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。設定したいコンテキストを変更するには、**changeto context***name* コマンドを入力します。

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」の章を参照してください。
- 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、またはフェー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。
- FirePOWER 2100 シリーズでは、ルーテッド モードのブリッジ グループは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。
- Firepower 2100 シリーズ では、ルーテッド モードのブリッジ グループはサポートされません。
- Firepower 1010 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。
- トランスペアレントモードは、Amazon Web Services、Microsoft Azure、Google Cloud Platform、および Oracle Cloud Infrastructure に展開された脅威防御仮想インスタンスでは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。

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、**changeto context** *name* コマンドを入力します。

手順

ステップ 1 インターフェイス コンフィギュレーション モードを開始します。

interface *id*

例：

```
ciscoasa(config)# interface gigabithethernet 0/0
```

インターフェイス ID には、次のものがあります。

- **冗長**
- **port-channel**
- *physical*：**ethernet**、**gigabitethernet**、**tengigabitethernet**、**management** など。インターフェイス名については、使用しているモデルのハードウェア インストール ガイドを参照してください。
- *physical.subinterface*：**gigabitethernet0/0.100** など。
- **vni**
- **vlan**
- *mapped_name*：マルチ コンテキスト モードの場合。

（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 2 インターフェイスの名前を指定します。

nameif *name*

例：

```
ciscoasa(config-if)# nameif inside
```

name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。その名前を参照するすべてのコマンドが削除されるため、**no** 形式は入力しないでください。

ステップ 3 次のいずれかの方法を使用して IP アドレスを設定します。

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 と PPPoE はサポートされません。

- IP アドレスを手動で設定します。

  ip address *ip_address* [*mask*] [**standby** *ip_address*]

  例：

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
  ```

  standby *ip_address* 引数は、フェールオーバーで使用します。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。

  ip_address 引数および *mask* 引数には、インターフェイスの IP アドレスとサブネット マスクを設定します。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。

  例：

  ```
  ciscoasa(config-if)# ip address 10.1.1.0 255.255.255.254
  ```

- DHCP サーバーから IP アドレスを取得します。

  ip address dhcp [**setroute**]

  例：

  ```
  ciscoasa(config-if)# ip address dhcp
  ```

  setroute キーワードを指定すると、ASA が DHCP サーバーから渡されたデフォルト ルートを使用できるようになります。

  DHCP リースをリセットし、新規リースを要求するには、このコマンドを再入力します。

  （注） **ip address dhcp** コマンドを入力する前に、**no shutdown** コマンドを使用してインターフェイスを有効化していない場合、一部の DHCP 要求が送信されないことがあります。

- PPPoE サーバから IP アドレスを取得します。

  ip address pppoe [**setroute**]

例：

```
ciscoasa(config-if)# ip address pppoe setroute
```

または、IP アドレスを手動で入力して PPPoE を有効化することができます。

ip address *ip_address mask* **pppoe**

例：

```
ciscoasa(config-if)# ip address 10.1.1.78 255.255.255.0 pppoe
```

setroute オプションを指定すると、PPPoE クライアントが接続をまだ確立していない場合に、デフォルトルートが設定されます。**setroute** 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コンフィギュレーションに含めることはできません。

（注） 2 つのインターフェイス（プライマリとバックアップのインターフェイスなど）で PPPeE が有効化されているときに、デュアル ISP サポートを設定しない場合、ASA では、最初のインターフェイスに限り、IP アドレスを取得するためにトラフィックを送信できます。

ステップ 4 セキュリティ レベルを設定します。

security-level *number*

例：

```
ciscoasa(config-if)# security-level 50
```

number には、0（最下位）～ 100（最上位）の整数を指定します。

ステップ 5 （オプション）インターフェイスを管理専用モードに設定してトラフィックが通過しないようにします。

management-only

デフォルトでは、管理インターフェイスは管理専用として設定されます。

例

次に、VLAN 101 のパラメータの設定例を示します。

```
ciscoasa(config)# interface vlan 101
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

次に、マルチコンテキストモードでコンテキストコンフィギュレーションにパラメータを設定する例を示します。インターフェイス ID はマップ名です。

```
ciscoasa/contextA(config)# interface int1
ciscoasa/contextA(config-if)# nameif outside
ciscoasa/contextA(config-if)# security-level 100
ciscoasa/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
```

関連トピック

IPv6 アドレスの設定 （18 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 この接続を表す任意のバーチャルプライベート ダイヤルアップ ネットワーク（VPDN）グループ名を定義します。

vpdn group *group_name* **request dialout pppoe**

例：

```
ciscoasa(config)# vpdn group pppoe-sbc request dialout pppoe
```

ステップ 2 ISP が認証を要求する場合は、認証プロトコルを選択します。

vpdn group *group_name* **ppp authentication** {**chap** | **mschap** | **pap**}

例：

```
ciscoasa(config)# vpdn group pppoe-sbc ppp authentication chap
```

ISP で使用する認証方式に応じた適切なキーワードを入力します。

CHAP または MS-CHAP を使用する場合は、ユーザー名がリモート システム名として参照され、パスワードが CHAP シークレットとして参照されます。

ステップ 3 ISP で割り当てられたユーザー名を VPDN グループに関連付けます。

vpdn group *group_name* **localname** *username*

例：

```
ciscoasa(config)# vpdn group pppoe-sbc localname johncrichton
```

ステップ 4 PPPoE 接続用のユーザー名とパスワードのペアを作成します。

vpdn username *username* **password** *password* [**store-local**]

例：

```
ciscoasa(config)# vpdn username johncrichton password moya
```

store-local オプションを指定すると、ユーザー名とパスワードが ASA の NVRAM の特別な場所に保存されます。Auto Update Server が **clear config** コマンドを ASA に送信し、その後に接続が中断された場合、ASA は、ユーザー名とパスワードを NVRAM から読み取り、アクセス コンセントレータに対して再認証できます。

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、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 BVI を作成します。

interface bvi *bridge_group_number*

例：

```
ciscoasa(config)# interface bvi 2
```

bridge_group_number は、1 ～ 250 の整数です。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 2 （トランスペアレント モード）BVI の IP アドレスを指定します。

ip address *ip_address* [*mask*] [**standby** *ip_address*]

例：

```
ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

BVI にはホスト 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 つ未満の他のサブネットを使用しないでください（ホスト アドレスは、アップストリーム ルータ、ダウンストリーム ルータ、BVI にそれぞれ 1 つずつです）。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。このため、/30 サブネットを使用し、このサブネットからアップストリーム ルータに予約済みアドレスを割り当てると、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。

フェールオーバーには、**standby** キーワードおよびアドレスを使用します。

ステップ 3 （ルーテッド モード）次のいずれかの方法を使用して IP アドレスを設定します。

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します。

  ip address *ip_address* [*mask*] [**standby** *ip_address*]

  例：

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
  ```

standby *ip_address* 引数は、フェールオーバーで使用します。

ip_address 引数および *mask* 引数には、インターフェイスの IP アドレスとサブネット マスクを設定します。

- DHCP サーバーから IP アドレスを取得します。

  ip address dhcp [**setroute**]

  例：

```
ciscoasa(config-if)# ip address dhcp
```

  setroute キーワードを指定すると、ASA が DHCP サーバーから渡されたデフォルト ルートを使用できるようになります。

  DHCP リースをリセットし、新規リースを要求するには、このコマンドを再入力します。

  ip address dhcp コマンドを入力する前に、no shutdown コマンドを使用してインターフェイスを有効化していない場合、一部の DHCP 要求が送信されないことがあります。

ステップ 4 （ルーテッド モード）インターフェイスに名前を付けます。

nameif *name*

例：

```
ciscoasa(config-if)# nameif inside
```

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。*name* は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。その名前を参照するすべてのコマンドが削除されるため、**no** 形式は入力しないでください。

ステップ 5 （ルーテッド モード）セキュリティ レベルを設定します。

security-level *number*

例：

```
ciscoasa(config-if)# security-level 50
```

number には、0（最下位）～ 100（最上位）の整数を指定します。

例

次の例では、BVI 2 アドレスとスタンバイ アドレスを設定します。

```
ciscoasa(config)# interface bvi 2
```

```
ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
```

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、冗長インターフェイス、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、**changeto context** *name* コマンドを入力します。
- 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 （16 ページ）を参照してください。

手順

ステップ 1 インターフェイス コンフィギュレーション モードを開始します。

interface *id*

例：

```
ciscoasa(config)# interface gigabithethernet 0/0
```

インターフェイス ID には、次のものがあります。

- **冗長**
- **port-channel**
- *physical*：**ethernet**、**gigabitethernet**、**tengigabitethernet** など。管理インターフェイスはサポートされていません。インターフェイス名については、使用しているモデルのハードウェア インストール ガイドを参照してください。
- *physical_or_port-channel_or_redundant.subinterface*：たとえば、**gigabitethernet0/0.100**、**redundant2.100**、または **port-channel1.100** など。

- **vni**
- **vlan**
- *mapped_name*：マルチ コンテキスト モードの場合。

（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 2 インターフェイスをブリッジ グループに割り当てます。

bridge-group *number*

例：

```
ciscoasa(config-if)# bridge-group 1
```

number は 1 ~ 250 の整数で、BVI インターフェイス番号に一致する必要があります。ブリッジグループには最大 64 個のインターフェイスを割り当てることができます。同一インターフェイスを複数のブリッジ グループに割り当てることはできません。

ステップ 3 インターフェイスの名前を指定します。

nameif *name*

例：

```
ciscoasa(config-if)# nameif inside1
```

name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。その名前を参照するすべてのコマンドが削除されるため、**no** 形式は入力しないでください。

ステップ 4 セキュリティ レベルを設定します。

security-level *number*

例：

```
ciscoasa(config-if)# security-level 50
```

number には、0（最下位）～ 100（最上位）の整数を指定します。

関連トピック

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（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、**changeto context** *name* コマンドを入力します。

手順

ステップ 1 インターフェイス コンフィギュレーション モードを開始します。

interface {{**port-channel** *number* | **management** *slot*/*port* | *mgmt-type_interface_id* }[**.** *subinterface*] | *mapped_name*}

例：

```
ciscoasa(config)# interface management 0/0.1
```

port-channel *number* 引数は、**port-channel 1** などの EtherChannel インターフェイス ID です。EtherChannelインターフェイスには、管理メンバーインターフェイスのみが設定されている必要があります。

冗長インターフェイスは、Management *slot*/*port* インターフェイスをメンバとしてサポートしません。ただし、管理インターフェイス以外の複数インターフェイスからなる冗長インターフェイスを、管理専用として設定できます。

マルチ コンテキスト モードで、**allocate-interface** コマンドを使用して割り当てた場合、*mapped_name* を入力します。

Firepower 4100/9300 シャーシでは、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）のインターフェイス ID を指定します。

ステップ 2 インターフェイスの名前を指定します。

nameif *name*

例：

```
ciscoasa(config-if)# nameif management
```

name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。その名前を参照するすべてのコマンドが削除されるため、**no** 形式は入力しないでください。

ステップ 3 次のいずれかの方法を使用して IP アドレスを設定します。

- IP アドレスを手動で設定します。

  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。

  ip_address 引数および *mask* 引数には、インターフェイスの IP アドレスとサブネット マスクを設定します。

  standby *ip_address* 引数は、フェールオーバーで使用します。

  ip address *ip_address* [*mask*] [**standby** *ip_address*]

  例：

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
  ```

- DHCP サーバーから IP アドレスを取得します。

  ip address dhcp [**setroute**]

  例：

  ```
  ciscoasa(config-if)# ip address dhcp
  ```

  setroute キーワードを指定すると、ASA が DHCP サーバーから渡されたデフォルト ルートを使用できるようになります。

  DHCP リースをリセットし、新規リースを要求するには、このコマンドを再入力します。

  ip address dhcp コマンドを入力する前に、no shutdown コマンドを使用してインターフェイスを有効化していない場合、一部の DHCP 要求が送信されないことがあります。

ステップ 4 セキュリティ レベルを設定します。

security-level *number*

例：

```
ciscoasa(config-if)# security-level 100
```

number には、0（最下位）～ 100（最上位）の整数を指定します。

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。

（注） リンクローカル アドレスの設定だけを行う場合は、コマンド リファレンスの **ipv6 enable** コマンド（自動設定）または **ipv6 address link-local** コマンド（手動設定）を参照してください。

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

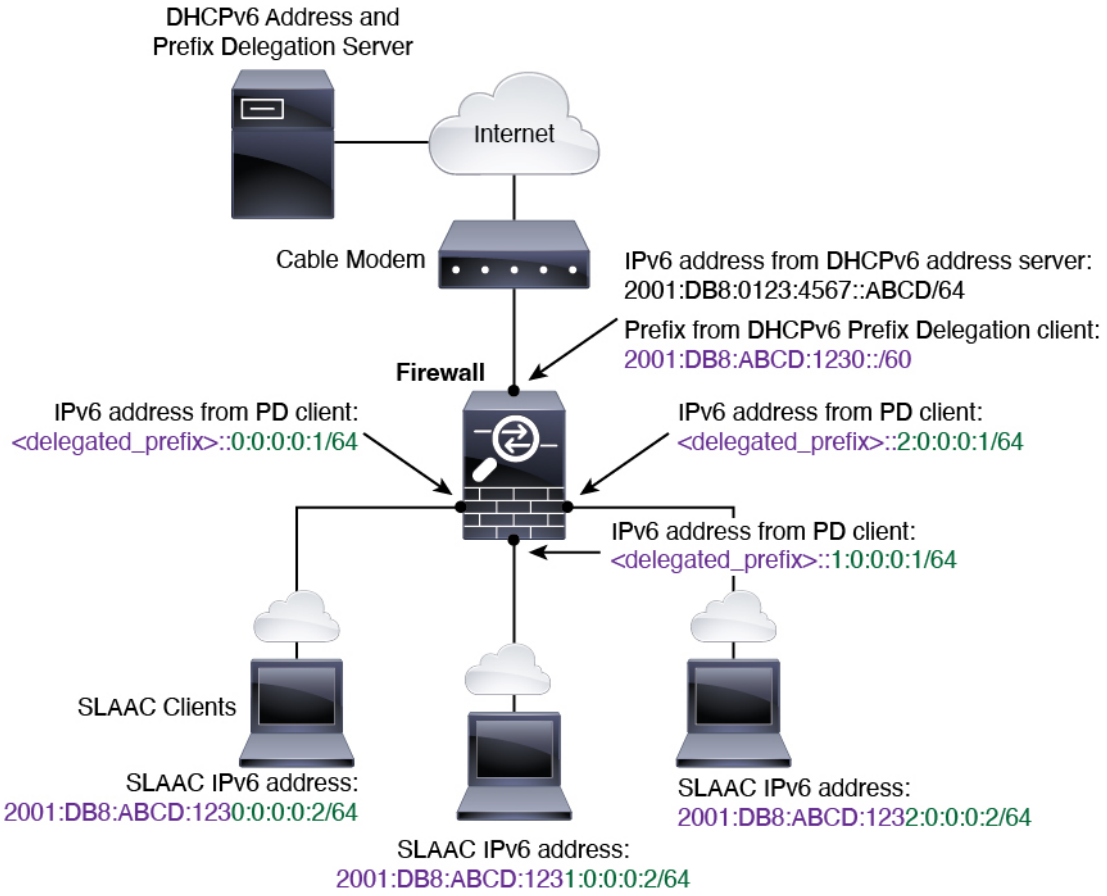
ASA は、（ケーブルモデムに接続された外部インターフェイスなどの）クライアント インターフェイスが 1 つ以上の IPv6 プレフィックスを受け取れるように DHPCv6 プレフィックス委任クライアントとして機能することができ、ASA はそのプレフィックスをサブネット化して内部インターフェイスに割り当てることが可能です。これにより、内部インターフェイスに接続されているホストは、StateLess Address Auto Configuration（SLAAC）を使用してグローバル IPv6 アドレスを取得できます。ただし、内部 ASA インターフェイスはプレフィックス委任サーバーとして機能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。

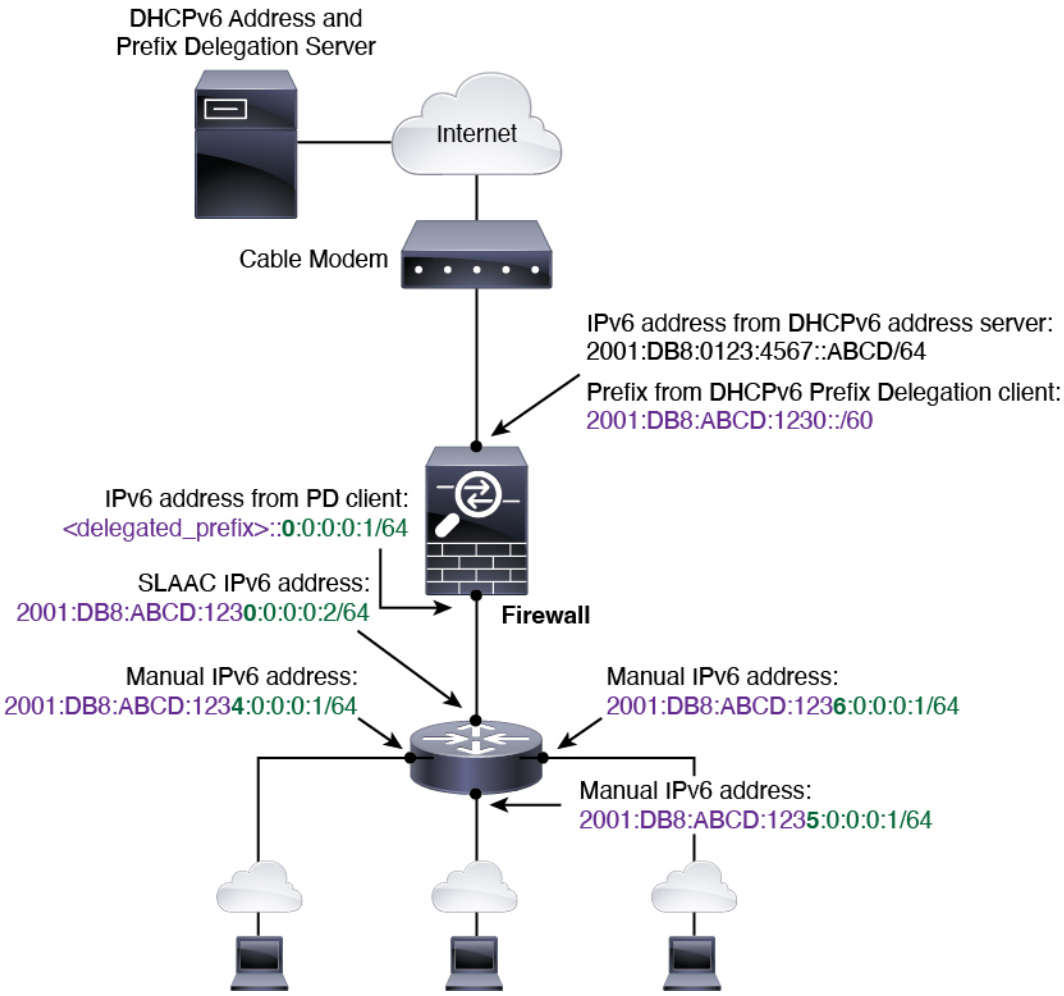
IPv6 プレフィックス委任 /64 サブネットの例

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。



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 （27 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 DHCPv6 サーバー ネットワークに接続されるインターフェイスのインターフェイス コンフィギュレーション モードを開始します。

interface *id*

例：

```
ciscoasa(config)# interface gigabithethernet 0/0
ciscoasa(config-if)#
```

ステップ 2 DHCPv6プレフィックス委任クライアントを有効にし、このインターフェイスで取得したプレフィックスに名前を付けます。

ipv6 dhcp client pd *name*

例：

```
ciscoasa(config-if)# ipv6 dhcp client pd Outside-Prefix
```

name には最大 200 文字を使用できます。

ステップ 3 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。

ipv6 dhcp client pd hint*ipv6_prefix/ prefix_length*

例：

```
ciscoasa(config-if)# ipv6 dhcp client pd hint 2001:DB8:ABCD:1230::/60
```

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。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 4 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 （24 ページ） を参照してください。

ステップ 5 （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 6 （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。

例

次に、GigabitEthernet 0/0 で DHCPv6 アドレスクライアントおよびプレフィックス委任クライアントを設定した後に、アドレスをプレフィックスとともに GigabitEthernet 0/1 および 0/2 に割り当てる例を示します。

```
interface gigabitethernet 0/0
  ipv6 address dhcp default
  ipv6 dhcp client pd Outside-Prefix
  ipv6 dhcp client pd hint ::/60
interface gigabitethernet 0/1
  ipv6 address Outside-Prefix ::1:0:0:0:1/64
interface gigabitethernet 0/2
  ipv6 address Outside-Prefix ::2:0:0:0:1/64
```

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。を参照してください。MAC アドレスの手動設定

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、**changeto context** *name* コマンドを入力します。

手順

ステップ 1 インターフェイス コンフィギュレーション モードを開始します。

interface *id*

例：

```
ciscoasa(config)# interface gigabithethernet 0/0
```

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 を指定します。

例：

```
ciscoasa(config)# interface bvi 1
```

トランスペアレント モードでは、BVI に加え、管理インターフェイスを指定することもできます。

例：

```
ciscoasa(config)# interface management 1/1
```

ステップ 2 （ルーテッド インターフェイス）次のいずれかの方法を使用して IP アドレスを設定します。

- インターフェイスでステートレスな自動設定をイネーブルにします。

  ipv6 address autoconfig [**default trust** {**dhcp** |**ignore**}]

  インターフェイスでステートレスな自動設定をイネーブルにすると、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に基づいて IPv6 アドレスが設定されます。ステートレスな自動設定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、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、**ipv6 nd suppress-ra** コマンドを参照してください。

  デフォルトルートをインストールするには、 **default trust dhcp** か **ignore** を指定します。**dhcp** を指定すると、ASA は信頼できる送信元から（IPv6 アドレスを提供した同じサーバーから）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）。

- DHCPv6 を使用してアドレスを取得します。

  ipv6 address dhcp [**default**]

  例：

```
ciscoasa(config-if)# ipv6 address dhcp default
```

default キーワードを指定すると、ルータ アドバタイズメントからデフォルト ルートが取得されます。

- インターフェイスに手動でグローバル アドレスを割り当てます。

  ipv6 address *ipv6_address/prefix-length* [**standby** *ipv6_address*]

  例：

```
ciscoasa(config-if)# ipv6 address 2001:0DB8:BA98::3210/64 standby 2001:0DB8:BA98::3211
```

  グローバル アドレスを割り当てると、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作成されます。

  standby は、フェールオーバー ペアのセカンダリ ユニットまたはフェールオーバー グループで使用されるインターフェイス アドレスを指定します。

- Modified EUI-64 形式を使用してインターフェイスの MAC アドレスから生成されたインターフェイス ID と、指定されたプレフィックスを結合することによって、インターフェイスにグローバル アドレスを割り当てます。

  ipv6 address *ipv6-prefix/prefix-length* **eui-64**

  例：

```
ciscoasa(config-if)# ipv6 address 2001:0DB8:BA98::/64 eui-64
```

  グローバル アドレスを割り当てると、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作成されます。

  スタンバイ アドレスを指定する必要はありません。インターフェイス ID が自動的に生成されます。

- 委任されたプレフィックスを使用します。

  ipv6 address *prefix_name ipv6_address/prefix_length*

  例：

```
ciscoasa(config-if)# ipv6 address Outside-Prefix ::1:0:0:0:1/64
```

  この機能は、ASA に別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有効にさせるために必要です。IPv6 プレフィックス委任クライアントの有効化 （22 ページ）を参照してください。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。

ステップ 3 （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。

ipv6 address *ipv6_address*/*prefix-length* [**standby** *ipv6_address*]

例：

```
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
```

グローバル アドレスを割り当てると、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作成されます。

standby は、フェールオーバー ペアのセカンダリ ユニットまたはフェールオーバー グループで使用されるインターフェイス アドレスを指定します。

ステップ 4 （オプション）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します。

ipv6 enforce-eui64 *if_name*

例：

```
ciscoasa(config)# ipv6 enforce-eui64 inside
```

if_name 引数には、**nameif** コマンドで指定したインターフェイスの名前を指定します。このインターフェイスに対してアドレス形式を適用できます。

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 設定する IPv6 インターフェイスを指定します。

interface *name*

例：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)#
```

ステップ 2 重複アドレス検出（DAD）の試行回数を指定します。

ipv6 nd dad attempts *value*

value 引数の有効な値の範囲は 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。

例：

```
ciscoasa(config-if)# ipv6 nd dad attempts 20
```

ステップ 3 IPv6 ネイバー送信要求の再送信する間隔を設定します。

ipv6 nd ns-interval *value*

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。

例：

```
ciscoasa(config-if)# ipv6 nd ns-interval 9000
```

ステップ 4 リモートの IPv6 ノードに到達可能な時間を設定します。

ipv6 nd reachable-time *value*

value 引数の有効な値は、0 ～ 3600000 ミリ秒です。value に 0 を使用すると、到達可能時間が判定不能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。

例：

```
ciscoasa config-if)# ipv6 nd reachable-time 1700000
```

ステップ 5 IPv6 ルータ アドバタイズメントの送信間隔を設定します。

ipv6 nd ra-interval [**msec**] *value*

msec キーワードは、この値がミリ秒単位で指定されることを示します。このキーワードが存在しない場合、値は秒単位で指定されます。*value* 引数の有効な値の範囲は 3 ～ 1800 秒、**msec** キーワードが指定されている場合は 500 ～ 1800000 ミリ秒です。デフォルトは 200 秒です。

送信間隔の値は、このインターフェイスから送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。

ASA がデフォルト ルータとして設定されている場合、送信間隔は IPv6 ルータ アドバタイズメント ライフタイム以下にする必要があります。他の IPv6 ノードと同期しないようにするには、使用する実際値を必要値の 20 % 以内にランダムに調整します。

例：

```
ciscoasa(config-if)# ipv6 nd ra-interval 201
```

ステップ 6 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指定します。

ipv6 nd ra-lifetime [**msec**] *value*

オプションの **msec** キーワードは、この値がミリ秒単位で指定されることを示します。このキーワードを指定しない場合、値は秒単位です。*value* 引数の有効な値は 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。

ルータの有効期間の値は、このインターフェイスから送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。この値は、このインターフェイス上のデフォルト ルータとしての ASA の有用性を示します。

例：

```
ciscoasa(config-if)# ipv6 nd ra-lifetime 2000
```

ステップ 7 ルータ アドバタイズメントを抑制します。

ipv6 nd suppress-ra

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。

このコマンドを入力すると、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 8 取得されるステートレス自動設定のアドレス以外の IPv6 アドレスの取得に DHCPv6 を使用するように IPv6 自動設定クライアントに通知するには、IPv6 ルータ アドバタイズメントにフラグを追加します。

ipv6 nd managed-config-flag

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 9 DNS サーバー アドレスや他の情報の取得に DHCPv6 を使用するように IPv6 自動設定クライアントに通知するには、IPv6 ルータ アドバタイズメントにフラグを追加します。

ipv6 nd other-config-flag

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 10 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。

ipv6 nd prefix {*ipv6_prefix*/*prefix_length* |**default**} [*valid_lifetime preferred_lifetime* | **at** *valid_date preferred_date*] [**no-advertise**] [**no-autoconfig**] [ ] [**off-link**]

ネイバー デバイスは、プレフィックス アドバタイズメントを使用して、そのインターフェイス アドレスを自動設定できます。ステートレス自動設定では、ルータ アドバタイズメント メッセージで提供される IPv6 プレフィックスを使用して、リンクローカル アドレスからグローバル ユニキャスト アドレスを作成します。

デフォルトでは、**ipv6 address** コマンドを使用してインターフェイスにアドレスとして設定されるプレフィックスは、ルータ アドバタイズメントでアドバタイズされます。**ipv6 nd prefix**

コマンドを使用してプレフィックスをアドバタイズメント用に設定すると、これらのプレフィックスだけがアドバタイズされます。

ステートレス自動設定が正しく機能するには、ルータ アドバタイズメント メッセージでアドバタイズされるプレフィックス長が常に 64 ビットでなければなりません。

- **default**: デフォルトのプレフィックスが使用されていることを示します。
- *valid_lifetime preferred_lifetime* ：指定した IPv6 プレフィックスを有効かつ優先されるものとしてアドバタイズする時間を指定します。優先の有効期間中には、アドレスの制限はありません。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。値の範囲は 0 ～ 4294967295 秒です。最大値は無限ですが、これは **infinite** キーワードを使用して指定することもできます。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。
- **at** *valid_date preferred_date*：プレフィックスの有効期限が切れる特定の日付と時刻を示します。日付は *month_name day hh*:*mm* と指定します。たとえば、**dec 1 13:00** と入力します。
- **no-advertise**：プレフィックスのアドバタイズメントを無効にします。
- **no-autoconfig**：プレフィックスは IPv6 自動設定には使用できないことを指定します。
- **off-link**：指定したプレフィックスをオフリンクとして設定します。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。

  onlink がオン（デフォルト）のときは、指定されたプレフィックスがそのリンクに割り当てられます。指定されたプレフィックスを含むそのようなアドレスにトラフィックを送信するノードは、宛先がリンク上でローカルに到達可能であると見なします。

例：

```
ciscoasa(config-if)# ipv6 nd prefix 2001:DB8::/32 1000 900
```

ステップ 11 IPv6 ネイバー探索キャッシュのスタティック エントリを設定します。

ipv6 neighbor *ipv6_address if_name mac_address*

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。

- **ipv6 neighbor** コマンドは **arp** コマンドに似ています。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のスタティック エントリを表示するには、**show ipv6 neighbor** コマンドを使用します。

- **clear ipv6 neighbor** コマンドにより、スタティック エントリを除く、IPv6 ネイバー探索キャッシュ内のすべてのエントリを削除します。**no ipv6 neighbor** コマンドは、指定したスタティック エントリをネイバー探索キャッシュから削除します。このコマンドは、IPv6 ネイバー探索プロセスから認識されるエントリであるダイナミック エントリはキャッシュから削除しません。**no ipv6 enable** コマンドを使用してインターフェイスで IPv6 をディセーブルにすると、スタティック エントリを除いて、そのインターフェイス用に設定されたすべての IPv6 ネイバー探索キャッシュ エントリが削除されます（エントリの状態が INCMP [Incomplete] に変更されます）。
- 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。
- **clear ipv6 neighbor** コマンドを実行しても、スタティック エントリが IPv6 ネイバー探索キャッシュから削除されることはありません。ダイナミック エントリのクリアだけが行われます。
- 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。

例：

```
ciscoasa(config)# ipv6 neighbor 3001:1::45A inside 002.7D1A.9472
```

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 をモニターできます。

（注） Firepower 1000、2100 および Firepower 4100/9300 の場合、一部の統計は 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**

プラットフォームモードの Firepower 2100 の場合は、次の FXOS connect local-mgmt コマンドも参照してください。

- (local-mgmt)# **show portmanager counters**
- (local-mgmt)# **show lacp**
- (local-mgmt)# **show portchannel**

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

- **show interface**

  インターフェイス統計情報を表示します。

- **show interface ip brief**

  インターフェイスの IP アドレスとステータスを表示します。

- **show bridge-group**

  指定されたインターフェイス、MAC アドレスと IP アドレスなどのブリッジグループ情報を表示します。

DHCP Information

- **show ipv6 dhcp interface** [*ifc_name* [**statistics**]]

  show ipv6 dhcp interface コマンドは、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）、このコマンド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、このコマンド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。特定のインターフェイスについて、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を表示できます。次に、このコマンドで提供される情報例を示します。

```
ciscoasa(config-if)# show ipv6 dhcp interface
GigabitEthernet1/1 is in server mode
  Using pool: Sample-Pool

GigabitEthernet1/2 is in client mode
  Prefix State is OPEN
  Renew will be sent in 00:03:46
  Address State is OPEN
  Renew for address will be sent in 00:03:47
  List of known servers:
    Reachable via address: fe80::20c:29ff:fe96:1bf4
    DUID: 000100011D9D1712005056A07E06
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x00030001, T1 250, T2 400
        Prefix: 2005:abcd:ab03::/48
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      IA NA: IA ID 0x00030001, T1 250, T2 400
        Address: 2004:abcd:abcd:abcd:abcd:abcd:abcd:f2cb/128
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      DNS server: 2004:abcd:abcd:abcd::2
      DNS server: 2004:abcd:abcd:abcd::4
      Domain name: relay.com
      Domain name: server.com
      Information refresh time: 0
  Prefix name: Sample-PD

Management1/1 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 11:26:44
  List of known servers:
    Reachable via address: fe80::4e00:82ff:fe6f:f6f9
    DUID: 000300014C00826FF6F8
    Preference: 0
    Configuration parameters:
      IA NA: IA ID 0x000a0001, T1 43200, T2 69120
        Address: 2308:2308:210:1812:2504:1234:abcd:8e5a/128
                preferred lifetime INFINITY, valid lifetime INFINITY
      Information refresh time: 0


ciscoasa(config-if)# show ipv6 dhcp interface outside statistics

DHCPV6 Client PD statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:
```

```
 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0

DHCPV6 Client address statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0
```

- **show ipv6 dhcp client [pd] statistics**

  show ipv6 dhcp client statistics コマンドは、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。**show ipv6 dhcp client pd statistics** コマンドは、プレフィックス委任クライアントの統計情報を表示します。次に、このコマンドで提供される情報例を示します。

```
ciscoasa(config)# show ipv6 dhcp client statistics

Protocol Exchange Statistics:
  Total number of Solicit messages sent:              4
  Total number of Advertise messages received:        4
  Total number of Request messages sent:              4
  Total number of Renew messages sent:                92
  Total number of Rebind messages sent:               0
  Total number of Reply messages received:            96
  Total number of Release messages sent:              6
  Total number of Reconfigure messages received:      0
  Total number of Information-request messages sent:  0

Error and Failure Statistics:
  Total number of Re-transmission messages sent:                  8
  Total number of Message Validation errors in received messages: 0


ciscoasa(config)# show ipv6 dhcp client pd statistics

Protocol Exchange Statistics:


 Total number of Solicit messages sent:              1
 Total number of Advertise messages received:        1
 Total number of Request messages sent:              1
 Total number of Renew messages sent:                92
 Total number of Rebind messages sent:               0
 Total number of Reply messages received:            93
```

```
 Total number of Release messages sent:              0
 Total number of Reconfigure messages received:      0
 Total number of Information-request messages sent:  0

Error and Failure Statistics:


 Total number of Re-transmission messages sent:                  1
 Total number of Message Validation errors in received messages: 0
```

- **show ipv6 dhcp ha statistics**

  show ipv6 dhcp ha statistics コマンドは、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。次に、このコマンドで提供される情報例を示します。

  アクティブ ユニット上：

```
ciscoasa(config)# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              1
  DUID sync messages received:          0

DHCPv6 HA error statistics:
  Send errors:                          0
```

  スタンドバイ ユニット上：

```
ciscoasa(config)# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              0
  DUID sync messages received:          1

DHCPv6 HA error statistics:
  Send errors:                          0
```

- **show ipv6 general-prefix**

  show ipv6 general-prefix コマンドは、DHCPv6 プレフィックス委任クライアントによって獲得されたすべてのプレフィックスとそのプレフィックスの他のプロセスへの ASA 配布（「コンシューマ リスト」）を表示します。次に、このコマンドで提供される情報例を示します。

```
ciscoasa(config)# show ipv6 general-prefix
IPv6 Prefix Sample-PD, acquired via DHCP PD
  2005:abcd:ab03::/48 Valid lifetime 524, preferred lifetime 424
   Consumer List                Usage count
    BGP network command         1
    inside (Address command)    1
```

PPPoE

- **show ip address** *interface_name* **pppoe**

  現在の PPPoE クライアントの設定情報を表示します。

- **debug pppoe** {**event** | **error** | **packet**}

  PPPoE クライアントのデバッグをイネーブルにします。

- **show vpdn session**[**l2tp** |**pppoe**] [**id** *sess_id* |**packets** |**state** | **window**]

  PPPoE セッションのステータスを表示します。

  次に、このコマンドで提供される情報例を示します。

```
ciscoasa# show vpdn

Tunnel id 0, 1 active sessions
     time since change 65862 secs
     Remote Internet Address 10.0.0.1
    Local Internet Address 199.99.99.3
     6 packets sent, 6 received, 84 bytes sent, 0 received
Remote Internet Address is 10.0.0.1
     Session state is SESSION_UP
       Time since event change 65865 secs, interface outside
       PPP interface id is 1
       6 packets sent, 6 received, 84 bytes sent, 0 received
ciscoasa#
ciscoasa# show vpdn session
PPPoE Session Information (Total tunnels=1 sessions=1)
Remote Internet Address is 10.0.0.1
  Session state is SESSION_UP
    Time since event change 65887 secs, interface outside
    PPP interface id is 1
    6 packets sent, 6 received, 84 bytes sent, 0 received
ciscoasa#
ciscoasa# show vpdn tunnel
PPPoE Tunnel Information (Total tunnels=1 sessions=1)
Tunnel id 0, 1 active sessions
   time since change 65901 secs
   Remote Internet Address 10.0.0.1
   Local Internet Address 199.99.99.3
   6 packets sent, 6 received, 84 bytes sent, 0 received
ciscoasa#
```

IPv6 ネイバー探索

IPv6 ネイバー探索パラメータをモニターするには、次のコマンドを入力します。

- **show ipv6 interface**

  このコマンドは、「外部」などのインターフェイス名を含む、IPv6 用に設定されているインターフェイスのユーザビリティ状態を表示し、指定されたインターフェイスの設定を表示します。しかし、このコマンドは名前を除外し、IPv6 が有効になっているすべてのインターフェイスの設定を表示します。コマンドの出力では、次の項目が表示されます。

- インターフェイスの名前とステータス
- リンクローカルおよびグローバルなユニキャスト アドレス
- インターフェイスが属するマルチキャスト グループ
- ICMP リダイレクトおよびエラー メッセージの設定
- ネイバー探索の設定
- コマンドが 0 に設定されているときの実際の時間
- 使用されているネイバー探索の到達可能時間

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

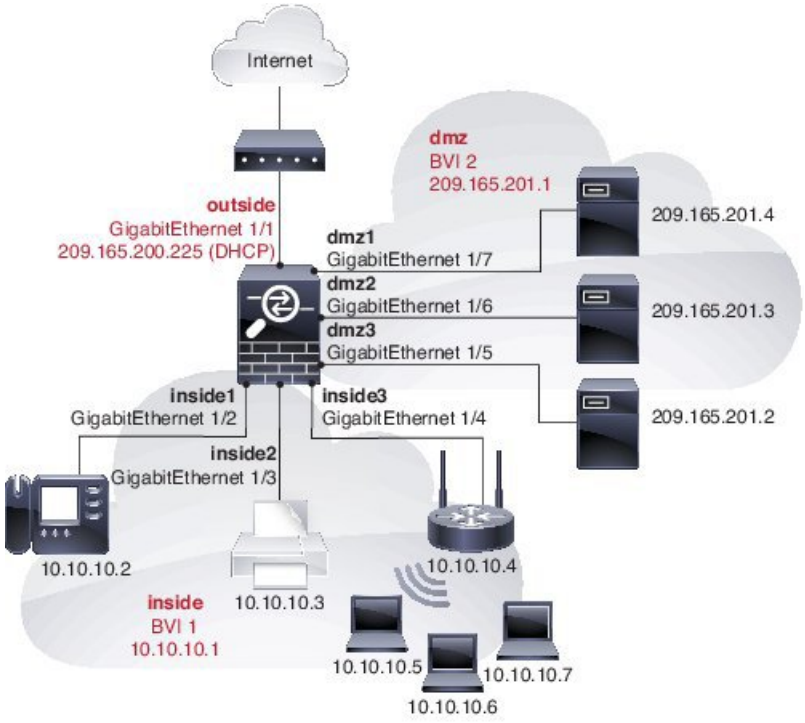
トランスペアレント モードの次の例では、3 つのインターフェイスそれぞれの 2 つのブリッジグループと管理専用インターフェイスを示します。

```
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。 **ipv6 nd ns-interval**、**ipv6 nd ra-lifetime**、**ipv6 nd suppress-ra**、**ipv6 neighbor**、**ipv6 nd prefix**、**ipv6 nd dad-attempts**、**ipv6 nd reachable-time**、**ipv6 address**、および **ipv6 enforce-eui64** コマンドが導入されました。
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。 次のコマンドが導入されました。**interface bvi**、**show bridge-group**

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)	コマンド **ipv6 nd managed-config-flag**、**ipv6 nd other-config-flag** 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。 **interface bvi** および **bridge-group** コマンドが変更されました。
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。 変更されたコマンドはありません。

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。 次のコマンドが追加または変更されました。**clear ipv6 dhcp statistics**、**domain-name**、**dns-server**、**import**、**ipv6 address autoconfig**、**ipv6 address dhcp**、**ipv6 dhcp client pd**、**ipv6 dhcp client pd hint**、**ipv6 dhcp pool**、**ipv6 dhcp server**、**network**、**nis address**、**nis domain-name**、**nisp address**、**nisp domain-name**、**show bgp ipv6 unicast**、**show ipv6 dhcp**、**show ipv6 general-prefix**、**sip address**、**sip domain-name**、**sntp address**

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)	

機能名	プラットフォームリリース	機能情報
		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、

機能名	プラットフォームリリース	機能情報
		BVI ではサポートされません。 次のコマンドが変更されました。**access-group**、**access-list ethertype**、**arp-inspection**、**dhcpd**、**mac-address-table static**、**mac-address-table aging-time**、**mac-learn**、**route**、**show arp-inspection**、**show bridge-group**、**show mac-address-table**、**show mac-learn**
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。 次のコマンドを変更しました。**ip address**、**http**、**logging host**、**snmp-server**、**ssh**

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。