IPv6 コマンド

clear ipv6 access-list

IPv6 アクセス リストの一致カウンタをリセットするには、特権 EXEC モードで **clearipv6access-list** コマンドを使用します。

clear ipv6 access-list [*access-list-name*]

構文の説明

access-list-name	（任意）一致カウンタをクリアする IPv6 アクセス リストの名前。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

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

clearipv6access-list コマンドは、IPv6 に固有であることを除き、**clearipaccess-listcounters** コマンドと同様です。

access-list-name 引数なしで **clearipv6access-list** コマンドを使用すると、ルータに設定されているすべての IPv6 アクセス リストの一致カウンタがリセットされます。

このコマンドは、IPv6 グローバル ACL ハードウェア カウンタをリセットします。

例

次に、marketing という IPv6 アクセス リストの一致カウンタをリセットする例を示します。

```
Device# clear ipv6 access-list marketing
```

関連コマンド

コマンド	説明
hardwarestatistics	ハードウェア統計情報の収集をイネーブルにします。
ipv6access-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。
showipv6access-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。

clear ipv6 dhcp

IPv6 Dynamic Host Configuration Protocol（DHCP）情報をクリアするには、特権 EXEC モードで **clearipv6dhcp** コマンドを使用します。

clear ipv6 dhcp

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 モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

clearipv6dhcp コマンドは IPv6 の DHCP 情報を削除します。

例

次に例を示します。

```
Device# clear ipv6 dhcp
```

clear ipv6 dhcp binding

IPv6 サーバのバインディング テーブルの Dynamic Host Configuration Protocol（DHCP）から自動クライアント バインディングを削除するには、特権 EXEC モードで **clearipv6dhcpbinding** コマンドを使用します。

clear ipv6 dhcp binding [*ipv6-address*] [**vrf** *vrf-name*]

構文の説明

ipv6-address	（任意）IPv6 クライアントの DHCP のアドレス。 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。
vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

clearipv6dhcpbinding コマンドはサーバ関数として使用します。

IPv6 用 DHCP サーバのバインディング テーブル エントリに対して、次の処理が自動的に行われます。

- コンフィギュレーション プールからプレフィックスがクライアントに委任されるたびに作成されます。
- クライアントがプレフィックスの委任を更新、再バインディング、または確認すると更新されます。
- クライアントがバインディング内のすべてのプレフィックスを自発的に解放したか、すべてのプレフィックスの有効期限が切れたか、または管理者が**clearipv6dhcpbinding** コマンドを実行した場合に、削除されます。

clearipv6dhcpbinding コマンドをオプションの *ipv6-address* 引数とともに使用すると、特定のクライアントのバインディングのみが削除されます。**clearipv6dhcpbinding** コマンドを *ipv6-address* 引数なしに使用すると、IPv6 バインディング テーブルの DHCP からすべての自動クライアント バインディングが削除されます。オプションの **vrf** キーワードと *vrf-name* 引数の組み合わせを使用すると、特定の VRF のバインディングのみがクリアされます。

例

次に、IPv6 サーバのバインディング テーブルの DHCP からすべての自動クライアント バインディングを削除する例を示します。

```
Device# clear ipv6 dhcp binding
```

関連コマンド

コマンド	説明
showipv6dhcpbinding	IPv6 サーバのバインディング テーブルの DHCP から自動クライアント バインディングを表示します。

clear ipv6 dhcp client

インターフェイス上の IPv6 クライアントの Dynamic Host Configuration Protocol（DHCP）を再起動するには、特権 EXEC モードで **clearipv6dhcpclient** コマンドを使用します。

clear ipv6 dhcp client *interface-type interface-number*

構文の説明

interface-type interface-number	インターフェイスのタイプと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 モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

clearipv6dhcpclient コマンドは、以前に取得したプレフィックスとその他のコンフィギュレーション オプション（ドメイン名システム [DNS] サーバなど）を最初に解放し、設定を解除した後に、特定のインターフェイス上の IPv6 クライアントの DHCP を再起動します。

例

次に、イーサネット インターフェイス 1/0 の IPv6 クライアントの DHCP を再起動する例を示します。

```
Device# clear ipv6 dhcp client Ethernet 1/0
```

関連コマンド

コマンド	説明
showipv6dhcpinterface	IPv6 用 DHCP のインターフェイス情報を表示します。

clear ipv6 dhcp conflict

IPv6（DHCPv6）サーバ データベースの Dynamic Host Configuration Protocol からアドレス競合をクリアするには、特権 EXEC モードで **clearipv6dhcpconflict** コマンドを使用します。

clear ipv6 dhcp conflict {*****|*ipv6-address*|**vrf** *vrf-name*}

構文の説明

*	すべてのアドレス競合をクリアします。
ipv6-address	競合するアドレスを含むホストIPv6アドレスをクリアします。
vrf *vrf-name*	Virtual Routing and Forwarding（VRF）名を指定します。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

競合を検出するようにDHCPv6サーバを設定する場合、DHCPv6サーバはpingを使用します。クライアントはネイバー探索を使用してクライアントを検出し、DECLINE メッセージを介してサーバに報告します。アドレス競合が検出されると、このアドレスはプールから削除されます。管理者がこのアドレスを競合リストから削除するまでこのアドレスは割り当てることができません。

アドレス パラメータとしてアスタリスク（*）文字を使用すると、DHCP はすべての競合をクリアします。

vrf キーワードと *vrf-name* 引数を指定すると、特定の VRF に属しているアドレス競合のみがクリアされます。

例

次に、DHCPv6 サーバ データベースからすべてのアドレス競合をクリアする例を示します。

```
Device# clear ipv6 dhcp conflict *
```

関連コマンド

コマンド	説明
showipv6dhcpconflict	アドレスをクライアントに提供する際にDHCPv6サーバによって検出されたアドレス競合を表示します。

clear ipv6 dhcp relay binding

IPv6 リレー バインディングの Dynamic Host Configuration Protocol（DHCP）の IPv6 アドレスまたは IPv6 プレフィックスをクリアするには、特権 EXEC モードで **clearipv6dhcprelaybinding** コマンドを使用します。

clear ipv6 dhcp relay binding{**vrf** *vrf-name*}{**ipv6-addressipv6-prefix*}

clear ipv6 dhcp relay binding{**vrf** *vrf-name*}{** ipv6-prefix*}

構文の説明

vrf *vrf-name*	Virtual Routing and Forwarding（VRF）のコンフィギュレーションを指定します。
*	すべての DHCPv6 リレー バインディングをクリアします。
ipv6-address	DHCPv6 アドレス。
ipv6-prefix	IPv6 prefix.

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

clearipv6dhcprelaybinding コマンドは、IPv6 リレー バインディングの DHCP の特定の IPv6 アドレスまたは IPv6 プレフィックスを削除します。リレー クライアントを指定しないと、バインディングは削除されません。

例

次に、指定した IPv6 アドレスを持つクライアントのバインディングをクリアする例を示します。

```
Device# clear ipv6 dhcp relay binding 2001:0DB8:3333:4::5
```

次に、Cisco uBR10012 ユニバーサル ブロードバンド デバイス上の vrf1 という VRF 名と特定のプレフィックスを持つクライアントのバインディングをクリアする例を示します。

```
Device# clear ipv6 dhcp relay binding vrf vrf1 2001:DB8:0:1::/64
```

関連コマンド

コマンド	説明
show ipv6dhcp relay binding	リレー エージェント上の DHCPv6 IANA バインディングと DHCPv6 IAPD バインディングを表示します。

clear ipv6 eigrp

IPv6 ルーティング テーブルの Enhanced Interior Gateway Routing Protocol（EIGRP）からエントリを削除するには、特権 EXEC モードで **clearipv6eigrp** コマンドを使用します。

clear ipv6 eigrp [*as-number*] [**neighbor** [{*ipv6-address*|*interface-type interface-number*}]]

構文の説明

as-number	（任意）自律システム番号。
neighbor	（任意）ネイバー ルータのエントリを削除します。
ipv6-address	（任意）隣接ルータの IPv6 アドレス。
interface-type	（任意）ネイバー ルータのインターフェイス タイプ。
interface-number	（任意）ネイバー ルータのインターフェイス番号。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

IPv6 ルーティング テーブル エントリのすべての EIGRP をクリアするには、引数およびキーワードを指定せずに **clearipv6eigrp** コマンドを使用します。指定したプロセスのルーティング テーブルのエントリをクリアするには *as-number* 引数を使用し、ネイバー テーブルから特定のネイバーを削除するには **neighbor** キーワードと *ipv6-address* 引数、または *interface-typeinterface-number* 引数を使用します。

例

次に、IPv6 アドレスが 3FEE:12E1:2AC1:EA32 のネイバーを削除する例を示します。

```
Device# clear ipv6 eigrp neighbor 3FEE:12E1:2AC1:EA32
```

clear ipv6 mfib counters

アクティブなすべてのマルチキャスト転送情報ベース（MFIB）のトラフィック カウンタをリセットするには、特権 EXEC モードで **clearipv6mfibcounters** コマンドを使用します。

clear ipv6 mfib [**vrf** *vrf-name*] **counters** [{*group-name*|*group-address* [{*source-addresssource-name*}]}]

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
group-name | *group-address*	（任意）マルチキャスト グループの IPv6 アドレスまたは名前。
source-address | *source-name*	（任意）送信元の IPv6 アドレスまたは名前。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

clearipv6mfibcounters コマンドを有効にした後、トラフィック カウンタを表示する次の show コマンドのいずれかを使用して追加のトラフィックを転送するかどうかを決定できます。

- **showipv6mfib**
- **showipv6mfibactive**
- **showipv6mfibcount**
- **showipv6mfibinterface**
- **showipv6mfibsummary**

例

次に、すべての MFIB トラフィック カウンタをクリアしてからリセットする例を示します。

```
Device# clear ipv6 mfib counters
```

clear ipv6 mld counters

マルチキャスト リスナー検出（MLD）インターフェイス カウンタをクリアするには、特権 EXEC モードで **clearipv6mldcounters** コマンドを使用します。

clear ipv6 mld [**vrf** *vrf-name*] **counters** [*interface-type*]

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
interface-type	（任意）インターフェイス タイプ。詳細については、疑問符（**?**）オンラインヘルプ機能を使用してください。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

受信した join と leave の数を追跡する MLD カウンタをクリアするには、**clearipv6mldcounters** コマンドを使用します。オプションの *interface-type* 引数を省略すると、**clearipv6mldcounters** コマンドはすべてのインターフェイスのカウンタをクリアします。

例

次に、イーサネット インターフェイス 1/0 のカウンタをクリアする例を示します。

```
Device# clear ipv6 mld counters Ethernet1/0
```

関連コマンド

コマンド	説明
showipv6mldinterface	インターフェイスのマルチキャスト関連情報を表示します。

clear ipv6 mld traffic

マルチキャストリスナー検出（MLD）トラフィック カウンタをリセットするには、特権EXECモードで **clearipv6mldtraffic** コマンドを使用します。

clear ipv6 mld [**vrf** *vrf-name*] **traffic**

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

clearipv6mldtraffic コマンドを使用して、すべての MLD トラフィック カウンタをリセットします。

例

次に、MLD トラフィック カウンタをリセットする例を示します。

```
Device# clear ipv6 mld traffic
```

コマンド	説明
showipv6mldtraffic	MLD トラフィック カウンタを表示します。

clear ipv6 mtu

メッセージの最大伝送ユニット（MTU）のキャッシュをクリアするには、特権 EXEC モードで **clearipv6mtu** 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 キャッシュからはクリアされません。

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 Everest 16.5.1a	このコマンドが導入されました。

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ている場合、そのルータは利用可能なすべてのメモリが消費されるまで、MTUキャッシュ内にエントリを無制限に作成します。MTUキャッシュからメッセージをクリアするには、**clearipv6mtu** コマンドを使用します。

例

次に、メッセージの MTU をクリアする例を示します。

```
Device# clear ipv6 mtu
```

関連コマンド

コマンド	説明
ipv6flowset	ルータによって送信された 1,280 バイト以上のパケット内にフローラベル マーキングを設定します。

clear ipv6 multicast aaa authorization

IPv6 マルチキャスト ネットワークへのユーザ アクセスを制限する認証パラメータをクリアするには、特権 EXEC モードで **clearipv6multicastaaaauthorization** コマンドを使用します。

clear ipv6 multicast aaa authorization [*interface-type interface-number*]

構文の説明

interface-type interface-number	インターフェイスのタイプと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 モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

オプションの *interface-type* 引数と *interface-number* 引数なしで **clearipv6multicastaaaauthorization** コマンドを使用すると、ネットワーク上のすべての認証パラメータがクリアされます。

例

次に、IPv6 ネットワーク上に設定されているすべての認証パラメータをクリアする例を示します。

```
Device# clear ipv6 multicast aaa authorization FastEthernet 1/0
```

関連コマンド

コマンド	説明
aaaauthorizationmulticastdefault	IPv6 マルチキャスト ネットワークへのユーザ アクセスを制限するパラメータを設定します。

clear ipv6 nd destination

IPv6 ホストモードの宛て先キャッシュのエントリをクリアするには、特権 EXEC モードで **clear ipv6 nd destination** コマンドを使用します。

clear ipv6 nd destination ［**vrf** *vrf-name*］

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

clear ipv6 nd destination コマンドは IPv6 ホストモードの宛て先キャッシュのエントリをクリアします。**vrf** キーワードと *vrf-name* 引数のペアを使用すると、指定した VRF に関する情報のみがクリアされます。

例

次に、IPv6 ホストモードの宛て先キャッシュのエントリをクリアする例を示します。

```
Device# clear ipv6 nd destination
```

関連コマンド

コマンド	説明
ipv6 nd host mode strict	conformant または strict の IPv6 ホスト モードを有効にします。

clear ipv6 nd on-link prefix

ルータ アドバタイズメント（RA）を通じて学習したオンリンク プレフィックスをクリアするには、特権 EXEC モードで **clear ipv6 nd on-link prefix** コマンドを使用します。

clear ipv6 nd on-link prefix ［**vrf** *vrf-name*］

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

RA を通じて学習したローカルに到達可能な IPv6 アドレス（on-link プレフィックス）をクリアするには、**clear ipv6 nd on-link prefix** コマンドを使用します。**vrf** キーワードと *vrf-name* 引数のペアを使用すると、指定した VRF に関する情報のみがクリアされます。

例

次に、RA を通じて学習したオンリンク プレフィックスをクリアする例を示します。

```
Device# clear ipv6 nd on-link prefix
```

関連コマンド

コマンド	説明
ipv6 nd host mode strict	conformant または strict の IPv6 ホスト モードを有効にします。

clear ipv6 nd router

ルータアドバタイズメント（RA）を通じて学習したネイバー探索（ND）デバイスのエントリをクリアするには、特権 EXEC モードで **clear ipv6 nd router** コマンドを使用します。

clear ipv6 nd router ［**vrf** *vrf-name*］

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

RA を通じて学習した ND デバイスをクリアするには **clear ipv6 nd router** コマンドを使用します。**vrf** キーワードと *vrf-name* 引数のペアを使用すると、指定した VRF に関する情報のみがクリアされます。

例

次に、RAを通じて学習したネイバー探索NDデバイスのエントリをクリアする例を示します。

```
Device# clear ipv6 nd router
```

関連コマンド

コマンド	説明
ipv6 nd host mode strict	conformant または strict の IPv6 ホスト モードを有効にします。

clear ipv6 neighbors

Virtual Routing and Forwarding（VRF）以外のインターフェイス上の静的エントリおよびNDキャッシュのエントリを除き、IPv6ネイバー探索キャッシュ内のすべてのエントリを削除するには、特権 EXEC モードで **clearipv6neighbors** コマンドを使用します。

clear ipv6 neighbors [{**interface** *type number* [**ipv6** *ipv6-address*]|**statistics**|**vrf** *table-name* [{*ipv6-address*|**statistics**}]}]

clear ipv6 neighbors

構文の説明

interface *type number*	（任意）指定したインターフェイスのIPv6ネイバー探索キャッシュをクリアします。
ipv6 *ipv6-address*	（任意）指定したインターフェイス上の指定したIPv6アドレスに一致するIPv6ネイバー探索キャッシュをクリアします。
statistics	（任意）IPv6ネイバー探索エントリのキャッシュをクリアします。
vrf	（任意）バーチャル プライベート ネットワーク（VPN）のルーティング インスタンスまたは転送インスタンスのエントリをクリアします。
table-name	（任意）テーブル名または識別子。値の範囲は 0x0 ～ 0xFFFFFFFF（10進数では 0 ～ 65535）です。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

clear ipv6 neighbor コマンドはNDキャッシュのエントリをクリアします。**vrf** キーワードなしにコマンドを発行すると、このコマンドはデフォルトのルーティングテーブルに関連付けられているインターフェイス（**vrf forwarding** ステートメントを持たないインターフェイス）上のNDキャッシュのエントリをクリアします。**vrf**キーワードを指定してコマンドを発行すると、指定した VRF に関連付けられているインターフェイス上の ND キャッシュのエントリをクリアします。

例

次に、静的エントリおよびVRF以外のインターフェイス上のNDキャッシュのエントリを除き、ネイバー探索キャッシュ内のすべてのエントリを削除する例を示します。

```
Device# clear ipv6 neighbors
```

次に、静的エントリおよびVRF以外のインターフェイス上のNDキャッシュのエントリを除き、イーサネットインターフェイス0/0上のIPv6ネイバー探索キャッシュのすべてのエントリをクリアする例を示します。

```
Device# clear ipv6 neighbors interface Ethernet 0/0
```

次に、イーサネットインターフェイス0/0上の2001:0DB8:1::1のネイバー探索キャッシュのエントリをクリアする例を示します。

```
Device# clear ipv6 neighbors interface Ethernet0/0 ipv6 2001:0DB8:1::1
```

次の例では、インターフェイスイーサネット0/0がredというVRFと関連付けられています。インターフェイスのイーサネット1/0とイーサネット2/0は（VRFと関連付けられていないため）デフォルトのルーティングテーブルと関連付けられています。したがって、**clear ipv6 neighbor**コマンドはインターフェイスのイーサネット1/0とイーサネット2/0上のNDキャッシュのエントリのみをクリアします。インターフェイスイーサネット0/0上のNDキャッシュのエントリをクリアするには、**clear ipv6 neighbor vrf** redコマンドを発行する必要があります。

```
interface ethernet0/0
  vrf forward red
  ipv6 address 2001:db8:1::1/64

interface ethernet1/0
   ipv6 address 2001:db8:2::1/64

interface ethernet2/0
   ipv6 address 2001:db8:3::1/64
```

関連コマンド

コマンド	説明
ipv6neighbor	IPv6ネイバー探索キャッシュのスタティックエントリを設定します。
showipv6neighbors	IPv6ネイバー探索キャッシュ情報を表示します。

clear ipv6 nhrp

Next Hop Resolution Protocol（NHRP）キャッシュからすべてのダイナミック エントリをクリアするには、特権 EXEC モードで **clearipv6nhrp** コマンドを使用します。

clear ipv6 nhrp [{*ipv6-address*|**counters**}]

構文の説明

ipv6-address	（任意）削除する IPv6 ネットワーク。
counters	（任意）削除する NHRP カウンタを指定します。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

このコマンドでは、静的（設定済み）IPv6から非ブロードキャストマルチアクセス（NBMA）アドレスへのマッピングを NHRP キャッシュからクリアしません。

例

次に、インターフェイスの NHRP キャッシュからすべてのダイナミック エントリをクリアする例を示します。

```
Device# clear ipv6 nhrp
```

関連コマンド

コマンド	説明
showipv6nhrp	NHRP キャッシュを表示します。

clear ipv6 ospf

Open Shortest Path First（OSPF）ルーティング プロセス ID に基づく OSPF 状態をクリアするには、特権 EXEC モードで **cl earipv6ospf** コマンドを使用します。

clear ipv6 ospf [*process-id*] {**process**|**force-spf**|**redistribution**}

構文の説明

process-id	（任意）内部ID。ローカルで割り当てられ、任意の正の整数を使用できます。ここで使用される数は、OSPF ルーティング プロセスをイネーブルにするときに管理目的で割り当てられた数です。
process	OSPF プロセスを再起動します。
force-spf	最初にOSPFデータベースをクリアせずに、最短パス優先（SPF）アルゴリズムを起動します。
redistribution	OSPF ルート再配布をクリアします。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

process キーワードを **clearipv6ospf** コマンドで使用すると、OSPF データベースはいったんクリアされてから再入力された後、最短パス優先（SPF）アルゴリズムが実行されます。**force-spf** キーワードを **clearipv6ospf** コマンドで使用すると、SPF アルゴリズムが実行される前に OSPF データベースはクリアされません。

1 つの OSPF プロセスのみをクリアするには、*process-id* オプションを使用します。*process-id* オプションを指定しなかった場合、すべての OSPF プロセスがクリアされます。

例

次に、OSPFデータベースをクルアせずにSPFアルゴリズムを起動する例を示します。

```
Device# clear ipv6 ospf force-spf
```

clear ipv6 ospf counters

Open Shortest Path First（OSPF）ルーティング プロセス ID に基づく OSPF 状態をクリアするには、特権 EXEC モードで **cl earipv6ospf** コマンドを使用します。

clear ipv6 ospf [*process-id*] **counters** [**neighbor** [{*neighbor-interfaceneighbor-id*}]]

構文の説明

process-id	（任意）内部 ID。ローカルで割り当てられ、任意の正の整数を使用できます。ここで使用される数は、OSPFルーティングプロセスをイネーブルにするときに管理目的で割り当てられた数です。
neighbor	（任意）インターフェイスごとまたはネイバー ID ごとのネイバー統計。
neighbor-interface	（任意）ネイバー インターフェイス。
neighbor-id	（任意）ネイバーの IPv6 アドレスまたは IP アドレス。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

指定したインターフェイス上のすべてのネイバーのカウンタをクリアするには、**neighbor** *neighbor-interface* オプションを使用します。**neighbor** *neighbor-interface* オプションを使用しないと、すべての OSPF カウンタがクリアされます。

指定したネイバーのカウンタをクリアするには、**neighbor** *neighbor-id* オプションを使用します。**neighbor** *neighbor-id* オプション を使用しないと、すべての OSPF カウンタがクリアされます。

例

次に、ネイバー ルータに関する詳細情報を表示する例を示します。

```
Device# show ipv6 ospf neighbor detail
 Neighbor 10.0.0.1
    In the area 1 via interface Serial19/0
    Neighbor:interface-id 21, link-local address FE80::A8BB:CCFF:FE00:6F00
    Neighbor priority is 1, State is FULL, 6 state changes
    Options is 0x194AE05
    Dead timer due in 00:00:37
    Neighbor is up for 00:00:15
    Index 1/1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

次に、指定したインターフェイス上のすべてのネイバーをクリアする例を示します。

```
Device# clear ipv6 ospf counters neighbor s19/0
```

次の例は、**clearipv6ospfcountersneighbors19/0** コマンドを使用して以来状態変化がないことを示しています。

```
Device# show ipv6 ospf neighbor detail
 Neighbor 10.0.0.1
    In the area 1 via interface Serial19/0
    Neighbor:interface-id 21, link-local address FE80::A8BB:CCFF:FE00:6F00
    Neighbor priority is 1, State is FULL, 0 state changes
    Options is 0x194AE05
    Dead timer due in 00:00:39
    Neighbor is up for 00:00:43
    Index 1/1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

関連コマンド

コマンド	説明
showipv6ospfneighbor	OSPF ネイバー情報をインターフェイスごとに表示します。

clear ipv6 ospf events

Open Shortest Path First（OSPF）ルーティング プロセス ID に基づく IPv6 イベント ログ カウンタの OSPF をクリアするには、特権 EXEC モードで **cl earipv6ospfevents** コマンドを使用します。

clear ipv6 ospf [*process-id*] **events**

構文の説明

process-id	（任意）内部ID。ローカルで割り当てられ、任意の正の整数を使用できます。ここで使用される数は、OSPF ルーティング プロセスをイネーブルにするときに管理目的で割り当てられた数です。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

指定した OSPF ルーティング プロセスの IPv6 イベント ログ カウンタをクリアするには、任意の *process-id* 引数を使用します。*process-id* 引数を使用しなかった場合は、すべてのイベント ログ カウンタがクリアされます。

例

次に、ルーティング プロセス 1 の IPv6 イベント ログ カウンタの OSPF をクリアする例を示します。

```
Device# clear ipv6 ospf 1 events
```

clear ipv6 pim reset

トポロジ テーブルからすべてのエントリを削除し、マルチキャスト ルーティング情報ベース（MRIB）接続をリセットするには、特権 EXEC モードで **clearipv6pimreset** コマンドを使用します。

clear ipv6 pim [**vrf** *vrf-name*] **reset**

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

clearipv6pimreset コマンドを使用すると、PIM-MRIB 接続が切断され、トポロジ テーブルがクリアされてから PIM-MRIB 接続が再確立されます。このプロシージャは MRIB を強制的に再同期します。

⚠

注意 **clearipv6pimreset** コマンドは PIM トポロジ テーブルからすべての PIM プロトコル情報をクリアするため、使用する際は注意が必要です。**clearipv6pimreset** コマンドは、PIM と MRIB の通信が正常に動作しない場合に使用してください。

例

次に、トポロジ テーブルからすべてのエントリを削除し、MRIB 接続をリセットする例を示します。

```
Device# clear ipv6 pim reset
```

clear ipv6 pim topology

Protocol Independent Multicast（PIM）トポロジ テーブルをクリアするには、特権 EXEC モードで **clearipv6pimtopology** コマンドを使用します。

clear ipv6 pim [**vrf** *vrf-name*] **topology** [{*group-namegroup-address*}]

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
group-name | *group-address*	（任意）マルチキャスト グループの IPv6 アドレスまたは名前。

コマンド デフォルト

引数を指定しないでこのコマンドを使用すると、PIM トポロジテーブルにあるすべてのグループ エントリから PIM プロトコル情報がクリアされます。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、PIM トポロジ テーブルにあるすべてのグループ エントリから PIM プロトコル 情報をクリアします。MRIB テーブルから取得した情報は保持されます。マルチキャスト グループを指定した場合は、それらのグループ エントリだけがクリアされます。

例

次に、PIM トポロジテーブルにあるすべてのグループエントリをクリアする例を示します。

```
Device# clear ipv6 pim topology
```

clear ipv6 pim traffic

Protocol Independent Multicast（PIM）トラフィック カウンタをクリアするには、特権 EXEC モードで **clearipv6pimtraffic** コマンドを使用します。

clear ipv6 pim [**vrf** *vrf-name*] **traffic**

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。

コマンド デフォルト

引数なしでこのコマンドを使用すると、すべてのトラフィック カウンタがクリアされます。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、PIM トラフィック カウンタをクリアします。**vrf** キーワードと *vrf-name* 引数を使用すると、それらのカウンタのみがクリアされます。

例

次に、すべての PIM トラフィック カウンタをクリアする例を示します。

```
Device# clear ipv6 pim traffic
```

clear ipv6 prefix-list

IPv6プレフィックス リストのエントリのヒット カウントをリセットするには、特権EXECモードで **clearipv6prefix-list** コマンドを使用します。

clear ipv6 prefix-list [*prefix-list-name*] [*ipv6-prefix/prefix-length*]

構文の説明

prefix-list-name	（任意）ヒット カウントをクリアするプレフィックス リストの名前。
ipv6-prefix	（任意）ヒット カウントをクリアする 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*	（オプション）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

すべての IPv6 プレフィックス リストのヒット カウントがクリアされます。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

clearipv6prefix-list コマンドは、IPv6 に固有であることを除き、**clearipprefix-list** コマンドと同様です。

ヒット カウントは、特定のプレフィックス リスト エントリに一致する数を示す値です。

例

次に、ネットワーク マスク 2001:0DB8::/35 に一致する first_list というプレフィックス リストのプレフィックス リスト エントリからヒット カウントをクリアする例を示します。

```
Device# clear ipv6 prefix-list first_list 2001:0DB8::/35
```

関連コマンド

コマンド	説明
ipv6prefix-list	IPv6 プレフィックス リストのエントリを作成します。
ipv6prefix-listsequence-number	IPv6 プレフィックス リスト内のエントリのシーケンス番号の生成を有効にします。

コマンド	説明
showipv6prefix-list	IPv6 プレフィックス リストまたはプレフィックス リストのエントリに関する情報を表示します。

clear ipv6 rip

Routing Information Protocol（RIP）ルーティング テーブルからルートを削除するには、特権 EXEC モードで **clearipv6rip** コマンドを使用します。

clear ipv6 rip ［*name*］［**vrf** *vrf-name*］

clear ipv6 rip ［*name*］

構文の説明

name	（任意）IPv6 RIP プロセスの名前。
vrf *vrf-name*	（任意）指定した Virtual Routing and Forwarding（VRF）インスタンスに関する情報をクリアします。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

name 引数を指定すると、指定した IPv6 RIP プロセスのルートのみが IPv6 RIP ルーティング テーブルから削除されます。*name* 引数を指定しないと、すべての IPv6 RIP ルートが削除されます。

IPv6 RIP ルートを表示するには、**showipv6rip** コマンドを使用します。

指定した IPv6 RIP プロセスの指定した VRF インスタンスを削除するには、**clearipv6rip** *name* **vrf** *vrf-name* コマンドを使用します。

例

次に、one という RIP プロセスのすべての IPv6 ルートを削除する例を示します。

```
Device# clear ipv6 rip one
```

次に、one という RIP プロセスの vrf1 という IPv6 VRF インスタンスを削除する例を示します。

```
Device# clear ipv6 rip one vrf vrf1

*Mar 15 12:36:17.022: RIPng: Deleting 2001:DB8::/32
*Mar 15 12:36:17.022: [Exec]IPv6RT[vrf1]: rip <name>, Delete all next-hops for 2001:DB8::1
*Mar 15 12:36:17.022: [Exec]IPv6RT[vrf1]: rip <name>, Delete 2001:DB8::1 from table
*Mar 15 12:36:17.022: [IPv6 RIB Event Handler]IPv6RT[<red>]: Event: 2001:DB8::1, Del,
owner rip, previous None
```

関連コマンド

コマンド	説明
debugipv6rip	IPv6 RIP ルーティング テーブルの現在の内容を表示します。
ipv6 rip vrf-mode enable	IPv6 RIP の VRF 認識型サポートを有効にします。
showipv6rip	IPv6 RIP ルーティング テーブルの現在の内容を表示します。

clear ipv6 route

IPv6 ルーティング テーブルからルートを削除するには、特権 EXEC モードで **clearipv6route** コマンドを使用します。

{**clear ipv6 route** {*ipv6-addressipv6-prefix/prefix-length*}|*****}

構文の説明

ipv6-address	テーブルから削除する IPv6 ネットワーク 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。
ipv6-prefix	テーブルから削除する IPv6 ネットワーク番号。 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。
*	すべての IPv6 ルートをクリアします。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

clearipv6route コマンドは、IPv6 に固有であることを除き、**cleariproute** コマンドと同様です。

ipv6-address 引数または *ipv6-prefix*/ *prefix-length* 引数を指定した場合は、IPv6 ルーティングテーブルからそのルートが削除されます。***** キーワードを指定した場合は、すべてのルートがルーティング テーブルから削除されます（宛て先単位の最大伝送単位（MTU）キャッシュもクリアされます）。

例

次に、IPv6 ネットワーク 2001:0DB8::/35 を削除する例を示します。

```
Device# clear ipv6 route 2001:0DB8::/35
```

関連コマンド

コマンド	説明
ipv6route	スタティック IPv6 ルートを確立します。

コマンド	説明
showipv6route	IPv6 ルーティング テーブルの現在の内容を表示します。

clear ipv6 spd

最新の選択的パケット廃棄（SPD）の状態遷移をクリアするには、特権 EXEC モードで **clearipv6spd** コマンドを使用します。

clear ipv6 spd

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 モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

clearipv6spd コマンドは、最新の SPD 状態遷移と傾向履歴データを削除します。

例

次に、最新の SPD 状態遷移をクリアする例を示します。

```
Device# clear ipv6 spd
```

clear ipv6 traffic

IPv6 トラフィック カウンタをリセットするには、特権 EXEC モードで **clearipv6traffic** コマンドを使用します。

clear ipv6 traffic [*interface-type interface-number*]

構文の説明

interface-type interface-number	インターフェイスのタイプと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 モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、**showipv6traffic** コマンドの出力内のカウンタをリセットします。

例

次に、IPv6 トラフィック カウンタをリセットする例を示します。**showipv6traffic** コマンドの出力にはカウンタがリセットされたことが示されます。

```
Device# clear ipv6 traffic
Device# show ipv6 traffic
IPv6 statistics:
  Rcvd:  1 total, 1 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  1 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 0 received, 0 sent
ICMP statistics:
  Rcvd: 1 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 1 neighbor advert
Sent: 1 output
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
```

```
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 1 neighbor advert
UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 0 output
TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted
```

関連コマンド

コマンド	説明
showipv6traffic	IPv6 トラフィックの統計情報を表示します。

clear ipv6 wccp

特定のサービスのルータに保存されている IPv6 Web Cache Communication Protocol（WCCP）の統計（カウント）を削除するには、特権 EXEC モードで **clearipv6wccp** コマンドを使用します。

```
clear ipv6 wccp[{vrf vrf-name}][{service-number}][{web-cache}][{デフォルト}]
```

構文の説明

vrf *vrf-name*	（任意）特定の Virtual Routing and Forwarding（VRF）インスタンスの統計情報を削除するようにルータに指示します。
service-number	（任意）削除するキャッシュ サービスの数。番号は、0 ～ 254 です。
web-cache	（任意）Web キャッシュ サービスの統計情報を削除するようにルータに指示します。
default	（任意）デフォルトのルーティング テーブルの統計情報を削除するようにルータに指示します。

コマンド デフォルト

WCCP の統計情報は削除されません。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

WCCP の統計情報を表示するには、**showipv6wccp** コマンドと **showipv6wccpdetail** コマンドを使用します。シスコのキャッシュ エンジンをサービス グループで使用する場合、リバース プロキシ サービスは値 99 で指定されます。

すべての VRF のすべての WCCP サービス用の WCCP のカウンタをクリアするには、**clearipv6wccp** コマンドを使用します。

例

次の例では、Web キャッシュ サービスに関連付けられたすべての統計情報をクリアする方法を示します。

```
Device# clear ipv6 wccp web-cache
```

関連コマンド

コマンド	説明
ipv6wccp	サービス グループに参加できるように、指定した WCCP サービスのサポートをイネーブルにします。
showipv6wccp	WCCP に関連するグローバル統計情報を表示します。

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**ipv6access-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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

ipv6access-list コマンドは、IPv6 に固有であることを除き、**ipaccess-list** コマンドと同様です。

標準的な IPv6 ACL 機能は、送信元アドレスと宛て先アドレスに基づくトラフィック フィルタリングの他に、IPv6 オプション ヘッダーに基づくトラフィックのフィルタリングと、より詳細な制御を行うための任意の上位層プロトコル情報のフィルタリング（IPv4 での拡張 ACL と同様な機能）をサポートしています。IPv6 ACL は、グローバル コンフィギュレーション モードで**ipv6access-list** コマンドを使用して定義し、それらの許可と拒否の条件はIPv6アクセス リスト コンフィギュレーション モードで **deny** コマンドと **permit** コマンドを使用して設定します。**ipv6access-list** コマンドを設定すると、デバイスはIPv6アクセス リスト コンフィギュレーション モードになり、デバイス プロンプトは 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。

後位互換性を得るため、グローバル コンフィギュレーション モードでの **ipv6access-list** コマンドと **deny** キーワードおよび **permit** キーワードの組み合わせは現在もサポートされていますが、グローバル コンフィギュレーション モードでの deny 条件と permit 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 タイプ情報に基づく IPv6 トラフィックのフィルタリングの詳細については、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） すべての IPv6 ACL には、最終一致条件として、暗黙の **permiticmpanyanynd-na**、**permiticmpanyanynd-ns** および **denyipv6anyany** の各ステートメントがあります（前の 2 つの一致条件は、ICMPv6 ネイバー探索を許可します）。1 つの IPv6 ACL には、暗黙の **denyipv6anyany** 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ている必要があります。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 **ipv6traffic-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。IPv6 ACL をデバイスとの着信および発信 IPv6 仮想端末接続に適用するには、*access-list-name* 引数を指定して、**ipv6access-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） **ipv6traffic-filter** コマンドでインターフェイスに適用される IPv6 ACL は、デバイスによって発信されたトラフィックではなく、転送されたトラフィックをフィルタ処理します。

（注） このコマンドを使用して、ブートストラップ ルータ（BSR）の候補のランデブー ポイント（RP）（**ipv6pimbsrcandidaterp** コマンドを参照）または静的 RP（**ipv6pimrp-address** コマンドを参照）とすでに関連付けられている ACL を変更する場合は、PIM SSM グループ アドレスの範囲（FF3x::/96）と重複している、追加し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、重複しているアドレス範囲は ACL に追加されますが、それらは設定した BSR の候補の RP や静的 RP のコマンドの操作には影響を与えません。

重複する remark ステートメントは IPv6 アクセス コントロール リストからは設定できなくなりました。各 remark ステートメントは個別のエンティティであるため、それぞれが固有であることが必要です。

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での例を示します。次に、list1 という名前の IPv6 ACL 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 モードにする例を示します。

```
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 での例を示します。この例では、list2 という IPv6 ACL を設定し、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 番目の 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
```

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に同じ設定が入力されていた場合、その設定は次のように 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 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 **permitanyany** ステートメントおよび **denyanyany** ステートメントでプロトコル タイプとして自動的に設定されます。

（注） 暗黙の deny 条件に依存しているか、またはトラフィックをフィルタ処理するために **denyanyany** ステートメントを指定した 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 を実行しているデバイスに定義されている IPv6 ACL には、プロトコル パケット（Neighbor Discovery Protocol に関連付けられたパケットなど）のフィルタリングを回避するためのリンクローカルとマルチキャスト アドレスの **permit** ステートメントを含める必要があります。さらに、**deny** ステートメントを使用してトラフィックをフィルタ処理する IPv6 ACL では、**permitanyany** ステートメントをリスト内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、送信元アドレスまたは宛て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、パケットの宛て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。
ipv6access-class	IPv6アクセスリストに基づいて、デバイスとの間の着信接続と発信接続をフィルタ処理します。
ipv6pimbsrcandidaterp	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。
ipv6pimrp-address	特定のグループ範囲の PIM RP のアドレスを設定します。
ipv6traffic-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。
showipv6access-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 cef

Cisco Express Forwarding for IPv6 を有効にするには、グローバル コンフィギュレーション モードで **ipv6cef** コマンドを使用します。Cisco Express Forwarding for IPv6 を無効にするには、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

デフォルトでは、Cisco Express Forwarding for IPv6 は無効になっています。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

ipv6cef コマンドは、IPv6 に固有であることを除き、**ipcef** コマンドと同様です。

ipv6cef コマンドは Cisco 12000 シリーズのインターネット ルータでは利用できません。これは、Distributed Cisco Express Forwarding for IPv6 モードでのみこの分散型プラットフォームが動作するためです。

（注） **ipv6cef** コマンドはインターフェイス コンフィギュレーション モードではサポートされていません。

（注） 一部の分散アーキテクチャ プラットフォームで、Cisco Express Forwarding for IPv6 と Distributed Cisco Express Forwarding for IPv6 の両方がサポートされています。分散型プラットフォーム上に Cisco Express Forwarding for IPv6 が設定されている場合、Cisco Express Forwarding スイッチングがルート プロセッサ（RP）によって実行されます。

（注） **ipv6cef** 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 を有効にする前に、**ipcef** 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 を有効にする必要があります。

Cisco Express Forwarding for IPv6 は、Cisco Express Forwarding for IPv4 と同様に機能し、同じメリットを提供する高度なレイヤ 3 スイッチング テクノロジーです。Cisco Express Forwarding for IPv6 は、Web ベース アプリケーションやインタラクティブ セッションに関連付けられている、ダイナミックでトポロジ的に分散されたトラフィック パターンを使用して、ネットワークのパフォーマンスと拡張性を最適化します。

例

次に、標準的な Cisco Express Forwarding for IPv4 の動作を有効にしてから、標準的な Cisco Express Forwarding for IPv6 の動作を Device 上でグローバルに有効にする例を示します。

```
ip cef
Device(config)# ipv6 cef
```

関連コマンド

コマンド	説明
iproute-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。
ipv6cefaccounting	Cisco Express Forwarding for IPv6 と Distributed Cisco Express Forwarding for IPv6 のネットワーク アカウンティングを有効にします。
ipv6cefdistributed	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。
showcef	ラインカードがドロップしたパケットを表示し、高速伝送されなかったパケットを表示します。
showipv6cef	IPv6 FIB 内のエントリを表示します。

ipv6 cef accounting

Cisco Express Forwarding for IPv6 と Distributed Cisco Express Forwarding for IPv6 のネットワーク アカウンティング有効にするには、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 **ipv6cefaccounting** 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 を無効にするには、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*

インターフェイス コンフィギュレーション モードを介した特定の Cisco Express Forwarding アカウンティング情報
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 1 つ以上で置換する必要があります。必要に応じて、他のキーワードのいずれかまたは全部をこのキーワードに続けることはできますが、各キーワードを使用できるのは 1 回のみです。 • **load-balance-hash**：ロードバランシング ハッシュ バケット カウンタを有効にします。 • **non-recursive**：非再帰的なプレフィックスを介したアカウンティングを有効にします。 • **per-prefix**：宛て先（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有効にします。 • **prefix-length**：プレフィックス長を介したアカウンティングを有効にします。
non-recursive	非再帰的なプレフィックスを介したアカウンティングを有効にします。 このキーワードは、別のキーワードを入力した後に、必要に応じてグローバル コンフィギュレーション モードで使用します。*accounting-types* 引数を参照してください。
external	非再帰的な外部ビン内の入力トラフィックをカウントします。
internal	非再帰的な内部ビン内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

デフォルトでは、Cisco Express Forwarding for IPv6 のネットワーク アカウンティングは無効になっています。

コマンド モード

グローバル コンフィギュレーション

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

ipv6cefaccounting コマンドは、IPv6 に固有であることを除き、**ipcefaccounting** コマンドと同様です。

Configuring 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、ネットワーク内の IPv6 トラフィック パターンについて Cisco Express Forwarding の統計情報を収集できます。

ipv6cefaccounting コマンドをグローバル コンフィギュレーション モードで使用して Cisco Express Forwarding for IPv6 のネットワーク アカウンティングを有効にすると、Cisco Express Forwarding for IPv6 モードが有効になっている場合のルート プロセッサ（RP）と、Distributed Cisco Express Forwarding for IPv6 が有効になっている場合のラインカードでアカウンティング情報が収集されます。**showipv6cef** EXEC コマンドを使用すると、収集されたアカウンティング情報を表示できます。

直接接続されたネクスト ホップがあるプレフィックスの場合、**non-recursive** キーワードはプレフィックスを介したパケットとバイトのコレクションの高速伝送を可能にします。**ipv6cefaccounting** コマンドに別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 モードでこのコマンドをしようする場合、このキーワードはオプションです。

インターフェイス コンフィギュレーション モードでは、このコマンドをグローバル コンフィギュレーション コマンドと併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、統計情報の累積に 2 つの異なるビン（内部または外部）を指定できます。デフォルトでは、内部ビンが使用されます。統計情報は **showipv6cefdetail** コマンドを介して表示されます。

宛て先ごとのロードバランシングでは、一連の利用可能パスが分散している一連の 16 ハッシュ バケットを使用します。使用するパスが含まれているバケットを選択するには、パケットの特定のプロパティで動作するハッシュ関数を適用します。送信元と宛先の IP アドレスは、宛て先ごとのロード バランシング用のバケットを選択するために使用するプロパティです。ハッシュバケットごとのカウンタを有効にするには、**load-balance-hash** キーワードと **ipv6cefaccounting** コマンドを使用します。ハッシュバケットごとのカウンタを表示するには、**showipv6cef** *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に IPv6 アカウンティング情報の収集を有効にする例を示します。

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

関連コマンド

コマンド	説明
ipcefaccounting	Cisco Express Forwarding ネットワーク アカウンティング（IPv4 の場合）を有効にします。
showcef	Cisco Express Forwarding によって転送されたパケットに関する情報を表示します。
showipv6cef	IPv6 FIB 内のエントリを表示します。

ipv6 cef distributed

Distributed Cisco Express Forwarding for IPv6 を有効にするには、グローバル コンフィギュレーション モードで **ipv6cefdistributed** コマンドを使用します。Cisco Express Forwarding for IPv6 を無効にするには、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

デフォルトでは、Distributed Cisco Express Forwarding for IPv6 は無効になっています。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

ipv6cefdistributed コマンドは、IPv6 に固有であることを除き、**ipcefdistributed** コマンドと同様です。

ipv6cefdistributed をグローバル コンフィギュレーション モードで使用し、Distributed Cisco Express Forwarding for IPv6 をルータでグローバルに有効にすると、IPv6 パケットの Cisco Express Forwarding 処理をルート プロセッサ（RP）から分散型アーキテクチャのプラットフォームのライン カードに配信します。

（注） ルータ上で Distributed Cisco Express Forwarding IPv6 トラフィックを転送するには、**ipv6unicast-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上に IPv6 ユニキャスト データグラムをグローバルに設定し、**ipv6address** インターフェイス コンフィギュレーション コマンドを使用してインターフェイス上に IPv6 アドレスと IPv6 処理を設定します。

（注） Distributed Cisco Express Forwarding for IPv4 は、**ipv6cefdistributed** 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 Distributed Cisco Express Forwarding for IPv6 を有効にする前に、**ipcefdistributed** 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有効にする必要があります。

Cisco Express Forwarding は、高度なレイヤ 3 IP スイッチング テクノロジーです。Cisco Express Forwarding は、Web ベース アプリケーションとインタラクティブ セッションに関連付けられ

ているダイナミックで、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と拡張性を最適化します。

例

次に、Distributed Cisco Express Forwarding for IPv6 動作を有効にする例を示します。

```
ipv6 cef distributed
```

関連コマンド

コマンド	説明
iproute-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。
showipv6cef	IPv6 FIB 内のエントリを表示します。

ipv6 cef load-sharing algorithm

Cisco Express Forwarding ロード バランシング アルゴリズムを IPv6 に選択するには、グローバル コンフィギュレーション モードで **ipv6cefload-sharingalgorithm** コマンドを使用します。デフォルトのユニバーサル ロードバランシング アルゴリズムに戻るには、このコマンドの **no** 形式を使用します。

ipv6 cef load-sharing algorithm {**original**|**universal** [*id*]|**include-ports** {**source** [*id*]|**[destination]** [*id*]|**source** [*id*] **destination** [*id*] **gtp**}}
no ipv6 cef load-sharing algorithm

構文の説明

original	送信元および宛て先のハッシュに基づいて、ロードバランス アルゴリズムを元のアルゴリズムに設定します。
universal	送信元ハッシュ、宛て先ハッシュ、ID ハッシュを使用するユニバーサル アルゴリズムに、ロードバランシング アルゴリズムを設定します。
id	（任意）16 進数形式の固定識別子。
include-portssource	ロードバランシング アルゴリズムを、レイヤ 4 送信元ポートを使用するポート番号包含アルゴリズムに設定します。
include-portsdestination	ロードバランシング アルゴリズムを、レイヤ 4 宛て先ポートを使用するポート番号包含アルゴリズムに設定します。
include-portssourcedestination	ロードバランシング アルゴリズムを、レイヤ 4 送信元ポートおよび宛て先ポートを使用するポート番号包含アルゴリズムに設定します。
include-portssourcedestination gtp	GTP-U パケットに GPRS Tunneling Protocol トンネル エンドポイント識別子（GTP TEID）に基づくロード バランシング アルゴリズムを設定します。 GTP-U 以外のパケットにレイヤ 4 送信元ポートおよび宛て先ポートに基づくロード バランシング アルゴリズムを設定します。

コマンド デフォルト

ユニバーサル ロードバランシング アルゴリズムが選択されています。ロードバランシング アルゴリズムに固定識別子を設定しなかった場合、ルータは固有 ID を自動的に生成します。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

ipv6cefload-sharingalgorithm コマンドは、IPv6 に固有であることを除き、**ipcefload-sharingalgorithm** コマンドと同様です。

Cisco Express Forwarding for IPv6 のロードバランシング アルゴリズムはユニバーサル モードに設定され、ネットワーク上の各ルータは送信元アドレスと宛て先アドレスのペアごとに異なるロード共有を決定できます。

インクルード ポート アルゴリズムでは、ロード バランシングの判断の一部として、レイヤ 4 の発信元および宛先ポートを使用できます。この方法は、リアルタイム プロトコル（RTP）ストリームなど、トラフィックの大半が異なるポート番号を使用するピア アドレス間のものであるという理由で、ロード シェアリングされていない同コストのパスを通るトラフィック ストリームに効果があります。

例

次に、Cisco Express Forwarding の IPv6 用のロード バランシング アルゴリズムをレイヤ 4 の送信元ポートと宛て先ポートに対して有効にする例を示します。

```
Router(config)# ipv6 cef load-sharing algorithm include-ports source destination
```

ルータは、アルゴリズムに固定 ID を自動的に生成します。

次に、GTP TEID に基づく IPv6 CEF ロードバランシング アルゴリズムを有効にする例を示します。

```
configure terminal
!
 ipv6 cef load-sharing algorithm include-ports source destination gtp
 exit
```

関連コマンド

コマンド	説明
debugipv6cefhash	Cisco Express Forwarding for IPv6 と Distributed Cisco Express Forwarding for IPv6 のロード共有ハッシュ アルゴリズム イベントのデバック メッセージを表示します。
ipcefload-sharingalgorithm	Cisco Express Forwarding のロードバランシング アルゴリズムを選択します（IPv4 の場合）。

ipv6 cef optimize neighbor resolution

Cisco Express Forwarding for IPv6 から直接接続ネイバーに対してアドレス解決を設定するには、グローバル コンフィギュレーション モードで **ipv6cefoptimizeneighborresolution** コマンドを使用します。Cisco Express Forwarding for IPv6 から直接接続ネイバーに対するアドレス解決の最適化を無効にするには、このコマンドの **no** 形式を使用します。

ipv6 cef optimize neighbor resolution
no ipv6 cef optimize neighbor resolution

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

このコマンドを設定しなかった場合、Cisco Express Forwarding for IPv6 は直接接続ネイバーのアドレス解決を最適化しません。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

ipv6cefoptimizeneighborresolution コマンドは、IPv6 に固有であることを除き、**ip cefoptimizeneighborresolution** コマンドと極めて類似しています。

このコマンドを使用して、直接 Cisco Express Forwarding for IPv6 からネイバーのレイヤ 2 アドレス解決をトリガーします。

例

次に、Cisco Express Forwarding for IPv6 から直接接続ネイバーに対してアドレス解決を最適化する例を示します。

```
Device(config)# ipv6 cef optimize neighbor resolution
```

関連コマンド

コマンド	説明
ipcefoptimizeneighborresolution	Cisco Express Forwarding for IPv4 からの直接接続ネイバーに対するアドレス解決の最適化を設定します。

ipv6 destination-guard policy

宛て先ガード ポリシーを定義するには、グローバル コンフィギュレーション モードで **ipv6destination-guardpolicy** コマンドを使用します。宛て先ガード 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 destination-guard policy [*policy-name*]
no ipv6 destination-guard policy [*policy-name*]

構文の説明

policy-name	（任意）宛て先ガードポリシーの名前。

コマンド デフォルト

宛て先ガード ポリシーは定義されません。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

このコマンドを実行すると、宛て先ガード コンフィギュレーション モードが開始されます。宛て先ガード ポリシーは、宛て先アドレスに基づいて IPv6 トラフィックをフィルタ処理し、不明な送信元からのデータ トラフィックをブロックするのに使用できます。

例

次に、宛て先ガード ポリシーの名前を定義する例を示します。

```
Device> enable
Device# configure terminalDevice(config)# ipv6 destination-guard policy
policy1Device(config-destguard)#
```

関連コマンド

コマンド	説明
showipv6destination-guard policy	宛て先ガード情報を表示します。

ipv6 dhcp-relay bulk-lease

bulk lease クエリ パラメータを設定するには、グローバル コンフィギュレーション モードで **ipv6dhcp-relaybulk-lease** コマンドを使用します。bulk lease クエリ設定を削除するには、このコマンドの **no** 形式を使用します。

ipv6 dhcp-relay bulk-lease {**data-timeout** *seconds*|**retry** *number*} **[disable]**
no ipv6 dhcp-relay bulk-lease [disable]

構文の説明

data-timeout	（任意）bulk lease クエリ データ転送のタイムアウト。
seconds	（任意）範囲は 60 ～ 600 秒です。デフォルトは 300 秒です。
retry	（任意）bulk lease クエリの再試行回数を設定します。
number	（任意）範囲は 0 ～ 5 です。デフォルトは 5 分です。
disable	（任意）DHCPv6 bulk lease クエリ機能を無効にします。

コマンド デフォルト

bulk lease クエリは、DHCP for IPv6（DHCPv6）リレー エージェント機能が有効になっている場合は自動的に有効になります。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

データ転送のタイムアウトや bulk lease TCP 接続の試行回数などの bulk lease クエリ パラメータを設定するには、グローバル コンフィギュレーション モードで **ipv6dhcp-relaybulk-lease** コマンドを使用します。

DHCPv6 リレー エージェントが有効になっている場合、DHCPv6 bulk lease クエリ機能は自動的に有効になります。この機能を使用して DHCPv6 bulk lease クエリ機能自体を有効にすることはできません。この機能を無効にするには、**ipv6dhcp-relaybulk-lease** コマンドと **disable** キーワードを使用します。

例

次に、bulk lease クエリ データ転送のタイムアウトを 60 秒に設定する例を示します。

```
Device(config)# ipv6 dhcp-relay bulk-lease data-timeout 60
```

ipv6 dhcp-relay option vpn

DHCP for IPv6 リレーの VRF 認識型機能を有効にするには、グローバル コンフィギュレーション モードで ipv6 dhcp-relay オプション vpn コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

ipv6 dhcp-relay option vpn
no ipv6 dhcp-relay option vpn

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

DHCP for IPv6 リレーの VRF 認識型機能はルータ上では有効になりません。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

ipv6dhcp-relayoptionvpn コマンドは DHCPv6 リレーの VRF 認識型機能をルータ上でグローバルに有効にすることができます。**ipv6dhcprelayoptionvpn** コマンドが指定したインターフェイス上で有効になっている場合は、グローバル **ipv6dhcp-relayoptionvpn** コマンドをオーバーライドします。

例

次に、DHCPv6 リレーの VRF 認識型機能をルータ上でグローバルに有効にする例を示します。

```
Device(config)# ipv6 dhcp-relay option vpn
```

関連コマンド

コマンド	説明
ipv6dhcprelayoptionvpn	インターフェイス上で DHCPv6 リレーの VRF 認識型機能を有効にします。

ipv6 dhcp-relay source-interface

メッセージをリレーする場合に送信元として使用するインターフェイスを設定するには、グローバル コンフィギュレーション モードで **ipv6dhcp-relaysource-interface** コマンドを使用します。送信元としてのインターフェイスの使用を削除するには、このコマンドの no 形式を使用します。

ipv6 dhcp-relay source-interface *interface-type interface-number*
no ipv6 dhcp-relay source-interface *interface-type interface-number*

構文の説明

interface-type interface-number	（任意）宛て先の出力インターフェイスを指定するインターフェイスのタイプと番号。この引数が設定されている場合、クライアントのメッセージは、この出力インターフェイスが接続されたリンクを経由して宛先アドレスに転送されます。

コマンド デフォルト

このサーバ側のインターフェイスのアドレスは、IPv6 リレーの送信元として使用されます。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

設定済みのインターフェイスがシャットダウンされた場合、またはその IPv6 アドレスのすべてが削除された場合、リレーは標準の動作に戻ります。

インターフェイス設定（インターフェイス コンフィギュレーション モードで **ipv6dhcprelaysource-interface** コマンドを使用）とグローバル設定の両方が設定されている場合は、インターフェイス設定はグローバル設定よりも優先されます。

例

次に、リレーの送信元として使用するループバック 0 インターフェイスを設定する例を示します。

```
Device(config)# ipv6 dhcp-relay source-interface loopback 0
```

関連コマンド

コマンド	説明
ipv6dhcprelaysource-interface	インターフェイス上で DHCP for IPv6 サービスを有効にします。

ipv6 dhcp binding track ppp

Dynamic Host Configuration Protocol（DHCP）for IPv6 を設定し、接続が閉じた時点で PPP 接続と関連付けられているバインディングを解放するには、グローバル コンフィギュレーション モードで **ipv6dhcpbindingtrackppp** コマンドを使用します。デフォルトの動作に戻すには、このコマンドの **no** 形式を使用します。

ipv6 dhcp binding track ppp
no ipv6 dhcp binding track ppp

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

PPP 接続を閉じても、その接続に関連付けられている DHCP バインディングは解放されません。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

ipv6dhcpbindingtrackppp コマンドは、PPP 接続を閉じたときにその接続と関連付けられているバインディングを自動的に解放するように DHCP for IPv6 を設定します。バインディングを自動的に解放し、十分なリソースを提供することで、後続の新しい登録に対応します。

（注） DHCPv6 を使用した IPv6 ブロードバンド展開では、このコマンドを使用して、PPP 仮想インターフェイスに関連付けられているプレフィックス バインディングを解放できるようにする必要があります。これにより、DHCPv6 バインディングが PPP セッションとともに追跡されるようになり、DHCP REBIND が失敗した場合には、クライアントが DHCPv6 ネゴシエーションを再度開始するようになります。

IPv6 用 DHCP サーバのバインディング テーブル エントリに対して、次の処理が自動的に行われます。

- コンフィギュレーション プールからプレフィックスがクライアントに委任されるたびに作成されます。
- クライアントがプレフィックスの委任を更新、再バインディング、または確認すると更新されます。
- クライアントがバインディング内のすべてのプレフィックスを自発的に解放したか、すべてのプレフィックスの有効期限が切れたとき、または管理者がアインディングをクリアしたときに削除されます。

例

次に、PPP に関連付けられているプレフィックス バインディングを解放する例を示します。

```
Device(config)# ipv6 dhcp binding track ppp
```

ipv6 dhcp database

Dynamic Host Configuration Protocol（DHCP）for IPv6 バインディング データベースを設定するには、グローバル コンフィギュレーション モードで **ipv6dhcpdatabase** コマンドを使用します。データベース エージェントを削除するには、このコマンドの **no** 形式を使用します。

ipv6 dhcp database *agent* [**write-delay** *seconds*] [**timeout** *seconds*]
no ipv6 dhcp database *agent*

構文の説明

agent	フラッシュ、ローカルブートフラッシュ、Compact Flash、NVRAM、FTP、TFTP、または Remote Copy Protocol（RCP）の Uniform Resource Locator。
write-delay *seconds*	（任意）IPv6 用 DHCP がデータベース更新を送信する頻度（秒単位）。デフォルトは 300 秒です。最小書き込み遅延は 60 秒です。
timeout *seconds*	（任意）ルータがデータベース転送を待機する時間（秒単位）。

コマンド デフォルト

書き込み遅延のデフォルト値は 300 秒です。タイムアウトのデフォルト値は 300 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

ipv6dhcpdatabase コマンドは、DHCP for IPv6 バインディング データベース エージェントのパラメータを指定します。ユーザは複数のデータベース エージェントを設定できます。

バインディング テーブルのエントリは、プレフィックスがコンフィギュレーション プールからクライアントに委任されるたびに自動的に作成され、クライアントがプレフィックス委任を更新、再バインディング、または確認すると更新されます。また、クライアントが自発的にバインディング内のすべてのプレフィックスを解放したとき、すべてのプレフィックスの有効期間が経過したとき、または管理者が clear ipv6 dhcp binding コマンドを有効にしたときに削除されます。これらのバインディングは RAM に保持され、*agent* 引数を使用して永続的なストレージに保存できます。これにより、システムのリロード後や電源切断後でも、クライアントに割り当てられたプレフィックスなどの設定に関する情報が失われなくなります。バインディングはテキスト レコードとして格納されるため、メンテナンスが容易です。

バインディング データベースが保存される永続的な各ストレージのことをデータベース エージェントと呼びます。データベース エージェントには、FTP サーバなどのリモート ホストや NVRAM などのローカル ファイル システムがあります。

write-delay キーワードは、DHCP がデータベース更新を送信する頻度を秒単位で指定します。デフォルトでは、IPv6 用 DHCP サーバは、データベース変更の送信前に 300 秒間待機します。

timeout キーワードは、ルータがデータベース転送を待機する時間を秒単位で指定します。無限は0秒として定義され、タイムアウト期間を超えた転送は中断されます。デフォルトでは、IPv6用DHCPサーバは、データベース転送の中断前に300秒間待機します。システムがリロードされる場合、バインディングテーブルが完全に保存されるように転送タイムアウトはありません。

例

次に、DHCP for IPv6 バインディング データベース エージェントのパラメータを指定し、バインディング エントリを TFTP に格納する例を示します。

```
Device(config)# ipv6 dhcp database tftp://10.0.0.1/dhcp-binding
```

次の例では、DHCP for IPv6 バインディング データベース エージェントのパラメータを指定し、バインディング エントリをブートフラッシュに格納しています。

```
Device(config)# ipv6 dhcp database bootflash
```

関連コマンド

コマンド	説明
clear ipv6 dhcp binding	DHCP for IPv6 サーバのバインディング テーブルからクライアントのバインディングを自動的に削除します。
showipv6dhcpdatabase	DHCP for IPv6 バインディング データベース エージェントの情報を表示します。

ipv6 dhcp iana-route-add

リレーまたはサーバ上に個別に割り当てられたIPv6アドレスのルートを追加するには、グローバル コンフィギュレーション モードで **ipv6 dhcp iana-route-add** コマンドを使用します。リレーまたはサーバ上に個別に割り当てられたIPv6アドレスのルートの追加を無効にするには、このコマンドの **no** 形式を使用します。

ipv6 dhcp iana-route-add
no ipv6 dhcp iana-route-add

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

デフォルトでは、リレーまたはサーバ上に個別に割り当てられた IPv6 アドレスのルートの追加は無効になっています。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、**ipv6 dhcp iana-route-add** コマンドは無効になっているため、ルートの追加が必要な場合は有効にする必要があります。アンナンバードインターフェイスを通じてクライアントがリレーまたはサーバに接続されている場合、およびこのコマンドを使用してルートの追加を有効にした場合、Internet Assigned Numbers Authority（IANA）のルートを追加することができます。

例

次に、個別に割り当てられているIPv6アドレスのルートの追加を有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 dhcp iana-route-add
```

ipv6 dhcp iapd-route-add

Dynamic Host Configuration Protocol for IPv6（DHCPv6）リレーおよびサーバによって委任プレフィックスに対してルートの追加を有効にするには、グローバル コンフィギュレーション モードで **ipv6 dhcp iapd-route-add** コマンドを使用します。ルートの追加を無効にするには、このコマンドの **no** 形式を使用します。

ipv6 dhcp iapd-route-add
no ipv6 dhcp iapd-route-add

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

デフォルトでは、DHCPv6 リレーおよびDHCPv6 サーバは委任プレフィックスのルートを追加します。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、DHCPv6 リレーおよびDHCPv6 サーバは委任プレフィックスのルートを追加します。このコマンドのルート上のプレゼンスは、ルートがそのルータに追加されるという意味ではありません。このコマンドを設定すると、委任プレフィックスのルートは最初のレイヤ 3 リレーおよびサーバ上にのみ追加されます。

例

次に、DHCPv6 リレーおよびサーバを有効にして委任プレフィックスのルートを追加する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 dhcp iapd-route-add
```

ipv6 dhcp-ldra

Lightweight DHCPv6 Relay Agent （LDRA）機能をアクセス ノードで有効にするには、グローバル コンフィギュレーション モードで **ipv6 dhcp-ldra** コマンドを使用します。LDRA 機能を無効にするには、このコマンドの **no** 形式を使用します。

ipv6 dhcp-ldra {enable | disable}
no ipv6 dhcp-ldra {enable | disable}

構文の説明

enable	アクセス ノード上でLDRA機能を有効にします。
disable	アクセス ノード上でLDRA機能を無効にします。

コマンド デフォルト

デフォルトでは、アクセス ノード上で LDRA 機能は有効になっていません。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

LDRA 機能を VLAN 上またはアクセス ノード（Digital Subscriber Link Access Multiplexer（DSLAM）またはイーサネット スイッチ）インターフェイスで設定する前に、**ipv6 dhcp-ldra** コマンドを使用して、この機能を有効にする必要があります。

例

次に、LDRA 機能を有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 dhcp-ldra enable
Device(config)# exit
```

（注） 上記の例では、デバイスはアクセス ノードとなっています。

関連コマンド

コマンド	説明
ipv6dhcpldraattach-policy	VLAN 上で LDRA 機能を有効にします。
ipv6dhcp-ldraattach-policy	インターフェイス上でLDRA機能を有効にします。

ipv6 dhcp ping packets

Dynamic Host Configuration Protocol for IPv6（DHCPv6）サーバが ping 動作の一部としてプールアドレスに送信するパケット数を指定するには、グローバル コンフィギュレーション モードで **ipv6dhcppingpackets** コマンドを使用します。サーバがプール アドレスに ping を送信しないようにするには、このコマンドの **no** 形式を使用します。

ipv6 dhcp ping packets *number*
ipv6 dhcp ping packets

構文の説明

number	アドレスが要求元のクライアントに割り当てられる前に送信された ping パケット数。有効な範囲は 0 ～ 10 です。

コマンド デフォルト

要求元のクライアントにアドレスが割り当てられるまで、ping パケットは送信されません。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

DHCPv6 サーバは、要求元クライアントにアドレスを割り当てる前にプール アドレスに ping を送信します。ping の応答がない場合、サーバはアドレスが使用されていない可能性が高いと想定し、アドレスを要求元クライアントに割り当てます。

number 引数を 0 に設定すると、DHCPv6 サーバの ping 動作がオフになります。

例

次に、ping 試行を停止するまでに DHCPv6 サーバが 4 回試行することを指定する例を示します。

```
Device(config)# ipv6 dhcp ping packets 4
```

関連コマンド

コマンド	説明
clearipv6dhcpconflict	DHCPv6 サーバ データベースからアドレス競合をクリアします。
show ipv6 dhcp conflict	DHCPv6 サーバによって検出された、またはクライアントから DECLINE メッセージにより報告されたアドレス競合を表示します。

ipv6 dhcp pool

Dynamic Host Configuration Protocol（DHCP）for IPv6 のサーバ設定情報プールを設定して DHCP for IPv6 プール 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 **ipv6dhcppool** コマンドを使用します。DHCP for IPv6 プールを削除するには、このコマンドの **no** 形式を使用します。

ipv6 dhcp pool *poolname*
no ipv6 dhcp pool *poolname*

構文の説明

poolname	ローカルなプレフィックス プールのユーザ定義名。プール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

DHCP for IPv6 プールは設定されません。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

DHCP for IPv6 サーバ設定情報プールを作成するには、**ipv6dhcppool** コマンドを使用します。**ipv6dhcppool** コマンドが有効になっている場合、コンフィギュレーション モードは DHCP for IPv6 プール コンフィギュレーション モードに変更されます。このモードでは、次のコマンドを使用して、管理者はプレフィックスが委任されるようにプール パラメータを設定し、ドメイン ネーム システム（DNS）サーバを設定できます。

- **addressprefix** *IPv6-prefix* [**lifetime** {*valid-lifetime preferred-lifetime* | **infinite**}] はアドレス割り当てにアドレス プレフィックスを設定します。このアドレスは、16 ビット値をコロンで区切った 16 進数で指定する必要があります。
- **link-address** *IPv6-prefix* はリンクアドレス IPv6 プレフィックスを設定します。着信インターフェイスのアドレスまたはパケット内のリンク アドレスが指定した IPv6 プレフィックスと一致する場合、サーバは設定情報プールを使用します。このアドレスは、16 ビット値をコロンで区切った 16 進数で指定する必要があります。
- **vendor-specific** *vendor-id* は DHCPv6 ベンダー固有のコンフィギュレーション モードを有効にします。ベンダーの識別番号を指定します。この番号は、ベンダーの IANA プライベート エンタープライズ番号です。指定できる範囲は 1 ～ 4294967295 です。次のコンフィギュレーション コマンドが利用できます。
  - **suboption** *number* はベンダー固有のサブオプション番号を設定します。指定できる範囲は 1 ～ 65535 です。IPv6 アドレス、ASCII テキスト、または 16 進文字列をサブオプション パラメータで定義されている束リに入力できます。

（注） **suboption** キーワードの下に **hex** 値を使用すると、入力できるのは 16 進数（0 ～ f）のみとなります。無効な **hex** 値を入力しても以前の設定は削除されません。

DHCP for IPv6 設定情報プールが作成されたら、**ipv6dhcpserver** コマンドを使用して、プールとインターフェイス上のサーバを関連付けます。情報プールを設定しない場合は、**ipv6dhcpserverinterface** コンフィギュレーション コマンドを使用して DHCPv6 サーバ関数をインターフェイス上で有効にする必要があります。

DHCPv6 プールとインターフェイスを関連付けると、関連付けられているインターフェイス上の要求を処理するのはそのプールだけとなります。プールは、他のインターフェイスについても処理を行います。DHCPv6 プールとインターフェイスを関連付けない場合は、すべてのインターフェイスに対する要求を処理できます。

IPv6 アドレス プレフィックスを使用しない場合、プールは設定済みのオプションのみを返します。

link-address コマンドでは、必ずしもアドレスを割り当てなくてもリンクアドレスの照合を行うことができます。プール内の複数のリンク アドレス コンフィギュレーション コマンドを使用して、複数のリレーのプールを照合できます。

アドレス プール情報またはリンク情報のいずれかについて最長一致が行われるため、あるプールについてはアドレスを割り当てるように設定して、サブプレフィックスの別のプールについては設定されたオプションだけを返すように設定できます。

例

次に、cisco1 という DHCP for IPv6 設定情報プールを指定して、ルータを DHCP for IPv6 プール コンフィギュレーション モードにする例を示します。

```
Device(config)# ipv6 dhcp pool cisco1
Device(config-dhcpv6)#
```

次に、IPv6 コンフィギュレーション プール cisco1 に IPv6 アドレス プレフィックスを設定する例を示します。

```
Device(config-dhcpv6)# address prefix 2001:1000::0/64
Device(config-dhcpv6)# end
```

次に、3 つのリンクアドレス プレフィックスと IPv6 アドレス プレフィックスを含む engineering という名前のプールを設定する例を示します。

```
Device# configure terminal
Device(config)# ipv6 dhcp pool engineering
Device(config-dhcpv6)# link-address 2001:1001::0/64Device(config-dhcpv6)# link-address
2001:1002::0/64Device(config-dhcpv6)# link-address 2001:2000::0/48Device(config-dhcpv6)#
 address prefix 2001:1003::0/64
Device(config-dhcpv6)# end
```

次に、ベンダー固有オプションを含む 350 という名前のプールを設定する例を示します。

```
Device# configure terminal
```

```
Device(config)# ipv6 dhcp pool 350
Device(config-dhcpv6)# vendor-specific 9
Device(config-dhcpv6-vs)# suboption 1 address 1000:235D::1Device(config-dhcpv6-vs)#
suboption 2 ascii "IP-Phone"
Device(config-dhcpv6-vs)# end
```

関連コマンド

コマンド	説明
ipv6dhcpserver	インターフェイス上で DHCP for IPv6 サービスを有効にします。
showipv6dhcppool	DHCP for IPv6 コンフィギュレーションプール情報を表示します。

ipv6 flow monitor

このコマンドは、着信または発信トラフィックを分析するためにインターフェイスに割り当てることで、作成済みのフロー モニタをアクティブにします。

以前に作成したフロー モニタをアクティブにするには、**ipv6flowmonitor** コマンドを使用します。フロー モニタを非アクティブにするには、このコマンドの **no** 形式を使用します。

ipv6 flow monitor *ipv6-monitor-name* [**sampler** *ipv6-sampler-name*] {**input**|**output**}
no ipv6 flow monitor *ipv6-monitor-name* [**sampler** *ipv6-sampler-name*] {**input**|**output**}

構文の説明

ipv6-monitor-name	着信または発信トラフィックを分析するためにインターフェイスに割り当てることで、作成済みのフロー モニタをアクティブにします。
sampler *ipv6-sampler-name*	フロー モニタ サンプラーを適用します。
input	入力トラフィックにフロー モニタを適用します。
output	出力トラフィックにフロー モニタを適用します。

コマンド デフォルト

IPv6 フロー モニタは、インターフェイスに割り当てられるまでアクティブになりません。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

ポート チャネル インターフェイスには NetFlow モニタを接続できません。サービス モジュールの両方のインターフェイスが EtherChannel の一部である場合、両方の物理インターフェイスに監視を接続する必要があります。

次に、フロー モニタをインターフェイスに適用する例を示します。

```
Device(config)# interface gigabitethernet 1/1/2
Device(config-if)# ip flow monitor FLOW-MONITOR-1 input
Device(config-if)# ip flow monitor FLOW-MONITOR-2 output
Device(config-if)# end
```

ipv6 dhcp server vrf enable

DHCP for IPv6 サーバの VRF 認識型機能を有効にするには、グローバル コンフィギュレーション モードで **ipv6dhcpservervrfenable** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

ipv6 dhcp server vrf enable
no ipv6 dhcp server vrf enable

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

DHCPv6 サーバの VRF 認識型機能はルータ上では有効になりません。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

ipv6dhcpserveroptionvpn コマンドは DHCPv6 サーバの VRF 認識型機能をルータ上でグローバルに有効にすることができます。

例

次に、DHCPv6 サーバの VRF 認識型機能をルータ上でグローバルに有効にする例を示します。

```
Device(config)# ipv6 dhcp server option vpn
```

ipv6 general-prefix

IPv6 の汎用プレフィックスを定義するには、グローバル コンフィギュレーション モードで **ipv6general-prefix** コマンドを使用します。IPv6 の汎用プレフィックスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 general-prefix *prefix-name* {*ipv6-prefix/prefix-length*|**6to4** *interface-type interface-number*|**6rd** *interface-type interface-number*}
no ipv6 general-prefix *prefix-name*

構文の説明

prefix-name	プレフィックスに割り当てられている名前。
ipv6-prefix	汎用プレフィックスに割り当てられている 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。 汎用プレフィックスを手動で定義する場合は、*ipv6-prefix* 引数と */prefix-length* 引数の両方を指定します。
/ 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。 汎用プレフィックスを手動で定義する場合は、*ipv6-prefix* 引数と */prefix-length* 引数の両方を指定します。
6to4	6to4 トンネリングに使用するインターフェイスに基づいて汎用プレフィックスを設定できます。 6to4 インターフェイスに基づいて汎用プレフィックスを定義する場合は、**6to4** キーワードと *interface-type interface-number* 引数を指定します。
interface-type interface-number	インターフェイスのタイプと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。 6to4 インターフェイスに基づいて汎用プレフィックスを定義する場合は、**6to4** キーワードと *interface-type interface-number* 引数を指定します。
6rd	IPv6 高速展開（6RD）トンネリングに使用するインターフェイスからキャプチャした汎用プレフィックスを設定できます。

コマンド デフォルト

汎用プレフィックスは定義されません。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

ipv6 general-prefix コマンドを使用して IPv6 汎用プレフィックスを定義します。

汎用プレフィックスには、短いプレフィックスが保持されます。このプレフィックスに基づいて、より長く詳細な複数のプレフィックスを定義できます。汎用プレフィックスが変更されると、そのプレフィックスに基づくより詳細なプレフィックスもすべて変更されます。この機能により、ネットワーク リナンバリングが大幅に簡略化され、自動化されたプレフィックス定義が可能になります。

汎用プレフィックスに基づくより詳細なプレフィックスは、インターフェイスに IPv6 を設定する場合に使用できます。

6to4 トンネリングに使用するインターフェイスに基づく汎用プレフィックスを定義する場合、汎用プレフィックスは 2002:a.b.c.d::/48 の形式になります。「a.b.c.d」は、参照されるインターフェイスの IPv4 アドレスです。

例

次に、my-prefix という IPv6 汎用プレフィックスを手動で定義する例を示します。

```
Device(config)# ipv6 general-prefix my-prefix 2001:DB8:2222::/48
```

次に、my-prefix という IPv6 汎用プレフィックスを 6to4 インターフェイスに基づいて定義する例を示します。

```
Device(config)# ipv6 general-prefix my-prefix 6to4 ethernet0
```

関連コマンド

コマンド	説明
showipv6general-prefix	IPv6アドレスの汎用プレフィックスに関する情報を表示します。

ipv6 local policy route-map

ローカル ポリシーベース ルーティング（PBR）を IPv6 パケットに有効にするには、グローバル コンフィギュレーション モードで **ipv6localpolicyroute-map** コマンドを使用します。IPv6 パケットのローカル ポリシーベース ルーティングを無効にするには、このコマンドの **no** 形式を使用します。

ipv6 local policy route-map *route-map-name*
no ipv6 local policy route-map *route-map-name*

構文の説明

route-map-name	ローカル IPv6 PBR に使用するルート マップの名前。この名前は、**route-map** コマンドで指定した *route-map-name* 値に一致している必要があります。

コマンド デフォルト

IPv6 パケットはポリシー ルーティングされません。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

通常、ルータから発信されるパケットはポリシー ルーティングされません。ただし、このようなパケットをポリシー ルーティングするには、**ipv6localpolicyroute-map** コマンドを使用します。明白な最短パス以外のルートを取るルータでパケットを発信する場合は、ローカル PBR を有効にすることができます。

ipv6localpolicyroute-map コマンドは、ローカル PBR に使用するルート マップを識別します。**route-map** コマンドのそれぞれには、それらに関連付けられた **match** コマンドと **set** コマンドのリストが備わっています。**match** コマンドは一致基準を指定します。この基準は、パケットをポリシー ルーティングする条件となります。**set** コマンドは **match** コマンドによって適用された基準が満たされている場合に実行される特定のポリシー ルーティング アクションである set アクションを指定します。**noipv6localpolicyroute-map** コマンドは、ルート マップへの参照を削除し、ローカル ポリシー ルーティングを無効にします。

例

次に、宛て先 IPv6 アドレスがアクセス リスト pbr-src-90 で許可されているアドレスに一致するパケットが IPv6 アドレス 2001:DB8::1: のルータに送信される例を示します。

```
ipv6 access-list src-90
 permit ipv6 host 2001::90 2001:1000::/64
route-map pbr-src-90 permit 10
 match ipv6 address src-90
 set ipv6 next-hop 2001:DB8::1
ipv6 local policy route-map pbr-src-90
```

関連コマンド

コマンド	説明
ipv6policyroute-map	インターフェイス上に IPv6 PBR を設定します。
matchipv6address	IPv6 の PBR でパケットの照合に使用する IPv6 アクセス リストを指定します。
matchlength	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。
route-map(IP)	あるルーティング プロトコルから別のルーティング プロトコルへルートを再配布する条件を定義するか、ポリシー ルーティングをイネーブルにします。
setdefaultinterface	ポリシー ルーティングのルート マップの match 句を満たし、宛て先までの明示的なルートを持たないパケットを出力するデフォルトのインターフェイスを指定します。
setinterface	ポリシー ルーティングのルート マップの match 句を満たしたパケットを出力するデフォルトのインターフェイスを指定します。
setipv6defaultnext-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。
setipv6next-hop(PBR)	ポリシー ルーティングのルート マップの match 句を満たした IPv6 パケットの出力先を指定します。
setipv6precedence	IPv6 パケット ヘッダーのプリファレンス値を設定します。

ipv6 local pool

ローカル IPv6 プレフィックス プールを設定するには、プレフィックスにプール名を指定した ipv6 local pool コンフィギュレーション コマンドを使用します。プールを無効にするには、このコマンドの **no** 形式を使用します。

ipv6 local pool poolname prefix/prefix-length assigned-length [shared] [**cache-size** *size*]
no ipv6 local pool poolname

構文の説明

poolname	ローカルなプレフィックス プールのユーザ定義名。
prefix	プールに割り当てられている IPv6 プレフィックス。 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*	プールに割り当てられている 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。
assigned-length	プールからユーザに割り当てられがプレフィックスの長さ（ビット単位）。*assigned-length* 引数の値は、/ *prefix-length* 引数の値未満であってはなりません。
shared	（任意）プールが共有プールであることを示します。
cache-size *size*	（任意）キャッシュのサイズを指定します。

コマンド デフォルト

プールは設定されません。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

すべてのプール名が固有である必要があります。

IPv6 プレフィックス プールには IPv4 アドレス プールに類似している関数があります。IPv4 とは対照的に、割り当てられているアドレスのブロック（アドレス プレフィックス）は単一アドレスではありません。

プレフィックス プールの重複は許可されていません。

プールが設定されたあとは、プールを変更できません。設定を変更するには、プールを削除して作成し直す必要があります。すでに割り当てられていたすべてのプレフィックスが解放されます。

例

次に、IPv6 プレフィックス プールを作成する例を示します。

```
Device(config)# ipv6 local pool pool1 2001:0DB8::/29 64
Device# show ipv6 local pool
Pool Prefix Free In use
pool1  2001:0DB8::/29  65516  20
```

関連コマンド

コマンド	説明
debugipv6pool	IPv6 プールのデバッグを有効にします。
peerdefaultipv6addresspool	クライアント プレフィックスを PPP リンクに割り当てるプールを指定します。
prefix-delegationpool	プレフィックスを IPv6 クライアントの DHCP に委任する名前付きの IPv6 ローカル プレフィックス プールを指定します。
showipv6localpool	定義済みの IPv6 アドレス プールに関する情報を表示します。

ipv6 mld snooping

マルチキャスト リスナー検出バージョン 2（MLDv2）プロトコル スヌーピングをグローバルに有効にするには、グローバル コンフィギュレーション モードで **ipv6mldsnooping** コマンドを使用します。MLDv2 スヌーピングをグローバルに無効にするには、このコマンドの **no** 形式を使用します。

ipv6 mld snooping
no ipv6 mld snooping

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

このコマンドは有効です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが Supervisor Engine 720 に導入されました。

使用上のガイドライン

MLDv2 スヌーピングは、ポリシー フィーチャ カード 3（PFC3）の何らかのバージョンが搭載された Supervisor Engine 720 でサポートされています。

MLDv2 スヌーピングを使用するには、IPv6 マルチキャスト ルーティング用のサブネットでレイヤ 3 インターフェイスを設定するか、またはサブネットで MLDv2 スヌーピング クエリアを有効にします。

例

次に、MLDv2 スヌーピングをグローバルにイネーブルにする例を示します。

```
Device(config)# ipv6 mld snooping
```

関連コマンド

コマンド	説明
showipv6mldsnooping	MLDv2 スヌーピング情報を表示します。

ipv6 mld ssm-map enable

Source Specific Multicast（SSM）マッピング機能を設定済みの SSM 範囲内にあるグループに有効にするには、グローバル コンフィギュレーション モードで **ipv6mldssm-mapenable** 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。

ipv6 mld [**vrf** *vrf-name*] **ssm-map enable**
no ipv6 mld [**vrf** *vrf-name*] **ssm-map enable**

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。

コマンド デフォルト

SSM マッピング機能は有効になりません。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

ipv6mldssm-mapenable コマンドは、設定済みの SSM 範囲内にあるグループに SSM マッピング機能を有効にします。**ipv6mldssm-mapenable** コマンドを使用すると、SSM マッピングはデフォルトでドメイン ネーム システム（DNS）を使用します。

SSM マッピングは、受信したマルチキャスト リスナー検出（MLD）バージョン 1 または MLD バージョン 2 のメンバーシップ レポートにのみ適用されます。

例

次に、SSM マッピング機能を有効にする例を示します。

```
Device(config)# ipv6 mld ssm-map enable
```

関連コマンド

コマンド	説明
debugipv6mldssm-map	SSM マッピングのデバッグ メッセージを表示します。
ipv6mldssm-mapquerydns	DNS ベースの SSM マッピングを有効にします。
ipv6mldssm-mapstatic	スタティック SSM マッピングを設定します。
showipv6mldssm-map	SSM マッピング情報を表示します。

ipv6 mld state-limit

マルチキャスト リスナー検出（MLD）の状態数をグローバルに制限するには、グローバル コンフィギュレーション モードで **ipv6mldstate-limit** コマンドを使用します。設定済みの MLD 状態の制限を無効にするには、このコマンドの **no** 形式を使用します。

ipv6 mld [**vrf** *vrf-name*] **state-limit** *number*
no ipv6 mld [**vrf** *vrf-name*] **state-limit** *number*

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
number	ルータで許可される MLD の状態の最大数。有効な範囲は 1 ～ 64000 です。

コマンド デフォルト

MLD 制限のデフォルト数は設定されません。このコマンドの設定時に、ルータ上でグローバルに許可する最大 MLD 状態数を設定する必要があります。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

MLD メンバーシップ レポートの結果の MLD 状態数の制限をグローバルに設定するには、**ipv6mldstate-limit** コマンドを使用します。設定した制限を超過した後に送信されたるメンバーシップ レポートはMLDキャッシュには入力されず、超過した分のメンバーシップ レポートのトラフィックは転送されません。

インターフェイスごとの MLD 状態の制限を設定するには、インターフェイス コンフィギュレーション モードで **ipv6mldlimit** コマンドを使用します。

インターフェイスごとの制限およびシステムごとの制限はそれぞれ個別に機能し、設定済みのさまざまな制限を適用できます。メンバーシップの状態は、インターフェイスごとの制限またはグローバル制限のいずれかを超過した場合は無視されます。

例

次に、ルータ上の MLD 状態数を 300 に制限する例を示します。

```
Device(config)# ipv6 mld state-limit 300
```

関連コマンド

コマンド	説明
ipv6mldaccess-group	IPv6 マルチキャスト受信者アクセス制御のパフォーマンスを有効にします。

コマンド	説明
ipv6mldlimit	MLD メンバーシップ状態の結果の MLD 状態数をインターフェイスごとに制限します。

ipv6 multicast-routing

Protocol Independent Multicast（PIM）とマルチキャスト リスナー検出（MLD）を使用してルータの IPv6 対応のすべてのインターフェイス上でマルチキャスト ルーティングを有効にし、マルチキャスト転送を有効にするには、グローバル コンフィギュレーション モードで **ipv6multicast-routing** コマンドを使用します。マルチキャスト ルーティングと転送を停止するには、このコマンドの **no** 形式を使用します。

ipv6 multicast-routing [**vrf** *vrf-name*]
no ipv6 multicast-routing

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。

コマンド デフォルト

マルチキャスト ルーティングは有効になりません。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

マルチキャスト転送を有効にするには、**ipv6 multicast-routing** コマンドを使用します。このコマンドは、設定するルータの IPv6 対応のすべてのインターフェイス上で Protocol Independent Multicast（PIM）とマルチキャスト リスナー検出（MLD）も有効にします。

マルチキャストを有効にする前に個々のインターフェイスを設定し、必要に応じてそれらのインターフェイス上での PIM および MLD のプロトコル処理を明示的に無効にすることができます。IPv6 PIM または MLD のルータ側の処理を無効にするには、それぞれ **noipv6pim** コマンドまたは **noipv6mldrouter** コマンドを使用します。

例

次に、マルチキャスト ルーティングを有効にし、すべてのインターフェイス上で PIM と MLD をオンにする例を示します。

```
Device(config)# ipv6 multicast-routing
```

関連コマンド

コマンド	説明
ipv6pimrp-address	特定のグループ範囲の PIM RP のアドレスを設定します。
noipv6pim	指定したインターフェイスで IPv6 PIM をオフにします。
noipv6mldrouter	指定したインターフェイスで MLD ルータ側処理をディセーブルにします。

ipv6 multicast group-range

すべてのインターフェイス上で未承認グループまたはチャネルのマルチキャストプロトコルのアクションとトラフィック転送を無効にするには、グローバル コンフィギュレーション モードで **ipv6multicastgroup-range** コマンドを使用します。コマンドのデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ipv6 multicast [**vrf** *vrf-name*] **group-range** [*access-list-name*]
no ipv6 multicast [**vrf** *vrf-name*] **group-range** [*access-list-name*]

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
access-list-name	（任意）トラフィックをルータに送信できる認証済みのサブスクライバ グループと承認済みのチャネルを含んでいるアクセス リストの名前。

コマンド デフォルト

指定したアクセスリストで許可されているグループとチャネルに対してマルチキャストが有効になり、指定したアクセスリストで拒否されているグループとチャネルのマルチキャストは無効になります。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

ipv6multicastgroup-range コマンドは、IPv6 マルチキャスト エッジ ルーティングにアクセス制御メカニズムを提供します。*access-list-name* 引数で指定されたアクセス リストは、許可または拒否されるマルチキャスト グループまたはチャネルを指定します。拒否されたグループまたはチャネルについては、ルータがプロトコル トラフィックとアクションを無視し（たとえば、マルチキャスト リスナー検出（MLD）状態が作成されない、マルチキャスト ルータの状態が作成されない、Protocol Independent Multicast （PIM）の join は転送されないなど）、システム内のすべてのインターフェイスでデータ トラフィックをドロップします。そのため、拒否されたグループまたはチャネルのマルチキャストは無効になります。

ipv6multicastgroup-range グローバル コンフィギュレーション コマンドを使用すると、システム内のすべてのインターフェイス上で MLD アクセス制御コマンドとマルチキャスト境界作成コマンドを設定することになります。ただし、**ipv6multicastgroup-range** コマンドは、次のインターフェイス コンフィギュレーション コマンドを使用することで、選択したインターフェイス上でオーバーライドできます。

- **ipv6mldaccess-group** *access-list-name*
- **ipv6multicastboundaryscope** *scope-value*

noipv6multicastgroup-range コマンドはルータをデフォルト設定に戻すため、既存のマルチキャスト展開は破損しません。

例

次に、list2 というアクセス リストによって拒否されたグループまたはチャネルのマルチキャストをルータが確実に無効にする例を示します。

```
Device(config)# ipv6 multicast group-range list2
```

次に、前出の例のコマンドが int2 によって指定されたインターフェイス上でオーバーライドされる例を示します。

```
Device(config)# interface int2
Device(config-if)# ipv6 mld access-group int-list2
```

int2 では、int-list2 によって許可されたグループまたはチャネルに MLD の状態が作成されますが、int-list2 によって拒否されたグループまたはチャネルには作成されません。その他のすべてのインターフェイスでは、list2 というアクセス リストがアクセス制御に使用されます。

この例では、すべて、またはほとんどのマルチキャスト グループまたはチャネルを拒否するように list2 を指定することができ、int-list2 はインターフェイス int2 に対してのみ、承認済みのグループまたはチャネルを許可するように指定できます。

関連コマンド

コマンド	説明
ipv6mldaccess-group	IPv6 マルチキャスト受信者アクセス制御を実行します。
ipv6multicastboundaryscope	指定されたスコープのインターフェイスでマルチキャスト境界を設定します。

ipv6 multicast pim-passive-enable

IPv6 ルータ上で Protocol Independent Multicast（PIM）パッシブ機能を有効にするには、グローバル コンフィギュレーション モードで **ipv6multicastpim-passive-enable** 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。

ipv6 multicast pim-passive-enable
no ipv6 multicast pim-passive-enable

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

PIM パッシブ モードはルータ上で有効になりません。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

ルータ上で IPv6 PIM パッシブ モードを設定するには、**ipv6multicastpim-passive-enable** コマンドを使用します。PIM パッシブ モードがグルーバルに設定されたら、インターフェイス コンフィギュレーション モードで **ipv6pimpassive** コマンドを使用して特定のインターフェイス上で PIM パッシブ モードを設定します。

例

次に、ルータ上で IPv6 PIM パッシブ モードを設定する例を示します。

```
Device(config)# ipv6 multicast pim-passive-enable
```

関連コマンド

コマンド	説明
ipv6pimpassive	特定のインターフェイス上で PIM パッシブ モードを設定します。

ipv6 multicast rpf

ルーティング情報ベース（RIB）内でBorder Gateway Protocol（BGP）ユニキャスト ルートを使用するように IPv6 マルチキャスト リバース パス フォワーディング（RPF）チェックを有効にするには、グローバル コンフィギュレーション モードで **ipv6multicastrpf** 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。

ipv6 multicast [**vrf** *vrf-name*] **rpf** {**backoff** *initial-delay max-delay*|**use-bgp**}
no ipv6 multicast [**vrf** *vrf-name*] **rpf** {**backoff** *initial-delay max-delay*|**use-bgp**}

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
backoff	ユニキャスト ルーティングを変更した後、バックオフ遅延を指定します。
initial-delay	初期 RPF バックオフ遅延（ミリ秒（ms）単位）。範囲は 200 ～ 65535 です。
max-delay	最大 RPF バックオフ遅延（ミリ秒（ms）単位）。範囲は 200 ～ 65535 です。
use-bgp	マルチキャスト RPF ルックアップの BGP ルートを使用するように指定します。

コマンド デフォルト

マルチキャスト RPF チェックは、BGP ユニキャスト ルートを使用しません。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

ipv6multicastrpf コマンドを設定すると、マルチキャスト RPF チェックは RIB 内の BGP ユニキャスト ルートを使用します。これはデフォルトでは実行されません。

例

次に、マルチキャスト RPF チェック関数を有効にする例を示します。

```
Device# configure terminal
Device(config)# ipv6 multicast rpf use-bgp
```

関連コマンド

コマンド	説明
ipv6multicastlimit	IPv6 内のインターフェイスごとのマルチキャスト ルート（mroute）状態を設定します。

コマンド	説明
ipv6multicastmultipath	複数の等価パス間での IPv6 マルチキャスト トラフィックのロード スプリッティングを有効にします。

ipv6 nd cache expire

IPv6 ネイバー探索（ND）のキャッシュエントリの有効期限が切れるまでの時間を設定するには、インターフェイス コンフィギュレーション モードで **ipv6ndcacheexpire** コマンドを使用します。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

ipv6 nd cache expire *expire-time-in-seconds* **[refresh]**
no ipv6 nd cache expire *expire-time-in-seconds* **[refresh]**

構文の説明

expire-time-in-seconds	時間の範囲は 1 ～ 65,536 秒です。デフォルトは 14,400 秒、つまり 4 時間です。
refresh	（任意）ND キャッシュエントリを自動的に更新します。

コマンド デフォルト

この有効期限は 14,400 秒（4 時間）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

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、14,400 秒間、つまり 4 時間にわたって STALE 状態が続いた場合は、キャッシュエントリの有効期限が切れて削除されます。**ipv6ndcacheexpire** コマンドを使用すると、ユーザは有効期限を変更したり、エントリが削除される前に期限切れのエントリの自動更新をトリガーすることができます。

refresh キーワードを使用すると、ND キャッシュエントリが自動更新されます。エントリは DELAY に移行し、近隣到達不能検出（NUD）プロセスが実行され、5秒後にエントリはDELAY 状態から PROBE 状態に遷移します。エントリが PROBE 状態に到達すると、ネイバー送信要求（NS）メッセージが送信され、設定に従って再送信されます。

例

次に、ND キャッシュエントリが 7,200 秒（2 時間）で期限が切れるように設定する例を示します。

```
Device(config-if)# ipv6 nd cache expire 7200
```

ipv6 nd cache interface-limit (global)

デバイス上のすべてのインターフェイスにネイバー探索のキャッシュ制限を設定するには、グローバル コンフィギュレーション モードで **ipv6ndcacheinterface-limit** コマンドを使用します。デバイス上のすべてのインターフェイスからネイバー探索を削除するには、このコマンドの **no** 形式を使用します。

ipv6 nd cache interface-limit *size* [**log** *rate*]
no ipv6 nd cache interface-limit *size* [**log** *rate*]

構文の説明

size	キャッシュ サイズ。
log *rate*	（任意）調節可能なロギング レート（秒単位）。有効な値は0と1です。

コマンド デフォルト

デバイスのデフォルトのロギング レートは 1 秒あたり 1 エントリです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

グローバル コンフィギュレーション モードで **ipv6ndcacheinterface-limit** コマンドを実行すると、デバイスのすべてのインターフェイスに共通のインターフェイスごとのキャッシュ サイズを適用します。

このコマンドの **no** 形式またはデフォルトの形式を発行すると、グローバル コンフィギュレーション モードを使用して設定したデバイス上のすべてのインターフェイスからネイバー探索制限が削除されます。インターフェイス コンフィギュレーション モードで **ipv6ndcacheinterface-limit** コマンドを使用して設定したインターフェイスのネイバー探索制限は削除されません。

デバイスのデフォルト（および最大）のロギング レートは 1 秒あたり 1 エントリです。

例

次に、デバイス上のすべてのインターフェイスに共通のインターフェイスごとのキャッシュ サイズ制限を設定する例を示します。

```
Device(config)# ipv6 nd cache interface-limit 4
```

関連コマンド

コマンド	説明
ipv6ndcacheinterface-limit(interface)	デバイス上の指定したインターフェイスにネイバー探索キャッシュ制限を設定します。

ipv6 nd host mode strict

conformant または strict IPv6 ホスト モードを有効にするには、グローバル コンフィギュレーション モードで **ipv6 nd host mode strict** コマンドを使用します。conformant または loose ホスト モードを再度有効にするには、このコマンドの **no** 形式を使用します。

ipv6 nd host mode strict

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

nonconformant、または loose IPv6 ホスト モードが有効になります。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

デフォルトの IPv6 ホスト モード タイプは loose または nonconformant です。IPv6 strict または conformant のホスト モードを有効にするには、**ipv6 nd host mode strict** コマンドを使用します。2 つの IPv6 ホスト モード間で変更を行うには、このコマンドの **no** 形式を使用します。

ipv6 nd host mode strict コマンドは、IPv6 ホスト モード動作タイプを選択し、インターフェイス コンフィギュレーション モードに移行します。ただし、**ipv6 nd host mode strict** コマンドは、**ipv6 unicast-routing** コマンドを使用して設定した IPv6 ルーティングがある場合は無視されます。この状況では、デフォルトの IPv6 ホスト モード タイプの loose が使用されます。

例

次に、strict IPv6 ホストとしてデバイスを設定し、イーサネット インターフェイス 0/0 で IPv6 アドレスの自動設定を有効にする例を示します。

```
Device(config)# ipv6 nd host mode strict
Device(config-if)# interface ethernet0/0
Device(config-if)# ipv6 address autoconfig
```

次に、strict IPv6 ホストとしてデバイスを設定し、イーサネット インターフェイス 0/0 で静的 IPv6 アドレスを設定する例を示します。

```
Device(config)# ipv6 nd host mode strict
Device(config-if)# interface ethernet0/0
Device(config-if)# ipv6 address 2001::1/64
```

関連コマンド

コマンド	説明
ipv6 unicast-routing	IPv6ユニキャストデータグラムの転送をイネーブルにします。

ipv6 nd ns-interval

インターフェイスで IPv6 ネイバー送信要求（NS）メッセージが再送信される時間間隔を設定するには、インターフェイス コンフィギュレーション モードで **ipv6ndns-interval** コマンドを使用します。デフォルトの間隔に戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd ns-interval *milliseconds*
no ipv6 nd ns-interval

構文の説明

milliseconds	アドレス解決のための IPv6 ネイバー探索伝送の間隔。許容範囲は 1,000 ～ 3,600,000 ミリ秒です。

コマンド デフォルト

0 ミリ秒（未指定）の場合、ルータ アドバタイズメントでアドバタイズされます。値 1000 は、ルータ自体のネイバー探索アクティビティに使用されます。

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

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、**ipv6ndns-interval** コマンドはアドレス解決と重複アドレス検出（DAD）の両方の NS 再送信間隔を変更します。DAD に別の NS の再送信間隔を指定するには、**ipv6nddadtime** コマンドを使用します。

この値は、このインターフェイスから送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。通常の IPv6 操作には、短すぎる間隔はお勧めできません。デフォルト以外の値が設定されている場合、設定時間は、ルータ自体により、アドバタイズおよび使用されます。

例

次に、イーサネット インターフェイス 0/0 の IPv6 ネイバー送信要求メッセージの送信間隔を 9,000 ミリ秒に設定する例を示します。

```
Device(config)# interface ethernet 0/0
Device(config-if)# ipv6 nd ns-interval 9000
```

関連コマンド

コマンド	説明
ipv6nddadtime	アドレス解決のための NS 再送信間隔とは別に DAD の NS 再送信間隔を設定します。
showipv6interface	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 nd reachable-time

何らかの到達可能性確認イベントが発生してからリモート IPv6 ノードが到達可能と見なされるまでの時間を設定するには、インターフェイス コンフィギュレーション モードで **ipv6ndreachable-time** コマンドを使用します。デフォルト値に戻す場合は、このコマンドの **no** 形式を入力します。

ipv6 nd reachable-time *milliseconds*
no ipv6 nd reachable-time

構文の説明

milliseconds	リモート IPv6 ノードが到達可能であると見なされる時間（ミリ秒単位）。

コマンド デフォルト

0 ミリ秒（未指定）の場合、ルータ アドバタイズメントでアドバタイズされます。値 30000（30 秒）は、ルータ自体のネイバー探索アクティビティに使用されます。

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

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

設定時間により、ルータは、利用不可隣接を検出できます。設定時間を短くすると、ルータは、より速く利用不可隣接を検出できます。ただし、設定時間を短くすると、すべての IPv6 ネットワーク デバイスで消費される IPv6 ネットワーク帯域幅および処理リソースが多くなります。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。

設定時間は、インターフェイスから送信されるすべてのルータ アドバタイズメントに含まれるため、同じリンクのノードは同じ時間値を共有します。値に 0 を設定すると、設定時間がこのルータで指定されていないことを示します。

例

次に、イーサネット インターフェイス 0/0 に 1,700,000 ミリ秒の IPv6 到達可能時間を設定する例を示します。

```
Device(config)# interface ethernet 0/0
Device(config-if)# ipv6 nd reachable-time 1700000
```

関連コマンド

コマンド	説明
showipv6interface	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 nd resolution data limit

ネイバー探索保留中のキュー登録データ パケットの数を設定するには、グローバル コンフィギュレーション モードで **ipv6ndresolutiondatalimit** コマンドを使用します。

ipv6 nd resolution data limit *number-of-packets*
no ipv6 nd resolution data limit *number-of-packets*

構文の説明

number-of-packets	キュー登録データ パケット数。範囲は 16 ～ 2048 パケットです。

コマンド デフォルト

キュー制限は 16 パケットです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

ipv6ndresolutiondatalimit コマンドを使用すると、顧客はネイバー探索解決保留中のパケットのキュー登録数を設定できます。IPv6 ネイバー探索は、未解決の宛て先の解決を開始するデータ パケットをキューに登録します。ネイバー探索は、宛て先ごとに 1 つのパケットのみをキューに登録します。また、ネイバー探索はキューに登録されるパケットの数にグローバル（ルータごとの）制限も適用します。グローバル キュー制限に到達すると、未解決の宛て先へのそれ以降のパケットが破棄されます。最小値（およびデフォルト値）は 16 パケットで、最大値は 2048 です。

ほとんどの場合は、ネイバー探索解決保留中のキュー登録パケットのデフォルト値の 16 で十分です。ただし、極めて多くのネイバーとの通信をほぼ同時に開始する必要があるルータの高拡張性シナリオでは、この値では不十分な場合があります。そのため、一部のネイバーに送信された最初のパケットが失われる可能性があります。ほとんどの場合、最初のパケットは再送信されるため、通常は、最初のパケットの損失について心配する必要はありません（未解決の宛て先への最初のパケットのドロップは IPv4 では正常な動作です）。ただし、最初のパケットの損失が問題となる大規模設定もあります。このような場合は **ipv6ndresolutiondatalimit** コマンドを使用し、未解決パケット キューのサイズを拡大することで最初のパケット損失を防ぎます。

例

次に、解決待機中に保持されるデータ パケットのグローバル数を 32 に設定する例を示します。

```
Device(config)# ipv6 nd resolution data limit 32
```

ipv6 nd route-owner

ネイバー探索で学習したルートを「ND」ステータスでルーティング テーブルに挿入し、ND 自動設定動作を有効にするには、 **ipv6 nd route-owner** コマンドを使用します。ルーティング テーブルからこの情報を削除するには、このコマンドの **no** 形式を使用します。

ipv6　ndroute-owner

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

ネイバー探索で学習したルートのステータスは「Static」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

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

ipv6 nd route-owner コマンドはネイバー探索で学習したルートを「Static」または「Connected」ではなく、「ND」のステータスでルーティング テーブルに挿入します。

また、このグローバル 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 **ipv6 nd autoconfig default** コマンドまたは **ipv6 nd autoconfig prefix** コマンドも使用できるようにします。 **ipv6 nd route-owner** コマンドを発行しないと、**ipv6 nd autoconfig default** コマンドと **ipv6 nd autoconfig prefix** コマンドはルータには承認されますが、機能しません。

例

```
Device(config)# ipv6 nd route-owner
```

関連コマンド

コマンド	説明
ipv6 nd autoconfig default	ネイバー探索によって、ネイバー探索で取得されたデフォルト ルータにデフォルト ルートをインストールできるようにします。
ipv6 nd autoconfig prefix	ネイバー探索を使用して、インターフェイスで受信した RA から有効なすべてのオンリンク プレフィックスをインストールします。

ipv6 neighbor

IPv6 ネイバー探索キャッシュに静的エントリを設定するには、グローバル コンフィギュレーション モードで **ipv6neighbor** コマンドを使用します。IPv6 ネイバー探索キャッシュから静的 IPv6 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。

ipv6 neighbor *ipv6-address interface-type interface-number hardware-address*
no ipv6 neighbor *ipv6-address interface-type interface-number*

構文の説明

ipv6-address	ローカル データリンク アドレスに対応する 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。
interface-type	指定されたインターフェイス タイプ。サポートされているインターフェイス タイプについては、疑問符（?）オンライン ヘルプ機能を使用してください。
interface-number	指定されたインターフェイス番号。
hardware-address	ローカル データリンク アドレス（48 ビット アドレス）。

コマンド デフォルト

スタティック エントリは、IPv6 ネイバー探索キャッシュに設定されません。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

ipv6neighbor コマンドは **arp**（グローバル）コマンドに類似しています。

指定された IPv6 アドレスのエントリが（IPv6 ネイバー探索プロセスを通して学習された）ネイバー探索キャッシュ内にすでに存在する場合、そのエントリは自動的に静的エントリに変換されます。

IPv6 ネイバー探索キャッシュの静的エントリを表示するには、**showipv6neighbors** コマンドを使用します。IPv6 ネイバー探索キャッシュ内のスタティック エントリは次のいずれかの状態になります。

- INCMP（不完全）：このエントリのインターフェイスがダウンしています。
- REACH（到達可能）：このエントリのインターフェイスがアップしています。

（注） 到達可能性検出は、IPv6 ネイバー探索キャッシュ内のスタティック エントリに適用されません。そのため、INCMP および REACH 状態に関する説明とダイナミックおよびスタティック キャッシュ エントリに関する説明は一致しません。ダイナミック キャッシュ エントリの INCMP ステータスおよび REACH ステータスの説明については、**showipv6neighbors** コマンドを参照してください。

clearipv6neighbors コマンドにより、静的エントリを除き、IPv6 ネイバー探索キャッシュ内のすべてのエントリを削除します。**noipv6neighbor** コマンドは、ネイバー探索キャッシュから指定の静的エントリを削除します。ダイナミック エントリ（IPv6 ネイバー探索プロセスから学習したエントリ）はキャッシュから削除されません。**noipv6enable** コマンドまたは **noipv6unnumbered** コマンドを使用してインターフェイスで IPv6 を無効にすると、静的エントリを除き、そのインターフェイス用に設定したすべての IPv6 ネイバー探索キャッシュ エントリが削除されます（エントリの状態が INCMP に変更されます）。

IPv6 ネイバー探索キャッシュ内のスタティック エントリがネイバー探索プロセスによって変更されることはありません。

（注） IPv6 隣接のスタティック エントリは、IPv6 がイネーブルにされている LAN および ATM LAN Emulation インターフェイスだけで設定できます。

例

次の例では、イーサネット インターフェイス 1 上の IPv6 アドレスが 2001:0DB8::45A で、リンク層アドレスが 0002.7D1A.9472 のネイバーに関する IPv6 ネイバー探索キャッシュ内の静的エントリを設定します。

```
Device(config)# ipv6 neighbor 2001:0DB8::45A ethernet1 0002.7D1A.9472
```

関連コマンド

コマンド	説明
arp(global)	パーマネント エントリを ARP キャッシュに追加します。
clearipv6neighbors	スタティック エントリを除く、IPv6 ネイバー探索キャッシュ内のすべてのエントリを削除します。
noipv6enable	明示的な IPv6 アドレスで設定されていないインターフェイスでの IPv6 処理をディセーブルにします。
noipv6unnumbered	アンナンバード インターフェイス上の IPv6 を無効にします。
showipv6neighbors	IPv6 ネイバー探索キャッシュ情報を表示します。

ipv6 ospf name-lookup

Open Shortest Path First（OSPF）ルータ ID を Domain Naming System（DNS）名として表示するには、グローバル コンフィギュレーション モードで **ipv6ospfname-lookup** コマンドを使用します。DNS 名として OSPF ルータ ID の表示を停止するには、このコマンドの **no** 形式を使用します。

ipv6 ospf name-lookup
no ipv6 ospf name-lookup

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

このコマンドはデフォルトでは無効になっています。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するとルータがルータ ID やネイバー ID ではなく名前で表示されるため、ルータを識別しやすくなります。

例

次に、すべての OSPF show EXEC コマンドの表示で使用する DNS 名を検索するように OSPF を設定する例を示します。

```
Device(config)# ipv6 ospf name-lookup
```

ipv6 pim

IPv6 Protocol Independent Multicast（PIM）を指定したインターフェイス上で再度有効にするには、インターフェイス コンフィギュレーション モードで **ipv6pim** コマンドを使用します。指定したインターフェイス上で PIM を無効にするには、このコマンドの **no** 形式を使用します。

ipv6 pim
no ipv6 pim

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

PIM はすべてのインターフェイス上で自動的に有効になります。

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

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

ipv6multicast-routing コマンドを有効にすると、PIM はすべてのインターフェイス上で実行できるようになります。PIM はデフォルトですべてのインターフェイス上で有効になるため、**ipv6pim** コマンドの **no** 形式を使用し、指定したインターフェイス上で PIM を無効にします。PIMがインターフェイス上で無効になっている場合は、マルチキャスト リスナー検出（MLD）プロトコルからのホスト メンバーシップ通知に反応しません。

例

次に、ファスト イーサネット インターフェイス 1/0 で PIM をオフにする例を示します。

```
Device(config)# interface FastEthernet 1/0
Device(config-if)# no ipv6 pim
```

関連コマンド

コマンド	説明
ipv6multicast-routing	ルータのすべての IPv6 対応インターフェイス上で PIMと MLD を使用したマルチキャスト ルーティングを有効にし、マルチキャスト転送を有効にします。

ipv6 pim accept-register

ランデブー ポイント（RP）で登録を承認または拒否するには、グローバル コンフィギュレーション モードで **ipv6pimaccept-register** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ipv6 pim [**vrf** *vrf-name*] **accept-register** {**list** *access-list*|**route-map** *map-name*}
no ipv6 pim [**vrf** *vrf-name*] **accept-register** {**list** *access-list*|**route-map** *map-name*}

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
list *access-list*	アクセス リスト名を定義します。
route-map *map-name*	ルート マップを定義します。

コマンド デフォルト

すべての送信元が RP で承認されます。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

名前付きのアクセス リストまたはルート マップを一致属性で設定するには、**ipv6pimaccept-register** コマンドを使用します。*access-list* 引数と *map-name* 引数で定義された permit 条件が満たされている場合、登録メッセージは承認されます。それ以外の場合、登録メッセージは承認されず、即時登録停止メッセージがカプセル化する宛て先ルータに返されます。

例

次に、ローカル マルチキャスト Border Gateway Protocol（BGP）のプレフィックスが備わっていないすべての送信元上でフィルタ処理する例を示します。

```
ipv6 pim accept-register route-map reg-filter
route-map reg-filter permit 20
 match as-path 101
ip as-path access-list 101 permit
```

ipv6 pim allow-rp

PIM Allow RP 機能を IPv6 デバイス内のすべての IP マルチキャスト対応のインターフェイスに有効にするには、グローバル コンフィギュレーション モードで **ip pim allow-rp** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ipv6 pim allow-rp [{**group-list** *access-list*|**rp-list** *access-list* [**group-list** *access-list*]}]
no ipv6 pim allow-rp

構文の説明

group-list	（任意）PIM Allow RP に許可されたグループ範囲のアクセス コントロール リスト（ACL）を指定します。
rp-list	（任意）PIM Allow RP に許可されたランデブー ポイント（RP）アドレスの ACL を指定します。
access-list	（任意）標準 ACL の固有番号または固有名。

コマンド デフォルト

PIM Allow RP は無効になっています。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して、IP マルチキャスト ネットワーク内の受信側デバイスを有効にして、予期しない（別の）RP アドレスからの (*, G) join を承認します。

PIM Allow RP を有効にする前に、最初に **ipv6 pim rp-address** コマンドを使用して RP を定義する必要があります。

関連コマンド

コマンド	説明
ipv6 pim rp-address	マルチキャスト グループの PIM RP のアドレスを静的に設定します。

ipv6 pim anycast-RP

エニーキャスト グループ範囲に Protocol-Independent Multicast（PIM）ランデブー ポイント（RP）のアドレスを設定するには、グローバル コンフィギュレーション モードで **ipv6 pim anycast-RP** コマンドを使用します。エニーキャスト グループ範囲の RP 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 pim anycast-RP {*rp-address peer-address*}
no ipv6 pim anycast-RP

構文の説明

anycast-rp-address	グループの範囲に割り当てられている RP に設定されたエニーキャスト RP これは、ファースト ホップ PIM ルータとラスト ホップ PIM ルータが登録と参加に使用するアドレスです。
peer-address	登録メッセージのコピー先アドレスを送信します。このアドレスはRPルータに割り当てられているアドレスであり、これには *anycast-rp-address* 変数を使用して割り当てられたアドレスは含まれていません。

コマンド デフォルト

エニーキャスト グループの範囲に PIM RP アドレスを設定しません。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

エニーキャスト RP 機能は、ドメイン間接続が不要な場合に便利です。エニーキャスト グループの範囲に PIM RP のアドレスを設定するには、このコマンドを使用します。

例

```
Device# ipv6 pim anycast-rp 2001:DB8::1:1 2001:DB8::3:3
```

関連コマンド

コマンド	説明
show ipv6 pim anycast-RP	IPv6 PIM RP エニーキャストの設定を確認します。

ipv6 pim neighbor-filter list

特定の IPv6 アドレスからの Protocol Independent Multicast（PIM）ネイバー メッセージをフィルタ処理するには、グローバル コンフィギュレーション モードで **ipv6pimneighbor-filter** コマンドを使用します。デフォルトに戻すには、**no** 形式のコマンドを使用します。

ipv6 pim [**vrf** *vrf-name*] **neighbor-filter list** *access-list*
no ipv6 pim [**vrf** *vrf-name*] **neighbor-filter list** *access-list*

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
access-list	送信元からの PIM の hello パケットを拒否する IPv6 アクセス リストの名前。

コマンド デフォルト

PIM ネイバー メッセージはフィルタリングされません。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

ipv6pimneighbor-filterlist コマンドは、LAN 上の不正ルータが PIM ネイバーになるのを防止するために使用します。このコマンドで指定されているアドレスからの hello メッセージが無視されます。

例

次に、PIM に IPv6 アドレス FE80::A8BB:CCFF:FE03:7200: からのすべての hello メッセージを無視させる例を示します。

```
Device(config)# ipv6 pim neighbor-filter list nbr_filter_acl
Device(config)# ipv6 access-list nbr_filter_acl
Device(config-ipv6-acl)# deny ipv6 host FE80::A8BB:CCFF:FE03:7200 any
Device(config-ipv6-acl)# permit any any
```

ipv6 pim rp-address

特定のグループ範囲に Protocol-Independent Multicast（PIM）ランデブー ポイント（RP）のアドレスを設定するには、グローバル コンフィギュレーション モードで **ipv6pimrp-address** コマンドを使用します。RP 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 pim [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-access-list*] **[bidir]**
no ipv6 pim rp-address *ipv6-address* [*group-access-list*] **[bidir]**

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
ipv6-address	PIM RP になるルータの IPv6 アドレス。 *ipv6-address* 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。
group-access-list	（任意）RP をどのマルチキャスト グループに使用するかを定義するアクセス リストの名前。 アクセス リストに割り当てられた Source-Specific Multicast（SSM）グループ アドレスの範囲（FF3x::/96）に重複するグループ アドレスの範囲が含まれている場合、警告メッセージが表示され、重複する範囲は無視されます。アクセス リストを指定しない場合は、有効なマルチキャスト非 SSM アドレスのすべての範囲に指定した RP が使用されます。 組み込み RP をサポートするには、RP として設定したルータが、組み込み RP アドレスから生成した組み込み RP グループの範囲を許可する設定済みのアクセス リストを使用する必要があります。 組み込み RP グループの範囲にすべての範囲（3 ～ 7 など）を含める必要はありません。
bidir	（任意）双方向共有ツリー転送に使用するグループ範囲を指定します。指定しないと、スパース モード転送に使用されます。単一の IPv6 アドレスは、双方向またはスパース モード範囲のいずれかにのみ RP として設定できます。単一のグループ範囲リストは、双方向モードかスパース モードのいずれかで動作するように設定できます。

コマンド デフォルト

PIM RP は事前に設定されていません。組み込み RP サポートは、IPv6 PIM が有効になっている（組み込み RP サポートが提供される）場合に、デフォルトで有効になります。マルチキャスト グループは PIM スパース モードで動作します。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

PIM がスパース モードで設定されている場合は、RP として動作する 1 つ以上のルータを選択する必要があります。RP は、共有配布ツリーの唯一かつ共通のルートで、各ルータではスタティックに設定されます。

組み込み RP サポートが利用できる場合、RP を組み込み RP 範囲の RP として静的に設定する必要があるだけです。他の IPv6 PIM ルータでのその他の設定は必要ありません。他のルータは、IPv6 グループ アドレスから RP アドレスを検出します。これらのルータが組み込み RP の代わりに静的 RP を選択する場合、特定の組み込み RP グループ範囲を静的 RP のアクセス リストに設定する必要があります。

送信元マルチキャスト ホストの代わりに、ファーストホップ ルータが使用する RP アドレスを使用して登録パケットを送信します。また、グループのメンバーにするマルチキャスト ホストの代わりに、ルータが RP アドレスを使用します。これらのルータは join メッセージと prune メッセージを RP に送信します。

オプションの *group-access-list* 引数を指定しないと、FFX[3-f]::/8 ～ FF3X::/96 の範囲の SSM を除き、ルーティング可能な IPv6 マルチキャスト グループの範囲全体に RP が適用されます。*group-access-list* 引数を指定した場合、IPv6 アドレスは *group-access-list* 引数内に指定したグループの範囲の RP アドレスになります。

複数のグループに単一の RP を使用するように Cisco IOS ソフトウェアを設定できます。アクセス リストで指定されている条件によって、RP を使用できるグループが決定されます。アクセス リストが設定されていない場合は、すべてのグループに RP が使用されます。

PIM ルータは複数の RP を使用できますが、グループごとに 1 つのみです。

例

次に、すべてのマルチキャスト グループの PIM RP アドレスを 2001::10:10 に設定する例を示します。

```
Device(config)# ipv6 pim rp-address 2001::10:10
```

次に、マルチキャスト グループ FF04::/64 についてのみ PIM RP アドレスを 2001::10:10 に設定する例を示します。

```
Device(config)# ipv6 access-list acc-grp-1
Device(config-ipv6-acl)# permit ipv6 any ff04::/64
Device(config)# ipv6 pim rp-address 2001::10:10 acc-grp-1
```

次に、IPv6 アドレス 2001:0DB8:2::2 から生成した組み込み RP の範囲を許可するグループ アクセス リストを設定する例を示します。

```
Device(config)# ipv6 pim rp-address 2001:0DB8:2::2 embd-ranges
Device(config)# ipv6 access-list embd-ranges
Device(config-ipv6-acl)# permit ipv6 any ff73:240:2:2:2::/96
Device(config-ipv6-acl)# permit ipv6 any ff74:240:2:2:2::/96
Device(config-ipv6-acl)# permit ipv6 any ff75:240:2:2:2::/96
```

```
Device(config-ipv6-acl)# permit ipv6 any ff76:240:2:2:2::/96
Device(config-ipv6-acl)# permit ipv6 any ff77:240:2:2:2::/96
Device(config-ipv6-acl)# permit ipv6 any ff78:240:2:2:2::/96
```

次に、アドレス 100::1 をマルチキャスト範囲 FF::/8 全体の双方向 RP として有効にする例を示します。

```
ipv6 pim rp-address 100::1 bidir
```

次に、IPv6 アドレス 200::1 を、bidir-grps というアクセス リストで許可された範囲の双方向 RP として有効にする例を示します。このリストで許可された範囲は ff05::/16 と ff06::/16 です。

```
Device(config)# ipv6 access-list bidir-grps
Device(config-ipv6-acl)# permit ipv6 any ff05::/16
Device(config-ipv6-acl)# permit ipv6 any ff06::/16
Device(config-ipv6-acl)# exit
Device(config)# ipv6 pim rp-address 200::1 bidir-grps bidir
```

関連コマンド

コマンド	説明
debugipv6pimdf-election	PIM 双方向 DF 選択メッセージ処理のデバッグ メッセージを表示します。
ipv6access-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。
showipv6pimdf	各 RP の各インターフェイスの DF 選択状態を表示します。
showipv6pimdfwinner	各 RP の各インターフェイスの DF 選択ウィナーを表示します。

ipv6 pim rp embedded

IPv6 Protocol Independent Multicast（PIM）で組み込みランデブー ポイント（RP）サポートを有効にするには、グローバル コンフィギュレーション モードで**ipv6pimrp-embedded** コマンドを使用します。組み込みRPサポートを無効にするには、このコマンドの**no**形式を使用します。

ipv6 pim [**vrf** *vrf-name*] **rp embedded**
no ipv6 pim [**vrf** *vrf-name*] **rp embedded**

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。

コマンド デフォルト

組み込み RP サポートはデフォルトで有効になっています。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

組み込み RP サポートはデフォルトで有効になるため、組み込み RP サポートをオフにするには、ユーザは通常、このコマンドの **no** 形式を使用します。

ipv6pimrpembedded コマンドは、組み込み RP グループ範囲の ff7X::/16 と fffX::/16 にのみ適用されます。ルータが有効になっている場合、組み込み RP グループ範囲の ff7X::/16 と fffX::/16 のグループを解析し、使用する RP をグループ アドレスから抽出します。

例

次に、IPv6 PIM の組み込み RP サポートを無効にする例を示します。

```
no ipv6 pim rp embedded
```

ipv6 pim spt-threshold infinity

Protocol Independent Multicast（PIM）リーフ ルータが指定したグループの最短パス ツリー（SPT）にいつ参加するかを設定するには、グローバル コンフィギュレーション モードで **ipv6pimspt-thresholdinfinity** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ipv6 pim [**vrf** *vrf-name*] **spt-threshold infinity** [**group-list** *access-list-name*]
no ipv6 pim spt-threshold infinity

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
group-list *access-list-name*	（任意）しきい値を適用するグループを指定します。標準的な IPv6 アクセス リスト名である必要があります。この値を省略すると、すべてのグループにしきい値が適用されます。

コマンド デフォルト

このコマンドを使用しない場合、最初のパケットが新しい送信元から到着するとすぐに、PIM リーフ ルータが SPT に参加します。ルータが SPT に参加した後では、**ipv6pimspt-thresholdinfinity** コマンドによって共有ツリーに切り替わりません。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

ipv6pimspt-thresholdinfinity コマンドを使用すると、共有ツリーを使用するよう指定したグループのすべての送信元が有効になります。**group-list** キーワードは、SPT しきい値を適用するグループを指定します。

access-list-name 引数は IPv6 アクセス リストを参照します。*access-list-name* 引数を値 0 で指定するか、または **group-list** キーワードを使用しない場合は、SPT しきい値がすべてのグループに適用されます。デフォルト設定（このコマンドが無効になっている）では、新しい送信元から最初のパケットが着信した直後に SPT に参加します。

例

次に、PIM のラストホップ ルータが共有ツリーに留まり、グループの範囲の ff04::/64 の SPT に切り替わらない例を示します。

```
Device(config)# ipv6 access-list acc-grp-1
Device(config-ipv6-acl)# permit ipv6 any FF04::/64
Device(config-ipv6-acl)# exit
Device(config)# ipv6 pim spt-threshold infinity group-list acc-grp-1
```

ipv6 prefix-list

IPv6 プレフィックス リストのエントリを作成するには、グローバル コンフィギュレーション モードで **ipv6prefix-list** コマンドを使用します。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。

ipv6 prefix-list *list-name* [**seq** *seq-number*] {**deny** *ipv6-prefix*/*prefix-length*|**permit** *ipv6-prefix*/*prefix-length*|**説明** *text*} [**ge** *ge-value*] [**le** *le-value*]
no ipv6 prefix-list *list-name*

構文の説明

list-name	プレフィックス リストの名前。 • 既存のアクセス リストと同じ名前にすることはできません。 • **showipv6prefix-list** コマンドのキーワードであるため、名前に「detail」や「summary」を使用することはできません。
seq *seq-number*	（オプション）設定するプレフィックス リスト エントリのシーケンス番号。
deny	条件に一致するネットワークを拒否します。
permit	条件に一致するネットワークを許可します。
ipv6-prefix	指定したプレフィックス リストに割り当てられている 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。
説明 *text*	プレフィックス リストの説明。最大 80 文字です。
ge *ge-value*	（任意）*ipv6-prefix*/*prefix-length* 引数の値と等しいかそれよりも長いプレフィックス長を指定します。これは *length* の範囲の最小値です（長さ範囲の「下限」に該当する値）。
le *le-value*	（任意）*ipv6-prefix*/*prefix-length* 引数の値と等しいかそれよりも短いプレフィックス長を指定します。これは *length* の範囲の最大値です（長さ範囲の「上限」に該当する値）。

コマンド デフォルト

プレフィックス リストは作成されません。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

ipv6prefix-list コマンドは、IPv6 に固有であることを除き、**ipprefix-list** コマンドと同様です。

ネットワークが更新でアドバタイズされることを抑制するには、**distribute-listout** コマンドを使用します。

プレフィックス リスト エントリのシーケンス番号によって、リスト中のエントリの順番が決まります。ルータは、ネットワーク アドレスとプレフィックス リスト エントリを比較します。ルータは、プレフィックス リストの先頭（最も小さいシーケンス番号）から比較を開始します。

プレフィックス リストの複数のエントリがプレフィックスに一致する場合、シーケンス番号が最も小さいエントリが実際の一致と見なされます。一致または拒否が発生すると、プレフィックス リストの残りのエントリは処理されません。効率を向上させるため、*seq-number* 引数を使用して最も一般的な permit や deny をリストの最上部近くに配置できます。

showipv6prefix-list はエントリのシーケンス番号を表示します。

IPv6 プレフィックス リストは、permit 文または deny 文を適用する前に照合が必要な特定のプレフィックスまたはプレフィックスの範囲を指定するために使用されます。2 つのオペランド キーワードを使用して、照合するプレフィックス長の範囲を指定できます。ある値以下のプレフィックス長は、**le** キーワードで設定します。ある値以上のプレフィックス長は、**ge** キーワードを使用して指定します。**ge** および **le** キーワードを使用すると、通常の *ipv6-prefix*/*prefix-length* 引数よりも詳細に照合するプレフィックス長の範囲を指定できます。プレフィックス リストのエントリと照合される候補プレフィックスに対して、次の 3 つの条件が存在する可能性があります。

- 候補プレフィックスは、指定したプレフィックス リストおよびプレフィックス長エントリと一致している必要があります。
- 省略可能な **le** キーワードの値によって、許可されるプレフィックス長が、*prefix-length* 引数から **le** キーワードの値（この値を含む）までの範囲で指定されます。
- 省略可能な **ge** キーワードの値によって、許可されるプレフィックス長が、**ge** キーワードの値から 128（この値を含む）までの範囲で指定されます。

（注） 最初の条件は、他の条件が有効になる前に一致している必要があります。

ge または **le** キーワードを指定しなかった場合は、完全一致であると想定されます。1 つのキーワード オペランドだけを指定した場合、そのキーワードの条件が適用され、もう 1 つの条件は適用されません。*prefix-length* 値は、**ge** 値よりも小さい必要があります。**ge** 値は、**le** 値以下である必要があります。**le** 値は、128 以下である必要があります。

すべての IPv6 プレフィックス リスト（許可および拒否の条件文が含まれていないプレフィックス リストを含む）には、最後の一致条件として暗黙の deny any any ステートメントが含まれています。

例

次に、プレフィックス ::/0 を持つすべてのルートを拒否する例を示します。

```
Device(config)# ipv6 prefix-list abc deny ::/0
```

次に、プレフィックス 2002::/16 を許可する例を示します。

```
Device(config)# ipv6 prefix-list abc permit 2002::/16
```

次に、プレフィックス 5F00::/48 以上でプレフィックス 5F00::/64 を含むすべてのプレフィックスを承認するプレフィックスのグループを指定する例を示します。

```
Device(config)# ipv6 prefix-list abc permit 5F00::/48 le 64
```

次に、プレフィックス 2001:0DB8::/64 を持つルート内の 64 ビットよりも大きいプレフィックス長を拒否する例を示します。

```
Device(config)# ipv6 prefix-list abc permit 2001:0DB8::/64 le 128
```

次に、すべてのアドレス空間で 32 ～ 64 ビットのマスク長を許可する例を示します。

```
Device(config)# ipv6 prefix-list abc permit ::/0 ge 32 le 64
```

次に、すべてのアドレス空間で32 ビットよりも大きいマスク長を拒否する例を示します。

```
Device(config)# ipv6 prefix-list abc deny ::/0 ge 32
```

次に、プレフィックス 2002::/128 を持つすべてのルートを拒否する例を示します。

```
Device(config)# ipv6 prefix-list abc deny 2002::/128
```

次に、プレフィックス ::/0 を持つすべてのルートを許可する例を示します。

```
Device(config)# ipv6 prefix-list abc permit ::/0
```

関連コマンド

コマンド	説明
clearipv6prefix-list	IPv6 プレフィックス リスト エントリのヒット カウントをリセットします。
distribute-listout	ネットワークが更新時にアドバタイズされないようにします。
ipv6prefix-listsequence-number	IPv6 プレフィックス リスト内のエントリのシーケンス番号の生成を有効にします。

コマンド	説明
matchipv6address	プレフィクス リストによって許可されるプレフィックスを持つ IPv6 ルートを配信します。
showipv6prefix-list	IPv6 プレフィックス リストまたは IPv6 プレフィックス リストのエントリに関する情報を表示します。

ipv6 source-guard attach-policy

インターフェイス上の IPv6 送信元ガード ポリシーを適用するには、インターフェイス コンフィギュレーション モードで **ipv6 source-guard attach-policy** を使用します。インターフェイスから送信元ガードを削除するには、このコマンドの **no** 形式を使用します。

ipv6 source-guard attach-policy ［*source-guard-policy* ］

構文の説明

source-guard-policy	（任意）送信元ガード 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 送信元ガード ポリシーはインターフェイスに適用されません。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

source-guard-policy 引数を使用してポリシーを指定しないと、デフォルトの送信元ガード ポリシーが適用されます。

IPv6 送信元ガードと IPv6 スヌーピング間には依存関係があります。IPv6 送信元ガードが設定されるたびに、**ipv6 source-guard attach-policy** が入力されると、スヌーピングが有効になっていることを確認し、有効になっていない場合は警告を発行します。IPv6 スヌーピングが無効になっている場合、ソフトウェアは IPv6 送信元ガードが有効になっていることを確認し、有効になっていれば警告を送信します。

例

次に、インターフェイスに IPv6 送信元ガードを適用する例を示します。

```
Device(config)# interface gigabitethernet 0/0/1
Device(config-if)# ipv6 source-guard attach-policy mysnoopingpolicy
```

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 source-route

IPv6 タイプ 0 のルーティング ヘッダー（IPv6 送信元ルーティング ヘッダー）の処理を有効にするには、グローバル コンフィギュレーション モードで **ipv6source-route** コマンドを使用します。IPv6 拡張ヘッダーの処理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 source-route
no ipv6 source-route

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

デフォルトは、**ipv6source-route** コマンドの **no** バージョンです。ルータがタイプ 0 のルーティング ヘッダーを持つパケットを受信すると、そのルータはパケットをドリップして Internet Control Message Protocol（ICMP）エラー メッセージを送信元に送り返し、適切なデバッグ メッセージをログに記録します。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

デフォルトが **ipv6source-route** コマンドの **no** バージョンに変更されました。つまり、この機能は有効になっていません。この変更以前は、この機能は自動的に有効になっていました。デフォルトが変更される前に **noipv6source-route** コマンドを設定した場合、このコマンドの **no** バージョンがデフォルトであるとしても、**showconfig** コマンドの出力内にこの設定が引き続き表示されます。

noipv6source-route コマンド（デフォルト）は、ホストがルータを使用して送信元ルーティングを実行しないようにします。**noipv6source-route** コマンドが設定されている場合に、ルータが type0 の送信元ルーティング ヘッダーを持つパケットを受信すると、ルータはそのパケットをドロップして、送信元に IPv6 ICMP エラー メッセージを返信し、適切なデバッグ メッセージを記録します。

IPv6 では、パケットの宛て先によってのみ、送信元ルーティングが実行されます。そのため、送信元ルーティングがネットワーク内で実行されないようにするには、次のルールを含む IPv6 アクセス コントロール リスト（ACL）を設定する必要があります。

```
deny ipv6 any any routing
```

ルータが IPv6 ICMP エラーメッセージを生成するレートを制限するには、**ipv6 icmp error-interval** コマンドを使用します。

例

次に、IPv6 タイプ 0 のルーティング ヘッダーの処理を無効にする例を示します。

```
no ipv6 source-route
```

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。
ipv6icmperror-interval	IPv6 ICMP エラー メッセージの間隔を設定します。

ipv6 spd mode

IPv6選択的パケット廃棄（SPD）モードを設定するには、グローバルコンフィギュレーションモードで **ipv6spdmode** コマンドを使用します。IPv6 SPD モードを削除するには、このコマンドの **no** 形式を使用します。

ipv6 spd mode {**aggressive**|**tos protocol ospf**}
no ipv6 spd mode {**aggressive**|**tos protocol ospf**}

構文の説明

aggressive	aggressive drop モードでは、IPv6 SPD が random drop 状態の場合にフォーマットに誤りのあるパケットがドロップされます。
tosprotocolo spf	OSPF モードでは、SPD 優先度で処理する OSPF パケットを使用できます。

コマンド デフォルト

IPv6 SPD モードは設定されません。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

IPv6 SPDモードのデフォルト設定はありませんが、**ipv6spdmode** コマンドを使用して、特定のSPD 状態に到達したときに使用するモードを設定できます。

aggressive キーワードは、IPv6 SPD が random drop 状態のときにフォーマットが崩れているパケットをドロップするaggressive dropモードを有効にします。**ospf** キーワードは、OSPFパケットを SPD 優先度で処理する OSPF モードを有効にします。

プロセス入力キューのサイズによってSDPステートがnormal（ドロップなし）か、random dropか、maxかが決まります。プロセス入力キューがSPDの最小しきい値よりも小さい場合、SPDは何も行わず、normalステートになります。normalステートでは、パケットはドロップされません。入力キューが最大しきい値に到達すると、SPDはmaxステートになります。このステートでは、通常プライオリティのパケットが廃棄されます。入力キューが最小しきい値と最大しきい値の間にある場合、SPD は random drop ステートになります。このステートでは、通常パケットがドロップされることがあります。

例

次に、ルータがrandom drop状態のときにフォーマットが崩れたパケットをルータでドロップできるようにする例を示します。

```
Device(config)# ipv6 spf mode aggressive
```

関連コマンド

コマンド	説明
ipv6spdqueuemax-threshold	IPv6 SPD プロセス入力キュー内の最大パケット数を設定します。
ipv6spdqueuemin-threshold	IPv6 SPD プロセス入力キュー内の最小パケット数を設定します。
showipv6spd	IPv6 SPD 設定を表示します。

ipv6 spd queue max-threshold

IPv6 選択的パケット廃棄（SPD）プロセスの入力キュー内のパケットの最大数を設定するには、グローバル コンフィギュレーション モードで **ipv6spdqueuemax-threshold** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ipv6 spd queue max-threshold *value*
no ipv6 spd queue max-threshold

構文の説明

value	パケット数。指定できる範囲は 0 ～ 65535 です。

コマンド デフォルト

SPD キューの最大しきい値は設定されません。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

SPD キューの最大しきい値を設定するには、**ipv6spdqueuemax-threshold** コマンドを使用します。

プロセス入力キューのサイズによって SDP ステートが normal（ドロップなし）か、random drop か、max かが決まります。プロセス入力キューが SPD の最小しきい値よりも小さい場合、SPD は何も行わず、normal ステートになります。normal ステートでは、パケットはドロップされません。入力キューが最大しきい値に到達すると、SPD は max ステートになります。このステートでは、通常プライオリティのパケットが廃棄されます。入力キューが最小しきい値と最大しきい値の間にある場合、SPD は random drop ステートになります。このステートでは、通常パケットがドロップされることがあります。

例

次に、キューの最大しきい値を 60,000 に設定する例を示します。

```
Device(config)# ipv6 spd queue max-threshold 60000
```

関連コマンド

コマンド	説明
ipv6spdqueuemin-threshold	IPv6 SPD プロセス入力キュー内の最小パケット数を設定します。
showipv6spd	IPv6 SPD 設定を表示します。

ipv6 traffic interface-statistics

すべてのインターフェイスのIPv6転送統計を収集するには、グローバル コンフィギュレーション モードで**ipv6trafficinterface-statistics** コマンドを使用します。どのインターフェイスのIPv6転送統計も収集しないようにするには、このコマンドの **no** 形式を使用します。

ipv6 traffic interface-statistics [unclearable]
no ipv6 traffic interface-statistics [unclearable]

構文の説明

unclearable	（任意）IPv6 転送統計はすべてのインターフェイスについて保管されますが、任意のインターフェイスの統計をクリアすることはできません。

コマンド デフォルト

IPv6 転送統計は、すべてのインターフェイスについて収集されます。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

オプションの unclearable キーワードを使用すると、インターフェイスごとの統計ストレージの要件が半減します。

例

次に、任意のインターフェイス上で統計をクリアできないようにする例を示します。

```
ipv6 traffic interface-statistics unclearable
```

ipv6 unicast-routing

IPv6 ユニキャスト データグラムの転送を有効にするには、グローバル コンフィギュレーション モードで **ipv6unicast-routing** コマンドを使用します。IPv6 ユニキャスト データグラムの転送を無効にするには、このコマンドの **no** 形式を使用します。

ipv6 unicast-routing
no ipv6 unicast-routing

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

IPv6 ユニキャスト ルーティングはディセーブルに設定されています。

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
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

no ipv6unicast-routing コマンドを設定すると、IPv6 ルーティング テーブルから IPv6 ルーティング プロトコルのすべてのエントリが削除されます。

例

次に、IPv6 ユニキャスト データグラムの転送を有効にする例を示します。

```
Device(config)# ipv6 unicast-routing
```

関連コマンド

コマンド	説明
ipv6addresslink-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。
ipv6addresseui-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。
ipv6enable	明示的な IPv6 アドレスが設定されていないインターフェイスにおける IPv6 処理をイネーブルにします。
ipv6unnumbered	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。
showipv6route	IPv6 ルーティング テーブルの現在の内容を表示します。

ipv6 wccp

サービス グループに参加できるように、指定した Web キャッシュ通信プロトコル（WCCP）サービスのサポートを有効にするには、グローバル コンフィギュレーション モードで**ipv6wccp** コマンドを使用します。サービス グループを無効にするには、このコマンドの **no** 形式を使用します。

ipv6 wccp vrf *vrf-name* {**web-cache***service-number*} [**service-list** *service-access-list*] [**mode** {**open**|**closed**}] [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** [{**0**|**7**}] *password*]
no ipv6 wccp vrf *vrf-name* {**web-cache***service-number*} [**service-list** *service-access-list*] [**mode** {**open**|**closed**}] [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** [{**0**|**7**}] *password*]

構文の説明

vrf *vrf-name*	（任意）サービス グループに関連付ける Virtual Routing and Forwarding（VRF）インスタンスを指定します。
web-cache	Web キャッシュ サービスを指定します。 （注） Web キャッシュは、サービスの 1 つです。サービスの最大数（*service-number* 引数で割り当てられたサービスを含む）は 256 です。
service-number	ダイナミック サービス ID。このサービスの定義は、キャッシュによって示されます。ダイナミック サービス番号は 0 ～ 254 の範囲で指定できます。サービスの最大数（**web-cache** キーワードで指定する Web キャッシュ サービスを含む）は 256 です。 （注） シスコのキャッシュ エンジンがサービス グループで使用される場合、リバース プロキシ サービスは、値 99 で指定されます。
service-list *service-access-list*	（任意）サービスと一致するパケットを定義する名前付き拡張 IP アクセス リストを指定します。
mode open	（任意）サービスを開いていると見なします。これがデフォルト サービス モードです。
mode closed	（任意）サービスが閉じていると見なします。
group-address *multicast-address*	（任意）WCCP サービス グループと通信するマルチキャスト IP アドレスを指定します。マルチキャスト アドレスは、ルータが使用してリダイレクトされたメッセージを受信する Web キャッシュを決定します。

redirect-list *access-list*	（任意）このサービス グループにリダイレクトされるトラフィックを制御するアクセス リストを指定します。*access-list* 引数は、アクセス リストを指定する 64 文字以下の長さの文字列（名前または番号）で構成する必要があります。
group-list *access-list*	（任意）サービス グループへの参加を許可する Web キャッシュを決定するアクセスリストを指定します。*access-list* 引数には、標準または拡張アクセス リストの番号または名前を指定します。
password [**0** | **7**] *password*	（任意）サービス グループから受信したメッセージにメッセージ ダイジェスト アルゴリズム 5（MD5）認証を指定します。認証で受け入れられなかったメッセージは廃棄されます。暗号化タイプには 0 ～ 7 のタイプを指定できます。0 は暗号化されないことを、7 は独自の暗号化を示します。*password* 引数の長さは最大 8 文字です。

コマンド デフォルト

WCCP サービスはデフォルトで無効になっています。

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

Release	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

Cisco Express Forwarding スイッチングが有効になっている場合、WCCP の透過的キャッシングはネットワーク アドレス変換（NAT）をバイパスします。この状況に対処するには、発信方向でWCCP透過キャッシングを設定し、コンテンツエンジンインターフェイスでCisco Express Forwarding スイッチングを有効にし、**ipv6wccpweb-cacheredirectout** コマンドを指定します。キャッシュに面するルータ インターフェイスで **ipv6wccpredirectexcludein** コマンドを指定し、内部インターフェイスの着信方向に WCCP を設定します。この設定は、そのインターフェイスに到着したパケットのリダイレクションを回避します。

サービス グループを設定するときにリダイレクト リストを含めることもできます。指定されたリダイレクト リストは、NAT（送信元）IP アドレスを含むパケットを拒否して、リダイレクションを阻止します。

このコマンドは、指定したサービス番号または Web キャッシュ サービス名のサポートを有効または無効にするようにルータに指示します。サービス番号は 0 ～ 254 の範囲で指定できます。サービス番号または名前がイネーブルになると、ルータはサービス グループの確立に参加できます。

vrf キーワードと *vrf-name* 引数のペアは任意です。サービス グループに関連付ける VRF を指定できます。次に、Web キャッシュ サービス名またはサービス番号を指定できます。

同じサービス（Web キャッシュまたはサービス番号）を他の VRF テーブルで設定できます。各サービスは個別に動作します。

noipv6wccp コマンドを入力すると、ルータはサービス グループへの参加を終了し、設定されたサービスがインターフェイスにない場合はスペースの割り当てを解除し、他にサービスが設定されていなければ WCCP タスクを終了します。

web-cache に続くキーワードと *service-number* 引数はオプションで、任意の順序で指定できますが、1 回しか指定できません。以降の各項で、このコマンドのオプション形式それぞれの特定の使用方法について概説します。

ipv6wccp [vrf *vrf-name*] {web-cache | *service-number*} group-address *multicast-address*

ルータと連動するマルチキャストをセットアップするように WCCP グループ アドレスを設定し、Web キャッシュを使用して WCCP プロトコル メッセージを交換できます。このようなアドレスを使用する場合、IPマルチキャストルーティングを有効にし、設定済みのグループ（マルチキャスト）アドレスを使用するメッセージを正しく受信できるようにする必要があります。

このオプションは、このグループ アドレスで受信した「Here I Am」メッセージに対する「I See You」応答を結合するために、指定されたマルチキャスト IP アドレスを使用するようにルータに指示します。また、応答はグループアドレスに送信されます。デフォルトではグループ アドレスは設定されていないため、すべての「Here I Am」メッセージにユニキャスト応答が返されます。

ipv6wccp [vrf *vrf-name*] {web-cache | *service-number*} redirect-list *access-list*

このオプションは、サービス名で指定されたサービス グループの Web キャッシュにリダイレクトされるトラフィックの制御にアクセス リストを使用するようにルータに指示します。*access-list* 引数には、標準または拡張アクセス リストの番号または名前を指定します。アクセス リストは、リダイレクトを許可されるトラフィックを指定します。デフォルトでは、リダイレクト リストは設定されません（すべてのトラフィックがリダイレクトされます）。

WCCP では、次のプロトコルとポートが、いかなるアクセス リストによってもフィルタリングされないようにする必要があります。

- UDP（プロトコル タイプ 17）ポート 2048。このポートを使用してシグナリングを制御します。このタイプのトラフィックをブロックすることで、WCCP によるルータと Web キャッシュ間での接続の確立を阻止します。
- Generic Routing Encapsulation（GRE）（プロトコル タイプ 47 カプセル化フレーム）。このタイプのトラフィックをブロックすることで、代行受信したパケットの表示を阻止します。

ipv6wccp [vrf *vrf-name*] {web-cache | *service-number*} group-list *access-list*

このオプションは、指定したサービス グループへの参加が許可される Web キャッシュの制御にアクセス リストを使用するようにルータに指示します。*access-list* 引数には、標準または拡張アクセス リストの番号、または任意のタイプの名前付きアクセス リストの名前を指定します。アクセス リスト自体は、サービス グループへの参加を許可される Web キャッシュを指定します。デフォルトでは、グループ リストは設定されていないため、すべての Web キャッシュがサービス グループに参加する可能性があります。

（注） The **ipv6wccp** {**web-cache** | *service-number*} **group-list** command syntax resembles the **ipv6wccp** {**web-cache** | *service-number*} **group-listen** command, but these are entirely different commands.**ipv6wccpgroup-listen** コマンドは、キャッシュ クラスタからのマルチキャスト通知を受信するようインターフェイスを設定するのに使用する、インターフェイス コンフィギュレーション コマンドです。『*Cisco IOS IP Application Services Command Reference*』の **ipv6wccpgroup-listen** コマンドの説明を参照してください。

ipv6wccp [vrf *vrf-name*] web-cache | *service-number*} password *password*

このオプションは、指定したサービス名で、指定したサービス グループから受信したメッセージのMD5認証を使用するようにルータに指示します。この形式のコマンドを使用すると、ルータ上にパスワードを設定できます。また、各 Web キャッシュ上に同じパスワードを個別に設定する必要があります。パスワードは最大8文字を使用できます。ルータで認証がイネーブルになっているとき、認証されないメッセージは廃棄されます。デフォルトは認証パスワードは設定されておらず、認証はディセーブルになっています。

ipv6wccp *service-number* service-list *service-access-list*modeclosed

機能処理を適用する目的で、外部仲介デバイスに対する WCCP パケットの代行受信とリダイレクションが Cisco IOS ソフトウェアで利用できないアプリケーションでは、仲介デバイスが利用できないときにアプリケーションのパケットをブロックする必要があります。このブロックは、クローズド サービスと呼ばれます。デフォルトでは、WCCP はオープン サービスとして動作します。この場合、中間デバイスがなくても、クライアントとサーバ間の通信は正常に進行します。**service-list** キーワードを使用できるのは、クローズド モード サービスの場合だけです。WCCPサービスをクローズドに設定すると、WCCPが、トラフィックを受信するためのクライアントアプリケーションが登録されていないパケットを破棄します。**service-list** キーワードと *service-access-list* 引数は、アプリケーション プロトコル タイプまたはポート番号を登録するために使用します。

サービス リスト内のサービスの定義と WCCP プロトコルを介して受信した宛て先が競合する場合、次のような警告メッセージが表示されます。

```
Sep 28 14:06:35.923: %WCCP-5-SERVICEMISMATCH: Service 90 mismatched on WCCP client
10.1.1.13
```

サービス リストの定義に競合がある場合、WCCP プロトコル メッセージを介して受信した外部定義よりも設定した定義が優先されます。

例

次に、マルチキャスト アドレス 239.0.0.0 を使用して、WCCP 逆プロキシ サービスを実行するように Device を設定する例を示します。

```
Device(config)# ipv6 multicast-routing
Device(config)# ipv6 wccp 99 group-address 239.0.0.0
Device(config)# interface ethernet 0
Device(config-if)# ipv6 wccp 99 group-listen
```

次に、宛て先が 10.168.196.51 以外の Web 関連パケットを Web キャッシュにリダイレクトするように Device を設定する例を示します。

```
Device(config)# access-list 100 deny ip any host 10.168.196.51
Device(config)# access-list 100 permit ip any any
Device(config)# ipv6 wccp web-cache redirect-list 100
Device(config)# interface ethernet 0
Device(config-if)# ipv6 wccp web-cache redirect out
```

次に、ネットワーク 10.0.0.0 からのトラフィックがファスト イーサネット インターフェイス 0/0 を離れないようにアクセス リストを設定する例を示します。アウトバウンドアクセスコントロールリスト（ACL）チェックが有効になっているため、WCCP はそのトラフィックをリダイレクトしません。WCCP は、パケットのリダイレクト前に、ACL に対してパケットをチェックします。

```
Device(config)# ipv6 wccp web-cache
Device(config)# ipv6 wccp check acl outbound
Device(config)# interface fastethernet0/0
Device(config-if)# ip access-group 10 out
Device(config-if)# ipv6 wccp web-cache redirect out
Device(config-if)# access-list 10 deny 10.0.0.0 0.255.255.255
Device(config-if)# access-list 10 permit any
```

アウトバウンド ACL チェックが無効になっている場合、ネットワーク 10.0.0.0 からの HTTP パケットはキャッシュにリダイレクトされます。ネットワーク管理者がその動作が行われないようにする場合、そのネットワーク アドレスを持つユーザは Web ページを取得できることがあります。

次に、閉じられた WCCP サービスを設定する例を示します。

```
Device(config)# ipv6 wccp 99 service-list access1 mode closed
```

関連コマンド

コマンド	説明
ipv6wccpcheckservicesall	すべての WCCP サービスをイネーブルにします。
ipv6wccpredirectexcludein	インターフェイスで受信したパケットを、リダイレクトのチェックから除外するようにインターフェイスを設定します。
showipv6wccp	WCCP に関連するグローバル統計情報を表示します。

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するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6access-list** コマンドを使用します。

show ipv6 access-list [*access-list-name*]

構文の説明

access-list-name	（任意）アクセス リストの名前

コマンド デフォルト

すべての IPv6 アクセス リストが表示されます。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

showipv6access-list コマンドの出力は、IPv6 に固有である点を除き、**showipaccess-list** コマンドの出力と似ています。

例

次の **showipv6access-list** コマンドの出力には、inbound、tcptraffic、および outbound という IPv6 アクセス リストが表示されます。

```
Device# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
    permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
    permit udp any any reflect udptraffic sequence 30
IPv6 access list tcptraffic (reflexive) (per-user)
    permit tcp host 2001:0DB8:1::1 eq bgp host 2001:0DB8:1::2 eq 11000 timeout 300 (time
         left 243) sequence 1
    permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300
       (time left 296) sequence 2
IPv6 access list outbound
    evaluate udptraffic
    evaluate tcptraffic
```

次に、IPSec で使用する IPv6 アクセス リスト情報を表示する例を示します。

```
Device#  show ipv6 access-list
IPv6 access list Tunnel0-head-0-ACL (crypto)
     permit ipv6 any any (34 matches) sequence 1
IPv6 access list Ethernet2/0-ipsecv6-ACL (crypto)
     permit 89 FE80::/10 any (85 matches) sequence 1
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *1 : show ipv6 access-list* フィールドの説明

フィールド	説明
ipv6 access list inbound	IPv6 アクセス リスト名（例：inbound）。
permit	指定されたプロトコル タイプと一致するパケットを許可します。
tcp	伝送制御プロトコル。パケットが一致しなければならない高いレベル（レイヤ 4）のプロトコル タイプ。
any	::/0 と同じです。
eq	TCP または UDP パケットの送信元または宛先ポートを比較する equal オペランド。
bgp	ボーダー ゲートウェイ プロトコル。パケットが一致しなければならない低いレベル（レイヤ 3）のプロトコル タイプ。
reflect	再帰 IPv6 アクセス リストを示します。
tcptraffic (8 matches)	再帰 IPv6 アクセス リストの名前と、そのアクセス リストの一致数。**clearipv6access-list** 特権 EXEC コマンドは IPv6 アクセス リストの一致カウンタをリセットします。
sequence 10	着信パケットが比較されるアクセス リストの行のシーケンス。アクセス リストの行は、最初のプライオリティ（最低の数、たとえば 10）から最後のプライオリティ（最高の数、たとえば 80）の順に並んでいます。
host 2001:0DB8:1::1	パケットの送信元アドレスが一致していなければならない送信元 IPv6 ホスト アドレス。
host 2001:0DB8:1::2	パケットの宛て先アドレスが一致していなければならない宛て先 IPv6 ホスト アドレス。
11000	発信接続用の一時送信元ポート番号。
timeout 300	tcptraffic という一時 IPv6 再帰アクセス リストが指定したセッションでタイム アウトするまでのアイドル時間の総間隔（秒単位）。
(time left 243)	tcptraffic という一時 IPv6 再帰アクセス リストが指定したセッションで削除されるまでの残りのアイドル時間（秒単位）。指定したセッションに一致する追加の受信トラフィックがこの値を 300 秒にリセットします。

フィールド	説明
evaluate udptraffic	udptraffic という IPv6 再帰アクセス リストが outbound という IPv6 アクセス リスト内に入れ子になっていることを示します。

関連コマンド

コマンド	説明
clearipv6access-list	IPv6 アクセス リストの一致カウンタをリセットします。
hardwarestatistics	ハードウェア統計情報の収集をイネーブルにします。
showipaccess-list	現在のすべての IP アクセス リストの内容を表示します。
showipprefix-list	プレフィックス リストまたはプレフィックス リスト エントリに関する情報を表示します。
showipv6prefix-list	IPv6 プレフィックス リストまたは IPv6 プレフィックス リストのエントリに関する情報を表示します。

show ipv6 destination-guard policy

宛て先ガード情報を表示するには、特権 EXEC モードで **showipv6destination-guardpolicy** コマンドを使用します。

show ipv6 destination-guard policy [*policy-name*]

構文の説明

policy-name	（任意）宛て先ガードポリシーの名前。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

policy-name 引数を指定すると、指定したポリシー情報のみが表示されます。*policy-name* 引数を指定しないと、すべてのポリシーの情報が表示されます。

例

次に、ポリシーを VLAN に適用した場合の **showipv6destination-guardpolicy** コマンドの出力例を示します。

```
Device# show ipv6 destination-guard policy pol1
Destination guard policy destination:
  enforcement always
        Target: vlan 300
```

次に、ポリシーをインターフェイスに適用した場合の **showipv6destination-guardpolicy** コマンドの出力例を示します。

```
Device# show ipv6 destination-guard policy pol1
Destination guard policy destination:
  enforcement always
        Target: Gi0/0/1
```

関連コマンド

コマンド	説明
ipv6destination-guard policy	宛て先ガードポリシーを定義します。

show ipv6 dhcp

指定したデバイス上の Dynamic Host Configuration Protocol（DHCP）固有識別子（DUID）を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6dhcp** コマンドを使用します。

show ipv6 dhcp

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 モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

showipv6dhcp コマンドは、クライアント識別子とサーバ識別子の両方にリンクレイヤ アドレスに基づく DUID を使用します。デバイスは、最も小さい番号のインターフェイスの MAC アドレスを使用して DUID を形成します。ネットワーク インターフェイスは、デバイスに永続的に接続されていると見なされます。デバイスの DUID を表示するには、**showipv6dhcp** コマンドを使用します。

例

次は、**showipv6dhcp** コマンドの出力例です。出力の内容は一目瞭然です。

```
Device# show ipv6 dhcp
This device's DHCPv6 unique identifier(DUID): 000300010002FCA5DC1C
```

show ipv6 dhcp binding

IPv6 サーバのバインディング テーブルの Dynamic Host Configuration Protocol（DHCP）から自動クライアント バインディングを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6dhcpbinding** コマンドを使用します。

show ipv6 dhcp binding [*ipv6-address*] [**vrf** *vrf-name*]

構文の説明

ipv6-address	（任意）IPv6 クライアントの DHCP のアドレス。
vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

showipv6dhcpbinding コマンドは、*ipv6-address* 引数を指定しないと、IPv6 サーバ バインディング テーブルの DHCPからすべての自動クライアント バインディングを表示します。*ipv6-address* 引数が指定されている場合、指定したクライアントのバインディングだけが表示されます。

vrf キーワードと *vrf-name* 引数の組み合わせを使用すると、指定した VRF に属するすべてのバインディングが表示されます。

例

次に、IPv6 サーバ バインディング テーブルの DHCP からすべての自動クライアント バインディングが表示された出力例を示します。

```
Device# show ipv6 dhcp binding
Client: FE80::A8BB:CCFF:FE00:300
  DUID: 00030001AABBCC000300
  Username : client_1
  Interface: Virtual-Access2.1
  IA PD: IA ID 0x000C0001, T1 75, T2 135
    Prefix: 2001:380:E00::/64
            preferred lifetime 150, valid lifetime 300
            expires at Dec 06 2007 12:57 PM (262 seconds)
Client: FE80::A8BB:CCFF:FE00:300 (Virtual-Access2.2)
  DUID: 00030001AABBCC000300
  IA PD: IA ID 0x000D0001, T1 75, T2 135
    Prefix: 2001:0DB8:E00:1::/64
            preferred lifetime 150, valid lifetime 300
            expires at Dec 06 2007 12:58 PM (288 seconds)
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *2 : show ipv6 dhcp binding* フィールドの説明

フィールド	説明
Client	指定したクライアントのアドレス。
DUID	DHCP 固有識別子（DUID）。
Virtual-Access2.1	最初の仮想クライアント。IPv6 DHCP クライアントが 2 つのプレフィックスを要求し、そのプレフィックスの DUID が同じで、プレフィックス委任（IAPD）に 2 つの異なるインターフェイスで異なる ID の関連付けがある場合、これらのプレフィックスは 2 つの異なるクライアント用として見なされ、両方のインターフェイス情報が保持されます。
Username : client_1	バインディングに関連付けられているユーザ名。
IA PD	クライアントに関連付けられているプレフィックスのコレクション。
IA ID	この IAPD の識別子。
Prefix	指定したクライアント上に指定された IAPD に委任されたプレフィックス。
preferred lifetime, valid lifetime	指定したクライアントの優先ライフタイムと有効なライフタイム設定（秒単位）。
Expires at	有効なライフタイムの有効期限が切れる日時。
Virtual-Access2.2	2 番目の仮想クライアント。IPv6 DHCP クライアントが 2 つのプレフィックスを要求し、そのプレフィックスの DUID が同じで IAID が 2 つの異なるインターフェイス上で異なる場合、これらのプレフィックスは 2 つの異なるクライアント用と見なされ、両方のインターフェイス情報が保持されます。

Cisco IOS DHCPv6 サーバの DHCPv6 プールを設定して、認証、認可、およびアカウンティング（AAA）サーバから委任のプレフィックスを取得すると、着信 PPP セッションから AAA サーバに PPP ユーザ名が送信され、プレフィックスを取得します。バインディングに関連付けられている PPP ユーザ名が **showipv6dhcpbinding** コマンドの出力に表示されます。バインディングに関連付けられている PPP ユーザ名がない場合、このフィールドには値として「unassigned」が表示されます

次に、バインディングに関連付けられている PPP ユーザ名が「client_1」である例を示します。

```
Device# show ipv6 dhcp binding
Client: FE80::2AA:FF:FEBB:CC
  DUID: 0003000100AA00BB00CC
```

```
  Username : client_1
  Interface : Virtual-Access2
  IA PD: IA ID 0x00130001, T1 75, T2 135
    Prefix: 2001:0DB8:1:3::/80
            preferred lifetime 150, valid lifetime 300
            expires at Aug 07 2008 05:19 AM (225 seconds)
```

次に、バインディングに関連付けられている値が「unassigned」である例を示します。

```
Device# show ipv6 dhcp binding
Client: FE80::2AA:FF:FEBB:CC
  DUID: 0003000100AA00BB00CC
  Username : unassigned
  Interface : Virtual-Access2
  IA PD: IA ID 0x00130001, T1 150, T2 240
    Prefix: 2001:0DB8:1:1::/80
            preferred lifetime 300, valid lifetime 300
            expires at Aug 11 2008 06:23 AM (233 seconds)
```

関連コマンド

コマンド	説明
clearipv6dhcpbinding	DHCP for IPv6 バインディング テーブルから自動クライアント バインディングを削除します。

show ipv6 dhcp conflict

アドレスがクライアントに提供されるときに Dynamic Host Configuration Protocol for IPv6（DHCPv6）サーバが検出したアドレス競合を表示するには、特権 EXEC モードで **showipv6dhcpconflict** コマンドを使用します。

show ipv6 dhcp conflict [*ipv6-address*] [**vrf** *vrf-name*]

構文の説明

ipv6-address	（任意）IPv6 クライアントの DHCP のアドレス。
vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

競合を検出するようにDHCPv6サーバを設定する場合、DHCPv6サーバはpingを使用します。クライアントはネイバー探索を使用してクライアントを検出し、DECLINE メッセージを介してサーバに報告します。アドレス競合が検出されると、このアドレスはプールから削除されます。管理者がこのアドレスを競合リストから削除するまでこのアドレスは割り当てることができません。

例

次に、**showipv6dhcpconflict** コマンドの出力例を示します。このコマンドは DHCP 競合のプール値とプレフィックス値を表示します。

```
Device# show ipv6 dhcp conflict
Pool 350, prefix 2001:0DB8:1005::/48
     2001:0DB8:1005::10
```

関連コマンド

コマンド	説明
clear ipv6 dhcp conflict	DHCPv6サーバデータベースからアドレス競合をクリアします。

show ipv6 dhcp database

IPv6 バインディング データベース エージェント情報の Dynamic Host Configuration Protocol（DHCP）を表示するには、ユーザ EXEC モードまたは特権モードで **showipv6dhcpdatabase** コマンドを使用します。

show ipv6 dhcp database [*agent-URL*]

構文の説明

agent-URL	（任意）フラッシュ、NVRAM、FTP、TFTP、または Remote Copy Protocol（RCP）の Uniform Resource Locator。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

バインディング データベースが保存される永続的な各ストレージのことをデータベース エージェントと呼びます。エージェントを設定するには、**ipv6dhcpdatabase** コマンドを使用します。サポート対象のデータベース エージェントには、FTP サーバや TFTP サーバ、RCP、フラッシュ ファイル システム、NVRAM などがあります。

showipv6dhcpdatabase コマンドは、DHCP for IPv6 バインディング データベース エージェントの情報を表示します。*agent-URL* 引数が指定される場合、指定されたエージェントだけが表示されます。*agent-URL* 引数が指定されていない場合、すべてのデータベース エージェントが表示されます。

例

次は、**showipv6dhcpdatabase** コマンドの出力例です。

```
Device# show ipv6 dhcp database
Database agent tftp://172.19.216.133/db.tftp:
  write delay: 69 seconds, transfer timeout: 300 seconds
  last written at Jan 09 2003 01:54 PM,
     write timer expires in 56 seconds
  last read at Jan 06 2003 05:41 PM
  successful read times 1
  failed read times 0
  successful write times 3172
  failed write times 2
Database agent nvram:/dhcpv6-binding:
  write delay: 60 seconds, transfer timeout: 300 seconds
  last written at Jan 09 2003 01:54 PM,
     write timer expires in 37 seconds
  last read at never
```

```
  successful read times 0
  failed read times 0
  successful write times 3325
  failed write times 0
Database agent flash:/dhcpv6-db:
  write delay: 82 seconds, transfer timeout: 3 seconds
  last written at Jan 09 2003 01:54 PM,
    write timer expires in 50 seconds
  last read at never
  successful read times 0
  failed read times 0
  successful write times 2220
  failed write times 614
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *3 : show ipv6 dhcp database* フィールドの説明

フィールド	説明
Database agent	データベース エージェントを指定します。
Write delay	データベースを更新するまでの待機時間（秒単位）。
transfer timeout	データベースの転送を中断するまでに DHCP サーバが待機する時間（秒単位）を指定します。タイムアウト期間を超えた転送は中断されます。
Last written	バインディングがファイル サーバに書き込まれた最後の日付と時刻。
Write timer expires...	書き込みタイマーの期限が切れるまでの時間（秒単位）。
Last read	バインディングがファイル サーバから読み取られた最後の日付と時刻。
Successful/failed read times	読み取りの成功回数と失敗回数。
Successful/failed write times	書き込みの成功回数と失敗回数。

関連コマンド

コマンド	説明
ipv6dhcpdatabase	DHCP for IPv6 バインディング データベース エージェントのパラメータを指定します。

show ipv6 dhcp guard policy

Dynamic Host Configuration Protocol for IPv6（DHCPv6）ガード情報を表示するには、特権 EXEC モードで **showipv6dhcpguardpolicy** コマンドを使用します。

show ipv6 dhcp guard policy [*policy-name*]

構文の説明

policy-name	（任意）DHCPv6 ガードポリシー名。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

policy-name 引数を指定すると、指定したポリシー情報のみが表示されます。*policy-name* 引数を指定しないと、すべてのポリシーの情報が表示されます。

例

次に、**showipv6dhcpguardguard** コマンドの出力例を示します。

```
Device#show ipv6 dhcp guard policy

Dhcp guard policy: default
        Device Role: dhcp client
        Target: Et0/3

Dhcp guard policy: test1
        Device Role: dhcp server
        Target: vlan 0    vlan 1    vlan 2    vlan 3    vlan 4
        Max Preference: 200
        Min Preference: 0
        Source Address Match Access List: acl1
        Prefix List Match Prefix List: pfxlist1

Dhcp guard policy: test2
        Device Role: dhcp relay
        Target: Et0/0 Et0/1 Et0/2
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *4 : show ipv6 dhcp guard* フィールドの説明

フィールド	説明
Device Role	デバイスのロール。ロールは、クライアント、サーバ、またはリレーのいずれかです。
Target	ターゲットの名前。ターゲットは、インターフェイスまたはVLANのいずれかです。

関連コマンド

コマンド	説明
ipv6dhcpguardpolicy	DHCPv6ガードポリシー名を定義します。

show ipv6 dhcp interface

IPv6 インターフェイス情報の Dynamic Host Configuration Protocol（DHCP）を表示するには、ユーザ EXEC モードまたは特権モードで **showipv6dhcpinterface** コマンドを使用します。

show ipv6 dhcp interface [*type number*]

構文の説明

type 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 モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

インターフェイスが指定されていない場合は、IPv6用DHCP（クライアントまたはサーバ）がイネーブルになっているすべてのインターフェイスが表示されます。インターフェイスが指定される場合、指定されているインターフェイスに関する情報だけが表示されます。

例

次に、**showipv6dhcpinterface** コマンドの出力例を示します。最初の例では、DHCP for IPv6 サーバとして機能するインターフェイスを持つルータでコマンドを使用しています。2 番目の例では、DHCP for IPv6 クライアントとして機能するインターフェイスを持つルータでコマンドを使用しています。

```
Device# show ipv6 dhcp interface
Ethernet2/1 is in server mode
  Using pool: svr-p1
  Preference value: 20
  Rapid-Commit is disabled
Router2# show ipv6 dhcp interface
Ethernet2/1 is in client mode
  State is OPEN (1)
  List of known servers:
    Address: FE80::202:FCFF:FEA1:7439, DUID 000300010002FCA17400
    Preference: 20
      IA PD: IA ID 0x00040001, T1 120, T2 192
        Prefix: 3FFE:C00:C18:1::/72
                preferred lifetime 240, valid lifetime 54321
                expires at Nov 08 2002 09:10 AM (54319 seconds)
        Prefix: 3FFE:C00:C18:2::/72
                preferred lifetime 300, valid lifetime 54333
                expires at Nov 08 2002 09:11 AM (54331 seconds)
        Prefix: 3FFE:C00:C18:3::/72
                preferred lifetime 280, valid lifetime 51111
                expires at Nov 08 2002 08:17 AM (51109 seconds)
```

```
    DNS server: 1001::1
    DNS server: 1001::2
    Domain name: domain1.net
    Domain name: domain2.net
    Domain name: domain3.net
  Prefix name is cli-p1
  Rapid-Commit is enabled
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *5 : show ipv6 dhcp interface* フィールドの説明

フィールド	説明
Ethernet2/1 is in server/client mode	指定したインターフェイスがサーバモードまたはクライアントモードのいずれであるかを表示します。
Preference value:	指定したサーバのアドバタイズされた（またはデフォルトの 0 の）プリファレンス値。
Prefix name is cli-p1	このインターフェイス上で正常に取得したプレフィックスを格納する IPv6 汎用プレフィックス プール名を表示します。
Using pool: svr-p1	インターフェイスが使用しているプールの名前。
State is OPEN	このインターフェイス上の DHCP for IPv6 クライアントの状態。「Open」は、設定情報を受信したことを示します。
List of known servers	インターフェイス上のサーバのリストを表示します。
Address, DUID	指定したインターフェイス上で聴取したサーバのアドレスと DHCP 固有識別子（DUID）。
Rapid commit is disabled	**rapid-commit** キーワードがインターフェイス上で有効になっているかどうかを表示します。

次に、FastEthernet インターフェイス 0/0 上の DHCP for IPv6 リレー エージェントの設定と **showipv6dhcpinterface** コマンドを使用した FastEthernet インターフェイス 0/0 上のリレー エージェント情報の表示の例を示します。

```
Device(config-if)# ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 FastEthernet0/1
Device# show ipv6 dhcp interface FastEthernet 0/0
FastEthernet0/0 is in relay mode
  Relay destinations:
    FE80::250:A2FF:FEBF:A056 via FastEthernet0/1
```

関連コマンド

コマンド	説明
ipv6dhcpclientpd	DHCP for IPv6 クライアント プロセスを有効にし、指定したインターフェイスを通じてプレフィックス委任の要求を有効にします。

コマンド	説明
ipv6dhcprelaydestination	クライアント メッセージを転送する宛て先アドレスを指定し、インターフェイスで DHCP for IPv6 リレー サービスを有効にします。
ipv6dhcpserver	インターフェイス上で DHCP for IPv6 サービスを有効にします。

show ipv6 dhcp relay binding

DHCPv6 Internet Assigned Numbers Authority（IANA）と DHCPv6 Identity Association for Prefix Delegation（IAPD）のリレーエージェント上でのバインディングを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6dhcprelaybinding** コマンドを使用します。

show ipv6 dhcp relay binding [**vrf** *vrf-name*]

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

vrf キーワードと *vrf-name* 引数のペアを指定すると、指定した VRF に属するすべてのバインディングが表示されます。

（注） リレー エージェント上の DHCPv6 IAPD バインディングは、Cisco uBR10012 および Cisco uBR7200 シリーズのユニバーサル ブロードバンド デバイス上に表示されます。

例

次に、**showipv6dhcprelaybinding** コマンドの出力例を示します。

```
Device# show ipv6 dhcp relay binding
```

次に、Cisco uBR10012 ユニバーサル ブロードバンド デバイス上に指定した VRF 名を使用した **show ipv6 dhcp relay binding** コマンドの出力例を示します。

```
Device# show ipv6 dhcp relay binding vrf vrf1

Prefix: 2001:DB8:0:1:/64 (Bundle100.600)
  DUID: 000300010023BED94D31
  IAID: 3201912114
  lifetime: 600
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *6 : show ipv6 dhcp relay binding* フィールドの説明

フィールド	説明
Prefix	DHCP の IPv6 プレフィックス。
DUID	IPv6 リレーバインディングの DHCP 固有識別子（DUID）。
IAID	DHCP のアイデンティティ関連付け識別（IAID）。
lifetime	プレフィックスのライフタイム（秒単位）。

関連コマンド

コマンド	説明
clear ipv6 dhcp relaybinding	IPv6 リレー バインディングの DHCP の特定の IPv6 アドレスまたは IPv6 プレフィックスをクリアします。

show ipv6 eigrp events

IPv6 について記録された Enhanced Interior Gateway Routing Protocol（EIGRP）イベントを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6eigrpevents** コマンドを使用します。

show ipv6 eigrp events [{[{**errmsg**|**sia**}] [*event-num-start event-num-end*]|**type**}]

構文の説明

errmsg	（任意）ログに記録されているエラー メッセージを表示します。
sia	（任意）Stuck In Active（SIA）メッセージを表示します。
event-num-start	（任意）イベントの範囲の開始番号。範囲は 1 ～ 4294967295 です。
event-num-end	（任意）イベントの範囲の終了番号。範囲は 1 ～ 4294967295 です。
type	（任意）ログに記録されているイベント タイプを表示します。

コマンド デフォルト

イベントの範囲を指定しないと、IPv6 EIGRP のすべてのイベントに関する情報が表示されます。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

showipv6eigrpevents コマンドは、シスコサポートチームがネットワーク障害の分析に使用します。一般的な使用は意図していません。このコマンドは、EIGRP に関する内部状態情報と、ルート通知と変更の処理方法を表示します。

例

次に、**showipv6eigrpevents** コマンドの出力例を示します。フィールドの説明は自明です。

```
Device# show ipv6 eigrp events
Event information for AS 65535:
1    00:56:41.719 State change: Successor Origin Local origin
2    00:56:41.719 Metric set: 2555:5555::/32 4294967295
3    00:56:41.719 Poison squashed: 2555:5555::/32 lost if
4    00:56:41.719 Poison squashed: 2555:5555::/32 rt gone
5    00:56:41.719 Route installing: 2555:5555::/32 FE80::ABCD:4:EF00:1
6    00:56:41.719 RDB delete: 2555:5555::/32 FE80::ABCD:4:EF00:2
7    00:56:41.719 Send reply: 2555:5555::/32 FE80::ABCD:4:EF00:1
```

```
8    00:56:41.719 Find FS: 2555:5555::/32 4294967295
9    00:56:41.719 Free reply status: 2555:5555::/32
10   00:56:41.719 Clr handle num/bits: 0 0x0
11   00:56:41.719 Clr handle dest/cnt: 2555:5555::/32 0
12   00:56:41.719 Rcv reply met/succ met: 4294967295 4294967295
13   00:56:41.719 Rcv reply dest/nh: 2555:5555::/32 FE80::ABCD:4:EF00:2
14   00:56:41.687 Send reply: 2555:5555::/32 FE80::ABCD:4:EF00:2
15   00:56:41.687 Rcv query met/succ met: 4294967295 4294967295
16   00:56:41.687 Rcv query dest/nh: 2555:5555::/32 FE80::ABCD:4:EF00:2
17   00:56:41.687 State change: Local origin Successor Origin
18   00:56:41.687 Metric set: 2555:5555::/32 4294967295
19   00:56:41.687 Active net/peers: 2555:5555::/32 65536
20   00:56:41.687 FC not sat Dmin/met: 4294967295 2588160
21   00:56:41.687 Find FS: 2555:5555::/32 2588160
22   00:56:41.687 Rcv query met/succ met: 4294967295 4294967295
23   00:56:41.687 Rcv query dest/nh: 2555:5555::/32 FE80::ABCD:4:EF00:1
24   00:56:41.659 Change queue emptied, entries: 1
25   00:56:41.659 Metric set: 2555:5555::/32 2588160
```

関連コマンド

コマンド	説明
clearipv6eigrp	EIGRP for IPv6 ルーティング テーブルからエントリを削除します。
debugipv6eigrp	IPv6 プロトコル用の EIGRP に関する情報を表示します。
ipv6eigrp	指定したインターフェイスで EIGRP for IPv6 を有効にします。

show ipv6 eigrp interfaces

IPv6 トポロジで Enhanced Interior Gateway Routing Protocol（EIGRP）に設定されているインターフェイスに関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6eigrpinterfaces** コマンドを使用します。

show ipv6 eigrp [*as-number*] **interfaces** [*type number*] **[detail]**

構文の説明

as-number	（任意）自律システム番号。
type	（任意）インターフェイス タイプ。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。
number	（任意）インターフェイス番号。ネットワーキング デバイスに対する番号付け構文の詳細については、疑問符（?）のオンライン ヘルプ機能を使用してください。
detail	（任意）インターフェイスの詳細情報を表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

EIGRP がアクティブになっているインターフェイスを特定し、それらのインターフェイスに関連する EIGRP プロセスの情報を取得するには、**showipv6eigrpinterfaces** コマンドを使用します。オプションの *type number* 引数と **detail** キーワードは任意の順序で入力できます。

インターフェイスが指定された場合、そのインターフェイスのみが表示されます。指定されない場合、EIGRP を実行しているすべてのインターフェイスが表示されます。

自律システムが指定された場合、指定された自律システムについてのルーティング プロセスのみが表示されます。指定されない場合、すべての EIGRP プロセスが表示されます。

例

次に、**showipv6eigrpinterfaces** コマンドの出力例を示します。

```
Device# show ipv6 eigrp 1 interfaces

IPv6-EIGRP interfaces for process 1
                     Xmit Queue    Mean    Pacing Time    Multicast     Pending
Interface    Peers   Un/Reliable   SRTT    Un/Reliable    Flow Timer    Routes
Et0/0         0         0/0          0        0/10            0          0
```

次に、**showipv6eigrpinterfaces detail** コマンドの出力例を示します。

```
Device# show ipv6 eigrp interfaces detail

IPv6-EIGRP interfaces for process 1
                     Xmit Queue    Mean    Pacing Time    Multicast    Pending
Interface    Peers   Un/Reliable   SRTT    Un/Reliable    Flow Timer    Routes
Et0/0          0        0/0           0        0/10           0           0
Hello interval is 5 sec
Next xmit serial <none>
Un/reliable mcasts: 0/0 Un/reliable ucasts: 0/0
Mcast exceptions: 0 CR packets: 0 ACKs suppressed: 0
Retransmissions sent: 0 Out-of-sequence rcvd: 0
Authentication mode is not set
```

次に、**no ipv6 next-hop self** コマンドを **no-ecmp-mode** オプションを指定して設定した特定のインターフェイスに関する詳細情報を表示する **show ipv6 eigrp interface detail** コマンドの出力例を示します。

```
DeviceDevice# show ipv6 eigrp interfaces detail tunnel 0

EIGRP-IPv6 Interfaces for AS(1)
                      Xmit Queue   PeerQ        Mean   Pacing Time   Multicast   Pending

Interface        Peers  Un/Reliable  Un/Reliable  SRTT   Un/Reliable   Flow Timer
Routes
Tu0/0              2        0/0       0/0          29       0/0         136           0
Hello-interval is 5, Hold-time is 15
  Split-horizon is disabled
  Next xmit serial <none>
  Packetized sent/expedited: 48/1
  Hello's sent/expedited: 13119/49
  Un/reliable mcasts: 0/20  Un/reliable ucasts: 31/398
  Mcast exceptions: 5  CR packets: 5  ACKs suppressed: 1
  Retransmissions sent: 355  Out-of-sequence rcvd: 6
  Next-hop-self disabled, next-hop info forwarded, ECMP mode Enabled
  Topology-ids on interface - 0
  Authentication mode is not set
```

下の表で、この出力で表示される重要なフィールドについて説明します。

表 *7: show ipv6 eigrp interfaces* フィールドの説明

フィールド	説明
Interface	EIGRP が設定されているインターフェイス
Peers	直接接続された EIGRP ネイバーの数。
Xmit Queue Un/Reliable	信頼性の低い送信キューおよび信頼性の高い送信キューに残っているパケットの数。
Mean SRTT	平均スムーズ ラウンドトリップ時間（SRTT）間隔（秒単位）
Pacing Time Un/Reliable	インターフェイスから EIGRP パケット（信頼性の低いパケットおよび信頼性の高いパケット）を送信するタイミングを決定するために使用するペーシング時間（秒単位）。
Multicast Flow Timer	デバイスがマルチキャスト EIGRP パケットを送信する最大秒数。

フィールド	説明
Pending Routes	送信キュー内で送信を待機しているルートの数。
Hello interval is 5 sec	hello 間隔の時間（秒単位）。

show ipv6 eigrp topology

Enhanced Interior Gateway Routing Protocol（EIGRP）IPv6 トポロジ テーブルのエントリを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6eigrptopology** コマンドを使用します。

show ipv6 eigrp topology [{*as-number ipv6-address*}] [{**active**|**all-links**|**pending**|**summary**|**zero-successors**}]

構文の説明

as-number	（任意）自律システム番号。
ipv6-address	（任意）IPv6 アドレス。
active	（任意）EIGRP トポロジ テーブル内のアクティブ エントリのみ表示します。
all-links	（任意）（到達不能な後継ソースを含む）EIGRP トポロジ テーブル内の全エントリを表示します。
pending	（任意）ネイバーからのアップデートを待機しているか、ネイバーへの応答を待機している、EIGRP トポロジテーブル内のすべてのエントリを表示します。
summary	（任意）EIGRP トポロジ テーブルの要約を表示します。
zero-successors	（任意）サクセサがない利用可能なルートを表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

このコマンドがキーワードや引数なしで使用される場合、到達可能な後継ルータのルートだけが表示されます。**showipv6eigrptopology** コマンドを使用すると、Diffusing Update Algorithm（DUAL）の状態を判断し、起こり得る DUAL の問題をデバッグできます。

例

次に、**showipv6eigrptopology** コマンドの出力例を示します。出力にはフィールドの説明も表示されます。

```
Device# show ipv6 eigrp topology

IPv6-EIGRP Topology Table for AS(1)/ID(2001:0DB8:10::/64)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status
```

```
P 2001:0DB8:3::/64, 1 successors, FD is 281600
via Connected, Ethernet1/0
```

次に、EIGRP トポロジに **no-ecmp-mode** を指定せずに **no ipv6 next-hop-self** コマンドを設定した場合に ECMP モード情報を表示する **show ipv6 eigrp topology** *prefix* コマンドの出力例を示します。ECMP モードは、アドバタイズされているパスに関する情報を提供します。複数のサクセサが存在する場合、一番上のパスがすべてのインターフェイス上のデフォル トパスとしてアドバタイズされ、出力に「ECMP Mode: Advertise by default」というメッセージが表示されます。デフォルト パス以外のパスがアドバタイズされる場合は、「ECMP Mode: Advertise out <Interface name>」というメッセージが表示されます。出力にはフィールドの説明も表示されます。

```
Device# show ipv6 eigrp topology 2001:DB8:10::1/128

EIGRP-IPv6 Topology Entry for AS(1)/ID(192.0.2.100) for 2001:DB8:10::1/128
  State is Passive, Query origin flag is 1, 2 Successor(s), FD is 284160
  Descriptor Blocks:
  FE80::A8BB:CCFF:FE01:2E01 (Tunnel0), from FE80::A8BB:CCFF:FE01:2E01, Send flag is 0x0
      Composite metric is (284160/281600), route is Internal
      Vector metric:
        Minimum bandwidth is 10000 Kbit
        Total delay is 1100 microseconds
        Reliability is 255/255
        Load is ½55
        Minimum MTU is 1400
        Hop count is 1
        Originating router is 10.10.1.1
      ECMP Mode: Advertise by default
FE80::A8BB:CCFF:FE01:3E01 (Tunnel1), from FE80::A8BB:CCFF:FE01:3E01, Send flag is 0x0
      Composite metric is (284160/281600), route is Internal
      Vector metric:
        Minimum bandwidth is 10000 Kbit
        Total delay is 1100 microseconds
        Reliability is 255/255
        Load is ½55
        Minimum MTU is 1400
        Hop count is 1
        Originating router is 10.10.2.2
      ECMP Mode: Advertise out Tunnel1
```

関連コマンド

コマンド	説明
show eigrp address-family topology	EIGRP トポロジテーブル内のエントリを表示します。

show ipv6 eigrp traffic

送受信される Enhanced Interior Gateway Routing Protocol（EIGRP）for IPv6 のパケットを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6eigrptraffic** コマンドを使用します。

show ipv6 eigrp traffic [*as-number*]

構文の説明

as-number	（任意）自律システム番号。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

送受信されるパケットの情報を表示するには、**showipv6eigrptraffic** コマンドを使用します。

例

次は、**showipv6eigrptraffic** コマンドの出力例です。

```
Device# show ipv6 eigrp traffic
IPv6-EIGRP Traffic Statistics for process 9
 Hellos sent/received: 218/205
 Updates sent/received: 7/23
 Queries sent/received: 2/0
 Replies sent/received: 0/2
 Acks sent/received: 21/14
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *8 : show ipv6 eigrp traffic* フィールドの説明

フィールド	説明
process 9	**ipv6routereigrp** コマンドに指定された自律システム番号。
Hellos sent/received	送受信された hello パケットの数
Updates sent/received	送受信されたアップデート パケットの数
Queries sent/received	送受信されたクエリー パケットの数
Replies sent/received	送受信された応答パケットの数

フィールド	説明
Acks sent/received	送受信された確認応答（ACK）パケットの数

関連コマンド

コマンド	説明
ipv6routereigrp	EIGRP for IPv6 ルーティング プロセスを設定します。

show ipv6 general-prefix

IPv6 の汎用プレフィックスを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6general-prefix** コマンドを使用します。

show ipv6 general-prefix

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 モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

IPv6 の汎用プレフィックスに関する情報を表示するには、**showipv6general-prefix** コマンドを使用します。

例

次に、6to4 に基づいて定義された my-prefix という IPv6 汎用プレフィックスの例を示します。また、汎用プリフィックスは、インターフェイス loopback42 上にアドレスを定義するためにも使用します。

```
Device# show ipv6 general-prefix
IPv6 Prefix my-prefix, acquired via 6to4
2002:B0B:B0B::/48
 Loopback42 (Address command)
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *9 : show ipv6 general-prefix*フィールドの説明

フィールド	説明
IPv6 Prefix	IPv6 汎用プレフィックスのユーザ定義名。
Acquired via	汎用プレフィックスは 6to4 インターフェイスに基づいて定義されています。また、汎用プレフィックスは手動で定義するか、または IPv6 プレフィックス委任の DHCP を使用して取得することもできます。
2002:B0B:B0B::/48	この汎用プレフィックスのプレフィックス値。

フィールド	説明
Loopback42（Address コマンド）	この汎用プレフィックスを使用するインターフェイスのリスト。

関連コマンド

コマンド	説明
ipv6general-prefix	IPv6アドレスの汎用プレフィックスを手動で定義します。

show ipv6 interface

IPv6に設定したインターフェイスのユーザビリティ ステータスを表示するには、ユーザEXECモードまたは特権 EXEC モードで **showipv6interface** コマンドを使用します。

show ipv6 interface [brief] [*type number*] **[prefix]**

構文の説明

brief	（任意）各インターフェイスのIPv6ステータスおよび設定の簡単なサマリーを表示します。
type	（任意）情報を表示するインターフェイス タイプ。
number	（任意）情報を表示するインターフェイス番号。
prefix	（任意）ローカルの IPv6 プレフィックス プールから生成されるプレフィックス。

コマンド デフォルト

すべての IPv6 インターフェイスが表示されます。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

showipv6interface コマンドは、IPv6 に固有であることを除き、show ip interface コマンドと同様です。

インターフェイスの IPv6 ステータスとそれに設定されているアドレスを検証するには、**showipv6interface** コマンドを使用します。また、show ipv6 インターフェイス コマンドは、このインターフェイスおよび設定されている機能の動作に IPv6 が使用しているパラメータも表示します。

インターフェイスのハードウェアが使用できる場合、インターフェイスは up とマークされます。インターフェイスが双方向通信を IPv6 に提供できる場合、回線プロトコルのステータスは up とマークされます。

オプションのインターフェイス タイプと番号を指定すると、このコマンドはその特定のインターフェイスに関する情報のみを表示します。特定のインターフェイスについて、インターフェイスに設定されている IPv6 ネイバー探索（ND）プレフィックスを表示するには、prefix キーワードを使用します。

例

IPv6 が設定された特定のインターフェイスに関するインターフェイス情報

showipv6interface コマンドは、指定したインターフェイスに関する情報を表示します。

```
Device(config)# show ipv6 interface ethernet0/0
Ethernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:6700
  No Virtual link-local address(es):
  Global unicast address(es):
    2001::1, subnet is 2001::/64 [DUP]
    2001::A8BB:CCFF:FE00:6700, subnet is 2001::/64 [EUI]
    2001:100::1, subnet is 2001:100::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FF00:6700
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *10 : show ipv6 interface* フィールドの説明

フィールド	説明
Ethernet0/0 is up, line protocol is up	インターフェイスハードウェアがアクティブかどうか（回線信号が存在するかどうか）と、それが管理者によりダウン状態にされているかどうかを示します。インターフェイスのハードウェアが使用できる場合、インターフェイスはupとマークされます。インターフェイスを使用するには、インターフェイスハードウェアと回線プロトコルの両方がアップ状態になっている必要があります。
line protocol is up, down（出力例にdownは表示されていません）	回線プロトコルを処理するソフトウェアプロセスが回線を使用可能と見なしているかどうか（つまり、キープアライブが成功しているかどうか、またはIPv6 CPがネゴシエートされているかどうか）を示します。インターフェイスが双方向通信を提供できる場合、回線プロトコルはupとマークされます。インターフェイスを使用するには、インターフェイスハードウェアと回線プロトコルの両方がアップ状態になっている必要があります。

フィールド	説明
IPv6 is enabled, stalled, disabled（出力例には stalled と disabled は表示されていません）	IPv6 がインターフェイスでイネーブル、ストールまたはディセーブルかを示します。IPv6 が有効になっている場合は、インターフェイスのステータスが「enabled」と表示されます。重複アドレス検出でインターフェイスのリンクローカルアドレスが重複していると特定された場合は、そのインターフェイスでの IPv6 パケットの処理が無効になり、インターフェイスのステータスが「stalled」になります。IPv6 が有効になっていない場合は、インターフェイスのステータスが「disabled」と表示されます。
link-local address	インターフェイスに割り当てられているリンクローカルアドレスを表示します。
Global unicast address(es):	インターフェイスに割り当てられているグローバルユニキャストアドレスを表示します。
Joined group address(es):	インターフェイスが属するマルチキャストグループを示します。
MTU	インターフェイスの最大伝送単位
ICMP error messages	このインターフェイスで送信されるエラーメッセージ間の最小間隔（ミリ秒単位）を指定します。
ICMP redirects	インターフェイスでの Internet Control Message Protocol（ICMP）IPv6 リダイレクトメッセージの状態（メッセージの送信が有効か無効か）。
ND DAD	インターフェイスでの重複アドレス検出の状態（enabled または disabled）。
number of DAD attempts:	重複アドレス検出が実行されているときに、インターフェイスで送信されるネイバー送信要求メッセージの連続数。
ND reachable time	このインターフェイスに割り当てられているネイバー探索到達可能時間（ミリ秒）を表示します。
ND advertised reachable time	このインターフェイスでアドバタイズされるネイバー探索到達可能時間（ミリ秒）を表示します。
ND advertised retransmit interval	このインターフェイスでアドバタイズされるネイバー探索再送信間隔（ミリ秒）を表示します。

フィールド	説明
ND router advertisements	このインターフェイスで送信されるネイバー探索ルータアドバタイズメント（RA）の間隔（秒単位）およびアドバタイズメントが期限切れになるまでの時間数を指定します。 Cisco IOS Release 12.4(2)T 現在、このフィールドには、このインターフェイス上のこのデバイスが送信したデフォルトのルータ設定が表示されます。
ND advertised default router preference is Medium	特定のインターフェイス上のデバイスの DRP。

showipv6interface コマンドは、インターフェイスに割り当てられている IPv6 アドレスと関連付けられている可能性がある属性に関する情報を表示します。

属性	説明
ANY	エニーキャスト。アドレスは **ipv6 address** コマンドを使用して設定した時点で指定したとおりのエニーキャスト アドレスです。
CAL	カレンダー。アドレスには時間制限が設定されており、有効な優先期間があります。
DEP	非推奨。時限アドレスは推奨されません。
DUP	重複。アドレスは、重複アドレス検出（DAD）によって決定されたとおり、重複しています。DAD を再試行するには、**shutdown** または **no shutdown** コマンドをインターフェイス上で実行する必要があります。
EUI	EUI-64 ベース。アドレスは EUI-64 を使用して生成されました。
消灯	オフリンク。アドレスはオフリンクです。
OOD	過度に楽観的な DAD。このアドレスに対して DAD は実行されません。この属性は仮想アドレスに適用されます。
PRE	優先時限アドレスが優先されます。
TEN	暫定。アドレスは DAD により暫定的な状態になっています。

属性	説明
UNA	アクティブ化されていません。仮想アドレスはアクティブになっておらず、スタンバイ状態です。
VIRT	仮想。アドレスは仮想であり、HSRP、VRRP、またはGLBPによって管理されます。

brief キーワードを使用した show ipv6 interface コマンド

次に、**brief**キーワードを使用して入力した場合の**showipv6interface**コマンドの出力例を示します。

```
Device# show ipv6 interface brief
Ethernet0 is up, line protocol is up
Ethernet0                  [up/up]
    unassigned
Ethernet1                  [up/up]
    2001:0DB8:1000:/29
Ethernet2                  [up/up]
    2001:0DB8:2000:/29
Ethernet3                  [up/up]
    2001:0DB8:3000:/29
Ethernet4                  [up/down]
    2001:0DB8:4000:/29
Ethernet5                  [administratively down/down]
    2001:123::210:7BFF:FEC2:ACD8
Interface         Status                IPv6 Address
Ethernet0         up                    3FFE:C00:0:1:260:3EFF:FE11:6770
Ethernet1         up                    unassigned
Fddi0             up                    3FFE:C00:0:2:260:3EFF:FE11:6772
Serial0           administratively down unassigned
Serial1           administratively down unassigned
Serial2           administratively down unassigned
Serial3           administratively down unassigned
Tunnel0           up                    unnumbered (Ethernet0)
Tunnel1           up                    3FFE:700:20:1::12
```

ND プレフィックスを設定した IPv6 インターフェイス

次に、ローカルIPv6プレフィックス プールからプレフィックスを生成したインターフェイスの特性の出力例を示します。

```
Device# show ipv6 interface Ethernet 0/0 prefix

interface Ethernet0/0
 ipv6 address 2001:0DB8::1/64
 ipv6 address 2001:0DB8::2/64
 ipv6 nd prefix 2001:0DB8:2::/64
 ipv6 nd prefix 2001:0DB8:3::/64 2592000 604800 off-link
end
.
.
.
```

```
IPv6 Prefix Advertisements Ethernet0/0
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default
       N - Not advertised, C - Calendar
     default [LA] Valid lifetime 2592000, preferred lifetime 604800
AD   2001:0DB8:1::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
APD  2001:0DB8:2::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
P    2001:0DB8:3::/64 [A] Valid lifetime 2592000, preferred lifetime 604800
```

デフォルトのプレフィックスでは、ipv6 nd prefix default コマンドを使用して設定したパラメータを表示します。

DRP を設定した IPv6 インターフェイス

次に、インターフェイスを通じてこのデバイスがアドバタイズしたDRPプリファレンス値の状態の出力例を示します。

```
Device# show ipv6 interface gigabitethernet 0/1
  GigabitEthernet0/1 is up, line protocol is up
    IPv6 is enabled, link-local address is FE80::130
    Description: Management network (dual stack)
    Global unicast address(es):
      FEC0:240:104:1000::130, subnet is FEC0:240:104:1000::/64
    Joined group address(es):
      FF02::1
      FF02::2
      FF02::1:FF00:130
    MTU is 1500 bytes
    ICMP error messages limited to one every 100 milliseconds
    ICMP redirects are enabled
    ND DAD is enabled, number of DAD attempts: 1
    ND reachable time is 30000 milliseconds
    ND advertised reachable time is 0 milliseconds
    ND advertised retransmit interval is 0 milliseconds
    ND router advertisements are sent every 200 seconds
    ND router advertisements live for 1800 seconds
    ND advertised default router preference is Low
    Hosts use stateless autoconfig for addresses.
```

HSRP が設定された IPv6 インターフェイス

最初に HSRP IPv6 をインターフェイス上に設定すると、インターフェイス IPv6 リンクローカルアドレスは非アクティブ（UNA）とマークされます。これは、アドバタイズされることがなく、HSRP IPv6 仮想リンク ローカル アドレスが UNA 属性および暫定 DAD（TEN）属性が設定された仮想リンク ローカル アドレス リストに追加されるためです。また、インターフェイスも HSRP IPv6 マルチキャスト アドレスをリッスンするようにプログラミングされます。

次に、HSRP IPv6 がインターフェイス上に設定されている場合の UNA 属性と TEN 属性のステータスの出力例を示します。

```
Device# show ipv6 interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80:2::2 [UNA]
  Virtual link-local address(es):
```

```
    FE80::205:73FF:FEA0:1 [UNA/TEN]
  Global unicast address(es):
    2001:2::2, subnet is 2001:2::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::66
    FF02::1:FF00:2
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ND DAD is enabled, number of DAD attempts: 1
```

HSRP グループがアクティブになると UNA 属性と TEN 属性がクリアされ、過度に楽観的な DAD（OOD）属性が設定されます。HSRP 仮想 IPv6 アドレスの要請ノード マルチキャスト アドレスもインターフェイスに追加されます。

次に、HSRP グループがアクティブになっている場合の UNA 属性、TEN 属性、および OOD 属性のステータスの出力例を示します。

```
# show ipv6 interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80:2::2 [UNA]
  Virtual link-local address(es):
    FE80::205:73FF:FEA0:1 [OPT]
  Global unicast address(es):
    2001:2::2, subnet is 2001:2::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::66
    FF02::1:FF00:2
    FF02::1:FFA0:1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
```

次の表で、HSRP を設定した **showipv6interface** コマンドの表示に示された追加の重要フィールドについて説明します。

表 *11 : HSRP* を設定した *show ipv6 interface* コマンドのフィールドの説明

フィールド	説明
IPv6 is enabled, link-local address is FE80:2::2 [UNA]	インターフェイス IPv6 リンクローカル アドレスは、アドバタイズされないため、UNA とマークされます。
FE80::205:73FF:FEA0:1 [UNA/TEN]	UNA 属性と TEN 属性が設定された仮想リンクローカル アドレス リスト。
FF02::66	HSRP IPv6 マルチキャスト アドレス。
FE80::205:73FF:FEA0:1 [OPT]	HSRP がアクティブになり、HSRP 仮想アドレスは OPT とマークされます。
FF02::1:FFA0:1	HSRP 要請ノード マルチキャスト アドレス。

最小 RA 間隔が設定された IPv6 インターフェイス

インターフェイス上でモバイル IPv6 を有効にすると、IPv6 ルータ アドバタイズメント（RA）伝送間の最小間隔を設定できます。**showipv6interface** コマンドの出力には、最小 RA 間隔が設定されていれば、その間隔が報告されます。最小 RA 間隔が明示的に設定されていない場合は表示されません。

次の例では、イーサネット インターフェイス 1/0 上で最大 RA 間隔は 100 秒、最小 RA 間隔は 60 秒に設定されています。

```
Device(config-if)# ipv6 nd ra-interval 100 60
```

その後で **showipv6interface** を使用すると、間隔が次のように表示されます。

```
Device(config)# show ipv6 interface ethernet 1/0
Ethernet1/0 is administratively down, line protocol is down
  IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:5A01 [TEN]
  No Virtual link-local address(es):
  No global unicast address is configured
  Joined group address(es):
    FF02::1
    FF02::2
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 60 to 100 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

次の例では、イーサネット インターフェイス 1/0 上で最大 RA 間隔は 100 ミリ秒（ms）、最小 RA 間隔は 60 ms に設定されています。

```
Device(config)# show ipv6 interface ethernet 1/0
Ethernet1/0 is administratively down, line protocol is down
  IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:5A01 [TEN]
  No Virtual link-local address(es):
  No global unicast address is configured
  Joined group address(es):
    FF02::1
    FF02::2
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 60 to 100 milliseconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

次の表で、最小 RA 間隔情報を設定した **showipv6interface** コマンドの表示に示された追加の重要フィールドについて説明します。

表 *12 :* 最小 *RA* 間隔情報を設定した *show ipv6 interface* コマンドのフィールドの説明

フィールド	説明
ND router advertisements are sent every 60 to 100 seconds	最小値と最大値の間の値からランダムに選択した間隔で ND RA が送信されます。次の例では、最小値は 60 秒、最大値は 100 秒です。
ND router advertisements are sent every 60 to 100 milliseconds	最小値と最大値の間の値からランダムに選択した間隔で ND RA が送信されます。次の例では、最小値は 60 ミリ秒、最大値は 100 ミリ秒です。

関連コマンド

コマンド	説明
ipv6ndprefix	IPv6 ルータアドバタイズメントに含める IPv6 プレフィックスを設定します。
ipv6ndrainterval	インターフェイス上の IPv6 RA 送信間隔を設定します。
showipinterface	IP 用に設定されたインターフェイスが使用可能かどうかのステータスを表示します。

show ipv6 mfib

IPv6 Multicast Forwarding Information Base（MFIB）内の転送エントリとインターフェイスを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6mfib** コマンドを使用します。

show ipv6 mfib [**vrf** *vrf-name*] [{**all**|**linkscope**|**verbose** *group-address-name*| *ipv6-prefix* / *prefix-length source-address-name*|**interface**|**status**|**summary**}]

show ipv6 mfib [**vrf** *vrf-name*] [{**all**|**linkscope**|**verbose**|**interface**|**status**|**summary**}]

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
all	（任意）IPv6 MFIB 内のすべての転送エントリとインターフェイスを表示します。
linkscope	（任意）リンク ローカル グループを表示します。
verbose	（任意）MAC カプセル化ヘッダーおよびプラットフォーム固有情報などの追加情報を表示します。
ipv6-prefix	（任意）インターフェイスに割り当てられた IPv6 ネットワーク。デフォルトの IPv6 プレフィックス は 128 です。 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。
/ *prefix-length*	（オプション）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。
group-address-name	（任意）マルチキャスト グループの IPv6 アドレスまたは名前。
source-address-name	（任意）マルチキャスト グループの IPv6 アドレスまたは名前。
interface	（任意）インターフェイスの設定とステータス。
status	（任意）一般的な設定とステータス。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

MFIB のエントリと転送インターフェイスおよびそれらのトラフィック統計を表示するには、**showipv6mfib** コマンドを使用します。ルータが分散モードで動作している場合、仮想IP（VIP）上でこのコマンドをイネーブルにできます。

MFIB の転送エントリには、転送とシグナリングのデフォルト動作を決定するフラグがあり、エントリに一致するパケットで使用されます。エントリにはインターフェイス単位のフラグもあり、特定のインターフェイスで受信または転送されるパケットについての転送動作をさらに詳しく指定します。次の表に、MFIB 転送エントリとインターフェイス フラグを示します。

表 *13 : MFIB* エントリとインターフェイスのフラグ

Flag	説明
F	Forward：データは、このインターフェイスから転送されます。
A	Accept：このインターフェイス上で受信されたデータは、転送用として受け入れられます。
IC	Internal copy：このインターフェイスで受信または転送されたパケットのコピーをルータに配信します。
NS	Negate signal：このインターフェイスで受信されたパケットについては、デフォルトのエントリ シグナリング動作を逆にします。
DP	Do not preserve：このインターフェイスでのパケット受信を信号で通知するときに、コピーを保存しません（廃棄します）。
SP	Signal present：このインターフェイスでのパケットの受信が信号で通知されました。
S	Signal：デフォルトでは、このエントリに一致するパケットの受信を信号で通知します。
C	このエントリに一致するパケットについて、直接接続チェックを実行します。パケットが、直接接続されている送信元から発信されていた場合は、受信を信号で通知します。

例

次に、MFIB での転送エントリおよびインターフェイスを表示する例を示します。ルータは高速スイッチング用に設定されており、受信側はイーサネット 1/1 の FF05::1 に加入し、送信元（2001::1:1:20）はイーサネット 1/2 で送信しています。

```
Device# show ipv6 mfib
IP Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
```

```
            IC - Internal Copy, NP - Not platform switched
            SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,FF00::/8) Flags: C
   Forwarding: 0/0/0/0, Other: 0/0/0
   Tunnel0 Flags: NS
(*,FF00::/15) Flags: D
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF05::1) Flags: C
   Forwarding: 2/0/100/0, Other: 0/0/0
   Tunnel0 Flags: A NS
   Ethernet1/1 Flags: F NS
     Pkts: 0/2
(2001::1:1:200,FF05::1) Flags:
   Forwarding: 5/0/100/0, Other: 0/0/0
   Ethernet1/2 Flags: A
   Ethernet1/1 Flags: F NS
     Pkts: 3/2
(*,FF10::/15) Flags: D
   Forwarding: 0/0/0/0, Other: 0/0/0
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *14 : show ipv6 mfib* フィールドの説明

フィールド	説明
Entry Flags	エントリに関する情報です。
Forwarding Counts	少なくとも 1 つのインターフェイスから受信され、少なくとも 1 つのインターフェイスに転送されたパケットに関する統計。
Pkt Count/	このカウンタが適用されるマルチキャスト転送状態の作成後に受信され転送されたパケットの総数。
Pkts per second/	1 秒間に受信され転送されたパケット数。
Avg Pkt Size/	このマルチキャスト転送状態についての合計バイト数/合計パケット数。合計バイト数は直接は表示されません。平均パケット サイズにパケット数を乗算すると、合計バイト数を計算できます。
Kbits per second	1 秒間のバイト数/1 秒間のパケット数/1000。
Other counts:	受信パケットに関する統計。これらのカウンタには、受信され転送されたパケットと受信されても転送されなかったパケットに関する統計が含まれます。
Interface Flags:	インターフェイスに関する情報。
Interface Counts:	インターフェイス統計情報。

次に、グループ アドレスに FF03:1::1 を指定した MFIB 内の転送エントリとインターフェイスの例を示します。

```
Device# show ipv6 mfib FF03:1::1
```

```
IP Multicast Forwarding Information Base
Entry Flags:C - Directly Connected, S - Signal, IA - Inherit A
flag,
            AR - Activity Required, D - Drop
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kbits per
second
Other counts:Total/RPF failed/Other drops
Interface Flags:A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts:FS Pkt Count/PS Pkt Count
*,FF03:1::1) Flags:C
  Forwarding:0/0/0/0, Other:0/0/0
  Tunnel1 Flags:A NS
  GigabitEthernet5/0.25 Flags:F NS
    Pkts:0/0
  GigabitEthernet5/0.24 Flags:F NS
    Pkts:0/0
(5002:1::2,FF03:1::1) Flags:
  Forwarding:71505/0/50/0, Other:42/0/42
  GigabitEthernet5/0 Flags:A
  GigabitEthernet5/0.19 Flags:F NS
    Pkts:239/24
  GigabitEthernet5/0.20 Flags:F NS
    Pkts:239/24
  GigabitEthernet5/0.21 Flags:F NS
    Pkts:238/24
.
.
.
GigabitEthernet5/0.16 Flags:F NS
Pkts:71628/24
```

次に、グループ アドレス FF03:1::1、送信元アドレス 5002:1::2 を指定した MFIB 内の転送エントリとインターフェイスの例を示します。

```
Device# show ipv6 mfib FF03:1::1 5002:1::2

IP Multicast Forwarding Information Base
Entry Flags:C - Directly Connected, S - Signal, IA - Inherit A flag,
            AR - Activity Required, D - Drop
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:Total/RPF failed/Other drops
Interface Flags:A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts:FS Pkt Count/PS Pkt Count
(5002:1::2,FF03:1::1) Flags:
   Forwarding:71505/0/50/0, Other:42/0/42
   GigabitEthernet5/0 Flags:A
   GigabitEthernet5/0.19 Flags:F NS
     Pkts:239/24
   GigabitEthernet5/0.20 Flags:F NS
     Pkts:239/24
.
.
.
   GigabitEthernet5/0.16 Flags:F NS
     Pkts:71628/24
```

次に、グループ アドレス FF03:1::1 とデフォルト プレフィックス 128 を指定した MFIB 内の転送エントリとインターフェイスの例を示します。

```
Device# show ipv6 mfib FF03:1::1/128
IP Multicast Forwarding Information Base
Entry Flags:C - Directly Connected, S - Signal, IA - Inherit A flag,
            AR - Activity Required, D - Drop
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:Total/RPF failed/Other drops
Interface Flags:A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts:FS Pkt Count/PS Pkt Count
(*,FF03:1::1) Flags:C
   Forwarding:0/0/0/0, Other:0/0/0
   Tunnel1 Flags:A NS
   GigabitEthernet5/0.25 Flags:F NS
     Pkts:0/0
   GigabitEthernet5/0.24 Flags:F NS
     Pkts:0/0
.
.
.
   GigabitEthernet5/0.16 Flags:F NS
     Pkts:0/0
```

次に、グループ アドレス FFE0 とプレフィックス 15 を指定した MFIB 内の転送エントリとインターフェイスの例を示します。

```
Device# show ipv6 mfib FFE0::/15
IP Multicast Forwarding Information Base
Entry Flags:C - Directly Connected, S - Signal, IA - Inherit A flag,
            AR - Activity Required, D - Drop
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:Total/RPF failed/Other drops
Interface Flags:A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts:FS Pkt Count/PS Pkt Count
(*,FFE0::/15) Flags:D
   Forwarding:0/0/0/0, Other:0/0/0
```

次に、**show ipv6mfib** コマンドと **verbose** キーワードを使用した出力の例を示します。ここでは、MFIB 内の転送エントリおよびインターフェイスと、MAC カプセル化ヘッダーやプラットフォーム固有情報などの追加情報が表示されます。

```
Device# show ipv6 mfib ff33::1:1 verbose
IP Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, K - Keepalive
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Platform per slot HW-Forwarding Counts: Pkt Count/Byte Count
Platform flags: HF - Forwarding entry,HB - Bridge entry,HD - NonRPF Drop entry,
                NP - Not platform switchable,RPL - RPF-ltl linkage,
                MCG - Metset change,ERR - S/w Error Flag,RTY - In RetryQ,
                LP - L3 pending,MP - Met pending,AP - ACL pending
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: Distributed FS Pkt Count/FS Pkt Count/PS Pkt Count
(10::2,FF33::1:1) Flags: K
   RP Forwarding: 0/0/0/0, Other: 0/0/0
```

```
LC Forwarding: 0/0/0/0, Other: 0/0/0
HW Forwd:   0/0/0/0, Other: NA/NA/NA
Slot 6: HW Forwarding: 0/0, Platform Flags:  HF RPL
Slot 1: HW Forwarding: 0/0, Platform Flags:  HF RPL
Vlan10 Flags: A
Vlan30 Flags: F NS
  Pkts: 0/0/0 MAC: 33330001000100D0FFFE180086DD
```

次の表に、この出力で表示されるフィールドについて説明します。

表 *15 : show ipv6 mfib verbose* フィールドの説明

フィールド	説明
Platform flags	プラットフォームに関する情報
Platform per slot HW-Forwarding Counts	転送されたバイトあたりのパケット総数

関連コマンド

コマンド	説明
showipv6mfibactive	アクティブな送信元からマルチキャスト グループへの送信レートを表示します。
showipv6mfibcount	MFIB からのグループおよび送信元に関するサマリー トラフィック統計情報を表示します。
showipv6mfibinterface	IPv6 マルチキャスト対応インターフェイスとその転送ステータスに関する情報を表示します。
showipv6mfibstatus	一般的な MFIB 設定と動作ステータスを表示します。
showipv6mfibsummary	IPv6 MFIB エントリ（リンクローカル グループを含む）およびインターフェイスの数に関するサマリー情報を表示します。

show ipv6 mld groups

ルータに直接接続されたマルチキャスト グループと、マルチキャスト リスナー検出（MLD）を通じて学習したマルチキャスト グループを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6mldgroups** コマンドを使用します。

show ipv6 mld [**vrf** *vrf-name*] **groups [link-local]** [{*group-namegroup-address*}] [*interface-type interface-number*] [{**detail**|**explicit**}]

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
link-local	（任意）リンク ローカル グループを表示します。
group-name | *group-address*	（任意）マルチキャスト グループの IPv6 アドレスまたは名前。
interface-type interface-number	（任意）インターフェイス タイプおよび番号
detail	（任意）個々の送信元の詳細情報を表示します。
explicit	（任意）各グループの各インターフェイスで明示的に追跡しているホストに関する情報を表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

オプションの引数をすべて省略すると、**showipv6mldgroups** グループ アドレス別およびインターフェイス タイプと番号別に直接接続されたすべてのマルチキャスト グループを表示します。これには、使用したリングローカル グループ（**link-local** キーワードが利用できない場合）が含まれています。

例

次に、**showipv6mldgroups** コマンドの出力例を示します。この例では、ネットワーク プロトコルで使用されているリンクローカル グループを含め、ファストイーサネット インターフェイス 2/1 が加入しているすべてのグループが示されています。

```
Device# show ipv6 mld groups FastEthernet 2/1
MLD Connected Group Membership
Group Address           Interface           Uptime        Expires
FF02::2                 FastEthernet2/1     3d18h         never
```

```
FF02::D                 FastEthernet2/1     3d18h         never
FF02::16                FastEthernet2/1     3d18h         never
FF02::1:FF00:1          FastEthernet2/1     3d18h         00:00:27
FF02::1:FF00:79         FastEthernet2/1     3d18h         never
FF02::1:FF23:83C2       FastEthernet2/1     3d18h         00:00:22
FF02::1:FFAF:2C39       FastEthernet2/1     3d18h         never
FF06:7777::1            FastEthernet2/1     3d18h         00:00:26
```

次に、**detail** キーワードを使用した **showipv6mldgroups** コマンドの出力例を示します。

```
Device# show ipv6 mld groups detail
Interface:      Ethernet2/1/1
Group:          FF33::1:1:1
Uptime:         00:00:11
Router mode:    INCLUDE
Host mode:      INCLUDE
Last reporter:  FE80::250:54FF:FE60:3B14
Group source list:
Source Address                          Uptime    Expires   Fwd  Flags
2004:4::6                               00:00:11  00:04:08  Yes  Remote Ac 4
```

次に、**explicit** キーワードを使用した **showipv6mldgroups** コマンドの出力例を示します。

```
Device# show ipv6 mld groups explicit
Ethernet1/0, FF05::1
    Up:00:43:11 EXCLUDE(0/1) Exp:00:03:17
    Host Address                            Uptime   Expires
    FE80::A8BB:CCFF:FE00:800                00:43:11 00:03:17
    Mode:EXCLUDE
Ethernet1/0, FF05::6
    Up:00:42:22 INCLUDE(1/0) Exp:not used
    Host Address                            Uptime   Expires
    FE80::A8BB:CCFF:FE00:800                00:42:22 00:03:17
    Mode:INCLUDE
        300::1
        300::2
        300::3
Ethernet1/0 - Interface
ff05::1 - Group address
Up:Uptime for the group
EXCLUDE/INCLUDE - The mode the group is in on the router.
(0/1) (1/0) - (Number of hosts in INCLUDE mode/Number of hosts in EXCLUDE moe)
Exp:Expiry time for the group.
FE80::A8BB:CCFF:FE00:800 - Host ipv6 address.
00:43:11 - Uptime for the host.
00:03:17 - Expiry time for the host
Mode:INCLUDE/EXCLUDE - Mode the Host is operating in.
300::1, 300::2, 300::3 - Sources that the host has joined in the above specified mode.
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *16 : show ipv6 mld groups* フィールドの説明

フィールド	説明
Group Address	マルチキャスト グループのアドレス。
Interface	グループに到達可能なインターフェイス。

フィールド	説明
Uptime	このマルチキャスト グループが認識されている時間（時間、分、および秒）。
Expires	エントリが MLD グループ テーブルから削除されるまでの時間（時間、分、秒）。 ルータ自体がグループに参加している場合は満了タイマーに「never」が表示され、グループのルータ モードが INCLUDE の場合は満了タイマーに「not used」と表示されます。この状況では、送信元のエントリの満了タイマーが使用されます。
Last reporter:	マルチキャスト グループのメンバーであることを最後に報告したホスト。
Flags Ac 4	設定した MLD 状態の制限に向けてカウントされたフラグ。

関連コマンド

コマンド	説明
ipv6mldquery-interval	Cisco IOS ソフトウェアが MLD ホストクエリー メッセージを送信する頻度を設定します。

show ipv6 mld interface

インターフェイスに関するマルチキャスト関連情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6mldinterface** コマンドを使用します。

show ipv6 mld [**vrf** *vrf-name*] **interface** [*type number*]

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
type number	（任意）インターフェイス タイプおよび番号

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

オプションの *type* 引数と *number* 引数を省略すると、**showipv6mldinterface** コマンドはすべてのインターフェイスに関する情報を表示します。

例

次に、イーサネット インターフェイス 2/1/1 に対する **showipv6mldinterface** コマンドの出力例を示します。

```
Device# show ipv6 mld interface Ethernet 2/1/1
Global State Limit : 2 active out of 2 max
Loopback0 is administratively down, line protocol is down
  Internet address is ::/0
.
.
.
Ethernet2/1/1 is up, line protocol is up
  Internet address is FE80::260:3EFF:FE86:5649/10
  MLD is enabled on interface
  Current MLD version is 2
  MLD query interval is 125 seconds
  MLD querier timeout is 255 seconds
  MLD max query response time is 10 seconds
  Last member query response interval is 1 seconds
  Interface State Limit : 2 active out of 3 max
  State Limit permit access list:
  MLD activity: 83 joins, 63 leaves
  MLD querying router is FE80::260:3EFF:FE86:5649 (this system)
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *17 : show ipv6 mld interface* フィールドの説明

フィールド	説明
Global State Limit: 2 active out of 2 max	グローバルに設定されている 2 つの MLD 状態がアクティブです。
Ethernet2/1/1 is up, line protocol is up	インターフェイスのタイプ、番号、およびステータス。
Internet address is...	インターフェイスに適用されているインターフェイスとサブネット マスクのインターネット アドレス。
MLD is enabled in interface	マルチキャスト リスナー検出（MLD）が **ipv6multicast-routing** コマンドによりインターフェイス上で有効になっていたかどうかを示します。
Current MLD version is 2	現在の MLD バージョン。
MLD query interval is 125 seconds	**ipv6mldquery-interval** コマンドで指定したように、Cisco IOS ソフトウェアが MLD クエリ メッセージを送信する間隔（秒単位）。
MLD querier timeout is 255 seconds	**ipv6mldquery-timeout** コマンドで指定したように、インターフェイスのクエリアとしてルータを継承するまでの時間（秒単位）。
MLD max query response time is 10 seconds	**ipv6mldquery-max-response-time** コマンドで指定したように、ルータがグループを削除するまでに MLD クエリ メッセージにホストが応答する必要がある時間（秒単位）。
Last member query response interval is 1 seconds	グループおよび送信元固有のクエリを対象とする最大応答コードの計算に使用されます。また、リンクの「離脱遅延」の調整にも使用されます。小さい値は、グループを最後に離脱するメンバーを検出する時間を短縮します。
Interface State Limit : 2 active out of 3 max	設定されているインターフェイスの状態の 3 つのうち 2 つがアクティブです。
State Limit permit access list: change	state permit アクセス リストのアクティビティ。
MLD activity: 83 joins, 63 leaves	受信しているグループの join と leave の数。
MLD querying router is FE80::260:3EFF:FE86:5649 (this system)	クエリ ルータの IPv6 アドレス。

関連コマンド

コマンド	説明
ipv6mldjoin-group	指定したグループおよび送信元に対してMLD レポートを設定します。
ipv6mldquery-interval	Cisco IOS ソフトウェアが MLD ホストクエリー メッセージを送信する頻度を設定します。

show ipv6 mld snooping

スイッチまたは VLAN の IP Version 6（IPv6）マルチキャスト リスナー検出（MLD）スヌーピング設定を表示するには、**show ipv6 mld snooping** コマンドを EXEC モードで使用します。

show ipv6 mld snooping [**vlan** *vlan-id*]

構文の説明

vlan *vlan-id*	（任意）VLAN を指定します。指定できる範囲は 1 ～ 1001 および 1006 ～ 4094 です。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

スイッチまたは特定の VLAN の MLD スヌーピングの設定を表示するのにこのコマンドを使用します。

1002 ～ 1005 の VLAN 番号は、トークンリング VLAN および FDDI VLAN のために予約されているため、MLD スヌーピングには使用できません。

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

例

次に、show ipv6 mld snooping vlan コマンドの出力例を示します。ここでは、特定の VLAN のスヌーピング特性を表示します。

```
Device# show ipv6 mld snooping vlan 100
Global MLD Snooping configuration:
-------------------------------------------
MLD snooping : Enabled
MLDv2 snooping (minimal) : Enabled
Listener message suppression : Enabled
TCN solicit query : Disabled
TCN flood query count : 2
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000
Vlan 100:
--------
MLD snooping : Disabled
MLDv1 immediate leave : Disabled
Explicit host tracking : Enabled
Multicast router learning mode : pim-dvmrp
```

```
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000
```

次の例では、**show ipv6 mld snooping** コマンドの出力を示します。ここでは、スイッチ上の VLAN すべてのスヌーピング特性を表示します。

```
Device# show ipv6 mld snooping
Global MLD Snooping configuration:
-------------------------------------------
MLD snooping : Enabled
MLDv2 snooping (minimal) : Enabled
Listener message suppression : Enabled
TCN solicit query : Disabled
TCN flood query count : 2
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000

Vlan 1:
--------
MLD snooping : Disabled
MLDv1 immediate leave : Disabled
Explicit host tracking : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable : 1
Last listener query count : 2
Last listener query interval : 1000

<output truncated>

Vlan 951:
--------
MLD snooping : Disabled
MLDv1 immediate leave : Disabled
Explicit host tracking : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000
```

関連コマンド

コマンド	説明
ipv6mldsnooping	スイッチ上または VLAN 上の MLD スヌーピングをイネーブルにし、設定を行います。
sdmprefer	スイッチの使用方法に基づきシステム リソースを最適化するよう SDM テンプレートを設定します。

show ipv6 mld ssm-map

Source Specific Multicast（SSM）マッピング情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6mldssm-mapstatic** コマンドを使用します。

show ipv6 mld [**vrf** *vrf-name*] **ssm-map** [*source-address*]

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
source-address	（任意）アクセス リストで識別されたグループの MLD メンバーシップに関連付けられている送信元アドレス。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

オプションの *source-address* 引数を使用しないと、すべての SSM マッピング情報が表示されます。

例

次に、ルータの SSM マッピングの例を示します。

```
Device# show ipv6 mld ssm-map
SSM Mapping  : Enabled
DNS Lookup   : Enabled
```

次に、送信元アドレス 2001:0DB8::1 に対する SSM マッピングの例を示します。

```
Device# show ipv6 mld ssm-map 2001:0DB8::1
 Group address  : 2001:0DB8::1
 Group mode ssm : TRUE
 Database       : STATIC
 Source list    : 2001:0DB8::2
                  2001:0DB8::3
Router# show ipv6 mld ssm-map 2001:0DB8::2
 Group address  : 2001:0DB8::2
 Group mode ssm : TRUE
 Database       : DNS
 Source list    : 2001:0DB8::3
                  2001:0DB8::1
```

下の表で、この出力で表示される重要なフィールドについて説明します。

表 *18 : show ipv6 mld ssm-map* フィールドの説明

フィールド	説明
SSM Mapping	SSM マッピング機能が有効になります。
DNS Lookup	SSM マッピング機能が有効になっている場合、DNS ルックアップ機能は自動的に有効になります。
Group address	特定のアクセス リストで識別されているグループ アドレス。
Group mode ssm : TRUE	特定のグループがSSM モードで機能しています。
Database : STATIC	静的 SSM マッピング設定を確認することで送信元アドレスを特定するようにルータが設定されます。
Database : DNS	DNS ベースの SSM マッピングを使用して送信元アドレスを特定するようにルータが設定されます。
Source list	アクセス リストによって識別されているグループに関連付けられている送信元アドレス。

関連コマンド

コマンド	説明
debugipv6mldssm-map	SSM マッピングのデバッグ メッセージを表示します。
ipv6mldssm-mapenable	設定済みの SSM 範囲内のグループに対して SSM マッピング機能をイネーブルにします。
ipv6mldssm-mapquerydns	DNS ベースの SSM マッピングを有効にします。
ipv6mldssm-mapstatic	スタティック SSM マッピングを設定します。

show ipv6 mld traffic

マルチキャスト リスナー検出（MLD）トラフィック カウンタを表示するには、特権 EXEC モードで **showipv6mldtraffic** コマンドを使用します。

show ipv6 mld [**vrf** *vrf-name*] **traffic**

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

予測した数の MLD プロトコル メッセージを送受信したかどうかを確認するには、**showipv6mldtraffic** コマンドを使用します。

例

次に、送受信された MLD プロトコル メッセージを表示する例を示します。

```
Device# show ipv6 mld traffic

MLD Traffic Counters
Elapsed time since counters cleared:00:00:21
                              Received     Sent
Valid MLD Packets               3           1
Queries                         1           0
Reports                         2           1
Leaves                          0           0
Mtrace packets                  0           0
Errors:
Malformed Packets                           0
Bad Checksums                               0
Martian source                              0
Packets Received on MLD-disabled Interface  0
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *19 : show ipv6 mld traffic* フィールドの説明

フィールド	説明
Elapsed time since counters cleared	カウンタをクリアしてからの時間を示します（時間、分、秒単位）。

フィールド	説明
Valid MLD packets	送受信された有効な MLD パケットの数。
Queries	送受信された有効なクエリの数。
Reports	送受信された有効なレポートの数。
Leaves	送受信された有効な leave の数。
Mtrace packets	送受信されたマルチキャスト トレース パケットの数。
Errors	発生したエラーのタイプと数。

show ipv6 mrib client

Multicast Routing Information Base（MRIB）のクライアントに関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6mribclient** コマンドを使用します。

show ipv6 mrib [**vrf** *vrf-name*] **client [filter]** [**name** {*client-name*|*client-name* **:** *client-id*}]

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
filter	（任意）各クライアントが所有し、各クライアントが対象としているMRIB フラグに関する情報を表示します。
name	（任意）マルチキャスト リスナー検出（MLD）や Protocol Independent Multicast（PIM）などのようにMRIB のクライアントとして機能するマルチキャスト ルーティング プロトコルの名前。
client-name **:** *client-id*	（任意）MLD またはPIM など、MRIB のクライアントとして動作するマルチキャスト ルーティング プロトコルの名前と ID。コロン記号が必要です。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

各クライアントが所有するMRIB フラグと、各クライアントが対象とするフラグに関する情報を表示するには、**filter** キーワードを使用します。

例

次は、**showipv6mribclient** コマンドの出力例です。

```
Device# show ipv6 mrib client
IP MRIB client-connections
igmp:145        (connection id 0)
pim:146 (connection id 1)
mfib ipv6:3     (connection id 2)
slot 3  mfib ipv6 rp agent:16   (connection id 3)
slot 1  mfib ipv6 rp agent:16   (connection id 4)
slot 0  mfib ipv6 rp agent:16   (connection id 5)
slot 4  mfib ipv6 rp agent:16   (connection id 6)
slot 2  mfib ipv6 rp agent:16   (connection id 7)
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *20 : show ipv6 mrib client* フィールドの説明

フィールド	説明
igmp:145 (connection id 0) pim:146 (connection id 1) mfib ipv6:3 (connection id 2) mfib ipv6 rp agent:16 (connection id 3)	Client ID (client name:process ID)

show ipv6 mrib route

マルチキャストルーティング情報ベース（MRIB）のルート情報を表示するには、ユーザEXECモードまたは特権 EXEC モードで **showipv6mribroute** コマンドを使用します。

show ipv6 mrib [**vrf** *vrf-name*] **route** [{**link-local**|**summary**|[{*source-addresssource-name*|*****}] [*groupname-or-address* [*prefix-length*]]}]

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
link-local	（任意）リンク ローカル グループを表示します。
summary	（任意）MRIB エントリ（リンクローカル グループを含む）と MRIB テーブルに存在するインターフェイスの数を表示します。
source address-or-name	（任意）送信元の IPv6 アドレスまたは名前。
*	（任意）MRIB ルート情報を表示します。
groupname or-address	（任意）マルチキャスト グループの IPv6 アドレスまたは名前。
prefix-length	（任意）IPv6 プレフィックス長。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

マルチキャスト リスナー検出（MLD）、Protocol Independent Multicast（PIM）、マルチキャスト転送情報ベース（MFIB）など、すべてのエントリがMRIBのさまざまなクライアントによって作成されます。各エントリまたはインターフェイスのフラグはMRIBのさまざまなクライアント間の通信メカニズムとして機能します。エントリには、新しい送信元や実行したアクションについて PIM が登録メッセージをどのように送信したかが示されます。

summary キーワードは、リンクローカル エントリを含めて、すべてのエントリのカウントを表示します。

次の表で、インターフェイス フラグについて説明します。

表 *21 :* インターフェイス フラグの説明

フラグ	説明
F	Forward：データはこのインターフェイスから転送されます。
A	Accept：このインターフェイス上で受信されたデータは、転送用として受け入れられます。
IC	Internal copy（内部コピー）
NS	Negate signal（信号を無効化）
DP	Do not preserve（保存せず）
SP	Signal present（信号あり）
II	Internal interest（内部対象）
ID	Internal uninterest（内部対象外）
LI	Local interest（ローカル対象）
LD	Local uninterest（ローカル非対称）
C	直接接続チェックを実行します。

MRIB 内の特殊なエントリは、通常動作からの例外を示します。たとえば、no signaling または no notification は、特殊なグループの範囲のいずれかと一致するデータ パケットの着信に必要です。特殊なグループの範囲は次のとおりです。

- 未定義の範囲（FFX0::/16）
- ノード ローカル グループ（FFX1::/16）
- リンクローカル グループ （FFX2::/16）
- Source Specific Multicast（SSM）グループ（FF3X::/32）

残りの（通常はスパースモードの）すべての IPv6 マルチキャスト グループについては、直接接続チェックが実行され、直接接続の送信元が着信した場合は PIM に通知されます。このプロシージャは、新しい送信元の登録メッセージを PIM がどのように送信するかを指定します。

例

次に、**summary** キーワードを使用した **showipv6mribroute** コマンドの出力例を示します。

```
Device# show ipv6 mrib route summary
MRIB Route-DB Summary
  No. of (*,G) routes = 52
  No. of (S,G) routes = 0
  No. of Route x Interfaces (RxI) = 10
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *22 : show ipv6 mrib route* フィールドの説明

フィールド	説明
No. of (*, G) routes	MRIB 内の共有ツリー ルートの数。
No. of (S, G) routes	MRIB 内の送信元ツリー ルートの数。
No. of Route x Interfaces (RxI)	各 MRIB ルートエントリ上のすべてのインターフェイスの合計。

show ipv6 mroute

showipmroute コマンドに似た形式で PIM トポロジ テーブルに情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6mroute** コマンドを使用します。

show ipv6 mroute [**vrf** *vrf-name*] [{**link-local**|[{*group-name*|*group-address* [{*source-addresssource-name*}]}]}] **[summary] [count]**

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
link-local	（任意）リンク ローカル グループを表示します。
group-name | *group-address*	（任意）マルチキャスト グループの IPv6 アドレスまたは名前。
source-address | *source-name*	（任意）送信元の IPv6 アドレスまたは名前。
summary	（任意）IPv6 マルチキャスト ルーティング テーブル内の各エントリの要約を 1 行で表示します。
count	（任意）パケット数、パケット/秒、平均パケットサイズ、および、バイト/秒などのグループと送信元に関するマルチキャスト転送情報ベース（MFIB）からの統計を表示します。

コマンド デフォルト

showipv6mroute コマンドはすべてのグループおよび送信元を表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

IPv6 マルチキャストの実装には、個別の mroute テーブルがありません。そのため、**showipv6mroute** コマンドで、**showipmroute** コマンドに似た形式の PIM トポロジテーブルに情報を表示できます。

オプションの引数とキーワードをすべて省略すると、**showipv6mroute** コマンドは PIM トポロジテーブル内のすべてのエントリを表示します（**link-local** キーワードが利用できるリンクローカル グループを除く）。

Cisco IOS ソフトウェア は、PIM プロトコル メッセージ、MLD レポート、およびトラフィックに基づいて (S,G) および (*,G) エントリを作成して PIM トポロジ テーブルにデータを入力します。アスタリスク（*）は、すべてのソース アドレスを示し、「S」は単一ソース アドレスを示し、「G」は宛先マルチキャスト グループ アドレスを示します。(S, G) エントリの作成時に、ソフトウェアはユニキャスト ルーティング テーブルで見つかった（つまり、Reverse Path Forwarding（RPF）によって）、該当する宛先グループへの最適なパスを使用します。

各 IPv6 マルチキャスト ルートの転送ステータスを表示するには、**showipv6mroute** コマンドを使用します。

例

次に、**showipv6mroute** コマンドの出力例を示します。

```
Device# show ipv6 mroute ff07::1
Multicast Routing Table
Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers:Uptime/Expires
Interface state:Interface, State
(*, FF07::1), 00:04:45/00:02:47, RP 2001:0DB8:6::6, flags:S
  Incoming interface:Tunnel5
  RPF nbr:6:6:6::6
  Outgoing interface list:
    POS4/0, Forward, 00:04:45/00:02:47
(2001:0DB8:999::99, FF07::1), 00:02:06/00:01:23, flags:SFT
  Incoming interface:POS1/0
  RPF nbr:2001:0DB8:999::99
  Outgoing interface list:
    POS4/0, Forward, 00:02:06/00:03:27
```

次に、**summary** キーワードを指定した **showipv6mroute** コマンドの出力例を示します。

```
Device# show ipv6 mroute ff07::1 summary
Multicast Routing Table
Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers:Uptime/Expires
Interface state:Interface, State
(*, FF07::1), 00:04:55/00:02:36, RP 2001:0DB8:6::6, OIF count:1, flags:S
(2001:0DB8:999::99, FF07::1), 00:02:17/00:01:12, OIF count:1, flags:SFT
```

次に、**count** キーワードを指定した **showipv6mroute** コマンドの出力例を示します。

```
Device# show ipv6 mroute ff07::1 count
IP Multicast Statistics
71 routes, 24 groups, 0.04 average sources per group
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts:Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Group:FF07::1
  RP-tree:
   RP Forwarding:0/0/0/0, Other:0/0/0
   LC Forwarding:0/0/0/0, Other:0/0/0
  Source:2001:0DB8:999::99,
   RP Forwarding:0/0/0/0, Other:0/0/0
   LC Forwarding:0/0/0/0, Other:0/0/0
```

```
   HW Forwd:  20000/0/92/0, Other:0/0/0
  Tot. shown:Source count:1, pkt count:20000
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *23 : show ipv6 mroute* フィールドの説明

フィールド	説明
Flags:	エントリに関する情報を提供します。 • S：スパース。エントリはスパース モードで動作しています。 • s：SSM グループ。マルチキャスト グループが SSM の IP アドレス範囲内であることを示します。このフラグは、SSM の範囲が変更されるとリセットされます。 • C：接続中。マルチキャスト グループのメンバーは、直接接続されたインターフェイス上に存在します。 • L：ローカル。ルータ自体が、マルチキャスト グループのメンバーです。 • I：送信元固有のホスト レポートを受信。(S,G) エントリが (S,G) レポートによって作成されたことを示します。このフラグは、代表ルータ（DR）上にのみ設定できます。 • P：プルーニング済み。ルートがプルーニングされています。Cisco IOS ソフトウェアは、この情報を保持して、ダウンストリーム メンバーが送信元に加入できるようにします。 • R：RP ビットを設定。(S,G) エントリが RP をポイントしていることを示します。通常、これは特定の送信元に関する共有ツリーに沿ったプルーニング ステートを示します。 • F：登録フラグ。ソフトウェアがマルチキャスト送信元に登録されていることを示します。 • T：SPT ビットを設定。パケットが最短パス送信元ツリーで受信されていることを示します。 • J：SPT に参加。(*,G)エントリの場合、共有ツリーの下方向に流れるトラフィックの速度が、グループの SPT しきい値設定を超えていることを示します（デフォルトの SPT しきい値設定は 0 kbps です）。J の最短パス ツリー（SPT）参加フラグが設定されている場合に、共有ツリーの下流で次の (S,G) パケットが受信されると、送信元の方向に (S,G) join がトリガーされます。これにより、ルータは送信元ツリーに参加します。デフォルトの SPT しきい値の 0 kbps がグループに使用され、J - SPT 参加フラグは常に (*, G) エントリ上に設定され、クリアされることはありません。ルータは、新しい送信元からのトラフィックを受信すると、最短パス送信元ツリーに切り替えます。

フィールド	説明
Timers: Uptime/Expires	「Uptime」はインターフェイスごとの、IPv6 マルチキャスト ルーティング テーブル内にエントリが存在する時間（時間、分、秒）を示します。「Expires」は、IPv6 マルチキャスト ルーティング テーブルからエントリが削除されるまでの時間（時間、分、秒）をインターフェイスごとに示します。
Interface state:	着信インターフェイスまたは発信インターフェイスの状態を示します。 • [Interface]。タイプと、着信インターフェイスまたは発信インターフェイスのリストに記載されているインターフェイスの数を示します。 • Next-Hop。「Next-Hop」は、ダウンストリーム ネイバーの IP アドレスを指定します。 • State/Mode。「State」はアクセス リストによる制限があるかどうかに応じて、インターフェイス上で転送、プルーニング、ヌル値化のいずれの処理がパケットに対して実行されるかを示します。「Mode」は、インターフェイスがスパース モードで動作していることを示します。
(*, FF07::1) and (2001:0DB8:999::99)	IPv6 マルチキャスト ルーティング テーブルのエントリ。エントリは、送信元ルータの IPv6 アドレスと、それに続くマルチキャスト グループの IPv6 アドレスで構成されます。送信元ルータの位置に置かれたアスタリスク（*）は、すべての送信元を意味します。 最初の形式のエントリは、(*, G) または「スター カンマ G」エントリと呼ばれます。2 番目の形式のエントリは (S, G) または「S カンマ G」エントリと呼ばれ、(S, G) エントリの構築に使用されます。
RP	RP ルータのアドレス。
flags:	この MRIB エントリ上の MRIB クライアントが設定した情報。
Incoming interface:	送信元からのマルチキャスト パケット用のインターフェイスです。パケットがこのインターフェイスに着信しなかった場合、廃棄されます。
RPF nbr	RP または送信元に対するアップストリーム ルータの IP アドレス。
Outgoing interface list:	パケットが転送される際に通過したインターフェイス。(S,G) のエントリについては、このリストは (*,G) エントリから継承したインターフェイスは含めません。

関連コマンド

コマンド	説明
ipv6multicast-routing	ルータのすべての IPv6 対応インターフェイス上で PIMと MLD を使用したマルチキャストルーティングを有効にし、マルチキャスト転送を有効にします。
showipv6mfib	IPv6 MFIB での転送エントリおよびインターフェイスを表示します。

show ipv6 mtu

IPv6 インターフェイスの最大伝送ユニット（MTU）のキャッシュ情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6mtu** コマンドを使用します。

show ipv6 mtu [**vrf** *vrfname*]

構文の説明

vrf	（任意）IPv6 バーチャル プライベート ネットワーク（VPN）ルーティング/転送インスタンス（VRF）。
vrfname	（任意）IPv6 VRF の名前。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

vrf キーワードと *vrfname* 引数を使用すると、特定の VRF に関連する MTU を表示できます。

例

次に、**showipv6mtu** コマンドの出力例を示します。

```
Device# show ipv6 mtu
MTU     Since    Destination Address
1400    00:04:21  5000:1::3
1280    00:04:50  FE80::203:A0FF:FED6:141D
```

次に、**vrf** キーワードと *vrfname* 引数を使用した **showipv6mtu** コマンドの出力例を示します。次の例では、vrfname1 という VRF に関する情報が表示されます。

```
Device# show ipv6 mtu vrf vrfname1
MTU   Since       Source Address     Destination Address
1300  00:00:04    2001:0DB8:2        2001:0DB8:7
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *24 : show ipv6 mtu* フィールドの説明

フィールド	説明
MTU	宛て先アドレスへのパスに使用され、Internet Control Message Protocol（ICMP）の packet-too-big メッセージに含まれている MTU。

フィールド	説明
Since	ICMP packet-too-big メッセージを受信してからのエントリの期間経過。
Destination Address	受信した ICMP packet-too-big メッセージに含まれているアドレス。このルータからこのアドレスに発信されるパケットは指定した MTU 未満の大きさであることが必要です。

関連コマンド

コマンド	説明
ipv6mtu	インターフェイス上で送信する IPv6 パケットの MTU サイズを設定します。

show ipv6 nd destination

IPv6ホストモードの宛て先キャッシュのエントリに関する情報を表示するには、ユーザEXECモードまたは特権 EXEC モードで **show ipv6 nd destination** コマンドを使用します。

show ipv6 nd destination ［**vrf** *vrf-name*］［*interface-type interface-number*］

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
interface- type	（任意）インターフェイス タイプを指定します。
interface-number	（任意）インターフェイス番号を指定します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

IPv6 ホストモードの宛て先キャッシュのエントリに関する情報を表示するには、**show ipv6 nd destination** コマンドを使用します。**vrf** キーワードと *vrf-name* 引数のペアを使用すると、指定した VRF に関する情報のみが表示されます。*interface-type* 引数と *interface-number* 引数を使用すると、指定したインターフェイスに関する情報のみが表示されます。

例

```
Device# show ipv6 nd destination

IPv6 ND destination cache (table: default)
Code: R - Redirect
   2001::1 [8]
    via FE80::A8BB:CCFF:FE00:5B00/Ethernet0/0
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *25 : show ipv6 nd destination* フィールドの説明

フィールド	説明
Code: R - Redirect	リダイレクトを通じて学習した宛て先。

フィールド	説明
2001::1 [8]	カッコ内に表示される値は、宛て先キャッシュエントリが最後に使用されてからの秒単位の時間です。

関連コマンド

コマンド	説明
ipv6 nd host mode strict	conformant または strict の IPv6 ホスト モードを有効にします。

show ipv6 nd on-link prefix

ルータ アドバタイズメント（RA）を通じて学習したオンリンク プレフィックスに関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 nd on-link prefix** コマンドを使用します。

show ipv6 nd on-link prefix ［**vrf** *vrf-name*］［*interface-type interface-number*］

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
interface-type	（任意）インターフェイス タイプを指定します。
interface-number	（任意）インターフェイス番号を指定します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

RA を通じて学習したオンリンク プレフィックスに関する情報を表示するには、**show ipv6 nd on-link prefix** コマンドを使用します。

RA から学習したプレフィックスは **show ipv6 nd on-link prefix** コマンドを使用して検査できます。**vrf** キーワードと *vrf-name* 引数のペアを使用すると、指定した VRF に関する情報のみが表示されます。*interface-type* 引数と *interface-number* 引数を使用すると、指定したインターフェイスに関する情報のみが表示されます。

例

次に、RA を通じて学習したオンリンク プレフィックスに関する情報を表示する例を示します。

```
Device# show ipv6 nd on-link prefix

IPv6 ND on-link Prefix (table: default), 2 prefixes
Code: A - Autonomous Address Config
A  2001::/64  [2591994/604794]
router FE80::A8BB:CCFF:FE00:5A00/Ethernet0/0
2001:1:2::/64  [2591994/604794]
router FE80::A8BB:CCFF:FE00:5A00/Ethernet0/0
```

関連コマンド

コマンド	説明
ipv6 nd host mode strict	conformant または strict の IPv6 ホスト モードを有効にします。

show ipv6 neighbors

IPv6 ネイバー探索（ND）のキャッシュ情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6neighbors** コマンドを使用します。

show ipv6 neighbors [{*interface-type interface-numberipv6-addressipv6-hostname*|**statistics**}]

構文の説明

interface-type	（任意）IPv6 ネイバー情報が表示されるインターフェイスのタイプを指定します。
interface-number	（任意）IPv6 ネイバー情報が表示されるインターフェイスの番号を指定します。
ipv6-address	（任意）ネイバーの IPv6 アドレスを指定します。 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。
ipv6-hostname	（任意）リモート ネットワーク デバイスの IPv6 ホスト名を指定します。
statistics	（任意）ND キャッシュの統計を表示します。

コマンド デフォルト

すべての IPv6 ND キャッシュのエントリがリストされます。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

interface-type と *interface-number* 引数が指定されていない場合は、すべての IPv6 ネイバーのキャッシュ情報が表示されます。*interface-type* と *interface-number* 引数を指定すると、特定のインターフェイスのキャッシュ情報だけが表示されます。

statistics キーワードを指定すると、ND キャッシュの統計が表示されます。

次に、インターフェイス タイプおよび番号を指定して入力した **showipv6neighbors** コマンドの出力例を示します。

```
Device# show ipv6 neighbors ethernet 2
IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH Ethernet2
```

```
FE80::203:A0FF:FED6:141E                    0 0003.a0d6.141e  REACH Ethernet2
3001:1::45a                                 - 0002.7d1a.9472  REACH Ethernet2
```

次に IPv6 アドレスを指定して入力した **showipv6neighbors** コマンドの出力例を示します。

```
Device# show ipv6 neighbors 2000:0:0:4::2
IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH Ethernet2
```

下の表で、この出力で表示される重要なフィールドについて説明します。

表 *26 : show ipv6 neighbors* フィールドの説明

フィールド	説明
IPv6 Address	隣接またはインターフェイスの IPv6 アドレス。
Age	アドレスが到達可能と確認されてから経過した時間（分）。ハイフン（-）はスタティック エントリを示します。
Link-layer Addr	MAC アドレス。アドレスが不明の場合、ハイフン（-）が表示されます。

フィールド	説明
State	隣接キャッシュ エントリの状態。次に、IPv6 ネイバー探索キャッシュのダイナミック エントリの状態を示します。 • INCMP (Incomplete)：アドレス解決がエントリで実行中です。ネイバー送信要求メッセージがターゲットの送信要求ノード マルチキャスト アドレスに送信されましたが、対応するネイバー アドバタイズメント メッセージが受信されていません。 • REACH (Reachable)：ネイバーへの転送パスが正しく機能していたことを示す確認が、最後の ReachableTime ミリ秒内に受信されました。REACH 状態になっている間は、パケットが送信されるときにデバイスは特別なアクションを実行しません。 • STALE：転送パスが正しく機能していたことを示す確認が最後に受信されてから経過した時間が ReachableTime ミリ秒を超えています。STALE 状態になっている間は、パケットが送信されるまでデバイスはアクションを実行しません。 • DELAY：転送パスが正しく機能していたことを示す確認が最後に受信されてから経過した時間が ReachableTime ミリ秒を超えています。パケットは直近の DELAY_FIRST_PROBE_TIME 秒以内に送信されました。DELAY 状態に入ってから、DELAY_FIRST_PROBE_TIME 秒以内に到達可能性確認を受信できない場合は、ネイバー送信要求メッセージが送信され、状態が PROBE に変更されます。 • PROBE：到達可能性確認が受信されるまで、RetransTimer ミリ秒ごとに、ネイバー送信要求メッセージを再送信することで、到達可能性確認がアクティブに求められます。 • ????：不明な状態。 次に、IPv6 ネイバー探索キャッシュのスタティック エントリの可能な状態を示します。 • INCMP（不完全）：このエントリのインターフェイスがダウンしています。 • REACH（到達可能）：このエントリのインターフェイスがアップしています。 （注） 到達可能性検出は IPv6 ネイバー探索キャッシュのスタティック エントリに適用されないため、INCMP（不完全）状態と REACH（到達可能）状態の記述は、ダイナミック キャッシュ エントリとスタティック キャッシュ エントリで異なります。
Interface	アドレスに到達可能であったインターフェイス。

次に、**statistics** キーワードを指定した **showipv6neighbors** コマンドの出力例を示します。

```
Device# show ipv6 neighbor statistics

IPv6 ND Statistics
 Entries 2, High-water 2, Gleaned 1, Scavenged 0
 Entry States
   INCMP 0  REACH 0  STALE 2  GLEAN 0  DELAY 0  PROBE 0
 Resolutions (INCMP)
   Requested 1, timeouts 0, resolved 1, failed 0
   In-progress 0, High-water 1, Throttled 0, Data discards 0
 Resolutions (PROBE)
   Requested 3, timeouts 0, resolved 3, failed 0
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *27 : show ipv6 neighbors statistics* フィールドの説明

フィールド	説明
Entries	ND キャッシュ内の ND ネイバー エントリの総数。
High-Water	ND キャッシュ内の ND ネイバー エントリの（現在までの）最大量。
Gleaned	収集した（つまり、ネイバーNAはたは他のNDパケットから学習した）ND ネイバー エントリの数。
Scavenged	タイム アウトし、キャッシュから削除されている古いND ネイバー エントリの数。
Entry States	各状態の ND ネイバー エントリの数。
Resolutions (INCMP)	INCMP状態で試行されたネイバー解決（データ パケットによるプロンプトでの解決）の統計。INCMP状態で試行された解決の詳細は次のとおりです。 • Requested：要求された解決の総数。 • Timeouts：解決時のタイムアウトの数。 • Resolved：正常に解決された数。 • Failed：失敗した解決の数。 • In-progress：進行中の解決の数。 • High-water：進行中の解決の（現在までの）最大数。 • Throttled：進行中の解決の最大数制限のため、解決要求が無視された回数。 • Data discards：ネイバー解決待機中のデータ パケットが破棄された数。

フィールド	説明
Resolutions (PROBE)	PROBE 状態で試行されたネイバー解決（データ パケットによるプロンプトでの既存エントリの再解決）の統計。 • Requested：要求された解決の総数。 • Timeouts：解決時のタイムアウトの数。 • Resolved：正常に解決された数。 • Failed：失敗した解決の数。

show ipv6 nhrp

Next Hop Resolution Protocol（NHRP）のマッピング情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6nhrp** コマンドを使用します。

show ipv6 nhrp [{**dynamic** [*ipv6-address*]|**incomplete**|**static**}] [{**address**|**interface**}] [{**brief**|**detail**}] **[purge]**

構文の説明

dynamic	（任意）ダイナミック（学習した）IPv6から非ブロードキャストマルチアクセスアドレス（NBMA）へのマッピングエントリを表示します。ダイナミックNHRPマッピングエントリは、NHRP解決/登録の交換から取得されます。タイプ、番号範囲、説明については、下の表を参照してください。
ipv6-address	（任意）キャッシュエントリの IPv6 アドレス。
incomplete	（任意）IPv6 から NBMA に解決されていない NHRP マッピング エントリに関する情報を表示します。タイプ、番号範囲、説明については、下の表を参照してください。
static	（任意）静的 IPv6 から NBMA アドレスへのマッピング エントリを表示します。静的NHRPマッピングエントリは、**ipv6nhrpmap** コマンドを使用して設定します。タイプ、番号範囲、説明については、下の表を参照してください。
address	（任意）指定したプロトコル アドレスの NHRP マッピング エントリ。
interface	（任意）指定したインターフェイスのNHRPマッピングエントリ。タイプ、番号範囲、説明については、下の表を参照してください。
brief	（任意）NHRP マッピングの短い出力を表示します。
detail	（任意）NHRP マッピングに関する詳細な情報を表示します。
purge	（任意）NHRP 消去情報を表示します。

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

次の表に、オプションの *interface* 引数の有効なタイプ、番号の範囲、および説明を示します。

（注） 有効なタイプは、プラットフォームとプラットフォーム上のインターフェイスによって異なります。

表 *28 :* 有効なタイプ、番号の範囲、およびインターフェイスの説明

有効なタイプ	番号の範囲	インターフェイスの説明
async	1	Async
atm	0 ～ 6	ATM
bvi	1 ～ 255	ブリッジ グループ仮想インターフェイス
cdma-ix	1	CDMA Ix
ctunnel	0 ～ 2,147,483,647	C トンネル
dialer	0 ～ 20049	ダイヤラ
ethernet	0 ～ 4294967295	イーサネット
fastethernet	0 ～ 6	FastEthernet IEEE 802.3
lex	0 ～ 2,147,483,647	Lex
loopback	0 ～ 2,147,483,647	ループバック
mfr	0 ～ 2,147,483,647	マルチリンク フレーム リレー バンドル
multilink	0 ～ 2,147,483,647	マルチリンク グループ
null	0	ヌル
port-channel	1 ～ 64	ポート チャネル
tunnel	0 ～ 2,147,483,647	Tunnel
vif	1	PGM マルチキャスト ホスト
virtual-ppp	0 ～ 2,147,483,647	仮想 PPP
virtual-template	1 ～ 1000	Virtual template

有効なタイプ	番号の範囲	インターフェイスの説明
virtual-tokenring	0 ～ 2,147,483,647	仮想トークンリング
xtagatm	0 ～ 2,147,483,647	拡張タグ ATM

例

次に、**showipv6nhrp** コマンドの出力例を示します。

```
Device# show ipv6 nhrp
2001:0db8:3c4d:0015::1a2f:3d2c/48  via
2001:0db8:3c4d:0015::1a2f:3d2c
Tunnel0 created 6d05h, never expire
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *29 : show ipv6 nhrp* フィールドの説明

フィールド	説明
2001:0db8:3c4d:0015::1a2f: 3d2c/48	ターゲット ネットワーク。
2001:0db8:3c4d:0015::1a2f:3d2c	ターゲット ネットワークに到達するためのネクスト ホップ。
Tunnel0	ターゲットネットワークに到達するために経由するインターフェイス。
created 6d05h	エントリが作成されてからの時間（dayshours）。
never expire	静的エントリの期限が満了することはないことを指定します。

次に、**brief** キーワードを使用した **showipv6nhrp** コマンドの出力例を示します。

```
Device# show ipv6 nhrp brief
2001:0db8:3c4d:0015:0000:0000:1a2f:3d2c/48
 via 2001:0db8:3c4d:0015:0000:0000:1a2f:3d2c
Interface: Tunnel0 Type: static
NBMA address: 10.11.11.99
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *30 : show ipv6 nhrp brief* フィールドの説明

フィールド	説明
2001:0db8:3c4d:0015:0000:0000: 1a2f:3d2c/48	ターゲット ネットワーク。

フィールド	説明
via 2001:0db8:3c4d:0015:0000:0000:1a2f:3d2c	ターゲット ネットワークに到達するためのネクスト ホップ。
Interface: Tunnel0	ターゲット ネットワークに到達するために経由するインターフェイス。
Type: static	トンネルのタイプ。タイプは次のいずれかになります。 • dynamic：NHRPマッピングをダイナミックに取得します。マッピング エントリはNHRP の解決と登録の情報を使用して作成されます。 • static：NHRP マッピングは静的に設定されます。**ipv6nhrpmap** コマンドによって作成されたエントリは「static」というマークが付けられます。 • incomplete：ターゲット ネットワークの NBMA アドレスが不明です。

関連コマンド

コマンド	説明
ipv6nhrpmap	NBMA ネットワークに接続された IP の宛て先の IPv6 から NBMA へのアドレス マッピングを静的に設定します。

show ipv6 ospf

Open Shortest Path First（OSPF）ルーティング プロセスに関する一般情報を表示するには、ユーザ EXEC または特権 EXEC モードで **showipv6ospf** コマンドを使用します。

show ipv6 ospf [*process-id*] [*area-id*] **[rate-limit]**

構文の説明

process-id	（任意）内部ID。ローカルで割り当てられ、任意の正の整数を使用できます。ここで使用される番号は、OSPF ルーティング プロセスが有効になっているときに管理する目的で割り当てられた番号です。
area-id	（任意）エリアID。（任意）この引数は指定したエリアに関する情報のみを表示します。
rate-limit	（任意）レート制限リンクステートアドバタイズメント（LSA）。このキーワードは、現在レートが制限されているLSAとともに、次の生成までの残り時間を表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

show ipv6 ospf の出力例

次に、**showipv6ospf** コマンドの出力例を示します。

```
Device# show ipv6 ospf
Routing Process "ospfv3 1" with ID 10.10.10.1
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of areas in this device is 1. 1 normal 0 stub 0 nssa
    Area BACKBONE(0)
        Number of interfaces in this area is 1
        MD5 Authentication, SPI 1000
        SPF algorithm executed 2 times
        Number of LSA 5. Checksum Sum 0x02A005
        Number of DCbitless LSA 0
        Number of indication LSA 0
```

```
        Number of DoNotAge LSA 0
        Flood list length 0
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *31 : show ipv6 ospf* フィールドの説明

フィールド	説明
Routing process "ospfv3 1" with ID 10.10.10.1	プロセス ID と OSPF デバイス ID。
LSA group pacing timer	設定されている LSA グループ ペーシング タイマー（秒単位）。
Interface flood pacing timer	設定されている LSA フラッド ペーシング タイマー（ミリ秒単位）。
Retransmission pacing timer	設定されている LSA 再送信ペーシング タイマー（ミリ秒単位）。
Number of areas	デバイス内のエリアの数、エリア アドレスなど。

エリア 暗号化を使用した show ipv6 ospf の例

次に、エリア暗号化情報を使用した **showipv6ospf** コマンドの出力例を示します。

```
Device# show ipv6 ospf
Routing Process "ospfv3 1" with ID 10.0.0.1
It is an area border device
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this device is 2. 2 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps
    Area BACKBONE(0)
        Number of interfaces in this area is 2
        SPF algorithm executed 3 times
        Number of LSA 31. Checksum Sum 0x107493
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 20
        Flood list length 0
    Area 1
        Number of interfaces in this area is 2
        NULL Encryption SHA-1 Auth, SPI 1001
        SPF algorithm executed 7 times
        Number of LSA 20. Checksum Sum 0x095E6A
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *32 :* エリア 暗号化情報を使用した *show ipv6 ospf* フィールドの説明

フィールド	説明
Area 1	後続のフィールドでエリア 1 を説明します。
NULL Encryption SHA-1 Auth, SPI 1001	暗号化アルゴリズム（この場合はヌル。つまり暗号化アルゴリズムは使用されていない）、認証アルゴリズム（SHA-1）、およびセキュリティ ポリシー インデックス（SPI）値（1001）を表示します。

次に、SPF およびLSA のスロットリング タイマーの設定値を表示する例を示します。

```
Device# show ipv6 ospf
 Routing Process "ospfv3 1" with ID 10.9.4.1
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 It is an autonomous system boundary device
 Redistributing External Routes from,
    ospf 2
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *33 : SPF* および *LSA* スロットリングを使用した *show ipv6 ospf* フィールドの説明

フィールド	説明
Initial SPF schedule delay	SPF 計算の遅延時間
Minimum hold time between two consecutive SPFs	連続する SPF 計算間の最小保持時間。
Maximum wait time between two consecutive SPFs 10000 msecs	連続する SPF 計算間の最大保持時間。
Minimum LSA interval 5 secs	リンクステート アドバタイズメント間の最小時間間隔（秒単位）。
Minimum LSA arrival 1000 msecs	リンクステート アドバタイズメントの最大着信時間（ミリ秒単位）。

次に、現在レートが制限されている LSA に関する情報の例を示します。

```
Device# show ipv6 ospf rate-limit
List of LSAs that are in rate limit Queue
    LSAID: 0.0.0.0 Type: 0x2001 Adv Rtr: 10.55.55.55 Due in: 00:00:00.500
    LSAID: 0.0.0.0 Type: 0x2009 Adv Rtr: 10.55.55.55 Due in: 00:00:00.500
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *34 : show ipv6 ospf rate-limit* フィールドの説明

フィールド	説明
LSAID	LSA のリンクステート ID
Type	LSA の説明
Adv Rtr	アドバタイジング デバイスの ID。
Due in:	次のイベント生成までの残り時間。

show ipv6 ospf border-routers

エリア境界ルータ（ABR）および自律システム境界ルータ（ASBR）に対する内部Open Shortest Path First（OSPF）ルーティング テーブルのエントリを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6ospfborder-routers** コマンドを使用します。

show ip ospf [*process-id*] **border-routers**

構文の説明

process-id	（任意）内部ID。ローカルで割り当てられ、任意の正の整数を使用できます。ここで使用される番号は、OSPF ルーティング プロセスが有効になっているときに管理する目的で割り当てられた番号です。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

例

次に、**showipv6ospfborder-routers** コマンドの出力例を示します。

```
Device# show ipv6 ospf border-routers

OSPFv3 Process 1 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 172.16.4.4 [2] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ABR, Area 1, SPF 13
i 172.16.4.4 [1] via FE80::205:5FFF:FED3:5406, POS4/0, ABR, Area 0, SPF 8
i 172.16.3.3 [1] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ASBR, Area 1, SPF 3
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *35 : show ipv6 ospf border-routers* フィールドの説明

フィールド	説明
i - Intra-area route, I - Inter-area route	このルートのタイプ。
172.16.4.4, 172.16.3.3	宛て先ルータのルータ ID。
[2], [1]	宛て先ルータに到達するために使用するメトリック。
FE80::205:5FFF:FED3:5808, FE80::205:5FFF:FED3:5406, FE80::205:5FFF:FED3:5808	リンクローカル ルータ。

フィールド	説明
FastEthernet0/0, POS4/0	IPv6 OSPF プロトコルを設定するインターフェイス。
ABR	エリア境界ルータ。
ASBR	自律システム境界ルータ。
Area 0, Area 1	このルートが学習されるエリアのエリア ID。
SPF 13, SPF 8, SPF 3	このルートをインストールする Shortest Path First（SPF）計算の内部番号。

show ipv6 ospf event

IPv6 Open Shortest Path First（OSPF）イベントに関する詳細情報を表示するには、特権 EXEC モードで **show ipv6 ospf event** コマンドを使用します。

show ipv6 ospf [*process-id*] **event** [{**generic**|**interface**|**lsa**|**neighbor**|**reverse**|**rib**|**spf**}]

構文の説明

process-id	（任意）内部ID。ローカルで割り当てられ、任意の正の整数を使用できます。ここで使用される番号は、OSPF ルーティング プロセスが有効になっているときに管理する目的で割り当てられた番号です。
generic	（任意）IPv6 イベントに関する一般的な情報。
interface	（任意）新旧の状態を含むインターフェイス状態変更イベント。
lsa	（任意）LSA 着信イベントおよび LSA 生成イベント。
neighbor	（任意）新旧の状態を含むネイバー状態変更イベント。
reverse	（任意）イベントの表示を最新のものから最も古いものへ、または最も古いものから最新のものへと逆転させるためのキーワード。
rib	（任意）ルーティング情報ベース（RIB）の更新イベント、削除イベント、および再配布イベント。
spf	（任意）スケジューリングおよび SPF 実行イベント。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

OSPF イベントログは OSPF インスタンスごとに保持されます。キーワードを指定せずに **showipv6ospfevent** コマンドを入力すると、OSPF イベントログ内のすべての情報が表示されます。特定の情報をフィルタ処理するには、このキーワードを使用します。

例

次の例は、スケジューリングと SPF 実行イベント、LSA 着信イベント、および LSA 生成イベントを最も古いイベントから最新の生成済みイベントの順に示しています。

```
Device# show ipv6 ospf event spf lsa reverse

OSPFv3 Router with ID (10.0.0.1) (Process ID 1)
1 *Sep 29 11:59:18.367: Rcv Changed Type-0x2009 LSA, LSID 10.0.0.0, Adv-Rtr 192.168.0.1,
 Seq# 80007699, Age 3600
```

```
3 *Sep 29 11:59:18.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type P
4 *Sep 29 11:59:18.367: Rcv Changed Type-0x2001 LSA, LSID 10.0.0.0, Adv-Rtr 192.168.0.1,
 Seq# 80007699, Age 2
5 *Sep 29 11:59:18.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type R
6 *Sep 29 11:59:18.367: Rcv Changed Type-0x2002 LSA, LSID 10.1.0.1, Adv-Rtr 192.168.0.1,
 Seq# 80007699, Age 3600
8 *Sep 29 11:59:18.367: Schedule SPF, Area 0, Change in LSID 10.1.0.1, LSA type N
9 *Sep 29 11:59:18.367: Rcv Changed Type-0x2001 LSA, LSID 10.0.0.0, Adv-Rtr 1.1.1.1,
Seq# 80007699, Age 2
10 *Sep 29 11:59:18.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type R
11 *Sep 29 11:59:18.867: Starting SPF
12 *Sep 29 11:59:18.867: Starting Intra-Area SPF in Area 0
16 *Sep 29 11:59:18.867: Starting Inter-Area SPF in area 0
17 *Sep 29 11:59:18.867: Starting External processing
18 *Sep 29 11:59:18.867: Starting External processing in area 0
19 *Sep 29 11:59:18.867: Starting External processing in area 1
20 *Sep 29 11:59:18.867: End of SPF
21 *Sep 29 11:59:19.367: Generate Changed Type-0x2003 LSA, LSID 10.0.0.4, Seq# 80000002,
 Age 3600, Area 1, Prefix 3000:11:22::/64
23 *Sep 29 11:59:20.367: Rcv Changed Type-0x2009 LSA, LSID 10.0.0.0, Adv-Rtr 192.168.0.1,
 Seq# 8000769A, Age 2
24 *Sep 29 11:59:20.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type P
25 *Sep 29 11:59:20.367: Rcv Changed Type-0x2001 LSA, LSID 10.0.0.0, Adv-Rtr 192.168.0.1,
 Seq# 8000769A, Age 2
26 *Sep 29 11:59:20.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type R
27 *Sep 29 11:59:20.367: Rcv Changed Type-0x2002 LSA, LSID 10.1.0.1, Adv-Rtr 192.168.0.1,
 Seq# 8000769A, Age 2
28 *Sep 29 11:59:20.367: Schedule SPF, Area 0, Change in LSID 10.1.0.1, LSA type N
29 *Sep 29 11:59:20.367: Rcv Changed Type-0x2001 LSA, LSID 10.0.0.0, Adv-Rtr 1.1.1.1,
Seq# 8000769A, Age 2
30 *Sep 29 11:59:20.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type R
31 *Sep 29 11:59:20.867: Starting SPF
32 *Sep 29 11:59:20.867: Starting Intra-Area SPF in Area 0
36 *Sep 29 11:59:20.867: Starting Inter-Area SPF in area 0
37 *Sep 29 11:59:20.867: Starting External processing
38 *Sep 29 11:59:20.867: Starting External processing in area 0
39 *Sep 29 11:59:20.867: Starting External processing in area 1
40 *Sep 29 11:59:20.867: End of SPF
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *36 : show ip ospf* フィールドの説明

フィールド	説明
OSPFv3 Router with ID (10.0.0.1) (Process ID 1)	プロセス ID および OSPF ルータ ID。
Rcv Changed Type-0x2009 LSA	新たに着信した LSA の説明。
LSID	LSA のリンクステート ID
Adv-Rtr	アドバタイジング ルータの ID です。
Seq#	リンク ステート シーケンス番号（以前の、または重複した LSA を検出します）
Age	リンク状態の期間経過（秒単位）。
Schedule SPF	実行する SPF を有効にします。

フィールド	説明
Area	OSPF エリア ID。
Change in LSID	LSA の変更後のリンクステート ID。
LSA type	LSA タイプ

show ipv6 ospf graceful-restart

Open Shortest Path First for IPv6（OSPFv3）グレースフル リスタート情報を表示するには、特権 EXEC モードで **showipv6ospfgraceful-restart** コマンドを使用します。

show ipv6 ospf graceful-restart

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 モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

OSPFv3 グレースフル リスタート機能に関する情報を検出するには、**showipv6ospfgraceful-restart** コマンドを使用します。

例

次に、OSPFv3 グレースフル リスタート情報を表示する例を示します。

```
Device# show ipv6 ospf graceful-restart
Routing Process "ospf 1"
 Graceful Restart enabled
    restart-interval limit: 120 sec, last restart 00:00:15 ago (took 36 secs)
  Graceful Restart helper support enabled
  Router status : Active
  Router is running in SSO mode
  OSPF restart state : NO_RESTART
  Router ID 10.1.1.1, checkpoint Router ID 10.0.0.0
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 37 : show ipv6 ospf graceful-restart フィールドの説明

フィールド	説明
Routing Process "ospf 1"	OSPFv3 ルーティング プロセス ID。
Graceful Restart enabled	このルータでグレースフル リスタート機能が有効になっています。
restart-interval limit: 120 sec	リスタート間隔の制限。
last restart 00:00:15 ago (took 36 secs)	最後にグレースフル リスタートが実行されてからの経過時間と、実行に要した時間。

フィールド	説明
Graceful Restart helper support enabled	グレースフル リスタート ヘルパー モードが有効になっています。このルータ上でもグレースフル リスタート モードが有効になっているため、このルータはグレースフルリスタート対応として識別できます。グレースフルリスタート認識型のルータはグレースフルリスタート モードでは設定できません。
Router status : Active	このルータは、スタンバイとは対照的に、アクティブモードです。
Router is running in SSO mode	ルータはステートフル スイッチオーバー モードです。
OSPF restart state : NO_RESTART	現在の OSPFv3 のリスタート状態。
Router ID 10.1.1.1, checkpoint Router ID 10.0.0.0	現在のルータとチェックポイント ルータの IPv6 アドレス。

関連コマンド

コマンド	説明
showipv6ospfinterface	OSPFv3 関連のインターフェイス情報を表示します。

show ipv6 ospf interface

Open Shortest Path First（OSPF）関連のインターフェイス情報を表示するには、ユーザ EXEC または特権 EXEC モードで **showipv6ospfinterface** コマンドを使用します。

show ipv6 ospf [*process-id*] [*area-id*] **interface** [*type number*] **[brief]**

構文の説明

process-id	（任意）内部ID。ローカルで割り当てられ、任意の正の整数を使用できます。ここで使用される番号は、OSPF ルーティング プロセスが有効になっているときに管理する目的で割り当てられた番号です。
area-id	（オプション）指定したエリアに関する情報だけを表示します。
type number	（任意）インターフェイス タイプおよび番号
brief	（任意）OSPFインターフェイス、状態、アドレスとマスク、およびルータのエリアに関する簡単な概要情報を表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

例

show ipv6 ospf interface 標準出力例

次は、**showipv6ospfinterface** コマンドの出力例です。

```
Device# show ipv6 ospf interface
ATM3/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 13
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type POINT_TO_POINT, Cost: 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.4.4
  Suppress hello for 0 neighbor(s)
FastEthernet0/0 is up, line protocol is up
```

```
Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 3
Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 172.16.6.6, local address 2001:0DB1:205:5FFF:FED3:6408
Backup Designated router (ID) 172.16.3.3, local address 2001:0DB1:205:5FFF:FED3:5808
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:05
Index 1/1/1, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 12, maximum is 12
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 172.16.6.6  (Designated Router)
Suppress hello for 0 neighbor(s)
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *38 : show ipv6 ospf interface* フィールドの説明

フィールド	説明
ATM3/0	物理リンクのステータス、およびプロトコルの動作ステータス。
Link Local Address	インターフェイス IPv6 アドレス
Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3	このルータを学習するエリアのエリア ID、プロセス ID、インスタンス ID、およびルータ ID。
Network Type POINT_TO_POINT, Cost: 1	ネットワーク タイプとリンクステート コスト。
Transmit Delay	転送遅延、インターフェイス ステート、およびルータ プライオリティ
Designated Router	指定ルータ ID および各インターフェイス IP アドレス。
Backup Designated router	バックアップ指定ルータ ID および各インターフェイス IP アドレス。
Timer intervals configured	タイマー インターバルの設定
Hello	次の hello パケットがこのインターフェイスから送信されるまでの時間（秒単位）。
Neighbor Count	ネットワーク ネイバーの数、および隣接ネイバーのリスト。

Cisco IOS Release 12.2(33) SRB の例

次に、**brief** キーワードを入力した場合の **showipv6ospfinterface** コマンドの出力例を示します。

```
Device# show ipv6 ospf interface brief

Interface    PID   Area            Intf ID    Cost  State Nbrs F/C
VL0          6     0               21         65535 DOWN  0/0
Se3/0        6     0               14         64    P2P   0/0
Lo1          6     0               20         1     LOOP  0/0
Se2/0        6     6               10         62    P2P   0/0
Tu0          1000  0               19         11111 DOWN  0/0
```

インターフェイス上で認証を使用した OSPF の例

次に、インターフェイスでの認証が有効になっている **showipv6ospfinterface** コマンドの出力例を示します。

```
Device# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  MD5 Authentication SPI 500, secure socket state UP (errors:0)
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.11.11.1, local address 2001:0DB1:A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address
2001:0DB1:A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.11.11.1  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

ヌル認証を使用した OSPF の例

次に、ヌル認証をインターフェイス上に設定した **showipv6ospfinterface** コマンドの出力例を示します。

```
Device# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  Authentication NULL
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.11.11.1, local address 2001:0DB1:A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address
2001:0DB1:A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
```

```
    Adjacent with neighbor 10.11.11.1  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

エリアに認証を使用した OSPF の例

次に、エリアに認証を設定した **showipv6ospfinterface** コマンドの出力例を示します。

```
Device# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  MD5 Authentication (Area) SPI 1000, secure socket state UP (errors:0)
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.11.11.1, local address 2001:0DB1:A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address
FE80::A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.11.11.1  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

ダイナミック コストを使用した OSPF の例

次に、OSPF コスト ダイナミックを設定した場合の **showipv6ospfinterface** コマンドの出力例を示します。

```
Device# show ipv6 ospf interface serial 2/0
Serial2/0 is up, line protocol is up
   Link Local Address 2001:0DB1:A8BB:CCFF:FE00:100, Interface ID 10
   Area 1, Process ID 1, Instance ID 0, Router ID 172.1.1.1
   Network Type POINT_TO_MULTIPOINT, Cost: 64 (dynamic), Cost Hysteresis: 200
   Cost Weights: Throughput 100, Resources 20, Latency 80, L2-factor 100
   Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT,
   Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
     Hello due in 00:00:19
   Index 1/2/3, flood queue length 0
   Next 0x0(0)/0x0(0)/0x0(0)
   Last flood scan length is 0, maximum is 0
   Last flood scan time is 0 msec, maximum is 0 msec
   Neighbor Count is 0, Adjacent neighbor count is 0
   Suppress hello for 0 neighbor(s)
```

OSPF グレースフル リスタートの例

次に、OSPF グレースフル リスタート機能を設定した場合の **showipv6ospfinterface** コマンドの出力例を示します。

```
Device# show ipv6 ospf interface
```

```
Ethernet0/0 is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE00:300, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.3.3.3
  Network Type POINT_TO_POINT, Cost: 10
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   Graceful Restart p2p timeout in 00:00:19
    Hello due in 00:00:02
  Graceful Restart helper support enabled
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.1.1
  Suppress hello for 0 neighbor(s)
```

有効化されたプロトコルの例

次に、Bidirectional Forwarding Detection（BFD）にOSPFインターフェイスが有効になっている例を示します。

```
Device# show ipv6 ospf interface
Serial10/0 is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE00:6500, Interface ID 42
  Area 1, Process ID 1, Instance ID 0, Router ID 10.0.0.1
  Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT, BFD enabled
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.0.1
  Suppress hello for 0 neighbor(s)
```

関連コマンド

コマンド	説明
showipv6ospfgraceful-restart	OSPFv3 グレースフル リスタートの情報を表示します。

show ipv6 ospf request-list

ルータが要求したすべてのリンクステートアドバタイズメントのリストを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6ospfrequest-list** コマンドを使用します。

show ipv6 ospf [*process-id*] [*area-id*] **request-list** [*neighbor*] [*interface*] [*interface-neighbor*]

構文の説明

process-id	（任意）内部 ID。ローカルで割り当てられ、任意の正の整数を使用できます。ここで使用される番号は、Open Shortest Path First（OSPF）ルーティング プロセスが有効になっているときに管理する目的で割り当てられた番号です。
area-id	（任意）指定したエリアに関する情報のみを表示します。
neighbor	（任意）このネイバーからルータにより要求されるすべての LSA のリストを表示します。
interface	（任意）このインターフェイスからルータにより要求されるすべての LSA のリストを表示します。
interface-neighbor	（任意）このネイバーのインターフェイスのルータが要求するすべての LSA のリストを表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

showipv6ospfrequest-list コマンドによって表示される情報は、OSPF ルーティング動作のデバッグに役立ちます。

例

次に、ルータが要求する LSA に関する情報の例を示します。

```
Device# show ipv6 ospf request-list

           OSPFv3 Router with ID (192.168.255.5) (Process ID 1)
 Neighbor 192.168.255.2, interface Ethernet0/0 address
FE80::A8BB:CCFF:FE00:6600
 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
  1      0.0.0.0         192.168.255.3   0x800000C2  1      0x0014C5
  1      0.0.0.0         192.168.255.2   0x800000C8  0      0x000BCA
  1      0.0.0.0         192.168.255.1   0x800000C5  1      0x008CD1
```

```
  2       0.0.0.3         192.168.255.3   0x800000A9  774     0x0058C0
  2       0.0.0.2         192.168.255.3   0x800000B7  1       0x003A63
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *39 : show ipv6 ospf request-list* フィールドの説明

フィールド	説明
OSPFv3 Router with ID (192.168.255.5) (Process ID 1)	情報が表示されるルータの ID。
Interface Ethernet0/0	情報が表示されるインターフェイス
Type	LSA のタイプ
LS ID	LSA のリンクステート ID
ADV RTR	アドバタイズ ルータの IP アドレス
Seq NO	LSA のシーケンス番号
Age	LSA の経過時間（秒単位）
Checksum	LSA のチェックサム

show ipv6 ospf retransmission-list

再送信を待機しているすべてのリンクステートアドバタイズメントのリストを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6ospfretransmission-list** コマンドを使用します。

show ipv6 ospf [*process-id*] [*area-id*] **retransmission-list** [*neighbor*] [*interface*] [*interface-neighbor*]

構文の説明

process-id	（任意）内部 ID。ローカルで割り当てられ、任意の正の整数を使用できます。ここで使用される番号は、OSPF ルーティング プロセスが有効になっているときに管理する目的で割り当てられた番号です。
area-id	（任意）指定したエリアに関する情報のみを表示します。
neighbor	（任意）このネイバーの再送信を待機しているすべての LSA のリストを表示します。
interface	（任意）このインターフェイスで再送信を待機しているすべての LSA のリストを表示します。
interface neighbor	（任意）このネイバーからこのインターフェイスで再送信を待機しているすべての LSA のリストを表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

showipv6ospfretransmission-list コマンドによって表示される情報は、Open Shortest Path First（OSPF）ルーティング動作のデバッグに役立ちます。

例

次は、**showipv6ospfretransmission-list** コマンドの出力例です。

```
Device# show ipv6 ospf retransmission-list

        OSPFv3 Router with ID (192.168.255.2) (Process ID 1)
 Neighbor 192.168.255.1, interface Ethernet0/0
 Link state retransmission due in 3759 msec, Queue length 1
 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
 0x2001  0               192.168.255.2   0x80000222  1      0x00AE52
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *40 : show ipv6 ospf retransmission-list* フィールドの説明

フィールド	説明
OSPFv3 Router with ID (192.168.255.2) (Process ID 1)	情報が表示されるルータの ID。
Interface Ethernet0/0	情報が表示されるインターフェイス
Link state retransmission due in	次のリンクステート送信までの時間
Queue length	再送信キューのエレメントの数
Type	LSA のタイプ
LS ID	LSA のリンクステート ID
ADV RTR	アドバタイズ ルータの IP アドレス
Seq NO	LSA のシーケンス番号.
Age	LSA の経過時間（秒単位）
Checksum	LSA のチェックサム

show ipv6 ospf statistics

Open Shortest Path First for IPv6（OSPFv6）最短パス優先（SPF）計算の統計を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6ospfstatistics** コマンドを使用します。

show ipv6 ospf statistics [detail]

構文の説明

detail	（任意）各 OSPF エリアの統計情報を個別に表示し、追加の詳細統計情報を含めます。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

showipv6ospfstatistics コマンドは、SPF 計算およびそれらをトリガーするイベントに関する重要な情報を提供します。この情報は、OSPF ネットワーク メンテナンスおよびトラブルシューティングの両方に役に立ちます。たとえば、**showipv6ospfstatistics** コマンドは、リンクステートアドバタイズメント（LSA）フラッピングのトラブルシューティングの最初のステップとして入力することをお勧めします。

例

次に、各 OSPFv6 エリアの詳細な統計の例を示します。

```
Device# show ipv6 ospf statistics detail
  Area 0: SPF algorithm executed 3 times
SPF 1 executed 00:06:57 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
  0      0      0      0      0      0      0      0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
  0             0
  LSIDs processed R:1 N:0 Prefix:0 SN:0 SA:0 X7:0
  Change record R N SN SA L
  LSAs changed 1
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  10.2.2.2/0(R)
SPF 2 executed 00:06:47 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
  0      0      0      0      0      0      0      0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
  0             0
  LSIDs processed R:1 N:0 Prefix:1 SN:0 SA:0 X7:0
  Change record R L P
```

```
LSAs changed 4
Changed LSAs. Recorded is Advertising Router, LSID and LS type:
10.2.2.2/2(L) 10.2.2.2/0(R) 10.2.2.2/2(L) 10.2.2.2/0(P)
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *41 : show ipv6 ospf statistics* フィールドの説明

フィールド	説明
Area	OSPF エリア ID。
SPF	OSPF エリアで実行された SPF アルゴリズムの数。この数は、エリアで SPF アルゴリズムが実行されるたびに 1 つずつ増加します。
Executed ago	SPF アルゴリズムが実行されてから現在の時間までの経過時間（ミリ秒単位）。
SPF type	SPF タイプは Full または Incremental のいずれかです。
SPT	SPF アルゴリズムの最初のステージの計算（ショート パス ツリーの構築）に必要な時間（ミリ秒単位）。SPT 時間とスタブ ネットワークのリンクの処理に必要な時間の合計が、内部時間と等しくなります。
Ext	SPF アルゴリズムが外部および Not So Stubby Area（NSSA）の LSA を処理し、外部および NSSA ルートをルーティング テーブルにインストールする時間（ミリ秒単位）。
Total	SPF アルゴリズム プロセスの合計継続時間（ミリ秒単位）。
LSIDs processed	SPF 計算中に処理された LSA の数： • N：ネットワーク の LSA。 • R：ルータ の LSA。 • SA：サマリー自律システム境界ルータ（ASBR）（SA）の LSA。 • SN：サマリー ネットワーク（SN）の LSA。 • Stub：スタブ リンク。 • X7：外部タイプ 7（X7）の LSA。

show ipv6 ospf summary-prefix

OSPF プロセスに設定されているすべてのサマリー アドレス再配布情報のリストを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6ospfsummary-prefix** コマンドを使用します。

show ipv6 ospf [*process-id*] **summary-prefix**

構文の説明

process-id	（任意）内部ID。ローカルで割り当てられ、任意の正の整数を使用できます。ここで使用される番号は、OSPF ルーティング プロセスが有効になっているときに管理する目的で割り当てられた番号です。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

引数 *process-id* は、10 進数または IPv6 アドレス フォーマットで入力できます。

例

次は、**showipv6ospfsummary-prefix** コマンドの出力例です。

```
Device# show ipv6 ospf summary-prefix

OSPFv3 Process 1, Summary-prefix
FEC0::/24 Metric 16777215, Type 0, Tag 0
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *42 : show ipv6 ospf summary-prefix* フィールドの説明

フィールド	説明
OSPFv3 Process	情報が表示されるルータのプロセス ID。
Metric	宛て先ルータに到達するために使用するメトリック。
Type	リンクステートアドバタイズメント（LSA）のタイプ。
Tag	LSA タグ。

show ipv6 ospf timers rate-limit

レート制限キュー内のすべてのリンクステートアドバタイズメント（LSA）を表示するには、特権 EXEC モードで **showipv6ospftimersrate-limit** コマンドを使用します。

show ipv6 ospf timers rate-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 モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

キュー内の LSA がいつ送信されるかを把握するには、**showipv6ospftimersrate-limit** コマンドを使用します。

例

show ipv6 ospf timers rate-limit の出力例

次に、**showipv6ospftimersrate-limit** コマンドの出力例を示します。

```
Device# show ipv6 ospf timers rate-limit
List of LSAs that are in rate limit Queue
    LSAID: 0.0.0.0 Type: 0x2001 Adv Rtr: 55.55.55.55 Due in: 00:00:00.500
    LSAID: 0.0.0.0 Type: 0x2009 Adv Rtr: 55.55.55.55 Due in: 00:00:00.500
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 43 : show ipv6 ospf timers rate-limit フィールドの説明

フィールド	説明
LSAID	LSA の ID
Type	LSA のタイプ
Adv Rtr	アドバタイジング ルータの ID です。
Due in:	LSA の送信スケジュール（時:分:秒形式）

show ipv6 ospf traffic

IPv6 Open Shortest Path First バージョン 3（OSPFv3）のトラフィック統計を表示するには、特権 EXEC モードで **show ipv6 ospf traffic** コマンドを使用します。

show ipv6 ospf [*process-id*] **traffic** [*interface-type interface-number*]

構文の説明

process-id	（任意）トラフィック統計情報を必要とする OSPF プロセス ID（たとえば、キュー統計情報、OSPF プロセス下の各インターフェイスの統計情報、OSPF ごとのプロセス統計情報などです）。
interface-type interface-number	（任意）特定の OSPF インターフェイスに関連付けられるタイプおよび番号。

コマンド デフォルト

引数を指定せずに **show ipv6 ospf traffic** コマンドを入力すると、グローバル OSPF トラフィック統計が表示されます。これには、各 OSPF プロセスのキュー統計、各インターフェイスの統計、および OSPF プロセスごとの統計が含まれています。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

表示されるトラフィック統計を特定の OSPF プロセスに限定するには、引数 *process-id* に値を入力します。または、出力を OSPF プロセスに関連付けられている特定のインターフェイスのトラフィック統計に限定するには、*interface-type* 引数と *interface-number* 引数に値を入力します。カウンタをリセットし、統計をクリアするには、**clear ipv6 ospf traffic** コマンドを使用します。

例

次に、OSPFv3 に対する **show ipv6 ospf traffic** コマンドの表示出力例を示します。

```
Device# show ipv6 ospf traffic
OSPFv3 statistics:
  Rcvd: 32 total, 0 checksum errors
        10 hello, 7 database desc, 2 link state req
        9 link state updates, 4 link state acks
        0 LSA ignored
  Sent: 45 total, 0 failed
        17 hello, 12 database desc, 2 link state req
        8 link state updates, 6 link state acks
        OSPFv3 Router with ID (10.1.1.4) (Process ID 6)
OSPFv3 queues statistic for process ID 6
  Hello queue size 0, no limit, max size 2
  Router queue size 0, limit 200, drops 0, max size 2
Interface statistics:
    Interface Serial2/0
```

```
OSPFv3 packets received/sent
  Type          Packets               Bytes
  RX Invalid    0                     0
  RX Hello      5                     196
  RX DB des     4                     172
  RX LS req     1                     52
  RX LS upd     4                     320
  RX LS ack     2                     112
  RX Total      16                    852
  TX Failed     0                     0
  TX Hello      8                     304
  TX DB des     3                     144
  TX LS req     1                     52
  TX LS upd     3                     252
  TX LS ack     3                     148
  TX Total      18                    900
OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,
OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
    Interface Ethernet0/0
OSPFv3 packets received/sent
  Type          Packets               Bytes
  RX Invalid    0                     0
  RX Hello      6                     240
  RX DB des     3                     144
  RX LS req     1                     52
  RX LS upd     5                     372
  RX LS ack     2                     152
  RX Total      17                    960
  TX Failed     0                     0
  TX Hello      11                    420
  TX DB des     9                     312
  TX LS req     1                     52
  TX LS upd     5                     376
  TX LS ack     3                     148
  TX Total      29                    1308
OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,
OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
Summary traffic statistics for process ID 6:
OSPFv3 packets received/sent
  Type          Packets               Bytes
  RX Invalid    0                     0
  RX Hello      11                    436
  RX DB des     7                     316
  RX LS req     2                     104
  RX LS upd     9                     692
  RX LS ack     4                     264
  RX Total      33                    1812
  TX Failed     0                     0
  TX Hello      19                    724
  TX DB des     12                    456
  TX LS req     2                     104
  TX LS upd     8                     628
  TX LS ack     6                     296
  TX Total      47                    2208
```

```
OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,
OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
```

ネットワーク管理者は、次に示すように **clear ipv6 ospf traffic** コマンドを入力することで、新しい統計の収集、カウンタのリセット、およびトラフィック統計のクリアを開始できます。

```
Device# clear ipv6 ospf traffic
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *44 : show ipv6 ospf traffic* フィールドの説明

フィールド	説明
OSPFv3 statistics	ルータで実行されるすべてのOSPFプロセスで集められたトラフィック統計情報。**showiptraffic** コマンドとの互換性を確保するため、チェックサム エラーのみが表示されます。ルート マップ名を識別します。
OSPFv3 queues statistic for process ID	Cisco IOS ソフトウェア固有のキュー統計。
Hello queue	パケット スイッチング コード（プロセス IP 入力）と受信したすべての OSPF パケットの OSPF hello プロセス間の内部 Cisco IOS キューの統計。
Router queue	OSPF hello プロセスと受信したすべての OSPF パケット（OSPF hello を除く）の OSPF ルータ間の内部 Cisco IOS キューの統計。
queue size	キューの実際のサイズ。
queue limit	キューの最大許容サイズ。
queue max size	キューの最大記録サイズ。
Interface statistics	指定 OSPFv3 プロセス ID に属するすべてのインターフェイスのインターフェイスごとのトラフィック統計情報。
OSPFv3 packets received/sent	パケット タイプ別にソートされた、インターフェイスで受信および送信された OSPFv3 パケットの数。
OSPFv3 header errors	パケットが OSPFv3 パケットのヘッダー エラーのために廃棄された場合、そのパケットがこのセクションに表示されます。廃棄されたパケットは、適切な廃棄理由に従いカウントされます。

フィールド	説明
OSPFv3 LSA errors	パケットが OSPF リンクステート アドバタイズメント（LSA）のヘッダー エラーのために廃棄された場合、そのパケットがこのセクションに表示されます。廃棄されたパケットは、適切な廃棄理由に従いカウントされます。
Summary traffic statistics for process ID	OSPFv3 プロセスで集められたサマリー トラフィック統計情報。 （注） OSPFv3 プロセス ID は、設定で OSPF プロセスに割り当てられる一意な値です。 受け取ったエラーに関する値は、グローバル OSPF 統計情報にリストされるチェックサム エラーの合計とは異なり、OSPFv3 プロセスにより検出される OSPFv3 ヘッダー エラーの合計です。

関連コマンド

コマンド	説明
clearipospftraffic	OSPFv2 トラフィック統計情報をクリアします。
clearipv6ospftraffic	OSPFv3 トラフィック統計情報をクリアします。
showipospftraffic	OSPFv2 トラフィック統計情報を表示します。

show ipv6 ospf virtual-links

Open Shortest Path First（OSPF）仮想リンクのパラメータおよび現在の状態を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **s howipv6ospfvirtual-links** コマンドを使用します。

show ipv6 ospf virtual-links

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 モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

showipv6ospfvirtual-links コマンドによって表示される情報は、OSPF ルーティング動作のデバッグに役立ちます。

例

次に、**showipv6ospfvirtual-links** コマンドの出力例を示します。

```
Device# show ipv6 ospf virtual-links
Virtual Link OSPF_VL0 to router 172.16.6.6 is up
  Interface ID 27, IPv6 address FEC0:6666:6666::
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 2, via interface ATM3/0, Cost of using 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *45 : show ipv6 ospf virtual-links* フィールドの説明

フィールド	説明
Virtual Link OSPF_VL0 to router 172.16.6.6 is up	OSPF ネイバー、およびそのネイバーとのリンクがアップまたはダウン状態であるか指定します。
Interface ID	ルータのインターフェイス ID および IPv6 アドレス。
Transit area 2	仮想リンクが形成される移行エリア。
via interface ATM3/0	仮想リンクが形成されるインターフェイス。

フィールド	説明
Cost of using 1	仮想リンクを介して OSPF ネイバーに到達するときのコスト。
Transmit Delay is 1 sec	仮想リンクの移行遅延（秒単位）。
State POINT_TO_POINT	OSPF ネイバーの状態。
Timer intervals...	リンクに設定されるさまざまなタイマー間隔。
Hello due in 0:00:06	ネイバーからの次の hello の予想時間。

次の **showipv6ospfvirtual-links** コマンドの出力例には、2 つの仮想リンクが含まれています。1 つは認証によって保護されており、もう 1 つは暗号化によって保護されています。

```
Device# show ipv6 ospf virtual-links
Virtual Link OSPFv3_VL1 to router 10.2.0.1 is up
   Interface ID 69, IPv6 address 2001:0DB8:11:0:A8BB:CCFF:FE00:6A00
   Run as demand circuit
   DoNotAge LSA allowed.
   Transit area 1, via interface Serial12/0, Cost of using 64
   NULL encryption SHA-1 auth SPI 3944, secure socket UP (errors: 0)
   Transmit Delay is 1 sec, State POINT_TO_POINT,
   Timer intervals configured, Hello 2, Dead 10, Wait 40, Retransmit 5
     Adjacency State FULL (Hello suppressed)
     Index 1/2/4, retransmission queue length 0, number of retransmission 1
     First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
     Last retransmission scan length is 1, maximum is 1
     Last retransmission scan time is 0 msec, maximum is 0 msec
Virtual Link OSPFv3_VL0 to router 10.1.0.1 is up
   Interface ID 67, IPv6 address 2001:0DB8:13:0:A8BB:CCFF:FE00:6700
   Run as demand circuit
   DoNotAge LSA allowed.
   Transit area 1, via interface Serial11/0, Cost of using 128
   MD5 authentication SPI 940, secure socket UP (errors: 0)
   Transmit Delay is 1 sec, State POINT_TO_POINT,
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
     Adjacency State FULL (Hello suppressed)
     Index 1/1/3, retransmission queue length 0, number of retransmission 1
First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
     Last retransmission scan length is 1, maximum is 1
     Last retransmission scan time is 0 msec, maximum is 0 msec
```

show ipv6 pim anycast-RP

IPv6 PIM エニーキャストの RP 動作を確認するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 pim anycast-RP** コマンドを使用します。

show ipv6 pim anycast-RP *rp-address*

構文の説明

rp-address	確認する RP アドレス。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

例

```
Device# show ipv6 pim anycast-rp 110::1:1:1

Anycast RP Peers For 110::1:1:1   Last Register/Register-Stop received
  20::1:1:1 00:00:00/00:00:00
```

関連コマンド

コマンド	説明
ipv6 pim anycast-RP	エニーキャスト グループ範囲の PIM RP のアドレスを設定します。

show ipv6 pim bsr

PIM（Protocol Independent Multicast）ブートストラップ ルータ（BSR）プロトコル処理に関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 pim bsr** コマンドを使用します。

show ipv6 pim [**vrf** *vrf-name*] **bsr** {**election**|**rp-cache**|**candidate-rp**}

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
election	BSR の状態、BSR の選択、およびブートストラップ メッセージ（BSM）関連のタイマーを表示します。
rp-cache	選択した BSR 上のユニキャスト ランデブー ポイント候補（C-RP）のアナウンスメントから学習した C-RP キャッシュを表示します。
candidate-rp	C-RP として設定されているデバイス上の C-RP の状態を表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

BSR 選択ステート マシン、C-RP アドバタイズメント ステート マシン、および C-RP キャッシュの詳細を表示するには、**showipv6pimbsr** コマンドを使用します。C-RP キャッシュの情報は、選択した BSR デバイス上にのみ表示され、C-RP ステートマシンの情報は C-RP として設定されているデバイス上にのみ表示されます。

例

次に、BSM 選択情報を表示する例を示します。

```
Device# show ipv6 pim bsr election
PIMv2 BSR information
BSR Election Information
Scope Range List: ff00::/8
This system is the Bootstrap Router (BSR)
BSR Address: 60::1:1:4
Uptime: 00:11:55, BSR Priority: 0, Hash mask length: 126
RPF: FE80::A8BB:CCFF:FE03:C400,Ethernet0/0
BS Timer: 00:00:07
This system is candidate BSR
Candidate BSR address: 60::1:1:4, priority: 0, hash mask length: 126
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *46 : show ipv6 pim bsr election* のフィールドの説明

フィールド	説明
Scope Range List	この BSR 情報を適用する範囲。
This system is the Bootstrap Router (BSR)	このデバイスが BSR であること、およびそれに関連付けられているパラメータに関する情報を表示します。
BS Timer	選択した BSR について、BS タイマーは次の BSM が発信される時間を表示します。 ドメイン内のその他すべてのデバイスについては、BS タイマーは選択した BSR の期限が切れる時間を表示します。
This system is candidate BSR	このデバイスが BSR 候補であること、およびそれに関連付けられているパラメータに関する情報を表示します。

次に、BSR でさまざまな C-RP から学習した情報を表示する例を示します。この例では、2 つの RP 候補が FF00::/8 またはデフォルトの IPv6 マルチキャストの範囲にアドバタイズメントを送信しています。

```
Device# show ipv6 pim bsr rp-cache
PIMv2 BSR C-RP Cache
BSR Candidate RP Cache
Group(s) FF00::/8, RP count 2
  RP 10::1:1:3
    Priority 192, Holdtime 150
    Uptime: 00:12:36, expires: 00:01:55
  RP 20::1:1:1
    Priority 192, Holdtime 150
    Uptime: 00:12:36, expires: 00:01:5
```

次に、C-RP に関する情報を表示する例を示します。この RP は特定の範囲の値を指定せずに設定されているため、RP は 受信した BSM を通じて学習したすべての BSR に C-RP アドバタイズメントを送信します。

```
Device# show ipv6 pim bsr candidate-rp
PIMv2 C-RP information
    Candidate RP: 10::1:1:3
      All Learnt Scoped Zones, Priority 192, Holdtime 150
      Advertisement interval 60 seconds
      Next advertisement in 00:00:33
```

次に、IPv6 C-BSR が PIM 対応であることを確認する例を示します。IPv6 C-BSR インターフェイスで PIM が無効になっているか、あるいは C-BSR または C-RP が PIM が有効になっていないインターフェイスのアドレスで設定されている場合、**show ipv6 pim bsr** コマンドを **election** キーワードを指定して使用すると、代わりにその情報を表示します。

```
Device# show ipv6 pim bsr election
```

```
PIMv2 BSR information

BSR Election Information
  Scope Range List: ff00::/8
     BSR Address: 2001:DB8:1:1:2
     Uptime: 00:02:42, BSR Priority: 34, Hash mask length: 28
     RPF: FE80::20:1:2,Ethernet1/0
     BS Timer: 00:01:27
```

show ipv6 pim df

各ランデブー ポイント（RP）の各インターフェイスの代表フォワーダ（DF）の選択状態を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6pimdf** コマンドを使用します。

show ipv6 pim [**vrf** *vrf-name*] **df** [*interface-type interface-number*] [*rp-address*]

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
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。
rp-address	（任意）RP IPv6 アドレス。

コマンド デフォルト

インターフェイスまたは RP のアドレスを指定しないと、すべての DF が表示されます。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

双方向マルチキャスト トラフィックが予想どおりにフローしない場合に各 Protocol Independent Multicast（PIM）対応のインターフェイスの DF の選択状態を表示するには、**showipv6pimdf** を使用します。

例

次に、DF の選択状態を表示する例を示します。

```
Device# show ipv6 pim df
Interface          DF State     Timer         Metrics
Ethernet0/0        Winner       4s 8ms        [120/2]
    RP :200::1
Ethernet1/0        Lose         0s 0ms        [inf/inf]
    RP :200::1
```

次に、RP に関する情報を表示する例を示します。

```
Device# show ipv6 pim df
Interface          DF State     Timer         Metrics
Ethernet0/0        None:RP LAN 0s 0ms        [inf/inf]
    RP :200::1
Ethernet1/0        Winner       7s 600ms      [0/0]
    RP :200::1
```

```
Ethernet2/0        Winner       9s 8ms        [0/0]
    RP :200::1
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *47 : show ipv6 pim df* フィールドの説明

フィールド	説明
Interface	PIM を実行するように設定されているインターフェイスのタイプと番号。
DF State	インターフェイスでの DF の選択状態。状態は次のいずれかになります。 • Offer • Winner • Backoff • Lose • None:RP LAN None:RP LAN 状態は、RP がこの LAN に直接接続されているために、この LAN 上では DF の選択が実行されないことを示します。
Timer	DF 選択タイマー。
Metrics	DF によってアナウンスされた RP へのルーティング メトリック。
RP	RP の IPv6 アドレス。

関連コマンド

コマンド	説明
debugipv6pimdf-election	PIM 双方向 DF 選択メッセージ処理のデバッグ メッセージを表示します。
ipv6pimrp-address	特定のグループ範囲の PIM RP のアドレスを設定します。
showipv6pimdfwinner	各 RP の各インターフェイスの DF 選択ウィナーを表示します。

show ipv6 pim group-map

IPv6 Protocol Independent Multicast（PIM）のグループ マッピング テーブルを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6pimgroup-map** コマンドを使用します。

{**show ipv6 pim** [**vrf** *vrf-name*] **group-map** [{*group-namegroup-address*}][{*group-rangegroup-mask*}] [**info-source** {**bsr**|**default**|**embedded-rp**|**static**}]}

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
group-name | *group-address*	（任意）マルチキャスト グループの IPv6 アドレスまたは名前。
group-range | *group-mask*	（任意）グループの範囲のリスト。同じプレフィックス長またはマスク長のグループの範囲が含まれています。
info-source	（任意）ブートストラップ ルータ（BSR）やスタティック設定など、特定の送信元から学習したすべてのマッピングを表示します。
bsr	BSR を通じて学習した範囲を表示します。
default	デフォルトで有効になった範囲を表示します。
embedded-rp	組み込みランデブー ポイント（RP）を通じて学習したグループの範囲を表示します。
static	スタティック設定によって有効になっている範囲を表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

BSR やスタティック設定など、指定した情報源がインストールしたすべてのグループ マッピングを検索するには、**showipv6pimgroup-map** コマンドを使用します。

また、このコマンドは、指定した IPv6 グループ アドレスのルータがグループ アドレスを使用しているグループ マッピングを検索したり、グループの範囲とマスク長を指定して正確なグループ マッピング エントリを検索するためにも使用できます。

例

次は、**showipv6pimgroup-map** コマンドの出力例です。

```
Device# show ipv6 pim group-map
FF33::/32*
      SSM
      Info source:Static
      Uptime:00:08:32, Groups:0
  FF34::/32*
      SSM
      Info source:Static
      Uptime:00:09:42, Groups:0
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *48 : show ipv6 pim group-map* のフィールドの説明

フィールド	説明
RP	プロトコルがスパース モードまたは bidir の場合の RP ルータのアドレス。
Protocol	使用するプロトコル：スパース モード（SM）、送信元特定マルチキャスト（SSM）、リンクローカル（LL）、または NOROUTE（NO）。 LL は、リンクローカル範囲の IPv6 アドレス範囲（ff[0-f]2::/16）に使用されます。LL は個別のプロトコル タイプとして扱われます。これは、このような宛て先アドレスで受信したパケットは転送されず、ルータがそれらを受信して処理する必要があるためです。 NOROUTE または NO は予約された、ノードローカル範囲の IPv6 アドレス範囲（ff[0-f][0-1]::/16）に使用されます。これらのアドレスはルーティングができないため、ルータはそれらを処理する必要がありません。
Groups	この範囲のトポロジ テーブル内に存在するグループの数。
Info source	特定の送信元から学習したマッピング。この場合はスタティック設定。
Uptime	表示されたグループ マッピングの稼働時間。

次に、PIM の group-to-RP キャッシュまたは mode-mapping キャッシュ に存在する BSR から学習したグループマッピングを表示する例を示します。次に、グループ マッピングを学習した BSR のアドレスと、関連付けられているタイムアウトを表示する例を示します。

```
Router# show ipv6 pim group-map info-source bsr
FF00::/8*
    SM, RP: 20::1:1:1
    RPF: Et1/0,FE80::A8BB:CCFF:FE03:C202
```

```
    Info source: BSR From: 60::1:1:4(00:01:42), Priority: 192
    Uptime: 00:19:51, Groups: 0
FF00::/8*
    SM, RP: 10::1:1:3
    RPF: Et0/0,FE80::A8BB:CCFF:FE03:C102
    Info source: BSR From: 60::1:1:4(00:01:42), Priority: 192
    Uptime: 00:19:51, Groups: 0
```

show ipv6 pim interface

Protocol Independent Multicast（PIM）に設定されているインターフェイスに関する情報を表示するには、特権 EXEC モードで **showipv6piminterface** コマンドを使用します。

show ipv6 pim [**vrf** *vrf-name*] **interface [state-on] [state-off]** [*type number*]

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
state-on	（任意）PIM がイネーブルになっているインターフェイスを表示します。
state-off	（任意）PIM がディセーブルになっているインターフェイスを表示します。
type number	（任意）インターフェイス タイプおよび番号

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

PIMがインターフェイスで有効になっているかどうか、およびネイバーの数とインターフェイス上の代表ルータ（DR）を確認するには、**showipv6piminterface** コマンドを使用します。

例

次に、**state-on** キーワードを使用した **showipv6piminterface** コマンドの出力例を示します。

```
Device# show ipv6 pim interface state-on
Interface          PIM  Nbr   Hello  DR
                        Count Intvl  Prior
Ethernet0          on   0     30     1
    Address:FE80::208:20FF:FE08:D7FF
    DR     :this system
POS1/0             on   0     30     1
    Address:FE80::208:20FF:FE08:D554
    DR     :this system
POS4/0             on   1     30   1
    Address:FE80::208:20FF:FE08:D554
    DR     :FE80::250:E2FF:FE8B:4C80
POS4/1             on   0     30   1
    Address:FE80::208:20FF:FE08:D554
    DR     :this system
Loopback0          on   0     30     1
    Address:FE80::208:20FF:FE08:D554
    DR     :this system
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *49 : show ipv6 pim interface* フィールドの説明

フィールド	説明
Interface	PIM を実行するように設定されているインターフェイスのタイプと番号。
PIM	インターフェイス上で PIM が有効になっているかどうか。
Nbr Count	このインターフェイスを通じて検出された PIM ネイバーの数。
Hello Intvl	PIM の hello メッセージの頻度（秒単位）。
DR	ネットワーク上の代表ルータ（DR）の IP アドレス。
Address	ネクストホップ ルータのインターフェイス IP アドレス。

次に、パッシブ インターフェイス情報を表示するように変更した **showipv6piminterface** コマンドの出力例を示します。

```
Device(config)# show ipv6 pim interface gigabitethernet0/0/0

    Interface              PIM   Nbr   Hello  DR  BFD
                           Count Intvl Prior

    GigabitEthernet0/0/0   on/P  0     30     1   On
       Address: FE80::A8BB:CCFF:FE00:9100
       DR     : this system
```

次の表で、この出力に表示される重要な変更事項を説明します。

表 *50 : show ipv6 pim interface* フィールドの説明

フィールド	説明
PIM	インターフェイス上で PIM が有効になっているかどうか。PIM パッシブ モードを使用している場合、出力に「P」が表示されます。

関連コマンド

コマンド	説明
showipv6pimneighbor	Cisco IOS ソフトウェアで検出された PIM ネイバーを表示します。

show ipv6 pim join-prune statistic

各インターフェイスについて最近集約された 1,000 個、10,000 個、および 50,000 個のパケットの平均 join-prune 集約を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6pimjoin-prunestatistic** コマンドを使用します。

show ipv6 pim [**vrf** *vrf-name*] **join-prune statistic** [*interface-type*]

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
interface-type	（任意）インターフェイス タイプ。詳細については、疑問符（**?**）オンラインヘルプ機能を使用してください。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

Protocol Independent Multicast（PIM）が複数の join と prune を同時に送信する場合は、それらを単一のパケットに集約します。**showipv6pimjoin-prunestatistic** コマンドは、それまでの 1,000 個の PIM join-prune パケット、それまでの 10,000 個の PIM join-prune パケット、およびそれまでの 50,000 個の PIM join-prune パケットにわたって単一のパケットに集約した join と prune の平均数を表示します。

例

次に、イーサネット インターフェイス 0/0/0 での join/prune 集約の例を示します。

```
Device# show ipv6 pim join-prune statistic Ethernet0/0/0
PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface             Transmitted             Received
Ethernet0/0/0      0    / 0    / 0         1    / 0    / 0
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *51 : show ipv6 pim join-prune statistics* フィールドの説明

フィールド	説明
Interface	指定したパケットを送信するインターフェイス、または指定したパケットを受信するインターフェイス。

フィールド	説明
Transmitted	このインターフェイスで送信したパケットの数。
Received	このインターフェイスで受信したパケットの数。

show ipv6 pim limit

Protocol Independent Multicast（PIM）インターフェイスの制限を表示するには、特権 EXEC モードで **showipv6pimlimit** コマンドを使用します。

show ipv6 pim [**vrf** *vrf-name*] **limit** [*interface*]

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
interface	（任意）制限情報が提供される特定のインターフェイス。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

showipv6pimlimit コマンドはインターフェイス統計の制限を確認します。オプションの引数 *interface* を有効にすると、指定したインターフェイスの情報のみが表示されます。

例

次に、PIM インターフェイスの制限情報を表示する例を示します。

```
Device# show ipv6 pim limit
```

関連コマンド

コマンド	説明
ipv6multicastlimit	IPv6 のインターフェイス単位の mroute ステート リミッタを設定します。
ipv6multicastlimitcost	IPv6 のインターフェイスごとの mroute ステート リミッタと一致する mroute にコストを適用します。

show ipv6 pim neighbor

Cisco ソフトウェアが検出した Protocol Independent Multicast（PIM）ネイバーを表示するには、特権 EXEC モードで **show ipv6 pim neighbor** コマンドを使用します。

show ipv6 pim ［**vrf** *vrf-name* ］**neighbor**［**detail**］［*interface-type interface-number* ｜ **count**］

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
detail	（任意）ルーティング可能なアドレス hello オプションを通じて学習したネイバーがある場合は、そのネイバーの追加アドレスを表示します。
interface-type interface-number	（任意）インターフェイス タイプおよび番号
count	（任意）各インターフェイスのネイバー カウントを表示します。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

Show ipv6 pim neighbor コマンドは、PIM 用に設定されている LAN 上のルータを表示します。

例

次に、**show ipv6 pim neighbor** コマンドで detail キーワードを指定して、ルーティング可能アドレスの hello オプションを通して学習されたネイバーの追加アドレスを識別する場合の出力例を示します。

```
Device# show ipv6 pim neighbor detail

Neighbor Address(es)       Interface          Uptime    Expires DR pri Bidir

FE80::A8BB:CCFF:FE00:401   Ethernet0/0        01:34:16  00:01:16 1      B
60::1:1:3

FE80::A8BB:CCFF:FE00:501   Ethernet0/0        01:34:15  00:01:18 1      B
60::1:1:4
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *52 : show ipv6 pim neighbor* フィールドの説明

フィールド	説明
Neighbor addresses	PIM ネイバーの IPv6 アドレス。
Interface	ネイバーに到達可能なインターフェイスのタイプと番号
Uptime	PIM ネイバー テーブル内にエントリが存在する時間（時間、分、秒）。
Expires	IPv6 マルチキャスト ルーティング テーブルからエントリが削除されるまでの期間（時間、分、秒）。
DR	このネイバーが LAN の代表ルータ（DR）であることを示します。
pri	このネイバーが使用する DR の優先順位。
Bidir	ネイバーは双方向モードで PIM に対応します。

関連コマンド

コマンド	説明
show ipv6 pim interfaces	PIM に対して設定されたインターフェイスに関する情報を表示します。

show ipv6 pim range-list

IPv6 マルチキャストの範囲のリストに関する情報を表示するには、特権 EXEC モードで **showipv6pimrange-list** コマンドを使用します。

show ipv6 pim [**vrf** *vrf-name*] **range-list [config]** [{*rp-addressrp-name*}]

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
config	（任意）クライアント。ルータで設定されている範囲のリストを表示します。
rp-address | *rp-name*	（任意）Protocol Independent Multicast（PIM）ランデブー ポイント（RP）のアドレス。

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

showipv6pimrange-list コマンドは、クライアントごとおよびモードごとに IPv6 マルチキャストの範囲のリストを表示します。クライアントは、指定した範囲のリストの学習元のエンティティです。クライアントはconfig、モードは送信元特定マルチキャスト（SSM）モードまたはスパース モードである場合があります。

例

次は、**showipv6pimrange-list** コマンドの出力例です。

```
Device# show ipv6 pim range-list
config SSM Exp:never Learnt from :::
 FF33::/32 Up:00:26:33
 FF34::/32 Up:00:26:33
 FF35::/32 Up:00:26:33
 FF36::/32 Up:00:26:33
 FF37::/32 Up:00:26:33
 FF38::/32 Up:00:26:33
 FF39::/32 Up:00:26:33
 FF3A::/32 Up:00:26:33
 FF3B::/32 Up:00:26:33
 FF3C::/32 Up:00:26:33
 FF3D::/32 Up:00:26:33
 FF3E::/32 Up:00:26:33
 FF3F::/32 Up:00:26:33
config SM RP:40::1:1:1 Exp:never Learnt from :::
 FF13::/64 Up:00:03:50
```

```
config SM RP:40::1:1:3 Exp:never Learnt from :::
 FF09::/64 Up:00:03:50
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *53 : show ipv6 pim range-list* フィールドの説明

フィールド	説明
config	Configがクライアントです。
SSM	使用中のプロトコル。
FF33::/32	グループの範囲。
Up:	稼働時間。

show ipv6 pim topology

特定のグループまたはすべてのグループの Protocol Independent Multicast（PIM）トポロジ テーブルの情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6pimtopology** コマンドを使用します。

show ipv6 pim [**vrf** *vrf-name*] **topology** [{*group-name*|*group-address* [{*source-addresssource-name*}]|**link-local**}]**route-count [detail]**

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
group-name | *group-address*	（任意）マルチキャスト グループの IPv6 アドレスまたは名前。
source-address | *source-name*	（任意）送信元の IPv6 アドレスまたは名前。
link-local	（任意）リンク ローカル グループを表示します。
route-count	（任意）PIM トポロジ テーブル内のルートの数を表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、指定したグループ（(*, G)、(S, G)、(S, G) ランデブー ポイント ツリー (RPT)）を PIM トポロジ テーブルに内部的に格納したとおりに表示します。PIM トポロジ テーブルには、指定したグループのさまざまなエントリが含まれており、それぞれが固有のインターフェイス リストを備えている場合があります。結果の転送状態が Multicast Routing Information Base（MRIB）テーブルに保持されます。このテーブルは、データ パケットを承認するインターフェイスと、データ パケットを指定した (S, G) エントリに転送するインターフェイスが示されています。また、転送時にはマルチキャスト転送情報ベース（MFIB）テーブルを使用して、パケットごとの転送アクションを決定します。

route-count キーワードは、リンクローカル エントリを含めて、すべてのエントリのカウントを表示します。

PIM は、これらのエントリの内容を MRIB を通じてやり取りします。MRIB は、PIM などのマルチキャスト ルーティング プロトコルと、マルチキャスト リスナー検出（MLD）などのロー

カル メンバーシップ プロトコルとの通信における仲介手段であり、システムのマルチキャスト転送エンジンです。

たとえば、MLD レポートまたは PIM (*, G) join メッセージの受信時にインターフェイスが PIM トポロジ テーブルの (*, G) エントリに追加されるとします。同様に、S と G の MLD INCLUDE レポートまたは PIM (S, G) join メッセージの受信時にインターフェイスが (S, G) エントリに追加されるとします。次に、PIM が (S, G) エントリを immediate olist（(S, G) から）および inherited olist（(*, G) から）で MRIB にインストールします。そのため、指定したエントリ (S, G) の正しいフォワーディング ステートは、PIM トポロジ テーブルではなく、MRIB または MFIB でのみ確認できます。

例

次は、**showipv6pimtopology** コマンドの出力例です。

```
Device# show ipv6 pim topology
IP PIM Multicast Topology Table
Entry state:(*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags:KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR - Sending Registers, E - MSDP External,
    DCC - Don't Check Connected
Interface state:Name, Uptime, Fwd, Info
Interface flags:LI - Local Interest, LD - Local Dissinterest,
II - Internal Interest, ID - Internal Dissinterest,
LH - Last Hop, AS - Assert, AB - Admin Boundary
(*,FF05::1)
SM UP:02:26:56 JP:Join(now) Flags:LH
RP:40::1:1:2
RPF:Ethernet1/1,FE81::1
  Ethernet0/1          02:26:56  fwd LI LH
(50::1:1:200,FF05::1)
SM UP:00:00:07 JP:Null(never) Flags:
RPF:Ethernet1/1,FE80::30:1:4
  Ethernet1/1          00:00:07  off LI
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *54 : show ipv6 pim topology* フィールドの説明

フィールド	説明
Entry flags: KAT	送信元が起動している間の 2 つの間隔を追跡するには、送信元に関連付けられているキープアライブ タイマー（KAT）を使用します。送信元が最初にアクティブに時点で、ファーストホップ ルータがキープアライブ タイマーを 3 分 30 秒に設定します。その間は送信元が起動しているかどうかを確認するためのプローブは行いません。このタイマーが満了すると、ルータはプローブ間隔を開始し、タイマーを 65 秒にリセットします。その間、ルータは送信元が起動していると想定し、実際にそうであるかどうかを判断するためのプローブを開始します。ルータが送信元は起動していると判断すると、ルータはプローブ間隔を終了し、キープアライブ タイマーを 3 分 30 秒にリセットします。送信元が起動していない場合は、プローブ間隔の終了時点でエントリが削除されます。

フィールド	説明
AA, PA	ルータが特定の送信元のプローブ間隔に入っているときに、推定アライブ（AA）フラグとプローブ アライブ（PA）フラグが設定されます。
RR	RP が送信元の代表ルータ（DR）から登録を受信し、送信元の状態を ルート プロセッサ上で alive に保っている限り、登録受信済み（RR）フラグがルート プロセッサ（RP）の (S, G) エントリ上に設定されます。
SR	DR が RP に登録を送信している限り、送信側登録（SR）フラグが DR 上の (S, G) エントリ上に設定されます。

関連コマンド

コマンド	説明
showipv6mribclient	MRIB のクライアントに関する情報を表示します。
showipv6mribroute	MRIB ルート情報を表示します。

show ipv6 pim traffic

Protocol Independent Multicast（PIM）トラフィック カウンタを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6pimtraffic** コマンドを使用します。

show ipv6 pim [**vrf** *vrf-name*] **traffic**

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

予想した数の PIM プロトコル メッセージを送受信したかどうかを確認するには、**showipv6pimtraffic** コマンドを使用します。

例

次に、送受信された PIM プロトコル メッセージの数を表示する例を示します。

```
Device# show ipv6 pim traffic

PIM Traffic Counters
Elapsed time since counters cleared:00:05:29
                              Received     Sent
Valid PIM Packets               22          22
Hello                           22          22
Join-Prune                      0           0
Register                        0           0
Register Stop                   0           0
Assert                          0           0
Bidir DF Election               0           0
Errors:
Malformed Packets                           0
Bad Checksums                               0
Send Errors                                 0
Packet Sent on Loopback Errors              0
Packets Received on PIM-disabled Interface  0
Packets Received with Unknown PIM Version   0
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *55 : show ipv6 pim traffic* フィールドの説明

フィールド	説明
Elapsed time since counters cleared	カウンタをクリアしてからの時間を示します（時間、分、秒単位）。
Valid PIM Packets	送受信した有効な PIM パケットの数。
Hello	送受信した有効な hello メッセージの数。
Join-Prune	送受信した join アナウンスメントと prune アナウンスメントの数。
Register	送受信した PIM register メッセージの数。
Register Stop	送受信した PIM register stop メッセージの数。
Assert	送受信したアサートの数。

show ipv6 pim tunnel

インターフェイス上の Protocol Independent Multicast（PIM）登録カプセル化トンネルおよびカプセル化解除トンネルを表示するには、特権 EXEC モードで **showipv6pimtunnel** コマンドを使用します。

show ipv6 pim [**vrf** *vrf-name*] **tunnel** [*interface-type interface-number*]

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
interface-type interface-number	（任意）トンネル インターフェイスのタイプおよび番号

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

オプションの *interface* キーワードを指定せずに **showipv6pimtunnel** コマンドを使用すると、PIM 登録カプセル化トンネル インターフェイスとカプセル化解除トンネル インターフェイスに関する情報が表示されます。

PIM カプセル化トンネルは、レジスタ トンネルです。カプセル化トンネルは、各ルータ上のすべての既知のランデブー ポイント（RP）に対して作成されます。PIM カプセル化解除トンネルは、レジスタ カプセル化解除トンネルです。カプセル化解除トンネルは、RP アドレスとして設定されているアドレスの RP に作成されます。

例

次に、RP での **showipv6pimtunnel** コマンドの出力例を示します。

```
Device# show ipv6 pim tunnel
Tunnel0*
 Type  :PIM Encap
 RP    :100::1
 Source:100::1
Tunnel0*
 Type  :PIM Decap
 RP    :100::1
 Source: -
```

次に、RP 以外での **showipv6pimtunnel** コマンドの出力例を示します。

```
Device# show ipv6 pim tunnel
Tunnel0*
 Type  :PIM Encap
 RP    :100::1
 Source:2001::1:1:1
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *56 : show ipv6 pim tunnel* フィールドの説明

フィールド	説明
Tunnel0*	トンネルの名前。
Type	トンネルのタイプ。PIM のカプセル化または PIM カプセル化の解除ができます。
source	RP にカプセル化登録を送信しているルータの送信元アドレス。

show ipv6 policy

IPv6 ポリシーベースのルーティング（PBR）設定を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6policy** コマンドを使用します。

show ipv6 policy

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 モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

IPv4 の場合と同じように、ルート マップ上で IPv6 ポリシーの一致がカウントされます。そのため、IPv6 ポリシーの一致も **showroute-map** コマンドで表示できます。

例

次に、PBR 設定を表示する例を示します。

```
Device# show ipv6 policy

Interface                Routemap
Ethernet0/0              src-1
```

次の表で、この出力に表示される重要なフィールドを説明します。

フィールド	説明
Interface	Protocol-Independent Multicast（PIM）を実行するように設定されているインターフェイスのタイプと番号。
Routemap	IPv6 ポリシーの一致がカウントされたルート マップの名前。

関連コマンド

コマンド	説明
showroute-map	設定されたすべてのルート マップ、または指定した 1 つのルート マップだけを表示します。

show ipv6 prefix-list

IPv6 プレフィックス リストまたは IPv6 プレフィックスのエントリに関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6prefix-list** コマンドを使用します。

show ipv6 prefix-list [{**detail**|**summary**}] [*list-name*]
show ipv6 prefix-list *list-name ipv6-prefix/prefix-length* [{**longer**|**first-match**}]
show ipv6 prefix-list *list-name* **seq** *seq-num*

構文の説明

detail| **summary**	（任意）すべてのIPv6プレフィックスリストに関する詳細情報または要約情報を表示します。
list-name	（任意）特定の IPv6 プレフィックス リストの名前。
ipv6-prefix	指定した IPv6 ネットワークのすべてのプレフィックス リスト エントリ。 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。
longer	（任意）指定した*ipv6-prefix* / *prefix-length*valuesよりも詳細に *IPv6* プレフィックス リストのすべてのエントリを表示します。
first-match	（任意）指定した *ipv6-prefix* / *prefix-length* の値と一致する IPv6 プレフィックス リストのエントリを表示します。
seq *seq-num*	IPv6 プレフィックス リスト エントリのシーケンス番号。

コマンド デフォルト

すべての IPv6 プレフィックス リストに関する情報を表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

showipv6prefix-list コマンドの出力は、IPv6 に固有である点を除き、**showipprefix-list** コマンドの出力と似ています。

例

次に、**detail** を使用した **showipv6prefix-list** コマンドの出力例を示します。

```
Device# show ipv6 prefix-list detail
Prefix-list with the last deletion/insertion: bgp-in
ipv6 prefix-list 6to4:
   count: 1, range entries: 0, sequences: 5 - 5, refcount: 2
   seq 5 permit 2002::/16 (hit count: 313, refcount: 1)
ipv6 prefix-list aggregate:
   count: 2, range entries: 2, sequences: 5 - 10, refcount: 30
   seq 5 deny 3FFE:C00::/24 ge 25 (hit count: 568, refcount: 1)
   seq 10 permit ::/0 le 48 (hit count: 31310, refcount: 1)
ipv6 prefix-list bgp-in:
   count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
   seq 5 deny 5F00::/8 le 128 (hit count: 0, refcount: 1)
   seq 10 deny ::/0 (hit count: 0, refcount: 1)
   seq 15 deny ::/1 (hit count: 0, refcount: 1)
   seq 20 deny ::/2 (hit count: 0, refcount: 1)
   seq 25 deny ::/3 ge 4 (hit count: 0, refcount: 1)
   seq 30 permit ::/0 le 128 (hit count: 240664, refcount: 0)
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *57 : show ipv6 prefix-list* フィールドの説明

フィールド	説明
Prefix list with the latest deletion/insertion:	最後に変更されたプレフィックス リスト。
count	リスト内のエントリの数。
range entries	範囲が一致するエントリの数。
sequences	プレフィックス エントリのシーケンス番号。
refcount	このプレフィックスリストを現在使用しているオブジェクトの数。
seq	リスト内のエントリ番号。
permit, deny	ステータスの付与。
hit count	プレフィックス エントリの一致の数。

次に、**summary** を使用した **showipv6prefix-list** コマンドの出力例を示します。

```
Device# show ipv6 prefix-list summary
Prefix-list with the last deletion/insertion: bgp-in
ipv6 prefix-list 6to4:
   count: 1, range entries: 0, sequences: 5 - 5, refcount: 2
ipv6 prefix-list aggregate:
   count: 2, range entries: 2, sequences: 5 - 10, refcount: 30
ipv6 prefix-list bgp-in:
   count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
```

関連コマンド

コマンド	説明
clearipv6prefix-list	プレフィックス リスト エントリのヒット カウントをリセットします。
distribute-listin	アップデートで受信するネットワークをフィルタリングします。
distribute-listout	ネットワークが更新時にアドバタイズされないようにします。
ipv6prefix-list	IPv6 プレフィックス リストのエントリを作成します。
ipv6prefix-list説明	IPv6 プレフィックス リストのテキスト説明を追加します。
matchipv6address	プレフィクス リストによって許可されるプレフィックスを持つ IPv6 ルートを配信します。
neighborprefix-list	プレフィックス リストで指定された BGP ネイバー情報を配布します。
remark(prefix-list)	プレフィックス リストのエントリにコメントを追加します。

show ipv6 protocols

アクティブな IPv6 ルーティング プロトコル プロセスのパラメータおよび現在の状態を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6protocols** コマンドを使用します。

show ipv6 protocols [summary]

構文の説明

summary	（任意）設定されているルーティング プロトコル プロセスの名前を表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

showipv6protocols コマンドによって表示される情報は、ルーティング動作のデバッグに役立ちます。

例

次に、Intermediate System-to-Intermediate System（IS-IS）ルーティング プロトコル情報を表示する **showipv6protocols** コマンドの出力例を示します。

```
Device# show ipv6 protocols

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "isis"
  Interfaces:
    Ethernet0/0/3
    Ethernet0/0/1
    Serial1/0/1
    Loopback1 (Passive)
    Loopback2 (Passive)
    Loopback3 (Passive)
    Loopback4 (Passive)
    Loopback5 (Passive)
  Redistribution:
    Redistributing protocol static at level 1
  Inter-area redistribution
    Redistributing L1 into L2 using prefix-list word
  Address Summarization:
    L2: 33::/16  advertised with metric 0
    L2: 44::/16  advertised with metric 20
    L2: 66::/16  advertised with metric 10
    L2: 77::/16  advertised with metric 10
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *58 : IS-IS* プロトコルの場合の *show ipv6 protocols* フィールドの説明

フィールド	説明
IPv6 Routing Protocol is	使用した IPv6 ルーティング プロトコルを指定します。
Interfaces	IPv6 IS-IS が設定されているインターフェイスを指定します。
Redistribution	再配布されているプロトコルのリストを表示します。
Inter-area redistribution	他のレベルに再配布されている IS-IS レベルのリストを表示します。
using prefix-list	エリア間の再配布で使用されたプレフィックス リストを指定します。
[Address Summarization]	すべてのサマリー プレフィックスのリストを表示します。サマリー プレフィックスがアドバタイズされている場合、後ろに「advertised with metric *x*」が表示されます。

次に、自律システム 30 の Border Gateway Protocol（BGP）情報を表示する **showipv6protocols** コマンドの出力例を示します。

```
Device# show ipv6 protocols

IPv6 Routing Protocol is "bgp 30"
  IGP synchronization is disabled
  Redistribution:
    Redistributing protocol connected
  Neighbor(s):
    Address                    FiltIn FiltOut Weight RoutemapIn RoutemapOut
    2001:DB8:0:ABCD::1            5       7    200
    2001:DB8:0:ABCD::2                                rmap-in    rmap-out
    2001:DB8:0:ABCD::3                                rmap-in    rmap-out
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *59 : BGP* プロトコルの場合の *show ipv6 protocols* フィールドの説明

フィールド	説明
IPv6 Routing Protocol is	使用したIPv6ルーティングプロトコルを指定します。
Redistribution	再配布されているプロトコルのリストを表示します。
Address	ネイバー IPv6 アドレス。
FiltIn	入力に適用された AS パス フィルタ。
FiltOut	出力に適用する AS パス フィルタ。
Weight	BGP ベスト パスの選択に使用するネイバー重み値。
RoutemapIn	入力に適用されたネイバー ルート マップ。

フィールド	説明
RoutemapOut	出力に適用されたネイバー ルート マップ。

次に、**showipv6protocolssummary** コマンドの出力例を示します。

```
Device# show ipv6 protocols summary

Index Process Name
0     connected
1     static
2     rip myrip
3     bgp 30
```

次に、ベクトル メトリックおよび EIGRP IPv6 NSF を含む EIGRP 情報を表示する **showipv6protocols** コマンドの出力例を示します。

```
Device# show ipv6 protocols

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "bgp 1"
  IGP synchronization is disabled
  Redistribution:
    None
IPv6 Routing Protocol is "bgp multicast"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "eigrp 1"
EIGRP-IPv6 VR(name) Address-Family Protocol for AS(1)
  Metric weight K1=1, K2=0, K3=1, K4=0, K5=0 K6=0
  Metric rib-scale 128
  Metric version 64bit
  NSF-aware route hold timer is 260
  EIGRP NSF enabled
     NSF signal timer is 15s
     NSF converge timer is 65s
  Router-ID: 10.1.2.2
  Topology : 0 (base)
    Active Timer: 3 min
    Distance: internal 90 external 170
    Maximum path: 16
    Maximum hopcount 100
    Maximum metric variance 1
    Total Prefix Count: 0
    Total Redist Count: 0

  Interfaces:
  Redistribution:
    None
```

次に、Open Shortest Path First（OSPF）ドメイン内に再配布を設定した後の IPv6 プロトコル情報を表示する例を示します。

```
Device# redistribute ospf 1 match internal
Device(config-rtr)# end
Device# show ipv6 protocols

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip 1"
```

```
  Interfaces:
    Ethernet0/1
    Loopback9
  Redistribution:
    Redistributing protocol ospf 1 (internal)
IPv6 Routing Protocol is "ospf 1"
  Interfaces (Area 0):
    Ethernet0/0
  Redistribution:
    None
```

show ipv6 rip

現在の IPv6 Routing Information Protocol（RIP）プロセスに関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6rip** コマンドを使用します。

show ipv6 rip ［*name*］［**vrf** *vrf-name*］［{**database** |**next-hops**}］

show ipv6 rip ［*name*］［{**database** |**next-hops**}］

構文の説明

name	（任意）RIP プロセスの名前。名前を入力しないと、設定されているすべての RIP プロセスの詳細が表示されます。
vrf *vrf-name*	（任意）指定した Virtual Routing and Forwarding（VRF）インスタンスに関する情報を表示します。
database	（任意）指定した RIP IPv6 ルーティング テーブル内のエントリに関する情報を表示します。
next-hops	（任意）指定した RIP IPv6 プロセスのネクスト ホップ アドレスに関する情報を表示します。RIP プロセス名を指定しないと、すべての RIP IPv6 プロセスのネクストホップ アドレスが表示されます。

コマンド デフォルト

現在のすべての IPv6 RIP プロセスに関する情報を表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

例

次に、**showipv6rip** コマンドの出力例を示します。

```
Device# show ipv6 rip

RIP process "one", port 521, multicast-group FF02::9, pid 55
     Administrative distance is 25. Maximum paths is 4
     Updates every 30 seconds, expire after 180
     Holddown lasts 0 seconds, garbage collect after 120
     Split horizon is on; poison reverse is off
     Default routes are not generated
     Periodic updates 8883, trigger updates 2
  Interfaces:
    Ethernet2
  Redistribution:
RIP process "two", port 521, multicast-group FF02::9, pid 61
     Administrative distance is 120. Maximum paths is 4
```

```
    Updates every 30 seconds, expire after 180
    Holddown lasts 0 seconds, garbage collect after 120
    Split horizon is on; poison reverse is off
    Default routes are not generated
    Periodic updates 8883, trigger updates 0
  Interfaces:
    None
  Redistribution:
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *60 : show ipv6 rip* フィールドの説明

フィールド	説明
RIP process	RIP プロセスの名前。
port	RIP プロセスが使用しているポート。
multicast-group	RIP がメンバーとなっている IPv6 マルチキャスト グループ。
pid	RIP プロセスに割り当てられているプロセス識別番号（pid）。
Administrative distance	ルーティング情報の送信元の優先度のランク付けに使用されます。接続されているルータにアドミニストレーティブ ディスタンス 1 があり、より大きなアドミニストレーティブ ディスタンス値を持つプロトコルによって学習されたルータよりも優先されます。
Updates	更新タイマーの値（秒単位）。
expire	更新の期限が切れる間隔（秒単位）。
Holddown	ホールドダウン タイマーの値（秒単位）。
garbage collect	ガーベッジコレクション タイマーの値（秒単位）。
Split horizon	スプリット ホライズン状態は on か off のいずれかです。
poison reverse	ポイズン リバース状態は on か off のいずれかです。
Default routes	RIP へのデフォルト ルートの起点。デフォルト ルートを生成するか、しないかです。
Periodic updates	更新タイマーに送信した RIP アップデート パケットの数。
trigger updates	トリガーされた更新として送信された RIP アップデート パケットの数。

次に、**showipv6ripdatabase** コマンドの出力例を示します。

```
Device# show ipv6 rip one database

RIP process "one", local RIB
 2001:72D:1000::/64, metric 2
     Ethernet2/2001:DB8:0:ABCD::1, expires in 168 secs
```

```
 2001:72D:2000::/64, metric 2, installed
     Ethernet2/2001:DB8:0:ABCD::1, expires in 168 secs
 2001:72D:3000::/64, metric 2, installed
     Ethernet2/2001:DB8:0:ABCD::1, expires in 168 secs
     Ethernet1/2001:DB8::1, expires in 120 secs
 2001:72D:4000::/64, metric 16, expired, [advertise 119/hold 0]
     Ethernet2/2001:DB8:0:ABCD::1
 3004::/64, metric 2 tag 2A, installed
     Ethernet2/2001:DB8:0:ABCD::1, expires in 168 secs
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *61 : show ipv6 rip database* フィールドの説明

フィールド	説明
RIP process	RIP プロセスの名前。
2001:72D:1000::/64	IPv6 ルート プレフィックス。
metric	ルートのメトリック。
installed	ルートが IPv6 ルーティング テーブルにインストールされています。
Ethernet2/2001:DB8:0:ABCD::1	IPv6 ルートが学習されたインターフェイスおよび LL ネクストホップ。
expires in	ルートの期限が切れるまでの間隔（秒単位）。
advertise	期限切れのルートについて、そのルートが期限切れとアドバタイズされる時間の値（秒単位）。
hold	ホールドダウン タイマーの値（秒単位）。
tag	ルート タグ。

次に、**showipv6ripnext-hops** コマンドの出力例を示します。

```
Device# show ipv6 rip one next-hops

RIP process "one", Next Hops
  FE80::210:7BFF:FEC2:ACCF/Ethernet4/2 [1 routes]
  FE80::210:7BFF:FEC2:B286/Ethernet4/2 [2 routes]
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *62 : show ipv6 rip next-hops* フィールドの説明

フィールド	説明
RIP process	RIP プロセスの名前。

フィールド	説明
2001:DB8:0:1::1/Ethernet4/2	ネクストホップアドレスおよびそれを学習したインターフェイス。ネクスト ホップは、ルートを学習した IPv6 RIP ネイバーのアドレスか、または IPv6 RIP アドバタイズメントで受信した明示的なネクストホップのいずれかです。 （注） IPv6 RIP ネイバーが明示的なネクスト ホップを使用してそのネイバーのすべてのルータをアドバタイズすることがあります。この場合、ネイバーのアドレスはネクストホップの表示に表示されません。
[1 routes]	指定したネクスト ホップを使用している IPv6 RIP ルーティング テーブル内のルートの数。

次は、**showipv6ripvrf** コマンドの出力例です。

```
Device# show ipv6 rip vrf red

     RIP VRF "red", port 521, multicast-group 2001:DB8::/32, pid 295
     Administrative distance is 120. Maximum paths is 16
     Updates every 30 seconds, expire after 180
     Holddown lasts 0 seconds, garbage collect after 120
     Split horizon is on; poison reverse is off
     Default routes are not generated
     Periodic updates 99, trigger updates 3
     Full Advertisement 0, Delayed Events 0
  Interfaces:
    Ethernet0/1
    Loopback2
  Redistribution:
    None
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *63 : show ipv6 rip vrf* フィールドの説明

フィールド	説明
RIP VRF	RIP VRF の名前。
port	RIP プロセスが使用しているポート。
multicast-group	RIP がメンバーとなっている IPv6 マルチキャスト グループ。
Administrative distance	ルーティング情報の送信元の優先度のランク付けに使用されます。接続されているルータにアドミニストレーティブ ディスタンス 1 があり、より大きなアドミニストレーティブ ディスタンス値を持つプロトコルによって学習されたルータよりも優先されます。
Updates	更新タイマーの値（秒単位）。
expires after	更新の期限が切れる間隔（秒単位）。

フィールド	説明
Holddown	ホールドダウン タイマーの値（秒単位）。
garbage collect	ガーベッジコレクション タイマーの値（秒単位）。
Split horizon	スプリット ホライズン状態は on か off のいずれかです。
poison reverse	ポイズン リバース状態は on か off のいずれかです。
Default routes	RIP へのデフォルト ルートの起点。デフォルト ルートを生成するか、しないかです。
Periodic updates	更新タイマーに送信した RIP アップデート パケットの数。
trigger updates	トリガーされた更新として送信された RIP アップデート パケットの数。

次に、**showipv6ripvrfnext-hops** コマンドの出力例を示します。

```
Device# show ipv6 rip vrf blue next-hops

     RIP VRF "blue", local RIB
      AAAA::/64, metric 2, installed
     Ethernet0/0/FE80::A8BB:CCFF:FE00:7C00, expires in 177 secs
```

表 *64 : show ipv6 rip vrf next-hops* フィールドの説明

フィールド	説明
RIP VRF	RIP VRF の名前。
metric	ルートのメトリック。
installed	ルートが IPv6 ルーティング テーブルにインストールされています。
Ethernet0/0/FE80::A8BB:CCFF:FE00:7C00	ネクストホップ アドレスおよびそれを学習したインターフェイス。ネクスト ホップは、ルートを学習した IPv6 RIP ネイバーのアドレスか、または IPv6 RIP アドバタイズメントで受信した明示的なネクストホップのいずれかです。 （注） IPv6 RIP ネイバーが明示的なネクスト ホップを使用してそのネイバーのすべてのルータをアドバタイズすることがあります。この場合、ネイバーのアドレスはネクスト ホップの表示に表示されません。
expires in	ルートの期限が切れるまでの間隔（秒単位）。

次に、**showipv6ripvrfdatabase** コマンドの出力例を示します。

```
Device# show ipv6 rip vrf blue database

        RIP VRF "blue", Next Hops
       FE80::A8BB:CCFF:FE00:7C00/Ethernet0/0 [1 paths]
```

表 *65 : show ipv6 rip vrf database* フィールドの説明

フィールド	説明
RIP VRF	RIP VRF の名前。
FE80::A8BB:CCFF:FE00:7C00/Ethernet0/0	IPv6 ルートが学習されたインターフェイスおよびLL ネクスト ホップ。
1 paths	ルーティング テーブル内に存在するこのルータへの固有のパスの数を示します。

関連コマンド

コマンド	説明
clearipv6rip	IPv6 RIP ルーティング テーブルからルートを削除します。
debugipv6rip	IPv6 RIP ルーティング テーブルの現在の内容を表示します。
ipv6 rip vrf-mode enable	IPv6 RIP の VRF 認識型サポートを有効にします。

show ipv6 route

IPv6 ルーティング テーブルの内容を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6route** コマンドを使用します。

show ipv6 route [{*ipv6-address*|*ipv6-prefix*/*prefix-length* [{**longer-prefixes**}][{*protocol*}] | [**repair**] | [{**updated** [{**boot-up**}] [{*day month*}] [{*time*}]}]|**interface** *type number*| **nd**|**nsf**|**table** *table-id* |**watch**}]

構文の説明

ipv6-address	（任意）特定の IPv6 アドレスのルーティング情報を表示します。
ipv6-prefix	（任意）特定の IPv6 ネットワークのルーティング情報を表示します。
/prefix-length	（オプション）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。
longer-prefixes	（任意）長いプレフィックス エントリの出力を表示します。
protocol	（任意）ルーティング プロトコルの名前または**connected**、**local**、**mobile**、または**static** キーワード。ルーティング プロトコルを指定する場合は、キーワードの **bgp**、**isis**、**eigrp**、**ospf**、または **rip** のいずれかを使用します。
repair	（任意）修復パスを持つルートを表示します。
updated	（任意）タイム スタンプを持つルートを表示します。
boot-up	（任意）ブートアップ以降のルーティング情報を表示します。
day month	（任意）指定した月日以降のルートを表示します。
time	（任意） *hh:mm* 形式で指定した時刻以降のルートを表示します。
interface	（任意）インターフェイスに関する情報を表示します。
type	（任意）インターフェイス タイプ。
number	（任意）インターフェイス番号。
nd	（任意）ネイバー探索（ND）が所有している IPv6 ルーティング情報ベース（RIB）からのルートのみを表示します。
nsf	（任意）ノンストップ フォワーディング（NSF）状態のルートを表示します。
repair	（任意）
table *table-id*	（任意）指定したテーブル ID の IPv6 RIB テーブル情報を表示します。テーブル ID は 16 進形式である必要があります。有効な範囲は 0 ～ 0-0xFFFFFFFF です。

watch	（任意）ルート ウォッチャに関する情報を表示します。

コマンド デフォルト

オプションのシンタックス要素を選択しないと、アクティブなすべてのルーティング テーブルのすべての IPv6 ルーティング情報が表示されます。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

showipv6route コマンドは、情報が IPv6 に固有であることを除き、**showiproute** コマンドと類似した出力を提供します。

ipv6-address 引数または *ipv6-prefix*/*prefix-length* 引数を指定すると、ルーティング テーブルから最長一致のルックアップが実行され、そのアドレスまたはネットワークのルータ情報のみが表示されます。ルーティング プロトコルを指定すると、そのプロトコルのルータのみが表示されます。**connected** キーワード、**local** キーワード、**mobile** キーワード、または **static** キーワードを指定すると、指定したタイプのルートのみが表示されます。**interface** キーワードと *type* 引数および *number* 引数を指定すると、指定したインターフェイスのルートのみが表示されます。

例

次に、キーワードまたは引数を指定しない場合の **showipv6route** コマンドの出力例を示します。

```
Device# show ipv6 route

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - IIS interarea
B   2001:DB8:4::2/48 [20/0]
     via FE80::A8BB:CCFF:FE02:8B00, Serial6/0
L   2001:DB8:4::3/48 [0/0]
     via ::, Ethernet1/0
C   2001:DB8:4::4/48 [0/0]
     via ::, Ethernet1/0
LC  2001:DB8:4::5/48 [0/0]
     via ::, Loopback0
L   2001:DB8:4::6/48 [0/0]
     via ::, Serial6/0
C   2001:DB8:4::7/48 [0/0]
     via ::, Serial6/0
S   2001:DB8:4::8/48 [1/0]
     via 2001:DB8:1::1, Null
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *66 : show ipv6 route* フィールドの説明

フィールド	説明
Codes:	ルートを生成したプロトコルを示します。表示される値は次のとおりです。 • B：BGP 生成 • C：接続済み • I1：ISIS L1：統合 IS-IS Level 1 生成 • I2：ISIS L2：統合 IS-IS Level 2 生成 • IA：ISIS エリア間：統合 IS-IS エリア間生成 • L：ローカル • R：RIP 生成 • S：スタティック
2001:DB8:4::2/48	リモート ネットワークの IPv6 プレフィックスを示します。
[20/0]	カッコ内の最初の数値は情報ソースのアドミニストレーティブディスタンスです。2 番目の数値はルートのメトリックです。
via FE80::A8BB:CCFF:FE02:8B00	リモート ネットワークまでの次のデバイスのアドレスを指定します。

ipv6-address 引数または *ipv6-prefix/prefix-length* 引数を指定すると、そのアドレスまたはネットワークのルート情報のみが表示されます。次に、IPv6 プレフィックスとして 2001:DB8::/35 を指定した場合の **showipv6route** コマンドの出力例を示します。出力にはフィールドの説明も表示されます。

```
Device# show ipv6 route 2001:DB8::/35

IPv6 Routing Table - 261 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
B 2001:DB8::/35 [20/3]
  via FE80::60:5C59:9E00:16, Tunnel1
```

プロトコルを指定すると、その特定のルーティング プロトコルのルートのみが表示されます。次に、**show ipv6 route bgp** コマンドの出力例を示します。出力にはフィールドの説明も表示されます。

```
Device# show ipv6 route bgp

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
```

```
B   2001:DB8:4::4/64 [20/0]
     via FE80::A8BB:CCFF:FE02:8B00, Serial6/0
```

次に、**show ipv6 route local** コマンドの出力例を示します。出力にはフィールドの説明も表示されます。

```
Device# show ipv6 route local

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
L   2001:DB8:4::2/128 [0/0]
     via ::, Ethernet1/0
LC  2001:DB8:4::1/128 [0/0]
     via ::, Loopback0
L   2001:DB8:4::3/128 [0/0]
     via ::, Serial6/0
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```

次に、6PE マルチパス機能を有効にした場合の **show ipv6 route** コマンドの出力例を示します。出力にはフィールドの説明も表示されます。

```
Device# show ipv6 route

IPv6 Routing Table - default - 19 entries
Codes:C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
.
.
.
B   2001:DB8::/64 [200/0]
     via ::FFFF:172.16.0.1
     via ::FFFF:172.30.30.1
```

関連コマンド

コマンド	説明
ipv6route	静的 IPv6 ルートを確立します。
showipv6interface	IPv6 インターフェイス情報を表示します。
showipv6routesummary	IPv6 ルーティング テーブルの現在の内容をサマリー形式で表示します。
showipv6tunnel	IPv6 トンネル情報を表示します。

show ipv6 routers

オンリンク デバイスから受信した IPv6 ルータ アドバタイズメント（RA）情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6routers** コマンドを使用します。

show ipv6 routers [*interface-type interface-number*] ［**conflicts**］ ［**vrf vrf-name**］［**detail**］

構文の説明

interface-type	（任意）インターフェイス タイプを指定します。
interface-number	（任意）インターフェイス番号を指定します。
conflicts	（任意）指定したインターフェイスに設定されている RA とは異なる RA を表示します。
vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
detail	（任意）デフォルトのデバイスとして選択するためのネイバーの資格に関する詳細を提供します。

コマンド デフォルト

インターフェイスを指定しないと、すべてのインターフェイス タイプのオンリンク RA 情報が表示されます（用語 *onl-link* は、リンク上のローカルで到達可能なアドレスのことです）。

コマンド モード

ユーザ EXEC

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

RA を受信するインターフェイスに設定されている RA パラメータとは異なるパラメータをアドバタイズするデバイスに conflicting というマークが付けられます。

例

次に、IPv6 インターフェイス タイプおよび番号を指定せずに入力した **showipv6routers** コマンドの出力例を示します。

```
Device# show ipv6 routers

Device FE80::83B3:60A4 on Tunnel5, last update 3 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
    Valid lifetime -1, preferred lifetime -1
```

```
Device FE80::290:27FF:FE8C:B709 on Tunnel57, last update 0 min
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
```

次に、デフォルトデバイスの高いプリファレンスをアドバタイズし、このリンク上でモバイルIPv6ホームエージェントとして機能している単一の隣接デバイスの出力例を示します。

```
Device# show ipv6 routers

IPV6 ND Routers (table: default)
  Device FE80::100 on Ethernet0/0, last update 0 min
  Hops 64, Lifetime 50 sec, AddrFlag=0, OtherFlag=0, MTU=1500
  HomeAgentFlag=1, Preference=High
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 2001::100/64 onlink autoconfig
    Valid lifetime 2592000, preferred lifetime 604800
```

次の表に、この出力で表示される重要なフィールドについて説明します。

表 *67 : show ipv6 routers* フィールドの説明

フィールド	説明
Hops	RA に設定されているホップ制限値。
Lifetime	RA に設定されているライフタイム値。値 0 は、デバイスがデフォルトのデバイスではないことを示します。0以外の値は、そのデバイスがデフォルトのデバイスであることを示します。
AddrFlag	値が 0 の場合は、デバイスから受信した RA はアドレスがステートフル自動設定メカニズムを使用して設定されていないことを示します。値が 1 の場合は、このメカニズムを使用してアドレスが設定されています。
OtherFlag	値が 0 の場合は、デバイスから受信した RA がアドレス以外の情報はステートフル自動設定メカニズムを使用して取得されていないことを示します。値が 1 の場合は、このメカニズムを使用してその他の情報が取得されています（値 OtherFlag は、AddrFlag の値が 1 の場合にのみ、1 になります）。
MTU	最大伝送単位（MTU）。
HomeAgentFlag=1	値は 0 または 1 のいずれかです。値 1 は、RA を受信するデバイスがこのリンク上でモバイル IPv6 ホーム エージェントとして機能していることを示し、値 0 はこのリンク上でモバイル IPv6 ホーム エージェントとして機能していないことを示します。
Preference=High	DRP 値（High、Medium、または Low のいずれか）。
Retransmit time	設定されている RetransTimer 値。ネイバー送信要求伝送用のこのリンクで使用する時間値。これは、アドレス解決と近隣到達不能検出に使用されます。値 0 は、アドバタイジング デバイスによってこの時間値が指定されていないことを意味します。

フィールド	説明
Prefix	デバイスによってアドバタイズされたプレフィックス。また、RA メッセージ内に on-link ビットまたは autoconfig ビットが設定されたかどうかも示します。
Valid lifetime	アドバタイズメントが送信された時間を基準にして、オンリンク判定のためにプレフィックスが有効である時間（秒単位）。値 -1 （すべて 1、0xffffffff）は無限を意味します。
preferred lifetime	アドバタイズメントが送信された時間を基準にし、アドレスの自動設定を介してプレフィックスから生成されたアドレスが有効なままになる時間（秒単位）。値 -1 （すべて 1、0xffffffff）は無限を意味します。

interface-type 引数と *interface-number* 引数を指定すると、その特定のインターフェイスに関する RA の詳細が表示されます。次に、インターフェイス タイプおよび番号を指定して入力した **showipv6routers** コマンドの出力例を示します。

```
Device# show ipv6 routers tunnel 5

Device FE80::83B3:60A4 on Tunnel5, last update 5 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
    Valid lifetime -1, preferred lifetime -1
```

showipv6routers コマンドと **conflicts** キーワードを入力すると、アドバタイズメントを受信するインターフェイスに設定されているパラメータとは異なるアドバタイジングパラメータのデバイスに関する情報が表示されます。次に、この出力例を示します。

```
Device# show ipv6 routers conflicts

Device FE80::203:FDFF:FE34:7039 on Ethernet1, last update 1 min, CONFLICT
   Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
   Reachable time 0 msec, Retransmit time 0 msec
   Prefix 2003::/64 onlink autoconfig
     Valid lifetime -1, preferred lifetime -1
Device FE80::201:42FF:FECA:A5C on Ethernet1, last update 0 min, CONFLICT
   Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
   Reachable time 0 msec, Retransmit time 0 msec
   Prefix 2001::/64 onlink autoconfig
     Valid lifetime -1, preferred lifetime -1
```

detail キーワードを使用すると、デバイスの優先ランク、デフォルトのデバイスとして選択されるための資格、およびデバイスが選択されたことがあるかないかに関する情報が表示されます。

```
Device# show ipv6 routers detail

Device FE80::A8BB:CCFF:FE00:5B00 on Ethernet0/0, last update 0 min
  Rank 0x811 (elegible), Default Router
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0, MTU=1500
  HomeAgentFlag=0, Preference=Medium, trustlevel = 0
  Reachable time 0 (unspecified), Retransmit time 0 (unspecified)
```

```
Prefix 2001::/64 onlink autoconfig
  Valid lifetime 2592000, preferred lifetime 604800
```

show ipv6 rpf

指定したユニキャスト ホストアドレスとプレフィックスのリバース パス フォワーディング（RPF）情報を確認するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6rpf** コマンドを使用します。

show ipv6 rpf {*source-vrf* [*access-list*]|**vrf** *receiver-vrf*{*source-vrf* [*access-list*]|**select**}}

構文の説明

source-vrf	ルックアップが実行される Virtual Routing and Forwarding（VRF）の名前またはアドレス。
receiver-vrf	ルックアップを開始する VRF の名前またはアドレス。
access-list	グループベースの VRF 選択ポリシーに適用するアクセス コントロール リスト（ACL）の名前またはアドレス。
vrf	VRF インスタンスに関する情報を表示します。
select	グループから VRF へのマッピング情報を表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

showipv6rpf コマンドは、IPv6 マルチキャスト ルーティングがリバース パス フォワーディング（RPF）をどのように実行したかに関する情報を表示します。ルータは複数のルーティング テーブル（ユニキャスト ルーティング情報ベース（RIB）、マルチプロトコル Border Gateway Protocol（BGP）ルーティング テーブル、静的 mroute など）から RPF 情報を検索できるため、**showipv6rpf** コマンドでは情報が取得される送信元を表示します。

例

次に、IPv6 アドレス 2001::1:1:2 を持つユニキャスト ホストの RPF 情報を表示する例を示します。

```
Device# show ipv6 rpf 2001::1:1:2
RPF information for 2001::1:1:2
  RPF interface:Ethernet3/2
  RPF neighbor:FE80::40:1:3
  RPF route/mask:20::/64
  RPF type:Unicast
  RPF recursion count:0
```

```
Metric preference:110
Metric:30
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *68 : show ipv6 rpf* フィールドの説明

フィールド	説明
RPF information for 2001::1:1:2	この情報に関係する送信元アドレス。
RPF interface:Ethernet3/2	指定した送信元について、ルータがパケットの取得を予定しているインターフェイス。
RPF neighbor:FE80::40:1:3	指定した送信元について、ルータがパケットの取得を予定しているネイバー。
RPF route/mask:20::/64	この送信元と照合するルート番号およびマスク。
RPF type:Unicast	このルートを取得したルーティングテーブル。ユニキャスト、Multiprotocol BGP、または静的 mroute のいずれかです。
RPF recursion count	ルートが再帰的に解決された回数を示します。
Metric preference:110	代表フォワーダ（DF）によってアナウンされたルートプロセッサ（RP）に対してユニキャスト ルーティング メットリックを選択するために使用するプリフェレンス値。
Metric:30	DF によってアナウンスされた RP に対するユニキャスト ルーティング メトリック。

show ipv6 source-guard policy

IPv6 送信元ガード ポリシーの設定を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 source-guard policy** コマンドを使用します。

show ipv6 source-guard policy [*source-guard-policy*]

構文の説明

source-guard-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 モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

show ipv6 source-guard policy コマンドは、IPv6 送信元ガード ポリシーの設定と、そのポリシーを適用するすべてのインターフェイスを表示します。また、このコマンドは、IPv6 プレフィックス ガード機能がデバイス上で有効になっている場合は IPv6 プレフィックス ガード情報も表示します。

例

```
Device# show ipv6 source-guard policy policy1

Policy policy1 configuration:
data-glean
prefix-guard
address-guard

Policy policy1 is applied on the following targets:
Target           Type  Policy              Feature        Target range
Et0/0            PORT   policy1            source-guard   vlan all
vlan 100         VLAN   policy1            source-guard   vlan all
```

関連コマンド

コマンド	説明
ipv6 source-guard attach-policy	インターフェイスに IPv6 ソース ガードを適用します。
ipv6 source-guard policy	IPv6 送信元ガード ポリシー名を定義して、送信元ガード ポリシー設定モードを開始します。

show ipv6 spd

IPv6 選択的パケット廃棄（SPD）設定を表示するには、特権 EXEC モードで **show ipv6spd** コマンドを使用します。

show ipv6 spd

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 モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

トラブルシューティングに役立つ情報が提供される場合がある SPD 設定を表示するには、**showipv6spd** コマンドを使用します。

例

次に、**showipv6spd** コマンドの出力例を示します。

```
Device# show ipv6 spd
Current mode: normal
Queue max threshold: 74, Headroom: 100, Extended Headroom: 10
IPv6 packet queue: 0
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *69 : show ipv6 spd* フィールドの説明

フィールド	説明
Current mode: normal	現在の SPD の状態またはモード。
Queue max threshold: 74	プロセス入力キューの最大値。

関連コマンド

コマンド	説明
ipv6spdqueuemax-threshold	SPD プロセス入力キュー内の最大パケット数を設定します。

show ipv6 static

IPv6 ルーティング テーブルの現在の内容を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6static** コマンドを使用します。

show ipv6 static [{*ipv6-address*|*ipv6-prefix*/*prefix-length*}] [{**interface** *type number*|**recursive**}] **[detail]**

構文の説明

ipv6-address	（任意）特定の IPv6 アドレスのルーティング情報を提供します。 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。
ipv6-prefix	（任意）特定の IPv6 ネットワークのルーティング情報を提供します。 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。
/prefix-length	（オプション）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。
interface	（任意）インターフェイスの名前。
type	（任意。ただし、**interface** キーワードを使用した場合は必須）インターフェイス タイプ。サポートされているインターフェイスのタイプについては、疑問符（?）のオンライン ヘルプ機能を使用してください。
number	（任意。ただし、**interface** キーワードを使用した場合は必須）インターフェイス番号。サポートされているインターフェイスの特定の番号シンタックスについては、疑問符（?）のオンライン ヘルプ機能を使用してください。
recursive	（任意）再帰的な静的ルートのみを表示できます。
detail	（任意）次の追加情報を指定します。 • 有効な再帰ルートの場合は、出力パス セットおよび最大解決深度 • 無効な再帰ルートの場合は、ルートが有効でない理由 • 無効なダイレクト ルートまたは完全指定のルートの場合は、ルートが有効でない理由

コマンド デフォルト

アクティブなすべてのルーティング テーブルのすべての IPv6 ルーティング情報が表示されます。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

showipv6static コマンドの出力は、IPv6 に固有である点を除き、**showiproute** コマンドの出力と似ています。

ipv6-address 引数または *ipv6-prefix*/*prefix-length* 引数を指定すると、ルーティング テーブルから最長一致のルックアップが実行され、そのアドレスまたはネットワークのルータ情報のみが表示されます。コマンド シンタックス内に指定した条件に一致する情報のみが表示されます。たとえば、*type number* 引数を指定すると、指定したインターフェイス固有のルートのみが表示されます。

例

コマンド シンタックスでオプションが指定されていない show ipv6 static コマンド：例

コマンドにオプションを使用しないと、IPv6 ルーティング情報ベース（RIB）にインストールされているルートがアスタリスクでマークされます。次に、この例を示します。

```
Device# show ipv6 static

IPv6 Static routes
Code: * - installed in RIB
* 3000::/16, interface Ethernet1/0, distance 1
* 4000::/16, via nexthop 2001:1::1, distance 1
  5000::/16, interface Ethernet3/0, distance 1
* 5555::/16, via nexthop 4000::1, distance 1
  5555::/16, via nexthop 9999::1, distance 1
* 5555::/16, interface Ethernet2/0, distance 1
* 6000::/16, via nexthop 2007::1, interface Ethernet1/0, distance 1
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *70 : show ipv6 static* フィールドの説明

フィールド	説明
via nexthop	リモート ネットワークへのパス内にある次の Device のアドレスを指定します。
distance 1	指定したルートまでのアドミニストレーティブ ディスタンス示します。

IPv6 アドレスとプレフィックスを指定した show ipv6 static コマンド：例

ipv6-address 引数または *ipv6-prefix*/*prefix-length* 引数を指定すると、そのアドレスまたはネットワークの静的ルートに関する情報のみが表示されます。次に、IPv6プレフィックス 2001:200::/35 を指定して入力した **showipv6route** コマンドの出力例を示します。

```
Device# show ipv6 static 2001:200::/35

IPv6 Static routes
Code: * - installed in RIB
* 2001:200::/35, via nexthop 4000::1, distance 1
  2001:200::/35, via nexthop 9999::1, distance 1
* 2001:200::/35, interface Ethernet2/0, distance 1
```

show ipv6 static interface コマンド：例

インターフェイスを指定した場合、指定したインターフェイスを発信インターフェイスとして使用する静的ルートだけが表示されます。**interface** キーワードは、コマンドステートメント内にIPv6アドレスとプレフィックスが指定されていても、されていなくても使用できます。

```
Device# show ipv6 static interface ethernet 3/0
```

IPv6 Static routes Code: * - installed in RIB 5000::/16, interface Ethernet3/0, distance 1

show ipv6 static recursive コマンド：例

recursive キーワードを指定すると、再帰的な静的ルートのみが表示されます。

```
Device# show ipv6 static recursive
```

IPv6 Static routes Code: * - installed in RIB * 4000::/16, via nexthop 2001:1::1, distance 1 * 5555::/16, via nexthop 4000::1, distance 1 5555::/16, via nexthop 9999::1, distance 1

show ipv6 static detail コマンド：例

detail キーワードを指定した場合、次の追加情報が表示されます。

- 有効な再帰ルートの場合は、出力パス セットおよび最大解決深度
- 無効な再帰ルートの場合は、ルートが有効でない理由
- 無効なダイレクト ルートまたは完全指定のルートの場合は、ルートが有効でない理由

```
Device# show ipv6 static detail

IPv6 Static routes
```

```
Code: * - installed in RIB
* 3000::/16, interface Ethernet1/0, distance 1
* 4000::/16, via nexthop 2001:1::1, distance 1
     Resolves to 1 paths (max depth 1)
     via Ethernet1/0
  5000::/16, interface Ethernet3/0, distance 1
     Interface is down
* 5555::/16, via nexthop 4000::1, distance 1
     Resolves to 1 paths (max depth 2)
     via Ethernet1/0
  5555::/16, via nexthop 9999::1, distance 1
     Route does not fully resolve
* 5555::/16, interface Ethernet2/0, distance 1
* 6000::/16, via nexthop 2007::1, interface Ethernet1/0, distance 1
```

関連コマンド

コマンド	説明
ipv6route	静的 IPv6 ルートを確立します。
showiproute	ルーティング テーブルの現在の状態を表示します。
showipv6interface	IPv6 インターフェイス情報を表示します。
showipv6routesummary	IPv6 ルーティング テーブルの現在の内容をサマリー形式で表示します。
showipv6tunnel	IPv6 トンネル情報を表示します。

show ipv6 traffic

IPv6 トラフィックを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6traffic** コマンドを使用します。

show ipv6 traffic [**interface** [*interface type number*]]

構文の説明

interface	（任意）すべてのインターフェイス。IPv6 転送統計が保持されているすべてのインターフェイスの IPv6 転送統計が表示されます。
interface type number	（任意）指定したインターフェイス。特定のインターフェイス上で統計が最後にクリアされてから発生したインターフェイス統計が表示されます。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

showipv6traffic コマンドの出力は、IPv6 に固有である点を除き、**showiptraffic** コマンドの出力と似ています。

例

次に、**showipv6traffic** コマンドの出力例を示します。

```
Device# show ipv6 traffic
IPv6 statistics:
  Rcvd:  0 total, 0 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a device
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
         0 unicast RPF drop, 0 suppressed RPF drop
  Sent:  0 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 0 received, 0 sent
ICMP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
```

```
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 device solicit, 0 device advert, 0 redirects
```

次に、IPv6 CEF を実行しない **show ipv6 interface** コマンドの出力例を示します。

```
Device# show ipv6 interface ethernet 0/1/1
Ethernet0/1/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::203:FDFF:FE49:9
  Description: sat-2900a f0/12
  Global unicast address(es):
    7::7, subnet is 7::/32
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:7
    FF02::1:FF49:9
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  Input features: RPF
  Unicast RPF access-list MINI
    Process Switching:
      0 verification drops
      0 suppressed verification drops
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
```

次に、IPv6 CEF を実行する **show ipv6 interface** コマンドの出力例を示します。

```
Device# show ipv6 interface ethernet 0/1/1
Ethernet0/1/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::203:FDFF:FE49:9
  Description: sat-2900a f0/12
  Global unicast address(es):
    7::7, subnet is 7::/32
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:7
    FF02::1:FF49:9
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  Input features: RPF
  Unicast RPF access-list MINI
    Process Switching:
      0 verification drops
      0 suppressed verification drops
    CEF Switching:
      0 verification drops
      0 suppressed verification drops
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *71 : show ipv6 traffic* フィールドの説明

フィールド	説明
source-routed	送信元ルーティング パケットの数。
truncated	切り捨てられたパケットの数。
format errors	ヘッダー フィールド、バージョン番号、およびパケット長に実行したチェックにより発生した可能性のあるエラー。
not a device	IPv6 ユニキャスト ルーティングを有効にしていない場合に送信されるメッセージ。
0 unicast RPF drop, 0 suppressed RPF drop	ユニキャストと抑制されたリバース パス フォワーディング（RPF）のドロップの数
failed	失敗したフラグメント伝送の数。
encapsulation failed	未解決のアドレスまたはtry-and-queueパケットにより発生する可能性のある障害。
no route	ルーティング方法が不明なデータグラムをソフトウェアが破棄するときにカウントされます。
unreach	受信した到達不能メッセージは次のとおりです。 • routing：宛て先までのルートがないことを示します。 • admin：宛て先との通信が管理上の理由で禁止されていることを示します。 • neighbor：宛て先が送信元アドレスの範囲を超えていることを示します。たとえば、送信元がローカル サイトであるか、または送信元に戻るルートが宛て先にない場合があります。 • address：アドレスに到達不能であることを示します。 • port：ポートに到達不能であることを示します。
Unicast RPF access-list MINI	使用中のユニキャスト RPF アクセスリスト。
Process Switching	検証ドロップや抑制された検証ドロップなどのプロセス RPF カウントを表示します。
CEF Switching	検証ドロップや抑制された検証ドロップなどの CEF スイッチング カウントを表示します。

show ipv6 pim tunnel

インターフェイス上の Protocol Independent Multicast（PIM）登録カプセル化トンネルおよびカプセル化解除トンネルを表示するには、特権 EXEC モードで **showipv6pimtunnel** コマンドを使用します。

show ipv6 pim [**vrf** *vrf-name*] **tunnel** [*interface-type interface-number*]

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
interface-type interface-number	（任意）トンネル インターフェイスのタイプおよび番号

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 Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

オプションの *interface* キーワードを指定せずに **showipv6pimtunnel** コマンドを使用すると、PIM 登録カプセル化トンネル インターフェイスとカプセル化解除トンネル インターフェイスに関する情報が表示されます。

PIM カプセル化トンネルは、レジスタ トンネルです。カプセル化トンネルは、各ルータ上のすべての既知のランデブー ポイント（RP）に対して作成されます。PIM カプセル化解除トンネルは、レジスタ カプセル化解除トンネルです。カプセル化解除トンネルは、RP アドレスとして設定されているアドレスの RP に作成されます。

例

次に、RP での **showipv6pimtunnel** コマンドの出力例を示します。

```
Device# show ipv6 pim tunnel
Tunnel0*
 Type  :PIM Encap
 RP    :100::1
 Source:100::1
Tunnel0*
 Type  :PIM Decap
 RP    :100::1
 Source: -
```

次に、RP 以外での **showipv6pimtunnel** コマンドの出力例を示します。

```
Device# show ipv6 pim tunnel
Tunnel0*
 Type  :PIM Encap
 RP    :100::1
 Source:2001::1:1:1
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *72 : show ipv6 pim tunnel* フィールドの説明

フィールド	説明
Tunnel0*	トンネルの名前。
Type	トンネルのタイプ。PIM のカプセル化または PIM カプセル化の解除ができます。
source	RP にカプセル化登録を送信しているルータの送信元アドレス。

show ipv6 wccp

IPv6 Web キャッシュ通信プロトコル（WCCP）のグローバル設定と統計を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showipv6wccp** コマンドを使用します。

```
show ipv6 wccp [[all] [capabilities] [summary] [
interfaces[{cef|counts|detail}] ][vrf
vrf-name][{web-cacheservice-number}[[assignment] [clients] [counters] [detail]
[service] [view]]]]
```

構文の説明

summary	（任意）WCCP サービスのサマリーを表示します。
capabilities	（任意）WCCP プラットフォーム機能の情報を表示します。
vrf *vrf-name*	（任意）表示するサービス グループに関連付けられている Virtual Routing and Forwarding（VRF）インスタンスを指定します。
service-number	（任意）キャッシュが制御する Web キャッシュ サービス グループの ID 番号。番号は、0 ～ 254 です。Cisco Cache Engine を使用する Web キャッシュの場合、リバース プロキシ サービスの値には 99 を指定します。
interfaces	（任意）WCCP リダイレクト インターフェイスを表示します。
cef	（任意）Cisco Express Forwarding インターフェイスの統計（入力、出力、ダイナミック、静的、マルチキャストの各サービスの数を含む）を表示します。
counts	（任意）WCCP インターフェイス カウント統計（リダイレクトされた Cisco Express Forwarding およびプロセス スイッチングされた出力パケットと入力パケットの数を含む）を表示します。
detail	（任意）WCCP インターフェイス設定の統計（入力、出力、ダイナミック、静的、マルチキャストの各サービスの数を含む）を表示します。
web-cache	（任意）Web キャッシュ サービスの統計を表示します。
all	（任意）既知のすべてのサービスの統計を表示します。
assignment	（任意）サービス グループの割り当て情報を表示します。
service	（任意）サービスに関する詳細情報（サービス定義およびその他のサービスごとのすべての情報を含む）を表示します。
clients	（任意）サービスのクライアントに関する詳細情報（クライアントごとのすべての情報を含む）を表示します。サービスごとの情報は表示されません。
detail	（任意）サービスのクライアントに関する詳細情報（クライアントごとのすべての情報を含む）を表示します。サービスごとの情報は表示されません。割り当て情報も表示されます。

counters	（任意）トラフィック カウンタを表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

すべての WCCP カウンタをリセットするには、**clearipv6wccp** コマンドを使用します。

WCCP クライアントのタイムアウト間隔およびリダイレクト割り当てのタイムアウト間隔がそれらのデフォルト値の 10 秒に設定されていない場合、それらの間隔に関する情報を表示するには、**showipv6wccp** *service-number***detail** コマンドを使用します。

設定されている WCCP サービスおよびそれらの現在の状態のサマリーを表示するには、**showipv6wccpsummary** コマンドを使用します。

例

この項には、次の形式のこのコマンドの例とフィールドの説明が記載されています。

- **showipv6wccp** *service-number*（サービス モードを表示）
- **showipv6wccp** *service-number***detail**
- **showipv6wccpinterfaces**
- **showipv6wccpweb-cache**
- **showipv6wccpweb-cachecounters**
- **showipv6wccpweb-cachedetail**
- **showipv6wccpweb-cachedetail** （バイパス カウンタを表示）
- **showipv6wccpweb-cacheservice**
- **showipv6wccpsummary**

show ipv6 wccp *service-number*（サービス モードを表示）

次に、**showipv6wccp** *service-number* コマンドの出力例を示します。

```
Device# show ipv6 wccp 61

Global WCCP information:
    Router information:
        Router Identifier:                   2001:DB8:100::1

    Service Identifier: 61
        Protocol Version:                    2.01
```

```
Number of Service Group Clients:     2
Number of Service Group Routers:     1
Total Packets Redirected:            0
  Process:                           0
  CEF:                               0
Service mode:                        Open
Service Access-list:                 -none-
Total Packets Dropped Closed:        0
Redirect access-list:                -none-
Total Packets Denied Redirect:       0
Total Packets Unassigned:            0
Group access-list:                   -none-
Total Messages Denied to Group:      0
Total Authentication failures:       0
Total GRE Bypassed Packets Received: 0
  Process:                           0
  CEF:                               0
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *73 : show ipv6 wccp service-number* フィールドの説明

フィールド	説明
Device information	現在のルータによって検出された Device のリスト。
Protocol Version	サービス グループ内の Device で使用されている WCCP のバージョン。
Service Identifier	サービスの識別情報を示します。
Number of Service Group Clients	サービス グループ内の Device とその他のクライアントで認識可能なクライアントの数。
Number of Service Group Device(s)	サービス グループ内の Device の数。
Total Packets s/w Redirected	Device によってリダイレクトされたパケットの総数。
Service mode	WCCP サービス モードを識別します。オプションは Open と Closed です。
Service Access-list	サービスと一致するパケットが定義された名前付き拡張 IP アクセス リスト。
Total Packets Dropped Closed	WCCP が、クローズドサービス用に設定されており、サービスの処理に仲介デバイスが使用できない場合にドロップされたパケットの総数。
Redirect Access-list	リダイレクトするパケットが決定されるアクセスリストの名前または番号。
Total Packets Denied Redirect	アクセスリストと一致しないためにリダイレクトされなかったパケットの総数。

フィールド	説明
Total Packets Unassigned	キャッシュエンジンに割り当てられていないためにリダイレクトされなかったパケットの数。キャッシュエンジンの初期検出中またはクラスタからキャッシュが取り外されたときは、パケットが割り当てられない可能性があります。
Group Access-list	ルータに接続できるキャッシュ エンジンを示します。
Total Messages Denied to Group	*group-list* アクセス リストによって拒否されたパケットの数を示します。
Total Authentication failures	パスワードが一致しなかったインスタンス数。
Total Bypassed Packets Received	バイパスされたパケット数。プロセスおよび Cisco Express Forwarding は、Cisco IOS ソフトウェア内のスイッチング パスです。

show ipv6 wccp *service-number* detail

次の例では、サービス タイプを含む WCCP ルータ統計情報および WCCP クライアント情報を表示します。

```
Device# show ipv6 wccp 61 detail

WCCP Client information:
        WCCP Client ID:          2001:DB8:1::11
        Protocol Version:        2.01
        State:                   Usable
        Redirection:             L2
        Packet Return:           L2
        Assignment:              MASK
        Connect Time:            1w0d
        Redirected Packets:
          Process:               0
          CEF:                   0
        GRE Bypassed Packets:
          Process:               0
          CEF:                   0
        Mask Allotment:          32 of 64 (50.00%)
        Assigned masks/values:   1/32

        Mask  SrcAddr    DstAddr    SrcPort DstPort
        ----  -------    -------    ------- -------
        0000: ::3        ::F        0x0000  0x0000

        Value SrcAddr    DstAddr    SrcPort DstPort
        ----- -------    -------    ------- -------
        0000: ::         ::         0x0000  0x0000
        0001: ::         ::2        0x0000  0x0000
        0002: ::         ::4        0x0000  0x0000
        0003: ::         ::6        0x0000  0x0000
        0004: ::         ::8        0x0000  0x0000
        0005: ::         ::A        0x0000  0x0000
        0006: ::         ::C        0x0000  0x0000
```

```
0007: ::         ::E        0x0000  0x0000
0008: ::1        ::         0x0000  0x0000
0009: ::1        ::2        0x0000  0x0000
0010: ::1        ::4        0x0000  0x0000
0011: ::1        ::6        0x0000  0x0000
0012: ::1        ::8        0x0000  0x0000
0013: ::1        ::A        0x0000  0x0000
0014: ::1        ::C        0x0000  0x0000
0015: ::1        ::E        0x0000  0x0000
0016: ::2        ::         0x0000  0x0000
0017: ::2        ::2        0x0000  0x0000
0018: ::2        ::4        0x0000  0x0000
0019: ::2        ::6        0x0000  0x0000
0020: ::2        ::8        0x0000  0x0000
0021: ::2        ::A        0x0000  0x0000
0022: ::2        ::C        0x0000  0x0000
0023: ::2        ::E        0x0000  0x0000
0024: ::3        ::         0x0000  0x0000
0025: ::3        ::2        0x0000  0x0000
0026: ::3        ::4        0x0000  0x0000
0027: ::3        ::6        0x0000  0x0000
0028: ::3        ::8        0x0000  0x0000
0029: ::3        ::A        0x0000  0x0000
0030: ::3        ::C        0x0000  0x0000
0031: ::3        ::E        0x0000  0x0000


WCCP Client ID:          2001:DB8:1::12
Protocol Version:        2.01
State:                   Usable
Redirection:             L2
Packet Return:           L2
Assignment:              MASK
Connect Time:            1w0d
Redirected Packets:
  Process:               0
  CEF:                   0
GRE Bypassed Packets:
  Process:               0
  CEF:                   0
Mask Allotment:          32 of 64 (50.00%)
Assigned masks/values:   1/32

Mask  SrcAddr    DstAddr    SrcPort DstPort
----  -------    -------    ------- -------
0000: ::3        ::F        0x0000  0x0000

Value SrcAddr    DstAddr    SrcPort DstPort
----- -------    -------    ------- -------
0000: ::         ::1        0x0000  0x0000
0001: ::         ::3        0x0000  0x0000
0002: ::         ::5        0x0000  0x0000
0003: ::         ::7        0x0000  0x0000
0004: ::         ::9        0x0000  0x0000
0005: ::         ::B        0x0000  0x0000
0006: ::         ::D        0x0000  0x0000
0007: ::         ::F        0x0000  0x0000
0008: ::1        ::1        0x0000  0x0000
0009: ::1        ::3        0x0000  0x0000
0010: ::1        ::5        0x0000  0x0000
0011: ::1        ::7        0x0000  0x0000
0012: ::1        ::9        0x0000  0x0000
0013: ::1        ::B        0x0000  0x0000
0014: ::1        ::D        0x0000  0x0000
```

```
0015: ::1         ::F         0x0000  0x0000
0016: ::2         ::1         0x0000  0x0000
0017: ::2         ::3         0x0000  0x0000
0018: ::2         ::5         0x0000  0x0000
0019: ::2         ::7         0x0000  0x0000
0020: ::2         ::9         0x0000  0x0000
0021: ::2         ::B         0x0000  0x0000
0022: ::2         ::D         0x0000  0x0000
0023: ::2         ::F         0x0000  0x0000
0024: ::3         ::1         0x0000  0x0000
0025: ::3         ::3         0x0000  0x0000
0026: ::3         ::5         0x0000  0x0000
0027: ::3         ::7         0x0000  0x0000
0028: ::3         ::9         0x0000  0x0000
0029: ::3         ::B         0x0000  0x0000
0030: ::3         ::D         0x0000  0x0000
0031: ::3         ::F         0x0000  0x0000
```

表 *74 : show ipv6 wccp service-number detail* フィールドの説明

フィールド	説明
Protocol Version	サービス グループ内の Device で使用されている WCCP のバージョン。
State	WCCP クライアントが正常に動作しているかどうかと、サービス グループ内の Device やその他のクライアントから通信できるかどうかを示します。 WCCP クライアントに不適合なメッセージ間隔の設定が含まれている場合、そのクライアントの状態は「NOT Usable」と表示され、その後にクライアントが使用できない理由を説明するステータス メッセージが続きます。
Redirection	使用されたリダイレクション メソッドを示します。WCCP は、GRE または L2 を使用して、IP トラフィックをリダイレクトします。
Assignment	使用されたロードバランシング メソッドを示します。WCCP は、HASH 割り当てまたは MASK 割り当てを使用します。
Message Interval	WCCCP クライアントから WCCP Device に送信された連続キープアライブ メッセージ間の固定された時間間隔（秒単位）。デフォルトの間隔は 10 秒です。デフォルトの時間間隔が設定されている場合、[Message Interval] フィールドは表示されません。
Client timeout	WCCP Device がクライアントに到達できないと見なし、サービス グループからそのクライアントを削除するまでにクライアントからのキープアライブ メッセージを WCCP Device が受信せずに経過する必要がある時間（秒単位）。
Assignment timeout	WCCP Device が障害のあるクライアントを検出し、トラフィックのリダイレクトを開始した後に経過する必要がある時間（秒単位）。
Packets Redirected	コンテンツ エンジンにリダイレクトされたパケットの数。

フィールド	説明
Connect Time	クライアントが Device に接続されていた時間（時間、分、秒）。

show ipv6 wccp interfaces

次に、**showipv6wccpinterfaces** コマンドの出力例を示します。

```
Device# show ipv6 wccp interfaces

WCCP interface configuration:
    FastEthernet0/1/0
        Output services: 2
        Input services: 3
        Mcast services: 1
        Exclude In:      FALSE
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *75 : show ipv6 wccp interfaces* フィールドの説明

フィールド	説明
Output services	インターフェイスで設定されている出力サービスの数を示します。
Input services	インターフェイスで設定されている入力サービスの数を示します。
Mcast services	インターフェイスで設定されているマルチキャストサービスの数を示します。
Exclude In	インターフェイス上のトラフィックがリダイレクションから除外されているかどうかを表示します。

show ipv6 wccp web-cache

次は、**showipv6wccpweb-cache** コマンドの出力例です。

```
Device# show ipv6 wccp web-cache

Global WCCP information:
    Router information:
        Router Identifier:                  2001:DB8:100::1

    Service Identifier: web-cache
        Protocol Version:                   2.01
        Number of Service Group Clients:    2
        Number of Service Group Routers:    1
        Total Packets Redirected:           0
          Process:                          0
          CEF:                              0
        Service mode:                       Open
        Service Access-list:                -none-
        Total Packets Dropped Closed:       0
```

```
Redirect access-list:                -none-
Total Packets Denied Redirect:       0
Total Packets Unassigned:            0
Group access-list:                   -none-
Total Messages Denied to Group:      0
Total Authentication failures:       0
Total GRE Bypassed Packets Received: 0
  Process:                           0
  CEF:                               0
GRE tunnel interface:                Tunnel1
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *76 : show ipv6 wccp web-cache* フィールドの説明

フィールド	説明
Protocol Version	サービス グループ内のキャッシュ エンジンで使用されている WCCP のバージョン。
Service Identifier	サービスの識別情報を示します。
Number of Service Group Clients	ホーム Device として Device を使用しているクライアントの数。
Number of Service Group Device(s)	サービス グループ内の Device の数。
Total Packets Redirected	Device によってリダイレクトされたパケットの総数。
Service mode	WCCP オープン モードまたはクローズド モードが設定されているかどうかを示します。
Service Access-list	リダイレクトするパケットが決定されるサービス アクセス リストの名前または番号。
Redirect access-list	リダイレクトするパケットが決定されるアクセス リストの名前または番号。
Total Packets Denied Redirect	アクセス リストと一致しないためにリダイレクトされなかったパケットの総数。
Total Packets Unassigned	キャッシュ エンジンに割り当てられていないためにリダイレクトされなかったパケットの数。キャッシュ エンジンの初期検出中またはクラスタからキャッシュが取り外されたときは、パケットが割り当てられない可能性があります。
Group access-list	Device に接続できるキャッシュ エンジンを示します。
Total Messages Denied to Group	*group-list* アクセス リストによって拒否されたパケットの数を示します。

フィールド	説明
Total Authentication failures	パスワードが一致しなかったインスタンス数。

show ipv6 wccp web-cache counters

次に、Web キャッシュ エンジンの情報と WCCP トラフィック カウンタを表示する例を示します。

```
Device# show ipv6 wccp web-cache counters

WCCP Service Group Counters:
   Redirected Packets:
     Process:                    0
     CEF:                        0
   Non-Redirected Packets:
     Action - Forward:
       Reason - no assignment:
         Process:                0
         CEF:                    0
     Action - Ignore (forward):
       Reason - redir ACL check:
         Process:                0
         CEF:                    0
     Action - Discard:
       Reason - closed services:
         Process:                0
         CEF:                    0
   GRE Bypassed Packets:
     Process:                    0
     CEF:                        0
   GRE Bypassed Packet Errors:
     Total Errors:
       Process:                  0
       CEF:                      0

   WCCP Client Counters:
     WCCP Client ID:             2001:DB8:1::11
       Redirect Assignments:
         Received:               1
         Invalid:                0
         Duplicate:              0
        Redirected Packets:
          Process:               0
          CEF:                   0
        GRE Bypassed Packets:
          Process:               0
          CEF:                   0

     WCCP Client ID:             2001:DB8:1::12
        Redirected Packets:
          Process:               0
          CEF:                   0
        GRE Bypassed Packets:
          Process:               0
          CEF:                   0
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *77 : show ipv6 wccp web-cache counters* フィールドの説明

フィールド	説明
Redirected Packets	ルータによってリダイレクトされたパケットの総数
Non-Redirected Packets	ルータによってリダイレクトされていないパケットの総数

show ipv6 wccp web-cache detail

次に、Web キャッシュ エンジンの情報と Web キャッシュ サービスの WCCP Device 統計を表示する例を示します。

```
Device# show ipv6 wccp web-cache detail

WCCP Client information:
        WCCP Client ID:          2001:DB8:1::11
        Protocol Version:        2.01
        State:                   Usable
        Redirection:             GRE
        Packet Return:           GRE
        Assignment:              HASH
        Connect Time:            1w0d
        Redirected Packets:
          Process:               0
          CEF:                   0
        GRE Bypassed Packets:
          Process:               0
          CEF:                   0
        Hash Allotment:          128 of 256 (50.00%)
        Initial Hash Info:       00000000000000000000000000000000
                                 00000000000000000000000000000000
        Assigned Hash Info:      55555555555555555555555555555555
                                 55555555555555555555555555555555

        WCCP Client ID:          2001:DB8:1::12
        Protocol Version:        2.01
        State:                   Usable
        Redirection:             GRE
        Packet Return:           GRE
        Assignment:              HASH
        Connect Time:            1w0d
        Redirected Packets:
          Process:               0
          CEF:                   0
        GRE Bypassed Packets:
          Process:               0
          CEF:                   0
        Hash Allotment:          128 of 256 (50.00%)
        Initial Hash Info:       00000000000000000000000000000000
                                 00000000000000000000000000000000
        Assigned Hash Info:      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
                                 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *78 : show ipv6 wccp web-cache detail* フィールドの説明

フィールド	説明
WCCP Client Information	クライアントの情報に関するフィールドを含むエリアのヘッダー。
IP Address	サービス グループ内のキャッシュ エンジンの IP アドレス。
Protocol Version	サービス グループ内のキャッシュ エンジンで使用されている WCCP のバージョン。
State	キャッシュエンジンが正常に動作しいるかどうかと、サービスグループ内の Device やその他のキャッシュ エンジンから通信できるかどうかを示します。
Redirected Packets	キャッシュ エンジンにリダイレクトされたパケットの数。
Connect Time	キャッシュ エンジンが Device に接続されていた時間（時間、分、秒）。

show ipv6 wccp web-cache detail（バイパス カウンタ）

次に、Web キャッシュ エンジンの情報およびバイパス カウンタを含む WCCP Device 統計を表示する例を示します。

```
Device# show ipv6 wccp web-cache detail

WCCP Client information:
        WCCP Client ID:          2001:DB8:1::11
        Protocol Version:        2.01
        State:                   Usable
        Redirection:             GRE
        Packet Return:           GRE
        Assignment:              HASH
        Connect Time:            1w0d
        Redirected Packets:
          Process:               0
          CEF:                   0
        GRE Bypassed Packets:
          Process:               0
          CEF:                   0
        Hash Allotment:          128 of 256 (50.00%)
        Initial Hash Info:       00000000000000000000000000000000
                                 00000000000000000000000000000000
        Assigned Hash Info:      55555555555555555555555555555555
                                 55555555555555555555555555555555

        WCCP Client ID:          2001:DB8:1::12
        Protocol Version:        2.01
        State:                   Usable
        Redirection:             GRE
```

```
Packet Return:           GRE
Assignment:              HASH
Connect Time:            1w0d
Redirected Packets:
  Process:               0
  CEF:                   0
GRE Bypassed Packets:
  Process:               0
  CEF:                   0
Hash Allotment:          128 of 256 (50.00%)
Initial Hash Info:       00000000000000000000000000000000
                         00000000000000000000000000000000
Assigned Hash Info:      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
                         AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *79 : show ipv6 wccp web-cache detail* フィールドの説明

フィールド	説明
WCCP Device information	サービス グループ内のキャッシュ エンジンに接続されたルータに関連付けられている WCCP の IP アドレスとバージョン用のフィールドを含むエリアのヘッダー。
IP Address	サービス グループ内のキャッシュ エンジンに接続された Device の IP アドレス。
Protocol Version	サービス グループ内のキャッシュ エンジンで使用されている WCCP のバージョン。
WCCP Client Information	クライアントの情報に関するフィールドを含むエリアのヘッダー。
IP Address	サービス グループ内のキャッシュ エンジンの IP アドレス。
Protocol Version	サービス グループ内のキャッシュ エンジンで使用されている WCCP のバージョン。
State	キャッシュ エンジンが正常に動作しているかどうかと、サービス グループ内のルータやその他のキャッシュ エンジンから認識できるかどうかを示します。
Initial Hash Info	ハッシュ バケット割り当ての初期状態。
Assigned Hash Info	ハッシュ バケット割り当ての現在の状態。
Hash Allotment	現在のキャッシュ エンジンに割り当てられているバケットのパーセンテージ。値およびパーセントが両方とも表示されます。
Packets Redirected	キャッシュ エンジンにリダイレクトされたパケットの数。

フィールド	説明
Connect Time	キャッシュ エンジンが Device に接続されていた時間（時間、分、秒）。
Bypassed Packets	バイパスされたパケット数。プロセスおよびCisco Express Forwardingは、Cisco IOS ソフトウェア内のスイッチング パスです。

show ipv6 wccp web-cache service

次に、サービスに関する情報（サービス定義およびその他サービスごとのすべての情報を含む）を表示する例を示します。

```
Device# show ipv6 wccp web-cache service

WCCP service information definition:
        Type:          Standard
        Id:            0
        Priority:      240
        Protocol:      6
        Options:       0x00000512
        --------
            Mask/Value sets: 1
            Value elements: 4
            Dst Ports: 80 0 0 0 0 0 0 0
```

show ipv6 wccp summary

次に、設定されているWCCPサービスおよびそれらの現在の状態のサマリーを表示する例を示します。

```
Device# show ipv6 wccp summary

WCCP version 2 enabled, 2 services
Service     Clients   Routers   Assign      Redirect   Bypass
-------     -------   -------   ------      --------   ------
Default routing table (Router Id: 2001:DB8:100::1):
web-cache   2         1         HASH        GRE        GRE
61          2         1         MASK        L2         L2
62          2         1         MASK        L2         L2
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *80 : show ipv6 wccp summary* フィールドの説明

フィールド	説明
Service	サービスの識別情報を示します。
Clients	WCCP サービスに参加しているキャッシュ エンジンの数を示します。

フィールド	説明
Device(s)	WCCP サービスに参加している Device の数を示します。
Assign	使用されたロードバランシング メソッドを示します。WCCP は、HASH 割り当てまたは MASK 割り当てを使用します。
Redirect	使用されたリダイレクション メソッドを示します。WCCP は、GRE または L2 を使用して、IP トラフィックをリダイレクトします。
Bypass	使用されたバイパス メソッドを示します。WCCP は GRE または L2 を使用してパケットを Device に返します。

関連コマンド

コマンド	説明
clearipv6wccp	WCCP を使用してリダイレクトされたパケットのカウンタをクリアします。
ipv6wccp	サービス グループに参加できるように、WCCP サービスのサポートをイネーブルにします。
ipv6wccpredirect	WCCP を使用して、発信インターフェイスまたは受信インターフェイスでパケットのリダイレクションをイネーブルにします。
showipv6interface	インターフェイスの IP 情報とステータスのサマリーを列挙します。
showipv6wccpglobalcounters	ソフトウェアで処理されるパケットのグローバル WCCP 情報を表示します。