



# 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

この章では、ルーテッドファイアウォールモードおよび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コンフィギュレーションを実行するためのタスクについて説明します。



(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 \(2 ページ\)](#)
- [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ガイドラインおよび要件 \(3 ページ\)](#)
- [ルーテッドモードのインターフェイスの設定 \(5 ページ\)](#)
- [トランスペアレントモードのブリッジグループインターフェイスの設定 \(9 ページ\)](#)
- [IPv6 アドレスの設定 \(14 ページ\)](#)
- [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 \(27 ページ\)](#)
- [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 \(28 ページ\)](#)
- [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 \(30 ページ\)](#)

# 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は一意のサブネット上に IP アドレスを必要とします。

ブリッジ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は同じネットワーク内にあります。ブリッジグループはブリッジネットワーク上に IP アドレスを持つブリッジ仮想インターフェイス (BVI) で表されます。ルーテッドモードはルーテッドインターフェイスのみをサポートします。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。

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。

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спекションエンジン：一部のアプリケーションインспек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спек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спек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спекション エンジン : SQL\*Net (旧称 OraServ) ポートとの制御接続が一对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。

# 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ガイドラインおよび要件

### 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。

### フェールオーバー

- 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、フェールオーバーの章も参照してください。
- フェー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 と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およびクラスタリングではサポートされません。

### サポート モデル

- ASASM では、PPPoE および DHCP はサポートされません。

### ASASM の VLAN ID

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

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

### 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。
- IPv4 の場合は、管理トラフィックと、ASA を通過するトラフィックの両方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。IPv6 アドレスは BVI でサポートされませんが必須ではありません。
- 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。
- 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 *default* 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 管理 インターフェイスでサポートされません。
- 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したときに、既存の接続がタイムアウトするまで待機せずに新しいセキュリティ情報を使用する必要がある場合は、**clear local-host** コマンドを使用して接続をクリアできます。

## 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。

**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。

**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。

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

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

（注） フェールオーバーで使用する場合は、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 および PPPoE はサポートされません。[Configuration] > [Device Management] > [High Availability] > [Failover] > [Interfaces] タブのスタンバイ IP アドレスを設定します。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できず、リンク ステータスをトラッキングすることしかできません。

- 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ストレ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 of 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は、DHCP パケット ヘッダーでブロードキャスト フラグを 1 に設定するには、[Enable DHCP Broadcast flag for DHCP request and discover messages] をオンにします。

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

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名とパスワードを保存するには、[Store Username and Password in Local Flash] チェック ボックスをオンにします。  
ASA は、NVRAM の特定の場所にユーザ名とパスワードを保存します。Auto Update Server が **clear config** コマンドを ASA に送信して、接続が中断されると、ASA は NVRAM からユーザ名とパスワードを読み取り、アクセスコンセントレータに対して再度認証できます。
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、アドレスリ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](#) (14 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](#) (8 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。

## トランスペアレントモードの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でのみ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、接続されているネットワークと同じサブネット上になければなりません。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。

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 (ID301) 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** 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 4** (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 5** [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、冗長インターフェイス）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。
- 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（12 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、冗長インターフェイス、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。

**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。

#### 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 (ID301) 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。
- モデルに管理インターフェイスが含まれていない場合、データインターフェイスからトランスペアレントファイアウォールを管理する必要があります。この手順はスキップします。（たとえば、ASASM の場合。） 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 ポートチャンネル 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 Neighbor Discovery 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イネーブルになっていると、そのインターフェイスIDがModified EUI-64 形式を採用していることを確認するために、インターフェイスで受信した IPv6 パケットの送信元アドレスが送信元 MAC アドレスに照らして確認されます。IPv6 パケットがインターフェイス ID に Modified EUI-64 形式を採用していない場合、パケットはドロップされ、次のシステム ログ メッセージが生成されます。

```
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、クライアント インターフェイス (たとえば、ケーブル モデムに接続された外部インターフェイス) が 1 つ以上の IPv6 プレフィックスを受け取れるように DHCPv6 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内部インターフェイスをサブネット化および指定することができます。

## IPv6 プレフィックス委任の概要

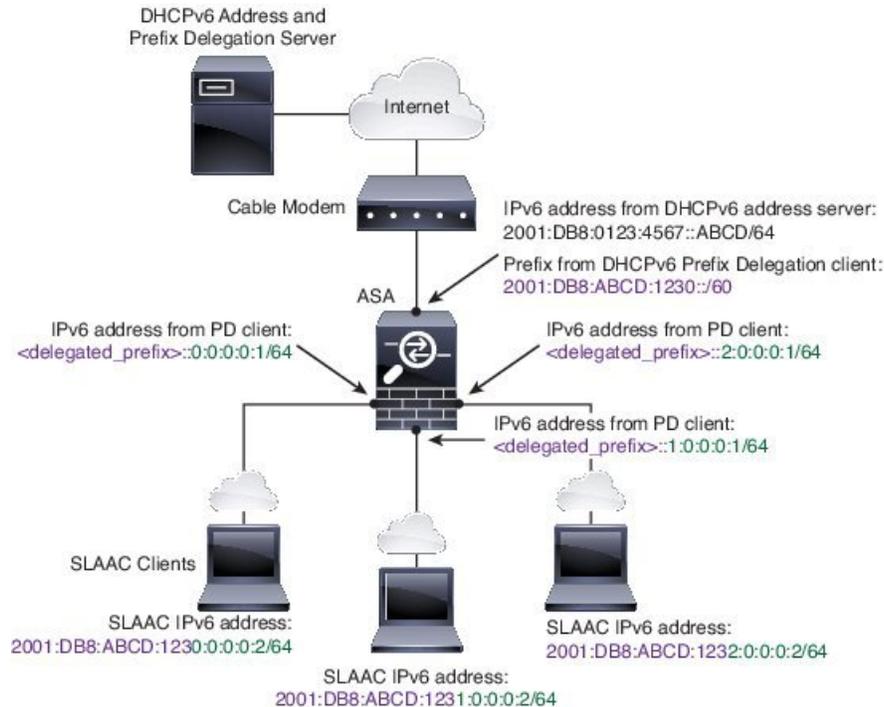
ASA は、クライアント インターフェイス (たとえば、ケーブル モデムに接続された外部インターフェイス) が 1 つ以上の IPv6 プレフィックスを受け取れるように DHCPv6 プレフィックス委任クライアントとして機能することができ、ASA はそのプレフィックスを内部インターフェイスをサブネット化および指定することができます。これにより、内部インターフェイスに接続されているホストは、StateLess Address Auto Configuration (SLAAC) を使用してグローバル IPv6 アドレスを取得できます。ただし、内部 ASA インターフェイスはプレフィックス委任サーバとして機能しませんのでご注意ください。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 には光 DHCPv6 サーバが含まれており、SLAAC クライアントが Information Request (IR) パケットを ASA に送信した場合、ASA は DNS サーバやドメイン名などの情報を SLAAC クラ

クライアントに提供することができます。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。

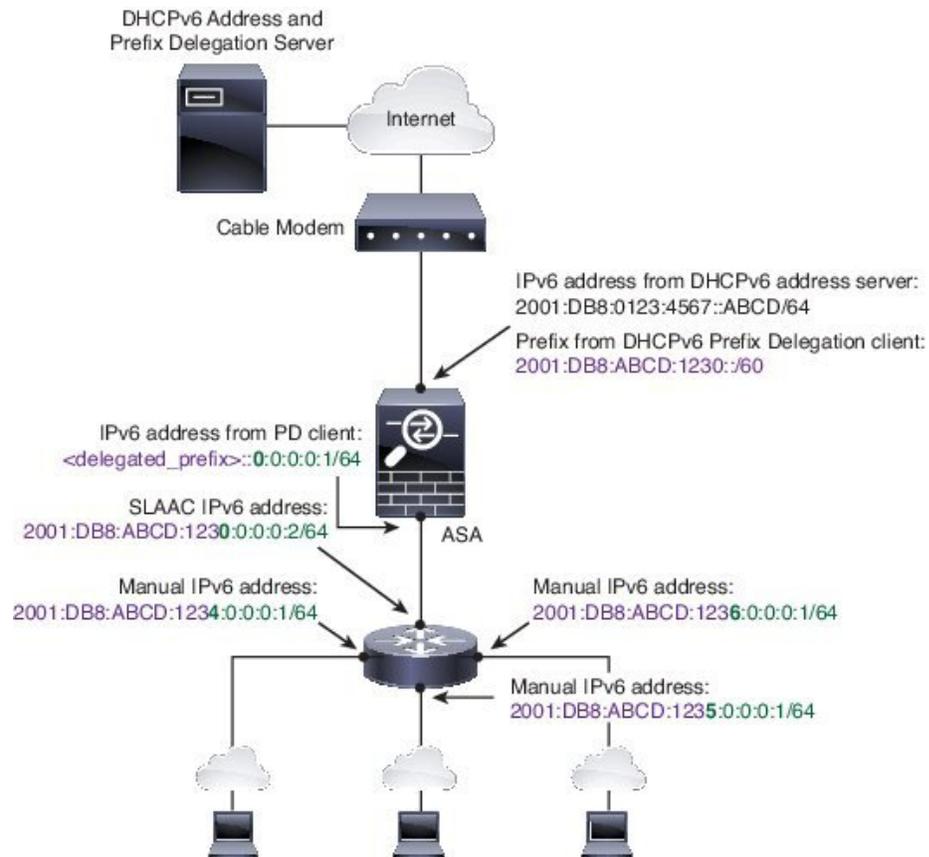
### IPv6 プレフィックス委任 /64 サブネットの例

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場所を示しています。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、代理プレフィックスを /64 ネットワークにサブネット化し、代理プレフィックスおよび手動で設定されたサブネット (::0, ::1, or ::2) と各インターフェイスごとの 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 アドレスを指定します。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場所を示しています。2001:DB8:ABCD:1230::/62, 2001:DB8:ABCD:1234::/62, 2001:DB8:ABCD:1238::/62, and 2001:DB8:ABCD:123C::/62. ASA は、内部ネットワーク (::0) に 2001:DB8:ABCD:1230::/62 の利用可能な 4 つの 64 サブネットのうちの 1 つを使用します。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動的に代理プレフィックスを取得することはできないため、ASA 上で代理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。



## 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 プレフィッ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 \(22 ページ\)](#) 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、特定のプレフィックス長 (::/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は DHCP サーバ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 \(18 ページ\)](#) 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パラメータを提供するには、[DHCPv6 ステートレスサーバの設定](#) 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 およびプレフィッ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。

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。

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

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

- (注) RFC 4862 では、ステートレスな自動設定に設定されたホストはルータ アドバタイズメントメッセージを送信しないと規定していますが、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 [DHCP] または [Ignore] を選択します。[DHCP] を指定すると、ASA は信頼できる送信元から（言い換えると、IPv6 アドレスを提供した同じサーバから）取得された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します。[Ignore] を指定すると、別のネットワークからルータアドバタイズメントを取得できるようになります（この方法では、リスクが高くなる可能性があります）。

- 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 プレフィッ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（17 ページ）](#)）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ックスは /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ックスが 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ックスは 2001:DB8:1234:5671::/64 です。この例では、プレフィックスが /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、プレフィックスが 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。トランスパ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 (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。

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

**ステップ3** [IPv6] タブをクリックします。

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

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

ステップ 5 [OK] をクリックします。

## (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、他のデバイスが Modified EUI-64 形式の使用を必要とする場合、手動で割り当てたリンクローカルアドレスのパケットはドロップされる可能性があります。

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:feec: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 メッセージおよび送信要求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決定し、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敗すると、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 パケットの処理はディセーブルになります。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。ノードがネイバーの到達可能性を確認するときに、ネイバー送信要求メッセージの宛先アドレスは、ネイバーのユニキャストアドレスです。

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。ルータ送信要求メッセージは、ホストからシステムの起動時に送信されるため、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あるインターフェイス (外部インターフェイス など) では、これらのメッセージをディセーブルにできます。

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。

- ステップ 10** [Hosts should use DHCP for address config] チェックボックスをオンにして、取得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の取得には DHCPv6 を使用する必要があることを IPv6 自動設定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** [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 自動設定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 自動設定を使用できません。
- 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。
- 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。プレフィックスは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。最大値は無制限です。
- [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 \(26 ページ\)](#) 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などをモニタできます。

### 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 情報

- **[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構成用に設定されている場合 ([DHCPv6 ステートレスサーバの設定](#) を参照)、この画面はサーバ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から受信した値を表示します。この画面は、DHCPサーバ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
```

## 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)	<p>この機能が導入されました。</p> <p>次の画面が導入されました。</p> <p>[Monitoring] &gt; [Interfaces] &gt; [IPv6 Neighbor Discovery Cache.Configuration] &gt; [Device Management] &gt; [Advanced] &gt; [IPv6 Neighbor Discovery Cache.Configuration] &gt; [Device Setup] &gt; [Interface Settings] &gt; [Interfaces] &gt; [IPv6]。</p>
トランスペアレントモードのIPv6のサポート	8.2(1)	<p>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。</p>
トランスペアレントモードのブリッジグループ	8.4(1)	<p>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。</p> <p>次の画面が変更または導入されました。</p> <p><b>[Configuration] &gt; [Device Setup] &gt; [Interface Settings] &gt; [Interfaces]</b></p> <p>[Configuration] &gt; [Device Setup] &gt; [Interface Settings] &gt; [Interfaces] &gt; [Add/Edit Bridge Group Interface]</p> <p>[Configuration] &gt; [Device Setup] &gt; [Interface Settings] &gt; [Interfaces] &gt; [Add/Edit Interface]</p>

機能名	プラットフォーム リリース	機能情報
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]。
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。  <b>[Configuration] &gt; [Device Setup] &gt; [Interface Settings] &gt; [Interfaces]</b>  [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Bridge Group Interface]  <b>[Configuration] &gt; [Device Setup] &gt; [Interface Settings] &gt; [Interfaces] &gt; [Add/Edit Interface]</b>
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)	<p>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。</p> <ul style="list-style-type: none"> <li>• DHCPv6 アドレスクライアント : ASA は DHCPv6 サーバから 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。</li> <li>• DHCPv6 プレフィックス委任クライアント : ASA は DHCPv6 サーバ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。</li> <li>• 委任プレフィックスの BGP ルータ アドバタイズメント</li> <li>• DHCPv6 ステートレス サーバ : 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。</li> </ul> <p>次の画面が追加または変更されました。</p> <p><b>[Configuration] &gt; [Device Setup] &gt; [Interface Settings] &gt; [Interfaces] &gt; [Add Interface] &gt; [IPv6]</b></p> <p><b>[Configuration] &gt; [Device Management] &gt; [DHCP] &gt; [DHCP Pool]</b></p> <p><b>[Configuration] &gt; [Device Setup] &gt; [Routing] &gt; [BGP] &gt; [IPv6 Family] &gt; [Networks]</b></p> <p><b>[Monitoring] &gt; [interfaces] &gt; [DHCP]</b></p>