PCR 以下である必要があり、データを損失させずにセルを送信できる最大レートとなります。 • [MBS]：出力の最大バースト セル サイズ。この値は、ペナルティなしで送信できるセルの数で、SCR よりも大きく、PCR よりも小さくなります。
VBR-RT	ビット レートとして [VBR-RT] を選択すると、次のフィールドが表示されます。 • [Peak Rate]：キロビット/秒（kbps）単位でのリアルタイム トラフィックのピーク情報レート。 • [Average Rate]：キロビット/秒（kbps）単位でのリアルタイム トラフィックの平均情報レート。この値は、ピーク レート以下である必要があります。 • [Burst]：セル数単位でのリアルタイム トラフィックのバースト サイズ。この値は、PVC がバースト トラフィックを伝送する場合に設定します。 これらの値はリアルタイム トラフィック（音声やビデオなど）とデータ トラフィックとの間のトラフィック シェーピングを設定するもので、これにより、音声コールなどのリアルタイム トラフィックが廃棄されなくなります。
IP QoS 設定	

要素	説明
Random Detect	選択されている場合、PVC で Weighted Random Early Detection（WRED; 重み付けランダム早期検出）または VIP-Distributed WRED（DWRED; VIP 分散 WRED）がイネーブルになります。 選択解除されている場合、WRED および DWRED がディセーブルになります。これがデフォルトです。 WRED はキュー管理方法の 1 つで、インターフェイスが輻輳状態になるとパケットを選択してドロップします。テール ドロップと WRED を参照してください。

[PVC] ダイアログボックス - [Protocol] タブ

[PVC] ダイアログボックスの [Protocol] タブは、PVC 用に設定されるプロトコル マッピングを追加、編集、または削除する場合に使用します。PVC ごとにスタティック マッピングまたは Inverse ARP（ブロードキャストまたは非ブロードキャスト）の両方ではなくいずれか一方を設定することもできます。

（注） IP は、ATM ネットワークのプロトコル マッピングに Security Manager がサポートする唯一のプロトコルです。管理 PVC（ILMI）にプロトコル マッピングは定義できません。

ナビゲーション パス

[PVC] ダイアログボックス （72 ページ）に移動し、[プロトコル（Protocol）] タブをクリックします。

関連項目

- [PVC] ダイアログボックス - [Settings] タブ （75 ページ）
- [PVC] ダイアログボックス - [QoS] タブ （78 ページ）
- [PVC Advanced Settings] ダイアログボックス （84 ページ）
- ATM PVC の定義 （67 ページ）

フィールド リファレンス

表 *25 : [PVC]* ダイアログボックス - *[Protocol]* タブ

要素	説明
IP Protocol Mapping	PVC 用に設定される IP プロトコル マッピングを表示します。
[追加（Add）] ボタン	[Define Mapping] ダイアログボックス （83 ページ）が開きます。ここから、IP プロトコル マッピングを定義できます。

要素	説明
[編集（Edit）] ボタン	[Define Mapping] ダイアログボックス （83 ページ）が開きます。ここから、選択したマッピングを編集できます。
[削除（Delete）] ボタン	選択したマッピングをテーブルから削除します。

[Define Mapping] ダイアログボックス

[Define Mapping] ダイアログボックスは、ATM PVC で使用する IP プロトコル マッピングを設定する場合に使用します。どの IP アドレスが接続の反対側に到達可能であるかを PVC が検出するには、マッピングが必要です。マッピングは、Inverse ARP（InARP）を使用して動的に学習することも、静的に定義することもできます。スタティック マッピングは、ノードの数が少ない簡単なネットワークに最適です。

（注） Inverse ARP は、カプセル化のタイプが aal5snap である場合にだけサポートされます。[PVC] ダイアログボックス - [Settings] タブ （75 ページ）を参照してください。

ヒント IP 以外のプロトコルのマッピングを設定するには、CLI または FlexConfig を使用します。

ナビゲーション パス

[PVC] ダイアログボックス - [Protocol] タブ （82 ページ）に移動し、[追加（Add）] または [編集（Edit）] をクリックします。

関連項目

- [PVC] ダイアログボックス （72 ページ）
- ATM PVC の定義 （67 ページ）

フィールド リファレンス

表 26 : [Define Mapping] ダイアログボックス

要素	説明
IP オプション	使用する IP プロトコル マッピングのタイプ。 • [IP Address]：スタティック マッピングを使用しているときには、このオプションを選択します。ネットワーク/ホストオブジェクトのアドレスまたは名前を入力するか、[選択（Select）]をクリックして選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 • [InARP]：Inverse ARP。ダイナミック マッピングを使用しているときには、このオプションを選択します。これにより、PVC はスタティック マップを設定せずに独自のネットワーク アドレスを解決できます。ダイナミック マッピングは、デフォルトでは 15 分おきに期限切れになってリフレッシュされます。 （注） InARP は、aal5snap が PVC のカプセル化のタイプとして定義されたときにだけ使用できます。[PVC] ダイアログボックス - [Settings] タブ（75 ページ）を参照してください。
Broadcast Options	IP ブロードキャスト パケット（EIGRP 更新など）の送信時に、このマップ エントリを使用するかどうかを示します。 • [Broadcast]：マップ エントリがブロードキャスト パケットに使用されます。 • [No Broadcast]：ユニキャスト パケットに対してだけマップ エントリが使用されます。 • [None]：ブロードキャスト オプションがディセーブルになります。

[PVC Advanced Settings] ダイアログボックス

[PVC Advanced Settings] ダイアログボックスは、ATM PVC に F5 Operation, Administration, and Maintenance（OAM; 運用管理および保守）機能を設定する場合に使用します。OAM を使用すると、ATM レイヤで接続障害を検出できます。

詳細については、ATM PVC での OAM 管理の定義 （69 ページ）を参照してください。

ナビゲーション パス

[PVC] ダイアログボックス （72 ページ）に移動し、[詳細設定（Advanced）] をクリックします。

関連項目

- [PVC] ポリシー ページ （71 ページ）

フィールド リファレンス

表 *27 : [PVC Advanced Settings]* ダイアログボックス

要素	説明
[OAM] タブ	ループバック、接続性チェック、およびAIS/RDI設定を定義します。[PVC Advanced Settings] ダイアログボックス - [OAM] タブ （85 ページ）を参照してください。
[OAM-PVC] タブ	PVC で OAM ループバックおよび接続性チェックをイネーブルにします。[PVC Advanced Settings] ダイアログボックス - [OAM-PVC] タブ （88 ページ） を参照してください。

[PVC Advanced Settings] ダイアログボックス - [OAM] タブ

[PVC Advanced Settings] ダイアログボックスの [OAM] タブは、次の項目を定義する場合に使用します。

- PVC がダウン状態またはアップ状態に移行するループバック セル応答の数。
- PVC がダウン状態またはアップ状態に移行する Alarm Indication Signal/Remote Defect Indication（AIS; アラーム表示信号/RDI; リモート障害表示）セルの数。
- この PVC で送信されるセグメント/エンド Continuity Check（CC; 連続性チェック）アクティベーション要求およびディアクティベーション要求の数と頻度。

詳細については、 ATM PVC での OAM 管理の定義 （69 ページ）を参照してください。

（注） このタブに定義される設定は、[OAM-PVC] タブに定義される設定によって異なります。[PVC Advanced Settings] ダイアログボックス - [OAM-PVC] タブ （88 ページ）を参照してください。

ナビゲーション パス

[PVC Advanced Settings] ダイアログボックス （84 ページ）に移動し、[OAM] タブをクリックします。

関連項目

- [PVC] ダイアログボックス （72 ページ）

フィールド リファレンス

表 28 : [PVC Advanced Settings] ダイアログボックス - [OAM] タブ

要素	説明
再試行設定	
Enable OAM Retry	選択されている場合、OAM 管理設定を定義できます。 選択解除されている場合、OAM 管理設定を定義できません。 （注） [OAM-PVC] タブで [Enable OAM Management] を選択しないと、これらの設定はデバイス設定に保存されますが、適用はされません。
Down Count	エンドツーエンド ループバック セル応答を連続していくつ受信しなかった場合に、PVC がダウン状態に移行するかを示す値。デフォルトは 3 です。
Up Count	連続していくつのエンドツーエンド ループバック セル応答を受信した場合に、PVC がアップ状態に移行するかを示す値。デフォルトは 5 です。
再試行の頻度（Retry Frequency）	秒単位でのループバック セル検証の伝送間隔。デフォルト値は 1 秒です。 PVC がアップ状態で、ループバック セル応答が（[PVC-OAM] タブの [Frequency] フィールドで定義されている）指定の間隔内に受信されなかった場合は、ここに定義された頻度でループバック セルが送信され、PVC がダウンしているかどうかが確認されます。連続して応答を受信しないセルの数が定義済みのダウン カウントに一致すると、PVC はダウン状態に移行します。
AIS-RDI 設定	
Enable AIS-RDI Detection	選択されている場合、Alarm Indication Signal（AIS; アラーム表示信号）セルおよび Remote Defect Indication（RDI; リモート障害表示）セルを使用して、PVC の ATM レイヤで発生した接続障害が報告されます。 選択解除されている場合、AIS/RDI セルがディセーブルになります。 AIS セルは、ダウンストリーム デバイスに接続障害を通知します。最後の ATM スイッチが、元の障害通知を送信したデバイスに至るアップストリーム方向に RDI セルを生成します。
Down Count	AIS/RDI セルがいくつ連続すると PVC のダウンを引き起こすかを示す値。有効値の範囲は 1 ～ 60 です。デフォルトは 1 です。
Up Count	AIS/RDI セルを受信しない場合に、PVC がアップするまでの秒数。有効値の範囲は、3 ～ 60 秒です。デフォルトは 3 です。

要素	説明
セグメント連続性チェック設定	
Enable Segment Continuity Check	選択されている場合、OAM F5 Continuity Check（CC; 連続性チェック）アクティベーション要求およびディアクティベーション要求がセグメントの反対側にあるデバイスに送信されます。 選択解除されている場合、セグメント CC アクティベーションおよびディアクティベーション要求はディセーブルになります。 （注） [OAM-PVC] タブで [Configure Continuity Check] が選択解除されている場合、これらの設定はデバイス設定に保存されますが、適用はされません。
Activation Count	確認応答の受信前にアクティベーション要求が送信される最大回数。有効値の範囲は 3 ～ 600 です。デフォルトは 3 です。
Deactivation Count	確認応答の受信前にディアクティベーション要求が送信される最大回数。有効値の範囲は 3 ～ 600 です。デフォルトは 3 です。
再試行の頻度（Retry Frequency）	アクティベーション/ディアクティベーションの再試行間隔（秒単位）。デフォルトは 30 秒です。
エンドツーエンド連続性チェック設定	
Enable End-to-End Continuity Check	選択されている場合、OAM F5 Continuity Check（CC; 連続性チェック）アクティベーション要求およびディアクティベーション要求が PVC の反対側にあるデバイスに送信されます。 選択解除されている場合、セグメント CC アクティベーションおよびディアクティベーション要求はディセーブルになります。 （注） [OAM-PVC] タブで [Configure Continuity Check] が選択解除されている場合、これらの設定はデバイス設定に保存されますが、適用はされません。
Activation Count	確認応答の受信前にアクティベーション要求が送信される最大回数。有効値の範囲は 3 ～ 600 です。デフォルトは 3 です。
Deactivation Count	確認応答の受信前にディアクティベーション要求が送信される最大回数。有効値の範囲は 3 ～ 600 です。デフォルトは 3 です。
再試行の頻度（Retry Frequency）	アクティベーション/ディアクティベーションの再試行間隔（秒単位）。デフォルトは 30 秒です。

[PVC Advanced Settings] ダイアログボックス - [OAM-PVC] タブ

[PVC Advanced Settings] ダイアログボックスの [OAM-PVC] タブは、PVC でループバック セルおよびConnectivity Check（CC; 接続性チェック）をイネーブルにする場合に使用します。その機能により、仮想接続の接続がテストされます。

詳細については、 ATM PVC での OAM 管理の定義 （69 ページ）を参照してください。

（注） [OAM] タブでは、このタブの設定に関連する他の設定を定義できます。 [PVC Advanced Settings] ダイアログボックス - [OAM] タブ （85 ページ）を参照してください。

ナビゲーション パス

[PVC Advanced Settings] ダイアログボックス （84 ページ）に移動し、[OAM-PVC] タブをクリックします。

関連項目

- [PVC] ダイアログボックス （72 ページ）

フィールド リファレンス

表 29 : [PVC Advanced Settings] ダイアログボックス - [OAM-PVC] タブ

要素	説明
OAM 設定	
[Enable OAM Management]	選択されている場合、PVC で OAM ループバック セル生成および OAM 管理がイネーブルになります。 選択解除されている場合、OAM ループバック セルおよび OAM 管理がディセーブルになります。ただし、連続性チェックは引き続き実行できます。
周波数（Frequency）	ループバック セルの伝送間隔。有効値の範囲は、0 ～ 600 秒です。
セグメント連続性チェック設定	

要素	説明
Segment Continuity Check	PVC セグメントで実行される OAM F5 連続性チェックの現在の設定。 • [None]：セグメント Continuity Check（CC; 連続性チェック）がディセーブルになります。 • [Deny Activation Requests]：PVC は、ピア デバイスからのアクティベーション要求を拒否します。これにより、OAM F5 CC 管理は PVC でアクティブにならなくなります。 • [Configure Continuity Check]：PVC でセグメント CC がイネーブルになります。CC 管理が設定されているルータは、CC アクティベーション要求をセグメントの反対側にあるルータに送信し、そのルータに対してソースまたはシンクとして機能するように指示します。 ルータと第 1 ホップ ATM スイッチとの間にある PVC セグメントで、セグメント CC が実行されます。
方向	CC 管理がイネーブルになっている場合にだけ適用されます。 CC セルが送信される方向。 • [both]：CC セルは両方向に送信されます。 • [sink]：CC セルは、CC アクティベーション要求を開始したルータの方向に送信されます。 • [source]：CC セルは、CC アクティベーション要求を開始したルータの方向から送信されます。
Keep VC up after segment failure	選択されている場合は、CC セルが接続の障害を検出した場合でも PVC はアップ状態のままになります。 選択解除されている場合は、CC セルが接続の障害を検出した場合に PVC がダウンします。
Keep VC up after end-to-end failure	選択されている場合、エンド CC 障害またはループバック障害が発生したために AIS/RDI セルを受信しても、PVC はダウンしません。 選択解除されている場合、エンド CC 障害またはループバック障害が発生した場合には、PVC がダウンします。
エンドツーエンド連続性チェック設定	

要素	説明
End-to-End Continuity Check	PVC で実行される OAM F5 エンドツーエンド連続性チェックの現在の設定。 • [None]：エンドツーエンド Continuity Check（CC; 連続性チェック）がディセーブルになります。 • [Deny Activation Requests]：PVC は、ピア デバイスからのアクティベーション要求を拒否します。これにより、OAM F5 CC 管理は PVC でアクティブにならなくなります。 • [Configure Continuity Check]：PVC でエンドツーエンド CC がイネーブルになります。CC 管理が設定されているルータは、CC アクティベーション要求を接続の反対側にあるルータに送信し、そのルータに対してソースまたはシンクとして機能するように指示します。 2 台の ATM 端末間にある PVC 全体で、エンドツーエンド CC モニタリングが実行されます。
方向	CC 管理がイネーブルになっている場合にだけ適用されます。 CC セルが送信される方向。 • [both]：CC セルは両方向に送信されます。 • [sink]：CC セルは、CC アクティベーション要求を開始したルータの方向に送信されます。 • [source]：CC セルは、CC アクティベーション要求を開始したルータの方向から送信されます。
Keep VC up after end-to-end failure	選択されている場合は、CC セルが接続の障害を検出した場合でも PVC はアップ状態のままになります。 選択解除されている場合は、CC セルが接続の障害を検出した場合に PVC がダウンします。
Keep VC up after segment failure	選択されている場合、セグメント CC 障害が発生したために AIS/RDI セルを受信しても、PVC はダウンしません。 選択解除されている場合、セグメント CC 障害が発生した場合には、PVC がダウンします。

Cisco IOS ルータでの PPP

Point-to-Point Protocol（PPP）は、RFC 1661 で規定されているように、物理リンクまたは論理リンクを使用して、2 つのデバイスまたはホスト間でパケットを転送するための手段となるも

のです。PPP は、IP、IPX、AppleTalk など複数のレイヤ 3 ネットワーク層プロトコルと連携して動作できるレイヤ 2 データリンク プロトコルです。

PPP は、次に挙げるようなよくあるシナリオに使用されます。

- ダイヤルイン接続でリモート ユーザを中央のネットワークに接続する。
- インターネットにアクセスするため、企業ネットワークのゲートウェイを ISP に接続する。
- 2 つの LAN（たとえば、本社と支社）を接続して両者間でデータを交換する。

PPP 接続は、段階的に確立されます。

1. まず、Link Control Protocol（LCP; リンク コントロール プロトコル）が、データリンク接続を確立、設定、およびテストします。
2. （任意）認証により、両当事者のアイデンティティが検証されます。
3. Network Control Protocol（NCP; ネットワーク コントロール プロトコル）のファミリが、必要なネットワーク層プロトコルを確立し、設定します。

Security Manager の PPP ポリシーを使用すると、LCP 段階で 2 つのノード間でネゴシエートされるパラメータを選択し、設定できます。このようなパラメータには、認証（一般に CHAP または PAP）や Multilink PPP（MLP; マルチリンク PPP）などがあります。MLP の詳細については、マルチリンク PPP バンドルの定義 （95 ページ）を参照してください。

ここでは、Cisco IOS ルータ上に PPP ポリシーを作成するために実行するタスクについて説明します。

- PPP 接続の定義 （92 ページ）
- マルチリンク PPP バンドルの定義 （95 ページ）

マルチリンク PPP（MLP）について

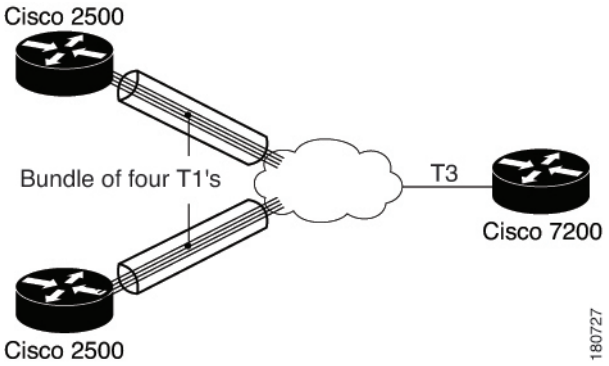
MLP は、RFC 1990 で規定されているように、複数の論理データ リンクでデータグラムを分割、再結合、および順序付けるための手段となるものです。MLP は、元々 ISDN で複数のベアラ チャネルを利用するために設計されたものですが、非同期リンクなど複数の PPP リンクが 2 つのシステムを接続するときにも使用できます。

MLP は、インバウンド トラフィックとアウトバウンド トラフィックを複数の物理的な WAN リンク（まとめてバンドルと呼ばれる）分散させます。これには、次の利点があります。

- パケットのフラグメンテーションと再構成
- 適切な順序付け
- マルチベンダーの相互運用性
- Load balancing

図 3 : マルチリンク PPP （92 ページ）に示すように、MLP リンクにルーティングされるトラフィックがフラグメント化され、そのフラグメントがそれぞれ異なる物理リンクで送信されます。リンクのリモート エンドで、フラグメントが再構築され、最終宛先に至るネクスト ホップに転送されます。MLP では、複数の物理リンクを使用することによって、このようなリンクから得られる追加の帯域幅を一時的に使用できます。

図 *3:* マルチリンク *PPP*



どの MLP バンドルも、バンドルディレクターと呼ばれる、仮想アクセスインターフェイスである単一のインターフェイスによって制御されます。このインターフェイスは、バンドルが初めて作成されるときに、バックグラウンドで作成されます。物理インターフェイスは、バンドルディレクターによって管理されるバンドルの一部になります。バンドルはこのほか、マルチリンク インターフェイスとその関連するシリアル インターフェイスで構成されるマルチリンク グループを作成するときにも使用されます。マルチリンク グループは、静的な専用線環境でよく見られるセットアップです。

MLP は、エンドポイント識別子を使用して、パケットを送信するシステムを識別します。デフォルトでは、この識別子はルータのホスト名に基づいていますが、インターフェイスの IP アドレスまたは MAC アドレス、電話番号、ユーザ定義の文字列など他の基準に基づくこともできます。エンドポイント識別子が既存のリンクの識別子に一致する場合、新規リンクは一致したバンドルに追加されます。一致する識別子がない場合は、新規バンドルが作成されます。認証を使用している場合、一致する識別子がないか、または2つのノード間で認証情報が交換されるたびに、新規バンドルが確立されます。

関連項目

- マルチリンク PPP バンドルの定義 （95 ページ）
- Cisco IOS ルータでの PPP （90 ページ）

PPP 接続の定義

PPP 接続を定義する場合、最初に実行する手順は、PPP をイネーブルにするインターフェイスを選択することです。次のいずれかのインターフェイス タイプを選択する必要があります。

- Async

- Group-Async
- シリアル
- HSSI（High-Speed Serial Interface）
- ダイヤラ
- [BRI]、[PRI]（ISDN）
- Virtual template
- マルチリンク

次の要素には、PPP 接続を定義できません。

- サブインターフェイス。
- フレーム リレー カプセル化のあるシリアル インターフェイス。
- イーサネットまたはトンネル タイプとして定義された仮想テンプレート インターフェイス（シリアルがサポートされます）。

（注） フレーム リレー カプセル化用に設定されているシリアル インターフェイスには、PPP を設定できません。 基本的なルータ インターフェイス設定の定義 （5 ページ）を参照。

（注） 802.1x ポリシーでも使用されている仮想テンプレートに PPP を定義した場合は、展開に失敗することがあります。802.1x ポリシーの定義を参照してください。

1 つ以上の認証プロトコルを選択し、いつ認証を実行するかを定義できます。

また、リモート セキュリティ サーバで AAA を実行するときに使用する認証と認可の方式を設定できます。すべての PPP 接続に使用するデフォルトの方式リストをデバイスに定義することも、特定の接続に適用する独自の方式リストを定義することもできます。

はじめる前に

- デバイスに PPP を設定できるインターフェイスが含まれていることを確認します。 Cisco IOS ルータでの基本的なインターフェイス設定 （2 ページ） を参照してください。

関連項目

- マルチリンク PPP バンドルの定義 （95 ページ）
- Cisco IOS ルータでの PPP （90 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[インターフェイス（Interfaces）] > [設定（Settings）] > [PPP/MLP]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータインターフェイス（Router Interfaces）] > [設定（Settings）] > [PPP/MLP]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[PPP/MLP] ページが表示されます。このページのフィールドの説明については、[PPP/MLP] ポリシー ページ （96 ページ）を参照してください。

ステップ 2 テーブルの下にある [追加（Add）] ボタンをクリックして、[PPP] ダイアログボックスを表示します。

ステップ 3 [インターフェイス（Interface）] フィールドに、PPP 接続を定義するインターフェイスまたはインターフェイスロールの名前を入力します。あるいは、[選択（Select）] をクリックしてリストからインターフェイスロールを選択するか新規にインターフェイスロールを作成します。

ステップ 4 （任意）[PPP] タブで、PPP 接続の認証を定義します。

a) 1 つ以上の認証プロトコルを選択します。

b) 1つ以上の認証オプションを選択します。これらのオプションでは、認証（コールイン、コールアウト、およびコールバック）をいつ実行するか、ワンタイム パスワードを使用するかどうか、および PDSN 設定でモバイル ステーションを許可して CHAP または PAP を使用せずに Simple IP サービスおよび Mobile IP サービスを受信するかどうかを決定します。

（注） [Call Back] オプションは、コールバック時に認証をイネーブルにするだけです。デバイスにコールバック機能を設定するには、CLI または FlexConfig を使用します。

c) このタブのフィールドの説明については、[PPP] ダイアログボックス - [PPP] タブ （100 ページ）を参照してください。

ステップ 5 （任意）リモート AAA サーバを使用して認証を実行している場合は、[Authenticate Using] フィールドで [Default List] または [Custom Method List] を選択し、[Prioritized Method List] フィールドに使用する方式を定義します。

（注） デフォルト リストを変更した場合、変更内容はそのリストを使用するデバイス上のすべての PPP 接続に影響を与えます。このフィールドを空白のままにした場合は、デバイス上のローカル データベースを使用して認証が実行されます。

ステップ 6 （任意）リモート AAA サーバを使用して認可を実行している場合は、[AAA Policy Default List] または [Custom Method List] を選択し、[Prioritized Method List] フィールドに使用する方式を定義します。

（注） [AAA Policy Default List] を選択した場合、デバイスは AAA ポリシーに定義されているデフォルトの認可方式を使用します。AAA サービスの定義を参照してください。

ステップ 7 （任意）PAP 認証要求に応えて送信するユーザ名およびパスワードを定義します。

（注） パスワードの暗号化バージョンを入力した場合は、[暗号化（Encrypted）] チェックボックスをオンにします。

ステップ 8 （任意）ルータ独自のホスト名の代わりに、すべての CHAP チャレンジおよびレスポンスで送信する別のホスト名を定義します。

（注） パスワードの暗号化バージョンを入力した場合は、[暗号化（Encrypted）] チェックボックスをオンにします。

ステップ 9 （任意）この接続でマルチリンク PPP をイネーブルにするには、[MLP] タブをクリックします。 マルチリンク PPP バンドルの定義 （95 ページ）を参照してください。

ステップ 10 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。定義が、[PPP] テーブルに表示されます。

（注） PPP 接続を編集するには、テーブルから目的の PVC を選択し、[編集（Edit）] をクリックします。PPP 接続を削除するには、目的の PVC を選択し、[削除（Delete）] をクリックします。

ステップ 11 他のインターフェイスで PPP 接続を定義するには、ステップ 2 （94 ページ）～ステップ 10 （95 ページ）を繰り返します。インターフェイスに定義できる PPP 接続は 1 つだけです。

マルチリンク PPP バンドルの定義

選択したインターフェイスで Multilink PPP（MLP; マルチリンク PPP）をイネーブルにするには、[PPP] ダイアログボックスの [Multilink] タブの最上部にあるチェックボックスをオンにします。任意で、Multiclass Multilink PPP（MCMP; マルチクラス マルチリンク PPP）をイネーブルにできます。これにより、遅延に影響されやすいトラフィックのフラグメント化とインターリーブを回避でき、その結果パケットをさらに大きなパケットのフラグメントに分散させることができます。シリアルインターフェイスを特定のバンドルに制限する場合は、そのバンドルを表すマルチリンク インターフェイスを選択できます。

また、任意で次のデフォルト設定を変更できます。

- 最大フラグメント遅延。
- MLP の使用をネゴシエートするときにルータを識別するエンドポイント識別子。
- ルータとそのピアによって許可される Maximum Receive Reconstructed Unit（MRRU）。
- First-In, First-Out（FIFO; ファーストイン ファーストアウト）キューおよび非 FIFO キューの最大キュー深度。

はじめる前に

- PPP 接続をイネーブルにするインターフェイスを選択します。

関連項目

- PPP 接続の定義 （92 ページ）
- Cisco IOS ルータでの PPP （90 ページ）

ステップ 1 [PPP] ダイアログボックスで、[MLP] タブをクリックします。このタブのフィールドの説明については、[PPP] ダイアログボックス - [MLP] タブ （103 ページ）を参照してください。

ステップ 2 [マルチリンクプロトコル（MLP）を有効にする（Enable Multilink Protocol (MLP)）] チェックボックスをオンにします。

ステップ 3 （任意）次のオプションを設定します。

a) 遅延に影響されやすいトラフィックのフラグメント化を回避するために、マルチクラス機能をイネーブルにするかどうかを指定します。そのためには、遅延に影響されやすいトラフィックを通常のトラフィックとは別のクラスに配置します。

b) MLP バンドルで大きなパケットのフラグメントに対してパケットのインターリーブをイネーブルにするかどうかを指定します。

c) 物理リンクを指定のマルチリンク グループだけの加入に制限するかどうかを指定します（マルチリンク インターフェイスを選択して定義します）。リンクの反対側のピアが別のバンドルに参加しようとした場合は、接続が重大になります。

d) MLP バンドルでフラグメントを送信するために必要なデフォルトの時間を変更するかどうかを指定します。デフォルトは 30 ミリ秒です。

（注） フラグメント遅延を定義せずにインターリーブをイネーブルにした場合は、デフォルトの遅延である 30 秒が設定されます。この値は、Security Manager またはデバイス設定に表示されません。

ステップ 4 （任意）[Endpoint] で、MLP バンドルで使用されるデフォルトのエンドポイント識別子を変更します。

エンドポイント識別子は、MLP バンドルでルータを識別する場合に使用します。デフォルトのエンドポイント識別子は、グローバルに設定したホスト名か、または（使用する認証プロトコルに応じて）PAP ユーザ名か CHAP ホスト名となります。ただし、[PPP] タブで対応する値を設定した場合にかぎります。 PPP 接続の定義 （92 ページ）を参照してください。

ステップ 5 （任意）MRRU のフィールドで、ルータ（ローカル）またはピア（リモート）が受信できるデフォルトの最大パケット サイズを変更します。

ステップ 6 （任意）FIFO キューおよび非 FIFO（QoS）キューを使用している場合、リンク送信キューのデフォルトの最大サイズを変更します。

ステップ 7 [OK] をクリックして、ダイアログボックスを閉じます。定義が、[PPP] ページに表示されます。

[PPP/MLP] ポリシー ページ

[PPP/MLP] ページは、ルータの PPP 接続を作成、編集、および削除する場合に使用します。詳細については、 PPP 接続の定義 （92 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[インターフェイス（Interfaces）] > [設定（Settings）] > [PPP/MLP]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータインターフェイス（Router Interfaces）] > [設定（Settings）] > [PPP/MLP]** を選択します。[PPP/MLP] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- Cisco IOS ルータでの PPP （90 ページ）
- テーブル カラムおよびカラム見出しの機能
- テーブルのフィルタリング

フィールド リファレンス

表 *30 : [PPP/MLP]* ページ

要素	説明
インターフェイス（Interface）	PPP/MLP 用に設定されているインターフェイス。
認証	PPP 接続で使用される認証タイプ。
許可	PPP 接続での AAA 認可に使用される方式リスト。
マルチリンク	この PPP 接続で Multilink PPP（MLP; マルチリンク PPP）がイネーブルになるかどうかを示します。
エンドポイント（Endpoint）	ピアと MLP の使用をネゴシエートするときに使用するデフォルトのエンドポイント識別子のタイプ。
Multiclass	この PPP 接続で Multiclass Multilink PPP（MCMP; マルチクラス マルチリンク PPP）機能がイネーブルになるかどうかを示します。
グループ	物理リンクが制限されているマルチリンク グループ インターフェイスの番号。
Interleave	この PPP 接続で PPP マルチリンク インターリーブ機能がイネーブルになるかどうかを示します。
[追加（Add）] ボタン	[PPP] ダイアログボックス （98 ページ）が開きます。ここから、PPP 接続の認証設定およびマルチリンク設定を定義できます。
[編集（Edit）] ボタン	[PPP] ダイアログボックス （98 ページ）が開きます。ここから、選択した PPP 接続を編集できます。
[削除（Delete）] ボタン	選択した PPP 接続をテーブルから削除します。

[PPP] ダイアログボックス

[PPP] ダイアログボックスは、ルータで PPP 接続を設定する場合に使用します。PPP 接続を設定した場合は、マルチリンク パラメータを実行および定義する認証および認可のタイプを定義できます。

ナビゲーション パス

に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

-

フィールド リファレンス

表 *31 : [PPP]* ダイアログボックス

要素	説明
インターフェイス（Interface）	PPP カプセル化がイネーブルになるインターフェイス。インターフェイスまたはインターフェイスロールの名前を入力するか、[選択（Select）]をクリックしてインターフェイスまたはインターフェイスロールを選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）]ボタンをクリックして作成します。 次のインターフェイス タイプが PPP をサポートしています。 • Async • Group-Async • シリアル • HSSI（High-Speed Serial Interface） • ダイヤラ • [BRI]、[PRI]（ISDN） • Virtual template • マルチリンク 次の要素には、PPP を定義できません。 • サブインターフェイス。 • フレーム リレー カプセル化のあるシリアル インターフェイス。 • イーサネットまたはトンネル タイプとして定義された仮想テンプレート インターフェイス（シリアルがサポートされます）。 （注） インターフェイスごとに PPP 接続を 1 つだけ定義できます。 （注） 802.1x ポリシーでも使用されている仮想テンプレートに PPP を定義した場合は、展開に失敗することがあります。を参照してください。
[PPP] タブ	PPP 接続で実行する認証および認可のタイプを定義します。[PPP] ダイアログボックス - [PPP] タブ （100 ページ）を参照してください。
[MLP] タブ	Multilink PPP（MLP; マルチリンク PPP）を使用して、複数の論理データ リンクで一連のデータグラムを分割し、再結合する方法を定義します。を参照してください。 デバイスがこの設定をサポートしていない場合には、このタブはグレーになり、開くことができません。

[PPP] ダイアログボックス - [PPP] タブ

[PPP] ダイアログボックスの [PPP] タブは、PPP 接続で実行する認証および認可のタイプを定義する場合に使用します。

ナビゲーション パス

[PPP] ダイアログボックス （98 ページ）に移動し、[PPP] タブをクリックします。

関連項目

- [PPP] ダイアログボックス - [MLP] タブ （103 ページ）

フィールド リファレンス

表 32 : [PPP] ダイアログボックス - [PPP] タブ

要素	説明
認証設定	
PPP のカプセル化	選択されている場合、選択したインターフェイスではPPPカプセル化がイネーブルになります。このフィールドは読み取り専用です。
プロトコル	使用する認証プロトコル。 • [CHAP]：チャレンジ ハンドシェイク認証プロトコル。 • [PAP]：パスワード認証プロトコル。 • [MS-CHAP]：Microsoft バージョンの CHAP のバージョン 1（RFC 2433）。 • [MS-CHAP-2]：Microsoft バージョンの CHAP のバージョン 2（RFC 2759）。 • [EAP]：拡張認証プロトコル。 必要に応じて 1 つ以上の認証プロトコルを選択できます。

要素	説明
オプション	使用する認証オプション。 • [Call In]：選択されている場合、着信コールで認証が実行されます。 • [Call Out]：選択されている場合、発信コールで認証が実行されます。 • [Call Back]：選択されている場合、コールバックで認証が実行されます。 • [One Time]：選択されている場合、認証にワンタイム パスワードが使用されます。ワンタイム パスワードは、各パスワードが 1 度しか使用されないため、セキュリティ強度が高いと考えられています。選択解除されている場合、ワンタイム パスワードは使用されません。 （注） ワンタイム パスワードを使用するには、AAA 認証をイネーブルにする必要があります。[AAA] ポリシー ページを参照してください。CHAP ではワンタイム パスワードを使用できません。 • [Optional]：選択されている場合、Packet Data Serving Node（PDSN; パケット データ サービス ノード）設定のモバイル ステーションが、CHAP または PAP を使用せずに、Simple IP サービスおよび Mobile IP サービスを受信できます。 選択解除されている場合、モバイル ステーションは、CHAP または PAP を使用して、Simple IP サービスおよび Mobile IP サービスを受信する必要があります。

要素	説明
Authenticate Using	PPP 接続の AAA 認証設定。 • [PPP Default List]：PPP のユーザを認証するときに問い合わせるデフォルトの方式リストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（最大4つ）の名前を[優先順位付けされた方式リスト（Prioritized Method List）]フィールドに入力するか、または[選択（Select）]をクリックして目的のオブジェクトを選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してユーザの認証を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 **ヒント** 1 つの PPP 接続のデフォルト リストを作成したあと、そのリストをこのデバイスの他の PPP 接続にも使用できます。 • [Prioritized Method List]：この PPP 接続だけのユーザを認証するときに問い合わせる一連の方式リストを定義します。 **（注）** ルータ上のローカルデータベースを使用して認証を実行するには、このフィールドを空白のままにします。
PAP 認証設定	
ユーザー名	PAP 認証要求で送信するユーザ名。ユーザ名は、大文字と小文字が区別されます。
パスワード	PAP 認証要求で送信するパスワード。[Confirm] フィールドにパスワードを再入力します。パスワードには、1 ～ 25 文字の大文字と小文字の英数字を使用できます。パスワードは大文字と小文字が区別されます。 ピアがルータに PAP を使用して自己認証するように要求すると、ユーザ名およびパスワードが送信されます。
Encrypted Password	選択されている場合、これは入力したパスワードがすでに暗号化されていることを示します。 選択解除されている場合、これは入力したパスワードがクリア テキストであることを示します。
CHAP 認証設定	

要素	説明
ホストネーム	デフォルトでは、ルータは自身のホスト名を使用して、ピアに対して自身の身元を明らかにします。必要に応じて、別のホスト名をすべての CHAP チャレンジおよびレスポンスに使用するホスト名として入力できます。たとえば、このフィールドを使用して、ロータリー グループのすべてのルータに共通のエイリアスを指定します。
秘密（Secret）	不明なピアから受け取った CHAP チャレンジのレスポンス値を計算するのに使用されるシークレット。[Confirm] フィールドにシークレットをもう一度入力します。
Encrypted Secret	選択されている場合、これは入力したパスワードがすでに暗号化されていることを示します。選択解除されている場合、これは入力したパスワードがクリア テキストであることを示します。
認可設定	
Authorize Using	PPP 接続の AAA 認可設定。 • [AAAポリシーデフォルトリスト（AAA Policy Default List）]：デバイスの AAA ポリシーで定義されているデフォルトの認証方式リストを使用します。[AAA] ポリシー ページを参照してください。 • [Prioritized Method List]：ユーザを認可する場合に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（最大 4 つ）の名前を入力するか、[選択（Select）] をクリックして選択します。上向きおよび下向き矢印を使用して、選択したサーバー グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してユーザの認可を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 （注） ルータ上のローカルデータベースを使用して認可を実行するには、このフィールドを空白のままにします。

[PPP] ダイアログボックス - [MLP] タブ

[PPP] ダイアログボックスの [MLP] タブは、選択した PPP 接続の Multilink PPP（MLP; マルチリンク PPP）パラメータを定義する場合に使用します。

ナビゲーション パス

[PPP] ダイアログボックス （98 ページ）に移動し、[MLP] タブをクリックします。

関連項目

- [PPP] ダイアログボックス （98 ページ）

フィールド リファレンス

表 *33 : [PPP]* ダイアログボックス - *[MLP]* タブ

要素	説明
Enable Multilink PPP (MLP)	選択されている場合、この PPP 接続で MLP がイネーブルになります。 選択解除されている場合、MLP がディセーブルになります。
Allow Multiple Data Classes	選択されている場合、MLP バンドルで複数のデータ クラスがイネーブルになります。遅延に影響されやすいトラフィックがクラス 1 に配置され、インターリーブはできますが、フラグメント化はできなくなります。通常のデータ トラフィックはクラス 0 に配置され、通常のマルチリンク パケットと同じく、フラグメント化の対象となります。 選択解除されている場合、すべてのトラフィックがフラグメント化の対象となります。
Enable Interleaving of Packets Among Fragments of Larger Packets	選択されている場合、MLP バンドルで大きなパケットのフラグメントに対してパケットのインターリーブがイネーブルになります。 （注） フラグメント遅延を定義せずにインターリーブをイネーブルにした場合は、デフォルトの遅延である 30 秒が設定されます。この値は、Security Manager またはデバイス設定に表示されません。 選択解除されている場合、インターリーブがディセーブルになります。 （注） シリアルインターフェイスは、インターリーブをサポートしません。

要素	説明
Multilink Group	シリアル インターフェイス、Group-Async インターフェイス、およびマルチリンク インターフェイスにだけ適用されます。 物理リンクは、選択したマルチリンク グループインターフェイスに制限されます。マルチリンクインターフェイスまたはインターフェイスロールの名前を入力するか、[選択（Select）] をクリックして選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 このオプションは、一般的に静的な専用線環境で、デバイスのシリアル回線が接続されているリモートシステムが事前にわかっている場合に使用されます。 このオプションは実質的に特定のインターフェイスを特定のユーザ専用にするもので、これはそのユーザが接続されていない場合でも同じです。リンクの反対側のピアが別のバンドルに参加しようとした場合は、接続が重大になります。
Maximum Fragment Delay	MLP バンドルでフラグメントを送信するために必要な最大期間。有効値の範囲は 1 ～ 1000 ミリ秒です。 フラグメントサイズは、定義されたフラグメント遅延およびリンクの帯域幅によって決まります。 （注）　シリアル インターフェイスは、この機能をサポートしません。

要素	説明
エンドポイントタイプ	MLP バンドルでパケットを送信するときにルータが使用する識別子。 • [null]：エンドポイント識別子を使用せずに、ネゴシエーションが実施されます（CLI コマンドが生成されません）。 • [Hostname]：ルータのホスト名。このオプションは、複数のルータが認証に同じユーザ名を使用しているものの、各ルータのホスト名が異なるときに便利です。 • [IP]：定義済みの IP アドレス。ネットワーク/ホストオブジェクトのアドレスまたは名前を入力するか、[選択（Select）] をクリックして選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 • [MAC]：特定のインターフェイスの MAC アドレス。インターフェイスまたはインターフェイスロールの名前を入力するか、[選択（Select）] をクリックして選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 • [None]：エンドポイント識別子を使用せずに、ネゴシエーションが実施されます（関連する CLI コマンドは生成されますが、エンドポイント識別子は提供されません）。このオプションは、ルータの接続先であるピアが正常に動作せず、エンドポイント識別子が正しく処理されないときに役立ちます。 • [Phone]：E.164 準拠の電話番号。表示されたフィールドに番号を入力します。 • [String]：文字列。表示されたフィールドに文字列を入力します。 デフォルトのエンドポイント識別子は、グローバルに設定したホスト名か、または（使用する認証プロトコルに応じて）PAP ユーザ名か CHAP ホスト名となります。ただし、[PPP] タブで対応する値を設定した場合にかぎります。
MRRU Local Peer	ローカル ピアの Maximum Receive Reconstructed Unit（MRRU）値。この値は、ローカル ルータが受信できる最大パケット サイズとなります。 有効値の範囲は 128 ～ 16384 バイトです。デフォルトはマルチリンク グループ インターフェイスでは最大伝送単位（MTU）で、それ以外のインターフェイスでは 1524 バイトとなります。
MRRU Remote Peer	リモート ピアの Maximum Receive Reconstructed Unit（MRRU）値。この値は、リモート ルータが受信できる最大パケット サイズとなります。 有効値の範囲は 128 ～ 16384 バイトです。デフォルトは 1524 バイトです。

要素	説明
Maximum FIFO Queue Size	バンドルが First-In, First-Out（FIFO; ファーストイン ファーストアウト）キューを使用する場合の最大キュー深度。有効値の範囲は 2 ～ 255 パケットです。デフォルトは 8 です。
Maximum QoS Queue Size	バンドルが非 FIFO キューを使用する場合の最大キュー深度。有効値の範囲は 2 ～ 255 パケットです。デフォルトは 2 です。

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。