ルーテッド モードおよびトランスペアレント モードのインターフェイス

この章では、ルーテッドまたはトランスペアレント ファイアウォール モードですべてのモデルのインターフェイス設定を完了するためのタスクについて説明します。

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

ルーテッドモードインターフェイスとトランスペアレント モード インターフェイスについて

ASA は、ルーテッドおよびブリッジという 2 つのタイプのインターフェイスをサポートします。

各レイヤ 3 ルーテッド インターフェイスに、固有のサブネット上の IP アドレスが必要です。

ブリッジされたインターフェイスはブリッジグループに属し、すべてのインターフェイスが同じネットワーク上にあります。ブリッジグループはブリッジ ネットワークに IP アドレスを持つブリッジ仮想インターフェイス（BVI）によって表されます。ルーテッド モードは、ルーテッド インターフェイスとブリッジ インターフェイスの両方をサポートし、ルーテッド インターフェイスと BVI との間のルーティングが可能です。トランスペアレント ファイアウォール モードでは、ブリッジ グループと BVI インターフェイスのみがサポートされます。

セキュリティ レベル

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

BVI にセキュリティ レベルを割り当てるかどうかは、ファイアウォール モードに応じて異なります。トランスペアレント モードでは、BVI インターフェイスはインターフェイス間のルーティングに参加しないため、BVI インターフェイスにはセキュリティ レベルが割り当てられていません。ルーテッド モードでは、BVI 間や他のインターフェイスとの間のルーティングを選択した場合、BVI インターフェイスはセキュリティ レベルを所有します。ルーテッド モードでは、ブリッジ グループ メンバー インターフェイスのセキュリティ レベルは、ブリッジ グループ内の通信にのみ適用されます。同様に、BVI のセキュリティ レベルは、BVI/レイヤ 3 インターフェイス通信にのみ適用されます。

レベルによって、次の動作が制御されます。

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

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

- インスペクション エンジン：一部のアプリケーション インスペクション エンジンはセキュリティ レベルに依存します。同じセキュリティ レベルのインターフェイス間では、インスペクション エンジンは発信と着信のいずれのトラフィックに対しても適用されます。

  - NetBIOS インスペクション エンジン：発信接続に対してのみ適用されます。
  - SQL*Net インスペクション エンジン：SQL*Net（旧称 OraServ）ポートとの制御接続が一対のホスト間に存在する場合、着信データ接続だけが ASA を通過することが許可されます。

デュアル IP スタック（IPv4 および IPv6）

ASA は、インターフェイスで IPv6 アドレスと IPv4 アドレスの両方をサポートしています。IPv4 と IPv6 の両方で、デフォルト ルートを設定してください。

31 ビット サブネット マスク

ルーテッド インターフェイスに関しては、ポイントツーポイント接続向けの 31 ビットのサブネットに IP アドレスを設定できます。31 ビット サブネットには 2 つのアドレスのみが含まれます。通常、サブネットの最初と最後のアドレスはネットワーク用とブロードキャスト用に予約されており、2 アドレス サブネットは使用できません。ただし、ポイントツーポイント接続があり、ネットワーク アドレスやブロードキャスト アドレスが不要な場合は、IPv4 形式でアドレスを保持するのに 31 サブネット ビットが役立ちます。たとえば、2 つの ASA 間のフェールオーバーリンクに必要なアドレスは 2 つだけです。リンクの一方の側から送信されるパケットはすべてもう一方の側で受信され、ブロードキャスティングは必要ありません。また、SNMP または Syslog を実行する管理ステーションを直接接続することもできます。

31 ビットのサブネットとクラスタリング

管理インターフェイスとクラスタ制御リンクを除き、スパンドクラスタリング モードで31 ビットのサブネットマスクを使用できます。

インターフェイス上では、クラスタリングモードで 31 ビットのサブネット マスクを使用できません。

31 ビットのサブネットとフェールオーバー

フェールオーバーに関しては、ASA インターフェイスの IP アドレスに 31 ビットのサブネットを使用した場合、アドレスが不足しているため、インターフェイス用のスタンバイ IP アドレスは設定できません。通常、アクティブなユニットがインターフェイスのテストを実行し、スタンバイのインターフェイスの健全性を保証できるよう、フェールオーバーインターフェイスはスタンバイ IP アドレスを必要とします。スタンバイ IP アドレスがないと、ASA はネットワークのテストを実行できず、リンクステートのみしか追跡できません。

ポイントツーポイント接続であるフェールオーバーと任意のステートリンクでは、31 ビットのサブネットも使用できます。

31 ビットのサブネットと管理

直接接続される管理ステーションがあれば、ASA 上で SSH または HTTP にポイントツーポイント接続を、または管理ステーション上で SNMP または Syslog にポイントツーポイント接続をそれぞれ使用できます。

31 ビットのサブネットをサポートしていない機能

次の機能は、31 ビットのサブネットをサポートしていません。

- ブリッジ グループ用 BVI インターフェイス - ブリッジ グループには BVI、2 つのブリッジ グループ メンバーに接続された 2 つのホスト用に、少なくとも 3 つのホスト アドレスが必要です。/ 29 サブネット以下を使用する必要があります。
- マルチキャスト ルーティング

ルーテッドモードおよびトランスペアレントモードのインターフェイスに関するガイドラインと制限事項

コンテキスト モード

- マルチ コンテキスト モードで設定できるのは、マルチ コンテキストの設定に従ってシステム コンフィギュレーションでコンテキストにすでに割り当てられているコンテキスト インターフェイスだけです。
- PPPoE は、マルチ コンテキスト モードではサポートされていません。
- トランスペアレント モードのマルチ コンテキスト モードでは、各コンテキストが別個のインターフェイスを使用する必要があります。コンテキスト間でインターフェイスを共有することはできません。
- トランスペアレント モードのマルチ コンテキスト モードでは、通常、各コンテキストが別個のサブネットを使用します。重複するサブネットを使用することもできますが、ルーティング スタンドポイントから可能にするため、ネットワーク トポロジにルータと NAT コンフィギュレーションが必要です。
- DHCPv6 およびプレフィクス委任オプションは、マルチ コンテキスト モードではサポートされていません。
- ルーテッド ファイアウォール モードでは、ブリッジ グループ インターフェイスはマルチ コンテキスト モードでサポートされません。

フェイルオーバー、クラスタリング

- フェールオーバー リンクは、この章の手順で設定しないでください。詳細については、「フェイルオーバー」の章を参照してください。
- クラスタインターフェイスの場合は、クラスタリングの章で要件を確認してください。
- フェイルオーバー を使用する場合、データ インターフェイスの IP アドレスとスタンバイ アドレスを手動で設定する必要があります。DHCPおよびPPPoEはサポートされません。

IPv6

- IPv6 はすべてのインターフェイスでサポートされます。
- トランスペアレント モードでは、IPv6 アドレスは手動でのみ設定できます。

- ASAは、IPv6 エニーキャスト アドレスはサポートしません。
- DHCPv6およびプレフィックス委任オプションは、マルチコンテキストモード、トランスペアレントモード、クラスタリング、またはフェイルオーバーではサポートされません。

モデルのガイドライン

- ASAv50 の場合、ブリッジグループは透過的モードまたはルーテッドモードのいずれでもサポートされません。

トランスペアレント モードとブリッジ グループのガイドライン

- 64 のインターフェイスをもつブリッジグループを 250 まで作成できます。
- 直接接続された各ネットワークは同一のサブネット上にある必要があります。
- ASA では、セカンダリ ネットワーク上のトラフィックはサポートされていません。BVI IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。
- デバイスとデバイス間の管理トラフィック、および ASA を通過するデータトラフィックの各ブリッジグループに対し、BVI の IP アドレスが必要です。IPv4 トラフィックの場合は、IPv4 アドレスを指定します。IPv6 トラフィックの場合は、IPv6 アドレスを指定します。
- IPv6 アドレスは手動でのみ設定できます。
- BVI IPアドレスは、接続されたネットワークと同じサブネット内にある必要があります。サブネットにホスト サブネット（255.255.255.255）を設定することはできません。
- 管理インターフェイスはブリッジグループのメンバーとしてサポートされません。
- ブリッジされた ixgbevf インターフェイスを備えた VMware の ASAv50 の場合、トランスペアレントモードはサポートされておらず、ブリッジグループはルーテッドモードではサポートされていません。
- 200/ 1010/ 1210// 1220 では、同じブリッジグループ内に論理 VLAN インターフェイスと物理ファイアウォール インターフェイスを混在させることはできません。
- トランスペアレント モードでは、少なくとも 1 つのブリッジ グループを使用し、データ インターフェイスがブリッジ グループに属している必要があります。
- トランスペアレントモードでは、接続されたデバイス用のデフォルトゲートウェイとして BVI IP アドレスを指定しないでください。デバイスは ASA の他方側のルータをデフォルトゲートウェイとして指定する必要があります。
- トランスペアレントモードでは、管理トラフィックの戻りパスを指定するために必要なデフォルトルートは、1つのブリッジグループ ネットワークからの管理トラフィックにだけ適用されます。これは、デフォルト ルートはブリッジグループのインターフェイスとブリッジグループ ネットワークのルータ IPアドレスを指定しますが、ユーザは1つのデフォルト ルートしか定義できないためです。複数のブリッジグループ ネットワークからの管

理トラフィックが存在する場合は、管理トラフィックの発信元ネットワークを識別する標準のスタティック ルートを指定する必要があります。

- トランスペアレント モードでは、PPPoE は Management インターフェイスでサポートされません。
- ルーテッドモードでは、ブリッジグループと他のルーテッドインターフェイスの間をルーティングするために、BVI を指定する必要があります。
- ルーテッド モードでは、ASA 定義の EtherChannel および VNI インターフェイスがブリッジ グループのメンバーとしてサポートされません。Firepower 4100/9300 上の Etherchannel は、ブリッジグループメンバーにすることができます。
- Bidirectional Forwarding Detection（BFD）エコー パケットは、ブリッジ グループ メンバを使用するときに、ASA を介して許可されません。BFD を実行している ASA の両側に 2 つのネイバーがある場合、ASA は BFD エコー パケットをドロップします。両方が同じ送信元および宛先 IP アドレスを持ち、LAND 攻撃の一部であるように見えるからです。

デフォルトのセキュリティ レベル

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

（注） インターフェイスのセキュリティレベルを変更する場合、既存の接続がタイムアウトするのを待たずに新しいセキュリティ情報を使用するときは、**clear conn** コマンドを使用して接続をクリアできます。

その他のガイドラインと要件

- ASA では、パケットで 802.1Q ヘッダーが 1 つだけサポートされ、複数のヘッダー（Q-in-Q）はサポートされません。
- 頻繁なアップ/ダウンステータスの変化などのインターフェイスの問題があると、フローティング接続タイマーが、インターフェイスを通過する接続に正しく適用されない場合があります。インターフェイスのステータスに問題がある場合は、無効な接続をクリアするため、ステータスが安定した後にすべての接続をクリアすることを検討してください。

ルーテッド モードのインターフェイスの設定

ルーテッド モードのインターフェイスを設定するには、次の手順を実行します。

ルーテッド モードの一般的なインターフェイス パラメータの設定

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

始める前に

マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** の順に選択します。

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

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

（注）
Firepower 1010 の場合、スイッチポートをルーテッド モード インターフェイスとして設定することはできません。

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

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

（注）
ループバック インターフェイスの場合、インターフェイスはデバイス間のトラフィックに対してのみサポートされるため、セキュリティ レベルは設定しません。

ステップ 5 （任意）このインターフェイスを管理専用インターフェイスとして設定するには、[Dedicate this interface to management-only] チェックボックスをオンにします。

管理専用インターフェイスでは、通過トラフィックは受け入れられません。

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

（注）
ループバック インターフェイスの場合、インターフェイスはデバイス間のトラフィックに対してのみサポートされるため、管理モードは設定しません。

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

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

（注）
フェールオーバーやクラスタリング、およびループバック インターフェイスの場合は、IP アドレスを手動で設定する必要があります。DHCP と PPPoE はサポートされません。

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

  フェールオーバーの場合は、[Configuration] > [Device Management] > [High Availability] > [Failover] > [Interfaces] タブでスタンバイ IP アドレスを設定します。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニターできず、リンク ステートをトラックすることしかできません。

  ポイントツーポイント接続の場合、31 ビットのサブネットマスク（255.255.255.254）を指定できます。この場合、ネットワークまたはブロードキャスト アドレス用の IP アドレスは予約されません。この場合、スタンバイ IP アドレスを設定できません。
- DHCP サーバーから IP アドレスを取得するには、[Obtain Address via DHCP] オプション ボタンをクリックします。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

  7. （オプション）[PPPoE IP Address and Route Settings] ダイアログボックスを表示し、アドレッシングおよびトラッキングのオプションを選択するには、[IP Address and Route Settings] をクリックします。

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

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

ステップ 9 [OK] をクリックします。

関連トピック

IPv6 アドレスの設定 （17 ページ）
物理インターフェイスのイネーブル化およびイーサネット パラメータの設定
PPPoE の設定 （10 ページ）

PPPoE の設定

インターフェイスが DSL、ケーブル モデム、またはその他の手段で ISP に接続されていて、ISP が PPPoE を使用して IP アドレスを割り当てる場合は、次のパラメータを設定します。

手順

ステップ 1 **[Configuration]** > **[Interfaces]** > **[Add/Edit Interface]** > **[General]** の順に選択し、[PPPoE IP Address and Route Settings] をクリックします。

ステップ 2 [IP Address] 領域で、次のいずれかを選択します。

- [Obtain IP Address using PPP]：IP アドレスを動的に設定します。
- [Specify an IP Address]：IP アドレスを手動で設定します。

ステップ 3 [Route Settings Area] で、次の設定を行います。

- [Obtain default route using PPPoE]：PPPoE クライアントがまだ接続を確立していない場合に、デフォルト ルートを設定します。このオプションを使用する場合は、スタティックに定義されたルートを設定に含めることができません。
- [PPPoE learned route metric]：アドミニストレーティブ ディスタンスを学習したルートに割り当てます。有効な値は、1 ～ 255 です。このフィールドを空白のままにすると、既知のルートのアドミニストレーティブ ディスタンスは 1 になります。
- [Enable tracking]：PPPoE の既知のルートのルート トラッキングをイネーブルにします。ルート トラッキングは、シングル ルーテッド モードでだけ使用できます。
- [Primary Track]：プライマリ PPPoE ルート トラッキングを設定します。
- [Track ID]：ルート トラッキング プロセスに使用される一意の識別子。有効な値は、1 ～ 500 です。

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

ステップ 4 [OK] をクリックします。

ブリッジグループ インターフェイスの設定

ブリッジ グループは、ASA がルーティングではなくブリッジするインターフェイスのグループです。ブリッジグループはトランスペアレント ファイアウォール モード、ルーテッド ファイアウォール モードの両方でサポートされています。ブリッジグループの詳細については、ブリッジグループについてを参照してください。

ブリッジグループと関連インターフェイスを設定するには、次の手順を実行します。

ブリッジ仮想インターフェイス（BVI）の設定

ブリッジ グループごとに、IP アドレスを設定する BVI が必要です。ASA は、ブリッジ グループから発信されるパケットの送信元アドレスとしてこの IP アドレスを使用します。BVI IP アドレスは、接続されたネットワークと同じサブネット内にある必要があります。IPv4 トラフィックの場合、すべてのトラフィックを通過させるには、BVI IP アドレスが必要です。IPv6 トラフィックの場合は、少なくとも、トラフィックを通過させるリンクローカルアドレスを設定する必要があります。リモート管理などの管理操作を含めたフル機能を実現するために、グローバル管理アドレスを設定することを推奨します。

ルーテッドモードの場合、BVIに名前を指定すると、BVIがルーティングに参加します。名前を指定しなければ、ブリッジ グループはトランスペアレント ファイアウォール モードの場合と同じように隔離されたままになります。

一部のモデルでは、デフォルト コンフィギュレーションにブリッジ グループと BVI が含まれています。追加のブリッジグループおよびBVIを作成して、グループの間でメンバーインターフェイスを再割り当てすることもできます。

（注） トランスペアレントモードの個別の管理インターフェイスでは（サポートされているモデルの場合）、設定できないブリッジグループ（ID 301）がコンフィギュレーションに自動的に追加されます。このブリッジ グループはブリッジ グループの制限に含まれません。

手順

ステップ 1 **[Configuration]** > **[Interfaces]** の順に選択し、**[Add]** > **[Bridge Group Interface]** を選択します。

ステップ 2 [Bridge Group ID] フィールドに、1 ～ 250 の間のブリッジ グループ ID を入力します。

このブリッジ グループ メンバーには、後で物理インターフェイスを割り当てます。

ステップ 3 （ルーテッド モード）[Interface Name] フィールドに、名前を 48 文字以内で入力します。

トラフィックをブリッジ グループ メンバーの外部（たとえば、外部インターフェイスや他のブリッジグループのメンバー）にルーティングする必要がある場合は、BVI に名前を付ける必要があります。

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

ステップ 5 （トランスペアレント モード）IP アドレスを設定します。

a) [IP Address] フィールドに、IPv4 アドレスを入力します。

b) [Subnet Mask] フィールド にサブネット マスクを入力するか、またはメニューから選択します。

トランスペアレント ファイアウォールにホスト アドレス（/32 または 255.255.255.255）を割り当てないでください。また、/30 サブネットなど（255.255.255.252）、ホスト アドレスが 3 つ未満（アップストリーム ルータ、ダウンストリーム ルータ、トランスペアレント ファイアウォールにそれぞれ 1 つずつ）の他のサブネットを使用しないでください。ASA は、サブネットの先頭アドレスと最終アドレスで送受信されるすべての ARP パケットをドロップします。たとえば、/30 サブネットを使用し、そのサブネットからアップストリーム ルータへの予約アドレスを割り当てた場合、ASA はダウンストリーム ルータからアップストリーム ルータへの ARP 要求をドロップします。

ステップ 6 （ルーテッドモード）IPアドレスを設定するには、次のいずれかのオプションを使用します。

フェールオーバーやクラスタリングの場合は、IPアドレスを手動で設定する必要があります。DHCP はサポートされません。

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

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

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

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

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

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

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

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

ステップ 7 （オプション）[Description] フィールドに、このブリッジ グループの説明を入力します。

ステップ 8 [OK] をクリックします。

ブリッジ仮想インターフェイス（BVI）が、物理およびサブインターフェイスとともに、インターフェイス テーブルに追加されます。

ブリッジ グループ メンバーの一般的なインターフェイス パラメータの設定

この手順は、ブリッジ グループ メンバー インターフェイスの名前、セキュリティ レベル、およびブリッジ グループを設定する方法について説明します。

始める前に

- 同じブリッジグループで、さまざまな種類のインターフェイス（物理インターフェイス、VLAN サブインターフェイス、VNI インターフェイス、EtherChannel インターフェイス）を含めることができます。管理インターフェイスはサポートされていません。ルーテッド モードでは、EtherChannel と VNI はサポートされません。
- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

- トランスペアレントモードの場合、管理インターフェイスにはこの手順を使用しないでください。管理インターフェイスを設定する場合は、トランスペアレントモードの管理インターフェイスの設定 （15 ページ）を参照してください。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** の順に選択します。

BVI は、物理インターフェイス、サブインターフェイス、EtherChannel ポートチャネル インターフェイスとともにテーブルに表示されます。マルチ コンテキスト モードでは、システム実行スペースでコンテキストに割り当てられたインターフェイスだけがテーブルに表示されます。

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

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

（注）
Firepower 1010 では、スイッチポートをブリッジグループメンバーとして設定することはできません。

同じブリッジグループ内に論理 VLAN インターフェイスと物理ルータインターフェイスを混在させることはできません。

（注）
ルーテッドモードでは、**port-channel** および **vni** インターフェイスはブリッジグループのメンバーとしてサポートされません。

ステップ 3 [Bridge Group] ドロップダウン メニューで、このインターフェイスを割り当てるブリッジ グループを選択します。

ステップ 4 [Interface Name] フィールドに、名前を 48 文字以内で入力します。

ステップ 5 [Security level] フィールドに、0（最低）～ 100（最高）のレベルを入力します。

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

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

ステップ 7 （任意） モジュールを取り付けて非実稼働 ASA 上でモジュール機能をデモンストレーションする場合、[Forward traffic to the ASA module for inspection and reporting] チェック ボックスをオンにします。詳細については、のモジュールに関する章またはクイック スタート ガイドを参照してください。

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

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

ステップ 9 [OK] をクリックします。

関連トピック

手動 MAC アドレス、MTU、および TCP MSS の設定

トランスペアレント モードの管理インターフェイスの設定

トランスペアレント ファイアウォール モードでは、すべてのインターフェイスがブリッジ グループに属している必要があります。唯一の例外は管理インターフェイス（物理インターフェイス、サブインターフェイス（ご使用のモデルでサポートされている場合）、または管理インターフェイスを構成する EtherChannel インターフェイス（複数の管理インターフェイスがある場合）のいずれか）です。管理インターフェイスは個別の管理インターフェイスとして設定できます。Firepower 4100/9300 シャーシ では、管理インターフェイス ID は ASA 論理デバイスに割り当てた mgmt タイプ インターフェイスに基づいています。他のインターフェイス タイプは管理インターフェイスとして使用できません。シングル モードまたはコンテキストごとに 1 つの管理インターフェイスを設定できます。詳細については、トランスペアレント モードの管理インターフェイスを参照してください。

管理インターフェイスは、To-the-Box および From-the-Box トラフィック専用で、トラフィックを通過することができません。

始める前に

- このインターフェイスをブリッジ グループに割り当てないでください。設定できないブリッジ グループ（ID 301）は、コンフィギュレーションに自動的に追加されます。このブリッジ グループはブリッジ グループの制限に含まれません。
- Firepower 4100/9300 シャーシ では、管理インターフェイス ID は ASA 論理デバイスに割り当てた mgmt-type インターフェイスに基づいています。
- マルチ コンテキスト モードでは、どのインターフェイスも（これには管理インターフェイスも含まれます）、コンテキスト間で共有させることはできません。データ インターフェイスに接続する必要があります。
- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システムからコンテキスト コンフィギュレーションに変更するには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** の順に選択します。

ステップ 2 管理インターフェイス、サブインターフェイス、または管理インターフェイスからなる EtherChannel ポートチャネル インターフェイスの行を選択して、[Edit] をクリックします。

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

Firepower 4100/9300 シャーシ では、管理インターフェイス ID は ASA 論理デバイスに割り当てた mgmt タイプ インターフェイス（個別インターフェイスまたは EtherChannel インターフェイス）に基づいています。

ステップ 3 [Bridge Group] ドロップダウン メニューで、デフォルトの [--None--] のままにします。管理インターフェイスをブリッジ グループに割り当てることはできません。

ステップ 4 [Interface Name] フィールドに、名前を 48 文字以内で入力します。

ステップ 5 [Security level] フィールドに、0（最低）～ 100（最高）のレベルを入力します。

（注）
[Dedicate this interface to management only] チェックボックスは、デフォルトでイネーブルであり、設定することはできません。

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

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

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

- IP アドレスを手動で設定するには、[Use Static IP] オプション ボタンをクリックして IP アドレスとマスクを入力します。
- DHCP サーバーから IP アドレスを取得するには、[Obtain Address via DHCP] オプション ボタンをクリックします。
  - MAC アドレスがオプション 61 の DHCP 要求パケット内に保存されるようにするには、[Use MAC Address] オプション ボタンをクリックします。

    いくつかの ISP はインターフェイスの MAC アドレスにオプション 61 が必要です。MAC アドレスが DHCP 要求パケットに含まれていない場合、IP アドレスは割り当てられません。
  - オプション 61 用に生成された文字列を使用するには、[Use “Cisco-<MAC>-<interface_name>-<host>”] をクリックします。

- （任意）DHCP サーバーからデフォルト ルートを取得するには、[Obtain Default Route Using DHCP] をオンにします。
- （オプション）DHCP クライアントが IP アドレス要求の探索を送信する場合に、DHCP パケット ヘッダーでブロードキャスト フラグを 1 に設定するには、[Enable DHCP Broadcast flag for DHCP request and discover messages] をオンにします。

  DHCP サーバーはこのブロードキャスト フラグをリッスンし、フラグが 1 に設定されている場合は応答パケットをブロードキャストします。
- （任意）リースを更新するには、[Renew DHCP Lease] をクリックします。

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

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。

ステップ 9 [OK] をクリックします。

IPv6 アドレスの設定

この項では、IPv6 アドレッシングを設定する方法について説明します。

IPv6 について

このセクションには、IPv6 に関する情報が含まれています。

IPv6 アドレス指定

次の 2 種類の IPv6 のユニキャスト アドレスを設定できます。

- グローバル：グローバル アドレスは、パブリック ネットワークで使用可能なパブリック アドレスです。ブリッジ グループの場合、このアドレスは各メンバー インターフェイスごとに設定するのではなく、BVI 用に設定する必要があります。また、トランスペアレント モードで管理インターフェイスのグローバルな IPv6 アドレスを設定することもできます。
- リンクローカル：リンクローカルアドレスは、直接接続されたネットワークだけで使用できるプライベート アドレスです。ルータは、リンクローカル アドレスを使用してパケットを転送するのではなく、特定の物理ネットワーク セグメント上で通信だけを行います。ルータは、アドレス設定またはアドレス解決などのネイバー探索機能に使用できます。ブリッジ グループでは、メンバー インターフェイスのみがリンクローカル アドレスを所有しています。BVI にはリンクローカル アドレスはありません。

最低限、IPv6 が動作するようにリンクローカル アドレスを設定する必要があります。グローバル アドレスを設定すると、リンクローカル アドレスがインターフェイスに自動的に設定されるため、リンクローカル アドレスを個別に設定する必要はありません。ブリッジ グループ

インターフェイスでは、BVIでグローバルアドレスを設定した場合、ASAが自動的にメンバーインターフェイスのリンクローカル アドレスを生成します。グローバル アドレスを設定しない場合は、リンクローカル アドレスを自動的にするか、手動で設定する必要があります。

Modified EUI-64 インターフェイス ID

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

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

```
325003: EUI-64 source address check failed.
```

アドレス形式の確認は、フローが作成される場合にのみ実行されます。既存のフローからのパケットは確認されません。また、アドレスの確認はローカル リンク上のホストに対してのみ実行できます。

IPv6 プレフィックス委任クライアントの設定

ASAは、（ケーブルモデムに接続された外部インターフェイスなどの）クライアントインターフェイスが 1 つ以上の IPv6 プレフィックスを受け取れるように DHPCv6 プレフィックス委任クライアントとして機能することができ、ASAはそのプレフィックスをサブネット化して内部インターフェイスに割り当てることが可能です。

IPv6 プレフィックス委任の概要

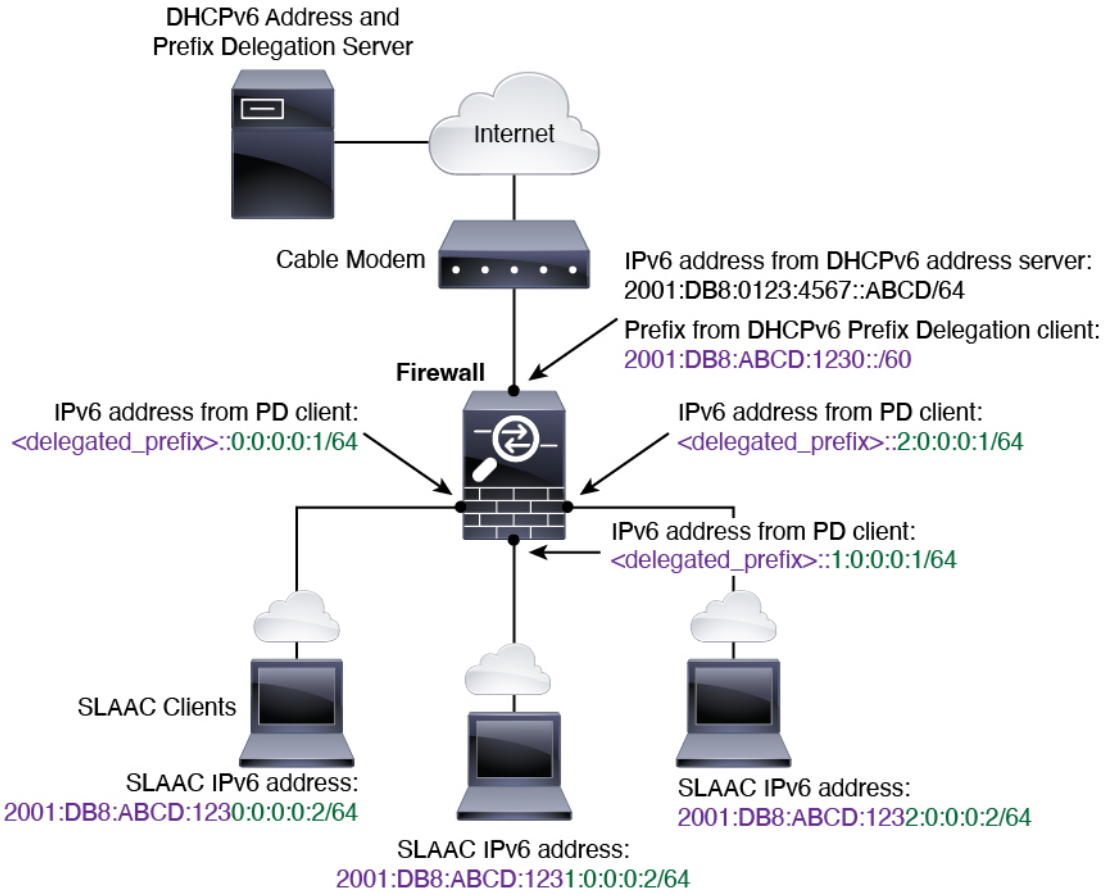
ASAは、（ケーブルモデムに接続された外部インターフェイスなどの）クライアントインターフェイスが 1 つ以上の IPv6 プレフィックスを受け取れるように DHPCv6 プレフィックス委任クライアントとして機能することができ、ASAはそのプレフィックスをサブネット化して内部インターフェイスに割り当てることが可能です。これにより、内部インターフェイスに接続されているホストは、StateLess Address Auto Configuration（SLAAC）を使用してグローバル IPv6 アドレスを取得できます。ただし、内部ASAインターフェイスはプレフィックス委任サーバーとして機能しないため注意してください。ASAは、SLAACクライアントにグローバルIPアドレスを提供することしかできません。たとえば、ルータが ASA に接続されている場合、ASAはSLAACクライアントとして機能し、IPアドレスを取得できます。しかし、ルータの背後のネットワークに代理プレフィックスのサブネットを使用したい場合、ルータの内部インターフェイス上でそれらのアドレスを手動で設定する必要があります。

ASA には軽量 DHCPv6 サーバーが含まれており、SLAAC クライアントが情報要求（IR）パケットを ASA に送信した場合、ASA は DNS サーバーやドメイン名などの情報を SLAAC クラ

イアントに提供できます。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。クライアントが独自の IPv6 アドレスを生成するように設定するには、クライアントで IPv6 自動設定を有効にします。クライアントでステートレスな自動設定を有効にすると、ルータ アドバタイズメント メッセージで受信したプレフィックス（ASA がプレフィックス委任を使用して受信したプレフィックス）に基づいて IPv6 アドレスが設定されます。

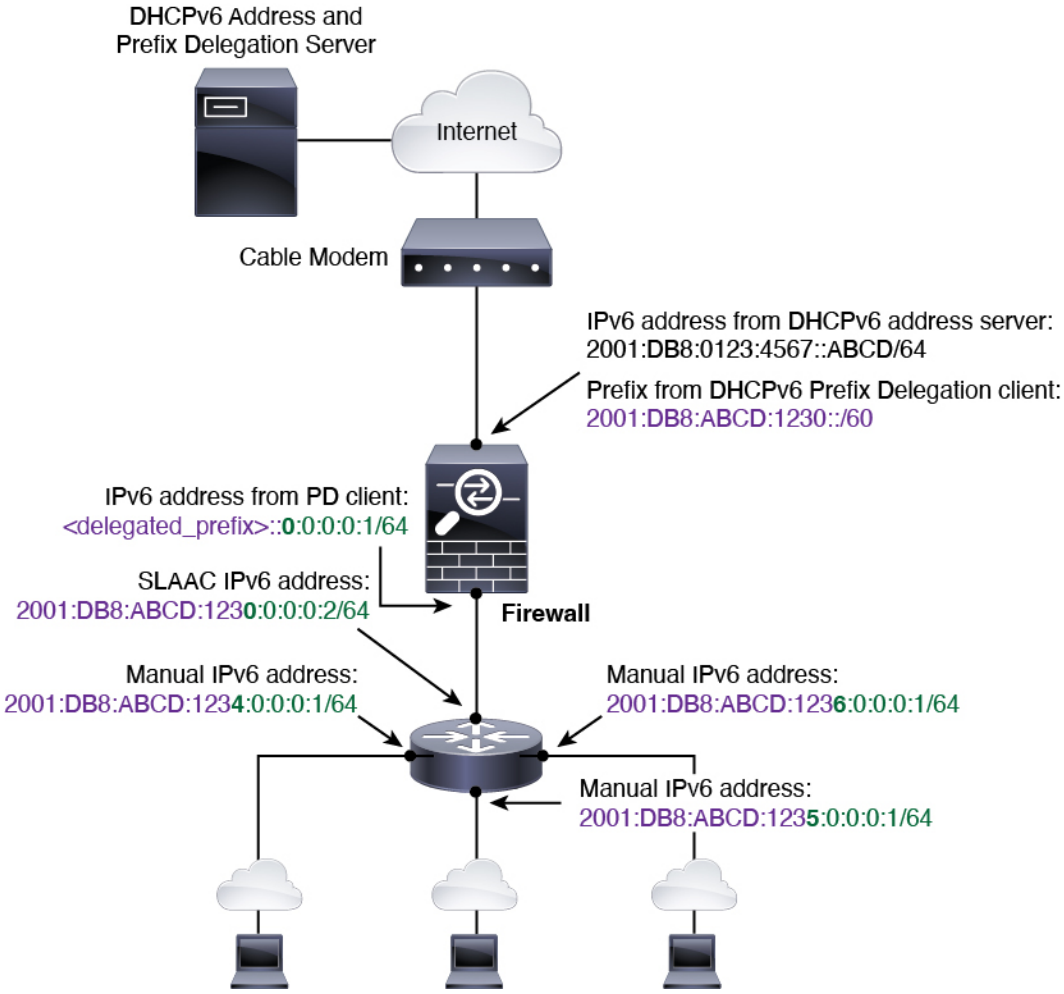
IPv6 プレフィックス委任 /64 サブネットの例

次の例では、ASA が DHCPv6 アドレスクライアントを使用して、外部インターフェイス上で IP アドレスを受け取るところを示しています。また、ASA は DHCPv6 プレフィックス委任クライアントを使用して代理プレフィックスを取得します。ASA は、委任されたプレフィックスを /64 ネットワークにサブネット化し、委任されたプレフィックスと手動で設定されたサブネット（::0、::1、または ::2）と各インターフェイスの IPv6 アドレス（0:0:0:1）を使用して、動的に内部インターフェイスにグローバル IPv6 アドレスを割り当てます。これらの内部インターフェイスに接続されている SLAAC クライアントは、各 /64 サブネットの IPv6 アドレスを取得します。



IPv6 プレフィックス委任 /62 サブネットの例

次の例は、ASA が 4/62 サブネットにプレフィックスをサブネット化するところを示しています。2001:DB8:ABCD:123**0**::/62、2001:DB8:ABCD:123**4**::/62、2001:DB8:ABCD:123**8**::/62、2001:DB8:ABCD:123**C**::/62。ASA は、内部ネットワーク（::0）に 2001:DB8:ABCD:1230::/62 の利用可能な 64 サブネット 4 つのいずれかを使用します。ダウンストリーム ルータには、手動で追加の /62 サブネットを使用できます。図のルータは、内部インターフェイス（::4, ::5, and ::6）に 2001:DB8:ABCD:1234::/62 の利用可能な 4 つの /64 サブネットのうちの 3 つを使用します。この場合、内部ルータインターフェイスは委任されたプレフィックスを動的に取得できないため、ASA 上で委任されたプレフィックスを表示し、ルータ設定にそのプレフィックスを使用する必要があります。通常、リースが期限切れになった場合、ISP は既定のクライアントに同じプレフィックスを委任しますが、ASA が新しいプレフィックスを受け取った場合、新しいプレフィックスを使用するようルータ設定を変更する必要があります。DHCP の一意識別子（DUID）は、再起動後も存続します。



IPv6 プレフィックス委任クライアントの有効化

1 つ以上のインターフェイスで DHCPv6 プレフィクス委任クライアントをイネーブルにします。ASA は、サブネット化して内部ネットワークに割り当てることができる 1 つ以上の IPv6 プレフィックスを取得します。通常、プレフィックス委任クライアントをイネーブルにしたインターフェイスは DHCPv6 アドレス クライアントを使用して IP アドレスを取得し、その他の ASA インターフェイスだけが、委任されたプレフィックスから取得されるアドレスを使用します。

始める前に

- この機能は、ルーテッド ファイアウォール モードに限りサポートされています。
- この機能はマルチ コンテキスト モードではサポートされません。
- この機能は、クラスタリングではサポートされていません。
- この機能は管理専用インターフェイスでは設定できません。
- プレフィックス委任を使用する場合は、IPv6 トラフィックの中断を防ぐために、ASA IPv6 ネイバー探索のルータ アドバタイズメント間隔を DHCPv6 サーバーによって割り当てられるプレフィックスの推奨有効期間よりもはるかに小さい値に設定する必要があります。たとえば、DHCPv6 サーバーがプレフィックス委任の推奨有効期間を 300 秒に設定している場合は、ASA RA の間隔を 150 秒に設定する必要があります。推奨有効期間を設定するには、**show ipv6 general-prefix** コマンドを使用します。ASA RA の間隔を設定するには、IPv6 ネイバー探索の設定 （26 ページ）を参照してください。デフォルトは 200 秒です。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** の順に選択します。

ステップ 2 インターフェイスを選択して、[Edit] をクリックします。

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

ステップ 3 [IPv6] タブをクリックします。

ステップ 4 [Interface IPv6 DHCP] エリアで、[Client Prefix Delegation Name] ラジオボタンをクリックして、プレフィックス名を入力します。

ステップ 5 （任意） [Prefix Hint] フィールドで、受信する委任されたプレフィックスに関する 1 つ以上のヒントを提供します。

通常、特定のプレフィクス長（::/60 など）を要求しますが、以前に特定のプレフィックスを受信しており、リースの期限が切れるときにそれを確実に再取得したい場合には、そのプレフィックスの全体をヒントとして入力できます（2001:DB8:ABCD:1230::/60）。複数のヒント（異なるプレフィックスまたはプレフィックス長）を入力すると、どのヒントに従うのか、またはそもそもヒントに従うのかどうかが DHCP サーバーによって決定されます。

ステップ 6 [OK] をクリックします。

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

ステップ 7 [Apply] をクリックします。

ステップ 8 ASA インターフェイスのグローバル IP アドレスとしてプレフィックスのサブネットを割り当てるには、グローバル IPv6 アドレスの設定 （22 ページ） を参照してください。

ステップ 9 （任意） SLAAC クライアントにドメイン名とサーバー パラメータを提供するには、DHCPv6 ステートレス サーバーの設定 を参照してください。

ステップ 10 （任意） BGP でプレフィックスをアドバタイズするには、IPv6 ネットワークの設定 を参照してください。

グローバル IPv6 アドレスの設定

ルーテッド モードの任意のインターフェイスとトランスペアレント モードまたはルーテッド モードの BVI に対してグローバル IPv6 アドレスを設定するには、次の手順を実行します。

DHCPv6 およびプレフィクス委任オプションは、マルチ コンテキスト モードではサポートされていません。

（注） グローバルアドレスを設定すると、リンクローカルアドレスは自動的に設定されるため、別々に設定する必要はありません。ブリッジ グループについて、BVI でグローバル アドレスを設定すると、すべてのメンバー インターフェイスのリンクローカル アドレスが自動的に設定されます。

サブインターフェイスの場合、親インターフェイスの同じ Burned-In MAC Address を使用するので、MAC アドレスも手動で設定することをお勧めします。IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカル アドレスが可能になり、ASA で特定のインスタンスでのトラフィックの中断を避けることができます。手動MACアドレス、MTU、およびTCP MSS の設定を参照してください。

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** の順に選択します。

ステップ 2 インターフェイスを選択して、[Edit] をクリックします。

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

トランスペアレント モード、またはルーテッド モードのブリッジ グループの場合、BVI を選択します。トランスペアレントモードの場合は、管理専用インターフェイスも選択できます。

ステップ 3 [IPv6] タブをクリックします。

ステップ 4 [Enable IPv6] チェックボックスをオンにします。

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

ステップ 6 （ルーテッド インターフェイス）グローバル IPv6 アドレスを次のいずれかの方法で設定します。

フェールオーバーやクラスタリング、およびループバック インターフェイスの場合は、IP アドレスを手動で設定する必要がありますクラスタリングの場合、リンクローカルアドレスの手動設定はサポートされていません。

- ステートレスアドレス自動構成（SLAAC）：[インターフェイスIPv6アドレス（Interface IPv6 Addresses）] エリアで、[アドレス自動構成（Enable address autoconfiguration）] チェックボックスをオンにします。

  インターフェイス上でSLAACを有効にすると、受信したルータ アドバタイズメント メッセージのプレフィックスに基づいて IPv6 アドレスを設定します。SLAAC が有効になっている場合、インターフェイスのリンクローカルアドレスは、Modified EUI-64 インターフェイス ID に基づいて自動的に生成されます。

  （注）
  RFC 4862 では、SLAAC に構成されたホストはルータ アドバタイズメント メッセージを送信しないと規定していますが、Cisco ASA はこの場合、ルータ アドバタイズメント メッセージを送信します。メッセージを抑制するには、[Suppress RA] チェックボックスをオンにします。

  デフォルトルートをインストールする場合は、ドロップダウンメニューから [デフォルトの信頼dhcp（default trust dhcp）] または [デフォルトの信頼ignore（default trust ignore）] を選択します。[デフォルトの信頼dhcp（default trust dhcp）] では、Cisco ASA が信頼できるソース（IPv6アドレスを提供したのと同じサーバー）のルータアドバタイズメントからのデフォルトルートのみを使用するよう指定します。[デフォルトの信頼ignore（default trust ignore）] では、別のネットワークからのルータアドバタイズメントを使用できるよう指定します。これは、リスクの高い方法になります。

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

  1. [Interface IPv6 Addresses] 領域で、[Add] をクリックします。

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

  2. [Address/Prefix Length] フィールドに入力する値は、使用する方法によって異なります。

     - 完全なグローバルアドレス：手動でアドレス全体を入力する場合は、完全なアドレスに加え、プレフィックス長を入力します。

- Modified EUI 64 形式：IPv6 プレフィックスとプレフィックス長を入力した後、[EUI 64] チェックボックスをオンにします。これにより、Modified EUI 64 形式を使用してインターフェイス ID が生成されるようになります。たとえば、2001:0DB8::BA98:0:3210/48（完全なアドレス）または 2001:0DB8::/48（プレフィックス、[EUI 64] はオン）。
- 委任されたプレフィックス：委任されたプレフィックスから IPv6 プレフィックスを生成するには、IPv6 アドレスとプレフィックス長を入力します。次に、DHCPv6 プレフィクス委任クライアントに設定したプレフィックス名（IPv6 プレフィックス委任クライアントの有効化 （21 ページ）を参照）を [Prefix Name] フィールドに入力してから、[Add] をクリックします。

  通常、委任されたプレフィクスは /60 以下であるため、複数 /64 ネットワークにサブネット化できます。接続されるクライアント用に SLAAC をサポートする必要がある場合は、/64 がサポートされるサブネット長です。/60 サブネットを補完するアドレス（1:0:0:0:1 など）を指定する必要があります。プレフィックスが /60 未満の場合は、アドレスの前に :: を入力します。たとえば、委任されたプレフィクスが 2001:DB8:1234:5670::/60 である場合、このインターフェイスに割り当てられるグローバル IP アドレスは 2001:DB8:1234:5671::1/64 です。ルータ アドバタイズメントでアドバタイズされるプレフィクスは 2001:DB8:1234:5671::/64 です。この例では、プレフィクスが /60 未満である場合、プレフィックスの残りのビットは、前に配置される :: によって示されるように、0 になります。たとえば、プレフィクスが 2001:DB8:1234::/48 である場合、IPv6 アドレスは 2001:DB8:1234::1:0:0:0:1/64 になります。

3. [OK] をクリックします。

- DHCPv6 を使用してアドレスを取得します。
  1. [Interface IPv6 DHCP] 領域で、[Enable DHCP] チェックボックスをオンにします。
  2. （オプション）ルータ アドバタイズメントからデフォルト ルータを取得する場合は、[Enable Default] チェックボックスをオンにします。

ステップ 7 （BVI インターフェイス）BVI に手動でグローバルアドレスを割り当てます。トランスペアレント モードの管理インターフェイスでも、この方法を使用します。

a) [Interface IPv6 Addresses] 領域で、[Add] をクリックします。

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

b) [Address/Prefix Length] フィールドに、完全なグローバル IPv6 アドレスと IPv6 プレフィックスの長さを入力します。

c) [OK] をクリックします。

ステップ 8 [OK] をクリックします。

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

（オプション）リンクローカル アドレスの自動設定

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

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

始める前に

ルーテッド モードのみでサポートされます。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** の順に選択します。

ステップ 2 インターフェイスを選択して、[Edit] をクリックします。

ルーテッド モードのブリッジグループの場合は、BVI を選択します。

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

ステップ 3 [IPv6] タブをクリックします。

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

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

ルーテッド モードのブリッジグループでは、BVI に対して IPv6 を有効にすると、すべてのメンバー インターフェイスのリンクローカル アドレスが生成されます。

ステップ 5 [OK] をクリックします。

（オプション）リンクローカル アドレスの手動設定

グローバル アドレスを設定する必要がなく、リンクローカル アドレスだけを設定する必要がある場合は、リンクローカル アドレスを手動で定義できます。Modified EUI-64 形式に基づくリンクローカルアドレスを自動的に割り当てることを推奨します。たとえば、その他のデバイスで Modified EUI-64 形式の使用が強制される場合、手動で割り当てたリンクローカル アドレスによりパケットがドロップされることがあります。

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

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** の順に選択します。

ステップ 2 インターフェイスを選択して、[Edit] をクリックします。

ブリッジグループの場合は、ブリッジグループ メンバー インターフェイスを選択します。

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

ステップ 3 [IPv6] タブをクリックします。

ステップ 4 （任意）ローカル リンクの IPv6 アドレスに Modified EUI-64 形式のインターフェイス識別子の使用を適用するには、[Enforce EUI-64] チェックボックスをオンにします。

ステップ 5 リンクローカル アドレスを設定するには、[Link-local address] フィールドにアドレスを入力します。

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

ステップ 6 [OK] をクリックします。

IPv6 ネイバー探索の設定

IPv6 ネイバー探索プロセスは、ICMPv6 メッセージおよび要請ノード マルチキャスト アドレスを使用して、同じネットワーク（ローカル リンク）上のネイバーのリンク層アドレスを特定し、ネイバーの読み出し可能性を確認し、隣接ルータを追跡します。

ノード（ホスト）はネイバー探索を使用して、接続リンク上に存在することがわかっているネイバーのリンク層アドレスの特定や、無効になったキャッシュ値の迅速なパージを行います。また、ホストはネイバー探索を使用して、ホストに代わってパケットを転送しようとしている隣接ルータを検出します。さらに、ノードはこのプロトコルを使用して、どのネイバーが到達可能でどのネイバーがそうでないかをアクティブに追跡するとともに、変更されたリンク層アドレスを検出します。ルータまたはルータへのパスが失われると、ホストは機能している代替ルータまたは代替パスをアクティブに検索します。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** の順に選択します。

ステップ 2 IPv6 ネイバーの設定を行う IPv6 インターフェイスを選択し、[Edit] をクリックします。

ステップ 3 [IPv6] タブをクリックします。

ステップ 4 許可される [DAD Attempts] の回数を入力します。

値の範囲は 0 ～ 600 です。この値が 0 の場合、指定されたインターフェイスでの DAD 処理が無効化されます。デフォルト値は 1 件です。

DAD は、割り当てられる前に、新しいユニキャスト IPv6 アドレスの一意性を確認し、ネットワークに重複する IPv6 アドレスが検出されていないかをリンク ベースで確認します。ASA は、ネイバー送信要求メッセージを使用して、DAD を実行します。

重複アドレスが検出されると、そのアドレスの状態は DUPLICATE に設定され、アドレスは使用対象外となり、次のエラー メッセージが生成されます。

```
325002: Duplicate address ipv6_address/MAC_address on interface
```

重複アドレスがインターフェイスのリンクローカルアドレスであれば、インターフェイス上で IPv6 パケットの処理は無効になります。重複アドレスがグローバル アドレスであれば、そのアドレスは使用されません。

ステップ 5 [NS Interval]（ミリ秒単位）に入力して、IPv6 ネイバー要請メッセージの再送信間隔を設定します。

value 引数の有効な値は、1000 ～ 3600000 ミリ秒です。

ローカル リンク上にある他のノードのリンクレイヤ アドレスを検出するため、ノードからネイバー送信要求メッセージ（ICMPv6 Type 135）がローカル リンクに送信されます。ネイバー送信要求メッセージを受信すると、宛先ノードは、ネイバー アドバタイズメント メッセージ（ICPMv6 Type 136）をローカル リンク上に送信して応答します。

送信元ノードがネイバーアドバタイズメントを受信すると、送信元ノードと宛先ノードが通信できるようになります。ネイバー送信要求メッセージは、ネイバーのリンク層アドレスが識別された後に、ネイバーの到達可能性の確認にも使用されます。ノードがあるネイバーの到達可能性を検証する場合、ネイバー送信要求メッセージ内の宛先アドレスとして、そのネイバーのユニキャスト アドレスを使用します。

ネイバー アドバタイズメント メッセージは、ローカル リンク上のノードのリンク層アドレスが変更されたときにも送信されます。

ステップ 6 [Reachable Time]（秒単位）に入力して、リモート IPv6 ノードに到達可能な時間を設定します。

到達可能時間を 0 ～ 3600000 ミリ秒で設定します。時間を 0 に設定すると、到達可能時間は「不明」として送信されます。到達可能時間の値を設定し、追跡するのは、受信デバイスの役割です。

ネイバー到達可能時間を設定すると、使用できないネイバーを検出できます。時間を短く設定すると、使用できないネイバーをより早く検出できます。ただし、時間を短くするほど、IPv6 ネットワーク帯域幅とすべての IPv6 ネットワーク デバイスの処理リソースの消費量が増えます。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。

ステップ 7 [RA Lifetime]（秒単位）に入力して、ローカル リンク上のノードが、ASA をリンク上のデフォルト ルータと見なす時間の長さを設定します。

値の範囲は 0 ～ 9000 秒です。0 を入力すると、ASA は選択したインターフェイスのデフォルト ルータと見なされません。

ステップ 8 ルータ アドバタイズメントを抑制するには、[Suppress RA] チェックボックスをオンにします。

ルータ要請メッセージ（ICMPv6 Type 133）に応答して、ルータ アドバタイズメント メッセージ（ICMPv6 Type 134）が自動的に送信されます。ルータ要請メッセージは、システムの起動時にホストから送信されるため、ホストは、次にスケジュールされているルータ アドバタイズメント メッセージを待つことなくただちに自動設定を行うことができます。

ASA で IPv6 プレフィックスを提供する必要がないインターフェイス（外部インターフェイスなど）では、これらのメッセージを無効にできます。

このオプションを有効にすると、ASA がリンク上では IPv6 ルータではなく、通常の IPv6 ネイバーのように見えるようになります。

ステップ 9 [RA Interval] に入力して、IPv6 ルータ アドバタイズメントの送信間隔を設定します。

有効値の範囲は 3 ～ 1800 秒です。デフォルトは 200 秒です。

ルータ アドバタイズメント送信間隔の値をミリ秒単位で追加するには、[RA Interval in Milliseconds] チェックボックスをオンにして、500 ～ 1800000 の範囲で値を入力します。

他の IPv6 ノードと同期しないように、Cisco ASA は設定値（ジッター）をランダムに調整します。

ステップ 10 [ホストはアドレス設定でDHCPを使用する（Hosts should use DHCP for address config）] チェックボックスをオンにして、派生されるステートレス自動設定のアドレス以外のアドレスを取得するにはDHCPv6を使用する必要があることを、IPv6ステートレスアドレス自動設定（SLAAC）クライアントに通知します。

このオプションは、IPv6 ルータ アドバタイズメント パケットの管理対象アドレス設定フラグを設定します。

ステップ 11 [ホストは非アドレスの設定にDHCPを使用する（Hosts should use DHCP for non-address config）] チェックボックスをオンにして、DNS サーバーアドレスなどの追加情報を DHCPv6 から取得するには DHCPv6 を使用する必要があることを IPv6 SLAAC クライアントに通知します。

このオプションは、IPv6 ルータ アドバタイズメント パケットのその他のアドレス設定フラグを設定します。

ステップ 12 IPv6 ルータ アドバタイズメントに含める IPv6 プレフィックスを設定します。

a) [Interface IPv6 Prefixes] 領域で、[Add] をクリックします。
b) デフォルトのプレフィックスを使用するには、[Address/Prefix Length] に入力するか、[Default] チェック ボックスをオンにします。
c) IPv6 アドレスを手動で設定するようにホストに強制するには、[No Auto-Configuration] チェックボックスをオンにします。指定したプレフィックスのローカルリンク上のホストでは、IPv6 SLAAC を使用できません。
d) プレフィックス アドバタイズメントを無効にするには、[No Advertisements] チェックボックスをオンにします。[デフォルト（Default）] プレフィックスの場合、この設定はオンリンクプレフィックスにのみ適用されます。特定のオフリンクプレフィックスに [アドバタイズしない（No Advertisements）] を指定しない限り、オフリンクプレフィックスは引き続きアドバタイズされます。

e) 指定したプレフィックスをオフリンクとして設定するには、[Off Link] チェック ボックスをオンにします。プレフィクスはLビットクリアでアドバタイズされます。プレフィックスは、接続されたプレフィックスとしてルーティング テーブルに挿入されません。

f) [Prefix Lifetime] 領域で、[Lifetime Duration] または [Lifetime Expiration Date] を指定します。

優先有効期間を過ぎると、アドレスは廃止状態になります。廃止状態のアドレスの使用は推奨されませんが、固く禁じられているわけではありません。有効期間の期限が切れた後に、アドレスは無効になり、使用できません。有効ライフタイムは優先ライフタイムと同じかそれより長い必要があります。

- [Lifetime Duration]：値の範囲は 0 ～ 4294967295 です。デフォルトの有効期間は 2592000（30 日間）です。デフォルトの優先有効期間は 604800（7 日間）です。最大値は無限大です。
- [Lifetime Expiration Date]：有効かつ優先する月と日をドロップダウンリストから選択し、時間を hh:mm 形式で入力します。

g) [OK] をクリックして設定内容を保存します。

ステップ 13 [OK] をクリックします。

ステップ 14 スタティック IPv6 ネイバーを設定します。

次のガイドラインと制限事項は、スタティック IPv6 ネイバーの設定に適用されます。

- この機能は、スタティック ARP エントリの追加に似ています。IPv6 ネイバー探索プロセスによる学習を通して、指定された IPv6 アドレスのエントリがネイバー探索キャッシュにすでに存在する場合、エントリは自動的にスタティック エントリに変換されます。これらのエントリは、copy コマンドを使用して設定を保存するときに設定に保存されます。
- IPv6 ネイバー探索キャッシュ内のスタティック エントリがネイバー探索プロセスによって変更されることはありません。
- 生成された ICMP syslog は、IPv6 ネイバー エントリの定期的な更新に起因します。IPv6 ネイバー エントリの ASA デフォルト タイマーは 30 秒であるため、ASA は 30 秒おきに ICMPv6 ネイバー探索および応答パケットを生成します。ASA にフェールオーバー LAN および IPv6 アドレスで設定された状態インターフェイスの両方がある場合は、30 秒ごとに、ICMPv6 ネイバー探索および応答パケットが、設定済みのリンクローカル IPv6 アドレスの 両方の ASA で生成されます。また、各パケットは複数の syslog（ICMP 接続およびローカル ホストの作成またはティアダウン）を生成するため、連続 ICMP syslog が生成されているように見えることがあります。IPV6 ネイバー エントリのリフレッシュ時間は、通常のデータ インターフェイスに設定可能ですが、フェールオーバー インターフェイスでは設定可能ではありません。ただし、この ICMP ネイバー探索トラフィックの CPU の影響はわずかです。

ダイナミックに検出されたネイバーの表示とクリア （30 ページ）も参照してください。

a) [Configuration] > [Device Management] > [Advanced] > [IPv6 Neighbor Discovery Cache] を選択します。

b) [Add] をクリックします。

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

c) [Interface Name] ドロップダウン リストから、ネイバーを追加するインターフェイスを選択します。
d) [IP Address] フィールドにローカル データリンク アドレスに対応する IPv6 アドレスを入力するか、省略符号（[...]）をクリックしてアドレスを参照します。
e) [MAC address] フィールドに、ローカルのデータ回線（ハードウェア）MAC アドレスを入力します。
f) [OK] をクリックします。

ステップ 15 [Apply] をクリックして、実行コンフィギュレーションを保存します。

ダイナミックに検出されたネイバーの表示とクリア

ホストまたはノードがネイバーと通信する場合、ネイバーはネイバー探索キャッシュに追加されます。ネイバーがキャッシュから削除されるのは、そのネイバーとの通信が行われなくなったときです。

ダイナミックに検出されたネイバーを表示し、そのネイバーを IPv6 ネイバー探索キャッシュから削除するには、次の手順を実行します。

手順

ステップ 1 [Monitoring] > [Interfaces] > [IPv6 Neighbor Discovery Cache] を選択します。

[IPv6 Neighbor Discovery Cache] ペインでは、スタティックおよびダイナミックに検出されたネイバーをすべて表示できます。

ステップ 2 ダイナミックに検出されたネイバーをすべてキャッシュから削除するには、[Clear Dynamic Neighbor Entries] をクリックします。

ダイナミックに検出されたネイバーがキャッシュから削除されます。

（注）
この手順では、ダイナミックに検出されたネイバーだけがキャッシュから削除され、スタティックなネイバーは削除されません。

ルーテッドモードおよびトランスペアレントモードのインターフェイスのモニタリング

インターフェイスの統計情報、ステータス、PPPoE などをモニターできます。

（注） Firepower および Cisco Secure Firewall モデルの場合、一部の統計は Cisco ASA コマンドで表示されません。FXOS コマンドを使用して、より詳細なインターフェイス統計情報を表示する必要があります。

- /eth-uplink/fabric# **show interface**
- /eth-uplink/fabric# **show port-channel**
- /eth-uplink/fabric/interface# **show stats**

詳細については、『FXOS troubleshooting guide』を参照してください。

インターフェイス統計情報

- **[Monitoring] > [Interfaces] > [Interface Graphs]**

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

- **[Monitoring] > [Interfaces] > [Interface Graphs] > [Graph/Table]**

  選択した統計情報のグラフを表示します。[Graph] ウィンドウには、最大 4 つのグラフおよびテーブルを同時に表示することができます。デフォルトで、グラフまたはテーブルにリアルタイムな統計情報が表示されます。履歴メトリックをイネーブルにすると、過去の期間の統計情報を表示できます。

DHCP Information

- **[Monitoring] > [Interfaces] > [DHCP] > [DHCP Client Lease Information]**

  この画面には、設定されている DHCP クライアントの IP アドレスが表示されます。

- **[Monitoring] > [Interfaces] > [DHCP] > [IPV6 DHCP Client PD Statistics]**

  この画面は DHCPv6 プレフィックス委任クライアント統計情報を表示し、送受信されたメッセージ数の出力を表示します。

- **[Monitoring] > [Interfaces] > [DHCP] > [IPV6 DHCP Client Statistics]**

  この画面は DHCPv6 クライアント統計情報を表示し、送受信されたメッセージ数の出力を表示します。

- **[Monitoring] > [Interfaces] > [DHCP] > [IPV6 DHCP Interface Statistics]**

  この画面は、すべてのインターフェイスの DHCPv6 情報を表示します。インターフェイスが DHCPv6 ステートレス サーバー構成用に設定されている場合（DHCPv6 ステートレス サーバーの設定 を参照）、この画面はサーバーによって使用されている DHCPv6 プール

をリストします。インターフェイスに DHCPv6 アドレス クライアントまたはプレフィックス委任クライアントの設定がある場合、この画面は各クライアントの状態とサーバーから受信した値を表示します。この画面は、DHCP サーバーまたはクライアントのメッセージの統計情報も表示します。

- **[Monitoring]** > **[Interfaces]** > **[DHCP]** > **[IPV6 DHCP HA Statistics]**

  この画面は、DUID 情報がフェールオーバー ユニット間で同期された回数を含め、フェールオーバー ユニット間のトランザクションの統計情報を表示します。

スタティック ルート トラッキング

- **[Monitoring] > [Interfaces] > [interface connection] > [Track Status]**

  追跡対象オブジェクトに関する情報を表示します。

- **[Monitoring] > [Interfaces] > [interface connection] > [Monitoring Statistics]**

  SLA モニタリング プロセスの統計情報を表示します。

PPPoE

- [Monitoring] > [Interfaces] > [PPPoE Client] > [PPPoE Client Lease Information]

  現在の PPPoE 接続に関する情報を表示します。

ダイナミック ACL

[Monitoring] > [Interfaces] > [Dynamic ACLs]

ダイナミック ACL のテーブルを表示します。ダイナミック ACL は、ASA によって自動的に作成、アクティブ化、および削除される点を除いて、ユーザー設定の ACL と機能上同じです。これらの ACL はコンフィギュレーションには表示されず、このテーブルだけに表示されます。ダイナミック ACL は、ACL ヘッダーの “(dynamic)” キーワードで区別されます。

ルーテッドモードおよびトランスペアレントモードのインターフェイスの例

2 つのブリッジグループを含むトランスペアレント モードの例

トランスペアレント モードの次の例では、3 つのインターフェイスそれぞれの 2 つのブリッジグループと管理専用インターフェイスを示します。

```
interface gigabitethernet 0/0
```

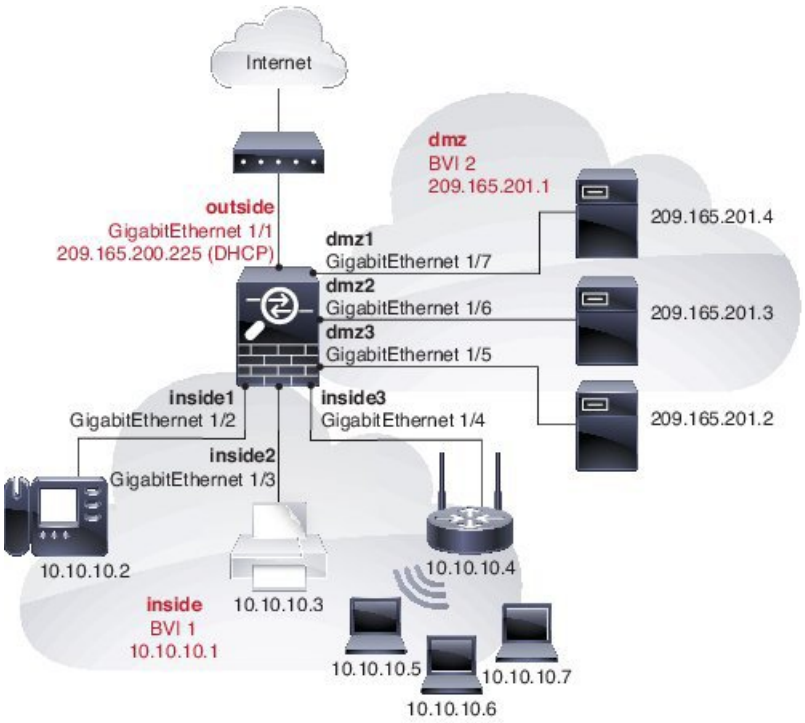
```
  nameif inside1
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 0/1
  nameif outside1
  security-level 0
  bridge-group 1
  no shutdown
interface gigabitethernet 0/2
  nameif dmz1
  security-level 50
  bridge-group 1
  no shutdown
interface bvi 1
  ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2

interface gigabitethernet 1/0
  nameif inside2
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/1
  nameif outside2
  security-level 0
  bridge-group 2
  no shutdown
interface gigabitethernet 1/2
  nameif dmz2
  security-level 50
  bridge-group 2
  no shutdown
interface bvi 2
  ip address 10.3.5.8 255.255.255.0 standby 10.3.5.9

interface management 0/0
  nameif mgmt
  security-level 100
  ip address 10.2.1.1 255.255.255.0 standby 10.2.1.2
  no shutdown
```

2 つのブリッジグループを含むスイッチド LAN セグメントの例

次の例では、3 つのインターフェイスのそれぞれと 1 つの通常の外部用ルーテッド インターフェイスに 2 つのブリッジグループを設定します。ブリッジグループ 1 は内部であり、ブリッジグループ 2 はパブリック Web サーバーが設定された dmz です。ブリッジグループのメンバーインターフェイスは、各メンバーのセキュリティ レベルが等しく、同一のセキュリティ通信が可能になっているため、ブリッジグループ内で自由に通信できます。内部メンバーのセキュリティ レベルが 100 で、dmz メンバーのセキュリティ レベルも 100 ですが、これらのセキュリティ レベルは BVI 間通信には適用されません。BVI のセキュリティ レベルのみ、BVI 間のトラフィックに影響します。BVI と外部のセキュリティ レベル（100、50、および 0）は、内部から dmz と内部から外部、および dmz から外部へのトラフィックを暗黙的に許可します。dmz 上のサーバーに対するトラフィックを許可するために、アクセス ルールが外部に適用されます。




```
interface gigabitethernet 1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface gigabitethernet 1/2
  nameif inside1
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 1/3
  nameif inside2
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 1/4
  nameif inside3
  security-level 100
  bridge-group 1
  no shutdown
!
interface bvi 1
  nameif inside
  security-level 100
  ip address 10.10.10.1 255.255.255.0
!
interface gigabitethernet 1/5
  nameif dmz1
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/6
  nameif dmz2
```

```
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/7
  nameif dmz3
  security-level 100
  bridge-group 2
  no shutdown
!
interface bvi 2
  nameif dmz
  security-level 50
  ip address 209.165.201.1 255.255.255.224
!
same-security-traffic permit inter-interface
!
# Assigns IP addresses to inside hosts
dhcpd address 10.10.10.2-10.10.10.200 inside
dhcpd enable inside
!
# Applies interface PAT for inside traffic going outside
nat (inside1,outside) source dynamic any interface
nat (inside2,outside) source dynamic any interface
nat (inside3,outside) source dynamic any interface
!
# Allows outside traffic to each server for specific applications
object network server1
  host 209.165.201.2
object network server2
  host 209.165.201.3
object network server3
  host 209.165.201.4
!
# Defines mail services allowed on server3
object-group service MAIL
  service-object tcp destination eq pop3
  service-object tcp destination eq imap4
  service-object tcp destination eq smtp
!
# Allows access from outside to servers on the DMZ
access-list SERVERS extended permit tcp any object server1 eq www
access-list SERVERS extended permit tcp any object server2 eq ftp
access-list SERVERS extended permit tcp any object server3 object-group MAIL
access-group SERVERS in interface outside
```

ルーテッドモードおよびトランスペアレントモードのインターフェイスの履歴

機能名	プラットフォームリリース	機能情報
IPv6 ネイバー探索	7.0(1)	この機能が導入されました。 次の画面が導入されました。 [Monitoring] > [Interfaces] > [IPv6 Neighbor Discovery Cache.Configuration] > [Device Management] > [Advanced] > [IPv6 Neighbor Discovery Cache.Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [IPv6]。
トランスペアレント モードの IPv6 のサポート	8.2(1)	トランスペアレント ファイアウォール モードの IPv6 サポートが導入されました。
トランスペアレント モードのブリッジ グループ	8.4(1)	セキュリティ コンテキストのオーバーヘッドを避けたい場合、またはセキュリティ コンテキストを最大限に使用したい場合、インターフェイスをブリッジ グループにグループ化し、各ネットワークに 1 つずつ複数のブリッジ グループを設定できます。ブリッジ グループのトラフィックは他のブリッジ グループから隔離されます。シングル モードまたはコンテキストごとに、それぞれ 4 つのインターフェイスからなる最大 8 個のブリッジ グループを設定できます。 次の画面が変更または導入されました。 **[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces]** [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Bridge Group Interface] [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface]
IPv6 DHCP リレーのアドレス設定フラグ	9.0(1)	次の画面が変更されました。[Configuration] > [Device Setup] > [Interfaces] > [IPv6]。

機能名	プラットフォームリリース	機能情報
トランスペアレント モードのブリッジ グループの最大数が 250 に増加	9.3(1)	ブリッジ グループの最大数が 8 個から 250 個に増えました。シングル モードでは最大 250 個、マルチ モードではコンテキストあたり最大 8 個のブリッジ グループを設定でき、各ブリッジ グループには最大 4 個のインターフェイスを追加できます。 次の画面が変更されました。 **[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces]** [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Bridge Group Interface] **[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface]**
トランスペアレント モードで、ブリッジ グループごとのインターフェイス数が最大で 64 に増加	9.6(2)	ブリッジ グループあたりのインターフェイスの最大数が 4 から 64 に拡張されました。 変更された画面はありません。

機能名	プラットフォームリリース	機能情報
IPv6 DHCP	9.6(2)	ASA で IPv6 アドレッシングの次の機能がサポートされました。 • DHCPv6 アドレス クライアント：ASA は DHCPv6 サーバーから IPv6 グローバル アドレスとオプションのデフォルト ルートを取得します。 • DHCPv6 プレフィックス委任クライアント：ASA は DHCPv6 サーバーから委任プレフィックスを取得します。ASA は、これらのプレフィックスを使用して他の ASA インターフェイスのアドレスを設定し、ステートレス アドレス自動設定（SLAAC）クライアントが同じネットワーク上で IPv6 アドレスを自動設定できるようにします。 • 委任プレフィックスの BGP ルータ アドバタイズメント • DHCPv6 ステートレス サーバー：SLAAC クライアントが ASA に情報要求（IR）パケットを送信すると、ASA はドメインインネームなどの他の情報を SLAAC クライアントに提供します。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。 次の画面が追加または変更されました。 **[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add Interface] > [IPv6]** **[Configuration] > [Device Management] > [DHCP] > [DHCP Pool]** **[Configuration] > [Device Setup] > [Routing] > [BGP] > [IPv6 Family] > [Networks]** **[Monitoring] > [interfaces] > [DHCP]**

機能名	プラットフォームリリース	機能情報
Integrated Routing and Bridging（IRB）	9.7(1)	Integrated Routing and Bridging（統合ルーティングおよびブリッジング）は、ブリッジグループとルーテッドインターフェイス間をルーティングする機能を提供します。ブリッジグループとは、ASAがルートの代わりにブリッジするインターフェイスのグループのことです。ASAは、ASAがファイアウォールとして機能し続ける点で本来のブリッジとは異なります。つまり、インターフェイス間のアクセス制御が実行され、通常のファイアウォール検査もすべて実行されます。以前は、トランスペアレントファイアウォールモードでのみブリッジグループの設定が可能だったため、ブリッジグループ間でのルーティングはできませんでした。この機能を使用すると、ルーテッド ファイアウォール モードのブリッジグループの設定と、ブリッジグループ間およびブリッジグループとルーテッド インターフェイス間のルーティングを実行できます。ブリッジグループは、ブリッジ仮想インターフェイス（BVI）を使用して、ブリッジグループのゲートウェイとして機能することによってルーティングに参加します。そのブリッジグループに指定する ASA 上に別のインターフェイスが存在する場合、Integrated Routing and Bridging（IRB）は外部レイヤ2スイッチの使用に代わる手段を提供します。ルーテッドモードでは、BVI は名前付きインターフェイスとなり、アクセス ルールやDHCPサーバーなどの一部の機能に、メンバーインターフェイスとは個別に参加できます。 トランスペアレント モードでサポートされるマルチ コンテキスト モードや ASA クラスタリングの各機能は、ルーテッド モードではサポートされません。マルチキャスト ルーティングとダイナミック ルーティングの機能も、BVI ではサポートされません。 次の画面が変更されました。 **[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces]** **[Configuration] > [Device Setup] > [Routing] > [Static Routes]** **[Configuration] > [Device Management] > [DHCP] > [DHCP Server]** **[Configuration] > [Firewall] > [Access Rules]** **[Configuration] > [Firewall] > [EtherType Rules]**

機能名	プラットフォームリリース	機能情報
31 ビット サブネット マスク	9.7(1)	ルーテッドインターフェイスに関しては、ポイントツーポイント接続向けの 31 ビットのサブネット に IP アドレスを設定できます。31 ビット サブネットには2つのアドレスのみが含まれます。通常、サブネットの最初と最後のアドレスはネットワーク用とブロードキャスト用に予約されており、2アドレス サブネットは使用できません。ただし、ポイントツーポイント接続があり、ネットワーク アドレスやブロードキャスト アドレスが不要な場合は、IPv4 形式でアドレスを保持するのに 31 サブネット ビットが役立ちます。たとえば、2 つの ASA 間のフェールオーバーリンクに必要なアドレスは2つだけです。リンクの一方の側から送信されるパケットはすべてもう一方の側で受信され、ブロードキャスティングは必要ありません。また、SNMP や Syslog を実行する管理ステーションを直接接続することもできます。この機能は、ブリッジグループ用の BVI、またはマルチキャストルーティングではサポートされていません。 次の画面が変更されました。 **[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add Interface] > [General]**

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。

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。