



ipv6-r1

- [sec-level minimum, 3 ページ](#)
- [server name \(IPv6 TACACS+\) , 5 ページ](#)
- [show ipv6 access-list, 7 ページ](#)
- [show ipv6 dhcp conflict, 11 ページ](#)
- [show ipv6 interface, 13 ページ](#)
- [show ipv6 mld snooping, 23 ページ](#)
- [show ipv6 nd ra-throttle policy, 25 ページ](#)
- [show ipv6 nd ra-throttle vlan, 26 ページ](#)
- [show ipv6 nd rguard policy, 27 ページ](#)
- [show ipv6 neighbor binding, 29 ページ](#)
- [show ipv6 neighbors, 31 ページ](#)
- [show ipv6 protocols, 38 ページ](#)
- [show ipv6 route, 43 ページ](#)
- [show ipv6 snooping capture-policy, 49 ページ](#)
- [show ipv6 snooping counters, 51 ページ](#)
- [show ipv6 snooping features, 53 ページ](#)
- [show ipv6 snooping policies, 55 ページ](#)
- [show ipv6 traffic, 57 ページ](#)
- [summary-prefix \(OSPFv3\) , 61 ページ](#)
- [throttle-period, 64 ページ](#)
- [timers spf \(IPv6\) , 65 ページ](#)
- [timers throttle lsa, 67 ページ](#)

- [tracking, 69 ページ](#)
- [tunnel mode ipv6ip, 72 ページ](#)
- [vlan configuration, 78 ページ](#)

sec-level minimum

暗号化生成アドレス（CGA）オプションを使用する場合の最小セキュリティレベルパラメータ値を指定するには、ネイバー探索（ND）インスペクションポリシーコンフィギュレーションモードで **sec-level minimum** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

sec-level minimum *value*

no sec-level minimum *value*

構文の説明

<i>value</i>	1～7の値で表す、最小限のセキュリティレベル。デフォルトのセキュリティレベルは1です。最も安全なレベルは3です。
--------------	--

コマンド デフォルト

デフォルトのセキュリティレベルは1です。

コマンド モード

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

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

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
15.3(1)S	このコマンドが Cisco IOS Release 15.3(1)S に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

sec-level minimum コマンドは、CGA オプションを使用する場合の最小セキュリティレベルパラメータ値を指定します。**sec-level minimum** コマンドは、**ipv6 nd inspection policy** コマンドを使用してNDインスペクションポリシーコンフィギュレーションモードをイネーブルにした後で使用します。

例

次に、`policy1` として ND ポリシー名を定義し、ルータを ND インスペクションポリシー コンフィギュレーションモードにして、最小 CGA セキュリティレベルとして 2 を指定する例を示します。

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# sec-level minimum 2
```

関連コマンド

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

server name (IPv6 TACACS+)

IPv6 TACACS+ サーバを指定するには、TACACS+ グループ サーバ コンフィギュレーション モードで **server name** コマンドを使用します。コンフィギュレーションから IPv6 TACACS+ サーバを削除するには、このコマンドの **no** 形式を使用します。

server name *server-name*

no server name *server-name*

構文の説明

server-name	使用する IPv6 TACACS+ サーバ。
-------------	------------------------

コマンド デフォルト

サーバ名は指定されていません。

コマンド モード

TACACS+ グループ サーバ コンフィギュレーション (config-*sg-tacacs+*)

コマンド履歴

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

使用上のガイドライン

このコマンドを設定する前に、**aaa group server tacacs** コマンドを設定します。

IPv6 TACACS+ サーバを指定するには、**server name** コマンドを入力します。

例

次に、server1 という名前の IPv6 TACACS+ サーバを指定する例を示します。

```
Router(config)# aaa group server tacacs+
Router(config-sg-tacacs+)# server name server1
```

関連コマンド

コマンド	説明
aaa group server tacacs	IPv6 または IPv4 の TACACS+ サーバを設定し、TACACS+サーバ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 デフォルト

すべての IPv6 アクセス リストが表示されます。

コマンド モード

ユーザ EXEC 特権 EXEC

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.0(23)S	プライオリティフィールドがシーケンスに変更され、レイヤ4プロトコル情報（拡張 IPv6 アクセス リスト機能）が表示出力に追加されました。
12.2(13)T	このコマンドが、Cisco IOS Release 12.2(13)T に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
12.2(50)SY	このコマンドが変更されました。IPv4 および IPv6 ハードウェア統計情報に関する情報が表示されます。

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

使用上のガイドライン IPv6 専用である点を除いて、**show ipv6 access-list** コマンドの出力は **show ip access-list** コマンドと類似しています。

例 次の例では、**show ipv6 access-list** コマンドで出力された inbound、tcptraffic、および outbound という名の IPv6 アクセス リストを示します。

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

次の出力例は、IPSec で使用するための IPv6 アクセス リスト情報を示しています。

```
Router# 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
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 1 : show ipv6 access-list のフィールドの説明

フィールド	説明
ipv6 access list inbound	IPv6 アクセス リスト名 (例 : inbound)。
permit	指定されたプロトコルタイプと一致するパケットを許可します。
tcp	伝送制御プロトコル。パケットが一致しなければならない高いレベル (レイヤ 4) のプロトコルタイプ。
any	::/0 と同じです。
eq	TCP または UDP パケットの送信元または宛先ポートを比較する equal オペランド。

フィールド	説明
bgp	ボーダー ゲートウェイ プロトコル。パケットが等しくなる必要がある低レベル（レイヤ 3）プロトコル タイプ。
reflect	再帰 IPv6 アクセス リストを示します。
tcptraffic (8 matches)	再帰 IPv6 アクセス リストの名前と、アクセスリストに一致した数。 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する必要がある送信元 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する必要がある宛先 IPv6 ホストアドレス。
11000	発信接続用の一時的な送信元ポート番号。
timeout 300	一時的な IPv6 再帰アクセス リスト tcptraffic が指定されたセッションをタイムアウトするまでのアイドル時間の間隔の合計（秒単位）。
(time left 243)	一時的な IPv6 再帰アクセス リスト tcptraffic が指定されたセッションを削除するまでのアイドル時間の合計（秒単位）。指定したセッションと一致するトラフィックを追加で受信すると、この値が 300 秒にリセットされます。
evaluate udptraffic	udptraffic という名前の IPv6 再帰アクセス リストが outbound という名前の IPv6 アクセス リスト内にネストされ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。
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 dhcp conflict

アドレスをクライアントに提供するときに、Dynamic Host Configuration Protocol for IPv6 (DHCPv6) サーバで見つかっ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 用 DHCP クライアントのアドレス。
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
12.4(24)T	このコマンドが導入されました。
Cisco IOS XE Release 2.5	このコマンドが、Cisco IOS XE Release 2.5 に統合されました。
15.1(2)S	このコマンドが変更されました。キーワードおよび引数 vrf <i>vrf-name</i> が追加されました。
Cisco IOS XE リリース 3.3S	このコマンドが変更されました。キーワードおよび引数 vrf <i>vrf-name</i> が追加されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

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

例

次に、**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示します。

```
Router# 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 interface

IPv6 用に設定されたインターフェイスの使用可能性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 ステータスおよびコンフィギュレーションの要約を表示します。
<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
12.2(2)T	このコマンドが導入されました。
12.2(4)T	OK、TENTATIVE、DUPLICATE、ICMP redirects、および ND DAD フィールドがコマンド出力に追加されました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。

リリース	変更内容
12.2(25)S	コマンド出力が、現在のユニキャスト RPF の設定情報を表示するように更新されました。
12.4(2)T	コマンド出力が、インターフェイスを介してデバイスによってアドバタイズされるデフォルトルータプリファレンス (DRP) のプリファレンス値のステータスを表示するように更新されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.4(4)T	コマンド出力が、IPv6 のホットスタンバイ ルータ プロトコル (HSRP) 情報を表示するように更新されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドは、Cisco ASR 1000 シリーズ デバイスで追加されました。
12.4(24)T	コマンド出力が、Dynamic Host Configuration Protocol (DHCP) から送信されたアドレスを表示するように更新されました。
12.2(50)SY	このコマンドが、Cisco IOS Release 12.2(50)SY に統合されました。
15.0(1)SY	このコマンドが、Cisco IOS Release 15.0(1)SY に統合されました。
15.2(2)SNG	このコマンドが、Cisco ASR 901 シリーズのアグリゲーションサービス デバイスに実装されました。
15.3(1)S	このコマンドが Cisco IOS Release 15.3(1)S に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン **show ipv6 interface** コマンドの出力は、IPv6 に固有である点を除き、**show ip interface** コマンドの出力と似ています。

インターフェイスの IPv6 ステータスおよび設定されたアドレスを確認するには、**show ipv6 interface** コマンドを使用します。**show ipv6 interface** コマンドは、IPv6 がこのインターフェイスおよび設定済みの機能の操作に使用しているパラメータも表示します。

インターフェイスのハードウェアが使用できる場合、インターフェイスはupとマークされます。インターフェイスがIPv6用の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。

オプションのインターフェイスタイプおよび番号を指定すると、その特定のインターフェイスに関する情報だけが表示されます。特定のインターフェイスについて、インターフェイスで設定されたIPv6ネイバー探索（ND）プレフィックスを表示するには、prefixキーワードを入力します。

例

例

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。

```
Device(config)# show ipv6 interface ethernet0/0
Ethernet0/0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:6700
No Virtual link-local address(es):
Global unicast address(es):
  2001::1, subnet is 2001::/64 [DUP]
  2001::A8BB:CCFF:FE00:6700, subnet is 2001::/64 [EUI]
  2001:100::1, subnet is 2001:100::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF00:1
  FF02::1:FF00:6700
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP 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.
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 2 : **show ipv6 interface** のフィールドの説明

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）、および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。インターフェイスハードウェアが使用可能な場合、インターフェイスは「up」とマークされます。インターフェイスが使用可能になるには、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ければなりません。

フィールド	説明
line protocol is up、down (down は、出力例では示されていません)	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するかどうか (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。インターフェイスが使用可能であるためには、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である必要があります。
IPv6 is enabled, stalled, disabled (ストールまたはディセーブルについては、出力例では示されていません)	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 がイネーブルの場合、インターフェイスは「 enabled 」とマークされます。重複アドレス検出処理がインターフェイスのリンクローカルアドレスを重複アドレスと識別した場合、IPv6 パケットは、そのインターフェイスでディセーブルであり、インターフェイスは「 stalled 」とマークされます。IPv6 がイネーブルでない場合、インターフェイスは「 disabled 」とマークされます。
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):	この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上で送信されるエラーメッセージ間の最小間隔をミリ秒で指定します。
ICMP redirects	インターフェイスでのインターネット制御メッセージプロトコル (ICMP) IPv6 リダイレクトメッセージの状態 (メッセージの送信かイネーブルかディセーブルか)。

フィールド	説明
ND DAD	インターフェイスでの重複アドレス検出の状態（イネーブルまたはディスーブル）。
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。
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 以降では、このインターフェイスのこのデバイスから送信されるデフォルトルータプリファレンス（DRP）値を表示します。
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。

例

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 アドレスに関連付けることができる属性の情報を表示します。

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ときの指定どおり、エニーキャストアドレスです。
CAL	カレンダー。アドレスは時限制で、有効な推奨ライフタイムがあります。

属性	説明
DEP	非推奨。時限アドレスは非推奨です。
DUP	重複。アドレスは、重複アドレス検出 (DAD) で判断されたとおり、重複しています。DAD を再試行するには、インターフェイスで shutdown または no shutdown コマンドを使用する必要があります。
EUI	EUI-64 ベース。アドレスは EUI-64 を使用して収集されました。
OFF	オフリンク。アドレスは、オフリンクです。
OOD	Overly Optimistic DAD。このアドレスに対しては 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	一時的。アドレスは、DAD ごとに一時的な状態です。
UNA	非アクティブ。仮想アドレスはアクティブではなく、スタンバイ状態です。
VIRT	仮想。アドレスは仮想で、HSRP、VRRP、または GLBP によって管理されます。

次に、**brief** キーワードを入力した **show ipv6 interface** コマンドの出力例を示します。

```
Device# show ipv6 interface brief
Ethernet0 is up, line protocol is up
Ethernet0          [up/up]
  unassigned
Ethernet1          [up/up]
  2001:0DB8:1000:/29
Ethernet2          [up/up]
  2001:0DB8:2000:/29
Ethernet3          [up/up]
  2001:0DB8:3000:/29
Ethernet4          [up/down]
  2001:0DB8:4000:/29
Ethernet5          [administratively down/down]
  2001:123::210:7BFF:FEC2:ACD8
Interface          Status          IPv6 Address
Ethernet0          up              3FFE:C00:0:1:260:3EFF:FE11:6770
Ethernet1          up              unassigned
Fddi0              up              3FFE:C00:0:2:260:3EFF:FE11:6772
Serial0            administratively down unassigned
Serial1            administratively down unassigned
Serial2            administratively down unassigned
```

```

Serial3      administratively down unassigned
Tunnel0     up                          unnumbered (Ethernet0)
Tunnel1     up                          3FFE:700:20:1::12

```

例

この出力例では、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を示します。

```

Device# show ipv6 interface Ethernet 0/0 prefix

interface Ethernet0/0
  ipv6 address 2001:0DB8::1/64
  ipv6 address 2001:0DB8::2/64
  ipv6 nd prefix 2001:0DB8:2::/64
  ipv6 nd prefix 2001:0DB8:3::/64 2592000 604800 off-link
end
.
.
.
IPv6 Prefix Advertisements Ethernet0/0
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default
       N - Not advertised, C - Calendar
       default [LA] Valid lifetime 2592000, preferred lifetime 604800
AD  2001:0DB8:1::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
APD 2001:0DB8:2::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
P   2001:0DB8:3::/64 [A] Valid lifetime 2592000, preferred lifetime 604800

```

デフォルトプレフィックスは `ipv6 nd prefix default` コマンドを使用して設定されるパラメータを示しています。

例

この出力例は、インターフェイス経由でこのデバイスによってアドバタイズされる DRP プリファレンス値の状態を示しています。

```

Device# show ipv6 interface gigabitethernet 0/1
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::130
Description: Management network (dual stack)
Global unicast address(es):
  FEC0:240:104:1000::130, subnet is FEC0:240:104:1000::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF00:130
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Low
Hosts use stateless autoconfig for addresses.

```

例

インターフェイスで HSRP IPv6 を初めて設定するとき、インターフェイスの IPv6 リンクローカルアドレスはアドバタイズされなくなるため、非アクティブ (UNA) にマークされます。また、HSRP IPv6 仮想リンクローカルアドレスが、UNA 属性と一時的な DAD (TEN) 属性が設定され

て仮想リンクローカルアドレスリストに追加されます。さらに、HSRP IPv6 マルチキャストアドレスをリッスンするようにインターフェイスがプログラムされます。

この出力例では、HSRP IPv6 がインターフェイスで設定されるときに UNA および TEN 属性のステータスが表示されています。

```
Device# show ipv6 interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80:2::2 [UNA]
Virtual link-local address(es):
  FE80::205:73FF:FEA0:1 [UNA/TEN]
Global unicast address(es):
  2001:2::2, subnet is 2001:2::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::66
  FF02::1:FF00:2
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ND DAD is enabled, number of DAD attempts: 1
```

HSRP グループがアクティブになると、UNA および TEN 属性はクリアされ、Overly Optimistic DAD (OOD) 属性が設定されます。HSRP 仮想 IPv6 アドレスの送信要求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。

この出力例では、HSRP グループがアクティブになったときの UNA、TEN、および OOD 属性のステータスが表示されています。

```
Device# show ipv6 interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80:2::2 [UNA]
Virtual link-local address(es):
  FE80::205:73FF:FEA0:1 [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 が設定されているときに `show ipv6 interface` コマンドで表示される追加の重要なフィールドについて説明します。

表 3: HSRP が設定されているときの `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]	インターフェイスの IPv6 リンクローカルアドレスはアドバタイズされないため、UNA にマークされます。
FE80::205:73FF:FEA0:1 [UNA/TEN]	UNA および 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。

フィールド	説明
FF02::66	HSRP IPv6 マルチキャストアドレス。
FE80::205:73FF:FEA0:1 [OPT]	HSRP はアクティブになり、HSRP 仮想アドレスは OPT にマークされます。
FF02::1:FFA0:1	HSRP 送信要求ノードマルチキャストアドレス。

例

インターフェイスでモバイルIPv6をイネーブルにすると、IPv6ルータアドバタイズメント (RA) の最小送信間隔を設定できます。設定されている場合、**show ipv6 interface** コマンドの出力で最小 RA 間隔がレポートされます。最小 RA 間隔が明示的に設定されていない場合、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 で最大 RA 間隔が 100 秒に設定され、最小 RA 間隔が 60 秒として設定されています。

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

その後、**show ipv6 interface** を使用すると、間隔は次のように表示されます。

```
Device(config)# show ipv6 interface ethernet 1/0
Ethernet1/0 is administratively down, line protocol is down
IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:5A01 [TEN]
No Virtual link-local address(es):
No global unicast address is configured
Joined group address(es):
  FF02::1
  FF02::2
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP 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 で最大 RA 間隔が 100 ミリ秒 (ms) に設定され、最小 RA 間隔が 60 ミリ秒として設定されています。

```
Device(config)# show ipv6 interface ethernet 1/0
Ethernet1/0 is administratively down, line protocol is down
IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:5A01 [TEN]
No Virtual link-local address(es):
No global unicast address is configured
Joined group address(es):
  FF02::1
  FF02::2
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP 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 間隔情報が設定されているときに **show ipv6 interface** コマンドで表示される追加の重要なフィールドについて説明します。

表 4: 最小 RA 間隔情報が設定されているときの **show ipv6 interface** コマンドのフィールドの説明

フィールド	説明
ND ルータ アドバタイズメントは 60 ~ 100 秒ごとに送信されます。	NDRA は最小値と最大値の間の値からランダムに選ばれた間隔で送信されます。この例では、最小値は 60 秒で、最大値は 100 秒です。
ND ルータ アドバタイズメントは 60 ~ 100 ミリ秒ごとに送信されます。	NDRA は最小値と最大値の間の値からランダムに選ばれた間隔で送信されます。この例では、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 mld snooping

マルチキャストリスナー検出バージョン2 (MLDv2) スヌーピング情報を表示するには、特権 EXEC モードで **show ipv6 mld snooping** コマンドを使用します。

```
show ipv6 mld [vrf vrf-name] snooping {explicit-tracking vlan vlan| mrouter [vlan vlan]|
report-suppression vlan vlan| statistics vlan vlan}
```

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。
explicit-tracking vlan <i>vlan</i>	明示的ホストトラッキングのステータスを表示します。
mrouter	オプションの VLAN 上のマルチキャストルータ インターフェイスを表示します。
vlan <i>vlan</i>	(任意) マルチキャストルータ インターフェイス上の VLAN 番号を指定します。
report-suppression vlan <i>vlan</i>	レポート抑制のステータスを表示します。
statistics vlan <i>vlan</i>	VLAN 上の MLD スヌーピング情報を表示します。

コマンド デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(18)SXE	このコマンドが Supervisor Engine 720 に導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
15.1(4)M	キーワードおよび引数 vrf vrf-name が追加されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン 引数を指定せずに **show ipv6 mld snooping mrouter** コマンドを入力すると、すべてのマルチキャスト ルータ インターフェイスを表示することができます。

例

次に、VLAN 25 の明示的トラッキング情報を表示する例を示します。

```
Router# show ipv6 mld snooping explicit-tracking vlan 25
Source/Group          Interface    Reporter    Filter_mode
-----
10.1.1.1/226.2.2.2    V125:1/2    10.27.2.3    INCLUDE
10.2.2.2/226.2.2.2    V125:1/2    10.27.2.3    INCLUDE
```

次に、VLAN 1 のマルチキャスト ルータ インターフェイスを表示する例を示します。

```
Router# show
ipv6 mld snooping mrouter vlan 1
vlan          ports
-----
1             Gi1/1,Gi2/1,Fa3/48,Router
```

次に、VLAN 25 の MLD スヌーピング統計情報を表示する例を示します。

```
Router# show ipv6 mld
snooping statistics interface vlan 25
Snooping statistics for Vlan25
#channels:2
#hosts :1

Source/Group          Interface    Reporter    Uptime      Last-Join    Last-Leave
-----
10.1.1.1/226.2.2.2    Gi1/2:V125  10.27.2.3    00:01:47    00:00:50    -
10.2.2.2/226.2.2.2    Gi1/2:V125  10.27.2.3    00:01:47    00:00:50    -
```

関連コマンド

コマンド	説明
ipv6 mld snooping	MLDv2 スヌーピングをグローバルにイネーブルにします。
ipv6 mld snooping explicit-tracking	明示的なホストトラッキングをイネーブルにします。
ipv6 mld snooping querier	MLDv2 スヌーピング クェリアをイネーブルにします。
ipv6 mld snooping report-suppression	VLAN 上でレポート抑制をイネーブルにします。

show ipv6 nd ra-throttle policy

IPv6 ルータ アドバタイズメント (RA) スロットル ポリシーに関する情報を表示するには、特権 EXEC モードで **show ipv6 nd ra-throttle policy** コマンドを使用します。

show ipv6 nd ra-throttle policy *policy-name*

構文の説明

policy-name RA スロットル 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 Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

トラブルシューティング用に IPv6 RA スロットル情報を表示するには、**show ipv6 nd ra-throttle policy** を使用します。

例

```
Device# show ipv6 nd ra-throttle policy policy2

Policy policy2 configuration:
  The throttle period will be coalesced and default to 600 seconds
  Applied to a port, this policy indicates a wired interface
  The maximum number of unthrottled RAs is configured on the vlan and defaults to 10
  The min and max numbers of unthrottled RAs per device will be coalesced and default
to 10
  The behaviour upon RAs with an RFC 3775 interval option will be coalesced and default
to passthrough

Policy applied on the following interfaces:
  Et0/0          vlan all
Policy applied on the following vlans:
  10,12-17
```

show ipv6 nd ra-throttle vlan

VLAN の IPv6 ルータ アドバタイズメント (RA) スロットル ポリシーのアクションに関する情報を表示するには、特権 EXEC モードで **show ipv6 nd ra-throttle vlan** コマンドを使用します。

show ipv6 nd ra-throttle vlan *vlan-id*[*advertising-routers*|*pending-hosts*]

構文の説明

<i>vlan-id</i>	VLAN または VLAN のコレクション。
advertising-routers	(任意) RA を最近発行したデバイスに関する情報を表示します。
pending-hosts	(任意) RA を待機している無線ホストに関する情報を表示します。

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 Release 3.2SE	このコマンドが導入されました。

使用上のガイドライン

VLAN の IPv6 RA スロットル ポリシーのアクションに関する情報を表示するには、**show ipv6 nd ra-throttle vlan** コマンドを使用します。

例

```
Device# show ipv6 nd ra-throttle vlan vlan1
general information for vlan1
-----
RAs
passed through 1      last period 1      this period 1      overall 2
throttled      4      last period 2      this period 2      overall 6

no pending host

current policy is tutu coalesced as:

throttle-period 90 seconds remaining 48
max-through 0
allow at-least 1 at-most 1
interval-option passthrough
```

show ipv6 nd rguard policy

RA ガード機能が設定されているすべてのインターフェイスのルーティングアドバタイズメント (RA) ガードポリシーを表示するには、特権 EXEC モードで **show ipv6 nd rguard policy** コマンドを使用します。

show ipv6 nd rguard policy [*policy-name*]

構文の説明

<i>policy-name</i>	(任意) RA 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
12.2(50)SY	このコマンドが導入されました。
15.2(4)S	このコマンドが Cisco IOS Release 15.2(4)S に統合されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

show ipv6 nd rguard policy コマンドは、RA ガード機能が設定されたすべてのインターフェイスのポリシーに設定されているオプションを表示します。

例

次の例では、**rguard1** という名前のポリシーおよびポリシーが適用されているすべてのインターフェイスのポリシー設定を表示します。

```
Router# show ipv6 nd rguard policy interface rguard1
```

```
Policy rguard1 configuration:
  device-role host
Policy applied on the following interfaces:
  Et0/0      vlan all
  Et1/0      vlan all
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 5 : *show ipv6 nd rguard policy* のフィールドの説明

フィールド	説明
Policy rguard1 configuration:	指定されたポリシーの設定。
device-role host	ポートに接続されているデバイスのロール。このデバイス設定はホストの設定です。
Policy applied on the following interfaces:	RA ガード機能が設定されている特定のインターフェイス。

show ipv6 neighbor binding

バインディングテーブルの内容を表示するには、特権 EXEC モードで **show ipv6 neighbor binding** コマンドを使用します。

show ipv6 neighbor binding [**vlan** *vlan-id*] **interface** *type number* | **ipv6** *ipv6-address* | **mac** *mac-address*]

構文の説明

vlan <i>vlan-id</i>	(任意) 指定した VLAN に一致するバインディングテーブルエントリを表示します。
interface <i>type number</i>	(任意) 指定したインターフェイスタイプおよび番号に一致するバインディングテーブルエントリを表示します。
ipv6 <i>ipv6-address</i>	(任意) 指定された IPv6 アドレスに一致するバインディングテーブルエントリを表示します。
mac <i>mac-address</i>	(任意) 指定されたメディアアクセスコントロール (MAC) アドレスに一致するバインディングテーブルエントリを表示します。

コマンドモード

特権 EXEC (#)

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
15.3(1)S	このコマンドが Cisco IOS Release 15.3(1)S に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

show ipv6 neighbor binding コマンドは、バインディングテーブルの内容を表示します。表示出力は、特定の VLAN、インターフェイス、IPv6 アドレス、または MAC アドレスで指定できます。

キーワードまたは引数を入力しないと、すべてのバインディングテーブルの内容が表示されません。

次のキーワードと引数の組み合わせを使用できます。

- **vlan *vlan-id*** : 指定された VLAN のすべてのエントリを表示します。
- **interface *type number*** : 指定されたインターフェイスのすべてのエントリを表示します。
- **ipv6 *ipv6-address* + interface *type number* + vlan *vlan-id*** : この3つのキーワードと引数の組み合わせに一致する1つのエントリを表示します。
- **ipv6 *ipv6-address* + interface *type number*** : 指定された IPv6 アドレスおよびインターフェイスのすべてのエントリを表示します。
- **ipv6 *ipv6-address*** : 指定された IPv6 アドレスのエントリを表示します。

例

次に、バインディングテーブルの内容を表示する例を示します。

```
Router# show ipv6 neighbor binding

address DB has 4 entries
Codes: L - Local, S - Static, ND - Neighbor Discovery
Preflevel (prlvl) values:
1:Not secure          2:MAC and LLA match    3:Cga authenticated
4:Dhcp assigned      5:Cert authenticated  6:Cga and Cert auth
7:Trusted port       8:Statically assigned

   IPv6 address          Link-Layer addr Interface  vlan  prlvl  age  state    Time left
ND FE80::A8BB:CCFF:FE01:F500  AABB.CC01.F500  Et0/0    100   0002   0  REACHABLE  8850
L  FE80::21D:71FF:FE99:4900   001D.7199.4900  V1100    100   0080  7203  DOWN      N/A
ND 2001:600::1                AABB.CC01.F500  Et0/0    100   0003   0  REACHABLE  3181
ND 2001:300::1                AABB.CC01.F500  Et0/0    100   0007   0  REACHABLE  9559
ND 2001:100::2                AABB.CC01.F600  Et1/0    200   0002   0  REACHABLE  9196
L  2001:400::1                001D.7199.4900  V1100    100   0080  7188  DOWN      N/A
S  2001:500::1                000A.000B.000C  Fa4/13   300   0080  8676  STALE     N/A
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 6 : show ipv6 neighbor binding のフィールドの説明

フィールド	説明
address DB has <i>n</i> entries	指定されたデータベースのエントリ数。

関連コマンド

コマンド	説明
ipv6 neighbor binding	バインディングテーブルのネイバーバインディングエントリのデフォルトを変更します。

show ipv6 neighbors

IPv6 ネイバー探索 (ND) 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 ネイバー情報を表示す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 ネイバー情報を表示す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 ネットワーキング デバイスの IPv6 ホスト名を指定します。
statistics	(任意) ND キャッシュ統計情報を表示します。

コマンド デフォルト

すべての IPv6 ND キャッシュ エントリを一覧表示します。

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
12.2(2)T	このコマンドが導入されました。
12.2(8)T	このコマンドが変更されました。IPv6 ネイバー探索キャッシュのスタティック エントリのサポートがコマンド出力に追加されました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。

リリース	変更内容
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合され、Cisco ASR 1000 シリーズ デバイスで導入されました。
Cisco IOS XE Release 2.6	このコマンドが変更されました。このコマンドは、特定のインターフェイスのNDキャッシュエントリの数と制限を表示するように更新されました。
15.1(3)T	このコマンドが Cisco IOS Release 15.1(3)T に統合されました。
15.2(2)SNG	このコマンドが、Cisco ASR 901 シリーズのアグリゲーション サービス デバイスに実装されました。
15.3(1)S	このコマンドが Cisco IOS Release 15.3(1)S に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン *interface-type* および *interface-number* 引数が指定されていない場合、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* および *interface-number* 引数を指定すると、指定された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 キャッシュ統計情報が表示されます。

例

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

```
Device# show ipv6 neighbors ethernet 2
IPv6 Address                               Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e REACH Ethernet2
FE80::203:A0FF:FED6:141E                     0 0003.a0d6.141e REACH Ethernet2
3001:1::45a                                  - 0002.7d1a.9472 REACH Ethernet2
```


次に、IPv6 アドレスを指定して入力された **show ipv6 neighbors** コマンドの出力例を示します。

```
Device# show ipv6 neighbors 2000:0:0:4::2
IPv6 Address                               Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e REACH Ethernet2
```

下の表で、ここで表示される重要なフィールドについて説明します。

表 7: **show ipv6 neighbors** のフィールドの説明

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	

フィールド	説明
	<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 (不完全) : エントリに対してアドレス解決を実行中です。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 (到達可能) : ネイバーへの転送パスが正常に機能していることを示す肯定確認が、直近の ReachableTime ミリ秒以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 : 転送パスが正常に機能していることを示す最後の肯定確認を受信してから ReachableTime ミリ秒を超える時間が経過しました。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 : 転送パスが正常に機能していることを示す最後の肯定確認を受信してから ReachableTime ミリ秒を超える時間が経過しました。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して、到達可能性確認をアクティブに要求します。 • ???? : 不明状態 <p>次に、IPv6 ネイバー探索キャッシュのスタ</p>

フィールド	説明
	<p>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はダウンしています。 • REACH (到達可能) : このエントリのインターフェイスは動作しています。 <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 **show ipv6 neighbors** コマンドの出力例を示します。

```
Device# show ipv6 neighbor statistics

IPv6 ND Statistics
Entries 2, High-water 2, Gleaned 1, Scavenged 0
Entry States
  INCMP 0 REACH 0 STALE 2 GLEAN 0 DELAY 0 PROBE 0
Resolutions (INCMP)
  Requested 1, timeouts 0, resolved 1, failed 0
  In-progress 0, High-water 1, Throttled 0, Data discards 0
Resolutions (PROBE)
  Requested 3, timeouts 0, resolved 3, failed 0
```

下の表で、ここで表示される重要なフィールドについて説明します。

表 8 : **show ipv6 neighbors statistics** のフィールドの説明

フィールド	説明
Entries	ND キャッシュの ND ネイバー エントリの総数。
High-Water	ND キャッシュの ND ネイバー エントリの最大数 (現時点)。
Gleaned	グリーンングされた (つまり、ネイバー NA または他の ND パケットから学習した) ND ネイバー エントリの数。

フィールド	説明
Scavenged	タイムアウトになってキャッシュから削除された古い ND ネイバーの数。
Entry States	各状態の ND ネイバーの数。
Resolutions (INCOMP)	<p>INCOMP 状態で試行された（つまり、データパケットによって発生した）ネイバー解決の統計情報。INCOMP 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 : 解決中に発生したタイムアウト回数。 • Resolved : 成功した解決の数。 • Failed : 成功しなかった解決の数。 • In-progress : 処理中の解決の数。 • High-water : 処理中の解決の最大数（現時点）。 • Throttled : 処理中の解決の最大数の制限によって解決要求が無視された回数。 • Data discards : ネイバー解決を待機しているデータパケットが破棄された数。
Resolutions (PROBE)	<p>PROBE 状態で試行されたネイバー解決（つまり、データパケットによって発生した既存エントリの再解決）の統計情報。</p> <ul style="list-style-type: none"> • Requested : 要求された解決の総数。 • Timeouts : 解決中に発生したタイムアウト回数。 • Resolved : 成功した解決の数。 • Failed : 成功しなかった解決の数。

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と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) 設定されたルーティング 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
12.2(8)T	このコマンドが導入されました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.4(15)T	このコマンドが変更されました。コマンド出力が、ベクトル メトリックを含む Enhanced Interior Gateway Routing Protocol (EIGRP) の情報を提供するように拡張されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.4	このコマンドが、Cisco ASR 1000 シリーズのアグリゲーション サービ ルータに実装されました。

リリース	変更内容
Cisco IOS XE Release 3.6	このコマンドが変更されました。コマンド出力が、EIGRP IPv6 Nonstop Forwarding (NSF) に関する情報を含むように拡張されました。
15.2(2)S	このコマンドが変更されました。コマンド出力が、EIGRP IPv6 NSF に関する情報を含むように拡張されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン `show ipv6 protocols` コマンドにより表示される情報は、ルーティング操作のデバッグに役立ちます。

例 `show ipv6 protocols` コマンドの次の出力例は、Intermediate System-to-Intermediate System (IS-IS) ルーティング プロトコルの情報を示しています。

```
Device# show ipv6 protocols

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "isis"
  Interfaces:
    Ethernet0/0/3
    Ethernet0/0/1
    Serial1/0/1
    Loopback1 (Passive)
    Loopback2 (Passive)
    Loopback3 (Passive)
    Loopback4 (Passive)
    Loopback5 (Passive)
  Redistribution:
    Redistributing protocol static at level 1
  Inter-area redistribution
    Redistributing L1 into L2 using prefix-list word
  Address Summarization:
    L2: 33::/16 advertised with metric 0
    L2: 44::/16 advertised with metric 20
    L2: 66::/16 advertised with metric 10
    L2: 77::/16 advertised with metric 10
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 9: IS-IS プロセスの `show ipv6 protocols` のフィールドの説明

フィールド	説明
IPv6 Routing Protocol is	使用される IPv6 ルーティング プロトコルを指定します。
Interfaces	IPv6 IS-IS プロトコルを設定するインターフェイスを指定します。

フィールド	説明
Redistribution	再配布されるプロトコルを示します。
Inter-area redistribution	他のレベルに再配布される IS-IS レベルを示します。
using prefix-list	エリア間再配布で使用されるプレフィックスリストに名前を付けます。
Address Summarization	すべてのサマリープレフィックスを示します。サマリープレフィックスをアドバタイズすると、プレフィックスの後に「advertised with metric x」と表示されます。

show ipv6 protocols コマンドの次の出力例では、自律システム 30 のボーダー ゲートウェイ プロトコル (BGP) の情報が表示されます。

Device# **show ipv6 protocols**

```
IPv6 Routing Protocol is "bgp 30"
  IGP synchronization is disabled
  Redistribution:
    Redistributing protocol connected
  Neighbor(s):
    Address                               FiltIn FiltOut Weight RoutemapIn RoutemapOut
    2001:DB8:0:ABCD::1                    5      7      200
    2001:DB8:0:ABCD::2                    rmap-in rmap-out
    2001:DB8:0:ABCD::3                    rmap-in rmap-out
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 10 : BGP プロセスの **show ipv6 protocols** のフィールドの説明

フィールド	説明
IPv6 Routing Protocol is	使用される IPv6 ルーティング プロトコルを指定します。
Redistribution	再配布されるプロトコルを示します。
Address	ネイバーの IPv6 アドレス。
FiltIn	入力に適用される AS パス フィルタ リスト。
FiltOut	出力に適用される AS パス フィルタ リスト。
Weight	BGP 最良パス選択に使用するネイバーの重み値。

フィールド	説明
RoutemapIn	入力に適用されるネイバー ルート マップ。
RoutemapOut	出力に適用されるネイバー ルート マップ。

show ipv6 protocols summary コマンドの出力例を示します。

```
Device# show ipv6 protocols summary
```

```
Index Process Name
0      connected
1      static
2      rip myrip
3      bgp 30
```

show ipv6 protocols コマンドの次の出力例は、バクトル メトリックおよび EIGRP IPv6 NSF を含む EIGRP 情報を表示しています。

```
Device# show ipv6 protocols
```

```
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "bgp 1"
  IGP synchronization is disabled
  Redistribution:
    None
IPv6 Routing Protocol is "bgp multicast"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "eigrp 1"
EIGRP-IPv6 VR(name) Address-Family Protocol for AS(1)
  Metric weight K1=1, K2=0, K3=1, K4=0, K5=0 K6=0
  Metric rib-scale 128
  Metric version 64bit
  NSF-aware route hold timer is 260
  EIGRP NSF enabled
    NSF signal timer is 15s
    NSF converge timer is 65s
Router-ID: 10.1.2.2
Topology : 0 (base)
  Active Timer: 3 min
  Distance: internal 90 external 170
  Maximum path: 16
  Maximum hopcount 100
  Maximum metric variance 1
  Total Prefix Count: 0
  Total Redist Count: 0

Interfaces:
Redistribution:
  None
```

次に、Open Shortest Path First (OSPF) ドメインで再配布を設定した後、IPv6 プロトコル情報を表示する例を示します。

```
Device# redistribute ospf 1 match internal
Device(config-rtr)# end
Device# show ipv6 protocols
```

```
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip 1"
  Interfaces:
    Ethernet0/1
    Loopback9
  Redistribution:
    Redistributing protocol ospf 1 (internal)
```

```
IPv6 Routing Protocol is "ospf 1"  
  Interfaces (Area 0):  
    Ethernet0/0  
  Redistribution:  
    None
```

show ipv6 route

IPv6 ルーティングテーブルの内容を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 route** コマンドを使用します。

show ipv6 route [*ipv6-address* | *ipv6-prefix/prefix-length* [**longer-prefixes**]] [*protocol*] | [**repair**] | [**updated** | **boot-up**] [*day month*] [*time*]] | **interface** *type number* | **nd** | **nsf** | **table** *table-id* | **watch**]

構文の説明

<i>ipv6-address</i>	(任意) 特定の IPv6 アドレスのルーティング情報を表示します。
<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表示します。
<i>/prefix-length</i>	(任意) IPv6 プレフィックスの長さ。プレフィックス (アドレスのネットワーク部分) を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。
longer-prefixes	(任意) より長いプレフィックスエントリの出力を表示します。
<i>protocol</i>	(任意) ルーティングプロトコルの名前、またはキーワード connected 、 local 、 mobile 、または static 。ルーティングプロトコルを指定する場合は、 bgp 、 isis 、 eigrp 、 ospf 、または rip のキーワードのいずれかを使用します。
repair	(任意) ルートと修復パスを表示します。
updated	(任意) ルートとタイムスタンプを表示します。
boot-up	(任意) 起動時以降のルーティング情報を表示します。
<i>day month</i>	(任意) 指定した月と日以降のルートを表示します。
<i>time</i>	(任意) <i>hh:mm</i> 形式で指定された時刻以降のルートを表示します。

interface	(任意) インターフェイスに関する情報を表示します。
<i>type</i>	(任意) インターフェイス タイプ。
<i>number</i>	(任意) インターフェイス番号。
nd	(任意) ネイバー探索 (ND) が所有する IPv6 ルーティング情報ベース (RIB) からのルートだけが表示されます。
nsf	(任意) ノンストップ フォワーディング (NSF) 状態のルートを表示します。
repair	(任意)
table <i>table-id</i>	(任意) 指定されたテーブルIDのIPv6 RIB テーブル情報を表示します。テーブルIDは16進表記である必要があります。範囲は0～0-0xFFFFFFFF です。
watch	(任意) ルートウォッチャに関する情報を表示します。

コマンド デフォルト

オプションの構文要素のいずれも選択しない場合、すべてのアクティブな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
12.2(2)T	このコマンドが導入されました。
12.2(8)T	このコマンドが変更されました。 isis キーワードが追加され、I1 - ISIS L1、I2 - ISIS L2、および IA - IS-IS エリア間のフィールドがコマンドの出力に含まれました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。

リリース	変更内容
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。タイマー情報が削除され、IPv6 マルチプロトコル ラベル スイッチング (MPLS) インターフェイスを表示するインジケータが追加されました。
12.2(13)T	このコマンドが変更されました。タイマー情報が削除され、IPv6 MPLS インターフェイスを表示するインジケータが追加されました。
12.2(14)S	このコマンドが変更されました。 longer-prefixes キーワードが追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco ASR 1000 シリーズのアグリゲーションサービス ルータに実装されました。
12.4(24)T	このコマンドは、Cisco IOS Release 12.4(24)T よりも前のリリースで変更されました。 table 、 nsf 、 watch 、および updated キーワードと、 <i>day</i> 、 <i>month</i> 、 <i>table-id</i> 、および <i>time</i> 引数が追加されました。
15.2(2)S	このコマンドが変更されました。コマンド出力が、ドット付き 10 進数形式のルート タグ値を含むように拡張されました。
Cisco IOS XE Release 3.6S	このコマンドが変更されました。コマンド出力が、ドット付き 10 進数形式のルート タグ値を含むように拡張されました。
15.1(1)SY	nd キーワードが追加されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

IPv6 専用の情報である点を除いて、**show ipv6 route** コマンドの出力は、**show ip route** コマンドと類似しています。

ipv6-address 引数または *ipv6-prefix/prefix-length* 引数が指定されている場合、最長一致検索がルーティング テーブルから実行され、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。ルーティングプロトコルが指定されている場合、そのプロトコルのルートだけが表示されます。**connected**、**local**、**mobile**、または **static** キーワードを指定した場合は、指定したルートタ

IPv6だけが表示されます。**interface** キーワードと **type** および **number** 引数が指定されている場合、指定インターフェイスに固有のルートだけが表示されます。

例

次に、キーワードまたは引数が指定されていない場合の **show ipv6 route** コマンドの出力例を示します。

```
Device# show ipv6 route

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - IIS interarea
B   2001:DB8:4::2/48 [20/0]
    via FE80::A8BB:CCFF:FE02:8B00, Serial6/0
L   2001:DB8:4::3/48 [0/0]
    via ::, Ethernet1/0
C   2001:DB8:4::4/48 [0/0]
    via ::, Ethernet1/0
LC  2001:DB8:4::5/48 [0/0]
    via ::, Loopback0
L   2001:DB8:4::6/48 [0/0]
    via ::, Serial6/0
C   2001:DB8:4::7/48 [0/0]
    via ::, Serial6/0
S   2001:DB8:4::8/48 [1/0]
    via 2001:DB8:1::1, Null
L   FE80::/10 [0/0]
    via ::, Null0
L   FF00::/8 [0/0]
    via ::, Null0
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 11 : **show ipv6 route** のフィールドの説明

フィールド	説明
Codes:	ルートを生成したプロトコルを示します。表示される値は次のとおりです。 <ul style="list-style-type: none"> • B : BGP 生成 • C : 接続済み • I1 : ISIS L1 : 統合 IS-IS Level 1 生成 • I2 : ISIS L2 : 統合 IS-IS Level 2 生成 • IA : ISIS エリア間 : 統合 IS-IS エリア間生成 • L : ローカル • R : RIP 生成 • S : スタティック
2001:DB8:4::2/48	リモートネットワークの IPv6 プレフィックスを示します。

フィールド	説明
[20/0]	角カッコ内の最初の数字は、情報の発信元からのアドミニストレティブディスタンスです。 2番目の数字はルートのメトリックです。
via FE80::A8BB:CCFF:FE02:8B00	リモートネットワークまでの次のデバイスのアドレスを指定します。

ipv6-address 引数または *ipv6-prefix/prefix-length* 引数が指定されている場合は、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。次に、IPv6 プレフィックス 2001:DB8::/35 が指定されている場合の **show ipv6 route** コマンドの出力例を示します。出力のフィールドは字句どおりです。

```
Device# show ipv6 route 2001:DB8::/35

IPv6 Routing Table - 261 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
B 2001:DB8::/35 [20/3]
   via FE80::60:5C59:9E00:16, Tunnel1
```

プロトコルを指定する場合、その特定のルーティングプロトコルのルートだけが表示されます。次に、**show ipv6 route bgp** コマンドの出力例を示します。出力のフィールドは字句どおりです。

```
Device# show ipv6 route bgp

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
B 2001:DB8:4::4/64 [20/0]
   via FE80::A8BB:CCFF:FE02:8B00, Serial6/0
```

次に、**show ipv6 route local** コマンドの出力例を示します。出力のフィールドは字句どおりです。

```
Device# show ipv6 route local

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
L 2001:DB8:4::2/128 [0/0]
   via ::, Ethernet1/0
LC 2001:DB8:4::1/128 [0/0]
   via ::, Loopback0
L 2001:DB8:4::3/128 [0/0]
   via ::, Serial6/0
L FE80::/10 [0/0]
   via ::, Null0
L FF00::/8 [0/0]
   via ::, Null0
```

次に、6PE マルチパス機能がイネーブルの場合の **show ipv6 route** コマンドの出力例を示します。出力のフィールドは字句どおりです。

```
Device# show ipv6 route

IPv6 Routing Table - default - 19 entries
Codes:C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
```

```

I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
.
.
.
B 2001:DB8::/64 [200/0]
  via ::FFFF:172.11.11.1
  via ::FFFF:172.30.30.1

```

 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。
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 snooping capture-policy

メッセージキャプチャのポリシーを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 snooping capture-policy** コマンドを使用します。

show ipv6 snooping capture-policy [*interface type number*]

構文の説明

<i>interface type number</i>	(任意) 指定したインターフェイスタイプおよび番号の第 1 ホップ メッセージタイプを表示します。
------------------------------	---

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
12.2(50)SY	このコマンドが導入されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
15.3(1)S	このコマンドが Cisco IOS Release 15.3(1)S に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

show ipv6 snooping capture-policy コマンドは、IPv6 第 1 ホップ メッセージ キャプチャ ポリシーを表示します。

例

次の例は、IPv6 ネイバー探索プロトコル (NDP) インスペクション機能およびルータアドバタイズメント (RA) ガード機能が設定されているイーサネット 0/0 インターフェイスでの **show ipv6 snooping capture-policy** コマンド出力を示しています。

```
Router# show ipv6 snooping capture-policy

Hardware policy registered on Et0/0
Protocol Protocol value Message Value Action Feature
ICMP      58             RS      85     punt    RA Guard
```

```

ICMP      58          RA      86      punt    ND Inspection
          drop      RA guard
          punt    ND Inspection
ICMP      58          NS      87      punt    ND Inspection
ICMP      58          NA      88      punt    ND Inspection
ICMP      58          REDIR   89      drop    RA Guard
          punt    ND Inspection
    
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 12 : *show ipv6 snooping capture-policy* のフィールドの説明

フィールド	説明
Hardware policy registered on Fa4/11	ハードウェアポリシーには、プログラマティック アクセス リスト (ACL) とアクセス コントロール エントリ (ACE) が含まれています。
Protocol	パケットが検査されるプロトコル。
Message	検査するメッセージのタイプ。
Action	パケットで実行するアクション。
Feature	この情報用のインスペクション機能。

show ipv6 snooping counters

インターフェイスカウンタによってカウントされたパケットに関する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 snooping counters** コマンドを使用します。

show ipv6 snooping counters [interface type number]

構文の説明

interface type number	(任意) 指定したインターフェイスタイプおよび番号と一致する第1ホップパケットを表示します。
------------------------------	--

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
12.2(50)SY	このコマンドが導入されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
15.3(1)S	このコマンドが Cisco IOS Release 15.3(1)S に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

show ipv6 snooping counters コマンドは、インターフェイスカウンタでカウントされている、スイッチャーによって処理されたパケットを表示します。スイッチャーはインターフェイスごとにキャプチャされたパケットをカウントし、パケットが受信されたか、送信されたか、ドロップされたかを記録します。パケットがドロップされた場合、ドロップの理由とドロップの原因となった機能の両方が記載されます。

例

次に、インターフェイス FastEthernet4/12 でカウントされたパケットに関する情報を表示する例を示します。

```
Router# show ipv6 snooping counters interface Fa4/12
Received messages on Fa4/12:
Protocol      Protocol message
ICMPv6        RS          RA          NS          NA          REDIR      CPS          CPA
```

```

0          4256    0      0      0      0      0
Bridged messages from Fa4/12:
Protocol      Protocol message
ICMPv6        RS      RA      NS      NA      REDIR  CPS    CPA
              0      4240    0      0      0      0      0
Dropped messages on Fa4/12:
Feature/Message RS      RA      NS      NA      REDIR  CPS    CPA
RA guard      0      16      0      0      0      0      0
Dropped reasons on Fa4/12:
RA guard      16      RA drop - reason:RA/REDIR received on un-authorized port

```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 13: show ipv6 snooping counters のフィールドの説明

フィールド	説明
Received messages on Fa4/12:	インターフェイスで受信されたメッセージ。
Protocol	メッセージがカウントされているプロトコル。
Protocol message	カウントされているプロトコルメッセージのタイプ。
Bridged messages from Fa4/12:	インターフェイスからブリッジされたメッセージ。
Dropped messages an Fa4/12:	インターフェイス上でドロップされたメッセージ。
Feature/message	ドロップの原因となった機能、およびドロップされたメッセージのタイプと数。
RA drop - reason:RA/REDIR received on un-authorized port	これらのメッセージがドロップされた理由。

show ipv6 snooping features

ルータに設定されているスヌーピング機能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 snooping features** コマンドを使用します。

show ipv6 snooping features

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
12.2(50)SY	このコマンドが導入されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。
15.3(1)S	このコマンドが Cisco IOS Release 15.3(1)S に統合されました。

使用上のガイドライン

show ipv6 snooping features コマンドは、ルータに設定されている第 1 ホップ機能を表示します。

例

次に、IPv6 ND インспекションと IPv6 RA ガードの両方がルータに設定されている例を示します。

```
Router# show ipv6 snooping features
```

```
Feature name  priority state
RA guard      100  READY
NDP inspection 20   READY
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 14 : **show ipv6 snooping features** のフィールドの説明

フィールド	説明
Feature name	ルータに設定されている IPv6 グローバル ポリシー機能の名前。

フィールド	説明
Priority	指定された機能のプライオリティ。
State	指定された機能のステータス。

show ipv6 snooping policies

設定したポリシーと、それが適用された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 snooping policies** コマンドを使用します。

show ipv6 snooping policies [*interface type number*]

構文の説明

interface <i>type number</i>	(任意) 指定したインターフェイスタイプおよび番号に一致するポリシーを表示します。
-------------------------------------	---

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
12.2(50)SY	このコマンドが導入されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SE に統合されました。

使用上のガイドライン

show ipv6 snooping policies コマンドは、設定されているすべてのポリシーと、それが適用されたインターフェイスを表示します。

例

次に、設定されているすべてのポリシーの情報を表示する例を示します。

```
Device# show ipv6 snooping policies
```

```
NDP inspection policies configured:
```

```
Policy      Interface  Vlan
-----
```

```
trusted    Et0/0      all
```

```
           Et1/0      all
```

```
untrusted  Et2/0      all
```

```
RA guard policies configured:
```

```
Policy      Interface  Vlan
-----
```

```
host       Et0/0      all
```

```
           Et1/0      all
```

```
router     Et2/0      all
```

```
-----
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 15 : *show ipv6 first-hop policies* フィールドの説明

フィールド	説明
NDP inspection policies configured:	特定の機能用に設定されたポリシーの説明。
Policy	ポリシーが信頼できるか、信頼できないか。
Interface	ポリシーが適用されるインターフェイス。

show ipv6 traffic

IPv6 トラフィックの統計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 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 転送の統計情報が保存されているすべてのインターフェイスの IPv6 転送の統計情報が表示されます。
<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で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
12.2(2)T	このコマンドが導入されました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合され、出力フィールドが追加されました。
12.2(13)T	出力フィールドを追加する変更がこのリリースに統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。

リリース	変更内容
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
12.2(33)SRC	<i>interface</i> 引数および interface キーワードが追加されました。
12.2(33)SB	このコマンドが、Cisco IOS Release 12.2(33)SB に統合されました。
Cisco IOS XE Release 2.1	このコマンドは、Cisco ASR 1000 シリーズ デバイスで追加されました。
15.2(2)SNG	このコマンドが、Cisco ASR 901 シリーズのアグリゲーションサービス デバイスに実装されました。
15.3(1)S	このコマンドが Cisco IOS Release 15.3(1)S に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン **show ipv6 traffic** コマンドの出力は、IPv6 に固有である点を除き、**show ip traffic** コマンドの出力と似ています。

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

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

次に、IPv6 CEF を実行しない **show ipv6 interface** コマンドの出力例を示します。

```
Device# show ipv6 interface ethernet 0/1/1
Ethernet0/1/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::203: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 を実行している show ipv6 interface コマンドの出力例を示します。

```
Device# show ipv6 interface ethernet 0/1/1
Ethernet0/1/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::203: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.
```

下の表で、この出力で表示される重要なフィールドについて説明しています。

表 16 : show ipv6 traffic のフィールドの説明

フィールド	説明
source-routed	発信元からルーティングされたパケットの数。
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、パケット長で実行されたチェックの結果として生じた可能性があるエラー。

フィールド	説明
not a device	IPv6 ユニキャストルーティングがイネーブルになっていないときに送信されたメッセージ。
0 unicast RPF drop, 0 suppressed RPF drop	ユニキャストリバースパス転送 (RPF) および抑制された RPF のドロップ数。
failed	失敗したフラグメント送信の数。
encapsulation failed	未解決のアドレスまたはトライアンドキューパケットが原因と考えられる失敗。
no route	ソフトウェアが送信方法を認識していなかったデータグラムを廃棄するときにカウントされます。
unreach	<p>受信される到達不能メッセージは次のとおりです。</p> <ul style="list-style-type: none"> • routing : 宛先へ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外であることを示します。たとえば、送信元がローカルサイトであるか、宛先に送信元へ戻るルートがない可能性があります。 • address : アドレスが到達不能であることを示します。 • port : ポートが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	検証や抑制された検証のドロップなど、プロセス RPF の数を表示します。
CEF Switching	検証のドロップや抑制された検証のドロップなど、CEF スイッチングの数を表示します。

summary-prefix (OSPFv3)

Open Shortest Path First バージョン 3 (OSPFv3) の IPv6 サマリープレフィックスを設定するには、OSPFv3 ルータ コンフィギュレーション モード、IPv6 アドレス ファミリ コンフィギュレーション モード、または IPv4 アドレス ファミリ コンフィギュレーション モードで **summary-prefix** コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

summary-prefix *prefix* [**not-advertise** | **tag** *tag-value*] [**nssa-only**]

no summary-prefix *prefix* [**not-advertise** | **tag** *tag-value*] [**nssa-only**]

構文の説明

<i>prefix</i>	宛先の IPv6 ルート プレフィックス。
not-advertise	(任意) 指定されたプレフィックス/マスク ペアと一致するルートを抑制します。このキーワードは OSPFv3 だけに適用されます。
tag <i>tag-value</i>	(任意) ルートマップを使用して再配布を制御する match 値として使用できるタグ値を指定します。このキーワードは OSPFv3 だけに適用されます。
nssa-only	(任意) プレフィックスの範囲をエリアに限定します。指定したプレフィックスに対して生成されるサマリールート (存在する場合) に nssa-only 属性を設定します。

コマンド デフォルト

IPv6 サマリープレフィックスは定義されていません。

コマンド モード

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

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

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

コマンド履歴

リリース	変更内容
12.0(24)S	このコマンドが導入されました。
12.2(15)T	このコマンドが、Cisco IOS Release 12.2(15)T に統合されました。

リリース	変更内容
12.2(18)S	このコマンドが、Cisco IOS Release 12.2(18)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
15.1(3)S	このコマンドが変更されました。コマンドは IPv4 または IPv6 OSPFv3 プロセスでイネーブルにできます。
Cisco IOS XE Release 3.4S	このコマンドが変更されました。コマンドは IPv4 または IPv6 OSPFv3 プロセスでイネーブルにできます。
15.2(1)T	このコマンドが変更されました。コマンドは IPv4 または IPv6 OSPFv3 プロセスでイネーブルにできます。
15.2(4)S	このコマンドが変更されました。キーワード nssa-only が追加されました。
15.1(1)SY	このコマンドが変更されました。コマンドは IPv4 または IPv6 OSPFv3 プロセスでイネーブルにできます。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

summary-prefix コマンドは、別のルーティング プロトコルから再配布されたデバイスを集約するために使用できます。複数のアドレス グループを集約できます。サマリーのアドバタイズに使用されるメトリックは、具体的なルートすべての中で最小のメトリックです。このコマンドは、ルーティング テーブルの容量縮小に有効です。

外部ルートが Not So Stubby Area (NSSA) に再配布される場合、Propagate ビット (P ビット) をクリアするために **nssa-only** キーワードを指定します。これにより、対応する NSSA 外部リンク ステート アドバタイズメント (LSA) が他のエリアに変換されることを防ぎます。

例

次の例で、サマリープレフィックス 2051:0:0:10::/60 には 2051:0:0:10::/60 から 2051:0:0:20::/128 (ただし、このアドレスは含まれない) までのアドレスが含まれます。アドレス 2051:0:0:10::/60 だけが外部 LSA でアドバタイズされます。

```
summary-prefix 2051:0:0:10::/60
```

関連コマンド

router ospfv3

IPv4 または IPv6 アドレス ファミリの OSPFv3 ルータ コンフィギュレーションモードをイネーブルにします。

throttle-period

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

throttle-period { **inherit** | *seconds* }

構文の説明

inherit	スロットル期間の設定はターゲット ポリシーから継承されます。
<i>seconds</i>	スロットル期間の時間 (秒単位)。範囲は 10 ~ 86,400 秒です。

コマンド デフォルト

600 秒 (10 分)

コマンド モード

IPv6 RA スロットル ポリシー コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

throttle-period コマンドは、VLAN に適用されたポリシーにのみ有効です。ポートでこのコマンドを設定しようとすると、ポートはこれを無視します。

例

```
Device(config)# ipv6 nd ra-throttle policy policy1
Device(config-nd-ra-throttle)# throttle-period 300
```


timers spf (IPv6)

IPv6 の Open Shortest Path First (OSPF) の Shortest Path First (SPF) スロットリングをオンにするには、ルータ コンフィギュレーション モードで **timers spf** コマンドを使用します。SPF スロットリングをオフにするには、このコマンドの **no** 形式を使用します。

timers spf delay holdtime

no timers spf

構文の説明

<i>delay</i>	SPF 計算の変更を受信する遅延 (ミリ秒)。指定できる範囲は 0 ~ 4294967295 です。デフォルトは 5 ミリ秒です。
<i>holdtime</i>	連続する SPF 計算間のホールド時間 (ミリ秒単位)。指定できる範囲は 0 ~ 4294967295 です。デフォルトは 10 ミリ秒です。

コマンド デフォルト

OSPF for IPv6 スロットリングは常にイネーブルです。

コマンド モード

ルータ コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(15)T	このコマンドが導入されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

SPF 計算間の初回待機時間は、*delay* 引数で指定される時間 (ミリ秒) です。続いて適用される各待機時間は、待機時間が *holdtime* 引数で指定される最大時間 (ミリ秒) に達するまで、現在の保持時間 (ミリ秒) を 2 倍した値になります。値がリセットされるまで、または SPF 計算間でリンクステートアドバタイズメント (LSA) が受信されるまで、従属待機時間は最大のまま残ります。

例

次に、**timers spf** コマンドの遅延時間とホールド時間の間隔値をそれぞれ 40 ミリ秒と 50 ミリ秒に設定したルータの例を示します。

```
Router(config)# ipv6 router ospf 1
Router(config-router)# timers spf 40 50
```

関連コマンド

コマンド	説明
show ipv6 ospf	OSPF for IPv6 ルーティング プロセスに関する一般情報を表示します。

timers throttle lsa

IPv6 の Open Shortest Path First (OSPF) のリンクステートアドバタイズメント (LSA) の生成に関するレート制限値を設定するには、ルータ コンフィギュレーション モードで **timers throttle lsa** 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 throttle lsa *start-interval* *hold-interval* *max-interval*

no timers throttle lsa

構文の説明

<i>start-interval</i>	LSA の生成の最小遅延 (ミリ秒単位)。LSA の最初のインスタンスは、ローカル OSPF for IPv6 トポロジの変更の直後に必ず生成されます。次の LSA の生成は、開始間隔の前ではありません。範囲は 0 ~ 600,000 ミリ秒です。デフォルト値は 0 ミリ秒です。つまり、遅延はなく、LSA は即座に送信されます。
<i>hold-interval</i>	増分時間 (ミリ秒単位)。この値は、LSA 生成の時間を制限する従属レートを計算するために使用されます。範囲は 1 ~ 600,000 ミリ秒です。デフォルト値は 5000 ミリ秒です。
<i>max-interval</i>	同じ LSA の生成間の最大待機時間 (ミリ秒単位)。範囲は 1 ~ 600,000 ミリ秒です。デフォルト値は 5000 ミリ秒です。

コマンド デフォルト

start-interval : 0 ミリ秒 *hold-interval* : 5000 ミリ秒 *max-interval* : 5000 ミリ秒

コマンド モード

OSPF for IPv6 ルータ コンフィギュレーション (config-rtr) ルータ コンフィギュレーション (config-router)

コマンド履歴

リリース	変更内容
12.2(33)SRC	このコマンドが導入されました。
12.2(33)SB	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドは、Cisco ASR 1000 シリーズ ルータで追加されました。
15.0(1)M	このコマンドが、Cisco IOS Release 12.5(1)Mに統合されました。
12.2(33)XNE	このコマンドが変更されました。Cisco IOS Release 12.2(33)XNEに統合されました。
15.1(1)SY	このコマンドが変更されました。Cisco IOS Release 15.1(1)SYに統合されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

「同じ LSA」とは、同じ LSA ID 番号、LSA タイプ、およびアドバタイズ ルータ ID を含む LSA インスタンスを意味します。 **timers lsa arrival** コマンドの *milliseconds* 値は、**timers throttle lsa** コマンドの *hold-interval* 値以下にすることを勧めます。

例

この例では、OSPF LSA スロットリングをカスタマイズして、開始間隔が 200 ミリ秒、ホールド間隔が 10,000 ミリ秒、最大間隔が 45,000 ミリ秒になるようにしています。同じ LSA を受信するインスタンス間の最小間隔は 2000 ミリ秒です。

```
router ospf 1
 log-adjacency-changes
 timers throttle lsa 200 10000 45000
 timers lsa arrival 2000
 network 10.10.4.0 0.0.0.255 area 24
 network 10.10.24.0 0.0.0.255 area 24
```

この例では、IPv6 OSPF LSA スロットリングをカスタマイズして、開始間隔が 500 ミリ秒、ホールド間隔が 1,000 ミリ秒、最大間隔が 10,000 ミリ秒になるようにしています。

```
ipv6 router ospf 1
 log-adjacency-changes
 timers throttle lsa 500 1000 10000
```

関連コマンド

コマンド	説明
show ipv6 ospf	OSPF for IPv6 ルーティング プロセスに関する情報を表示します。
timers lsa arrival	ソフトウェアが OSPF ネイバーから同一の LSA を受け入れる最小間隔を設定します。

tracking

ポートのデフォルト トラッキング ポリシーを上書きするには、ネイバー探索 (ND) インスペクション ポリシー コンフィギュレーション モードで **tracking** コマンドを使用します。

tracking {enable [reachable-lifetime {value| infinite}]}| disable [stale-lifetime {value| infinite}]}

構文の説明

enable	トラッキングはイネーブルです。
reachable-lifetime	<p>(任意) 到達可能なエントリが、到達可能性の確認なしで直接的または間接的に到達可能であると見なされる時間の上限。</p> <ul style="list-style-type: none"> • reachable-lifetime キーワードは、enable キーワードとのみ使用可能です。 • reachable-lifetime キーワードは、ipv6 neighbor binding reachable-lifetime コマンドで設定されたグローバルな到達可能ライフタイムよりも優先されます。
<i>value</i>	秒単位のライフタイム値。指定できる範囲は 1 ~ 86400 で、デフォルトは 300 です。
infinite	到達可能状態または STALE 状態のエントリを時間制限なしに保持します。
disable	トラッキングをディセーブルにします。
stale-lifetime	<p>(任意) STALE 状態のエントリを保持する時間で、グローバルな stale-lifetime 設定を上書きします。</p> <ul style="list-style-type: none"> • STALE ライフタイムは 86,400 秒です。 • stale-lifetime キーワードは、enable キーワードとのみ使用可能です。 • stale-lifetime キーワードは、ipv6 neighbor binding stale-lifetime コマンドで設定されたグローバルな STALE ライフタイムよりも優先されます。

コマンド デフォルト

ND エントリが到達可能状態を保持される時間。ユレーション (config-nd-inspection)

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.0(2)SE	このコマンドが、Cisco IOS Release 15.0(2)SEに統合されました。
15.3(1)S	このコマンドが Cisco IOS Release 15.3(1)S に統合されました。

使用上のガイドライン

tracking コマンドは、このポリシーが適用されるポートで **ipv6 neighbor tracking** コマンドによって設定されたデフォルトのトラッキングポリシーを上書きします。この機能は、たとえば、エントリを追跡したくはないが、エントリがなくならないようにバインディングテーブル内に保持したいような、信頼できるポートで便利です。

reachable-lifetime キーワードは、追跡による直接的な、または ND インスペクションによる間接的な到達可能性の確認なしで、エントリが到達可能と見なされる最大時間です。 **reachable-lifetime** 値に到達すると、エントリは STALE に移動されます。 **tracking** コマンドの **reachable-lifetime** キーワードは、 **ipv6 neighbor binding reachable-lifetime** コマンドで設定されたグローバルな到達可能ライフタイムよりも優先されます。

stale-lifetime キーワードは、エントリが削除されるか、エントリに到達可能であることが直接または間接的に確認される前に、エントリをテーブルに保持する最大時間です。 **tracking** コマンドの **stale-lifetime** キーワードは、 **ipv6 neighbor binding stale-lifetime** コマンドで設定されたグローバルな STALE ライフタイムよりも優先されます。

例

次の例では、 **policy1** として ND ポリシー名を定義し、ルータを ND インスペクションポリシー コンフィギュレーションモードにして、信頼できるポートで時間制限なしにエントリがバインディングテーブルに留まるように設定します。

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# tracking disable stale-lifetime infinite
```

関連コマンド

コマンド	説明
ipv6 nd inspection policy	ND インスペクションポリシー名を定義して、ND インスペクションポリシー コンフィギュレーションモードを開始します。
ipv6 neighbor binding	バインディングテーブルのネイバーバインディング エントリのデフォルトを変更します。

コマンド	説明
ipv6 neighbor tracking	バインディングテーブルのエントリのトラッキングをイネーブルにします。
ipv6 nd rguard policy	RA ガード ポリシー名を定義し、RA ガード ポリシー コンフィギュレーション モードを開始します。

tunnel mode ipv6ip

スタティック IPv6 トンネル インターフェイスを設定するには、インターフェイス コンフィギュレーション モードで **tunnel mode ipv6ip** コマンドを使用します。スタティック IPv6 トンネル インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

tunnel mode ipv6ip [6rd|6to4|auto-tunnel|isatap]

no tunnel mode ipv6ip

構文の説明

6rd	(任意) トンネルが IPv6 Rapid Deployment (6RD) を使用するように指定します。
6to4	(任意) IPv4 アドレスとプレフィックス 2002::/16 から動的に生成された宛先アドレス (6to4 アドレスと呼ばれます) を使用して IPv6 自動トンネルを設定します。
auto-tunnel	(任意) IPv4 互換 IPv6 アドレスを使用して IPv6 自動トンネルを設定します。
isatap	(任意) Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) を使用して IPv4 ネットワーク内の IPv6 ノード (ホストとルータ) に接続する IPv6 自動トンネルを設定します。

コマンド デフォルト

スタティック IPv6 トンネル インターフェイスは設定されていません。

コマンド モード

インターフェイス コンフィギュレーション (config-if)

コマンド履歴

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

リリース	変更内容
12.2(14)S	このコマンドが変更されました。 isatap キーワードが、ISATAP トンネルの実装の追加をサポートするために追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。
Cisco IOS XE Release 3.1S	このコマンドが変更されました。 6rd キーワードが追加されました。 auto-tunnel キーワードが、Cisco ASR 1000 シリーズルータで廃止されました。
15.1(3)T	このコマンドが Cisco IOS Release 15.1(3)T に統合されました。
15.1SY	このコマンドが Cisco IOS Release 15.1SY に統合されました。 auto-tunnel キーワードが廃止されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

IPv6 トンネリングとは、IPv4 パケットに IPv6 パケットをカプセル化し、IPv4 ルーティング インフラストラクチャを介してパケットを送信することです。

手動設定トンネル

tunnel mode ipv6ip コマンドは IPv6 トンネルを設定します。IPv6 トンネルの両端のデバイスは、IPv4 と IPv6 の両方のプロトコル スタックをサポートする必要があります。

このコマンドを使用するには、まず手動で以下を設定する必要があります。

- トンネル インターフェイスの IPv6 アドレス
- トンネルの送信元として IPv4 アドレス
- トンネルの宛先として IPv4 アドレス

トンネルの宛先の自動判別

tunnel mode ipv6ip auto-tunnel コマンドは自動 IPv6 トンネルを設定します。トンネル送信元は手動で設定します。トンネル宛先は、IPv4 互換 IPv6 アドレスの下位 32 ビットとして自動的に定められます。IPv4 互換 IPv6 アドレスは、アドレスの上位 96 ビットに IPv6 プレフィックス 0:0:0:0:0:0 を含み、アドレスの下位 32 ビットに IPv4 アドレスを含む 128 ビットの IPv6 アドレスです。自動

トンネルの両端のデバイスは、IPv4 と IPv6 の両方のプロトコルスタックをサポートする必要があります。

6to4 トンネル

tunnel mode ipv6ip 6to4 コマンドは、グローバルに一意な IPv4 アドレスを 6to4 アドレスに埋め込むことでトンネルエンドポイントが決定される自動 6to4 トンネルを設定します。6to4 アドレスは、プレフィックス 2002::/16 とグローバルに一意な 32 ビットの IPv4 アドレスの組み合わせです。(IPv4 互換アドレスは、6to4 トンネリングでは使用されません)。一意な IPv4 アドレスが、6to4 アドレスプレフィックスで、ネットワーク層アドレスとして使用されます。トンネルの送信元は、**tunnel source** コマンドを使用して手動で設定できるインターフェイスです。6to4 トンネルの両端の境界デバイスは、IPv4 プロトコルスタックと IPv6 プロトコルスタックの両方をサポートしている必要があります。さらに、6to4 アドレスプレフィックスでネットワークに宛先指定されたトラフィックは、**ipv6 route** コマンドを使用して、トンネルを介してルーティングされる必要があります。

6RD トンネル

tunnel mode ipv6ip 6rd コマンドは、トンネルが IPv6 RD 用に使用されることを指定します。6RD 機能は、6to4 トンネル機能に似ていますが、アドレスに 2002::/16 プレフィックスは必要ありません。IPv4 宛先の 32 ビットがすべて IPv6 ペイロードヘッダーにあることも必要としません。

ISATAP トンネル

ISATAP トンネルはネットワーク境界内での IPv6 パケットの転送をイネーブルにします。ISATAP トンネルによって、サイト内の IPv4 または IPv6 デュアルスタックホストが個別に IPv4 インフラストラクチャを使用して IPv6 ネットワークに接続できます。

IPv4 互換アドレスとは異なり、ISATAP IPv6 アドレスは任意のユニキャスト /64 の最初のプレフィックスを使用できます。最後の 64 ビットは、インターフェイス ID として使用されます。これらの、最初の 32 ビットは固定パターンの 0000:5EFE です。最後の 32 ビットには、トンネルエンドポイントの IPv4 アドレスが含まれます。

例

例

次に、手動で IPv6 トンネルを設定する例を示します。この例では、トンネルインターフェイス 0 が、グローバル IPv6 アドレスを使用して手動で設定されます。トンネル送信元およびトンネル宛先も、手動で設定されます。

```
Device(config)# interface tunnel 0
Device(config-if)# ipv6 address 3ffe:b00:c18:1::3/127
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel destination 192.168.30.1
Device(config-if)# tunnel mode ipv6ip
Device(config-if)# end
```

例

次に、トンネル送信元として、イーサネットインターフェイス0を使用する自動IPv6トンネルを設定する例を示します。トンネル宛先は、IPv4 互換 IPv6 アドレスの下位 32 ビットとして自動的に定められます。

```
Device(config)# interface tunnel 0
Device(config-if)# no ip address
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel mode ipv6ip auto-tunnel
Device(config-if)# end
```

例

次に、6to4 トンネルを設定する例を示します。この例では、イーサネットインターフェイス0が IPv4 アドレス 192.168.99.1 によって設定されます。サイト固有の 48 ビットプレフィックス 2002:c0a8:630 が、プレフィックス 2002::/16 を IPv4 アドレス 192.168.99.1 に追加することにより構築されます。

トンネルインターフェイス0は、IPv4 または IPv6 アドレスなしで設定されます。トンネル送信元アドレスは、イーサネットインターフェイス0として手動で設定されます。トンネル宛先アドレスは自動的に構築されます。IPv6 スタティックルートは、ネットワーク 2002::/16 に宛先指定されたトラフィックをトンネルインターフェイス0でルーティングするように設定されます。

```
Device(config)# interface ethernet 0
Device(config-if)# ip address 192.168.99.1 255.255.255.0
Device(config-if)# ipv6 address 2002:c0a8:6301:1::/64 eui-64
Device(config-if)# exit
Device(config)# interface tunnel 0
Device(config-if)# no ip address
Device(config-if)# ipv6 unnumbered ethernet 0
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel mode ipv6ip 6to4
Device(config-if)# exit
Device(config)# ipv6 route 2002::/16 tunnel 0
Device(config)# end
```

例

ipv6 unnumbered、**tunnel source**、および **tunnel mode ipv6ip** コマンドを使用してトンネルインターフェイスが設定されている場合、トンネルは、IPv6 アドレスとして送信元インターフェイスに設定されている最初の IPv6 アドレスを使用します。6to4 トンネルの場合、送信元インターフェイスに設定される最初の IPv6 アドレスは、6to4 アドレスである必要があります。次の例では、イーサネットインターフェイス0に最初に設定される IPv6 アドレス（6to4 アドレス 2002:c0a8:6301:1::/64）が、トンネル0の IPv6 アドレスとして使用されます。

```
Device(config)# interface tunnel 0
Device(config-if)# ipv6 unnumbered ethernet 0
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel mode ipv6ip 6to4
Device(config-if)# exit
Device(config)# interface ethernet 0
Device(config-if)# ipv6 address 2002:c0a8:6301:1::/64 eui-64
Device(config-if)# ipv6 address 3ffe:1234:5678::1/64
Device(config-if)# end
```

例 次に、6RD トンネルを設定する例を示します。

```
Device(config)# interface Tunnell
Device(config-if)# ipv6 address 2001:B000:100::1/32
Device(config-if)# tunnel source GigabitEthernet2/0/0
Device(config-if)# tunnel mode ipv6ip 6rd
Device(config-if)# tunnel 6rd prefix 2001:B000::/32
Device(config-if)# tunnel 6rd ipv4 prefix-len 16 suffix-len 8
Device(config-if)# end
Device# show tunnel 6rd Tunnell

Interface Tunnell:
  Tunnel Source: 10.1.1.1
  6RD: Operational, V6 Prefix: 2001:B000::/32
      V4 Common Prefix Length: 16, Value: 10.1.0.0
      V4 Common Suffix Length: 8, Value: 0.0.0.1
```

例 次に、イーサネット インターフェイス 0 に ISATAP トンネルを設定する例を示します。クライアントの自動設定を可能にするために、ルータ アドバタイズメントがイネーブルになっています。

```
Device(config)# interface Ethernet 0
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config)# interface Tunnel 0
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel mode ipv6ip isatap
Device(config-if)# ipv6 address 2001:0DB8::/64 eui-64
Device(config-if)# no ipv6 nd ra suppress
Device(config-if)# end
```

関連コマンド

コマンド	説明
ip address	IPv4 インターフェイスの IP アドレスを指定します。
ipv6 address	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ipv6 address eui-64	インターフェイスの IPv6 アドレスを設定し、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 IPv6 処理をイネーブルにします。
ipv6 route	スタティック IPv6 ルートを確立します。
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。

コマンド	説明
no ipv6 nd ra suppress	LAN インターフェイスでの IPv6 ルータ アドバタイズメントの送信を再びイネーブルにします。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。
show tunnel 6rd tunnel	トンネルに関する 6RD 情報を表示します。
tunnel 6rd ipv4	ドメイン内のすべての 6RD ルータに共通の IPv4 トランスポートアドレスのプレフィックス長およびサフィックス長を指定します。
tunnel 6rd prefix	6RD トンネルで共通の IPv6 プレフィックスを指定します。
tunnel destination	トンネルインターフェイスの宛先アドレスを設定します。
tunnel source	トンネルインターフェイスの送信元アドレスを設定します。

vlan configuration

VLAN または VLAN のコレクションを設定し、VLAN 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 **vlan configuration** コマンドを使用します。コマンドの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。

vlan configuration *vlan-id*

構文の説明

vlan-id VLAN または VLAN のコレクション。

コマンド デフォルト

VLAN または VLAN のコレクションは設定されていません。

コマンド モード

グローバル コンフィギュレーション (config)

コマンド履歴

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

使用上のガイドライン

VLAN または VLAN のコレクションを設定するには、**vlan configuration** コマンドを使用します。VLAN レベルで機能する IPv6 RA スロットルは、指定された時間、VLAN 上で複数のデバイスからのすべての RA をカウントします。

ipv6 nd ra-throttle policy コマンドを使用して IPv6 RA スロットル ポリシーを設定した後、**ipv6 nd ra-throttle attach-policy** コマンドを使用して VLAN または VLAN のコレクションに適用できます。

例

```
Device(config)# vlan configuration vlan1
Device(config-vlan-config)#
```