ipv6-a1

allow

RA スロットル ポリシーのスロットル期間ごとのデバイスあたりのマルチキャスト ルータ アドバタイズメント（RA）数を制限するには、IPv6 RA スロットル ポリシー コンフィギュレーション モードで **allow** コマンドを使用します。 コマンドをデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

allow {**at-least** | {*al-value*| **no-limit**}} | {**at-most** | {*am-value*| **no-limit**}} | {**inherited**}

構文の説明

at-least	スロットリング前にデバイスから受け入れるマルチキャストRAの最小数。
al-value	at-least の値。 • 0 ～ 32 の整数を指定できます。
no-limit	RA スロットリングは発生しません。
at-most	スロットリング前にデバイスから受け入れるマルチキャストRAの最大数。
am-value	at-most の値。 • 0 ～ 256 の整数を指定できます。
inherited	ターゲット ポリシー間の設定を継承または結合します。

コマンド デフォルト

at-least 値は 1 です。

at-most 値は 1 です。

コマンド モード

IPv6 RA スロットル ポリシー コンフィギュレーション モード（config-nd-ra-throttle）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

VLAN レベルで適用される **allow at-least** および **allow at-most** コマンド設定は、VLAN 内のすべてのデバイスのデフォルトを指定します。 RA を発行したデバイスが **allow at-least** コマンド設定によって設定されている RA 数を送信しなかった場合、RA はすべてのホストにマルチキャスト送信されます。 RA を発行したデバイスが **allow at-most** コマンド設定によって設定されている RA 数を送信している場合、RA はスロットリングされます。つまり、RA はすべての有線ホストと、保留中のルータ送信要求（RS）がある無線ホストにマルチキャスト送信されます。

allow at-least と **allow at-most** の値の設定が、すべてのポートのすべてのデバイスで同じ場合、その VLAN にポリシーを適用するだけで済みます。 有線ポートの一部が接続ワイヤレス アクセス ポイントである場合、これらのポートに適用する必要があるのは、設定するメディア タイプのポリシーだけです。

例

```
Device(config)# ipv6 nd ra-throttle policy policy1
Device(config-nd-ra-throttle)# allow at-least 2 at-most 2
```

clear bgp ipv6

IPv6 ボーダー ゲートウェイ プロトコル（BGP）セッションをリセットするには、特権 EXEC モードで **clear bgp ipv6** コマンドを使用します。

[1]

構文の説明

unicast	IPv6 ユニキャスト アドレス プレフィックスを指定します。
multicast	IPv6 マルチキャスト アドレス プレフィックスを指定します。
*	現在のすべての BGP セッションをリセットします。
autonomous-system-number	指定された自律システム内の BGP ネイバーの BGP セッションをリセットします。
ip-address	指定した IPv4 BGP ネイバーへの TCP 接続をリセットし、BGP テーブルからの接続から学習したすべてのルートを除外します。
ipv6-address	指定した IPv6 BGP ネイバーへの TCP 接続をリセットし、BGP テーブルからの接続から学習したすべてのルートを除外します。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
peer-group-name	指定した IPv6 BGP ネイバーへの TCP 接続をリセットし、BGP テーブルからの接続から学習したすべてのルートを除外します。
soft	（任意）ソフトリセットを行います。セッションはリセットしないでください。

1

in **out**	（任意）インバウンドまたはアウトバウンドソフト再設定を開始します。 オプション **in** または **out** が指定されていない場合、インバウンドソフトリセットとアウトバウンドソフトリセットの両方がトリガーされます。

コマンド デフォルト リセットは開始されません。

コマンド モード 特権 EXEC

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.3(2)T	**unicast** キーワードが、Cisco IOS Release 12.3(2)T で追加されました。
12.0(26)S	**unicast** および **multicast** キーワードが、Cisco IOS Release 12.0(26)S で追加されました。
12.3(4)T	**multicast** キーワードが、Cisco IOS Release 12.3(4)T で追加されました。
12.2(25)S	**multicast** キーワードが、Cisco IOS Release 12.2(25)S で追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
Cisco IOS XE Release 2.1	このコマンドは、Cisco ASR 1000 シリーズ ルータで追加されました。
12.2(33)SXI	このコマンドが、Cisco IOS Release 12.2(33)SXI に統合されました。

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

clear bgp ipv6 コマンドは **clear ip bgp** コマンドと類似していますが、これは IPv6 専用です。

clear bgp ipv6 コマンドを使用すると、指定されたキーワードと引数に応じた重大度レベルでネイバー セッションをリセットできます。

IPv6ユニキャストアドレスプレフィックスでネイバーセッションをドロップするには、**clear bgp ipv6 unicast** コマンドを使用します。

unicast キーワードは、Cisco IOS Release 12.3(2)T 以降のリリースで使用できます。 12.3(2)T よりも前のリリースでは使用できません。 **unicast** キーワードの使用は、Cisco IOS Release 12.3(2)T から必須です。

multicast キーワードは、Cisco IOS Release 12.0(26)S 以降のリリースで利用できます。 12.0(26)S よりも前のリリースでは使用できません。 **unicast** または **multicast** キーワードの使用は、Cisco IOS Release 12.0(26)S から必須です。

全ネイバー セッションをドロップするには、**clear bgp ipv6 *** コマンドを使用します。 Cisco IOS ソフトウェアは、ネイバー接続をリセットします。 この形式のコマンドは次の場合に使用してください。

- BGP タイマーの変更
- BGP アドミニストレーティブ ディスタンスの変更

アウトバウンド ネイバー接続だけをドロップするには、**clear bgp ipv6 soft out** または **clear bgp ipv6 unicast soft out** コマンドを使用します。 インバウンド ネイバー セッションはリセットされません。 この形式のコマンドは次の場合に使用してください。

- BGP 関連のアクセス リストの変更または追加の取得
- BGP 関連の重みの変更
- BGP 関連の配布リストの変更
- BGP 関連のルート マップの変更

インバウンド ネイバー接続だけをドロップするには、**clear bgp ipv6 soft in** または **clear bgp ipv6 unicast soft in** コマンドを使用します。 アウトバウンド ネイバー セッションはリセットされません。 ネイバーのインバウンド ルーティング テーブル アップデートを動的にリセットするには、ルータ リフレッシュ機能をサポートするようにネイバーを設定します。 BGP ネイバーがこの機能をサポートしているかどうかを判断するには、**show bgp ipv6 neighbors** または **show bgp ipv6 unicast neighbors** コマンドを使用します。 ネイバーがルータ リフレッシュ機能をサポートしている場合は、次のメッセージが表示されます。

```
Received route refresh capability from peer.
```

すべてのBGPネットワーク デバイスがルート リフレッシュ機能をサポートしている場合は、**clear bgp ipv6** {*****| ip-*address*| *ipv6-address*| *peer-group-name*} **in** または **clear bgp ipv6 unicast**{*****| ip-*address*| *ipv6-address*| *peer-group-name*} **in** コマンドを使用します。 ソフトウェアが自動的にソフト リセットを実行するため、**soft** キーワードの使用は、ルート リフレッシュ機能がすべての BGP ネットワーク デバイスによってサポートされている場合は必要ではありません。

この形式のコマンドは次の場合に使用してください。

- BGP 関連のアクセス リストの変更または追加の取得
- BGP 関連の重みの変更
- BGP 関連の配布リストの変更
- BGP 関連のルート マップの変更

例

次に、アウトバウンドセッションをリセットせずに、ネイバーが7000::2であるインバウンドセッションをクリアする例を示します。

```
Router# clear bgp ipv6 unicast 7000::2 soft in
```

次に、アウトバウンドセッションをリセットせずに、**unicast**キーワードを使用して、ネイバーが7000::2 であるインバウンド セッションをクリアする例を示します。

```
Router# clear bgp ipv6 unicast 7000::2 soft in
```

次に、インバウンド セッションをリセットせずに、marketing という名前のピア グループを持つアウトバウンド セッションをクリアする例を示します。

```
Router# clear bgp ipv6 unicast marketing soft out
```

次に、インバウンド セッションをリセットせずに、**unicast** キーワードを使用して、peer-group marketing という名前のピア グループを持つアウトバウンド セッションをクリアする例を示します。

```
Router# clear bgp ipv6 unicast peer-group marketing soft out
```

関連コマンド

コマンド	説明
show bgp ipv6	IPv6 BGP ルーティング テーブルのエントリを表示します。

clear ipv6 mtu

メッセージの最大伝送単位（MTU）キャッシュを削除するには、特権 EXEC モードで **clear ipv6 mtu** コマンドを使用します。

clear ipv6 mtu

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

メッセージは MTU キャッシュから削除されません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.6	このコマンドが導入されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ルータが ICMPv6 toobig メッセージでフラッドした場合、ルータはすべての使用可能なメモリが消費されるまで、MTU キャッシュに無制限にエントリを作成します。 MTU キャッシュからメッセージをクリアするには、**clear ipv6 mtu** コマンドを使用します。

例

次の例では、メッセージの MTU キャッシュをクリアします。

```
Router# clear ipv6 mtu
```

関連コマンド

コマンド	説明
ipv6 flowset	ルータが送信する 1280 バイト以上のパケットにフロー ラベル マーキングを設定します。

default-metric（OSPFv3）

Open Shortest Path First バージョン 3（OSPF）ルーティング プロトコルに再配布される IPv4 および IPv6 ルートのデフォルト メトリック値を設定するには、OSPFv3 ルータ コンフィギュレーション モード、IPv6 アドレス ファミリ コンフィギュレーション モード、または IPv4 アドレス ファミリ コンフィギュレーション モードで **default-metric** コマンドを使用します。 デフォルトの状態に戻すには、このコマンドの **no** 形式を使用します。

default-metric *metric-value*

no default-metric *metric-value*

構文の説明

metric-value	指定されたルーティング プロトコルに適したデフォルト メトリック値。 指定できる範囲は 1 ～ 4294967295 です。

コマンド デフォルト

各ルーティング プロトコルに適した、組み込みの自動的なメトリック変換。

コマンド モード

OSPFv3 ルータ コンフィギュレーション モード（config-router）

IPv6 アドレス ファミリ コンフィギュレーション（config-router-af）

IPv4 アドレス ファミリ コンフィギュレーション（config-router-af）

コマンド履歴

リリース	変更内容
12.2(15)T	このコマンドが導入されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
15.1(3)S	このコマンドが変更されました。 機能は、IPv4 または IPv6 OSPFv3 プロセスでイネーブルにできます。
Cisco IOS XE Release 3.4S	このコマンドが変更されました。 機能は、IPv4 または IPv6 OSPFv3 プロセスでイネーブルにできます。
15.2(1)T	このコマンドが変更されました。 機能は、IPv4 または IPv6 OSPFv3 プロセスでイネーブルにできます。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

default-metric コマンドと **redistribute** ルータ コンフィギュレーション コマンドを組み合わせて使用すると、現在のルーティング プロトコルで、すべての再配布ルートで同じメトリック値が使用されます。 デフォルトのメトリックは、互換性のないメトリックを持つルートを再配布するという問題を解決するために役立ちます。メトリックを変換しない場合、デフォルトメトリックの使用は妥当な代替手段で、再配布が可能となります。

redistribute コマンドのオプションを使用して、再配布されるルートのメトリックを細かく制御できます。

例

次に、IPv6 AF を入力し、process1 という OSPFv3 プロセスからルートを再配布する OSPFv3 ルーティング プロトコルを設定する例を示します。 再配布されるすべてのルートは 10 のメトリックでアドバタイズされます。

```
router ospfv3 100
 address-family ipv6 unicast
 default-metric 10
 redistribute ospfv3 process1
```

次に、process1 という OSPFv3 プロセスからルートを再配布する OSPFv3 ルーティング プロトコルを設定する例を示します。 再配布されるすべてのルートは 10 のメトリックでアドバタイズされます。

```
ipv6 router ospf 100
 default-metric 10
 redistribute ospfv3 process1
```

関連コマンド

コマンド	説明
redistribute（OSPFv3）	あるルーティング ドメインから別のルーティング ドメインへ IPv6 ルートを再配布します。
router ospfv3	IPv4 または IPv6 アドレス ファミリの OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。

deny（IPv6）

IPv6 アクセス リストの拒否条件を設定するには、IPv6 アクセス リスト コンフィギュレーション モードで **deny** コマンドを使用します。 拒否条件を削除するには、このコマンドの **no** 形式を使用します。

deny *protocol* {*source-ipv6-prefix*/*prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] **[routing]** [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] **[undetermined-transport]**

no deny *protocol* {*source-ipv6-prefix*/*prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] **[routing]** [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] **[undetermined-transport]**

Internet Control Message Protocol

deny icmp {*source-ipv6-prefix*/*prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] [*icmp-type* [*icmp-code*]| *icmp-message*] [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] **[routing]** [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Transmission Control Protocol

deny tcp {*source-ipv6-prefix*/*prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] **[ack]** [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] **[established] [fin]** [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] [**neq** {*port*| *protocol*}] **[psh]** [**range** {*port*| *protocol*}] **[routing]** [**routing-type** *routing-number*] **[rst]** [**sequence** *value*] **[syn]** [**time-range** *name*] **[urg]**

User Datagram Protocol

deny udp {*source-ipv6-prefix*/*prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] [**neq** {*port*| *protocol*}] [**range** {*port*| *protocol*}] **[routing]** [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

構文の説明

protocol	インターネットプロトコルの名前または番号。これは、キーワード **ahp**、**esp**、**icmp**、**ipv6**、**pcp**、**sctp**、**tcp**、**udp**、または **hbh** にするか、IPv6 プロトコル番号を表す 0 ～ 255 の整数にすることができます。
source-ipv6-prefix/prefix-length	拒否条件を設定する送信元 IPv6 ネットワークまたはネットワークのクラス。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
any	IPv6 プレフィックス ::/0 の省略形。
host *source-ipv6-address*	拒否条件を設定する送信元 IPv6 ホスト アドレス。 この *source-ipv6-address* 引数には RFC 2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。

operator [*port-number*]	（任意）指定のプロトコルの送信元または宛先ポートを比較するオペランドを指定します。オペランドには、**lt**（less than：より小さい）、**gt**（greater than：より大きい）、**eq**（equal：等しい）、**neq**（not equal：等しくない）、および **range**（inclusive range：包含範囲）があります。 *source-ipv6-prefix*/*prefix-length* 引数の後ろに演算子が置かれた場合、送信元ポートと一致する必要があります。 *destination-ipv6*/*prefix-length* 引数の後ろに演算子が置かれた場合、宛先ポートと一致する必要があります。 **range** 演算子には 2 つのポート番号が必要です。他のすべての演算子は 1 つのポート番号が必要です。 任意の *port-number* 引数は 10 進数、または TCP あるいは UDP ポートの名前です。 ポート番号の範囲は 0 ～ 65535 です。 TCP ポート名は TCP をフィルタリングする場合に限り使用できます。 UDP ポート名は UDP をフィルタリングする場合に限り使用できます。
destination-ipv6-prefix/*prefix-length*	拒否条件を設定する宛先 IPv6 ネットワークまたはネットワークのクラス。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
host *destination-ipv6-address*	拒否条件を設定する宛先 IPv6 ホストアドレス。 この *destination-ipv6-address* 引数には RFC 2373 に記載のように、コロンで区切られた 16 ビット値を使用した 16 進数形式でアドレスを指定する必要があります。
auth	任意のプロトコルと組み合わせて、認証ヘッダーのプレゼンスとトラフィックを照合できます。
dest-option-type	（任意）各 IPv6 パケット ヘッダー内のホップバイホップ オプション拡張ヘッダーと IPv6 パケットを照合します。

doh-number	（任意）IPv6宛先オプション拡張ヘッダーを表す 0 から 255 の範囲の整数。
doh-type	（任意）宛先オプション ヘッダー タイプ。 可能な宛先オプション ヘッダー タイプおよび対応する *doh-number* 値は、home-address と 201 です。
dscp *value*	（任意）各IPv6パケットヘッダーのトラフィック クラス フィールドのトラフィック クラス値と DiffServ コード ポイント値を照合します。 指定できる範囲は 0 ～ 63 です。
flow-label *value*	（任意）各 IPv6 パケット ヘッダーのフロー ラベル フィールドのフロー ラベルの値とフロー ラベルの値を照合します。 指定できる範囲は 0 ～ 1048575 です。
fragments	（任意）フラグメント拡張ヘッダーに 0 以外のフラグメント オフセットが含まれる場合、非初期フラグメント パケットを照合します。 **fragments** キーワードは、*operator* [*port-number*] 引数が指定されていない場合に限り指定できるオプションです。
hbh	（任意）ホップバイホップ オプション ヘッダーを指定します。
log	（任意）コンソールに送信されるエントリに一致するパケットに関するロギング メッセージ情報が出力されます。 コンソールにロギングするメッセージのレベルは、**logging console** コマンドで制御します。 メッセージには、アクセス リスト名、シーケンス番号、パケットが拒否されたかどうか、プロトコル（TCP、UDP、ICMP または番号のいずれか）、適正な場合には送信元/宛先アドレス、送信元/宛先ポート番号が含まれます。 メッセージは、一致した最初のパケットに対して生成され、その後、5 分間隔で拒否されたパケット数を含めて生成されます。
log-input	（任意）ロギング メッセージに入力インターフェイスも含まれることを除き、**log** キーワードと同じ機能を提供します。

mobility	（任意）拡張ヘッダーのタイプ。ヘッダー内のモビリティ ヘッダーのタイプ フィールドの値に関係なくモビリティ ヘッダーを含むすべてのIPv6 パケットを照合できます。
mobility-type	（任意）モビリティ ヘッダー タイプ。このキーワードと共に、*mh-number* または *mh-type* 引数を使用する必要があります。
mh-number	（任意）IPv6 モビリティ ヘッダー タイプを表す 0 から 255 の範囲の整数。
mh-type	（任意）モビリティ ヘッダー タイプの名前。次のようなモビリティ ヘッダー タイプと対応する *mh-number* 値が可能です。 • 0：bind-refresh • 1：hoti • 2：coti • 3：hot • 4：cot • 5：bind-update • 6：bind-acknowledgment • 7：bind-error
routing	（任意）ソースルート パケットを、各 IPv6 パケット ヘッダー内の拡張ヘッダーに一致させます。
routing-type	（任意）タイプ フィールドの値を持つルーティング ヘッダーを個別に照合できます。 このキーワードと共に、*routing-number* 引数を使用する必要があります。
routing-number	IPv6 ルーティング ヘッダー タイプを表す 0 から 255 の範囲の整数。 次のようなルーティング ヘッダー タイプと対応する *routing-number* 値が可能です。 • 0：標準 IPv6 ルーティング ヘッダー • 2：モバイル IPv6 ルーティング ヘッダー

sequence *value*	（任意）アクセスリストステートメントのシーケンス番号を指定します。 指定できる範囲は 1 ～ 4294967295 です。
time-range *name*	（任意）拒否ステートメントに適用する時間範囲を指定します。 時間範囲の名前と制限事項は、**time-range** コマンドと、**absolute** または **periodic** コマンドによってそれぞれ指定します。
undetermined-transport	（任意）レイヤ 4 プロトコルを判定できない送信元からのパケットに一致します。 **undetermined-transport** キーワードは、*operator* [*port-number*] 引数が指定されていない場合にのみ任意です。
icmp-type	（任意）ICMP パケットのフィルタリングに ICMP メッセージ タイプを指定します。 ICMP パケットは、ICMP メッセージ タイプでフィルタリングできます。 ICMP メッセージ タイプは、0 ～ 255 の数字で、次のような事前定義された文字列とそれに対応する数値が含まれています。 • 144：dhaad-request • 145：dhaad-reply • 146：mpd-solicitation • 147：mpd-advertisement
icmp-code	（任意）ICMP パケットのフィルタリングに ICMP メッセージ コードを指定します。 ICMP メッセージタイプによってフィルタリングされる ICMP パケットは、ICMP メッセージ コードによってもフィルタリングできます。 メッセージ コードの番号は 0 ～ 255 です。
icmp-message	（任意）ICMP パケットのフィルタリングに ICMP メッセージ名を指定します。 ICMP パケットは、ICMP メッセージ名、または ICMP メッセージタイプおよびコードによってフィルタリングできます。 使用可能な名前については、「使用上のガイドライン」を参照してください。

ack	（任意）TCPプロトコルの場合に限りACKビットを設定します。
established	（任意）TCPプロトコルの場合にだけ、確立された接続を表示します。 TCP データグラムにACKまたはRSTビットが設定されている場合、照合が行われます。 接続するための初期 TCP データグラムの場合は照合しません。
fin	（任意）TCP プロトコルの場合に限り、FIN ビットを設定します。送信元からのデータはこれ以上ありません。
neq {*port* | *protocol*}	（任意）指定のポート番号上にないパケットだけを照合します。
psh	（任意）TCPプロトコルの場合に限りPSHビットを設定します。
range {*port* | *protocol*}	（任意）ポート番号範囲のパケットだけを照合します。
rst	（任意）TCPプロトコルの場合に限りRSTビットを設定します。
syn	（任意）TCPプロトコルの場合に限りSYNビットを設定します。
urg	（任意）TCPプロトコルの場合に限りURGビットを設定します。

コマンド デフォルト

IPv6 アクセス リストは定義されていません。

コマンド モード

IPv6 アクセス リスト コンフィギュレーション (config-ipv6-acl)#

コマンド履歴

リリース	変更内容
12.0(23)S	このコマンドが導入されました。
12.2(13)T	このコマンドが、Cisco IOS Release 12.2(13)T に統合されました。

リリース	変更内容
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.4(2)T	*icmp-type* 引数が拡張されました。 **dest-option-type**、**mobility**、**mobility-type** および **routing-type** キーワードが追加されました。*doh-number*、*doh-type*、*mh-number*、*mh-type* および *routing-number* 引数が追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco ASR 1000 アグリゲーション シリーズ ルータに追加されました。
12.4(20)T	**auth** キーワードが追加されました。
12.2(33)SRE	このコマンドが、Cisco IOS Release 12.2(33)SRE に統合されました。
15.2(3)T	このコマンドが変更されました。 **hbh** キーワードのサポートが追加されました。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

deny（IPv6）コマンドは、IPv6 に固有のものを除き、**deny**（IP）コマンドと類似しています。

ipv6 access-list コマンドに続いて、**deny**（IPv6）コマンドを使用すると、パケットがアクセス リストを通過する条件を定義すること、または再帰アクセスリストとしてアクセスリストを定義することができます。

protocol 引数に IPv6 を指定すると、パケットの IPv6 ヘッダーに対して照合を行います。

デフォルトでは、アクセス リストの最初のステートメントの番号は 10 で、その次のステートメントからは 10 ずつ増加します。

permit、**deny**、**remark**、または **evaluate** ステートメントを、リスト全体を再入力せずに既存のアクセスリストに追加できます。新しいステートメントをリストの最後尾以外に追加するには、所属先を示すために 2 つの既存のエントリ番号の間にある適切なエントリ番号を持つ新しいステートメントを作成します。

Cisco IOS Release 12.2(2)T 以降のリリース、12.0(21)ST、および 12.0(22)S では、IPv6 アクセス コントロール リスト（ACL）の定義、および拒否条件と許可条件の設定は、グローバル コンフィギュレーション モードで **ipv6 access-list** コマンドと **deny** および **permit** キーワードを使用して行います。 Cisco IOS Release 12.0(23)S 以降のリリースでは、IPv6 ACL は、グローバル コンフィギュレーション モードで **ipv6 access-list** コマンドを使用することにより定義され、許可条件と拒否条件は、IPv6 アクセスリスト コンフィギュレーション モードで **deny** コマンドおよび **permit** コマンドを使用して設定されます。 IPv6 ACL の定義の詳細については、**ipv6 access-list** コマンドを参照してください。

（注） Cisco IOS Release 12.0(23)S 以降のリリースでは、IPv6 ACL に最後の一致条件として暗黙の **permit icmp any any nd-na**、**permit icmp any any nd-ns**、および**deny ipv6 any any** ステートメントがあります。（前の 2 つの一致条件により ICMPv6 ネイバー探索が可能になります）。IPv6 ACL には、暗黙の **deny ipv6 any any** ステートメントを有効にするために少なくとも 1 つのエントリが含まれる必要があります。 IPv6 ネイバー探索プロセスでは、IPv6 ネットワーク層サービスを利用するため、デフォルトで、インターフェイス上での IPv6 ネイバー探索パケットの送受信が IPv6 ACL によって暗黙的に許可されます。 IPv4 の場合、IPv6 ネイバー探索プロセスに相当するアドレス解決プロトコル（ARP）では、個別のデータ リンク層プロトコルを利用するため、デフォルトで、インターフェイス上での ARP パケットの送受信が IPv4 ACL によって暗黙的に許可されます。

source-ipv6-prefix/*prefix-length* と *destination-ipv6-prefix*/*prefix-length* の両方の引数をトラフィックのフィルタリングに使用します（送信元プレフィックスはトラフィックの送信元に基づいて、宛先プレフィックスはトラフィックの宛先に基づいてトラフィックをフィルタリングします）。

（注） アクセス リストでなく、IPv6 プレフィックス リストは、ルーティング プロトコル プレフィックスのフィルタリングに使用する必要があります。

fragments キーワードは、*operator* [*port-number*] 引数が指定されていない場合に限り指定できるオプションです。

undetermined-transport キーワードは、*operator* [*port-number*] 引数が指定されていない場合にのみ任意です。

次に、ICMP メッセージの名前のリストを示します。

- beyond-scope
- destination-unreachable
- echo-reply
- echo-request
- header
- hop-limit
- mld-query

- mld-reduction
- mld-report
- nd-na
- nd-ns
- next-header
- no-admin
- no-route
- packet-too-big
- parameter-option
- parameter-problem
- port-unreachable
- reassembly-timeout
- renum-command
- renum-result
- renum-seq-number
- router-advertisement
- router-renumbering
- router-solicitation
- time-exceeded
- unreachable

例

次に、toCISCO という名前の IPv6 アクセス リストを設定し、イーサネット インターフェイス 0 上の発信トラフィックにアクセスリストを適用する例を示します。具体的には、リストの最初の拒否エントリは、宛先 TCP ポート番号が 5000 よりも大きいすべてのパケットが、イーサネット インターフェイス 0 から出て行かないようにします。 リストの 2 番めの拒否エントリは、送信元 UDP ポート番号が 5000 より小さいすべてのパケットが、イーサネット インターフェイス 0 から出て行かないようにします。 また、この 2 番めの拒否エントリは、すべての一致をコンソールに表示します。 リスト内の最初の許可エントリは、イーサネットインターフェイス 0 から出るすべての ICMP パケットを許可します。 リスト内の 2 番めの許可エントリは、イーサネット インターフェイス 0 から出るその他すべてのトラフィックを許可します。 2 番目の許可エントリは、すべての条件の暗黙的な拒否は各 IPv6 アクセス リストの最後にあるという理由で必要です。

```
ipv6 access-list toCISCO
 deny tcp any any gt 5000
 deny ::/0 lt 5000 ::/0 log
 permit icmp any any
 permit any any
interface ethernet 0
 ipv6 traffic-filter toCISCO out
```

次に、IPsec AH がある場合でも、TCP または UDP の解析を許可する例を示します。

```
IPv6 access list example1
    deny tcp host 2001::1 any log sequence 5
    permit tcp any any auth sequence 10
    permit udp any any auth sequence 20
```

関連コマンド

コマンド	説明
ipv6 access-list	IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ipv6 traffic-filter	インターフェイス上の着信または発信 IPv6 トラフィックをフィルタリングします。
permit（IPv6）	IPv6アクセスリストに許可条件を設定します。
show ipv6 access-list	現在のすべての IPv6 アクセス リストの内容を表示します。

destination-glean

宛先アドレス グリーニングによる IPv6 第 1 ホップ セキュリティ バインディング テーブルのリカバリをイネーブルにする、またはリカバリ後に認識されないバインディングテーブルエントリに関する syslog メッセージを生成するには、IPv6 スヌーピング コンフィギュレーション モードで **destination-glean** コマンドを使用します。バインディングテーブルのリカバリを無効にするには、このコマンドの **no** 形式を使用します。

destination-glean {**recovery** | **log-only**} [**dhcp**]

no destination-glean

構文の説明

recovery	宛先アドレス グリーニングによるバインディングテーブルのリカバリをイネーブルにします。
log-only	リカバリ後に認識されないバインディングテーブルエントリに関する syslog メッセージを生成します。
dhcp	宛先アドレスを Dynamic Host Configuration Protocol（DHCP）からリカバリする必要があることを指定します。

コマンド デフォルト

宛先アドレス グリーニングによる IPv6 第 1 ホップ セキュリティ バインディング テーブルのリカバリはイネーブルになりません。

コマンド モード

IPv6 スヌーピング コンフィギュレーション モード（config-ipv6-snooping）

コマンド履歴

リリース	変更内容
15.2(4)S	このコマンドが導入されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ipv6 destination-guard policy コマンドを使用して IPv6 宛先ガードを設定した場合、その後 IPv6 第 1 ホップ セキュリティ バインディング テーブルのリカバリを設定できます。

ipv6 snooping policy コマンドによりスヌーピング ポリシーを設定できます。 このポリシーの一部として第 1 ホップ セキュリティ バインディング テーブルのリカバリを設定できます。 スヌーピング ポリシーは **ipv6 snooping attach-policy** コマンドを使用して、ポートまたは VLAN に適用する必要があります。

destination-glean コマンドと **log-only** キーワードを使用した場合、syslog メッセージだけが生成され、リカバリは試行されません。

例

次の例では、宛先アドレスを DHCP からリカバリする必要があることを示します。

```
Device(config-ipv6-snooping)# destination-glean recovery dhcp
```

次の例では、バインディング テーブルのリカバリ後に欠落したすべての宛先アドレスについて syslog メッセージが生成されます。

```
Device(config-ipv6-snooping)# destination-glean log-only
```

関連コマンド

コマンド	説明
ipv6 destination-guard policy	IPv6 宛先ガード ポリシーを設定します。
ipv6 snooping policy	IPv6 スヌーピング コンフィギュレーション モードを開始します。

device-role

ポートに接続されているデバイスのロールを指定するには、ネイバー探索（ND）インスペクション ポリシー コンフィギュレーション モードまたはルータ アドバタイズメント（RA）ガード ポリシー コンフィギュレーション モードで **device-role** コマンドを使用します。

device-role {**host**| **monitor**| **router**}

構文の説明

host	デバイスのロールをホストに設定します。
monitor	デバイスのロールをモニタに設定します。
router	デバイスのロールをルータに設定します。

コマンド デフォルト

デバイスのロールはホストです。

コマンド モード

ND インスペクション ポリシー コンフィギュレーション（config-nd-inspection）

RA ガード ポリシー コンフィギュレーション（config-ra-guard）

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.2(4)S	このコマンドが Cisco IOS Release 15.2(4)S に統合されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

device-role コマンドは、ポートに接続されたデバイスのロールを指定します。 デフォルトでは、デバイスのロールはホストであるため、すべてのインバウンドルータ アドバタイズメントとリダイレクト メッセージはブロックされます。 **router** キーワードを使用してデバイス ロールをイネーブルにすると、このポートで、すべてのメッセージ（ルータ送信要求（RS）、ルータ アドバタイズメント（RA）、またはリダイレクト）が許可されます。

router または **monitor** キーワードが使用されている場合、制限付きブロードキャストがイネーブルかどうかに関係なく、マルチキャスト RS メッセージがポートでブリッジングされます。 ただし、**monitor** キーワードはインバウンド RA またはリダイレクト メッセージを許可しません。 **monitor** キーワードを使用すると、必要とするデバイスがこれらのメッセージを受け取ります。

（注） Cisco IOS Release 15.2(4) S1 から、信頼できるポートがデバイス ロールよりも優先して、ポート上でルータへの RA を受信します。 このリリース以前は、デバイス ロールのルータが信頼できるポートよりも優先されていました。デバイス ロールのルータは、RS をポートに送信できるようにするために、現在も設定する必要があります。

例

次に、ネイバー探索プロトコル（NDP）ポリシー名を policy1 として定義し、デバイスを ND インスペクション ポリシー コンフィギュレーション モードにして、ホストとしてデバイスを設定する例を示します。

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# device-role host
```

次に、RA ガード ポリシー名を raguard1 として定義し、デバイスを RA ガード ポリシー コンフィギュレーション モードにして、ホストとしてデバイスを設定する例を示します。

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# device-role host
```

関連コマンド

コマンド	説明
ipv6 nd inspection policy	ND インスペクション ポリシー名を定義して、ND インスペクション ポリシー コンフィギュレーション モードを開始します。
ipv6 nd raguard policy	RA ガード ポリシー名を定義し、RA ガード ポリシー コンフィギュレーション モードを開始します。

drop-unsecure

オプションがないか、無効なオプションまたは無効なシグニチャが含まれるメッセージをドロップするには、ネイバー探索（ND）インスペクション ポリシー コンフィギュレーション モードまたはルータ アドバタイズメント（RA）ガード ポリシー コンフィギュレーション モードで **drop-unsecure** コマンドを使用します。 この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

drop-unsecure

no drop-unsecure

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

ND インスペクション ポリシーは設定されていません。

コマンド モード

ND インスペクション ポリシー コンフィギュレーション（config-nd-inspection）

RA ガード ポリシー コンフィギュレーション（config-ra-guard）

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

drop-unsecure コマンドは、RFC 3971『*Secure Discovery (SeND)*』に従い、暗号化生成アドレス（CGA）オプションまたは Rivest, Shamir, and Adleman（RSA）シグニチャがない、または無効であるメッセージをドロップします。 ただし、RFC 3972『*Cryptographically Generated Addresses (CGA)*』に準拠していない、または同RFCに従って検証されていないRSAシグニチャまたはCGAオプションが含まれているメッセージがドロップされることに注意してください。

drop-unsecure コマンドは、**ipv6 nd inspection policy** コマンドを使用して ND インスペクション ポリシー コンフィギュレーション モードをイネーブルにした後で使用します。

例

次に、NDポリシー名をpolicy1として定義し、ルータをNDインスペクション ポリシー コンフィギュレーション モードにして、無効なCGAオプションまたは無効なRSAシグニチャを含むメッセージをドロップするようルータをイネーブルにする例を示します。

```
Router(config)# ipv6 nd-inspection policy policy1
Router(config-nd-inspection)# drop-unsecure
```

関連コマンド

コマンド	説明
ipv6 nd inspection policy	NDインスペクション ポリシー名を定義して、NDインスペクション ポリシー コンフィギュレーション モードを開始します。
ipv6 nd raguard policy	RAガード ポリシー名を定義し、RAガード ポリシー コンフィギュレーション モードを開始します。

enforcement

宛先ガード ポリシーの適用レベルを設定するには、宛先ガード コンフィギュレーション モードで **enforcement** コマンドを使用します。

enforcement {**always**| **stressed**}

構文の説明

always	適用レベルを常時に設定します。
stressed	適用レベルをシステムにストレスがある場合にだけ適用するように設定します。

コマンド デフォルト

宛先ガード ポリシーの適用レベルは常時に設定されます。

コマンド モード

宛先ガード コンフィギュレーション（config-destguard）

コマンド履歴

リリース	変更内容
15.2(4)S	このコマンドが導入されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ネットワーク アーキテクチャ、バインディング テーブル情報のソース、およびシステムの変更の程度によっては、バインディング テーブルに VLAN のノード メンバーシップに関する詳細な情報が常にあるわけではない可能性があります。 適用レベル ポリシー要素は、VLAN メンバーシップに関して信頼される情報を持つシステムでは、適用レベルを always に設定する必要があることを意味します。 信頼性の低くてもよいシステム、または不用意なパケット損失を強く回避したいシステムでは、適用レベルを stressed に設定します

例

次に、適用レベルを常時に設定する例を示します。

```
Device(config)# ipv6 destination-guard policy destination
Device(config-destguard)# enforcement always
```

関連コマンド

コマンド	説明
ipv6 destination-guard policy	宛先ガード ポリシーを定義します。

graceful-restart

グレースフル リスタート対応ルータで Open Shortest Path First バージョン 3（OSPFv3）のグレースフル リスタート機能をイネーブルにするには、OSPF ルータ コンフィギュレーション モードで **graceful-restart** コマンドを使用します。 グレースフル リスタートをディセーブルにするには、このコマンドの **no** 形式を使用します。

graceful-restart [**restart-interval** *interval*]

no graceful-restart

構文の説明

restart-interval *interval*	（任意）秒単位の、グレースフル リスタートの間隔。 指定できる範囲は 1 ～ 1800 で、デフォルトは 120 です。

コマンド デフォルト

GR 対応ルータで GR 機能はイネーブルになっていません。

コマンド モード

OSPFv3 ルータ コンフィギュレーション モード（config-router）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが導入されました。
15.0(1)M	このコマンドが、Cisco IOS Release 12.5(1)M に統合されました。
12.2(33)SRE	このコマンドが変更されました。 Cisco IOS Release 12.2(33)SRE に統合されました。
12.2(33)XNE	このコマンドが変更されました。 Cisco IOS Release 12.2(33)XNE に統合されました。
15.1(3)S	このコマンドが変更されました。 機能は、IPv4 または IPv6 OSPFv3 プロセスでイネーブルにできます。
Cisco IOS XE Release 3.4S	このコマンドが変更されました。 機能は、IPv4 または IPv6 OSPFv3 プロセスでイネーブルにできます。
15.2(1)T	このコマンドが変更されました。 機能は、IPv4 または IPv6 OSPFv3 プロセスでイネーブルにできます。

リリース	変更内容
15.1(1)SY	このコマンドが変更されました。 機能は、IPv4 または IPv6 OSPFv3 プロセスでイネーブルにできます。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

graceful-restart コマンドは GR 対応ルータでだけイネーブルにできます。

例

次に、IPv6 および IPv4 で、GR 対応ルータでグレースフル リスタート モードをイネーブルにする例を示します。

```
Router(config)# ospfv3 router 1
Router(config-router)# graceful-restar
```

次に、IPv6 でのみ、GR 対応ルータでグレースフル リスタート モードをイネーブルにする例を示します。

```
Router(config)# ipv6 router ospf 1234
Router(config-router)# graceful-restart
```

関連コマンド

コマンド	説明
graceful-restart helper	GR 対応ルータで OSPFv3 グレースフル リスタート機能をイネーブルにします。
router ospfv3	IPv4 または IPv6 アドレス ファミリの OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。

hop-limit

アドバタイズされたホップ カウント制限を確認するには、RA ガード ポリシー コンフィギュレーション モードで **hop-limit** コマンドを使用します。

hop-limit {**maximum**| **minimum** } *limit*

構文の説明

maximum *limit*	ホップ カウント制限が *limit* 引数によって設定された値よりも低いことを確認します。
minimum *limit*	ホップ カウント制限が *limit* 引数によって設定された値よりも大きいことを確認します。

コマンド デフォルト

ホップ カウント制限は指定されていません。

コマンド モード

RA ガード ポリシー コンフィギュレーション（config-ra-guard）

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.2(4)S	このコマンドが Cisco IOS Release 15.2(4)S に統合されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

hop-limit コマンドによって、アドバタイズされたホップ カウント制限が *limit* 引数によって設定された値より大きいまたは小さいことを確認できます。 **minimum** キーワードと *limit* 引数を設定すると、攻撃者がホストに低いホップ カウント制限値を設定して、リモート接続先（デフォルト ルータの先）にトラフィックを生成できないようにすることを防止できます。 アドバタイズされたホップ カウント制限値が指定されていない場合（値 0 を設定した場合と同じ）、パケットはドロップされます。

maximum キーワードと *limit* 引数を設定すると、アドバタイズされたホップ カウント制限が *limit* 引数で設定した値未満であることを確認できます。アドバタイズされたホップカウント制限値が指定されていない場合（値 0 を設定した場合と同じ）、パケットはドロップされます。

例

次に、ルータ アドバタイズメント（RA）ガード ポリシー名を raguard1 として定義し、ルータを RA ガード ポリシー コンフィギュレーション モードにして、最小ホップ カウント制限を 3 に設定する例を示します。

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# hop-limit minimum 3
```

関連コマンド

コマンド	説明
ipv6 nd raguard policy	RA ガード ポリシー名を定義し、RA ガード ポリシー コンフィギュレーション モードを開始します。

interval-option

RA スロットル ポリシーの IPv6 ルータ アドバタイズメント（RA）間隔を調整するには、IPv6 RA スロットル ポリシー コンフィギュレーション モードで **interval-option** を使用します。 コマンドをデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

interval-option {**ignore**| **inherit**| **pass-through**| **throttle**}

構文の説明

ignore	間隔オプションはスロットリングに影響しません。
inherit	ターゲット ポリシー間の設定をマージします。
pass-through	間隔オプションを持つすべての RA が転送されます。
throttle	間隔オプションを持つすべての RA がスロットリングされます。

コマンド デフォルト

Pass-through

コマンド モード

IPv6 RA スロットル ポリシー コンフィギュレーション モード（config-nd-ra-throttle）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

interval-option コマンドは、RA スロットル ポリシーの間隔オプションを設定します。 RFC 6275 で定義されているように、間隔オプションは、送信側デバイスが非送信請求マルチキャスト RA を送信する間隔をアドバタイズするために RA メッセージで使用されます。

例

```
Device(config)# ipv6 nd ra-throttle policy policy1
Device(config-nd-ra-throttle)# interval-option inherit
```

ipv6 access-list

IPv6 アクセス リストを定義してデバイスを IPv6 アクセス リスト コンフィギュレーション モードに設定するには、グローバル コンフィギュレーション モードで **ipv6 access-list** コマンドを使用します。 アクセス リストを削除するには、このコマンドの **no** 形式を使用します。

ipv6 access-list *access-list-name*

no ipv6 access-list *access-list-name*

構文の説明

access-list-name	IPv6 アクセス リスト名。 名前は、スペース、疑問符を含むことができず、また、数字で始めることはできません。

コマンド デフォルト

IPv6 アクセス リストは定義されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.0(23)S	IPv6 アドレス コンフィギュレーション モードおよび拡張アクセス リスト機能（IPv6 オプション ヘッダー、およびオプションで上位層プロトコル タイプ情報に基づくトラフィック フィルタリング）のサポートが追加されました。 さらに、次のキーワードと引数がグローバル コンフィギュレーション モードから IPv6 アクセス リスト コンフィギュレーション モードに移動されました。**permit**、**deny**、*source-ipv6-prefix* / *prefix-length*、**any**、*destination-ipv6-prefix* / *prefix-length*、**priority**。 詳細については、「使用上のガイドライン」の項を参照してください。

リリース	変更内容
12.2(13)T	IPv6アドレス コンフィギュレーション モードおよび拡張アクセス リスト機能（IPv6 オプション ヘッダー、およびオプションで上位層プロトコル タイプ情報に基づくトラフィック フィルタリング）のサポートが追加されました。 さらに、次のキーワードと引数がグローバル コンフィギュレーション モードから IPv6 アクセス リスト コンフィギュレーション モードに移動されました。**permit**、**deny**、*source-ipv6-prefix* / *prefix-length*、**any**、*destination-ipv6-prefix* / *prefix-length*、**priority**。 詳細については、「使用上のガイドライン」の項を参照してください。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	重複する remark ステートメントは、IPv6 アクセス コントロール リストでは設定できません。
Cisco IOS XE Release 2.1	このコマンドは、Cisco ASR 1000 シリーズ デバイスで追加されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

IPv6 固有である点を除くと、**ipv6 access-list** コマンドは **ip access-list** コマンドと類似しています。

Cisco IOS Release 12.2(2)T 以降のリリース、12.0(21)ST、および 12.0(22)S では、標準の IPv6 アクセス コントロール リスト（ACL）機能が基本的なトラフィック フィルタリング機能に使用されます。トラフィック フィルタリングは、送信元アドレスと宛先アドレス、特定のインターフェイスへのインバウンドおよびアウトバウンド、各アクセス リストの末尾にある暗黙的な deny ステートメントに基づきます（IPv4 の標準の ACL に似た機能）。 IPv6 ACL を定義し、拒否条件と許可条件を設定するには、グローバル コンフィギュレーション モードで **deny** キーワードと **permit** キーワードを指定して **ipv6 access-list** コマンドを使用します。

Cisco IOS Release 12.0(23)S 以降のリリースでは、標準の IPv6 ACL 機能が拡張されています。送信元および宛先アドレスに基づくトラフィック フィルタリングに加えて、IPv6オプションヘッダー、およびオプションでより細かい制御を行うための上位層プロトコルタイプ情報に基づくトラフィック フィルタリングがサポートされています（IPv4 の拡張 ACL に似た機能）。 IPv6 ACL は **ipv6 access-list** コマンドをグローバル コンフィギュレーション モードで使用することにより定義され、その許可と拒否の条件は **deny** および **permit** コマンドを IPv6 アクセス リスト コンフィギュレーション モードで使用することにより設定されます。 **ipv6 access-list** コマンドを設定すると、デバイスが IPv6 アクセス リスト コンフィギュレーション モードに設定され、プロンプト device は

Device(config-ipv6-acl)# に変わります。 IPv6 アクセス リスト コンフィギュレーション モードから、定義済みの IPv6 ACL に許可および拒否の条件を設定できます。

（注） IPv6 ACL は一意な名前によって定義されます（IPv6 は番号付けされた ACL をサポートしません）。 IPv4 ACL と IPv6 ACL は同じ名前を共有できません。

Cisco IOS Release 12.0(23)S 以降のリリースおよび 12.2(11)S 以降のリリースでは、下位互換性のために、グローバル コンフィギュレーション モードでの **deny** キーワードと **permit** キーワードを指定した **ipv6 access-list** コマンドが引き続きサポートされています。ただし、グローバル コンフィギュレーション モードで拒否条件と許可条件を使用して定義された IPv6 ACL は、IPv6 アクセス リスト コンフィギュレーション モードに変換されます。

IPv6 オプション ヘッダーおよび任意の上位層プロトコル タイプ情報に基づいて IPv6 トラフィックをフィルタリングする方法の詳細については、deny（IPv6）コマンドおよびpermit（IPv6）コマンドを参照してください。 変換された IPv6 ACL の設定例については、「例」の項を参照してください。

（注） Cisco IOS Release 12.0(23)S 以降のリリースでは、IPv6 ACL に最後の一致条件として暗黙の **permit icmp any any nd-na**、**permit icmp any any nd-ns**、および**deny ipv6 any any** ステートメントがあります。（前の 2 つの一致条件により ICMPv6 ネイバー探索が可能になります）。IPv6 ACL には、暗黙の **deny ipv6 any any** ステートメントを有効にするために少なくとも 1 つのエントリが含まれる必要があります。 IPv6 ネイバー探索プロセスでは、IPv6 ネットワーク層サービスを利用するため、デフォルトで、インターフェイス上での IPv6 ネイバー探索パケットの送受信が IPv6 ACL によって暗黙的に許可されます。 IPv4 の場合、IPv6 ネイバー探索プロセスに相当するアドレス解決プロトコル（ARP）では、個別のデータ リンク層プロトコルを利用するため、デフォルトで、インターフェイス上での ARP パケットの送受信が IPv4 ACL によって暗黙的に許可されます。

（注） アクセス リストでなく、IPv6 プレフィックス リストは、ルーティング プロトコル プレフィックスのフィルタリングに使用する必要があります。

IPv6 ACL を IPv6 インターフェイスに適用するには、*access-list-name* 引数を指定して **ipv6 traffic-filter** インターフェイス コンフィギュレーション コマンドを使用します。 デバイスとの間で入力および出力 IPv6 仮想端末接続に IPv6 ACL を適用するには、*access-list-name* 引数を指定して **ipv6 access-class** ライン コンフィギュレーション コマンドを使用します。

（注） **ipv6 traffic-filter** コマンドでインターフェイスに適用された IPv6 ACL は、デバイスから発信されるトラフィックではなく、転送されるトラフィックをフィルタリングします。

（注） このコマンドを使用してブートストラップ ルータ（BSR）候補ランデブー ポイント（RP）（**ipv6 pim bsr candidate rp** コマンドを参照）、またはスタティック RP（**ipv6 pim rp-address** コマンドを参照）にすでに関連付けられている ACL を変更する場合、PIM SSM グループ アドレス範囲（FF3x::/96）に重複する追加されたアドレス範囲は無視されます。警告メッセージが生成され、重複するアドレス範囲は ACL に追加されますが、設定された BSR 候補 RP またはスタティック RP コマンドの動作には影響を与えません。

Cisco IOS Release 12.2(33)SXH およびそれに続く Cisco IOS SX リリースでは、重複した remark ステートメントは、IPv6 アクセス コントロール リストでは設定できません。 各 remark ステートメントは別のエンティティであるため、それぞれが一意である必要があります。

例

次に、Cisco IOS Release 12.0(23)S 以降のリリースを実行するデバイスからの例を示します。 この例では、list1 という IPv6 ACL リストを設定し、デバイスを IPv6 アクセス リスト コンフィギュレーション モードにします。

```
Device(config)# ipv6 access-list list1
Device(config-ipv6-acl)#
```

次に、Cisco IOS Release 12.2(2)T 以降のリリース、12.0(21)ST、または 12.0(22)S を実行するデバイスからの例を示します。 この例では、list2 という名前の IPv6 ACL を設定し、その ACL をイーサネット インターフェイス 0 上の発信トラフィックに適用します。 特に、最初の ACL エントリは、ネットワーク FEC0:0:0:2::/64（送信元 IPv6 アドレスの最初の 64 ビットとしてサイトローカル プレフィックス FEC0:0:0:2 を持つパケット）がイーサネット インターフェイス 0 から出て行くことを拒否します。 2 番めの ACL エントリは、その他のすべてのトラフィックがイーサネット インターフェイス 0 から出て行くことを許可します。 2 番めのエントリは、各 IPv6 ACL の末尾に暗黙的な deny all 条件があるため、必要となります。

```
Device(config)# ipv6 access-list list2 deny FEC0:0:0:2::/64 any
Device(config)# ipv6 access-list list2 permit any any
Device(config)# interface ethernet 0
Device(config-if)# ipv6 traffic-filter list2 out
```

同じ設定が Cisco IOS Release 12.0(23)S 以降のリリースを実行しているデバイスで入力された場合、設定は、IPv6 アクセス リスト コンフィギュレーション モードに、次のように変換されます。

```
ipv6 access-list list2
  deny FEC0:0:0:2::/64 any
  permit ipv6 any any
interface ethernet 0
 ipv6 traffic-filter list2 out
```

（注） IPv6 は、グローバル コンフィギュレーション モードから IPv6 アクセス リスト コンフィギュレーション モードに変換される **permit any any** 文および **deny any any** 文でプロトコル タイプとして自動的に設定されます。

（注） Cisco IOS Release 12.2(2)T 以降のリリース、12.0(21)ST または 12.0(22)S を実行するデバイスで定義され、暗黙の拒否条件に依存するか、トラフィックをフィルタリングする **deny any any** ステートメントを指定する IPv6 ACL には、プロトコル パケット（ネイバー探索プロトコルに関連付けられたパケットなど）のフィルタリングを避けるため、リンクローカル アドレスおよびマルチキャスト アドレスに対する **permit** ステートメントを含める必要があります。 また、**deny** ステートメントを使用してトラフィックをフィルタリングする IPv6 ACL では、**permit any any** ステートメントをリストの最後のステートメントとして使用する必要があります。

（注） IPv6 デバイスは、送信元または宛先アドレスのいずれかとしてリンクローカル アドレスを持つIPv6パケットを別のネットワークに転送しません（パケットの送信元インターフェイスは、パケットの宛先インターフェイスとは異なります）。

関連コマンド

コマンド	説明
deny（IPv6）	IPv6アクセス リストに拒否条件を設定します。
ipv6 access-class	IPv6 アクセス リストに基づいて、デバイスとの間で着信接続および発信接続をフィルタリングします。
ipv6 pim bsr candidate rp	BSR に PIM RP アドバタイズメントを送信するように候補 RP を設定します。
ipv6 pim rp-address	特定のグループ範囲の PIM RP のアドレスを設定します。
ipv6 traffic-filter	インターフェイス上の着信または発信 IPv6 トラフィックをフィルタリングします。
permit（IPv6）	IPv6アクセス リストに許可条件を設定します。
show ipv6 access-list	現在のすべての IPv6 アクセス リストの内容を表示します。

ipv6 address

IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ipv6 address** コマンドを使用します。 インターフェイスからアドレスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 address {*ipv6-prefix/prefix-length*| *prefix-name sub-bits/prefix-length*}

no ipv6 address {*ipv6-address/prefix-length*| *prefix-name sub-bits/prefix-length*}

構文の説明

ipv6-address	使用する IPv6 アドレス。
/ *prefix-length*	IPv6 プレフィックスの長さ。 プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す10進値です。10 進数値の前にスラッシュ記号が必要です。
prefix-name	インターフェイスに設定するネットワークの上位ビットを指定する一般的なプレフィックス。
sub-bits	*prefix-name* 引数で指定された一般的なプレフィックスによって提供されるプレフィックスと連結されるアドレスのサブプレフィックス ビットおよびホスト ビット。 *sub-bits* 引数は、RFC 2373 に記載された形式で指定する必要があります。この形式では、アドレスは、16 進数値を 16 ビット単位でコロンで区切って指定します。

コマンド デフォルト

IPv6 アドレスはインターフェイスに定義されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。

リリース	変更内容
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco ASR 1000 シリーズ デバイスに統合されました。
15.2(4)S	このコマンドが Cisco IOS Release 15.2(4)S に統合されました。
15.2(2)SNG	このコマンドが、Cisco ASR 901 シリーズのアグリゲーション サービス デバイスに実装されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ipv6 address コマンドは、さまざまなオプションを使用し、さまざまな方法で、複数の IPv6 アドレスをインターフェイスで設定できます。 最も一般的な方法は、IPv6 アドレスとプレフィックスの長さを指定する方法です。

アドレスは、サブプレフィックスおよびホスト ビットから集約された IPv6 プレフィックス ビットを区切る一般的なプレフィックスのメカニズムを使用して定義することもできます。 この場合、アドレスの上位ビットは、グローバルに設定または学習される一般的なプレフィックスで定義されます（Dynamic Host Configuration Protocol プレフィックス委任（DHCP-PD）を使用し、*prefix-name* 引数を使用して適用するなど）。 サブプレフィックス ビットおよびホスト ビットは *sub-bits* 引数を使用して定義されます。

引数を指定せずに **no ipv6 address autoconfig** コマンドを使用すると、インターフェイスからすべての IPv6 アドレスが削除されます。

インターフェイスで **ipv6 address link-local** コマンドを使用して、IPv6 リンクローカル アドレスを設定し、IPv6 処理をイネーブルにする必要があります。

例

次に、インターフェイスで IPv6 処理をイネーブルにし、一般的なプレフィックス my-prefix と直接指定したビットに基づいてアドレスを設定する例を示します。

```
Device(config-if) ipv6 address my-prefix 0:0:0:7272::72/64
```

my-prefix という名前の一般的なプレフィックスの値が 2001:DB8:2222::/48 であるとすると、グローバル アドレス 2001:DB8:2222:7272::72/64 でインターフェイスを設定する必要があります。

関連コマンド

コマンド	説明
ipv6 address anycast	IPv6 エニーキャスト アドレスを設定し、インターフェイスで IPv6 処理をイネーブルにします。
ipv6 address eui-64	IPv6アドレスを設定して、そのアドレスの下位64 ビットの EUI-64 インターフェイス ID を使用して、インターフェイスでの IPv6 処理をイネーブルにします。
ipv6 address link-local	インターフェイスの IPv6 リンクローカル アドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにします。
ipv6 unnumbered	インターフェイスに明示的な IPv6 アドレスを割り当てなくても、インターフェイスで IPv6 処理をイネーブルにします。
no ipv6 address autoconfig	インターフェイスからすべての IPv6 アドレスを削除します。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 address anycast

IPv6エニーキャストアドレスを設定し、インターフェイスでIPv6処理をイネーブルにするには、インターフェイス コンフィギュレーション モードで**ipv6 address anycast**コマンドを使用します。インターフェイスからアドレスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 address *ipv6-prefix/prefix-length* **anycast**

no ipv6 address [*ip6-prefix/prefix-length* **anycast**]

構文の説明

ipv6-prefix	インターフェイスに割り当てられた IPv6 ネットワーク。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの16ビット値を使用して、アドレスを 16 進数で指定します。
/ prefix-length	IPv6 プレフィックスの長さ。 プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す10進値です。10 進数値の前にスラッシュ記号が必要です。

コマンド デフォルト

IPv6 アドレスはインターフェイスに定義されません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.3(4)T	このコマンドが導入されました。
12.2(25)S	このコマンドが、Cisco IOS Release 12.2(25)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。

リリース	変更内容
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

引数を指定せずに **no ipv6 address** コマンドを使用すると、手動で設定したすべての IPv6 アドレスがインターフェイスから削除されます。

例

次に、インターフェイスで IPv6 処理をイネーブルにし、プレフィックス 2001:0DB8:1:1::/64 をインターフェイスに割り当て、IPv6 エニーキャスト アドレス 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE を設定する例を示します。

```
ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64 anycast
```

関連コマンド

コマンド	説明
ipv6 address eui-64	IPv6アドレスを設定して、そのアドレスの下位64 ビットの EUI-64 インターフェイス ID を使用して、インターフェイスでの IPv6 処理をイネーブルにします。
ipv6 address link-local	インターフェイスの IPv6 リンクローカル アドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにします。
ipv6 unnumbered	インターフェイスに明示的な IPv6 アドレスを割り当てなくても、インターフェイスで IPv6 処理をイネーブルにします。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 address autoconfig

インターフェイスでステートレス自動設定を使用する IPv6 アドレスの自動設定をイネーブルにし、インターフェイスでIPv6処理をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ipv6 address autoconfig** コマンドを使用します。 インターフェイスからアドレスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 address autoconfig [default]

no ipv6 address autoconfig

構文の説明

default	（任意）デフォルトのデバイスがこのインターフェイスで選択されている場合、**default** キーワードによって、デフォルト ルートがそのデフォルトデバイスを使用してインストールされます。 **default** キーワードは、1 個のインターフェイスでのみ指定できます。

コマンド デフォルト

IPv6 アドレスはインターフェイスに定義されません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(13)T	このコマンドが導入されました。
12.2(33)SRE	このコマンドが、Cisco IOS Release 12.2(33)SRE に統合されました。
Cisco IOS XE Release 2.5	このコマンドが、Cisco IOS XE Release 2.5 に統合されました。
12.2(33)XNE	このコマンドが、Cisco IOS Release 12.2(33)XNE に統合されました。
15.1(2)SNG	このコマンドが、Cisco ASR 901 シリーズのアグリゲーション サービス デバイスに実装されました。
15.3(1)S	このコマンドが Cisco IOS Release 15.3(1)S に統合されました。

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ipv6 address autoconfig コマンドによって、デバイスは IPv6 ステートレス アドレス自動設定を実行し、リンクのプレフィックスを検出してインターフェイス EUI-64 ベースのアドレスを追加します。アドレスは、ルータ アドバタイズメント（RA）メッセージで受信したプレフィックスによって設定されます。

引数を指定せずに **no ipv6 address autoconfig** コマンドを使用すると、インターフェイスからすべての IPv6 アドレスが削除されます。

例

次に、IPv6 アドレスを自動的に割り当てる例を示します。

```
Device(config)# interface ethernet 0
Device(config-if)# ipv6 address autoconfig
```

関連コマンド

コマンド	説明
ipv6 address eui-64	IPv6アドレスを設定して、そのアドレスの下位64 ビットの EUI-64 インターフェイス ID を使用して、インターフェイスでの IPv6 処理をイネーブルにします。
ipv6 address link-local	インターフェイスの IPv6 リンクローカル アドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにします。
ipv6 unnumbered	インターフェイスに明示的な IPv6 アドレスを割り当てなくても、インターフェイスで IPv6 処理をイネーブルにします。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 address dhcp

Dynamic Host Configuration Protocol for IPv6（DHCPv6）サーバからインターフェイスの IPv6 アドレスを取得するには、インターフェイス コンフィギュレーション モードで **ipv6 address dhcp** コマンドを使用します。 インターフェイスからアドレスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 address dhcp [rapid-commit]

no ipv6 address dhcp

構文の説明

rapid-commit	（任意）アドレス割り当て用に 2 メッセージ交換方式を許可します。

コマンド デフォルト

IPv6 アドレスは、DHCPv6 サーバから取得されません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.4(24)T	このコマンドが導入されました。
12.2(33)SRE	このコマンドが、Cisco IOS Release 12.2(33)SRE に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ipv6 address dhcp インターフェイス コンフィギュレーション コマンドを使用すると、インターフェイスは DHCP を使用して IPv6 アドレスを動的に学習できます。

rapid-commit キーワードは、アドレス割り当ておよびその他の設定について、2 つのメッセージ交換を使用できるようにします。 これをイネーブルにすると、クライアントは送信請求メッセージに rapid-commit オプションを含めます。

例

次に、IPv6 アドレスを取得して、rapid-commit オプションをイネーブルにする例を示します。

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ipv6 address dhcp
rapid-commit
```

特権 EXEC モードで **show ipv6 dhcp interface** コマンドを使用すると、設定を確認できます。

関連コマンド

コマンド	説明
show ipv6 dhcp interface	DHCPv6 インターフェイスの情報を表示します。

ipv6 address eui-64

インターフェイスに IPv6 アドレスを設定し、アドレスの下位 64 ビットで EUI-64 インターフェイス ID を使用してインターフェイスでの IPv6 処理をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ipv6 address eui-64** コマンドを使用します。 インターフェイスからアドレスを削除するには、このコマンドの **no** 形式を使用します。

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

no ipv6 address [*ip v6-prefix/prefix-length* **eui-64**]

構文の説明

ipv6-prefix	インターフェイスに割り当てられた IPv6 ネットワーク。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
/ prefix-length	IPv6 プレフィックスの長さ。 プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す10進値です。10 進数値の前にスラッシュ記号が必要です。

コマンド デフォルト

IPv6 アドレスはインターフェイスに定義されません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。

リリース	変更内容
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドは、Cisco ASR 1000 シリーズ ルータで追加されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

/ *prefix-length* 引数に指定される値が、64 ビットを超える場合、プレフィックス ビットは、インターフェイス ID より優先されます。

引数を指定せずに no ipv6 address コマンドを使用すると、手動で設定したすべての IPv6 アドレスがインターフェイスから削除されます。

Cisco IOS ソフトウェアが、その IPv6 アドレスのいずれかを使用する別のホストを検出すると、コンソールにエラー メッセージを表示します。

例

次に、IPv6 アドレス 2001:0DB8:0:1::/64 をイーサネット インターフェイス 0 に割り当て、アドレスの下位 64 ビットの EUI-64 インターフェイス ID を指定する例を示します。

```
Router(config)# interface ethernet 0
Router(config-if)# ipv6 address 2001:0DB8:0:1::/64 eui-64
```

関連コマンド

コマンド	説明
ipv6 address link-local	インターフェイスの IPv6 リンクローカル アドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにします。
ipv6 unnumbered	インターフェイスに明示的な IPv6 アドレスを割り当てなくても、インターフェイスで IPv6 処理をイネーブルにします。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 address link-local

インターフェイスの IPv6 リンクローカル アドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ipv6 address link-local** コマンドを使用します。インターフェイスからアドレスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 address *ipv6-address/prefix-length* **link-local [cga]**

no ipv6 address [*ipv6-address/prefix-length* **link-local**]

構文の説明

ipv6-address	インターフェイスに割り当てられた IPv6 アドレス。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
/ *prefix-length*	IPv6 プレフィックスの長さ。 プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。
link-local	リンクローカル アドレスを指定します。 このコマンドに指定された *ipv6-address* は、インターフェイス用に自動的に生成されるリンクローカル アドレスを上書きします。
cga	（任意）CGA インターフェイス ID を指定します。

コマンド デフォルト

IPv6 アドレスはインターフェイスに定義されません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。

リリース	変更内容
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドは、Cisco ASR 1000 シリーズ ルータで追加されました。
12.4(24)T	**cga** キーワードが追加されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

引数を指定せずに **no ipv6 address** コマンドを使用すると、手動で設定したすべての IPv6 アドレスがインターフェイスから削除されます。

Cisco ソフトウェアが、その IPv6 アドレスのいずれかを使用する別のホストを検出すると、コンソールにエラー メッセージを表示します。

IPv6 処理がインターフェイスでイネーブルにされていて、通常、IPv6 アドレスがインターフェイスで設定されている場合、インターフェイスのリンクローカル アドレスが自動的に生成されます。インターフェイスで使用されるリンクローカルアドレスを手動で指定するには、ipv6 address link-local コマンドを使用します。

連続する 16 ビット値がゼロとして指定されている場合は、2 つのコロンを *ipv6-address* 引数の一部として使用できます。インターフェイスごとに複数のIPv6アドレスを設定できますが、設定できるリンクローカル アドレスは 1 つだけです。

例

次に、イーサネットインターフェイス0のリンクローカルアドレスとしてFE80::260:3EFF:FE11:6770を割り当てる例を示します。

```
interface ethernet 0
 ipv6 address FE80::260:3EFF:FE11:6770 link-local
```

関連コマンド

コマンド	説明
ipv6 address eui-64	IPv6アドレスを設定して、そのアドレスの下位64ビットのEUI-64インターフェイスIDを使用して、インターフェイスでのIPv6処理をイネーブルにします。
ipv6 unnumbered	インターフェイスに明示的なIPv6アドレスを割り当てなくても、インターフェイスでIPv6処理をイネーブルにします。
show ipv6 interface	IPv6向けに設定されたインターフェイスの使用状況を表示します。

ipv6 cef

Cisco Express Forwarding for IPv6 をイネーブルにするには、グローバル コンフィギュレーション モードで **ipv6 cef** コマンドを使用します。 Cisco Express Forwarding for IPv6 をディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 cef

no ipv6 cef

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

Cisco Express Forwarding for IPv6 はデフォルトでディセーブルです。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.0(22)S	このコマンドが導入されました。
12.2(13)T	このコマンドが、Cisco IOS Release 12.2(13)T に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco ASR 1000 シリーズのアグリゲーション サービス ルータに実装されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ipv6 cef コマンドは **ip cef** コマンドと類似していますが、これは IPv6 専用です。

ipv6 cef コマンドは、Cisco 12000 シリーズ インターネット ルータでは使用できません。この分散プラットフォームは、分散型 Cisco Express Forwarding for IPv6 モードでだけ動作するためです。

（注） **ipv6 cef** コマンドはインターフェイス コンフィギュレーション モードでサポートされません。

（注） Cisco 7500 シリーズ ルータなど一部の分散型アーキテクチャ プラットフォームは、Cisco Express Forwarding for IPv6 と分散型 Cisco Express Forwarding for IPv6 の両方をサポートします。 Cisco Express Forwarding for IPv6 が分散プラットフォームで設定されている場合、シスコ エクスプレス フォワーディング スイッチングはルート プロセッサ（RP）によって実行されます。

（注） **ipv6 cef** グローバル コンフィギュレーション コマンドを使用して Cisco Express Forwarding for IPv6 をイネーブルにする前に、**ip cef** グローバル コンフィギュレーション コマンドを使用して、Cisco Express Forwarding for IPv4 をイネーブルにする必要があります。

Cisco Express Forwarding for IPv6 は高度なレイヤ 3 IP スイッチング テクノロジーで、Cisco Express Forwarding for IPv4 と同じように機能し、同じ利点があります。 Cisco Express Forwarding for IPv6 は Web ベースのアプリケーションおよび対話型セッションに関連付けられているような、動的でトポロジ的に分散したトラフィック パターンを持つネットワークのパフォーマンスおよびスケーラビリティを最適化します。

例

次に、標準の Cisco Express Forwarding for IPv4 の動作と標準の Cisco Express Forwarding for IPv6 の動作をルータでグローバルにイネーブルにする例を示します。

```
ip cef
ipv6 cef
```

関連コマンド

コマンド	説明
ip route-cache	IP ルーティングの高速スイッチング キャッシュの使用を制御します。
ipv6 cef accounting	Cisco Express Forwarding for IPv6 および分散型 Cisco Express Forwarding for IPv6 のネットワーク アカウンティングをイネーブルにします。
ipv6 cef distributed	IPv6 での分散型シスコ エクスプレス フォワーディングをイネーブルにします。

コマンド	説明
show cef	ラインカードがドロップしたパケットまたは高速転送されなかったパケットを表示します。
show ipv6 cef	IPv6 FIB のエントリを表示します。

ipv6 cef accounting

ネットワーク アカウンティング用に Cisco Express Forwarding for IPv6 および分散型 Cisco Express Forwarding for IPv6 をイネーブルにするには、グローバル コンフィギュレーション モードまたはインターフェイス コンフィギュレーション モードで **ipv6 cef accounting** コマンドを使用します。Cisco Express Forwarding for IPv6 のネットワーク アカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 cef accounting *accounting-types*

no ipv6 cef accounting *accounting-types*

Specific Cisco Express Forwarding Accounting Information Through Interface Configuration Mode

ipv6 cef accounting non-recursive {**external| internal**}

no ipv6 cef accounting non-recursive {**external| internal**}

構文の説明

accounting-types	*accounting-types* 引数は、次のキーワードのうち少なくとも 1 つで置き換える必要があります。任意で、他のキーワードの一部またはすべてをこのキーワードの後に入力できますが、各キーワードを使用できるのはそれぞれ一度だけです。 • **load-balance-hash**：ロード バランシング ハッシュ バケット カウンタをイネーブルにします。 • **non-recursive**：非再帰的プレフィックスによるアカウンティングをイネーブルにします。 • **per-prefix**：宛先（またはプレフィックス）へのパケット数とバイト数のコレクションの高速転送をイネーブルにします。 • **prefix-length**：プレフィックス長によるアカウンティングをイネーブルにします。
non-recursive	非再帰的プレフィックスによるアカウンティングをイネーブルにします。 このキーワードは、別のキーワードを入力した後、グローバル コンフィギュレーション モードで使用する場合、省略可能です。*accounting-types* 引数を参照してください。

external	非再帰的外部ビンの入力トラフィックをカウントします。
internal	非再帰的内部ビンの入力トラフィックをカウントします。

コマンド デフォルト

Cisco Express Forwarding for IPv6 のネットワーク アカウンティングは、デフォルトでディセーブルです。

コマンド モード

グローバル コンフィギュレーション（config）インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.0(22)S	このコマンドが導入されました。
12.2(13)T	このコマンドが、Cisco IOS Release 12.2(13)T に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(25)S	**non-recursive** および **load-balance-hash** キーワードが追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドは、Cisco ASR 1000 シリーズ ルータで追加されました。
12.4(20)T	このコマンドが、Cisco IOS Release 12.4(20)T に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ipv6 cef accounting コマンドは、**ip cef accounting** コマンドに似ていますが、IPv6 固有です。

Cisco Express Forwarding for IPv6 のネットワーク アカウンティングを設定すると、ネットワークで Cisco Express Forwarding for IPv6 トラフィック パターンの統計情報を収集することができます。

グローバル コンフィギュレーション モードで **ipv6 cef accounting** コマンドを使用して、Cisco Express Forwarding for IPv6 のネットワーク アカウンティングをイネーブルにする場合、アカウンティング情報は、Cisco Express Forwarding for IPv6 モードがイネーブルの場合はルート プロセッサ（RP）で、分散型 Cisco Express Forwarding for IPv6 モードがイネーブルの場合はラインカードで収集されます。 **show ipv6 cef** EXEC コマンドを使用して、収集したアカウンティング情報を表示できます。

直接接続されるネクスト ホップのプレフィックスの場合、**non-recursive** キーワードを使用すると、プレフィックスを通じてパケットとバイトのコレクションを高速転送できます。 このキーワードは、**ipv6 cef accounting** コマンドの他のキーワードを入力した後にグローバル コンフィギュレーション モードで使用する場合、省略可能です。

インターフェイス コンフィギュレーション モードでは、このコマンドはグローバル コンフィギュレーション コマンドと組み合わせて使用する必要があります。 インターフェイス コンフィギュレーション コマンドでは、統計情報の蓄積に 2 つの異なるビン（内部または外部）を指定することができます。 内部ビンがデフォルトで使用されます。 統計情報は、**show ipv6 cef detail** コマンドを使用して表示します。

宛先単位のロードバランシングでは、使用可能なパスのセットが分配される一連の 16 のハッシュ バケットが使用されます。 パケットのプロパティで動作するハッシュ関数が、使用するパスを含むバケットを選ぶために適用されます。 送信元と宛先の IP アドレスは、宛先単位のロード バランシングでバケットの選択に使用されるプロパティです。ハッシュ バケット単位のカウンタをイネーブルにするには、**ipv6 cef accounting** コマンドで **load-balance-hash** キーワードを使用します。ハッシュ バケット単位のカウンタを表示するには、**show ipv6 cef** *prefix* **internal** コマンドを入力します。

例

次に、直接接続されたネクスト ホップを持つプレフィックスの Cisco Express Forwarding for IPv6 アカウンティング情報の収集をイネーブルにする例を示します。

```
Router(config)# ipv6 cef accounting non-recursive
```

関連コマンド

コマンド	説明
ip cef accounting	シスコ エクスプレス フォワーディングのネットワーク アカウンティングをイネーブルにします（IPv4）。
show cef	**シスコ エクスプレス フォワーディングにより転送**されるパケットの情報を表示します。
show ipv6 cef	IPv6 FIB のエントリを表示します。

ipv6 cef distributed

分散型 Cisco Express Forwarding for IPv6 をイネーブルにするには、グローバル コンフィギュレーション モードで **ipv6 cef distributed** コマンドを使用します。 Cisco Express Forwarding for IPv6 をディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 cef distributed

no ipv6 cef distributed

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

分散型 Cisco Express Forwarding for IPv6 は、Cisco 7500 シリーズ ルータではディセーブルで、Cisco 12000 シリーズ インターネット ルータではイネーブルです。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.0(22)S	このコマンドが導入されました。
12.2(13)T	このコマンドが、Cisco IOS Release 12.2(13)T に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco ASR 1000 シリーズのアグリゲーション サービス ルータに実装されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ipv6 cef distributed コマンドは、**ip cef distributed** コマンドに似ていますが、IPv6 固有です。

グローバル コンフィギュレーション モードで **ipv6 cef distributed** を使用することにより、ルータで分散型 Cisco Express Forwarding for IPv6 をグローバルにイネーブルにすると、ルート プロセッサ（RP）から分散型アーキテクチャ プラットフォームのラインカードに IPv6 パケットのシスコ エクスプレス フォワーディング処理が分配されます。

（注） **ipv6 cef distributed** コマンドは Cisco 12000 シリーズ インターネット ルータ上ではサポートされません。このプラットフォームでは、分散型 Cisco Express Forwarding for IPv6 がデフォルトでイネーブルにされているためです。

（注） ルータの分散型 Cisco Express Forwarding for IPv6 トラフィックを転送するには、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用してルータで IPv6 ユニキャスト データグラムの転送をグローバルに設定し、**ipv6 address** インターフェイス コンフィギュレーション コマンドでインターフェイスに IPv6 アドレスおよび IPv6 処理を設定します。

（注） **ipv6 cef distributed** グローバル コンフィギュレーション コマンドを使用して分散型 Cisco Express Forwarding for IPv6 をイネーブルにする前に、**ip cef distributed** グローバル コンフィギュレーション コマンドを使用して、分散型 Cisco Express Forwarding for IPv4 をイネーブルにする必要があります。

シスコ エクスプレス フォワーディングは、高度なレイヤ 3 IP スイッチング テクノロジーです。シスコ エクスプレス フォワーディングは Web ベースのアプリケーションおよび対話型セッションに関連付けられているような、動的でトポロジ的に分散したトラフィック パターンを持つネットワークのパフォーマンスおよびスケーラビリティを最適化します。

例

次に、分散型 Cisco Express Forwarding for IPv6 の操作をイネーブルにする例を示します。

```
ipv6 cef distributed
```

関連コマンド

コマンド	説明
ip route-cache	IP ルーティングの高速スイッチング キャッシュの使用を制御します。
show ipv6 cef	IPv6 FIB のエントリを表示します。