



インターフェイス / 接続の編集

このウィンドウには、ルータのインターフェイスと接続が表示されます。また、このウィンドウで接続の追加、編集、削除、有効化、および無効化も行えます。

追加

設定されていない物理インターフェイスを選択して [追加] をクリックすると、メニューにはそのインターフェイスに接続を追加するためのオプションが表示されます。新しいループバックまたはトンネル インターフェイスを作成するには、[追加] をクリックします。ルータ上の Cisco IOS イメージで仮想テンプレート インターフェイス (VTI) がサポートされる場合は、コンテキストメニューに VTI を追加するためのオプションが表示されます。ルータにスイッチ ポートがある場合は、新しい VLAN を追加できます。

インターフェイスを再設定する必要がある場合に、[追加] をクリックしても [ループバック] と [トンネル] 以外のオプションが表示されなければ、インターフェイスを選択して [削除] をクリックしてください。その種類のインターフェイスに利用できるすべての接続タイプが [追加] メニューに表示されます。インターフェイスに利用できる設定については、「[使用可能なインターフェイス設定](#)」をクリックしてください。

編集

インターフェイスを選択して [編集] をクリックすると、ダイアログ ボックスが表示されます。選択したインターフェイスがサポートされている設定済みのインターフェイスであり、スイッチ ポートでない場合は、次のタブが表示されません。

- [接続] タブ
- [関連付け] タブ
- [NAT] タブ
- [アプリケーション サービス] タブ
- [全般] タブ

選択したインターフェイスがサポートされていない場合は、このダイアログ ボックスに [接続] タブは表示されません。スイッチ ポートを選択した場合は、[スイッチ ポートの編集] ダイアログ ボックスが表示されます。サポートされているが設定されていないインターフェイスを選択した場合、[編集] ボタンは無効になります。

削除

接続を選択して [削除] をクリックすると、この接続の関連付けがダイアログ ボックスに表示され、接続とともに関連付けを削除するかどうかを確認するメッセージが表示されます。接続だけを削除することも、接続とその関連付けをすべて削除することもできます。

要約

このボタンをクリックすると、接続に関する詳細は表示されず、IP アドレス、タイプ、スロット、ステータス、および説明だけが表示されます。

詳細

このボタンをクリックすると、次に説明する [インターフェイスの詳細] エリアが表示されます。インターフェイスの詳細は、デフォルトで表示されます。

有効 / 無効

選択したインターフェイスまたは接続が停止している場合は、このボタンは [有効] ボタンとして表示されます。[有効] ボタンをクリックすると、選択したインターフェイスまたは接続が起動します。選択したインターフェイスまたは接続が起動している場合は、このボタンは [無効] ボタンとして表示されます。[無効] ボタンをクリックすると、インターフェイスまたは接続を管理目的でシャットダウンできます。このボタンは、設定がルータに配信されていないインターフェイスに対しては使用できません。

接続のテスト

選択した接続をテストする場合にクリックします。ダイアログ ボックスが表示され、この接続を使用して ping を実行するリモート ホストを指定できます。ping を実行すると、このダイアログ ボックスにテスト結果（合格または不合格）が表示されます。テストが失敗した場合は、考えられる原因と問題の解決手順が表示されます。

インターフェイス リスト

物理インターフェイスと、それらのインターフェイスに設定されている論理接続が表示されます。

インターフェイス

このカラムには、物理インターフェイスと論理インターフェイスの名前が表示されます。物理インターフェイスに対して論理インターフェイスが設定されている場合は、物理インターフェイスの下に論理インターフェイスが表示されます。

Cisco Router and Security Device Manager (Cisco CP) が Cisco 7000 ファミリー ルータ上で実行されている場合は、イーサネット インターフェイスと Fast Ethernet インターフェイス上にしか接続を作成できません。

IP アドレス

このカラムには、次のいずれかのタイプの IP アドレスが表示されます。

- インターフェイスの設定済み IP アドレス。

- [DHCP クライアント] — インターフェイスは、DHCP (Dynamic Host Configuration Protocol) サーバから IP アドレスを受け取ります。
- [ネゴシエート済み IP アドレス] — インターフェイスはリモート デバイスとのネゴシエーションによって IP アドレスを受け取ります。
- [IP アンナナバード] — ルータ、および LAN 上のデバイスに対してサービス プロバイダから提供された IP アドレス プールのうちの 1 つが、ルータに使用されます。
- [該当なし] — このインターフェイス タイプには IP アドレスを割り当てることができません。

タイプ

このカラムには、イーサネット、シリアル、ATM などのインターフェイス タイプが表示されます。

スロット

インターフェイスがインストールされているルータの物理スロットの番号が表示されます。Cisco CP が Cisco 1710 ルータで実行されている場合、このフィールドは空になります。

ステータス

このカラムには、このインターフェイスが稼働しているか、または停止しているかを示すアイコンが表示されます。緑の上向き矢印のアイコンは、インターフェイスが稼働していることを示します。赤い下向き矢印のアイコンは、インターフェイスが停止していることを示します。

説明

このカラムには、この接続に関する説明が表示されます。

インターフェイスの詳細

ウィンドウのこのエリアには、[インターフェイス リスト] で選択したインターフェイスの関連付けの詳細と、接続の詳細（該当する場合）が表示されます。関連付けの詳細には、ネットワーク アドレス変換（NAT）、アクセス ルール、インスペクション ルール、IPSec ポリシー、Easy VPN 設定などの情報が含まれます。接続の詳細には、IP アドレス、カプセル化タイプ、DHCP オプションなどの情報が含まれます。

項目名

IP アドレス、サブネット マスク、IPSec ポリシーなどの設定項目の名前です。このカラムに表示される実際の項目は、選択したインターフェイスのタイプによって異なります。

項目値

名前付きの項目に値が設定されている場合は、その値がこのカラムに表示されません。

インターフェイスまたは接続が読み取り専用になる原因

設定済みのインターフェイスまたはサブインターフェイスを Cisco CP で変更できない場合があります。その原因は多数考えられます。

- 設定済みのシリアル インターフェイスまたはサブインターフェイスが [インターフェイス リスト] に読み取り専用で表示される原因については、ヘルプ トピック「[シリアル インターフェイスまたはシリアル サブインターフェイスの設定が読み取り専用になる原因](#)」を参照してください。
- 設定済みの ATM インターフェイスまたはサブインターフェイスが [インターフェイス リスト] に読み取り専用で表示される原因については、ヘルプ トピック「[ATM インターフェイスまたは ATM サブインターフェイスの設定が読み取り専用になる原因](#)」を参照してください。
- 設定済みのイーサネット LAN または WAN インターフェイスが [インターフェイス リスト] に読み取り専用で表示される原因については、ヘルプ トピック「[イーサネット インターフェイスの設定が読み取り専用になる原因](#)」を参照してください。

■ 接続 : IRB のイーサネット

- 設定済みの ISDN BRI インターフェイスが [インターフェイス リスト] に読み取り専用で表示される原因については、ヘルプ トピック「[ISDN BRI インターフェイスの設定が読み取り専用になる原因](#)」を参照してください。

接続 : IRB のイーサネット

[設定] リストから [IRB のイーサネット] を選択した場合、このダイアログ ボックスには次のフィールドが表示されます。

現在のブリッジ グループ / 関連付けられている BVI

これらの読み取り専用フィールドには、現在のブリッジ グループの値と、現在のブリッジ グループの仮想インターフェイス (BVI) 名が表示されます。

新しいブリッジ グループの作成 / 既存のブリッジ グループとの結合

このインターフェイスを新しいブリッジ グループのメンバにするかどうか、または既存のブリッジ グループに結合するかどうかを選択します。新しいブリッジ グループを作成する場合は、1 ~ 255 の範囲の数字を入力します。インターフェイスを既存のブリッジ グループに結合する場合は、すでにそのグループに属している BVI インターフェイスを選択します。

IP アドレス

IP アドレスおよびサブネット マスクを各フィールドに入力します。

動的 DNS

動的 DNS を有効にすると、WAN インターフェイスの IP アドレスが変更されるたびに、DNS サーバが自動更新されます。



(注)

この機能は、使用するルータの Cisco IOS リリースによってサポートされる場合のみ表示されます。

使用する動的 DNS 方式を選択するには、次のいずれかを実行します。

- 既存の動的 DNS 方式の名前を入力します。
[設定] > [ルータ] > [ルータ (詳細設定)] > [動的 DNS 方式] のリストに表示される名前を、[動的 DNS 方式] フィールドに正確に入力します。
- リストから既存の動的 DNS 方式を選択します。
ドロップダウン メニューをクリックして、既存の方式を選択します。既存の動的 DNS 方式が一覧表示されたウィンドウが開きます。このメニュー項目は、既存の動的 DNS 方式が存在する場合のみ有効です。
- 新規の動的 DNS 方式を作成します。
ドロップダウン メニューをクリックして、動的 DNS 方式の新規作成を選択します。

関連付けられた動的 DNS 方式をインターフェイスからクリアするには、ドロップダウン メニューから [なし] を選択します。

接続 : ルーティングのイーサネット

[設定] リストから [ルーティングのイーサネット] を選択した場合、このダイアログ ボックスには次のフィールドが表示されます。

IP アドレス

[IP アドレス] フィールドに IP アドレスとサブネット マスクを入力します。このアドレスは、このインターフェイスからのアウトバウンド トラフィックの送信元 IP アドレスとなり、このインターフェイスに接続されているホストに送信されるトラフィックの宛先 IP アドレスとなります。

DHCP リレー

ルータを DHCP リレーとして使用する場合にクリックします。DHCP リレーとして機能するデバイスは、DHCP 要求を DHCP サーバに転送します。デバイスは、IP アドレスのダイナミックな割り当てが必要になると、DHCP 要求をブロードキャストします。DHCP サーバはこの要求に応じて IP アドレスを返信します。サブネットワークごとに、最大 1 台の DHCP リレーまたは 1 台の DHCP サーバを配置できます。



(注) 複数のリモート DHCP サーバの IP アドレスを持つ DHCP リレーとしてルータを設定した場合、これらのフィールドは無効になります。

リモート DHCP サーバの IP アドレス

LAN 上のデバイスにアドレスを指定する DHCP サーバの IP アドレスを入力します。

動的 DNS

動的 DNS を有効にすると、WAN インターフェイスの IP アドレスが変更されるたびに、DNS サーバが自動更新されます。

**(注)**

この機能は、使用するルータの Cisco IOS リリースによってサポートされる場合のみ表示されます。

使用する動的 DNS 方式を選択するには、次のいずれかを実行します。

- 既存の動的 DNS 方式の名前を入力します。
[設定] > [ルータ] > [ルータ (詳細設定)] > [動的 DNS 方式] のリストに表示される名前を、[動的 DNS 方式] フィールドに正確に入力します。
- リストから既存の動的 DNS 方式を選択します。
ドロップダウンメニューをクリックして、既存の方式を選択します。既存の動的 DNS 方式が一覧表示されたウィンドウが開きます。このメニュー項目は、既存の動的 DNS 方式が存在する場合のみ有効です。
- 新規の動的 DNS 方式を作成します。
ドロップダウンメニューをクリックして、動的 DNS 方式の新規作成を選択します。

関連付けられた動的 DNS 方式をインターフェイスからクリアするには、ドロップダウンメニューから [なし] を選択します。

編集 動的 DNS 方式

このウィンドウでは、WAN インターフェイスに関連付ける動的 DNS 方式を選択できます。

既存の動的 DNS 方式のリストには、各メソッドの名前、および関連付けられたパラメータが表示されます。リストから方式を選択して [OK] をクリックすると、この方式が WAN インターフェイスに関連付けられます。

動的 DNS 方式を追加、編集、または削除するには、[設定] > [ルータ] > [ルータ (詳細設定)] > [動的 DNS 方式] の順に選択します。

追加 動的 DNS 方式

このウィンドウでは、動的 DNS 方式を追加できます。方式の種類（HTTP または IETF）を選択して、これを設定します。

HTTP

HTTP は、関連付けられたインターフェイスの IP アドレスの変更によって、DNS サービス プロバイダを更新する動的 DNS 方式です。

サーバ

HTTP を使用する場合、DNS サービス プロバイダのドメイン アドレスをドロップダウンメニューから選択します。

ユーザ名

HTTP を使用する場合、DNS サービス プロバイダへのアクセスに使用するユーザ名を入力します。

パスワード

HTTP を使用する場合、DNS サービス プロバイダへのアクセスに使用するパスワードを入力します。

IETF

IETF は、関連付けられたインターフェイスの IP アドレスの変更によって、DNS サーバを更新する動的 DNS 方式です。

DNS サーバ

IETF を使用する場合に、[設定] > [ルータ] > [DNS] でルータの DNS サーバを設定していないときは、DNS サーバの IP アドレスを入力します。

ホスト名

[設定] > [ルータ] > [ルータ オプション] > [編集] > [ホスト] でホスト名を設定していない場合、または設定済みのホスト名を上書きする場合は、任意のホスト名を入力します。インターフェイスの IP アドレスの更新時には、動的 DNS 方式によって、インターフェイスの新しい IP アドレスとともにこのホスト名が送信されます。

ドメイン名

[設定] > [ルータ] > [ルータ オプション] > [編集] > [ドメイン] でドメイン名を設定していない場合、または設定済みのドメイン名を上書きする場合は、任意のドメイン名を入力します。インターフェイスの IP アドレスの更新時には、動的 DNS 方式によって、インターフェイスの新しい IP アドレスとともにこのドメイン名が送信されます。

ワイヤレス

ルータでワイヤレス インターフェイスを使用している場合、このタブからワイヤレス アプリケーションを起動できます。[ツール] > [ワイヤレス アプリケーションの起動] の順に選択して、[ツール] メニューからワイヤレス アプリケーションを起動することもできます。

関連付け

このウィンドウでは、インターフェイスとルールまたは VPN 接続の関連付けを表示、作成、編集、または削除できます。

インターフェイス

[インターフェイスと接続] ウィンドウで選択したインターフェイスの名前です。

ゾーン

対象のインターフェイスが**セキュリティ ゾーン**のメンバである場合、そのゾーンの名前がこのフィールドに表示されます。対象のインターフェイスをセキュリティ ゾーンに追加する場合は、フィールドの右にあるボタンをクリックして [ゾーンの選択] を選択し、表示されるダイアログでゾーンを指定します。新しいゾーンを作成する必要がある場合は、[ゾーンの作成] を選択し、表示されるダイアログにゾーンの名前を入力して、[OK] をクリックします。作成したゾーンの名前が [ゾーン] フィールドに表示されます。

アクセス ルール

このインターフェイスに関連付けられているアクセス ルールの名前または番号です。アクセスルールを使用すると、指定した IP アドレスやサービスの条件に一致するトラフィックを許可または拒否できます

インバウンド

このインターフェイス上のインバウンド トラフィックに適用されるアクセス ルールの名前または番号です。ルールを適用する場合は、[...] ボタンをクリックして既存のルールを選択するか、または新しいルールを作成して、そのルールを選択します。

ルールがインターフェイス上のインバウンド トラフィックに適用されると、トラフィックがルータに到達する前にルールによるフィルタがかけられます。ルールが拒否したパケットは廃棄され、別のインターフェイスにもルーティングされません。インターフェイスのインバウンド方向にルールを適用すると、ルータに接続されている内部ネットワークへのインバウンド トラフィックの到達を防止するだけでなく、ローカル ルータによる他のネットワークへのインバウンド トラフィックのルーティングを防止することになります。

アウトバウンド

このインターフェイス上のアウトバウンド トラフィックに適用されるアクセス ルールの名前または番号です。ルールを適用する場合は、[...] ボタンをクリックして既存のルールを選択するか、または新しいルールを作成して、そのルールを選択します。

ルールがインターフェイス上のアウトバウンド トラフィックに適用されると、トラフィックがルータに到達してルータから出る前に、ルールによるフィルタがかけられます。ルールが拒否したパケットは、インターフェイスから出る前に廃棄されます。

インスペクション ルール

このインターフェイスに関連付けられるインスペクション ルールの名前です。インスペクション ルールを使用すると、ファイアウォールに一時的なホールが作成されます。これにより、ファイアウォール内部で特定タイプのセッションを開始したホストは、同じタイプのリターン トラフィックを受信できるようになります。

インバウンド

このインターフェイス上のインバウンド トラフィックに適用されるインスペクションルールの名前または番号です。インバウンドルールを適用するには、[インバウンド] ドロップダウンメニューをクリックして、任意のルールを選択します。

アウトバウンド

このインターフェイス上のアウトバウンド トラフィックに適用されるインスペクションルールの名前または番号です。アウトバウンドルールを適用するには、[アウトバウンド] ドロップダウンメニューをクリックして、任意のルールを選択します。

VPN

VPN は、組織によって制御されていない回線上で転送されるトラフィックを保護します。選択したインターフェイスに IPsec ポリシーを関連付けることによって、そのインターフェイスを VPN で使用できます。

IPsec ポリシー

このインターフェイスに関連付けられる設定済みの IPsec ポリシーです。インターフェイスに IPsec ポリシーを関連付けるには、リストからポリシーを選択します。



(注)

1 つのインターフェイスに関連付けられる IPsec ポリシーは 1 つだけです。



(注)

GRE over IPsec トンネルを作成するには、まずトンネル インターフェイスにポリシーを関連付けます。次に、そのポリシーをトンネルの送信元インターフェイスに関連付ける必要があります。たとえば、送信元インターフェイスが Serial0/0 である Tunnel3 にポリシーを関連付けるには、まず [インターフェイスと接続] ウィンドウで Tunnel3 を選択して [編集] をクリックし、Tunnel3 にポリシーを関連付けて [OK] をクリックします。次に、Serial0/0 インターフェイスを選択して、同じポリシーを関連付けます。

EzVPN

インターフェイスが Easy VPN 接続で使用される場合、その接続の名前がここに表示されます。



(注)

インターフェイスは、VPN（仮想プライベート ネットワーク）接続と Easy VPN 接続の両方で使用することはできません。

関連付けの変更

インターフェイスの関連付けプロパティを変更すると、その変更内容は [インターフェイス / 接続の編集] ウィンドウの下の部分に反映されます。たとえば、インターフェイスに IPSec ポリシーを関連付けると、その IPSec ポリシーの名前がウィンドウの下の部分に表示されます。関連付けを削除すると、[項目値] カラム内の値が <なし> に変わります。

NAT

このインターフェイスを NAT 設定で使用する場合は、内部インターフェイスまたは外部インターフェイスとして指定する必要があります。NAT を適用するトラフィックの方向を選択します。インターフェイスをルータの LAN に接続する場合は、[内部] を選択します。インターフェイスをインターネットまたは組織の WAN に接続する場合は、[外部] を選択します。NAT 設定で使用できないインターフェイス（論理インターフェイスなど）を選択した場合、このフィールドは無効になり、「サポート外」という値が表示されます。

スイッチ ポートの編集

このウィンドウでは、イーサネット スイッチ ポートの VLAN 情報を編集できます。

モード グループ

このイーサネット スイッチ ポートを介して伝送する VLAN 情報のタイプを選択します。[アクセス] を選択すると、スイッチ ポートは特定の VLAN 番号宛てのデータだけを転送します。[トランク] を選択すると、スイッチ ポートはその VLAN データ自体を含むすべての VLAN 宛てのデータを転送します。[トランク] は、複数の VLAN 内のデバイスに接続する他のネットワーク デバイス（別のスイッチなど）に接続される「トランク」VLAN ポートに対してのみ選択してください。

VLAN

VLAN にスイッチ ポートを割り当てるには、このスイッチ ポートを配置する VLAN の番号を入力します。スイッチ ポートにまだ VLAN が割り当てられていない場合、このフィールドには、デフォルト値である VLAN 1 が表示されます。VLAN ID に対応する新しい VLAN インターフェイスを作成するには、その VLAN ID をこのフィールドに入力して、[VLAN をインターフェイス リストに表示する] チェック ボックスを選択します。

VLAN をインターフェイス リスト チェック ボックスに表示する

[VLAN] フィールドで指定した VLAN ID を持つ新しい VLAN を作成する場合には選択します。

スタック パートナー

スタック パートナーとして使用するスイッチ モジュールを選択します。デバイスに複数のスイッチ モジュールが搭載されている場合は、これらのモジュールを他のスタック パートナーより先にスタックする必要があります。

ブリッジ グループ番号

このスイッチ ポートで、ワイヤレス ネットワークとのブリッジの一部を設定する場合は、既存のブリッジ グループの番号を入力します。

速度

スイッチ ポートの接続先のネットワークに一致する速度を選択します。または、[auto] を選択して、速度が自動的に最適値に設定されることを許可します。

duplex

[full]、[half]、または [auto] を選択して、スイッチ ポートの接続先のネットワークに一致するように、自動的に二重転送を設定することを許可します。

[速度] が [auto] に設定されている場合、[duplex] は無効になっています。

インライン パワー

スイッチ ポートでインライン パワー供給がサポートされている場合には、[インライン パワー] ドロップダウン リストが表示されます。次のいずれかの値を選択します。

- [auto] — 自動的にインライン デバイスを検出して電力を供給します。
- [never] — インライン パワーを使用しません。

アプリケーション サービス

このウィンドウでは、QoS ポリシー、およびアプリケーションとプロトコルの監視を、選択したインターフェイスに関連付けることができます。

QoS

QoS ポリシーをインバウンド方向でインターフェイスに関連付けるには、[インバウンド] ドロップダウンメニューから QoS ポリシーを選択します。

QoS ポリシーをアウトバウンド方向でインターフェイスに関連付けるには、[アウトバウンド] ドロップダウンメニューから QoS ポリシーを選択します。

インターフェイスの QoS 統計情報は、[監視] > [ルータ] > [QoS ステータス] の順に選択することにより監視できます。

Netflow

Netflow 統計をインバウンド方向でインターフェイスに関連付けるには、[インバウンド] チェックボックスを選択します。

Netflow 統計をアウトバウンド方向でインターフェイスに関連付けるには、[アウトバウンド] チェックボックスを選択します。

インターフェイスの Netflow 統計情報は、[監視] > [ルータ] > [インターフェイス ステータス] の順に選択することにより監視できます。Netflow の上位トーカーと上位プロトコルは、[監視] > [ルータ] > [トラフィック ステータス] > [上位 N トラフィック フロー] の順に選択することにより監視できます。

NBAR

Network-Based Application Recognition (NBAR) をインターフェイスに関連付けるには、[NBAR プロトコル] チェックボックスを選択します。

インターフェイスの NBAR 統計情報は、[監視] > [ルータ] > [トラフィック ステータス] > [アプリケーション/プロトコル トラフィック] の順に選択することにより監視できます。

全般

このウィンドウには、全般のセキュリティ設定が表示されます。設定の名前や説明の横にあるチェック ボックスを選択または選択解除することによって、その設定を有効または無効にできます。セキュリティ監査機能によって無効にされた特定のプロパティを再度有効にする必要がある場合は、このウィンドウで有効にできます。このウィンドウには次のプロパティが表示されます。

説明

このフィールドには、インターフェイス設定についての簡単な説明を入力できます。入力した説明は、[インターフェイス / 接続の編集] ウィンドウに表示されます。たとえば、「Accounting」、「Test Net 5」といった説明を入力しておくと、他の Cisco CP ユーザが設定の目的を把握しやすくなります。

IP ダイレクトブロードキャスト

IP ダイレクトブロードキャストは、送信側のマシンが直接接続していないサブネットのブロードキャスト アドレスに送信されるデータグラムです。ダイレクトブロードキャストは、送信先サブネットに到達するまでユニキャスト パケットとして伝送され、送信先サブネットでリンク層ブロードキャストに変換されます。IP のアドレス指定アーキテクチャの性質により、ダイレクトブロードキャストを最終的に識別できるのは、チェーン内の最後のルータ、つまり送信先サブネットに直接接続されているルータだけです。ダイレクトブロードキャストが正当な目的で使用される場合もありますが、そのような使用法は金融サービス業界以外では一般的ではありません。

IP ダイレクトブロードキャストは、よく知られている「smurf」というサービス拒否攻撃で悪用され、他の同じような攻撃でも悪用される場合があります。「smurf」攻撃では、攻撃者が偽装された送信元アドレスからダイレクトブロードキャストアドレスに ICMP エコー要求を送信します。その結果、送信先サブネット上のすべてのホストが偽装された送信元アドレスに応答を送信します。このような要求を連続的に送信することによって、攻撃者は大量の応答を生成し、アドレスが偽装されたホストを完全な過負荷状態にすることができます。

IP ダイレクト ブロードキャストを無効にすると、そのインターフェイスでリンク層ブロードキャストに大量に変換されるはずのダイレクト ブロードキャストが廃棄されます。

IP プロキシ ARP

ARP は、IP アドレスを MAC アドレスに変換するために使用されます。通常、ARP は単一の LAN に限定され、ルータは ARP 要求のためのプロキシとして機能できます。これにより、複数の LAN セグメントにまたがって ARP 要求を送信できるようになります。ただし、これは LAN というセキュリティ防護壁を破ることになるため、プロキシ ARP は同じセキュリティ レベルを持つ 2 つの LAN 間のみに限定して、必要な場合に限って使用してください。

IP ルート キャッシュフロー

このオプションを選択すると、Cisco ISO NetFlow 機能が有効になります。NetFlow では、ルータ上のパケット分布、プロトコル分布、およびデータの現在のフローを確認できます。これらのデータは、偽装 IP アドレス攻撃の送信元を検索する場合など、特定の用途で役立ちます。



(注)

[IP ルート キャッシュフロー] オプションは、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の両方で Netflow を有効にします。インバウンドトラフィックまたはアウトバウンドトラフィックのいずれかで Netflow を有効にするには、[アプリケーション サービス] タブで利用できる [Netflow] オプションを使用します。

IP リダイレクト

ICMP リダイレクト メッセージはエンド ノードに対し、特定の宛先までのパスの一部として、特定のルータを使用するように指示します。正常に機能している IP ネットワークでは、ルータはローカル サブネット上のホストだけにリダイレクトを送信し、エンド ノードはリダイレクトを送信しません。また、リダイレクトが複数のネットワーク ホップを経由して転送されることもありません。し

かし、攻撃者はこうしたルールを無視する可能性があります。ICMP リダイレクトを無効にすると、ネットワークに悪影響を与えることなく、リダイレクト攻撃を排除できます。

IP マスク応答

ICMP マスク応答メッセージは、ネットワーク デバイスがインターネットワーク内の特定のサブネットワークのサブネット マスクを認識する必要がある場合に送信されます。このメッセージは、必要な情報を持っているデバイスによって、情報を要求したデバイスに送信されます。これらのメッセージは、ネットワーク マッピング情報を取得するために攻撃者に悪用される可能性があります。

IP アンリーチャブル

ICMP ホストのアンリーチャブルメッセージは、ルータが、不明なプロトコルを使用する非ブロードキャスト パケットを受信した場合、または宛先アドレスまでのルートがないために最終的な宛先に配信できないパケットを受信した場合に送信されます。これらのメッセージは、ネットワーク マッピング情報を取得するために攻撃者に悪用される可能性があります。

イーサネット設定タイプの選択

このウィンドウは、[インターフェイスと接続] ウィンドウでインターフェイスをクリックし、そのインターフェイスが LAN インターフェイスとして設定されているか、または WAN インターフェイスとして設定されているかを Cisco CP が判断できない場合に表示されます。Cisco CP を使用してインターフェイスを設定する場合は、それを内部インターフェイスか外部インターフェイスのどちらにするかを指定します。Cisco CP はその指定に基づいてコンフィギュレーションファイルにコメントを追加します。CLI (コマンドラインインターフェイス) を使用してインターフェイスを設定した場合は、設定にこのコメントが追加されません。したがって、Cisco CP にはこの情報がわかりません。

インターフェイスを LAN インターフェイスとして指定するには

[LAN] をクリックしてから [OK] をクリックします。Cisco CP によって、インターフェイス設定に \$ETH-LAN\$ というコメント行が追加されます。インターフェイスは LAN ウィザードのウィンドウに表示され、[インターフェイスと接続] ウィンドウでは内部インターフェイスとして表示されます。

インターフェイスを WAN インターフェイスとして指定するには

[WAN] をクリックしてから [OK] をクリックします。Cisco CP によって、インターフェイス設定に \$ETH-WAN\$ というコメント行が追加されます。インターフェイスは WAN ウィザードのウィンドウに表示され、[インターフェイスと接続] ウィンドウでは外部インターフェイスとして表示されます。

接続 : VLAN

このウィンドウでは、VLAN インターフェイスを設定できます。

VLAN ID

新しい VLAN インターフェイスの ID 番号を入力します。VLAN インターフェイスを編集の場合、VLAN ID は変更できません。

[ネイティブ VLAN] チェック ボックス

この VLAN がトランク VLAN ではない場合に選択します。

IP アドレス フィールド

IP アドレスのタイプ

この VLAN インターフェイスにスタティック IP アドレスを指定するか、または IP アドレスを指定しないかを選択します。このフィールドは、[設定] フィールドで [VLAN のみ] が選択されている場合に表示されます。

IP アドレス

VLAN インターフェイスの IP アドレスを入力します。

サブネット マスク

VLAN インターフェイスのサブネット マスクを入力するか、またはスクロール フィールドを使用してサブネット ビット数を指定します。

DHCP リレー

詳細については、「[DHCP リレー](#)」を参照してください。

サブインターフェイス リスト

このウィンドウには、選択したインターフェイスに対して設定されたサブインターフェイスが表示されます。ここでは、設定済みのサブインターフェイスを追加、編集、および削除できます。このウィンドウでは設定済みの各サブインターフェイスに対し、サブインターフェイス ID、VLAN ID、IP アドレスとマスク、および説明（あらかじめ入力した場合）が表示されます。たとえば、ルータに FastEthernet 1 というインターフェイスがあり、サブインターフェイス FastEthernet1.3 および FastEthernet1.5 が設定されている場合は、このウィンドウには次のように表示されます。

```
5          56          56.8.1.1/255.255.255.0
3          67          Bridge No. 77
```

この例では、FastEthernet1.5 はルーティング用に設定され、FastEthernet1.3 は IRB 用に設定されています。



(注)

このウィンドウを表示するには、サブインターフェイスが設定されている物理インターフェイスを選択する必要があります。上記の例の場合は、このウィンドウを表示するには FastEthernet 1 を選択する必要があります。FastEthernet1.3 または FastEthernet1.5 を選択して [編集] をクリックすると、このインターフェイスの情報が表示された編集ダイアログが開きます。

追加 / 編集 / 削除ボタン

これらの各ボタンを使用すると、選択した物理インターフェイスのサブインターフェイスを設定、編集、および削除できます。

BVI インターフェイスの追加 / 編集

このウィンドウでは、ブリッジ グループ仮想インターフェイス (BVI) を追加または編集します。ルータで Dot11Radio インターフェイスを使用している場合、新しいブリッジ グループを作成すると、BVI が自動的に作成されます。それによって、IRB ブリッジがサポートされます。このウィンドウで IP アドレスとサブネット マスクを変更できます。

IP アドレス / サブネット マスク

BVI に指定する IP アドレスとサブネット マスクを入力します。

ループバックインターフェイスの追加 / 編集

このウィンドウでは、選択したインターフェイスにループバック インターフェイスを追加できます。

IP アドレス

ループバック インターフェイスにスタティック IP アドレスを指定するか、または IP アドレスを指定しないかを選択します。

スタティック IP アドレス

[スタティック IP アドレス] を選択した場合は、このフィールドに IP アドレスを入力します。

サブネット マスク

このフィールドにサブネット マスクを入力するか、または右側のフィールドからサブネット ビット数を選択します。サブネット マスクでは、IP アドレスのどのビットを使用してネットワーク アドレスとホスト アドレスを指定するかをルータに指示できます。

接続 : 仮想テンプレートインターフェイス

VTI は、802.1x または VPN 設定の一部として追加または編集できます。VTI の編集時は、[接続] タブに編集可能なフィールドが表示されます。

インターフェイス タイプ

[デフォルト] または [トンネル] を選択します。[トンネル] を選択した場合は、トンネルモードも選択する必要があります。

IP アドレス

[アンナンバード] を選択します。VTI では、[アンナンバード] フィールドで選択した物理インターフェイスの IP アドレスが使用されます。

アンナンバード

このフィールドは、[IP アドレス] フィールドで [アンナンバード] を選択した場合に表示されます。対象の VTI で使用する IP アドレスを持つインターフェイスを選択します。

トンネルモード

[IPSec-IPv4] を選択します。

接続 : イーサネット LAN

このウィンドウでは、LAN インターフェイスとして使用するイーサネット インターフェイスの IP アドレスと DHCP のプロパティを設定します。

IP アドレス

このインターフェイスの IP アドレスを入力します。この IP アドレスについては、サービス プロバイダまたはネットワーク管理者に確認してください。詳細については、「IP アドレスとサブネット マスク」を参照してください。

サブネット マスク

サブネット マスクを入力します。この値については、ネットワーク管理者に確認してください。サブネット マスクを指定すると、IP アドレスのうち、ネットワーク部およびサブネット部を定義するために何ビットが使用されているかをルータが判断できるようになります。

DHCP リレー

ルータを DHCP リレーとして使用する場合にクリックします。DHCP リレーとして機能するデバイスは、DHCP 要求を DHCP サーバに転送します。デバイスは、IP アドレスのダイナミックな割り当てが必要になると、DHCP 要求をブロードキャストします。DHCP サーバはこの要求に応じて IP アドレスを返信します。サブネットワークごとに、最大 1 台の DHCP リレーまたは 1 台の DHCP サーバを配置できます。



(注)

複数のリモート DHCP サーバの IP アドレスを持つ DHCP リレーとしてルータを設定した場合、このボタンは無効になります。

リモート DHCP サーバの IP アドレス

[DHCP リレー] をクリックした場合は、LAN 上のデバイスにアドレスを割り当てる DHCP サーバの IP アドレスを入力します。

接続 : イーサネット WAN

このウィンドウでは、イーサネット WAN 接続を追加できます。

PPPoE カプセル化を有効にする

接続で Point-to-Point Protocol over Ethernet (PPPoE) カプセル化を使用する必要がある場合は、このオプションをクリックします。接続で PPPoE を使用するかどうかについては、サービス プロバイダに確認してください。PPPoE 接続を設定すると、ダイヤラ インターフェイスが自動的に作成されます。

IP アドレス

次のいずれかの IP アドレス タイプを選択し、表示されるフィールドに情報を入力します。イーサネット接続で PPPoE を使用しない場合は、[スタティック IP アドレス] オプションと [ダイナミック] オプションのみが表示されます。

スタティック IP アドレス

このオプションを選択する場合は、IP アドレスとサブネット マスクまたはネットワーク ビットをフィールドに入力します。詳細については、「[IP アドレスとサブネット マスク](#)」を参照してください。

ダイナミック (DHCP クライアント)

このオプションを選択すると、ルータはリモート DHCP サーバから IP アドレスをリースします。アドレスをリースする DHCP サーバの名前を入力します。

IP アンナンバード

別のインターフェイスにすでに割り当てられている IP アドレスを共有する場合は、このオプションを選択します。次に、このインターフェイスが IP アドレスを共有するインターフェイスを選択します。

Easy IP (ネゴシエート済みの IP)

ルータで PPP/IPCIP (ポイントツーポイント プロトコル /IP 制御プロトコル) のアドレス ネゴシエーションによって IP アドレスを取得する場合は、このオプションを選択します。

認証

CHAP/PAP 認証のパスワード情報を入力する場合にクリックします。

動的 DNS

動的 DNS を有効にすると、WAN インターフェイスの IP アドレスが変更されるたびに、DNS サーバが自動更新されます。



(注)

この機能は、使用するルータの Cisco IOS リリースによってサポートされる場合のみ表示されます。

使用する動的 DNS 方式を選択するには、次のいずれかを実行します。

- 既存の動的 DNS 方式の名前を入力します。
[設定] > [ルータ] > [ルータ (詳細設定)] > [動的 DNS 方式] のリストに表示される名前を、[動的 DNS 方式] フィールドに正確に入力します。
- リストから既存の動的 DNS 方式を選択します。
ドロップダウン メニューをクリックして、既存の方式を選択します。既存の動的 DNS 方式が一覧表示されたウィンドウが開きます。このメニュー項目は、既存の動的 DNS 方式が存在する場合のみ有効です。
- 新規の動的 DNS 方式を作成します。
ドロップダウン メニューをクリックして、動的 DNS 方式の新規作成を選択します。

関連付けられた動的 DNS 方式をインターフェイスからクリアするには、ドロップダウン メニューから [なし] を選択します。

接続：イーサネット プロパティ

このウィンドウでは、イーサネット WAN 回線のプロパティを設定できます。

PPPoE カプセル化を有効にする

PPPoE カプセル化の使用がサービス プロバイダから要求される場合は、[PPPoE カプセル化を有効にする] をクリックします。PPPoE は、PPPoE カプセル化を指定します。

IP アドレス

スタティック IP アドレス

PPPoE カプセル化を使用する場合もカプセル化を使用しない場合も選択できます。このオプションを選択する場合は、IP アドレスとサブネット マスクまたはネットワーク ビットをフィールドに入力します。詳細については、「[IP アドレスとサブネット マスク](#)」を参照してください。

ダイナミック (DHCP クライアント)

PPPoE カプセル化を使用する場合もカプセル化を使用しない場合も選択できます。このオプションを選択すると、ルータはリモート DHCP サーバから IP アドレスをリースします。アドレスの割り当てを行う DHCP サーバの名前を入力します。

IP アンナウンバード

PPPoE カプセル化を使用する場合に選択できます。別のインターフェイスにすでに割り当てられている IP アドレスを共有する場合は、このオプションを選択します。次に、このインターフェイスが IP アドレスを共有するインターフェイスを選択します。

Easy IP (ネゴシエート済みの IP)

PPPoE カプセル化を使用する場合に選択できます。ルータで PPP/IPCIP アドレスネゴシエーションによって IP アドレスを取得する場合は、[Easy IP (ネゴシエート済みの IP)] を選択します。

認証

CHAP/PAP 認証のパスワード情報を入力する場合にクリックします。

動的 DNS

動的 DNS を有効にすると、WAN インターフェイスの IP アドレスが変更されるたびに、DNS サーバが自動更新されます。



(注)

この機能は、使用するルータの Cisco IOS リリースによってサポートされる場合のみ表示されます。

使用する動的 DNS 方式を選択するには、次のいずれかを実行します。

- 既存の動的 DNS 方式の名前を入力します。
[設定] > [ルータ] > [ルータ (詳細設定)] > [動的 DNS 方式] のリストに表示される名前を、[動的 DNS 方式] フィールドに正確に入力します。
- リストから既存の動的 DNS 方式を選択します。
ドロップダウン メニューをクリックして、既存の方式を選択します。既存の動的 DNS 方式が一覧表示されたウィンドウが開きます。このメニュー項目は、既存の動的 DNS 方式が存在する場合のみ有効です。
- 新規の動的 DNS 方式を作成します。
ドロップダウン メニューをクリックして、動的 DNS 方式の新規作成を選択します。

関連付けられた動的 DNS 方式をインターフェイスからクリアするには、ドロップダウン メニューから [なし] を選択します。

接続：カプセル化を使用しないイーサネット接続

このウィンドウでは、カプセル化を使用しないイーサネット接続を設定します。

IP アドレス

ルータがこのリンク用の **IP アドレス** を取得する方法を選択します。

- [スタティック IP アドレス] — このオプションを選択する場合は、IP アドレスとサブネット マスクまたはネットワーク ビットを各フィールドに入力します。詳細については、「**IP アドレスとサブネット マスク**」を参照してください。
- [ダイナミック IP アドレス] — このオプションを選択すると、ルータはリモート DHCP サーバから IP アドレスをリースします。DHCP サーバの名前または IP アドレスを入力します。

ホスト名

サービス プロバイダがダイナミック IP アドレスを含む DHCP 応答にルータのホスト名を挿入している場合は、その名前を情報としてこのフィールドに入力できます。

動的 DNS

動的 DNS を有効にすると、WAN インターフェイスの IP アドレスが変更されるたびに、DNS サーバが自動更新されます。



(注)

この機能は、使用するルータの Cisco IOS リリースによってサポートされる場合のみ表示されます。

使用する動的 DNS 方式を選択するには、次のいずれかを実行します。

- 既存の動的 DNS 方式の名前を入力します。
[設定] > [ルータ] > [ルータ (詳細設定)] > [動的 DNS 方式] のリストに表示される名前を、[動的 DNS 方式] フィールドに正確に入力します。

■ 接続 : カプセル化を使用しないイーサネット接続

- リストから既存の動的 DNS 方式を選択します。
ドロップダウンメニューをクリックして、既存の方式を選択します。既存の動的 DNS 方式が一覧表示されたウィンドウが開きます。このメニュー項目は、既存の動的 DNS 方式が存在する場合のみ有効です。
- 新規の動的 DNS 方式を作成します。
ドロップダウンメニューをクリックして、動的 DNS 方式の新規作成を選択します。

関連付けられた動的 DNS 方式をインターフェイスからクリアするには、ドロップダウンメニューから [なし] を選択します。

接続 : ADSL

このウィンドウでは、ADSL 接続でサポートされている PPPoE リンクのプロパティを指定または編集できます。

カプセル化

このリンクで使用するカプセル化のタイプを選択します。

- [PPPoE] を選択すると、イーサネットを介した PPP (ポイントツーポイントプロトコル) のカプセル化を指定します。
- [PPPoA] を選択すると、ATM を介した PPP (ポイントツーポイントプロトコル) のカプセル化を指定します。
- [RFC 1483 ルーティング (AAL5 SNAP)] を選択すると、各 PVC はそれぞれ複数のプロトコルを伝送できます。
- [RFC 1483 ルーティング (AAL5 MUX)] を選択すると、各 PVC は 1 つのプロトコルタイプのみ伝送できます。

接続を編集する場合、カプセル化タイプは表示されますが、編集できません。カプセル化タイプを変更する必要がある場合は、接続を一度削除し、必要なカプセル化タイプを指定して再度作成します。

これらのカプセル化タイプの詳細については、「[カプセル化タイプの自動検出](#)」を参照してください。

仮想パス識別子

仮想パス識別子 (VPI) は、ATM スイッチングとルーティングにおいて、多数の接続で使用されるパスを識別するために使用されます。サービス プロバイダから割り当てられた VPI 値をここに入力します。

既存の接続を編集する場合、このフィールドは無効になります。この値を変更する必要がある場合は、接続を一度削除し、必要な値を指定して再度作成します。

仮想回線識別子

仮想回線識別子 (VCI) は ATM スイッチングとルーティングにおいて、他の接続と共有するパス内の特定の接続を識別するために使用されます。サービス プロバイダから割り当てられた VCI 値をここに入力します。

■ 接続 : ADSL

既存の接続を編集する場合、このフィールドは無効になります。この値を変更する必要がある場合は、接続を一度削除し、必要な値を指定して再度作成します。

IP アドレス

ルータがこのリンク用の **IP アドレス** を取得する方法を選択します。

- [スタティック IP アドレス] — このオプションを選択する場合は、IP アドレスとサブネット マスクまたはネットワーク ビットを各フィールドに入力します。詳細については、「**IP アドレスとサブネット マスク**」を参照してください。
- [ダイナミック IP アドレス] — このオプションを選択すると、ルータはリモート DHCP サーバから IP アドレスをリースします。DHCP サーバの名前または IP アドレスを入力します。
- [アンナンバード IP アドレス] — 別のインターフェイスにすでに割り当てられている IP アドレスを共有する場合は、このオプションを選択します。次に、このインターフェイスが IP アドレスを共有するインターフェイスを選択します。
- [ネゴシエート済みの IP] — PPP/IPCP (IP 制御プロトコル) のアドレス ネゴシエーションによって IP アドレスを取得する場合は、このオプションを選択します。

ホスト名

サービス プロバイダから DHCP オプション 12 のホスト名が提供されている場合は、そのホスト名をここに入力します。

動作モード

次のいずれかの値を選択します。

- [auto] — 中央オフィスにあるデジタル加入者線アクセス マルチプレクサ (**DSLAM**) との自動ネゴシエーション後に、Asymmetric Digital Subscriber Line (ADSL; 非対称デジタル加入者回線) を設定します。
- [ansi-dmt] — ANSI T1.413 Issue 2 モードで調整するように ADSL 回線を設定します。
- [itu-dmt] — ADSL 回線を ITU G.992.1 モードで調整するように設定します。

- [adsl2] — ADSL 回線を ITU G.992.3 モードで調整するように設定します。このモードは、HWIC-ADSL-B/ST、HWIC-ADSLI-B/ST、HWIC-1ADSL、および HWIC-1ADSLI ADSL ネットワーク モジュールで使用できます。
- [adsl2+] — ADSL 回線を ITU G.992.4 モードで調整するように設定します。このモードは、HWIC-ADSL-B/ST、HWIC-ADSLI-B/ST、HWIC-1ADSL、および HWIC-1ADSLI ADSL ネットワーク モジュールで使用できます。
- [splitterless] — ADSL 回線を G.Lite モードで調整するように設定します。このモードは、WIC-1ADSL などの古い ADSL ネットワーク モジュールで使用できます。

認証

CHAP または **PAP** 認証の情報を入力する必要がある場合にクリックします。

動的 DNS

動的 DNS を有効にすると、WAN インターフェイスの IP アドレスが変更されるたびに、DNS サーバが自動更新されます。



(注)

この機能は、使用するルータの Cisco IOS リリースによってサポートされる場合のみ表示されます。

使用する動的 DNS 方式を選択するには、次のいずれかを実行します。

- 既存の動的 DNS 方式の名前を入力します。
[設定] > [ルータ] > [ルータ (詳細設定)] > [動的 DNS 方式] のリストに表示される名前を、[動的 DNS 方式] フィールドに正確に入力します。
- リストから既存の動的 DNS 方式を選択します。
ドロップダウン メニューをクリックして、既存の方式を選択します。既存の動的 DNS 方式が一覧表示されたウィンドウが開きます。このメニュー項目は、既存の動的 DNS 方式が存在する場合のみ有効です。
- 新規の動的 DNS 方式を作成します。
ドロップダウン メニューをクリックして、動的 DNS 方式の新規作成を選択します。

関連付けられた動的 DNS 方式をインターフェイスからクリアするには、ドロップダウンメニューから [なし] を選択します。

マルチリンク PPP を有効にする

このインターフェイスで Multilink Point-to-Point Protocol (MLP) を有効にする場合はこのチェックボックスを選択します。MLP では、負荷分散機能、パケットのフラグメンテーション、Bandwidth On Demand、およびその他の機能を使用することにより、複数の WAN 接続を持つネットワークのパフォーマンスが向上します。

接続 : ADSL over ISDN

このウィンドウでは、ADSL over ISDN 接続を追加または編集します。

カプセル化

このリンクで使用するカプセル化のタイプを選択します。

- [PPPoE] を選択すると、イーサネットを介した PPP (ポイントツーポイント プロトコル) のカプセル化を指定します。
- [RFC 1483 ルーティング (AAL5 SNAP)] を選択すると、各 PVC で複数のプロトコルを伝送できます。
- [RFC 1483 ルーティング (AAL5 MUX)] を選択すると、各 PVC で1つのプロトコルタイプのみ伝送できます。

接続を編集する場合、カプセル化タイプは表示されますが、編集できません。カプセル化タイプを変更する必要がある場合は、接続を一度削除し、必要なカプセル化タイプを指定して再度作成します。

仮想パス識別子

仮想パス識別子 (VPI) は、ATM スイッチングとルーティングにおいて、多数の接続で使用されるパスを識別するために使用されます。この値については、サービス プロバイダに確認してください。

既存の接続を編集する場合、このフィールドは無効になります。この値を変更する必要がある場合は、接続を一度削除し、必要な値を指定して再度作成します。

仮想回線識別子

仮想回線識別子 (VCI) は ATM スイッチングとルーティングにおいて、他の接続と共有するパス内の特定の接続を識別するために使用されます。この値については、サービス プロバイダに確認してください。

既存の接続を編集する場合、このフィールドは無効になります。この値を変更する必要がある場合は、接続を一度削除し、必要な値を指定して再度作成します。

IP アドレス

ルータがこのリンク用の **IP アドレス** を取得する方法を選択します。

- [スタティック IP アドレス] — このオプションを選択する場合は、IP アドレスとサブネット マスクまたはネットワーク ビットを各フィールドに入力します。詳細については、「**IP アドレスとサブネット マスク**」を参照してください。
- [ダイナミック IP アドレス] — このオプションを選択すると、ルータはリモート DHCP サーバから IP アドレスをリースします。DHCP サーバの名前または IP アドレスを入力します。
- [アンナンバード IP アドレス] — 別のインターフェイスにすでに割り当てられている IP アドレスを共有する場合は、このオプションを選択します。次に、このインターフェイスが IP アドレスを共有するインターフェイスを選択します。
- [ネゴシエート済みの IP] — PPP/IPCP (IP 制御プロトコル) のアドレス ネゴシエーションによって IP アドレスを取得する場合は、このオプションを選択します。

動作モード

ADSL 回線が調整時に使用するモードを選択します。



(注)

ルータ上で実行されている Cisco IOS リリースが次の 5 つの動作モードのすべてをサポートしていない場合は、そのリリースでサポートされている動作モードのオプションのみが表示されます。

- [annexb] — ITU-T G.992.1 の標準 Annex-B モード
- [annexb-ur2] — ITU-T G.992.1 の Annex-B モード
- [auto] — 中央オフィスにあるデジタル加入者線アクセス マルチプレクサ (**DSLAM**) との自動ネゴシエーション後に、非対称デジタル加入者回線 (ADSL) を設定します。
- [etsi] — ETSI (European Telecommunications Standards Institute) モード

- [マルチモード] — DSL（デジタル加入者線）上の最適な動作条件を満たすモードがファームウェアによって選択されます。最終的なモードは、現在の DSLAM 設定によって、ETSI モードまたは標準 Annex-B モードのどちらかになります。

認証

CHAP または PAP 認証の情報を入力する必要がある場合にクリックします。

動的 DNS

動的 DNS を有効にすると、WAN インターフェイスの IP アドレスが変更されるたびに、DNS サーバが自動更新されます。



(注)

この機能は、使用するルータの Cisco IOS リリースによってサポートされる場合のみ表示されます。

使用する動的 DNS 方式を選択するには、次のいずれかを実行します。

- 既存の動的 DNS 方式の名前を入力します。
[設定] > [ルータ] > [ルータ (詳細設定)] > [動的 DNS 方式] のリストに表示される名前を、[動的 DNS 方式] フィールドに正確に入力します。
- リストから既存の動的 DNS 方式を選択します。
ドロップダウン メニューをクリックして、既存の方式を選択します。既存の動的 DNS 方式が一覧表示されたウィンドウが開きます。このメニュー項目は、既存の動的 DNS 方式が存在する場合のみ有効です。
- 新規の動的 DNS 方式を作成します。
ドロップダウン メニューをクリックして、動的 DNS 方式の新規作成を選択します。

関連付けられた動的 DNS 方式をインターフェイスからクリアするには、ドロップダウン メニューから [なし] を選択します。

マルチリンク PPP を有効にする

このインターフェイスで Multilink Point-to-Point Protocol (MLP) を有効にする場合はこのチェック ボックスを選択します。MLP では、負荷分散機能、パケットのフラグメンテーション、Bandwidth On Demand、およびその他の機能を使用することにより、複数の WAN 接続を持つネットワークのパフォーマンスが向上します。

接続 : G.SHDSL

このウィンドウでは、[G.SHDSL](#) 接続を作成または編集できます。



(注)

設定している接続が DSL コントローラを使用する場合は、[設備の種類] および [動作モード] フィールドはダイアログに表示されません。

カプセル化

このリンクで使用するカプセル化のタイプを選択します。

- [PPPoE] を選択すると、イーサネットを介した PPP (ポイントツーポイントプロトコル) のカプセル化を指定します。
- [PPPoA] を選択すると、ATM を介した PPP (ポイントツーポイントプロトコル) のカプセル化を指定します。
- [RFC 1483 ルーティング (AAL5 SNAP)] を選択すると、各 PVC で複数のプロトコルを伝送できます。
- [RFC 1483 ルーティング (AAL5 MUX)] を選択すると、各 PVC で1つのプロトコルタイプのみ伝送できます。

接続を編集する場合、カプセル化タイプは表示されますが、編集できません。カプセル化タイプを変更する必要がある場合は、接続を一度削除し、必要なカプセル化タイプを指定して再度作成します。

これらのカプセル化タイプの詳細については、「[カプセル化タイプの自動検出](#)」を参照してください。

仮想パス識別子

仮想パス識別子 (VPI) は、ATM スイッチングとルーティングにおいて、多数の接続で使用されるパスを識別するために使用されます。この値については、サービスプロバイダに確認してください。

既存の接続を編集する場合、このフィールドは無効になります。この値を変更する必要がある場合は、接続を一度削除し、必要な値を指定して再度作成します。

仮想回線識別子

仮想回線識別子 (VCI) は ATM スイッチングとルーティングにおいて、他の接続と共有するパス内の特定の接続を識別するために使用されます。この値については、サービス プロバイダに確認してください。

既存の接続を編集する場合、このフィールドは無効になります。この値を変更する必要がある場合は、接続を一度削除し、必要な値を指定して再度作成します。

IP アドレス

ルータがこのリンク用の IP アドレスを取得する方法を選択します。このエリアに表示されるフィールドは、選択したカプセル化タイプによって異なります。ルータによる IP アドレスの取得方法については、サービス プロバイダまたはネットワーク管理者に確認してください。

スタティック IP アドレス

このオプションを選択する場合は、インターフェイスの IP アドレスとサブネット マスクまたはネットワーク ビットを入力します。この情報については、サービス プロバイダまたはネットワーク管理者に確認してください。詳細については、「[IP アドレスとサブネット マスク](#)」を参照してください。

ダイナミック IP アドレス

このオプションを選択すると、インターフェイスはネットワーク上の DHCP サーバから IP アドレスを取得します。DHCP サーバは、DHCP オプション 12 を使用している場合は、ルータのホスト名とその IP アドレスを送信します。送信されたホスト名については、サービス プロバイダまたはネットワーク管理者に確認してください。

IP アンナナバード

インターフェイスでルータ上のイーサネット インターフェイスと IP アドレスを共有する場合は、このオプションを選択します。このオプションを選択する場合は、IP アドレスを共有するイーサネット インターフェイスをドロップ ダウン リストから選択する必要があります。

中央オフィス内のリモート接続用の IP アドレス

このリンクの接続先ゲートウェイ システムの **IP アドレス** を入力します。この IP アドレスは、サービス プロバイダまたはネットワーク管理者から提供されます。ゲートウェイとは、ルータがインターネットまたは組織の WAN にアクセスするために接続する必要があるシステムです。

設備の種類

次のいずれかの値を選択します。

CPE

顧客宅内機器。カプセル化タイプが PPPoE の場合、CPE が自動的に選択され、このフィールドは無効になります。

CO

中央オフィス

動作モード

次のいずれかの値を選択します。

Annex A (米国のシグナリング)

北米に適した動作パラメータを設定します。

Annex B (ヨーロッパのシグナリング)

ヨーロッパに適した動作パラメータを設定します。

マルチリンク PPP を有効にする

このインターフェイスで Multilink Point-to-Point Protocol (MLP) を有効にする場合はこのチェック ボックスを選択します。MLP では、負荷分散機能、パケットのフラグメンテーション、Bandwidth On Demand、およびその他の機能を使用することにより、複数の WAN 接続を持つネットワークのパフォーマンスが向上します。

認証

CHAP または **PAP** 認証の情報を入力する必要がある場合にクリックします。

動的 DNS

動的 DNS を有効にすると、WAN インターフェイスの IP アドレスが変更されるたびに、DNS サーバが自動更新されます。



(注)

この機能は、使用するルータの Cisco IOS リリースによってサポートされる場合のみ表示されます。

使用する動的 DNS 方式を選択するには、次のいずれかを実行します。

- 既存の動的 DNS 方式の名前を入力します。
[設定] > [ルータ] > [ルータ (詳細設定)] > [動的 DNS 方式] のリストに表示される名前を、[動的 DNS 方式] フィールドに正確に入力します。
- リストから既存の動的 DNS 方式を選択します。
ドロップダウンメニューをクリックして、既存の方式を選択します。既存の動的 DNS 方式が一覧表示されたウィンドウが開きます。このメニュー項目は、既存の動的 DNS 方式が存在する場合のみ有効です。
- 新規の動的 DNS 方式を作成します。
ドロップダウンメニューをクリックして、動的 DNS 方式の新規作成を選択します。

関連付けられた動的 DNS 方式をインターフェイスからクリアするには、ドロップダウンメニューから [なし] を選択します。

接続 : ケーブル モデム

このダイアログでは、ケーブル モデム サービス モジュールのデフォルト IP アドレスを変更します。

フィールドの説明

表 6-1 ケーブル モデム

項目	説明
既定のサービス モジュールの IP アドレスを変更	
チェック ボックス	このサービス モジュールのデフォルト IP アドレスを変更する場合は、[既定のサービス モジュールの IP アドレスを変更] チェック ボックスを選択します。
IP アドレス	IP アドレスをドット (.) で区切った 10 進表記で入力します。たとえば、192.168.4.5 などです。
サブネット マスク	サブネット マスクを 10 進表記で入力します。また、サブネット マスクに含めるビット数を選択することもできます。たとえば、10 進表記のサブネット マスクは 255.255.255.0 のようになります。このサブネット マスク値は 24 ビットに相当します。ビット数を選択する場合は、上向き矢印と下向き矢印を使用してください。10 進値を入力すると、ビット値が自動的に更新されます。ビット値を入力すると、10 進値が自動的に更新されます。

接続 : シリアル インターフェイス、フレーム リレー カプセル化

シリアル サブインターフェイスに **フレーム リレー** カプセル化を設定する場合は、次のフィールドに値を入力します。[インターフェイス / 接続の編集] ウィンドウで接続を編集または作成する場合、カプセル化タイプは表示されますが、編集できません。カプセル化タイプを変更する必要がある場合は、接続を一度削除し、必要なカプセル化タイプを指定して再度作成します。

カプセル化

フレーム リレー が選択されています。

IP アドレス

[スタティック IP アドレス] または [IP アンナンバード] を選択します。

IP アドレス

[スタティック IP アドレス] を選択した場合は、このインターフェイスの **IP アドレス** を入力します。この値については、ネットワーク管理者またはサービスプロバイダに確認してください。詳細については、「**IP アドレスとサブネットマスク**」を参照してください。

サブネット マスク

[スタティック IP アドレス] を選択した場合は、**サブネット マスク** を入力します。サブネット マスクで、ネットワーク アドレスに使用する IP アドレス部分を指定します。この値はサブネット ビットに対応しています。サブネット マスクまたはネットワーク ビットの値は、ネットワーク管理者またはサービスプロバイダから提供されます。

サブネット ビット

サブネット マスクの代わりに **ネットワーク ビット** を入力して、IP アドレスの何ビットをネットワーク アドレスに使用するか指定します。

IP アnnンナナバード

[IP アnnンナナバード] を選択した場合、インターフェイスは、別のインターフェイスにすでに割り当てられている IP アドレスを共有します。このインターフェイスが IP アドレスを共有するインターフェイスを選択してください。

DLCI

DLCI (データリンク接続識別子) を入力します。この番号は、このインターフェイスで使用されるすべての DLCI の中で一意である必要があります。DLCI によって、この接続に一意のフレームリレー識別子が割り当てられます。

既存の接続を編集する場合、このフィールドは無効になります。DLCI を変更する必要がある場合は、接続を一度削除して再度作成します。

LMI タイプ

使用する LMI (Local Management Interface) タイプについては、サービス プロバイダに確認してください。LMI タイプでは、接続の監視に使用するプロトコルを指定します。

ANSI

ANSI (American National Standards Institute) 標準 T1.617 で定義されている Annex D

Cisco

Cisco と他の 3 社で共同定義した LMI タイプ

ITU-T Q.933

ITU-T Q.933 Annex A

自動検出

デフォルト。この設定では、ルータはスイッチで使用されている LMI タイプを検出し、そのタイプを使用します。自動検出に失敗した場合は、Cisco LMI タイプが使用されます。

IETF フレームリレーのカプセル化を使用する

IETF（インターネット技術特別調査委員会）のカプセル化方式を使用する場合は、このチェックボックスを選択します。このオプションは、Cisco 製以外のルータに接続するときに使用されます。このインターフェイスで Cisco 製以外のルータに接続する場合は、このチェックボックスを選択してください。

クロック設定

ほとんどの場合、クロック設定をデフォルト値から変更する必要はありません。要件がデフォルトと異なる場合は、クリックして表示されるウィンドウでクロック設定を調整します。

[クロック設定] ボタンは、T1 または E1 シリアル接続を設定する場合にのみ表示されます。

動的 DNS

動的 DNS を有効にすると、WAN インターフェイスの IP アドレスが変更されるたびに、DNS サーバが自動更新されます。



(注)

この機能は、使用するルータの Cisco IOS リリースによってサポートされる場合のみ表示されます。

使用する動的 DNS 方式を選択するには、次のいずれかを実行します。

- 既存の動的 DNS 方式の名前を入力します。
[設定] > [ルータ] > [ルータ (詳細設定)] > [動的 DNS 方式] のリストに表示される名前を、[動的 DNS 方式] フィールドに正確に入力します。
- リストから既存の動的 DNS 方式を選択します。
ドロップダウンメニューをクリックして、既存の方式を選択します。既存の動的 DNS 方式が一覧表示されたウィンドウが開きます。このメニュー項目は、既存の動的 DNS 方式が存在する場合のみ有効です。

- 新規の動的 DNS 方式を作成します。
ドロップダウンメニューをクリックして、動的 DNS 方式の新規作成を選択します。

関連付けられた動的 DNS 方式をインターフェイスからクリアするには、ドロップダウンメニューから [なし] を選択します。

接続：シリアルインターフェイス、PPP カプセル化

シリアルインターフェイスにポイントツーポイントカプセル化を設定する場合は、次のフィールドに値を入力します。[インターフェイス / 接続の編集] ウィンドウで接続を編集または作成する場合、カプセル化タイプは表示されますが、編集できません。カプセル化タイプを変更する必要がある場合は、接続を一度削除し、必要なカプセル化タイプを指定して再度作成します。

カプセル化

PPP が選択されています。

IP アドレス

[スタティック IP アドレス]、[IP アンナンバード]、[ネゴシエート済みの IP] からいずれかを選択します。[IP アンナンバード] を選択した場合は、このインターフェイスが IP アドレスを共有するインターフェイスを選択します。[ネゴシエート済みの IP] を選択すると、ルータは、このインターフェイスに対してサービスプロバイダから提供された IP アドレスを取得します。[IP アドレスの指定] を選択する場合は、次のフィールドに値を入力します。

IP アドレス

このポイントツーポイントサブインターフェイスの IP アドレスを入力します。この値については、ネットワーク管理者またはサービスプロバイダに確認してください。詳細については、「IP アドレスとサブネットマスク」を参照してください。

サブネット マスク

サブネット マスクを入力します。サブネット マスクで、ネットワーク アドレスに使用する IP アドレス部分を指定します。この値はネットワーク ビットに対応しています。サブネット マスクまたはネットワーク ビットの値については、ネットワーク管理者またはサービス プロバイダに確認してください。

サブネット ビット

サブネット マスクの代わりに**ネットワーク ビット**を入力して、IP アドレスの何ビットをネットワーク アドレスに使用するか指定します。

認証

CHAP または **PAP** 認証の情報を入力する必要がある場合にクリックします。

クロック設定

ほとんどの場合、クロック設定をデフォルト値から変更する必要はありません。要件がデフォルトと異なる場合は、クリックして表示されるウィンドウでクロック設定を調整します。

[クロック設定] ボタンは、T1 または E1 シリアル接続を設定する場合にのみ表示されます。

動的 DNS

動的 DNS を有効にすると、WAN インターフェイスの IP アドレスが変更されるたびに、DNS サーバが自動更新されます。



(注)

この機能は、使用するルータの Cisco IOS リリースによってサポートされる場合のみ表示されます。

使用する動的 DNS 方式を選択するには、次のいずれかを実行します。

- 既存の動的 DNS 方式の名前を入力します。
[設定] > [ルータ] > [ルータ (詳細設定)] > [動的 DNS 方式] のリストに表示される名前を、[動的 DNS 方式] フィールドに正確に入力します。
- リストから既存の動的 DNS 方式を選択します。
ドロップダウン メニューをクリックして、既存の方式を選択します。既存の動的 DNS 方式が一覧表示されたウィンドウが開きます。このメニュー項目は、既存の動的 DNS 方式が存在する場合のみ有効です。
- 新規の動的 DNS 方式を作成します。
ドロップダウン メニューをクリックして、動的 DNS 方式の新規作成を選択します。

関連付けられた動的 DNS 方式をインターフェイスからクリアするには、ドロップダウン メニューから [なし] を選択します。

接続 : シリアル インターフェイス、HDLC カプセル化

シリアル インターフェイスに **HDLC** カプセル化を設定する場合は、次のフィールドに値を入力します。[インターフェイス / 接続の編集] ウィンドウで接続を編集または作成する場合、カプセル化タイプは表示されますが、編集できません。カプセル化タイプを変更する必要がある場合は、接続を一度削除し、必要なカプセル化タイプを指定して再度作成します。

カプセル化

[HDLC] が選択されています。

IP アドレス

[スタティック IP アドレス] または [IP アンナナバード] を選択します。[IP アンナナバード] を選択した場合は、このインターフェイスが IP アドレスを共有するインターフェイスを選択します。[スタティック IP アドレス] を選択する場合は、次のフィールドに値を入力します。

IP アドレス

このインターフェイスの **IP アドレス**を入力します。この値については、ネットワーク管理者またはサービス プロバイダに確認してください。詳細については、「**IP アドレスとサブネット マスク**」を参照してください。

サブネット マスク

サブネット マスクを入力します。サブネット マスクで、ネットワークアドレスに使用する IP アドレス部分を指定します。この値はネットワーク ビットに対応しています。サブネット マスクまたはネットワーク ビットの値については、ネットワーク管理者またはサービス プロバイダに確認してください。

サブネット ビット

サブネット マスクの代わりに、IP アドレスの何ビットをネットワークアドレスに使用するかを指定します。

クロック設定

ほとんどの場合、クロック設定をデフォルト値から変更する必要はありません。要件がデフォルトと異なる場合は、クリックして表示されるウィンドウでクロック設定を調整します。

[クロック設定] ボタンは、T1 または E1 シリアル接続を設定する場合にのみ表示されます。

動的 DNS

動的 DNS を有効にすると、WAN インターフェイスの IP アドレスが変更されるたびに、DNS サーバが自動更新されます。



(注)

この機能は、使用するルータの Cisco IOS リリースによってサポートされる場合のみ表示されます。

使用する動的 DNS 方式を選択するには、次のいずれかを実行します。

- 既存の動的 DNS 方式の名前を入力します。
[設定] > [ルータ] > [ルータ (詳細設定)] > [動的 DNS 方式] のリストに表示される名前を、[動的 DNS 方式] フィールドに正確に入力します。
- リストから既存の動的 DNS 方式を選択します。
ドロップダウンメニューをクリックして、既存の方式を選択します。既存の動的 DNS 方式が一覧表示されたウィンドウが開きます。このメニュー項目は、既存の動的 DNS 方式が存在する場合のみ有効です。
- 新規の動的 DNS 方式を作成します。
ドロップダウンメニューをクリックして、動的 DNS 方式の新規作成を選択します。

関連付けられた動的 DNS 方式をインターフェイスからクリアするには、ドロップダウンメニューから [なし] を選択します。

GRE トンネルの追加 / 編集

このウィンドウでは、GRE トンネルをインターフェイスに追加したり、既存のインターフェイスを編集したりできます。GRE トンネルが **gre ip** モードを使用して設定されていない場合、このウィンドウは表示されません。

トンネル番号

このトンネルの番号を入力します。

トンネルの送信元

トンネルで使用するインターフェイスを選択します。トンネルのもう一方の端からこのインターフェイスに到達できる必要があります。したがって、このインターフェイスには、ルート指定可能なパブリック **IP アドレス**が必要です。

トンネルの宛先

トンネルの宛先は、トンネルのもう一方の端にあるルータ上のインターフェイスです。IP アドレスまたはホスト名のどちらかを指定するかを選択し、該当の情報を入力します。IP アドレスを選択した場合は、IP アドレスとサブネット マスクをドット (.) で区切った 10 進表記で入力します。たとえば、192.168.20.1 と 255.255.255.0 を入力します。

ping コマンドを使用してこのアドレスまたはホスト名に到達できるかどうかを確認します。到達できない場合、トンネルは正しく構築されません。

トンネルの IP アドレス

トンネルの IP アドレスをドット (.) で区切った 10 進表記で入力します (192.168.20.1 など)。詳細については、「**IP アドレスとサブネット マスク**」を参照してください。

[GRE キープアライブ] チェック ボックス

ルータから GRE キープアライブを送信する場合に選択します。キープアライブの送信間隔 (秒単位) と再試行間の待機時間 (秒単位) を指定します。

最大伝送ユニット

MTU（最大伝送ユニット）サイズを入力します。調整によってパケットのフラグメンテーションを回避するときにサイズを小さい値に調整する場合は、[フラグメンテーションが発生しないように MTU を調整する] をクリックします。

帯域幅

このトンネルの帯域幅を KB 単位で指定する場合にクリックします。

接続 : ISDN BRI

ISDN BRI 接続を設定する場合は、次のフィールドに値を入力します。Cisco CP は、ISDN BRI 接続に対して PPP カプセル化のみサポートします。したがって、表示されるカプセル化タイプは編集できません。

カプセル化

PPP が選択されています。

ISDN スイッチ タイプ

ISDN スイッチ タイプを選択します。接続に適したスイッチ タイプについては、サービス プロバイダに確認してください。

Cisco CP は、次の BRI スイッチ タイプをサポートしています。

- 北米 :
 - basic-5ess — Lucent (AT&T) 基本レート 5ESS スイッチ
 - basic-dms100 — Northern Telecom DMS-100 基本レート スイッチ
 - basic-ni — National ISDN スイッチ
- オーストラリア、ヨーロッパ、英国 :
 - 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、およびニュージーランド NET 3 スイッチ タイプ用の NET3 ISDN BRI。Euro-ISDN E-DSS1 シグナリング システム用の ETSI 対応のスイッチ タイプ
 - vn3 — フランス ISDN BRI スイッチ
- 日本 :
 - ntt — 日本 NTT ISDN スイッチ
- 音声 /PBX システム用 :
 - basic-qsig — Q931 に基づく QSIG シグナリング対応の PINX (PBX) スイッチ

SPID

SPID (サービス プロファイル ID) 情報を入力する必要がある場合にクリックします。

一部のサービス プロバイダは、ISDN サービス プロバイダにアクセスする ISDN デバイスの加入サービスを定義するために、SPID を使用しています。サービス に最初に加えるときに、サービス プロバイダから 1 つ以上の SPID が ISDN デバイスに割り当てられます。SPID を要求するサービス プロバイダを使用する場合は、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 SPID をそのプロバイダに送信しなければ、ISDN デバイスはコールを送受信できません。

SPID が必要なスイッチ タイプは DMS-100 と NI だけです。Lucent (AT&T) 5ESS スイッチ タイプも SPID をサポートしますが、SPID を使用せずに ISDN サービスをセットアップすることをお勧めします。また、SPID が重要になるのは、ローカルアクセス ISDN インターフェイスの場合だけです。リモートルータは SPID を受け取りません。

通常、SPID は 7 桁の電話番号に数桁のオプション番号が付加されたものです。ただし、別の方法で番号を付けるサービス プロバイダもあります。DMS-100 スイッチ タイプの場合、2 つの SPID (B チャネルごとに 1 つずつ) が割り当てられます。

リモート電話番号

ISDN 接続の宛先の電話番号を入力します。

オプション

ダイヤラ リストに ACL を関連付けて対象トラフィックを識別する場合、タイマー設定を入力する場合、マルチリンク PPP を有効または無効にする場合にクリックします。

対象トラフィックの識別を可能にすると、ルータは、対象トラフィックを検出したときだけダイヤラアウトして接続をアクティブにします。

タイマーを設定すると、ルータは回線がアイドル状態になってから指定した時間経過したときにコールを自動的に切断します。

マルチリンク PPP を設定すると、ISDN B チャネル間で負荷を分散できます。

IP アドレス

[スタティック IP アドレス]、[IP アンナナバード]、[ネゴシエート済みの IP] からいずれかを選択します。[IP アドレスの指定] を選択する場合は、次のフィールドに値を入力します。

IP アドレス

このポイントツーポイント サブインターフェイスの **IP アドレス** を入力します。この値については、ネットワーク管理者またはサービス プロバイダに確認してください。詳細については、「**IP アドレスとサブネットマスク**」を参照してください。

サブネット マスク

サブネット マスク を入力します。サブネット マスクで、ネットワーク アドレスに使用する IP アドレス部分を指定します。この値はネットワーク ビットに対応しています。サブネット マスクまたはネットワーク ビットの値については、ネットワーク管理者またはサービス プロバイダに確認してください。

サブネット ビット

サブネット マスクの代わりに **ネットワーク ビット** を入力して、IP アドレスの何ビットをネットワーク アドレスに使用するか指定します。

認証

CHAP または **PAP** 認証の情報を入力する必要がある場合にクリックします。

動的 DNS

動的 DNS を有効にすると、WAN インターフェイスの IP アドレスが変更されるたびに、DNS サーバが自動更新されます。



(注) この機能は、使用するルータの Cisco IOS リリースによってサポートされる場合のみ表示されます。

使用する動的 DNS 方式を選択するには、次のいずれかを実行します。

- 既存の動的 DNS 方式の名前を入力します。
[設定] > [ルータ] > [ルータ (詳細設定)] > [動的 DNS 方式] のリストに表示される名前を、[動的 DNS 方式] フィールドに正確に入力します。
- リストから既存の動的 DNS 方式を選択します。
ドロップダウン メニューをクリックして、既存の方式を選択します。既存の動的 DNS 方式が一覧表示されたウィンドウが開きます。このメニュー項目は、既存の動的 DNS 方式が存在する場合のみ有効です。
- 新規の動的 DNS 方式を作成します。
ドロップダウン メニューをクリックして、動的 DNS 方式の新規作成を選択します。

関連付けられた動的 DNS 方式をインターフェイスからクリアするには、ドロップダウン メニューから [なし] を選択します。

接続 : アナログ モデム

アナログ モデム接続を設定する場合は、次のフィールドに値を入力します。Cisco CP は、アナログ モデム接続に対して PPP カプセル化のみをサポートします。したがって、表示されるカプセル化タイプは編集できません。

カプセル化

PPP が選択されています。

リモート電話番号

アナログ モデム接続の宛先の電話番号を入力します。

オプション

ダイヤラ リストに ACL を関連付けて対象トラフィックを識別する必要がある場合、またはタイマー設定を入力する必要がある場合にクリックします。

対象トラフィックの識別を可能にすると、ルータは、対象トラフィックを検出したときだけダイヤルアウトして接続をアクティブにします。

タイマーを設定すると、ルータは回線がアイドル状態になってから指定した時間経過したときにコールを自動的に切断します。

回線のクリア

回線をクリアする場合にクリックします。非同期接続の作成後に回線をクリアして、対象トラフィックが検出されたときに接続がアクティブになるようにする必要があります。

IP アドレス

[スタティック IP アドレス]、[IP アンナンバード]、[ネゴシエート済みの IP] からいずれかを選択します。[IP アドレスの指定] を選択する場合は、次のフィールドに値を入力します。

IP アドレス

このポイントツーポイント サブインターフェイスの **IP アドレス**を入力します。この値については、ネットワーク管理者またはサービス プロバイダに確認してください。詳細については、「**IP アドレスとサブネット マスク**」を参照してください。

サブネット マスク

サブネット マスクを入力します。サブネット マスクで、ネットワーク アドレスに使用する IP アドレス部分を指定します。この値はネットワーク ビットに対応しています。サブネット マスクまたはネットワーク ビットの値については、ネットワーク管理者またはサービス プロバイダに確認してください。

サブネット ビット

サブネット マスクの代わりに**ネットワーク ビット**を入力して、IP アドレスの何ビットをネットワーク アドレスに使用するか指定します。

認証

CHAP または **PAP** 認証の情報を入力する必要がある場合にクリックします。

動的 DNS

動的 DNS を有効にすると、WAN インターフェイスの IP アドレスが変更されるたびに、DNS サーバが自動更新されます。



(注)

この機能は、使用するルータの Cisco IOS リリースによってサポートされる場合のみ表示されます。

使用する動的 DNS 方式を選択するには、次のいずれかを実行します。

- 既存の動的 DNS 方式の名前を入力します。
[設定] > [ルータ] > [ルータ (詳細設定)] > [動的 DNS 方式] のリストに表示される名前を、[動的 DNS 方式] フィールドに正確に入力します。
- リストから既存の動的 DNS 方式を選択します。
ドロップダウン メニューをクリックして、既存の方式を選択します。既存の動的 DNS 方式が一覧表示されたウィンドウが開きます。このメニュー項目は、既存の動的 DNS 方式が存在する場合のみ有効です。
- 新規の動的 DNS 方式を作成します。
ドロップダウン メニューをクリックして、動的 DNS 方式の新規作成を選択します。

関連付けられた動的 DNS 方式をインターフェイスからクリアするには、ドロップダウン メニューから [なし] を選択します。

接続 : (AUX バックアップ)

Cisco 831 または 837 ルータ上の AUX ポートとしても動作可能なコンソールポートを使用した非同期ダイヤルアップ接続を設定する場合は、次のフィールドに値を入力します。このウィンドウに情報を入力した後は [バックアップの詳細] をクリックして、この接続タイプに必要なダイヤルバックアップ情報を入力します。Cisco CP は、アナログ モデム接続に対して PPP カプセル化のみをサポートします。したがって、表示されるカプセル化タイプは編集できません。

AUX ポートをダイヤルアップ接続として設定するオプションは、Cisco 831 ルータおよび 837 ルータの場合のみ表示されます。次のいずれかの状況が発生すると、これらのルータに対してこのオプションを使用できません。

- ルータが Zutswang Cisco IOS リリースを使用していない。
- プライマリ WAN インターフェイスが設定されていない。
- 非同期インターフェイスがすでに設定されている。
- 既存の設定に Cisco CP でサポートされていない Cisco IOS コマンドが含まれているため、Cisco CP で非同期インターフェイスを設定できない。

カプセル化

PPP が選択されています。

リモート電話番号

アナログ モデム接続の宛先の電話番号を入力します。

オプション

ダイヤラ リストに ACL を関連付けて対象トラフィックを識別する必要がある場合、またはタイマー設定を入力する必要がある場合にクリックします。

対象トラフィックの識別を可能にすると、ルータは、対象トラフィックを検出したときだけダイヤルアウトして接続をアクティブにします。

タイマーを設定すると、ルータは回線がアイドル状態になってから指定した時間経過したときにコールを自動的に切断します。

■ 接続:(AUXバックアップ)

回線のクリア

回線をクリアする場合にクリックします。非同期接続の作成後に回線をクリアして、対象トラフィックが検出されたときに接続がアクティブになるようにする必要があります。

IP アドレス

[[スタティック IP アドレス](#)]、[[IP アンナナバード](#)]、[[ネゴシエート済みの IP](#)] からいずれかを選択します。[[IP アドレスの指定](#)] を選択する場合は、次のフィールドに値を入力します。

IP アドレス

このポイントツーポイント サブインターフェイスの [IP アドレス](#) を入力します。この値については、ネットワーク管理者またはサービス プロバイダに確認してください。詳細については、「[IP アドレスとサブネットマスク](#)」を参照してください。

サブネット マスク

[サブネット マスク](#) を入力します。サブネット マスクで、ネットワークアドレスに使用する IP アドレス部分を指定します。この値はネットワーク ビットに対応しています。サブネット マスクまたはネットワーク ビットの値については、ネットワーク管理者またはサービス プロバイダに確認してください。

サブネット ビット

サブネット マスクの代わりに [ネットワーク ビット](#) を入力して、IP アドレスの何ビットをネットワーク アドレスに使用するか指定します。

バックアップの詳細

[[バックアップ設定](#)] ウィンドウを表示してこの接続のダイヤルバックアップ情報を設定する場合にクリックします。ダイヤルバックアップ設定情報は、このタイプの接続では必須です。この情報を入力せずに接続設定を終了しようとすると、エラーが表示されます。

認証

CHAP または **PAP** 認証の情報を入力する必要がある場合にクリックします。

動的 DNS

動的 DNS を有効にすると、WAN インターフェイスの IP アドレスが変更されるたびに、DNS サーバが自動更新されます。



(注)

この機能は、使用するルータの Cisco IOS リリースによってサポートされる場合のみ表示されます。

使用する動的 DNS 方式を選択するには、次のいずれかを実行します。

- 既存の動的 DNS 方式の名前を入力します。
[設定] > [ルータ] > [ルータ (詳細設定)] > [動的 DNS 方式] のリストに表示される名前を、[動的 DNS 方式] フィールドに正確に入力します。
- リストから既存の動的 DNS 方式を選択します。
ドロップダウン メニューをクリックして、既存の方式を選択します。既存の動的 DNS 方式が一覧表示されたウィンドウが開きます。このメニュー項目は、既存の動的 DNS 方式が存在する場合のみ有効です。
- 新規の動的 DNS 方式を作成します。
ドロップダウン メニューをクリックして、動的 DNS 方式の新規作成を選択します。

関連付けられた動的 DNS 方式をインターフェイスからクリアするには、ドロップダウン メニューから [なし] を選択します。

認証

このページが表示されるのは、シリアル接続に対して PPP を有効にした場合、ATM またはイーサネット接続に対して PPPoE カプセル化を有効にした場合、そして ISDN BRI 接続またはアナログ モデム接続を設定する場合です。サービス プロバイダまたはネットワーク管理者は、CHAP (Challenge Handshake Authentication Protocol) パスワードまたは PAP (Password Authentication Protocol) パスワードを使用してデバイス間の接続を保護できます。このパスワードはインバウンドアクセスとアウトバウンドアクセスの両方を保護します。

CHAP/PAP

サービス プロバイダが使用する認証タイプのチェック ボックスを選択します。認証タイプがわからない場合は、両方のチェック ボックスを選択できます。その場合、ルータは両方の認証タイプを試行して、成功した方を使用します。

CHAP 認証は PAP 認証より安全です。

ログイン名

ログイン名はサービス プロバイダから割り当てられ、CHAP/PAP 認証のユーザ名として使用されます。

パスワード

サービス プロバイダから割り当てられたパスワードを正確に入力します。パスワードは大文字と小文字を区別します。たとえば、*test* というパスワードは *TEST* と同じではありません。

新しいパスワードの再入力

[パスワード] ボックスに入力したパスワードを再度入力します。

SPID の詳細

一部のサービス プロバイダは、ISDN サービス プロバイダにアクセスする ISDN デバイスの加入サービスを定義するために、SPID (サービス プロファイル ID 番号) を使用しています。サービスに最初に加入するときに、サービス プロバイダから 1 つ以上の SPID が ISDN デバイスに割り当てられます。SPID を要求するサービス プロバイダを使用する場合は、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 SPID をそのプロバイダに送信しなければ、ISDN デバイスはコールを送受信できません。

SPID が必要なスイッチ タイプは DMS-100 と NI だけです。AT&T 5ESS スイッチ タイプも SPID をサポートします。SPID を使用せずにその ISDN サービスをセットアップすることをお勧めします。また、SPID が重要になるのは、ローカルアクセス ISDN インターフェイスの場合だけです。リモート ルータは SPID を受け取りません。

通常、SPID は 7 桁の電話番号に数桁のオプション番号が付加されたものです。ただし、別の方法で番号を付けるサービス プロバイダもあります。DMS-100 スイッチ タイプの場合、2 つの SPID (B チャネルごとに 1 つずつ) が割り当てられます。

SPID1

ISP から割り当てられた 1 つめの BRI B チャネルの SPID を入力します。

SPID2

ISP から割り当てられた 2 つめの BRI B チャネルの SPID を入力します。

ダイアラ オプション

ISDN BRI およびアナログ モデム インターフェイスには、DDR (ダイヤルオンデマンド ルーティング) を設定できます。これにより、特定の状況でのみ接続をダイヤルアウトしてアクティブにできるため、接続にかかる時間とコストが節約されます。このウィンドウでは、ISDN BRI 接続またはアナログ モデム接続の開始と終了に関するオプションを設定できます。

ダイアラ リストの関連付け

ダイアラ リストを使用すると、ISDN BRI 接続またはアナログ モデム接続に ACL を関連付けて、対象トラフィックを識別できます。対象トラフィックの識別を可能にすると、インターフェイスは、ACL に一致するデータ トラフィックがルータによって検出されたときだけダイヤルアウトして接続を確立します。

すべての IP トラフィックを許可する

このオプションを選択すると、インターフェイスは、任意の IP トラフィックがそのインターフェイス経由で送信されるたびにダイヤルアウトして接続を確立します。

選択した ACL でトラフィックをフィルタする

このオプションを選択すると、ACL がインターフェイスに関連付けられます。ACL は、ルール インターフェイスを使用して作成する必要があります。ACL で指定されたトラフィックに一致するトラフィックが検出された場合のみ、インターフェイスはダイヤルアウトして接続を確立します。

対象トラフィックを識別するためにダイアラ インターフェイスに関連付ける ACL 番号を入力します。または、このフィールドの隣にあるボタンをクリックして ACL 一覧を表示することも、新規の ACL を作成してこれを選択することもできます。

タイマー設定

タイマー設定では、トラフィックのない接続がアクティブな状態を維持する最大時間を設定できます。タイマーを設定すると接続が自動的に切断されるため、接続にかかる時間とコストを節約できます。

アイドル タイムアウト

アイドル状態の接続（トラフィックのない接続）が切断されるまでの時間を秒単位で入力します。

ファースト アイドル タイムアウト

ファースト アイドル タイムアウトは、ある 1 つの接続がアクティブであるとき、接続を待機している別の接続が存在する場合に使用されます。ファースト アイドル タイムアウトは、対象トラフィックの存在しない状態が続き、アクティブな接続が切断されるまでの最大秒数を設定します。この時間の経過後に、待機していた接続が確立されます。

このタイムアウトは、インターフェイスにネクスト ホップ IP アドレスへのアクティブな接続がある状態で、そのアドレスとは異なるネクスト ホップ IP アドレス宛ての対象データをインターフェイスが受信したときに発生します。ダイヤラ接続はポイントツーポイントであるため、現在の接続が確立されている間は競合するパケットを配信できません。このタイマーは、最初の接続をアイドル状態のまま保持する必要がある時間を設定します。この時間の経過後にその接続は切断され、別の接続が確立されます。

マルチリンク PPP を有効にする

マルチリンク PPP を使用すると、複数の ISDN BRI B チャネルと非同期インターフェイスにデータを分散できます。マルチリンク PPP を使用して最初の ISDN 接続を確立すると、その接続には 1 つの B チャネルのみが使用されます。その接続のトラフィック負荷が指定されたしきい値（合計帯域幅に対する割合）を超えると、2 つめの B チャネルを持つ接続が確立され、データ トラフィックは両方の接続に分散されます。この方法には、データ トラフィックが少ない場合に接続にかかる時間とコストを節約でき、必要な場合はすべての ISDN BRI 帯域幅を使用できるという利点があります。

マルチリンク PPP を有効にする場合はこのチェック ボックスを選択します。有効にしない場合は、選択を解除します。

負荷のしきい値

このフィールドでは、1 つの ISDN BRI チャンネルで使用する必要がある帯域幅の割合を設定できます。このしきい値を超えると、別の ISDN BRI チャンネル接続が確立されてトラフィックが分散されます。1 ～ 255 の範囲内の値を入力します。255 は、最初の接続で帯域幅を 100% 利用することを意味します。

データの方向

Cisco CP では、アウトバウンド方向のネットワーク トラフィックに対してのみマルチリンク PPP を設定できます。

バックアップ設定

ISDN BRI およびアナログ モデム インターフェイスは、他のプライマリ インターフェイスのバックアップ インターフェイスとして機能するように設定できます。その場合、ISDN またはアナログ モデム接続は、プライマリ インターフェイスが何かの理由でダウンしたときだけ確立されます。プライマリ インターフェイスと接続がダウンすると、ISDN またはダイヤル モデム インターフェイスは、ネットワーク サービスが停止しないように直ちにダイヤルアウトして接続を確立しようとします。

バックアップを有効にする

この ISDN BRI またはアナログ モデム インターフェイスをバックアップ接続として機能させる場合に選択します。バックアップ接続として機能させない場合は、このチェック ボックスの選択を解除します。

プライマリ インターフェイス

プライマリ接続を保持するルータ上のインターフェイスを選択します。ISDN BRI またはアナログ モデム接続は、選択したインターフェイス上の接続が切断されたときだけ確立されます。

追跡の詳細

特定のホストへの接続を保持する必要がある場合は、このオプションを選択します。ルータはそのホストへの接続を追跡し、接続がプライマリ インターフェイスによって切断されたことを検出すると、ISDN BRI またはアナログ モデム インターフェイスを使用したバックアップ接続が開始されます。

追跡するホスト名または IP アドレス

接続を追跡する宛先ホストのホスト名または IP アドレスを入力します。追跡するサイトとして、接続頻度の低い宛先を指定してください。

追跡オブジェクト番号

読み取り専用のフィールドです。リモート ホストへの接続を追跡するために、Cisco CP によって生成され、使用される内部オブジェクト番号が表示されます。

ネクスト ホップ先

これらのフィールドはオプションです。プライマリおよびバックアップ インターフェイスがアクティブな場合に接続する IP アドレスを入力できます。これはネクスト ホップ IP アドレスとして知られています。ネクスト ホップ IP アドレスを入力しない場合は、Cisco CP がインターフェイス名を使用してスタティック ルートを設定します。イーサネット接続などのマルチポイント WAN 接続をバックアップする場合は、ルーティングが正常に行われるようにネクスト ホップ IP アドレスを入力する必要があります。ただし、ポイントツーポイント接続をバックアップする場合は、この情報を入力する必要はありません。

プライマリのネクスト ホップ IP アドレス

プライマリ インターフェイスのネクスト ホップ IP アドレスを入力します。

バックアップのネクスト ホップ IP アドレス

ISDN BRI またはアナログ モデム バックアップ インターフェイスのネクスト ホップ IP アドレスを入力します。

接続の削除

[インターフェイス / 接続の編集] ウィンドウに表示される WAN 接続を削除できます。インターフェイス設定を削除する場合で、そのインターフェイスに適用されているアクセス ルールなどの関連付けが、削除する接続に含まれるときに、このウィンドウが表示されます。このウィンドウでは、別の接続で使用できるように、そうした関連付けを保存することができます。

接続を削除した結果、削除前に使用できなかった接続タイプが使用できるようになると、[新しい接続の作成] リストが更新されます。

接続とその関連付けをすべて自動的に削除することもでき、関連付けだけを後で解除することもできます。

接続に定義されている関連付けを表示するには

[詳細の表示] をクリックします。

接続とその関連付けをすべて削除するには

[すべての関連付けを自動的に解除する]、[OK] の順にクリックすると、接続とその関連付けがすべて削除されます。

関連付けを手動で解除するには

関連付けを手動で解除するには、[詳細の表示] をクリックして、この接続に定義されているすべての関連付けのリストを確認します。すべての関連付けを書き留めたら、[後で関連付けを解除する] を選択して [OK] をクリックします。関連付けは、以下の手順に従って手動で解除できます。

各関連付けと、それらを削除する手順を以下に示します。

- デフォルトのスタティック ルート — 特定のインターフェイスが、デフォルトのスタティック ルートの転送先インターフェイスとして設定されているとします。このインターフェイスに関連付けられているスタティック ルートを削除するには、[設定]、[ルーティング] の順にクリックします。次に、[スタティック ルーティング] テーブルでスタティック ルートを選択して [削除] をクリックします。

■ 接続の削除

- ポートアドレス変換 — この接続が作成されたインターフェイスを使用して PAT が設定されているとします。この PAT 関連付けを解除するには、[設定]、[NAT] の順にクリックします。次に、この接続に関連付けられたルールを選択して [削除] をクリックします。
- NAT — 特定のインターフェイスが、NAT 内部または NAT 外部のどちらかのインターフェイスとして指定されているとします。この NAT 関連付けを解除するには、[設定]、[インターフェイスと接続] の順にクリックします。次に、[インターフェイス リスト] から目的の接続を選択して、[編集] をクリックします。[NAT] タブをクリックして、[NAT] プルダウンメニューから [なし] を選択します。
- ACL — 接続が作成されたインターフェイスに ACL が適用されているとします。この ACL を削除するには、[設定]、[インターフェイスと接続] の順にクリックします。次に、[インターフェイス リスト] から目的の接続を選択して、[編集] をクリックします。[関連付け] タブをクリックし、[アクセス ルール] グループ内で、[インバウンド] および [アウトバウンド] フィールドの横にある [...] ボタンをクリックして、[なし] をクリックします。
- インспекション — 接続が作成されたインターフェイスにインспекションルールが適用されているとします。このインспекションルールを削除するには、[設定]、[インターフェイスと接続] の順にクリックします。次に、[インターフェイス リスト] から目的の接続を選択して、[編集] をクリックします。[関連付け] タブをクリックし、[インспекションルール] グループ内の [インバウンド] および [アウトバウンド] の各フィールドで [なし] を選択します。
- 暗号 — 接続が作成されたインターフェイスに暗号マップが適用されているとします。この暗号マップを解除するには、[設定]、[インターフェイスと接続] の順にクリックします。次に、[インターフェイス リスト] から目的の接続を選択して、[編集] をクリックします。[関連付け] タブをクリックし、[VPN] グループ内の [IPSec ポリシー] フィールドで [なし] を選択します。
- EZVPN — 接続が作成されたインターフェイスに Easy VPN が適用されているとします。この Easy VPN を解除するには、[設定]、[インターフェイスと接続] の順にクリックします。次に、[インターフェイス リスト] から目的の接続を選択して、[編集] をクリックします。[関連付け] タブをクリックし、[VPN] グループ内の [Easy VPN] フィールドで [なし] を選択します。
- VPDN — PPPoE 設定に必要な VPDN コマンドがルータ設定内に存在するとします。ルータ上に他の PPPoE 接続が設定されている場合は、VPDN コマンドを削除してはなりません。

- `ip tcp adjust mss` — このコマンドは、TCP の最大サイズを調整するために LAN インターフェイスに適用されます。ルータ上に他の PPPoE 接続が設定されている場合は、このコマンドを削除してはなりません。
- バックアップ接続 — プライマリ インターフェイスにバックアップ接続が設定されている場合、バックアップの関連付けを削除するには、[設定]、[インターフェイスと接続] の順にクリックします。次に、[インターフェイスリスト] でバックアップ インターフェイスを選択して、[編集] をクリックします。[バックアップ] タブをクリックし、[バックアップを有効にする] チェック ボックスの選択を解除します。
- バックアップ接続上の PAT — PAT がバックアップ インターフェイス上に設定されているとします。この PAT 関連付けを解除するには、[設定]、[NAT] の順にクリックします。次に、この接続に関連付けられたルールを選択して [削除] をクリックします。
- バックアップ接続上のフローティング デフォルト ルート — フローティング デフォルト スタティック ルートがバックアップ インターフェイス上に設定されているとします。このフローティング スタティック ルートを削除するには、[設定]、[ルーティング] の順にクリックします。次に、スタティック ルーティング テーブルでフローティング スタティック ルートを選択して [削除] をクリックします。

接続テストとトラブルシューティング

このウィンドウでは、リモート ホストに対して ping を実行することで、設定した接続をテストできます。ping が失敗すると、Cisco CP は考えられる原因を報告し、問題を修正するためのアクションを提示します。

SDM でテストできる接続タイプ

Cisco CP では、PPPoE、AAL5SNAP、または AAL5MUX カプセル化を使用した ADSL、G.SHDSL V1、G.SHDSL V2 接続のトラブルシューティングを実行できません。

Cisco CP は、PPPoE カプセル化を使用したイーサネット接続のトラブルシューティングを実行できます。

Cisco CP では、カプセル化されていないイーサネット接続、シリアルおよび T1/E1 接続、アナログ接続、ISDN 接続のトラブルシューティングを実行できません。これらの接続タイプに対しては、基本的な ping テストを実行します。

基本的な ping テストとは

Cisco CP が実行する基本的な ping テストの内容は次のとおりです。

1. インターフェイスのステータスをチェックして、稼働状態か停止状態かを確認します。
2. DNS の設定をチェックして、Cisco CP のデフォルト オプションかユーザ指定のホスト名のどちらが使用されているかを確認します。
3. インターフェイスの DHCP および IPCP 設定をチェックします。
4. インターフェイス テストを終了します。
5. 宛先に対して ping を実行します。

Cisco CP は、これらのチェックの結果をアクティビティ/ステータス カラムに表示します。ping が成功すると、その接続は正常であると報告されます。それ以外の場合、接続はダウンと報告され、不合格になったテストが指摘されます。

Cisco CP がトラブルシューティングを実行する方法

Cisco CP による接続のトラブルシューティングでは、基本的な ping テストよりも広範なテストを実行します。ルータがテストに失敗すると、Cisco CP は追加のチェックを実行して、考えられる原因を列挙します。たとえば、レイヤ 2 のステータスがダウンしている場合、Cisco CP は、ダウンの原因を調べて報告し、問題を修正するために推奨されるアクションを提示します。Cisco CP は次のタスクを実行します。

1. インターフェイス ステータスをチェックします。レイヤ 2 のプロトコルが正常に稼働している場合は、手順 2 に進みます。

レイヤ 2 のプロトコル ステータスがダウンしている場合は、xDSL 接続の ATM PVC ステータス、またはカプセル化されたイーサネット接続の PPPoE ステータスをチェックします。

- ATM PVC テストに失敗すると、Cisco CP は、考えられる原因を列挙し、問題を修正するためのアクションを提示します。
- PPPoE 接続がダウンしている場合は、ケーブルの接続に問題があります。Cisco CP は該当する原因とアクションを表示します。

これらのチェックがすべて実行されると、テストが終了し、Cisco CP によってテスト結果が報告され、推奨されるアクションが提示されます。

2. DNS の設定をチェックして、Cisco CP のデフォルト オプションかユーザ指定のホスト名のどちらが使用されているかを確認します。
3. DHCP および IPCP 設定とそのステータスをチェックします。ルータが、DHCP または IPCP を使用して IP アドレスを取得済みの場合は、手順 4 に進みます。

ルータが DHCP または IPCP を使用するように設定されているにもかかわらず、そのどちらの方法でも IP アドレスを取得していない場合、手順 1. が実行されます。テストが終了し、Cisco CP によってテスト結果が報告され、推奨されるアクションが提示されます。

4. 宛先に対して ping を実行します。ping が成功すると、接続は正常であると報告されます。

PPPoE カプセル化を使用した xDSL 接続上で ping に失敗すると、Cisco CP は次の項目をチェックします。

- ATM PVC ステータス
- PPPoE トンネル ステータス
- PPP 認証ステータス

■ 接続テストとトラブルシューティング

これらのチェックをすべて実行すると、Cisco CP は、ping が失敗した原因を報告します。

PPPoE カプセル化を使用したイーサネット接続上で ping に失敗すると、Cisco CP は次の項目をチェックします。

- PPPoE トンネル ステータス
- PPP 認証ステータス

これらのチェックをすべて実行すると、Cisco CP は、ping が失敗した原因を報告します。

AAL5SNAP または AAL5MUX カプセル化を使用した xDSL 接続上で ping が失敗すると、Cisco CP は、ATM PVC ステータスをチェックし、ping が失敗した原因を報告します。

IP アドレス / ホスト名

WAN インターフェイスをテストするために実行する ping の宛先サーバ名を指定します。

Cisco CP による自動指定

Cisco CP は、WAN インターフェイスをテストするために、デフォルトのホストに ping を実行します。Cisco CP は、ルータにスタティックに設定されている DNS サーバ、およびダイナミックにインポートされた DNS サーバを検出します。Cisco CP はこれらのサーバに対して ping を実行し、テストされているインターフェイスを ping が正常に通過すると、接続が正常であると報告します。すべての ping が失敗して、テストされているインターフェイスを正常に通過した ping が検出されない場合、Cisco CP は失敗と報告します。

ユーザ指定

WAN インターフェイスをテストするために選択したホスト名の IP アドレスを指定します。

要約

要約されたトラブルシューティング情報を表示する場合にこのボタンをクリックします。

詳細

詳細なトラブルシューティング情報を表示する場合にこのボタンをクリックします。

アクティビティ

このカラムには、トラブルシューティングのアクティビティが表示されます。

ステータス

個々のトラブルシューティングのアクティビティのステータスが、次のアイコンとテキストアラートで表示されます。



接続されています。



接続は切断されています。



テストは成功しました。



テストは失敗しました。

原因

このボックスには、WAN インターフェイス接続の失敗で考えられる原因が表示されます。

推奨アクション

このボックスには、問題を修正するためのアクション / 解決策が表示されます。

■ 接続テストとトラブルシューティング

実行する操作

目的	手順
WAN インターフェイス接続のトラブルシューティングを実行する。	<p>[開始] ボタンをクリックする。</p> <p>テストの実行中は、[開始] ボタンのラベルが [終了] に変わる。テストの実行中にトラブルシューティングを中止するオプションがある。</p>
テストレポートを保存する。	<p>テストレポートを HTML 形式で保存する場合は、[レポートの保存] ボタンをクリックする。</p> <p>このボタンは、テストが実行中の場合、またはテストが完了した場合だけ使用可能になる。</p>