ipv6-i1

ipv6 dhcp guard attach-policy

Dynamic Host Configuration Protocol for IPv6（DHCPv6）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 モードまたは VLAN コンフィギュレーション モードで **ipv6 dhcp guard attach-policy** コマンドを使用します。 DHCPv6 ガード ポリシーを適用解除するには、このコマンドの **no** 形式を使用します。

Syntax Available In Interface Configuration Mode

ipv6 dhcp guard [**attach-policy** [*policy-name*]] [**vlan** {**add**| **all**| **except**| **none**| **remove**} *vlan-id* [*... vlan-id*]]

no ipv6 dhcp guard [**attach-policy** [*policy-name*]] [**vlan** {**add**| **all**| **except**| **none**| **remove**} *vlan-id* [*... vlan-id*]]

Syntax Available In VLAN Configuration Mode

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

no ipv6 dhcp guard attach-policy [*policy-name*]

構文の説明

policy-name	（任意）DHCPv6 ガード ポリシー名。
vlan	（任意）DHCPv6 ポリシーを VLAN に適用するように指定します。
add	（任意）指定した VLAN に DHCPv6 ガード ポリシーを適用します。
all	（任意）全 VLAN に DHCPv6 ガード ポリシーを適用します。
except	（任意）指定した VLAN を除くすべての VLAN に DHCPv6 ガード ポリシーを適用します。
none	（任意）指定した VLAN のいずれにも DHCPv6 ガード ポリシーを適用しません。
remove	（任意）指定した VLAN から DHCPv6 ガード ポリシーを削除します。
vlan-id	（任意）DHCP ガード ポリシーが適用される VLAN の ID。

コマンド デフォルト

DHCPv6 ガード ポリシーは適用されません。（config-if）

VLAN コンフィギュレーション（config-vlan）

コマンド履歴

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

使用上のガイドライン

このコマンドによって、インターフェイスまたは 1 つ以上の VLAN に DHCPv6 ポリシーを適用できます。 DHCPv6 ガード ポリシーは、不正な DHCP サーバおよび DHCP パケットをサーバからクライアントに転送するリレーエージェントからの応答およびアドバタイズメント メッセージをブロックするために使用できます。 クライアント メッセージまたはリレー エージェントによってクライアントからサーバに送信されたメッセージが妨げられることはありません。

例

次に、インターフェイスに DHCPv6 ガード ポリシーを適用する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet 0/2/0
Router# switchport
Router(config-if)# ipv6 dhcp guard attach-policy pol1 vlan add 1
```

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 guard policy	DHCPv6 ガード ポリシー情報を表示します。

ipv6 dhcp guard policy

Dynamic Host Configuration Protocol for IPv6（DHCPv6）ガードポリシー名を定義するには、グローバル コンフィギュレーション モードで **ipv6 dhcp guard policy** コマンドを使用します。 DHCPv6 ガード ポリシー名を削除するには、このコマンドの **no** 形式を使用します。

ipv6 dhcp guard policy [*policy-name*]

no ipv6 dhcp guard policy [*policy-name*]

構文の説明

policy-name	（任意）DHCPv6 ガード ポリシー名。

コマンド デフォルト

DHCPv6 ガード ポリシー名は定義されません。

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

使用上のガイドライン

このコマンドで、DHCPv6 ガード コンフィギュレーション モードを開始することができます。 DHCPv6 ガード ポリシーは、不正な DHCP サーバおよび DHCP パケットをサーバからクライアントに転送するリレーエージェントからの応答およびアドバタイズメント メッセージをブロックするために使用できます。 クライアント メッセージまたはリレー エージェントによってクライアントからサーバに送信されたメッセージが妨げられることはありません。

例

次に、DHCPv6 ガード ポリシー名を定義する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# ipv6 dhcp guard policy policy1
```

関連コマンド

コマンド	説明
show ipv6 dhcp guard policy	DHCPv6 ガード ポリシー情報を表示します。

ipv6 dhcp ping packets

Dynamic Host Configuration Protocol for IPv6（DHCPv6）サーバが ping 操作の一部としてプール アドレスに送信するパケットの数を指定するには、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

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

コマンド デフォルト

アドレスが要求元クライアントに割り当てられる前に、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（config）

コマンド履歴

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

使用上のガイドライン

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 操作がオフになります。

例

次の例では、DHCPv6 サーバで ping 試行を中止するまでに 4 回の ping を試行するように指定します。

```
Router(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 server

インターフェイスで IPv6 サービス用の Dynamic Host Configuration Protocol（DHCP）をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ipv6 dhcp server** を使用します。インターフェイスで IPv6 用 DHCP サービスをディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 dhcp server [*poolname*| **automatic**] **[rapid-commit]** [**preference** *value*] **[allow-hint]**

no ipv6 dhcp server

構文の説明

poolname	（任意）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。
automatic	（任意）サーバが、クライアントにアドレスを割り当てるときに使用するプールを自動的に決定できるようにします。
rapid-commit	（任意）プレフィックス委任用に 2 メッセージ交換方式を許可します。
preference *value*	（任意）サーバにより送信されるアドバタイズ メッセージのプリファレンス オプションで伝送されるプリファレンス値を指定します。有効な範囲は 0 ～ 255 です。 プリファレンス値のデフォルトは 0 です。
allow-hint	（任意）サーバがクライアントによって提示されたプレフィックスの委任を考慮するかどうかを指定します。デフォルトでは、サーバはクライアントが提示したプレフィックスを無視します。

コマンド デフォルト

インターフェイスで IPv6 サービス用の DHCP はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.3(4)T	このコマンドが導入されました。
12.2(18)SXE	このコマンドが、Cisco IOS Release 12.2(18)SXE に統合されました。
12.4(24)T	**automatic** キーワードが追加されました。
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。
12.2(33)SRE	このコマンドが、Cisco IOS Release 12.2(33)SRE に統合されました。
12.2(33)XNE	このコマンドが、Cisco IOS Release 12.2(33)XNE に統合されました。
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 dhcp server コマンドは、指定されたインターフェイスを介してプレフィックス委任のプールおよびその他の設定を使用し、そのインターフェイスで IPv6 サービス用の DHCP をイネーブルにします。

automatic キーワードは、クライアントにアドレスを割り当てるときに使用するプールを自動的に決定できるようにします。 サーバが IPv6 DHCP パケットを受信すると、サーバはそのパケットを DHCP リレーから受信したか、クライアントから直接受信したかを判別します。 リレーからパケットを受信した場合、サーバは、クライアントに最も近い最初のリレーと関連付けられているパケット内部のリンク アドレス フィールドを確認します。 サーバは、このリンク アドレスと、すべてのアドレス プレフィックスおよび IPv6 DHCP プールのリンク アドレス設定とを照合して、最長のプレフィックス一致を探します。 サーバは最長一致と関連付けられているプールを選択します。

パケットをクライアントから直接受信した場合、サーバは同じ照合を行いますが、照合を行うときに着信インターフェイスに設定されているすべての IPv6 アドレスを使用します。 そして再度、サーバは最長のプレフィックス照合を選択します。

rapid-commit キーワードは、プレフィックス委任およびその他の設定について、2 メッセージ交換を使用できるようにします。 クライアントが送信請求メッセージに高速コミット オプションを含め、サーバで **rapid-commit** キーワードがイネーブルになっている場合、サーバは応答メッセージを使用して送信請求メッセージに応答します。

preference キーワードを 0 以外の値とともに設定すると、サーバはプリファレンス オプションを追加して、アドバタイズ メッセージのプリファレンス値を伝送します。 この動作は、クライアントによるサーバの選択に影響を与えます。 プリファレンス オプションを含まないアドバタイズ

メッセージのプリファレンス値は 0 であると見なされます。 クライアントが 255 のプリファレンス値を持つプリファレンスオプションを含むアドバタイズメッセージを受信した場合、クライアントはアドバタイズ メッセージの送信元であるサーバに要求メッセージをすぐに送信します。

allow-hint キーワードを指定した場合、サーバは送信請求メッセージおよび要求メッセージに含まれる有効なクライアント提案のプレフィックスを委任します。 プレフィックスは、関連付けられているローカルプレフィックスプール内にあり、デバイスに割り当てられていない場合は有効です。 **allow-hint** キーワードを指定しない場合、提案は無視され、プレフィックスはプールの空きリストから委任されます。

IPv6 用 DHCP クライアント、サーバ、およびリレーの機能は、インターフェイス上で相互排他的です。 これらの機能のいずれかがすでにイネーブルになっていて、同じインターフェイスで別の機能を設定しようとすると、次のメッセージのいずれかが表示されます。

```
Interface is in DHCP client mode
Interface is in DHCP server mode
Interface is in DHCP relay mode
```

例

次に、server1 という名前のローカル プレフィックス プールに対して IPv6 用 DHCP をイネーブルにする例を示します。

```
Router(config-if)# ipv6 dhcp server server1
```

関連コマンド

コマンド	説明
ipv6 dhcp pool	IPv6 用 DHCP プールを設定し、IPv6 用 DHCP プール コンフィギュレーション モードを開始します。
show ipv6 dhcp interface	IPv6 用 DHCP のインターフェイス情報を表示します。

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上で IPv6 処理をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ipv6 enable** コマンドを使用します。明示的な IPv6 アドレスでまだ設定されていないインターフェイスで IPv6 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 enable

no ipv6 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

IPv6 はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
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。
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。

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 enable コマンドは、インターフェイスに IPv6 リンクローカル ユニキャスト アドレスを自動的に設定し、さらにインターフェイスを IPv6 処理用にイネーブルにします。 明示的な IPv6 アドレスで設定されているインターフェイスで no **ipv6 enable** コマンドを実行しても、IPv6 処理はディセーブルになりません。

例

次に、イーサネット インターフェイス 0/0 で IPv6 処理をイネーブルにする例を示します。

```
Device(config)# interface ethernet 0/0
Device(config-if)# ipv6 enable
```

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 unnumbered	インターフェイスに明示的な IPv6 アドレスを割り当てなくても、インターフェイスで IPv6 処理をイネーブルにします。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 host

ホスト名キャッシュにスタティックなホスト名/アドレスマッピングを定義するには、グローバル コンフィギュレーション モードで **ipv6 host** コマンドを使用します。 ホスト名/アドレス マッピ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。

ipv6 host *name* [*port*] *ipv6-address*

no ipv6 host *name*

構文の説明

name	IPv6 ホストの名前。 名前の冒頭は、文字と数字のいずれも使用できます。 数字を使用すると、実行できるアクションは限られます。
port	（任意）対応付けられる IPv6 アドレスのデフォルト Telnet ポート番号。
ipv6-address	対応付けられる IPv6 アドレス。 ホスト名 1 つに最大 4 つのアドレスをバインドできます。

コマンド デフォルト

ホスト名キャッシュにスタティックなホスト名/アドレス マッピングは定義されていません。 デフォルトの Telnet ポートは 23 です。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

リリース	変更内容
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 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

*name*変数の先頭には、文字または数字を指定できます。 数字を使用すると、実行できる操作（**ping** など）が制限されます。

例

次の例では、2 つのスタティック マッピングを定義します。

```
Device(config)# ipv6 host cisco-sj 2001:0DB8:1::12
Device(config)# ipv6 host cisco-hq 2002:C01F:768::1 2001:0DB8:1::12
```

関連コマンド

コマンド	説明
show hosts	デフォルトのドメイン名、名前ルックアップ サービス、ネーム サーバ ホストのリスト、およびホスト名とアドレスのキャッシュされたリストを表示します。

ipv6 icmp error-interval

IPv6 インターネット制御メッセージ プロトコル（ICMP）エラー メッセージの間隔およびバケット サイズを設定するには、グローバル コンフィギュレーション モードで **ipv6 icmp error-interval** コマンドを使用します。 間隔をそ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 icmp error-interval *milliseconds* [*bucketsize*]

no ipv6 icmp error-interval

構文の説明

milliseconds	バケットにトークンが保存される間隔。 許容範囲は 0 ～ 2147483647 です。デフォルトは 100 ミリ秒です。
bucketsize	（任意）バケットに保存されるトークンの最大数。 許容範囲は 1 ～ 200 です。デフォルトは 10 トークンです。

コマンド デフォルト

デフォルトでは、ICMP レート制限はイネーブルです。 ICMP レート制限をディセーブルにするには、間隔をゼロに設定します。 バケットにトークンが保存される間隔は 100 ミリ秒です。 バケットに保存されるトークンの最大数は 10 です。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。
12.2(8)T	IPv6 ICMP レート制限のサポートが、トークン バケットを使用するように拡張されました。
12.0(21)ST	トークン バケットを使用する拡張なしのこのコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	トークン バケットを使用する拡張なしのこのコマンドが Cisco IOS Release 12.0(22)S に統合されました。

リリース	変更内容
12.0(23)S	トークン バケットを使用するように拡張された IPv6 ICMP レート制限をサポートするこのコマンドが、Cisco IOS Release 12.0(23)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 2.1	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 ICMP エラー メッセージが送信され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。 トークン バケット アルゴリズムは、1 件の IPv6 ICMP エラー メッセージを表す 1 つのトークンで使用されます。 トークンは、バケットで許可されているトークンの最大数に達するまで、指定された間隔で、仮想バケットに保存されます。

milliseconds 引数は、トークンがバケットに到達する間隔を指定します。 オプションの *bucketsize* 引数は、バケットで許可されるトークンの最大数の定義に使用されます。 トークンは、IPv6 ICMP エラー メッセージが送信されるときにバケットから削除されます。つまり、*bucketsize* が 20 に設定されている場合、20 の IPv6 ICMP エラー メッセージを連続して送信することができます。 トークンのバケットが空になると、新しいトークンがバケットに配置されるまで、IPv6 ICMP エラー メッセージは送信されません。

show ipv6 traffic コマンドを使用すると、IPv6 ICMP レート制限カウンタを表示できます。

例

次の例は、50 ミリ秒の間隔と 20 トークンのバケット サイズが IPv6 ICMP エラー メッセージに対して設定されていることを示します。

```
ipv6 icmp error-interval 50 20
```

関連コマンド

コマンド	説明
show ipv6 traffic	IPv6 トラフィックに関する統計情報を表示します。

ipv6 nd cache expire

IPv6 ネイバー探索（ND）のキャッシュ エントリの期限が切れるまでの時間を設定するには、**ipv6 nd cache expire** コマンドをインターフェイス コンフィギュレーション モードで使用します。 このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

ipv6 nd cache expire *expire-time-in-seconds* **[refresh]**

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

構文の説明

expire-time-in-seconds	時間の範囲は 1 ～ 65536 秒です。 デフォルトは 14400 秒、つまり 4 時間です。
refresh	（任意）自動的に ND キャッシュ エントリをリフレッシュします。

コマンド デフォルト

この有効期限は 14400 秒（4 時間）です。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(33)SXI7	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

デフォルトでは、ND キャッシュ エントリが 14,400 秒間（4 時間）、STALE 状態になると、期限切れとなり削除されます。 **ipv6 nd cache expire** コマンドは、エントリが削除される前にユーザが有効期限を変更して、期限切れのエントリの自動更新をトリガーできるようにします。

refresh キーワードを使用すると、ND キャッシュ エントリは自動更新されます。 エントリが DELAY 状態になり、ネイバー到達不能検出（NUD）プロセスが発生し、5 秒後に DELAY 状態から PROBE 状態にエントリが遷移します。 エントリが PROBE 状態になると、設定に従ってネイバー送信要求（NS）が送信され、再送信されます。

例

次に、ND キャッシュ エントリが 7200 秒（2 時間）で期限切れになるように設定する例を示します。

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

ipv6 nd inspection

ネイバー探索プロトコル（NDP）チェック機能を適用するには、インターフェイス コンフィギュレーション モードで **ipv6 nd inspection** コマンドを使用します。 NDP インスペクション機能を削除するには、このコマンドの **no** 形式を使用します。

ipv6 nd inspection [**attach-policy** [*policy-name*] | **vlan** {**add** | **except** | **none** | **remove** | **all**} **vlan** *vlan-id*]]

no ipv6 nd inspection

構文の説明

attach-policy	（任意）NDP インスペクション ポリシーを適用します。
policy-name	（任意）NDP インスペクション ポリシー名。
vlan	（任意）インターフェイスの VLAN に ND インスペクション機能を適用します。
add	（任意）検査される VLAN を追加します。
except	（任意）指定した 1 つ以外のすべての VLAN を検査します。
none	（任意）VLAN を検査しないように指定します。
remove	（任意）NDP インスペクションから特定の VLAN を削除します。
all	（任意）ポートのすべての VLAN からの NDP トラフィックを検査します。
vlan-id	（任意）インターフェイスの特定の VLAN。 複数の VLAN を指定できます。 使用できる VLAN 番号は 1 ～ 4094 です。

コマンド デフォルト

すべての NDP メッセージが検査されます。 セキュア ネイバー探索（SeND）オプションは無視されます。 ネイバーはネイバー トラッキング機能で定義された基準に基づいて検査されます。 ポート単位の IPv6 アドレス制限の適用はディセーブルです。 レイヤ 2 ヘッダーの送信元 MAC アドレ

ス検証はディセーブルです。ソフトウェアでのNDPメッセージのポート単位のレート制限はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(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)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

ipv6 nd inspection コマンドは、指定されたインターフェイスの NDP インスペクション機能を適用します。オプションの **attach-policy** または **vlan** キーワードをイネーブルにすると、NDP トラフィックがポリシーまたはVLANによって検査されます。VLANを指定しない場合は、ポートのすべての VLAN からの NDP のトラフィックが検査されます（**vlan all** キーワードを使用した場合と同じ）。

ポリシーがこのコマンドで指定されていない場合、デフォルトの条件は次のとおりです。

- すべての NDP メッセージが検査されます。
- SeND オプションは無視されます。
- ネイバーはネイバー トラッキング機能で定義された基準に基づいて検査されます。
- ポート単位の IPv6 アドレス制限の適用はディセーブルです。
- レイヤ 2 ヘッダーの送信元 MAC アドレス検証はディセーブルです。
- ソフトウェアでの NDP メッセージのポート単位のレート制限はディセーブルです。

VLAN を指定する場合、パラメータは、1 ～ 4094 の単一の VLAN 番号、または 2 つの VLAN 番号の小さい方を先にして、ダッシュで区切って記述した VLAN 範囲です（**vlan 1-100,200,300-400** など）。カンマで区切ったVLANパラメータの間、またはダッシュで指定した範囲の間には、スペースを入れないでください。

例

次に、指定されたインターフェイスのNDPインスペクションをイネーブルにする例を示します。

```
Router(config-if)# ipv6 nd inspection
```

ipv6 nd inspection policy

ネイバー探索（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 モードを開始するには、ND インスペクション コンフィギュレーション モードで **ipv6 nd inspection** コマンドを使用します。 ND インスペクション 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 nd inspection policy *policy-name*

no ipv6 nd inspection policy *policy-name*

構文の説明

policy-name	ND インスペクション ポリシー名。

コマンド デフォルト

ND インスペクション ポリシーは設定されていません。

コマンド モード

ND インスペクション コンフィギュレーション（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。
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 nd inspection policy コマンドは、ND インスペクション ポリシー名を定義し、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。 ND インスペクション ポリシー コンフィギュレーション モードでは、次のコマンドのいずれかを使用できます。

- **device-role**
- **drop-unsecure**
- **limit address-count**
- **sec-level minimum**

- **tracking**
- **trusted-port**
- **validate source-mac**

例

次に、policy1 として ND ポリシー名を定義する例を示します。

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

関連コマンド

コマンド	説明
device-role	ポートに接続されているデバイスのロールを指定します。
drop-unsecure	オプションが指定されていないか無効なオプションが指定されているか、またはシグニチャが無効なメッセージをドロップします。
limit address-count	ポートで使用できる IPv6 アドレスの数を制限します。
sec-level minimum	CGA オプションを使用する場合の最小のセキュリティ レベル パラメータ値を指定します。
tracking	ポートでデフォルトのトラッキング ポリシーを上書きします。
trusted-port	信頼できるポートにするポートを設定します。
validate source-mac	リンク層アドレスと比較して送信元 MAC アドレスを検査します。

ipv6 nd na glean

ネイバー探索（ND）を設定し、非送信請求ネイバー アドバタイズメント（NA）からエントリを取り出すには、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 nd na glean

no ipv6 nd na glean

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

ルータは、非送信請求 NA を無視します。

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
12.2(33)SXI7	このコマンドが導入されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

IPv6 ノードは、重複アドレス検出（DAD）が正常に完了すると、マルチキャスト非送信請求 NA パケットを発行する場合があります。 デフォルトでは、これらの非送信請求 NA パケットは他の IPv6 ノードによって無視されます。 **ipv6 nd na glean** コマンドは、ルータを非送信請求 NA パケットの受信時にND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存在せず、NAにリンク層アドレス オプションがあるものとします）。 このコマンドを使用すると、ルータがネイバーに対するデータ トラフィック交換の前にネイバーのエントリを ND キャッシュに読み込むことができます。

例

次に、非送信請求ネイバー アドバタイズメントからエントリを取り出すように ND を設定する例を示します。

```
Router(config-if)# ipv6 nd na glean
```

ipv6 nd nud retry

ネイバー到達不能検出（NUD）がネイバー送信要求（NS）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 nd nud retry *base interval max-attempts*

no ipv6 nd nud retry *base interval max-attempts*

構文の説明

base	ベース NUD 値。
interval	再試行の時間間隔（ミリ秒単位）。
max-attempts	再試行の最大数。base 値に依存します。

コマンド デフォルト

1 秒間隔で 3 回、NS パケットが送信されます。

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
12.2(33)SXI7	このコマンドが導入されました。
Cisco IOS XE Release 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

ルータがネイバーの ND エントリを再解決するために NUD を実行するときに、1 秒間隔で 3 回、NS パケットを送信します。 特定の状況（スパニングツリー イベント、トラフィックが多い、エンド ホストがリロードされたなど）では、1 秒間隔で 3 回 NS パケットが送信されても十分でない場合があります。 こうした状況でネイバー キャッシュを維持するために、NS の再送信の指数タイマーを設定するには、**ipv6 nd nud retry** コマンドを使用します。

最大リトライ試行回数は *max-attempts* 引数を使用して設定します。 再送信間隔は、次の式を使用して計算されます。

tm

• *t* = 時間間隔

• *m* = ベース（1、2、または 3）

• *n* = 現在の NS の数（最初の NS が 0 に相当します）

ipv6 nd nud retry コマンドは、NUD の再送信のレートにのみ影響し、1 秒間隔で 3 回の NS パケット送信というデフォルトを使用する最初の解決には影響しません。

例

次に、1 秒間隔固定で 3 回再送信する例を示します。

```
Router(config-if)# ipv6 nd nud retry 1 1000 3
```

次に、1、2、4、8 の間隔で再送信する例を示します。

```
Router(config-if)# ipv6 nd nud retry 2 1000 4
```

次に、1、3、9、27、81 の間隔で再送信する例を示します。

```
Router(config-if)# ipv6 nd nud retry 3 1000 5
```

ipv6 nd ra-throttle attach-policy

レイヤ2インターフェイスまたはVLANのコレクションにIPv6ルータアドバタイズメント（RA）スロットル 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 モードまたはVLAN コンフィギュレーション モードで **ipv6 nd ra-throttle attach-policy** コマンドを使用します。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 nd ra-throttle attach-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 デフォルト

ポリシーはインターフェイスに適用されません。

ポリシーは VLAN 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）

VLAN コンフィギュレーション（config-VLAN-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

デバイス ポートのレイヤ2インターフェイスにIPv6 RA スロットル 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 nd ra-throttle attach-policy** コマンドを使用します。 VLANまたはVLANのコレクションにIPv6 RA スロットル ポリシーを適用するには、VLAN コンフィギュレーション モードで **ipv6 nd ra-throttle attach-policy** コマンドを使用します。RA スロットル ポリシーを作成するには、グローバル コンフィギュレーション モードで **ipv6 nd ra-throttle policy** コマンドを使用します。

IPv6 RA スロットル ポリシーは、ポート レベルで動作させるために、VLAN またはボックス レベルで適用する必要があります。 ポリシーがポート レベルだけで適用されている場合、IPv6 RA スロットルは動作しません。

ポリシーがポートに適用されると、ポリシーで設定されていない値は VLAN 設定から継承されます。 値が VLAN 設定で設定されていない場合、デフォルト値が使用されます。

例

次に、policy1 という名前の IPv6 RA スロットル ポリシーを作成してイーサネット 0/0 インターフェイスに適用する例を示します。

```
Device(config)# ipv6 nd ra-throttle policy policy1
Device(config-nd-ra-throttle)# exit
.
.
Device(config)# interface ethernet0/0
Device(config-if)# ipv6 nd ra-throttle attach-policy policy1
```

次に、policy1 という名前の IPv6 RA スロットル ポリシーを作成して vlan1 という名前の VLAN のコレクションに適用する例を示します。

```
Device(config)# ipv6 nd ra-throttle policy policy1
Device(config-nd-ra-throttle)# exit
.
.
Device(config)# vlan configuration vlan1
Device(config-vlan-config)# ipv6 nd ra-throttle attach-policy policy1
```

ipv6 nd ra-throttle policy

ルータアドバタイズメント（RA）スロットルポリシー名を定義し、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 nd ra-throttle policy** コマンドを使用します。 コマンドをデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

ipv6 nd ra-throttle policy *policy-name* **no 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 デフォルト

- throttle-period：600 秒（10 分）
- max-through：10 分あたり VLAN あたり 10 RA
- allow：少なくとも 1、最大 1
- interval-option：パススルー
- medium-type：有線（ポートのみ）

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

IPv6 RA スロットル ポリシーを定義し、IPv6 RA スロットル ポリシー コンフィギュレーション モードを開始するには、**ipv6 nd ra-throttle policy** コマンドを使用します。

VLAN レベルで適用される **allow at-least** および **allow at-most** コマンド設定は、VLAN 内のすべてのデバイスのデフォルトを指定します。 値は、指定されたポートに別のポリシーを適用することによって、ポート単位で上書きできます。

IPv6 RA スロットル ポリシーは、ポート レベルで動作させるために、VLAN またはボックス レベルで適用する必要があります。 ポリシーがポート レベルだけで適用されている場合、IPv6 RA スロットルは動作しません。

ポリシーがポートに適用されると、ポリシーで設定されていない値はVLAN設定から継承されます。 値がVLAN設定で設定されていない場合、デフォルト値が使用されます。

例

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

ipv6 nd raguard attach-policy

指定したインターフェイスにIPv6ルータアドバタイズメント（RA）ガード機能を適用するには、インターフェイス コンフィギュレーション モードで **ipv6 nd raguard attach-policy** コマンドを使用します。

ipv6 nd raguard attach-policy [*policy-name* [**vlan** {**add**| **except**| **none**| **remove**| **all**} *vlan* [*vlan1, vlan2, vlan3...*]]]

構文の説明

policy-name	（任意）IPv6 RA ガード ポリシー名。
vlan	（任意）インターフェイスの VLAN に IPv6 RA ガード機能を適用します。
add	検査する VLAN を追加します。
except	指定した 1 つ以外のすべての VLAN を検査します。
none	VLAN は検査されません。
remove	RA ガード インスペクションから特定の VLAN を削除します。
all	ポートのすべての VLAN からの ND のトラフィックが検査されます。
vlan	（任意）インターフェイスの特定の VLAN。 複数の VLAN を指定できます（*vlan1*, *tb-vlan2*, *vlan3...*）。 使用できる VLAN 番号の範囲は 1 ～ 4094 です。

コマンド デフォルト

IPv6 RA ガード ポリシーは設定されません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(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

policy-name 引数を使用してポリシーが指定されない場合、ポートデバイス ロールはホストに設定され、すべてのインバウンド ルータ トラフィック（RA メッセージ、リダイレクト メッセージなど）がブロックされます。

VLAN が指定されない場合（**vlan all** キーワードを *policy-name* 引数に続けて入力した場合と同じ）、ポートのすべての VLAN からの RA ガード トラフィックが解析されます。

VLAN パラメータは、1 ～ 4094 の間の 1 つの VLAN 番号、または 2 つの VLAN 番号で指定する（小さい方の数を先にして、間をダッシュで区切る）VLAN 範囲です。 カンマで区切った vlan パラメータの間、またはダッシュで指定した範囲の間には、スペースを入れないでください（例：vlan 1-100,200,300-400）。

例

次の例では、IPv6 RA ガード機能が GigabitEthernet インターフェイス 0/0 に適用されます。

```
Device(config)# interface GigabitEthernet 0/0
Device(config-if)# ipv6 nd raguard attach-policy
```

ipv6 nd raguard policy

ルータアドバタイズメント（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 raguard policy** コマンドを使用します。

ipv6 nd raguardpolicy *policy-name*

構文の説明

policy-name	IPv6 RA ガード ポリシー名。

コマンド デフォルト

RA ガード ポリシーは設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
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

ルータでRAガードをグローバルに設定するには、**ipv6 nd raguard policy** コマンドを使用します。デバイスが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の場合、次のコマンドのいずれかを使用できます。

- **device-role**
- **drop-unsecure**
- **limit address-count**
- **sec-level minimum**
- **trusted-port**

- **validate source-mac**

IPv6 RA ガードをグローバルに設定した後、**ipv6 nd raguard attach-policy** コマンドを使用して、特定のインターフェイスで IPv6 RA ガードをイネーブルにできます。

例

次に、policy1 という RA ガード ポリシー名を定義し、デバイスをポリシー 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 nd raguard policy policy1
Device(config-ra-guard)#
```

関連コマンド

コマンド	説明
device-role	ポートに接続されているデバイスのロールを指定します。
drop-unsecure	オプションが指定されていないか無効なオプションが指定されているか、またはシグニチャが無効なメッセージをドロップします。
ipv6 nd raguard attach-policy	指定したインターフェイスで IPv6 RA ガード機能を適用します。
limit address-count	ポートで使用できる IPv6 アドレスの数を制限します。
sec-level minimum	CGA オプションを使用する場合の最小のセキュリティ レベル パラメータ値を指定します。
trusted-port	信頼できるポートにするポートを設定します。
validate source-mac	リンク層アドレスと比較して送信元 MAC アドレスを検査します。

ipv6 nd router-preference

特定のインターフェイス上のルータにデフォルト ルータ プリファレンス（DRP）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 router-preference** コマンドを使用します。 デフォルト DRP に戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd router-preference {**high**| **medium**| **low**}

no ipv6 nd router-preference

構文の説明

high	インターフェイスで指定されたルータの優先順位は高です。
medium	インターフェイスで指定されたルータの優先順位は中です。
low	インターフェイスで指定されたルータの優先順位は低です。

コマンド デフォルト

ルータ アドバタイズメント（RA）は、**medium** プリファレンスとともに送信されます。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.4(2)T	このコマンドが導入されました。
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(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	このコマンドが、Cisco IOS XE Release 2.1 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

RA メッセージは、**ipv6 nd router-preference** コマンドで設定された DRP とともに送信されます。DRP が設定されていない場合は、RA は中小規模のプリファレンスとともに送信されます。

DRP は、リンク上の 2 台のルータが、同等だがコストが等しくないルーティングを提供するときに、ホストがいずれかのルータを優先するようにポリシーで指示する場合に役立ちます。

例

次に、ギガビット イーサネット インターフェイス 0/1 上のルータに高い DRP を設定する例を示します。

```
Router(config)# interface Gigabit ethernet 0/1
Router(config-if)# ipv6 nd router-preference high
```

関連コマンド

コマンド	説明
ipv6 nd ra interval	インターフェイスで IPv6 ルータ アドバタイズメント メッセージが送信される時間間隔を設定します。
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 suppress attach-policy

指定したインターフェイスに IPv6 ネイバー探索（ND）抑制機能を適用するには、インターフェイス コンフィギュレーション モードで **ipv6 nd suppress attach-policy** コマンドを使用します。

ipv6 nd suppress attach-policy [*policy-name* [**vlan** {**add| except| none| remove| all**} *vlan* [*vlan1, vlan2, vlan3...*]]]

構文の説明

policy-name	（任意）IPv6 ND 抑制ポリシー名。
vlan	（任意）インターフェイスの VLAN に IPv6 ND 抑制機能を適用します。
add	検査する VLAN を追加します。
except	指定した 1 つ以外のすべての VLAN を検査します。
none	VLAN は検査されません。
remove	IPv6 ND 抑制から特定の VLAN を削除します。
all	ポートのすべての VLAN からの ND のトラフィックが検査されます。
vlan	（任意）インターフェイスの特定の VLAN。 複数の VLAN を指定できます（*vlan1*, *tb-vlan2*, *vlan3...*）。 使用できる VLAN 番号の範囲は 1 ～ 4094 です。

コマンド デフォルト

IPv6 ND 抑制ポリシー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
15.3(1)S	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 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

VLAN が指定されない場合（**vlan all** キーワードを *policy-name* 引数に続けて入力した場合と同じ）、ポートのすべての VLAN からの RA ガード トラフィックが解析されます。

VLAN パラメータは、1 ～ 4094 の間の 1 つの VLAN 番号、または 2 つの VLAN 番号で指定する（小さい方の数を先にして、間をダッシュで区切る）VLAN 範囲です。 カンマで区切った vlan パラメータの間、またはダッシュで指定した範囲の間には、スペースを入れないでください（例：vlan 1-100,200,300-400）。

例

次の例では、IPv6 ND 抑制機能がイーサネット インターフェイス 0/0 に適用されます。

```
Device(config)# interface Ethernet 0/0
Device(config-if)# ipv6 nd suppress attach-policy
```

関連コマンド

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

ipv6 nd suppress policy

IPv6 ネイバー探索（ND）マルチキャスト抑制をイネーブルにして、ND 抑制ポリシー コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **ipv6 nd suppress policy** コマンドを使用します。

ipv6 nd suppress policy *policy-name*

構文の説明

policy-name	IPv6 ND 抑制ポリシー名。

コマンド デフォルト

ND 抑制ポリシーは設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

使用上のガイドライン

デバイスの NA 抑制をグローバルに設定するには、**ipv6 nd suppress policy** コマンドを使用します。IPv6 ND 抑制をグローバルに設定した後、**ipv6 nd suppress attach-policy** コマンドを使用して、特定のインターフェイスで IPv6 ND 抑制をイネーブルにできます。

例

次に、policy1 という ND 抑制ポリシー名を定義し、デバイスをポリシー 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 nd suppress policy policy1
Device(config-nd-suppress)#
```

関連コマンド

コマンド	説明
ipv6 nd suppress attach-policy	指定したインターフェイスで IPv6 ND 抑制機能を適用します。

ipv6 neighbor binding logging

バインディング テーブルの主要イベントのロギング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 neighbor binding logging** コマンドを使用します。 この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 neighbor binding logging

no ipv6 neighbor binding logging

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

バインディング テーブルのイベントはログに記録されません。

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
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

ipv6 neighbor binding logging コマンドによって、次のようなバインディング テーブルのイベントをロギングできます。

- エントリがバインディング テーブルに挿入される。
- バインディング テーブル エントリが更新された。
- バインディング テーブル エントリがバインディング テーブルから削除された。
- バインディング テーブル エントリが既存エントリと衝突するため、またはエントリの最大数に到達したため、バインディング テーブルに挿入されなかった。

例

次に、バインディング テーブルのイベントのロギングをイネーブルにする例を示します。

```
Router(config)# ipv6 neighbor binding logging
```

関連コマンド

コマンド	説明
ipv6 neighbor binding vlan	バインディング テーブル データベースにスタティック エントリを追加します。
ipv6 neighbor tracking	バインディングテーブルのエントリを追跡します。
ipv6 snooping logging packet drop	IPv6 スヌーピング セキュリティのロギングを設定します。

ipv6 neighbor binding max-entries

バインディングテーブルキャッシュに挿入できるエントリの最大数を指定するには、グローバル コンフィギュレーション モードで **ipv6 neighbor binding max-entries** コマンドを使用します。 デフォルトに戻るには、**no** 形式のコマンドを使用します。

ipv6 neighbor binding max-entries *entries* [**vlan-limit** *number*| **interface-limit** *number*| **mac-limit** *number*]

no ipv6 neighbor binding max-entries *entries* [**vlan-limit**| **mac-limit**]

構文の説明

entries	キャッシュに挿入できるエントリ数。
vlan-limit *number*	（任意）VLAN数ごとにネイバーバインディング制限を指定します。
interface-limit *number*	（任意）インターフェイスごとにネイバーバインディング制限を指定します。
mac-limit *number*	（任意）メディア アクセス コントロール（MAC）アドレスごとにネイバー バインディング制限を指定します。

コマンド デフォルト

このコマンドはディセーブルです。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.2(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

ipv6 neighbor binding max-entries コマンドは、バインディング テーブルの内容を制御するために使用されます。 このコマンドは、バインディング テーブル キャッシュに挿入できるエントリの最大数を指定します。 この制限に到達すると、新しいエントリは拒否され、新しいエントリとネイバー探索プロトコル（NDP）トラフィックの送信元はドロップされます。

指定できるエントリの最大数がデータベース内の現在のエントリ数未満の場合、エントリはクリアされず、通常のキャッシュ削減後に新しいしきい値に到達します。

エントリの最大数は VLAN 数または MAC アドレス数によってグローバルに設定できます。

例

次に、キャッシュに挿入されるエントリの最大数をグローバルに指定する例を示します。

```
Router(config)# ipv6 neighbor binding max-entries 100
```

関連コマンド

コマンド	説明
ipv6 neighbor binding vlan	バインディング テーブル データベースにスタティック エントリを追加します。
ipv6 neighbor tracking	バインディングテーブルのエントリを追跡します。

ipv6 neighbor binding vlan

バインディング テーブル データベースにスタティック エントリを追加するには、グローバル コンフィギュレーション モードで **ipv6 neighbor binding vlan** コマンドを使用します。 スタティック 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 binding vlan *vlan-id* {**interface** *type number*| *ipv6-address*| *mac-address*} [**tracking** [**disable**| **enable**| **retry-interval** *value*]| **reachable-lifetime** *value*]

no ipv6 neighbor binding vlan *vlan-id*

構文の説明

vlan-id	指定した VLAN の ID。
interface *type number*	指定したインターフェイス タイプおよび番号でスタティック エントリを追加します。
ipv6-address	スタティック エントリの IPv6 アドレス。
mac-address	スタティック エントリのメディア アクセス コントロール（MAC）アドレス。
tracking	（任意）スタティック エントリの到達可能性を直接確認します。
disable	（任意）特定のスタティック エントリのトラッキングをディセーブルにします。
enable	（任意）特定のスタティック エントリのトラッキングをイネーブルにします。
retry-interval *value*	（任意）設定された間隔でスタティック エントリの到達可能性を秒単位で確認します。 指定できる範囲は 1 ～ 3600 で、デフォルトは 300 です。
reachable-lifetime *value*	（任意）到達可能という証明（トラッキングを介した直接的な到達可能、またはネイバー探索プロトコル（NDP）インスペクションを介した間接的な到達可能性）を受け取らずにエントリが到達可能と見なされる最大時間（秒単位）です。 その後、エントリは期限切れになります。 有効な範囲は 1 ～ 3600 秒で、デフォルトは 300 秒です。

コマンド デフォルト

再試行間隔：300 秒

到達可能ライフタイム：300 秒

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.2(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

ipv6 neighbor binding vlan コマンドは、バインディング テーブルの内容を制御するために使用されます。 バインディング テーブル データベースにスタティック エントリを追加するには、このコマンドを使用します。バインディングテーブルマネージャがエントリをエージングアウトし、プローブして到達可能性を直接確認します（**tracking** キーワードがイネーブルの場合）。 **tracking** キーワードは、このスタティック エントリの **ipv6 neighbor tracking** コマンドによってグローバルに提供される一般的な動作をオーバーライドします。 **disable** キーワードは、このスタティック エントリのトラッキングをディセーブルにします。 **stale-lifetime** キーワードは、到達可能でない（または期限切れ）と判断してからエントリを保持する最大時間を定義します。

例

次に、バインディング エントリの到達可能ライフタイムを 100 秒に変更する例を示します。

```
Router(config)# ipv6 neighbor binding vlan reachable-lifetime 100
```

関連コマンド

コマンド	説明
ipv6 neighbor binding max-entries	キャッシュに挿入できるエントリの最大数を指定します。
ipv6 neighbor tracking	バインディングテーブルのエントリを追跡します。

ipv6 neighbor tracking

バインディング テーブルのエントリを追跡するには、グローバル コンフィギュレーション モードで **ipv6 neighbor tracking** コマンドを使用します。 エントリ追跡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 neighbor tracking [**retry-interval** *value*]

no ipv6 neighbor tracking [**retry-interval** *value*]

構文の説明

retry-interval *value*	（任意）設定された間隔でスタティック エントリの到達可能性を確認します（秒単位）。2 回のプローブの間隔です。 指定できる範囲は1～3600 で、デフォルトは 300 です。

コマンド デフォルト

再試行間隔：300 秒

到達可能ライフタイム：300 秒

期限切れライフタイム：1440 分

ダウン ライフタイム：1440 分

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.2(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

ipv6 neighbor tracking コマンドは、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。 エントリの到達可能性は、ネイバー到達可能性の直接トラッキングに使用するネイバー到達不能検出（NUD）メカニズムを使用して、オプションの **retry-interval** キーワードで設定された間隔で（またはデフォルトの再試行間隔である 300 秒ごとに）テストされます。

到達可能性は、VERIFY_MAX_RETRIES 値（デフォルトは 10 秒）までネイバー探索プロトコル（NDP）インスペクションを使用して間接的に確立することもできます。 応答がない場合、エントリは期限切れライフタイム値に到達した後に期限切れと見なされ、削除されます（デフォルトは 1440 分）。

ipv6 neighbor tracking コマンドがディセーブルの場合、エントリは到達可能ライフタイム値（デフォルトは 300 秒）に達すると期限切れと見なされ、期限切れライフタイム値に達すると削除されます。

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値を変更するには、**ipv6 neighbor binding** コマンドを使用します。

例

次に、バインディング テーブルのエントリを追跡する例を示します。

```
Router(config)# ipv6 neighbor tracking
```

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。

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

list-name	プレフィックス リストの名前。 • 既存のアクセス リストと同じ名前にはできません。 • 「detail」または「summary」という名前にはできません。これらは、**show ipv6 prefix-list** コマンドのキーワードです。
seq *seq-number*	（任意）設定されるプレフィックス リスト エントリのシーケンス番号。
deny	基準を満たすネットワークを拒否します。
permit	基準を満たすネットワークを許可します。
ipv6-prefix	指定したプレフィックス リストに割り当てられる IPv6 ネットワーク。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの16ビット値を使用して、アドレスを 16 進数で指定します。
/*prefix-length*	IPv6 プレフィックスの長さ。 プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す10進値です。10 進数値の前にスラッシュ記号が必要です。
description *text*	プレフィックス リストの説明。長さは 80 文字までです。

ge *ge-value*	（任意）*ipv6-prefix*/*prefix-length* 引数と同じ、またはそれよりも長いプレフィックス長を指定します。 *length* の範囲の最小値です（長さの範囲の「から」の部分）。
le *le-value*	（任意）*ipv6-prefix*/*prefix-length* 引数と同じ、またはそれよりも短いプレフィックス長を指定します。 *length* の範囲の最大値です（長さの範囲の「まで」の部分）。

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
12.2(2)T	このコマンドが導入されました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
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 3.2SE	このコマンドが Cisco IOS XE Release 3.2SE に統合されました。

使用上のガイドライン

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

ネットワークがアップデートでアドバタイズされないようにするには、**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。 効率性のために、*seq-number* 引数を使用して、リストの上部に最も一般的な許可または拒否を配置できます。

show ipv6 prefix-list コマンドは、エントリのシーケンス番号を表示します。

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

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

（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的な deny any any 文が含まれています。

例

次の例は、プレフィックス ::/0 のすべてのルートを拒否します。

```
Router(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。

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

次に、プレフィックス 5F00::/48 からプレフィックス 5F00::/64 までのすべてのプレフィックスを受け入れるようにプレフィックスのグループを指定する例を示します。

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

次の例は、プレフィックス 2001:0DB8::/64 のルートで 64 ビットを超えるプレフィックス長を拒否します。

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

次の例は、すべてのアドレス空間で 32 ～ 64 ビットのマスク長を許可します。

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

次の例は、すべてのアドレス空間で 32 ビットを超えるマスク長を拒否します。

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

次の例は、プレフィックス 2002::/128 のすべてのルートを拒否します。

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

次の例は、プレフィックス ::/0 のすべてのルートを許可します。

```
Router(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	ネットワークがアップデート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 リストのエントリのシーケンス番号の生成をイネーブルにします。
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 ルートを配布します。
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。