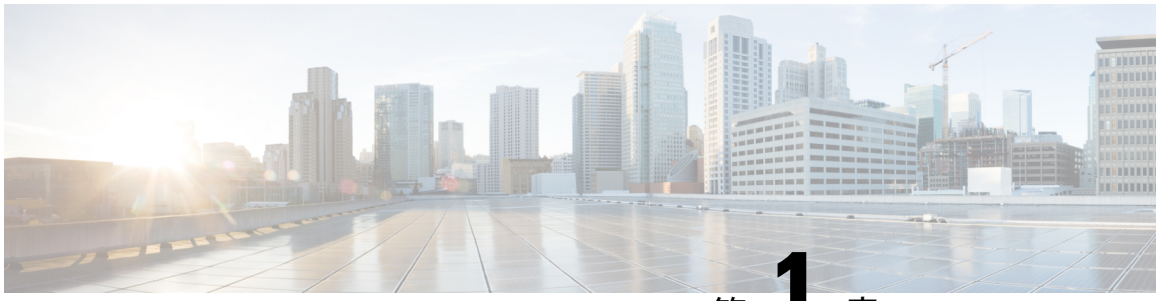
Cisco IOS XE Fuji 16.9.x（Catalyst 9300 スイッチ）IPv6 コンフィギュレーション ガイド

初版：2018 年 7 月 18 日

最終更新：2018 年 7 月 26 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/

目 次



第 1 章

MLD スヌーピングの設定

このモジュールには、MLD スヌーピングの設定の詳細が含まれています。

IPv6 MLD スヌーピングの設定に関する情報

スイッチ上で Multicast Listener Discovery（MLD）スヌーピングを使用して、スイッチド ネットワーク内のクライアントおよびルータに IP Version 6（IPv6）マルチキャスト データを効率的に配信することができます。特に指示がないかぎり、スイッチという用語は、スタンドアロン スイッチおよびスイッチ スタックを指します。

IPv6 を使用するには、デュアル IPv4 および IPv6 スイッチング データベース管理（SDM）テンプレートがスイッチに設定されている必要があります。

この章で使用するコマンドの構文と使用方法の詳細については、『*Command Reference (Catalyst 9300 Series Switches)* 』を参照してください。

MLD スヌーピングの概要

IP Version 4（IPv4）では、レイヤ 2 スイッチはインターネット グループ管理プロトコル（IGMP）スヌーピングを使用して、動的にレイヤ 2 インターフェイスを設定することにより、マルチキャスト トラフィックのフラッディングを抑制します。そのため、マルチキャスト トラフィックは IP マルチキャスト デバイスに対応付けられたインターフェイスにだけ転送されます。IPv6 では、MLD スヌーピングが同様の機能を実行します。MLD スヌーピングを使用すると、IPv6 マルチキャスト データは VLAN（仮想 LAN）内のすべてのポートにフラッディングされるのではなく、データを受信するポートのリストに選択的に転送されます。このリストは、IPv6 マルチキャスト制御パケットをスヌーピングすることにより構築されます。

MLD は IPv6 マルチキャスト ルータで使用されるプロトコルで、ルータに直接接続されたリンク上のマルチキャスト リスナー（IPv6 マルチキャスト パケットを受信するノード）の存在、および隣接ノードを対象とするマルチキャスト パケットを検出します。MLD は IGMP から派生しています。MLD バージョン 1（MLDv1）は IGMPv2 と、MLD バージョン 2（MLDv2）は IGMPv3 とそれぞれ同等です。MLD は Internet Control Message Protocol バージョン 6（ICMPv6）のサブプロトコルです。MLD メッセージは ICMPv6 メッセージのサブセットで、IPv6 パケット内で先頭の Next Header 値 58 により識別されます。

スイッチは、次の 2 つのバージョンの MLD スヌーピングをサポートします。

- MLDv1 スヌーピング：MLDv1 制御パケットを検出し、IPv6 宛先マルチキャスト アドレスに基づいてトラフィックのブリッジングを設定します。
- MLDv2 基本スヌーピング（MBSS）：MLDv2 制御パケットを使用して、IPv6 宛先マルチキャスト アドレスに基づいてトラフィックの転送を設定します。

スイッチは MLDv1 プロトコル パケットと MLDv2 プロトコル パケットの両方でスヌーピングでき、IPv6 宛先マルチキャスト アドレスに基づいて IPv6 マルチキャスト データをブリッジングします。

（注） スイッチは、IPv6 送信元および宛先マルチキャスト アドレスベースの転送を設定する MLDv2 拡張スヌーピングをサポートしません。

MLD スヌーピングは、グローバルまたは VLAN 単位でイネーブルまたはディセーブルに設定できます。MLD スヌーピングがイネーブルの場合、VLAN 単位の IPv6 マルチキャスト アドレス テーブルはソフトウェアおよびハードウェアで構築されます。その後、スイッチはハードウェアで IPv6 マルチキャストアドレスに基づくブリッジングを実行します。

IPv6 マルチキャスト標準に従い、スイッチは自身の MAC アドレスの下位 4 オクテットと MAC アドレス 33:33:00:00:00:00 の論理 OR を実行して、MAC マルチキャストアドレスを抽出します。たとえば、IPv6 の MAC アドレス FF02:DEAD:BEEF:1:3 は、イーサネットの MAC アドレス 33:33:00:01:00:03 にマッピングされます。

IPv6 宛先アドレスと MAC 宛先アドレスが一致しない場合、マルチキャスト パケットは一致しません。スイッチは、一致しないパケットをハードウェア ベースの MAC アドレス テーブルによって転送します。MAC 宛先アドレスが MAC アドレス テーブルにない場合、スイッチは受信したポートと同じ VLAN 内のすべてのポートにパケットをフラッディングします。

MLD メッセージ

MLDv1 は、次の 3 種類のメッセージをサポートします。

- Listener Query：IGMPv2 クエリーと同等で、General Query または Mulicast-Address-Specific Query（MASQ）のいずれかになります。
- Multicast Listener Report：IGMPv2 レポートと同等です。
- Multicast Listener Done メッセージ：IGMPv2 Leave メッセージと同等です。

MLDv2 では、MLDv1 レポートおよび Done メッセージに加えて、MLDv2 クエリーおよび MLDv2 レポートもサポートします。

メッセージの送受信の結果生じるメッセージ タイマーおよびステート移行は、IGMPv2 メッセージの場合と同じです。リンクに対してローカルで有効な IPv6 送信元アドレスを持たない MLD メッセージは、MLD ルータおよび MLD スイッチで無視されます。

MLD クエリー

スイッチは MLD クエリーを送信し、IPv6 マルチキャスト アドレス データベースを構築し、MLD グループ固有クエリー、MLD グループおよび送信元固有クエリーを生成して、MLD Done メッセージに応答します。また、スイッチはレポート抑制、レポート プロキシング、即時脱退機能、およびスタティックな IPv6 マルチキャスト グループ アドレス設定もサポートします。

MLD スヌーピングがディセーブルの場合、すべての MLD クエリーが入力 VLAN でフラッディングされます。

MLD スヌーピングがイネーブルの場合、受信された MLD クエリーが入力 VLAN でフラッディングされ、クエリーのコピーは CPU に送信され、処理されます。MLD スヌーピングでは、受信されたクエリーから IPv6 マルチキャスト アドレス データベースを構築します。MLD スヌーピングは、マルチキャスト ルータ ポートを検出して、タイマーを維持し、レポート応答時間を設定します。また、VLAN のクエリア IP 送信元アドレス、VLAN 内のクエリア ポートを学習して、マルチキャスト アドレス エージングを維持します。

（注） IPv6 マルチキャスト ルータが Catalyst 6500 スイッチであり、拡張 VLAN（範囲 1006 ～ 4094）を使用する場合、Catalyst 2960、2960-S、2960-C、2960-X、または 2960-CX スイッチが VLAN 上でクエリを受信できるようにするため、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの拡張 VLAN でイネーブルにする必要があります。標準範囲 VLAN（1 ～ 1005）の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。

グループが MLD スヌーピング データベースに存在する場合、スイッチは MLDv1 レポートを送信して、グループ固有のクエリーに応答します。このグループが不明の場合、グループ固有のクエリーは入力 VLAN にフラッディングされます。

ホストがマルチキャスト グループから脱退する場合、MLD Done メッセージ（IGMP Leave メッセージと同等）を送信できます。スイッチが MLDv1 Done メッセージを受信した際に、即時脱退がイネーブルでなければ、スイッチは メッセージを受信したポートに MASQ を送信して、ポートに接続する他のデバイスがマルチキャスト グループに残る必要があるかどうか判別します。

マルチキャスト クライアント エージングの堅牢性

クエリー数に基づいて、アドレスからのポート メンバーシップの削除を設定できます。1 つのアドレスに対するメンバーシップからポートが削除されるのは、設定された数のクエリーに関してポート上のアドレスに対するレポートがない場合のみです。デフォルトの回数は 2 回です。

マルチキャスト ルータ検出

IGMP スヌーピングと同様に、MLD スヌーピングでは次の特性を持つマルチキャスト ルータ検出を行います。

- ユーザにより設定されたポートには、期限切れがありません。
- ダイナミックなポート学習は、MLDv1 スヌーピング クエリーおよび IPv6 PIMv2 パケットにより行われます。
- 複数のルータが同じレイヤ2インターフェイス上にある場合、MLD スヌーピングではポート上の単一のマルチキャスト ルータ（直前にルータ制御パケットを送信したルータ）を追跡します。
- マルチキャスト ルータ ポートのダイナミックなエージングは、デフォルト タイマーの 5 分に基づきます。ポート上で制御パケットが 5 分間受信されない場合、マルチキャスト ルータはルータのポート リストから削除されます。
- IPv6 マルチキャスト ルータ検出が実行されるのは、MLD スヌーピングがスイッチでイネーブルの場合のみです。
- 受信された IPv6 マルチキャスト ルータ制御パケットは、スイッチで MLD スヌーピングがイネーブルかどうかにかかわらず、常に入力 VLAN にフラッディングされます。
- 最初の IPv6 マルチキャスト ルータ ポートが検出された後は、不明の IPv6 マルチキャスト データは、検出されたルータ ポートに対してのみ転送されます（それまでは、すべての IPv6 マルチキャスト データは入力 VLAN にフラッディングされます）。

MLD レポート

MLDv1 join メッセージは、本質的には IGMPv2 と同じように処理されます。IPv6 マルチキャスト ルータが VLAN で検出されない場合は、レポートが処理されないか、またはスイッチから転送されません。IPv6 マルチキャスト ルータが検出され、MLDv1 レポートが受信されると、IPv6 マルチキャスト グループ アドレスが VLAN の MLD データベースに入力されます。その後、VLAN 内のグループに対するすべての IPv6 マルチキャスト トラフィックが、このアドレスを使用して転送されます。MLD スヌーピングがディセーブルの場合、レポートは入力 VLAN でフラッディングされます。

MLD スヌーピングがイネーブルの場合は、MLD レポート抑制（リスナー メッセージ抑制）は自動的にイネーブルになります。レポート抑制により、スイッチはグループで受信された最初の MLDv1 レポートを IPv6 マルチキャスト ルータに転送します。グループのそれ以降のレポートはルータに送信されません。MLD スヌーピングがディセーブルの場合は、レポート抑制がディセーブルになり、すべての MLDv1 レポートは入力 VLAN にフラッディングされます。

スイッチは、MLDv1 プロキシ レポーティングもサポートします。MLDv1 MASQ が受信されると、スイッチに他のポートのグループが存在する場合、およびクエリーを受信したポートとアドレスの最後のメンバ ポートが異なる場合は、スイッチはクエリーを受信したアドレスに関する MLDv1 レポートで応答します。

MLD Done メッセージおよび即時脱退

即時脱退機能がイネーブルの場合にホストが MLDv1 Done メッセージ（IGMP Leave メッセージと同等）を送信すると、Done メッセージを受信したポートはグループからただちに削除されます。VLAN で即時脱退をイネーブルにする場合は（IGMP スヌーピングと同様に）、ポートに単一のホストが接続されている VLAN でのみこの機能を使用します。ポートがグループの最後のメンバである場合、グループも削除され、検出された IPv6 マルチキャスト ルータに脱退情報が転送されます。

VLAN で即時脱退がイネーブルでない場合に（1 つのポート上にグループのクライアントが複数ある場合）、Done メッセージがポートで受信されると、このポートで MASQ が生成されます。ユーザは、既存アドレスのポート メンバーシップが削除される時期を MASQ 数の観点から制御できます。アドレスに対するメンバーシップからポートが削除されるのは、設定された数のクエリーに関してポート上のアドレスに対する MLDv1 レポートがない場合です。

生成される MASQ 数は、 **ipv6 mld snooping last-listener-query count** グローバル コンフィギュレーション コマンドにより設定されます。デフォルトの回数は 2 回です。

MASQ は、Done メッセージが送信された IPv6 マルチキャスト アドレスに送信されます。スイッチの最大応答時間内に MASQ で指定された IPv6 マルチキャスト アドレスにレポートが送信されなければ、MASQ が送信されたポートは IPv6 マルチキャスト アドレス データベースから削除されます。最大応答時間は、 **ipv6 mld snooping last-listener-query-interval** グローバル コンフィギュレーション コマンドにより設定します。削除されたポートがマルチキャスト アドレスの最後のメンバである場合は、マルチキャストアドレスも削除され、スイッチは検出されたマルチキャスト ルータすべてにアドレス脱退情報を送信します。

即時脱退がイネーブルでない場合に、ポートが MLD Done メッセージを受信すると、スイッチはポートで MASQ を生成して、Done メッセージが送信された IPv6 マルチキャスト アドレスに送信します。ポートがマルチキャスト グループから削除される前に、送信される MASQ 数およびスイッチが応答を待機する時間を任意で設定できます。

MLDv1 即時脱退をイネーブルにした場合、スイッチはポートで MLD Done メッセージを検出するとただちに、マルチキャスト グループからポートを削除します。即時脱退機能を使用するのは、VLAN の各ポート上にレシーバが 1 つだけ存在する場合に限定してください。同一ポートにマルチキャスト グループのクライアントが複数ある場合は、VLAN で即時脱退をイネーブルにしてはなりません。

TCN 処理

ipv6 mld snooping tcn query solicit グローバル コンフィギュレーション コマンドを使用して、トポロジ変更通知（TCN）送信要求を有効にすると、MLDv1 スヌーピングは、設定された数の MLDv1 クエリによりすべての IPv6 マルチキャストトラフィックをフラッディングするよう VLAN に設定してから、選択されたポートにのみマルチキャストデータの送信を開始します。この値は、 **ipv6 mld snooping tcn flood query count** グローバルコンフィギュレーションコマンドを使用して設定します。デフォルトでは、2 つのクエリーが送信されます。スイッチが VLAN 内の STP ルートになる場合、またはスイッチがユーザにより設定された場合は、リンクに対してローカルで有効な IPv6 送信元アドレスを持つ MLDv1 グローバル Done メッセージも生成されます。これは IGMP スヌーピングの場合と同じです。

IPv6 MLD スヌーピングの設定方法

MLD スヌーピングのデフォルト設定

表 *1: MLD* スヌーピングのデフォルト設定

機能	デフォルト設定
MLD スヌーピング（グローバル）	ディセーブル。
MLD スヌーピング（VLAN 単位）	イネーブルVLAN MLD スヌーピングが実行されるためには、MLD スヌーピングがグローバルにイネーブルである必要があります。
IPv6 マルチキャスト アドレス	未設定
IPv6 マルチキャスト ルータ ポート	未設定
MLD スヌーピング即時脱退	ディセーブル。
MLD スヌーピングの堅牢性変数	グローバル：2、VLAN 単位：0 （注） VLAN値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバル数を使用します。
最後のリスナー クエリー カウント	グローバル：2、VLAN 単位：0 （注） VLAN値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバル数を使用します。
最後のリスナー クエリー インターバル	グローバル：1000（1 秒）、VLAN：0 （注） VLAN値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバルのインターバルを使用します。
TCN クエリー送信請求	ディセーブル。
TCN クエリー カウント	2
MLD リスナー抑制	ディセーブル

MLD スヌーピング設定時の注意事項

MLD スヌーピングの設定時は、次の注意事項に従ってください。

- MLD スヌーピングの特性はいつでも設定できますが、設定を有効にする場合は、 **ipv6 mld snooping** グローバル コンフィギュレーション コマンドを使用して MLD スヌーピングをグローバルにイネーブルにする必要があります。
- MLD スヌーピングと IGMP スヌーピングは相互に独立して動作します。スイッチで両方の機能を同時にイネーブルにできます。
- スイッチまたはスイッチ スタックに保持可能なアドレス エントリの最大数は 4000 です。

スイッチでのMLDスヌーピングのイネーブル化またはディセーブル化

デフォルトでは、IPv6 MLD スヌーピングはスイッチではグローバルにディセーブルで、すべての VLAN ではイネーブルです。MLD スヌーピングがグローバルにディセーブルの場合は、すべての VLAN でもディセーブルです。MLD スヌーピングをグローバルにイネーブルにすると、VLAN 設定はグローバル設定を上書きします。つまり、MLD スヌーピングはデフォルト ステート（イネーブル）の VLAN インターフェイスでのみイネーブルになります。

VLAN 単位または VLAN 範囲で MLD スヌーピングをイネーブルおよびディセーブルにできますが、MLD スヌーピングをグローバルにディセーブルにした場合は、すべての VLAN でディセーブルになります。グローバル スヌーピングがイネーブルの場合、VLAN スヌーピングをイネーブルまたはディセーブルに設定できます。

スイッチでグローバルにMLDスヌーピングをイネーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 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： `デバイス# 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 mld snooping** 例： `デバイス(config)# ipv6 mld snooping`	スイッチで MLD スヌーピング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 4	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config** 例： デバイス(config)# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ 6	**reload** 例： デバイス(config)# **reload**	OS（オペレーティング システム）をリロードします。

VLAN に対する MLD スヌーピングのイネーブル化またはディセーブル化

VLAN で MLD スヌーピングをイネーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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 mld snooping** 例： デバイス(config)# **ipv6 mld snooping**	スイッチで MLD スヌーピング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 4	**ipv6 mld snooping vlan** *vlan-id* 例： `デバイス(config)# ipv6 mld snooping vlan 1`	VLAN でMLD スヌーピングをイネーブルにします。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 （注） VLAN スヌーピングをイネーブルにするには、MLD スヌーピングがグローバルにイネーブルである必要があります。
ステップ 5	**end** 例： `デバイス(config)# ipv6 mld snooping vlan 1`	特権 EXEC モードに戻ります。

スタティックなマルチキャスト グループの設定

ホストまたはレイヤ 2 ポートは、通常マルチキャスト グループにダイナミックに加入しますが、VLAN に IPv6 マルチキャスト アドレスおよびメンバ ポートをスタティックに設定することもできます。

マルチキャスト グループのメンバとしてレイヤ 2 ポートを追加するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 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： `デバイス# 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 mld snooping vlan** *vlan-id* **static** *ipv6_multicast_address* **interface** *interface-id* 例： `デバイス(config)# ipv6 mld snooping vlan 1 static FF12::3 interface gigabitethernet 0/1`	マルチキャスト グループのメンバとしてレイヤ 2 ポートにマルチキャスト グループを設定します。 • *vlan-id* は、マルチキャスト グループの VLAN ID です。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。

	コマンドまたはアクション	目的
		• *ipv6_multicast_address* は、128 ビットのグループ IPv6 アドレスです。このアドレスは RFC 2373 で指定された形式でなければなりません。 • *interface-id* は、メンバ ポートです。物理インターフェイスまたはポートチャネル（1 ～ 48）に設定できます。
ステップ 4	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	次のいずれかを使用します。 • **show ipv6 mld snooping address** • **show ipv6 mld snooping address vlan** *vlan-id* 例： デバイス# **show ipv6 mld snooping address** または デバイス# **show ipv6 mld snooping vlan 1**	スタティック メンバ ポートおよび IPv6 アドレスを確認します。

マルチキャスト ルータ ポートの設定

（注） マルチキャスト ルータへのスタティック接続は、スイッチ ポートに限りサポートされます。

VLAN にマルチキャスト ルータ ポートを追加するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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：	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
	デバイス# **configure terminal**	
ステップ 3	**ipv6 mld snooping vlan** *vlan-id* **mrouter interface** *interface-id* 例： デバイス(config)# **ipv6 mld snooping vlan 1 mrouter interface gigabitethernet 0/2**	マルチキャスト ルータの VLAN ID を指定して、マルチキャスト ルータにインターフェイスを指定します。 • 指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 • このインターフェイスには物理インターフェイスまたはポート チャネルを指定できます。指定できるポートチャネルの範囲は 1 ～ 48 です。
ステップ 4	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show ipv6 mld snooping mrouter** [**vlan** *vlan-id*] 例： デバイス# **show ipv6 mld snooping mrouter vlan 1**	VLAN インターフェイスで IPv6 MLD スヌーピングがイネーブルになっていることを確認します。

MLD 即時脱退のイネーブル化

MLDv1 即時脱退をイネーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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 mld snooping vlan** *vlan-id* **immediate-leave** 例：	VLAN インターフェイスで MLD 即時脱退をイネーブルにします。

	コマンドまたはアクション	目的
	デバイス(config)# **ipv6 mld snooping vlan 1 immediate-leave**	
ステップ 4	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show ipv6 mld snooping vlan** *vlan-id* 例： デバイス# **show ipv6 mld snooping vlan 1**	VLAN インターフェイス上で即時脱退がイネーブルになっていることを確認します。

MLD スヌーピング クエリーの設定

スイッチまたはVLANにMLDスヌーピング クエリの特性を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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 mld snooping robustness-variable** *value* 例： デバイス(config)# **ipv6 mld snooping robustness-variable 3**	（任意）スイッチが一般クエリーに応答しないリスナー（ポート）を削除する前に、送信されるクエリー数を設定します。指定できる範囲は 1 ～ 3 です。デフォルトは 2 です。
ステップ 4	**ipv6 mld snooping vlan** *vlan-id* **robustness-variable** *value* 例： デバイス(config)# **ipv6 mld snooping vlan 1 robustness-variable 3**	（任意）VLAN 単位でロバストネス変数を設定します。これにより、MLD レポート応答がない場合にマルチキャスト アドレスがエージング アウトされるまでに、MLD スヌーピングが送信する一般クエリー数が決定されます。指定できる範囲は 1 ～ 3 です。デフォルトは 0 です。0 に設定すると、使用

	コマンドまたはアクション	目的
		される数はグローバルな堅牢性変数の値になります。
ステップ 5	**ipv6 mld snooping last-listener-query-count** *count* 例： デバイス(config)# **ipv6 mld snooping last-listener-query-count 7**	（任意）MLD クライアントがエージング アウトされる前にスイッチが送信する MASQ 数を設定します。指定できる範囲は 1 ～ 7 です。デフォルトは 2 です。クエリーは 1 秒後に送信されます。
ステップ 6	**ipv6 mld snooping vlan** *vlan-id* **last-listener-query-count** *count* 例： デバイス(config)# **ipv6 mld snooping vlan 1 last-listener-query-count 7**	（任意）VLAN 単位でラスト リスナー クエリー カウントを設定します。この値はグローバルに設定された値を上書きします。指定できる範囲は1～7です。デフォルトは0です。0に設定すると、グローバルなカウント値が使用されます。クエリーは1秒後に送信されます。
ステップ 7	**ipv6 mld snooping last-listener-query-interval** *interval* 例： デバイス(config)# **ipv6 mld snooping last-listener-query-interval 2000**	（任意）スイッチが MASQ を送信したあと、マルチキャスト グループからポートを削除するまで待機する最大応答時間を設定します。指定できる範囲は、100 ～ 32,768 ミリ秒です。デフォルト値は 1000（1 秒）です。
ステップ 8	**ipv6 mld snooping vlan** *vlan-id* **last-listener-query-interval** *interval* 例： デバイス(config)# **ipv6 mld snooping vlan 1 last-listener-query-interval 2000**	（任意）VLAN 単位で last-listener クエリー インターバルを設定します。この値はグローバルに設定された値を上書きします。指定できる範囲は、0 ～ 32,768 ミリ秒です。デフォルトは 0 です。0 に設定すると、グローバルな最後のリスナー クエリー インターバルが使用されます。
ステップ 9	**ipv6 mld snooping tcn query solicit** 例： デバイス(config)# **ipv6 mld snooping tcn query solicit**	（任意）トポロジ変更通知（TCN）をイネーブルにします。これにより、VLAN は設定された数のクエリーに関する IPv6 マルチキャスト トラフィックすべてをフラッディングしてから、マルチキャスト データをマルチキャスト データの受信を要求するポートに対してのみ送信します。デフォルトでは、TCN はディセーブルに設定されています。
ステップ 10	**ipv6 mld snooping tcn flood query count** *count* 例： デバイス(config)# **ipv6 mld snooping tcn flood query count 5**	（任意）TCN がイネーブルの場合、送信される TCN クエリー数を指定します。指定できる範囲は 1 ～ 10 で、デフォルトは 2 です。
ステップ 11	**end**	特権 EXEC 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 12	**show ipv6 mld snooping querier** [**vlan** *vlan-id*] 例： `デバイス(config)# show ipv6 mld snooping querier vlan 1`	（任意）スイッチまたはVLANのMLDスヌーピング クエリア情報を確認します。

MLD リスナー メッセージ抑制のディセーブル化

デフォルトでは、MLD スヌーピング リスナー メッセージ抑制はイネーブルに設定されています。この機能がイネーブルの場合、スイッチはマルチキャスト ルータ クエリーごとに 1 つの MLD レポートのみを転送します。メッセージ抑制がディセーブルの場合は、複数のマルチキャスト ルータに MLD レポートが転送されます。

MLD リスナー メッセージ抑制をディセーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 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： `デバイス# 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	**no ipv6 mld snooping listener-message-suppression** 例： `デバイス(config)# no ipv6 mld snooping listener-message-suppression`	MLD メッセージ抑制をディセーブルにします。
ステップ 4	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ipv6 mld snooping** 例： `デバイス# show ipv6 mld snooping`	IPv6 MLD スヌーピング レポート抑制がディセーブルであることを確認します。

MLD スヌーピング情報の表示

ダイナミックに学習された、あるいはスタティックに設定されたルータ ポートおよびVLAN インターフェイスのMLDスヌーピング情報を表示できます。また、MLDスヌーピング用に設定された VLAN の IPv6 グループ アドレス マルチキャスト エントリを表示することもできます。

表 *2 : MLD* スヌーピング情報表示用のコマンド

コマンド	目的
show ipv6 mld snooping [**vlan** *vlan-id*]	スイッチのすべての VLAN または指定された VLAN の MLD スヌーピング設定情報を表示します。 （任意）個々のVLANに関する情報を表示するには、**vlan** *vlan-id* を入力します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show ipv6 mld snooping mrouter [**vlan** *vlan-id*]	ダイナミックに学習され、手動で設定されたマルチキャスト ルータ インターフェイスの情報を表示します。MLD スヌーピングをイネーブルにすると、スイッチはマルチキャスト ルータの接続先であるインターフェイスを自動的に学習します。これらのインターフェイスは動的に学習されます。 （任意）個々のVLANに関する情報を表示するには、**vlan** *vlan-id* を入力します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show ipv6 mld snooping querier [**vlan** *vlan-id*]	VLAN 内で直前に受信した MLD クエリー メッセージの IPv6 アドレスおよび着信ポートに関する情報を表示します。 （任意） **vlan** *vlan-id* を入力して、単一の VLAN 情報を表示します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show ipv6 mld snooping address [**vlan** *vlan-id*] [**count** | **dynamic** | **user**]	すべての IPv6 マルチキャスト アドレス情報あるいはスイッチまたはVLANの特定のIPv6マルチキャスト アドレス情報を表示します。 • **count** を入力して、スイッチまたは VLAN のグループ数を表示します。 • **dynamic** を入力して、スイッチまたはVLANのMLDスヌーピング学習済みグループ情報を表示します。 • **user** を入力して、スイッチまたは VLAN の MLD スヌーピングユーザ設定グループ情報を表示します。

コマンド	目的
show ipv6 mld snooping address vlan *vlan-id* [*ipv6-multicast-address*]	指定の VLAN および IPv6 マルチキャスト アドレスの MLD スヌーピングを表示します。

MLD スヌーピングの設定例

スタティックなマルチキャスト グループの設定：例

次に、IPv6 マルチキャスト グループをスタティックに設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# ipv6 mld snooping vlan 2 static FF12::3 interface gigabitethernet1/0/1
デバイス(config)# end
```

マルチキャスト ルータ ポートの設定：例

次に、VLAN 200 にマルチキャスト ルータ ポートを追加する例を示します。

```
デバイス# configure terminal
デバイス(config)# ipv6 mld snooping vlan 200 mrouter interface gigabitethernet
          0/2
デバイス(config)# exit
```

MLD 即時脱退のイネーブル化：例

次に、VLAN 130 で MLD 即時脱退をイネーブルにする例を示します。

```
デバイス# configure terminal
デバイス(config)# ipv6 mld snooping vlan 130 immediate-leave
デバイス(config)# exit
```

MLD スヌーピング クエリーの設定：例

次に、MLD スヌーピングのグローバルな堅牢性変数を 3 に設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# ipv6 mld snooping robustness-variable 3
デバイス(config)# exit
```

次に、VLAN の MLD スヌーピングの最後のリスナー クエリー カウントを 3 に設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# ipv6 mld snooping vlan 200 last-listener-query-count 3
デバイス(config)# exit
```

次に、MLD スヌーピングの最後のリスナー クエリー インターバル（最大応答時間）を 2000（2 秒）に設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# ipv6 mld snooping last-listener-query-interval 2000
デバイス(config)# exit
```

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』

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	リンク
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

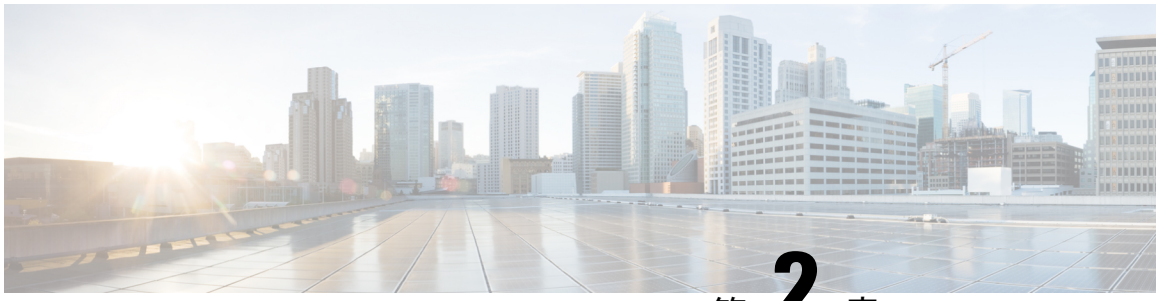
MLD スヌーピングに関する機能情報

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 : MLD* スヌーピングに関する機能情報

機能名	リリース	機能情報
MLD スヌーピング	Cisco IOS XE Everest 16.5.1a	MLD スヌーピングにより、スイッチで MLD パケットを調べ、パケットの内容に基づいて転送先を決定できます。



第 2 章

IPv6 ユニキャスト ルーティングの設定

IPv6 ユニキャスト ルーティングの設定について

この章では、スイッチに IPv6 ユニキャストルーティングを設定する方法について説明します。

（注） この章のすべての IPv6 機能を使用するには、スイッチまたはスタック マスターが Network Advantage ライセンスを実行している必要があります。Network Essentials ライセンスを実行しているスイッチは、IPv6 スタティック ルーティングと IPv6 用の RIP をサポートしています。Network Advantage ライセンスを実行しているスイッチは、IPv6 に対し OSPF、EIGRP および BGP をサポートしています。

IPv6 の概要

IPv4 ユーザーは IPv6 に移行することができ、エンドツーエンドのセキュリティ、Quality of Service（QoS）、およびグローバルに一意なアドレスのようなサービスを利用できます。IPv6 アドレス スペースによって、プライベート アドレスの必要性が低下し、ネットワーク エッジの境界ルータで Network Address Translation（NAT; ネットワーク アドレス変換）処理を行う必要性も低下します。

シスコの IPv6 の実装方法については、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html

IPv6 およびこの章のその他の機能については、

- 『*Cisco IOS IPv6 Configuration Library*』を参照してください。
- Cisco.com の [Search] フィールドを使用して、Cisco IOS ソフトウェア マニュアルを特定します。たとえば、スタティック ルートについての情報が必要な場合は、[Search] フィールドで *Implementing Static Routes for IPv6* と入力すると、スタティック ルートについて調べられます。

IPv6 アドレス

スイッチがサポートするのは、IPv6ユニキャストアドレスのみです。サイトローカルユニキャスト アドレスおよびマルチキャスト アドレスはサポートされません。

IPv6 の 128 ビット アドレスは、コロンで区切られた一連の 8 つの 16 進フィールド（n:n:n:n:n:n:n:n. の形式）で表されます。次に、IPv6 アドレスの例を示します。

2031:0000:130F:0000:0000:09C0:080F:130B

実装を容易にするために、各フィールドの先行ゼロは省略可能です。上記アドレスは、先行ゼロを省略した次のアドレスと同じです。

2031:0:130F:0:0:9C0:80F:130B

2 つのコロン（::）を使用して、ゼロが連続する 16 進フィールドを表すことができます。ただし、この短縮形を使用できるのは、各アドレス内で 1 回のみです。

2031:0:130F::09C0:080F:130B

IPv6 アドレス形式、アドレス タイプ、および IPv6 パケット ヘッダーの詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/xe-3e/ip6b-xe-3e-book.html を参照してください。

「Information About Implementing Basic Connectivity for IPv6」の章では、次の項の内容がスイッチに適用されます。

- IPv6 アドレス形式
- IPv6 アドレス タイプ：ユニキャスト
- IPv6 アドレス タイプ：マルチキャスト
- Ipv6 アドレス 出力表示
- 簡易 IPv6 パケット ヘッダー

サポート対象の IPv6 ユニキャスト ルーティング機能

ここでは、スイッチでサポートされている IPv6 プロトコル機能について説明します。

スイッチは、IPv6 の Routing Information Protocol（RIP）、および Open Shortest Path First（OSPF）バージョン 3 プロトコルによる IPv6 ルーティング機能を提供します。等コスト ルートは 16 個までサポートされ、IPv4 および IPv6 フレームを回線レートで同時に転送できます。

128 ビット幅のユニキャスト アドレス

スイッチは集約可能なグローバル ユニキャスト アドレスおよびリンク ローカル ユニキャスト アドレスをサポートします。サイト ローカル ユニキャスト アドレスはサポートされていません。

- 集約可能なグローバル ユニキャスト アドレスは、集約可能グローバル ユニキャスト プレフィックスの付いた IPv6 アドレスです。このアドレス構造を使用すると、ルーティング プレフィックスを厳格に集約することができ、グローバル ルーティング テーブル内のルーティング テーブル エントリ数が制限されます。これらのアドレスは、組織を経由して最終的にインターネット サービス プロバイダに至る集約リンク上で使用されます。

  これらのアドレスはグローバル ルーティング プレフィックス、サブネット ID、およびインターフェイス ID によって定義されます。現在のグローバル ユニキャスト アドレス割り当てには、バイナリ値 001（2000::/3）で開始するアドレス範囲が使用されます。プレフィックスが 2000::/3（001）～ E000::/3（111）のアドレスには、Extended Unique Identifier（EUI）64 フォーマットの 64 ビット インターフェイス ID を設定する必要があります。

- リンク ローカル ユニキャスト アドレスをすべてのインターフェイスに自動的に設定するには、修飾 EUI フォーマット内で、リンク ローカル プレフィックス FE80::/10（1111 1110 10）およびインターフェイスID を使用します。ネイバー探索プロトコル（NDP）およびステートレス自動設定プロセスでは、リンクローカルアドレスが使用されます。ローカル リンク上のノードは、リンクローカルアドレスを使用します。通信する場合に、グローバルに一意なアドレスは不要です。IPv6 ルータは、リンクローカルの送信元または宛先アドレスを持つパケットをその他のリンクに転送しません。

詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library* 』の「Implementing IPv6 Addressing and Basic Connectivity」の章にある IPv6 ユニキャスト アドレスに関する項を参照してください。

IPv6 の DNS

IPv6 は、ドメイン ネーム システム（DNS）のレコード タイプを、DNS 名前/アドレスおよびアドレス/名前の検索プロセスでサポートします。DNS AAAA リソース レコード タイプは IPv6 アドレスをサポートし、IPv4 の A アドレス レコードと同等です。スイッチは IPv4 および IPv6 の DNS 解決をサポートします。

IPv6 ユニキャストのパス MTU ディスカバリ

スイッチはシステム最大伝送単位（MTU）の IPv6 ノードへのアドバタイズおよびパス MTU ディスカバリをサポートします。パス MTU ディスカバリを使用すると、ホストは指定されたデータ パスを通るすべてのリンクの MTU サイズを動的に検出して、サイズに合せて調整できます。IPv6 では、パスを通るリンクの MTU サイズが小さくてパケット サイズに対応できない場合、パケットの送信元がフラグメンテーションを処理します。

ICMPv6

IPv6 のインターネット制御メッセージ プロトコル（ICMP）は、ICMP 宛先到達不能メッセージなどのエラー メッセージを生成して、処理中に発生したエラーや、その他の診断機能を報告

します。IPv6 では、ネイバー探索プロトコルおよびパス MTU ディスカバリに ICMP パケットも使用されます。

ネイバー探索

スイッチは、IPv6 対応の NDP、ICMPv6 の最上部で稼働するプロトコル、および NDP をサポートしない IPv6 ステーション対応のスタティック ネイバー エントリをサポートします。IPv6 ネイバー探索プロセスは ICMP メッセージおよび送信請求ノード マルチキャスト アドレスを使用して、同じネットワーク（ローカル リンク）上のネイバーのリンク層アドレスを判別し、ネイバーに到達できるかどうかを確認し、近接ルータを追跡します。

スイッチは、マスク長が 64 未満のルートに対して ICMPv6 リダイレクトをサポートしています。マスク長が 64 ビットを超えるホスト ルートまたは集約ルートでは、ICMP リダイレクトがサポートされません。

ネイバー探索スロットリングにより、IPv6 パケットをルーティングするためにネクスト ホップ転送情報を取得するプロセス中に、スイッチ CPU に不必要な負荷がかかりません。IPv6 パケットのネクストホップがスイッチによってアクティブに解決しようとしている同じネイバーである場合は、そのようなパケットが追加されると、スイッチはそのパケットをドロップします。このドロップにより、CPU に余分な負荷がかからないようになります。

デフォルト ルータ プリファレンス

スイッチは、ルータのアドバタイズメント メッセージの拡張機能である、IPv6 Default Router Prefernce（DRP）をサポートします。DRP では、特にホストがマルチホーム構成されていて、ルータが異なるリンク上にある場合に、ホストが適切なルータを選択する機能が向上しました。スイッチは、Route Information Option（RFC 4191）をサポートしません。

IPv6 ホストは、オフリンク宛先へのトラフィック用にルータを選択する、デフォルト ルータ リストを維持します。次に、宛先用に選択されたルータは、宛先キャッシュに格納されます。IPv6 NDP では、到達可能であるルータまたは到達可能性の高いルータが、到達可能性が不明または低いルータよりも優先されます。NDPは、到達可能または到達できる可能性の高いルータとして、常に同じルータを選択するか、またはルータ リストを循環して選択できます。DRP を使用することにより、両方ともが到達可能または到達できる可能性の高い2台のルータの一方を他方に対して優先させるよう IPv6 ホストを設定することができます。

DRP for IPv6 の設定については、「*DRP* の設定」を参照してください。

DRP for IPv6 の詳細情報については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』を参照してください。

IPv6 のステートレス自動設定および重複アドレス検出

スイッチではステートレス自動設定が使用されているため、ホストやモバイル IP アドレスの管理のような、リンク、サブネット、およびサイトアドレス指定の変更を管理することができます。ホストは独自のリンクローカルアドレスを自動的に設定します。起動元ノードはルータに送信請求を送信して、インターフェイス設定をアドバタイズするようルータに要求します。

自動設定および重複アドレス検出の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv6 アプリケーション

スイッチは、次のアプリケーションについて IPv6 をサポートします。

- ping、Traceroute、Telnet、および Trivial File Transfer Protocol（TFTP）
- IPv6 トランスポートによるセキュア シェル（SSH）
- IPv6 トランスポートによる HTTP サーバー アクセス
- IPv4 トランスポートによる AAAA の DNS レゾルバ
- IPv6 アドレスの Cisco Discovery Protocol（CDP）サポート

これらのアプリケーションの管理に関する詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』を参照してください。

DHCP for IPv6 アドレスの割り当て

DHCPv6 を使用すると、DHCP サーバーは IPv6 ネットワーク アドレスなどの設定パラメータを IPv6 クライアントに渡すことができます。このアドレス割り当て機能により、ホストが接続するネットワークに基づいて、適切なプレフィックス内での重複しないアドレス割り当てが管理されます。アドレスは、1つまたは複数のプレフィックス プールから割り当てることができます。デフォルトのドメインおよびDNS ネーム サーバー アドレスなど、その他のオプションは、クライアントに戻すことができます。アドレス プールは、特定のインターフェイス、複数のインターフェイス上で使用する場合に割り当てられます。または、サーバーが自動的に適切なプールを検出できます。

DHCP for IPv6 の設定については、「*DHCP for IPv6* アドレス割り当ての設定」のセクションを参照してください。

DHCPv6 クライアント、サーバー、またはリレーエージェント機能の設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』を参照してください。

IPv6 のスタティック ルート

スタティック ルートは手動で設定され、2つのネットワーキング デバイス間のルートを明示的に定義します。スタティック ルートが有効なのは、外部ネットワークへのパスが1つしかない小規模ネットワークの場合、または大規模ネットワークで特定のトラフィック タイプにセキュリティを設定する場合です。

IPv6 のスタティック ルーティングの設定（CLI）

IPv6 用のスタティックルートの設定については、「*IPv6* 用のスタティックルーティングの設定」を参照してください。

スタティック ルートの詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing Static Routes for IPv6」の章を参照してください。

IPv6 のポリシーベース ルーティング

ポリシーベース ルーティング（PBR）は、トラフィック フローに定義ポリシーを設定し、ルートにおけるルーティング プロトコルへの依存度を軽くして、パケットのルーティングを柔軟に

行えるようにします。したがって、PBR は、ルーティング プロトコルで提供される既存のメカニズムを拡張および補完することにより、ルーティングの制御を強化します。PBR を使用すると、IPv6 precedence を設定できます。単純なポリシーでは、これらのタスクのいずれかを使用し、複雑なポリシーでは、これらすべてのタスクを使用できます。高コストリンク上のプライオリティ トラフィックなど、特定のトラフィックのパスを指定することもできます。

PBR for IPv6 は、転送される IPv6 パケットおよび送信される IPv6 パケットの両方に適用できます。転送されるパケットの場合、PBR for IPv6 は、次の転送パスでサポートされる IPv6 入力インターフェイス機能として実装されます。

- プロセス
- シスコ エクスプレス フォワーディング（旧称 CEF）
- 分散型シスコ エクスプレス フォワーディング

ポリシーは、IPv6アドレス、ポート番号、プロトコル、またはパケットのサイズに基づいて作成できます。

PBR を使用すると、次の処理を実行できます。

- 拡張アクセス リスト基準に基づいてトラフィックを分類する。リストにアクセスし、次に一致基準を設定します。
- 差別化されたサービス クラスを有効にする機能をネットワークに与える IPv6 precedence ビットを設定する。
- 特定のトラフィック エンジニアリング パスにパケットをルーティングする。ネットワークを介して特定の Quality of Service（QoS）を得るためにパケットをルーティングする必要がある場合があります。

PBR を使用すると、ネットワークのエッジでパケットを分類およびマーキングできます。PBR では、precedence 値を設定することにより、パケットをマーキングします。precedence 値は、ネットワーク コアにあるデバイスが適切な QoS をパケットに適用するために直接使用でき、これにより、パケットの分類がネットワーク エッジで維持されます。

PBR for IPv6 の有効化については、「ローカル *PBR for IPv6* の有効化」を参照してください。

インターフェイスの IPv6 PBR の有効化については、「インターフェイスでの *IPv6 PBR* の有効化」を参照してください。

RIP for IPv6

IPv6 の Routing Information Protocol（RIP）は、ルーティング メトリックとしてホップ カウントを使用するディスタンスベクトル プロトコルです。IPv6 アドレスおよびプレフィックスのサポート、すべての RIP ルータを含むマルチキャスト グループ アドレス FF02::9 を RIP アップデート メッセージの宛先アドレスとして使用する機能などがあります。

IPv6 の RIP の設定については、「*IPv6* の *RIP* の設定」を参照してください。

IPv6 の RIP の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing RIP for IPv6」の章を参照してください。

OSPF for IPv6

スイッチは、IP のリンクステート プロトコルの 1 つである、IPv6 の Open Shortest Path First（OSPF）をサポートしています。

IPv6 用の OSPF の設定については、「*IPv6* 用の *OSPF* の設定」を参照してください。

詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』を参照してください。

EIGRP IPv6

スイッチは、IPv6 の Enhanced Interior Gateway Routing Protocol（EIGRP）をサポートしています。IPv6 の EIGRP は稼働するインターフェイス上で設定されるため、グローバルな IPv6 アドレスは不要です。Network Essentials を実行しているスイッチは EIGRPv6 スタブルーティングのみをサポートします。

EIGRP IPv6 インスタンスでは、実行する前に暗示的または明示的なルータ ID が必要です。暗示的なルータ ID はローカルの IPv6 アドレスを基にして作成されるため、すべての IPv6 ノードには常に使用可能なルータ ID があります。ただし、EIGRP IPv6 は IPv6 ノードのみが含まれるネットワークで稼働するため、使用可能な IPv6 ルータ ID がない場合があります。

IPv6 用の EIGRP の設定については、「*IPv6* 用の *EIGRP* の設定」を参照してください。

IPv6 用の EIGRP の詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』を参照してください。

EIGRPv6 スタブ ルーティング

EIGRPv6 スタブ ルーティング機能は、エンド ユーザーの近くにルーテッド トラフィックを移動することでリソースの利用率を低減させます。

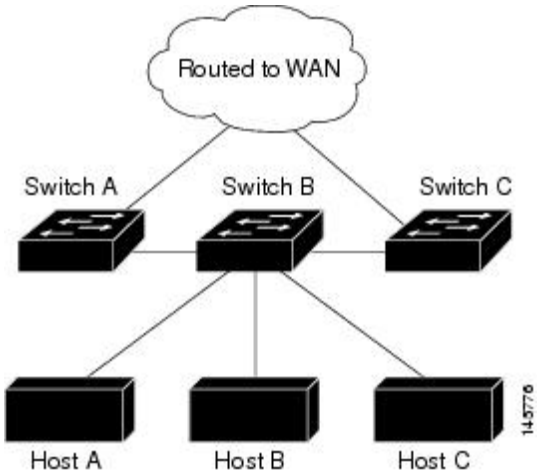
EIGRPv6 スタブ ルーティングを使用するネットワークでは、ユーザーに対する IPv6 トラフィックの唯一の許容ルートは、EIGRPv6 スタブ ルーティングを設定しているスイッチ経由のみです。スイッチは、ユーザーインターフェイスとして設定されているインターフェイスまたは他のデバイスに接続されているインターフェイスにルーテッド トラフィックを送信します。

EIGRPv6 スタブ ルーティングを使用しているときは、EIGRPv6 を使用してスイッチだけをスタブとして設定するように、ディストリビューションルータおよびリモートルータを設定する必要があります。指定したルートだけがスイッチから伝播されます。スイッチは、サマリー、接続ルート、およびルーティング アップデートに対するすべてのクエリーに応答します。

スタブ ルータの状態を通知するパケットを受信した隣接ルータは、ルートについてはスタブ ルータに照会しません。また、スタブ ピアを持つルータは、そのピアについては照会しません。スタブ ルータは、ディストリビューション ルータを使用して適切なアップデートをすべてのピアに送信します。

次の図では、スイッチ B は EIGRPv6 スタブ ルータとして設定されています。スイッチ A および C は残りの WAN に接続されています。スイッチ B は、接続ルート、スタティック ルート、再配布ルート、およびサマリー ルートをスイッチ A と C にアドバタイズします。 スイッチ B は、スイッチ A から学習したルートをアドバタイズしません（逆の場合も同様です）。

図 *1 : EIGRP* スタブ ルータ設定



EIGRPv6 スタブ ルーティングの詳細については、『*Cisco IOS IP Configuration Guide, Volume 2 of 3: Routing Protocols, Release 12.4*』の「Implementing EIGRP for IPv6」を参照してください。

SNMP and Syslog Over IPv6

IPv4 と IPv6 の両方をサポートするには、IPv6 のネットワーク管理で IPv4 および IPv6 のトランスポートが必要になります。Syslog over IPv6 は、このトランスポートのアドレス データ タイプをサポートします。

Simple Network Management Protocol (SNMP) と syslog over IPv6 は、次の機能を提供します。

- IPv4 と IPv6 両方のサポート
- SNMP に対する IPv6 トランスポート、および SNMP 変更による IPv6 ホストのトラップのサポート
- IPv6 アドレス指定をサポートするための SNMP および syslog に関連する MIB
- IPv6 ホストをトラップ レシーバとして設定

Over IPv6 をサポートするため、SNMP は既存の IP トランスポート マッピングを変更して、IPv4 と IPv6 を同時にサポートします。次の SNMP 動作は、IPv6 トランスポート管理をサポートします。

- デフォルト設定のユーザー データグラム プロトコル（UDP）SNMP ソケットを開く
- *SR_IPV6_TRANSPORT* と呼ばれる新しいトランスポート メカニズムを提供
- IPv6 トランスポートによる SNMP 通知の送信
- IPv6 トランスポートの SNMP 名のアクセス リストのサポート
- IPv6 トランスポートを使用した SNMP プロキシ転送のサポート
- SNMP マネージャ機能と IPv6 トランスポートの連動確認

設定手順を含む、SNMP over IPv6 については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」の章を参照してください。

設定手順を含む、syslog over IPv6 については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

HTTP(S) Over IPv6

HTTP クライアントは要求を IPv4 HTTP サーバーと IPv6 HTTP サーバーの両方に送信し、これらのサーバーは IPv4 HTTP クライアントと IPv6 HTTP クライアントの両方からの要求に応答します。IPv6 アドレスを含む URL は、16 ビット値をコロンで区切った 16 進数で指定する必要があります。

受信ソケット コールは、IPv4 アドレス ファミリまたは IPv6 アドレス ファミリを選択します。受信ソケットは、IPv4 ソケットまたは IPv6 ソケットのいずれかです。リスニング ソケットは、接続を示す IPvv4 と IPv6 の両方の信号を待ち受け続けます。IPv6 リスニング ソケットは、IPv6 ワイルドカード アドレスにバインドされています。

基本 TCP/IP スタックは、デュアル スタック環境をサポートします。HTTP には、TCP/IP スタック、およびネットワーク層相互作用を処理するためのソケットが必要です。

HTTP 接続を確立するには、基本ネットワーク接続（**ping**）がクライアントとサーバーホストとの間に存在する必要があります。

詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」の章を参照してください。

サポートされていない IPv6 ユニキャスト ルーティング機能

スイッチは、次の IPv6 機能をサポートしません。

- サイトローカルアドレス宛ての IPv6 パケット
- IPv4/IPv6 や IPv6/IPv4 などのトンネリング プロトコル
- IPv4/IPv6 または IPv6/IPv4 トンネリング プロトコルをサポートするトンネル エンドポイントとしてのスイッチ
- IPv6 Web Cache Communication Protocol（WCCP）

IPv6 機能の制限

スイッチでは IPv6 はハードウェアに実装されるため、ハードウェア メモリ内の IPv6 圧縮アドレスによる制限がいくつか発生します。これらのハードウェア制限により、機能の一部が失われて、制限されます。

機能の制限は次のとおりです。

- スイッチはハードウェアで SNAP カプセル化 IPv6 パケットを転送できません。これらはソフトウェアで転送されます。

- スイッチはソースルート IPv6 パケットに関する QoS 分類をハードウェアで適用できません。

IPv6 とスイッチ スタック

スイッチにより、スタック全体で IPv6 転送がサポートされ、スタック マスターで IPv6 ホスト機能がサポートされます。スタック マスターは IPv6 ユニキャスト ルーティング プロトコルを実行してルーティング テーブルを計算します。スタック メンバー スイッチはテーブルを受信して、転送用にハードウェア IPv6 ルートを作成します。スタック マスターも、すべての IPv6 アプリケーションを実行します。

新しいスイッチがスタック マスターになる場合、新しいマスターは IPv6 ルーティング テーブルを再計算してこれをメンバー スイッチに配布します。新しいスタック マスターが選択中およびリセット中の間には、スイッチ スタックによる IPv6 パケットの転送は行われません。スタック MAC アドレスが変更され、これによって IPv6 アドレスが変更されます。**ipv6 address** *ipv6-prefix/prefix length* **eui-64** インターフェイス コンフィギュレーション コマンドを使用して、拡張固有識別子（EUI）でスタック IPv6 アドレスを指定する場合、アドレスは、インターフェイス MAC アドレスに基づきます。「*IPv6* アドレッシングの設定と *IPv6* ルーティングの有効化」を参照してください。

スタック上で永続的な MAC アドレスを設定し、スタック マスターが変更された場合、スタック MAC アドレスは、約 4 分間、変更されません。

IPv6 スタック マスターおよびメンバーの機能は次のとおりです。

- スタック マスター
  - IPv6 ルーティングプロトコルの実行
  - ルーティング テーブルの生成
  - 分散型 Cisco Express Forwarding for IPv6 を使用するスタックメンバにルーティングテーブルを配布します
  - IPv6 ホスト機能および IPv6 アプリケーションの実行
- スタックメンバ
  - スタックマスターから Cisco Express Forwarding for IPv6 ルーティングテーブルを受信します
  - ハードウェアへのルートのプログラミング

（注） IPv6 パケットに例外（IPv6 オプション）がなく、スタック内のスイッチでハードウェア リソースが不足していない場合、IPv6 パケットがスタック全体にわたってハードウェアでルーティングされます。

• マスター再選択時に Cisco Express Forwarding for IPv6 テーブルをフラッシュします

IPv6 のデフォルト設定

表 *4 : IPv6* のデフォルト設定

機能	デフォルト設定
SDM テンプレート	デフォルトは拡張テンプレート
IPv6 ルーティング	すべてのインターフェイスでグローバルに無効
IPv6 用 Cisco Express Forwarding または IPv6 用 distributed Cisco Express Forwarding（dCEF; 分散型シスコ エクスプレス フォワーディング）	無効（IPv4 Cisco Express Forwarding および distributed Cisco Express Forwarding（dCEF; 分散型シスコ エクスプレス フォワーディング）はデフォルトでは有効） （注） IPv6 ルーティングを有効にすると、IPv6 用 Cisco Express Forwarding および IPv6 用 distributed Cisco Express Forwarding（dCEF; 分散型シスコ エクスプレス フォワーディング）は自動的に有効になります。
IPv6 アドレス	未設定

IPv6 ユニキャストルーティングの設定方法

ここでは、IPv6ユニキャストルーティングに関して使用できるさまざまな設定オプションを示します。

IPv6 アドレッシングの設定と IPv6 ルーティングの有効化

ここでは、IPv6 アドレスを各レイヤ 3 インターフェイスに割り当てて、IPv6 トラフィックをスイッチ上でグローバル転送する方法を説明します。

スイッチ上の IPv6 を設定する前に、次の注意事項に従ってください。

- スイッチでは、この章で説明されたすべての機能がサポートされるわけではありません。「サポートされていない IPv6 ユニキャスト ルーティング機能」を参照してください。
- **ipv6 address** インターフェイス コンフィギュレーション コマンドでは、16 ビット値を使用したコロン区切りの 16 進形式で指定したアドレスで *ipv6-address* 変数および *ipv6-prefix* 変数を入力する必要があります。*prefix-length* 変数（スラッシュ（/）で始まる）は、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。

インターフェイス上の IPv6 トラフィックを転送するには、そのインターフェイス上でグローバル IPv6 アドレスを設定する必要があります。インターフェイス上で IPv6 アドレスを設定すると、リンクローカルアドレスの設定、およびそのインターフェイスに対する IPv6 のアクティブ化が自動的に行われます。設定されたインターフェイスは、次に示す、該当リンクの必須マルチキャスト グループに自動的に参加します。

- インターフェイスに割り当てられた各ユニキャストアドレスの送信要求ノードマルチキャスト グループ FF02:0:0:0:0:1:ff00::/104（このアドレスはネイバー探索プロセスで使用される）
- 全ノード向けリンクローカルマルチキャストグループ FF02::1
- 全ルータ向けリンクローカルマルチキャストグループ FF02::2

IPv6 アドレスをインターフェイスから削除するには、 **no ipv6 address** *ipv6-prefix/prefix length* **eui-64** または **no ipv6 address** *ipv6-address* **link-local** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスから手動で設定したすべての IPv6 アドレスを削除するには、**no ipv6 address** インターフェイス コンフィギュレーション コマンドを引数なしで使用します。IPv6 アドレスが明確に設定されていないインターフェイスで IPv6 処理を無効にするには、**no ipv6 enable** インターフェイス コンフィギュレーション コマンドを使用します。IPv6 ルーティングをグローバルに無効にするには、**no ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用します。

IPv6 ルーティングの設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing Addressing and Basic Connectivity for IPv6」の章を参照してください。

IPv6 アドレスをレイヤ 3 インターフェイスに割り当て、IPv6 ルーティングを有効にするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** デバイス> **enable**	特権 EXEC モードを有効にします。 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：** デバイス# **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	**sdm prefer access** **例：**	スイッチをアクセステンプレートに設定します。

	コマンドまたはアクション	目的
	デバイス(config)# **sdm prefer access**	
ステップ 4	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**reload** 例： デバイス# **reload**	オペレーティング システムをリロードします。
ステップ 6	**configure terminal** 例： デバイス# **configure terminal**	スイッチのリロード後、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 7	**interface** *interface-id* 例： デバイス(config)# **interface gigabitethernet 1/0/1**	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、設定するレイヤ3インターフェイスを指定します。インターフェイスは物理インターフェイス、スイッチ仮想インターフェイス（SVI）、またはレイヤ 3 EtherChannel に設定できます。
ステップ 8	**no switchport** 例： デバイス(config-if)# **no switchport**	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。
ステップ 9	次のいずれかを使用します。 • **ipv6 address** *ipv6-prefix/prefix length* **eui-64** • **ipv6 address** *ipv6-address/prefix length* • **ipv6 address** *ipv6-address* **link-local** • **ipv6 enable** • **ipv6 address** *WORD* • **ipv6 address** *autoconfig* • **ipv6 address** *[dhcp]* 例： デバイス(config-if)# **ipv6 address 2001:0DB8:c18:1::/64 eui 64**	• IPv6 アドレスの下位 64 ビットの拡張固有識別子（EUI）を使用して、グローバル IPv6 アドレスを指定します。ネットワーク プレフィックスだけを指定します。最終の 64 ビットは、スイッチの MAC アドレスから自動的に計算されます。これにより、インターフェイス上で IPv6 処理が有効になります。 • インターフェイスの IPv6 アドレスを手動で設定します。 • インターフェイスで IPv6 が有効な場合に自動設定されるリンクローカルアドレスでなく、イ

	コマンドまたはアクション	目的
	デバイス(config-if)# **ipv6 address 2001:0DB8:c18:1::/64** デバイス(config-if)# **ipv6 address 2001:0DB8:c18:1:: link-local** デバイス(config-if)# **ipv6 enable**	ンターフェイス上の特定のリンクローカルなアドレスを使用するように指定します。このコマンドにより、インターフェイス上で IPv6 処理が有効になります。 • インターフェイスに IPv6 リンクローカルアドレスを自動設定し、インターフェイスでの IPv6 処理を有効にします。リンクローカルアドレスを使用できるのは、同じリンク上のノードと通信する場合だけです。
ステップ 10	**exit** **例：** デバイス(config-if)# **exit**	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 11	**ip routing** **例：** デバイス(config)# **ip routing**	スイッチ上で IP ルーティングをイネーブルにします。
ステップ 12	**ipv6 unicast-routing** **例：** デバイス(config)# **ipv6 unicast-routing**	IPv6 ユニキャスト データ パケットの転送を有効にします。
ステップ 13	**end** **例：** デバイス(config)# **end**	特権 EXEC モードに戻ります。
ステップ 14	**show ipv6 interface** *interface-id* **例：** デバイス# **show ipv6 interface gigabitethernet 1/0/1**	入力を確認します。
ステップ 15	**copy running-config startup-config** **例：** デバイス# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IPv4 および IPv6 プロトコル スタックの設定

IPv4 と IPv6 の両方をサポートし、IPv6 ルーティングが有効になるようにレイヤ 3 インターフェイスを設定するには、次の手順を実行します。

（注） IPv6 アドレスが設定されていないインターフェイスで IPv6 処理を無効にするには、**no ipv6 enable** インターフェイス コンフィギュレーション コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip routing**
4. **ipv6 unicast-routing**
5. **interface** *interface-id*
6. **no switchport**
7. **ip address** *ip-address mask* [**secondary**]
8. 次のいずれかを使用します。
   - **ipv6 address** *ipv6-prefix/prefix length* **eui-64**
   - **ipv6 address** *ipv6-address/prefix length*
   - **ipv6 address** *ipv6-address* **link-local**
   - **ipv6 enable**
   - **ipv6 address** *WORD*
   - **ipv6 address** *autoconfig*
   - **ipv6 address** *[dhcp]*
9. **end**
10. 次のいずれかを使用します。
    - **show interface** *interface-id*
    - **show ip interface** *interface-id*
    - **show ipv6 interface** *interface-id*
11. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `デバイス# 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	**ip routing** 例： `デバイス(config)# ip routing`	スイッチ上でルーティングを有効にします。
ステップ 4	**ipv6 unicast-routing** 例： `デバイス(config)# ipv6 unicast-routing`	スイッチ上で IPv6 データ パケットの転送を有効にします。
ステップ 5	**interface** *interface-id* 例： `デバイス(config)# interface gigabitethernet 1/0/1`	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、設定するレイヤ 3 インターフェイスを指定します。
ステップ 6	**no switchport** 例： `デバイス(config-if)# no switchport`	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。
ステップ 7	**ip address** *ip-address mask* [**secondary**] 例： `デバイス(config-if)# ip address 10.1.2.3 255.255.255`	インターフェイスのプライマリまたはセカンダリ IPv4 アドレスを指定します。
ステップ 8	次のいずれかを使用します。 • **ipv6 address** *ipv6-prefix/prefix length* **eui-64** • **ipv6 address** *ipv6-address/prefix length* • **ipv6 address** *ipv6-address* **link-local** • **ipv6 enable** • **ipv6 address** *WORD* • **ipv6 address** *autoconfig* • **ipv6 address** *[dhcp]*	• グローバル IPv6 アドレスを指定します。ネットワーク プレフィックスだけを指定します。最終の 64 ビットは、スイッチの MAC アドレスから自動的に計算されます。 • インターフェイスで IPv6 が有効な場合に自動設定されるリンクローカルアドレスでなく、インターフェイス上のリンクローカルアドレスを使用するように指定します。 • インターフェイスに IPv6 リンクローカルアドレスを自動設定し、インターフェイスでの IPv6

	コマンドまたはアクション	目的
		処理を有効にします。リンクローカルアドレスを使用できるのは、同じリンク上のノードと通信する場合だけです。 （注） インターフェイスから手動で設定したすべての IPv6 アドレスを削除するには、**no ipv6 address** インターフェイス コンフィギュレーション コマンドを引数なしで使用します。
ステップ 9	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。
ステップ 10	次のいずれかを使用します。 • **show interface** *interface-id* • **show ip interface** *interface-id* • **show ipv6 interface** *interface-id*	入力を確認します。
ステップ 11	**copy running-config startup-config** 例： `デバイス# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト ルータ プリファレンス（DRP）の設定

ルータアドバタイズメント（RA）メッセージは、**ipv6 nd router-preference** インターフェイス コンフィギュレーション コマンドによって設定されるデフォルト ルータ プリファレンス（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 はプリファレンス「中」とともに送信されます。

リンク上の 2 つのルータが等価ではあっても、等コストではないルーティングを提供する可能性がある場合、およびポリシーでホストがいずれかのルータを選択するよう指示された場合は、DRP が有効です。

IPv6 の DRP の設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addresses and Basic Connectivity」の章を参照してください。

インターフェイス上のルータの DRP を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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** *interface-id* 例： デバイス(config)# **interface gigabitethernet 1/0/1**	インターフェイス コンフィギュレーション モードを開始して、DRP を指定するレイヤ 3 インターフェイスを特定します。
ステップ 4	**ipv6 nd router-preference** {**high** | **medium** | **low**} 例： デバイス(config-if)# **ipv6 nd router-preference medium**	スイッチ インターフェイス上のルータに DRP を指定します。
ステップ 5	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show ipv6 interface** 例： デバイス# **show ipv6 interface**	設定を確認します。
ステップ 7	**copy running-config startup-config** 例： デバイス# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IPv6 ICMP レート制限の設定

ICMP レート制限はデフォルトで有効です。エラー メッセージのデフォルト間隔は 100 ミリ秒、デフォルト バケット サイズ（バケットに格納される最大トークン数）は 10 です。

ICMP のレート制限パラメータを変更するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 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： `デバイス# 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 icmp error-interval** *interval* [*bucketsize*] 例： `デバイス(config)# ipv6 icmp error-interval 50 20`	IPv6 ICMP エラー メッセージの間隔とバケット サイズを設定します。 • *interval*：バケットに追加されるトークンの間隔（ミリ秒）。指定できる範囲は 0 ～ 2147483647 ミリ秒です。 • *bucketsize*：（任意）バケットに格納される最大トークン数。指定できる範囲は 1 ～ 200 です。
ステップ 4	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ipv6 interface** [*interface-id*] 例： `デバイス# show ipv6 interface gigabitethernet 1/0/1`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例：	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	デバイス# **copy running-config startup-config**	

IPv6 用のシスコ エクスプレス フォワーディングおよび分散型シスコ エクスプレス フォワーディングの設定

シスコ エクスプレス フォワーディングは、ネットワークパフォーマンスを最適化するためのレイヤ 3 IP スイッチングテクノロジーです。シスコ エクスプレス フォワーディングには高度な IP 検索および転送アルゴリズムが実装されているため、レイヤ 3 スイッチングのパフォーマンスを最大化できます。高速スイッチング ルート キャッシュよりも CPU にかかる負担が少ないため、CEF はより多くの CPU 処理能力をパケット転送に振り分けることができます。スイッチスタックでは、ハードウェアによって分散型シスコ エクスプレス フォワーディングが使用されます。IPv4 用のシスコ エクスプレス フォワーディングおよび分散型シスコ エクスプレス フォワーディングはデフォルトで有効になっています。IPv6 用のシスコ エクスプレス フォワーディングおよび分散型シスコ エクスプレス フォワーディングはデフォルトでは無効になっていますが、IPv6 ルーティングを設定すると自動的に有効になります。

IPv6 ルーティングの設定を解除すると IPv6 用のシスコ エクスプレス フォワーディングおよび分散型シスコ エクスプレス フォワーディングは自動的に無効になります。IPv6 用のシスコ エクスプレス フォワーディングおよび分散型シスコ エクスプレス フォワーディングを設定で無効にすることはできません。IPv6 の状態を確認するには、**show ipv6 cef**特権 EXEC コマンドを入力します。

IPv6 ユニキャストパケットをルーティングするには、最初に **ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して、IPv6 ユニキャストパケットの転送をグローバルに設定してから、**ipv6 address** インターフェイス コンフィギュレーション コマンドを使用して、特定のインターフェイスに IPv6 アドレスおよび IPv6 処理を設定する必要があります。

シスコ エクスプレス フォワーディングおよび分散型シスコ エクスプレス フォワーディングの設定の詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』を参照してください。

IPv6 のスタティック ルーティングの設定

スタティック IPv6 ルーティングの設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing Static Routes for IPv6」の章を参照してください。

スタティック IPv6 ルーティングを設定するには、次の手順を実行します。

始める前に

ip routing グローバル コンフィギュレーション コマンドを使用してルーティングを有効にし、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの

転送を有効にします。また、インターフェイスに IPv6 アドレスを設定して少なくとも 1 つのレイヤ 3 インターフェイス上で IPv6 を有効にする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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 route** *ipv6-prefix/prefix length* {*ipv6-address* | *interface-id* [*ipv6-address*]} [*administrative distance*] 例： デバイス(config)# **ipv6 route 2001:0DB8::/32 gigabitethernet2/0/1 130**	スタティック IPv6 ルートを設定します。 • *ipv6-prefix*：スタティック ルートの宛先となる IPv6 ネットワーク。スタティック ホスト ルートを設定する場合は、ホスト名も設定できます。 • */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。 • *ipv6-address*：指定したネットワークに到達するために使用可能なネクスト ホップの IPv6 アドレス。ネクスト ホップの IPv6 アドレスを直接接続する必要はありません。再帰処理が実行されて、直接接続されたネクスト ホップの IPv6 アドレスが検出されます。このアドレスは RFC 2373 に記載された形式（16 ビット値を使用したコロン区切りの 16 進表記で指定）で設定する必要があります。 • *interface-id*：Point-To-Point（ポイントツーポイント）インターフェイスおよびブロードキャスト インターフェイスからのダイレクト スタティック ルートを指定します。ポイントツーポイント インターフェイスの場合、ネクスト ホップの IPv6 アドレスを指定する必要はありません。ブロードキャスト インターフェイスの場合

	コマンドまたはアクション	目的
		は、常にネクストホップの IPv6 アドレスを指定するか、または指定したプレフィックスをリンクに割り当てて、リンクローカルアドレスをネクストホップとして指定する必要があります。パケットの送信先となるネクストホップの IPv6 アドレスを指定することもできます。 （注） リンクローカルアドレスをネクストホップとして使用する場合は、*interface-id* を指定する必要があります（リンクローカルのネクストホップを隣接ルータに設定する必要もあります）。 • *administrative distance*：（任意）アドミニストレーティブ ディスタンス。指定できる範囲は 1 ～ 254 です。デフォルト値は 1 で、この場合、接続されたルートを除くその他のどのルートタイプよりも、スタティック ルートが優先します。フローティング スタティック ルートを設定する場合は、ダイナミック ルーティング プロトコルよりも大きなアドミニストレーティブ ディスタンスを使用します。
ステップ 4	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。

ステップ 5	次のいずれかを使用します。
	• **show ipv6 static** [*ipv6-address* | *ipv6-prefix/prefix length*] [**interface** *interface-id*] [**detail**]][**recursive**] [**detail**]
	• **show ipv6 route static** [*updated*]
	例：
	`デバイス# show ipv6 static 2001:0DB8::/32 interface gigabitethernet2/0/1`
	
	または
	`デバイス# show ipv6 route static`
		IPv6 ルーティング テーブルの内容を表示して、設定を確認します。
		• **interface** *interface-id*：（任意）出力インターフェイスとして指定されたインターフェイスを含むスタティック ルートのみを表示します。
		• **recursive**：（任意）再帰スタティック ルートのみを表示します。**recursive** キーワードは **interface** キーワードと相互に排他的です。ただし、コマンド構文に IPv6 プレフィックスが指定されているかどうかに関係なく、使用できます。
		• **detail**：（任意）次に示す追加情報を表示します。

	コマンドまたはアクション	目的
		• 有効な再帰ルートの場合、出力パス セットおよび最大分解深度 • 無効なルートの場合、ルートが無効な理由
ステップ 6	**copy running-config startup-config** 例： デバイス# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスでの IPv6 PBR の有効化

IPv6 のポリシーベース ルーティング（PBR）を有効にするには、パケットの一致基準と目的のポリシールーティング アクションを指定する、ルート マップを作成する必要があります。次に、そのルートマップを必要なインターフェイスに関連付けます。指定されたインターフェイスに到着し、match 句に一致するすべてのパケットに対して、PBR が実行されます。

PBR では、**set vrf** コマンドにより Virtual Routing and Forwarding（VRF）インスタンスとインターフェイス アソシエーションを切り離し、既存の PBR またはルートマップ設定を使用して、アクセスコントロールリスト（ACL）ベースの分類に基づいて VRF を選択できるようになります。このコマンドは、1 つのルータに複数ルーティング テーブルを提供し、ACL 分類に基づいてルートを選択できるようにします。ルータは、ACL に基づいてパケットを分類し、ルーティング テーブルを選択し、宛先アドレスを検索し、パケットをルーティングします。

PBR for IPv6 を有効にするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
4. 次のいずれかを実行します。
   - **match length** *minimum-length maximum-length*
   - **match ipv6 address** {**prefix-list** *prefix-list-name* | *access-list-name*}
5. 次のいずれかを実行します。
   - **set ipv6 next-hop** *global-ipv6-address* [*global-ipv6-address...*]
   - **set interface** *type number* [*...type number*]
   - **set ipv6 default next-hop** *global-ipv6-address* [*global-ipv6-address...*]
   - **set vrf** *vrf-name*
6. **exit**
7. **interface** *type number*
8. **ipv6 policy route-map** *route-map-name*

9. **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	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 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： `デバイス# 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	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] 例： `デバイス(config)# route-map rip-to-ospf permit`	ルーティング プロトコル間でルートを再配布する条件を定義するか、ポリシー ルーティングを有効にしてルート マップ 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	次のいずれかを実行します。
	• **match length** *minimum-length maximum-length*
	• **match ipv6 address** {**prefix-list** *prefix-list-name* | *access-list-name*}
	例：
	`デバイス(config-route-map)# match length 3 200`
	例：
	`デバイス(config-route-map)# match ipv6 address marketing`
		一致基準を指定します。
		• 次のうちの任意の項目またはすべてを指定できます。
		• レベル 3 のパケット長とのマッチング。
		• 指定された IPv6 アクセス リストとのマッチング。
		• **match**コマンドを指定しない場合、ルート マップはすべてのパケットに適用されます。

ステップ 5	次のいずれかを実行します。
	• **set ipv6 next-hop** *global-ipv6-address* [*global-ipv6-address...*]
	• **set interface** *type number* [*...type number*]
	• **set ipv6 default next-hop** *global-ipv6-address* [*global-ipv6-address...*]
	• **set vrf** *vrf-name*
	例：
	`デバイス(config-route-map)# set ipv6 next-hop 2001:DB8:2003:1::95`
	例：
	`デバイス(config-route-map)# set ipv6 default next-hop 2001:DB8:2003:1::95`
		基準に一致したパケットに適用するアクション（1つまたは複数）を指定します。
		• 次のうちの任意の項目またはすべてを指定できます。
		• パケットのルーティング先となるネクストホップを設定します（ネクストホップは隣接している必要があります）。
		• 宛先への明示的なルートがない場合に、パケットのルーティング先となるネクストホップを設定します。

	コマンドまたはアクション	目的
	例： デバイス(config-route-map)# **set vrf vrfname**	
ステップ 6	**exit** 例： デバイス(config-route-map)# **exit**	ルート マップ 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、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 7	**interface** *type number* 例： デバイス(config)# **interface FastEthernet 1/0**	インターフェイスのタイプと番号を指定し、ルータ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 8	**ipv6 policy route-map** *route-map-name* 例： デバイス(config-if)# **ipv6 policy-route-map interactive**	インターフェイスで IPv6 PBR に使用するルート マップを特定します。
ステップ 9	**end** 例： デバイス(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。

ローカル PBR for IPv6 のイネーブル化

デバイスが生成したパケットに対して、通常はポリシーによるルーティングは行われません。これらのパケットのためのローカル IPv6 ポリシーベース ルーティング（PBR）をイネーブルにするには、この作業を実行して、どのルート マップをデバイスで使用するべきかを示します。

ローカル PBR for IPv6 を有効にするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 local policy route-map** *route-map-name*
4. **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	**enable** 例：	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	デバイス> **enable**	
ステップ 2	**configure terminal** 例： デバイス# **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 local policy route-map** *route-map-name* 例： デバイス(config)# **ipv6 local policy route-map pbr-src-90**	デバイスによって生成されるパケットに対する IPv6 PBR を設定します。
ステップ 4	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。

IPv6 RIP の設定

IPv6 の RIP ルーティングの設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing RIP for IPv6」の章を参照してください。

IPv6 の RIP ルーティングを設定するには、次の手順を実行します。

始める前に

IPv6 RIP を実行するようにスイッチを設定する前に、**ip routing** グローバル コンフィギュレーション コマンドを使用してルーティングを有効にし、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送を有効にして、IPv6 RIP を有効にするレイヤ 3 インターフェイス上で IPv6 を有効にする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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	**ipv6 router rip** *name* 例： `デバイス(config)# ipv6 router rip cisco`	IPv6 RIP ルーティング プロセスを設定し、このプロセスに対してルータ 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	**maximum-paths** *number-paths* 例： `デバイス(config-router)# maximum-paths 6`	（任意）IPv6 RIP がサポートできる等コスト ルートの最大数を定義します。指定できる範囲は 1 ～ 32 で、デフォルトは 16 ルートです。
ステップ 5	**exit** 例： `デバイス(config-router)# exit`	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** *interface-id* 例： `デバイス(config)# interface gigabitethernet 1/0/1`	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、設定するレイヤ3インターフェイスを指定します。
ステップ 7	**ipv6 rip** *name* **enable** 例： `デバイス(config-if)# ipv6 rip cisco enable`	指定された IPv6 RIP ルーティング プロセスをインターフェイス上で有効にします。
ステップ 8	**ipv6 rip** *name* **default-information** {**only** | **originate**} 例： `デバイス(config-if)# ipv6 rip cisco default-information only`	（任意）IPv6 デフォルト ルート（::/0）を RIP ルーティング プロセス アップデートに格納して、指定インターフェイスから送信します。 （注） 任意のインターフェイスから IPv6 デフォルト ルート（::/0）を送信したあとに、ルーティング ループが発生しないようにするために、ルーティング プロセスは任意のインターフェイスで受信したすべてのデフォルト ルートを無視します。 • **only**：このインターフェイスから送信するアップデートに、デフォルト ルートを格納し、そ

	コマンドまたはアクション	目的
		の他のすべてのルートを含めない場合に選択します。 • **originate**：このインターフェイスから送信するアップデートに、デフォルト ルートおよびその他のすべてのルートを格納する場合に選択します。
ステップ 9	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。
ステップ 10	次のいずれかを使用します。 • **show ipv6 rip** [*name*] [**interface** *interface-id*] [**database**] [**next-hops**] • **show ipv6 rip** 例： デバイス# **show ipv6 rip cisco interface gigabitethernet2/0/1** または デバイス# **show ipv6 rip**	• 現在の IPv6 RIP プロセスに関する情報を表示します。 • IPv6 ルーティング テーブルの現在の内容を表示します。
ステップ 11	**copy running-config startup-config** 例： デバイス# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IPv6 OSPF の設定

IPv6 の OSPF ルーティングの設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing OSPF for IPv6」の章を参照してください。

IPv6 の OSPF ルーティングを設定するには、次の手順を実行します。

始める前に

ネットワークでは、IPv6 の OSPF をカスタマイズできます。ただし、IPv6 の OSPF のデフォルト設定は、ほとんどのお客様および機能の要件を満たします。

次の注意事項に従ってください。

- IPv6 コマンドのデフォルト設定を変更する場合は注意してください。デフォルト設定を変更すると、IPv6 ネットワークの OSPF に悪影響が及ぶことがあります。
- インターフェイスで IPv6 OSPF を有効にする前に、**ip routing** グローバル コンフィギュレーション コマンドを使用してルーティングを有効にし、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送を有効にし、IPv6 OSPF を有効にするレイヤ 3 インターフェイスで IPv6 を有効にする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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 router ospf** *process-id* 例： デバイス(config)# **ipv6 router ospf 21**	プロセスに対して OSPF ルータ コンフィギュレーション モードを有効にします。プロセス ID は、IPv6 OSPF ルーティング プロセスを有効にする場合に管理上割り当てられる番号です。この ID はローカルに割り当てられ、1 ～ 65535 の正の整数を指定できます。
ステップ 4	**area** *area-id* **range** {*ipv6-prefix/prefix length*} [**advertise** | **not-advertise**] [**cost** *cost*] 例： デバイス(config)# **area .3 range 2001:0DB8::/32 not-advertise**	（任意）エリア境界でルートを統合および集約します。 • *area-id*：ルートをサマライズするエリアの ID。10 進数または IPv6 プレフィックスのどちらかを指定できます。 • *ipv6-prefix/prefix length*：宛先 IPv6 ネットワーク、およびプレフィックス（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 進数。10 進値の前にスラッシュ（/）を付加する必要があります。 • **advertise**：（任意）アドバタイズするアドレス範囲ステータスを設定し、タイプ 3 のサマリー リンクステート アドバタイズメント（LSA）を生成します。

	コマンドまたはアクション	目的
		• **not-advertise**：（任意）アドレス範囲ステータスを DoNotAdvertise に設定します。Type3 サマリー LSA は抑制され、コンポーネント ネットワークは他のネットワークから隠された状態のままです。 • **cost** *cost*：（任意）現在のサマリー ルートのメトリックまたはコストを設定します。宛先への最短パスを判別する場合に、OSPF SPF 計算で使用します。指定できる値は 0 ～ 16777215 です。
ステップ 5	**maximum paths** *number-paths* 例： `デバイス(config)# maximum paths 16`	（任意）IPv6 OSPF がルーティング テーブルに入力する必要がある、同じ宛先への等コスト ルートの最大数を定義します。指定できる範囲は 1 ～ 32 で、デフォルトは 16 です。
ステップ 6	**exit** 例： `デバイス(config-if)# exit`	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 7	**interface** *interface-id* 例： `デバイス(config)# interface gigabitethernet 1/0/1`	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、設定するレイヤ 3 インターフェイスを指定します。
ステップ 8	**ipv6 ospf** *process-id* **area** *area-id* [**instance** *instance-id*] 例： `デバイス(config-if)# ipv6 ospf 21 area .3`	インターフェイスで IPv6 の OSPF を有効にします。 • **instance** *instance-id*：（任意）インスタンス ID
ステップ 9	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。
ステップ 10	次のいずれかを使用します。 • **show ipv6 ospf** [*process-id*] [*area-id*] **interface** [*interface-id*]	• OSPF インターフェイス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
	• **show ipv6 ospf** [*process-id*] [*area-id*] 例： デバイス# **show ipv6 ospf 21 interface gigabitethernet2/0/1** または デバイス# **show ipv6 ospf 21**	• OSPF ルーティング プロセスに関する一般情報を表示します。
ステップ 11	**copy running-config startup-config** 例： デバイス# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IPv6 の EIGRP の設定

IPv6 EIGRP を実行するようにスイッチを設定する前に、 **ip routing global configuration** グローバル コンフィギュレーション コマンドを入力してルーティングを有効にし、**ipv6 unicast-routing global** グローバル コンフィギュレーション コマンドを入力して IPv6 パケットの転送を有効にし、IPv6 EIGRP を有効にするレイヤ 3 インターフェイス上で IPv6 を有効にします。

明示的なルータ ID を設定するには、**show ipv6 eigrp** コマンドを使用して設定済みのルータ ID を確認してから、**router-id** コマンドを使用します。

EIGRP IPv4 の場合と同様に、EIGRPv6 を使用して EIGRP IPv6 インターフェイスを指定し、これらのサブセットを受動インターフェイスとして選択できます。**passive-interface** コマンドを使用してインターフェイスをパッシブに設定してから、選択したインターフェイスで **no passive-interface** コマンドを使用してこれらのインターフェイスをアクティブにします。受動インターフェイスでは、EIGRP IPv6 を設定する必要がありません。

設定手順の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing EIGRP for IPv6」の章を参照してください。

IPv6 ユニキャスト リバース パス転送の設定

ユニキャスト リバース パス転送（ユニキャスト RPF）機能は、検証できない送信元 IP アドレスの IP パケットを廃棄することで、間違ったまたは偽造（スプーフィングされた）送信元 IP アドレスがネットワークに流れて発生する問題を軽減するのに役立ちます。たとえば、Smurf や Tribal Flood Network（TFN）など、多くの一般的なタイプの DoS 攻撃は、偽造された、または次々に変わる送信元 IP アドレスを使用して、攻撃を突き止めたりフィルタすることを攻撃者が阻止できるようにします。パブリック アクセスを提供するインターネット サービス プロバイダ（ISP）の場合、uRPF が IP ルーティング テーブルと整合性の取れた有効な送信元アド

レスを持つパケットだけを転送することによって、そのような攻撃をそらします。この処理により、ISP のネットワーク、その顧客、および残りのインターネットが保護されます。

（注）
- スイッチが複数のスイッチタイプが混在する混合ハードウェア スタック内にある場合は、ユニキャスト RPF を設定しないでください。

IP ユニキャスト RPF 設定の詳細については、『*Cisco IOS Security Configuration Guide, Release 12.4*』の「*Other Security Features*」の章を参照してください。

DHCP for IPv6 アドレス割り当ての設定

この項では、DHCPv6 のアドレス割り当てについてだけ説明します。DHCPv6 クライアント、サーバー、またはリレー エージェント機能の設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing DHCP for IPv6」の章を参照してください。

DHCPv6 アドレス割り当てのデフォルト設定

デフォルトで、DHCPv6 機能はスイッチに設定されています。

DHCPv6 アドレス割り当ての設定時の注意事項

DHCPv6 アドレス割り当てを設定する場合は、次の注意事項に従ってください。

- 以下の手順では、次に示すレイヤ 3 インターフェイスの 1 つを指定する必要があります。
  - DHCPv6 IPv6 ルーティングは、レイヤ 3 インターフェイス上で有効である必要があります。
  - SVI：**interface vlan** *vlan_id* コマンドを使用して作成された VLAN インターフェイスです。
  - レイヤ 3 モードの EtherChannel ポートチャネル：**interface port-channel** **port-channel-number** コマンドを使用して作成されたポートチャネル論理インターフェイス。
- スイッチは、DHCPv6 クライアント、サーバー、またはリレー エージェントとして動作できます。DHCPv6 クライアント、サーバー、およびリレー機能は、インターフェイスで相互に排他的です。
- DHCPv6 クライアント、サーバー、またはリレー エージェントは、マスター スイッチ上でだけ稼働します。スタック マスターの再選出があった場合、新しいマスター スイッチは DHCPv6 設定を維持します。ただし、DHCP サーバー データベース リース情報のローカルの RAM コピーは、維持されません。

DHCPv6 サーバー機能の有効化（CLI）

DHCPv6 プールの特性を変更するには、**no** 形式の DHCP プール コンフィギュレーション モード コマンドを使用します。インターフェイスに対して DHCPv6 サーバー機能を無効にするには、**no ipv6 dhcp server** インターフェイス コンフィギュレーション コマンドを使用します。

インターフェイスで DHCPv6 サーバー機能を有効にするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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 dhcp pool** *poolname* 例： デバイス(config)# **ipv6 dhcp pool 7**	DHCP プール コンフィギュレーション モードを開始して、IPv6 DHCP プールの名前を定義します。プール名は、記号文字列（Engineering など）または整数（0 など）です。
ステップ 4	**address prefix** *IPv6-prefix* {**lifetime**} {*t1 t1* | **infinite**} 例： デバイス(config-dhcpv6)# **address prefix 2001:1000::0/64 lifetime 3600**	（任意）アドレス割り当て用のアドレスプレフィックスを指定します。 このアドレスは、16 ビット値をコロンで区切った 16 進数で指定する必要があります。 **lifetime** *t1 t1*：IPv6 アドレス プレフィックスが有効な状態を維持するタイム インターバル（秒）を指定します。指定できる範囲は 5 ～ 4294967295 秒です。時間間隔なしの場合は、**infinite** を指定します。
ステップ 5	**link-address** *IPv6-prefix* 例： デバイス(config-dhcpv6)# **link-address 2001:1002::0/64**	（任意）link-address IPv6 プレフィックスを指定します。 着信インターフェイス上のアドレスまたはパケットのリンクアドレスが指定した IPv6 プレフィックスに一致する場合、サーバーは設定情報プールを使用します。 このアドレスは、16 ビット値をコロンで区切った 16 進数で指定する必要があります。

	コマンドまたはアクション	目的
ステップ 6	**vendor-specific** *vendor-id* 例： `デバイス(config-dhcpv6)# vendor-specific 9`	（任意）ベンダー固有のコンフィギュレーション モードを開始して、ベンダー固有の ID 番号を指定します。この番号は、ベンダーの IANA プライベート エンタープライズ番号です。指定できる範囲は 1 ～ 4294967295 です。
ステップ 7	**suboption** *number* { **address** *IPv6-address* | **ascii** *ASCII-string* | **hex** *hex-string*} 例： `デバイス(config-dhcpv6-vs)# suboption 1 address 1000:235D::`	（任意）ベンダー固有のサブオプション番号を入力します。指定できる範囲は 1 ～ 65535 です。IPv6 アドレス、ASCII テキスト、または 16 進文字列をサブオプション パラメータで定義されているように入力します。
ステップ 8	**exit** 例： `デバイス(config-dhcpv6-vs)# exit`	DHCP プール コンフィギュレーション モードに戻ります。
ステップ 9	**exit** 例： `デバイス(config-dhcpv6)# exit`	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 10	**interface** *interface-id* 例： `デバイス(config)# interface gigabitethernet 1/0/1`	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、設定するインターフェイスを指定します。
ステップ 11	**ipv6 dhcp server** [*poolname* | **automatic**] [**rapid-commit**] [**preference** *value*] [**allow-hint**] 例： `デバイス(config-if)# ipv6 dhcp server automatic`	インターフェイスに対して DHCPv6 サーバー機能を有効にします。 • *poolname*：（任意）IPv6 DHCP プールのユーザー定義の名前。プール名は、記号文字列（Engineering など）または整数（0 など）です。 • **automatic**：（任意）サーバーが、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）2 つのメッセージを交換する方式を許可します。

	コマンドまたはアクション	目的
		• **preference** 値：（任意）サーバーによって送信されるアドバタイズメント メッセージ内のプリファレンス オプションで指定するプリファレンス値を設定します。範囲は 0 ～ 255 です。デフォルトのプリファレンス値は 0 です。 • **allow-hint**：（任意）サーバーが SOLICIT メッセージに含まれるクライアントの提案を考慮するかどうかを指定します。デフォルトでは、サーバーはクライアントのヒントを無視します。
ステップ 12	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。

ステップ 13	次のいずれかを実行します。
	• **show ipv6 dhcp pool**
	• **show ipv6 dhcp interface**
	例：
	`デバイス# show ipv6 dhcp pool`
	または
	`デバイス# show ipv6 dhcp interface`
		• DHCPv6 プール設定を確認します。
		• DHCPv6 サーバー機能がインターフェイス上で有効であることを確認します。

ステップ 14	**copy running-config startup-config** 例： `デバイス# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

DHCPv6 クライアント機能の有効化

インターフェイスで DHCPv6 クライアントを有効にするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	デバイス> **enable**	
ステップ 2	**configure terminal** 例： デバイス# **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** *interface-id* 例： デバイス(config)# **interface gigabitethernet 1/0/1**	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、設定するインターフェイスを指定します。
ステップ 4	**ipv6 address dhcp** [**rapid-commit**] 例： デバイス(config-if)# **ipv6 address dhcp rapid-commit**	インターフェイスで DHCPv6 サーバーから IPv6 アドレスを取得できるようにします。 **rapid-commit**：（任意）アドレス割り当てに 2 つのメッセージを交換する方式を許可します。
ステップ 5	**ipv6 dhcp client request** [**vendor-specific**] 例： デバイス(config-if)# **ipv6 dhcp client request vendor-specific**	（任意）インターフェイスでベンダー固有のオプションを要求できるようにします。
ステップ 6	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**show ipv6 dhcp interface** 例： デバイス# **show ipv6 dhcp interface**	DHCPv6 クライアントがインターフェイスで有効になっていることを確認します。

IPv6 の表示

次のコマンドの構文および使用方法の詳細については、Cisco IOS のコマンド リファレンスを参照してください。

表 *5 : IPv6* をモニタリングするコマンド

コマンド	目的
show ipv6 access-list	アクセス リストのサマリーを表示します。
show ipv6 cef	IPv6 の Cisco エクスプレス フォワーディングを表示します。
show ipv6 interface *interface-id*	IPv6 インターフェイスのステータスと設定を表示します。
show ipv6 mtu	宛先キャッシュごとに IPv6 MTU を表示します。
show ipv6 neighbors	IPv6 ネイバーキャッシュ エントリを表示します。
show ipv6 ospf	IPv6 OSPF 情報を表示します。
show ipv6 prefix-list	IPv6 プレフィックス リストを表示します。
show ipv6 protocols	スイッチの IPv6 ルーティング プロトコルのリストを表示します。
show ipv6 rip	IPv6 RIP ルーティング プロトコル ステータスを表示します。
show ipv6 rip	IPv6 RIP ルーティング プロトコル ステータスを表示します。
show ipv6 route	IPv6 ルート テーブル エントリを表示します。
show ipv6 routers	ローカル IPv6 ルータを表示します。
show ipv6 static	IPv6 スタティック ルートを表示します。
show ipv6 traffic	IPv6 トラフィックの統計情報を表示します。

表 *6 : EIGRP IPv6* 情報を表示するためのコマンド

コマンド	目的
show ipv6 eigrp [*as-number*] *interface*	EIGRP IPv6 用に設定されたインターフェイスの情報を表示します。
show ipv6 eigrp [*as-number*] *neighbor*	EIGRP IPv6 で検出されたネイバーを表示します。

コマンド	目的
show ipv6 interface[*as-number*] *traffic*	送受信される EIGRP IPv6 パケット数を表示します。
show ipv6 eigrptopology [*as-number* | *ipv6-address*] [**active** | **all-links** | **detail-links** | **pending** | **summary** | **zero-successors** | **Base**]	IPv6 トポロジテーブルの EIGRP エントリを表示します。

IPv6 ユニキャスト ルーティングの設定例

IPv6 アドレッシングの設定と IPv6 ルーティングの有効化：例

次に、IPv6 プレフィックス 2001:0DB8:c18:1::/64 に基づく、リンクローカルアドレスおよびグローバルアドレスを使用して、IPv6 を有効にする例を示します。EUI-64 インターフェイス ID が、両方のアドレスの下位 64 ビットで使用されます。**show ipv6 interface** EXEC コマンドの出力は、インターフェイスのリンクローカル プレフィックス FE80::/64 にインターフェイス ID（20B:46FF:FE2F:D940）を付加する方法を示すために追加されています。

```
デバイス(config)# ipv6 unicast-routing
デバイス(config)# interface gigabitethernet1/0/11
デバイス(config-if)# no switchport
デバイス(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
デバイス(config-if)# end
デバイス# show ipv6 interface gigabitethernet1/0/11
GigabitEthernet1/0/11 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
  Global unicast address(es):
  2001:0DB8:c18:1:20B:46FF:FE2F:D940, subnet is 2001:0DB8:c18:1::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF2F:D940
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
```

デフォルト ルータ プリファレンスの設定：例

次に、インターフェイス上のルータに高い DRP を設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ipv6 nd router-preference high
デバイス(config-if)# end
```

IPv4 および IPv6 プロトコル スタックの設定：例

次に、インターフェイス上で IPv4 および IPv6 ルーティングを有効にする例を示します。

```
デバイス(config)# ip routing
デバイス(config)# ipv6 unicast-routing
デバイス(config)# interface fastethernet1/0/11
デバイス(config-if)# no switchport
デバイス(config-if)# ip address 192.168.99.1 255.255.255.0
デバイス(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
デバイス(config-if)# end
```

DHCPv6 サーバー機能の有効化：例

次の例では、*engineering* という IPv6 アドレス プレフィックスを持つプールを設定する方法を示します。

```
デバイス# configure terminal
デバイス(config)# ipv6 dhcp pool engineering
デバイス(config-dhcpv6)#address prefix 2001:1000::0/64
デバイス(config-dhcpv6)# end
```

次に、3 リンクアドレスおよび IPv6 アドレス プレフィックスを持つ *testgroup* と呼ばれるプールを設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# ipv6 dhcp pool testgroup
デバイス(config-dhcpv6)# link-address 2001:1001::0/64
デバイス(config-dhcpv6)# link-address 2001:1002::0/64
デバイス(config-dhcpv6)# link-address 2001:2000::0/48
デバイス(config-dhcpv6)# address prefix 2001:1003::0/64
デバイス(config-dhcpv6)# end
```

次の例では、*350* というベンダー固有オプションを持つプールを設定する方法を示します。

```
デバイス# configure terminal
デバイス(config)# ipv6 dhcp pool 350
デバイス(config-dhcpv6)# address prefix 2001:1005::0/48
デバイス(config-dhcpv6)# vendor-specific 9
```

```
デバイス(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
デバイス(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
デバイス(config-dhcpv6-vs)# end
```

DHCPv6 クライアント機能の有効化：例

次に、IPv6 アドレスを取得して、rapid-commit オプションを有効にする例を示します。

```
デバイス(config)# interface gigabitethernet2/0/1
デバイス(config-if)# ipv6 address dhcp rapid-commit
```

IPv6 ICMP レート制限の設定：例

次に、IPv6 ICMP エラー メッセージ間隔を 50 ミリ秒に、バケット サイズを 20 トークンに設定する例を示します。

```
デバイス(config)#ipv6 icmp error-interval 50 20
```

IPv6 のスタティック ルーティングの設定：例

次に、アドミニストレーティブ ディスタンスが 130 のフローティング スタティック ルートをインターフェイスに設定する例を示します。

```
デバイス(config)# ipv6 route 2001:0DB8::/32 gigabitethernet2/0/1 130
```

例：インターフェイスでの PBR のイネーブル化

次の例では、pbr-dest-1 という名前のルート マップを作成および設定し、パケット一致基準および目的のポリシー ルーティング アクションを指定します。次に、PBR が GigabitEthernet インターフェイス 0/0/1 で有効にされます。

```
ipv6 access-list match-dest-1
  permit ipv6 any 2001:DB8:2001:1760::/32
route-map pbr-dest-1 permit 10
  match ipv6 address match-dest-1
  set interface GigabitEthernet 0/0/0
interface GigabitEthernet0/0/1
  ipv6 policy-route-map interactive
```

例：ローカル PBR for IPv6 のイネーブル化

次の例では、宛先 IPv6 アドレスがアクセス リスト pbr-src-90 で許可されている IPv6 アドレス範囲に一致するパケットが、IPv6 アドレス 2001:DB8:2003:1::95 のデバイスに送信されています。

```
ipv6 access-list src-90
  permit ipv6 host 2001:DB8:2003::90 2001:DB8:2001:1000::/64
route-map pbr-src-90 permit 10
  match ipv6 address src-90
  set ipv6 next-hop 2001:DB8:2003:1::95
ipv6 local policy route-map pbr-src-90
```

IPv6 の RIP の設定：例

次に、最大 8 の等コスト ルートにより RIP ルーティング プロセス *cisco* を有効にし、インターフェイス上でこれを有効にする例を示します。

```
デバイス(config)# ipv6 router rip cisco
デバイス(config-router)# maximum-paths 8
デバイス(config)# exit
デバイス(config)# interface gigabitethernet2/0/11
デバイス(config-if)# ipv6 rip cisco enable
```

IPv6 の表示：例

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

```
デバイス# show ipv6 interface
Vlan1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
  Global unicast address(es):
    3FFE:C000:0:1:20B:46FF:FE2F:D940, subnet is 3FFE:C000:0:1::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF2F:D940
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
<output truncated>
```

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』

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	リンク
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

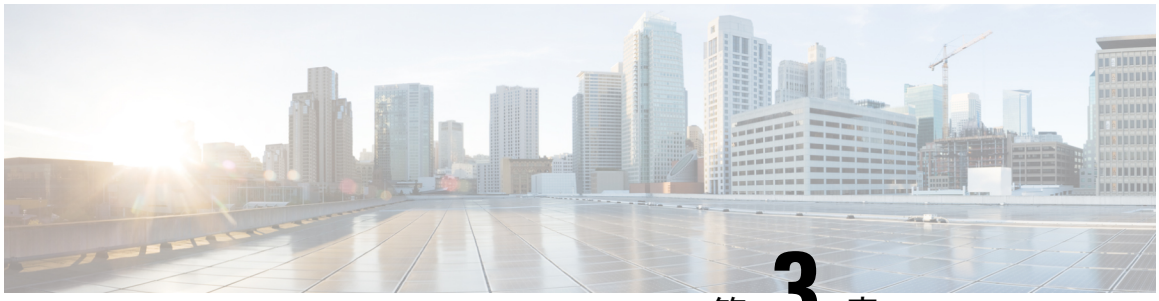
機能情報

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* ユニキャストおよびルーティングの機能情報

機能名	リリース	機能情報
IPv6 ユニキャストおよびルーティング	Cisco IOS XE Everest 16.5.1a	ユニキャストおよびルーティング機能が IPv6 に対してサポートされました。



第 3 章

IPv6 マルチキャストの実装

IPv6 マルチキャスト ルーティングの実装に関する情報

この章では、スイッチに IPv6 マルチキャスト ルーティングを実装する方法について説明します。

従来の IP 通信では、ホストはパケットを単一のホスト（ユニキャスト伝送）またはすべてのホスト（ブロードキャスト伝送）に送信できます。IPv6マルチキャストは、第三の方式を提供するものであり、ホストが単一のデータ ストリームをすべてのホストのサブセット（グループ伝送）に同時に送信できるようにします。

IPv6 マルチキャストの概要

IPv6 マルチキャスト グループは、特定のデータ ストリームを受信する受信側の任意のグループです。このグループには、物理的境界または地理的境界はありません。受信側は、インターネット上または任意のプライベート ネットワーク内の任意の場所に配置できます。特定のグループへのデータ フローの受信に関与する受信側は、ローカル スイッチに対してシグナリングすることによってそのグループに加入する必要があります。このシグナリングは、MLD プロトコルを使用して行われます。

スイッチは、MLD プロトコルを使用して、直接接続されているサブネットにグループのメンバが存在するかどうかを学習します。ホストは、MLD レポート メッセージを送信することによってマルチキャスト グループに加入します。ネットワークでは、各サブネットでマルチキャスト データのコピーを 1 つだけ使用して、潜在的に無制限の受信側にデータが伝送されます。トラフィックの受信を希望する IPv6 ホストはグループ メンバと呼ばれます。

グループ メンバに伝送されるパケットは、単一のマルチキャスト グループ アドレスによって識別されます。マルチキャスト パケットは、IPv6 ユニキャスト パケットと同様に、ベストエフォート型の信頼性を使用してグループに伝送されます。

マルチキャスト環境は、送信側と受信側で構成されます。どのホストも、グループのメンバであるかどうかにかかわらず、グループに送信できます。ただし、グループのメンバだけがメッセージをリッスンして受信できます。

マルチキャストアドレスがマルチキャストグループの受信先として選択されます。送信者は、データグラムの宛先アドレスとしてグループのすべてのメンバに到達するためにそのアドレスを使用します。

マルチキャストグループ内のメンバーシップはダイナミックです。ホストはいつでも加入および脱退できます。マルチキャストグループ内のメンバの場所または数に制約はありません。ホストは、一度に複数のマルチキャスト グループのメンバにすることができます。

マルチキャストグループがどの程度アクティブであるか、その期間、およびメンバーシップはグループおよび状況によって異なります。メンバを含むグループにアクティビティがない場合もあります。

IPv6 マルチキャスト ルーティングの実装

Cisco IOS ソフトウェアでは、IPv6 マルチキャスト ルーティングを実装するため、次のプロトコルがサポートされています。

- MLD は、直接接続されているリンク上のマルチキャスト リスナー（特定のマルチキャスト アドレスを宛先としたマルチキャスト パケットを受信するために使用するノード）を検出するために IPv6 スイッチで使用されます。MLD には 2 つのバージョンがあります。MLD バージョン 1 はバージョン 2 のインターネット グループ管理プロトコル（IGMP）for IPv4 をベースとしています。MLD バージョン 2 はバージョン 3 の IGMP for IPv4 をベースとしています。Cisco IOS ソフトウェアの IPv6 マルチキャストでは、MLD バージョン 2 と MLD バージョン 1 の両方が使用されます。MLD バージョン 2 は、MLD バージョン 1 と完全な下位互換性があります（RFC 2710 で規定）。MLD バージョン 1 だけをサポートするホストは、MLD バージョン 2 を実行しているスイッチと相互運用します。MLD バージョン 1 ホストと MLD バージョン 2 ホストの両方が混在する LAN もサポートされています。
- PIM-SM は、相互に転送されるマルチキャストパケット、および直接接続されている LAN に転送されるマルチキャスト パケットを追跡するためにスイッチ間で使用されます。
- PIM in Source Specific Multicast（PIM-SSM）は PIM-SM と類似していますが、IP マルチキャストアドレスを宛先とした特定の送信元アドレス（または特定の送信元アドレスを除くすべてのアドレス）からのパケットを受信する対象をレポートする機能を別途備えています。

IPv6 マルチキャスト リスナー ディスカバリ プロトコル

キャンパス ネットワークでマルチキャストの実装を開始するには、ユーザーは最初に、誰がマルチキャストを受信するかを定義する必要があります。MLD プロトコルは、直接接続されているリンク上のマルチキャストリスナー（たとえば、マルチキャストパケットを受信するノード）の存在を検出するため、およびこれらのネイバー ノードを対象にしている特定のマルチ

キャスト アドレスを検出するために、IPv6 スイッチによって使用されます。これは、ローカル グループおよび送信元固有のグループ メンバーシップの検出に使用されます。

MLD プロトコルは、特別なマルチキャスト クエリアおよびホストを使用して、ネットワーク全体でマルチキャスト トラフィックのフローを自動的に制御および制限する手段を提供します。

マルチキャスト クエリアとマルチキャスト ホスト

マルチキャスト クエリアは、クエリー メッセージを送信して、特定のマルチキャスト グループのメンバーであるネットワーク デバイスを検出するネットワーク デバイス（スイッチなど）です。

マルチキャスト ホストは、受信側（スイッチを含む）としてレポート メッセージを送信し、クエリアにホスト メンバーシップを通知します。

同じ送信元からのマルチキャスト データ ストリームを受信する一連のクエリアおよびホストは、マルチキャスト グループと呼ばれます。クエリアおよびホストは、MLD レポートを使用して、マルチキャスト グループに対する加入および脱退を行ったり、グループ トラフィックの受信を開始したりします。

MLD では、メッセージの伝送に インターネット制御メッセージ プロトコル（ICMP）が使用されます。すべての MLD メッセージはホップ制限が 1 のリンクローカルであり、すべてにスイッチ アラート オプションが設定されています。スイッチ アラート オプションは、ホップバイホップ オプション ヘッダーの実装を意味します。

MLD アクセス グループ

MLD アクセス グループは、Cisco IOS IPv6 マルチキャスト スイッチでの受信側アクセス コントロールを実現します。この機能では、受信側が加入できるグループのリストを制限し、SSM チャネルへの加入に使用される送信元を許可または拒否します。

受信側の明示的トラッキング

明示的トラッキング機能を使用すると、スイッチが IPv6 ネットワーク内のホストの動作を追跡できるようになります。また、この機能により、高速脱退メカニズムを MLD バージョン 2 のホスト レポートで使用できるようになります。

プロトコル独立マルチキャスト

PIM（Protocol Independent Multicast）は、相互に転送されるマルチキャスト パケット、および直接接続されている LAN に転送されるマルチキャスト パケットを追跡するためにスイッチ間で使用されます。PIM は、ユニキャスト ルーティング プロトコルとは独立して動作し、他のプロトコルと同様に、マルチキャスト ルート アップデートの送受信を実行します。ユニキャスト ルーティング テーブルに値を入力するために LAN でどのユニキャスト ルーティング プロトコルが使用されているかどうかにかかわらず、Cisco IOS PIM では、独自のルーティング テーブルを構築および管理する代わりに、既存のユニキャスト テーブル コンテンツを使用して、Reverse Path Forwarding（RPF）チェックを実行します。

PIM-SM または PIM-SSM のいずれかを使用するように IPv6 マルチキャストを設定することも、ネットワークで PIM-SM と PIM-SSM の両方を使用することもできます。

PIM スパース モード

IPv6 マルチキャストでは、PIM-SM を使用したドメイン内マルチキャスト ルーティングがサポートされています。PIM-SM は、ユニキャスト ルーティングを使用して、マルチキャスト ツリー構築用のリバースパス情報を提供しますが、特定のユニキャスト ルーティング プロトコルには依存しません。

PIM-SM は、トラフィックに対して明示的な要求がある場合を除いて、各マルチキャストに関与しているスイッチの数が比較的少なく、これらのスイッチがグループのマルチキャスト パケットを転送しないときに、マルチキャスト ネットワークで使用されます。PIM-SMは、共有ツリー上のデータ パケットを転送することによって、アクティブな送信元に関する情報を配布します。PIM-SM は最初に共有ツリーを使用しますが、これにはRPの使用が必要となります。

要求は、ツリーのルート ノードに向けてホップバイホップで送信される PIM join を使用して行われます。PIM-SM のツリーのルート ノードは、共有ツリーの場合は RP、最短パス ツリー（SPT）の場合はマルチキャスト送信元に直接接続されているファーストホップ スイッチになります。RP はマルチキャスト グループを追跡し、マルチキャスト パケットを送信するホストはそのホストのファーストホップ スイッチによって RP に登録されます。

PIM join がツリーの上位方向に送信されると、要求されたマルチキャスト トラフィックがツリーの下位方向に転送されるように、パス上のスイッチがマルチキャスト転送ステートを設定します。マルチキャスト トラフィックが不要になったら、スイッチはルート ノードに向けてツリーの上位方向に PIM prune を送信し、不必要なトラフィックをプルーニング（削除）送信します。この PIM prune がホップごとにツリーを上位方向に移動する際、各スイッチはその転送状態を適切に更新します。最終的に、マルチキャスト グループまたは送信元に関連付けられている転送ステートは削除されます。

マルチキャスト データの送信側は、マルチキャスト グループを宛先としたデータを送信します。送信側の指定スイッチ（DR）は、これらのデータ パケットを受け取り、ユニキャストでカプセル化し、RPに直接送信します。RPは、カプセル化されたこれらのデータ パケットを受信し、カプセル化を解除し、共有ツリー上に転送します。そのあと、パケットは、RP ツリー上のスイッチの（*, G）マルチキャスト ツリー ステートに従って、RP ツリー ブランチの任意の場所に複製され、そのマルチキャスト グループのすべての受信側に最終的に到達します。RP へのデータ パケットのカプセル化のプロセスは登録と呼ばれ、カプセル化されたパケットは PIM レジスタ パケットと呼ばれます。

IPv6 BSR：RP マッピングの設定

ドメイン内のPIMスイッチは、各マルチキャスト グループを正しいRPアドレスにマッピングできる必要があります。PIM-SM 対応の BSR プロトコルは、グループと RP のマッピング情報をドメイン全体に迅速に配布するためのダイナミック適応メカニズムを備えています。IPv6 BSR機能を使用すると、到達不能になったRPが検出され、マッピング テーブルが変更されます。これにより、到達不能な RP が今後使用されなくなり、新しいテーブルがドメイン全体に迅速に配布されるようになります。

すべての PIM-SM マルチキャスト グループを RP の IP または IPv6 アドレスに関連付ける必要があります。新しいマルチキャスト送信側が送信を開始すると、そのローカル DR がこれらのデータ パケットを PIM register メッセージにカプセル化し、そのマルチキャスト グループの RP に送信します。新しいマルチキャスト受信側が加入すると、そのローカル DR がそのマルチキャスト グループの RP に PIM join メッセージを送信します。PIM スイッチは、（*, G）join メッセージを送信するとき、RP 方向への次のスイッチを認識して、G（グループ）がそのスイッチにメッセージを送信できるようにする必要があります。また、PIM スイッチは、（*, G）ステートを使用してデータ パケットを転送するとき、G を宛先としたパケットの正しい着信インターフェイスを認識する必要があります。これは、他のインターフェイスに着信するパケットを拒否する必要があるためです。

ドメイン内の少数のスイッチが候補ブートストラップ スイッチ（C-BSR）として設定され、単一の BSR がそのドメイン用に選択されます。また、ドメイン内の一連のスイッチが候補 RP（C-RP）として設定されます。通常、これらのスイッチは、C-BSR として設定されているものと同じスイッチです。候補 RP は、候補 RP アドバタイズメント（C-RP-Adv）メッセージをそのドメインの BSR に定期的にユニキャストし、RP になる意思をアドバタイズします。C-RP-Adv メッセージには、アドバタイズを行っている C-RP のアドレス、およびグループ アドレスとマスク長のフィールドの任意のリストが含まれています。これらのフィールドは、立候補のアドバタイズの対象となるグループ プレフィックスを示します。BSR は、定期的に発信するブートストラップ メッセージ（BSM）にこれらの一連の C-RP とそれに対応するグループ プレフィックスを含めます。BSM は、ドメイン全体にホップバイホップで配布されます。

双方向 BSR がサポートされているため、双方向 RP を C-RP メッセージおよび BSM の双方向範囲でアドバタイズできます。システム内のすべてのスイッチは、BSM で双方向範囲を使用できる必要があります。使用できない場合は、双方向 RP 機能が機能しません。

PIM-Source Specific Multicast (PIM-SSM)

PIM-SSM は、SSM の実装をサポートするルーティング プロトコルであり、PIM-SM から派生したものです。ただし、PIM-SM では PIM join を受けてすべてのマルチキャスト送信元からデータが送信されるのに対し、SSM機能では、受信側が明示的に加入しているマルチキャスト送信元だけからその受信側にデータグラム トラフィックが転送されます。これにより、帯域利用率が最適化され、不要なインターネット ブロードキャスト トラフィックが拒否されます。さらに、SSM では、RP と共有ツリーを使用する代わりに、マルチキャスト グループの送信元アドレスで見つかった情報を使用します。この情報は、MLD メンバーシップ レポートによってラストホップ スイッチにリレーされる送信元アドレスを通して受信側から提供されます。その結果として、送信元に直接つながる最短パス ツリーが得られます。

SSM では、データグラムは（S, G）チャネルに基づいて配信されます。1 つの（S, G）チャネルのトラフィックは、IPv6 ユニキャスト送信元アドレス S とマルチキャスト グループ アドレス G を IPv6 宛先アドレスとして使用するデータグラムで構成されます。システムは、（S, G）チャネルのメンバになることによって、このトラフィックを受信します。シグナリングは不要ですが、受信側は特定の送信元からのトラフィックを受信する場合は（S, G）チャネルに加入し、トラフィックを受信しない場合はチャネルから脱退する必要があります。

SSM を動作させるには、MLD バージョン 2 が必要です。MLD を使用すると、ホストが送信元の情報を提供できるようになります。MLD を使用して SSM を動作させるには、Cisco IOS IPv6

スイッチ、アプリケーションが実行されているホスト、およびアプリケーション自体で SSM がサポートされている必要があります。

ルーティング可能アドレスの hello オプション

IPv6 内部ゲートウェイ プロトコルを使用してユニキャスト ルーティング テーブルを構築する場合、アップストリーム スイッチ アドレスを検出するための手順では、PIM ネイバーとネクストホップ スイッチが同じスイッチを表しているかぎり、これらのアドレスは常に同じであるものと想定されます。ただし、スイッチがリンク上に複数のアドレスを持つ場合は、このことが当てはまるとはかぎりません。

この状況は IPv6 において、2 つの一般的な状況で発生することがあります。1 つめの状況は、ユニキャスト ルーティング テーブルが IPv6 内部ゲートウェイ プロトコル（マルチキャスト BGP など）によって構築されない場合に発生します。2 つめの状況は、RP のアドレスがダウンストリーム スイッチとサブネット プレフィックスを共有している場合に発生します（RP スイッチ アドレスはドメインワイドにする必要があるため、リンクローカル アドレスにはできないことに注意してください）。

ルーティング可能アドレスの hello オプションによって、PIM プロトコルでこのような状況を回避できます。このためには、PIM hello メッセージがアドバタイズされるインターフェイス上のすべてのアドレスを含む PIM hello メッセージ オプションを追加します。PIM スイッチが何らかのアドレスのアップストリーム スイッチを検出すると、RPF 計算の結果は、PIM ネイバーのアドレス自体に加えて、このオプションのアドレスとも比較されます。このオプションにはそのリンク上の PIM スイッチの考えられるアドレスがすべて含まれているため、対象の PIM スイッチがこのオプションをサポートしている場合、常に RPF 計算の結果が含まれます。

PIM メッセージにサイズ制限があることと、ルーティング可能アドレスの hello オプションが単一の PIM hello メッセージ内に収まる必要があるため、インターフェイスで設定できるアドレスの制限は 16 個になっています。

PIM IPv6 スタブ ルーティング

PIM スタブ ルーティング機能は、エンド ユーザーの近くにルーテッド トラフィックを移動し、リソースの利用率を軽減します。

PIM スタブ ルーティングを使用するネットワークでは、ユーザーに対する IPv6 トラフィックの唯一の許容ルートは、PIM スタブ ルーティングを設定しているスイッチ経由です。PIM 受動インターフェイスは、VLAN などのレイヤ 2 アクセス ドメイン、または他のレイヤ 2 デバイスに接続されているインターフェイスに接続されます。直接接続されたマルチキャスト レシーバおよび送信元のみが、レイヤ 2 アクセス ドメインで許可されます。PIM 受動インターフェイスは、受信した PIM 制御パケットを送信または処理しません。

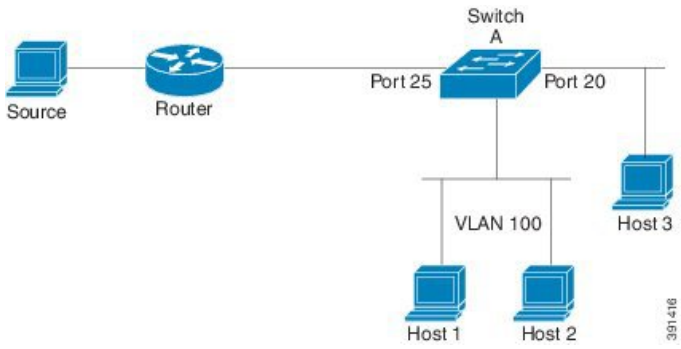
PIM スタブ ルーティングを使用しているときは、IPv6 マルチキャスト ルーティングを使用し、スイッチだけを PIM スタブ ルータとして設定するように、分散ルータおよびリモート ルータを設定する必要があります。スイッチは分散ルータ間の伝送トラフィックをルーティングしません。スイッチのルーテッドアップリンク ポートも設定する必要があります。SVI の場合は、スイッチのアップリンク ポートを使用できません。

また、PIM スタブ ルーティングをスイッチに設定するときは、EIGRP スタブ ルーティングも設定する必要があります。

冗長 PIM スタブ ルータ トポロジーはサポートされません。単一のアクセス ドメインにマルチキャスト トラフィックを転送している複数の PIM ルータがある場合、冗長トポロジーが存在します。PIM メッセージはブロックされ、PIM アサートおよび指定されたルータ選出メカニズムは PIM 受動インターフェイスではサポートされません。PIM スタブ機能では、非冗長アクセス ルータ トポロジーだけがサポートされます。非冗長トポロジーを使用することで、PIM 受動インターフェイスはそのアクセス ドメインで唯一のインターフェイスおよび指定ルータであると想定します。

次に示す図では、スイッチ A ルーテッド アップリンク ポート 25 がルータに接続され、PIM スタブ ルーティングが VLAN 100 インターフェイスとホスト 3 でイネーブルになっています。この設定により、直接接続されたホストはマルチキャスト発信元からトラフィックを受信できます。

図 *2 : PIM* スタブ ルータ設定



ランデブー ポイント

IPv6 PIM では、組み込み RP がサポートされています。組み込み RP サポートを利用すると、デバイスは、静的に設定されている RP の代わりに、マルチキャスト グループ宛先アドレスを使用して RP 情報を学習できるようになります。デバイスが RP である場合、RP として静的に設定する必要があります。

デバイスは、MLD レポート内、または PIM メッセージおよびデータ パケット内の組み込み RP グループ アドレスを検索します。このようなアドレスが見つかったら、デバイスはアドレス自体からグループの RP を学習します。この学習された RP は、グループのすべてのプロトコル アクティビティに使用されます。デバイスが RP である場合、組み込み RP を RP として設定する必要があり、デバイスはそのようにアドバタイズされます。

組み込み RP よりも優先するスタティック RP を選択するには、特定の組み込み RP グループ範囲またはマスクをスタティック RP のアクセス リストに設定する必要があります。PIM がスパースモードで設定されている場合は、RP として動作する 1 つ以上のデバイス選択も必要です。RP は、共有配布ツリーの選択ポイントに配置された単一の共通ルートであり、各ボックスでスタティックに設定されます。

PIM DR は、共有ツリーの下位方向に配布するために、直接接続されているマルチキャスト送信元から RP にデータを転送します。データは次の 2 つの方法のいずれかを使用して RP に転送されます。

- データは、登録パケットにカプセル化され、DR として動作するファーストホップデバイスによって直接 RP にユニキャストされます。
- RP 自身が送信元ツリーに加入している場合は、PIM スパース モードの項で説明したように、RPF 転送アルゴリズムに従ってマルチキャスト転送されます。

RP アドレスは、パケットをグループに送信するホストの代わりに PIM Register メッセージを送信するためにファーストホップデバイスによって使用されます。また、RP アドレスは、ラストホップデバイスによって PIM join および prune メッセージを RP に送信してグループメンバーシップについて通知するためにも使用されます。すべてのデバイス（RPデバイスを含む）で RP アドレスを設定する必要があります。

1 台の PIM デバイスを、複数のグループの RP にできます。特定のグループの PIM ドメイン内で一度に使用できるRPアドレスは1つだけです。アクセスリストで指定されている条件によって、デバイスがどのグループの RP であるかが判別されます。

IPv6 マルチキャストでは、PIM accept register 機能がサポートされています。これは、RP で PIM-SM register メッセージのフィルタリングを実行するための機能です。ユーザーは、アクセス リストを照合するか、または登録されている送信元の AS パスとルート マップに指定されている AS パスを比較できます。

スタティック mroute

IPv6 スタティック mroute は、RPF チェックを変化させるために使用する IPv4 スタティック mroute とほぼ同様に動作します。IPv6 スタティック mroute は、IPv6 スタティック ルートと同じデータベースを共有し、RPF チェックに対するスタティック ルート サポートを拡張することによって実装されます。スタティック mroute では、等コスト マルチパス mroute がサポートされています。また、ユニキャスト専用スタティック ルートもサポートされています。

MRIB

マルチキャストルーティング情報ベース（MRIB）は、マルチキャストルーティングプロトコル（ルーティング クライアント）によってインスタンス化されるマルチキャスト ルーティング エントリのプロトコル非依存リポジトリです。その主要機能は、ルーティング プロトコルとマルチキャスト転送情報ベース（MFIB）間の非依存性を実現することです。また、クライアント間の調整および通信ポイントとしても機能します。

ルーティング クライアントは、MRIB が提供するサービスを使用して、ルーティング エントリをインスタンス化し、他のクライアントによってルーティングエントリに加えられた変更を取得します。MRIB では、ルーティング クライアント以外に、転送クライアント（MFIB インスタンス）や特別なクライアント（MLD など）も扱われます。MFIB は、MRIB からその転送エントリを取得し、パケットの受信に関連するイベントについてMRIBに通知します。これら

の通知は、ルーティング クライアントによって明示的に要求されることも、MFIB によって自発的に生成されることもあります。

MRIB のもう 1 つの重要な機能は、同じマルチキャスト セッション内でマルチキャスト接続を確立する際に、複数のルーティング クライアントの調整を可能にすることです。また、MRIB では、MLD とルーティング プロトコル間の調整も可能です。

MFIB

MFIB は、IPv6 ソフトウェア用のプラットフォーム非依存およびルーティング プロトコル非依存ライブラリです。その主な目的は、転送テーブルが変更されたときに、Cisco IOS プラットフォームに、IPv6 マルチキャスト転送テーブルおよび通知を読み取るインターフェイスを提供することです。MFIB が提供する情報には、明確に定義された転送セマンティクスが含まれています。この情報は、プラットフォームが特定のハードウェアまたはソフトウェア転送メカニズムに容易に変換できる設計になっています。

ネットワーク内でルーティングまたはトポロジが変更されると、IPv6 ルーティング テーブルがアップデートされ、これらの変更が MFIB に反映されます。MFIB は、IPv6 ルーティング テーブル内の情報に基づいて、ネクストホップ アドレス情報を管理します。MFIB エントリとルーティング テーブル エントリの間には 1 対 1 の相互関係があるため、MFIB には既知のすべてのルートが含まれ、高速スイッチングや最適スイッチングなどのスイッチング パスに関連付けられているルート キャッシュ管理の必要がなくなります。

MFIB

（注） 分散 MFIB は、マスターが他のスタック メンバーに MFIB 情報を配布するスタック環境でのみ意味を持ちます。次のセクションでは、ラインカードは単にスタックのメンバー スイッチです。

MFIB（MFIB）は、分散型プラットフォーム上でマルチキャスト IPv6 パケットをスイッチングするために使用されます。また、MFIB には、ラインカード間での複製に関するプラットフォーム固有の情報も含まれることがあります。転送ロジックのコアを実装する基本 MFIB ルーチンは、すべての転送環境に共通です。

MFIB は、次の機能を実装します。

- ラインカードで生成されたデータ駆動型プロトコル イベントを PIM にリレーします。
- MFIB プラットフォーム アプリケーション プログラム インターフェイス（API）を提供し、ハードウェア アクセラレーション エンジンのプログラミングを担っている、プラットフォーム固有のコードに MFIB の変更を伝播します。また、この API には、ソフトウェアでパケットをスイッチングしたり（パケットがデータ駆動型イベントのトリガーとなっている場合に必要）、ソフトウェアにトラフィックの統計情報をアップロードしたりするエントリ ポイントも含まれています。

また、MFIB および MRIB サブシステムを組み合わせて使用すると、スイッチが各ラインカードで MFIB データベースの「カスタマイズ」コピーを保有したり、MFIB 関連のプラットフォーム固有の情報を RP からラインカードに転送したりできるようになります。

IPv6 マルチキャストのプロセス スイッチングおよび高速スイッチング

統合 MFIB は、IPv6 マルチキャストでの PIM-SM および PIM-SSM に対するファスト スイッチングおよびプロセス スイッチングの両サポートを提供するために使用されます。プロセス スイッチングでは、のが各パケットの調査、書き換え、および転送を行う必要があります。最初にパケットが受信され、システム メモリにコピーされます。次に、スイッチがルーティング テーブル内でレイヤ 3 ネットワーク アドレスを検索します。そのあと、レイヤ 2 フレームがネクストホップの宛先アドレスで書き換えられ、発信インターフェイスに送信されます。また、は、巡回冗長検査（CRC）も計算します。このスイッチング方式は、IPv6 パケットをスイッチングする方式の中でスケーラビリティが最も低い方式です。

IPv6 マルチキャストの高速スイッチングを使用すると、スイッチは、プロセス スイッチングよりも高いパケット転送パフォーマンスを実現できます。従来ルート キャッシュに格納される情報は、IPv6 マルチキャスト スイッチング用にいくつかのデータ構造に格納されます。これらのデータ構造では、ルックアップが最適化され、パケット転送を効率的に行えるようになっています。

IPv6 マルチキャスト転送では、PIM プロトコル ロジックで許可されていれば、最初のパケットのファスト スイッチングが行われます。IPv6 マルチキャストの高速スイッチングでは、MAC カプセル化ヘッダーが事前に計算されます。IPv6 マルチキャストの高速スイッチングでは、MFIB を使用して、IPv6 送信先プレフィックス ベースのスイッチング判定が行われます。IPv6 マルチキャストの高速スイッチングでは、MFIB に加えて、隣接関係テーブルを使用して、レイヤ 2 アドレッシング情報が付加されます。隣接関係テーブルでは、すべての MFIB エントリのレイヤ 2 ネクストホップ アドレスが管理されます。

隣接が検出されると、隣接関係テーブルにそのデータが入力されます。（ARP などを使用して）隣接エントリが作成されるたびに、その隣接ノードのリンク層ヘッダーが事前に計算され、隣接関係テーブルに格納されます。ルートが決定されると、そのヘッダーはネクストホップおよび対応する隣接エントリを指します。そのあと、そのヘッダーはパケット スイッチング時のカプセル化に使用されます。

ロード バランシングと冗長性の両方に対応するようにスイッチが設定されている場合など、ルートには送信先プレフィックスへの複数のパスが存在することがあります。解決されたパスごとに、そのパスのネクストホップ インターフェイスに対応する隣接へのポインタが追加されます。このメカニズムは、複数のパスでのロード バランシングに使用されます。

IPv6 マルチキャスト アドレス ファミリのマルチプロトコル BGP

IPv6 マルチキャスト アドレス ファミリのマルチプロトコル BGP 機能では、マルチプロトコル BGP for IPv6 拡張を提供し、IPv4 BGP と同じ機能と機能性をサポートします。マルチキャスト BGP に対する IPv6 拡張には、IPv6 マルチキャスト アドレス ファミリ、ネットワーク層到達可能性情報（NLRI）、および IPv6 アドレスを使用するネクスト ホップ（宛先へのパス内の次のスイッチ）属性のサポートが含まれています。

マルチキャスト BGP は、ドメイン間 IPv6 マルチキャストの配布を可能にする、拡張された BGP です。マルチプロトコル BGP では、複数のネットワーク層プロトコル アドレス ファミリ（IPv6 アドレス ファミリなど）および IPv6 マルチキャスト ルートに関するルーティング情報を伝送します。IPv6 マルチキャスト アドレス ファミリには、IPv6 PIM プロトコルによる RPF ルックアップに使用される複数のルートが含まれており、マルチキャスト BGP IPv6 は、同じドメイン間転送を提供します。ユニキャスト BGP が学習したルートは IPv6 マルチキャストには使用されないため、ユーザーは、BGP で IPv6 マルチキャストを使用する場合は、マルチプロトコル BGP for IPv6 マルチキャストを使用する必要があります。

マルチキャスト BGP 機能は、個別のアドレス ファミリ コンテキストを介して提供されます。Subsequent Address Family Identifier（SAFI）では、属性で伝送されるネットワーク層到達可能性情報のタイプに関する情報を提供します。マルチプロトコル BGP ユニキャストでは SAFI 1 メッセージを使用し、マルチプロトコル BGP マルチキャストでは SAFI 2 メッセージを使用します。SAFI 1 メッセージは、ルートは IP ユニキャストだけに使用でき、IP マルチキャストには使用できないことを示します。この機能があるため、IPv6 ユニキャスト RIB 内の BGP ルートは、IPv6 マルチキャスト RPF ルックアップでは無視される必要があります。

IPv6 マルチキャスト RPF ルックアップを使用して、異なるポリシーおよびトポロジ（IPv6 ユニキャストとマルチキャストなど）を設定するよう、個別の BGP ルーティング テーブルが維持されています。マルチキャスト RPF ルックアップは、IP ユニキャスト ルート ルックアップと非常によく似ています。

IPv6 マルチキャスト BGP テーブルと関連付けられている MRIB はありません。ただし、必要な場合、IPv6 マルチキャスト BGP は、ユニキャスト IPv6 RIB で動作します。マルチキャスト BGP では、IPv6 ユニキャスト RIB へのルートの挿入や更新は行いません。

IPv6 マルチキャストの実装

IPv6 マルチキャスト ルーティングのイネーブル化

IPV6 マルチキャストルーティングを有効にするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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**	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 multicast-routing** 例：	すべての IPv6 対応インターフェイスでマルチキャスト ルーティングをイネーブルにし、イネーブルに

	コマンドまたはアクション	目的
	デバイス(config)# **ipv6 multicast-routing**	なっているすべてのスイッチ インターフェイスで PIM および MLD に対してマルチキャスト転送をイネーブルにします。
ステップ 4	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MLD プロトコルのカスタマイズおよび確認

インターフェイスでの MLD のカスタマイズおよび確認

インターフェイスの MLD をカスタマイズして確認するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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**	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： デバイス(config)# **interface GigabitEthernet 1/0/1**	インターフェイスのタイプと番号を指定し、スイッチ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	**ipv6 mld join-group** [*group-address*] [**include** | **exclude**] {*source-address* | **source-list** [*acl*]} 例： デバイス(config-if)# **ipv6 mld join-group FF04::10**	指定したグループおよび送信元に対して MLD レポートを設定します。
ステップ 5	**ipv6 mld access-group** *access-list-name* 例： デバイス(config-if)# **ipv6 access-list acc-grp-1**	ユーザーに IPv6 マルチキャストの受信側アクセス コントロールの実行を許可します。

	コマンドまたはアクション	目的
ステップ 6	**ipv6 mld static-group** [*group-address*] [**include** | **exclude**] {*source-address* | source-list [*acl*]} 例： `デバイス(config-if)# ipv6 mld static-group ff04::10 include 100::1`	指定したインターフェイスにマルチキャスト グループのトラフィックをスタティックに転送し、MLD ジョイナがインターフェイスに存在するかのようにインターフェイスが動作するようにします。
ステップ 7	**ipv6 mld query-max-response-time** *seconds* 例： `デバイス(config-if)# ipv6 mld query-timeout 130`	スイッチがインターフェイスのクエリアとして引き継ぐまでのタイムアウト値を設定します。
ステップ 8	**exit** 例： `デバイス(config-if)# exit`	このコマンドを 2 回入力して、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 モードを開始します。
ステップ 9	**show ipv6 mld groups [link-local]** [*group-name* | *group-address*] [*interface-type interface-number*] [**detail** | **explicit**] 例： `デバイス# show ipv6 mld groups GigabitEthernet 1/0/1`	スイッチに直接接続されており、MLD を介して学習したマルチキャスト グループを表示します。
ステップ 10	**show ipv6 mld groups summary** 例： `デバイス# show ipv6 mld groups summary`	MLD キャッシュに存在する (*, G) および (S, G) メンバーシップ レポートの番号を表示します。
ステップ 11	**show ipv6 mld interface** [*type number*] 例： `デバイス# show ipv6 mld interface GigabitEthernet 1/0/1`	インターフェイスのマルチキャスト関連情報を表示します。
ステップ 12	**debug ipv6 mld** [*group-name* | *group-address* | *interface-type*] 例： `デバイス# debug ipv6 mld`	MLD プロトコル アクティビティに対するデバッグをイネーブルにします。
ステップ 13	**debug ipv6 mld explicit** [*group-name* | *group-address* 例：	ホストの明示的トラッキングに関連する情報を表示します。

	コマンドまたはアクション	目的
	デバイス# **debug ipv6 mld explicit**	
ステップ 14	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MLD グループ制限の実装

インターフェイス単位の MLD 制限とグローバル MLD 制限は相互に独立して機能します。インターフェイス単位の MLD 制限とグローバル MLD 制限の両方を同じスイッチで設定できます。MLD 制限の数は、グローバルの場合もインターフェイス単位の場合も、デフォルトでは設定されません。ユーザーが制限を設定する必要があります。インターフェイス単位のステート制限またはグローバル ステート制限を超えるメンバーシップ レポートは無視されます。

MLD グループ制限のグローバルな実装

MLD グループ制限をグローバルに実装するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 mld** [*vrf vrf-name*] **state-limit** *number*
4. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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 mld** [*vrf vrf-name*] **state-limit** *number* 例： デバイス(config)# **ipv6 mld state-limit 300**	MLD ステートの数をグローバルに制限します。
ステップ 4	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MLD グループ制限のインターフェイス単位での実装

MLD グループ制限をインターフェイスごとに実装するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface type** *number*
4. **ipv6 mld limit** *number* [**except**]*access-list*
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 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： `デバイス# 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： `デバイス(config)# interface GigabitEthernet 1/0/1`	インターフェイスのタイプと番号を指定し、スイッチ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	**ipv6 mld limit** *number* [**except**]*access-list* 例： `デバイス(config-if)# ipv6 mld limit 100`	MLD ステートの数をインターフェイス単位で制限します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

受信側の明示的トラッキングによってホストの動作を追跡するための設定

明示的トラッキング機能を使用すると、スイッチが IPv6 ネットワーク内のホストの動作を追跡できるようになります。また、高速脱退メカニズムを MLD バージョン 2 のホスト レポートで使用できるようになります。

受信側の明示的トラッキングを設定してホストの動作を追跡するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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**	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： デバイス(config)# **interface GigabitEthernet 1/0/1**	インターフェイスのタイプと番号を指定し、スイッチ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	**ipv6 mld explicit-tracking** *access-list-name* 例： デバイス(config-if)# **ipv6 mld explicit-tracking list1**	ホストの明示的トラッキングをイネーブルにします。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MLD トラフィック カウンタのリセット

MLD トラフィックカウンタをリセットするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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	**clear ipv6 mld traffic** 例： デバイス# **clear ipv6 mld traffic**	すべての MLD トラフィック カウンタをリセットします。
ステップ 4	**show ipv6 mld traffic** 例： デバイス# **show ipv6 mld traffic**	MLD トラフィック カウンタを表示します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MLD インターフェイス カウンタのクリア

MLD インターフェイスカウンタをクリアするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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	**clear ipv6 mld counters** *interface-type* 例： デバイス# **clear ipv6 mld counters Ethernet1/0**	MLD インターフェイス カウンタをクリアします。
ステップ 4	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

PIM の設定

ここでは、PIM の設定方法について説明します。

PIM-SM の設定およびグループ範囲の PIM-SM 情報の表示

PIM-SM を設定し、グループ範囲の PIM-SM 情報を表示するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 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： `デバイス# 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 pim **rp-address** *ipv6-address*[*group-access-list*] 例： `デバイス(config)# ipv6 pim rp-address 2001:DB8::01:800:200E:8C6C acc-grp-1`	特定のグループ範囲の PIM RP のアドレスを設定します。
ステップ 4	**exit** 例： `デバイス(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、スイッチを特権 EXEC モードに戻します。
ステップ 5	**show ipv6 pim interface** [state-on] [**state-off**] [*type-number*] 例： `デバイス# show ipv6 pim interface`	PIM に対して設定されたインターフェイスに関する情報を表示します。
ステップ 6	**show ipv6 pim group-map** [*group-name* | group-address] | [*group-range* | *group-mask*] [**info-source {bsr** | **default** | **embedded-rp** | **static**}] 例： `デバイス# show ipv6 pim group-map`	IPv6 マルチキャスト グループ マッピング テーブルを表示します。
ステップ 7	**show ipv6 pim neighbor** [**detail**] [*interface-type interface-number* | **count**] 例： `デバイス# show ipv6 pim neighbor`	Cisco IOS ソフトウェアで検出された PIM ネイバーを表示します。

	コマンドまたはアクション	目的
ステップ 8	**show ipv6 pim range-list** [**config**] [*rp-address* | *rp-name*] 例： デバイス# **show ipv6 pim range-list**	IPv6 マルチキャスト範囲リストに関する情報を表示します。
ステップ 9	**show ipv6 pim tunnel** [*interface-type interface-number*] 例： デバイス# **show ipv6 pim tunnel**	インターフェイス上の PIM レジスタのカプセル化およびカプセル化解除トンネルに関する情報を表示します。
ステップ 10	**debug ipv6 pim** [*group-name* | *group-address* | **interface** *interface-type* | **bsr** | **group** | **mvpn** | **neighbor**] 例： デバイス# **debug ipv6 pim**	PIM プロトコル アクティビティに対するデバッグをイネーブルにします。
ステップ 11	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

PIM オプションの設定

PIM オプションを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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 pim spt-threshold infinity** [**group-list** *access-list-name*] 例： デバイス(config)# **ipv6 pim spt-threshold infinity group-list acc-grp-1**	PIM リーフ スイッチが指定したグループの SPT に加入するタイミングを設定します。

	コマンドまたはアクション	目的
ステップ 4	**ipv6 pim accept-register** { **list** *access-list* | **route-map** *map-name*} 例： デバイス(config)# **ipv6 pim accept-register route-map reg-filter**	RP のレジスタを許可または拒否します。
ステップ 5	**interface** *type number* 例： デバイス(config)# **interface GigabitEthernet 1/0/1**	インターフェイスのタイプと番号を指定し、スイッチ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 6	**ipv6 pim dr-priority** *value* 例： デバイス(config-if)# **ipv6 pim dr-priority 3**	PIM スイッチの DR プライオリティを設定します。
ステップ 7	**ipv6 pim hello-interval** *seconds* 例： デバイス(config-if)# **ipv6 pim hello-interval 45**	インターフェイスにおける PIM hello メッセージの頻度を設定します。
ステップ 8	**ipv6 pim join-prune-interval** *seconds* 例： デバイス(config-if)# **ipv6 pim join-prune-interval 75**	指定したインターフェイスに対して join および prune の定期的な通知間隔を設定します。
ステップ 9	**exit** 例： デバイス(config-if)# **exit**	このコマンドを 2 回入力して、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 モードを開始します。
ステップ 10	**ipv6 pim join-prune statistic** [*interface-type*] 例： デバイス(config-if)# **show ipv6 pim join-prune statistic**	各インターフェイスの最後の集約パケットに関する平均 join-prune 集約を表示します。
ステップ 11	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

PIM トラフィック カウンタのリセット

PIM が誤動作する場合、または予想される PIM パケット数が送受信されていることを確認するために、ユーザーは PIM トラフィック カウンタをクリアできます。トラフィック カウンタがクリアされたら、ユーザーは show ipv6 pim traffic コマンドを入力して、PIM が正しく機能していること、および PIM パケットが正しく送受信されていることを確認できます。

PIM トラフィックカウンタをリセットするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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	**clear ipv6 pim traffic** 例： デバイス# **clear ipv6 pim traffic**	PIM トラフィック カウンタをリセットします。
ステップ 4	**show ipv6 pim traffic** 例： デバイス# **show ipv6 pim traffic**	PIM トラフィック カウンタを表示します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

PIM トポロジ テーブルをクリアすることによる MRIB 接続のリセット

MRIB を使用するのに設定は不要です。ただし、特定の状況においては、ユーザーは PIM トポロジ テーブルをクリアして MRIB 接続をリセットし、MRIB 情報を確認する必要がある場合があります。

PIM トポロジテーブルをクリアして MRIB 接続をリセットするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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	**clear ipv6 pim topology** [*group-name* | *group-address*] 例： デバイス# **clear ipv6 pim topology FF04::10**	PIM トポロジ テーブルをクリアします。
ステップ 4	**show ipv6 mrib client** [**filter**] [**name** {*client-name* | *client-name* **: client-id**}] 例： デバイス# **show ipv6 mrib client**	インターフェイスのマルチキャスト関連情報を表示します。
ステップ 5	**show ipv6 mrib route** {**link-local** | **summary** | [*sourceaddress-or-name* | *] [*groupname-or-address*[*prefix-length*]]] 例： デバイス# **show ipv6 mrib route**	MRIB ルート情報を表示します。
ステップ 6	**show ipv6 pim topology** [*groupname-or-address* [*sourceaddress-or-name*] | **link-local** | **route-count** [**detail**]] 例： デバイス# **show ipv6 pim topology**	特定のグループまたはすべてのグループの PIM トポロジ テーブル情報を表示します。
ステップ 7	**debug ipv6 mrib client** 例： デバイス# **debug ipv6 mrib client**	MRIB クライアント管理アクティビティに対するデバッグをイネーブルにします。
ステップ 8	**debug ipv6 mrib io** 例：	MRIB I/O イベントに対するデバッグをイネーブルにします。

	コマンドまたはアクション	目的
	デバイス# **debug ipv6 mrib io**	
ステップ 9	**debug ipv6 mrib proxy** 例： デバイス# **debug ipv6 mrib proxy**	分散型スイッチ プラットフォームにおけるスイッチ プロセッサとラインカード間の MRIB プロキシ アクティビティに対するデバッグをイネーブルにします。
ステップ 10	**debug ipv6 mrib route** [*group-name* | *group-address*] 例： デバイス# **debug ipv6 mrib route**	MRIB ルーティング エントリ関連のアクティビティに関する情報を表示します。
ステップ 11	**debug ipv6 mrib table** 例： デバイス# **debug ipv6 mrib table**	MRIB テーブル管理アクティビティに対するデバッグをイネーブルにします。
ステップ 12	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

PIM IPv6 スタブ ルーティングの設定

PIM スタブ ルーティング機能は、ディストリビューション レイヤとアクセス レイヤの間のマルチキャスト ルーティングをサポートします。サポート対象の PIM インターフェイスは、アップリンク PIM インターフェイスと PIM パッシブ インターフェイスの 2 種類です。PIM パッシブ モードに設定されているルーテッド インターフェイスは、PIM 制御トラフィックの通過も転送も行いません。通過させたり転送したりするのは MLD トラフィックだけです。

PIM IPv6 スタブ ルーティングの設定時の注意事項

- PIM スタブ ルーティングを設定する前に、スタブ ルータと中央のルータの両方に IPv6 マルチキャスト ルーティングが設定されている必要があります。また、スタブ ルータのアップリンク インターフェイス上に、PIM モード（スパースモード）が設定されている必要があります。
- PIM スタブ ルータは、ディストリビューション ルータ間の伝送トラフィックのルーティングは行いません。ユニキャスト（EIGRP）スタブ ルーティングではこの動作が強制されます。PIM スタブ ルータの動作を支援するためにユニキャスト スタブ ルーティングを設定する必要があります。詳細については、「*EIGRP* スタブ ルーティング」の項を参照してください。
- 直接接続されたマルチキャスト（MLD）レシーバおよび送信元だけが、レイヤ 2 アクセス ドメインで許可されます。アクセス ドメインでは、PIM プロトコルはサポートされません。
- 冗長 PIM スタブ ルータ トポロジーはサポートされません。

IPv6 PIM ルーティングのデフォルト設定

次の表に、デバイス の IPv6 PIM ルーティングのデフォルト設定を示します。

表 *8:* マルチキャスト ルーティングのデフォルト設定

機能	デフォルト設定
マルチキャスト ルーティング	すべてのインターフェイスでディ
PIM のバージョン	バージョン 2
PIM モード	モードは未定義
PIM スタブ ルーティング	未設定
PIM RP アドレス	未設定
PIM ドメイン境界	ディセーブル。
PIM マルチキャスト境界	なし
候補 BSR	ディセーブル。
候補 RP	ディセーブル。
SPT しきい値レート	0 kb/s
PIM ルータ クエリー メッセージ インターバル	30 秒

IPv6 PIM スタブ ルーティングのイネーブル化

IPV6 PIM スタブルーティングをイネーブルにするには、次の手順を実行します。

始める前に

PIM スタブ ルーティングは IPv6 ではデフォルトでディセーブルです。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 multicast pim-passive-enable**
4. **interface** *interface-id*
5. **ipv6 pim**
6. **ipv6 pim** {**bsr**} | {**dr-priority** | *value*} | {**hello-interval** | *seconds*} | {**join-prune-interval** | *seconds*} | {**passive**}
7. **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	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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 multicast pim-passive-enable** 例： デバイス(config-if)# **ipv6 multicast pim-passive-enable**	スイッチで IPv6 マルチキャスト PIM ルーティングをイネーブルにします。
ステップ 4	**interface** *interface-id* 例： デバイス(config)# **interface gigabitethernet 9/0/6**	PIM スタブ ルーティングをイネーブルにする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。 次のいずれかのインターフェイスを指定する必要があります。 • ルーテッドポート：レイヤ 3 ポートとして **no switchport** インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。また、インターフェイスの IP PIM スパース モードをイネーブルにして、静的に接続されたメンバーとしてインターフェイスを MLD スタティック グループに結合する必要があります。 • SVI：**interface vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。また、VLAN 上で IP PIM スパース モードをイネーブルにして、静的に接続されたメンバーとして VLAN を MLD スタティック グループに結合し、VLAN、MLD スタティック グループ、および物理インターフェイスで MLD スヌーピングをイネーブルにする必要があります。

	コマンドまたはアクション	目的
		これらのインターフェイスには、IPv6アドレスを割り当てる必要があります。
ステップ 5	**ipv6 pim** 例： `デバイス(config-if)# ipv6 pim`	インターフェイスで PIM をイネーブルにします。
ステップ 6	**ipv6 pim** {**bsr**} | {**dr-priority** | *value*} | {**hello-interval** | *seconds*} | {**join-prune-interval** | *seconds*} | {**passive**} 例： `デバイス(config-if)# ipv6 pim bsr|dr-priority|hello-interval|join-prune-interval|passive`	インターフェイスでさまざまなPIMスタブ機能を設定します。 **bsr** を入力して PIM スイッチの BSR を設定します。 **dr-priority** を入力して、PIM スイッチの DR 優先順位を設定します。 **hello-interval** を入力して、インターフェイスの PIM hello メッセージの頻度を設定します。 **join-prune-interval** を入力して、指定したインターフェイスに対して join および prune の定期的な通知間隔を設定します。 **passive** を入力して、パッシブモードの PIM を設定します。
ステップ 7	**end** 例： `デバイス(config-if)# end`	特権 EXEC モードに戻ります。

IPv6 PIM スタブ ルーティングのモニター

表 *9: PIM* スタブ設定の *show* コマンド

コマンド	目的
show ipv6 pim interface `デバイス# show ipv6 pim interface`	各インターフェイスで有効になっている PIM スタブを表示します。
show ipv6 mld groups `デバイス# show ipv6 mld groups`	特定のマルチキャスト グループを結合した対象クライアントを表示します。

コマンド	目的
show ipv6 mroute デバイス# **show ipv6 mroute**	ソースから対象クライアントへのマルチキャスト ストリーム転送を確認します。

BSR の設定

ここでの作業について、以下に説明します。

BSR の設定および BSR 情報の確認

BSR 情報を設定および確認するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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 pim bsr candidate bsr** *ipv6-address*[*hash-mask-length*] [**priority** *priority-value*] 例： デバイス(config)# **ipv6 pim bsr candidate bsr 2001:DB8:3000:3000::42 124 priority 10**	候補 BSR になるようにスイッチを設定します。
ステップ 4	**interface** *type number* 例： デバイス(config)# **interface GigabitEthernet 1/0/1**	インターフェイスのタイプと番号を指定し、スイッチ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 5	**ipv6 pim bsr border** 例： デバイス(config-if)# **ipv6 pim bsr border**	インターフェイスのタイプと番号を指定し、スイッチ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 6	**exit** 例： デバイス(config-if)# **exit**	このコマンドを2回入力して、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 モードを開始します。
ステップ 7	**show ipv6 pim** bsr {**election** | **rp-cache** | **candidate-rp**} 例： デバイス(config-if)# **show ipv6 pim bsr election**	PIM BSR プロトコル処理に関連する情報を表示します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

BSR への PIM RP アドバタイズメントの送信

BSR に PIM RP アドバタイズメントを送信するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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 pim bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] **[priority** *priority-value*] [**interval** seconds] 例： デバイス(config)# **ipv6 pim bsr candidate rp 2001:DB8:3000:3000::42 priority 0**	BSR に PIM RP アドバタイズメントを送信します。
ステップ 4	**interface** *type number* 例： デバイス(config)# **interface GigabitEthernet 1/0/1**	インターフェイスのタイプと番号を指定し、スイッチ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 5	**ipv6 pim bsr border** 例： デバイス(config-if)# **ipv6 pim bsr border**	指定したインターフェイスの任意のスコープの全 BSM に対して境界を設定します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

限定スコープ ゾーン内で BSR を使用できるようにするための設定

スコープゾーン内で使用する BSR を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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 pim bsr candidate rp** *ipv6-address* [*hash-mask-length*] [**priority** priority-value] 例： デバイス(config)# **ipv6 pim bsr candidate bsr 2001:DB8:1:1:4**	候補 BSR になるようにスイッチを設定します。
ステップ 4	**ipv6 pim bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** seconds] 例： デバイス(config)# **ipv6 pim bsr candidate rp 2001:DB8:1:1:1 group-list list scope 6**	BSR に PIM RP アドバタイズメントを送信するように候補 RP を設定します。

	コマンドまたはアクション	目的
ステップ 5	**interface** *type number* 例： `デバイス(config-if)# interface GigabitEthernet 1/0/1`	インターフェイスのタイプと番号を指定し、スイッチ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 6	**ipv6 multicast boundary scope** *scope-value* 例： `デバイス(config-if)# ipv6 multicast boundary scope 6`	指定されたスコープのインターフェイスでマルチキャスト境界を設定します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

BSR スイッチにスコープと RP のマッピングをアナウンスさせるための設定

IPv6 BSR スイッチは、スコープと RP のマッピングを候補 RP メッセージから学習するのではなく、直接アナウンスするようにスタティックに設定できます。ユーザーは、スコープと RP のマッピングをアナウンスするように BSR スイッチを設定して、BSR をサポートしていない RP がその BSR にインポートされるように設定できます。この機能をイネーブルにすると、ローカルの候補 BSR スイッチの既知のリモート RP が、企業の BSR ドメインの外部に配置されている RP を学習できるようになります。

スコープと RP のマッピングをアナウンスするように BSR スイッチを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 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： `デバイス# 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 pim bsr announced rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] 例：	指定した候補 RP の BSR からスコープと RP のマッピングを直接アナウンスします。

	コマンドまたはアクション	目的
	デバイス(config)# **ipv6 pim bsr announced rp 2001:DB8:3000:3000::42 priority 0**	
ステップ 4	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SSM マッピングの設定

SSM マッピング機能をイネーブルにすると、DNS ベースの SSM マッピングが自動的にイネーブルになります。つまり、スイッチは、マルチキャスト MLD バージョン 1 レポートの送信元を DNS サーバーから検索するようになります。

スイッチ設定に応じて、DNS ベースのマッピングまたはスタティック SSM マッピングのいずれかを使用できます。スタティック SSM マッピングを使用する場合は、複数のスタティック SSM マッピングを設定できます。複数のスタティック SSM マッピングを設定すると、一致するすべてのアクセス リストの送信元アドレスが使用されるようになります。

（注） DNS ベースの SSM マッピングを使用するには、スイッチは正しく設定されている DNS サーバーを少なくとも 1 つ見つける必要があります。スイッチは、その DNS サーバーに直接接続される可能性があります。

SSM マッピングを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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 mld ssm-map enable** 例： デバイス(config)# **ipv6 mld ssm-map enable**	設定済みの SSM 範囲内のグループに対して SSM マッピング機能をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**no ipv6 mld ssm-map query dns** 例： `デバイス(config)# no ipv6 mld ssm-map query dns`	DNS ベースの SSM マッピングをディセーブルにします。
ステップ 5	**ipv6 mld ssm-map static** *access-list source-address* 例： `デバイス(config-if)# ipv6 mld ssm-map static SSM_MAP_ACL_2 2001:DB8:1::1`	スタティック SSM マッピングを設定します。
ステップ 6	**exit** 例： `デバイス(config-if)# exit`	グローバル コンフィギュレーション モードを終了し、スイッチを特権 EXEC モードに戻します。
ステップ 7	**show ipv6 mld ssm-map** [*source-address*] 例： `デバイス(config-if)# show ipv6 mld ssm-map`	SSM マッピング情報を表示します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スタティック mroute の設定

IPv6 のスタティック マルチキャスト ルート（mroute）は、IPv6 スタティック ルートの拡張として実装できます。スイッチを設定する際には、ユニキャスト ルーティング専用としてスタティック ルートを使用するか、マルチキャスト RPF 選択専用としてスタティック マルチキャスト ルートを使用するか、またはユニキャスト ルーティングとマルチキャスト RPF 選択の両方にスタティック ルートを使用するように設定できます。

静的 mroute を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 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：	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
	デバイス# **configure terminal**	
ステップ 3	**ipv6 route** {*ipv6-prefix / prefix-length ipv6-address* | *interface-type interface-number ipv6-address*]} [*administrative-distance*] [*administrative-multicast-distance* | *unicast* | *multicast*] [**tag** *tag*] 例： デバイス(config)# **ipv6 route 2001:DB8::/64 6::6 100**	スタティック IPv6 ルートを確立します。この例は、ユニキャスト ルーティングとマルチキャスト RPF 選択の両方に使用されるスタティック ルートを示しています。
ステップ 4	**exit** 例： デバイス# **exit**	グローバル コンフィギュレーション モードを終了し、スイッチを特権 EXEC モードに戻します。
ステップ 5	**show ipv6 mroute** [link-local | [*group-name* | *group-address* [*source-address* | *source-name*]] **[summary]** [**count**] 例： デバイス# **show ipv6 mroute ff07::1**	IPv6 マルチキャスト ルーティング テーブルの内容を表示します。
ステップ 6	**show ipv6 mroute** [**link-local** | *group-name* | *group-address*] **active** [*kbps*] 例： デバイス(config-if)# **show ipv6 mroute active**	スイッチ上のアクティブなマルチキャスト ストリームを表示します。
ステップ 7	**show ipv6 rpf** [*ipv6-prefix*] 例： デバイス(config-if)# **show ipv6 rpf 2001::1:1:2**	特定のユニキャスト ホスト アドレスおよびプレフィックスの RPF 情報を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IPv6 マルチキャストでの MFIB の使用

IPv6 マルチキャスト ルーティングをイネーブルにすると、マルチキャスト転送が自動的にイネーブルになります。

IPv6 マルチキャストでの MFIB の動作の確認

IPv6 マルチキャストで MFIB の動作を確認するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**show ipv6 mfib** [**linkscope** | **verbose** | *group-address-name* | *ipv6-prefix / prefix-length* | *source-address-name* | **count** | **interface** | **status** | **summary**] 例： デバイス# **show ipv6 mfib**	IPv6 MFIB での転送エントリおよびインターフェイスを表示します。
ステップ 3	**show ipv6 mfib** [all | linkscope | group-name | group-address [source-name | source-address]] **count** 例： デバイス# **show ipv6 mfib ff07::1**	IPv6 マルチキャスト ルーティング テーブルの内容を表示します。
ステップ 4	**show ipv6 mfib interface** 例： デバイス# **show ipv6 mfib interface**	IPv6マルチキャスト対応インターフェイスとその転送ステータスに関する情報を表示します。
ステップ 5	**show ipv6 mfib status** 例： デバイス# **show ipv6 mfib status**	一般的なMFIB設定と動作ステータスを表示します。
ステップ 6	**show ipv6 mfib summary** 例： デバイス# **show ipv6 mfib summary**	IPv6 MFIB エントリおよびインターフェイスの数に関するサマリー情報を表示します。
ステップ 7	**debug ipv6 mfib** [*group-name* | *group-address*] [**adjacency** | **db** | **fs** | **init** | **interface** | **mrib** [**detail**] | **nat** | **pak** | **platform** | **ppr** | **ps** | **signal** | **table**] 例：	IPv6 MFIB に対するデバッグ出力をイネーブルにします。

	コマンドまたはアクション	目的
	デバイス# **debug ipv6 mfib FF04::10 pak**	

MFIB トラフィック カウンタのリセット

MFIB トラフィックカウンタをリセットするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**clear ipv6 mfib counters** [*group-name* | **group-address** [*source-address* | *source-name*]] 例： デバイス# **clear ipv6 mfib counters FF04::10**	アクティブなすべての MFIB トラフィック カウンタをリセットします。

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
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

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	リンク
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

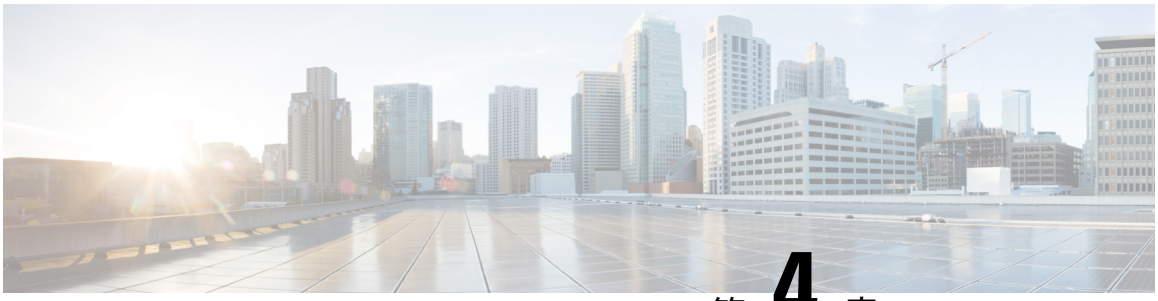
機能情報

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 *10 : IPv6* マルチキャストの機能情報

機能名	リリース	機能情報
IPv6 マルチキャスト	Cisco IOS XE Everest 16.5.1a	IPv6 向けマルチキャスト機能



第 4 章

IPv6 クライアントの IP アドレス ラーニング

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クライアントを設定します。

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、クライアントの IPv4 および IPv6 アドレス、device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、device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。device 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。

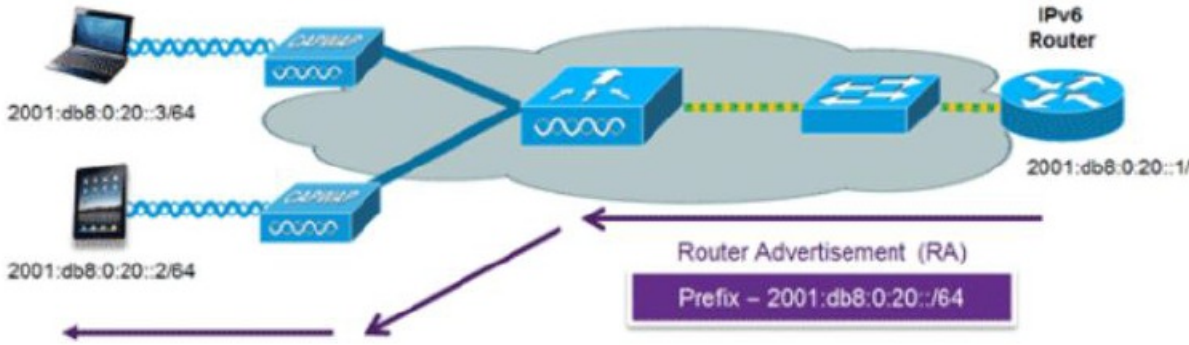
次のように、ステートレス アドレス自動設定（SLAAC）は設定されています。

- 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 *3 : SLAAC* アドレス割り当て

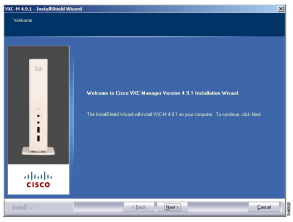


Cisco 対応 IPv6 ルータからの次の Cisco IOS コンフィギュレーション コマンドを使用して、SLAAC のアドレッシングとルータ アドバタイズメントをイネーブルにします。

```
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
```

ステートフル DHCPv6 アドレス割り当て

図 *4 :* 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 サーバー、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 に対して同じように動作します。つまり固有のアドレスを、SLAAC のとおりにアドレスの最後の 64 ビットを生成するクライアントではなく、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 デバイスのステートフル 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 サーバーのステートフル 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
```

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。

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。

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。

ネイバー探索抑制

クライアントの IPv6 アドレスは、deviceによってキャッシュされます。deviceが IPv6 アドレスを検索する NS マルチキャストを受信して、device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、device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） device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。

deviceにクライアントの IPv6 アドレスがない場合、deviceは NA で応答せず、NS パケットを転送します。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、device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、転送します。このパケットは、目的の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。

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、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 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deviceで行われます。deviceで RA メッセージをドロップするようにdevice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
```

IPv6 ユニキャストの設定

IPv6 ユニキャストはスイッチ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。

IPv6 ユニキャストを設定するには、次の手順を実行します。

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。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast routing**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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 unicast routing** 例： デバイス(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

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、deviceで RA ガード ポリシーを設定します。

RA ガードポリシーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 nd raguard policy raguard-router**
4. **trustedport**
5. **device-role router**
6. **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	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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 raguard policy raguard-router** 例： デバイス(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。
ステップ 4	**trustedport** 例： デバイス(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 5	**device-role router** 例： デバイス(config-ra-guard)# **device-role router**	ポートに接続されているデバイスの役割を指定します。
ステップ 6	**exit** 例： デバイス(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。

RA ガードポリシーの適用

device 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。

RA ガードポリシーを適用するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface tengigabitethernet 1/0/1**
4. **ipv6 nd raguard attach-policy raguard-router**
5. **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	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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 tengigabitethernet 1/0/1** 例： デバイス(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。
ステップ 4	**ipv6 nd raguard attach-policy raguard-router** 例： デバイス(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 5	**exit** 例： デバイス(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。

IPv6 スヌーピングの設定

IPv6 スヌーピングはスイッチで常にイネーブルにする必要があります。

IPv6 スヌーピングを設定するには、次の手順を実行します。

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。

手順の概要

1. **enable**
2. **configure terminal**
3. **vlan configuration 1**
4. **ipv6 snooping**
5. **ipv6 nd suppress**
6. **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	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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	**vlan configuration 1** 例： デバイス(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 4	**ipv6 snooping** 例： デバイス(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 5	**ipv6 nd suppress** 例： デバイス(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 6	**exit** 例： デバイス(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。

IPv6 ND 抑制ポリシーの設定

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。

IPv6 ND 抑制ポリシーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 nd suppress 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	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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： デバイス(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。

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。

VLAN/PortChannel で IPv6 スヌーピングを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **vlan config901**
4. **ipv6 nd suppress**
5. **end**
6. **interface gi1/0/1**
7. **ipv6 nd suppress**
8. **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	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 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： `デバイス# 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	**vlan config901** 例： `デバイス(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。
ステップ 4	**ipv6 nd suppress** 例： `デバイス(config-vlan)# ipv6 nd suppress`	VLAN に IPv6 nd 抑制を適用します。
ステップ 5	**end** 例： `デバイス(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 6	**interface gi1/0/1** 例： `デバイス(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 7	**ipv6 nd suppress** 例： `デバイス(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 8	**end** 例： `デバイス(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。

インターフェイスでの IPv6 の設定

インターフェイスで IPv6 を設定するには、次の手順を実行します。

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。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface vlan 1**
4. **ip address fe80::1 link-local**
5. **ipv6 enable**
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	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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 vlan 1** 例： デバイス(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 4	**ip address fe80::1 link-local** 例： デバイス(config-if)# **ip address 198.51.100.1 255.255.255.0** デバイス(config-if)# **ipv6 address fe80::1 link-local** デバイス(config-if)# **ipv6 address 2001:DB8:0:1:FFFF:1234::5/64** デバイス(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 5	**ipv6 enable** 例： デバイス(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。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： デバイス(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

インターフェイス上で DHCP プールを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool Vlan21**
4. **address prefix 2001:DB8:0:1:FFFF:1234::/64 lifetime 300 10**
5. **dns-server 2001:100:0:1::1**
6. **domain-name example.com**
7. **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	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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 dhcp pool Vlan21** 例： デバイス(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 4	**address prefix 2001:DB8:0:1:FFFF:1234::/64 lifetime 300 10** 例： デバイス(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。

	コマンドまたはアクション	目的
ステップ 5	**dns-server 2001:100:0:1::1** 例： デバイス(config-dhcpv6)# **dns-server 2001:20:21::1**	DHCP プールの DNS サーバーを設定します。
ステップ 6	**domain-name example.com** 例： デバイス(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 7	**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。

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）

DHCPを使用せずにステートレス自動アドレス設定を構成するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface vlan 1**
4. **ip address fe80::1 link-local**
5. **ipv6 enable**
6. **no ipv6 nd managed-config-flag**
7. **no ipv6 nd other-config-flag**
8. **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	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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 vlan 1** 例： `デバイス(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 4	**ip address fe80::1 link-local**
	例：
	`デバイス(config-if)# ip address 198.51.100.1 255.255.255.0`
	`デバイス(config-if)# ipv6 address fe80::1 link-local`
	`デバイス(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`デバイス(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 5	**ipv6 enable** 例： `デバイス(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 6	**no ipv6 nd managed-config-flag**
	例：
	`デバイス(config)# interface vlan 1`
	`デバイス(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 7	**no ipv6 nd other-config-flag** 例： `デバイス(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 8	**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。

DHCP を使用したステートレス自動アドレス設定の指定

DHCP を使用してステートレス自動アドレス設定を構成するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface vlan 1**
4. **ip address fe80::1 link-local**
5. **ipv6 enable**

6. **no ipv6 nd managed-config-flag**
7. **ipv6 nd other-config-flag**
8. **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	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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 vlan 1** 例： デバイス(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 4	**ip address fe80::1 link-local** 例： デバイス(config-if)# **ip address 198.51.100.1 255.255.255.0** デバイス(config-if)# **ipv6 address fe80::1 link-local** デバイス(config-if)# **ipv6 address 2001:DB8:0:1:FFFF:1234::5/64** デバイス(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 5	**ipv6 enable** 例： デバイス(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 6	**no ipv6 nd managed-config-flag** 例： デバイス(config)# **interface vlan 1** デバイス(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 7	**ipv6 nd other-config-flag** 例： デバイス(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。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： デバイス(config)# **end**	インターフェイス モードを終了します。

ステートフル DHCP のローカル設定

次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。 デバイス

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **ipv6 dhcp pool IPv6_DHCPPOOL**
5. **address prefix 2001:DB8:0:1:FFFF:1234::/64**
6. **dns-server 2001:100:0:1::1**
7. **domain-name example.com**
8. **exit**
9. **interface vlan1**
10. **description IPv6-DHCP-Stateful**
11. **ipv6 address 2001:DB8:0:20::1/64**
12. **ip address 192.168.20.1 255.255.255.0**
13. **ipv6 nd prefix 2001:db8::/64 no-advertise**
14. **ipv6 nd managed-config-flag**
15. **ipv6 nd other-config-flag**
16. **ipv6 dhcp server IPv6_DHCPPOOL**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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	**ipv6 unicast-routing** 例： `デバイス(config)# ipv6 unicast-routing`	ユニキャスト用に IPv6 を設定します。
ステップ 4	**ipv6 dhcp pool IPv6_DHCPPOOL** 例： `デバイス (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 5	**address prefix 2001:DB8:0:1:FFFF:1234::/64** 例： `デバイス (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 6	**dns-server 2001:100:0:1::1** 例： `デバイス (config-dhcpv6)# dns-server 2001:100:0:1::1`	DHCP クライアントに DNS サーバーのオプションを提供します。
ステップ 7	**domain-name example.com** 例： `デバイス (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 8	**exit** 例： `デバイス (config-dhcpv6)# exit`	前のモードに戻ります。
ステップ 9	**interface vlan1** 例： `デバイス (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 10	**description IPv6-DHCP-Stateful** 例： `デバイス (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 11	**ipv6 address 2001:DB8:0:20::1/64** 例： `デバイス (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 12	**ip address 192.168.20.1 255.255.255.0** 例：	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
	デバイス (config-if)# **ip address 192.168.20.1 255.255.255.0**	
ステップ 13	**ipv6 nd prefix 2001:db8::/64 no-advertise** 例： デバイス (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 14	**ipv6 nd managed-config-flag** 例： デバイス (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 15	**ipv6 nd other-config-flag** 例： デバイス (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 16	**ipv6 dhcp server IPv6_DHCPPOOL** 例： デバイス (config-if)# **ipv6 dhcp server IPv6_DHCPPOOL**	インターフェイスに DHCP サーバーを設定します。

ステートフル DHCP の外部設定

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

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **dns-server 2001:100:0:1::1**
5. **domain-name example.com**
6. **exit**
7. **interface vlan1**
8. **description IPv6-DHCP-Stateful**
9. **ipv6 address 2001:DB8:0:20::1/64**
10. **ip address 192.168.20.1 255.255.255.0**
11. **ipv6 nd prefix 2001:db8::/64 no-advertise**
12. **ipv6 nd managed-config-flag**
13. **ipv6 nd other-config-flag**
14. **ipv6 dhcp_relaydestination 2001:DB8:0:20::2**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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 unicast-routing** 例： デバイス(config)# **ipv6 unicast-routing**	ユニキャスト用に IPv6 を設定します。
ステップ 4	**dns-server 2001:100:0:1::1** 例： デバイス(config-dhcpv6)# **dns-server 2001:100:0:1::1**	DHCP クライアントに DNS サーバーのオプションを提供します。
ステップ 5	**domain-name example.com** 例： デバイス(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 6	**exit** 例： デバイス(config-dhcpv6)# **exit**	前のモードに戻ります。
ステップ 7	**interface vlan1** 例： デバイス(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 8	**description IPv6-DHCP-Stateful** 例： デバイス(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 9	**ipv6 address 2001:DB8:0:20::1/64** 例： デバイス(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 10	**ip address 192.168.20.1 255.255.255.0** 例： デバイス(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 11	**ipv6 nd prefix 2001:db8::/64 no-advertise** 例： デバイス(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 12	**ipv6 nd managed-config-flag** 例： デバイス(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 13	**ipv6 nd other-config-flag** 例： デバイス(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 14	**ipv6 dhcp_relaydestination 2001:DB8:0:20::2** 例： デバイス(config-if)# **ipv6 dhcp_relay destination 2001:DB8:0:20::2**	インターフェイスに DHCP サーバーを設定します。

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、device上の IPv6 サービス設定を表示します。vlan21 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。

手順の概要

1. **show ipv6 dhcp pool**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show ipv6 dhcp pool** 例： デバイスshow ipv6 dhcp pool DHCPv6 pool: vlan21 Address allocation prefix: 2001:DB8:0:1:FFFF:1234::/64 valid 86400 preferred	device上の IPv6 サービス設定を表示します。

	コマンドまたはアクション	目的
	86400 (6 in use, 0 conflicts) DNS server: 2001:100:0:1::1 Domain name: example.com Active clients: 6	

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』

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

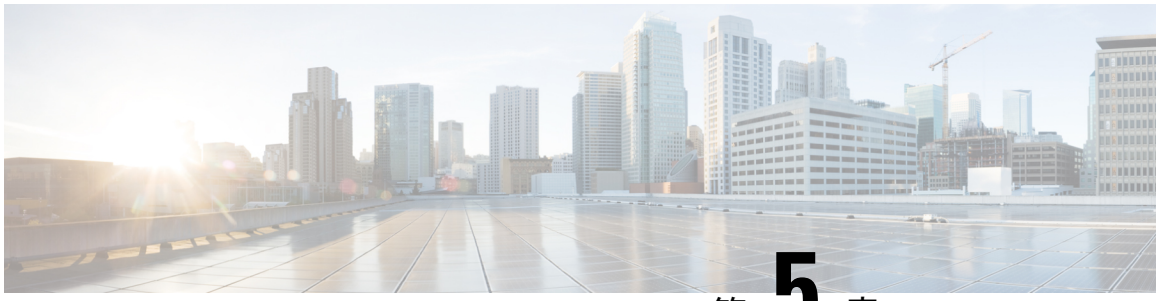
シスコのテクニカル サポート

説明	リンク
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 Everest 16.5.1a	この機能が導入されました。



第 5 章

IPv6 ACL の設定

IPv6 ACL の設定の前提条件

IP Version 6（IPv6）アクセス コントロール リスト（ACL）を作成し、それをインターフェイスに適用することによって、IPv6 トラフィックをフィルタリングできます。これは、IP Version 4（IPv4）の名前付き ACL を作成し、適用する方法と同じです。また、スイッチが Network Essentials ライセンスで稼働している場合、入力ルータ ACL を作成し、それを適用してレイヤ 3 管理トラフィックをフィルタリングすることもできます。

IPv6 ACL の設定の制約事項

IPv4 では、番号制の標準 IP ACL および拡張 IP ACL、名前付き IP ACL、および MAC ACL を設定できます。IPv6 がサポートするのは名前付き ACL だけです。

device は Cisco IOS がサポートする IPv6 ACL の大部分をサポートしますが、一部例外もあります。

- device は、**flowlabel**、**routing header**、および **undetermined-transport** というキーワードの照合をサポートしません。

- deviceは再帰 ACL（**reflect** キーワード）をサポートしません。
- deviceは IPv6 フレームに MAC ベース ACL を適用しません。
- ACL を設定する場合、ACL に入力されるキーワードには、それがプラットフォームでサポートされるかどうかにかかわらず、制限事項はありません。ハードウェア転送が必要なインターフェイス（物理ポートまたは SVI）に ACL を適用する場合、deviceはインターフェイスで ACL がサポートされるかどうかを判別します。サポートされない場合、ACL の付加は拒否されます。
- インターフェイスに適用される ACL に、サポートされないキーワードを持つアクセス コントロール エントリ（ACE）を追加しようとする場合、deviceは現在インターフェイスに適用されている ACL に ACE が追加されることを許可しません。

IPv6 ACL について

アクセス コントロール リスト（ACL）とは、特定のインターフェイスへのアクセスを制限するために使用されるルール セットのことです。ACLは device に設定され、管理インターフェイスおよび任意の動的インターフェイスに適用されます。

Web 認証用に事前認証 ACL を作成することもできます。このような ACL は、認証が完了するまでに特定のタイプのトラフィックを許可するために使用されます。

IPv6 ACL は、送信元、宛先、送信元ポート、宛先ポートなど、IPv4 ACL と同じオプションをサポートします。

（注） ネットワーク内で IPv4 トラフィックだけを有効にするには、IPv6 トラフィックをブロックします。つまり、すべての IPv6 トラフィックを拒否するように IPv6 ACL を設定し、これを特定またはすべての WLAN 上で適用します。

IPv6 ACL の概要

スイッチは、次の 2 種類の IPv6 ACL をサポートします。

- IPv6 ルータ ACL は、ルーテッド ポート、スイッチ仮想インターフェイス（SVI）、またはレイヤ 3 EtherChannel に設定できるレイヤ 3 インターフェイスのアウトバウンド トラフィックまたはインバウンド トラフィックでサポートされます。IPv6 ルータ ACL は、ルーティングされる IPv6 パケットに対してだけ適用されます。
- IPv6 ポート ACL は、レイヤ 2 インターフェイスのインバウンド トラフィックでだけサポートされます。IPv6 ポート ACL は、インターフェイスに着信するすべての IPv6 パケットに対して適用されます。

Network Essentials ライセンスで稼働しているスイッチは、入力ルータ IPv6 ACL だけをサポートしています。ポート ACL または出力ルータ IPv6 ACL はサポートされません。

（注） サポートされない IPv6 ACL を設定した場合、エラー メッセージが表示され、その設定は有効になりません。

スイッチは、IPv6 トラフィックの Virtual LAN（VLAN）ACL（VLAN マップ）をサポートしません。

1 つのインターフェイスに、IPv4 ACL および IPv6 ACL の両方を適用できます。IPv4 ACL の場合と同様に、IPv6 ポート ACL はルータ ACL よりも優先されます。

- SVI に入力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートに着信したパケットはポート ACL によってフィルタリングされます。その他のポートに着信したルーテッド IP パケットは、ルータ ACL によってフィルタリングされます。他のパケットはフィルタリングされません。
- SVI に出力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートに

  着信したパケットはポート ACL によってフィルタリングされます。発信ルーテッド IPv6 パケットは、ルータ ACL によってフィルタリングされます。他のパケットはフィルタリングされません。

（注） いずれかのポート ACL（IPv4、IPv6、または MAC）がインターフェイスに適用された場合、そのポート ACL を使用してパケットをフィルタリングし、ポート VLAN の SVI に適用されたルータ ACL は無視されます。

ACL のタイプ

ユーザーあたりの IPv6 ACL

ユーザあたりの ACL の場合、テキスト文字列として、完全アクセス制御エントリ（ACE）が ACS で設定されます。

フィルタ ID IPv6 ACL

filter-Id ACL の場合、完全な ACE および `acl name(filter-id)` がdeviceで設定され、`filter-id` のみが ACS で設定されます。

IPv6 ACL とスイッチ スタック

スタック マスターは IPv6 ACL をハードウェアでサポートし、IPv6 ACL をスタック メンバーに配信します。

（注） スイッチ スタック内で IPv6 を完全に機能させるには、すべてのスタック メンバで Network Advantage ライセンスを実行している必要があります。

新しいスイッチがスタック マスターを引き継ぐと、ACL 設定がすべてのスタック メンバーに配信されます。メンバ スイッチは、新しいスタック マスターによって配信された設定との同期をとり、不要なエントリを一掃します。

ACL の修正、インターフェイスへの適用、またはインターフェイスからの解除が行われると、スタック マスターは変更内容をすべてのスタック メンバーに配信します。

IPv6 ACL の設定

IPv6 トラフィックをフィルタリングする場合は、次の手順を実行します。

始める前に

IPv6 ACL を設定する場合は、事前にデュアル IPv4 および IPv6 SDM テンプレートのいずれかを選択する必要があります。

手順の概要

1. IPv6 ACL を作成し、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。
2. IPv6 ACL が、トラフィックをブロックする（deny）または通過させる（permit）よう設定します。
3. トラフィックをフィルタリングする必要があるインターフェイスに IPv6 ACL を適用します。
4. インターフェイスに IPv6 ACL を適用します。ルータ ACL では、ACL が適用されるレイヤ 3 インターフェイスにも IPv6 アドレスを設定する必要があります。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	IPv6 ACL を作成し、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 2	IPv6 ACL が、トラフィックをブロックする（deny）または通過させる（permit）よう設定します。	
ステップ 3	トラフィックをフィルタリングする必要があるインターフェイスに IPv6 ACL を適用します。	
ステップ 4	インターフェイスに IPv6 ACL を適用します。ルータ ACL では、ACL が適用されるレイヤ 3 インター	

	コマンドまたはアクション	目的
	フェイスにも IPv6 アドレスを設定する必要があります。	

IPv6 ACL のデフォルト設定

デフォルトでは、IPv6 ACL は設定または適用されていません。

他の機能およびスイッチとの相互作用

- IPv6 ルータ ACL がパケットを拒否するよう設定されている場合、パケットはルーティングされません。パケットのコピーがインターネット制御メッセージ プロトコル（ICMP）キューに送信され、フレームに ICMP 到達不能メッセージが生成されます。
- ブリッジド フレームがポート ACL によってドロップされる場合、このフレームはブリッジングされません。
- IPv4 ACL および IPv6 ACL の両方を 1 つのスイッチまたはスイッチ スタックに作成したり、同一インターフェイスに適用できます。各 ACL には一意の名前が必要です。設定済みの名前を使用しようとすると、エラー メッセージが表示されます。

  IPv4 ACL と IPv6 ACL の作成、および同一のレイヤ 2 インターフェイスまたはレイヤ 3 インターフェイスへの IPv4 ACL または IPv6 ACL の適用には、異なるコマンドを使用します。ACL を付加するのに誤ったコマンドを使用すると（例えば、IPv6 ACL の付加に IPv4 コマンドを使用するなど）、エラー メッセージが表示されます。

- MAC ACL を使用して、IPv6 フレームをフィルタリングできません。MAC ACL は非 IP フレームだけをフィルタリングできます。
- ハードウェア メモリが満杯の場合、設定済みの ACL を追加すると、パケットは CPU に転送され、ACL はソフトウェアで適用されます。ハードウェアが一杯になると、ACL がアンロードされたことを示すメッセージがコンソールに出力され、パケットはインターフェイスでドロップされます。

IPv6 ACL の設定方法

IPv6 ACL の作成

IPv6 ACL を作成するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**

3. **ipv6 access-list** *acl_name*
4. **{deny|permit} protocol**
5. **{deny|permit} tcp**
6. **{deny|permit} udp**
7. **{deny|permit} icmp**
8. **end**
9. **show ipv6 access-list**
10. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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 access-list** *acl_name* 例： デバイス# **ipv6 access-list access-list-name**	名前を使用して 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	**{deny|permit} protocol** 例： `{deny | permit} protocol {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length | any |host destination-ipv6-address} [operator [port-number]][dscp value] [fragments][log] [log-input] [routing][sequence value] [time-range name]`	条件が一致した場合にパケットを拒否する場合は deny、許可する場合は permit を指定します。次に、条件について説明します。 • protocol には、インターネット プロトコルの名前または番号を入力します。ahp、esp、icmp、ipv6、pcp、stcp、tcp、udp、または IPv6 プロトコル番号を表す 0 ～ 255 の整数を使用できます。 • source-ipv6-prefix/prefix-length または destination-ipv6-prefix/ prefix-length は、拒否条件または許可条件を設定する送信元または宛先 IPv6 ネットワークあるいはネットワーク クラスで、コロン区切りの 16 ビット値を使用した 16 進形式で指定します（RFC 2373 を参照）。 • IPv6 プレフィックス ::/0 の短縮形として、any を入力します。

	コマンドまたはアクション	目的
		• host source-ipv6-address または destination-ipv6-address には、拒否条件または許可条件を設定する送信元または宛先 IPv6 ホスト アドレスを入力します。アドレスはコロン区切りの 16 ビット値を使用した 16 進形式で指定します。 • （任意）operator には、指定のプロトコルの送信元ポートまたは宛先ポートを比較するオペランドを指定します。オペランドには、lt（より小さい）、gt（より大きい）、eq（等しい）、neq（等しくない）、range（包含範囲）があります。 source-ipv6-prefix/prefix-length 引数のあとの operator は、送信元ポートに一致する必要があります。destination-ipv6- prefix/prefix-length 引数のあとの operator は、宛先ポートに一致する必要があります。 • （任意）port-number は、0 ～ 65535 の 10 進数または TCP あるいは UDP ポートの名前です。TCP ポート名を使用できるのは、TCP のフィルタリング時だけです。UDP ポート名を使用できるのは、UDP のフィルタリング時だけです。 • （任意）dscp value を入力して、各 IPv6 パケット ヘッダーの Traffic Class フィールド内のトラフィック クラス値と DiffServ コード ポイント値を照合します。指定できる範囲は 0 ～ 63 です。 • （任意）fragments を入力して、先頭ではないフラグメントを確認します。このキーワードが表示されるのは、プロトコルが ipv6 の場合だけです。 • （任意）log を指定すると、エントリと一致するパケットに関するログ メッセージがコンソールに送信されます。log-input を指定すると、ログ エントリに入力インターフェイスが追加されます。ロギングはルータ ACL でだけサポートされます。

	コマンドまたはアクション	目的
		• （任意）routing を入力して、IPv6 パケットのルーティングを指定します。 • （任意）sequence value を入力して、アクセス リスト ステートメントのシーケンス番号を指定します。指定できる範囲は 1 ～ 4294967295 です。 • （任意）time-range name を入力して、拒否または許可ステートメントに適用される時間の範囲を指定します。
ステップ 5	**{deny|permit} tcp** 例： `{deny | permit} tcp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length | any |hostdestination-ipv6-address} [operator [port-number]][ack] [dscp value][established] [fin] [log][log-input] [neq {port |protocol}] [psh] [range{port | protocol}] [rst][routing] [sequence value] [syn] [time-range name][urg]`	（任意）TCP アクセス リストおよびアクセス条件を定義します。 TCP の場合は tcp を入力します。パラメータはステップ 3 で説明されているパラメータと同じですが、次に示すオプションのパラメータが追加されています。 • ack：確認応答（ACK）ビット セット • established：確立された接続。TCP データグラムに ACK または RST ビットが設定されている場合、照合が行われます。 • fin：終了ビット セット。送信元からのデータはそれ以上ありません。 • neq {port | protocol}：所定のポート番号上にないパケットだけを照合します。 • psh：プッシュ機能ビット セット • range {port | protocol}：ポート番号の範囲内のパケットだけを照合します。 • rst：リセット ビット セット • syn：同期ビット セット • urg：緊急ポインタ ビット セット
ステップ 6	**{deny|permit} udp** 例： `{deny | permit} udp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length`	（任意）UDP アクセス リストおよびアクセス条件を定義します。 ユーザ データグラム プロトコルの場合は、udp を入力します。UDP パラメータは TCP に関して説明されているパラメータと同じです。ただし、

	コマンドまたはアクション	目的
	``	any	hostdestination-ipv6-address} [operator [port-number]][dscp value] [log][log-input] [neq {port	protocol}] [range {port	protocol}] [routing][sequence value][time-range name]```	[operator [port]] のポート番号またはポート名は、UDP ポートの番号または名前でなければなりません。UDP の場合、established パラメータは無効です。
ステップ 7	**{deny|permit} icmp** 例： ```{deny	permit} icmp {source-ipv6-prefix/prefix-length	any	hostsource-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length	any	hostdestination-ipv6-address} [operator [port-number]][icmp-type [icmp-code] |icmp-message] [dscpvalue] [log] [log-input] [routing] [sequence value][time-range name]```	（任意）ICMP アクセス リストおよびアクセス条件を定義します。 インターネット制御メッセージ プロトコルの場合は、icmp を入力します。ICMP パラメータはステップ 3a の IP プロトコルの説明にあるパラメータとほとんど同じですが、ICMP メッセージ タイプおよびコード パラメータが追加されています。オプションのキーワードの意味は次のとおりです。 • icmp-type：ICMP メッセージ タイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。 • icmp-code：ICMP パケットを ICMP メッセージ コード タイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。 • icmp-message：ICMP パケットを ICMP メッセージ タイプ名または ICMP メッセージ タイプとコード名でフィルタリングする場合に入力します。ICMP メッセージのタイプ名およびコード名のリストについては、?キーを使用するか、またはこのリリースのコマンド リファレンスを参照してください。
ステップ 8	**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。
ステップ 9	**show ipv6 access-list** 例： ```show ipv6 access-list```	アクセス リストの設定を確認します。
ステップ 10	**copy running-config startup-config** 例： ```copy running-config startup-config```	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスへの IPv6 の適用

ここでは、ネットワーク インターフェイスに IPv6 ACL を適用する手順について説明します。レイヤ 2 およびレイヤ 3 インターフェイスの発信または着信トラフィックに IPv6 ACL を適用できます。IPv6 ACL はレイヤ 3 インターフェイスの着信管理トラフィックにだけ適用できます。

インターフェイスへのアクセスを制御するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface_id*
4. **no switchport**
5. **ipv6 address** *ipv6_address*
6. **ipv6 traffic-filter** *acl_name*
7. **end**
8. **show running-config interface tenGigabitEthernet 1/0/3**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 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： `デバイス# 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** *interface_id* 例： `デバイス# interface interface-id`	アクセス リストを適用するレイヤ 2 インターフェイス（ポート ACL 用）またはレイヤ 3 スイッチ仮想インターフェイス（ルータ ACL 用）を特定して、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 switchport** 例： `デバイス# no switchport`	レイヤ 2 モード（デフォルト）からレイヤ 3 モードにインターフェイスを変更します（ルータ ACL を適用する場合のみ）。

	コマンドまたはアクション	目的
ステップ 5	**ipv6 address** *ipv6_address* 例： デバイス# **ipv6 address ipv6-address**	レイヤ3インターフェイス（ルータ ACL 用）で Ipv6 アドレスを設定します。 （注） このコマンドは、レイヤ2インターフェイスでは、またはインターフェイスに明示的な IPv6 アドレスが設定されている場合には、必要ありません。
ステップ 6	**ipv6 traffic-filter** *acl_name* 例： デバイス# **ipv6 traffic-filter access-list-name {in | out}**	インターフェイスの着信トラフィックまたは発信トラフィックにアクセス リストを適用します。
ステップ 7	**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。
ステップ 8	**show running-config interface tenGigabitEthernet 1/0/3** 例： デバイス# show running-config interface tenGigabitEthernet 1/0/3 .... Building configuration .... Current configuration : 98 bytes ! interface TenGigabitEthernet1/0/3 switchport mode trunk ipv6 traffic-filter MyFilter out end	設定の概要を示します。
ステップ 9	**copy running-config startup-config** 例： copy running-config startup-config	（任意）コンフィギュレーション ファイルに設定を保存します。

IPv6 ACL の確認

IPv6 ACL の表示

IPv6 ACL を表示するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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	**show access-list** 例： デバイス# **show access-lists**	deviceに設定されたすべてのアクセス リストを表示します。
ステップ 4	**show ipv6 access-list** *acl_name* 例： デバイス# **show ipv6 access-list** *[access-list-name]*	設定済みのすべての IPv6 アクセス リストまたは名前付けされたアクセス リストを表示します。

RA ガード ポリシーの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 nd raguard policy** *policy name*
4. **trusted-port**
5. **device-role router**
6. **interface** *interface-id*
7. **ipv6 nd raguard attach-policy** *policy name*
8. **vlan** *vlan-id*
9. **ipv6 nd suppress**
10. **ipv6 snooping**
11. **ipv6 nd raguard attach-policy** *policy name*
12. **ipv6 nd ra-throttler attach-policy** *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	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 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： デバイス# **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 raguard policy** *policy name* 例： デバイス(config)# **ipv6 nd raguard policy MyPolicy**	
ステップ 4	**trusted-port** 例： デバイス(config-nd-raguard)# **trusted-port**	上記で作成したポリシーの信頼できるポートを設定します。
ステップ 5	**device-role router** 例： デバイス(config-nd-raguard)# **device-role [host|monitor|router|switch]** デバイス(config-nd-raguard)# **device-role router** d	上記で作成した信頼できるポートにRA を送信可能な信頼できるデバイスを定義します。
ステップ 6	**interface** *interface-id* 例： デバイス(config)# **interface tenGigabitEthernet 1/0/1**	信頼できるデバイスにインターフェイスを設定します。
ステップ 7	**ipv6 nd raguard attach-policy** *policy name* 例： デバイス(config-if)# **ipv6 nd raguard attach-policy Mypolicy**	ポートから受信したRA を信頼するようにポリシーを設定し、接続します。
ステップ 8	**vlan** *vlan-id* 例： デバイス(config)# **vlan configuration 19-21,23**	ワイヤレス クライアントの vlan を設定します。
ステップ 9	**ipv6 nd suppress** 例： デバイス(config-vlan-config)# **ipv6 nd suppress**	無線上で ND メッセージを抑制します。

	コマンドまたはアクション	目的
ステップ 10	**ipv6 snooping** 例： `デバイス(config-vlan-config)# ipv6 snooping`	IPv6 トラフィックをキャプチャします。
ステップ 11	**ipv6 nd raguard attach-policy** *policy name* 例： `デバイス(config-vlan-config)# ipv6 nd raguard attach-policy Mypolicy`	ワイヤレス クライアントの vlan に RA ガード ポリシーを接続します。
ステップ 12	**ipv6 nd ra-throttler attach-policy** *policy name* 例： `デバイス(config-vlan-config)# ipv6 nd ra-throttler attach-policy Mythrottle`	ワイヤレス クライアントの vlan に RA スロットリング ポリシーを接続します。

IPv6 ネイバー バインディングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 neighbor binding** [vlan] **19 2001:db8::25:4 interface tenGigabitEthernet 1/0/3 aaa.bbb.ccc**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 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： `デバイス# 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** [vlan] **19 2001:db8::25:4 interface tenGigabitEthernet 1/0/3 aaa.bbb.ccc** 例：	送信元 MAC アドレスとして aaa.bbb.ccc が設定されたインターフェイス te1/0/3 を介して VLAN 19 で送信する場合にのみ有効なネイバー 2001:db8::25: 4 を設定して検証します。

	コマンドまたはアクション	目的
	デバイス(config)# **ipv6 neighbor binding vlan 19 2001:db8::25:4 interface tenGigabitEthernet 1/0/3 aaa.bbb.ccc**	

IPv6 ACL の設定例

例：IPv6 ACL の作成

次に、CISCO と名前が付けられた IPv6 アクセス リストを設定する例を示します。リスト内の最初の拒否エントリは、宛先 TCP ポート番号が 5000 より大きいパケットをすべて拒否します。2 番めの拒否エントリは、送信元 UDP ポート番号が 5000 未満のパケットを拒否します。また、この 2 番めの拒否エントリは、すべての一致をコンソールに表示します。リスト内の最初の許可エントリは、すべての ICMP パケットを許可します。リスト内の 2 番めの許可エントリは、その他のすべてのトラフィックを許可します。暗黙の全否定の条件が各 IPv6 アクセス リストの末尾にあるため、2 番めの許可エントリは必要です。

（注） ロギングは、レイヤ 3 インターフェイスでのみサポートされます。

```
デバイス(config)# ipv6 access-list CISCO
デバイス(config-ipv6-acl)# deny tcp any any gt 5000
デバイス (config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
デバイス(config-ipv6-acl)# permit icmp any any
デバイス(config-ipv6-acl)# permit any any
```

例：IPv6 ACL の適用

次に、レイヤ 3 インターフェイスの発信トラフィックに対して、アクセス リスト Cisco を適用する例を示します。

```
デバイス(config)# interface TenGigabitEthernet 1/0/3

デバイス(config-if)# no switchport
デバイス(config-if)# ipv6 address 2001::/64 eui-64
デバイス(config-if)# ipv6 traffic-filter CISCO out
```

例：IPv6 ACL の表示

次に、**show access-lists** 特権 EXEC コマンドの出力例を示します。出力には、スイッチまたはスイッチ スタックに設定済みのすべてのアクセス リストが表示されます。

```
デバイス #show access-lists
Extended IP access list hello
10 permit ip any any
```

```
IPv6 access list ipv6
permit ipv6 any any sequence 10
```

次に、show ipv6 access-lists 特権 EXEC コマンドの出力例を示します。出力には、スイッチまたはスイッチ スタックに設定済みの IPv6 アクセス リストだけが表示されます。

```
デバイス# show ipv6 access-list
IPv6 access list inbound
permit tcp any any eq bgp (8 matches) sequence 10
permit tcp any any eq telnet (15 matches) sequence 20
permit udp any any sequence 30

IPv6 access list outbound
deny udp any any sequence 10
deny tcp any any eq telnet sequence 20
```

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』

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	リンク
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 ACL 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 ACL 機能	Cisco IOS XE Everest 16.5.1a	この機能が導入されました。

翻訳について
このドキュメントは、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。