



IP アドレッシング サービス コマンド

- [clear ipv6 access-list](#) (6 ページ)
- [clear ipv6 dhcp](#) (7 ページ)
- [clear ipv6 dhcp binding](#) (8 ページ)
- [clear ipv6 dhcp client](#) (10 ページ)
- [clear ipv6 dhcp conflict](#) (11 ページ)
- [clear ipv6 dhcp relay binding](#) (12 ページ)
- [clear ipv6 eigrp](#) (13 ページ)
- [clear ipv6 mfib counters](#) (14 ページ)
- [clear ipv6 mld counters](#) (15 ページ)
- [clear ipv6 mld traffic](#) (16 ページ)
- [clear ipv6 mtu](#) (17 ページ)
- [clear ipv6 multicast aaa authorization](#) (18 ページ)
- [clear ipv6 nd destination](#) (19 ページ)
- [clear ipv6 nd on-link prefix](#) (20 ページ)
- [clear ipv6 nd router](#) (21 ページ)
- [clear ipv6 neighbors](#) (22 ページ)
- [clear ipv6 ospf](#) (24 ページ)
- [clear ipv6 ospf counters](#) (25 ページ)
- [clear ipv6 ospf events](#) (27 ページ)
- [clear ipv6 pim reset](#) (28 ページ)
- [clear ipv6 pim topology](#) (29 ページ)
- [clear ipv6 pim traffic](#) (30 ページ)
- [clear ipv6 prefix-list](#) (31 ページ)
- [clear ipv6 rip](#) (33 ページ)
- [clear ipv6 route](#) (35 ページ)
- [clear ipv6 spd](#) (37 ページ)
- [fhrp delay](#) (38 ページ)
- [fhrp version vrrp v3](#) (39 ページ)
- [ip address dhcp](#) (40 ページ)

- ip address pool (DHCP) (44 ページ)
- ip address (45 ページ)
- ip wccp (48 ページ)
- ipv6 access-list (54 ページ)
- ipv6 address-validate (58 ページ)
- ipv6 cef (59 ページ)
- ipv6 cef accounting (61 ページ)
- ipv6 cef distributed (64 ページ)
- ipv6 cef load-sharing algorithm (66 ページ)
- ipv6 cef optimize neighbor resolution (68 ページ)
- ipv6 destination-guard policy (69 ページ)
- ipv6 dhcp-relay bulk-lease (70 ページ)
- ipv6 dhcp-relay option vpn (71 ページ)
- ipv6 dhcp-relay source-interface (72 ページ)
- ipv6 dhcp binding track ppp (73 ページ)
- ipv6 dhcp database (75 ページ)
- ipv6 dhcp iana-route-add (77 ページ)
- ipv6 dhcp iapd-route-add (78 ページ)
- **ipv6 dhcp-ldra** (79 ページ)
- ipv6 dhcp ping packets (80 ページ)
- ipv6 dhcp pool (81 ページ)
- ipv6 dhcp server vrf enable (84 ページ)
- ipv6 flow monitor (85 ページ)
- ipv6 general-prefix (86 ページ)
- ipv6 local policy route-map (88 ページ)
- ipv6 local pool (90 ページ)
- ipv6 mld snooping (92 ページ)
- ipv6 mld ssm-map enable (93 ページ)
- ipv6 mld state-limit (94 ページ)
- ipv6 multicast-routing (96 ページ)
- ipv6 multicast group-range (97 ページ)
- ipv6 multicast pim-passive-enable (99 ページ)
- ipv6 nd cache expire (100 ページ)
- ipv6 nd cache interface-limit (global) (102 ページ)
- ipv6 nd host mode strict (103 ページ)
- ipv6 nd na glean (104 ページ)
- ipv6 nd ns-interval (105 ページ)
- ipv6 nd nud retry (106 ページ)
- ipv6 nd reachable-time (108 ページ)
- ipv6 nd resolution data limit (109 ページ)
- ipv6 nd route-owner (110 ページ)

- [ipv6 neighbor](#) (111 ページ)
- [ipv6 ospf name-lookup](#) (113 ページ)
- [ipv6 pim](#) (114 ページ)
- [ipv6 pim accept-register](#) (115 ページ)
- [ipv6 pim allow-rp](#) (116 ページ)
- [ipv6 pim neighbor-filter list](#) (117 ページ)
- [ipv6 pim rp-address](#) (118 ページ)
- [ipv6 pim rp embedded](#) (121 ページ)
- [ipv6 pim spt-threshold infinity](#) (122 ページ)
- [ipv6 prefix-list](#) (123 ページ)
- [ipv6 source-guard attach-policy](#) (127 ページ)
- [ipv6 source-route](#) (128 ページ)
- [ipv6 spd mode](#) (130 ページ)
- [ipv6 spd queue max-threshold](#) (132 ページ)
- [ipv6 traffic interface-statistics](#) (133 ページ)
- [ipv6 unicast-routing](#) (134 ページ)
- [key chain](#) (135 ページ)
- [key-string](#) (認証) (136 ページ)
- [key](#) (137 ページ)
- [show ip ports all](#) (139 ページ)
- [show ip wccp](#) (141 ページ)
- [show ipv6 access-list](#) (156 ページ)
- [show ipv6 destination-guard policy](#) (159 ページ)
- [show ipv6 dhcp](#) (160 ページ)
- [show ipv6 dhcp binding](#) (161 ページ)
- [show ipv6 dhcp conflict](#) (164 ページ)
- [show ipv6 dhcp database](#) (165 ページ)
- [show ipv6 dhcp guard policy](#) (167 ページ)
- [show ipv6 dhcp interface](#) (169 ページ)
- [show ipv6 dhcp relay binding](#) (172 ページ)
- [show ipv6 eigrp events](#) (174 ページ)
- [show ipv6 eigrp interfaces](#) (176 ページ)
- [show ipv6 eigrp topology](#) (179 ページ)
- [show ipv6 eigrp traffic](#) (181 ページ)
- [show ipv6 general-prefix](#) (183 ページ)
- [show ipv6 interface](#) (185 ページ)
- [show ipv6 mfib](#) (194 ページ)
- [show ipv6 mld groups](#) (200 ページ)
- [show ipv6 mld interface](#) (203 ページ)
- [show ipv6 mld snooping](#) (206 ページ)
- [show ipv6 mld ssm-map](#) (208 ページ)

- [show ipv6 mld traffic \(210 ページ\)](#)
- [show ipv6 mrib client \(212 ページ\)](#)
- [show ipv6 mrib route \(214 ページ\)](#)
- [show ipv6 mroute \(217 ページ\)](#)
- [show ipv6 mtu \(222 ページ\)](#)
- [show ipv6 nd destination \(224 ページ\)](#)
- [show ipv6 nd on-link prefix \(226 ページ\)](#)
- [show ipv6 neighbors \(227 ページ\)](#)
- [show ipv6 ospf \(232 ページ\)](#)
- [show ipv6 ospf border-routers \(236 ページ\)](#)
- [show ipv6 ospf event \(238 ページ\)](#)
- [show ipv6 ospf graceful-restart \(241 ページ\)](#)
- [show ipv6 ospf interface \(243 ページ\)](#)
- [show ipv6 ospf request-list \(248 ページ\)](#)
- [show ipv6 ospf retransmission-list \(250 ページ\)](#)
- [show ipv6 ospf statistics \(252 ページ\)](#)
- [show ipv6 ospf summary-prefix \(254 ページ\)](#)
- [show ipv6 ospf timers rate-limit \(255 ページ\)](#)
- [show ipv6 ospf traffic \(256 ページ\)](#)
- [show ipv6 ospf virtual-links \(260 ページ\)](#)
- [show ipv6 pim anycast-RP \(262 ページ\)](#)
- [show ipv6 pim bsr \(263 ページ\)](#)
- [show ipv6 pim df \(266 ページ\)](#)
- [show ipv6 pim group-map \(268 ページ\)](#)
- [show ipv6 pim interface \(270 ページ\)](#)
- [show ipv6 pim join-prune statistic \(272 ページ\)](#)
- [show ipv6 pim limit \(274 ページ\)](#)
- [show ipv6 pim neighbor \(275 ページ\)](#)
- [show ipv6 pim range-list \(277 ページ\)](#)
- [show ipv6 pim topology \(279 ページ\)](#)
- [show ipv6 pim traffic \(282 ページ\)](#)
- [show ipv6 pim tunnel \(284 ページ\)](#)
- [show ipv6 policy \(286 ページ\)](#)
- [show ipv6 prefix-list \(287 ページ\)](#)
- [show ipv6 protocols \(290 ページ\)](#)
- [show ipv6 rip \(292 ページ\)](#)
- [show ipv6 routers \(298 ページ\)](#)
- [show ipv6 rpf \(302 ページ\)](#)
- [show ipv6 source-guard policy \(304 ページ\)](#)
- [show ipv6 spd \(305 ページ\)](#)
- [show ipv6 static \(306 ページ\)](#)

- [show ipv6 traffic](#) (310 ページ)
- [show key chain](#) (313 ページ)
- [show track](#) (314 ページ)
- [track](#) (316 ページ)
- [vrrp](#) (318 ページ)
- [vrrp description](#) (319 ページ)
- [vrrp preempt](#) (320 ページ)
- [vrrp priority](#) (322 ページ)
- [vrrp timers advertise](#) (323 ページ)
- [vrrs leader](#) (325 ページ)

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 **clear ipv6 access-list** コマンドを使用します。

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

構文の説明

<i>access-list-name</i>	(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 Fuji 16.9.2	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 access-list コマンドは、IPv6 固有である点を除いて、**clear ip access-list counters** コマンドに似ています。

access-list-name 引数なしで **clear ipv6 access-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。

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

関連コマンド

コマンド	説明
hardware statistics	ハードウェア統計情報の収集をイネーブルにします。
ipv6 access-list	IPv6 アクセスリストを定義し、IPv6 アクセスリスト コンフィギュレーション モードを開始します。
show ipv6 access-list	現在のすべての IPv6 アクセスリストの内容を表示します。

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 **clear ipv6 dhcp** 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 Fuji 16.9.2	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 dhcp 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。

```
# 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 **clear ipv6 dhcp binding** コマンドを使用します。

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

構文の説明		
	<i>ipv6-address</i>	(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 <i>vrf-name</i>	(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 Fuji 16.9.2	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 dhcp binding** 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 **clear ipv6 dhcp binding** コマンドを実行した場合に、削除されます。

clear ipv6 dhcp binding 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。**clear ipv6 dhcp binding** コマンドを *ipv6-address* 引数なしで使用すると、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** *vrf-name* キーワードと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。


```
# clear ipv6 dhcp binding
```

関連コマンド

Command	Description
show ipv6 dhcp binding	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 **clear ipv6 dhcp client** コマンドを使用します。

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

構文の説明	<i>interface-type interface-number</i>	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 (?) を使用してオンラインヘルプを参照してください。
-------	--	---

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 Fuji 16.9.2	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 dhcp client** 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 (ドメインネームシステム (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。

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

関連コマンド	Command	Description
	show ipv6 dhcp interface	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 **clear ipv6 dhcp conflict** 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。
	<i>ipv6-address</i>	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 <i>vrf-name</i>	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 Fuji 16.9.2	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せん。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 vrf-name キーワードと引数を指定すると、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。

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

関連コマンド	コマンド	説明
	show ipv6 dhcp conflict	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 **clear ipv6 dhcp relay binding** コマンドを使用します。

```
clear ipv6 dhcp relay binding vrf vrf-name *ipv6-address ipv6-prefix
```

```
clear ipv6 dhcp relay binding vrf vrf-name *ipv6-prefix
```

構文の説明	vrf <i>vrf-name</i>	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。
	<i>ipv6-address</i>	DHCPv6 アドレス。
	<i>ipv6-prefix</i>	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 Fuji 16.9.2 Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

clear ipv6 dhcp relay binding 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。

```
# 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。

```
# 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 ipv6 dhcp 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) からエントリーを削除するには、特権 EXEC モードで **clear ipv6 eigrp** 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		
	<i>as-number</i>	(任意) 自律システム番号。
	neighbor	(任意) ネイバルルータのエントリーを削除します。
	<i>ipv6-address</i>	(任意) 隣接ルータの IPv6 アドレス。
	<i>interface-type</i>	(任意) ネイバルルータのインターフェイスタイプ。
	<i>interface-number</i>	(任意) ネイバル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 Fuji 16.9.2	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 エントリーのすべての 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 **clear ipv6 eigrp** 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ーをクリアするには *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***ipv6-address* キーワードと引数、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。

```
# 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 **clear ipv6 mfib counters** コマンドを使用します。

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

構文の説明	vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
	<i>group-name</i> <i>group-address</i>	(任意) マルチキャストグループのIPv6アドレスまたは名前。
	<i>source-address</i> <i>source-name</i>	(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 Fuji 16.9.2	このコマンドが導入されました。

clear ipv6 mfib counters 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。

- **show ipv6 mfib**
- **show ipv6 mfib active**
- **show ipv6 mfib count**
- **show ipv6 mfib interface**
- **show ipv6 mfib summary**

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。

```
# 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 **clear ipv6 mld counters** 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 (?) を使用してオンラインヘルプを参照してください。

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 Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン 受信した参加および脱退の数を追跡する MLD カウンタをクリアするには、**clear ipv6 mld counters** コマンドを使用します。オプションの *interface-type* 引数を省略した場合、**clear ipv6 mld counters** 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。

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

関連コマンド	コマンド	説明
	show ipv6 mld interface	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 **clear ipv6 mld traffic** 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 Fuji 16.9.2	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 mld traffic** 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。

```
# clear ipv6 mld traffic
```

コマンド	説明
show ipv6 mld traffic	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 **clear ipv6 mtu** コマンドを使用します。

clear ipv6 mtu

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドデフォルト

メッセージは、MTU キャッシュから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 Fuji 16.9.2	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、**clear ipv6 mtu** 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。

```
# clear ipv6 mtu
```

関連コマンド

コマンド	説明
ipv6 flowset	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 **clear ipv6 multicast aaa authorization** コマンドを使用します。

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

構文の説明	<i>interface-type interface-number</i>	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 (?) を使用してオンラインヘルプを参照してください。
-------	--	---

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 Fuji 16.9.2	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 **clear ipv6 multicast aaa authorization** 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。

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

関連コマンド	コマンド	説明
	aaa authorization multicast default	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

vr <i>vrf-name</i>	(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 Fuji 16.9.2	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 ホストモードの宛先キャッシュのエントリをクリアします。**vr** *vrf-name* キーワードと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 ホストモードの宛先キャッシュのエントリをクリアする例を示します。

```
# 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 <i>vrf-name</i>	(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 Fuji 16.9.2	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 vrf-name** キーワードと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。

```
# 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

ルータアダプタイズメント (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 <i>vrf-name</i>	(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 Fuji 16.9.2	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 vrf-name** キーワードと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。

```
# 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 **clear ipv6 neighbors** 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 <i>type number</i>	(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 <i>ipv6-address</i>	(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。	
<i>table-name</i>	(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 Fuji 16.9.2	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。

```
# 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。

```
# 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。

```
# 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
ipv6 neighbor	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。
show ipv6 neighbors	IPv6 ネイバー探索キャッシュ情報を表示します。

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 **clear ipv6 ospf** コマンドを使用します。

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

構文の説明		
	<i>process-id</i>	(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 Fuji 16.9.2	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 **clear ipv6 ospf** 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 **clear ipv6 ospf** 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 データベースをクリアせずに SPF アルゴリズムを起動する例を示します。

```
# 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 **clear ipv6 ospf** コマンドを使用します。

clear ipv6 ospf [*process-id*] **counters** [**neighbor** [*neighbor-interface*neighbor-id]]

構文の説明

<i>process-id</i>	(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。
<i>neighbor-interface</i>	(任意) ネイバーインターフェイス。
<i>neighbor-id</i>	(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 Fuji 16.9.2	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せん。

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。

```
# 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。

clear ipv6 ospf counters

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

次の例は、**clear ipv6 ospf counters neighbor s19/0** 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。

```
# 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
show ipv6 ospf neighbor	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 **clear ipv6 ospf events** コマンドを使用します。

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

構文の説明

<i>process-id</i>	(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 Fuji 16.9.2	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。

```
# 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 **clear ipv6 pim reset** コマンドを使用します。

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

構文の説明

vrf <i>vrf-name</i>	(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 Fuji 16.9.2	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 pim reset 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。このプロセスは MRIB を強制的に再同期します。



注意

clear ipv6 pim reset 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。**clear ipv6 pim reset** 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。

```
# 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 **clear ipv6 pim topology** 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 <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
	<i>group-name</i> <i>group-address</i>	(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 Fuji 16.9.2	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。

```
# 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 **clear ipv6 pim traffic** 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 Fuji 16.9.2	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 vrf-name** キーワードと引数を使用すると、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。

```
# 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 **clear ipv6 prefix-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	
<i>prefix-list-name</i>	(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。
<i>ipv6-prefix</i>	(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。
<i>/ prefix-length</i>	(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 Fuji 16.9.2	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 prefix-list** コマンドは、IPv6 固有である点を除いて、**clear ip prefix-list** コマンドに似ています。

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

次の例では、ネットワークマスク 2001:0DB8::/35 と一致する、**first_list** という名前の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します。

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

関連コマンド	コマンド	説明
	ipv6 prefix-list	IPv6 プレフィックスリストのエントリを作成します。
	ipv6 prefix-list sequence-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
show ipv6 prefix-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削除するには、特権 EXEC モードで **clear ipv6 rip** 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	
<i>name</i>	(任意) IPv6 RIP プロセスの名前。
vrf <i>vrf-name</i>	(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 Fuji 16.9.2	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、**show ipv6 rip** 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、**clear ipv6 rip 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。

```
# 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。

```
# 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
	debug ipv6 rip	IPv6 RIP ルーティングテーブルの現在の内容を表示します。

コマンド	説明
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 rip	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削除するには、特権 EXEC モードで **clear ipv6 route** コマンドを使用します。

clear ipv6 route *ipv6-address*/*ipv6-prefix/prefix-length* | *

構文の説明	
<i>ipv6-address</i>	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。
<i>ipv6-prefix</i>	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。
<i>/ prefix-length</i>	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 Fuji 16.9.2	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 route** コマンドは、IPv6 固有である点を除いて、**clear ip route** コマンドに似ています。

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（宛先単位の最大伝送ユニット（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。

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

関連コマンド	コマンド	説明
	ipv6 route	スタティック IPv6 ルートを確立します。

コマンド	説明
show ipv6 route	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破棄（SPD）の状態遷移をクリアするには、特権 EXEC モードで **clear ipv6 spd** 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 Fuji 16.9.2	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 spd** 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。

```
# clear ipv6 spd
```

fhrp delay

First Hop Redundancy Protocol (FHRP) クライアントの初期化の遅延時間を指定するには、インターフェイス コンフィギュレーション モードで **fhrp delay** コマンドを使用します。指定した時間を削除するには、このコマンドの **no** 形式を使用します。

```
fhrp delay {[minimum] [reload] seconds}
no fhrp delay {[minimum] [reload] seconds}
```

構文の説明

minimum	(任意) インターフェイスが使用可能になった後の遅延時間を設定します。
reload	(任意) デバイスのリロード後の遅延時間を設定します。
<i>seconds</i>	秒単位の遅延時間。範囲は 0 ~ 3600 です。

コマンド デフォルト なし

コマンド モード インターフェイス コンフィギュレーション (config-if)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

例
次に、FHRP クライアントの初期化の遅延期間を指定する例を示します。

```
Device(config-if)# fhrp delay minimum 90
```

関連コマンド

コマンド	説明
show fhrp	ファーストホップ冗長性プロトコル (FHRP) の情報を表示します。

fhrp version vrrp v3

Virtual Router Redundancy Protocol バージョン 3 (VRRPv3) と Virtual Router Redundancy Service (VRRS) をデバイスで有効にするには、グローバル コンフィギュレーション モードで **fhrp version vrrp v3** コマンドを使用します。VRRPv3 と VRRS の設定機能をデバイスで無効にするには、このコマンドの **no** 形式を使用します。

fhrp version vrrp v3
no fhrp version vrrp v3

構文の説明 このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト VRRPv3 と VRRS 設定はデバイスで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 (config)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン VRRPv3 が使用中の場合、VRRP バージョン 2 (VRRPv2) は使用できません。

例

次の例では、トラッキングプロセスは、VRRPv3 グループを使用して IPv6 オブジェクトの状態を追跡するように設定されています。ギガビットイーサネットインターフェイス 0/0/0 の VRRP は、VRRPv3 グループで IPv6 オブジェクトに何らかの変更が生じた場合には通知されるように、トラッキングプロセスに登録します。シリアル インターフェイス VRRPv3 の IPv6 オブジェクトステータスがダウンになると、VRRP グループのプライオリティは 20 だけ引き下げられます。

```
Device(config)# fhrp version vrrp v3
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# vrrp 1 address-family ipv6
Device(config-if-vrrp)# track 1 decrement 20
```

関連コマンド	コマンド	説明
	track (VRRP)	VRRPv3 グループを使用したオブジェクトの追跡を有効にします。

ip address dhcp

DHCP からインターフェイスの IP アドレスを取得するには、インターフェイス コンフィギュレーション モードで **ip address dhcp** コマンドを使用します。取得されたいずれかの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。

```
ip address dhcp [client-id interface-type number] [hostname hostname]
no ip address dhcp [client-id interface-type number] [hostname hostname]
```

構文の説明

client-id	(任意) クライアント ID を指定します。デフォルトでは、クライアント識別子は ASCII 値です。 client-id interface-type number オプションは、クライアント識別子を、指定されたインターフェイスの 16 進数 MAC アドレスに設定します。
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ます。
number	(任意) インターフェイスまたはサブインターフェイスの番号です。ネットワーク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。
hostname	(任意) ホスト名を指定します。
hostname	(任意) ホスト名を DHCP オプション 12 フィールドに配置します。この名前は、グローバル コンフィギュレーション モードで入力されたホスト名と同じにする必要はありません。

コマンド デフォルト

ホスト名は、デバイスのグローバル コンフィギュレーション ホスト名です。クライアント識別子は ASCII 値です。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

ip address dhcp コマンドを使用すると、インターフェイスは DHCP プロトコルを使用して IP アドレスを動的に学習できます。これはインターネット サービス プロバイダー (ISP) に動的に接続するイーサネット インターフェイスで特に役立ちます。このインターフェイスにダイナミック アドレスを割り当てると、同インターフェイスを使用して、Cisco IOS ネットワーク アドレス変換 (NAT) のポート アドレス変換 (PAT) で、デバイスに接続済みの個別に処理されたネットワークにインターネット アクセスを提供できます。

また **ip address dhcp** コマンドは、ATM ポイントツーポイント インターフェイスと連動し、どのカプセル化方式でも受け入れます。ただし、ATM マルチポイント インターフェイスの場合、

protocol ip inarp インターフェイス コンフィギュレーション コマンドで Inverse ARP を指定し、**aa15snap** カプセル化タイプのみを使用する必要があります。

一部の ISP の場合、DHCPDISCOVER メッセージに、特定のホスト名と、インターフェイスの MAC アドレスであるクライアント識別子を含める必要があります。**ip address dhcp client-id interface-type number hostname hostname** コマンドは、*interface-type* が、このコマンドが設定されたイーサネット インターフェイスであり、*interface-type number* が ISP によって提供されたホスト名である場合に最も一般的に使用されます。

クライアント識別子 (DHCP オプション 61) には、16 進数または ASCII 値を使用できます。デフォルトでは、クライアント識別子は ASCII 値です。**client-id interface-type number** オプションは、デフォルトの値を上書きし、指定されたインターフェイスの 16 進数 MAC アドレスの使用を強制します。

DHCP サーバから IP アドレスを取得するようシスコ デバイスが設定されている場合、デバイスは、ネットワークの DHCP サーバにデバイスに関する情報を提供する DHCPDISCOVER メッセージを送信します。

ip address dhcp コマンドを使用する場合、オプションキーワードの有無にかかわらず、DHCP オプション 12 フィールド (ホスト名 オプション) が DISCOVER メッセージに含まれます。デフォルトでは、オプション 12 で指定されたホスト名は、デバイスのグローバル コンフィギュレーション ホスト名になります。ただし、**ip address dhcp hostname hostname** コマンドを使用して、デバイスのグローバル コンフィギュレーション ホスト名ではない別の名前を DHCP オプション 12 フィールドに入力することもできます。

no ip address dhcp コマンドは、取得済みの IP アドレスを削除して、DHCPRELEASE メッセージを送信します。

DHCP サーバで必要なものを判別するため、さまざまな設定を試行しなければならない場合があります。下の表に、使用可能なコンフィギュレーション方式と、各方式の DISCOVER メッセージに含まれる情報を示します。

表 1: コンフィギュレーション方式と生成される DISCOVER メッセージの内容

コンフィギュレーション方式	DISCOVER メッセージの内容
ip address dhcp	DISCOVER メッセージのクライアント ID フィールドには「cisco-mac-address-Eth1」が含まれます。 <i>mac-address</i> は、イーサネット 1 インターフェイスの MAC アドレスで、オプション 12 フィールドのデバイスのデフォルト ホスト名を含んでいます。
ip address dhcp hostname hostname	DISCOVER メッセージのクライアント ID フィールドには「cisco-mac-address-Eth1」が含まれます。 <i>mac-address</i> は、イーサネット 1 インターフェイスの MAC アドレスで、オプション 12 フィールドの <i>hostname</i> を含んでいます。

コンフィギュレーション方式	DISCOVER メッセージの内容
ip address dhcp client-id ethernet 1	DISCOVER メッセージは、クライアント ID フィールドにイーサネット 1 インターフェイスの MAC アドレスを含んでおり、オプション 12 フィールドにデバイスのデフォルト ホスト名を含んでいます。
ip address dhcp client-id ethernet 1 hostname hostname	DISCOVER メッセージは、クライアント ID フィールドにイーサネット 1 インターフェイスの MAC アドレスを含んでおり、オプション 12 フィールドに <i>hostname</i> を含んでいます。

例

次の例では、**ip address dhcp** コマンドがイーサネット インターフェイス 1 に入力されます。次の例のように設定されたデバイスによって送信された DISCOVER メッセージには、クライアント ID フィールドの「**cisco- mac-address -Eth1**」と、オプション 12 フィールドの値 **abc** が含まれます。

```
hostname abc
!
interface GigabitEthernet 1/0/1
 ip address dhcp
```

次の例のように設定されたデバイスによって送信された DISCOVER メッセージには、クライアント ID フィールドの「**cisco- mac-address -Eth1**」と、オプション 12 フィールドの値 **def** が含まれます。

```
hostname abc
!
interface GigabitEthernet 1/0/1
 ip address dhcp hostname def
```

次の例のように設定されたデバイスによって送信された DISCOVER メッセージには、クライアント ID フィールドのイーサネット インターフェイス 1 の MAC アドレスと、オプション 12 フィールドの値 **abc** が含まれます。

```
hostname abc
!
interface Ethernet 1
 ip address dhcp client-id GigabitEthernet 1/0/1
```

次の例のように設定されたデバイスによって送信された DISCOVER メッセージには、クライアント ID フィールドのイーサネット インターフェイス 1 の MAC アドレスと、オプション 12 フィールドの値 **def** が含まれます。

```
hostname abc
!
interface Ethernet 1
 ip address dhcp client-id GigabitEthernet 1/0/1 hostname def
```

関連コマンド

コマンド	説明
ip dhcp pool	Cisco IOS DHCP サーバに DHCP アドレス プールを設定し、DHCP プール コンフィギュレーション モードを開始します。

ip address pool (DHCP)

Dynamic Host Configuration Protocol (DHCP) に IP Control Protocol (IPCP) ネゴシエーションからサブネットが入力されるときに、インターフェイスの IP アドレスが自動設定されるようにするには、インターフェイス コンフィギュレーション モードで **ip address pool** コマンドを使用します。インターフェイスの IP アドレスの自動設定を無効にするには、このコマンドの **no** 形式を使用します。

ip address pool name

no ip address pool

構文の説明

<i>name</i>	DHCP プールの名前。インターフェイスの IP アドレスは、 <i>name</i> で指定された DHCP プールから自動設定されます。
-------------	--

コマンド デフォルト

IP アドレスのプーリングは無効になっています。

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 Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

デバイスの DHCP プールによって処理する必要のある LAN に接続されている DHCP クライアントが存在する場合、このコマンドを使用して LAN インターフェイスの IP アドレスを自動設定します。DHCP プールは、IPCP サブネット ネゴシエーションによってサブネットを動的に取得します。

例

次の例では、GigabitEthernet インターフェイス 1/0/1 の IP アドレスが abc という名前のアドレス プールから自動設定されるように指定します。

```
ip dhcp pool abc
  import all
  origin ipcp
!
interface GigabitEthernet 1/0/1
  ip address pool abc
```

関連コマンド

コマンド	説明
show ip interface	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。

ip address

インターフェイスのプライマリまたはセカンダリ IP アドレスを設定するには、インターフェイス コンフィギュレーション モードで **ip address** コマンドを使用します。IP アドレスを削除するか、IP 処理を無効にするには、このコマンドの **no** 形式を使用します。

```
ip address ip-address mask [secondary [vrf vrf-name ]]
no ip address ip-address mask [secondary [vrf vrf-name ]]
```

構文の説明

<i>ip-address</i>	IP アドレス。
<i>mask</i>	関連する IP サブネットのマスク。
secondary	(任意) 設定されたアドレスをセカンダリ IP アドレスに指定します。このキーワードが省略された場合、設定されたアドレスはプライマリ IP アドレスになります。 (注) セカンダリ アドレスが vrf のキーワードでの VRF テーブルの設定に使用される場合には、 vrf キーワードも指定する必要があります。
vrf	(任意) VRF テーブルの名前 <i>vrf-name</i> 引数は、入力インターフェイスの VRF 名を指定します。

コマンド デフォルト

IP アドレスはインターフェイスに定義されません。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

インターフェイスには、1 つのプライマリ IP アドレスと複数のセカンダリ IP アドレスを設定できます。Cisco IOS ソフトウェアにより生成されるパケットは、必ずプライマリ IP アドレスを使用します。そのため、セグメントのすべてのデバイスとアクセスサーバは、同じプライマリ ネットワーク番号を共有する必要があります。

ホストは、Internet Control Message Protocol (ICMP) マスク要求メッセージを使用して、サブネットマスクを判別できます。デバイスは、ICMP マスク応答メッセージでこの要求に応答できます。

no ip address コマンドを使用して IP アドレスを削除することにより、特定のインターフェイス上の IP 処理を無効にできます。ソフトウェアが、その IP アドレスのいずれかを使用する別のホストを検出すると、コンソールにエラー メッセージを出力します。

オプションの **secondary** キーワードを使用すると、セカンダリ アドレスを無制限に指定できます。システムがセカンダリの送信元アドレスのルーティングの更新以外にデータグラムを生成

しないということを除けば、セカンダリ アドレスはプライマリ アドレスのように処理されます。IP ブロードキャストおよび Address Resolution Protocol (ARP) 要求は、IP ルーティング テーブルのインターフェイス ルートのように、正しく処理されます。

セカンダリ IP アドレスは、さまざまな状況で使用できます。次に、一般的な使用状況を示します。

- 特定のネットワーク セグメントに十分なホスト アドレスがない場合。たとえば、サブネット化により、論理サブネットあたり最大 254 のホストを使用できますが、1 つの物理サブネットでは、300 のホスト アドレスが必要になります。デバイスまたはアクセス サーバでセカンダリ IP アドレスを使用すると、2 つの論理サブネットで 1 つの物理サブネットを使用できます。
- レベル 2 ブリッジを使用して構築された旧式ネットワークがたくさんある場合。セカンダリ アドレスは、慎重に使用することで、サブネット化されたデバイスベース ネットワークへの移行に役立ちます。旧式のブリッジ セグメントのデバイスでは、そのセグメントに複数のサブネットがあることを簡単に認識させることができます。
- 1 つのネットワークの 2 つのサブネットは、別の方法で、別のネットワークにより分離できる場合があります。サブネットが使用中の場合、この状況は許可されません。このような場合、最初のネットワークは、セカンダリ アドレスを使用している 2 番目のネットワークの上に拡張されます。つまり、上の階層となります。



- (注)
- ネットワーク セグメント上のすべてのデバイスがセカンダリ アドレスを使用した場合、同一のセグメント上にある他のデバイスも、同一のネットワークまたはサブネットからセカンダリ アドレスを使用しなければなりません。ネットワーク セグメント上のセカンダリ アドレスの使用に矛盾があると、ただちにルーティング ループが引き起こされる可能性があります。
 - Open Shortest Path First (OSPF) アルゴリズムを使用してルーティングする場合は、インターフェイスのすべてのセカンダリ アドレスがプライマリ アドレスと同じ OSPF エリアにあることを確認してください。
 - セカンダリ IP アドレスを設定する場合は、CPU 使用率が高くないように、**no ip redirects** コマンドを入力して ICMP リダイレクト メッセージの送信を無効にする必要があります。

例

次の例では、192.108.1.27 がプライマリ アドレスで、192.31.7.17 が GigabitEthernet インターフェイス 1/0/1 のセカンダリ アドレスです。

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 192.108.1.27 255.255.255.0
Device(config-if)# ip address 192.31.7.17 255.255.255.0 secondary
```

関連コマンド

Command	Description
match ip route-source	送信元 IP アドレスを、VRF で接続されたルートに基づいて設定された必要なルート マップに一致するように指定します。
route-map	1 つのルーティング プロトコルから他のルーティング プロトコルへのルート を再配布するか、またはポリシー ルーティングを有効にするための条件を定義します。
set vrf	ポリシーベース ルーティング VRF の選択のために、ルート マップ内で VPN VRF 選択を有効にします。
show ip arp	SLIP アドレスが固定 ARP テーブル エントリとして表示される ARP キャッシュを表示します。
show ip interface	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 route-map	静的ルートマップと動的ルートマップを表示します。

ip wccp

サービスグループに参加できるように、指定した Web Cache Communication Protocol (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 **ip wccp** 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。

```
ip 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 ip 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 <i>vrf-name</i>	(任意) サービスグループに関連付ける Virtual Routing and Forwarding インスタンス (VRF) を指定します。
web-cache	Web キャッシュ サービスを指定します (WCCP バージョン 1 とバージョン 2)。 (注) Web キャッシュはサービスの 1 つとしてカウントされます。サービスの最大数 (<i>service-number</i> 引数で割り当てられたサービスを含む) は 256 です。
<i>service-number</i>	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) キャッシュクラスターで Cisco Cache Engine が使用されている場合、リバースプロキシサービスは値 99 で指定されます。
service-list <i>service-access-list</i>	(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 <i>multicast-address</i>	(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、デバイス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。 <i>access-list</i> 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。 <i>access-list</i> 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。 <i>password</i> 引数の長さは最大 8 文字です。

コマンド デフォルト WCCP サービスがデバイスでイネーブルにされていません。

コマンド モード グローバル コンフィギュレーション (config)

コマンド履歴

リリース	変更内容
	このコマンドが導入されました。
Cisco IOS XE Bengaluru 17.6.1	vrf キーワードと <i>vrf-name</i> 引数のペアが追加されました。

使用上のガイドライン

シスコ エクスプレス フォワーディング スイッチングがイネーブルのとき、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、**ip wccp web-cache redirect out** コマンドを指定します。キャッシュに面するデバイス インターフェイスで **ip wccp redirect exclude in** 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、指定され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イネーブルまたはディセーブルにするようデバイスに指示します。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、デバイスはサービス グループの確立に参加できます。



(注) すべての WCCP パラメータを単一の IP WCCP コマンドに含める必要があります。例: **ip wccp 61 redirect-list 10 password password**。

vrf vrf-name キーワードと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。

no ip wccp コマンドが入力されると、デバイスはサービスグループへの参加を終了し、引き続きサービスが設定されているインターフェイスがなければ領域の割り当てを解除し、他のサービスが設定されていない場合は 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。

ip wccp [vrf vrf-name] {web-cache | service-number} group-address multicast-address

デバイスと連動するマルチキャストアドレス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デバイスに指示します。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。

ip wccp [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デバイスに指示します。*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 によるデバイスと 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。

ip wccp [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デバイスに指示します。*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) **ip wccp {web-cache | service-number} group-list** コマンドの構文は、**ip wccp {web-cache | service-number} group-listen** コマンドと似ていますが、これらはまったく別のコマンドです。**ip wccp group-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。

ip wccp [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デバイスに指示します。この形式のコマンドを使用すると、デバイス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。デバイス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。

ip wccp service-number service-list service-access-list mode closed

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、中間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。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には、**service-list** キーワードと *service-access-list* 引数を使用します。

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> enable
Device# configure terminal
Device(config)# ip multicast-routing
Device(config)# ip wccp 99 group-address 239.0.0.0
```

```
Device(config)# interface ethernet 0
Device(config-if)# ip 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> enable
Device# configure terminal
Device(config)# access-list 100 deny ip any host 10.168.196.51
Device(config)# access-list 100 permit ip any any
Device(config)# ip wccp web-cache redirect-list 100
Device(config)# interface ethernet 0
Device(config-if)# ip 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> enable
Device# configure terminal
Device(config)# ip wccp web-cache
Device(config)# ip wccp check acl outbound
Device(config)# interface fastethernet0/0
Device(config-if)# ip access-group 10 out
Device(config-if)# ip 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> enable
Device# configure terminal
Device(config)# ip wccp 99 service-list access1 mode closed
```



- (注)
- 複数のパラメータが必要な場合、**ip wccp [vrf vrf-name] web-cache | service-number** の下のすべてのパラメータを、1つのコマンドとして設定する必要があります。
 - 異なるパラメータを指定してコマンドを再発行すると、既存のパラメータが削除され、新しいパラメータが設定されます。

次に、複数のパラメータを 1つのコマンドとして設定する例を示します。

```
Device> enable
Device# configure terminal
```

```
Device(config)# ip wccp 61 group-address 10.0.0.1 password 0 password mode closed  
redirect-list 121
```

関連コマンド

コマンド	説明
ip wccp check services all	すべての WCCP サービスをイネーブルにします。
ip wccp group listen	デバイスでインターフェイスを設定して、WCCP の IP マルチキャストパケットの受信をイネーブルまたはディセーブルにします。
ip wccp redirect exclude in	インターフェイスでのリダイレクトの除外をイネーブルにします。
ip wccp redirect out	発信方向のインターフェイスにリダイレクションを設定します。
ip wccp version	デバイスで使用する WCCP のバージョンを指定します。
show ip wccp	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 **ipv6 access-list** コマンドを使用します。アクセス リストを削除するには、このコマンドの **no** 形式を使用します。

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

構文の説明

<i>access-list-name</i>	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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 access-list コマンドは、IPv6 固有である点を除いて、**ip access-list** コマンドに似ています。

標準的な IPv6 ACL 機能は、送信元アドレスと宛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 **ipv6 access-list** コマンドを使用することで定義され、そ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** コマンドおよび **permit** コマンドを使用することで設定されます。**ipv6 access-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 **ipv6 access-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) IPv6 ACL にはそれぞれ、最後に一致した条件として、暗黙の **permit icmp any any nd-na** ステートメント、**permit icmp any any nd-ns** ステートメント、および **deny ipv6 any any** ステートメントがあります（前の 2 つの一致条件は、ICMPv6 ネイバー探索を許可します）。1 つの IPv6 ACL には、暗黙の **deny ipv6 any any** ステートメントを有効にするために少なくとも 1 つのエントリが含まれ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 **ipv6 traffic-filter** インターフェイスコンフィギュレーションコマンドを使用します。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、**ipv6 access-class** ラインコンフィギュレーションコマンドを使用します。



- (注) **ipv6 traffic-filter** コマンドでインターフェイスに適用される 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）（**ipv6 pim bsr candidate rp** コマンドを参照）または静的 RP（**ipv6 pim rp-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 番目のエントリは、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 **permit any any** ステートメントおよび **deny any any** 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 **deny any any** 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（ネイバー探索プロトコルに関連付けられたパケットなど）のフィルタリングを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、**permit any any** 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先アドレスのいずれかとしてリンクローカルアドレスを持つIPv6 パケットを別のネットワークに転送しません（パケットの送信元インターフェイスは、パケットの宛先インターフェイスとは異なります）。

関連コマンド

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

ipv6 address-validate

IPv6 アドレス検証をイネーブルにするには、グローバル コンフィギュレーション モードで **ipv6 address-validate** を使用します。IPv6 アドレス検証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 address-validate
no ipv6 address-validate

コマンド デフォルト このコマンドは、デフォルトでイネーブルになっています。

コマンド モード グローバル コンフィギュレーション (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	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 address-validate** コマンドは、割り当てられた IPv6 アドレスのインターフェイス識別子が RFC5453 で規定されている予約済み IPv6 インターフェイス識別子の範囲に含まれていないかどうかを検証するために使用します。割り当てられた IPv6 アドレスのインターフェイス識別子が予約済みの範囲に含まれている場合は、新しい IPv6 アドレスが割り当てられます。

検証されるのは、自動設定されたアドレスと DHCPv6 によって設定されたアドレスのみです。



(注) **no ipv6-address validate** コマンドを使用すると、IPv6 アドレス検証がディセーブルになり、予約済み IPv6 インターフェイス識別子の範囲に含まれるインターフェイス識別子を使用した IPv6 アドレスの割り当てが可能になります。このコマンドを使用することは推奨しません。

この **ipv6-address validate** コマンドの構文を完成させるために CLI ヘルプ (?) を使用する場合は、コマンドの 8 文字以上を入力する必要があります。入力が 8 文字未満だと、コマンドはインターフェイス コンフィギュレーション モードの **no ipv6 address** コマンドと競合します。

例

次に、IPv6 アドレス検証が **no ipv6-address validate** コマンドを使用してディセーブルにされた場合に再度イネーブルにする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 address-validate
```

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 **ipv6 cef** 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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 cef コマンドは、IPv6 固有である点を除いて、**ip cef** コマンドに似ています。

ipv6 cef 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) **ipv6 cef** コマンドはインターフェイス コンフィギュレーションモードで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) **ipv6 cef** グローバル コンフィギュレーション コマンドを使用して Cisco Express Forwarding for IPv6 を有効にする前に、**ip cef** グローバル コンフィギュレーション コマンドを使用して Cisco Express Forwarding for IPv4 を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、同じメモリ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 の動作を上でグローバルに有効にする例を示します。

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

関連コマンド

コマンド	説明
ip route-cache	IP ルーティングの高速スイッチング キャッシュの使用を制御します。
ipv6 cef accounting	Cisco Express Forwarding for IPv6 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。
ipv6 cef distributed	IPv6 での分散型シスコ エクスプレス フォワーディングをイネーブルにします。
show cef	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。
show ipv6 cef	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 モードまたはインターフェイス コンフィギュレーション モードで **ipv6 cef accounting** コマンドを使用します。Cisco Express Forwarding for IPv6 のネットワーク アカウンティングを無効にするには、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

<i>accounting-types</i>	<p><i>accounting-types</i> 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。</p> <ul style="list-style-type: none"> • 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	<p>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。 <i>accounting-types</i> 引数を参照してください。</p>
external	<p>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。</p>
internal	<p>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。</p>

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 (config)

インターフェイス コンフィギュレーション (config-if)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 cef accounting コマンドは、IPv6 固有である点を除いて、**ip cef accounting** コマンドに似ています。

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。

ipv6 cef accounting 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。**show ipv6 cef 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。**ipv6 cef accounting** 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使用する場合、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 **show ipv6 cef detail** コマンドを介して表示されます。

宛先ごとのロード 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、バ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 **ipv6 cef accounting** 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、**show ipv6 cef prefix internal** コマンドを入力します。

例

次に、直接接続されたネクストホップを持つプレフィックスに 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。

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

関連コマンド

Command	Description
ip cef accounting	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。
show cef	パケットに関する情報を表示します。 forwarded by Cisco Express Forwarding.
show ipv6 cef	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 **ipv6 cef distributed** 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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 cef distributed コマンドは、IPv6 固有である点を除いて、**ip cef distributed** コマンドに似ています。

ipv6 cef distributed 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、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用してルータ上に IPv6 ユニキャスト データグラムをグローバルに設定し、**ipv6 address** インターフェイス コンフィギュレーション コマンド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、**ip cef distributed** グローバル コンフィギュレーション コマンドを使用して Distributed Cisco Express Forwarding for IPv6 を有効にする前に、**ipv6 cef distributed** グローバル コンフィギュレーション コマンドを使用して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。

```
(config)# ipv6 cef distributed
```

関連コマンド

コマンド	説明
ip route-cache	IP ルーティングの高速スイッチングキャッシュの使用を制御します。
show ipv6 cef	IPv6 FIB 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 **ipv6 cef load-sharing algorithm** 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]
no ipv6 cef load-sharing algorithm

構文の説明

original	送信元および宛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。
<i>id</i>	(任意) 16 進数形式の固定識別子。

コマンド デフォルト

ユニバーサル ロードバランシング アルゴリズムがデフォルトで選択されています。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、デバイスは固有 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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 cef load-sharing algorithm コマンドは、IPv6 固有である点を除いて、**ip cef load-sharing algorithm** コマンドに似ています。

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デバイスは送信元アドレスと宛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。

例

次に、Cisco Express Forwarding の IPv6 用の元の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。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 cef load-sharing algorithm original
```

関連コマンド

コマンド	説明
ip cef load-sharing algorithm	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 **ipv6 cef optimize neighbor resolution** 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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 cef optimize neighbor resolution コマンドは、IPv6 固有である点を除いて、**ip cef optimize neighbor resolution** コマンドに非常に似ています。

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。

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

関連コマンド

コマンド	説明
ip cef optimize neighbor resolution	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 **ipv6 destination-guard policy** コマンドを使用します。宛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	<i>policy-name</i> (任意) 宛先ガードポリシーの名前。
-------	---------------------------------------

コマンド デフォルト 宛先ガード 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 (config)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	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。宛先ガード ポリシーは、宛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、宛先ガード ポリシーの名前を定義する例を示します。

```
(config)#ipv6 destination-guard policy policy1
```

関連コマンド	コマンド	説明
	show ipv6 destination-guard policy	宛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 **ipv6 dhcp-relay bulk-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。
<i>seconds</i>	(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。
<i>number</i>	(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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 **ipv6 dhcp-relay bulk-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、**ipv6 dhcp-relay bulk-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。

```
(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 option 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 認識型機能はデバイス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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 dhcp-relay option vpn コマンドは DHCPv6 リレーの VRF 認識型機能をデバイス上でグローバルに有効にすることができます。**ipv6 dhcp relay option vpn** 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 **ipv6 dhcp-relay option vpn** コマンドをオーバーライドします。

例

次に、DHCPv6 リレーの VRF 認識型機能をデバイス上でグローバルに有効にする例を示します。

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

関連コマンド

コマンド	説明
ipv6 dhcp relay option vpn	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 **ipv6 dhcp-relay source-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

<i>interface-type</i> <i>interface-number</i>	(任意) 宛先の出カ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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 **ipv6 dhcp relay source-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。

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

関連コマンド

Command	Description
ipv6 dhcp relay source-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 **ipv6 dhcp binding track ppp** 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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 dhcp binding track ppp 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、または管理者がバ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。

```
(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 **ipv6 dhcp database** 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 ] abort [ timeout seconds ]
no ipv6 dhcp database agent
```

構文の説明

<i>agent</i>	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 <i>seconds</i>	(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 <i>seconds</i>	(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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 dhcp database 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キャンセルされます。デフォルトでは、IPv6 用 DHCP サーバは、データベース転送のキャンセル前に 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。

```
(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。

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

関連コマンド

Command	Description
<code>clear ipv6 dhcp binding</code>	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。
<code>show ipv6 dhcp database</code>	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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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(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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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、デバイスがそのデバイス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も追加されます。

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(config)# ipv6 dhcp iapd-route-add
```

ipv6 dhcp-ldra

Lightweight DHCPv6 リレーエージェント (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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 (デジタル加入者線アクセスマルチプレクサ (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。

```
(config)# ipv6 dhcp-ldra enable
(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
ipv6 dhcp ldra attach-policy	VLAN 上で LDRA 機能を有効にします。
ipv6 dhcp-ldra attach-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 **ipv6 dhcp ping packets** 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	<i>number</i>	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 Fuji 16.9.2	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。

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

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 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 **ipv6 dhcp pool** 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	<i>poolname</i> 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 (config)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	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 用 DHCP サーバ設定情報プールを作成するには、**ipv6 dhcp pool** コマンドを使用します。**ipv6 dhcp pool** コマンドがイネーブルの場合、コンフィギュレーションモードが IPv6 用 DHCP 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。

- **address prefix** *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東りに入力できます。



(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。

IPv6 用 DHCP 設定情報プールが作成されたら、**ipv6 dhcp server** 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、**ipv6 dhcp server interface** 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。

```
(config)# ipv6 dhcp pool cisco1
(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。

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

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

```
# configure terminal
```

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

関連コマンド

Command	Description
ipv6 dhcp server	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 pool	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 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 **ipv6 dhcp server vrf enable** 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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 dhcp server option vpn コマンドは DHCPv6 サーバの VRF 認識型機能をデバイス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 認識型機能をデバイス上でグローバルに有効にする例を示します。

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

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、**ipv6 flow monitor** 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		
	<i>ipv6-monitor-name</i>	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 <i>ipv6-sampler-name</i>	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 (config-if)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	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モニタ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。

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

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 **ipv6 general-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

<i>prefix-name</i>	プレフィックスに割り当てられている名前。
<i>ipv6-prefix</i>	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、 <i>ipv6-prefix</i> 引数と <i>/ prefix-length</i> 引数の両方を指定します。
<i>/ prefix-length</i>	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、 <i>ipv6-prefix</i> 引数と <i>/ prefix-length</i> 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 <i>interface-type interface-number</i> 引数を指定します。
<i>interface-type interface-number</i>	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 (?) を使用してオンラインヘルプを参照してください。 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 <i>interface-type interface-number</i> 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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

```
(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。

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

関連コマンド

Command	Description
show ipv6 general-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 **ipv6 local policy route-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

<i>route-map-name</i>	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 <i>route-map-name</i> 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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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、**ipv6 local policy route-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。

ipv6 local policy route-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。**no ipv6 local policy route-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
ipv6 policy route-map	インターフェイス上に IPv6 PBR を設定します。
match ipv6 address	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。
match length	パケットのレベル 3 長に基づいてポリシー ルーティングを実行します。
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。
set default interface	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。
set interface	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。
set ipv6 default next-hop	一致パケットが転送されるデフォルトの IPv6 ネクスト ホップを指定します。
set ipv6 next-hop (PBR)	ポリシー ルーティングのルート 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。
set ipv6 precedence	IPv6 パケット ヘッダーのプリファレンス値を設定します。

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

<i>poolname</i>	ローカルなプレフィックス プールのユーザ定義名。
<i>prefix</i>	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。
<i>/ prefix-length</i>	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。
<i>assigned-length</i>	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)。 <i>assigned-length</i> 引数の値は、 <i>/ prefix-length</i> 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 (global)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

```
(config)# ipv6 local pool pool1 2001:0DB8::/29 64
(config)# end
# 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
debug ipv6 pool	IPv6 プールのデバッグを有効にします。
peer default ipv6 address pool	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-delegation pool	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。
show ipv6 local pool	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 **ipv6 mld snooping** 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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

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

関連コマンド

コマンド	説明
show ipv6 mld snooping	MLDv2 スヌーピング情報を表示します。

ipv6 mld ssm-map enable

送信元特定マルチキャスト（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 **ipv6 mld ssm-map enable** 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 mld [vrf vrf-name] ssm-map enable
no ipv6 mld [vrf vrf-name] ssm-map enable

構文の説明

vrf <i>vrf-name</i>	(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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 mld ssm-map enable 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。**ipv6 mld ssm-map enable** 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。

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

関連コマンド

コマンド	説明
debug ipv6 mld ssm-map	SSM マッピングのデバッグ メッセージを表示します。
ipv6 mld ssm-map query dns	DNS ベースの SSM マッピングを有効にします。
ipv6 mld ssm-map static	スタティック SSM マッピングを設定します。
show ipv6 mld ssm-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 **ipv6 mld state-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 (config)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	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、**ipv6 mld state-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 **ipv6 mld limit** 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。

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

関連コマンド	コマンド	説明
	ipv6 mld access-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
ipv6 mld limit	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 **ipv6 multicast-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 <i>vrf-name</i>	(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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 **no ipv6 pim** コマンドまたは **no ipv6 mld router** 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。

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

関連コマンド

コマンド	説明
ipv6 pim rp-address	特定のグループ範囲の PIM RP のアドレスを設定します。
no ipv6 pim	指定したインターフェイスで IPv6 PIM をオフにします。
no ipv6 mld router	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ン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 **ipv6 multicast group-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 <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
	<i>access-list-name</i>	(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リバグループと承認済みのチャン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ン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ン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 (config)

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 multicast group-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ンネルを指定します。拒否されたグループまたはチャンネルについては、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ンネルのマルチキャストは無効になります。

ipv6 multicast group-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、**ipv6 multicast group-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。

- **ipv6 mld access-group** *access-list-name*
- **ipv6 multicast boundary scope** *scope-value*

no ipv6 multicast group-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ン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。

```
(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。

```
(config)# interface int2
(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ンネルに 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ン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ン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ンネルを許可するように指定できます。

関連コマンド

Command	Description
ipv6 mld access-group	IPv6 マルチキャスト受信者アクセス制御を実行します。
ipv6 multicast boundary scope	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 **ipv6 multicast pim-passive-enable** 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 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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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、**ipv6 multicast pim-passive-enable** コマンドを使用します。PIM パッシブモードがグロ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 **ipv6 pim passive** 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。

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

関連コマンド

コマンド	説明
ipv6 pim passive	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 nd cache expire

IPv6 ネイバー探索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 **ipv6 nd cache expire** コマンドを使用します。この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 nd cache expire *expire-time-in-seconds* [**refresh**]
no ipv6 nd cache expire *expire-time-in-seconds* [**refresh**]

構文の説明	<i>expire-time-in-seconds</i>	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) ネイバー探索キャッシュエントリを自動的に更新します。
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 (config-if)	
コマンド履歴	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	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、ネイバー探索キャッシュエントリの有効期限が切れて削除されます。**ipv6 nd cache expire** コマンドを使用すると、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、ネイバー探索キャッシュエントリが自動更新されます。エントリは DELAY 状態に移行し、ネイバー到達不能検出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、ネイバー送信要求が送信され、設定に従って再送信されます。

例

次に、ネイバー探索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> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd cache expire 7200
```

関連コマンド	コマンド	説明
	ipv6 nd na glean	非送信要求ネイバー アドバタイズメントからエントリを収集するネイバー探索を設定します。

コマンド	説明
ipv6 nd nud retry	ネイバー到達不能検出でネイバー送信要求を再送信する回数を設定します。
show ipv6 interface	IPv6 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。

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 **ipv6 nd cache interface-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

<i>size</i>	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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 **ipv6 nd cache interface-limit** コマンドを実行すると、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 **ipv6 nd cache interface-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。

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

関連コマンド

コマンド	説明
ipv6 nd cache interface-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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

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

```
(config)# ipv6 nd host mode strict
(config-if)# interface ethernet0/0
(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 na glean

非送信要求ネイバーアドバタイズメントからエントリを収集するようにネイバー探索を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd na glean** 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 nd na glean
no ipv6 nd na glean

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 Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン 重複アドレス検出 (DAD) が正常に完了すると、IPv6 ノードからマルチキャスト非送信要求ネイバー アドバタイズメント パケットが発行されることがあります。デフォルトでは、これらの非送信要求ネイバー アドバタイズメント パケットは他の IPv6 ノードから無視されます。**ipv6 nd na glean** コマンドは、非送信要求ネイバー アドバタイズメント パケットの受信時にルータでネイバー アドバタイズメント エントリを作成するように設定します (これらのエントリがまだ存在せず、ネイバーアドバタイズメントにリンク層アドレスオプションがある場合)。このコマンドを使用すると、データトラフィックをネイバーと交換する前に、デバイスのネイバーアドバタイズメント キャッシュにネイバーのエントリを読み込むことができます。

例

次に、非送信要求ネイバーアドバタイズメントからエントリを収集するようにネイバー探索を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd na glean
```

関連コマンド

コマンド	説明
ipv6 nd cache expire	IPv6 ネイバー探索キャッシュ エントリの期限が切れるまでの時間を設定します。
ipv6 nd nud retry	ネイバー到達不能検出でネイバー送信要求を再送信する回数を設定します。
show ipv6 interface	IPv6 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。

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 **ipv6 nd ns-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

<i>milliseconds</i>	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 (config-if)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 nd ns-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、**ipv6 nd dad time** 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。

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

関連コマンド

コマンド	説明
ipv6 nd dad time	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。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 nd nud retry

ネイバー到達不能検出プロセスでネイバー送信要求を再送信する回数を設定するには、インターフェイスコンフィギュレーションモードで **ipv6 nd nud retry** 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 nd nud retry base interval max-attempts final-wait-time
no ipv6 nd nud retry base interval max-attempts final-wait-time

構文の説明	<i>base</i>	ネイバー到達不能検出プロセスのベース値。
	間隔	再試行の時間間隔（ミリ秒）。 有効な範囲は 1000 ～ 32000 です。
	<i>max-attempts</i>	再試行の最大回数（ベース値に依存）。 有効な範囲は 1 ～ 128 です。
	<i>final-wait-time</i>	最後のプローブの待機時間（ミリ秒）。 有効な範囲は 1000 ～ 32000 です。
コマンドモード	インターフェイス コンフィギュレーション (config-if)	
コマンド履歴	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

ネイバーのネイバー検出エントリを再度解決するためにデバイスでネイバー到達不能検出を実行する際、ネイバー送信要求パケットが 1 秒間隔で 3 回送信されます。スパンニングツリーイベント、トラフィックの多いイベント、エンドホストのリロードなどの特定の状況においては、ネイバー送信要求が 1 秒間隔で 3 回送信されても十分でない場合があります。このような状況でネイバーキャッシュを維持するには、**ipv6 nd nud retry** コマンドを使用してネイバー送信要求の再送信の指数タイマーを設定します。

再試行の最大回数は、*max-attempts* 引数を使用して設定されます。再送信間隔は、次の式で計算されます。

$$tm^n$$

各値は次のとおりです。

- t = 時間間隔
- m = ベース (1、2、または 3)
- n = 現在のネイバー送信要求番号 (最初のネイバー送信要求が 0)

したがって、**ipv6 nd nud retry 3 1000 5** コマンドは、1、3、9、27、81 秒の間隔で再送信します。最終待機時間が設定されていない場合、エントリは 243 秒後に削除されます。

ipv6 nd nud retry コマンドはネイバー到達不能検出プロセスの再送信レートにのみ影響し、最初の解決には影響しません。最初の解決では、デフォルトに基づいてネイバー送信要求パケットが 1 秒間隔で 3 回送信されます。

例

次に、1 秒の固定間隔で 3 回再送信するように設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd nud retry 1 1000 3
```

次に、再送信間隔を 1、2、4、8 に設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd nud retry 2 1000 4
```

次に、再送信間隔を 1、3、9、27、81 に設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd nud retry 3 1000 5
```

関連コマンド

コマンド	説明
ipv6 nd cache expire	IPv6 ネイバー探索 (ND) キャッシュエントリの期限が切れるまでの時間を設定します。
ipv6 nd na glean	非送信要求ネイバー アドバタイズメントからエントリを収集するネイバー探索を設定します。
show ipv6 interface	IPv6 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。

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 **ipv6 nd reachable-time** コマンドを使用します。デフォルトの時間に戻すには、このコマンドの **no** 形式を使用します。

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

構文の説明

<i>milliseconds</i>	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、ルータアダプタイズメントでアダプタイズされます。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（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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ダプ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。

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

関連コマンド

コマンド	説明
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

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 **ipv6 nd resolution data limit** 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	<i>number-of-packets</i> 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 (config)				
コマンド履歴	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Fuji 16.9.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
リリース	変更内容				
Cisco IOS XE Fuji 16.9.2	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 resolution data limit** 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 **ipv6 nd resolution data limit** 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。

```
(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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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

```
(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スタティック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 **ipv6 neighbor** コマンドを使用します。IPv6 ネイバー探索キャッシュからスタティック 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

<i>ipv6-address</i>	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。
<i>interface-type</i>	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。
<i>interface-number</i>	指定されたインターフェイス番号。
<i>hardware-address</i>	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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 neighbor 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。

show ipv6 neighbors コマンドは、IPv6 ネイバー探索キャッシュ内のスタティック エントリを表示するために使用します。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。

- INCOMP (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、**show ipv6 neighbors** コマンドを参照してください。

clear ipv6 neighbors コマンドは、スタティック エントリを除く、IPv6 ネイバー探索キャッシュ内のすべての エントリを削除します。**no ipv6 neighbor** コマンドは、指定されたスタティック エントリをネイバー探索キャッシュから削除します。IPv6 ネイバー探索プロセスで学習されたダイナミック エントリはキャッシュから削除されません。**no ipv6 enable** コマンドまたは **no ipv6 unnumbered** 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、スタティック 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。

```
(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。
clear ipv6 neighbors	スタティック エントリを除く、IPv6 ネイバー探索キャッシュ内のすべての エントリを削除します。
no ipv6 enable	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。
no ipv6 unnumbered	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。
show ipv6 neighbors	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 をドメインネームシステム (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 **ipv6 ospf name-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 (config)

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 ではなく名前が表示されるため、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。

```
(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 **ipv6 pim** 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 (config-if)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 multicast-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、**ipv6 pim** 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。

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

関連コマンド

コマンド	説明
ipv6 multicast-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 **ipv6 pim accept-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	パラメータ	説明
	vrf <i>vrf-name</i>	(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 <i>access-list</i>	アクセス リスト名を定義します。
	route-map <i>map-name</i>	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 (config)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	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、**ipv6 pim accept-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先ルータに返されます。

例

次に、ローカルマルチキャストルート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 (config)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	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 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 **ipv6 pim neighbor-filter** コマンドを使用します。ルータをデフォルトに戻すには、このコマンドの **no** 形式を使用します。

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

構文の説明

vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
<i>access-list</i>	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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 pim neighbor-filter list 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。

```
(config)# ipv6 pim neighbor-filter list nbr_filter_acl
(config)# ipv6 access-list nbr_filter_acl
(config-ipv6-acl)# deny ipv6 host FE80::A8BB:CCFF:FE03:7200 any
(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 **ipv6 pim rp-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 <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
<i>ipv6-address</i>	PIM RP になるルータの IPv6 アドレス。 <i>ipv6-address</i> 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。
<i>group-access-list</i>	(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 Fuji 16.9.2	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ります。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。

```
(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。

```
(config)# ipv6 access-list acc-grp-1
(config-ipv6-acl)# permit ipv6 any ff04::/64
(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。

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

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

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

関連コマンド

コマンド	説明
debug ipv6 pim df-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。
ipv6 access-list	IPv6 アクセスリストを定義し、ルータを IPv6 アクセスリストコンフィギュレーションモードにします。
show ipv6 pim df	各 RP の各インターフェイスの DF 選択状態を表示します。
show ipv6 pim df winner	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 **ipv6 pim rp-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 <i>vrf-name</i>	(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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

ipv6 pim rp embedded コマンドは、組み込み RP グループ範囲の ff7X::/16 と fffX::/16 にも適用されます。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 **ipv6 pim spt-threshold infinity** 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 <i>vrf-name</i>	(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 <i>access-list-name</i>	(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、**ipv6 pim spt-threshold infinity** 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 (config)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	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 pim spt-threshold infinity** 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。

```
(config)# ipv6 access-list acc-grp-1
(config-ipv6-acl)# permit ipv6 any FF04::/64
(config-ipv6-acl)# exit
(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 **ipv6 prefix-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 | description text [ge ge-value] [le le-value]
no ipv6 prefix-list list-name
```

構文の説明

<i>list-name</i>	プレフィックス リストの名前。 <ul style="list-style-type: none"> 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。 show ipv6 prefix-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 <i>seq-number</i>	(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。
<i>ipv6-prefix</i>	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。
<i>lprefix-length</i>	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。
description <i>text</i>	プレフィックス リストの説明。最大 80 文字です。
ge <i>ge-value</i>	(任意) <i>ipv6-prefix/lprefix-length</i> 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 <i>length</i> の範囲の最小値です (長さ範囲の「下限」に該当する値)。
le <i>le-value</i>	(任意) <i>ipv6-prefix/lprefix-length</i> 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 <i>length</i> 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 (config)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	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 prefix-list** コマンドは、IPv6 固有である点を除いて、**ip prefix-list** コマンドに似ています。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-list out** 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。

show ipv6 prefix-list コマンドを使用すると、エントリのシーケンス番号が表示されます。

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。

```
(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。

```
(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。

```
(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。

```
(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。

```
(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。

```
(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。

```
(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。

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

関連コマンド

コマンド	説明
clear ipv6 prefix-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-list out	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。
ipv6 prefix-list sequence-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
match ipv6 address	プレフィッ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。
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 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	<i>source-guard-policy</i>	(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 (config-if)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	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** コマンドが入力されると、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。

```
(config)# interface gigabitethernet 0/0/1
(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 **ipv6 source-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、**ipv6 source-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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 **ipv6 source-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 **no ipv6 source-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、**show config** コマンドの出力内にこの設定が引き続き表示されます。

no ipv6 source-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。**no ipv6 source-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。
ipv6 icmp error-interval	IPv6 ICMP エラーメッセージの間隔を設定します。

ipv6 spd mode

IPv6 選択的パケット破棄 (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 **ipv6 spd mode** 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。
tos protocol o 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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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、**ipv6 spd mode** 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 SPD 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破棄されます。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。

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

関連コマンド

コマンド	説明
ipv6 spd queue max-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。
ipv6 spd queue min-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。
show ipv6 spd	IPv6 SPD 設定を表示します。

ipv6 spd queue max-threshold

IPv6 選択的パケット破棄 (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 **ipv6 spd queue max-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	<i>value</i>	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 (config)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	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、**ipv6 spd queue max-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 SPD 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破棄されます。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。

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

関連コマンド	コマンド	説明
	ipv6 spd queue min-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。
	show ipv6 spd	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 **ipv6 traffic interface-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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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。

```
(config)# 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 **ipv6 unicast-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 (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 ipv6 unicast-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。

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

関連コマンド

コマンド	説明
ipv6 address link-local	インターフェイスの IPv6 リンクローカルアドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにします。
ipv6 address eui-64	IPv6 アドレスを設定して、そのアドレスの下位 64 ビットの EUI-64 インターフェイス ID を使用して、インターフェイスでの IPv6 処理をイネーブルにします。
ipv6 enable	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。
ipv6 unnumbered	インターフェイスに明示的な IPv6 アドレスを割り当てなくても、インターフェイスで IPv6 処理をイネーブルにします。
show ipv6 route	IPv6 ルーティングテーブルの現在の内容を表示します。

key chain

ルーティングプロトコルの認証を有効にするために必要な認証キーチェーンを定義して、キーチェーン 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 **key chain** コマンドを使用します。キーチェーンを削除するには、このコマンドの **no** 形式を使用します。

key chain *name-of-chain*
no key chain *name-of-chain*

構文の説明	<i>name-of-chain</i>	キーチェーンの名前。キーチェーンには、少なくとも1つのキーを含める必要がありますが、最大 2147483647 個のキーを含めることができます。
-------	----------------------	--

コマンド デフォルト キーチェーンは存在しません。

コマンド モード グローバル コンフィギュレーション (config)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン 認証を有効にするには、キーでキーチェーンを設定する必要があります。

複数のキーチェーンの識別が可能ですが、ルーティングプロトコルごとのインターフェイスごとに1つのキーチェーンを使用することを推奨します。**key chain** コマンドを指定すると、キーチェーン コンフィギュレーション モードが開始されます。

例 次に、キーチェーンを指定する例を示します。

```
Device(config-keychain-key)# key-string chestnut
```

関連コマンド	Command	Description
	accept-lifetime	キーチェーンの認証キーが有効として受信される期間を設定します。
	key	キーチェーンの認証キーを識別します。
	key-string (authentication)	キーの認証文字列を指定します。
	send-lifetime	キーチェーンの認証キーが有効に送信される期間を設定します。
	show key chain	認証キーの情報を表示します。

key-string (認証)

キーの認証文字列を指定するには、キーチェーン キー コンフィギュレーション モードで **key-string** (認証) コマンドを使用します。認証文字列を削除するには、このコマンドの **no** 形式を使用します。

key-string key-string text

no key-string text

構文の説明

<i>text</i>	認証されるルーティング プロトコルを使用してパケットで送信および受信される必要のある認証文字列。文字列には、大文字小文字の英数字 1 ~ 80 文字を含めることができます。
-------------	--

コマンド デフォルト

キーの認証文字列は存在しません。

コマンド モード

キー チェーン キー コンフィギュレーション (config-keychain-key)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

例

次に、キーの認証文字列を指定する例を示します。

```
Device(config-keychain-key)# key-string key1
```

関連コマンド

Command	Description
accept-lifetime	キー チェーンの認証キーが有効として受信される期間を設定します。
key	キー チェーンの認証キーを識別します。
key chain	ルーティング プロトコルの認証をイネーブルにするために必要な認証キーチェーンを定義します。
send-lifetime	キー チェーンの認証キーが有効に送信される期間を設定します。
show key chain	認証キーの情報を表示します。

key

キーチェーンの認証キーを識別するには、キーチェーンコンフィギュレーションモードで **key** コマンドを使用します。キーチェーンからキーを削除するには、このコマンドの **no** 形式を使用します。

key *key-id*
no key *key-id*

構文の説明	<i>key-id</i> キーチェーンの認証キーの識別番号。キーの範囲は 0 ~ 2147483647 です。キーの ID 番号は連続している必要はありません。
-------	---

コマンドデフォルト キーチェーンにキーは存在しません。

コマンドモード キーチェーンコンフィギュレーション (config-keychain)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン キーチェーンに複数のキーを設定し、**accept-lifetime** および **send-lifetime** キーチェーンキーコマンド設定に基づいてキーが将来無効になるように、ソフトウェアでキーを配列できるようにすると便利です。

各キーには、ローカルに格納される独自のキー識別子があります。キー ID、およびメッセージに関連付けられたインターフェイスの組み合わせにより、使用中の認証アルゴリズムおよび Message Digest 5 (MD5) 認証キーが一意に識別されます。有効なキーの数にかかわらず、1 つの認証パケットのみが送信されます。ソフトウェアは、最小のキー識別番号の検索を開始し、最初の有効なキーを使用します。

最後のキーが期限切れになった場合、認証は続行されますが、エラーメッセージが生成されません。認証を無効にするには、手動で有効な最後のキーを削除する必要があります。

すべてのキーを削除するには、**no key chain** コマンドを使用してキーチェーンを削除します。

例

次に、キーを指定してキーチェーンでの認証を確認する例を示します。

```
Device(config-keychain)# key 1
```

関連コマンド	Command	Description
	accept-lifetime	キーチェーンの認証キーが有効として受信される期間を設定します。

Command	Description
key chain	ルーティング プロトコルの認証をイネーブ爾にするために必要な認証キー チェーンを定義します。
key-string (authentication)	キーの認証文字列を指定します。
send-lifetime	キーチェーンの認証キーが有効に送信される期間を設定します。
show key chain	認証キーの情報を表示します。

show ip ports all

デバイス上で開いているすべてのポートを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip ports all** を使用します。

show ip ports all

構文の説明

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

デフォルトの動作や値はありません。

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 Fuji 16.9.2	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、Cisco ネットワーキング スタックを使用して開かれたポートを含むシステム上で開いているすべての TCP/IP ポートのリストを表示します。

開いているポートを閉じるには、次のいずれかの方法を使用します。

- アクセスコントロールリスト (ACL) を使用します。
- UDP 2228 ポートを閉じるには、**no l2 traceroute** コマンドを使用します。
- TCP 80、TCP 443、TCP 6970、TCP 8090 ポートを閉じるには、**no ip http server** および **no ip http secure-server** コマンドを使用します。

例

次に、**show ip ports all** コマンドの出力例を示します。

```
Device#
show ip ports all
Proto Local Address Foreign Address State PID/Program Name
TCB Local Address Foreign Address (state)
tcp *:4786 *:* LISTEN 224/[IOS]SMI IBC server process
tcp *:443 *:* LISTEN 286/[IOS]HTTP CORE
tcp *:443 *:* LISTEN 286/[IOS]HTTP CORE
tcp *:80 *:* LISTEN 286/[IOS]HTTP CORE
tcp *:80 *:* LISTEN 286/[IOS]HTTP CORE
udp *:10002 *:* 0/[IOS] Unknown
udp *:2228 10.0.0.0:0 318/[IOS]L2TRACE SERVER
```

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 ip ports all* のフィールドの説明

フィールド	説明
Protocol	使用されている転送プロトコル。
Local Address.	デバイスの IP アドレス。
Foreign Address	リモートまたはピア アドレス。
State	接続の状態。リッスン、確立済み、または接続済みを選択できます。
PID/Program Name	プロセス ID または名前。

関連コマンド

Command	Description
show tcp brief all	TCP 接続のエンドポイントに関する情報を表示します。
show ip sockets	IP ソケット情報を表示します。

show ip wccp

IPv4 Web Cache Communication Protocol (WCCP) のグローバル設定と統計を表示するには、ユーザー EXEC モードまたは特権 EXEC モードで **show ip wccp** コマンドを使用します。

```
show ip wccp [ all ] [ capabilities ] [ summary ] [ interfaces [ cef |
counts | detail ] ] [ vrf vrf-name ] [ web-cache service-number [ assignment ]
[ clients ] [ counters ] [ detail ] [ service ] [ view ] ]
```

構文の説明

all	(任意) 既知のすべてのサービスの統計を表示します。
capabilities	(任意) WCCP プラットフォーム機能の情報を表示します。
summary	(任意) WCCP サービスのサマリーを表示します。
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。
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。
web-cache	(任意) Web キャッシュ サービスの統計を表示します。
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。
assignment	(任意) サービスグループの割り当て情報を表示します。
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。
counters	(任意) トラフィック カウンタを表示します。
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。

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。
view	(任意) 特定のサービスグループまたはすべてのサービスグループの他のメンバーが検出されたかどうかを表示します。

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
	このコマンドが導入されました。
Cisco IOS XE Bengaluru 17.6.1	vrf キーワードと <i>vrf-name</i> 引数のペアが追加されました。

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、**clear ip wccp** 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、**show ip wccp 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、**show ip wccp summary** 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。

- **show ip wccp service-number** (サービスモードを表示)
- **show ip wccp service-number view**
- **show ip wccp service-number detail**
- **show ip wccp service-number clients**
- **show ip wccp interfaces**
- **show ip wccp web-cache**
- **show ip wccp web-cache counters**
- **show ip wccp web-cache detail**
- **show ip wccp web-cache detail** (バイパス カウンタを表示)
- **show ip wccp web-cache clients**
- **show ip wccp web-cache service**
- **show ip wccp summary**

show ip wccp service-number (サービスモードを表示)

次に、**show ip wccp service-number** コマンドの出力例を示します。

```
Device# show ip wccp 90

Global WCCP information:
  Router information:
    Router Identifier:                10.10.0.0

    Service Identifier: 90
      Protocol Version:                2.00
      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 3: **show ip wccp service-number** のフィールドの説明

フィールド	Description
Router information	現在のルータによって検出されたルータのリスト。
プロトコルバージョン	サービスグループ内のルータで使用されている 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ルータで認識可能なクライアントとその他のクライアントの数。
Number of Service Group Routers	サービスグループ内のルータ数。
Total Packets Redirected	ルータ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。

フィールド	Description
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。
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	<i>group-list</i> 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 GRE Bypassed Packets Received	バイパスされた Generic Routing Encapsulation (GRE) パケットの数。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 ip wccp service-number view

次に、サービスグループ 1 の **show ip wccp service-number view** コマンドの出力例を示します。

```
Device# show ip wccp 90 view

WCCP Routers Informed of:
 209.165.200.225
 209.165.200.226
WCCP Clients Visible
 209.165.200.227
 209.165.200.228
WCCP Clients Not Visible:
 -none-
```



(注) 設定可能な最大サービス グループ数は 256 です。

WCCP Cache Engines Not Visible フィールドに Web キャッシュが表示される場合は、認識できない Web キャッシュをマッピングするようにルータを設定し直す必要があります。

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 ip wccp service-number view のフィールドの説明

フィールド	Description
WCCP Router Informed of	現在のルータによって検出されたルータのリスト。
WCCP Clients Visible	サービスグループ内のルータで認識可能なクライアントとその他のクライアントのリスト。
WCCP Clients Not Visible	サービスグループ内のルータで認識できないクライアントとその他のクライアントのリスト。

show ip 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 ip wccp 91 detail

WCCP Client information:
WCCP Client ID: 209.165.200.226
Protocol Version: 2.0
State:                Usable
  Redirection:         L2
  Packet Return:      L2
  Assignment:          MASK
  Connect Time:        6d20h
  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: 0x00000000 0x00001741 0x0000  0x0000

  Value SrcAddr  DstAddr  SrcPort  DstPort
  ----  -
  0000: 0x00000000 0x00000001 0x0000  0x0000
  0001: 0x00000000 0x00000041 0x0000  0x0000
  0002: 0x00000000 0x00000101 0x0000  0x0000
  0003: 0x00000000 0x00000141 0x0000  0x0000
  0004: 0x00000000 0x00000201 0x0000  0x0000
  0005: 0x00000000 0x00000241 0x0000  0x0000
  0006: 0x00000000 0x00000301 0x0000  0x0000
  0007: 0x00000000 0x00000341 0x0000  0x0000
```

show ip wccp

```

0008: 0x00000000 0x00000401 0x0000 0x0000
0009: 0x00000000 0x00000441 0x0000 0x0000
0010: 0x00000000 0x00000501 0x0000 0x0000
0011: 0x00000000 0x00000541 0x0000 0x0000
0012: 0x00000000 0x00000601 0x0000 0x0000
0013: 0x00000000 0x00000641 0x0000 0x0000
0014: 0x00000000 0x00000701 0x0000 0x0000
0015: 0x00000000 0x00000741 0x0000 0x0000
0016: 0x00000000 0x00001001 0x0000 0x0000
0017: 0x00000000 0x00001041 0x0000 0x0000
0018: 0x00000000 0x00001101 0x0000 0x0000
0019: 0x00000000 0x00001141 0x0000 0x0000
0020: 0x00000000 0x00001201 0x0000 0x0000
0021: 0x00000000 0x00001241 0x0000 0x0000
0022: 0x00000000 0x00001301 0x0000 0x0000
0023: 0x00000000 0x00001341 0x0000 0x0000
0024: 0x00000000 0x00001401 0x0000 0x0000
0025: 0x00000000 0x00001441 0x0000 0x0000
0026: 0x00000000 0x00001501 0x0000 0x0000
0027: 0x00000000 0x00001541 0x0000 0x0000
0028: 0x00000000 0x00001601 0x0000 0x0000
0029: 0x00000000 0x00001641 0x0000 0x0000
0030: 0x00000000 0x00001701 0x0000 0x0000
0031: 0x00000000 0x00001741 0x0000 0x0000

```

```

WCCP Client ID:          192.0.2.11
Protocol Version:        2.01
State:                   Usable
Redirection:             L2
Packet Return:           L2
Assignment:              MASK
Connect Time:            6d20h
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:	0x00000000	0x00001741	0x0000	0x0000

Value	SrcAddr	DstAddr	SrcPort	DstPort
0000:	0x00000000	0x00000000	0x0000	0x0000
0001:	0x00000000	0x00000040	0x0000	0x0000
0002:	0x00000000	0x00000100	0x0000	0x0000
0003:	0x00000000	0x00000140	0x0000	0x0000
0004:	0x00000000	0x00000200	0x0000	0x0000
0005:	0x00000000	0x00000240	0x0000	0x0000
0006:	0x00000000	0x00000300	0x0000	0x0000
0007:	0x00000000	0x00000340	0x0000	0x0000
0008:	0x00000000	0x00000400	0x0000	0x0000
0009:	0x00000000	0x00000440	0x0000	0x0000
0010:	0x00000000	0x00000500	0x0000	0x0000
0011:	0x00000000	0x00000540	0x0000	0x0000
0012:	0x00000000	0x00000600	0x0000	0x0000
0013:	0x00000000	0x00000640	0x0000	0x0000
0014:	0x00000000	0x00000700	0x0000	0x0000
0015:	0x00000000	0x00000740	0x0000	0x0000

```

0016: 0x00000000 0x00001000 0x0000 0x0000
0017: 0x00000000 0x00001040 0x0000 0x0000
0018: 0x00000000 0x00001100 0x0000 0x0000
0019: 0x00000000 0x00001140 0x0000 0x0000
0020: 0x00000000 0x00001200 0x0000 0x0000
0021: 0x00000000 0x00001240 0x0000 0x0000
0022: 0x00000000 0x00001300 0x0000 0x0000
0023: 0x00000000 0x00001340 0x0000 0x0000
0024: 0x00000000 0x00001400 0x0000 0x0000
0025: 0x00000000 0x00001440 0x0000 0x0000
0026: 0x00000000 0x00001500 0x0000 0x0000
0027: 0x00000000 0x00001540 0x0000 0x0000
0028: 0x00000000 0x00001600 0x0000 0x0000
0029: 0x00000000 0x00001640 0x0000 0x0000
0030: 0x00000000 0x00001700 0x0000 0x0000
0031: 0x00000000 0x00001740 0x0000 0x0000

```

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 ip wccp service-number detail` のフィールドの説明

フィールド	Description
Protocol Version	WCCPv1 または WCCPv2 が有効かどうかを示します。
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ルータ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。
Connect Time	クライアントがルータに接続されている時間。
Redirected Packets	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。

show ip wccp service-number clients

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 ip wccp 91 clients
```

```

WCCP Client information:
WCCP Client ID: 10.1.1.14
Protocol Version: 2.0
State:                Usable
  Redirection:         L2
  Packet Return:      L2

```

show ip wccp

```

Assignment:           MASK
Connect Time:         6d20h
Redirected Packets:
  Process:            0
  CEF:                0
GRE Bypassed Packets:
  Process:            0
  CEF:                0
Mask Allotment:       32 of 64 (50.00%)

WCCP Client ID:       192.0.2.11
Protocol Version:     2.01
State:                Usable
Redirection:          L2
Packet Return:        L2
Assignment:           MASK
Connect Time:         6d20h
Redirected Packets:
  Process:            0
  CEF:                0
GRE Bypassed Packets:
  Process:            0
  CEF:                0
Mask Allotment:       32 of 64 (50.00%)

```

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 ip wccp service-number clients` のフィールドの説明

フィールド	Description
Protocol Version	WCCPv1 または WCCPv2 が有効かどうかを示します。
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ルータ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。
Connect Time	クライアントがルータに接続されている時間 (秒)。
Redirected Packets	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。

show ip wccp interfaces

次に、`show ip wccp interfaces` コマンドの出力例を示します。

```
Device# show ip wccp interfaces
```

```
IPv4 WCCP interface configuration:
  FastEthernet2/1
    Output services: 0
    Input services: 1
    Mcast services: 0
    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 7: *show ip wccp interfaces* のフィールドの説明

フィールド	Description
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 ip wccp web-cache

次に、**show ip wccp web-cache** コマンドの出力例を示します。

```
Device# show ip wccp web-cache
```

```
Global WCCP information:
  Router information:
    Router Identifier:                209.165.200.225

  Service Identifier: web-cache
    Protocol Version:                 2.00
    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:              Tunnel0
```

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 ip wccp web-cache` のフィールドの説明

フィールド	Description
Service Identifier	サービスの識別情報を示します。
プロトコルバージョン	WCCPv1 または WCCPv2 が有効かどうかを示します。
Number of Service Group Clients	ホーム ルータとしてルータを使用しているクライアントの数。
Number of Service Group Routers	サービス グループ内のルータ数。
Total Packets Redirected	ルータ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	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	<i>group-list</i> 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。

show ip 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 ip 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: 192.0.2.12
Redirected Packets:
Process: 0
CEF: 0
GRE Bypassed Packets:
Process: 0
CEF: 0

WCCP Client ID: 192.0.2.11
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 9: `show ip wccp web-cache counters` のフィールドの説明

フィールド	Description
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 ip wccp web-cache detail

次に、Web キャッシュサービスの Web キャッシュエンジンの情報および WCCP ルータ統計情報を表示する例を示します。

```
Device# show ip wccp web-cache detail
```

```
WCCP Client information:
```

show ip wccp

```

WCCP Client ID:      209.165.200.225
Protocol Version:    2.0
State:               Usable
Redirection:         GRE
Packet Return:       GRE
Assignment:          HASH
Connect Time:        1w5d
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:  AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

WCCP Client ID:      192.0.2.11
Protocol Version:    2.01
State:               Usable
Redirection:         GRE
Packet Return:       GRE
Assignment:          HASH
Connect Time:        1w5d
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

```

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 ip wccp web-cache detail` のフィールドの説明

フィールド	Description
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。
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。
Connect Time	キャッシュエンジンがルータに接続されている時間。
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。

show ip wccp web-cache detail (バイパスカウンタを表示)

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 ルータ統計情報を表示する例を示します。

```
Device# show ip wccp web-cache detail

WCCP Client information:
  WCCP Client ID:          209.165.200.225
  Protocol Version:        2.01
  State:                    Usable
  Redirection:              GRE
  Packet Return:           GRE
  Assignment:               HASH
  Connect Time:             1w5d
  Redirected Packets:
    Process:                0
    CEF:                     0
  GRE Bypassed Packets:
    Process:                0
    CEF:                     0
  Hash Allotment:          128 of 256 (50.00%)
  Initial Hash Info:       00000000000000000000000000000000
  Assigned Hash Info:      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
                          AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

  WCCP Client ID:          209.165.200.226
  Protocol Version:        2.01
  State:                    Usable
  Redirection:              GRE
  Packet Return:           GRE
  Assignment:               HASH
  Connect Time:             1w5d
  Redirected Packets:
    Process:                0
    CEF:                     0
  GRE Bypassed Packets:
    Process:                0
    CEF:                     0
  Hash Allotment:          128 of 256 (50.00%)
  Initial Hash Info:       00000000000000000000000000000000
  Assigned Hash Info:      55555555555555555555555555555555
                          55555555555555555555555555555555
```

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 11: *show ip wccp web-cache detail* のフィールドの説明

フィールド	Description
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。
プロトコルバージョン	サービスグループ内のルータで使用されている WCCP のバージョン。

フィールド	Description
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。
Connect Time	キャッシュエンジンがルータに接続されている時間。
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。
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。
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。
GRE 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 ip 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 ip wccp web-cache service
```

```
WCCP service information definition:
  Type:          Standard
  Id:            0
  Priority:      240
  Protocol:      6
  Flags:         0x00000512
  Hash:          DstIP
  Alt Hash:      SrcIP SrcPort
  Ports used:    Destination
  Ports:         80
```

show ip 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に関する情報を表示する例を示します。

```
Device# show ip wccp summary
```

```
WCCP version 2 enabled, 2 services
Service      Clients  Routers  Assign      Redirect    Bypass
-----
Default routing table (Router Id: 209.165.200.225):
web-cache    2        1        HASH        GRE         GRE
90           0        0        HASH/MASK   GRE/L2      GRE/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 12: *show ip wccp summary* のフィールドの説明

フィールド	Description
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。
ルータ	WCCP サービスに参加しているルータの数を示します。
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ルータに返します。

関連コマンド

コマンド	説明
clear ip wccp	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。
ip wccp	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。
ip wccp redirect	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。
show ip interface	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。
show ip wccp global counters	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。
show ip wccp service-number detail	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します。
show ip wccp summary	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 **show ipv6 access-list** コマンドを使用します。

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

構文の説明	<i>access-list-name</i>	(任意) アクセス リストの名前。
-------	-------------------------	-------------------

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 Fuji 16.9.2	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 access-list** コマンドは、IPv6 専用である点を除き、**show ip access-list** コマンドと同様の出力を提供します。

例

次の **show ipv6 access-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 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 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 13: **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)。

フィールド	説明
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。
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。 clear ipv6 access-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	パケットの宛先アドレスが一致していなければならない宛先 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。
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
clear ipv6 access-list	IPv6 アクセス リストの一致カウンタをリセットします。
hardware statistics	ハードウェア統計情報の収集をイネーブルにします。
show ip access-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。

コマンド	説明
show ip prefix-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。
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 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

宛先ガード情報を表示するには、特権 EXEC モードで **show ipv6 destination-guard policy** コマンドを使用します。

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

構文の説明

<i>policy-name</i>	(任意) 宛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 Fuji 16.9.2	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 **show ipv6 destination-guard policy** コマンドの出力例を示します。

```
# show ipv6 destination-guard policy poll
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 **show ipv6 destination-guard policy** コマンドの出力例を示します。

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

関連コマンド

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

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 **show ipv6 dhcp** 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 Fuji 16.9.2	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 dhcp コマンドは、クライアントとサーバの両方の ID に対して、リンク層アドレスに基づいた 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、**show ipv6 dhcp** コマンドを使用します。

例

次に、**show ipv6 dhcp** コマンドの出力例を示します。出力の内容は一目瞭然です。

```
# 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 **show ipv6 dhcp binding** コマンドを使用します。

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

構文の説明

<i>ipv6-address</i>	(任意) IPv6 クライアントの DHCP のアドレス。
vrf <i>vrf-name</i>	(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 Fuji 16.9.2	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 dhcp binding 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 vrf-name キーワードと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。



- (注) 設定した VRF が機能するには、**ipv6 dhcp server vrf enable** コマンドをイネーブルにしておく必要があります。このコマンドが設定されていない場合、**show ipv6 dhcp binding** コマンドの出力に設定した VRF が表示されず、デフォルトの VRF の詳細のみが表示されます。

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。

```
# show ipv6 dhcp binding

Client: FE80::A8BB:CCFF:FE00:300
DUID: 00030001AABCC000300
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
```

show ipv6 dhcp binding

```

        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 14: 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、およびアカウントリング (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 **show ipv6 dhcp binding** 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。

```
# 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。

```
# 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

Command	Description
ipv6 dhcp server vrf enable	DHCPv6 サーバ VRF 対応機能をイネーブルにします。
clear ipv6 dhcp binding	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 **show ipv6 dhcp conflict** コマンドを使用します。

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

構文の説明		
	<i>ipv6-address</i>	(任意) IPv6 クライアントの DHCP のアドレス。
	vrf <i>vrf-name</i>	(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 Fuji 16.9.2	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せん。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、**show ipv6 dhcp conflict** 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。

```
# 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

Dynamic Host Configuration Protocol (DHCP) for IPv6 バインディング データベース エージェント情報を表示するには、ユーザ EXEC モードまたは特権モードで **show ipv6 dhcp database** コマンドを使用します。

show ipv6 dhcp database [*agent-URL*]

構文の説明

<i>agent-URL</i>	(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 Fuji 16.9.2	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、**ipv6 dhcp database** 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。

show ipv6 dhcp database 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

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

```
# 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
```

show ipv6 dhcp database

```

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 15: 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キャンセルするまでに 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キャンセルされます。
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

Command	Description
ipv6 dhcp database	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 **show ipv6 dhcp guard policy** コマンドを使用します。

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

構文の説明

<i>policy-name</i>	(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 Fuji 16.9.2	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、**show ipv6 dhcp guard guard** コマンドの出力例を示します。

```
# 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 16 : **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。

show ipv6 dhcp guard policy

フィールド	説明
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
ipv6 dhcp guard policy	DHCPv6 ガード ポリシー名を定義します。

show ipv6 dhcp interface

Dynamic Host Configuration Protocol (DHCP) for IPv6 インターフェイス情報を表示するには、ユーザ EXEC モードまたは特権モードで **show ipv6 dhcp interface** コマンドを使用します。

show ipv6 dhcp interface [*type number*]

構文の説明

<i>type number</i>	(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 (?) を使用してオンラインヘルプを参照してください。
--------------------	---

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 Fuji 16.9.2	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、**show ipv6 dhcp interface** 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。

```
# show ipv6 dhcp interface
Ethernet2/1 is in server mode
  Using pool: svr-pl
  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
```

show ipv6 dhcp interface

```

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 17: 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 **show ipv6 dhcp interface** 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。

```

(config-if)# ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 FastEthernet0/1
# 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

Command	Description
ipv6 dhcp client pd	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。

Command	Description
ipv6 dhcp relay destination	クライアントメッセージを転送する宛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。
ipv6 dhcp server	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 **show ipv6 dhcp relay binding** 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

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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 *vrf-name* キーワードと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、**show ipv6 dhcp relay binding** 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 18 : show ipv6 dhcp relay binding フィールドの説明

フィールド	Description
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 relay binding	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。
debug ipv6 dhcp relay	IPv6 DHCP リレーエージェントのデバッグをイネーブルにします。
debug ipv6 dhcp relay bulk-lease	IPv6 DHCP リレーエージェントの bulk lease クエリのデバッグをイネーブルにします。

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 **show ipv6 eigrp events** 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	パラメータ	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 Fuji 16.9.2	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 eigrp events** 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、**show ipv6 eigrp events** 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。

```
# 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
clear ipv6 eigrp	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。
debug ipv6 eigrp	IPv6 プロトコル用の EIGRP に関する情報を表示します。
ipv6 eigrp	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 **show ipv6 eigrp interfaces** コマンドを使用します。

show ipv6 eigrp [*as-number*] **interfaces** [*type number*] [**detail**]

構文の説明	
<i>as-number</i>	(任意) 自律システム番号。
<i>type</i>	(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。
<i>number</i>	(任意) インターフェイス番号。ネットワーク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 Fuji 16.9.2	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、**show ipv6 eigrp interfaces** 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、**show ipv6 eigrp interfaces** コマンドの出力例を示します。

```
# 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、**show ipv6 eigrp interfaces detail** コマンドの出力例を示します。

show ipv6 eigrp interfaces detail

```
IPv6-EIGRP interfaces for process 1
Interface      Peers    Xmit Queue Un/Reliable  Mean    Pacing Time  Multicast  Pending
              0        0/0        0/0         SRTT    Un/Reliable  Flow Timer  Routes
Et0/0          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。

Device# show ipv6 eigrp interfaces detail tunnel 0

```
EIGRP-IPv6 Interfaces for AS(1)
Interface      Peers    Xmit Queue PeerQ      Mean    Pacing Time  Multicast  Pending
              2        0/0        0/0         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
```

次の表で、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 19: show ipv6 eigrp interfaces フィールドの説明

フィールド	Description
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。

show ipv6 eigrp interfaces

フィールド	Description
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 **show ipv6 eigrp topology** 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

<i>as-number</i>	(任意) 自律システム番号。
<i>ipv6-address</i>	(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 Fuji 16.9.2	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。**show ipv6 eigrp topology** 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、**show ipv6 eigrp topology** 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。

```
# 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,
```

show ipv6 eigrp topology

```
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。

```
# 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 1/55
        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 1/55
        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 **show ipv6 eigrp traffic** コマンドを使用します。

show ipv6 eigrp traffic [*as-number*]

構文の説明	<i>as-number</i>	(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 Fuji 16.9.2	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、**show ipv6 eigrp traffic** コマンドを使用します。

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

```
# 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 20 : **show ipv6 eigrp traffic** フィールドの説明

フィールド	説明
process 9	ipv6 router eigrp コマンドで指定された自律システム (AS) 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
Acks sent/received	送受信された確認応答 (ACK) パケットの数

show ipv6 eigrp traffic

関連コマンド

コマンド	説明
ipv6 router eigrp	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 **show ipv6 general-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 Fuji 16.9.2	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、**show ipv6 general-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、汎用プレフィックスは、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。

```
# 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 21 : **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。
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。

show ipv6 general-prefix

関連コマンド

Command	Description
ipv6 general-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 **show ipv6 interface** 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。
<i>type</i>	(任意) 情報を表示するインターフェイス タイプ。
<i>number</i>	(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 Fuji 16.9.2	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 interface 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。

show ipv6 interface コマンドを使用して、インターフェイスの IPv6 ステータスと設定されたアドレスを検証します。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** とマークされません。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。

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

show ipv6 interface コマンドは、指定されたインターフェイスに関する情報を表示します。

```
(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 unreachable 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 22: 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。

show ipv6 interface 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の重複しています。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。
OFF	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 **show ipv6 interface** コマンドの出力例を示します。

```
# 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。

```
# 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。

```
# 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。

```
# 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 **show ipv6 interface** コマンドの表示に示された追加の重要なフィールドについて説明します。

表 23: 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、アドレスサイズされないため、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。show ipv6 interface 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。

```
(config-if)# ipv6 nd ra-interval 100 60
```

その後で show ipv6 interface を使用すると、間隔が次のように表示されます。

```
(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 unreachable 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。

```
(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 unreachable 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 **show ipv6 interface** 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 24: 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
ipv6 nd prefix	IPv6 ルータ アドバタイズメントに含める IPv6 プレフィックスを設定します。
ipv6 nd ra interval	インターフェイス上の IPv6 RA 送信間隔を設定します。
show ip interface	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 マルチキャスト転送情報ベース (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 **show ipv6 mfib** 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 <i>vrf-name</i>	(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。
<i>ipv6-prefix</i>	(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。
<i>/ prefix-length</i>	(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。
<i>group-address-name</i>	(任意) マルチキャストグループの IPv6 アドレスまたは名前。
<i>source-address-name</i>	(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 Fuji 16.9.2	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、**show ipv6 mfib** 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 25: MFIB エントリとインターフェイスのフラグ

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 : 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 (破棄します)。
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。

```
# 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 26: show ipv6 mfib フィールドの説明

フィールド	Description
Entry Flags	エントりに関する情報です。
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。

```
# 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。

```
# 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。

```
# 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
  Tunnell 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。

```
# 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 ipv6 mfib** コマンドで **verbose** キーワードを指定した場合の出力例を示します。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。

```
# 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 27: `show ipv6 mfib verbose` フィールドの説明

フィールド	Description
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
<code>show ipv6 mfib active</code>	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。
<code>show ipv6 mfib count</code>	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。
<code>show ipv6 mfib interface</code>	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。
<code>show ipv6 mfib status</code>	一般的な MFIB 設定と動作ステータスを表示します。
<code>show ipv6 mfib summary</code>	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 **show ipv6 mld groups** コマンドを使用します。

show ipv6 mld [**vrf** *vrf-name*] **groups** [**link-local**] [*group-name* *group-address*] [*interface-type* *interface-number*] [**detail** | **explicit**]

構文の説明		
	vrf <i>vrf-name</i>	(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。
	<i>group-name</i> <i>group-address</i>	(任意) マルチキャストグループの IPv6 アドレスまたは名前。
	<i>interface-type</i> <i>interface-number</i>	(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 Fuji 16.9.2	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、**show ipv6 mld groups** コマンドは、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、使用したリンクローカルグループ (**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、**show ipv6 mld groups** 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。

```
# 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、**show ipv6 mld groups** コマンドで **detail** キーワードを指定した場合の出力例を示します。

```

# 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、**show ipv6 mld groups** コマンドで **explicit** キーワードを指定した場合の出力例を示します。

```

# 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 28: **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。
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）。

show ipv6 mld groups

フィールド	説明
Expires	<p>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）。</p> <p>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。</p>
Last reporter:	マルチキャストグループのメンバ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

Command	Description
ipv6 mld query-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 **show ipv6 mld interface** 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 Fuji 16.9.2	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、**show ipv6 mld interface** 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 **show ipv6 mld interface** コマンドの出力例を示します。

```
# 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 29 : 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 ipv6 multicast-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	ipv6 mld query-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	ipv6 mld query-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	ipv6 mld query-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

Command	Description
ipv6 mld join-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。
ipv6 mld query-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 <i>vlan-id</i>	(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 Fuji 16.9.2	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。

```
# 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
```

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

```
# 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

Command	Description
ipv6 mld snooping	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。
sdm prefer	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

送信元特定マルチキャスト (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 **show ipv6 mld ssm-map static** 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 <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
	<i>source-address</i>	(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 Fuji 16.9.2	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。

```
# 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。

```
# 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
```

次の表で、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 30 : 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
debug ipv6 mld ssm-map	SSM マッピングのデバッグ メッセージを表示します。
ipv6 mld ssm-map enable	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。
ipv6 mld ssm-map query dns	DNS ベースの SSM マッピングを有効にします。
ipv6 mld ssm-map static	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、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 mld traffic** コマンドを使用します。

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

構文の説明	vrf <i>vrf-name</i>	(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 Fuji 16.9.2	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、**show ipv6 mld traffic** 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。

```
# 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 31 : **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)。
Valid MLD packets	送受信された有効な MLD パケットの数。

フィールド	説明
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

マルチキャストルーティング情報ベース (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 **show ipv6 mrib client** 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	パラメータ	説明
	vrf <i>vrf-name</i>	(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。
	<i>client-name</i> : <i>client-id</i>	(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 Fuji 16.9.2	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

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

```
# 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 32 : *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) mrib ipv6:3 (connection id 2) mrib 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 **show ipv6 mrib route** コマンドを使用します。

show ipv6 mrib [**vrf** *vrf-name*] **route** [**link-local** | **summary**] [*source-address* *source-name* | *] [*groupname-or-address* [*prefix-length*]]]

構文の説明		
vrf <i>vrf-name</i>		(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。
<i>source address-or-name</i>		(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。
<i>groupname or-address</i>		(任意) マルチキャスト グループの IPv6 アドレスまたは名前。
<i>prefix-length</i>		(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 Fuji 16.9.2	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 33: 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 (ローカル非対象)
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、**show ipv6 mrib route** コマンドで **summary** キーワードを指定した場合の出力例を示します。

```
# 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 34: *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

show ip mroute 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 **show ipv6 mroute** 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 **show ipv6 mroute** 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 Fuji 16.9.2	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、**show ipv6 mroute** コマンドで、**show ip mroute** 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、**show ipv6 mroute** 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、**show ipv6 mroute** コマンドを使用します。

例

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

```
# 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場合の **show ipv6 mroute** コマンドの出力例を示します。

```
# 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場合の **show ipv6 mroute** コマンドの出力例を示します。

```
# 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 35 : show ipv6 mroute フィールドの説明

フィールド	説明
Flags:	<p>エントリーに関する情報を提供します。</p> <ul style="list-style-type: none"> • S : スパース。エントリーはスパース 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) エントリーが (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) 上にものみ設定できます。 • 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が送信元に参加できるようにします。 • R : RP ビットを設定。(S,G) エントリーが 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タスを示します。 • 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) エントリーの場合、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) エントリー上に設定され、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	<p>「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。</p> <p>「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。</p>
Interface state:	<p>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。</p> <ul style="list-style-type: none"> • [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、ブルーニング、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)	<p>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。</p> <p>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。</p>
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、破棄されます。
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
ipv6 multicast-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。
show ipv6 mfib	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 **show ipv6 mtu** 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 Fuji 16.9.2	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、**show ipv6 mtu** コマンドの出力例を示します。

```
# 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 **show ipv6 mtu** 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。

```
# 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 36: **show ipv6 mtu** フィールドの説明

フィールド	Description
MTU	宛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。
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。

フィールド	Description
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
ipv6 mtu	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 <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
	<i>interface-type</i>	(任意) インターフェイス タイプを指定します。
	<i>interface-number</i>	(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 Fuji 16.9.2	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 vrf-name** キーワードと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

```
# 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 37: **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先。
2001::1 [8]	カッコ内に表示される値は、宛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 <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
	<i>interface -type</i>	(任意) インターフェイス タイプを指定します。
	<i>interface -number</i>	(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 Fuji 16.9.2	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** *vrf-name* キーワードと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。

```
# 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 **show ipv6 neighbors** コマンドを使用します。

show ipv6 neighbors [*interface-type interface-number* *ipv6-address* *ipv6-hostname* | **statistics**]

構文の説明	
<i>interface-type</i>	(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。
<i>interface-number</i>	(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。
<i>ipv6-address</i>	(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。
<i>ipv6-hostname</i>	(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 Fuji 16.9.2	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 **show ipv6 neighbors** コマンドの出力例を示します。

```
# 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 **show ipv6 neighbors** コマンドの出力例を示します。

```
# 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
```

次の表で、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 38: *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	<p>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。</p> <ul style="list-style-type: none"> • 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。 <p>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。</p> <ul style="list-style-type: none"> • 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。 <p>(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。</p>
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場合の **show ipv6 neighbors** コマンドの出力例を示します。

```
# 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 39: 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)	<p>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。</p> <ul style="list-style-type: none"> • 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)	<p>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。</p> <ul style="list-style-type: none">• 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 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 **show ipv6 ospf** コマンドを使用します。

show ipv6 ospf [*process-id*] [*area-id*] [*rate-limit*]

構文の説明	
<i>process-id</i>	(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。
<i>area-id</i>	(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。
<i>rate-limit</i>	(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 Fuji 16.9.2	このコマンドが導入されました。

show ipv6 ospf の出力例

次に、**show ipv6 ospf** コマンドの出力例を示します。

```
# 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 msec
Retransmission pacing timer 66 msec
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 40: *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 *show ipv6 ospf* コマンドの出力例を示します。

```
# 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 msec
Retransmission pacing timer 66 msec
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 41: 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。

```
# 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 msec
Minimum hold time between two consecutive SPF 10000 msec
Maximum wait time between two consecutive SPF 10000 msec
Minimum LSA interval 5 sec
Minimum LSA arrival 1000 msec
```

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: 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 SPF	連続する SPF 計算間の最小保持時間。
Maximum wait time between two consecutive SPF 10000 msec	連続する SPF 計算間の最大保持時間。
Minimum LSA interval 5 sec	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 msec	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。

```
# 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 43 : *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 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 **show ipv6 ospf border-routers** コマンドを使用します。

show ip ospf [*process-id*] **border-routers**

構文の説明

<i>process-id</i>	(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 Fuji 16.9.2	このコマンドが導入されました。

例

次に、**show ipv6 ospf border-routers** コマンドの出力例を示します。

```
# 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 44: **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	宛先ルータのルータ ID。
[2], [1]	宛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。
FastEthernet0/0, POS4/0	IPv6 OSPF プロトコルを設定するインターフェイス。

フィールド	説明
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	
<i>process-id</i>	(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 Fuji 16.9.2	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 **show ipv6 ospf event** 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。

```
# 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 45: *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。

show ipv6 ospf event

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 **show ipv6 ospf graceful-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 Fuji 16.9.2	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、**show ipv6 ospf graceful-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。

```
# 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 46: 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。

show ipv6 ospf graceful-restart

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
show ipv6 ospf interface	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

<i>process-id</i>	(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。
<i>area-id</i>	(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。
<i>type number</i>	(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 Fuji 16.9.2	このコマンドが導入されました。

例

show ipv6 ospf interface 標準出力例

次に、**showipv6ospfinterface** コマンドの出力例を示します。

```
# 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
```

show ipv6 ospf interface

```

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 47: show ipv6 ospf interface フィールドの説明

フィールド	Description
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 **show ipv6 ospf interface** コマンドの出力例を示します。

```
# 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。

```
# 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。

```
# 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。

```
# 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。

```
# 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。

```
# 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。

```

# 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
show ipv6 ospf graceful-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 **show ipv6 ospf request-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		
<i>process-id</i>	(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。	
<i>area-id</i>	(任意) 指定したエリアに関する情報のみを表示します。	
<i>neighbor</i>	(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。	
<i>interface</i>	(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。	
<i>interface-neighbor</i>	(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 Fuji 16.9.2	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 ospf request-list** コマンドで表示される情報は、OSPF ルーティング操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。

```
# 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 48 : *show ipv6 ospf request-list* フィールドの説明

フィールド	Description
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 **show ipv6 ospf retransmission-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		
	<i>process-id</i>	(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。
	<i>area-id</i>	(任意) 指定したエリアに関する情報のみを表示します。
	<i>neighbor</i>	(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。
	<i>interface</i>	(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。
	<i>interface neighbor</i>	(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 Fuji 16.9.2	このコマンドが導入されました。

show ipv6 ospf retransmission-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

次に、**show ipv6 ospf retransmission-list** コマンドの出力例を示します。

```
# 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 49 : 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 **show ipv6 ospf statistics** 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 Fuji 16.9.2	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 ospf statistics 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、**show ipv6 ospf statistics** 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。

```
# 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 50: *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： <ul style="list-style-type: none"> • 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 **show ipv6 ospf summary-prefix** コマンドを使用します。

show ipv6 ospf [*process-id*] **summary-prefix**

構文の説明

<i>process-id</i>	(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 Fuji 16.9.2	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

次に、**show ipv6 ospf summary-prefix** コマンドの出力例を示します。

```
# show ipv6 ospf summary-prefix
```

```
OSPFv3 Process 1, Summary-prefix
FE00::/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 51 : **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 **show ipv6 ospf timers rate-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 Fuji 16.9.2	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、**show ipv6 ospf timers rate-limit** コマンドを使用します。

例

show ipv6 ospf timers rate-limit の出力例

次に、**show ipv6 ospf timers rate-limit** コマンドの出力例を示します。

```
# 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 52: 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	<i>process-id</i>	(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)。
	<i>interface-type</i> <i>interface-number</i>	(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 Fuji 16.9.2	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、統計情報をクリアするには、**clear ipv6 ospf traffic** コマンドを使用します。

例 次に、OSPFv3 の **show ipv6 ospf traffic** コマンドの出力例を示します。

```
# 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

```

show ipv6 ospf traffic

```

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。

```
# 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 53: show ipv6 ospf traffic フィールドの説明

フィールド	Description
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 エラーのために破棄された場合、そのパケットがこのセクションに表示されます。破棄されたパケットは、適切な破棄理由に従いカウントされます。

フィールド	Description
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破棄された場合、そのパケットがこのセクションに表示されます。破棄されたパケットは、適切な破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
clear ip ospf traffic	OSPFv2 トラフィック統計情報をクリアします。
clear ipv6 ospf traffic	OSPFv3 トラフィック統計情報をクリアします。
show ip ospf traffic	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 **show ipv6 ospf virtual-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 Fuji 16.9.2	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 ospf virtual-links コマンドで表示される情報は、OSPF ルーティング操作のデバッグに役立ちます。

例

次に、**show ipv6 ospf virtual-links** コマンドの出力例を示します。

```
# 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 54: 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 **show ipv6 ospf virtual-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。

```
# 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

<i>rp-address</i>	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 Fuji 16.9.2	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

```
# 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

Protocol Independent Multicast (PIM) 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 Fuji 16.9.2	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、**show ipv6 pim bsr** 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。

```
# 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 55: show ipv6 pim bsr election のフィールドの説明

フィールド	Description
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。

```
# 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。

```
# 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。

```
# 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 **show ipv6 pim df** 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	パラメータ	説明
	vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
	<i>interface-type interface-number</i>	(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。
	<i>rp-address</i>	(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 Fuji 16.9.2	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、**show ipv6 pim df** コマンドを使用します。

例

次に、DF の選択状態を表示する例を示します。

```
# 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。

```
# 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 56 : *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。 <ul style="list-style-type: none"> • 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
debug ipv6 pim df-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。
ipv6 pim rp-address	特定のグループ範囲の PIM RP のアドレスを設定します。
show ipv6 pim df winner	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 **show ipv6 pim group-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 Fuji 16.9.2	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、**show ipv6 pim group-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したりするためにも使用できます。

例

次に、**show ipv6 pim group-map** コマンドの出力例を示します。

```
# 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 57: 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りますためです。 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 **show ipv6 pim interface** 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 Fuji 16.9.1	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、**show ipv6 pim interface** コマンドを使用します。

例

次に、**show ipv6 pim interface** コマンドで **state-on** キーワードを指定した場合の出力例を示します。

```
# 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 58: show ipv6 pim interface フィールドの説明

フィールド	Description
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 **show ipv6 pim interface** コマンドの出力例を示します。

```
(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 59: show ipv6 pim interface フィールドの説明

フィールド	Description
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

Command	Description
show ipv6 pim neighbor	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 **show ipv6 pim join-prune statistic** 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 <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
	<i>interface-type</i>	(任意) インターフェイスタイプ。詳細については、疑問符 (?) を使用してオンラインヘルプを参照してください。

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 Fuji 16.9.2	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。 **show ipv6 pim join-prune statistic** 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。

```
# 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 60: 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。
Transmitted	このインターフェイスで送信したパケットの数。

フィールド	説明
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 **show ipv6 pim limit** コマンドを使用します。

```
show ipv6 pim [vrf vrf-name] limit [interface]
```

構文の説明	vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
	<i>interface</i>	(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 Fuji 16.9.2	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 limit** 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。

```
# show ipv6 pim limit
```

関連コマンド	コマンド	説明
	ipv6 multicast limit	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。
	ipv6 multicast limit cost	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	
<i>vrf vrf-name</i>	(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。
<i>interface-type interface-number</i>	(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 Fuji 16.9.2	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。

```
# 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 61 : 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。

show ipv6 pim neighbor

フィールド	説明
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 **show ipv6 pim range-list** コマンドを使用します。

```
show ipv6 pim [vrf vrf-name ] range-list [config] [rp-address|rp-name]
```

構文の説明		
vrf <i>vrf-name</i>	(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。	
<i>rp-address</i> <i>rp-name</i>	(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 Fuji 16.9.2	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 range-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) モードまたはスペースモードである場合があります。

例

次に、**show ipv6 pim range-list** コマンドの出力例を示します。

```
# 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 62: *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 **show ipv6 pim topology** コマンドを使用します。

```
show ipv6 pim [vrf vrf-name] topology [group-name | group-address [source-address source-name]
| link-local] route-count [detail]
```

構文の説明

vrf <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
<i>group-name</i> <i>group-address</i>	(任意) マルチキャストグループの IPv6 アドレスまたは名前。
<i>source-address</i> <i>source-name</i>	(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 Fuji 16.9.2	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 のみ確認できます。

例

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

```
# 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 63: 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。
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。

フィールド	説明
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
show ipv6 mrib client	MRIB のクライアントに関する情報を表示します。
show ipv6 mrib route	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 **show ipv6 pim traffic** 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 Fuji 16.9.2	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 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、**show ipv6 pim traffic** 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。

```
# 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 64 : 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 **show ipv6 pim tunnel** 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 <i>vrf-name</i>	(任意) Virtual Routing and Forwarding (VRF) コンフィギュレーションを指定します。
	<i>interface-type interface-number</i>	(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 Fuji 16.9.2	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 **show ipv6 pim tunnel** 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 **show ipv6 pim tunnel** コマンドの出力例を示します。

```
# 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 **show ipv6 pim tunnel** コマンドの出力例を示します。

```
# 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 65 : *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 **show ipv6 policy** 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 Fuji 16.9.2	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 **show route-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。

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
show route-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 プレフィックスリスト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 prefix-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。
<i>list-name</i>	(任意) 特定の IPv6 プレフィックスリストの名前。
<i>ipv6-prefix</i>	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。
<i>/ prefix-length</i>	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 <i>ipv6-prefix / prefix-length</i> 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 <i>ipv6-prefix / prefix-length</i> 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 Fuji 16.9.2	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 prefix-list コマンドは、IPv6 専用である点を除き、**show ip prefix-list** コマンドと同様の出力を提供します。

例

次に、**show ipv6 prefix-list** コマンドで **detail** キーワードを指定した場合の出力例を示します。

```
# show ipv6 prefix-list detail
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)
```

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 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、**show ipv6 prefix-list** コマンドで **summary** キーワードを指定した場合の出力例を示します。

```
# show ipv6 prefix-list summary
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
```

関連コマンド

コマンド	説明
clear ipv6 prefix-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-list in	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。

コマンド	説明
distribute-list out	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。
ipv6 prefix-list	IPv6 プレフィックス リストのエントリを作成します。
ipv6 prefix-list description	IPv6 プレフィックス リストのテキスト説明を追加します。
match ipv6 address	プレフィックス 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。
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 **show ipv6 protocols** 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 Fuji 16.9.2	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 protocols コマンドにより表示される情報は、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 **show ipv6 protocols** コマンドの出力例を示します。

```
# 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 67: 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。

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 **show ipv6 rip** 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 Fuji 16.9.2	このコマンドが導入されました。

例

次に、**show ipv6 rip** コマンドの出力例を示します。

```
# 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 68: `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、`show ipv6 rip database` コマンドの出力例を示します。

```

# show ipv6 rip one database

RIP process "one", local RIB
 2001:72D:1000::/64, metric 2

```

show ipv6 rip

```

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 69: 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、show ipv6 rip next-hops コマンドの出力例を示します。

```

# 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 70: 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	<p>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。</p> <p>(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。</p>
[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。

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

```
# 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 71 : **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、**show ipv6 rip vrf next-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 72: 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、**show ipv6 rip vrf database** コマンドの出力例を示します。

```
# show ipv6 rip vrf blue database

RIP VRF "blue", Next Hops
FE80::A8BB:CCFF:FE00:7C00/Ethernet0/0 [1 paths]
```

表 73: **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
clear ipv6 rip	IPv6 RIP ルーティング テーブルからルートを削除します。
debug ipv6 rip	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 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 **show ipv6 routers** 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		
	<i>interface -type</i>	(任意) インターフェイス タイプを指定します。
	<i>interface -number</i>	(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-ink* 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 Fuji 16.9.2	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 **show ipv6 routers** コマンドの出力例を示します。

```
# show ipv6 routers

Device FE80::83B3:60A4 on Tunnel15, 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 Tunnel157, 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。

```
# 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 74 : 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タ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タ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を示します。
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 **show ipv6 routers** コマンドの出力例を示します。

```
# 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
```

show ipv6 routers 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。

```
# show ipv6 routers conflicts
```

```
Device FE80::203:FDFE: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。

```
# show ipv6 routers detail
```

```
Device FE80::A8BB:CCFF:FE00:5B00 on Ethernet0/0, last update 0 min
  Rank 0x811 (elegant), 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 **show ipv6 rpf** 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	
<i>source-vrf</i>	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。
<i>receiver-vrf</i>	ルックアップを開始する VRF の名前またはアドレス。
<i>access-list</i>	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 Fuji 16.9.2	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 rpf 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)、静的 mroute など) から RPF 情報を検索できるため、**show ipv6 rpf** 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。

```
# 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 75: 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	<i>source-guard-policy</i>	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 Fuji 16.9.2	このコマンドが導入されました。

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

```
# 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 選択的パケット破棄 (SPD) 設定を表示するには、特権 EXEC モードで **show ipv6 spd** 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 Fuji 16.9.2	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、**show ipv6 spd** コマンドを使用します。

例

次に、**show ipv6 spd** コマンドの出力例を示します。

```
# 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 76: show ipv6 spd フィールドの説明

フィールド	Description
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
ipv6 spd queue max-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 **show ipv6 static** 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	
<i>ipv6-address</i>	(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。
<i>ipv6-prefix</i>	(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。
<i>/prefix-length</i>	(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。
<i>type</i>	(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。
<i>number</i>	(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。 <ul style="list-style-type: none"> 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 Fuji 16.9.2	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 static コマンドは、IPv6 固有である点を除き、**show ip route** コマンドと同様の出力を提供します。

ipv6-address 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ト情報だけが表示されます。コマンドシンタックスで指定された条件に一致する情報だけが表示されます。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。

```
# 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 77: **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を示します。

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場合の **show ipv6 route** コマンドの出力例を示します。

```
# 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。

```
# 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。

```
# 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、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、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、ルートが有効でない理由

```
# 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
ipv6 route	静的 IPv6 ルートを確立します。
show ip route	ルーティング テーブルの現在の状態を表示します。
show ipv6 interface	IPv6 インターフェイス情報を表示します。
show ipv6 route summary	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。
show ipv6 tunnel	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 **show ipv6 traffic** 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。
	<i>interface type number</i>	(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 Fuji 16.9.2	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 traffic** コマンドは、IPv6 専用である点を除き、**show ip traffic** コマンドと同様の出力を提供します。

例

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

```
# 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。

```
# 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:FDFE: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。

```
# 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:FDFE: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 78 : 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。 <ul style="list-style-type: none"> • routing : 宛先までのルートがないことを示します。 • admin : 宛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先には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 key chain

キーチェーンを表示するには、**show key chain** コマンドを使用します。

show key chain [*name-of-chain*]

構文の説明

<i>name-of-chain</i>	(任意) キーチェーンコマンドで命名された表示対象のキーチェーン名。
----------------------	------------------------------------

コマンド デフォルト

パラメータを指定せずにコマンドを使用すると、すべてのキーチェーンのリストを表示します。

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 Fuji 16.9.2	このコマンドが導入されました。

例

次に、**show key chain** コマンドの出力例を示します。

```

show key chain
Device# show key chain

Key-chain AuthenticationGLBP:
  key 1 -- text "Thisisasecretkey"
    accept lifetime (always valid) - (always valid) [valid now]
    send lifetime (always valid) - (always valid) [valid now]
Key-chain glbp2:
  key 100 -- text "abc123"
    accept lifetime (always valid) - (always valid) [valid now]
    send lifetime (always valid) - (always valid) [valid now]

```

関連コマンド

コマンド	説明
key-string	キーの認証文字列を指定します。
send-lifetime	キーチェーンの認証キーが有効に送信される期間を設定します。

show track

トラッキングプロセスが追跡したオブジェクトに関する情報を表示するには、特権 EXEC モードで **show track** コマンドを使用します。

```
show track [object-number [brief] | application [brief] | interface [brief] | ip[route [brief] |
[sla [brief]] | ipv6 [route [brief]] | list [route [brief]] | resolution [ip | ipv6] | stub-object [brief]
| summary | timers]
```

構文の説明

object-number	(任意) トラッキング対象オブジェクトを表すオブジェクト番号。範囲は 1 ~ 1000 です。
brief	(任意) 先行する引数やキーワードに関連する 1 行の情報を表示します。
application	(任意) トラッキング対象のアプリケーション オブジェクトを表示します。
interface	(任意) トラッキング対象のインターフェイス オブジェクトを表示します。
ip route	(任意) トラッキング対象の IP ルート オブジェクトを表示します。
ip sla	(任意) トラッキング対象の IP SLA オブジェクトを表示します。
ipv6 route	(任意) トラッキング対象の IPv6 ルート オブジェクトを表示します。
list	(任意) プール オブジェクトを表示します。
resolution	(任意) トラッキング対象パラメータの解像度を表示します。
summary	(任意) 指定されたオブジェクトの概要を表示します。
timers	(任意) ポーリング間隔タイマーを表示します。

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 Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

トラッキングプロセスによってトラッキングされているオブジェクトに関する情報を表示するには、このコマンドを使用します。引数やキーワードを指定しない場合は、すべてのオブジェクトの情報が表示されます。

最大 1000 のオブジェクトを追跡できます。トラッキング対象オブジェクトは 1000 個設定できますが、各トラッキング対象オブジェクトは CPU リソースを使用します。デバイスで使用可能な CPU リソースの合計は、トラフィック負荷などの変数や、他のプロトコルがどのように設定され実行されているかに応じて異なります。1000 個の追跡対象オブジェクトが使用できる

かどうかは、使用可能な CPU によって異なります。特定のサイト トラフィック条件下でサービスが機能することを保証するには、サイト上でテストを実施する必要があります。

例

次に、インターフェイスで IP ルーティングの状態をトラッキングした場合の例を示します。

```
Device# show track 1

Track 1
Interface GigabitEthernet 1/0/1 ip routing
IP routing is Down (no IP addr)
  1 change, last change 00:01:08
```

次の表で、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 79: *show track* フィールドの説明

フィールド	説明
Track	トラッキング対象オブジェクトの数。
Interface GigabitEthernet 1/0/1 IP routing	インターフェイス タイプ、インターフェイス番号、およびトラッキング対象オブジェクト。
IP routing is	Up または Down で表示されるオブジェクトの状態の値。オブジェクトがダウンしている場合は、理由が示されます。
1 change、last change	トラッキング対象オブジェクトの状態が変更された回数と、最後の変更からの経過時間 (hh:mm:ss で表示)。

関連コマンド

Command	Description
show track resolution	追跡対象パラメータの解像度を表示します。
track interface	インターフェイスをトラッキングされるように設定し、トラッキング コンフィギュレーション モードを開始します。
track ip route	IP ルートの状態を追跡し、トラッキング コンフィギュレーション モードを開始します。

track

Gateway Load Balancing Protocol (GLBP) の重み付けがインターフェイスの状態に基づいて変更されている場合にトラッキング対象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 **track** コマンドを使用します。トラッキングを削除するには、このコマンドの **no** 形式を使用します。

track *object-number* **interface** *type number* **line-protocol** | **ip routing** | **ipv6 routing**
no track *object-number* **interface** *type number* **line-protocol** | **ip routing** | **ipv6 routing**

構文の説明

<i>object-number</i>	トラッキングされるインターフェイスを表すオブジェクト番号。値の範囲は 1 ~ 1000 です。
interface <i>type number</i>	トラッキングするインターフェイス タイプおよび番号。
line-protocol	インターフェイスがアップ状態かどうかをトラッキングします。
ip routing	インターフェイスがアップの状態であることを GLBP に報告する前に、IP ルーティングが有効かどうか、インターフェイスに IP アドレスが設定されているか、インターフェイスがアップの状態かどうかをトラッキングします。
ipv6 routing	インターフェイスがアップの状態であることを GLBP に報告する前に、IPv6 ルーティングが有効かどうか、インターフェイスに IP アドレスが設定されているか、インターフェイスがアップの状態かどうかをトラッキングします。

コマンド デフォルト

インターフェイスの状態はトラッキングされません。

コマンド モード

グローバル コンフィギュレーション (config)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

トラッキング対象インターフェイスのパラメータを設定するには、**track** コマンドと併せて **glbp weighting** および **glbp weighting track** コマンドを使用します。GLBP デバイスのトラッキング対象インターフェイスがダウンすると、そのデバイスの重み値は減らされます。重み値が指定された最小値を下回った場合、デバイスは、アクティブ GLBP 仮想フォワーダとしての機能を失います。

最大 1000 のオブジェクトを追跡できます。トラッキング対象オブジェクトは 1000 個設定できますが、各トラッキング対象オブジェクトは CPU リソースを使用します。デバイスで使用可能な CPU リソースの合計は、トラフィック負荷などの変数や、他のプロトコルがどのように設定され実行されているかに応じて異なります。1000 個の追跡対象オブジェクトが使用できる

かどうかは、使用可能な CPU によって異なります。特定のサイト トラフィック条件下でサービスが機能することを保証するには、サイト上でテストを実施する必要があります。

例

次に、TenGigabitEthernet インターフェイス 0/0/1 が、GigabitEthernet インターフェイス 1/0/1 および 1/0/3 がアップの状態にあるかどうかをトラッキングする例を示します。GigabitEthernet インターフェイスのいずれかがダウンすると、GLBP の重み値は、デフォルト値である 10 まで減らされます。両方の GigabitEthernet インターフェイスがダウンすると、GLBP の重み値は下限しきい値未満に下がり、デバイスはアクティブフォワーダではなくなります。アクティブフォワーダとしての役割を再開するには、デバイスは、両方のトラッキング対象インターフェイスをアップの状態に戻し、重み値を上限しきい値を超える値に上げる必要があります。

```
Device(config)# track 1 interface GigabitEthernet 1/0/1 line-protocol
Device(config-track)# exit
Device(config)# track 2 interface GigabitEthernet 1/0/3 line-protocol
Device(config-track)# exit
Device(config)# interface TenGigabitEthernet 0/0/1
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 weighting 110 lower 95 upper 105
Device(config-if)# glbp 10 weighting track 1
Device(config-if)# glbp 10 weighting track 2
```

関連コマンド

コマンド	説明
glbp weighting	GLBP ゲートウェイの初期重み値を指定します。
glbp weighting track	GLBP ゲートウェイの重み付けに影響する、追跡対象のオブジェクトを指定します。

vrrp

Virtual Router Redundancy Protocol バージョン 3 (VRRPv3) グループを作成し、VRRPv3 グループ コンフィギュレーション モードを開始するには、**vrrp** を使用します。VRRPv3 グループを削除するには、このコマンドの **no** 形式を使用します。

```
vrrp group-id address-family {ipv4 | ipv6}
no vrrp group-id address-family {ipv4 | ipv6}
```

構文の説明

<i>group-id</i>	仮想ルータ グループ番号。範囲は 1 ~ 255 です。
address-family	この VRRP グループのアドレス ファミリを指定します。
ipv4	(任意) IPv4 アドレスを指定します。
ipv6	(任意) IPv6 アドレスを指定します。

コマンド デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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

次の例は、VRRPv3 グループの作成方法と VRRP コンフィギュレーション モードの開始方法を示しています。

```
Device(config-if)# vrrp 3 address-family ipv4
```

関連コマンド

コマンド	説明
timers advertise	アドバタイズメントタイマーを設定します (ミリ秒単位)。

vrrp description

Virtual Router Redundancy Protocol (VRRP) に説明を割り当てるには、インターフェイス コンフィギュレーション モードで **vrrp description** コマンドを使用します。説明を削除するには、このコマンドの **no** 形式を使用します。

description *text*

no description

構文の説明

<i>text</i>	グループの目的または用途を説明するテキスト (最大 80 文字)。
-------------	-----------------------------------

コマンド デフォルト

VRRP グループの説明はありません。

コマンド モード

VRRP 設定 (config-if-vrrp)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

例

次の例では、VRRP を有効にしています。VRRP グループ 1 は、「Building A – Marketing and Administration (ビルディング A : マーケティングおよび管理)」と説明されます。

```
Device(config-if-vrrp)# description Building A - Marketing and Administration
```

関連コマンド

コマンド	説明
vrrp	VRRPv3 グループを作成し、VRRPv3 グループ コンフィギュレーション モードを開始します。

vrrp preempt

デバイスに現在のプライマリ仮想ルータより高い優先順位が与えられている場合、そのデバイスが Virtual Router Redundancy Protocol (VRRP) グループのプライマリ仮想ルータの機能を引き継ぐように設定するには、VRRP コンフィギュレーション モードで **preempt** 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。

preempt [**delay minimum seconds**]
no preempt

構文の説明

delay minimum seconds	(任意) プライマリの所有権を要求するアドバタイズメントを発行するまでに、デバイスが待機する秒数。デフォルト遅延値は 0 秒です。
------------------------------	---

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

VRRP 設定 (config-if-vrrp)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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、このコマンドで設定されるデバイスは、現在のプライマリ仮想ルータよりも高い優先順位を持つ場合、プライマリ仮想ルータとしての機能を引き継ぎます。VRRP デバイスが、プライマリ所有権を要求するアドバタイズメントを発行するまで、指定された秒数待機するように遅延時間を設定できます。



(注) このコマンドの設定にかかわらず、IP アドレスの所有者であるデバイスがプリエンプション処理します。

例

次に、デバイスの 200 の優先順位が現在のプライマリ仮想ルータの優先順位よりも高い場合に、デバイスが現在のプライマリ仮想ルータをプリエンプション処理するように設定する例を示します。デバイスは、現在のプライマリ仮想ルータをプリエンプション処理する場合、プライマリ仮想ルータであることを要求するアドバタイズメントを発行するまでに 15 秒待機します。

```
Device(config-if-vrrp)#preempt delay minimum 15
```


関連コマンド

コマンド	説明
vrrp	VRRPv3 グループを作成し、VRRPv3 グループ コンフィギュレーション モードを開始します。
priority	VRRP グループ内のデバイスの優先度レベルを設定します。

vrrp priority

Virtual Router Redundancy Protocol (VRRP) 内のデバイスの優先度レベルを設定するには、インターフェイス コンフィギュレーション モードで **priority** コマンドを使用します。デバイスの優先度レベルを削除するには、このコマンドの **no** 形式を使用します。

priority level
no priority level

構文の説明

<i>level</i>	VRRP グループ内のデバイスの優先順位。有効な範囲は 1 ~ 254 です。デフォルトは 100 です。
--------------	---

コマンド デフォルト

優先度レベルはデフォルト値の 100 に設定されています。

コマンド モード

VRRP 設定 (config-if-vrrp)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	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、どのデバイスをプライマリ仮想ルータにするかを制御できます。

例

次に、デバイスを 254 の優先順位に設定する例を示します。

```
Device(config-if-vrrp)# priority 254
```

関連コマンド

コマンド	説明
vrrp	VRRPv3 グループを作成し、VRRPv3 グループ コンフィギュレーション モードを開始します。
vrrp preempt	デバイスに現在のプライマリ仮想ルータより高い優先順位が与えられている場合、そのデバイスが VRRP グループのプライマリ仮想ルータの機能を引き継ぐように設定します。

vrrp timers advertise

Virtual Router Redundancy Protocol (VRRP) グループ内のプライマリ仮想ルータによる連続したアドバタイズメント間の間隔を設定するには、VRRP コンフィギュレーションモードで **timers advertise** 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。

timers advertise [*msec*] *interval*
no timers advertise [*msec*] *interval*

構文の説明	
<i>group</i>	仮想ルータ グループ番号。グループ番号の範囲は 1 ~ 255 です。
<i>msec</i>	(任意) アドバタイズメント時間の単位を秒からミリ秒に変更します。このキーワードを付加しないと、アドバタイズメント間隔は秒単位になります。
<i>interval</i>	プライマリ仮想ルータによる連続したアドバタイズメント間の時間間隔。 msec キーワードを指定しなかった場合、間隔は秒単位になります。デフォルト値は 1 秒です。有効範囲は 1 ~ 255 秒です。 msec キーワードを指定した場合、有効な範囲は 50 ~ 999 ミリ秒です。

コマンドデフォルト デフォルトの間隔である 1 秒に設定されています。

コマンドモード VRRP 設定 (config-if-vrrp)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン プライマリ仮想ルータから送信されるアドバタイズメントは、現在のプライマリ仮想ルータの状態と優先順位を伝えます。

vrrp timers advertise コマンドは、連続するアドバタイズメントパケットの間の時間間隔と、プライマリルータがダウンしていると他のルータが宣言するまでの時間を設定します。タイマー値が設定されていないルータまたはアクセスサーバは、プライマリルータからタイマー値を取得できます。プライマリルータで設定されたタイマーは、他のすべてのタイマー設定を常に上書きします。VRRP グループ内のすべてのルータが同じタイマー値を使用する必要があります。同じタイマー値が設定されていないと、VRRP グループ内のデバイスが相互通信せず、正しく設定されていないデバイスのステータスがプライマリに変わります。

例

次に、プライマリ仮想ルータがアドバタイズメントを 4 秒ごとに送信するように設定する例を示します。

```
Device(config-if-vrrp)# timers advertise 4
```

関連コマンド

コマンド	説明
vrrp	VRRPv3 グループを作成し、VRRPv3 グループ コンフィギュレーション モードを開始します。
timers learn	VRRP グループのバックアップ仮想ルータとして動作するときに、プライマリ仮想ルータが使用していたアドバタイズ間隔を学習するようにデバイスを設定します。

vrrs leader

リーダーの名前を Virtual Router Redundancy Service (VRRS) に登録されるように指定するには、**vrrs leader** コマンドを使用します。指定された VRRS リーダーを削除するには、このコマンドの **no** 形式を使用します。

vrrs leader *vrrs-leader-name*
no vrrs leader *vrrs-leader-name*

構文の説明

<i>vrrs-leader-name</i>	リードする VRRS タグの名前。
-------------------------	-------------------

コマンド デフォルト

登録済みの VRRS 名はデフォルトで使用不可になっています。

コマンド モード

VRRP 設定 (config-if-vrrp)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

例

次に、VRRS に登録されるリーダーの名前を指定する例を示します。

```
Device(config-if-vrrp)# vrrs leader leader-1
```

関連コマンド

コマンド	説明
vrrp	VRRP グループを作成し、VRRP コンフィギュレーションモードを開始します。

