ipv6-i4

- router-preference maximum, 66 ページ

ipv6 snooping attach-policy

ターゲットに IPv6 スヌーピング ポリシーを適用するには、IPv6 スヌーピング コンフィギュレーション モードで **ipv6 snooping attach-policy** コマンドを使用します。 ターゲットからポリシーを削除するには、このコマンドの **no** 形式を使用します。

ipv6 snooping policy attach-policy *snooping-policy*

構文の説明

snooping-policy	スヌーピング ポリシーのユーザ定義名。 ポリシー名には象徴的な文字列（Engineering など）または整数（0 など）を使用できます。

コマンド デフォルト

IPv6 スヌーピング ポリシーは、ターゲットに適用されていません。

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（config-ipv6-snooping）

コマンド履歴

リリース	変更内容
15.0(2)SE	このコマンドが導入されました。
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。
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

ポリシーを識別または設定した後、**ipv6 snooping attach-policy** コマンドを使用してターゲットに適用します。 このコマンドは、プラットフォームに応じて、任意のターゲットに適用されます。ターゲットの例（使用するプラットフォームによる）として、デバイス ポート、スイッチポート、レイヤ 2 インターフェイス、レイヤ 3 インターフェイス、VLAN があります。

例

次に、policy1 という名前の IPv6 スヌーピング ポリシーをターゲットに適用する例を示します。

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# ipv6 snooping attach-policy policy1
```

関連コマンド

コマンド	説明
ipv6 snooping policy	IPv6 スヌーピング ポリシーを設定し、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。

ipv6 snooping policy

IPv6 スヌーピング ポリシーを設定し、IPv6 スヌーピング コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **ipv6 snooping policy** コマンドを使用します。 IPv6 スヌーピング ポリシーを削除するには、このコマンドの **no** 形式を使用します。

ipv6 snooping policy *snooping-policy*

no ipv6 snooping policy *snooping-policy*

構文の説明

snooping-policy	スヌーピング ポリシーのユーザ定義名。 ポリシー名には象徴的な文字列（Engineering など）または整数（0 など）を使用できます。

コマンド デフォルト

IPv6 スヌーピング ポリシーは設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
15.0(2)SE	このコマンドが導入されました。
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。
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 snooping policy コマンドを使用して、IPv6 スヌーピング ポリシーを作成できます。 **ipv6 snooping policy** コマンドをイネーブルにすると、コンフィギュレーション モードが IPv6 スヌーピング コンフィギュレーション モードに変わります。 このモードでは、管理者が次の IPv6 第 1 ホップ セキュリティ コマンドを設定できます。

- **data-glean/destination-glean** コマンドは、データまたは宛先アドレス グリーニングを使用した 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します。
- **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。

- **limit address-count** *maximum* コマンドは、ポートで使用できる IPv6 アドレスの数を制限します。
- **security-level** は、適用されるセキュリティのレベルを指定します。
- **tracking** コマンドは、ポートのデフォルトのトラッキング ポリシーを上書きします。
- **trusted-port** コマンドは、信頼できるポートとしてポートを設定します。つまり、メッセージの受信時に検証が実行されないか、限られた検証だけが実行されます。

ポリシーを識別または設定した後、**ipv6 snooping attach-policy** コマンドを使用してデバイスに適用します。

例

次に、IPv6 スヌーピング ポリシーを設定する例を示します。

```
Device(config)# ipv6 snooping policy policy1
```

関連コマンド

コマンド	説明
ipv6 snooping attach-policy	ターゲットに IPv6 スヌーピングにポリシーを適用します。

ipv6 traffic-filter

インターフェイスで着信または発信 IPv6 トラフィックをフィルタリングするには、インターフェイス コンフィギュレーション モードで **ipv6 traffic-filter** コマンドを使用します。 インターフェイスで IPv6 トラフィックのフィルタリ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 traffic-filter *access-list-name* {**in**| **out**}

no ipv6 traffic-filter *access-list-name*

構文の説明

access-list-name	IPv6 アクセス名を指定します。
in	着信 IPv6 トラフィックを指定します。
out	発信 IPv6 トラフィックを指定します。

コマンド デフォルト

インターフェイス上での IPv6 トラフィックのフィルタリングは設定されません。

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。
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。

リリース	変更内容
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)SXI4	**out** キーワード、すなわち発信トラフィックのフィルタリングは IPv6 ポート ベース アクセス リスト（PACL）設定ではサポートされません。
12.2(54)SG	このコマンドが変更されました。 Cisco IOS Release 12.2(54)SG のサポートが追加されました。
12.2(50)SY	このコマンドが変更されました。 **out** キーワードはサポートされません。
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。

例

次に、cisco という名前のアクセス リストの定義に従って、イーサネット インターフェイス 0/0 でインバウンド IPv6 トラフィックをフィルタリングする例を示します。

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 traffic-filter cisco in
```

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、定義されたアクセス リストに拒否または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。
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 verify unicast source reachable-via

送信元アドレスがFIBテーブルに存在し、ユニキャストリバースパス転送（ユニキャストRPF）がイネーブルであることを確認するには、インターフェイス コンフィギュレーション モードで **ipv6 verify unicast source reachable-via** コマンドを使用します。URPF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 verify unicast source reachable-via {**rx**| **any**} **[allow-default] [allow-self-ping]** [*access-list-name*]

no ipv6 verify unicast

構文の説明

rx	送信元は、パケットを受信したインターフェイスを通じて到達できます。
any	送信元は、どのインターフェイスからでも到達可能です。
allow-default	（任意）ルックアップ テーブルがデフォルトルートを照合し、確認のためにルートを使用できるようにします。
allow-self-ping	（任意）ルータがセカンダリアドレスへのpingを実行できるようにします。
access-list-name	（任意）IPv6アクセス リストの名前。名前にはスペースまたは引用符を含めることはできません。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

ユニキャストRPFはディセーブルです。

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(25)S	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。

リリース	変更内容
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 ルータで導入されました。

使用上のガイドライン

ipv6 verify unicast reverse-path コマンドは、ルーズ チェック モードで IPv6 のユニキャスト RPF をイネーブルにするために使用します。

ipv6 verify unicast source reachable-via コマンドは、IPv6 ルータをパススルーする不正形式または偽造（スプーフィング）IP送信元アドレスによって発生する問題を減少させるために使用します。不正形式または偽造送信元アドレスは、送信元IPv6アドレススプーフィングに基づくサービス拒絶（DoS）攻撃を示すことがあります。

URPF 機能は、ルータ インターフェイスで受信されるパケットが、パケットの送信元への最良リターンパスのいずれかで到達するかどうかを確認します。 これは、CEFテーブルの逆ルックアップを実行することによって行います。 URPF でパケットのリバース パスが見つからない場合、アクセス コントロール リスト（ACL）が **ipv6 verify unicast source reachable-via** コマンドで指定されているかどうかに応じて、URPF はパケットをドロップまたは転送できます。 コマンドで ACL を指定し、パケットがURPFの確認に失敗した場合にのみ、ACLを確認して（ACLでdenyステートメントを使用して）パケットをドロップするか、（ACLでpermitステートメントを使用して）転送するかを参照します。 パケットがドロップされるか転送されるかにかかわらず、パケットは、URPF ドロップのグローバル IP トラフィック統計情報とユニキャスト RPF のインターフェイス統計情報でカウントされます。

ipv6 verify unicast source reachable-via コマンドで ACL を指定しない場合、ルータは偽造または不正な形式のパケットをただちにドロップし、ACLのロギングは発生しません。 ルータおよびインターフェイス ユニキャスト RPF カウンタが更新されます。

URPF イベントをロギングするには、**ipv6 verify unicast source reachable-via** コマンドで使用する ACL エントリのロギング オプションを指定します。 ログ情報を使用して、送信元アドレスや時間など、攻撃に関する情報を収集できます。

例

次に、インターフェイスでユニキャスト RPF をイネーブルにする例を示します。

```
ipv6 verify unicast source reachable-via any
```

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、ルータを 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。

コマンド	説明
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。

managed-config-flag

アドバタイズされた管理対象アドレス設定パラメータを確認するには、RA ガード ポリシー コンフィギュレーション モードで **managed-config-flag** コマンドを使用します。

managed-config-flag {**on**| **off**}

構文の説明

on	検証はイネーブルです。
off	検証はディセーブルです。

コマンド デフォルト

検証はイネーブルになりません。

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

managed-config-flag コマンドによって、アドバタイズされた管理対象アドレス設定パラメータ（「M」フラグ）を検証できます。 このフラグは、信頼できない可能性がある DHCPv6 サーバを通じてホストにアドレスを取得させるために、攻撃者によって設定されることがあります。

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、M フラグの検証をイネーブルにする例を示します。

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# managed-config-flag on
```

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。

match ipv6

フロー レコードのキー フィールドとして IPv6 フィールドの 1 つ以上を設定するには、Flexible NetFlow フロー レコード コンフィギュレーション モードで **match ipv6** コマンドを使用します。フロー レコードのキー フィールドとして IPv6 フィールドの 1 つ以上の使用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。

match ipv6 {**dscp**| **flow-label**| **next-header**| **payload-length**| **precedence**| **protocol**| **traffic-class**| **version**}

no match ipv6 {**dscp**| **flow-label**| **next-header**| **payload-length**| **precedence**| **protocol**| **traffic-class**| **version**}

Cisco Catalyst 6500 Switches in Cisco IOS Release 12.2(50)SY

match ipv6 {**dscp**| **precedence**| **protocol**| **tos**}

no match ipv6 {**dscp**| **precedence**| **protocol**| **tos**}

Cisco IOS XE Release 3.2SE

match ipv6 {**protocol**| **traffic-class**| **version**}

no match ipv6 {**protocol**| **traffic-class**| **version**}

構文の説明

dscp	キー フィールドとして IPv6 DiffServ コード ポイント DSCP（タイプ オブ サービス（ToS）の一部）を設定します。
flow-label	キー フィールドとして IPv6 フロー ラベルを設定します。
next-header	キー フィールドとして IPv6 次ヘッダーを設定します。
payload-length	キー フィールドとして IPv6 ペイロード長を設定します。
Precedence	キー フィールドとして IPv6 precedence（ToS の一部）を設定します。
protocol	キー フィールドとして IPv6 プロトコルを設定します。
tos	キーフィールドとして IPv6 ToS を設定します。
traffic-class	キー フィールドとして IPv6 トラフィック クラスを設定します。

version	キー フィールドとして IPv6 ヘッダーから IPv6 バージョンを設定します。

コマンド デフォルト

IPv6 フィールドはキー フィールドとして設定されません。

コマンド モード

Flexible NetFlow フロー レコード コンフィギュレーション（config-flow-record）

コマンド履歴

リリース	変更内容
12.4(20)T	このコマンドが導入されました。
12.2(33)SRE	このコマンドが変更されました。 このコマンドのサポートが Cisco 7200 および Cisco 7300 ネットワーク処理エンジン（NPE）シリーズ ルータに実装されました。
12.2(50)SY	このコマンドが変更されました。 **flow-label**、**next-header**、**payload-length**、**traffic-class**、および **version** キーワードが削除されました。
15.2(2)T	このコマンドが変更されました。 Cisco Performance Monitor のサポートが追加されました。
Cisco IOS XE Release 3.5S	このコマンドが変更されました。 Cisco Performance Monitor のサポートが追加されました。
Cisco IOS XE Release 3.2SE	このコマンドが変更されました。 **dscp**、**flow-label**、**next-header**、**payload-length**、および **precedence** キーワードが削除されました。

使用上のガイドライン

このコマンドは、Flexible NetFlow と Performance Monitor の両方で使用できます。 これらの製品は、このコマンドを発行するコンフィギュレーション モードを開始するために異なるコマンドを使用しますが、モード プロンプトは両方の製品で同じです。 Performance Monitor では、このコマンドを使用する前に、**flow record type performance-monitor** コマンドを入力します。

モード プロンプトが両方の製品で同じであるため、ここでは両方の製品のコマンド モードをフロー レコード コンフィギュレーション モードと呼びます。 ただし、Flexible NetFlow では、モードは Flexible NetFlow フロー レコード コンフィギュレーション モードとも呼ばれます。Performance Monitor では、モードは Performance Monitor フロー レコード コンフィギュレーション モードとも呼ばれます。

フロー レコードは、フロー モニタで使用する前に、少なくとも 1 つのキー フィールドを必要とします。 キー フィールドは、各フローがキー フィールドの値の一意のセットを持つことで、フローを区別します。 キー フィールドは、**match** コマンドを使用して定義されます。

（注） **match ipv6** コマンドのキーワードの一部は別のコマンドとして説明します。 別に記載されている **match ipv6** コマンドのすべてのキーワードは、**match ipv6** で始まります。 たとえば、フロー レコードのキー フィールドとして IPv6 ホップ制限を設定する方法の詳細については、**match ipv6 hop-limit** コマンドを参照してください。

例

次に、キー フィールドとして IPv6 DSCP フィールドを設定する例を示します。

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 dscp
```

次に、キー フィールドとして IPv6 DSCP フィールドを設定する例を示します。

```
Router(config)# flow record type performance-monitor RECORD-1
Router(config-flow-record)# match ipv6 dscp
```

関連コマンド

コマンド	説明
flow record	フロー レコードを作成し、Flexible NetFlow フロー レコード コンフィギュレーション モードを開始します。
flow record type performance-monitor	フロー レコードを作成し、Performance Monitor フロー レコード コンフィギュレーション モードを開始します。

match ipv6 access-list

承認されたプレフィックスリストからの検査対象メッセージに含まれる送信者のIPv6アドレスを確認するには、RA ガード ポリシー コンフィギュレーション モードで **match ipv6 access-list** コマンドを使用します。

match ipv6 access-list *ipv6-access-list-name*

構文の説明

ipv6-access-list-name	照合される IPv6 アクセス リスト。

コマンド デフォルト

送信者の IPv6 アドレスは確認されません。

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

match ipv6 access-list コマンドは、設定された承認済みルータの送信元アクセス リストからの検査対象メッセージに含まれる送信者の IPv6 アドレスの検証をイネーブルにします。 **match ipv6 access-list** コマンドが設定されていない場合、この承認はバイパスされます。

アクセスリストは **ipv6 access-list** コマンドを使用して設定されます。 たとえば、リンクローカル アドレス FE80::A8BB:CCFF:FE01:F700 のルータだけを承認するには、次の IPv6 アクセス リストを定義します。

```
Router(config)# ipv6 access-list list1
Router(config-ipv6-acl)# permit host FE80::A8BB:CCFF:FE01:F700 any
```

（注） ここでは、アクセス リストを複数の明示的なルータ ソースを定義する便利な方法として使用していますが、ポートベースのアクセス リスト（PACL）ではありません。 **match ipv6 access-list** コマンドは、ルータ メッセージの IPv6 送信元アドレスを検証するため、アクセス リストで宛先を指定することには意味がありません。アクセス コントロール リスト（ACL）のエントリの宛先は常に「Any」にする必要があります。宛先がアクセス リストで指定されている場合、照合が失敗します。

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、list1 という名前のアクセス リストの IPv6 アドレスと照合する例を示します。

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# match ipv6 access-list list1
```

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。
ipv6 access-list	IPv6 アクセス リストを定義し、ルータを 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。

match ipv6 address

プレフィックス リストで許可されたプレフィックスを持つ IPv6 ルートを配布する、または IPv6 のポリシーベース ルーティング（PBR）用にパケットを照合するために使用する IPv6 アクセス リストを指定するには、ルートマップ コンフィギュレーション モードで **match ipv6 address** コマンドを使用します。 **match ipv6 address** エントリを削除するには、このコマンドの **no** 形式を使用します。

match ipv6 address {**prefix-list** *prefix-list-name*| *access-list-name*}

no match ipv6 address

構文の説明

prefix-list *prefix-list-name*	IPv6 プレフィックス リストの名前を指定します。
access-list-name	IPv6 アクセス リスト名。 名前にはスペースまたは引用符を含めることはできません。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

宛先ネットワーク番号またはアクセス リストに基づいて配布されるルートはありません。

コマンド モード

ルートマップ コンフィギュレーション（config-route-map）

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。
12.3(7)T	このコマンドが変更されました。 引数 *access-list-name* 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。

リリース	変更内容
12.2(33)SXI4	このコマンドが変更されました。 **prefix-list** *prefix-list-name* キーワード/引数ペアの引数は、Cisco IOS Release 12.2(33)SXI4 ではサポートされません。
Cisco IOS XE Release 3.2S	このコマンドが Cisco IOS XE Release 3.2SG に統合されました。
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

route-map コマンドと **match** および **set** コマンドを使用して、あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義します。 **route-map** コマンドごとに、それに関連した **match** および **set** コマンドのリストがあります。 **match** コマンドは、一致基準、つまり現在の **route-map** コマンドについて再配布を許可する条件を指定します。 **set** コマンドは、**match** コマンドによって強制される基準が満たされた場合に実行される特定の再配布アクションである設定アクションを指定します。

match ipv6 address コマンドは、アクセス リストまたはプレフィックス リストを指定するために使用できます。 PBR を使用する場合は、*access-list-name* 引数を使用する必要があります。**prefix-list** *prefix-list-name* キーワード/引数ペアの引数は機能しません。

例

次の例では、marketing という名前のプレフィックス リストで指定されたアドレスを持つ IPv6 ルートが一致します。

```
Device(config)# route-map name
Device(config-route-map)# match ipv6 address prefix-list marketing
```

次の例では、marketing という名前のアクセス リストで指定されたアドレスを持つ IPv6 ルートが一致します。

```
Device(config)# route-map
Device(config-route-map)# match ipv6 address marketing
```

関連コマンド

コマンド	説明
match as-path	BGP 自律システム パス アクセス リストを照合します。
match community	BGP コミュニティを照合します。
match ipv6 address	IPv6 の PBR のパケットと照合するために使用する IPv6 アクセス リストを指定します。

コマンド	説明
match ipv6 next-hop	プレフィックス リストによって許可されているネクスト ホップ プレフィックスを持つ IPv6 ルートを配布します。
match ipv6 route-source	プレフィックス リストに指定されているアドレスのルータによってアドバタイズされた IPv6 ルートを配布します。
match length	パケットのレベル3長に基づいてポリシー ルーティングを実行します。
match metric	指定したメトリックを持つルートを再配布します。
match route-type	指定されたタイプのルートを再配布します。
route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義します。
set as-path	BGP ルートの自律システム パスを変更します。
set community	BGP コミュニティ属性を設定します。
set default interface	ポリシー ルーティング用のルート マップの match 句を通過し、宛先への明示的ルートがないパケットを出力するデフォルト インターフェイスを指定します。
set interface	ポリシー ルーティング用のルート マップの match 句を通過したパケットを出力するデフォルト インターフェイスを指定します。
set ipv6 default next-hop	一致パケットが転送されるデフォルトの IPv6 ネクスト ホップを指定します。
set ipv6 next-hop（PBR）	ポリシー ルーティング用のルート マップの match 句を通過した IPv6 パケットの送出先を示します。
set ipv6 precedence	IPv6 パケット ヘッダーのプリファレンス値を設定します。
set level	ルートのインポート先を示します。

コマンド	説明
set local preference	自律システムパスのプリファレンス値を指定します。
set metric	ルーティングプロトコルのメトリック値を設定します。
set metric-type	宛先ルーティング プロトコルのメトリック タイプを設定します。
set tag	宛先ルーティングプロトコルのタグ値を設定します。
set weight	ルーティング プロトコルの BGP 重みを指定します。

match ipv6 destination

フロー レコードのキー フィールドとして IPv6 宛先アドレスを設定するには、Flexible NetFlow フロー レコード コンフィギュレーション モードで **match ipv6 destination** コマンドを使用します。フロー レコードのキー フィールドとしての IPv6 宛先アドレス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。

match ipv6 destination {**address**| {**mask**| **prefix**} [**minimum-mask** *mask*]}

no match ipv6 destination {**address**| {**mask**| **prefix**} [**minimum-mask** *mask*]}

Cisco Catalyst 6500 Switches in Cisco IOS Release 12.2(50)SY

match ipv6 destination address

no match ipv6 destination address

Cisco IOS XE Release 3.2SE

match ipv6 destination address

no match ipv6 destination address

構文の説明

address	キー フィールドとして IPv6 宛先アドレスを設定します。
mask	キー フィールドとして IPv6 宛先アドレスのマスクを設定します。
prefix	キー フィールドとして IPv6 宛先アドレスのプレフィックスを設定します。
minimum-mask *mask*	（任意）最小マスクのサイズをビット単位で指定します。 有効な範囲は、1 ～ 128 です。

コマンド デフォルト

IPv6 宛先アドレスはキー フィールドとして設定されません。

コマンド モード

Flexible NetFlow フロー レコード コンフィギュレーション（config-flow-record）

コマンド履歴

リリース	変更内容
12.4(20)T	このコマンドが導入されました。
12.2(33)SRE	このコマンドが変更されました。 このコマンドのサポートが Cisco 7200 および Cisco 7300 ネットワーク処理エンジン（NPE）シリーズ ルータに実装されました。
12.2(50)SY	このコマンドが変更されました。 **mask**、**prefix**、および **minimum-mask** キーワードが削除されました。
15.2(2)T	このコマンドが変更されました。 Cisco Performance Monitor のサポートが追加されました。
Cisco IOS XE Release 3.5S	このコマンドが変更されました。 Cisco Performance Monitor のサポートが追加されました。
Cisco IOS XE Release 3.2SE	このコマンドが変更されました。 **mask**、**prefix**、および **minimum-mask** キーワードが削除されました。

使用上のガイドライン

このコマンドは、Flexible NetFlow と Performance Monitor の両方で使用できます。 これらの製品は、このコマンドを発行するコンフィギュレーション モードを開始するために異なるコマンドを使用しますが、モード プロンプトは両方の製品で同じです。 Performance Monitor では、このコマンドを使用する前に、**flow record type performance-monitor** コマンドを入力します。

モード プロンプトが両方の製品で同じであるため、ここでは両方の製品のコマンド モードをフロー レコード コンフィギュレーション モードと呼びます。 ただし、Flexible NetFlow では、モードは Flexible NetFlow フロー レコード コンフィギュレーション モードとも呼ばれます。Performance Monitor では、モードは Performance Monitor フロー レコード コンフィギュレーション モードとも呼ばれます。

フロー レコードは、フロー モニタで使用する前に、少なくとも 1 つのキー フィールドを必要とします。 キー フィールドは、各フローがキー フィールドの値の一意のセットを持つことで、フローを区別します。 キー フィールドは、**match** コマンドを使用して定義されます。

例

次に、キー フィールドとして 16 ビット IPv6 宛先アドレス プレフィックスを設定する例を示します。

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 destination prefix minimum-mask 16
```

次に、キー フィールドとして 16 ビット IPv6 宛先アドレス マスクを指定する例を示します。

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 destination mask minimum-mask 16
```

次に、キー フィールドとして 16 ビット IPv6 宛先アドレス マスクを設定する例を示します。

```
Router(config)# flow record type performance-monitor RECORD-1
Router(config-flow-record)# match ipv6 destination mask minimum-mask 16
```

関連コマンド

コマンド	説明
flow record	フロー レコードを作成し、Flexible NetFlow フロー レコード コンフィギュレーション モードを開始します。
flow record type performance-monitor	フロー レコードを作成し、Performance Monitor フロー レコード コンフィギュレーション モードを開始します。

match ipv6 hop-limit

フロー レコードのキー フィールドとしてIPv6ホップ制限を設定するには、FlexibleNetFlowフロー レコード コンフィギュレーション モードで **match ipv6 hop-limit** コマンドを使用します。 フロー レコードのキーフィールドとしてIPv6パケットのセクションの使用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。

match ipv6 hop-limit

no match ipv6 hop-limit

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

ユーザ定義のフロー レコードのキー フィールドとして IPv6 ホップ制限を使用することはデフォルトでイネーブルになっていません。

コマンド モード

Flexible NetFlow フロー レコード コンフィギュレーション（config-flow-record）

コマンド履歴

リリース	変更内容
12.4(20)T	このコマンドが導入されました。
12.2(33)SRE	このコマンドが変更されました。 このコマンドのサポートがCisco 7200 およびCisco 7300 ネットワーク処理エンジン（NPE）シリーズ ルータに実装されました。
15.2(2)T	このコマンドが変更されました。 Cisco Performance Monitor のサポートが追加されました。
Cisco IOS XE Release 3.5S	このコマンドが変更されました。 Cisco Performance Monitor のサポートが追加されました。
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

このコマンドは、Flexible NetFlow と Performance Monitor の両方で使用できます。 これらの製品は、このコマンドを発行するコンフィギュレーション モードを開始するために異なるコマンドを使用しますが、モード プロンプトは両方の製品で同じです。 Performance Monitor では、このコマンドを使用する前に、**flow record type performance-monitor** コマンドを入力します。

モード プロンプトが両方の製品で同じであるため、ここでは両方の製品のコマンド モードをフロー レコード コンフィギュレーション モードと呼びます。 ただし、Flexible NetFlow では、モードはFlexible NetFlowフロー レコードコンフィギュレーションモードとも呼ばれます。Performance Monitor では、モードは Performance Monitor フロー レコード コンフィギュレーション モードとも呼ばれます。

フロー レコードは、フロー モニタで使用する前に、少なくとも 1 つのキー フィールドを必要とします。 キー フィールドは、各フローがキー フィールドの値の一意のセットを持つことで、フローを区別します。 キー フィールドは、**match** コマンドを使用して定義されます。

例

次に、キー フィールドとしてパケットのホップ制限をフローで設定する例を示します。

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 hop-limit
```

次に、キー フィールドとしてパケットのホップ制限をフローで設定する例を示します。

```
Router(config)# flow record type performance-monitor RECORD-1
Router(config-flow-record)# match ipv6 hop-limit
```

関連コマンド

コマンド	説明
flow record	フロー レコードを作成し、Flexible NetFlow フロー レコード コンフィギュレーション モードを開始します。
flow record type performance-monitor	フロー レコードを作成し、Performance Monitor フロー レコード コンフィギュレーション モードを開始します。

match ra prefix-list

承認されたプレフィックス リストからの検査対象メッセージに含まれるアドバタイズされたプレフィックスを確認するには、RA ガード ポリシー コンフィギュレーション モードで **match ra prefix-list** コマンドを使用します。

match ra prefix-list *ipv6-prefix-list-name*

構文の説明

ipv6-prefix-list-name	照合される IPv6 プレフィックスのリスト。

コマンド デフォルト

アドバタイズされたプレフィックスは確認されません。

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

match ra prefix-list コマンドは、設定された承認済みルータのプレフィックス リストからの検査対象メッセージに含まれるアドバタイズされたプレフィックスの検証をイネーブルにします。 IPv6 プレフィックス リストを設定するには **ipv6 prefix-list** コマンドを使用します。 たとえば、プレフィックス 2001:101::/64 を承認し、プレフィックス 2001:100::/64 を拒否するには、次の IPv6 プレフィックス リストを定義します。

```
Router(config)# ipv6 prefix-list listname1 deny 2001:0DB8:101:/64
Router(config)# ipv6 prefix-list listname1 permit 2001:0DB8:100::/64
```

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、listname1 のアドバタイズされたプレフィックスを検証する例を示します。

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# match ra prefix-list listname1
```

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。
ipv6 prefix-list	IPv6 プレフィックス リストのエントリを作成します。

max-through

スロットル期間ごとの VLAN 単位のマルチキャスト ルータ アドバタイズメント（RA）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 **max-through** 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。

max-through {*mt-value*| **inherit**| **no-limit**}

構文の説明

mt-value	スロットリングが発生するまでに VLAN で許可されるマルチキャスト RA 数。 指定できる範囲は 0 ～ 256 です。
inherit	ターゲット ポリシー間の設定をマージします。
no-limit	マルチキャスト RA は VLAN で制限されません。

コマンド デフォルト

10 分あたり VLAN あたり 10 RA

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（config-nd-ra-throttle）

コマンド履歴

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

使用上のガイドライン

max-through コマンドで、スロットル期間ごとに VLAN へパススルーされるマルチキャスト RA の量を制限します。 このコマンドは、VLAN 上でのみ設定できます。

例

```
Device(config)# ipv6 nd ra-throttle policy policy1
Device(config-nd-ra-throttle)# max-through 25
```

medium-type

デバイスが有線か無線かを示すには、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 **media-type** 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。

medium-type {**access-point**| **wired**}

構文の説明

access-point	接続デバイスは無線アクセスポイントで、スロットリングされます。
wired	接続デバイスは有線で、スロットリングされません。

コマンド デフォルト

有線

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（config-nd-ra-throttle）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release XE3.2S	このコマンドが導入されました。

使用上のガイドライン

medium-type コマンドは、ポートのアクセスのタイプだけを示します。 VLAN は、**media-type** コマンドで指定された値を無視します。

例

```
Device(config)# ipv6 nd ra-throttle policy policy1
Device(config-nd-ra-throttle)# medium-type wired
```

mode dad-proxy

IPv6 ネイバー探索（ND）抑制のために重複アドレス検出（DAD）プロキシ モードをイネーブルにするには、ND 抑制ポリシー コンフィギュレーション モードで **mode dad-proxy** 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。

mode dad-proxy

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

マルチキャスト ネイバー送信要求（NS）のすべてのメッセージが抑制されます。

コマンド モード

ND 抑制ポリシー コンフィギュレーション モード（config-nd-suppress）

コマンド履歴

リリース	変更内容
15.1(2)SG	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 DAD プロキシ機能は、アドレスがすでに使用されている場合に、アドレスの所有者に代わって応答します。 IPv6 ND 抑制の使用時に IPv6 DAD プロキシをイネーブルにするには、**mode dad-proxy** コマンドを使用します。 デバイスが IPv6 マルチキャスト抑制をサポートしない場合は、グローバル コンフィギュレーション モードで **ipv6 nd dad-proxy** コマンドを入力して、IPv6 DAD プロキシをイネーブルにできます。

例

```
Device(config)# ipv6 nd suppress policy policy1
Device(config-nd-suppress)# mode dad-proxy
```

関連コマンド

コマンド	説明
ipv6 nd dad-proxy	デバイスの IPv6 ND DAD プロキシ機能をイネーブルにします。

コマンド	説明
ipv6 nd suppress policy	IPv6 ND マルチキャスト抑制をイネーブルにして、ND 抑制ポリシー コンフィギュレーション モードを開始します。

network（IPv6）

ネクスト ホップのネットワーク ソースを PE VPN で使用されるように設定するには、ルータ コンフィギュレーション モードで network コマンドを使用します。 ソース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。

network *ipv6-address/prefix-length*

no network *ipv6-address/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。

コマンド デフォルト

ネクスト ホップのネットワーク ソースは設定されていません。

コマンド モード

アドレス ファミリ コンフィギュレーション ルータ 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(33)SRB	このコマンドが導入されました。
12.2(33)SB	このコマンドが、Cisco IOS Release 12.2(33)SB に統合されました。
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。
Cisco IOS XE Release 3.1S	このコマンドが Cisco IOS XE Release 3.1S 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

このコマンドの *ipv6-address* 引数は、IPv6 ネットワーク番号を設定します。

例

次に、ルータをアドレス ファミリ コンフィギュレーション モードにし、ネットワーク ソースをネクスト ホップとして使用するように設定します。

```
Router(config)# router bgp 100
Router(config-router)# network 2001:DB8:100::1/128
```

関連コマンド

コマンド	説明
address-family ipv6	標準 IPv6 アドレス プレフィックスを使用する BGP などのルーティング セッションを設定するために、アドレス ファミリ コンフィギュレーション モードを開始します。
address-family vpnv6	標準 VPNv6 アドレス プレフィックスを使用するルーティング セッションを設定するために、ルータをアドレス ファミリ コンフィギュレーション モードにします。

other-config-flag

アドバタイズされた「その他」の設定パラメータを確認するには、RA ガード ポリシー コンフィギュレーション モードで **other-config-flag** コマンドを使用します。

other-config-flag {**on**| **off**}

構文の説明

on	検証はイネーブルです。
off	検証はディセーブルです。

コマンド デフォルト

検証はイネーブルになりません。

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

other-config-flag コマンドによって、アドバタイズされた「その他」の設定パラメータ（「O」フラグ）を検証できます。 このフラグは、信頼できない可能性がある Dynamic Host Configuration Protocol for IPv6（DHCPv6）サーバを通じてホストにその他の設定情報を取得させるために、攻撃者によって設定されることがあります。

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、O フラグの検証をイネーブルにする例を示します。

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# other-config-flag on
```

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。

passive-interface（IPv6）

インターフェイス上のルーティングアップデートの送信をディセーブルにするには、ルータ コンフィギュレーション モードで **passive-interface** コマンドを使用します。 ルーティング アップデートの送信を再度イネーブルにするには、このコマンドの **no** 形式を使用します。

passive-interface [**default**| *interface-type interface-number*]

no passive-interface [**default**| *interface-type interface-number*]

構文の説明

default	（任意）すべてのインターフェイスがパッシブとなります。
interface-type interface-number	（任意）インターフェイス タイプおよび番号 詳細については、疑問符（**?**）オンライン ヘルプ機能を使用します。

コマンド デフォルト

インターフェイスはパッシブではありません。 ルーティング アップデートは、ルーティング プロトコルがイネーブルであるすべてのインターフェイスに送信されます。

コマンド モード

ルータ 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(15)T	このコマンドが導入されました。
12.4(6)T	Enhanced Interior Gateway Routing Protocol（EIGRP）IPv6 のサポートが追加されました。
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(33)SRB	このコマンドが、Cisco IOS Release 12.2(33)SRB 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

インターフェイス上でルーティング アップデートの送信をディセーブルにした場合でも、特定のアドレス プレフィックスは引き続き他のインターフェイスにアドバタイズされ、このインターフェイス上の他のルータからのアップデートは引き続き受信および処理されます。

default キーワードを指定すると、すべてのインターフェイスがデフォルトでパッシブに設定されます。 この場合、隣接情報を必要とする個別のインターフェイスを設定するには、**no passive-interface** コマンドを使用します。 **default** キーワードは、インターネット サービス プロバイダー（ISP）や大規模な企業ネットワークなど、多数のディストリビューション ルータに 200 以上ものインターフェイスが搭載されるような環境で役立ちます。

OSPF for IPv6 ルーティング情報は、指定されたルータ インターフェイスから送受信されません。指定したインターフェイス アドレスは、OSPF for IPv6 ドメイン内のスタブ ネットワークとして表示されます。

Intermediate System-to-Intermediate System（IS-IS）プロトコルの場合、このコマンドでは IS-IS に対し、指定したインターフェイスでは実際に IS-IS を実行せずに、このインターフェイスの IP アドレスをアドバタイズするように指示します。 IS-IS に対してこのコマンドの **no** 形式を使用すると、指定したアドレスの IP アドレスのアドバタイズがディセーブルになります。

例

次の例では、すべてのインターフェイスをパッシブに設定してから、インターフェイス ethernet0 をアクティブにする方法を示します。

```
Router(config-router)# passive-interface default
Router(config-router)# no passive-interface ethernet0/0
```

passive-interface（OSPFv3）

IPv4 Open Shortest Path First バージョン 3（OSPFv3）プロセスを使用するときに、インターフェイスのルーティング アップデートの送信を抑制するには、ルータ コンフィギュレーション モードで **passive-interface** コマンドを使用します。 ルーティング アップデートの送信を再度イネーブルにするには、このコマンドの **no** 形式を使用します。

passive-interface [**default**| *interface-type interface-number*]

no passive-interface [**default**| *interface-type interface-number*]

構文の説明

default	（任意）すべてのインターフェイスがパッシブとなります。
interface-type interface-number	（任意）インターフェイス タイプおよび番号 詳細については、疑問符（**?**）オンライン ヘルプ機能を使用します。

コマンド デフォルト

インターフェイスはパッシブではありません。 ルーティング アップデートは、ルーティング プロトコルがイネーブルであるすべてのインターフェイスに送信されます。

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
15.1(3)S	このコマンドが導入されました。
Cisco IOS XE Release 3.4S	このコマンドが Cisco IOS XE Release 3.4S に統合されました。
15.2(1)T	このコマンドが Cisco IOS Release 15.2(1)T に統合されました。
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

インターフェイス上でルーティングアップデートの送信を抑制した場合でも、特定のアドレスプレフィックスは引き続き他のインターフェイスにアドバタイズされ、このインターフェイス上の他のルータからのアップデートは引き続き受信および処理されます。

default キーワードを指定すると、すべてのインターフェイスがデフォルトでパッシブに設定されます。 この場合、隣接情報を必要とする個別のインターフェイスを設定するには、**no passive-interface** コマンドを使用します。 **default** キーワードは、インターネット サービス プロバイダー（ISP）や大規模な企業ネットワークなど、多数のディストリビューション ルータに 200 以上ものインターフェイスが搭載されるような環境で役立ちます。

例

次の例では、すべてのインターフェイスをパッシブに設定してから、イーサネット インターフェイス 0/0 をアクティブにする方法を示します。

```
Router(config-router)# passive-interface default
Router(config-router)# no passive-interface ethernet0/0
```

関連コマンド

コマンド	説明
default（OSPFv3）	OSPFv3 パラメータをデフォルト値に戻します。
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。

permit（IPv6）

IPv6 アクセス リストの許可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 **permit** コマンドを使用します。 許可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。

permit *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*]] [**reflect** *name* [**timeout** *value*]] **[routing]** [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

no permit *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*]] [**reflect** *name* [**timeout** *value*]] **[routing]** [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Internet Control Message Protocol

permit 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

permit 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*}] [**reflect** *name* [**timeout** *value*]] **[routing]** [**routing-type** *routing-number*] **[rst]** [**sequence** *value*] **[syn]** [**time-range** *name*] **[urg]**

User Datagram Protocol

permit 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*}] [**reflect** *name* [**timeout** *value*]] **[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	許可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*	許可条件の設定先である送信元 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。
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。

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*/*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*	許可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*	許可条件の設定先である宛先 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。
dest-option-type	（任意）各 IPv6 パケット ヘッダー内の宛先拡張ヘッダーと 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。 このキーワードが使用されている場合、最初のフラグメントにレイヤ 4 情報が含まれていない場合にも照合を行います。
hbh	（任意）各 IPv6 パケット ヘッダー内のホップバイホップ拡張ヘッダーと IPv6 パケットを照合します。
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。 このメッセージに含まれるものには、アクセス リスト名とシーケンス番号、パケットが許可されたか、プロトコルが TCP、UDP、ICMP、または番号であったか、さらに、該当する場合は、送信元と宛先アドレス、および送信元と宛先ポート番号があります。 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 分間隔で許可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	（mobility）各 IPv6 パケット ヘッダー内のモビリティ拡張ヘッダーと IPv6 パケットを照合します。
mobility-type	（任意）各 IPv6 パケット ヘッダー内のモビリティ タイプ拡張ヘッダーと IPv6 パケットを照合します。 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。 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
reflect *name*	（任意）再帰 IPv6 アクセス リストを指定します。 再帰 IPv6 アクセス リストは、IPv6 パケットが **reflect** キーワードを含む permit ステートメントに一致すると動的に作成されます。 再帰 IPv6 アクセス リストは、permit ステートメントに一致する IPv6 パケットがない場合、permit ステートメントをミラーリングし、自動的にタイムアウトします。 再帰 IPv6 アクセス リストは、IPv6 パケットの TCP、UDP、SCTP、および ICMP に適用できます。

timeout *value*	（任意）再帰 IPv6 アクセス リストがタイムアウトになる前のアイドル時間の間隔（秒単位）。 指定できる範囲は 1 ～ 4294967295 です。 デフォルト値は 180 秒です。
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）各 IPv6 パケット ヘッダー内のルーティング タイプ拡張ヘッダーと IPv6 パケットを照合します。 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）許可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。
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。
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	このコマンドは、Cisco ASR 1000 シリーズ ルータで追加されました。
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

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

ipv6 access-list コマンドに続いて、**permit**（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。

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

再帰アクセス リストの定義

セッション フィルタリングの形式でIPv6 再帰リストを定義するには、**permit**（IPv6）コマンドで **reflect** キーワードを使用します。 **reflect** キーワードは、IPv6 再帰アクセス リストを作成し、再帰アクセス リストのエントリの作成をトリガーします。 **reflect** キーワードは、IPv6 アクセス リストのエントリ（条件ステートメント）である必要があります。

（注） IPv6 再帰アクセス リストを機能させるには、**evaluate** コマンドを使用して再帰アクセス リストをネストする必要があります。

外部インターフェイスの IPv6 再帰アクセス リストを設定する場合、IPv6 アクセス リストはアウトバウンド トラフィックに適用されるものにする必要があります。

内部インターフェイスの IPv6 再帰アクセス リストを設定する場合、IPv6 アクセス リストはインバウンド トラフィックに適用されるものにする必要があります。

ネットワーク内から発信される IPv6 セッションは、ネットワークから出て行くパケットで開始されます。 このようなパケットが IPv6 アクセス リストのステートメントで評価されるとき、パケットは、IPv6 再帰許可エントリでも評価されます。

すべての IPv6 アクセス リスト エントリと同様に、エントリの順序は、順番に評価されるため、重要です。 IPv6 パケットがインターフェイスに到達すると、一致が見つかるまでアクセス リストの各エントリで、順に評価されます。

パケットが再帰許可エントリよりも前のエントリに一致した場合、そのパケットは、再帰許可エントリによって評価されず、再帰アクセス リストの一時エントリが作成されません（セッション フィルタリングはトリガーされません）。

パケットは、他の一致が先に発生しない場合にのみ、再帰許可エントリによって評価されます。 次に、パケットが再帰許可エントリで指定されたプロトコルに一致すると、パケットが転送され、対応する一時エントリが再帰アクセス リストに作成されます（そのパケットが進行中のセッションに属することを示す対応するエントリがまだ存在しない場合）。 一時エントリは、同じセッションでのみネットワークへのトラフィックを許可する条件を指定します。

再帰アクセス リスト エントリの特性

reflect キーワードを指定した **permit**（IPv6）コマンドは、**permit**（IPv6）コマンドで定義されている IPv6 再帰アクセス リストの一時エントリの作成をイネーブルにします。 一時エントリは、**permit**（IPv6）コマンドで指定されたプロトコルと、ネットワークから出て行く IPv6 パケットが一致するときに作成されます。 （パケットが、エントリの作成を「トリガー」します）。これらのエントリには次の特性があります。

- エントリは許可エントリです。
- エントリは元のトリガー パケットと同じ IP 上位層プロトコルを指定します。
- エントリは元のトリガー パケットと同じ送信元および宛先アドレスを指定します。ただし、これらのアドレスが入れ替わります。
- 元のトリガー パケットが TCP または UDP である場合、そのエントリは元のパケットと同じ送信元および宛先ポート番号を指定します。ただし、これらのポート番号が入れ替わります。
- 元のトリガー パケットが TCP または UDP 以外のプロトコルの場合、ポート番号は適用されず、他の条件が指定されます。 たとえば、ICMP の場合、タイプ番号が使用されます。一時エントリは元のパケットと同じタイプ番号を指定します（ただし、1 つだけ例外があり、元

の ICMP パケットがタイプ 8 の場合、一致する回帰 ICMP パケットはタイプ 0 である必要があります）。

- エントリは、上記 4 件の項目で示す例外を除き、元のトリガー パケットのすべての値を継承します。
- 内部ネットワークに入る IPv6 トラフィックは、エントリが期限切れになるまで、エントリに対して評価されます。 IPv6 パケットがエントリに一致した場合、パケットはネットワークに転送されます。
- エントリは、セッションの最後のパケットが照合された後に失効（または削除）されます。
- セッションに属するパケットが設定された時間（タイムアウト期間）検出されない場合、エントリは期限切れになります。

例

次の例では、OUTBOUND および INBOUND という名の IPv6 アクセス リスト 2 つを設定し、そのアクセス リストをイーサネット インターフェイス 0 上の発信および着信トラフィックに適用する方法を示します。 OUTBOUND リスト内の最初と 2 番めの許可エントリは、ネットワーク 2001:ODB8:0300:0201::/64 から送信されたすべての TCP および UDP 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許可します。 また、エントリは REFLECTOUT という名前の一時的な IPv6 再帰アクセス リストを設定して、イーサネット インターフェイス 0 上で回帰（着信）TCP および UDP パケットをフィルタリングします。 OUTBOUND リストの最初の拒否エントリは、ネットワーク FEC0:0:0:0201::/64 から送信されたすべてのパケット（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 FEC0:0:0:0201 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。 OUTBOUND リストの 3 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 から出るすべての ICMP パケットを許可します。

INBOUND リストの許可エントリは、すべての ICMP パケットをイーサネット インターフェイス 0 で受信するのを許可します。 リストの **evaluate** コマンドは、REFLECTOUT という名前の一時的な IPv6 再帰アクセス リストをイーサネット インターフェイス 0 上の着信 TCP および UDP パケットに適用します。 OUTBOUND リストによって発信 TCP または UDP パケットがイーサネット インターフェイス 0 上で許可された場合、INBOUND リストは REFLECTOUT リストを使用して、回帰（着信）TCP および UDP パケットを照合（評価）します。 IPv6 ACL 内に IPv6 再帰アクセス リストをネストさせる方法の詳細については **evaluate** コマンドを参照してください。

```
ipv6 access-list OUTBOUND
 permit tcp 2001:0DB8:0300:0201::/64 any reflect REFLECTOUT
 permit udp 2001:0DB8:0300:0201::/64 any reflect REFLECTOUT
 deny FEC0:0:0:0201::/64 any
 permit icmp any any
ipv6 access-list INBOUND
 permit icmp any any
 evaluate REFLECTOUT
interface ethernet 0
 ipv6 traffic-filter OUTBOUND out
 ipv6 traffic-filter INBOUND in
```

（注） **permit any any** ステートメントが OUTBOUND または INBOUND アクセス リストの最後のエントリとして含まれていない場合、TCP、UDP、およびICMPパケットだけがイーサネットインターフェイス 0 の双方向（着信および発信）で許可されます（アクセス リストの末尾にある、暗黙の条件によりインターフェイス上のその他のパケット タイプはすべて拒否されます）。

次に、UDPトラフィック照合を許可する例を示します。 認証ヘッダーが存在する可能性があります。

```
permit udp any any sequence 10
```

次に、認証ヘッダーも存在する場合に、TCP トラフィックだけの照合を許可する例を示します。

```
permit tcp any any auth sequence 20
```

次に、認証ヘッダーが存在する場合に、任意の IPv6 トラフィックの照合を許可する例を示します。

```
permit ahp any any sequence 30
```

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。
evaluate（IPv6）	IPv6 アクセス リスト内に IPv6 再帰アクセス リストをネストします。
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。
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。

prefix-glean

デバイスが IPv6 ルータ アドバタイズメント（RA）または Dynamic Host Configuration Protocol（DHCP）からプレフィックスを取り出せるようにするには、ipv6 スヌーピング コンフィギュレーション モードで **prefix-glean** コマンドを使用します。 これらのプロトコルのいずれかで収集したプレフィックスだけを学習し、残りを除外するには、このコマンドの **no** 形式を使用します。

prefix-glean [**only**]

no prefix-glean [**only**]

構文の説明

only	（任意）プレフィックスだけ収集します。

コマンド デフォルト

プレフィックスは RA または DHCP から学習されません。

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
15.0(2)SE	このコマンドが導入されました。
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。
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-glean コマンドは、デバイスが RA および DHCP トラフィックでプレフィックスを学習できるようにします。

例

次に、デバイスがプレフィックスを学習できるようにする例を示します。

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# prefix-glean
```

関連コマンド

コマンド	説明
ipv6 snooping attach-policy	ターゲットに IPv6 スヌーピングにポリシーを適用します。
ipv6 snooping policy	IPv6 スヌーピング ポリシーを設定し、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。

protocol（IPv6）

アドレスを Dynamic Host Configuration Protocol（DHCP）またはネイバー探索プロトコル（NDP）で収集するように指定する、またはIPv6プレフィックス リストにプロトコルを関連付けるには、**protocol** コマンドを使用します。 DHCP または NDP によるアドレス収集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。

protocol {**dhcp** | **ndp**} [**prefix-list** *prefix-list-name*]

no protocol {**dhcp** | **ndp**}

構文の説明

dhcp	アドレスを Dynamic Host Configuration Protocol（DHCP）パケットで取り出す必要があることを指定します。
ndp	アドレスをネイバー探索プロトコル（NDP）パケットで取り出す必要があることを指定します。
prefix-list *prefix-list-name*	（任意）保護されたプレフィックスのプレフィックス リストを使用することを指定します。

コマンド デフォルト

スヌーピングとリカバリは DHCP および NDP 両方を使用して試行されます。 プレフィックス リストは使用されず、すべてのアドレス範囲が受け入れられます。

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

アドレスが DHCP または NDP に関連付けられたプレフィックス リストと一致しなければ、制御パケットがドロップされ、バインディングテーブルエントリのリカバリはそのプロトコルでは試みられません。

- 指定されたプレフィックスリストがない場合、すべてのプロトコルがデフォルトでサポートされます。 チェックがないため、すべてのアドレスが受け入れられます。
- **no protocol** {**dhcp** | **ndp**} コマンドを使用すると、プロトコルがスヌーピングまたはグリーニングに使用されないことを示します。
- ただし、**no protocol dhcp** コマンドが使用されなければ、DHCP はまだバインディング テーブルのリカバリに使用できます。
- DHCP で取得されたアドレスが NDP によって確認される必要があるため、NDP プレフィックス リストは DHCP プレフィックス リストのスーパーセットである必要があります。
- プレフィックス リストが指定され、プロトコル パケットでそのプロトコルのプレフィックス リストに一致しないアドレスが示された場合、パケットはドロップされます（セキュリティ レベルが「glean」でない場合）。
- データのグリーニングは DHCP および NDP でリカバリできますが、宛先ガードは DHCP でのみリカバリします。

（注） **protocol** コマンドを設定する前に、プレフィックス リストを **ipv6 prefix-list** コマンドを使用して設定するときに、**ge** *ge-value* オプションの値を指定する必要があります。

例

次の例では、IPv6プレフィックスリスト（「abc」）の有効な設定を示し、DHCPを使用してプレフィックス リスト abc と一致したアドレスを回復します。

```
Device(config)# ipv6 prefix-list abc seq 5 permit 2001:DB8::/64 ge 128
!
Device(config-ipv6-snooping)# protocol dhcp prefix-list abc
```

関連コマンド

コマンド	説明
ipv6 prefix-list	IPv6 プレフィックス リストのエントリを作成します。
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。

redistribute（IPv6）

あるルーティング ドメインから別のルーティング ドメインに IPv6 ルートを再配布するには、アドレス ファミリ コンフィギュレーション モードまたはルータ コンフィギュレーション モードで **redistribute** コマンドを使用します。 再配布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。

redistribute source-protocol [*process-id*] [**include-connected** {**level-1**| **level-1-2**| **level-2**}] [*as-number*] [**metric** {*metric-value*| **transparent**}] [**metric-type** *type-value*] [**match** {**external** [**1**| **2**]| **internal**| **nssa-external** [**1**| **2**]}] [**tag** *tag-value*] [**route-map** *map-tag*]

no redistribute source-protocol [*process-id*] **[include-connected]** {**level-1**| **level-1-2**| **level-2**} [*as-number*] [**metric** {*metric-value*| **transparent**}] [**metric-type** *type-value*] [**match** {**external** [**1**| **2**]| **internal**| **nssa-external** [**1**| **2**]}] [**tag** *tag-value*] [**route-map** *map-tag*]

構文の説明

source-protocol	ルートの再配布元であるソース プロトコルです。 **bgp**、connected、**eigrp**、**isis**、**ospf**、**rip**、または **static** のキーワードのいずれかになります。
process-id	（任意）**bgp** または **eigrp** キーワードの場合、プロセス ID は 16 ビットの 10 進数であるボーダー ゲートウェイ プロトコル（BGP）の自律システム番号です。 **isis** キーワードの場合、プロセス ID はルーティング プロセスのわかりやすい名前を定義するオプションの値です。 各ルータに指定できる IS-IS プロセスは 1 つだけです。 ルーティング プロセスの名前を作成することは、ルーティングを設定するときに名前を使用することを意味します。 **ospf** キーワードの場合、プロセス ID は、IPv6 ルーティング プロセスの Open Shortest Path First（OSPF）がイネーブルのときに管理上割り当てられる番号です。 **rip** キーワードの場合、プロセス ID は IPv6 Routing Information Protocol（RIP）ルーティング プロセスのわかりやすい名前を定義するオプションの値です。

include-connected	（任意）ソースプロトコルから学習したルートと、ソースプロトコルが動作しているインターフェイス上の接続先プレフィックスを、ターゲット プロトコルが再配布できるようにします。
level-1	Intermediate System-to-Intermediate System（IS-IS）用に、レベル 1 ルートが他の IP ルーティングプロトコルに個別に再配布されることを指定します。
level-1-2	IS-IS 用に、レベル 1 とレベル 2 の両方のルートが他の IP ルーティング プロトコルに再配布されることを指定します。
level-2	IS-IS 用に、レベル 2 ルートが他の IP ルーティングプロトコルに個別に再配布されることを指定します。
as-number	（任意）再配布ルートの自律システム番号。
metric *metric-value*	（任意）同じルータ上で 1 つの OSPF プロセスから別の OSPF プロセスに再配布する場合、メトリック値を指定しないと、メトリックは 1 つのプロセスから他のプロセスへ存続します。他のプロセスを OSPF プロセスに再配布するときに、メトリック値を指定しない場合、デフォルトのメトリックは 20 です。
metric transparent	（任意）RIP が、RIP メトリックとして再配布ルートのルーティング テーブル メトリックを使用します。

metric-type *type-value*	（任意）OSPF の場合、OSPF ルーティング ドメインにアドバタイズされるデフォルトのルートに関連付けられる外部リンク タイプを指定します。 次の2つの値のいずれかにすることができます。 • **1**：タイプ 1 外部ルート • **2**：タイプ 2 外部ルート **metric-type** キーワードに値が指定されていない場合、Cisco IOS ソフトウェアは、タイプ 2 外部ルートを受け入れます。 IS-IS の場合、リンク タイプは次の 2 つの値のいずれかになります。 • **internal**：63 までの IS-IS メトリック。 • **external**:64 から 128 の IS-IS メトリック。 デフォルトは、**internal** です。
match {**external [1 | 2]**| **internal | nssa-external [1 | 2]**	（任意）OSPF では、ルートが match キーワードを使用して他のルーティング ドメインに再配布されます。 これは次のいずれかで使用されます。 • **external [1 | 2]**：自律システム外部のルートである一方で、タイプ 1 またはタイプ 2 の外部ルートとして OSPF にインポートされているルート。 • **internal**：特定の自律システムの内部にあるルート。 • **nssa-external** [**1** | **2**]：自律システムの外部にあるが、Not So Stubby Area（NSSA）で OSPF for IPv6 にタイプ 1 またはタイプ 2 の外部ルートとしてインポートされているルート。

tag *tag-value*	（任意）各外部ルートに付加する 32 ビットの 10 進値を指定します。 これは OSPF 自体には使用されません。 自律システム境界ルータ（ASBR）間で情報を通信するために使用できます。 何も指定しない場合、BGP および外部ゲートウェイ プロトコル（EGP）からのルートにはリモート自律システムの番号が使用され、その他のプロトコルには 0 が使用されます。
route-map	（任意）このソース ルーティング プロトコルから現在のルーティング プロトコルへのルートのインポートをフィルタリングするために検査する必要のあるルート マップを指定します。 route-map キーワードが指定されない場合、すべてのルートが再配布されます。 このキーワードが指定されていて、ルート マップ タグがリストされていない場合、ルートはインポートされません。
map-tag	（任意）設定されたルート マップの ID。

コマンド デフォルト　ルートの再配布はディセーブルです。

コマンド モード　アドレス ファミリ コンフィギュレーション ルータ 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(15)T	このコマンドが導入されました。
12.4(6)T	Enhanced Interior Gateway Routing Protocol（EIGRP）IPv6 のサポートが追加されました。
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。

リリース	変更内容
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

いずれかのキーワードを変更またはディセーブルにしても、他のキーワードの状態には影響しません。

内部メトリックを持つ IPv6 IS-IS ルートを受信するルータは、それ自身から再配布するルータまでのルートのコストと、アドバタイズされたコストの合計で、宛先に到達すると判断します。 外部メトリックでは、宛先に達するまでのアドバタイズされたコストだけを考慮します。

IS-IS は include-connected キーワードで設定されたルートの設定された再配布を無視します。 IS-IS は、IS-IS がインターフェイス上で実行されているか、インターフェイスがパッシブに設定されている場合、インターフェイスのプレフィックスをアドバタイズします。

IPv6 ルーティング プロトコルから学習したルートは、接続されたエリアにレベル 1 で IPv6 IS-IS に、またはレベル 2 で再配布できます。 **level-1-2** キーワードはレベル 1 とレベル 2 の両方のルートを 1 つのコマンドで許可します。

IPv6 RIP の場合、直接接続されたルートであるかのようにスタティック ルートをアドバタイズするには、**redistribute** コマンドを使用します。

注意 不適切に設定されている場合は、直接接続されたルートとしてスタティック ルートをアドバタイジングすると、ルーティング ループが発生する可能性があります。

再配布された IPv6 RIP ルーティング情報は、**distribute-list prefix-list** ルータ コンフィギュレーション コマンドによって常にフィルタリングする必要があります。 **distribute-list prefix-list** コマンドの使用により、管理者が意図するルートだけが、受信側のルーティング プロトコルに渡されることを保障します。

（注） IPv6 RIP の **redistribute** コマンドで指定された **metric** 値は、**default-metric** コマンドを使用して指定された **metric** 値よりも優先されます。

（注） IPv4では、プロトコルを再配布する場合、デフォルトでプロトコルが実行されているインターフェイスのサブネットも再配布されます。 IPv6 では、これはデフォルトの動作ではありません。 プロトコルが IPv6 で動作しているインターフェイスのサブネットを再配布するには、include-connected キーワードを使用します。 IPv6 では、この機能は、ソースプロトコルが BGP の場合はサポートされません。

redistribute コマンドが設定されていない場合、パラメータ設定は、クライアント プロトコルが IS-IS または EIGRP の場合は無視されます。

IS-IS 再配布は、IS-IS レベル 1 およびレベル 2 がユーザによって削除されると完全に削除されます。 IS-IS レベル設定は、redistribute コマンドだけを使用して設定できます。

すべてのルート タイプ値がユーザによって削除されると、デフォルトの再配布タイプは OSPF にリストアされます。

例

次の例では、IPv6 IS-IS の IPv6 BGP ルートを再配布するように設定します。 メトリックは 5 として指定され、メトリック タイプは、内部メトリックより優先順位が低いことを示す外部に設定されます。

```
Router(config)# router isis
Router(config-router)# address-family ipv6
Router(config-router-af)# redistribute bgp 64500 metric 5 metric-type external
```

次に、cisco という名前の IPv6 RIP ルーティング プロセスに IPv6 BGP ルートを再配布する例を示します。

```
Router(config)# ipv6 router rip cisco
Router(config-router)# redistribute bgp 42
```

次に、OSPF for IPv6 ルーティング プロセス 1 に IS-IS for IPv6 ルートを再配布する例を示します。

```
Router(config)# ipv6 router ospf 1
Router(config-router)# redistribute isis 1 metric 32 metric-type 1 tag 85
```

次の例では、ospf 1 がプレフィックス 2001:1:1::/64 および 2001:99:1::/64 と、rip 1 を通じて学習したプレフィックスを再配布します。

```
interface ethernet0/0
 ipv6 address 2001:1:1::90/64
 ipv6 rip 1 enable
interface ethernet1/1
 ipv6 address 2001:99:1::90/64
 ipv6 rip 1 enable
interface ethernet2/0
 ipv6 address 2001:1:2::90/64
 ipv6 ospf 1 area 1
ipv6 router ospf 1
  redistribute rip 1 include-connected
```

次の設定例および出力例は、最後のルート タイプ値を削除すると、redistribute コマンド パラメータがなくなることを示しています。

```
Router(config-router)# redistribute rip process1 metric 7
Router(config-router)# do show run | include redistribute
 redistribute rip process1 metric 7
Router(config-router)# no redistribute rip process1 metric 7
```

```
Router(config-router)# do show run | include redistribute
 redistribute rip process1
Router(config-router)#
```

関連コマンド

コマンド	説明
default-metric	再配布されるルートのデフォルト メトリックを指定します。
distribute-list prefix-list（IPv6 EIGRP）	インターフェイス上で受信または送信される EIGRP for IPv6 ルーティング アップデートに、プレフィックス リストを適用します。
distribute-list prefix-list（IPv6 RIP）	インターフェイス上で受信または送信される IPv6 RIP ルーティング アップデートに、プレフィックス リストを適用します。
redistribute isis（IPv6）	ターゲット プロトコルとソース プロトコルの両方として IS-IS を使用して、あるルーティング ドメインから別のルーティング ドメインに IPv6 ルートを再配布します。

router-preference maximum

アドバタイズされたデフォルト ルータ プリファレンス パラメータ値を確認するには、RA ガード ポリシー コンフィギュレーション モードで **router-preference maximum** コマンドを使用します。

router-preference maximum {**high**| **low**| **medium**}

構文の説明

high	デフォルト ルータ プリファレンス パラメータ値が指定された制限を超えています。
medium	デフォルト ルータ プリファレンス パラメータ値が指定された制限と同じです。
low	デフォルト ルータ プリファレンス パラメータ値が指定された制限よりも低くなっています。

コマンド デフォルト

ルータ プリファレンスの最大値は設定されていません。

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

router-preference maximum コマンドによって、アドバタイズされたデフォルト ルータ プリファレンス パラメータ値が指定された制限以下であることを確認できます。このコマンドは、トランク ポートでアドバタイズされるデフォルト ルータに低いプライオリティを指定し、アクセス ポートでアドバタイズされるデフォルト ルータを優先するために使用できます。

router-preference maximum コマンドの制限は、high、medium、low です。 たとえば、この値が **medium** に設定され、受信パケットのアドバタイズされたデフォルト ルータ プリファレンスが **high** に設定されている場合、パケットはドロップされます。受信パケットでコマンドオプションが **medium** または **low** に設定されている場合、パケットはドロップされません。

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、router-preference maximum の検証を high に設定する例を示します。

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# router-preference maximum high
```

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。