IPv6 ファーストホップ セキュリティ コンフィギュレーション ガイド

初版：2012 年 11 月 29 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

第 1 章

最初にお読みください

Cisco IOS XE 16 についての重要事項

Cisco IOS XE Release 3.7.0E（Catalyst スイッチ）と Cisco IOS XE Release 3.17S（アクセスおよびエッジ ルーティング）という有効な 2 つのリリースが統合され、スイッチングおよびルーティング ポートフォリオ内のアクセスおよびエッジ製品を幅広く網羅する 1 つの統合リリース バージョン（Cisco IOS XE 16）へと進化しました。

（注） 機能が導入されると、技術構成ガイドの [Feature Information] テーブルで通知されます。その機能に対応している他のプラットフォームについては、通知される場合と通知されない場合があります。特定の機能がプラットフォームでサポートされているかどうかを確認するには、製品のランディングページに表示される技術構成ガイドをご覧ください。製品のランディングページに技術構成ガイドが表示された場合、そのプラットフォームでは機能がサポートされています。

第 2 章

IPv6 RA ガード

IPv6 RA ガード機能は、ネットワーク デバイス プラットフォームに到着した不要または不正なルータ アドバタイズメント（RA）ガード メッセージを、ネットワーク管理者がブロックまたは拒否できるようにするためのサポートを提供します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

IPv6 RA ガードの制限

- IPv6 RA ガード機能は、IPv6 トラフィックがトンネリングされる環境では保護を行いません。

- この機能は、TCAM（Ternary Content Addressable Memory）がプログラムされているハードウェアでのみサポートされています。
- この機能は、入力方向のスイッチ ポート インターフェイスで設定できます。
- この機能は、ホスト モードとルータ モードをサポートしています。
- この機能は、入力方向だけでサポートされます。出力方向ではサポートされません。
- この機能は、EtherChannel および EtherChannel ポート メンバーではサポートされません。
- この機能は、マージ モードのトランク ポートではサポートされません。
- この機能は、補助 VLAN およびプライベート VLAN（PVLAN）でサポートされています。PVLAN の場合、プライマリ VLAN の機能が継承され、ポート機能とマージされます。
- IPv6 RA ガード機能によってドロップされたパケットはスパニングできます。
- **platform ipv6 acl icmp optimize neighbor-discovery** コマンドが設定されている場合、IPv6 RA ガード機能は設定できず、エラー メッセージが表示されます。このコマンドは、RA ガードの ICMP エントリを上書きするデフォルトのグローバル Internet Control Message Protocol（ICMP）エントリを追加します。

IPv6 RA ガードに関する情報

IPv6 グローバル ポリシー

IPv6 グローバル ポリシーは、ストレージおよびアクセス ポリシー データベースのサービスを提供します。IPv6 ND 検査と IPv6 RA ガードは、IPv6 グローバル ポリシー機能です。ND インスペクションまたは RA ガードをグローバルに設定するたびに、ポリシーの属性が、ソフトウェア ポリシー データベースに保存されます。その後ポリシーはインターフェイスに適用され、ポリシーが適用されたこのインターフェイスを含めるためにソフトウェア ポリシー データベース エントリが更新されます。

IPv6 RA ガード

IPv6 RA ガード機能は、ネットワーク デバイス プラットフォームに到着した不要または不正な RA ガード メッセージを、ネットワーク管理者がブロックまたは拒否できるようにするためのサポートを提供します。RA は、リンクで自身をアナウンスするためにデバイスによって使用されます。IPv6 RA ガード機能は、それらの RA を分析して、承認されていないデバイスから送信された RA を除外します。ホスト モードでは、ポート上の RA とルータ リダイレクト メッセージはすべて許可されません。RA ガード機能は、レイヤ 2（L2）デバイスの設定情報を、受信した RA フレームで検出された情報と比較します。L2 デバイスは、RA フレームとルータ リダイレクト フレームの内容を設定と照らし合わせて検証した後で、RA をユニキャストまたはマルチキャストの宛先に転送します。RA フレームの内容が検証されない場合は、RA はドロップされます。

IPv6 RA ガードの設定方法

デバイスでの IPv6 RA ガード ポリシーの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipv6ndraguardpolicy***policy-name*
4. **device-role** {**host** | **router**}
5. **hop-limit** {**maximum** | **minimum** *limit*}
6. **managed-config-flag** {**on** | **off**}
7. **match ipv6 access-list***ipv6-access-list-name*
8. **match ra prefix-list***ipv6-prefix-list-name*
9. **other-config-flag** {**on** | **off**}
10. **router-preference maximum** {**high** | **low** | **medium**}
11. **trusted-port**
12. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 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	**ipv6ndraguardpolicy***policy-name* 例： `Device(config)# ipv6 nd raguard policy policy1`	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 4	**device-role** {**host** | **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	**hop-limit** {**maximum** | **minimum** *limit*} 例： `Device(config-ra-guard)# hop-limit minimum 3`	（任意）アドバタイズされたホップ カウント制限の検証をイネーブルにします。 • 設定されていない場合、このチェックは回避されます。
ステップ 6	**managed-config-flag** {**on** | **off**} 例： `Device(config-ra-guard)# managed-config-flag on`	（任意）アドバタイズされた管理アドレスの設定フラグが on であることの検証をイネーブルにします。 • 設定されていない場合、このチェックは回避されます。
ステップ 7	**match ipv6 access-list***ipv6-access-list-name* 例： `Device(config-ra-guard)# match ipv6 access-list list1`	（任意）検査済みメッセージ内の送信者の IPv6 アドレスが設定された承認デバイス ソース アクセス リストからのものであることの検証をイネーブルにします。 • 設定されていない場合、このチェックは回避されます。
ステップ 8	**match ra prefix-list***ipv6-prefix-list-name* 例： `Device(config-ra-guard)# match ra prefix-list listname1`	（任意）検証済みメッセージ内のアドバタイズされたプレフィックスが設定された承認プレフィックス リストからのものであることの検証をイネーブルにします。 • 設定されていない場合、このチェックは回避されます。
ステップ 9	**other-config-flag** {**on** | **off**} 例： `Device(config-ra-guard)# other-config-flag on`	（任意）アドバタイズされた [Other] 設定パラメータの検証をイネーブルにします。
ステップ 10	**router-preference maximum** {**high** | **low** | **medium**} 例： `Device(config-ra-guard)# router-preference maximum high`	（任意）アドバタイズされたデフォルト ルータの設定パラメータの値が指定された制限値以下であることの検証をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 11	**trusted-port** 例： `Device(config-ra-guard)# trusted-port`	（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。 • すべての RA ガード ポリシングが無効になります。
ステップ 12	**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。

インターフェイスの IPv6 RA ガードの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipv6ndraguardattach-policy** [*policy-name* [**vlan** {**add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1,vlan2,vlan3...*]]]
5. **exit**
6. **showipv6ndraguardpolicy** [*policy-name*]
7. **debugipv6snoopingraguard** [*filter* | *interface* | *vlanid*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 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。

	コマンドまたはアクション	目的
ステップ 3	**interface***typenumber* 例： `Device(config)# interface fastethernet 3/13`	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。
ステップ 4	**ipv6ndraguardattach-policy** [*policy-name* [**vlan** {**add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1,vlan2,vlan3...*]]] 例： `Device(config-if)# ipv6 nd raguard attach-policy`	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 5	**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 6	**showipv6ndraguardpolicy** [*policy-name*] 例： `Device# show ipv6 nd raguard policy raguard1`	RA ガードを使用して設定されているすべてのインターフェイスで RA ガード ポリシーを表示します。
ステップ 7	**debugipv6snoopingraguard** [*filter* | *interface* | *vlanid*] 例： `Device# debug ipv6 snooping raguard`	IPv6 RA ガード スヌーピング情報のデバッグをイネーブルにします。

IPv6 RA ガードの設定例

例：IPv6 RA ガードの設定

```
Device(config)# interface fastethernet 3/13

Device(config-if)# ipv6 nd raguard attach-policy


Device# show running-config interface fastethernet 3/13

Building configuration...
Current configuration : 129 bytes
```

```
!
interface FastEthernet3/13
 switchport
 switchport access vlan 222
 switchport mode access
 access-group mode prefer port
 ipv6 nd raguard
end
```

例：IPv6 ND インスペクションおよび RA ガードの設定

この例は、ネイバー探索インスペクションおよびRAガード機能の両方が設定されているインターフェイスに関する情報を示しています。

```
Device# show ipv6 snooping capture-policy interface ethernet 0/0

Hardware policy registered on Ethernet 0/0
Protocol      Protocol value   Message   Value     Action     Feature
ICMP          58               RS        85        punt       RA Guard
                                                   punt       ND Inspection
ICMP          58               RA        86        drop       RA guard
                                                   punt       ND Inspection
ICMP          58               NS        87        punt       ND Inspection
ICM           58               NA        88        punt       ND Inspection
ICMP          58               REDIR     89        drop       RA Guard
                                                   punt       ND Inspection
```

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 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準規格および RFC

規格/RFC	タイトル
IPv6 に関する RFC	*IPv6 の RFC*

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	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	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする場合、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 RA ガードの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1*：*IPv6 RA* ガードの機能情報

機能名	リリース	機能情報
IPv6 RA ガード	12.2(33)SXI4 12.2(50)SY 12.2(54)SG 15.0(2)SE 15.0(2)SG Cisco IOS XE Release 3.8S Cisco IOS XE Release 3.2SE Cisco IOS XE Release 3.2SG	IPv6 RA ガード機能は、ネットワーク デバイス プラットフォームに到着した不要または不正なルータ アドバタイズメント（RA）ガード メッセージを、ネットワーク管理者がブロックまたは拒否できるようにするためのサポートを提供します。 導入または変更されたコマンドは次のとおりです。**debug ipv6 snooping raguard**、**device-role**、**hop-limit**、**ipv6 nd raguard attach-policy**、**ipv6 nd raguard policy**、**managed-config-flag**、**match ipv6 access-list**、**match ra prefix-list**、**other-config-flag**、**router-preference maximum**、**show ipv6 nd raguard policy**。

第 3 章

IPv6 スヌーピング

IPv6 スヌーピング機能は、複数のレイヤ 2 IPv6 ファーストホップ セキュリティ機能（IPv6 ネイバー探索インスペクション、IPv6 デバイス トラッキング、IPv6 アドレス収集、および IPv6 バインディングテーブルのリカバリを含む）をバンドルして、セキュリティと拡張性を提供します。IPv6 ND インスペクションは、レイヤ 2（またはレイヤ 2 とレイヤ 3 の間）で動作し、IPv6 の機能にセキュリティと拡張性を提供します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

IPv6 スヌーピングの制限

IPv6 スヌーピング機能は、EtherChannel ポートではサポートされません。

IPv6 スヌーピングに関する情報

IPv6 スヌーピング

IPv6 スヌーピング機能によって、複数のレイヤ 2 IPv6 ファーストホップ セキュリティ機能（IPv6 アドレス収集と IPv6 デバイス トラッキングを含む）がバンドルされます。この機能は、レイヤ 2（またはレイヤ 2 とレイヤ 3 の間）で動作し、IPv6 の機能にセキュリティと拡張性を提供します。この機能によって、Duplicate Address Detection（DAD）、アドレス解決、デバイス検出やネイバー キャッシュに対する攻撃といった、ネイバー探索メカニズムに固有のいくつかの脆弱性が軽減されます。

IPv6 スヌーピングは、レイヤ 2 ネイバー テーブルのステートレス自動設定アドレスのバインディングを学習して保護し、信頼できるバインディング テーブルを構築するために ND メッセージを分析します。有効なバインディングのない IPv6 ND メッセージはドロップされます。ND メッセージは、その IPv6 から MAC へのマッピングが検証可能な場合に信頼できると見なされます。

ターゲット（プラットフォームのターゲット サポートによって異なり、デバイス ポート、スイッチ ポート、レイヤ 2 インターフェイス、レイヤ 3 インターフェイス、および VLAN が含まれることがある）に IPv6 スヌーピングが設定されている場合、IPv6 トラフィックの ND プロトコルと Dynamic Host Configuration Protocol（DHCP）をルーティング デバイスのスイッチ統合セキュリティ機能（SISF）インフラストラクチャにリダイレクトするためのキャプチャ命令がハードウェアにダウンロードされます。ND トラフィックの場合、NS、NA、RS、RA、REDIRECT などのメッセージが SISF にリダイレクトされます。DHCP の場合、ポート 546 または 547 から送信された UDP メッセージがリダイレクトされます。

IPv6 スヌーピングはその「キャプチャ ルール」を分類子に登録します。分類子では、特定のターゲットにあるすべての機能のルールがすべて集約され、対応する ACL がプラットフォーム依存モジュールにインストールされます。分類子は、リダイレクトされたトラフィックを受信すると、（トラフィックを受信しているターゲットに対して）登録されているすべての機能からすべてのエントリ ポイント（IPv6 スヌーピングのエントリ ポイントを含む）を呼び出します。IPv6 スヌーピングのエントリ ポイントは最後に呼び出されるため、他の機能によって行われた決定が IPv6 スヌーピングの決定よりも優先されます。

IPv6 デバイス トラッキング

IPv6 デバイス トラッキングは、IPv6 ホストが非表示になったときにネイバー テーブルを即時に更新できるように、IPv6 ホストの活性トラッキングを提供します。

IPv6 ファーストホップ セキュリティ バインディング テーブル

IPv6 ファーストホップ セキュリティ バインディング テーブルのリカバリ メカニズム機能を使用すると、デバイスのリブート時にバインディング テーブルをリカバリできます。デバイスに接続されている IPv6 ネイバーのデータベース テーブルは、ND スヌーピングなどの情報源から作成されます。このデータベース（またはバインディング）テーブルは、スプーフィングやリダイレクト攻撃を防止するために、リンク層アドレス（LLA）、IPv4 または IPv6 アドレス、およびネイバーのプレフィックス バインディングを検証するためにさまざまな IPv6 ガード機能によって使用されます。

このメカニズムにより、デバイスのリブート時にバインディング テーブルをリカバリできます。リカバリ メカニズムは、不明な送信元、（バインディング テーブルにまだ指定されていない送信元や、ND または DHCP グリーニングを使用して学習されていない送信元）からのデータ トラフィックをブロックします。この機能は、宛先ガードで宛先アドレスの解決に失敗したときに、不足しているバインディング テーブルのエントリをリカバリします。障害が発生すると、バインディング テーブルのエントリは、設定に応じて、DHCP サーバまたは宛先ホストにクエリを実行することでリカバリできます。

リカバリ プロトコルとプレフィックス リスト

IPv6 ファーストホップ セキュリティ バインディング テーブルのリカバリ メカニズム機能は、DHCP と NDP の両方でリカバリを試みる前に、一致するプレフィックス リストを提供する機能を導入します。

アドレスがプロトコルと関連付けられているプレフィックス リストと一致しない場合、そのプロトコルではバインディング テーブル エントリのリカバリは試行されません。プレフィックス リストは、プロトコルを使用してレイヤ 2 ドメインに割り当てられているアドレスに対して有効なプレフィックスに対応している必要があります。デフォルトではプレフィックス リストは存在せず、すべてのアドレスのリカバリが試行されます。プロトコルにプレフィックス リストを関連付けるコマンドは、**protocol** {**dhcp** | **ndp**} [**prefix-list***prefix-list-name*] です。

IPv6 デバイス トラッキング

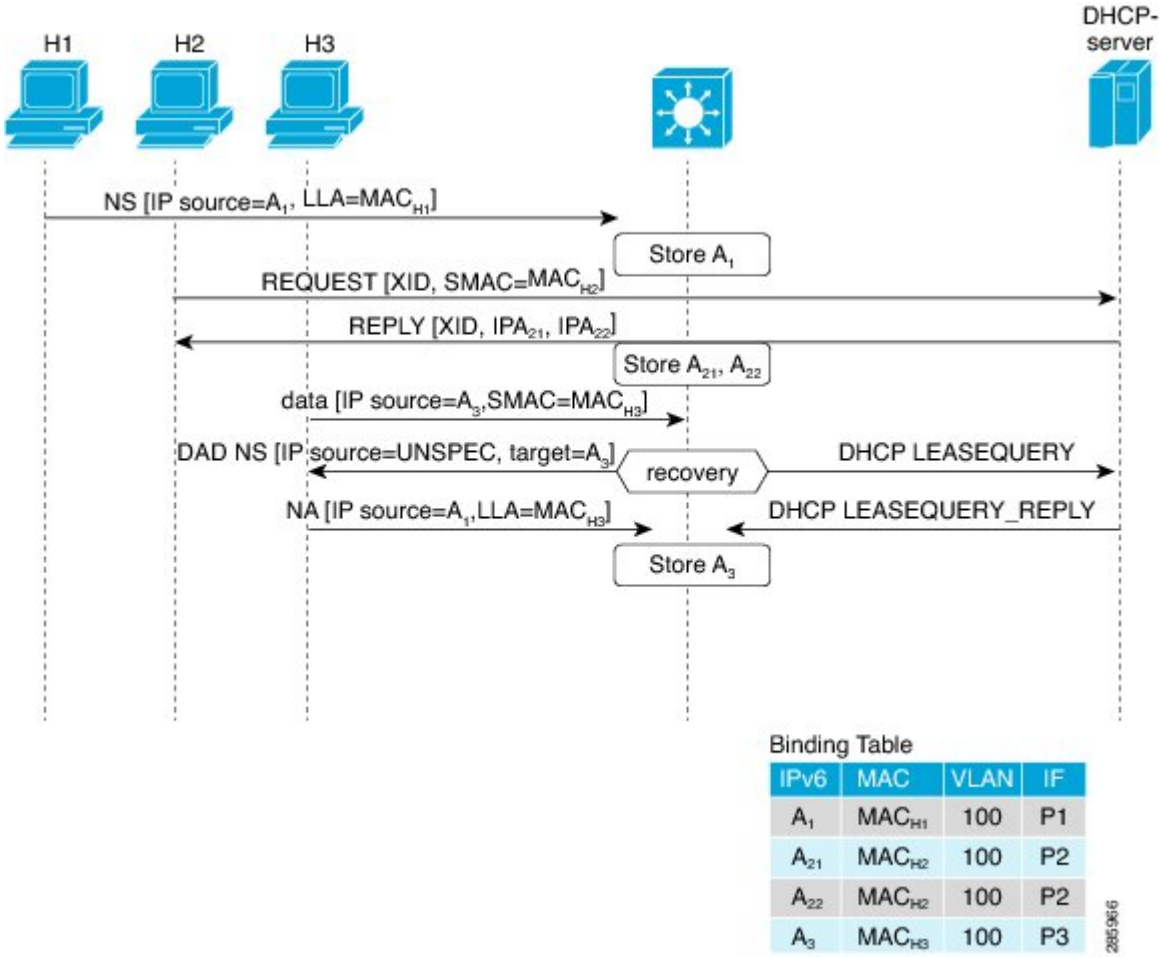
IPv6 デバイス トラッキングは、IPv6 ホストが非表示になったときにネイバー テーブルを即時に更新できるように、IPv6 ホストの活性トラッキングを提供します。

IPv6 アドレス収集

IPv6 アドレス収集は、正確なバインディング テーブルに依存するその他多くの IPv6 の機能の基盤です。この機能は、アドレス収集のためにリンク上の ND および DHCP メッセージを検査した後に、それらのアドレスをバインディング テーブルに入力します。また、この機能は、アドレスの所有権を強制し、特定のノードが要求可能なアドレスの数を制限します。

次の図は、IPv6 アドレス収集の仕組みを示しています。

図 *1*：*IPv6* アドレス収集



IPv6 スヌーピングの設定方法

インターフェイスの IPv6 スヌーピングの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipv6 snooping policy** *snooping-policy*
4. **exit**
5. **interface** *type number*
6. **ipv6snooping attach-policy***snooping-policy*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 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	**ipv6 snooping policy** *snooping-policy* 例： `Device(config)# ipv6 snooping policy policy1`	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 4	**exit** 例： `Device(config-ipv6-snooping)# exit`	IPv6 スヌーピング コンフィギュレーション モードを終了します。
ステップ 5	**interface** *type number* 例： `Device(config)# interface Gigabitethernet 0/0/1`	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。

	コマンドまたはアクション	目的
ステップ 6	**ipv6snooping attach-policy***snooping-policy* 例： `Device(config-if)# ipv6 snooping attach-policy policy1`	インターフェイスに IPv6 スヌーピング ポリシーを対応付けます。

IPv6 ND インスペクションの確認とトラブルシューティング

手順の概要

1. イネーブル化
2. **showipv6snoopingcapture-policy** [**interface***typenumber*]
3. **showipv6snoopingcounter** [**interface***typenumber*]
4. **showipv6snoopingfeatures**
5. **showipv6snoopingpolicies**[**interface***typenumber*]
6. **debugipv6snooping**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 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	**showipv6snoopingcapture-policy** [**interface***typenumber*] 例： `Device# show ipv6 snooping capture-policy interface ethernet 0/0`	スヌーピング ND メッセージ キャプチャ ポリシーを表示します。
ステップ 3	**showipv6snoopingcounter** [**interface***typenumber*] 例： `Device# show ipv6 snooping counter interface FastEthernet 4/12`	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します。

	コマンドまたはアクション	目的
ステップ 4	**showipv6snoopingfeatures** 例： `Device# show ipv6 snooping features`	デバイス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します。
ステップ 5	**showipv6snoopingpolicies**[**interface***typenumber*] 例： `Device# show ipv6 snooping policies`	設定されているポリシーと、ポリシーが接続されているインターフェイスに関する情報を表示します。
ステップ 6	**debugipv6snooping** 例： `Device# debug ipv6 snooping`	IPv6 でスヌーピング情報のデバッグをイネーブルにします。

IPv6 デバイス トラッキングの設定

IPv6 ファーストホップ セキュリティ バインディング テーブルの内容の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipv6neighborbinding** {*ipv6-address* | *ipv6-prefix*} **interface***typenumber* [*hardware-address* | *mac-address*][**tracking** [**disable** | **enable** | **retry-interval***value*] | **reachable-lifetime***value*]
4. **ipv6neighborbindingmax-entries***entries*
5. **ipv6neighborbindinglogging**
6. **exit**
7. **showipv6neighborbinding**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Device> enable`	• 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	**ipv6neighborbinding** {*ipv6-address* | *ipv6-prefix*} **interface***typenumber* [*hardware-address* | *mac-address*][**tracking** [**disable** | **enable** | **retry-interval***value*] | **reachable-lifetime***value*] 例： `Device(config)# ipv6 neighbor binding 2001:DB8:0:ABCD::1 interface GigabitEthernet 0/0/1 reachable-lifetime 100`	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。
ステップ 4	**ipv6neighborbindingmax-entries***entries* 例： `Device(config)# ipv6 neighbor binding max-entries 100`	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。
ステップ 5	**ipv6neighborbindinglogging** 例： `Device(config)# ipv6 neighbor binding logging`	バインディング テーブル メイン イベントのロギングをイネーブルにします。
ステップ 6	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 7	**showipv6neighborbinding** 例： `Device# show ipv6 neighbor binding`	バインディング テーブルの内容を表示します。

IPv6 ファーストホップ セキュリティ バインディング テーブルのリカバリ メカニズムの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipv6 neighbor binding***ipv6-address***interface***type number*
4. **ipv6 prefix-list***list-name***permit***ipv6-prefix/prefix-length***ge***ge-value*
5. **ipv6 snooping policy***snooping-policy-id*
6. **destination-glean** {**recovery** | **log-only**} [**dhcp**]
7. **data-glean** {**recovery** | **log-only**} [**ndp** | **dhcp**]
8. **prefix-glean**
9. **protocol dhcp** [**prefix-list***prefix-list-name*]
10. **exit**
11. **ipv6 destination-guard policy***policy-name*
12. **enforcement** {**always** | **stressed**}
13. **exit**
14. **interface** *type number*
15. **ipv6snooping attach-policy***snooping-policy*
16. **ipv6 destination-guard attach-policy***policy-name*
17. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 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	**ipv6 neighbor binding***ipv6-address***interface***type number* 例： `Device(config)# ipv6 neighbor binding 2001:db8::1 interface Gigabitethernet3/0/1`	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。

	コマンドまたはアクション	目的
ステップ 4	**ipv6 prefix-list***list-name***permit***ipv6-prefix/prefix-length***ge***ge-value* 例： `Device(config)# ipv6 prefix-list abc permit 2001:DB8::/64 ge 128`	IPv6 プレフィックス リストのエントリを作成します。
ステップ 5	**ipv6 snooping policy***snooping-policy-id* 例： `Device(config)# ipv6 snooping policy xyz`	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、指定されたスヌーピング ポリシーの設定を変更できるようします。
ステップ 6	**destination-glean** {**recovery** | **log-only**} [**dhcp**] 例： `Device(config-ipv6-snooping)# destination-glean recovery dhcp`	宛先アドレスは DHCP からリカバリする必要があることを指定します。 （注） ロギング（リカバリなし）が必要な場合は、**destination-glean log-only** コマンドを使用します。
ステップ 7	**data-glean** {**recovery** | **log-only**} [**ndp** | **dhcp**] 例： `Device(config-ipv6-snooping)# data-glean recovery ndp`	ソース（または「データ」）アドレス グリーニングを使用して、IPv6 ファーストホップ セキュリティ バインディング テーブルのリカバリをイネーブルにします。 （注） ロギング（リカバリなし）が必要な場合は、**data-glean log-only** コマンドを使用します。
ステップ 8	**prefix-glean** 例： `Device(config-ipv6-snooping)# prefix-glean`	デバイスが IPv6 ルータ アドバタイズメント（RA）または Dynamic Host Configuration Protocol（DHCP）からプレフィックスを収集できるようにします。
ステップ 9	**protocol dhcp** [**prefix-list***prefix-list-name*] 例： `Device(config-ipv6-snooping)# protocol dhcp prefix-list abc`	（任意）アドレスを DHCP で収集し、プロトコルを特定の IPv6 プレフィックス リストと関連付ける必要があることを指定します。
ステップ 10	**exit** 例： `Device(config-ipv6-snooping)# exit`	IPv6 スヌーピング 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 モードに戻ります。

	コマンドまたはアクション	目的
ステップ 11	**ipv6 destination-guard policy***policy-name* 例： `Device(config)# ipv6 destination-guard policy xyz`	（任意）宛先ガード コンフィギュレーション モードを開始し、指定した宛先ガードポリシーの設定を変更できるようにします。
ステップ 12	**enforcement** {**always** | **stressed**} 例： `Device(config-destguard)# enforcement stressed`	ポリシーの強制レベルを、すべての条件下で強制するか、システムに負荷がかかっている場合のみ強制するか設定します。
ステップ 13	**exit** 例： `Device(config-destguard)# exit`	宛先ガード 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 モードに戻ります。
ステップ 14	**interface** *type number* 例： `Device(config)# interface Gigabitethernet 0/0/1`	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 15	**ipv6snooping attach-policy***snooping-policy* 例： `Device(config-if)# ipv6 snooping attach-policy xyz`	インターフェイスに IPv6 スヌーピング ポリシーを対応付けます。
ステップ 16	**ipv6 destination-guard attach-policy***policy-name* 例： `Device(config-if)# ipv6 destination-guard attach-policy xyz`	指定したインターフェイスに宛先ガード ポリシーを対応付けます。 （注） IPv6宛先ガードポリシーの設定方法の詳細については、「IPv6宛先ガード」を参照してください。
ステップ 17	**end** 例： `Device(config-if)# end`	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、特権 EXEC モードに戻ります。

アドレス収集の設定およびリカバリプロトコルとプレフィックスリストの関連付け

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipv6 snooping policy***snooping-policy-id*
4. **protocol** {**dhcp** | **ndp**} [**prefix-list***prefix-list-name*]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 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	**ipv6 snooping policy***snooping-policy-id* 例： `Device(config)# ipv6 snooping policy 200`	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、指定されたスヌーピング ポリシーの設定を変更できるようします。
ステップ 4	**protocol** {**dhcp** | **ndp**} [**prefix-list***prefix-list-name*] 例： `Device(config-ipv6-snooping)# protocol dhcp prefix-list dhcp_prefix_list`	Dynamic Host Configuration Protocol（DHCP）で収集される必要があるアドレスを指定し、リカバリ プロトコル（DHCP）とプレフィックス リストを関連付けます。
ステップ 5	**end** 例： `Device(config-ipv6-snooping)# end`	IPv6 スヌーピング コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPv6 デバイス トラッキングの設定

IPv6 デバイス トラッキング機能のバインディング テーブルでエントリのライフ サイクルを細かく調整するには、次の作業を実行します。IPv6 デバイス トラッキ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。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipv6neighbortracking** [**retry-interval***value*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 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	**ipv6neighbortracking** [**retry-interval***value*] 例： `Device(config)# 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 プレフィックス収集の設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipv6 snooping policy** *snooping-policy*
4. **prefix-glean** [**only**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 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	**ipv6 snooping policy** *snooping-policy* 例： `Device(config)# ipv6 snooping policy policy1`	IPv6 スヌーピング ポリシーを設定し、IPv6 スヌーピング 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 4	**prefix-glean** [**only**] 例： `Device(config-ipv6-snooping)# prefix-glean`	デバイスが IPv6 RA または DHCPv6 トラフィックからプレフィックスを収集できるようにします。

IPv6 スヌーピングの設定例

例：インターフェイスの IPv6 ND インスペクションの設定

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# exit
Device(config)# interface Gigabitethernet 0/0/1
Device(config-if)# ipv6 snooping attach-policy policy1
.
.
.
Device# show ipv6 snooping policies interface gigabitethernet 0/0/1
Target               Type  Policy               Feature        Target range
Gi0/0/1              PORT  my_policy            Destination Gu vlan all
Gi0/0/1              PORT  policy1              Snooping       vlan all
```

例：IPv6 バインディング テーブルの内容の設定

```
Device(config)# ipv6 neighbor binding 2001:DB8:0:ABCD::1 interface GigabitEthernet 0/0/1
reachable-lifetime 100
```

```
Device(config)# ipv6 neighbor binding max-entries 100
Device(config)# ipv6 neighbor binding logging
Device(config)# exit
```

例：IPv6 ファーストホップ セキュリティ バインディング テーブルのリカバリの設定

```
Device> enable
Device# configure terminal
Device(config)# ipv6 neighbor binding 2001:db8::1 interface Gigabitethernet3/0/1
Device(config)# ipv6 prefix-list abc permit 2001:DB8::/64 ge 128
Device(config)# ipv6 snooping policy xyz
Device(config-ipv6-snooping)# destination-glean recovery dhcp
Device(config-ipv6-snooping)# data-glean recovery ndp
Device(config-ipv6-snooping)# prefix-glean
Device(config-ipv6-snooping)# protocol dhcp prefix-list abc
Device(config-ipv6-snooping)# exit
Device(config)# ipv6 destination-guard policy xyz
Device(config-destguard)# enforcement stressed
Device(config-destguard)# exit
Device(config)# interface Gigabitethernet 0/0/1
Device(config-if)# ipv6 snooping attach-policy xyz
Device(config-if)# ipv6 destination-guard attach-policy xyz
Device(config-if)# end
```

例：アドレス収集の設定およびリカバリプロトコルとプレフィックス リストの関連付け

次の例は、NDP がすべてのアドレスのリカバリに使用され、DHCP が dhcp_prefix_list という名前のプレフィックス リストと一致するアドレスのリカバリに使用されることを示しています。

```
Device(config-ipv6-snooping)# protocol ndp
Device(config-ipv6-snooping)# protocol dhcp prefix-list dhcp_prefix_list
```

IPv6 ソース ガードとプレフィックス ガードのその他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
IPv4 アドレス指定	『*IP Addressing: IPv4 Addressing Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準規格および RFC

規格/RFC	タイトル
IPv6 に関する RFC	*IPv6 の RFC*

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする場合、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 スヌーピングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *2*：*IPv6* スヌーピングの機能情報

機能名	リリース	機能情報
IPv6 スヌーピング	12.2(50)SY 15.0(1)SY 15.0(2)SE 15.1(2)SG 15.3(1)S Cisco IOS XE Release 3.2SE Cisco IOS XE Release 3.8S Cisco IOS Release 15.2(1)E	IPv6 スヌーピングは、複数のレイヤ 2 IPv6 ファーストホップセキュリティ機能（IPv6 ND インスペクション、IPv6 デバイストラッキング、IPv6 アドレス収集、および IPv6 ファーストホップ セキュリティ バインディング テーブルのリカバリを含む）をバンドルして、セキュリティと拡張性を提供します。IPv6 スヌーピングは、レイヤ 2（またはレイヤ 2 とレイヤ 3 の間）で動作し、IPv6 の機能にセキュリティと拡張性を提供します。 導入または変更されたコマンドは次のとおりです。 **data-glean**、**debug ipv6 snooping**、**destination-glean**、**device-role**、**drop-unsecure**、**ipv6 nd inspection**、**ipv6 nd inspection policy**、**ipv6 neighbor binding logging**、**ipv6 neighbor binding max-entries**、**ipv6 neighbor binding vlan**、**ipv6 neighbor tracking**、**ipv6 snooping attach-policy**、**ipv6 snooping policy**、**prefix-glean**、**protocol (IPv6)**、**sec-level minimum**、**show ipv6 neighbor binding**、**show ipv6 snooping capture-policy**、**show ipv6 snooping counters**、**show ipv6 snooping features**、**show ipv6 snooping policies**、**tracking**、**trusted-port**。

第 4 章

IPv6 DAD プロキシ

IPv6 Duplicate Address Detection（DAD）プロキシ機能は、クエリされたアドレスを所有するノードに代わって DAD クエリに応答します。この機能は、ノードがリンク上で直接通信できない環境で役立ちます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

IPv6 DAD プロキシの制限

- IPv6 Duplicate Address Detection（DAD）機能は、EtherChannel ポートではサポートされません。

IPv6 DAD プロキシに関する情報

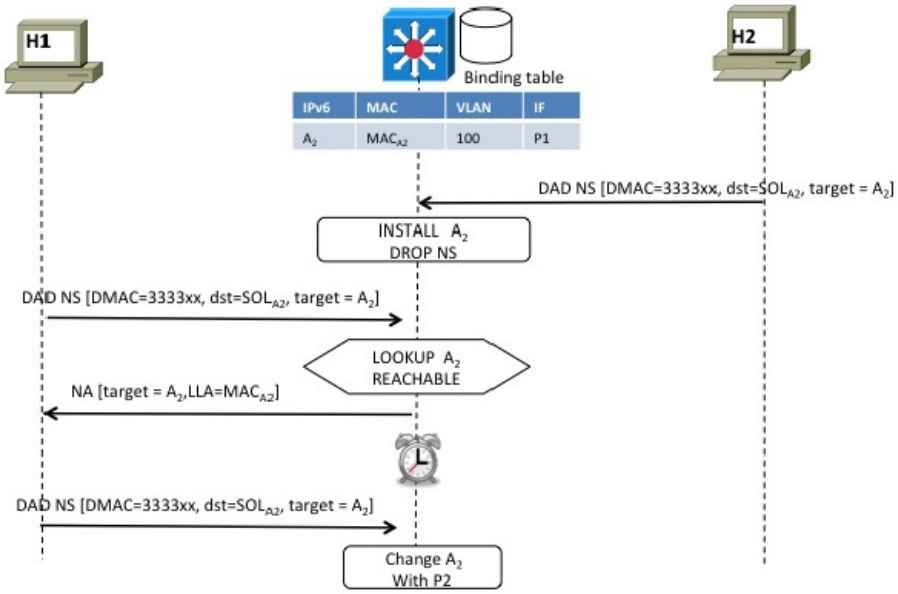
IPv6 DAD プロキシの概要

IPv6 Duplicate Address Detection（DAD）機能は、特定のセグメントに割り当てられるすべての IP アドレスを一意なアドレスにします。このプロセスは、ホストが直接通信できず、プロキシが必要な場合に IPv6 ホスト同士が互いに直接通信するときに動作します。

ホストはそのアドレスが一意であることを確認すると、DAD 手順を有効にします。ただし、2 台のホストが互いに通信ができない場合、この手順では重複アドレスを検出できません。DAD 手順を実行できない場合、両方のホストが同じリンクローカルアドレスを割り当てるため、どちらのホストも Dynamic Host Configuration Protocol バージョン 6（DHCPv6）サーバに接続を試みると失敗します。IPv6 DAD プロキシ機能は、アドレスが使用中の場合、そのアドレスの所有者に代わって応答します。

次の図は、IPv6 DAD プロキシ機能の概要を示しています。

図 *2*：*IPv6 DAD* プロキシ



IPv6 DAD プロキシの設定方法

IPv6 DAD プロキシの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***type number*
4. **[no] ipv6 nd dad-proxy**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 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	**interface***type number* 例： `Device(config)# interface GigabitEthernet 0/0/1`	インターフェイスのタイプおよび番号を指定し、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 4	**[no] ipv6 nd dad-proxy** 例： `Device(config-if)# ipv6 nd dad-proxy`	ND 抑制を DAD プロキシ モードで動作させる必要があるかどうか指定します。 このモードでは、DAD メッセージは転送されません。メッセージは既存のエントリに応答したり、バインディングテーブルに追加されたりします。
ステップ 5	**end** 例： `Device(config-if)# end`	ルータ 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、特権 EXEC モードに戻ります。

IPv6 DAD プロキシの設定例

例：IPv6 DAD プロキシの設定

```
Device> enable
Device# configure terminal
Device(config)# interface Ethernet 0/0
Device(config-if)# ipv6 nd dad-proxy
Device(config-if)# end
```

IPv6 DAD プロキシのその他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

MIB

MIB	MIB のリンク
	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	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする場合、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 DAD プロキシの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *3* : ***IPv6 DAD*** プロキシの機能情報

機能名	リリース	機能情報
IPv6 DAD プロキシ	Cisco IOS XE Release 3.8S Cisco IOS XE Release 3SE Cisco IOS XE Release 3.9S	IPv6 Duplicate Address Detection（DAD）プロキシ機能は、クエリされたアドレスを所有するノードに代わって DAD クエリに応答します。この機能は、ノードがリンク上で直接通信できない環境で役立ちます。 導入または変更されたコマンドは次のとおりです。**ipv6 nd dad-proxy**、**mode dad-proxy**、**mode md-proxy**。

第 5 章

IPv6 ネイバー探索マルチキャスト抑制

IPv6 ネイバー探索（ND）マルチキャスト抑制機能は、ND マルチキャスト ネイバー送信要求（NS）メッセージをドロップする（およびターゲットに代わって送信要求に応答する）か、またはユニキャスト トラフィックに変換することでメッセージを抑制します。マルチキャスト トラフィックからユニキャスト トラフィックへの変換は、レイヤ 2 マルチキャスト宛先 MAC をレイヤ 2 ユニキャスト宛先 MAC で置き換えることで行われます。変換するには、リンク上のアドレスと各アドレスのレイヤ2へのバインディングを把握している必要があります。抑制されたマルチキャスト メッセージは、ネイバー送信要求（NS）メッセージです。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

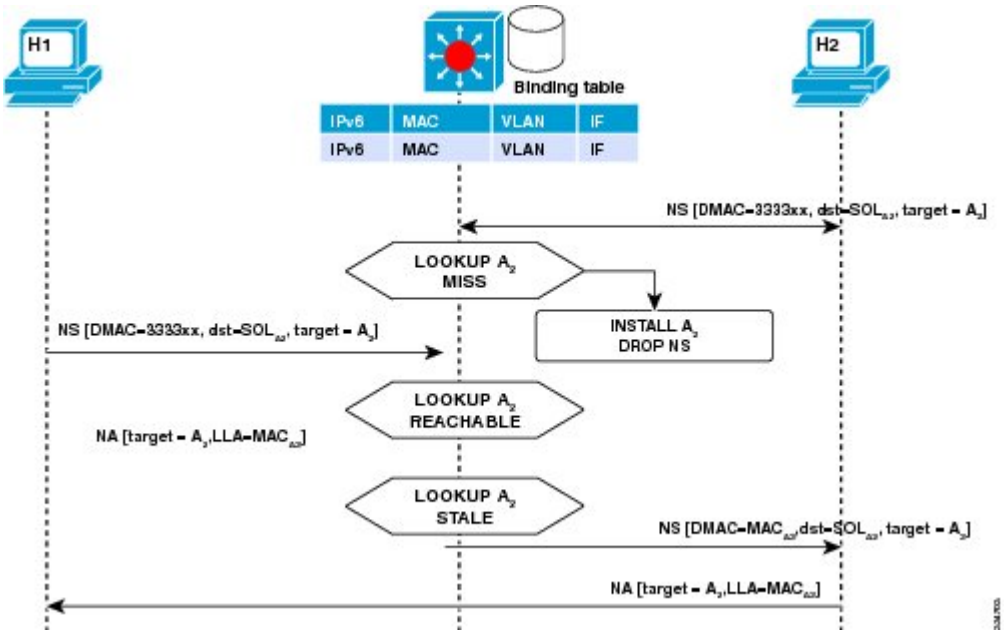
IPv6 ネイバー探索マルチキャスト抑制に関する情報

IPv6 ネイバー探索マルチキャスト抑制の概要

IPv6 ネイバー探索（ND）マルチキャスト抑制機能では、ND マルチキャスト ネイバー送信要求（NS）メッセージを、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）か、またはユニキャスト トラフィックに変換することで停止します。この機能は、適切なリンク運用に必要な制御トラフィックの量を削減します。

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、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。

次の図は、この機能の概要を示しています。



IPv6 ネイバー探索マルチキャスト抑制の設定方法

インターフェイスの IPv6 ネイバー探索マルチキャスト抑制の設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **ipv6 nd suppress policy***policy-name*
4. **[no] mode mc-proxy**
5. **[no] mode full-proxy**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 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	**configure terminal** 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***policy-name*
	
	例：
	`Device (config)# ipv6 nd suppress policy policy1`
	`Device (config-nd-suppress)#`
		設定するネイバー探索（ND）抑制ポリシーの名前を指定します。

ステップ 4	**[no] mode mc-proxy** 例： `Device (config-nd-suppress)# mode mc-proxy`	ND 抑制ですべてのマルチキャスト ネイバー送信要求（NS）メッセージをプロキシする必要があるかどうか指定します。

	コマンドまたはアクション	目的
ステップ 5	**[no] mode full-proxy** 例： `Device (config-nd-suppress)# mode full-proxy`	ND 抑制でユニキャストとマルチキャストの両方の NS メッセージをプロキシする必要があるかどうか指定します。
ステップ 6	**end** 例： `Device (config-nd-suppress)# end`	ND 抑制モードを終了し、特権 EXEC モードに戻ります。

IPv6 ネイバー探索マルチキャスト抑制の設定例

例：インターフェイスの IPv6 ネイバー探索抑制の設定

```
Device> enable
Device(config)# interface Ethernet 0/0
Device(config-if)# ipv6 nd suppress attach-policy policy1
```

IPv6 ネイバー探索マルチキャスト抑制のその他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

MIB

MIB	MIB のリンク
	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	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする場合、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 ネイバー探索マルチキャスト抑制の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *4* : ***IPv6*** ネイバー探索マルチキャスト抑制の機能情報

機能名	リリース	機能情報
IPv6 ネイバー探索マルチキャスト抑制と DAD プロキシ	Cisco IOS XE Release 3.8S Cisco IOS XE Release 3SE Cisco IOS XE Release 3.9S	IPv6 Duplicate Address Detection（DAD）プロキシ機能は、クエリされたアドレスを所有するノードに代わって DAD クエリに応答します。この機能は、ノードがリンク上で直接通信できない環境で役立ちます。 導入または変更されたコマンドは次のとおりです。**ipv6 nd dad-proxy**、**mode dad-proxy**、**mode md-proxy**。

第 6 章

DHCP—DHCPv6 ガード

このモジュールでは、Dynamic Host Configuration Protocol バージョン 6（DHCPv6）ガード機能について説明します。この機能は、サーバからクライアントにDHCPパケットを転送する、承認されていない DHCP サーバとリレー エージェントから発信される DHCP 応答やアドバタイズメント メッセージをブロックします。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るクライアント メッセージはブロックされません。フィルタリングの判断は、受信側のスイッチ ポート、トランク、または VLAN に割り当てられているデバイスのロールによって決まります。また、より細かいレベルのフィルタ精度を提供するために、送信元サーバやリレーエージェントのアドレスに基づいて、または応答メッセージに記載されているプレフィックスやアドレスの範囲によってメッセージをフィルタリングできます。この機能により、トラフィック リダイレクションやサービス妨害（DoS）を防ぐことができます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

DHCPv6 ガードの制限

- DHCPv6 ガード機能は、EtherChannel ポートではサポートされません。

DHCPv6 ガードに関する情報

DHCPv6 ガードの概要

DHCPv6 ガード機能は、承認されていない DHCP サーバおよびリレー 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します。

パケットは 3 つの DHCP メッセージ タイプのいずれかに分類されます。すべてのクライアント メッセージは、デバイスのロールに関係なく、常にスイッチングされます。DHCP サーバのメッセージは、デバイスのロールがサーバに設定されている場合のみさらに処理されます。DHCP サーバのアドバタイズメント（送信元の検証とサーバの設定の場合）および DHCP サーバの応答（許可されたプレフィックスの場合）を含むサーバ メッセージはさらに処理されます。

デバイスが DHCP サーバとして設定されている場合、デバイスのロールの設定に関係なく、すべてのメッセージをスイッチングする必要があります。

DHCPv6 ガードの設定方法

DHCP—DHCPv6 ガードの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipv6access-list***access-list-name*
4. **permithost***address***any**
5. **exit**
6. **ipv6prefix-list***list-name***permit***ipv6-prefix***128**
7. **ipv6dhcpguardpolicy***policy-name*
8. **device-role** {**client** | **server**}
9. **matchserveraccess-list***ipv6-access-list-name*
10. **matchreplyprefix-list***ipv6-prefix-list-name*
11. **preferencemin***limit*
12. **preferencemax***limit*
13. **trusted-port**
14. **exit**
15. **interface***typenumber*
16. **switchport**
17. **exit**
18. **exit**
19. **showipv6dhcpguardpolicy** [*policy-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 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。

	コマンドまたはアクション	目的
ステップ 3	**ipv6access-list***access-list-name* 例： `Device(config)# ipv6 access-list acl1`	IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ステップ 4	**permithost***address***any** 例： `Device(config-ipv6-acl)# permit host FE80::A8BB:CCFF:FE01:F700 any`	名前付き IP アクセス リストに条件を設定します。
ステップ 5	**exit** 例： `Device(config-ipv6-acl)# exit`	IPv6アクセス リスト 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。
ステップ 6	**ipv6prefix-list***list-name***permit***ipv6-prefix***128** 例： `Device(config)# ipv6 prefix-list abc permit 2001:0DB8::/64 le 128`	IPv6 プレフィックス リストのエントリを作成します。
ステップ 7	**ipv6dhcpguardpolicy***policy-name* 例： `Device(config)# ipv6 dhcp guard policy pol1`	DHCPv6 ガード ポリシー名を定義して、DHCP ガード コンフィギュレーション モードを開始します。
ステップ 8	**device-role** {**client** | **server**} 例： `Device(config-dhcp-guard)# device-role server`	ターゲット（インターフェイスまたは VLAN）に接続されているデバイスのデバイス ロールを指定します。
ステップ 9	**matchserveraccess-list***ipv6-access-list-name* 例： `Device(config-dhcp-guard)# match server access-list acl1`	（任意）検査済みメッセージ内のアドバタイズされた DHCPサーバおよびリレーアドレスが設定された承認サーバ アクセス リストからのものであることの検証をイネーブルにします。設定されていない場合、このチェックは回避されます。空のアクセス リストは、permit として処理されます。

	コマンドまたはアクション	目的
ステップ 10	**matchreplyprefix-list***ipv6-prefix-list-name* 例： `Device(config-dhcp-guard)# match reply prefix-list abc`	（任意）DHCP応答メッセージ内のアドバタイズされたプレフィックスが設定された承認プレフィックス リストからのものであることの検証をイネーブルにします。設定されていない場合、このチェックは回避されます。空のプレフィクス リストは、permit として処理されます。
ステップ 11	**preferencemin***limit* 例： `Device(config-dhcp-guard)# preference min 0`	（任意）アドバタイズされた設定（[preference] オプション内）が指定された制限を超過しているかどうかの検証をイネーブルにします。設定されていない場合、このチェックは回避されます。
ステップ 12	**preferencemax***limit* 例： `Device(config-dhcp-guard)# preference max 255`	（任意）アドバタイズされた設定（[preference] オプション内）が指定された制限未満であるかどうかの検証をイネーブルにします。設定されていない場合、このチェックは回避されます。
ステップ 13	**trusted-port** 例： `Device(config-dhcp-guard)# trusted-port`	（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。すべての DHCP ガード ポリシングが無効になります。
ステップ 14	**exit** 例： `Device(config-dhcp-guard)# exit`	DHCP ガード 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 モードに戻ります。
ステップ 15	**interface***typenumber* 例： `Device(config)# interface GigabitEthernet 0/2/0`	インターフェイスを指定し、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 16	**switchport** 例： `Device(config-if)# switchport`	レイヤ 3 モードになっているインターフェイスを、レイヤ 2 設定用にレイヤ 2 モードにします。
ステップ 17	**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、グローバル コンフィギュレーション 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 18	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 19	**showipv6dhcpguardpolicy** [*policy-name*] 例： `Device# show ipv6 dhcp policy guard pol1`	（任意）ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

DHCPv6 ガードの設定例

例：DHCP—DHCPv6 ガードの設定

次の例は、DHCPv6 ガードの設定例を示しています。

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
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
DHCP コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト、使用上の注意事項、および例	『*Cisco IOS IP Addressing Services Command Reference*』
DHCP の概念情報および設定情報	『*Cisco IOS IP Addressing Services Configuration Guide*』

標準規格/RFC

規格	タイトル
この機能によってサポートされる新しい規格/RFC または変更された規格/RFC はありません。	—

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。	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	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする場合、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

DHCP—DHCPv6 ガードの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *5*：***DHCP—DHCPv6*** ガードの機能情報

機能名	リリース	機能情報
DHCP—DHCPv6 ガード	Cisco IOS XE Release 3.8S	DHCP—DHCPv6 ガード機能は、サーバからクライアントにDHCPパケットを転送する、承認されていないDHCPサーバとリレー エージェントから発信されるDHCP応答やアドバタイズメント メッセージをブロックします。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るクライアント メッセージはブロックされません。 導入または変更されたコマンドは次のとおりです。 **device-role**、**ipv6 dhcp guard attach-policy**（**DHCPv6 ガード**）、**ipv6 dhcp guard policy**、**match reply prefix-list**、**match server access-list**、**preference**（**DHCPv6 ガード**）、**show ipv6 dhcp guard policy**、**trusted-port**（**DHCPv6 ガード**）。

第 7 章

IPv6 ソース ガードとプレフィックス ガード

IPv6 ソース ガードと IPv6 プレフィックス ガードは、IPv6 トラフィックの送信元を検証するレイヤ 2 スヌーピング機能です。IPv6 ソース ガードは、不明な送信元からのデータ トラフィックをブロックします。たとえば、バインディングテーブルにまだ入力されていないトラフィックや、ネイバー探索（ND）または Dynamic Host Configuration Protocol（DHCP）グリーニングを介して学習されていないトラフィックをブロックします。IPv6 プレフィックス ガードは、承認および委任されたトラフィック以外のホームノードが送信元のトラフィックを阻止します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

IPv6 ソース ガードとプレフィックス ガードに関する情報

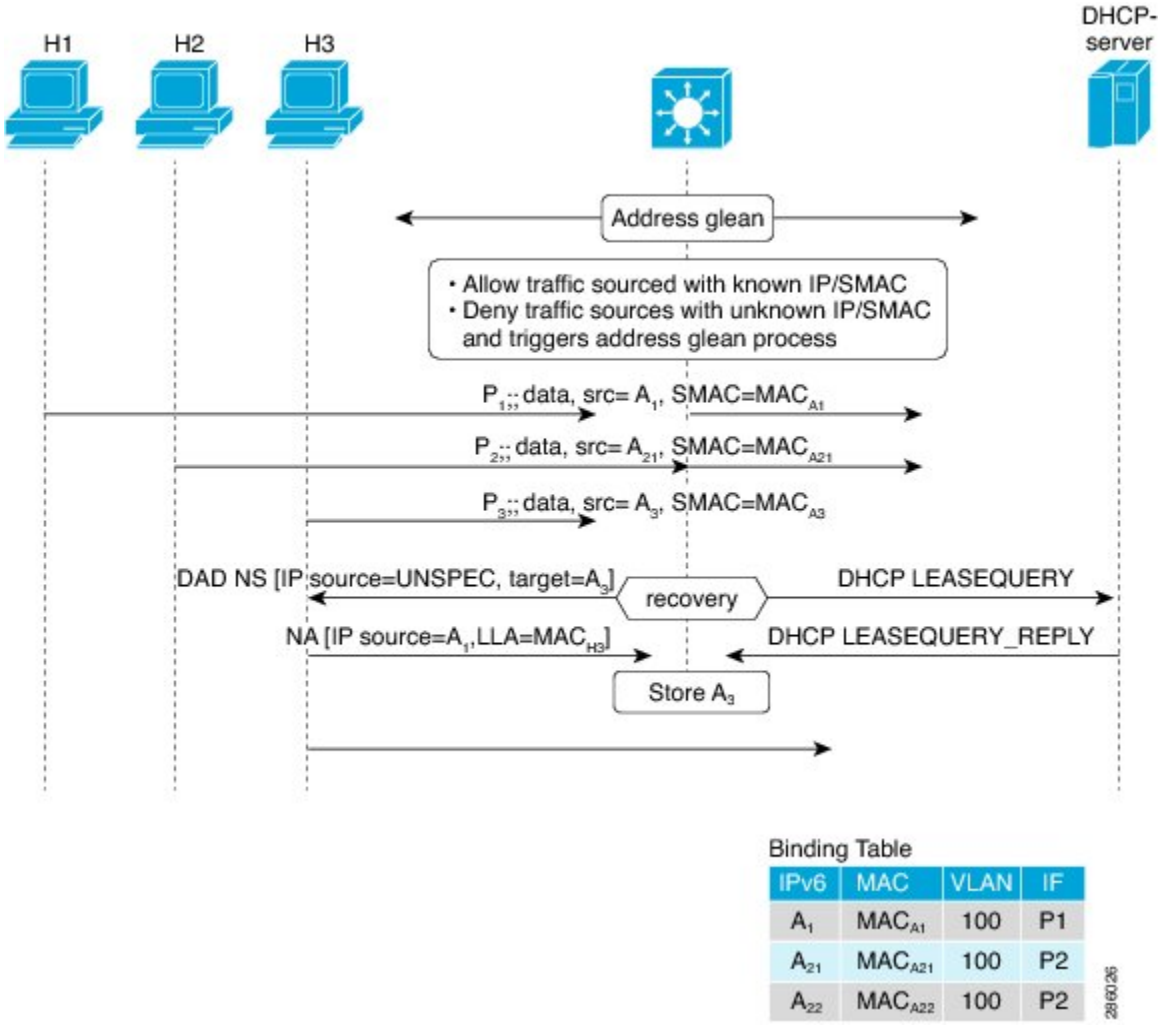
IPv6 ソース ガードの概要

IPv6 ソース ガードは、入力されたバインディング テーブルとデータ トラフィックのフィルタリング間で動作するインターフェイス機能です。この機能により、デバイスは、バインディング テーブルに保存されていないアドレスから送信されたトラフィックを拒否できます。IPv6 ソース ガードは ND や DHCP パケットを検査せず、むしろ、IPv6 ネイバー探索（ND）インスペクションや IPv6 アドレス収集（どちらもリンク上の既存アドレスを検出して、バインディング テーブルに保存する機能）と連動して機能します。IPv6 ソース ガードは、入力されたバインディング テーブルとデータ トラフィックのフィルタリング間で動作するインターフェイスであり、IPv6 ソース ガードが機能するためには、バインディング テーブルに IPv6 プレフィックスが入力されている必要があります。

IPv6 ソース ガードは、DHCP サーバによって割り当てられていない送信元からのトラフィックなど、不明な発信元や未割り当てのアドレスからのトラフィックを拒否できます。トラフィックが拒否されると、IPv6 アドレス収集機能に通知されるため、DHCP サーバをクエリして、または IPv6 ND を使用して、トラフィックのリカバリを試みることができます。データ収集機能は、有効なアドレスをバインディング テーブルに保存できず、復旧パスがなく、エンドユーザが接続できなくなるとすぐに、デバイスとエンド ユーザがデッドロックになるのを防ぎます。

次の図は、IPv6 ソース ガードと IPv6 アドレス収集の仕組みの概要を示しています。

図 *3* : *IPv6* ソース ガードとアドレス収集の概要



IPv6 プレフィックス ガードの概要

IPv6 プレフィックス ガード機能は、IPv6 ソース ガード機能内で動作し、トポロジ面で正しくないアドレスから発信されたトラフィックをデバイスが拒否できるようにします。IPv6 プレフィックス ガードは、IPv6 プレフィックスが DHCP プレフィックス委任を使用してデバイス（ホームゲートウェイなど）に委任される場合によく使用されています。この機能は、リンクに割り当てられたアドレスの範囲を検出し、この範囲に入っていないアドレスを発信元とするトラフィックをブロックします。

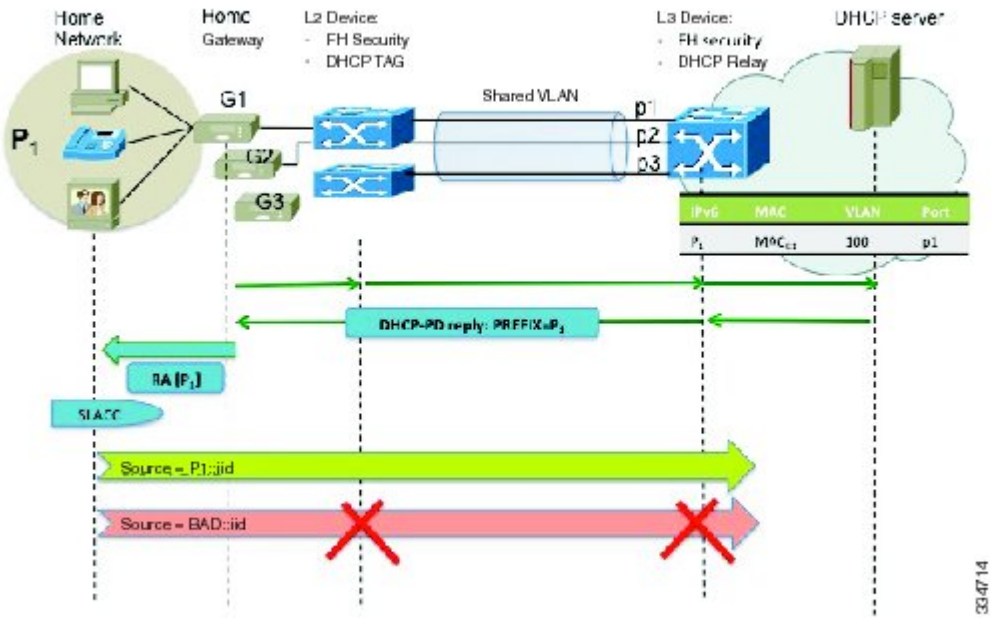
許可するプレフィックスとブロックするプレフィックスを決めるために、IPv6 プレフィックス ガードは以下の情報を使用します。

- ルータ アドバタイズメント（RA）でのプレフィックス収集
- DHCP プレフィックス委任でのプレフィックス収集
- 静的設定

IPv6プレフィックスガードでは、許可されるプレフィックスは常にハードウェアテーブルにダウンロードされます。ハードウェアは、パケットのスイッチングが行われるたびに、パケットの送信元をこのテーブルで照合し、一致するものがない場合そのパケットをドロップします。

次の図は、プレフィックスが DHCP-PD メッセージで収集されるサービス プロバイダー（SP）のシナリオを示しています。

図 *4*：プレフィックスが収集される *DHCP-PD* メッセージのシナリオ



IPv6 ソース ガードとプレフィックス ガードの設定方法

IPv6 ソース ガードの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipv6 source-guard policy** *source-guard-policy*
4. **permit link-local**
5. **deny global-autoconf**
6. **trusted**
7. **exit**
8. **show ipv6 source-guard policy** [*snooping-policy*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 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	**ipv6 source-guard policy** *source-guard-policy* 例： `Device(config)# ipv6 source-guard policy my_sourceguard_policy`	IPv6 ソースガード ポリシー名を定義して、スイッチ統合セキュリティ機能のソースガード ポリシー コンフィギュレーション モードを開始します。
ステップ 4	**permit link-local** 例： `Device(config-sisf-sourceguard)# permit link-local`	リンクローカル アドレスから発信されるすべてのデータ トラフィックに対するハードウェア ブリッジングを許可します。

	コマンドまたはアクション	目的
ステップ 5	**deny global-autoconf** 例： `Device(config-sisf-sourceguard)# deny global-autoconf`	自動設定されたグローバル アドレスからのデータ トラフィックを拒否します。
ステップ 6	**trusted** 例： `Device(config-sisf-sourceguard)# trusted`	ポリシーが適用されるターゲットのすべてのデータ トラフィックに対するハードウェア ブリッジングを許可します。
ステップ 7	**exit** 例： `Device(config-sisf-sourceguard)# exit`	ソース 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、特権 EXEC モードに戻ります。
ステップ 8	**show ipv6 source-guard policy** [*snooping-policy*] 例： `Device# show ipv6 source-guard policy policy1`	IPv6 ソースガード ポリシー設定を表示します。

インターフェイスの IPv6 ソース ガードの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipv6 source-guard attach-policy** *source-guard-policy*
5. **exit**
6. **show ipv6 source-guard policy** *source-guard-policy*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Device> enable`	• 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	**interface***typenumber* 例： `Device(config)# interface fastethernet 3/13`	インターフェイスのタイプおよび番号を指定し、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 4	**ipv6 source-guard attach-policy** *source-guard-policy* 例： `Device(config-if)# ipv6 source-guard attach-policy my_source_guard_policy`	インターフェイスに IPv6 ソース ガードを適用します。
ステップ 5	**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 モードを終了して、デバイスを特権 EXEC モードにします。
ステップ 6	**show ipv6 source-guard policy** *source-guard-policy* 例： `Device# show ipv6 source-guard policy policy1`	IPv6 ソース ガードが適用されているすべてのインターフェイスを表示します。

IPv6 プレフィックス ガードの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipv6 source-guard policy** *source-guard-policy*
4. **validate address**
5. **validate prefix**
6. **exit**
7. **show ipv6 source-guard policy** [*source-guard-policy*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 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	**ipv6 source-guard policy** *source-guard-policy* 例： `Device(config)# ipv6 source-guard policy my_snooping_policy`	IPv6 ソースガード ポリシー名を定義して、スイッチ統合セキュリティ機能のソースガードポリシー コンフィギュレーション モードを開始します。
ステップ 4	**validate address** 例： `Device(config-sisf-sourceguard)# no validate address`	アドレス検証機能をディセーブルにし、IPv6プレフィックス ガード機能を設定できるようにします。
ステップ 5	**validate prefix** 例： `Device(config-sisf-sourceguard)# validate prefix`	IPv6 ソース ガードをイネーブルにし、IPv6 プレフィックスガード動作を実行します。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Device(config-sisf-sourceguard)# exit`	スイッチ統合セキュリティ機能のソース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、特権 EXEC モードに戻ります。
ステップ 7	**show ipv6 source-guard policy** [*source-guard-policy*] 例： `Device# show ipv6 source-guard policy policy1`	IPv6 ソースガード ポリシー設定を表示します。

IPv6 ソース ガードとプレフィックス ガードの設定例

例：IPv6 ソース ガードとプレフィックス ガードの設定

```
Device# ipv6 source-guard policy policy1

Policy guard configuration:
  validate prefix
  validate address
```

IPv6 ソース ガードとプレフィックス ガードのその他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
IPv4 アドレス指定	『*IP Addressing: IPv4 Addressing Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』

関連項目	マニュアル タイトル
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準規格および RFC

規格/RFC	タイトル
IPv6 に関する RFC	*IPv6 の RFC*

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする場合、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 ソース ガードとプレフィックス ガードの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *6* : *IPv6* ソース ガードとプレフィックス ガードの機能情報

機能名	リリース	機能情報
IPv6 プレフィックス ガード	15.3(1)S	IPv6 プレフィックス ガード機能は、トポロジ面で正しくないアドレスから発信されたトラフィックをデバイスが拒否できるようにします。 導入または変更されたコマンドは次のとおりです。**ipv6 source-guard policy**、**permit link-local**、**show ipv6 source-guard policy**、**validate address**、**validate prefix**。
IPv6 ソース ガード	15.0(2)SE 15.3(1)S IOS XE 3.6.0E、IOS 15.2(2)E	IPv6 ソース ガード機能は、不明な送信元からのデータ トラフィックをブロックします。たとえば、バインディング テーブルにまだ入力されていないトラフィックや、ND または DHCP グリーニングを介して学習されていないトラフィックをブロックします。 導入または変更されたコマンドは次のとおりです。**deny global-autoconfig**、**ipv6 source-guard attach-policy**、**ipv6 source-guard policy**、**permit link-local**、**show ipv6 source-guard policy**、**trusted**。

第 8 章

IPv6 宛先ガード

IPv6 宛先ガード機能は、IPv6 ネイバー探索とともに動作して、リンク上でアクティブであると認識されているアドレスについてのみ、デバイスがアドレスを解決するようにします。アドレスグリーニング機能に依存して、リンク上でアクティブなすべての宛先をバインディング テーブルに挿入した後に、バインディング テーブルで宛先が見つからなかったときに実行される解決をブロックします。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

IPv6 宛先ガードの前提条件

- IPv6 ネイバー探索機能についての知識が必要です。IPv6 ネイバー探索の詳細については、「IPv6 アドレッシングと基本接続の実装」を参照してください。
- IPv6 ファーストホップ セキュリティ バインディング テーブル機能についての知識が必要です。詳細については、「IPv6 ファーストホップ セキュリティ バインディング テーブル」を参照してください。

IPv6 宛先ガードに関する情報

IPv6 宛先ガードの概要

IPv6 宛先ガード機能は、IPv6 ネイバー探索とともに動作して、リンク上でアクティブであると認識されているアドレスについてのみ、デバイスがアドレスを解決するようにします。アドレス グリーニング機能に依存して、リンク上でアクティブなすべての宛先をバインディング テーブルに挿入した後に、バインディング テーブルで宛先が見つからなかったときに実行される解決をブロックします。

デバイスはルーティングされた着信トラフィックをフィルタリングする前に、Neighbor Discovery Protocol（NDP）メッセージおよびDHCPメッセージをスヌーピングして、リンク上のアドレスを収集します。パケットがデバイスに到達し、宛先またはネクスト ホップの隣接関係（アジャセンシー）がまだ存在していない場合、NDP はデバイス バインディング テーブルを参照して、リンク上の宛先またはネクストホップがすでに収集済みであるか確認します。バインディングテーブルに当該宛先が存在しない場合、そのパケットはドロップされます。存在する場合、ネイバー探索の解決が実行されます。

IPv6 宛先ガードの設定方法

IPv6 宛先ガードの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipv6 destination-guard policy***policy-name*
4. **enforcement** {**always** | **stressed**}
5. **exit**
6. **interface***type number*
7. **ipv6destination-guardattach-policy** [*policy-name*]
8. **exit**
9. **showipv6destination-guardpolicy** [*policy-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 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	**ipv6 destination-guard policy***policy-name* 例： `Device(config)# ipv6 destination-guard policy pol1`	宛先ガード ポリシー名を定義して、宛先ガード 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	**enforcement** {**always** | **stressed**} 例： `Device(config-destguard)# enforcement always`	ターゲット アドレスの強制レベルを設定します。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Device(config-destguard)# exit`	宛先ガード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 モードに戻ります。
ステップ 6	**interface***type number* 例： `Device(config)# interface GigabitEthernet 0/0/1`	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 7	**ipv6destination-guardattach-policy** [*policy-name*] 例： `Device(config-if)# ipv6 destination-guard attach-policy pol1`	インターフェイスに宛先ガード ポリシーを対応付けます。
ステップ 8	**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、特権 EXEC コンフィギュレーション モードに戻ります。
ステップ 9	**showipv6destination-guardpolicy** [*policy-name*] 例： `Device# show ipv6 destination-guard policy pol1`	（任意）ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

IPv6 宛先ガードの設定例

例：IPv6 宛先ガード ポリシーの設定

次の例は、宛先ガード ポリシーの設定方法を示しています。

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet 0/0/1
Router(config-if)# ipv6 destination-guard attach-policy destination

Router# show ipv6 destination-guard policy destination
Destination guard policy Destination:
```

```
enforcement always
      Target: Gi0/0/1
```

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
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 宛先ガードの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *7*：*IPv6* 宛先ガードの機能情報

機能名	リリース	機能情報
IPv6 宛先ガード	15.2(4)S 15.1(2)SG IOS XE 3.6.0E、IOS 15.2(2)E	IPv6宛先ガードの機能は、不明な送信元からのデータ トラフィックをブロックし、宛先アドレスに基づいて IPv6 トラフィックをフィルタリングします。 導入または変更されたコマンドは次のとおりです。**enforcement**、**ipv6 destination-guard attach-policy**、**ipv6 destination-guard policy**、**show ipv6 destination-guard policy**。

第 9 章

IPv6 の RFC

標準規格および RFC

RFC	タイトル
RFC 1195	『*Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*』
RFC 1267	『*A Border Gateway Protocol 3 (BGP-3)*』
RFC 1305	『*Network Time Protocol (Version 3) Specification, Implementation and Analysis*』
RFC 1583	『*OSPF version 2*』
RFC 1772	『*Application of the Border Gateway Protocol in the Internet*』
RFC 1886	『*DNS Extensions to Support IP version 6*』
RFC 1918	『*Address Allocation for Private Internets*』
RFC 1981	『*Path MTU Discovery for IP version 6*』
RFC 2080	『*RIPng for IPv6*』
RFC 2281	『*Cisco Hot Standby Router Protocol (HSRP)*』
RFC 2332	『*NBMA Next Hop Resolution Protocol (NHRP)*』
RFC 2373	『*IP Version 6 Addressing Architecture*』
RFC 2374	『*An Aggregatable Global Unicast Address Format*』

RFC	タイトル
RFC 2375	『*IPv6 Multicast Address Assignments*』
RFC 2401	『*Security Architecture for the Internet Protocol*』
RFC 2402	『*IP Authentication Header*』
RFC 2404	『*The Use of Hash Message Authentication Code Federal Information Processing Standard 180-1 within Encapsulating Security Payload and Authentication Header*』
RFC 2406	『*IP Encapsulating Security Payload (ESP)*』
RFC 2407	『*The Internet Security Domain of Interpretation for ISAKMP*』
RFC 2408	『*Internet Security Association and Key Management Protocol*』
RFC 2409	『*Internet Key Exchange (IKE)*』
RFC 2427	『*Multiprotocol Interconnect over Frame Relay*』
RFC 2428	『*FTP Extensions for IPv6 and NATs*』
RFC 2460	『*Internet Protocol, Version 6 (IPv6) Specification*』
RFC 2461	『*Neighbor Discovery for IP Version 6 (IPv6)*』
RFC 2462	『*IPv6 Stateless Address Autoconfiguration*』
RFC 2463	『*Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*』
RFC 2464	『*Transmission of IPv6 Packets over Ethernet*』
RFC 2467	『*Transmission of IPv6 Packets over FDDI*』
RFC 2472	『*IP Version 6 over PPP*』
RFC 2473	『*Generic Packet Tunneling in IPv6 Specification*』
RFC 2474	『*Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*』

RFC	タイトル
RFC 2475	『*An Architecture for Differentiated Services Framework*』
RFC 2492	『*IPv6 over ATM*』
RFC 2545	『*Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*』
RFC 2590	『*Transmission of IPv6 Packets over Frame Relay Specification*』
RFC 2597	『*Assured Forwarding PHB*』
RFC 2598	『*An Expedited Forwarding PHB*』
RFC 2640	『*Internet Protocol, Version 6 Specification*』
RFC 2684	『*Multiprotocol Encapsulation over ATM Adaptation Layer 5*』
RFC 2697	『*A Single Rate Three Color Marker*』
RFC 2698	『*A Two Rate Three Color Marker*』
RFC 2710	『*Multicast Listener Discovery (MLD) for IPv6*』
RFC 2711	『*IPv6 Router Alert Option*』
RFC 2732	『*Format for Literal IPv6 Addresses in URLs*』
RFC 2765	『*Stateless IP/ICMP Translation Algorithm (SIIT)*』
RFC 2766	『*Network Address Translation-Protocol Translation (NAT-PT)*』
RFC 2858	『*Multiprotocol Extensions for BGP-4*』
RFC 2893	『*Transition Mechanisms for IPv6 Hosts and Routers*』
RFC 3056	『*Connection of IPv6 Domains via IPv4 Clouds*』
RFC 3068	『*An Anycast Prefix for 6to4 Relay Routers*』

RFC	タイトル
RFC 3095	『*RObust Header Compression (ROHC): Framework and Four Profiles: RTP, UDP, ESP, and Uncompressed*』
RFC 3107	『*Carrying Label Information in BGP-4*』
RFC 3137	『*OSPF Stub Router Advertisement*』
RFC 3147	『*Generic Routing Encapsulation over CLNS*』
RFC 3152	『*Delegation of IP6.ARPA*』
RFC 3162	『*RADIUS and IPv6*』
RFC 3315	『*Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*』
RFC 3319	『*Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiated Protocol (SIP) Servers*』
RFC 3392	『*Capabilities Advertisement with BGP-4*』
RFC 3414	『*User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*』
RFC 3484	『*Default Address Selection for Internet Protocol version 6 (IPv6)*』
RFC 3513	『*Internet Protocol Version 6 (IPv6) Addressing Architecture*』
RFC 3576	『*Change of Authorization*』
RFC 3587	『*IPv6 Global Unicast Address Format*』
RFC 3590	『*Source Address Selection for the Multicast Listener Discovery (MLD) Protocol*』
RFC 3596	『*DNS Extensions to Support IP Version 6*』
RFC 3633	『*DHCP IPv6 Prefix Delegation*』

RFC	タイトル
RFC 3646	『*DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*』
RFC 3697	『*IPv6 Flow Label Specification*』
RFC 3736	『*Stateless DHCP Service for IPv6*』
RFC 3756	『*IPv6 Neighbor Discovery (ND) Trust Models and Threats*』
RFC 3759	『*RObust Header Compression (ROHC): Terminology and Channel Mapping Examples*』
RFC 3775	『*Mobility Support in IPv6*』
RFC 3810	『*Multicast Listener Discovery Version 2 (MLDv2) for IPv6*』
RFC 3846	『*Mobile IPv4 Extension for Carrying Network Access Identifiers*』
RFC 3879	『*Deprecating Site Local Addresses*』
RFC 3898	『*Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*』
RFC 3954	『*Cisco Systems NetFlow Services Export Version 9*』
RFC 3956	『*Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address*』
RFC 3963	『*Network Mobility (NEMO) Basic Support Protocol*』
RFC 3971	『*SEcure Neighbor Discovery (SEND)*』
RFC 3972	『*Cryptographically Generated Addresses (CGA)*』
RFC 4007	『*IPv6 Scoped Address Architecture*』
RFC 4075	『*Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6*』

RFC	タイトル
RFC 4087	『*IP Tunnel MIB*』
RFC 4091	『*The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework*』
RFC 4092	『*Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)*』
RFC 4109	『*Algorithms for Internet Key Exchange version 1 (IKEv1)*』
RFC 4191	『*Default Router Preferences and More-Specific Routes*』
RFC 4193	『*Unique Local IPv6 Unicast Addresses*』
RFC 4214	『*Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)*』
RFC 4242	『*Information Refresh Time Option for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*』
RFC 4282	『*The Network Access Identifier*』
RFC 4283	『*Mobile Node Identifier Option for Mobile IPv6*』
RFC 4285	『*Authentication Protocol for Mobile IPv6*』
RFC 4291	『*IP Version 6 Addressing Architecture*』
RFC 4292	『*IP Forwarding Table MIB*』
RFC 4293	『*Management Information Base for the Internet Protocol (IP)*』
RFC 4302	『*IP Authentication Header*』
RFC 4306	『*Internet Key Exchange (IKEv2) Protocol*』
RFC 4308	『*Cryptographic Suites for IPsec*』
RFC 4364	『*BGP MPLS/IP Virtual Private Networks (VPNs)*』

RFC	タイトル
RFC 4382	『*MPLS/BGP Layer 3 Virtual Private Network (VPN) Management Information Base*』
RFC 4443	『*Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*』
RFC 4552	『*Authentication/Confidentiality for OSPFv3*』
RFC 4594	『*Configuration Guidelines for DiffServ Service Classes*』
RFC 4601	『*Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification*』
RFC 4610	『*Anycast-RP Using Protocol Independent Multicast (PIM)*』
RFC 4649	『*Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option*』
RFC 4659	『*BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*』
RFC 4724	『*Graceful Restart Mechanism for BGP*』
RFC 4798	『*Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)*』
RFC 4818	『*RADIUS Delegated-IPv6-Prefix Attribute*』
RFC 4861	『*Neighbor Discovery for IP version 6 (IPv6)*』
RFC 4862	『*IPv6 Stateless Address Autoconfiguration*』
RFC 4884	『*Extended ICMP to Support Multi-Part Messages*』
RFC 4885	『*Network Mobility Support Terminology*』
RFC 4887	『*Network Mobility Home Network Models*』
RFC 5015	『*Bidirectional Protocol Independent Multicast (BIDIR-PIM)*』

RFC	タイトル
RFC 5059	『*Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)*』
RFC 5072	『*IPv6 over PPP*』
RFC 5095	『*Deprecation of Type 0 Routing Headers in IPv6*』
RFC 5120	『*M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)*』
RFC 5130	『*A Policy Control Mechanism in IS-IS Using Administrative Tags*』
RFC 5187	『*OSPFv3 Graceful Restart*』
RFC 5213	『*Proxy Mobile IPv6*』
RFC 5308	『*Routing IPv6 with IS-IS*』
RFC 5340	『*OSPF for IPv6*』
RFC 5460	『*DHCPv6 Bulk Leasequery*』
RFC 5643	『*Management Information Base for OSPFv3*』
RFC 5838	『*Support of Address Families in OSPFv3*』
RFC 5844	『*IPv4 Support for Proxy Mobile IPv6*』
RFC 5845	『*Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6*』
RFC 5846	『*Binding Revocation for IPv6 Mobility*』
RFC 5881	『*Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)*』
RFC 5905	『*Network Time Protocol Version 4: Protocol and Algorithms Specification*』
RFC 5969	『*IPv6 Rapid Deployment on IPv4 Infrastructures (6RD) -- Protocol Specification*』
RFC 6105	『*IPv6 Router Advertisement Guard*』

RFC	タイトル
RFC 6620	『*FCFS SAVI: First-Come, First-Served Source Address Validation Improvement for Locally Assigned IPv6 Addresses*』