IPv6 クライアント IP アドレス ラーニングの設定

IPv6 クライアント アドレス ラーニングの前提条件

IPv6 クライアント アドレス ラーニングを設定する前に、IPv6 をサポートするようにワイヤレス クライアントを設定します。

関連トピック

RA ガード ポリシーの設定（CLI） （8 ページ）

IPv6 クライアント アドレス ラーニングについて

クライアント アドレス ラーニングは、アソシエーション、再アソシエーション、非認証、タイムアウト時に、ワイヤレス クライアントの IPv4 および IPv6 アドレス、デバイスによって維持されるクライアント遷移ステートについて学習するために、デバイスで設定されます。

IPv6 クライアントで IPv6 アドレスを取得するには、次の 3 つの方法があります。

- ステートレス アドレス自動設定（SLACC）
- ステートフル DHCPv6
- 静的設定

これらの方法のいずれの場合も、IPv6 クライアントは常にネイバー送信要求 DAD（重複アドレス検出）要求を送信して、ネットワークに重複する IP アドレスがないようにします。デバイスはクライアントの NDP および DHCPv6 パケットをスヌープして、そのクライアント IP アドレスについて学習します。

SLAAC アドレス割り当て

IPv6 クライアント アドレス割り当て用の最も一般的な方法は、ステートレス アドレス自動設定（SLAAC）です。SLAAC はクライアントが IPv6 プレフィクスに基づいてアドレスを自己割り当てするシンプルなプラグアンドプレイ接続を提供します。このプロセスが実現しました。

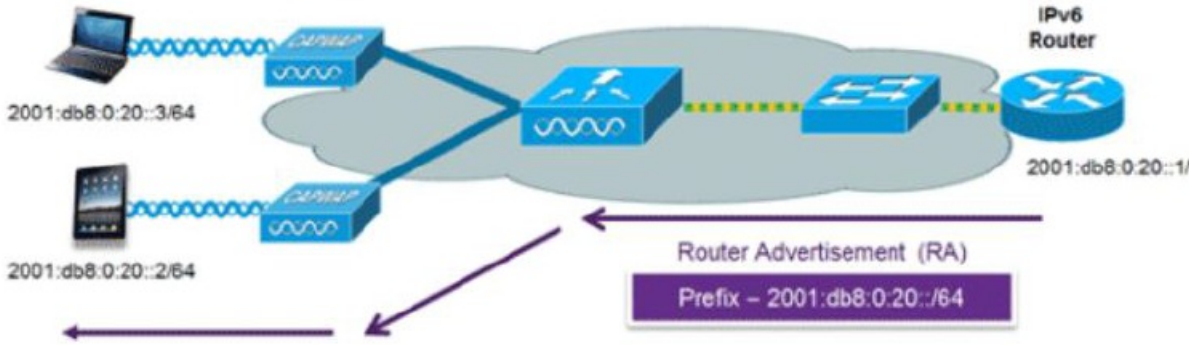
次のように、ステートレス アドレス自動設定（SLAAC）は設定されています。

- ホストは、ルータ送信要求メッセージを送信します。
- ホストは、ルータ アドバタイズメント メッセージを待機します。
- ホストは、ルータ アドバタイズメント メッセージから IPv6 プレフィックスの最初の 64 ビットを取得し、これを 64 ビット EUI-64 アドレス（イーサネットの場合、MAC アドレスから作成されます）と組み合わせて、グローバル ユニキャスト メッセージを作成します。ホストは、デフォルト ゲートウェイとして、ルータ アドバタイズメント メッセージの IP ヘッダーに含まれる送信元 IP アドレスも使用します。
- 重複アドレス検出は、選択されるランダムアドレスが他のクライアントと重複しないように、IPv6 クライアントによって実行されます。
- アルゴリズムの選択はクライアントに依存し、多くの場合は設定できます。

次の 2 種類のアルゴリズムに基づいて IPv6 アドレスの最後の 64 ビットが学習可能です。

- インターフェイスの MAC アドレスに基づく EUI-64、または
- ランダムに生成されるプライベート アドレス。

図 *1 : SLAAC* アドレス割り当て



Cisco 対応 IPv6 ルータからの次の Cisco IOS コンフィギュレーション コマンドを使用して、SLAAC のアドレッシングとルータ アドバタイズメントをイネーブルにします。

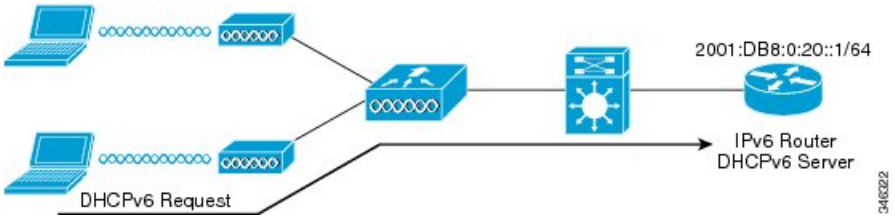
```
ipv6 unicast-routing
interface Vlan20
description IPv6-SLAAC
ip address 192.168.20.1 255.255.255.0
ipv6 address FE80:DB8:0:20::1 linklocal
ipv6 address 2001:DB8:0:20::1/64
ipv6 enable
end
```

関連トピック

IPv6 スヌーピングの設定（CLI） （16 ページ）
DHCP プールの設定（CLI） （19 ページ）
DHCP を使用しないステートレス自動アドレス設定の設定（CLI） （20 ページ）
DHCP によるステートレス自動アドレス設定の設定（CLI） （21 ページ）
ステートフル DHCP のローカル設定（CLI） （22 ページ）
ステートフル DHCP の外部的設定（CLI） （24 ページ）

ステートフル DHCPv6 アドレス割り当て

図 *2 :* ステートフル *DHCPv6* アドレス割り当て



DHCPv6 の使用は、SLAAC がすでに導入されている場合は、IPv6 クライアント接続で要求されません。DHCPv6 にはステートレスおよびステートフルという 2 種類の動作モードがあります。

DHCPv6 ステートレス モードは、ルータ アドバタイズメントで使用できない追加のネットワーク情報をクライアントに提供するために使用しますが、これはIPv6アドレスではありません。すでに SLAAC によって提供されているためです。この情報には DNS ドメイン名、DNS サーバ、その他のDHCPベンダー固有オプションを含めることができます。このインターフェイス設定は、SLAAC をイネーブルにしてステートレス DHCPv6 を実装する Cisco IOS IPv6 ルータ用です。

```
ipv6 unicast-routing
ipv6 dhcp pool IPV6_DHCPPOOL
address prefix 2001:db8:5:10::/64
domain-name cisco.com
dns-server 2001:db8:6:6::1
interface Vlan20
description IPv6-DHCP-Stateless
ip address 192.168.20.1 255.255.255.0
ipv6 nd other-config-flag
ipv6 dhcp server IPV6_DHCPPOOL
ipv6 address 2001:DB8:0:20::1/64
end
```

マネージド モードとも呼ばれる DHCPv6 ステートフル オプションは、DHCPv4 と同様に動作します。つまり、クライアント SLAAC のとおりにアドレスの最後の 64 ビットを生成するのではなく、固有のアドレスをそれぞれのクライアントに割り当てます。次のインターフェイス設定は、ローカル Deviceのステートフル DHCPv6 を実装している Cisco IOS IPv6 ルータ用です。

```
ipv6 unicast-routing
ipv6 dhcp pool IPV6_DHCPPOOL
address prefix 2001:db8:5:10::/64
domain-name cisco.com
dns-server 2001:db8:6:6::1
interface Vlan20
description IPv6-DHCP-Stateful
ip address 192.168.20.1 255.255.255.0
ipv6 address 2001:DB8:0:20::1/64
ipv6 nd prefix 2001:DB8:0:20::/64 no-advertise
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
ipv6 dhcp server IPV6_DHCPPOOL
end
```

次のインターフェイス設定は、外部DHCPサーバのステートフルDHCPv6を実装しているCisco IOS IPv6 ルータ用です。

```
ipv6 unicast-routing
domain-name cisco.com
dns-server 2001:db8:6:6::1
interface Vlan20
description IPv6-DHCP-Stateful
ip address 192.168.20.1 255.255.255.0
ipv6 address 2001:DB8:0:20::1/64
ipv6 nd prefix 2001:DB8:0:20::/64 no-advertise
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
ipv6 dhcp_relay destination 2001:DB8:0:20::2
end
```

関連トピック

IPv6 スヌーピングの設定（CLI） （16 ページ）

静的 IP アドレス割り当て

クライアントにスタティックに設定されたアドレス。

ルータ要求

ルータ送信要求メッセージは、ローカル ルーティングに関する情報を入手できる、またはステートレス自動設定を設定できるルータ アドバタイズメントを送信するようにローカル ルータを促進するために、ホスト コントローラによって発行されます。ルータ アドバタイズメントは定期的に送信され、起動時または再起動操作後などに、ホストはルータ送信要求を使用して即時ルータ アドバタイズメントを要求します。

関連トピック

IPv6 ND 抑制ポリシーの設定（CLI） （16 ページ）

ルータ アドバタイズメント

ルータ アドバタイズメント メッセージは、ルータから定期的に送信されるか、ホストからのルータ送信要求メッセージへの応答として送信されます。これらのメッセージに含まれる情報は、ホストでステートレス自動設定を実行し、ルーティング テーブルを変更するために使用されます。

関連トピック

IPv6 ND 抑制ポリシーの設定（CLI） （16 ページ）

ネイバー探索

IPv6 ネイバー ディスカバリとは、近隣のノード間の関係を決定するメッセージとプロセスのことです。ネイバー ディスカバリは、IPv4 で使用されていた ARP、ICMP ルータ探索、および ICMP リダイレクトに代わるものです。

信頼できるバインディング テーブル データベースを構築するために、IPv6 ネイバー ディスカバリ検査によってネイバー ディスカバリ メッセージが分析され、準拠しない IPv6 ネイバー ディスカバリ パケットはドロップされます。 スイッチ内のネイバー バインディング テーブルでは、各 IPv6 アドレスと、アソシエートされた MAC アドレスが追跡されます。クライアントは、ネイバー バインディング タイマーに従って、テーブルから消去されます。

関連トピック

IPv6 ND 抑制ポリシーの設定（CLI） （16 ページ）

ネイバー探索抑制

ワイヤレス クライアントの IPv6 アドレスは、デバイスによってキャッシュされます。デバイスが IPv6 アドレスを検索する NS マルチキャストを受信して、デバイスによって特定された目的のアドレスがクライアントのいずれかに属している場合、デバイスはクライアントに代わって NA メッセージで応答します。このプロセスによって IPv4 のアドレス解決プロトコル（ARP）テーブルと同等のテーブルが生成されますが、より効率的であり、たいていの場合、使用されるメッセージは少なくなります。

（注） デバイスがプロキシのように動作し NA で応答するのは、**ipv6 nd suppress** コマンドが設定されている場合だけです。

デバイスにワイヤレス クライアントの IPv6 アドレスがない場合、デバイスは NA で応答せず、NS パケットをワイヤレス側に転送します。この問題を解決するために、NS マルチキャスト フォワーディング ノブが用意されています。このノブがイネーブルの場合、デバイスは存在しない（キャッシュ欠落）IPv6 アドレスの NS パケットを取得し、ワイヤレス側に転送します。このパケットは、目的のワイヤレス クライアントに到達し、クライアントは NA で応答します。

このキャッシュ ミス シナリオが発生するのはまれで、完全な IPv6 スタックが実装されていないクライアントが、NDP 時にそれらの IPv6 アドレスをアドバタイズしない可能性はほとんどありません。

関連トピック

IPv6 ND 抑制ポリシーの設定（CLI） （16 ページ）

RA ガード

IPv6 クライアントは、IPv6 アドレスを設定し、IPv6 ルータ アドバタイズメント（RA）パケットに基づいてルータ テーブルにデータを入力します。RA ガード機能は、有線ネットワークの RA ガード機能に類似しています。RA ガードは、ワイヤレス クライアントから発信される不要な、または不正な RA パケットをドロップすることによって、IPv6 ネットワークのセキュリティを強化します。この機能が設定されていないと、悪意のある IPv6 ワイヤレス クライアントが、多くの場合は高い優先順位で、それ自体をネットワークのルータとして通知する可能性があり、そのため、正規の IPv6 ルータよりも優先されることになります。

また、RA ガードは、着信 RA を調べて、メッセージまたはスイッチ設定で検出された情報のみに基づいて、それらをスイッチするかブロックするかを決定します。受信したフレームで使用できる情報は、RA の検証に有用です。

- フレームが受信されるポート
- IPv6 送信元アドレス
- プレフィックス リスト

スイッチで作成された次の設定情報は、受信した RA フレームで検出された情報に対して検証するときに RA ガードで使用できます。

- RA ガード メッセージの受信用に信頼できる/信頼できないポート
- RA 送信者の信頼できる/信頼できない送信元 IPv6 アドレス
- 信頼できる/信頼できないプレフィックス リストおよびプレフィックス範囲
- ルータ プリファレンス

RA ガードはデバイスで行われます。デバイスで RA メッセージをドロップするようにデバイスを設定できます。すべての IPv6 RA メッセージがドロップされ、それによって他のワイヤレス クライアントおよびアップストリーム有線ネットワークが悪意のある IPv6 クライアントから保護されます。

```
//Create a policy for RA Guard//
ipv6 nd raguard policy raguard-router
trusted-port
device-role router

//Applying the RA Guard Policy on port/interface//
interface tengigabitethernet1/0/1 (Katana)
interface gigabitethernet1/0/1 (Edison)

ipv6 nd raguard attach-policy raguard-router
```

関連トピック

RA ガード ポリシーの設定（CLI） （8 ページ）
RA ガード ポリシーの適用（CLI） （9 ページ）
RA スロットル ポリシーの設定（CLI） （10 ページ）
VLAN への RA スロットル ポリシーの適用（CLI） （11 ページ）

RA スロットリング

RA スロットリングは、コントローラがワイヤレス ネットワーク宛ての RA パケットを強制的に制限できるようにします。RA スロットリングを有効にすることにより、多数の RA パケットを送信するルータを最小限の頻度に調整することができ、その場合も IPv6 クライアントの接続は維持されます。クライアントが RS パケットを送信すると、RA がクライアントに返送されます。この RA は、コントローラを通過でき、クライアントにユニキャストされます。このプロセスによって、新しいクライアントやローミング クライアントが RA スロットリングの影響を受けないようにすることができます。

関連トピック

RA ガード ポリシーの設定（CLI） （8 ページ）
RA ガード ポリシーの適用（CLI） （9 ページ）
RA スロットル ポリシーの設定（CLI） （10 ページ）
VLAN への RA スロットル ポリシーの適用（CLI） （11 ページ）

IPv6 ユニキャストの設定（CLI）

IPv6 ユニキャストはスイッチとコントローラで常にイネーブルにする必要があります。IPv6 ユニキャスト ルーティングはディセーブルに設定されています。

始める前に

IPv6ユニキャストデータグラムの転送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 unicast-routing** コマンドを使用します。IPv6 ユニキャスト データグラムの転送を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。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 unicast routing** 例： `Device (config)# ipv6 unicast routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。

RA ガード ポリシーの設定（CLI）

IPv6 クライアント アドレスを追加し、IPv6 ルータ アドバタイズメント パケットに基づいてルータ テーブルに入力するには、デバイスで RA ガード ポリシーを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 nd raguard policy raguard-router** 例： `Device(config)# ipv6 nd raguard policy raguard-router`	RA ガード ポリシー名を定義して、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。

	コマンドまたはアクション	目的
ステップ 3	**trustedport** 例： `Device(config-ra-guard)# trustedport`	（任意）このポリシーが信頼できるポートに適用されることを指定します。
ステップ 4	**device-role router** 例： `Device(config-ra-guard)# device-role router`	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。
ステップ 5	**exit** 例： `Device(config-ra-guard)# exit`	RA ガード ポリシー コンフィギュレーション モードを終了してグローバル コンフィギュレーション モードに戻ります。

関連トピック

RA ガード （6 ページ）
RA スロットリング （7 ページ）
RA ガード ポリシーの適用（CLI） （9 ページ）
RA スロットル ポリシーの設定（CLI） （10 ページ）
VLAN への RA スロットル ポリシーの適用（CLI） （11 ページ）
IPv6 クライアント アドレス ラーニングの前提条件 （1 ページ）

RA ガード ポリシーの適用（CLI）

デバイスで RA ガード ポリシーを適用すると、すべての信頼できない RA がブロックされます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface tengigabitethernet 1/0/1** 例： `Device (config)# interface tengigabitethernet 1/0/1`	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 nd raguard attach-policy raguard-router** 例： `Device(config-if)# ipv6 nd raguard attach-policy raguard-router`	指定したインターフェイスに IPv6 RA ガード機能を適用します。
ステップ 4	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

関連トピック

RA ガード ポリシーの設定（CLI） （8 ページ）
RA ガード （6 ページ）
RA スロットリング （7 ページ）
RA スロットル ポリシーの設定（CLI） （10 ページ）
VLAN への RA スロットル ポリシーの適用（CLI） （11 ページ）

RA スロットル ポリシーの設定（CLI）

強制的に制限できるように RA スロットル ポリシーを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 nd ra-throttler policy ra-throttler1** 例： `Device(config)# ipv6 nd ra-throttler policy ra-throttler1`	ルータ アドバタイズメント（RA）スロットラ ポリシー名を定義して、IPv6 RA スロットル ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**throttleperiod500** 例： `Device(config-nd-ra-throttle)# throttleperiod 500`	IPv6 RA スロットラ ポリシーのスロットル期間を設定します。

	コマンドまたはアクション	目的
ステップ 4	**max-through10** 例： `Device(config-nd-ra-throttle)# max-through 500`	スロットル期間ごとに、VLANあたりのマルチキャスト RA を制限します。
ステップ 5	**allow-atleast 5at-most 10** 例： `Device(config-nd-ra-throttle)# allow-atleast 5 at-most 10`	RA スロットラ ポリシーのスロットル期間ごとに、デバイスあたりのマルチキャスト RA 数を制限します。

関連トピック

RA ガード ポリシーの設定（CLI） （8 ページ）
RA ガード ポリシーの適用（CLI） （9 ページ）
RA ガード （6 ページ）
RA スロットリング （7 ページ）
VLAN への RA スロットル ポリシーの適用（CLI） （11 ページ）

VLAN への RA スロットル ポリシーの適用（CLI）

VLAN に RA スロットル ポリシーを適用します。RA スロットリングを有効にすることにより、多数の RA パケットを送信するルータを最小限の頻度に調整することができ、その場合も IPv6 クライアントの接続は維持されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan configuration 1** 例： `Device(config)# vlan configuration 1`	VLANまたはVLANの集合を設定して、VLAN コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 nd ra throttler attach-policy ra-throttler1** 例： `Device(config-vlan)# ipv6 nd ra throttler attach-policy ra-throttler1`	VLAN または VLAN の集合に IPv6 RA スロットル ポリシーを接続します。

関連トピック

RA ガード ポリシーの設定（CLI） （8 ページ）
RA ガード ポリシーの適用（CLI） （9 ページ）
RA スロットル ポリシーの設定（CLI） （10 ページ）
RA ガード （6 ページ）
RA スロットリング （7 ページ）

IPv6 ネイバー プロービングの設定方法

IPv6 ネイバー プロービングが機能するには、バインディング テーブルにデータを入力する必要があります。このタスクは、バインディング テーブル内のエントリのライフ サイクルで微調整を行うために実行します。

1 つの IPv6 クライアントは、随時に複数の IPv6 アドレスを持つことができます。**show ipv6 neighbor binding mac** *mac_address* コマンドを実行すると、これらのアドレスの状態は、そのクライアント MAC アドレスの IPv6 ネイバー バインディング テーブルで `REACHABLE` として表示されます。これらのアドレス上で300秒間コントロールアクティビティがない場合、アドレスは `STALE` 状態に移行し、それ以降はクライアントで使用できなくなります。

device-tracking tracking コマンドを使用して定期プローブ（デフォルトの間隔は 300 秒）をすべての IPv6 クライアントに送信し、クライアントの IPv6 アドレスがエージ アウトしておらず、`STALE` 状態に移行していないことを確かめます。これらのプローブは、送信元 IP アドレスがすべてゼロ、つまり、重複アドレス検出（DAD）プローブのスイッチから送信されます。DAD プローブに応答しないために 300 後にエージ アウトするクライアントがいくつか存在します。

（注） IPv6 ネイバー プロービングは、IP アドレスを取得するかまたは維持するのが難しいホストに関してネットワークの問題がある場合のみ、有効にしてください。特に、ホストが IP リースの更新をネゴシエーションしているときの時間枠内でDADプローブがホストに発行されると、DAD チャレンジによりホストが IP アドレスを放棄することがあります。不必要に IPv6 ネイバー プロービングを有効にすると、予期しないホストの動作が生じる場合があります。

（注） Cisco IOS 15.2(5)E リリース以前の場合は、インターフェイス レベルで IPv6 スヌーピング ポリシーを削除し、VLAN レベルでポリシーをアタッチする必要があります。手順 8 と手順 9 を実行し、VLAN レベルで IPv6 スヌーピング ポリシーをアタッチします。

IPv6 ネイバー プロービングが VLAN で有効な場合は、トランク ポートを介する学習やホストを無効にするために、追加の設定を実行する必要があります。トランク ポートを介した学習を無効にするには、**trusted-port** および **device-role switch** でポリシーを設定する必要があります。この設定では、トランク ポートに接続されている他のアクセス スイッチに、それぞれが接続しているホストに対してファースト ホップ セキュリティを提供するポリシーを用意する必要があります。各スイッチはそれぞれのホストに対してセキュリティを提供する必要があります。手順 10 ～ 12 を実行し、これらの属性でポリシーを設定します。

以下の手順を実行し、IPv6 ネイバー プロービングを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**device-trackingtracking** 例： `Device(config)# device-tracking tracking`	IPv6 ネイバープロービングを有効にします。 IPv6 ネイバープロービングを無効にするには、このコマンドの **no** フォームを使用します。
ステップ 4	**interface vlan** *vlan-id* 例： `Device(config)# interface vlan 1810`	インターフェイス コンフィギュレーション モードを開始して、IP 情報が割り当てられている VLAN を指定します。指定できる範囲は 1 ～ 4094 です。
ステップ 5	**ipv6 enable** 例： `Device(config-if)# ipv6 enable`	明示的な IPv6 アドレスが設定されていないインターフェイスにおける IPv6 処理をイネーブルにします。

	コマンドまたはアクション	目的
		（注） **ipv6 enable** を設定して VLAN に SVI を作成すると、結果として、SVI のリンク ローカル アドレスがプローブのソース アドレスとして使われます。このため、プロービングは DAD メッセージではなく、NS メッセージとして実行されます。この設定ではプローブ応答のレートが高くなります。一部のホストは DAD リクエストを無視することがあります。ただし、NS メッセージにはすべてのホストが応答します。
ステップ 6	**no shutdown** 例： `Device(config-if)# no shutdown`	インターフェイスをイネーブルにします。 dot1x を IPv4 に対して有効にする場合、dot1x が有効になっているインターフェイス上のポリシーは自動的に設定され、トラッキングは特に IPv6 ネイバー プロービングに対して有効になります。この場合、グローバル設定レベルでトラッキング動作を変更しても、これらの自動的に設定されているポリシーのトラッキングには何の影響もありません。トラッキングはすべてのインターフェイスで常に有効になります。
ステップ 7	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 8	**vlan configuration** *vlan_list* 例： `Device(config)# vlan configuration 1815`	VLAN インターフェイスのコンフィギュレーション モードを開始し、IPv6 スヌーピング ポリシーをアタッチする VLAN を指定します。
ステップ 9	**ipv6 snooping** [**attach-policy** *policy_name*] 例：	すべてのスイッチおよびスタック インターフェイスで、IPv6 スヌーピング ポ

	コマンドまたはアクション	目的
	`Device(config-vlan-config)# ipv6 snooping attach-policy example_policy`	リシーを指定した VLAN にアタッチします。attach-policy オプションを使用しない場合、デフォルト ポリシーがアタッチされます。デフォルトポリシーは、セキュリティ レベル guard、デバイス ロール node、プロトコル ndp および dhcp です。 （注） すべてのインターフェイスで同じユーザ定義のポリシーが設定されている場合、このポリシーを VLAN 上に設定して、インターフェイスから削除できます。インターフェイス上に設定されているポリシーが異なる場合、インターフェイスに設定されているポリシーは削除しないでください。上記のデフォルト ポリシーは VLAN レベルで適用してください。
ステップ 10	**ipv6 snooping policy** *policy_name* 例： `Device(config-vlan-config)# ipv6 snooping policy example_policy`	IPv6 スヌーピング ポリシーを設定し、IPv6 スヌーピング コンフィギュレーション モードを開始します。
ステップ 11	**trusted-port** 例： `Device(config-ipv6-snooping)# trusted-port`	信頼できるポートにするポートを設定します。
ステップ 12	**device-roleswitch** 例： `Device(config-ipv6-snooping)# device-role switch`	スイッチに接続されているデバイスの役割を設定します。
ステップ 13	**end** 例： `Device(config-ipv6-snooping)# end`	設定モードを終了します。

IPv6 スヌーピングの設定（CLI）

IPv6 スヌーピングはスイッチとコントローラで常にイネーブルにする必要があります。

始める前に

クライアント マシンで IPv6 をイネーブルにします。

手順

	コマンドまたはアクション	目的
ステップ 1	**vlan configuration 1** 例： `Device(config)# vlan configuration 1`	VLAN コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 snooping** 例： `Device(config-vlan)# ipv6 snooping`	Vlan で IPv6 スヌーピングをイネーブルにします。
ステップ 3	**ipv6 nd suppress** 例： `Device(config-vlan-config)# ipv6 nd suppress`	Vlan で IPv6 ND 抑制をイネーブルにします。
ステップ 4	**exit** 例： `Device(config-vlan-config)# exit`	設定を保存し、Vlan コンフィギュレーション モードを終了します。

関連トピック

SLAAC アドレス割り当て （2 ページ）
ステートフル DHCPv6 アドレス割り当て （3 ページ）

IPv6 ND 抑制ポリシーの設定（CLI）

IPv6 ネイバー探索（ND）マルチキャスト抑制機能では、ドロップする（およびターゲットに代わって送信要求に応答する）、またはユニキャスト トラフィックに変換することで、できるだけ多くの ND マルチキャスト ネイバー送信要求（NS）メッセージを停止します。この機能は、レイヤ 2 スイッチまたはワイヤレス コントローラで実行され、適切なリンクの処理に必要な制御トラフィックの量を減らすために使用されます。

アドレスがバインディング テーブルに挿入されると、マルチキャスト アドレスに送信されたアドレス解決要求が代行受信され、デバイスはアドレスの所有者に代わって応答するか、レイヤ 2 で要求をユニキャスト メッセージに変換して宛先に転送します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device(config)# enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 nd suppress policy** 例： `Device (config)# ipv6 nd suppress policy`	ND 制御ポリシー名を定義して ND 制御ポリシー コンフィギュレーション モードを開始します。

関連トピック

ルータ要求 （5 ページ）
ルータ アドバタイズメント （5 ページ）
ネイバー探索 （5 ページ）
ネイバー探索抑制 （6 ページ）

VLAN/PortChannel での IPv6 スヌーピングの設定

ネイバー探索（ND）抑制は、VLAN またはスイッチ ポートでイネーブルまたはディセーブルにできます。

始める前に

手順

	コマンドまたはアクション	目的
ステップ 1	**vlan config901** 例： `Device(config)# vlan config901`	VLAN を作成し、VLAN コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**ipv6 nd suppress** 例： `Device(config-vlan)# ipv6 nd suppress`	VLAN に IPv6 nd 抑制を適用します。
ステップ 3	**end** 例： `Device(config-vlan)# end`	VLAN コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 4	**interface gi1/0/1** 例： `Device (config)# interface gi1/0/1`	ギガビット イーサネット ポート インターフェイスを作成します。
ステップ 5	**ipv6 nd suppress** 例： `Device(config-vlan)# ipv6 nd suppress`	インターフェイスに IPv6 nd 抑制を適用します。
ステップ 6	**end** 例： `Device(config-vlan)# end`	VLAN コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

Switch での IPv6 の設定（CLI）

インターフェイス上の IPv6 を設定するには、この設定例を使用します。

始める前に

クライアント上の IPv6 および有線インフラストラクチャ上の IPv6 サポートをイネーブルにします。

手順

	コマンドまたはアクション	目的
ステップ 1	**interface vlan 1** 例： `Device(config)# interface vlan 1`	インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 2	**ip address fe80::1 link-local**
	例：
	`Device(config-if)# ip address 198.51.100.1 255.255.255.0`
	`Device(config-if)# ipv6 address fe80::1 link-local`
	`Device(config-if)# ipv6 address`
		リンクローカル オプションを使用してインターフェイスで IPv6 アドレスを設定します。

	コマンドまたはアクション	目的
	2001:DB8:0:1:FFFF:1234::5/64 Device(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64	
ステップ 3	**ipv6 enable** 例： Device(config)# ipv6 enable	（任意）インターフェイス上で IPv6 をイネーブルにします。
ステップ 4	**end** 例： Device(config)# end	インターフェイスモードを終了します。

DHCP プールの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**ipv6 dhcp pool Vlan21** 例： Device(config)# ipv6 dhcp pool vlan1	コンフィギュレーション モードを開始し、VLAN の IPv6 DHCP プールを設定します。
ステップ 2	**address prefix 2001:DB8:0:1:FFFF:1234::/64lifetime 300 10** 例： Device(config-dhcpv6)# address prefix 2001:DB8:0:1:FFFF:1234::/64 lifetime 300 10	コンフィギュレーション DHCP モードを開始し、VLAN のアドレス プールとそのライフタイムを設定します。
ステップ 3	**dns-server 2001:100:0:1::1** 例： Device(config-dhcpv6)# dns-server 2001:20:21::1	DHCP プールの DNS サーバを設定します。
ステップ 4	**domain-name example.com** 例： Device(config-dhcpv6)# domain-name example.com	完全な非修飾ホスト名になるようにドメイン名を設定します。
ステップ 5	**end** 例： Device(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

SLAAC アドレス割り当て （2 ページ）
ステートフル DHCPv6 アドレス割り当て （3 ページ）

DHCP を使用しないステートレス自動アドレス設定の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**interface vlan 1** 例： `Device(config)# interface vlan 1`	インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 2	**ip address fe80::1 link-local**
	例：
	`Device(config-if)# ip address 198.51.100.1 255.255.255.0`
	`Device(config-if)# ipv6 address fe80::1 link-local`
	`Device(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`Device(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64`
		リンクローカル オプションを使用してインターフェイスで IPv6 アドレスを設定します。

ステップ 3	**ipv6 enable** 例： `Device(config)# ipv6 enable`	（任意）インターフェイス上で IPv6 をイネーブルにします。

ステップ 4	**no ipv6 nd managed-config-flag**
	例：
	`Device(config)#interface vlan 1`
	`Device(config-if)# no ipv6 nd managed-config-flag`
		接続されたホストで、アドレスの取得にステートフル自動設定が使用されないようにします。

ステップ 5	**no ipv6 nd other-config-flag** 例： `Device(config-if)# no ipv6 nd other-config-flag`	接続されたホストで、DHCP からの非アドレス オプションの取得に（ドメインなど）ステートフル自動設定が使用されないようにします。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

SLAAC アドレス割り当て （2 ページ）
ステートフル DHCPv6 アドレス割り当て （3 ページ）

DHCPによるステートレス自動アドレス設定の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**interface vlan 1** 例： `Device(config)# interface vlan 1`	インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 2	**ip address fe80::1 link-local**
	例：
	`Device(config-if)# ip address 198.51.100.1 255.255.255.0`
	`Device(config-if)# ipv6 address fe80::1 link-local`
	`Device(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`Device(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64`
		リンクローカル オプションを使用してインターフェイスで IPv6 アドレスを設定します。

ステップ 3	**ipv6 enable** 例： `Device(config)# ipv6 enable`	（任意）インターフェイス上で IPv6 をイネーブルにします。

ステップ 4	**no ipv6 nd managed-config-flag**
	例：
	`Device(config)#interface vlan 1`
	`Device(config-if)# no ipv6 nd managed-config-flag`
		接続されたホストで、アドレスの取得にステートフル自動設定が使用されないようにします。

ステップ 5	**ipv6 nd other-config-flag** 例： `Device(config-if)# no ipv6 nd other-config-flag`	接続されたホストで、DHCP からの非アドレス オプションの取得に（ドメインなど）ステートフル自動設定が使用されないようにします。
ステップ 6	**end** 例： `Device(config)# end`	インターフェイスモードを終了します。

関連トピック

SLAAC アドレス割り当て （2 ページ）

ステートフル DHCPv6 アドレス割り当て （3 ページ）

ステートフル DHCP のローカル設定（CLI）

このインターフェイス設定は、ローカル のステートフル DHCPv6 を実装している Cisco IOS Ipv6 ルータ用です。Device

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	ユニキャスト用に IPv6 を設定します。
ステップ 3	**ipv6 dhcp pool IPv6_DHCPPOOL** 例： `Device (config)# ipv6 dhcp pool IPv6_DHCPPOOL`	コンフィギュレーション モードを開始し、VLAN の IPv6 DHCP プールを設定します。
ステップ 4	**address prefix 2001:DB8:0:1:FFFF:1234::/64** 例： `Device (config-dhcpv6)# address prefix 2001:DB8:0:1:FFFF:1234::/64`	プールに入力するアドレス範囲を指定します。
ステップ 5	**dns-server 2001:100:0:1::1** 例： `Device (config-dhcpv6)# dns-server 2001:100:0:1::1`	DHCP クライアントに DNS サーバのオプションを提供します。
ステップ 6	**domain-name example.com** 例： `Device (config-dhcpv6)# domain-name example.com`	DHCP クライアントにドメイン名オプションを提供します。
ステップ 7	**exit** 例： `Device (config-dhcpv6)# exit`	前のモードに戻ります。

	コマンドまたはアクション	目的
ステップ 8	**interface vlan1** 例： `Device (config)# interface vlan 1`	インターフェイス モードを開始して、ステートフル DHCP を設定します。
ステップ 9	**description IPv6-DHCP-Stateful** 例： `Device (config-if)# description IPv6-DHCP-Stateful`	ステートフル IPv6 DHCP の説明を入力します。
ステップ 10	**ipv6 address 2001:DB8:0:20::1/64** 例： `Device (config-if)# ipv6 address 2001:DB8:0:20::1/64`	ステートフル IPv6 DHCP の IPv6 アドレスを入力します。
ステップ 11	**ip address 192.168.20.1 255.255.255.0** 例： `Device (config-if)# ip address 192.168.20.1 255.255.255.0`	ステートフル IPv6 DHCP の IPv6 アドレスを入力します。
ステップ 12	**ipv6 nd prefix 2001:db8::/64no-advertise** 例： `Device (config-if)# ipv6 nd prefix 2001:db8::/64 no-advertise`	アドバタイズしてはならない、IPv6 ルーティング プレフィックス アドバタイズメントを設定します。
ステップ 13	**ipv6 nd managed-config-flag** 例： `Device (config-if)# ipv6 nd managed-config-flag`	ホストでアドレス設定に DHCP を使用できるように、IPv6 インターフェイス ネイバー探索を設定します。
ステップ 14	**ipv6 nd other-config-flag** 例： `Device (config-if)# ipv6 nd other-config-flag`	ホストで非アドレス設定に DHCP を使用できるように、IPv6 インターフェイス ネイバー探索を設定します。
ステップ 15	**ipv6 dhcp server IPv6_DHCPPOOL** 例： `Device (config-if)# ipv6 dhcp server IPv6_DHCPPOOL`	インターフェイスに DHCP サーバを設定します。

関連トピック

SLAAC アドレス割り当て （2 ページ）
ステートフル DHCPv6 アドレス割り当て （3 ページ）

ステートフル DHCP の外部的設定（CLI）

このインターフェイス設定は、外部 DHCP サーバのステートフル DHCPv6 を実装している Cisco IOS IPv6 ルータ用です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	ユニキャスト用に IPv6 を設定します。
ステップ 3	**dns-server 2001:100:0:1::1** 例： `Device (config-dhcpv6)# dns-server 2001:100:0:1::1`	DHCP クライアントに DNS サーバのオプションを提供します。
ステップ 4	**domain-name example.com** 例： `Device (config-dhcpv6)# domain-name example.com`	DHCP クライアントにドメイン名オプションを提供します。
ステップ 5	**exit** 例： `Device (config-dhcpv6)# exit`	前のモードに戻ります。
ステップ 6	**interface vlan1** 例： `Device (config)# interface vlan 1`	インターフェイス モードを開始して、ステートフル DHCP を設定します。
ステップ 7	**description IPv6-DHCP-Stateful** 例： `Device (config-if)# description IPv6-DHCP-Stateful`	ステートフル IPv6 DHCP の説明を入力します。
ステップ 8	**ipv6 address 2001:DB8:0:20::1/64** 例： `Device (config-if)# ipv6 address 2001:DB8:0:20::1/64`	ステートフル IPv6 DHCP の IPv6 アドレスを入力します。

	コマンドまたはアクション	目的
ステップ 9	**ip address 192.168.20.1 255.255.255.0** 例： `Device (config-if)# ip address 192.168.20.1 255.255.255.0`	ステートフル IPv6 DHCP の IPv6 アドレスを入力します。
ステップ 10	**ipv6 nd prefix 2001:db8::/64no-advertise** 例： `Device (config-if)# ipv6 nd prefix 2001:db8::/64 no-advertise`	アドバタイズしてはならない、IPv6 ルーティングプレフィックスアドバタイズメントを設定します。
ステップ 11	**ipv6 nd managed-config-flag** 例： `Device (config-if)# ipv6 nd managed-config-flag`	ホストでアドレス設定に DHCP を使用できるように、IPv6 インターフェイス ネイバー探索を設定します。
ステップ 12	**ipv6 nd other-config-flag** 例： `Device (config-if)# ipv6 nd other-config-flag`	ホストで非アドレス設定に DHCP を使用できるように、IPv6 インターフェイス ネイバー探索を設定します。
ステップ 13	**ipv6 dhcp_relaydestination 2001:DB8:0:20::2** 例： `Device (config-if)# ipv6 dhcp_relay destination 2001:DB8:0:20::2`	インターフェイスに DHCP サーバを設定します。

関連トピック

SLAAC アドレス割り当て （2 ページ）
ステートフル DHCPv6 アドレス割り当て （3 ページ）

IPv6 アドレス ラーニング設定の確認

次に、**show ipv6 dhcp pool** コマンドの出力例を示します。このコマンドは、デバイス上の IPv6 サービス設定を表示します。vlan 21 の設定済みプールの詳細には、プールからアドレスを現在使用している 6 つのクライアントが表示されます。

手順

	コマンドまたはアクション	目的

ステップ 1	**show ipv6 dhcp pool**
	例：
	`Deviceshow ipv6 dhcp pool`
	`DHCPv6 pool: vlan21`
	`Address allocation prefix: 2001:DB8:0:1:FFFF:1234::/64 valid 86400 preferred 86400 (6 in use, 0 conflicts)`
	`DNS server: 2001:100:0:1::1`
	`Domain name: example.com`
	`Active clients: 6`
		デバイス上の IPv6 サービス設定を表示します。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 コマンド リファレンス	『*IPv6 Command Reference (Catalyst 3850 Switches)*』
IP コマンド リファレンス	『*IP Command Reference (Catalyst 3850 Switches)*』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IPv6 クライアント アドレス ラーニングの機能情報

次の表に、このモジュールで説明した機能をリストし、個別の設定情報へのリンクを示します。

機能	リリース	変更内容
IPv6 クライアント アドレス ラーニング機能	Cisco IOS XE 3.2SE	この機能が導入されました。