CHAPTER 12

IPv6 の設定

この章では、セキュリティ アプライアンスで IPv6 をイネーブルにする方法および設定する方法について説明します。IPv6 は、ルーテッド ファイアウォール モードだけで使用できます。

この章は、次の項で構成されています。

IPv6 コンフィギュレーションの例については、付録 B「設定例」を参照してください。

IPv6 対応のコマンド

次に示すセキュリティ アプライアンスのコマンドは、IPv6 アドレスの受け入れと表示が可能です。

- capture
- configure
- copy
- http
- name
- object-group
- ping
- show conn
- show local-host
- show tcpstat
- ssh
- telnet
- tftp-server
- who
- write

（注）　フェールオーバーは IPv6 をサポートしません。**ipv6 address** コマンドは、フェールオーバー コンフィギュレーションのスタンバイ アドレスの設定をサポートしません。**failover interface ip** コマンドは、フェールオーバー インターフェイスおよびステートフル フェールオーバー インターフェイスでの IPv6 アドレスの使用をサポートしません。

IPv6 対応コマンドに IPv6 アドレスを入力する場合、**ping fe80::2e0:b6ff:fe01:3b7a** など IPv6 の標準表記法で入力します。セキュリティ アプライアンス は、IPv6 アドレスを正しく認識し、処理します。ただし、次の場合は、IPv6 アドレスを角カッコ（[ ]）で囲む必要があります。

- アドレスと一緒にポート番号を指定する必要がある場合（例：**[fe80::2e0:b6ff:fe01:3b7a]:8080**）。
- **write net** コマンドや **config net** コマンドなど、コマンドが区切り文字としてコロンを使用する場合（例：**configure net [fe80::2e0:b6ff:fe01:3b7a]:/tftp/config/pixconfig**）。

次のコマンドは、IPv6 で動作するように変更されました。

- debug
- fragment
- ip verify
- mtu
- icmp（**ipv6 icmp** と入力されます）

次のインスペクション エンジンは IPv6 に対応しています。

- FTP
- HTTP
- ICMP
- SMTP
- TCP
- UDP

IPv6 の設定

ここでは、次の内容について説明します。

インターフェイスでの IPv6 の設定

少なくとも、各インターフェイスに IPv6 リンクローカル アドレスを設定する必要があります。インターフェイスにサイトローカル アドレスとグローバル アドレスを追加することもできます。

（注） セキュリティ アプライアンスは、IPv6 エニーキャスト アドレスはサポートしません。

1 つのインターフェイスに IPv6 アドレスと IPv4 アドレスの両方を設定できます。

インターフェイス上で IPv6 を設定する手順は、次のとおりです。

ステップ 1　IPv6 アドレスを設定するインターフェイスに対応するインターフェイス コンフィギュレーション モードに入ります。

```
hostname(config)# interface if
```

ステップ 2　インターフェイスで IPv6 アドレスを設定します。1 つのインターフェイスに、IPv6 リンクローカル、サイトローカル、グローバル アドレスなど複数の IPv6 アドレスを割り当てることができます。ただし、少なくとも、リンクローカル アドレスを設定する必要があります。

IPv6 アドレスを設定するには、いくつかの方法があります。次の中から、ニーズに合った方法を選択してください。

- 最も簡単な方法は、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方法です。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。ステートレス自動設定をイネーブルにするには、次のコマンドを入力します。

  ```
  hostname(config-if)# ipv6 address autoconfig
  ```

- インターフェイスのリンクローカル アドレスだけを設定する必要があり、その他の IPv6 アドレスをインターフェイスに割り当てない場合は、手動でリンクローカル アドレスを定義するか、インターフェイス MAC アドレス（Modified EUI-64 形式）に基づいて生成するかを選択できます。
  - リンクローカル アドレスを手動で指定するには、次のコマンドを入力します。

    ```
    hostname(config-if)# ipv6 address ipv6-address link-local
    ```

  - 次のコマンドを入力して、インターフェイス上で IPv6 をイネーブルにし、インターフェイス MAC アドレスに基づく修正 EUI-64 インターフェイス ID を使用してリンクローカル アドレスを自動生成します。

    ```
    hostname(config-if)# ipv6 enable
    ```

  （注） インターフェイス上に他の **ipv6 address** コマンドを入力する場合、**ipv6 enable** コマンドを使用する必要はありません。IPv6 アドレスをインターフェイスに割り当てると同時に、IPv6 対応は自動的にイネーブルになります。

- インターフェイスにサイトローカル アドレスまたはグローバル アドレスを割り当てます。サイトローカル アドレスまたはグローバル アドレスを割り当てると、リンクローカル アドレスが自動生成されます。インターフェイスにサイトローカル アドレスまたはグローバル アドレスを追加するには、次のコマンドを入力します。アドレスの下位 64 ビットに Modified EUI-64 インターフェイス ID を使用する場合は、オプションの **eui-64** キーワードを使用します。

```
hostname(config-if)# ipv6 address ipv6-address [eui-64]
```

ステップ 3　（任意）インターフェイス上でルータ アドバタイズメント メッセージをディセーブルにします。デフォルトでは、ルータ アドバタイズメント メッセージは、ルータ送信要求メッセージへの応答として自動的に送信されます。セキュリティ アプライアンスで 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ディセーブルにできます。

インターフェイス上でルータ アドバタイズメント メッセージをディセーブルにするには、次のコマンドを入力します。

```
hostname(config-if)# ipv6 nd suppress-ra
```

インターフェイスでのデュアル IP スタックの設定

セキュリティ アプライアンスは、1 つのインターフェイス上で IPv6 と IPv4 の両方のコンフィギュレーションをサポートします。そのために特別なコマンドを入力する必要はありません。単純に、IPv4 コンフィギュレーション コマンドと IPv6 コンフィギュレーション コマンドを通常と同じように入力します。IPv4 と IPv6 の両方で、デフォルト ルートを設定してください。

IPv6 アドレスでの Modified EUI-64 インターフェイス ID の使用

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。セキュリティ アプライアンスでは、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。

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、次のコマンドを入力します。

```
hostname(config)# ipv6 enforce-eui64 if_name
```

if_name 引数には、**namif** 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。

このコマンド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。

```
%PIX|ASA-3-325003: 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。ルータの背後にあるホストから受信したパケットは、アドレス形式の検証に失敗してドロップされます。これは、その送信元 MAC アドレスがルータの MAC アドレスであり、ホストの MAC アドレスではないためです。

IPv6 重複アドレス検出の設定

ステートレス自動設定プロセスにおいて、重複アドレス検出機能は、新規のユニキャスト IPv6 アドレスがインターフェイスに割り当てられる前に、その一意性を検証します（重複アドレス検出が実行されている間、新規アドレスは一時ステートのままです）。重複アドレス検出は、最初に新しいリンクローカル アドレスに対して行われます。リンクローカル アドレスが固有であることが検証されたら、次にインターフェイス上のその他すべての IPv6 ユニキャスト アドレスに対して重複アドレス検出が行われます。

重複アドレス検出は、管理上ダウンしているインターフェイスでは停止します。インターフェイスが管理上ダウンしている間、そのインターフェイスに割り当てられたユニキャスト IPv6 アドレスは保留状態に設定されます。管理上アップ状態に復帰したインターフェイスでは、重複アドレス検出がインターフェイス上のすべてのユニキャスト IPv6 アドレスに対して再開されます。

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。

```
%PIX|ASA-4-325002: 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。ただし、その重複アドレスに関連付けられたすべてのコンフィギュレーション コマンドは、アドレスの状態が DUPLICATE に設定されている間、設定されたままになります。

インターフェイスのリンクローカル アドレスが変更された場合、新しいリンクローカル アドレスで重複アドレス検出が実行され、インターフェイスに関連付けられた他のすべての IPv6 アドレスが再生成されます（重複アドレス検出は新規のリンクローカル アドレスでのみ実行されます）。

セキュリティ アプライアンスは、ネイバー送信要求メッセージを使用して、重複アドレス検出を実行します。デフォルトでは、インターフェイスが重複アドレス検出を行う回数は 1 回です。

重複アドレス検出の試行回数を変更するには、次のコマンドを入力します。

```
hostname(config-if)# ipv6 nd dad attempts value
```

value 引数には、0 ～ 600 の任意の値を指定できます。*value* 引数を 0 に設定すると、インターフェイスの重複アドレス検出がディセーブルになります。

複数の重複アドレス検出試行を送信するようにインターフェイスを設定する場合は、**ipv6 nd ns-interval** コマンドを使用してネイバー送信要求メッセージの送信間隔を設定できます。このメッセージは、デフォルトでは 1000 ミリ秒間に 1 回送信されます。

ネイバー送信要求メッセージの間隔を変更するには、次のコマンドを入力します。

```
hostname(config-if)# ipv6 nd ns-interval value
```

value 引数には、1000 ～ 3600000 ミリ秒の値を指定できます。

（注） この値を変更すると、重複アドレス検出で使用されるものだけでなく、インターフェイスで送信されるすべてのネイバー送信要求メッセージで変更されます。

IPv6 デフォルト ルートおよびスタティック ルートの設定

ホストが接続されているインターフェイスが IPv6 に対応し、IPv6 ACL でトラフィックが許可されていれば、セキュリティ アプライアンス は、直接接続されているホスト間で IPv6 トラフィックを自動的にルーティングします。

セキュリティ アプライアンスはダイナミック ルーティング プロトコルをサポートしません。このため、IPv6 トラフィックを接続されていないホストやネットワークにルーティングするには、そのホストやネットワークへのスタティック ルートを定義するか、少なくともデフォルト ルートを定義する必要があります。スタティック ルートまたはデフォルト ルートが定義されていない場合、直接接続されていないホストやネットワークへのトラフィックは次のようなエラーメッセージを生成します。

```
%PIX|ASA-6-110001: No route to dest_address from source_address
```

ipv6 route コマンドを使用して、デフォルト ルートおよびスタティック ルートを追加できます。

IPv6 デフォルト ルートおよびスタティック ルートを設定するには、次の手順を実行します。

ステップ 1　デフォルト ルートを追加するには、次のコマンドを入力します。

```
hostname(config)# ipv6 route if_name ::/0 next_hop_ipv6_addr
```

アドレス ::/0 は、IPv6 で「any」と同じです。

ステップ 2　（任意）IPv6 スタティック ルートを定義します。IPv6 スタティック ルートを IPv6 ルーティング テーブルに追加するには、次のコマンドを使用します。

```
hostname(config)# ipv6 route if_name destination next_hop_ipv6_addr [admin_distance]
```

（注）　**ipv6 route** コマンドは、IPv4 スタティック ルートを定義するための **route** コマンドと同じ役割を果たします。

IPv6 アクセス リストの設定

IPv6 アクセス リストの設定は、IPv4 アクセスの設定に似ていますが、IPv6 アドレスを使用するという違いがあります。

IPv6 アクセス リストを設定する手順は、次のとおりです。

ステップ 1　アクセス エントリを作成します。アクセス リストを作成するには、**ipv6 access-list** コマンドを使用してアクセス リストのエントリを作成します。このコマンドには ICMP トラフィック専用のアクセス リスト エントリを作成するための形式と、他のすべてのタイプの IP トラフィックのアクセス リスト エントリを作成するための形式という 2 つの形式があり、どちらかを選択します。

- ICMP トラフィック専用の IPv6 アクセス リスト エントリを作成するには、次のコマンドを入力します。

  ```
  hostname(config)# ipv6 access-list id [line num] {permit | deny} icmp source
  destination [icmp_type]
  ```

- IPv6 アクセス リスト エントリを作成するには、次のコマンドを入力します。

  ```
  hostname(config)# ipv6 access-list id [line num] {permit | deny} protocol source
  [src_port] destination [dst_port]
  ```

次に、**ipv6 access-list** コマンドの引数について説明します。

- *id：アクセス リストの名前です。アクセス リストに複数のエントリを入力する場合、各コマンドに同じ id を使用します。*

- **line** *num*：アクセス リストにエントリを追加するときに、エントリを表示するリスト内の行番号を指定できます。
- **permit** | **deny**：指定トラフィックをブロックするか通過させるかを決定します。
- **icmp**：アクセス リスト エントリを ICMP トラフィックに適用することを示します。
- *protocol*：アクセス リスト エントリで制御するトラフィックを指定します。IP プロトコルの名前（**ip**、**tcp**、または **udp**）または数字（1 ～ 254）を指定できます。**object-group** *grp_id* を使用してプロトコル オブジェクト グループを指定することもできます。
- *source* および *destination*：トラフィックの送信元または宛先を指定します。送信元または宛先には、アドレス範囲を示す *prefix*/*length* 形式の IPv6 プレフィックス、任意のアドレスを指定するキーワード **any**、または **host** *host_ipv6_addr* によって指定された特定ホストを指定できます。
- *src_port* および *dst_port*：送信元ポートと宛先ポート（またはサービス）の引数です。演算子（**lt** [より小さい]、**gt** [より大きい]、**eq** [等しい]、**neq** [等しくない]、**range**（包括的範囲））のあとにスペースとポート番号（または **range** キーワードをスペースで区切った 2 つのポート番号）を入力します。
- *icmp_type*：アクセス ルールでフィルタリングする ICMP メッセージ タイプを指定します。値には、有効な ICMP タイプ数（0 ～ 155）、または付録 D「アドレス、プロトコル、およびポート」に示す ICMP タイプの文字名の 1 つを指定できます。**object-group** *id* を使用して ICMP オブジェクト グループを指定することもできます。

ステップ 2　次のコマンドを入力して、アクセス リストをインターフェイスに適用します。

```
hostname(config)# access-group access_list_name {in | out} interface if_name
```

IPv6 ネイバー探索の設定

IPv6 ネイバー探索プロセスでは ICMPv6 メッセージおよび送信要求ノードのマルチキャスト アドレスを使用して、同一ネットワーク（ローカル リンク）上のネイバーのリンク層アドレスの特定、ネイバーの到達可能性の検証、近接ルータの追跡を行います。

ここでは、次の内容について説明します。

- 「ネイバー送信要求メッセージの設定」（P.12-7）
- 「ルータ アドバタイズメント メッセージの設定」（P.12-9）
- 「マルチキャスト リスナー検出のサポート」（P.12-11）

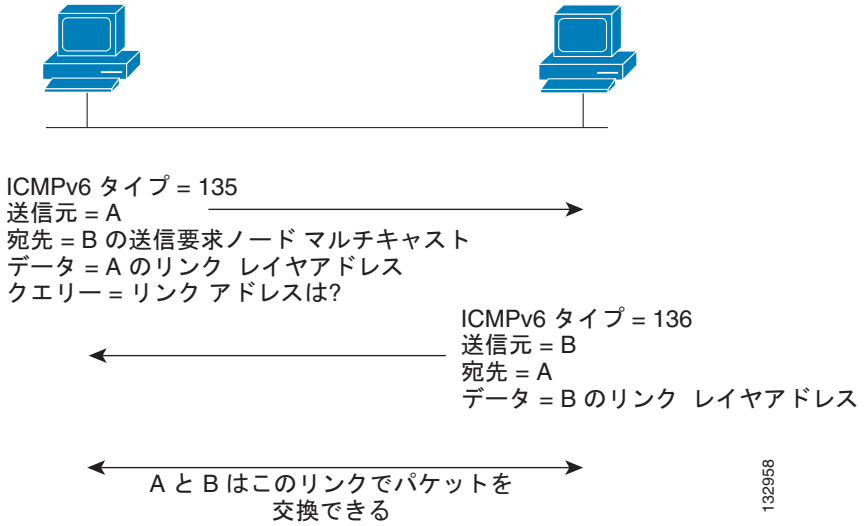
ネイバー送信要求メッセージの設定

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は送信要求ノード マルチキャスト アドレスに送信されます。ネイバー送信要求メッセージ内の送信元アドレスは、ネイバー送信要求メッセージを送信したノードの IPv6 アドレスです。ネイバー送信要求メッセージには、送信元ノードのリンク層アドレスも含まれます。

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。ネイバー アドバタイズメント メッセージ内の送信元アドレスは、ネイバー アドバタイズメント メッセージを送信したノードの IPv6 アドレスです。宛先アドレスは、ネイバー送信要求メッセージを送信したノードの IPv6 アドレスです。ネイバー アドバタイズメント メッセージのデータ部分には、ネイバー アドバタイズメント メッセージを送信するノードのリンク層アドレスが含まれます。

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。図 12-1 にネイバー送信要求と応答のプロセスを示します。

図 12-1　IPv6 ネイバー探索 - ネイバー送信要求メッセージ



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。そのような変更があった場合、ネイバー アドバタイズメントの宛先アドレスは全ノード マルチキャスト アドレスになります。

ネイバー送信要求メッセージの間隔とネイバー到達可能時間を、インターフェイス単位で設定できます。詳細については、次のトピックを参照してください。

- 「ネイバー送信要求メッセージの送信間隔の設定」（P.12-8）
- 「ネイバー到達可能時間の設定」（P.12-8）

ネイバー送信要求メッセージの送信間隔の設定

インターフェイスに IPv6 ネイバー送信要求メッセージを再送信する間隔を設定するには、次のコマンドを入力します。

```
hostname(config-if)# ipv6 nd ns-interval value
```

value 引数の有効値は 1,000 ～ 3,600,000 ミリ秒です。デフォルト値は 1000 ミリ秒です。

この設定は、ルータ アドバタイズメント メッセージでも送信されます。

ネイバー到達可能時間の設定

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。設定時間を短くすると、使用不可能なネイバーをさらに迅速に検出できます。ただし、時間を短くすると、すべての IPv6 ネットワーク デバイスで IPv6 ネットワーク帯域幅および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。

到達可能性確認イベントが発生した後でリモートの IPv6 ノードを到達可能と見なす時間を設定するには、次のコマンドを入力します。

```
hostname(config-if)# ipv6 nd reachable-time value
```

value 引数の有効値は 0 ～ 3,600,000 ミリ秒です。デフォルトは 0 です。

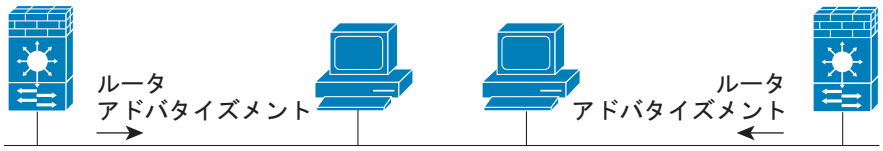
この情報は、ルータ アドバタイズメント メッセージでも送信されます。

value に 0 を使用すると、到達可能時間が未定のまま送信されます。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。この値を 0 に設定した場合に、セキュリティ アプライアンスで使用される時間を確認するには、**show ipv6 interface** コマンドを使用して、IPv6 インターフェイスに関する情報を表示します。使用中の ND 到達可能時間も含まれています。

ルータ アドバタイズメント メッセージの設定

ルータ アドバタイズメント メッセージ（ICMPv6 Type 134）は、セキュリティ アプライアンス の各 IPv6 対応インターフェイスに定期的に送信されます。ルータ アドバタイズメント メッセージは全ノード マルチキャスト アドレスに送信されます

図 12-2　IPv6 ネイバー探索 - ルータ アドバタイズメント メッセージ



ルータ アドバタイズメント パケットの定義：
ICMPv6 Type = 134
送信元 = ルータのリンクローカル アドレス
宛先 = 全ノードのマルチキャスト アドレス
データ = オプション、プレフィクス、ライフタイム、自動設定フラグ
132917

ルータ アドバタイズメント メッセージには、通常、次の情報が含まれています。

- ローカル リンク上のノードが IPv6 アドレスを自動設定するために使用できる 1 つまたは複数の IPv6 プレフィックス。
- アドバタイズメントに含まれるプレフィックスごとのライフタイム情報。
- 実行できる自動設定のタイプを示すフラグのセット（ステートレスまたはステートフル）。
- デフォルト ルータ情報（アドバタイズメントを送信するルータをデフォルト ルータとして使用する必要があるかどうか、デフォルト ルータであれば、そのルータをデフォルト ルータとして使用する秒単位の時間）。
- ホストに関する追加情報。たとえば、ホストから発信するパケットで使用するホップ制限や MTU など。
- 特定のリンク上でのネイバー送信要求メッセージの再送信間隔。
- ノードがネイバーを到達可能と見なす時間。

ルータ アドバタイズメントもルータ送信要求メッセージに応答して送信されます（ICMPv6 Type 133）。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。ルータ送信要求メッセージは、通常はホストからシステム起動時に送信されますが、ホストには設定済みのユニキャスト アドレスがないため、ルータ送信要求メッセージ内の送信元アドレスは通常は未指定 IPv6 アドレスとなります（0:0:0:0:0:0:0:0）。ホストに設定済みのユニキャスト アドレスがある場合、ルータ送信要求メッセージを送信するインターフェイスのユニキャスト アド

レスが、メッセージ内の送信元アドレスとして使用されます。ルータ送信要求メッセージの宛先アドレスは、スコープがリンクである全ルータ マルチキャスト アドレスです。ルータ送信要求に応答してルータ アドバタイズメントが送信される場合、ルータ アドバタイズメント メッセージ内の宛先アドレスはルータ送信要求メッセージの送信元のユニキャスト アドレスです。

次の設定値をルータ アドバタイズメント メッセージに対して設定できます。

- ルータ アドバタイズメント メッセージの定期的な時間間隔。
- ルータのライフタイム値。この値は、IPv6 ノードが セキュリティ アプライアンス をデフォルト ルータと見なす時間を示します。
- リンクで使用されている IPv6 ネットワークのプレフィックス。
- ルータ アドバタイズメント メッセージをインターフェイスが送信するかどうか。

特に指定のない限り、ルータ アドバタイズメント メッセージ設定はインターフェイス固有のものであり、インターフェイス コンフィギュレーション モードで入力されます。この設定の変更方法については、次の項目を参照してください。

- 「ルータ アドバタイズメントの送信間隔の設定」（P.12-10）
- 「ルータ ライフタイム値の設定」（P.12-10）
- 「IPv6 プレフィックスの設定」（P.12-10）
- 「ルータ アドバタイズメント メッセージの抑止」（P.12-11）

ルータ アドバタイズメントの送信間隔の設定

デフォルトでは、ルータ アドバタイズメントは 200 秒ごとに送信されます。インターフェイス上のルータ アドバタイズメント送信間隔を変更するには、次のコマンドを入力します。

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

有効値の範囲は 3 ～ 1,800 秒（**msec** キーワードを使用する場合は 500 ～ 1,800,000 ミリ秒）です。

セキュリティ アプライアンス が **ipv6 nd ra-lifetime** コマンドを使用してデフォルト 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のライフタイム以内でなければなりません。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。

ルータ ライフタイム値の設定

ルータのライフタイム値は、ローカル リンク上のノードが セキュリティ アプライアンス をリンクのデフォルト ルータと見なす時間を指定します。

インターフェイス上の IPv6 ルータ アドバタイズメントのルータ ライフタイム値を設定するには、次のコマンドを入力します。

```
hostname(config-if)# ipv6 nd ra-lifetime seconds
```

有効な値の範囲は、0 ～ 9000 秒です。デフォルトは 1,800 秒です。値 0 は、セキュリティ アプライアンス を選択したインターフェイス上のデフォルト ルータとして見なすべきではないことを示します。

IPv6 プレフィックスの設定

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。

どの IPv6 プレフィックスを IPv6 ルータ アドバタイズメントに含めるかを設定するには、次のコマンドを入力します。

```
hostname(config-if)# ipv6 nd prefix ipv6-prefix/prefix-length
```

（注）　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た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。

ルータ アドバタイズメント メッセージの抑止

デフォルトでは、ルータ アドバタイズメント メッセージは、ルータ送信要求メッセージへの応答として自動的に送信されます。セキュリティ アプライアンス で IPv6 プレフィックスを提供しないインターフェイス上において（外部インターフェイスなど）、ルータ アドバタイズメント メッセージをディセーブルにできます。

インターフェイス上で IPv6 ルータ アドバタイズメントを送信しないようにするには、次のコマンドを入力します。

```
hostname(config-if)# ipv6 nd suppress-ra
```

このコマンドを入力すると、セキュリティ アプライアンスがリンク上では 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。

マルチキャスト リスナー検出のサポート

マルチキャスト リスナー検出プロトコル（MLD）バージョン 2 は、直接接続されたリンク上のマルチキャスト アドレス リスナーの存在を検出するため、また、これらのネイバー ノードに関係のあるマルチキャスト アドレスを具体的に検出するためにサポートされています。ASA は、マルチキャスト アドレス リスナーまたはホストになりますが、マルチキャスト ルータにはなりません。また、マルチキャスト リスナー クエリーに応答し、マルチキャスト リスナー レポートのみを送信します。

次のコマンドが、MLD をサポートするために追加または拡張されました。

- clear ipv6 mld traffic コマンド
- show ipv6 mld コマンド

スタティック IPv6 ネイバーの設定

IPv6 ネイバー キャッシュでネイバーを手動で定義できます。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。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。

IPv6 ネイバー探索キャッシュにスタティック エントリを設定するには、次のコマンドを入力します。

```
hostname(config-if)# ipv6 neighbor ipv6_address if_name mac_address
```

ipv6_address 引数にはネイバーのリンクローカル IPv6 アドレス、*if_name* 引数にはネイバーを使用可能にするためのインターフェイス、*mac_address* 引数にはネイバー インターフェイスの MAC アドレスを指定します。

（注）　**clear ipv6 neighbors** コマンドは、スタティック エントリを IPv6 ネイバー探索キャッシュから削除しません。ダイナミック エントリを消去するだけです。

IPv6 コンフィギュレーションの確認

この項では、IPv6 コンフィギュレーションを確認する方法について説明します。さまざまな clear および show コマンドを使用して、IPv6 設定を確認できます。

この項では、次のトピックについて取り上げます。

- 「show ipv6 interface コマンド」（P.12-12）
- 「show ipv6 route コマンド」（P.12-12）
- 「show ipv6 mld traffic コマンド」（P.12-13）

show ipv6 interface コマンド

IPv6 インターフェイス設定を表示するには、次のコマンドを入力します。

```
hostname# show ipv6 interface [if_name]
```

「outside」などのインターフェイス名を含めると、指定したインターフェイスの設定が表示されます。名前をコマンドから除外すると、IPv6 がイネーブルになっているすべてのインターフェイスの設定が表示されます。コマンドの出力には次の事項が表示されます。

- 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

次に、**show ipv6 interface** コマンドの出力例を示します。

```
hostname# show ipv6 interface

ipv6interface is down, line protocol is down
  IPv6 is enabled, link-local address is fe80::20d:88ff:feee:6a82 [TENTATIVE]
  No global unicast address is configured
  Joined group address(es):
    ff02::1
    ff02::1:ffee:6a82
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
```

（注）　**show interface** コマンドは、インターフェイスの IPv4 設定だけを表示します。インターフェイスの IPv6 コンフィギュレーションを表示するには、**show ipv6 interface** コマンドを使用します。**show ipv6 interface** コマンドでは、インターフェイスの IPv4 設定は表示されません（そのインターフェイスで両方のタイプのアドレスが設定されている場合）。

show ipv6 route コマンド

IPv6 ルーティング テーブルのルートを表示するには、次のコマンドを入力します。

```
hostname# show ipv6 route
```

show ipv6 route コマンドの出力は、IPv4 **show route** コマンドの出力とほぼ同じです。次の情報を表示します。

- ルートを導出したプロトコル
- リモート ネットワークの IPv6 プレフィックス
- ルートのアドミニストレーティブ ディスタンスおよびメトリック
- ネクストホップ ルータのアドレス
- ネクスト ホップ ルータから指定ネットワークに到達するためのインターフェイス

次に、**show ipv6 route** コマンドの出力例を示します。

```
hostname# show ipv6 route

IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
L   fe80::/10 [0/0]
     via ::, inside
L   fec0::a:0:0:a0a:a70/128 [0/0]
     via ::, inside
C   fec0:0:0:a::/64 [0/0]
     via ::, inside
L   ff00::/8 [0/0]
     via ::, inside
```

show ipv6 mld traffic コマンド

IPv6 ルーティング テーブルの MLD トラフィック カウンタを表示するには、次のコマンドを入力します。

```
hostname# show ipv6 mld traffic
```

show ipv6 mld traffic コマンドの出力には、予測数の MLD プロトコル メッセージが受信および送信されたかどうかを表示します。

次に、**show ipv6 mld traffic** コマンドの出力例を示します。

```
hostname# show ipv6 mld traffic
show ipv6 mld traffic
MLD Traffic Counters
Elapsed time since counters cleared: 00:01:19
                  Received           Sent
Valid MLD Packets  1                  3
Queries            1                  0
Reports            0                  3
Leaves             0                  0
Mtrace packets     0              0
Errors:
Malformed Packets  0
Martian source     0
Non link-local source 0
Hop limit is not equal to 1 0
```