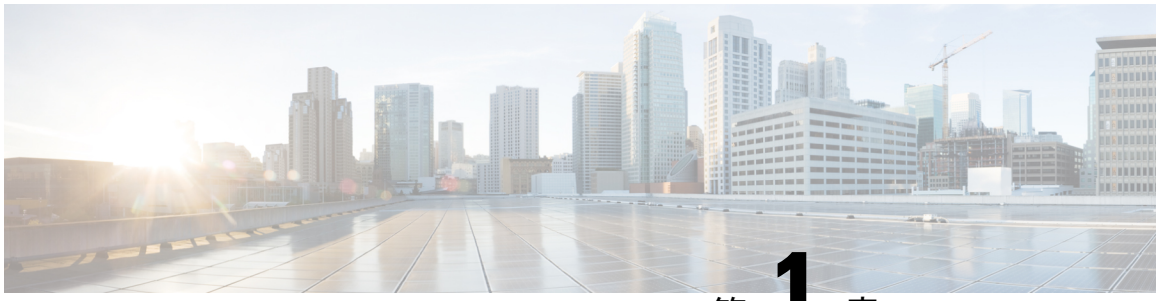
Cisco IOS XE Amsterdam 17.4.x（Catalyst 9200 スイッチ）IP アドレッシング サービス コンフィギュレーション ガイド

初版：2020 年 7 月 31 日

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

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

目 次



第 1 章

IP アドレッシングサービスの概要

このセクションでは、IP アドレッシングサービスについて説明します。

IPv6 の概要

IPv4 ユーザは 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。サイトローカルなユニキャスト 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。

- IPv6 アドレス形式
- 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

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に対してローカルなユニキャスト アドレスをサポートします。サイトに対してローカルなユニキャスト 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 プロバイダー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。

- リンクに対してローカルな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、リンクに対してローカルなプレフィックス 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、リンクに対してローカルなアドレスが使用されます。ローカルリンク上のノードは、リンクに対してローカルな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、リンクに対してローカルな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 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。ホストはリンクに対してローカルな独自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。

Cisco IOS XE Gibraltar 16.11.1 以降、自動設定された IPv6 アドレスには、RFC5453 で指定されている予約済みインターフェイス識別子の範囲に含まれないインターフェイス識別子が含まれるようになります。

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）
- FTP
- 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 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 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、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 上の HTTP（S）

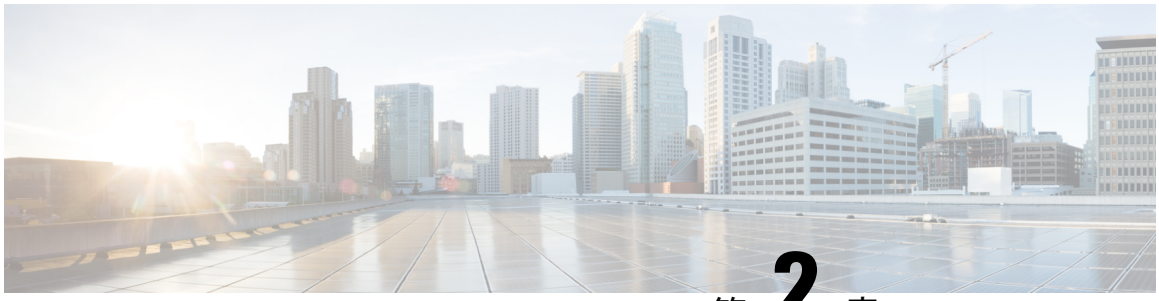
HTTP クライアントは要求を IPv4 HTTP サーバと IPv6 HTTP サーバの両方に送信し、これらのサーバは IPv4 HTTP クライアントと IPv6 HTTP クライアントの両方からの要求に応答します。IPv6 アドレスを含む URL は、16 ビット値をコロンで区切った 16 進数で指定する必要があります。

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。



第 2 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、関連付け、再関連付け、認証解除、タイムアウトの際に、クライアントの IPv4 および IPv6 アドレス、デバイスによって保持されるクライアント変換の状態について学習するために、デバイスで設定されます。

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

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

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

重複する IPv6 アドレスが設定されると、DAD は重複するアドレスを検出し、ルータアドバタイズメント（RA）でアドバタイズします。重複するアドレスは、システムから手動で削除できます。削除すると、接続されたアドレスに表示されず、RA プレフィックスにアドバタイズされません。

SLAAC アドレス割り当て

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

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

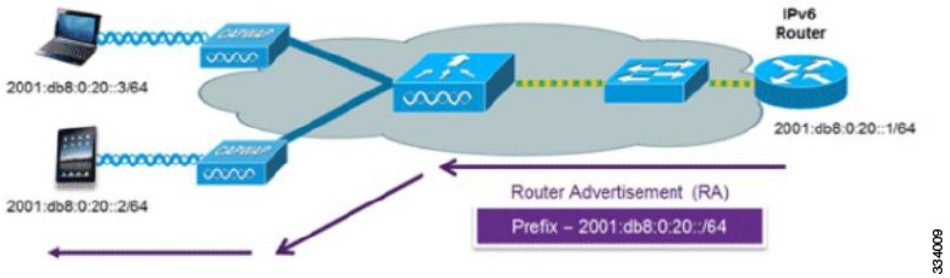
- ホストは、ルータ送信要求メッセージを送信します。
- ホストは、ルータ アドバタイズメント メッセージを待機します。
- ホストは、ルータ アドバタイズメント メッセージから IPv6 プレフィックスの最初の 64 ビットを取得し、これを 64 ビット EUI-64 アドレス（イーサネットの場合、MAC アドレスから作成されます）と組み合わせて、グローバル ユニキャスト メッセージを作成します。ホストは、デフォルト ゲートウェイとして、ルータ アドバタイズメント メッセージの IP ヘッダーに含まれる送信元 IP アドレスも使用します。
- 重複アドレス検出は、選択されるランダムアドレスが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

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

- インターフェイスの MAC アドレスに基づく EUI-64、または

- ランダムに生成されるプライベート アドレス。

図 *1 : SLAAC* アドレス割り当て

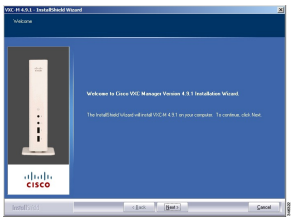


Cisco 対応 IPv6 ルータからの次の Cisco IOS コンフィギュレーション コマンドを使用して、SLAAC のアドレッシングとルータ アドバタイズメントをイネーブルにします。

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

ステートフル DHCPv6 アドレス割り当て

図 *2 :* ステートフル *DHCPv6* アドレス割り当て



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

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

```
ipv6 unicast-routing
ipv6 dhcp pool IPV6_DHCPPOOL
address prefix 2001:db8:5:10::/64
domain-name cisco.com
dns-server 2001:db8:6:6::1
```

```
interface Vlan20
description IPv6-DHCP-Stateless
ip address 192.168.20.1 255.255.255.0
ipv6 nd other-config-flag
ipv6 dhcp server IPV6_DHCPPOOL
ipv6 address 2001:DB8:0:20::1/64
end
```

マネージド モードとも呼ばれる DHCPv6 ステートフル オプションは、DHCPv4 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。こ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すために、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、関連付けられている 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、デバイスによってキャッシュされます。デバイスが IPv6 アドレスを検索する NS マルチキャストを受信したときに、デバイスによって特定された目的のアドレスがクライアントのいずれかに属している場合、デバイスはクライアントに代わって NA メッセージで応答します。このプロセスによって IPv4 のアドレス解決プロトコル（ARP）テーブルと同等のテーブルが生成されますが、より効率的であり、たいていの場合、使用されるメッセージは少なくなります。

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

デバイスにクライアントの IPv6 アドレスがない場合、デバイスは NA で応答せず、NS パケットを転送します。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。このノブが有効になっている場合、デバイスは、把握していない（キャッシュ欠落）IPv6 アドレスの NS パケットを取得して転送します。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、結果としてそのクライアントが正規の IPv6 ルータよりも優先されることになります。

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

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

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

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

RA ガードはデバイスに適用されます。デバイスで RA メッセージをドロップするようにデバイスを設定できます。すべての IPv6 RA メッセージがドロップされ、その結果、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有効にしておく必要があります。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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 unicast routing** 例： `Device(config)# ipv6 unicast routing`	IPv6ユニキャストデータグラムの転送をイネーブルにします。

RA ガード ポリシーの設定

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

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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 nd raguard policy raguard-router** 例： `Device(config)# ipv6 nd raguard policy raguard-router`	RA ガード ポリシー名を定義して、RA ガード ポリシー コンフィギュレーション モードを開始します。
ステップ 4	**trustedport** 例： `Device(config-ra-guard)# trustedport`	（任意）このポリシーが信頼できるポートに適用されることを指定します。
ステップ 5	**device-role router** 例： `Device(config-ra-guard)# device-role router`	ポートに接続されているデバイスの役割を指定します。
ステップ 6	**exit** 例： `Device(config-ra-guard)# exit`	RA ガードポリシー コンフィギュレーション モードを終了してグローバル コンフィギュレーション モードに戻ります。

RA ガードポリシーの適用

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

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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface tengigabitethernet 1/0/1** 例： `Device(config)# interface tengigabitethernet 1/0/1`	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 nd raguard attach-policy raguard-router** 例： `Device(config-if)# ipv6 nd raguard attach-policy raguard-router`	指定したインターフェイスに IPv6 RA ガード機能を適用します。
ステップ 5	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

IPv6 スヌーピングの設定

スイッチで IPv6 スヌーピングを常に有効にしておく必要があります。

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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vlan configuration 1** 例： `Device(config)# vlan configuration 1`	VLAN コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 snooping** 例： `Device(config-vlan)# ipv6 snooping`	Vlan で IPv6 スヌーピングをイネーブルにします。
ステップ 5	**ipv6 nd suppress** 例： `Device(config-vlan-config)# ipv6 nd suppress`	Vlan で IPv6 ND 抑制をイネーブルにします。
ステップ 6	**exit** 例： `Device(config-vlan-config)# exit`	設定を保存し、Vlan コンフィギュレーション モードを終了します。

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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 nd suppress policy** 例： `Device(config)# ipv6 nd suppress policy`	ND 制御ポリシー名を定義して ND 制御ポリシー コンフィギュレーション モードを開始します。

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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vlan config901** 例： `Device(config)# vlan config901`	VLAN を作成し、VLAN コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 nd suppress** 例： `Device(config-vlan)# ipv6 nd suppress`	VLAN に IPv6 nd 抑制を適用します。
ステップ 5	**end** 例： `Device(config-vlan)# end`	VLAN コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**interface gi1/0/1** 例： `Device(config)# interface gi1/0/1`	ギガビット イーサネット ポート インターフェイスを作成します。
ステップ 7	**ipv6 nd suppress** 例： `Device(config-vlan)# ipv6 nd suppress`	インターフェイスに IPv6 nd 抑制を適用します。
ステップ 8	**end** 例： `Device(config-vlan)# end`	VLAN コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

スイッチ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、次の手順に従います。

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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface vlan 1** 例： `Device(config)# interface vlan 1`	インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 4	**ip address fe80::1 link-local**
	例：
	`Device(config-if)# ip address 198.51.100.1 255.255.255.0`
	`Device(config-if)# ipv6 address fe80::1 link-local`
	`Device(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`Device(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64`
		リンクローカル オプションを使用してインターフェイスで IPv6 アドレスを設定します。

ステップ 5	**ipv6 enable** 例： `Device(config)# ipv6 enable`	（任意）インターフェイス上で IPv6 をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config)# end`	インターフェイス モードを終了します。

スイッチインターフェイスでの DHCP プールの設定

インターフェイスで DHCP プールを設定するには、次の手順に従います。

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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 dhcp pool Vlan21** 例： `Device(config)# ipv6 dhcp pool vlan1`	コンフィギュレーション モードを開始し、VLAN の IPv6 DHCP プールを設定します。
ステップ 4	**address prefix 2001:DB8:0:1:FFFF:1234::/64 lifetime 300 10** 例： `Device(config-dhcpv6)# address prefix 2001:DB8:0:1:FFFF:1234::/64 lifetime 300 10`	コンフィギュレーション DHCP モードを開始し、VLAN のアドレス プールとそのライフタイムを設定します。

	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： `Device(config-dhcpv6)# dns-server 2001:20:21::1`	DHCP プールの DNS サーバを設定します。
ステップ 6	**domain-name example.com** 例： `Device(config-dhcpv6)# domain-name example.com`	完全な非修飾ホスト名になるようにドメイン名を設定します。
ステップ 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の設定

DHCP を使用しないステートレス自動アドレス設定を指定するには、次の手順に従います。

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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface vlan 1** 例： `Device(config)# interface vlan 1`	インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 4	**ip address fe80::1 link-local**
	例：
	`Device(config-if)# ip address 198.51.100.1 255.255.255.0`
	`Device(config-if)# ipv6 address fe80::1 link-local`
	`Device(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`Device(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64`
		リンクローカル オプションを使用してインターフェイスで IPv6 アドレスを設定します。

ステップ 5	**ipv6 enable** 例： `Device(config)# ipv6 enable`	（任意）インターフェイス上で IPv6 をイネーブルにします。

ステップ 6	**no ipv6 nd managed-config-flag**
	例：
	`Device(config)# interface vlan 1`
	`Device(config-if)# no ipv6 nd managed-config-flag`
		接続されたホストで、アドレスの取得にステートフル自動設定が使用されないようにします。

ステップ 7	**no ipv6 nd other-config-flag** 例： `Device(config-if)# no ipv6 nd other-config-flag`	接続されたホストで、DHCP からの非アドレス オプションの取得に（ドメインなど）ステートフル自動設定が使用されないようにします。
ステップ 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の設定

DHCP を使用したステートレス自動アドレス設定を指定するには、次の手順に従います。

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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface vlan 1** 例： `Device(config)# interface vlan 1`	インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 4	**ip address fe80::1 link-local**
	例：
	`Device(config-if)# ip address 198.51.100.1 255.255.255.0`
	`Device(config-if)# ipv6 address fe80::1 link-local`
	`Device(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`Device(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64`
		リンクローカルオプションを使用してインターフェイスで IPv6 アドレスを設定します。

ステップ 5	**ipv6 enable** 例： `Device(config)# ipv6 enable`	（任意）インターフェイス上で IPv6 をイネーブルにします。

ステップ 6	**no ipv6 nd managed-config-flag**
	例：
	`Device(config)# interface vlan 1`
	`Device(config-if)# no ipv6 nd managed-config-flag`
		接続されたホストで、アドレスの取得にステートフル自動設定が使用されないようにします。

ステップ 7	**ipv6 nd other-config-flag** 例： `Device(config-if)# no ipv6 nd other-config-flag`	接続されたホストで、DHCP からの非アドレス オプションの取得に（ドメインなど）ステートフル自動設定が使用されないようにします。
ステップ 8	**end** 例：	インターフェイス モードを終了します。

	コマンドまたはアクション	目的
	`Device(config)# end`	

ステートフル DHCP のローカル設定

こ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。

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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	ユニキャスト用に IPv6 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 dhcp pool IPv6_DHCPPOOL** 例： `Device(config)# ipv6 dhcp pool IPv6_DHCPPOOL`	コンフィギュレーション モードを開始し、VLAN の IPv6 DHCP プールを設定します。
ステップ 5	**address prefix 2001:DB8:0:1:FFFF:1234::/64** 例： `Device(config-dhcpv6)# address prefix 2001:DB8:0:1:FFFF:1234::/64`	プールに入力するアドレス範囲を指定します。
ステップ 6	**dns-server 2001:100:0:1::1** 例： `Device(config-dhcpv6)# dns-server 2001:100:0:1::1`	DHCP クライアントに DNS サーバのオプションを提供します。
ステップ 7	**domain-name example.com** 例： `Device(config-dhcpv6)# domain-name example.com`	DHCP クライアントにドメイン名オプションを提供します。
ステップ 8	**exit** 例： `Device(config-dhcpv6)# exit`	前のモードに戻ります。
ステップ 9	**interface vlan1** 例： `Device(config)# interface vlan 1`	インターフェイス モードを開始して、ステートフル DHCP を設定します。
ステップ 10	**description IPv6-DHCP-Stateful** 例： `Device(config-if)# description IPv6-DHCP-Stateful`	ステートフル IPv6 DHCP の説明を入力します。
ステップ 11	**ipv6 address 2001:DB8:0:20::1/64** 例： `Device(config-if)# ipv6 address 2001:DB8:0:20::1/64`	ステートフル IPv6 DHCP の IPv6 アドレスを入力します。
ステップ 12	**ip address 192.168.20.1 255.255.255.0** 例： `Device(config-if)# ip address 192.168.20.1 255.255.255.0`	ステートフル IPv6 DHCP の IPv6 アドレスを入力します。
ステップ 13	**ipv6 nd prefix 2001:db8::/64 no-advertise** 例： `Device(config-if)# ipv6 nd prefix 2001:db8::/64 no-advertise`	アドバタイズしてはならない、IPv6 ルーティング プレフィックスアドバタイズメントを設定します。

	コマンドまたはアクション	目的
ステップ 14	**ipv6 nd managed-config-flag** 例： `Device(config-if)# ipv6 nd managed-config-flag`	ホストでアドレス設定に DHCP を使用できるように、IPv6 インターフェイス ネイバー探索を設定します。
ステップ 15	**ipv6 nd other-config-flag** 例： `Device(config-if)# ipv6 nd other-config-flag`	ホストで非アドレス設定に DHCP を使用できるように、IPv6 インターフェイス ネイバー探索を設定します。
ステップ 16	**ipv6 dhcp server IPv6_DHCPPOOL** 例： `Device(config-if)# ipv6 dhcp server IPv6_DHCPPOOL`	インターフェイスに DHCP サーバを設定します。

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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	ユニキャスト用に IPv6 を設定します。
ステップ 4	**dns-server 2001:100:0:1::1** 例： `Device(config-dhcpv6)# dns-server 2001:100:0:1::1`	DHCP クライアントに DNS サーバのオプションを提供します。
ステップ 5	**domain-name example.com** 例： `Device(config-dhcpv6)# domain-name example.com`	DHCP クライアントにドメイン名オプションを提供します。
ステップ 6	**exit** 例： `Device(config-dhcpv6)# exit`	前のモードに戻ります。
ステップ 7	**interface vlan1** 例： `Device(config)# interface vlan 1`	インターフェイス モードを開始して、ステートフル DHCP を設定します。
ステップ 8	**description IPv6-DHCP-Stateful** 例： `Device(config-if)# description IPv6-DHCP-Stateful`	ステートフル IPv6 DHCP の説明を入力します。
ステップ 9	**ipv6 address 2001:DB8:0:20::1/64** 例： `Device(config-if)# ipv6 address 2001:DB8:0:20::1/64`	ステートフル IPv6 DHCP の IPv6 アドレスを入力します。
ステップ 10	**ip address 192.168.20.1 255.255.255.0** 例： `Device(config-if)# ip address 192.168.20.1 255.255.255.0`	ステートフル IPv6 DHCP の IPv6 アドレスを入力します。
ステップ 11	**ipv6 nd prefix 2001:db8::/64 no-advertise** 例： `Device(config-if)# ipv6 nd prefix 2001:db8::/64 no-advertise`	アドバタイズしてはならない、IPv6 ルーティング プレフィックスアドバタイズメントを設定します。

	コマンドまたはアクション	目的
ステップ 12	**ipv6 nd managed-config-flag** 例： `Device(config-if)# ipv6 nd managed-config-flag`	ホストでアドレス設定に DHCP を使用できるように、IPv6 インターフェイス ネイバー探索を設定します。
ステップ 13	**ipv6 nd other-config-flag** 例： `Device(config-if)# ipv6 nd other-config-flag`	ホストで非アドレス設定に DHCP を使用できるように、IPv6 インターフェイス ネイバー探索を設定します。
ステップ 14	**ipv6 dhcp_relaydestination 2001:DB8:0:20::2** 例： `Device(config-if)# ipv6 dhcp_relay destination 2001:DB8:0:20::2`	インターフェイスに DHCP サーバを設定します。

IPv6 アドレス ラーニング設定の確認

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

手順の概要

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：
	`Device show ipv6 dhcp pool`
	`DHCPv6 pool: vlan21`
	`Address allocation prefix:`
	`2001:DB8:0:1:FFFF:1234::/64 valid 86400 preferred 86400 (6 in use, 0 conflicts)`
	`DNS server: 2001:100:0:1::1`
	`Domain name: example.com`
	`Active clients: 6`
		デバイスでの IPv6 サービスの設定を表示します。

その他の参考資料

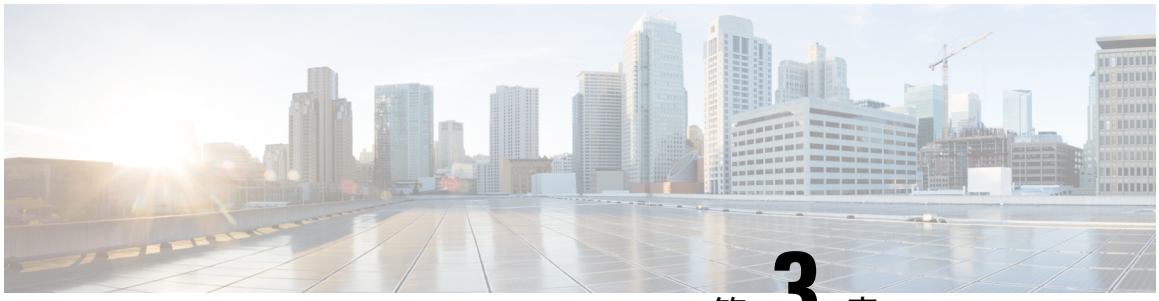
関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*Command Reference (Catalyst 9200 Series Switches)*

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。

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 Fuji 16.9.2	この機能が導入されました。



第 3 章

DHCP の設定

このセクションでは、DHCP の設定について説明します。

DHCP を設定するための前提条件

次の前提条件が DHCP スヌーピングおよびオプション 82 に適用されます。

- DHCP スヌーピングは、スイッチ上でグローバルにイネーブルにする必要があります。
- スイッチ上で DHCP スヌーピングをグローバルにイネーブルにする前に、DHCP サーバや DHCP リレーエージェントとして機能するデバイスが設定され、イネーブルになっていることを確認してください。
- スイッチを DHCP 要求に応答するようにする場合は、DHCP サーバとして設定する必要があります。
- スイッチで DHCP スヌーピング情報オプションを設定する前に、DHCP サーバとして機能するデバイスを設定してください。DHCP サーバが割り当てたり除外したりできる IP アドレスを指定するか、またはそれらのデバイスの DHCP オプションを設定する必要があります。
- DHCP スヌーピングを正しく機能させるためには、すべての DHCP サーバを信頼できるインターフェイス経由でスイッチに接続する必要があります。サービス プロバイダー ネットワークでは、同じネットワーク内のデバイスのポートに接続されたインターフェイスが信頼できるインターフェイスとなります。
- DHCP スヌーピングで Cisco IOS DHCP サーバ バインディング データベースを使用するには、Cisco IOS DHCP サーバ バインディング データベースを使用するようにスイッチを設定する必要があります。

- 信頼できない入力でパケットを受け入れる DHCP スヌーピング オプションを使用するには、スイッチがエッジ スイッチからオプション 82 情報を含むパケットを受信する集約スイッチである必要があります。
- 次の前提条件が DHCP スヌーピング バインディング データベースの設定に適用されます。
  - DHCP スヌーピング用にスイッチを使用するには、DHCP スヌーピング バインディング データベースで宛先を設定する必要があります。
  - NVRAM とフラッシュ メモリは、いずれも記憶容量が限られているため、バインディング ファイルを TFTP サーバに保存することを推奨します。
  - ネットワーク ベースの URL（TFTP や FTP など）については、スイッチがバインディングをその URL のバインディング ファイルに初めて書き込む前に、設定された URL に空のファイルを作成する必要があります。空のファイルをサーバ上に作成する必要があるかどうかについては、TFTP サーバのマニュアルを参照してください。TFTP サーバによっては、そのように設定できないことがあります。
  - データベースに正しいリース期間が記録されるように、ネットワーク タイム プロトコル（NTP）をイネーブルにし、設定することを推奨します。
  - NTP が設定されている場合、スイッチのシステム クロックが NTP と同期化されたときにだけ、スイッチがバインディングの変更内容をバインディング ファイルに書き込みます。
- スイッチで DHCP リレー エージェントを設定する前に、DHCP サーバとして機能するデバイスを設定してください。DHCP サーバが割り当てたり除外したりできる IP アドレスを指定するか、デバイスの DHCP オプションを設定するか、または DHCP データベース エージェントをセットアップする必要があります。
- スイッチが DHCP パケットをリレーするようにする場合は、DHCP サーバの IP アドレスは DHCP クライアントのスイッチ仮想インターフェイス（SVI）に設定する必要があります。
- スイッチポートが DHCP サーバに接続されている場合は、**ip dhcp snooping trust interface** コンフィギュレーション コマンドを入力して、ポートを信頼できるポートとして設定してください。
- スイッチポートが DHCP クライアントに接続されている場合は、**no ip dhcp snooping trust** 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、ポートを信頼できないポートとして設定してください。

DHCP の設定に関する制限

DHCP スヌーピング、DHCP リレーエージェントをサポートする送信（Tx）スイッチドポート アナライザ（SPAN）または出力 SPAN は使用しないことを推奨します。Tx での SPAN が必要な場合は、DHCP パケットの転送パスに含まれる VLAN ポートを使用しないでください。

DHCP に関する情報

DHCP サーバ

DHCP サーバは、スイッチまたはルータ上の指定されたアドレス プールから DHCP クライアントに IP アドレスを割り当て、それらのアドレスを管理します。DHCP サーバがそのデータベースから要求された設定パラメータを取得して DHCP クライアントに渡すことができない場合は、ネットワーク管理者が定義した 1 つまたは複数のセカンダリ DHCP サーバに要求を転送します。スイッチは、DHCP サーバとして機能できます。

DHCP リレー エージェント

DHCP リレー エージェントは、クライアントとサーバの間で DHCP パケットを転送するレイヤ 3 デバイスです。リレー エージェントは、同じ物理サブネット上にないクライアントとサーバの間で要求および応答を転送します。リレー エージェントによる転送は、IP データグラムをネットワーク間で透過的に交換するレイヤ 2 での通常の転送とは異なります。リレー エージェントは、DHCP メッセージを受け取ると、新しい DHCP メッセージを生成して、出力インターフェイス上で送信します。

DHCP スヌーピング

DHCP スヌーピングは、信頼できない DHCP メッセージのフィルタリングと DHCP スヌーピング バインディング データベース（DHCP スヌーピング バインディング テーブルとも呼ばれる）の作成および管理によってネットワーク セキュリティを確保する DHCP セキュリティ機能です。

DHCP スヌーピングは、信頼できないホストと DHCP サーバの間でファイアウォールに似た役割を果たします。DHCP スヌーピングを使用することにより、エンドユーザに接続された信頼できないインターフェイスと DHCP サーバまたは別のスイッチに接続された信頼できるインターフェイスを区別できます。

（注） DHCP スヌーピングを正しく機能させるためには、すべての DHCP サーバを信頼できるインターフェイス経由でスイッチに接続する必要があります。

信頼できない DHCP メッセージとは、信頼できないインターフェイス経由で送信されたメッセージのことです。デフォルトでは、スイッチはすべてのインターフェイスを信頼できないものと見なします。そのため、スイッチはいくつかのインターフェイスを信頼して DHCP スヌーピングを使用するように設定する必要があります。サービス プロバイダー環境で DHCP スヌーピングを使用する場合は、カスタマーのスイッチなど、サービス プロバイダー ネットワーク内には存在しないデバイスから送信されたメッセージが信頼できないメッセージとなります。

不明なデバイスから送信されたメッセージは、トラフィック攻撃の原因になりうるため、信頼できません。

DHCP スヌーピング バインディング データベースには、MAC アドレス、IP アドレス、リース期間、バインディングの種類、VLAN 番号、およびスイッチの信頼できないローカルインターフェイスのインターフェイス情報が含まれています。このデータベースには、信頼できるインターフェイスに接続されたホストの情報はありません。

サービス プロバイダー ネットワークでは、信頼できるインターフェイスとして設定できるものの例として、同じネットワーク内のデバイスのポートに接続されたインターフェイスがあります。信頼できないインターフェイスには、ネットワーク内の信頼できないインターフェイスまたはネットワークに属さないデバイスのインターフェイスに接続されたインターフェイスがあります。

スイッチが信頼できないインターフェイスでパケットを受信し、そのインターフェイスが属している VLAN で DHCP スヌーピングがイネーブルに設定されている場合、スイッチは送信元 MAC アドレスと DHCP クライアントのハードウェア アドレスを比較します。アドレスが一致した場合（デフォルト）、スイッチはパケットを転送します。アドレスが一致しない場合、スイッチはパケットをドロップします。

スイッチは、次のいずれかの状況が発生した場合に DHCP パケットをドロップします。

- DHCPOFFER パケット、DHCPACK パケット、DHCPNAK パケット、DHCPLEASEQUERY パケットなど、DHCP サーバからのパケットがネットワークまたはファイアウォールの外側から着信した。
- パケットが信頼できないインターフェイスに着信し、送信元 MAC アドレスと DHCP クライアントのハードウェア アドレスが一致しない。
- スイッチが DHCPRELEASE または DHCPDECLINE ブロードキャスト メッセージを受信し、その MAC アドレスは DHCP スヌーピング バインディング データベースに含まれているが、バインディング データベース内のインターフェイス情報がメッセージを受信したインターフェイスと一致しない。
- DHCP リレー エージェントが 0.0.0.0 以外のリレー エージェント IP アドレスを含む DHCP パケットを転送し、Option 82 情報が含まれないパケットを信頼できないポートに転送する。
- DHCP スヌーピングがイネーブルになっている場合に、最大スヌーピング キューサイズの 1000 を超える。

DHCP スヌーピングをサポートする集約スイッチであり、DHCP オプション 82 情報を挿入するエッジ スイッチに接続されているスイッチは、オプション 82 情報を含むパケットが信頼できないインターフェイスに着信した場合、それらのパケットをドロップします。DHCP スヌーピングがイネーブルに設定されている場合に、パケットが信頼できるポートに着信しても、集約スイッチは接続されたデバイスの DHCP スヌーピング バインディングを認識せず、完全な DHCP スヌーピング バインディング データベースを作成できません。

集約スイッチを信頼できないインターフェイス経由でエッジスイッチに接続できる場合、**ip dhcp snooping information option allow-untrusted** グローバル コンフィギュレーション コマン

ドを入力すると、集約スイッチはエッジスイッチによって挿入されたオプション 82 情報を含むパケットを受け入れます。集約スイッチは、信頼できないスイッチインターフェイスを介して接続されたホストのバインディングを認識します。集約スイッチで、ダイナミック ARP インスペクションや IP ソース ガードなど、DHCP セキュリティ機能をイネーブルに設定することもできますが、その場合でもスイッチは Option 82 情報を含むパケットをホストが接続されている信頼できない入力インターフェイスで受信します。集約スイッチ上のエッジスイッチとの接続ポートは、信頼できるインターフェイスとして設定する必要があります。

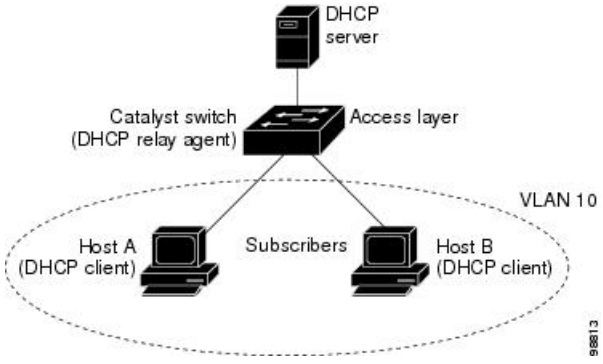
オプション 82 データ挿入

住宅地域にあるメトロポリタン イーサネット アクセス環境では、DHCP は多数の加入者に対し、IP アドレスの割り当てを一元的に管理できます。スイッチで DHCP スヌーピングの Option 82 機能をイネーブルにすると、加入者装置は MAC アドレスだけでなく、その装置をネットワークに接続するスイッチ ポートによっても識別されます。サブスクライバ LAN 上の複数のホストをアクセス スイッチの同じポートに接続できます。これらのホストは一意に識別されます。

（注） DHCP オプション 82 機能は、DHCP スヌーピングがグローバルに有効であり、オプション 82 を使用する加入者装置が割り当てられた VLAN で有効である場合に限りサポートされます。

次の図に、一元的な DHCP サーバがアクセス レイヤのスイッチに接続された加入者に IP アドレスを割り当てるメトロポリタン イーサネット ネットワークを示します。DHCP クライアントとそれらに関連付けられた DHCP サーバは同じ IP ネットワークまたはサブネット内に存在しないため、DHCP リレー エージェント（Catalyst スイッチ）にヘルパー アドレスを設定することにより、ブロードキャスト転送をイネーブルにし、クライアントとサーバ間で DHCP メッセージを転送します。

図 *3:* メトロポリタン イーサネット ネットワークにおける *DHCP* リレー エージェント



スイッチで DHCP スヌーピング情報 オプション 82 を有効にすると、次のイベントがこの順序で発生します。

- ホスト（DHCP クライアント）は DHCP 要求を生成し、これをネットワーク上にブロードキャストします。

- スイッチは、この DHCP 要求を受信すると、パケットに Option 82 情報を追加します。デフォルトでは、リモート ID サブオプションがスイッチの MAC アドレスで、回線 ID サブオプションはパケットを受信するポート ID（**vlan-mod-port**）です。リモート ID と回線 ID を設定できます。
- リレー エージェントの IP アドレスが設定されている場合、スイッチはこの IP アドレスを DHCP パケットに追加します。
- スイッチは、オプション 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。
- DHCP サーバはこのパケットを受信します。Option 82 に対応しているサーバであれば、リモート ID と回線 ID のいずれか一方または両方を使用して、IP アドレスを割り当てたり、1 つのリモート ID または回線 ID に割り当てることができる IP アドレスの数を制限するようなポリシーを実装したりできます。次に DHCP サーバは、DHCP 応答内にオプション 82 フィールドをエコーします。
- スイッチによって要求がサーバにリレーされた場合、DHCP サーバは応答をスイッチにユニキャストします。スイッチは、リモート ID フィールドと、場合によっては回線 ID フィールドを調べ、Option 82 データが挿入済みであることを確認します。スイッチは Option 82 フィールドを削除してから、DHCP 要求を送信した DHCP クライアントに接続するスイッチ ポートにパケットを転送します。

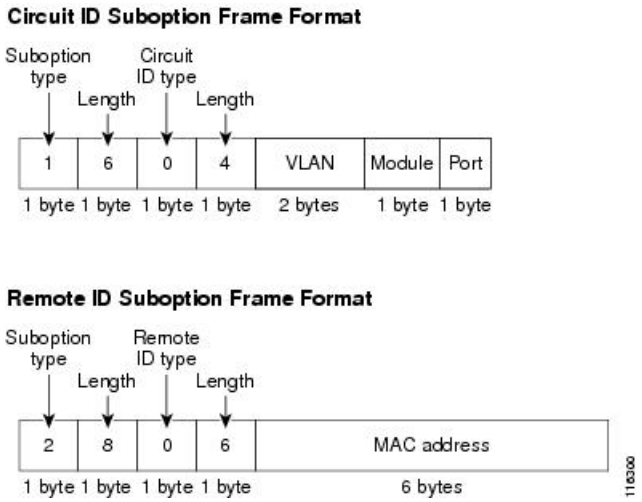
デフォルトのサブオプション設定では、前述のイベントのシーケンスが発生すると、次のフィールドの値は変化しません（図「サブオプションのパケット形式」を参照）。

- 回線 ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - 回線 ID タイプ
  - 回線 ID タイプの長さ
- リモート ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - リモート ID タイプ
  - リモート ID タイプの長さ

回線 ID サブオプションのポート フィールドでは、ポート番号が 3 から始まります。たとえば、24 個の 10/100/1000 ポートおよび 4 つの Small Form-Factor Pluggable（SFP）モジュール スロットを搭載するスイッチでは、ポート 3 がギガビット イーサネット 1/0/1 ポート、ポート 4 がギガビット イーサネット 1/0/2 ポートとなり、以降同様に続きます。ポート 27 は SFP モジュール スロットのギガビット イーサネット 1/0/25 となり、以降同様に続きます。

図「サブオプションのパケット形式」に、デフォルトのサブオプション設定が使用されている場合のリモート ID サブオプションおよび回線 ID サブオプションのパケット形式を示します。回線 ID サブオプションでは、モジュール番号は、スタックにあるスイッチ番号に対応します。スイッチがこれらのパケット形式を使用するのは、DHCP スヌーピングをグローバルに有効にし、ip dhcp snooping information option グローバル コンフィギュレーション コマンドを入力した場合です。

図 *4*:サブオプションのパケット形式

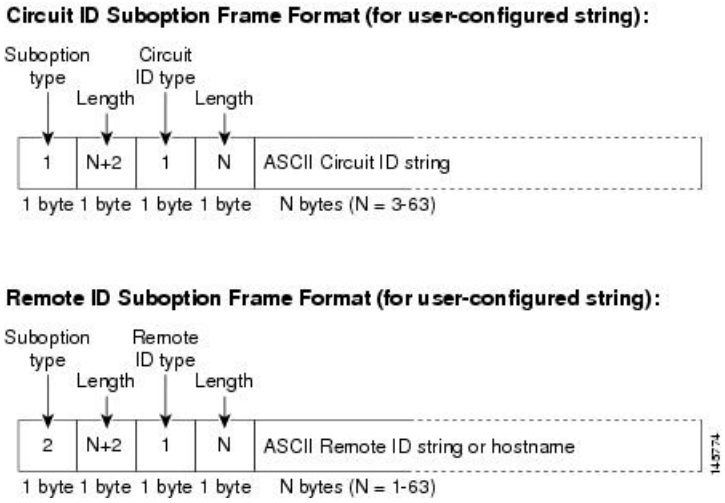


図「ユーザ設定のサブオプションのパケット形式」は、ユーザ設定のリモート ID サブオプション、および回線 ID サブオプションのパケット形式を示しています。スイッチでは、DHCP スヌーピングをグローバルにイネーブルにし、**ip dhcp snooping information option format remote-id** グローバル コンフィギュレーション コマンド、および **ip dhcp snooping vlan information option format-type circuit-id string** インターフェイス コンフィギュレーション コマンドを入力した場合に、これらのパケット形式が使用されます。

パケットでは、リモート ID および回線 ID サブオプションを次のように設定した場合、これらのフィールドの値がデフォルト値から変更されます。

- 回線 ID サブオプション フィールド
  - 回線 ID タイプが 1 である。
  - 設定した文字列の長さに応じて、長さの値が変化する。
- リモート ID サブオプション フィールド
  - リモート ID タイプが 1 である。
  - 設定した文字列の長さに応じて、長さの値が変化する。

図 *5:* ユーザ設定のサブオプションのパケット形式



Cisco IOS DHCP サーバ データベース

DHCP ベースの自動設定プロセスの間、指定 DHCP サーバは Cisco IOS DHCP サーバ データベースを使用します。これには IP アドレス、アドレス バインディング、およびブート ファイルなどの設定パラメータが含まれます。

アドレス バインディングは、Cisco IOS DHCP サーバ データベース内のホストの IP アドレスおよび MAC アドレス間のマッピングです。クライアント IP アドレスを手動で割り当てること、または、DHCP サーバが DHCP アドレス プールから IP アドレスを割り当てることが可能です。

DHCP スヌーピング バインディング データベース

DHCP スヌーピングをイネーブルにすると、スイッチは信頼できないインターフェイスに関する情報を DHCP スヌーピング バインディング データベースに保存します。データベースには、64,000 のバインディングを含めることができます。

各データベース エントリ（バインディング）は、IP アドレス、それに関連付けられた MAC アドレス、リース期間（16 進形式）、バインディングが適用されるインターフェイス、およびインターフェイスが属する VLAN で構成されます。データベース エージェントは、設定された場所のファイルにバインディングを保存します。各エントリの末尾にあるチェックサムは、ファイルの先頭のバイトを含め、エントリに関連付けられたすべてのバイトを対象として計算されます。各エントリは、まず 72 バイトのデータがあり、その後に 1 つのスペースとチェックサム値が続きます。

スイッチのリロード後もバインディングを保持するには、DHCP スヌーピング データベース エージェントを使用する必要があります。エージェントがディセーブルで、ダイナミック ARP インスペクションまたは IP ソース ガードがイネーブルにされ、DHCP スヌーピング バインディング データベースがダイナミック バインディングされている場合、スイッチは接続を切断されます。このエージェントがディセーブルで、DHCP スヌーピングだけがイネーブルである

場合、スイッチの接続は切断されませんが、DHCP スヌーピングは DHCP スプーフィング攻撃を防止できないことがあります。

リロードすると、スイッチはバインディング ファイルを読み込み、DHCP スヌーピング バインディングデータベースを作成します。スイッチは、データベースに変更が加えられたときにはバインディング ファイルを更新します。

スイッチは、新しいバインディングを認識するか、バインディングを失うと、ただちにデータベース内のエントリを更新します。スイッチはバインディング ファイル内のエントリも更新します。バインディング ファイルの更新頻度は設定可能な遅延時間によって決まり、更新はバッチ処理されます。ファイルが指定された時間内（書き込み遅延および中断タイムアウトの値によって設定される）に更新されない場合、更新は停止します。

バインディングが含まれるファイルの形式は次のとおりです。

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<entry-1> <checksum-1>
<entry-2> <checksum-1-2>
...
...
<entry-n> <checksum-1-2-..-n>
END
```

このファイルの各エントリにはチェックサム値を示すタグが付けられます。スイッチは、ファイルを読み取るときに、このチェックサムを使用してエントリを検証します。最初の行の initial-checksum エントリは、最新のファイル更新に関連するエントリを以前のファイル更新に関連するエントリと区別します。

次に、バインディング ファイルの例を示します。

```
2bb4c2a1
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
192.1.168.1 3 0003.47d8.c91f 2BB6488E Gi1/0/4 21ae5fbb
192.1.168.3 3 0003.44d6.c52f 2BB648EB Gi1/0/4 1bdb223f
192.1.168.2 3 0003.47d9.c8f1 2BB648AB Gi1/0/4 584a38f0
END
```

スイッチが起動し、計算されたチェックサム値が保存されているチェックサム値と一致した場合、スイッチはバインディング ファイルのエントリを読み取り、バインディングを DHCP スヌーピングバインディングデータベースに追加します。次のいずれかの状況が発生した場合、スイッチはエントリを無視します。

- スイッチがエントリを読み取り、計算されたチェックサム値が保存されているチェックサム値と一致しない。この場合、そのエントリとそれ以降のエントリは無視されます。
- エントリに含まれているリース期間が終了している（スイッチはリース期間の終了時にバインディング エントリを削除しないことがある）。
- エントリに含まれるインターフェイスが現在はシステムに存在しない。

- インターフェイスがルーテッド インターフェイスまたは DHCP スヌーピングにおける信頼できるインターフェイスである。

DHCP スヌーピングおよびスイッチ スタック

DHCP スヌーピングは、アクティブスイッチで管理されます。新しいスイッチは、スタックに追加されると、アクティブスイッチから DHCP スヌーピング設定を受信します。メンバがスタックから除外されると、スイッチに関連付けられているすべての DHCP スヌーピング アドレス バインディングがエージング アウトします。

すべてのスヌーピング統計情報は、アクティブスイッチ上で生成されます。新しいアクティブスイッチが選定された場合、統計カウンタはリセットされます。

スタックのマージが発生し、アクティブスイッチではなくなった場合、アクティブスイッチにあったすべての DHCP スヌーピングバインディングが失われます。スタックパーティションを使用すると、既存のアクティブスイッチは変更されず、パーティション分割されたスイッチに属しているバインディングはエージアウトします。パーティション分割されたスタックの新しいアクティブスイッチで、新たな着信 DHCP パケットの処理が開始されます。

DHCP スヌーピングのデフォルト設定

表 *1 : DHCP* のデフォルト設定

機能	デフォルト設定
DHCP サーバ	Cisco IOS ソフトウェアではイネーブル、設定が必要[1]
DHCP リレー エージェント	イネーブル[2]
DHCP パケット転送アドレス	未設定
リレー エージェント情報の確認	イネーブル（無効なメッセージは廃棄）
DHCP リレー エージェント転送ポリシー	既存のリレー エージェント情報を置換。
DHCP スヌーピングをグローバルにイネーブル	ディセーブル
DHCP スヌーピング情報オプション	イネーブル
パケットを信頼できない入力インターフェイスで受け取る DHCP スヌーピング オプション[3]	ディセーブル
DHCP スヌーピング レート制限	未設定
DHCP スヌーピング信頼状態	信頼できない

機能	デフォルト設定
DHCP スヌーピング VLAN	ディセーブル
DHCP スヌーピングの MAC アドレス検証	イネーブル
Cisco IOS DHCP サーバ バインディング データベース	Cisco IOS ソフトウェアではイネーブル、設定が必要。 （注） スイッチは、DHCP サーバとして設定されているデバイスからだけ、ネットワーク アドレスおよび設定パラメータを取得します。
DHCP スヌーピング バインディング データベース エージェント	Cisco IOS ソフトウェアではイネーブル、設定が必要。この機能は宛先が設定されている場合に限り有効。

[1] スイッチは、DHCP サーバとして設定されている場合に限り DHCP 要求に応答します。
[2] スイッチは、DHCP サーバの IP アドレスが DHCP クライアントの SVI に設定されている場合に限り DHCP パケットをリレーします。
[3] この機能は、スイッチがエッジスイッチによってオプション 82 情報が挿入されたパケットを受信する集約スイッチである場合に使用します。

DHCP スヌーピング設定時の注意事項

- スイッチポートが DHCP サーバに接続されている場合は、**ip dhcp snooping trust interface** コンフィギュレーション コマンドを入力して、ポートを信頼できるポートとして設定してください。
- スイッチポートが DHCP クライアントに接続されている場合は、**no ip dhcp snooping trust** 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、ポートを信頼できないポートとして設定してください。
- **show ip dhcp snooping statistics** ユーザ EXEC コマンドを入力して DHCP スヌーピング統計情報を表示したり、**clear ip dhcp snooping statistics** 特権 EXEC コマンドを入力してスヌーピング統計情報をクリアしたりできるようになりました。

DHCP サーバとスイッチ スタック

DHCPバインディングデータベースは、アクティブスイッチで管理されます。新しいアクティブスイッチが割り当てられると、新しいアクティブスイッチに、TFTP サーバで保存されているバインディングデータベースがダウンロードされます。スイッチの切り替えが発生した場合、新しいアクティブスイッチは、SSO機能を使用して以前のアクティブスイッチで同期されたデータベースファイルを使用します。失われたバインディングに関連付けられていた IP ア

ドレスは、解放されます。自動バックアップは、**ip dhcp database** *url* [**timeout** *seconds* | **write-delay** *seconds*] 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する必要があります。

DHCP サーバ ポートベースのアドレス割り当て

DHCP サーバ ポートベースのアドレス割り当ては、接続されたデバイス クライアントの ID またはクライアント ハードウェア アドレスに関係なく、DHCP がイーサネット スイッチ ポートで同じ IP アドレスを維持できるようにする機能です。

ネットワークに導入されたイーサネット スイッチは、直接接続されたデバイスに接続を提供します。工場の作業場など、一部の環境では、あるデバイスで不具合が発生した場合は、それと同時に、そのネットワークで代わりのデバイスが動作を開始しなければなりません。現在の DHCP 実装では、この代わりのデバイスに、DHCP が同じ IP アドレスを提供する保証はありません。コントロールやモニタリングなどを行うソフトウェアは、各デバイスに関連付けられた IP アドレスが一定であることを期待しています。デバイスを交換した場合、DHCP クライアントが変更された場合でも、アドレスの割り当ては一定のままでなければなりません。

DHCP サーバ ポートベースのアドレス割り当て機能が設定されている場合、この機能により、ある接続ポートで受信された DHCP メッセージでクライアント ID やクライアント ハードウェア アドレスが変更されたとしても、同じ接続ポートには常に同じ IP アドレスが提供されることが保証されます。DHCP プロトコルは、DHCP パケットのクライアント ID オプションにより、DHCP クライアントを識別します。クライアント ID オプションを含まないクライアントは、クライアント ハードウェア アドレスにより識別されます。この機能を設定すると、インターフェイスのポート名が、クライアント ID またはハードウェア アドレスよりも優先され、実際の接続ポイントであるスイッチ ポートがクライアント ID になります。

すべてのケースで、同じポートにイーサネット ケーブルを接続することにより、接続されたデバイスに、DHCP 経由で同じ IP アドレスが割り当てられます。

DHCP サーバ ポートベースのアドレス割り当て機能がサポートされているのは、Cisco IOS DHCP サーバだけです。サードパーティ製のサーバではサポートされていません。

ポートベースのアドレス テーブルのデフォルト設定

デフォルトでは、DHCP サーバ ポートベースのアドレス割り当てはディセーブルにされています。

ポートベースのアドレス割り当て設定時の注意事項

- デフォルトでは、DHCP サーバ ポートベースのアドレス割り当てはディセーブルにされています。
- DHCP プールから事前に設定された予約への割り当てを制限する（予約されていないアドレスはクライアントに提供されず、その他のクライアントはプールによるサービスを受けない）ために、**reserved-only** DHCP プール コンフィギュレーション コマンドを入力することができます。

DHCP の設定方法

DHCP サーバの設定

スイッチは、DHCP サーバとして機能できます。管理ポートを備えた DHCP クライアント用に DHCP サーバを使用する場合は、管理 VRF を使用して DHCP プールと対応するインターフェイスの両方を設定する必要があります。

DHCP リレー エージェントの設定

スイッチ上で DHCP リレー エージェントをイネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **service dhcp**
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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**service dhcp** 例： `Device(config)# service dhcp`	スイッチ上で DHCP サーバおよび DHCP リレー エージェントをイネーブルにします。デフォルトでは、この機能はイネーブルです。
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

次のタスク

- リレー エージェント情報のチェック（検証）
- リレー エージェント転送ポリシーの設定

パケット転送アドレスの指定

DHCP サーバおよび DHCP クライアントが異なるネットワークまたはサブネットにある場合、スイッチを **ip helper-address** *address* インターフェイス コンフィギュレーション コマンドで設定する必要があります。一般的なルールは、クライアントに最も近いレイヤ 3 インターフェイス上にコマンドを設定することです。**ip helper-address** コマンドで使用されているアドレスは、特定の DHCP サーバ IP アドレスか、または他の DHCP サーバが宛先ネットワークセグメントにある場合はネットワークアドレスにすることができます。ネットワーク アドレスを使用することで、どの DHCP サーバも要求に応答できるようになります。

パケット転送アドレスを指定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface vlan** *vlan-id*
4. **ip address** *ip-address subnet-mask*
5. **ip helper-address** *address*
6. **exit**
7. 次のいずれかを使用します。
   - **interface range** *port-range*
   - **interface** *interface-id*
8. **switchport mode access**
9. **switchport access vlan** *vlan-id*
10. **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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface vlan** *vlan-id* 例： `Device(config)# interface vlan 1`	VLAN ID を入力してスイッチの仮想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** *ip-address subnet-mask* 例： `Device(config-if)# ip address 192.108.1.27 255.255.255.0`	インターフェイスに IP アドレスおよび IP サブネットを設定します。
ステップ 5	**ip helper-address** *address* 例： `Device(config-if)# ip helper-address 172.16.1.2`	DHCP パケット転送アドレスを指定します。 • ヘルパー アドレスは特定の DHCP サーバ アドレスにするか、他の DHCP サーバが宛先ネットワーク セグメントにある場合は、ネットワーク アドレスにすることができます。ネットワーク アドレスを使用することで、他のサーバも DHCP 要求に応答できるようになります。 • 複数のサーバがある場合、各サーバに 1 つのヘルパー アドレスを設定できます。
ステップ 6	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	次のいずれかを使用します。 • **interface range** *port-range* • **interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/2`	DHCP クライアントに接続されている複数の物理ポートを設定し、インターフェイス範囲コンフィギュレーション モードを開始します。 または DHCP クライアントに接続されている単一の物理ポートを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**switchport mode access** 例： `Device(config-if)# switchport mode access`	ポートの VLAN メンバーシップ モードを定義します。
ステップ 9	**switchport access vlan** *vlan-id* 例： `Device(config-if)# switchport access vlan 1`	ステップ 2 で設定したのと同じ VLAN をポートに割り当てます。

	コマンドまたはアクション	目的
ステップ 10	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

DHCP for IPv6 アドレス割り当ての設定

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 アドレス割り当ての設定時には、次の前提条件が適用されます。

- 次の手順では、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。
  - IPv6 アドレスが明示的に設定されていない場合は、**ipv6 enable** コマンドを使用して IPv6 ルーティングを有効にします。
  - レイヤ 3 インターフェイスで DHCPv6 ルーティングが有効になっている必要があります。
  - 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。
  - 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。
- デバイスは、DHCPv6 クライアント、サーバ、またはリレーエージェントの役割を果たすことが可能です。DHCPv6 クライアント、サーバ、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。
- Cisco IOS XE Gibraltar 16.11.1 以降、DHCPv6 アドレスには、RFC5453 で指定されている予約済みインターフェイス識別子の範囲に含まれないインターフェイス識別子が含まれるようになります。

DHCPv6 サーバ機能のイネーブル化（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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 dhcp pool** *poolname* 例： `Device(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： `Device(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： `Device(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。
ステップ 6	**vendor-specific** *vendor-id* 例： `Device(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。

	コマンドまたはアクション	目的
ステップ 7	**suboption** *number* { **address** *IPv6-address* | **ascii** *ASCII-string* | **hex** *hex-string*} 例： `Device(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： `Device(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： `Device(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： `Device(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： `Device(config-if)# ipv6 dhcp server automatic`	インターフェイスに対して DHCPv6 サーバ機能をイネーブルにします。 • *poolname*：（任意）IPv6 DHCP プールのユーザ定義の名前。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。 • **preference** 値：（任意）サーバ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。

	コマンドまたはアクション	目的
		• **allow-hint**：（任意）サーバが 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、サーバはクライアントのヒントを無視します。
ステップ 12	**end** 例： `Device(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：
	`Device# show ipv6 dhcp pool`
	または
	`Device# show ipv6 dhcp interface`
		• DHCPv6 プール設定を確認します。
		• DHCPv6 サーバ機能がインターフェイス上でイネーブルであることを確認します。

ステップ 14	**copy running-config startup-config** 例： `Device# 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イネーブル化

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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *interface-id* 例： `Device(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： `Device(config-if)# ipv6 address dhcp rapid-commit`	インターフェイスで DHCPv6 サーバから 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： `Device(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： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show ipv6 dhcp interface** 例： `Device# show ipv6 dhcp interface`	DHCPv6 クライアントがインターフェイスでイネーブルになっていることを確認します。

Cisco IOS DHCP サーバ データベースのイネーブル化

Cisco IOS DHCP サーバデータベースを有効にして設定する手順については、『Cisco IOS IP Configuration Guide』の「Configuring DHCP」の章にある「DHCP Configuration Task List」のセクションを参照してください。

DHCP スヌーピング バインディング データベース エージェントのイネーブル化

スイッチ上で DHCP スヌーピング バインディング データベース エージェントをイネーブルにし、設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip dhcp snooping database** {**flash**[*number*]**:**/*filename* | **ftp:**//*user*:*password*@*host*/*filename* | **http:**//[[*username*:*password*]@]{*hostname* | *host-ip*}[/*directory*] /*image-name*.**tar** | **rcp:**//*user*@*host*/*filename*}| **tftp:**//*host*/*filename*
4. **ip dhcp snooping database timeout** *seconds*
5. **ip dhcp snooping database write-delay** *seconds*
6. **exit**
7. **ip dhcp snooping binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id* **expiry** *seconds*
8. **show ip dhcp snooping database** [**detail**]

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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip dhcp snooping database** {**flash**[*number*]**:**/*filename*	**ftp:**//*user*:*password*@*host*/*filename*	**http:**//[[*username*:*password*]@]{*hostname*	*host-ip*}[/*directory*] /*image-name*.**tar**	**rcp:**//*user*@*host*/*filename*}| **tftp:**//*host*/*filename* 例： `Device(config)# ip dhcp snooping database tftp://10.90.90.90/snooping-rp2`	次のいずれかの形式を使用して、データベース エージェントまたはバインディング ファイルの URL を指定します。 • **flash**[*number*]**:**/*filename* • **ftp:**//*user*:*password*@*host*/*filename* • **http:**//[[*username*:*password*]@]{*hostname*	*host-ip*}[/*directory*] /*image-name*.**tar** • **rcp:**//*user*@*host*/*filename* • **tftp:**//*host*/*filename*
ステップ 4	**ip dhcp snooping database timeout** *seconds* 例： `Device(config)# ip dhcp snooping database timeout 300`	データベース転送プロセスが完了するのを待ち、それまでに完了しない場合はプロセスを停止する時間（秒数）を指定します。 デフォルトは 300 秒です。指定できる範囲は 0 ～ 86400 です。無期限の期間を定義するには、0 を使用します。これは転送を無期限に試行することを意味します。

	コマンドまたはアクション	目的
ステップ 5	**ip dhcp snooping database write-delay** *seconds* 例： `Device(config)# ip dhcp snooping database write-delay 15`	バインディング データベースが変更されてから転送を開始するまでの遅延時間を指定します。指定できる範囲は 15 ～ 86400 秒です。デフォルトは 300 秒（5 分）です。
ステップ 6	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**ip dhcp snooping binding** *mac-address* **vlan** *vlan-id* *ip-address* **interface** *interface-id* **expiry** *seconds* 例： `Device# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface gigabitethernet 1/1/0 expiry 1000`	（任意）DHCP スヌーピング バインディング データベースにバインディング エントリを追加します。*vlan-id* に指定できる範囲は 1 ～ 4904 です。*seconds* の範囲は 1 ～ 4294967295 です。 このコマンドは、追加するエントリごとに入力します。 このコマンドは、スイッチをテストまたはデバッグするときに使用します。
ステップ 8	**show ip dhcp snooping database** [**detail**] 例： `Device# show ip dhcp snooping database detail`	DHCP スヌーピング バインディング データベース エージェントのステータスおよび統計情報を表示します。

DHCP スヌーピング情報のモニタリング

表 *2: DHCP* 情報を表示するためのコマンド

show ip dhcp snooping	スイッチの DHCP スヌーピングの設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング データベース内の動的に設定されたバインディングだけを表示します。このようなバインディングは、バインディング テーブルとも呼ばれます。
show ip dhcp snooping database	DHCP スヌーピング バインディング データベースのステータスおよび統計情報を表示します。

show ip dhcp snooping statistics	DHCP スヌーピングの統計情報を要約または詳細形式で表示します。
show ip source binding	動的および静的に設定されたバインディングを表示します。

（注） DHCP スヌーピングがイネーブルでインターフェイスがダウン ステートに変更された場合、静的に設定されたバインディングは削除されません。

DHCP サーバ ポートベースのアドレス割り当てのイネーブル化

ポートベースのアドレス割り当てをグローバルにイネーブル化し、インターフェイス上で加入者 ID を自動的に生成するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip dhcp use subscriber-id client-id**
4. **ip dhcp subscriber-id interface-name**
5. **interface** *interface-type interface-number*
6. **ip dhcp server use subscriber-id client-id**
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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip dhcp use subscriber-id client-id** 例： `Device(config)# ip dhcp use subscriber-id client-id`	すべての着信 DHCP メッセージで、加入者 ID がクライアント ID としてグローバルに使用されるように DHCP サーバを設定します。

	コマンドまたはアクション	目的
ステップ 4	**ip dhcp subscriber-id interface-name** 例： `Device(config)# ip dhcp subscriber-id interface-name`	インターフェイスの短い名前に基づいて、加入者 ID を自動的に生成します。 特定のインターフェイスで設定された加入者 ID は、このコマンドで優先されます。
ステップ 5	**interface** *interface-type interface-number* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定するインターフェイスを指定して、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 6	**ip dhcp server use subscriber-id client-id** 例： `Device(config-if)# ip dhcp server use subscriber-id client-id`	インターフェイス上ですべての着信 DHCP メッセージで、加入者 ID がクライアント ID として使用されるように DHCP サーバを設定します。
ステップ 7	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

次のタスク

スイッチ上での DHCP ポートベースのアドレス割り当てをイネーブルにした後で、**ip dhcp pool** 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、IP アドレスの事前割り当てと、クライアントへの関連付けを行います。

DHCP サーバ ポートベースのアドレス割り当てのモニタリング

表 *3 : DHCP* ポートベースのアドレス割り当て情報を表示するためのコマンド

コマンド	目的
show interface *interface id*	特定のインターフェイスのステータスおよび設定を表示します。
show ip dhcp pool	DHCP アドレス プールを表示します。
show ip dhcp binding	Cisco IOS DHCP サーバのアドレス バインディングを表示します。

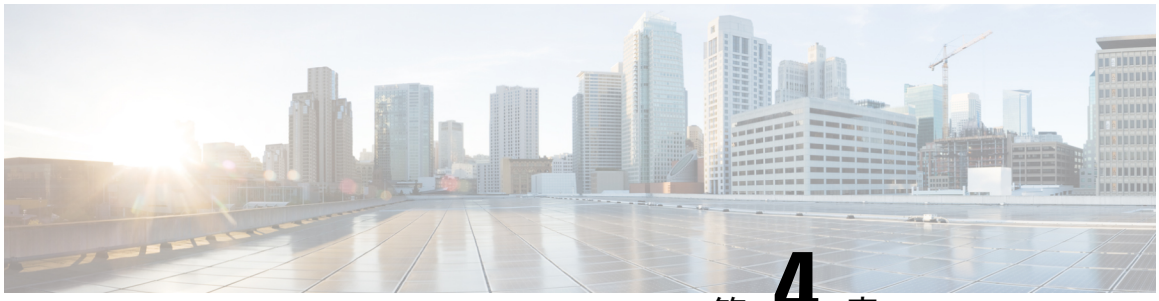
DHCP の機能情報

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

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

表 *4 : DHCP* の機能情報

機能名	リリース	機能情報
DHCP	Cisco IOS XE Fuji 16.9.2	DHCP はインターネット ホストに設定パラメータを提供します。DHCP は2つのコンポーネントで構成されます。1 つはホスト固有の設定パラメータを DHCP サーバからホストに配信するためのプロトコルで、もう 1 つはホストにネットワーク アドレスを割り当てるためのメカニズムです。DHCP はクライアント/サーバ モデルに基づいています。指定された DHCP サーバ ホストが、ダイナミックに設定されるホストに対して、ネットワーク アドレスを割り当て、設定パラメータを提供します。
DHCP クライアントオプション 12	Cisco IOS XE Fuji 16.9.2	DHCP クライアントオプション 12 機能により、クライアントのホスト名が指定されます。Dynamic Host Configuration Protocol（DHCP）サーバからインターフェイスの IP アドレスを取得する際に、クライアントデバイスが応答内の DHCP Hostname オプションを受信すると、このオプションのホスト名が設定されます。DHCP は、IP ネットワークにおける動作のための設定情報を取得するために DHCP クライアントによって使用されます。



第 4 章

DHCP グリーニング

このセクションでは、DHCP グリーニングについて説明します。

DHCP グリーニングの前提条件

- インターフェイスがレイヤ2インターフェイスとして設定されていることを確認します。
- グローバルスヌーピングが有効になっていることを確認します。

DHCP グリーニングに関する情報

DHCP グリーニングの概要

グリーニングは、Dynamic Host Configuration Protocol（DHCP）リレーエージェントによってメッセージが転送されるときに、DHCPメッセージからロケーション情報を抽出するのに役立ちます。このプロセスは完全にパッシブなスヌーピング機能であり、DHCPパケットのブロックも変更も行われません。またグリーニングは、エンドユーザに接続されている信頼できないデバイスポートと、DHCPサーバに接続されている信頼できるポートを区別するのに役立ちます。

DHCP グリーニングは、コンポーネントが DHCP バージョン 4 パケットのみを登録およびグリーニングできるようにする読み取り専用DHCP スヌーピング機能です。DHCP グリーニングを有効にすると、DHCPスヌーピングが無効になっているすべてのアクティブインターフェイスで読み取り専用スヌーピングが実行されます。プライベート VLAN にセカンダリ VLAN を

追加できます。セカンダリ VLAN をプライベート VLAN に追加する場合は、プライマリ VLAN でスヌーピングが無効になっている場合でも、セカンダリ VLAN でグリーニングが有効になっていることを確認します。デフォルトでは、グリーニング機能は無効になっています。ただし、デバイスセンサーを有効にすると、DHCP グリーニングが自動的に有効になります。

DHCP スヌーピング

Dynamic Host Configuration Protocol（DHCP）スヌーピングは、信頼できないホストと信頼された DHCP サーバとの間のファイアウォールのように機能するセキュリティ機能です。DHCP スヌーピング機能では、次のアクティビティが実行されます。

- 信頼できないソースからの DHCP メッセージを検証し、無効なメッセージをフィルタ処理して除外する。
- 信頼できるソースおよび信頼できないソースからの DHCP トラフィックのレートを制限する。
- DHCP スヌーピング バインディング データベースを構築し、管理します。このデータベースには、リース IP アドレスがある信頼できないホストに関する情報が保存されています。
- DHCP スヌーピング バインディング データベースを使用して、信頼できないホストからの以降の要求を検証します。

動的な Address Resolution Protocol（ARP）などの他のセキュリティ機能でも、DHCP スヌーピング バインディング データベースに保存されている情報が使用されます。

DHCP スヌーピングは、VLAN ベースごとにイネーブルに設定されます。デフォルトでは、すべての VLAN でこの機能は非アクティブです。この機能は、1 つの VLAN または特定の VLAN 範囲で有効にできます。

DHCP グリーニングの設定方法

DHCP グリーニングの信頼された送信元または信頼できない送信元としてのインターフェイスの設定

デバイスでの DHCP グリーニングを有効化または無効化できます。DHCP メッセージの信頼された送信元または信頼できない送信元としてインターフェイスを設定できます。信頼できないインターフェイスまたはデバイスポートで DHCP グリーニングが有効になっている場合、DHCP パケットがドロップされないことを確認します。

（注） デフォルトでは、DHCP グリーニングは無効になっています。

DHCP の信頼状態は、次のタイプのインターフェイスに設定できます。

- レイヤ 2 イーサネット インターフェイス
- レイヤ 2 ポート チャネル インターフェイス

（注） デフォルトでは、すべてのインターフェイスは信頼できません。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip dhcp snooping glean**
4. **interface** *type number*
5. [**no**] **ip dhcp snooping trust**
6. **end**
7. **show ip dhcp snooping statistics**
8. **show ip dhcp snooping**

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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip dhcp snooping glean** 例： `Device(config)# ip dhcp snooping glean`	インターフェイスで DHCP グリーニングを有効にします。
ステップ 4	**interface** *type number* 例： `Device(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 モードを開始します。*type number* は、DHCP スヌーピングのために信頼状態を設定するレイヤ 2 イーサネット インターフェイスです。
ステップ 5	[**no**] **ip dhcp snooping trust** 例： `Device(config-if)# ip dhcp snooping trust`	DHCP スヌーピングに関してインターフェイスを信頼できるインターフェイスとして設定します。**no** オプションを使用すると、ポートは信頼できないインターフェイスとして設定されます。
ステップ 6	**end** 例：	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。

	コマンドまたはアクション	目的
	`Device(config-if)# end`	
ステップ 7	**show ip dhcp snooping statistics** 例： `Device# show ip dhcp snooping statistics`	信頼できないインターフェイスとして設定されたデバイスポートでドロップされたパケットを表示します。
ステップ 8	**show ip dhcp snooping** 例： `Device# show ip dhcp snooping`	DHCP グリーニングに関する情報など、DHCP スヌーピングの設定情報を表示します。

DHCP グリーニングの設定例

例：DHCP グリーニングの信頼された送信元または信頼できない送信元としてのインターフェイスの設定

Dynamic Host Configuration Protocol（DHCP）グリーニングを有効にし、インターフェイスを信頼されたインターフェイスとして設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp snooping glean
Device(config)# interface gigabitEthernet 1/0/1
Device(config-if)# ip dhcp snooping trust
Device(config-if)# end
```

DHCP グリーニングに関する追加情報

標準および RFC

標準/RFC	タイトル
RFC-2131	『*Dynamic Host Configuration Protocol*』
RFC-4388	*DHCP リースクエリ*

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

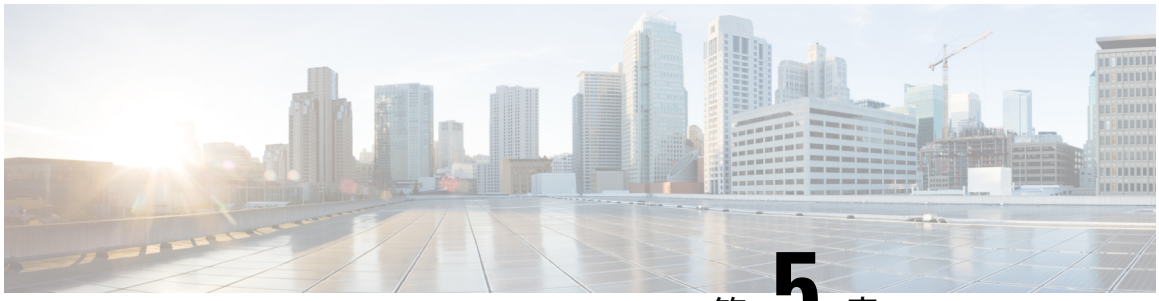
DHCP グリーニングの機能情報

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

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

表 *5 : DHCP* グリーニングの機能情報

機能名	リリース	機能情報
DHCP グリーニング	Cisco IOS XE Fuji 16.8.1a	DHCP グリーニングは、コンポーネントが DHCP バージョン 4 パケットのみを登録およびグリーニングできるようにする読み取り専用 DHCP スヌーピング機能です。



第 5 章

DHCP オプションのサポート

DHCP オプションサポートに関する制約事項

プライマリ VLAN に対して DHCP スヌーピングが設定されている場合は、いずれのセカンダリ VLAN に対しても、異なる設定を持つスヌーピングを設定できません。関連付けられているすべての VLAN 用の DHCP スヌーピングをプライマリ VLAN に対して設定する必要があります。プライマリ VLAN に対して DHCP スヌーピングが設定されていないときに、セカンダリ VLAN、たとえば VLAN 200 に対して設定しようとすると、次のメッセージが表示されます。

```
2w5d:%DHCP_SNOOPING-4-DHCP_SNOOPING_PVLAN_WARNING:DHCP Snooping configuration may not
take effect
on secondary vlan 200. DHCP Snooping configuration on secondary vlan is derived from its
 primary vlan.
```

show ip dhcp snooping コマンドを使用すると、プライマリかセカンダリかを問わず、DHCP スヌーピングが有効にされているすべての VLAN が表示されます。

DHCP オプションのサポートに関する情報

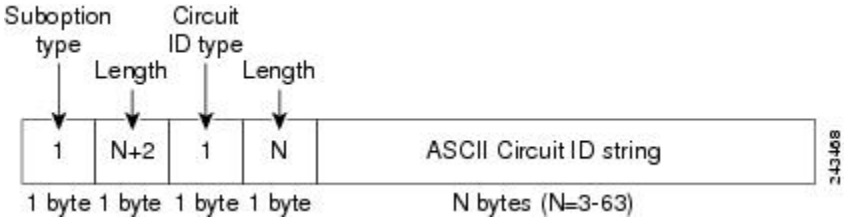
DHCP Option 82 の設定が可能な回線 ID およびリモート ID

DHCP Option 82 設定可能な回線 ID およびリモート ID 機能では、Option 82 リモート ID サブオプションおよび Option 82 回線 ID サブオプションで提供する情報を指定できるため、検証セキュリティが強化されます。

DHCP スヌーピングはプライベート VLAN 上でイネーブルにできます。DHCP スヌーピングがイネーブルの場合、設定はプライマリ VLAN およびそれに関連付けられているセカンダリ VLAN の両方に伝播します。プライマリ VLAN で DHCP スヌーピングがイネーブルの場合は、セカンダリ VLAN でもイネーブルにされます。

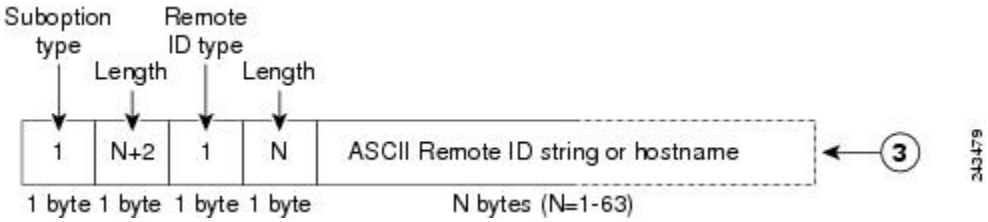
次の図に、DHCP スヌーピングがグローバルに有効になっており、回線 ID サブオプションを指定して **ip dhcp snooping information option** グローバル コンフィギュレーション コマンドを入力した場合に使用されるパケットフォーマットを示します。

図 *6:* 回線 *ID* を指定した場合のサブオプション パケット フォーマット



次の図に、DHCP スヌーピングがグローバルに有効になっており、リモート ID サブオプションを指定して **ip dhcp snooping information option** グローバル コンフィギュレーション コマンドを入力した場合に使用されるパケットフォーマットを示します。

図 *7:* リモート *ID* を指定した場合のサブオプション パケット フォーマット



DHCP クライアントオプション 12

DHCP クライアントオプション 12 機能により、クライアントのホスト名が指定されます。Dynamic Host Configuration Protocol（DHCP）サーバからインターフェイスの IP アドレスを取得する際に、クライアントデバイスが応答内の DHCP Hostname オプションを受信すると、このオプションのホスト名が設定されます。DHCP は、IP ネットワークにおける動作のための設定情報を取得するために DHCP クライアントによって使用されます。

設定パラメータやその他の制御情報は、DHCP メッセージのオプションフィールドに格納されたタグ付きデータ項目で伝送されます。DHCP クライアントに対してオプション 12 を設定できるため、DHCP クライアントには柔軟性があります。

オプション 12 により、クライアントの名前が指定されます。この名前は、ローカルドメインで修飾される場合と修飾されない場合があります。

DHCP オプションサポートの設定方法

プライベート VLAN に対する DHCP スヌーピングの設定

プライベートのプライマリ VLAN およびセカンダリ VLAN に対して DHCP スヌーピングを設定するには、次の作業を実行してください。

- プライベートのプライマリ VLAN を設定します。
- 独立 VLAN をこのプライマリ VLAN に関連付けます。
- プライマリ VLAN 用の SVI インターフェイスを作成し、適切なループバック IP およびヘルパー アドレスをインターフェイスに関連付けます。
- プライマリ VLAN で DHCP スヌーピングをイネーブルにします。その結果、関連付けられている VLAN でも DHCP スヌーピングがイネーブルになります。

（注） スヌーピングに実効性を持たせるには、IP アドレス、DHCP プール、およびリレー ルートを割り当てるサーバを設定する必要もあります。

手順の概要

1. **enable**
2. **configure terminal**
3. **vlan** *vlan-id*
4. **private-vlan primary**
5. **private-vlan association** *secondary-vlan-list*
6. **exit**
7. **vlan** *vlan_ID*
8. **private-vlan isolated**
9. **exit**
10. **interface vlan** *primary-vlan_id*
11. **ip unnumbered loopback**
12. **private-vlan mapping** [*secondary-vlan-list* | **add** *secondary-vlan-list*| **remove** *secondary-vlan-list*]
13. **exit**
14. **ip dhcp snooping vlan** *primary-vlan_id*
15. **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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vlan** *vlan-id* 例： `Device(config)# vlan 70`	指定したプライベート VLAN の 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	**private-vlan primary** 例： `Device(config-vlan)# private-vlan primary`	VLAN をプライマリ PVLAN として指定します。
ステップ 5	**private-vlan association** *secondary-vlan-list* 例： `Device(config-vlan)# private-vlan association 7`	プライベート VLAN（PVLAN）の設定および PVLAN とセカンダリ VLAN とのアソシエーションの設定を行います。
ステップ 6	**exit** 例： `Device(ocnfig-vlan)# exit`	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 モードに戻ります。
ステップ 7	**vlan** *vlan_ID* 例： `Device(config)# vlan 7`	指定したプライベート VLAN の VLAN コンフィギュレーション モードを開始します。 • この例では、関連付けられるセカンダリ VLAN は vlan 7 です。
ステップ 8	**private-vlan isolated** 例： `Device(config-vlan)# private-vlan isolated`	この VLAN を独立プライベート VLAN として指定します。

	コマンドまたはアクション	目的
ステップ 9	**exit** 例： `Device(config-vlan)# exit`	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 モードに戻ります。
ステップ 10	**interface vlan** *primary-vlan_id* 例： `Device(config)# interface vlan 70`	プライマリ VLAN でダイナミックスイッチ仮想インターフェイス（SVI）を作成して、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 11	**ip unnumbered loopback** 例： `Device(config-if)# ip unnumbered loopback1`	IP アンナンバード ループバックを指定します。
ステップ 12	**private-vlan mapping** [*secondary-vlan-list* | **add** *secondary-vlan-list*| **remove** *secondary-vlan-list*] 例： `Device(config-if)# private-vlan mapping 7`	プライマリ VLAN とセカンダリ VLAN のマッピングを作成して、それらに同じプライマリ VLAN SVI を共有させます。
ステップ 13	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 14	**ip dhcp snooping vlan** *primary-vlan_id* 例： `Device(config)# ip dhcp snooping vlan 70`	プライマリ VLAN および関連付けられた VLAN で DHCP スヌーピングをイネーブルにします。
ステップ 15	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

DHCP オプションサポートの設定例

例：プライベート VLAN 関連付けのマッピング

次のインターフェイス コンフィギュレーションの例は、プライベート VLAN アソシエーションのマッピング方法を示します。ユーザ設定可能な回線 ID「aabb11」がセカンダリ VLAN である vlan 7 に挿入されます。

```
Device> enable
Device# configure terminal
Device(config-if)# interface GigabitEthernet 9/0/1
Device(config-if)# switchport
Device(config-if)# switchport private-vlan host-association 70 7
Device(config-if)# switchport mode private-vlan host
Device(config-if)# no mls qos trust
Device(config-if)# spanning-tree portfast
Device(config-if)# exit
Device(config)# ip dhcp snooping vlan 7 information option format-type circuit-id string
 aabb11
Device(config)# end
```

次の例は、DHCP クラス「C1」を定義し、このインターフェイス コンフィギュレーションの例で入力された回線 ID 値と一致する 16 進文字列を使用して、サーバで対応するクラスの 16 進文字列を指定する方法を示しています。つまり、16 進文字列 00000000000000000000000000000066616162623131 マスク ffffffffffffffffffffffffffff0000000000000 は、回線 ID aabb11 と一致します。

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp class C1
Device(config-dhcp-class)# relay agent information
Device(config-dhcp-class-relayinfo)# relay-information hex
00000000000000000000000000000066616162623131
mask ffffffffffffffffffffffffffff0000000000000
Device(config-dhcp-class-relayinfo)# end
```

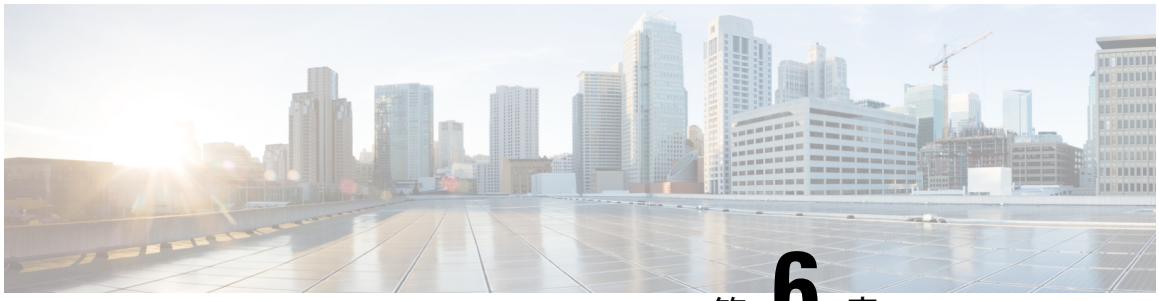
DHCP オプションサポートの機能情報

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

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

表 *6 : DHCP* オプションサポートの機能情報

機能名	リリース	機能情報
DHCP クライアントオプション 12	Cisco IOS XE Fuji 16.8.1a	DHCP クライアントオプション 12 機能により、クライアントのホスト名が指定されます。Dynamic Host Configuration Protocol（DHCP）サーバからインターフェイスの IP アドレスを取得する際に、クライアントデバイスが応答内の DHCP Hostname オプションを受信すると、このオプションのホスト名が設定されます。DHCP は、IP ネットワークにおける動作のための設定情報を取得するために DHCP クライアントによって使用されます。
DHCP Option 82 設定可能な回線 ID およびリモート ID	Cisco IOS XE Fuji 16.8.1a	Option 82 リモート ID サブオプションおよび Option 82 回線 ID サブオプションでの命名の選択肢を規定します。



第 6 章

DHCPv6 オプションのサポート

DHCPv6 オプションのサポートに関する情報

CAPWAP アクセスコントローラ DHCPv6 オプション

Control And Provisioning of Wireless Access Points（CAPWAP）プロトコルでは、中央管理型アクセスポイントが接続可能なワイヤレスコントローラをDHCPを使用して検出できます。CAPWAPは標準の相互運用プロトコルであり、コントローラによるワイヤレスアクセスポイントの集合の管理を可能にします。

ワイヤレスアクセスポイントは、プライマリ、セカンダリ、およびターシャリ ワイヤレス コントローラの IPv6 管理インターフェイスアドレスを提供する DHCPv6 オプション 52（RFC 5417）を使用します。

ステートレスとステートフル両方のDHCPv6アドレッシングモードがサポートされています。ステートレスモードでは、アクセスポイントがステートレスアドレス自動設定（SLAAC）を使用して IPv6 アドレスを取得する一方で、（ルータアドバタイズメントから取得されない）その他のネットワーク情報はDHCPv6サーバから取得されます。ステートフルモードでは、アクセスポイントが IPv6 アドレスと他のネットワーク情報の両方を DHCPv6 サーバのみから取得します。どちらのモードでも、DHCPv6を使用してワイヤレスコントローラを検出する必要がある場合、オプション 52 を可能にするには DHCPv6 サーバが必要です。

MAX_PACKET_SIZE が 15 を超えており、オプション 52 が設定されている場合、DHCPv6 サーバは DHCP パケットを送信しません。

DNS 検索リストのオプション

DNS 検索リスト（DNSSL）は、ドメインネームシステム（DNS）サフィックスドメイン名のリストであり、IPv6 ホストで短い、修飾子を持たないドメイン名に対する DNS クエリ検索を実行する際に使用されます。DNSSL オプションには、1 つ以上のドメイン名が含まれます。すべてのドメイン名が同じライフタイム値を共有します。ライフタイム値とは、DNSSL を使用できる最大時間を秒単位で示したものです。異なるライフタイム値が必要な場合は、複数の DNSSL オプションを使用できます。最大 5 つの DNSSL を設定できます。

長い DNSSL 名を持つ DHCP メッセージは、デバイスによって破棄されます。

（注） 複数のルータアドバタイズメント（RA）や DHCP から DNS 情報を入手できる場合、ホストはこの DNS 情報の順序付きリストを保持する必要があります。

RFC 6106 は、拡張 DNS 設定のため、IPv6 ルータが IPv6 ホストに DNS 検索リスト（DNSSL）をアドバタイズできるようする IPv6 ルータアドバタイズメント（RA）オプションを指定しています。

DNS ライフタイムの範囲は、次の例に示すように、最大 RA 間隔の値と最大 RA 間隔を 2 倍にした値の間に設定する必要があります。

```
(max ra interval) <= dns lifetime <= (2*(max ra interval))
```

最大 RA 間隔の値は 4 ー 1800 秒の間で指定できます（デフォルトは 240 秒）。次の例は、範囲外のライフタイムを示しています。

```
Device(config-if)# ipv6 nd ra dns-search-list sss.com 3600
! Lifetime configured out of range for the interface that has the  default maximum RA
interval.!
```

DHCPv6 クライアントのリンク層アドレスオプション

DHCPv6 クライアントのリンク層アドレスオプション（RFC 6939）は、ファーストホップ DHCPv6 リレーエージェント（クライアントと同じリンクに接続されたリレーエージェント）がサーバに送信されている DHCPv6 メッセージでクライアントのリンク層アドレスを提供できるようにするための、オプションのメカニズムと関連 DHCPv6 オプションを定義します。

クライアントのリンク層アドレスオプションは、リレーエージェントとサーバ間でのみ交換されます。DHCPv6 クライアントは、クライアントのリンク層アドレスオプションの使用を認識しません。DHCPv6 クライアントは、クライアントのリンク層アドレスオプションを送信してはならず、クライアントのリンク層アドレスオプションを無視する必要があります。

各 DHCPv6 クライアントとサーバは、DHCP 固有識別子（DUID）によって識別されます。DUID は、クライアント識別子およびサーバ識別子オプションで伝送されます。DUID はすべての DHCP クライアントとサーバで一意であり、特定のクライアントまたはサーバに固定され

ます。DHCPv6では、クライアントとサーバの両方の識別子にリンク層アドレスに基づくDUIDを使用します。デバイスは、最も小さい番号のインターフェイスのMACアドレスを使用してDUIDを形成します。ネットワークインターフェイスは、デバイスに永続的に接続されていると見なされます。

DHCP リレー エージェント

DHCP リレー エージェントは、クライアントとサーバの間でDHCPパケットを転送するレイヤ3デバイスです。リレーエージェントは、同じ物理サブネット上にないクライアントとサーバの間で要求および応答を転送します。リレー エージェントによる転送は、IP データグラムをネットワーク間で透過的に交換するレイヤ 2 での通常の転送とは異なります。リレー エージェントは、DHCPメッセージを受け取ると、新しいDHCPメッセージを生成して、出力インターフェイス上で送信します。

DHCPv6 オプションサポートの設定方法

このセクションでは、DHCPv6 オプションサポートを設定する方法について説明します。

CAPWAP アクセスポイントの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **capwap-ac address** *ipv6-address*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 dhcp pool** *poolname* 例： `Device(config)# ipv6 dhcp pool pool1`	DHCPv6 サーバ設定情報プールを設定し、DHCPv6 プール 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 4	**capwap-ac address** *ipv6-address* 例： `Device(config-dhcpv6)# capwap-ac address 2001:DB8::1`	CAPWAP アクセス コントローラ アドレスを設定します。
ステップ 5	**end** 例： `Device(config-dhcpv6)# end`	DHCPv6 プール コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPv6 ルータ アドバタイズメント オプションを使用した DNS 検索リストの設定

IPv6 ルータ アドバタイズメント オプションを使用して DNS 検索リストを設定するには、次のタスクを実行します。

（注） ドメイン名の設定は、RFC 1035 に従って行う必要があります。そうでない場合、設定が拒否されます。たとえば、次のドメイン名の設定はエラーになります。

```
Device(config-if)# ipv6 nd ra dns-search-list domain example.example.com infinite-lifetime
```

（注） **ipv6 nd ra dns-search-list domain** コマンドは、レイヤ 3 モードでルーテッドポートとして設定されている物理インターフェイスのみで設定できます。この設定は、インターフェイス コンフィギュレーション モードで **no switchport** コマンドを使用することにより実行できます。

インターフェイスで単一の DNS 検索リストを削除するには、インターフェイス コンフィギュレーション モードで **no ipv6 nd ra dns-search-list domain** *domain-name* コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-type interface-number*
4. **no switchport**
5. **ipv6 nd prefix** *ipv6-prefix/prefix-length*
6. **ipv6 nd ra lifetime** *seconds*
7. **ipv6 nd ra dns-search-list domain** *domain-name* [**lifetime** [*lifetime-value* | **infinite**]]
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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-type interface-number* 例： `Device(config)# interface GigabitEthernet 0/2/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**no switchport** 例： `Device(config-if)# no switchport`	物理ポートに限り、レイヤ 3 モードを開始します。
ステップ 5	**ipv6 nd prefix** *ipv6-prefix/prefix-length* 例： `Device(config-if)# ipv6 nd prefix 2001:DB8::1/64 1111 222`	IPv6 ネイバー探索（ND）ルータアドバタイズメントに含める IPv6 プレフィックスを設定します。
ステップ 6	**ipv6 nd ra lifetime** *seconds* 例： `Device(config-if)# ipv6 nd ra lifetime 9000`	インターフェイス上の IPv6 ルータアドバタイズメントに含まれるデバイスのライフタイム値を設定します。
ステップ 7	**ipv6 nd ra dns-search-list domain** *domain-name* [**lifetime** [*lifetime-value* | **infinite**]] 例： `Device(config-if)# ipv6 nd ra dns-search-list domain example.example.com lifetime infinite`	DNS 検索リストを設定します。検索リストのライフタイムを指定できます。 （注） Cisco IOS XE Giraltar 16.12.1 よりも前のリリースの場合、このコマンドは **ipv6 nd ra dns search list** *list-name***infinite-lifetime** として存在します。
ステップ 8	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

DHCPv6 オプションサポートの設定例

例：CAPWAP アクセスポイントの設定

次に、CAPWAP アクセスポイントの設定方法の例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 dhcp pool pool1
Device(config-dhcpv6)# capwap-ac address 2001:DB8::1
Device(config-dhcpv6)# end
Device#
```

DHCPv6 オプションサポートの確認

オプション 52 サポートの確認

次に、**show ipv6 dhcp pool** コマンドの出力例として DHCPv6 設定プールの情報を表示します。

```
Device# show ipv6 dhcp pool

DHCPv6 pool: svr-p1
  Static bindings:
    Binding for client 000300010002FCA5C01C
      IA PD: IA ID 00040002,
        Prefix: 2001:db8::3/72
                preferred lifetime 604800, valid lifetime 2592000
      IA PD: IA ID not specified; being used by 00040001
        Prefix: 2001:db8::1/72
                preferred lifetime 240, valid lifetime 54321
        Prefix: 2001:db8::2/72
                preferred lifetime 300, valid lifetime 54333
        Prefix: 2001:db8::3/72
                preferred lifetime 280, valid lifetime 51111
  Prefix from pool: local-p1, Valid lifetime 12345, Preferred lifetime 180
  DNS server: 1001::1
  DNS server: 1001::2
  CAPWAP-AC Controller address: 2001:DB8::1
  Domain name: example1.com
  Domain name: example2.com
  Domain name: example3.com
 Active clients: 2
```

次に、DHCPv6 のデバッグを有効にする例を示します。

```
Device# debug ipv6 dhcp detail

IPv6 DHCP debugging is on (detailed)
```

DHCPv6 オプションのサポートに関する追加情報

標準および RFC

標準/RFC	Title
RFC 6106	DNS 設定の IPv6 ルータ アドバタイズメント オプション
RFC 54171	Control And Provisioning of Wireless Access Points（CAPWAP）アクセスコントローラ DHCP オプション
RFC 6939	DHCPv6 のクライアントリンク層アドレスオプション

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

DHCPv6 オプションサポートの機能情報

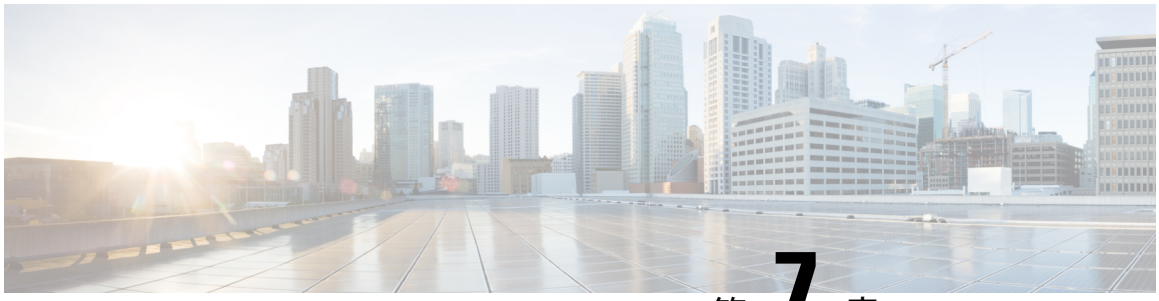
次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *7: DHCPv6* オプションサポートの機能情報

機能名	リリース	機能情報
CAPWAP アクセスコントローラ DHCPv6 オプション 52	Cisco IOS XE Everest 16.9.2	CAPWAP プロトコルでは、中央管理型アクセスポイントの接続先ワイヤレスコントローラを DHCPv6 を使用して検出できます。CAPWAP は標準の相互運用プロトコルであり、コントローラによるワイヤレスアクセスポイントの集合の管理を可能にします。
DHCPv6 クライアントのリンク層アドレスオプション	Cisco IOS XE Everest 16.9.2	DHCPv6 クライアントのリンク層アドレスオプション（RFC 6939）は、ファーストホップ DHCPv6 リレーエージェント（クライアントと同じリンクに接続されたリレーエージェント）がサーバに送信されている DHCPv6 メッセージでクライアントのリンク層アドレスを提供できるようにするための、オプションのメカニズムと関連 DHCPv6 オプションを定義します。
DNS 検索リスト	Cisco IOS XE Everest 16.9.2	DNS 検索リスト（DNSSL）は、ドメインネームシステム（DNS）サフィックスドメイン名のリストであり、IPv6 ホストで短い、修飾子を持たないドメイン名に対する DNS クエリ検索を実行する際に使用されます。DNSSL オプションには、1 つ以上のドメイン名が含まれます。

機能名	リリース	機能情報
DHCPv6 リレーチェーニングおよびルート挿入 DHCPv6 クライアントのリンク層アドレスオプション：コマンド変更 RFC 6106 および RFC 5417 の IPv6 サポート	Cisco IOS XE Gibraltar 16.12.1	DHCPv6 リレーチェーニングおよびルート挿入機能により、DHCPv6 メッセージを複数のリレーエージェントでリレーできます。 **ipv6 nd ra dns search list** コマンドのシンタックスが **ipv6 nd ra dns-search-list domain** に変更されました。**show ipv6 nd ra dns-search-list** コマンドが導入されました。 IPv6 のサポートは、DNS 設定の IPv6 ルータ アドバタイズメント オプション（RFC 6106）、および Control And Provisioning of Wireless Access Points（CAPWAP）アクセスコントローラ DHCP オプション（RFC 5417）で導入されました。



第 7 章

DHCPv6 リレー ソース設定

DHCPv6 リレー送信元の設定の制限事項

- 設定済みのインターフェイスがシャットダウンされた場合、またはその IPv6 アドレスのすべてが削除された場合、リレーは標準の動作に戻ります。
- IPv6アドレスが設定されていないインターフェイスを指定しようとすると、コマンドライン インターフェイス（CLI）によってエラーが報告されます。
- インターフェイス コンフィギュレーションとグローバル コンフィギュレーションの両方が設定されている場合、インターフェイス コンフィギュレーションが優先されます。

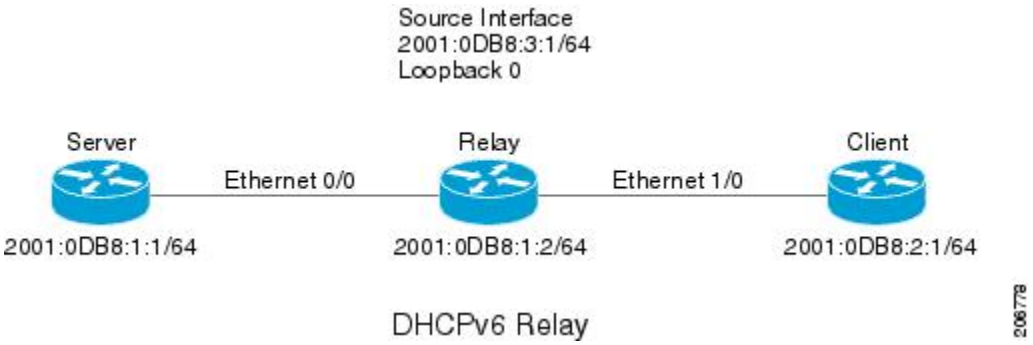
DHCPv6 リレー送信元の設定に関する情報

DHCPv6 リレー ソース設定

DHCPv6サーバは、応答を中継されたメッセージの送信元アドレスに送信します。通常、DHCPv6リレーは、メッセージ送信に使用されたサーバ方向インターフェイスのアドレスを送信元として使用します。ただし、一部のネットワークでは、より安定したアドレス（ループバック インターフェイスなど）を設定し、そのインターフェイスを中継されたメッセージの送信元アドレスとしてリレーで使用することが望ましい場合があります。DHCPv6リレー送信元設定機能には、この機能が用意されています。

次の図に、単一のクライアント、リレー、およびサーバで構成される簡単なネットワークを示します。リレーとサーバは 2001:DB8:1::/64 を介して通信し、リレーには 2001:DB8:2::/64 に対するクライアント方向インターフェイスがあります。リレーには、アドレス 2001:DB8:3:1/64 が設定されたループバック インターフェイスもあります。

図 *8 : DHCPv6* リレー送信元設定 - 簡単なネットワーク



リレーはクライアントから要求を受信すると、クライアント方向インターフェイス（イーサネット 1/0）のアドレスを relay-forward メッセージの link-address フィールドに含めます。このアドレスは、サーバによってアドレス プールの選択に使用されます。その後、リレーは relay-forward メッセージをサーバに送信します。デフォルトでは、サーバ方向（イーサネット 0/0）インターフェイスのアドレスが IPv6 送信元として使用され、サーバはそのアドレスに応答を送信します。

リレーの送信元インターフェイスが明示的に設定されている場合、リレーはそのインターフェイスのプライマリ IPv6 アドレスを、転送するメッセージの IPv6 送信元として使用します。たとえば、ループバック 0 を送信元として設定すると、リレーは、サーバに中継されるメッセージの IPv6 送信元アドレスとして 2001:DB8:3:1/64 を使用します。

DHCPv6 リレー送信元の設定方法

DHCPv6 リレー送信元の設定

DHCPv6 リレー送信元を設定するには、次の作業を実行します。

インターフェイスに対する DHCPv6 リレー送信元の設定

メッセージの中継時に送信元として使用するインターフェイスを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*

4. **ipv6 dhcp relay source-interface** *interface-type interface-number*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface loopback 0`	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 dhcp relay source-interface** *interface-type interface-number* 例： `Device(config-if)# ipv6 dhcp relay source-interface loopback 0`	このインターフェイスで受信したメッセージの中継時に送信元として使用するインターフェイスを設定します。
ステップ 5	**end** 例： `Device(config-if)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

DHCPv6 リレー送信元のグローバルな設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp-relay source-interface** *interface-type interface-number*
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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 dhcp-relay source-interface** *interface-type interface-number* 例： `Device(config)# ipv6 dhcp-relay source-interface loopback 0`	メッセージの中継時に送信元として使用するインターフェイスを設定します。
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

DHCPv6 リレー送信元の設定例

例：インターフェイスに対する DHCPv6 リレー送信元の設定

次の例で、リレーの送信元として使用するループバック 0 インターフェイスの設定方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface loopback 0
Device(config-if)# ipv6 dhcp relay source-interface loopback 0
Device(config-if)# end
```

DHCPv6 リレー送信元の設定に関する追加情報

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	*IPv6 RFCs*

シスコのテクニカル サポート

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

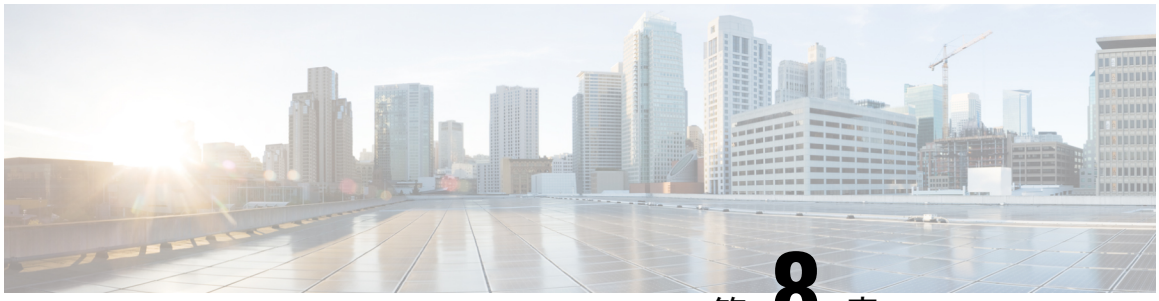
DHCPv6 リレー送信元の設定に関する機能情報

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 *8 : DHCPv6* リレー送信元の設定に関する機能情報

機能名	リリース	機能情報
DHCPv6 リレー ソース設定	Cisco IOS XE Fuji 16.8.1a	DHCPv6を使用する一部のネットワークでは、より安定したアドレス（ループバック インターフェイスなど）を設定し、そのインターフェイスを中継されたメッセージの送信元アドレスとしてリレーで使用することが望ましい場合があります。DHCPv6 リレー送信元設定機能には、この機能が用意されています。



第 8 章

GRE トンネル IP 送信元および宛先 VRF メンバーシップの設定

GRE トンネル IP 送信元および宛先 VRF メンバーシップの制約事項

- トンネルの両端は同じ VRF 内に存在する必要があります。
- tunnel vrf コマンドで関連付けられた VRF は、トンネルがパケットを送信する際に経由する物理インターフェイスに関連付けられている VRF と同じです（外部 IP パケット ルーティング）。
- ip vrf forwarding コマンドを使用してトンネルに関連付けられた VRF は、パケットがトンネルを出る際に転送される VRF です（内部 IP パケット ルーティング）。
- この機能では、マルチキャスト トンネルを通過するマルチキャスト パケットのフラグメンテーションはサポートされません。
- この機能では、ISIS（Intermediate System to Intermediate System）プロトコルはサポートされません。

GRE トンネル IP 送信元および宛先 VRF メンバーシップについての情報

この機能では、トンネルの送信元と宛先を任意のバーチャルプライベートネットワーク（VPN）ルーティングおよび転送（VRF）テーブルに所属するように設定できます。VRF テーブルには、各 VPN のルーティング データが保管されます。VRF テーブルでは、ネットワーク アクセス サーバ（NAS）に接続されているカスタマー サイトの VPN メンバーシップを定義します。各 VRF テーブルは、IP ルーティング テーブル、派生したシスコ エクスプレス フォワーディング（CEF）テーブル、およびルーティング テーブルに含まれる情報を制御するガイドラインおよびルーティング プロトコル パラメータから構成されます。

以前は、GRE IP トンネルでは IP トンネルの宛先がグローバル ルーティング テーブルに含まれている必要がありました。この機能の実装により、トンネルの送信元と宛先が任意の VRF に所属するよう設定できます。既存の GRE トンネルと同様、トンネルの宛先へのルートが定義されていない場合は、トンネルはディセーブルになります。

GRE トンネル IP 送信元および宛先 VRF メンバーシップの設定方法

GRE トンネル IP 送信元および宛先 VRF メンバーシップを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface tunnel***number*
4. **ip vrf forwarding***vrf-name*
5. **ip address***ip-address subnet-mask*
6. **tunnel source** {*ip-address* | *type number*}
7. **tunnel destination** {*hostname* | *ip-address*}
8. **tunnel vrf***vrf-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： `Device>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： `Device#configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface tunnel***number* 例： `Device(config)#interface tunnel 0`	指定したインターフェイスのインターフェイス コンフィギュレーション モードを開始します。 • *number* はトンネルインターフェイスに関連付けられた番号です。
ステップ 4	**ip vrf forwarding***vrf-name* 例： `Device(config-if)#ip vrf forwarding green`	バーチャルプライベート ネットワーク（VPN）ルーティングおよび転送（VRF）インスタンスをインターフェイスまたはサブインターフェイスに関連付けます。 • *vrf-name* は VRF に割り当てられる名前です。
ステップ 5	**ip address***ip-address subnet-mask* 例： `Device(config-if)#ip address 10.7.7.7 255.255.255.255`	インターフェイス IP アドレスとサブネット マスクを指定します。 • *ip-address* でインターフェイスの IP アドレスを指定します。 • *subnet-mask* でインターフェイスのサブネットマスクを指定します。
ステップ 6	**tunnel source** {*ip-address* | *type number*} 例： `Device(config-if)#tunnel source loop 0`	トンネルインターフェイスの送信元を指定します。 • *ip-address* でトンネル内のパケットの送信元アドレスとして使用する IP アドレスを指定します。 • *type* でインターフェイスのタイプ（シリアルなど）を指定します。 • *number* でポート、コネクタ、またはインターフェイスカードの番号を指定します。この番号は、設置時、またはシステムへの追加時に、工場で割り当てられます。また、show interfaces コマンドを使用して表示できます。
ステップ 7	**tunnel destination** {*hostname* | *ip-address*} 例： `Device(config-if)#tunnel destination 10.5.5.5`	トンネルの宛先を指定します。 • *hostname* で宛先ホストの名前を指定します。 • *ip-address* で宛先ホストの IP アドレスを指定します。

	コマンドまたはアクション	目的
ステップ 8	**tunnel vrf***vrf-name* 例： `Device(config-if)#tunnel vrf finance1`	特定のトンネル宛先に VPN ルーティングおよび転送（VRF）インスタンスを関連付けます。 • *vrf-name* は VRF に割り当てられる名前です。

GRE トンネル IP 送信元および宛先 VRF メンバーシップの設定例

次に、VRF green を使用してインターフェイス e0 で受信されたパケットを、VRF blue を使用し、インターフェイス e1 を通じてトンネルから外部へ転送する例を示します。

```
ip vrf blue rd 1:1

ip vrf green rd 1:2

interface loop0
ip vrf forwarding blue
ip address 10.7.7.7 255.255.255.255

interface tunnel0
ip vrf forwarding green
ip address 10.3.3.3 255.255.255.0 tunnel source loop 0
tunnel destination 10.5.5.5 tunnel vrf blue

interface ethernet0
ip vrf forwarding green
ip address 10.1.1.1 255.255.255.0

interface ethernet1
ip vrf forwarding blue
ip address 10.2.2.2 255.255.255.0

ip route vrf blue 10.5.5.5 255.255.255.0 ethernet 1
```

その他の参考資料

表 *9:* 関連資料

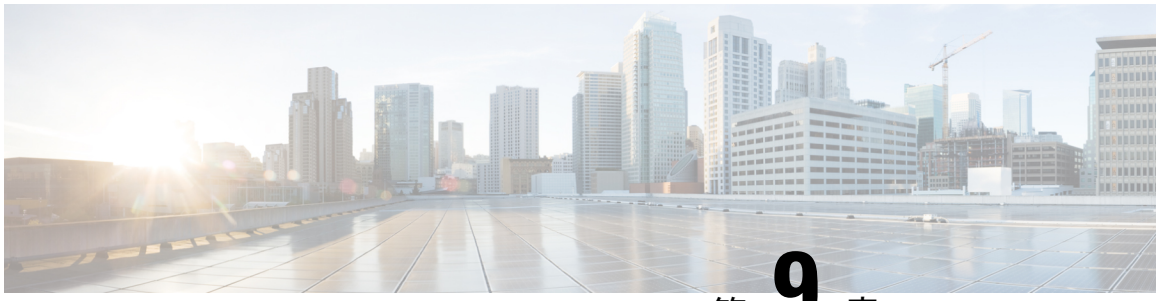
関連項目	マニュアル タイトル
VRF テーブル	『Cisco IOS Switching Services Configuration Guide, Release 12.2』の「Configuring Multiprotocol Label Switching」の章
トンネル	『Cisco IOS Interface Configuration Guide, Release 12.2』

Generic Routing Encapsulation（GRE）トンネル IP 送信元および宛先 VRF メンバーシップの機能履歴

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。

表 *10 : Generic Routing Encapsulation*（*GRE*）トンネル *IP* 送信元および宛先 *VRF* メンバーシップの機能履歴

機能名	リリース	機能情報
Generic Routing Encapsulation トンネル IP 送信元および宛先 VRF メンバーシップ	Cisco IOS 16.6.1	Generic Routing Encapsulation トンネルの IP 送信元および宛先の VRF メンバーシップ機能では、トンネルの送信元および宛先が任意のバーチャル プライベート ネットワーク（VPN）ルーティングおよび転送（VRF）テーブルに属するように設定できます。



第 9 章

IPv4 GRE トンネルを介した IPv6 の設定

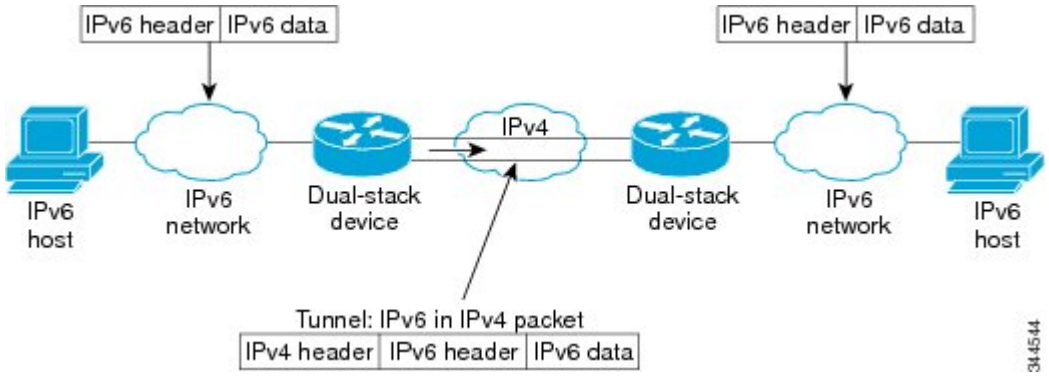
IPv4 GRE トンネルを介した IPv6 の設定に関する情報

続くセクションでは、IPv4 GRE トンネルを介した IPv6 の設定について説明します。

Ipv6 用オーバーレイ トンネル

オーバーレイ トンネリングでは、IPv4 パケット内で IPv6 パケットをカプセル化して、IPv4 インフラストラクチャ（コア ネットワークまたは以下の図）へ伝送します。オーバーレイ トンネルを使用することで、孤立した IPv6 ネットワークと通信できます。このとき、孤立した複数の IPv6 ネットワーク間にある IPv4 インフラストラクチャをアップグレードする必要はありません。オーバーレイ トンネルは、境界デバイス間、または境界デバイスとホスト間に設定できますが、両方のエンドポイントが IPv4 プロトコル スタックと IPv6 プロトコル スタックの両方をサポートしている必要があります。

図 *9:* オーバーレイ トンネル



（注） オーバーレイ トンネルにより、インターフェイスの最大伝送単位（MTU）が 20 オクテット減少します（ただし、基本 IPv4 パケット ヘッダーにオプション フィールドが含まれていないことを前提とします）。オーバーレイ トンネルを使用するネットワークは、トラブルシューティングが困難です。したがって、独立した IPv6 ネットワークに接続するオーバーレイ トンネルは、最終的な IPv6 ネットワーク アーキテクチャと見なしてはいけません。オーバーレイ トンネルの使用は、IPv4 と IPv6 の両方のプロトコル スタック、または IPv6 プロトコル スタックだけをサポートするネットワークへの移行方法と見なす必要があります。

IPv6 は、GRE タイプのオーバーレイトンネリングをサポートします。IPv4 GRE トンネルを介した IPv6 は、IPv6、Connectionless Network Service（CLNS）など、さまざまなタイプのパケットを伝送できます。

IPv6 トラフィック用の GRE IPv4 トンネル サポート

IPv6 トラフィックは、標準的なポイントツーポイントのカプセル化スキームの実装にサービスを提供するように設計されている標準 GRE トンネリング技術を使用して、IPv4 GRE トンネルを介して伝送できます。GRE トンネルは、手動で設定された IPv6 トンネルと同様、リンクごとに個別のトンネルが設定された 2 つのポイント間のリンクです。これらのトンネルは、特定のパッセンジャまたはトランスポート プロトコルに結合されていませんが、この場合、GRE を使用するパッセンジャ プロトコルとして IPv6 を伝送し、トランスポート プロトコルとして IPv4 または IPv6 を伝送します。

GRE トンネルは、2 つのエッジ デバイス間またはエッジ デバイスとエンド システム間に定期的でセキュアな通信を必要とする安定した接続のために主に使用されます。エッジデバイスとエンド システムは、デュアル スタック実装である必要があります。

IPv4 GRE トンネルを介した IPv6 の実装方法

次のセクションでは、IPv4 GRE トンネルを介した IPv6 の設定について説明します。

GRE IPv6 トンネルの設定

IPv6 ネットワーク上で GRE トンネルを設定するには、次の作業を実行します。GRE トンネルは、IPv6 ネットワーク層上で実行し、IPv6 トンネルの IPv6 パケットおよび IPv6 トンネルの IPv4 パケットを転送するように設定できます。

GRE IPv6トンネルを設定するには、次の手順を実行します。

始める前に

GRE IPv6 トンネルが設定されている場合、IPv6 アドレスは、トンネル送信元およびトンネル宛先に割り当てられます。トンネル インターフェイスは、割り当て済みの IPv4 アドレスまたは IPv6 アドレスを持つことができます（ここでは説明していません）。設定されたトンネル

の両端にあるホストまたはルータは、IPv4 プロトコル スタックと IPv6 プロトコル スタックの両方をサポートしている必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface tunnel** *tunnel-number*
4. **ipv6 address** *ipv6-prefix* / *prefix-length* [**eui-64**]
5. **tunnel source** {*ip-address* | *ipv6-address* | *interface-type interface-number*}
6. **tunnel destination** {*host-name* | *ip-address* | *ipv6-address*}
7. **tunnel mode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre**| **gre multipoint** | **gre ipv6** | **ipip** [**decapsulate-any**] | **iptalk** | **ipv6** | **mpls** | **nos**

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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface tunnel** *tunnel-number* 例： `Device(config)# interface tunnel 0`	トンネルインターフェイスおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 address** *ipv6-prefix* / *prefix-length* [**eui-64**] 例： `Device(config-if)# ipv6 address 3ffe:b00:c18:1::3/127`	インターフェイスに割り当てられている IPv6 ネットワークを指定し、インターフェイスで IPv6 処理をイネーブルにします。
ステップ 5	**tunnel source** {*ip-address* | *ipv6-address* | *interface-type interface-number*} 例： `Device(config-if)# tunnel source ethernet 0`	トンネル インターフェイスの送信元 IPv4 アドレスまたは送信元インターフェイス タイプと番号を指定します。 • インターフェイスが指定されている場合、そのインターフェイスは IPv4 アドレスを使用して設定されている必要があります。

	コマンドまたはアクション	目的
ステップ 6	**tunnel destination** {*host-name* | *ip-address* | *ipv6-address*} 例： `Device(config-if)# tunnel destination 2001:DB8:1111:2222::1/64`	宛先 IPv6 アドレスまたはトンネル インターフェイスのホスト名を指定します。
ステップ 7	**tunnel mode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre**| **gre multipoint** | **gre ipv6** | **ipip** [**decapsulate-any**] | **iptalk** | **ipv6** | **mpls** | **nos** 例： `Device(config-if)# tunnel mode gre ipv6`	GRE IPv6 トンネルを指定します。 （注） **tunnel mode gre ipv6** コマンドは、トンネルのカプセル化プロトコルとして GRE を指定します。

IPv4 GRE トンネルを介した IPv6 の設定例

続くセクションでは、IPv4 GRE トンネルを介した IPv6 の設定方法の例を示します。

例：IS-IS および IPv6 トラフィックを実行する GRE トンネル

次に、ルータ A とルータ B との間で IS-IS および IPv6 トラフィックをともに送出する GRE トンネルを設定する例を示します。

ルータ A の設定

```
Device> enable
Device# configure terminal
Device(config)# ipv6 unicast-routing
Device(config)# clns routing
!
Device(config)# interface tunnel 0
Device(config-if)# no ip address
Device(config-if)# ipv6 address 3ffe:b00:c18:1::3/127
Device(config-if)# ipv6 router isis
Device(config-if)# tunnel source Ethernet 0/0
Device(config-if)# tunnel destination 2001:DB8:1111:2222::1/64
Device(config-if)# tunnel mode gre ipv6
Device(config-if)# exit
!
Device(config)# interface Ethernet0/0
Device(config-if)# ip address 10.0.0.1 255.255.255.0
!
Device(config-if)# router isis
Device(config-if)# net 49.0000.0000.000a.00
```

ルータ B の設定

```
Device> enable
Device# configure terminal
Device(config)# ipv6 unicast-routing
Device(config)# clns routing
```

```
!
Device(config)# interface tunnel 0
Device(config-if)# no ip address
Device(config-if)# ipv6 address 3ffe:b00:c18:1::2/127
Device(config-if)# exit
Device(config)# ipv6 router isis
Device(config-router)# tunnel source Ethernet 0/0
Device(config-router)# tunnel destination 2001:DB8:1111:2222::2/64
Device(config-router)# tunnel mode gre ipv6
Device(config-router)# exit
!
Device(config)# interface Ethernet0/0
Device(config-if)# ip address 10.0.0.2 255.255.255.0
Device(config-if)# exit
!
Device(config)# router isis
Device(config-router)# net 49.0000.0000.000b.00
Device(config-router)# address-family ipv6
Device(config-router-af)# redistribute static
Device(config-router-af)# exit-address-family
```

例：IPv6 トンネルのトンネル宛先アドレス

```
Device> enable
Device# configure terminal
Device(config)# interface Tunnel 0
Device(config-if)# ipv6 address 2001:1:1::1/48
Device(config-if)# tunnel source GigabitEthernet 0/0/0
Device(config-if)# tunnel destination 10.0.0.2
Device(config-if)# tunnel mode gre ipv6
Device(config-if)# exit
!
Device(config)# interface GigabitEthernet0/0/0
Device(config-if)# ip address 10.0.0.1 255.255.255.0
Device(config-if)# exit
!
Device(config)# ipv6 unicast-routing
Device(config)# router isis
Device(config-router)# net 49.0000.0000.000a.00
```

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
この章で使用するコマンドの完全な構文および使用方法の詳細。	*Command Reference (Catalyst 9200 Series Switches)*

IPv4 GRE トンネルを介した IPv6 の機能履歴と情報

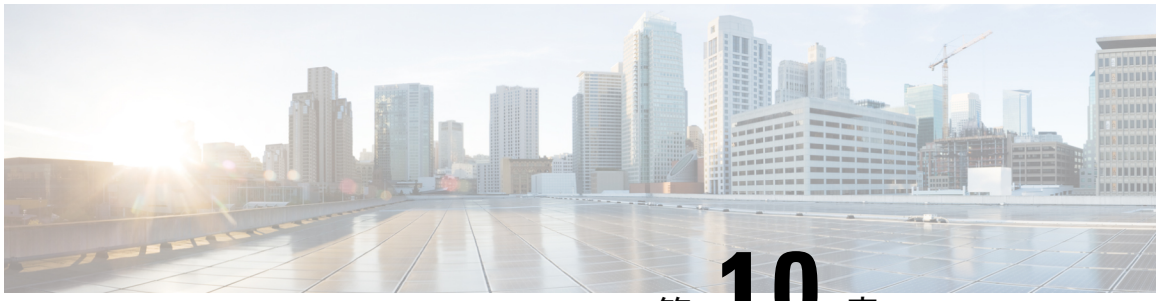
次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

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、https://www.cisco.com/go/cfnに進みます。Cisco.com のアカウントは必要ありません。

表 *11 : IPv4 GRE* トンネルを介する *IPv6* の機能情報

機能名	リリース	機能情報
IPv4 GRE トンネルを介する IPv6		GRE トンネルは、2 つのポイント間のリンクであり、リンクごとに個別のトンネルがあります。これらのトンネルは、特定のパッセンジャまたはトランスポート プロトコルに結合されていませんが、この場合、GRE を使用するパッセンジャ プロトコルとして IPv6 を伝送し、トランスポート プロトコルとして IPv4 または IPv6 を伝送します。



第 10 章

HSRP の設定

HSRP の設定に関する情報

HSRP の概要

HSRP は、デフォルト ゲートウェイ IP アドレスが設定された IEEE 802 LAN 上の IP ホストにファーストホップ冗長性を確保することでネットワークのアベイラビリティを高めるシスコの標準方式です。HSRPを使用すると、特定のルータのアベイラビリティに依存せずIPトラフィックをルーティングできます。また、一連のルータ インターフェイスを組み合わせることで、1台の仮想ルータ、またはLAN上のホストへのデフォルト ゲートウェイのように機能させることができます。ネットワークまたはセグメント上にHSRPを設定すると、仮想MAC（メディア アクセス コントロール）アドレス、および設定されたルータ グループ間で共有されるIPアドレスを使用できるようになりHSRP が設定された複数のルータは、仮想ルータの MAC アドレスおよび IP ネットワーク アドレスを使用できるようになります。仮想ルータは、実際には存在しません。仮想ルータは、相互にバックアップ機能を提供するように設定されている複数のルータの共通のターゲットを表します。1 台のルータがアクティブなルータとして、もう 1 台のルータがスタンバイ ルータとして選択されます。スタンバイ ルータは、指定されたアクティブ ルータが故障した場合に、グループのMACアドレスおよびIPアドレスを制御するルータです。

（注） HSRP グループ内のルータには、ルーテッド ポート、スイッチ仮想インターフェイス（SVI）など、HSRP をサポートする任意のルータ インターフェイスを指定できます。

HSRPは、ネットワーク上のホストからのIPトラフィックに冗長性を提供することで、ネットワークのアベイラビリティを高めます。アクティブ ルータは、ルータ インターフェイスのグループ内でパケットのルーティングを実行するために選択されたルータです。スタンバイ ルータは、アクティブ ルータが故障した場合、または事前に設定した条件が満たされた場合に、ルーティング作業を引き継ぐルータです。

HSRPは、ホストがルータ ディスカバリ プロトコルをサポートしておらず、選択されたルータのリロードや電源故障時に新しいルータに切り替えることができない場合に有効です。HSRPをネットワーク セグメントに設定すると、HSRPは仮想MACアドレスとIPアドレスを1つずつ提供します。このアドレスは、HSRPが動作するルータ インターフェイス グループ内のルータ インターフェイス間で共有できます。プロトコルによってアクティブ ルータとして選択されたルータは、グループのMACアドレス宛てのパケットを受信し、ルーティングします。n台のルータでHSRPが稼働している場合、n+1個のIPアドレスおよびMACアドレスが割り当てられます。

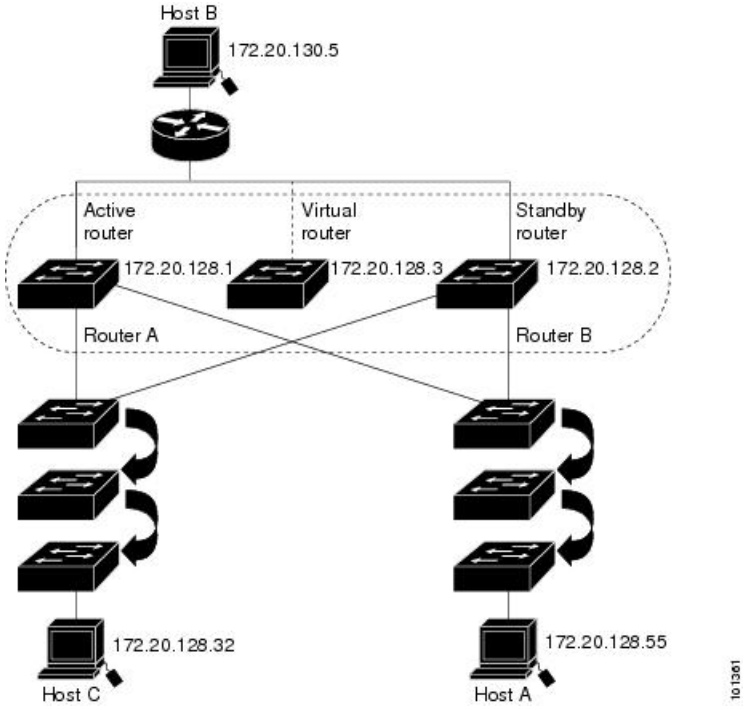
指定されたアクティブ ルータの故障をHSRPが検出すると、選択されているスタンバイ ルータがホットスタンバイ グループのMACアドレスおよびIPアドレスの制御を引き継ぎます。この時点で新しいスタンバイ ルータも選択されます。HSRPが稼働しているデバイスは、マルチキャストUDPベースのhelloパケットを送受信することにより、ルータ障害の検出、アクティブ ルータおよびスタンバイ ルータの指定を行います。インターフェイスにHSRPが設定されている場合、そのインターフェイスではインターネット制御メッセージプロトコル（ICMP）のリダイレクト メッセージが自動的にイネーブルになっています。

レイヤ3で動作するスイッチおよびスイッチ スタック間で複数のホット スタンバイ グループを設定すると、冗長ルータをさらに活用できます。

そのためには、インターフェイスに設定するホットスタンバイ コマンドグループごとにグループ番号を指定します。たとえば、スイッチ1のインターフェイスをアクティブ ルータ、スイッチ2のインターフェイスをスタンバイ ルータとして設定できます。また、スイッチ2の別のインターフェイスをアクティブ ルータ、スイッチ1の別のインターフェイスをスタンバイ ルータとして設定することもできます。

次の図に、HSRP用に設定されたネットワークのセグメントを示します。各ルータには、仮想ルータのMACアドレスおよびIPネットワーク アドレスが設定されています。ルータAのIPアドレスをネットワーク上のホストに設定する代わりに、デフォルト ルータとして仮想ルータのIPアドレスを設定します。ホストCからホストBにパケットが送信される場合、ホストCは仮想ルータのMACアドレスにパケットを送信します。何らかの理由により、ルータAがパケットの転送を停止すると、ルータBが仮想IPアドレスおよび仮想MACアドレスに応答してアクティブ ルータとなり、アクティブ ルータの作業を行います。ホストCは引き続き仮想ルータのIPアドレスを使用し、ホストB宛のパケットをアドレッシングします。ルータBはそのパケットを受信し、ホストBに送信します。ルータBはHSRPの機能を使用し、ルータAが動作を再開するまで、ホストBのセグメント上のユーザと通信する必要があるホストCのセグメント上のユーザに連続的にサービスを提供します。また、ホストAセグメントとホストBの間で、引き続き通常のパケット処理機能を実行します。

図 *10 : HSRP* の一般的な構成



HSRP のバージョン

Cisco IOS XE Fuji 16.9.x 以降のスイッチでサポートされている Hot Standby Router Protocol（HSRP）のバージョンは次のとおりです。

スイッチでは、次の HSRP バージョンがサポートされます。

- HSRPv1：HSRP のバージョン 1（デフォルトのバージョン）。次の機能があります。
  - HSRP グループ番号は 0 ～ 255 まで使用できます。
  - HSRPv1 は 224.0.0.2 のマルチキャスト アドレスを使用して hello パケットを送信しますが、これは Cisco Group Management Protocol（CGMP）の脱退処理と競合します。HSRPv1 と CGMP は相互に排他的なため、同時には使用できません。
- HSRPv2：HSRP のバージョン 2。このバージョンには次の機能があります。
  - HSRPv2 は 224.0.0.102 のマルチキャスト アドレスを使用して hello パケットを送信します。HSRPv2 と CGMP 脱退処理は相互に排他的ではありません。同時に使用できます。
  - HSRPv2 のパケット形式は、HSRPv1 とは異なります。

HSRPv1 を実行しているスイッチは、ルータの送信元 MAC アドレスが仮想 MAC アドレスのため、hello パケットを送信した物理的なルータを特定できません。

HSRPv2 のパケット形式は、HSRPv1 とは異なります。HSRPv2 パケットは、パケットを送信した物理ルータの MAC アドレスを格納できる 6 バイトの識別子フィールドを持った、Type Length Value（TLV）形式を使用します。

HSRPv1 を実行しているインターフェイスが HSRPv2 パケットを取得した場合、このタイプ フィールドは無視されます。

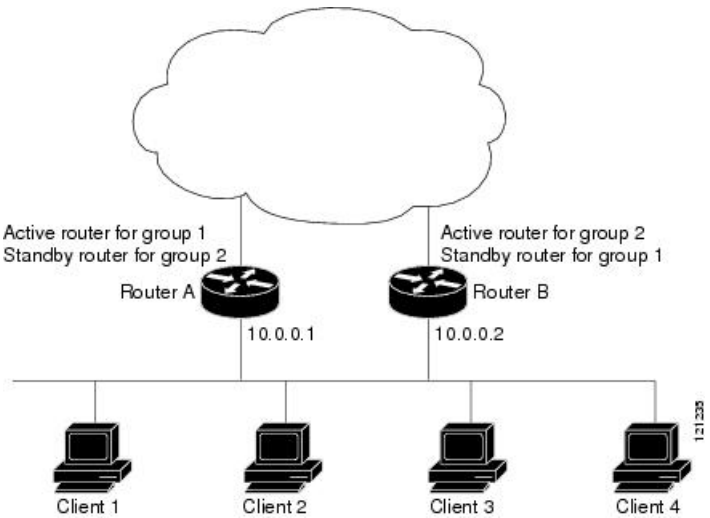
MHSRP

スイッチは、Multiple HSRP（MHSRP）をサポートします。MHSRP は HSRP の拡張版で、複数の HSRP グループ間でのロードシェアリングが可能です。ホストネットワークからサーバネットワークまで、ロード バランシングを実現して複数のスタンバイ グループ（およびパス）を使用するために、MHSRP を設定できます。

下の図では、半分のクライアントがルータ A に設定されており、もう半分はルータ B に設定されています。ルータ A およびルータ B の設定により、合計 2 つの HSRP グループが確立されています。グループ 1 では、ルータ A に最高のプライオリティが割り当てられているので、ルータ A がデフォルトのアクティブ ルータになり、ルータ B がスタンバイ ルータとなります。グループ 2 では、ルータ B に最も高いプライオリティが割り当てられているため、ルータ B がデフォルトのアクティブ ルータであり、ルータ A がスタンバイ ルータです。通常の運用では、2 つのルータが IP トラフィック負荷を分散します。いずれかのルータが使用できなくなると、もう一方のルータがアクティブになり、使用できないルータのパケット転送機能を引き継ぎます。

（注） MHSRP では、ルータに障害が発生して正常に戻った場合にプリエンプションによりロードシェアリングを復元するために、**standby preempt** インターフェイス コンフィギュレーション コマンドを HSRP インターフェイスで入力する必要があります。

図 ***11 : MHSRP*** ロード シェアリング



HSRP およびスイッチ スタック

HSRP の hello メッセージは、アクティブなスイッチで生成されます。アクティブなスイッチの HSRP に障害が発生すると、HSRP アクティブ状態のフラッピングが生じることがあります。これは、新規のアクティブなスイッチが選択および初期化されている間に HSRP hello メッセージが生成されず、アクティブなスイッチが故障した後でないとスタンバイルータがアクティブにならない可能性があるためです。

IPv6 の HSRP の設定

を実行中のスイッチは、IPv6 の Hot Standby Router Protocol（HSRP）をサポートします。HSRP は、任意の単一のルータのアベイラビリティに依存せず、ルーティング IPv6 トラフィックにルーティング冗長性を提供します。IPv6 ホストは、IPv6 ネイバー探索ルータのアドバタイズメントメッセージによって使用可能なルータを学習します。これらのメッセージは定期的にマルチキャストされるか、ホストにより送信請求されます。

HSRP IPv6 グループには、HSRP グループ番号に基づく仮想 MAC アドレス、およびデフォルトで HSRP 仮想 MAC アドレスに基づく HSRP の仮想 IPv6 リンクローカル アドレスがあります。

HSRP グループがアクティブな場合、定期的なメッセージが HSRP 仮想 IPv6 リンクローカル アドレスに送信されます。グループがアクティブ ステートでなくなった場合、これらのメッセージは最後のメッセージが送信されたあとで停止します。

（注） IPv6 の HSRP を設定する場合、インターフェイス上で HSRP version 2（HSRPv2）をイネーブルにする必要があります。

HSRP IPv6 仮想 MAC アドレスの範囲

HSRP IPv6 では、次に示すように、HSRP for IP とは異なる仮想 MAC アドレス ブロックを使用します。

0005.73A0.0000 through 0005.73A0.0FFF（4096 のアドレス）

HSRP IPv6 UDP ポート番号

HSRP IPv6 には、ポート番号 2029 が割り当てられています。

HSRP の設定方法

HSRP のデフォルト設定

表 *12 : HSRP* のデフォルト設定

機能	デフォルト設定
HSRP バージョン	バージョン 1
HSRP グループ	未設定
スタンバイ グループ番号	0
スタンバイ MAC アドレス	0000.0c07.acXX に指定されたシステム。XX は、HSRP グループ番号
スタンバイ プライオリティ	100
スタンバイ遅延	0（遅延なし）
スタンバイでのインターフェイス プライオリティの追跡	10
スタンバイ hello 時間	3 秒
スタンバイ ホールドタイム	10 秒

HSRP 設定時の注意事項

- HSRPv2 および HSRPv1 は相互に排他的です。HSRPv2 は、同じインターフェイス上で HSRPv1 と一緒には動作しません（その逆も同様）。
- 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。
  - ルーテッドポート：インターフェイス コンフィギュレーション モードで **no switchport** コマンドを入力することにより、レイヤ 3 ポートとして設定された物理ポート。
  - SVI：グローバル コンフィギュレーション モードで **interface vlan** *vlan_id* を使用して作成された VLAN インターフェイス。デフォルトではレイヤ 3 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：グローバル コンフィギュレーション モードで **interface port-channel** *port-channel-number* を使用し、イーサネット インターフェイスをチャネルグループにバインドして作成されたポートチャネル論理インターフェイス。

- すべてのレイヤ 3 インターフェイスに IP アドレスを割り当てる必要があります。
- HSRP のミリ秒タイマーはサポートされません。

HSRP のイネーブル化

standby ip インターフェイス コンフィギュレーション コマンドは、設定されているインターフェイスで HSRP をアクティブにします。IP アドレスを指定した場合は、IP アドレスがホットスタンバイ グループの指定アドレスとして使用されます。IP アドレスを指定しなかった場合は、スタンバイ機能によってアドレスが学習されます。指定アドレスを使用し、LAN 上に少なくとも 1 つのレイヤ 3 ポートを設定する必要があります。IP アドレスを設定すると、常に、現在使用されている別の指定アドレスが、設定した IP アドレスに変更されます。

standby ip コマンドがインターフェイス上で有効にされており、プロキシ ARP が有効な場合、インターフェイスのホットスタンバイ状態がアクティブになると、プロキシ ARP 要求に対する応答は、ホットスタンバイグループの MAC アドレスを使用して実行されます。インターフェイスが別のステートの場合、プロキシ ARP の応答は抑制されます。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **standby version** { **1** | **2** }
4. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
5. **end**
6. **show standby** [*interface-id* [*group*]]
7. **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	**configure terminal** 例： `Switch(config)# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	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、HSRP をイネーブルにするレイヤ 3 インターフェイスを入力します。
ステップ 3	**standby version** { **1** | **2** } 例： `Switch(config-if)# standby version 1`	（任意）インターフェイスに HSRP バージョンを設定します。 • 1：HSRPv1 を選択します。 • 2：HSRPv2 を選択します。

	コマンドまたはアクション	目的
		このコマンドを入力しない場合、またはキーワードを指定しない場合、インターフェイスはデフォルトの HSRP バージョンである HSRPv1 を実行します。
ステップ 4	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] 例： `Switch(config-if)# standby 1 ip`	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成（またはイネーブルに）します。 • （任意）group-number：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。指定できる範囲は 0 ～ 255 です。デフォルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • （1 つのインターフェイスで必須、それ以外は任意）ip-address：ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 • （任意）**secondary**：IP アドレスがセカンダリ ホット スタンバイ ルータ インターフェイスであることを指定します。ルータがセカンダリ ルータとスタンバイ ルータのいずれにも指定されず、かつプライオリティも設定されていない場合は、プライマリ IP アドレスが比較され、IP アドレスが大きいルータがアクティブ ルータ、IP アドレスが 2 番めに大きいルータがスタンバイ ルータになります。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります
ステップ 6	**show standby** [*interface-id* [*group*]] 例： `Switch # show standby`	スタンバイ グループの設定を確認します。
ステップ 7	**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
	`Switch# copy running-config startup-config`	

IPv6 用 HSRP グループの動作のイネーブル化と確認

この作業では、**standby ipv6** コマンドを入力すると、リンクローカルプレフィクスからリンクローカルアドレスが生成され、変更後の EUI-64 形式のインターフェイス識別子が生成されます。EUI-64 インターフェイス識別子は、関連する HSRP 仮想 MAC アドレスからこの形式で作成されます。

リンクローカル アドレスは、リンクローカル プレフィックス FE80::/10（1111 1110 10）と変更された EUI-64 形式のインターフェイス識別子を使用するすべてのインターフェイスを自動的に設定できる IPv6 ユニキャスト アドレスです。リンクローカル アドレスは、ステートレス自動設定プロセスで使用されます。ローカル リンク上のノードは、リンクローカル アドレスを使用して通信できます。ノードの通信にサイトローカルアドレスまたはグローバルに一意のアドレスは不要です。

IPv6 では、リンク上のデバイスが RA メッセージでサイトローカル プレフィックスやグローバル プレフィックス、およびリンクのデフォルト デバイスとして動作することをアドバタイズします。RA メッセージは、定期的に送信される場合と、システム始動時にホストから送信されるルータ送信要求メッセージに対する応答として送信される場合があります。

リンク上のノードは、RA メッセージに含まれるプレフィックス（64 ビット）にそのインターフェイス ID（64 ビット）を付加して、自動的にサイトローカルアドレスとグローバル IPv6 アドレスを設定できます。ノードによって設定された 128 ビットの IPv6 アドレスは、重複アドレス検出の対象となり、リンク上での一意性が確保されます。RA メッセージでアドバタイズされたプレフィックスがグローバルに一意である場合、ノードによって設定された IPv6 アドレスもグローバルに一意になります。ICMP パケット ヘッダーのタイプ フィールドの値が 133 であるルータ送信要求メッセージは、システム始動時にホストによって送信されるため、ホストは次のスケジュールされた RA メッセージを待機することなくすぐに自動設定できます。

IPv6 の HSRP グループを有効にして確認するには、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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。 • HSRP for IPv6 を機能させるには、**ipv6 unicast-routing** コマンドを有効にする必要があります。
ステップ 4	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/0/0`	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 5	**standby** [*group-number*] **ipv6** {*link-local-address* | **autoconfig**} 例： `Device(config-if)# standby 1 ipv6 autoconfig`	IPv6 の HSRP をアクティブにします。
ステップ 6	**standby** [*group-number*] **preempt** [**delay minimum** *seconds* | **reload** *seconds* | **sync** *seconds*] 例： `Device(config-if)# standby 1 preempt`	HSRP プリエンプションとプリエンプション遅延を設定します。
ステップ 7	**standby** [*group-number*] **priority** *priority* 例： `Device(config-if)# standby 1 priority 110`	HSRP プライオリティを設定します。
ステップ 8	**exit** 例： `Device(config-if)# exit`	デバイスを特権 EXEC モードに戻します。
ステップ 9	**show standby** [*type number* [*group*]] [**all** | **brief**] 例： `Device# show standby`	HSRP 情報を表示します。
ステップ 10	**show ipv6 interface** [**brief**] [*interface-type interface-number*] [**prefix**] 例： `Device# show ipv6 interface GigabitEthernet 0/0/0`	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

HSRP のプライオリティの設定

standby priority, **standby preempt**、および **standby track** インターフェイス コンフィギュレーション コマンドはいずれも、アクティブ ルータとスタンバイ ルータを検索するための特性、および新しいアクティブ ルータが処理を引き継いだ場合の動作を設定するために使用できます。

HSRP プライオリティを設定する場合の注意事項は、次のとおりです。

- プライオリティを割り当てておくと、アクティブ ルータおよびスタンバイ ルータを選択できます。プリエンプションがイネーブルの場合は、プライオリティが最高のルータがアクティブルータになります。プライオリティが等しい場合は、現在アクティブなルータに変更はありません。
- 最大の値（1 ～ 255）が、最高のプライオリティ（アクティブ ルータになる確率が最も高い）を表します。
- プライオリティ、プリエンプト、またはその両方を設定するときは、少なくとも 1 つのキーワード（**priority**、**preempt**、または両方）を指定する必要があります。
- インターフェイスが **standby track** コマンドによって設定されている場合、ルータ上の別のインターフェイスがダウンすると、デバイスのプライオリティが動的に変更されることもあります。
- **standby track** インターフェイス コンフィギュレーション コマンドを実行すると、ルータのホットスタンバイ プライオリティとインターフェイスのアベイラビリティが関連付けられます。この機能は、HSRP 用に設定されていないインターフェイスを追跡する場合に有効です。追跡対象のインターフェイスが故障すると、トラッキングが設定されているデバイスのホットスタンバイ プライオリティが 10 減少します。追跡対象でないインターフェイスの場合は、そのステートが変わっても、設定済みデバイスのホットスタンバイ プライオリティは変わりません。ホットスタンバイ用に設定されたインターフェイスごとに、追跡するインターフェイスのリストを個別に設定できます。
- **standby track** *interface-priority* インターフェイス コンフィギュレーション コマンドを実行すると、追跡対象のインターフェイスがダウンした場合のホットスタンバイ優先順位の減少幅を指定できます。インターフェイスが稼働状態に戻ると、プライオリティは同じ分だけ増加します。
- *interface-priority* 値が設定されている場合に、複数の追跡対象インターフェイスがダウンすると、設定済みプライオリティの減少幅が累積されます。プライオリティ値が設定されていない追跡対象インターフェイスが故障した場合、デフォルトの減少幅は 10 です。この値は累積されません。
- インターフェイスに対してルーティングを最初にイネーブルにした時点で、完全なルーティングテーブルは存在しません。このインターフェイスがプリエンプトに設定されている場合はアクティブ ルータになりますが、十分なルーティング処理はできません。この問題を解決するには、ルータがルーティングテーブルを更新できるように遅延時間を設定します。

インターフェイスにHSRPプライオリティ特性を設定するには、特権EXECモードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **standby** ［*group-number*］ **priority***priority*
4. **standby**［*group-number*］**preempt**［**delay**［**minimum***seconds*］［**reload***seconds*］［**sync***seconds*］］
5. **standby** ［*group-number*］ **track** *type number*［*interface-priority*］
6. **end**
7. **show running-config**
8. **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	**configure terminal** 例： `Switch # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	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、プライオリティを設定する HSRP インターフェイスを入力します。
ステップ 3	**standby** ［*group-number*］ **priority***priority* 例： `Switch(config-if)# standby 120 priority 50`	アクティブ ルータを選択するときに使用される **priority** 値を設定します。指定できる範囲は 1 ～ 255 です。デフォルト プライオリティは 100 です。最大の値が、最高のプライオリティを表します。 • （任意）group-number：コマンドが適用されるグループ番号です。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 4	**standby**［*group-number*］**preempt**［**delay**［**minimum***seconds*］［**reload***seconds*］［**sync***seconds*］］ 例： `Switch(config-if)# standby 1 preempt delay 300`	ルータを **preempt** に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとなります。 • （任意）group-number：コマンドが適用されるグループ番号です。 • （任意）**delay minimum**：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定でき

	コマンドまたはアクション	目的
		る範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 • （任意）**delay reload**：ローカル ルータがリロードの後アクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600（1 時間）で、デフォルトは 0 です（リロードの後、引き継ぐ前の遅延はありません）。 • （任意）**delay sync**：IP 冗長性クライアントが応答できるように（ok または wait 応答）、ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 5	**standby** ［*group-number*］ **track** *type number* ［*interface-priority*］ 例： `Switch(config-if)# standby track interface gigabitethernet1/1/1`	他のインターフェイスを追跡するようにインターフェイスを設定します。この設定により、他のインターフェイスの 1 つがダウンした場合は、そのデバイスのホットスタンバイ プライオリティが減少します。 • （任意）group-number：コマンドが適用されるグループ番号です。 • type：追跡対象のインターフェイス タイプを（インターフェイス番号とともに）入力します。 • number：追跡対象のインターフェイス番号を（インターフェイス タイプとともに）入力します。 • （任意）interface-priority：インターフェイスがダウンした場合、または稼働状態に戻った場合に、ルータのホットスタンバイ プライオリティを減少または増加させる幅を入力します。デフォルト値は 10 です。
ステップ 6	**end** 例：	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
	`Switch(config-if)# end`	
ステップ 7	**show running-config**	スタンバイ グループの設定を確認します。
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。

MHSRP の設定

MHSRP およびロード バランシングをイネーブルにするには、MHSRP の項の *MHSRP* ロード シェアリングの図に示したように、グループのアクティブ ルータとして 2 つのルータを設定し、スタンバイ ルータとして仮想ルータを設定します。ルータに障害が発生して正常に戻った場合、プリエンプションを発生させてロードバランシングを復元するために、**standby preempt** インターフェイス コンフィギュレーション コマンドをそれぞれの HSRP インターフェイスで入力する必要があります。

ルータ A はグループ 1 のアクティブ ルータとして、ルータ B はグループ 2 のアクティブ ルータとして設定されています。ルータ A の HSRP インターフェイスの IP アドレスは 10.0.0.1、グループ 1 のスタンバイ プライオリティは 110（デフォルトは 100）です。ルータ B の HSRP インターフェイスの IP アドレスは 10.0.0.2、グループ 2 のスタンバイ プライオリティは 110 です。

グループ 1 は仮想 IP アドレス 10.0.0.3 を使用し、グループ 2 は仮想 IP アドレス 10.0.0.4 を使用します。

ルータ A の設定

手順の概要

1. **configure terminal**
2. **interface** *type number*
3. **no switchport**
4. **ip address** *ip-address mask*
5. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
6. **standby** [*group-number*] **priority** *priority*
7. **standby** [*group-number*] **preempt** [**delay** [**minimum** *seconds*] [**reload** *seconds*] [**sync** *seconds*]]
8. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
9. **standby** [*group-number*] **preempt** [**delay** [**minimum** *seconds*] [**reload** *seconds*] [**sync** *seconds*]]
10. **end**
11. **show running-config**
12. **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	**configure terminal** 例： `Switch # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *type number* 例： `Switch (config)# interface gigabitethernet1/0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no switchport** 例： `Switch (config)# no switchport`	レイヤ 2 モードになっているインターフェイスを、レイヤ 3 設定用にレイヤ 3 モードに切り替えます。
ステップ 4	**ip address** *ip-address mask* 例： `Switch (config-if)# ip address 10.0.0.1 255.255.255.0`	インターフェイスの IP アドレスを指定します。
ステップ 5	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] 例： `Switch (config-if)# standby 1 ip 10.0.0.3`	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成します。 • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。指定できる範囲は 0 ～ 255 です。デフォルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • （1 つのインターフェイスで必須、それ以外は任意）*ip-address*：ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 • （任意）**secondary**：IP アドレスがセカンダリ ホット スタンバイ ルータ インターフェイスであることを指定します。ルータがセカンダリ ルータとスタンバイ ルータのいずれにも指定されず、かつプライオリティも設定されていない場合は、プライマリ IP アドレスが比較され、IP アドレスが大きいルータがアクティブ ルータ、IP アドレスが 2 番めに大きいルータがスタンバイ ルータになります。

	コマンドまたはアクション	目的
ステップ 6	**standby** ［*group-number*］ **priority** *priority* 例： `Switch(config-if)# standby 1 priority 110`	アクティブ ルータを選択するときに使用される **priority** 値を設定します。指定できる範囲は 1 ～ 255 です。デフォルト プライオリティは 100 です。最大の値が、最高のプライオリティを表します。 • （任意）*group-number*：コマンドが適用されるグループ番号です。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 7	**standby** ［*group-number*］ **preempt** ［**delay** ［**minimum** *seconds*］ ［**reload** *seconds*］ ［**sync** *seconds*］］ 例： `Switch(config-if)# standby 1 preempt delay 300`	ルータを **preempt** に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとなります。 • （任意）group-number：コマンドが適用されるグループ番号です。 • （任意）**delay minimum**：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 • （任意）**delay reload**：ローカル ルータがリロードの後アクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600（1 時間）で、デフォルトは 0 です（リロードの後、引き継ぐ前の遅延はありません） 。 • （任意）**delay sync**：IP 冗長性クライアントが応答できるように（ok または wait 応答）、ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

	コマンドまたはアクション	目的
ステップ 8	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] 例： `Switch (config-if)# standby 2 ip 10.0.0.4`	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成します。 • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。指定できる範囲は 0 ～ 255 です。デフォルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • （1 つのインターフェイスで必須、それ以外は任意）*ip-address*：ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 • （任意）**secondary**：IP アドレスがセカンダリ ホット スタンバイ ルータ インターフェイスであることを指定します。ルータがセカンダリ ルータとスタンバイ ルータのいずれにも指定されず、かつプライオリティも設定されていない場合は、プライマリ IP アドレスが比較され、IP アドレスが大きいルータがアクティブ ルータ、IP アドレスが 2 番めに大きいルータがスタンバイ ルータになります。
ステップ 9	**standby** [*group-number*] **preempt** [**delay** [**minimum** *seconds*] [**reload** *seconds*] [**sync** *seconds*]] 例： `Switch(config-if)# standby 2 preempt delay 300`	ルータを **preempt** に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとなります。 • （任意）group-number：コマンドが適用されるグループ番号です。 • （任意）**delay minimum**：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 • （任意）**delay reload**：ローカル ルータがリロードの後アクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600（1 時間）で、デフォルトは 0 です（リロードの後、引き継ぐ前の遅延はありません）。

	コマンドまたはアクション	目的
		• （任意）**delay sync**：IP 冗長性クライアントが応答できるように（okまたはwait応答）、ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は0～3600秒（1時間）で、デフォルトは0です（引き継ぐ前の遅延はありません）。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 10	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show running-config**	スタンバイ グループの設定を確認します。
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。

ルータ B の設定

手順の概要

1. **configure terminal**
2. **interface** *type number*
3. **no switchport**
4. **ip address** *ip-address mask*
5. **standby** ［*group-number*］ **ip** ［*ip-address* ［**secondary**］］
6. **standby** ［*group-number*］ **priority** *priority*
7. **standby** ［*group-number*］ **preempt** ［**delay** ［**minimum** *seconds*］ ［**reload** *seconds*］ ［**sync** *seconds*］］
8. **standby** ［*group-number*］ **ip** ［*ip-address* ［**secondary**］］
9. **standby** ［*group-number*］ **preempt** ［**delay** ［**minimum** *seconds*］ ［**reload** *seconds*］ ［**sync** *seconds*］］
10. **end**
11. **show running-config**
12. **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	**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
	`Switch # configure terminal`	
ステップ 2	**interface** *type number* 例： `Switch (config)# interface gigabitethernet1/0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no switchport** 例： `Switch (config)# no switchport`	レイヤ 2 モードになっているインターフェイスを、レイヤ 3 設定用にレイヤ 3 モードに切り替えます。
ステップ 4	**ip address** *ip-address mask* 例： `Switch (config-if)# ip address 10.0.0.2 255.255.255.0`	インターフェイスの IP アドレスを指定します。
ステップ 5	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] 例： `Switch (config-if)# standby 1 ip 10.0.0.3`	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成します。 • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。指定できる範囲は 0 ～ 255 です。デフォルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • （1 つのインターフェイスで必須、それ以外は任意）*ip-address*：ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 • （任意）**secondary**：IP アドレスがセカンダリ ホット スタンバイ ルータ インターフェイスであることを指定します。ルータがセカンダリ ルータとスタンバイ ルータのいずれにも指定されず、かつプライオリティも設定されていない場合は、プライマリ IP アドレスが比較され、IP アドレスが大きいルータがアクティブ ルータ、IP アドレスが 2 番めに大きいルータがスタンバイ ルータになります。
ステップ 6	**standby** ［*group-number*］ **priority** *priority* 例：	アクティブ ルータを選択するときに使用される **priority** 値を設定します。指定できる範囲は 1 ～

	コマンドまたはアクション	目的
	`Switch(config-if)# standby 2 priority 110`	255 です。デフォルト プライオリティは 100 です。最大の値が、最高のプライオリティを表します。 • （任意）*group-number*：コマンドが適用されるグループ番号です。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 7	**standby** ［*group-number*］ **preempt** ［**delay** ［**minimum** *seconds*］ ［**reload** *seconds*］ ［**sync** *seconds*］］ 例： `Switch(config-if)# standby 1 preempt delay 300`	ルータを **preempt** に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとなります。 • （任意）group-number：コマンドが適用されるグループ番号です。 • （任意）**delay minimum**：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 • （任意）**delay reload**：ローカル ルータがリロードの後アクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600（1 時間）で、デフォルトは 0 です（リロードの後、引き継ぐ前の遅延はありません）。 • （任意）**delay sync**：IP 冗長性クライアントが応答できるように（ok または wait 応答）、ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 8	**standby** ［*group-number*］ **ip** ［*ip-address* ［**secondary**］］ 例： `Switch (config-if)# standby 2 ip 10.0.0.4`	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成します。 • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。指定できる範囲は 0 ～ 255 です。デフォ

	コマンドまたはアクション	目的
		ルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • （1 つのインターフェイスで必須、それ以外は任意）*ip-address*：ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 • （任意）**secondary**：IP アドレスがセカンダリ ホット スタンバイ ルータ インターフェイスであることを指定します。ルータがセカンダリ ルータとスタンバイ ルータのいずれにも指定されず、かつプライオリティも設定されていない場合は、プライマリ IP アドレスが比較され、IP アドレスが大きいルータがアクティブ ルータ、IP アドレスが 2 番めに大きいルータがスタンバイ ルータになります。
ステップ 9	**standby** ［*group-number*］ **preempt** ［**delay** ［**minimum** *seconds*］ ［**reload** *seconds*］ ［**sync** *seconds*］］ 例： `Switch(config-if)# standby 2 preempt delay 300`	ルータを **preempt** に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとなります。 • （任意）group-number：コマンドが適用されるグループ番号です。 • （任意）**delay minimum**：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 • （任意）**delay reload**：ローカル ルータがリロードの後アクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600（1 時間）で、デフォルトは 0 です（リロードの後、引き継ぐ前の遅延はありません）。 • （任意）**delay sync**：IP 冗長性クライアントが応答できるように（ok または wait 応答）、ローカル ルータがアクティブ ルータの役割を引き

	コマンドまたはアクション	目的
		継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は0～3600秒（1時間）で、デフォルトは0です（引き継ぐ前の遅延はありません）。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 10	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show running-config**	スタンバイ グループの設定を確認します。
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。

HSRP 認証およびタイマーの設定

HSRP認証ストリングを設定したり、helloタイムインターバルやホールドタイムを変更することもできます。

これらの属性を設定する場合の注意事項は次のとおりです。

- 認証ストリングはすべてのHSRPメッセージで暗号化されずに送信されます。相互運用できるように、接続されたすべてのルータおよびアクセスサーバに同じ認証ストリングを設定する必要があります。認証ストリングが一致しないと、HSRPによって設定された他のルータから、指定されたホットスタンバイ IP アドレスおよびタイマー値を学習できません。
- スタンバイ タイマー値が設定されていないルータまたはアクセス サーバは、アクティブ ルータまたはスタンバイ ルータからタイマー値を学習できます。アクティブ ルータに設定されたタイマーは、常に他のタイマー設定よりも優先されます。
- ホットスタンバイ グループのすべてのルータで、同じタイマー値を使用する必要があります。通常、*holdtime* は *hellotime* の 3 倍以上です。

インターフェイスにHSRPの認証とタイマーを設定するには、特権EXECモードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **standby** ［*group-number*］ **authentication** *string*
4. **standby** ［*group-number*］ **timers** *hellotime holdtime*
5. **end**

6. **show running-config**
7. **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	**configure terminal** 例： `Switch # configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(config) # interface gigabitethernet1/0/1`	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、プライオリティを設定する HSRP インターフェイスを入力します。
ステップ 3	**standby** [*group-number*] **authentication** *string* 例： `Switch(config-if) # standby 1 authentication word`	（任意）**authentication** *string*：すべての HSRP メッセージで伝達されるストリングを入力します。認証ストリングには 8 文字までを指定できます。デフォルトのストリングは **cisco** です。 （任意）*group-number*：コマンドが適用されるグループ番号です。
ステップ 4	**standby** [*group-number*] **timers** *hellotime holdtime* 例： `Switch(config-if) # standby 1 timers 5 15`	（任意）helloパケット間隔、およびアクティブ ルータのダウンを他のルータが宣言するまでの時間を設定します。 • *group-number*：コマンドが適用されるグループ番号です。 •（任意）*hellotime*：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 • *holdtime*：ローカル ルータがリロードの後アクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600（1 時間）で、デフォルトは 0 です（リロードの後、引き継ぐ前の遅延はありません）。
ステップ 5	**end** 例： `Switch(config-if) # 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 6	**show running-config**	スタンバイ グループの設定を確認します。
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。

ICMP リダイレクト メッセージの HSRP サポートのイネーブル化

HSRP が設定されたインターフェイスでは、ICMP リダイレクト メッセージが自動的にイネーブルになります。ICMP は、エラーをレポートするためのメッセージ パケットや IP 処理に関連する他の情報を提供する、ネットワーク層インターネット プロトコルです。ICMP には、ホストへのエラーパケットの方向付けや送信などの診断機能があります。この機能は、HSRP を介した発信 ICMP リダイレクト メッセージをフィルタリングします。HSRP では、ネクストホップ IP アドレスが HSRP 仮想 IP アドレスに変更される可能性があります。詳細については、『Cisco IOS IP Configuration Guide, Release 12.4』を参照してください。

HSRP グループおよびクラスタリングの設定

デバイスが HSRP スタンバイ ルーティングに参加し、クラスタリングがイネーブルの場合は、同じスタンバイ グループを使用して、コマンド スイッチの冗長性および HSRP の冗長性を確保できます。同じ HSRP スタンバイ グループをイネーブルにし、コマンドスイッチおよびルーティングの冗長性を確保するには、**cluster standby-group** *HSRP-group-name* [**routing-redundancy**] 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。**routing-redundancy** キーワードを指定せずに同じ HSRP スタンバイ グループ名でクラスタを作成すると、そのグループに対する HSRP スタンバイ ルーティングはディセーブルになります。

HSRP の確認

HSRP コンフィギュレーションの確認

HSRP 設定を表示するには、次の特権 EXEC モードで次のコマンドを使用します。

show standby ［*interface-id*［*group*］］［**brief**］［**detail**］

スイッチ全体、特定のインターフェイス、HSRP グループ、またはインターフェイスの HSRP グループに関する HSRP 情報を表示できます。HSRP 情報の概要または詳細のいずれを表示するかを指定することもできます。デフォルトの表示は **detail** です。多数の HSRP グループがある場合に、修飾子を指定しないで **show standby** コマンドを使用すると、正確に表示されないことがあります。

例

```
Switch #show standby
VLAN1 - Group 1
```

```
Local state is Standby, priority 105, may preempt
Hellotime 3 holdtime 10
Next hello sent in 00:00:02.182
Hot standby IP address is 172.20.128.3 configured
Active router is 172.20.128.1 expires in 00:00:09
Standby router is local
Standby virtual mac address is 0000.0c07.ac01
Name is bbb

VLAN1 - Group 100
Local state is Standby, priority 105, may preempt
Hellotime 3 holdtime 10
Next hello sent in 00:00:02.262
Hot standby IP address is 172.20.138.51 configured
Active router is 172.20.128.1 expires in 00:00:09
Active router is local
Standby router is unknown expired
Standby virtual mac address is 0000.0c07.ac64
Name is test
```

HSRP の設定例

HSRP のイネーブル化：例

次に、インターフェイスのグループ 1 で HSRP をアクティブにする例を示します。ホットスタンバイ グループで使用される IP アドレスは、HSRP を使用して学習されます。

（注） これは、HSRPをイネーブルにするために必要な最小限の手順です。その他の設定は任意です。

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip
Switch(config-if)# end
Switch # show standby
```

例：HSRP グループの設定と確認

次に、デバイス 1 とデバイス 2 で構成される IPv6 用 HSRP グループの設定および確認の例を示します。デバイスの設定を確認するため、各デバイスに対して **show standby** コマンドが発行されます。

デバイス 1 の設定

```
interface FastEthernet0/0.100
description DATA VLAN for PCs
encapsulation dot1Q 100
ipv6 address 2001:DB8:CAFE:2100::BAD1:1010/64
standby version 2
```

```
standby 101 priority 120
standby 101 preempt delay minimum 30
standby 101 authentication ese
standby 101 track Serial0/1/0.17 90
standby 201 ipv6 autoconfig
standby 201 priority 120
standby 201 preempt delay minimum 30
standby 201 authentication ese
standby 201 track Serial0/1/0.17 90
Device1# show standby
FastEthernet0/0.100 - Group 101 (version 2)
State is Active
2 state changes, last state change 5w5d
Active virtual MAC address is 0000.0c9f.f065
Local virtual MAC address is 0000.0c9f.f065 (v2 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 2.296 secs
Authentication text "ese"
Preemption enabled, delay min 30 secs
Active router is local
Priority 120 (configured 120)
Track interface Serial0/1/0.17 state Up decrement 90
IP redundancy name is "hsrp-Fa0/0.100-101" (default)
FastEthernet0/0.100 - Group 201 (version 2)
State is Active
2 state changes, last state change 5w5d
Virtual IP address is FE80::5:73FF:FEA0:C9
Active virtual MAC address is 0005.73a0.00c9
Local virtual MAC address is 0005.73a0.00c9 (v2 IPv6 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 2.428 secs
Authentication text "ese"
Preemption enabled, delay min 30 secs
Active router is local
Standby router is FE80::20F:8FFF:FE37:3B70, priority 100 (expires in 7.856 sec)
Priority 120 (configured 120)
Track interface Serial0/1/0.17 state Up decrement 90
IP redundancy name is "hsrp-Fa0/0.100-201" (default)
```

デバイス 2 の設定

```
interface FastEthernet0/0.100
description DATA VLAN for Computers
encapsulation dot1Q 100
ipv6 address 2001:DB8:CAFE:2100::BAD1:1020/64
standby version 2
standby 101 preempt
standby 101 authentication ese
standby 201 ipv6 autoconfig
standby 201 preempt
standby 201 authentication ese
Device2# show standby
FastEthernet0/0.100 - Group 101 (version 2)
State is Standby
7 state changes, last state change 5w5d
Active virtual MAC address is 0000.0c9f.f065
Local virtual MAC address is 0000.0c9f.f065 (v2 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.936 secs
Authentication text "ese"
Preemption enabled
MAC address is 0012.7fc6.8f0c
Standby router is local
Priority 100 (default 100)
IP redundancy name is "hsrp-Fa0/0.100-101" (default)
```

```
FastEthernet0/0.100 - Group 201 (version 2)
State is Standby
7 state changes, last state change 5w5d
Virtual IP address is FE80::5:73FF:FEA0:C9
Active virtual MAC address is 0005.73a0.00c9
Local virtual MAC address is 0005.73a0.00c9 (v2 IPv6 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.936 secs
Authentication text "ese"
Preemption enabled
Active router is FE80::212:7FFF:FEC6:8F0C, priority 120 (expires in 7.548 sec)
MAC address is 0012.7fc6.8f0c
Standby router is local
Priority 100 (default 100)
IP redundancy name is "hsrp-Fa0/0.100-201" (default)
```

HSRP のプライオリティの設定：例

次に、ポートをアクティブにして、IP アドレスおよびプライオリティ 120（デフォルト値よりも高いプライオリティ）を設定して、アクティブ ルータになるまで 300 秒（5 分間）待機する例を示します。

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby ip 172.20.128.3
Switch(config-if)# standby priority 120 preempt delay 300
Switch(config-if)# end
Switch # show standby
```

MHSRP の設定：例

次に、*MHSRP* ロード シェアリングの図で示した MHSRP 設定をイネーブルにする例を示します。

ルータ A の設定

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.0.0.1 255.255.255.0
Switch(config-if)# standby ip 10.0.0.3
Switch(config-if)# standby 1 priority 110
Switch(config-if)#  standby 1 preempt
Switch(config-if)# standby 2 ip 10.0.0.4
Switch(config-if)#  standby 2 preempt
Switch(config-if)# end
```

ルータ B の設定

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
```

```
Switch(config-if)# ip address 10.0.0.2 255.255.255.0
Switch(config-if)# standby ip 10.0.0.3
Switch(config-if)#  standby 1 preempt
Switch(config-if)# standby 2 ip 10.0.0.4
Switch(config-if)# standby 2 priority 110
Switch(config-if)#  standby 2 preempt
Switch(config-if)# end
```

HSRP 認証およびタイマーの設定：例

次に、グループ 1 のホットスタンバイ ルータを相互運用させるために必要な認証ストリングとして、word を設定する例を示します。

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 authentication word
Switch(config-if)# end
```

次に、hello パケット間隔が 5 秒、ルータがダウンしたと見なされるまでの時間が 15 秒となるように、スタンバイ グループ 1 のタイマーを設定する例を示します。

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip
Switch(config-if)# standby 1 timers 5 15
Switch(config-if)# end
```

HSRP グループおよびクラスタリングの設定：例

次に、スタンバイ グループ my_hsrp をクラスタにバインドし、同じ HSRP グループをイネーブルにしてコマンド スイッチおよびルータの冗長性に使用する例を示します。このコマンドを実行できるのは、コマンド スイッチに対してだけです。スタンバイ グループの名前または番号が存在しない場合、またはスイッチがクラスタ メンバー スイッチである場合は、エラー メッセージが表示されます。

```
Switch # configure terminal
Switch(config) # cluster standby-group my_hsrp routing-redundancy
Switch(config-if)# end
```

HSRP の設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*Command Reference (Catalyst 9200 Series Switches)*

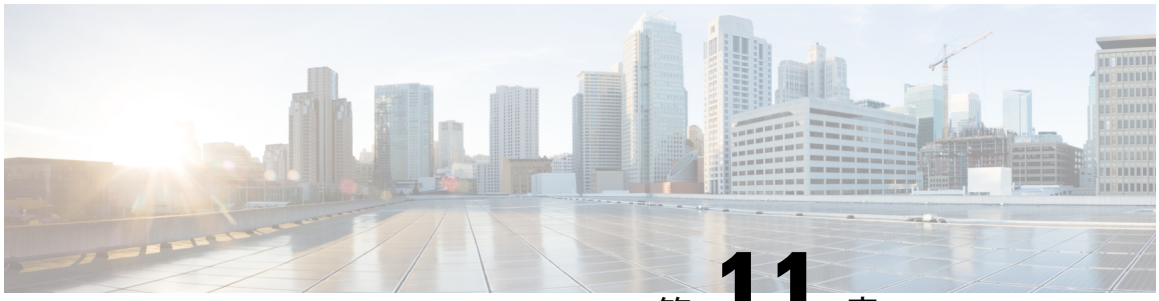
標準および RFC

標準/RFC	タイトル
RFC 2281	『Cisco Hot Standby Router Protocol』

HSRP の設定に関する機能情報

表 *13 : HSRP* の設定に関する機能情報

リリース	機能情報
Cisco IOS XE Fuji 16.9.1	この機能が導入されました。
Cisco IOS XE Fuji 16.9.1	HSRP は、ファーストホップ IPv6 ルータの透過的なフェールオーバーを可能にする FHRP です。



第 11 章

VRRPv3 プロトコルのサポート

VRRPv3 プロトコルのサポートの制限事項

- VRRPv3 は既存のダイナミック プロトコルの代替にはなりません。VRRPv3 は、マルチアクセス、マルチキャスト、またはブロードキャスト対応イーサネット LAN で使用するために設計されています。
- VRRPv3 は、イーサネット、ファストイーサネット、ブリッジグループ仮想インターフェイス（BVI）、およびギガビット イーサネット インターフェイス、 VLAN 上でサポートされます。
- BVI インターフェイスの初期化に関連して転送遅延が発生するため、VRRPv3 アドバタイズ タイマーの時間は BVI インターフェイスでの転送遅延時間より短く設定する必要があります。VRRPv3 アドバタイズタイマーの時間を BVI インターフェイスでの転送遅延時間以上の値に設定すると、最近初期化された BVI インターフェイス上にある VRRP デバイスが無条件にプライマリロールを引き継ぐことができなくなります。BVI インターフェイスでの転送遅延を設定するには、**bridge forward-time** コマンドを使用します。VRRP アドバタイズメントタイマーを設定するには、**vrrp timers advertise** コマンドを使用します。
- VRRPv3 は、ステートフル スイッチオーバー（SSO）をサポートしていません。
- VRRP が VRRS 経路の冗長インターフェイスと同じネットワーク パス上で動作する場合にのみ、完全なネットワークの冗長性を実現できます。完全な冗長性のために、次の制約事項が適用されます。
  - VRRS 経路は、親 VRRP グループと異なる物理インターフェイスを共有したり、親 VRRP グループと異なる物理インターフェイスを持つサブインターフェイス上で設定することはできません。

- VRRS 経路は、関連付けられた VLAN が親 VRRP グループが設定された VLAN と同じトランクを共有していない限り、スイッチ仮想インターフェイス（SVI）に設定することはできません。

VRRPv3 プロトコル サポートについて

VRRPv3 の利点

IPv4 と IPv6 のサポート

VRRPv3 は、VRRPv2 が IPv4 アドレスしかサポートしていないのに対し、IPv4 と IPv6 アドレス ファミリをサポートしています。

（注） VRRPv3 が使用中の場合、VRRPv2 は使用できません。VRRPv3 を設定可能にするには、**fhrp version vrrp v3** コマンドをグローバル コンフィギュレーション モードで使用する必要があります。

冗長性

VRRP により、複数のデバイスをデフォルト ゲートウェイ デバイスとして設定できるようになり、ネットワークに単一障害点が生じる可能性を低減できます。

ロード シェアリング

LAN クライアントとのトラフィックを複数のデバイスで共有するように VRRP を設定できるため、利用可能なデバイス間でより公平にトラフィックの負荷を共有できます。

複数の仮想デバイス

VRRP はデバイスの物理インターフェイス上で（拡張の制限に従って）最大 255 の仮想デバイス（VRRP グループ）をサポートします。複数の仮想デバイスをサポートすることで、LAN トポロジ内で冗長化とロード シェアリングを実装できます。拡張環境では、VRRS 経路は VRRP 制御グループと組み合わせて使用する必要があります。

複数の IP アドレス

仮想デバイスは、セカンダリ IP アドレスを含め複数の IP アドレスを管理できます。そのため、イーサネット インターフェイスに複数のサブネットを設定した場合、サブネットごとに VRRP を設定できます。

（注） VRRP グループでセカンダリ IP アドレスを使用するには、プライマリ アドレスを同じグループで設定する必要があります。

プリエンプション

VRRP の冗長性スキームにより、仮想デバイスバックアップのプリエンプションが可能になり、より高い優先順位が設定された仮想デバイスバックアップが、機能を停止したプライマリ仮想デバイスを引き継ぐことができます。

（注） 優先順位の低いプライマリデバイスのプリエンプションは、オプションの遅延時間を指定して有効にします。

アドバタイズメント プロトコル

VRRPは、VRRPアドバタイズメント専用のインターネット割り当て番号局（IANA）標準マルチキャスト アドレスを使用します。IPv4 では、マルチキャスト アドレスは 224.0.0.18 です。IPv6 では、マルチキャスト アドレスは FF02:0:0:0:0:0:0:12 です。このアドレッシング方式によって、マルチキャストを提供するデバイス数が最小限になり、テスト機器でセグメント上の VRRP パケットを正確に識別できるようになります。IANA では VRRP に IP プロトコル番号 112 を割り当てていました。

VRRP デバイスのプライオリティおよびプリエンプション

VRRP冗長性スキームの重要な一面に、VRRPデバイス プライオリティがあります。優先順位により、各VRRPデバイスが実行する役割と、仮想プライマリデバイスが機能を停止したときにどのようなことが起こるかが決定されます。

特定の VRRP デバイスが仮想デバイスの IP アドレスと物理インターフェイスの IP アドレスのオーナーである場合には、このデバイスが仮想プライマリデバイスとして機能します。

特定のVRRPデバイスが仮想バックアップデバイスとして機能するかどうか、および仮想プライマリデバイスが機能を停止した場合に仮想プライマリデバイスを引き継ぐ順序も、優先順位によって決定されます。各仮想バックアップデバイスの優先順位は、**priority** コマンドを使用して 1 ～ 254 の値に設定できます（**vrrp address-family** コマンドを使用して VRRP 設定モードに入り、**priority** オプションにアクセスします）。

たとえば、LANトポロジのプライマリ仮想デバイスであるデバイスAが機能を停止した場合、選択プロセスが実行され、仮想デバイスバックアップ B または C が引き継ぐかどうかが決定されます。デバイス B とデバイス C がそれぞれ優先順位 101 と 100 に設定されている場合、優先順位の高いデバイス B がプライマリ仮想デバイスになります。デバイス B とデバイス C が両方とも優先順位100に設定されている場合、IPアドレスが大きい方の仮想デバイスバックアップが選択されてプライマリ仮想デバイスになります。

デフォルトでは、プリエンプティブスキームが有効になっています。この場合、プライマリ仮想デバイスになるように選択されている仮想バックアップデバイスの中で、より高い優先順位が設定されている仮想バックアップデバイスがプライマリ仮想デバイスになります。このプリエンプティブスキームは、**no preempt** コマンドを使用して無効にできます（**vrrp address-family** コマンドを使用して VRRP 設定モードに入り、**no preempt** コマンドを入力します）。プリエンプションが無効になっている場合は、元のプライマリ仮想デバイスが回復して再びプライマリになるまで、プライマリ仮想デバイスになるように選択されている仮想デバイスバックアップがプライマリの役割を果たします。

（注） 優先順位の低いプライマリデバイスのプリエンプションは、オプションの遅延時間を指定して有効にします。

VRRP のアドバタイズメント

プライマリ仮想デバイスは、同じグループ内の他の VRRP デバイスに VRRP アドバタイズメントを送信します。アドバタイズメントでは、プライマリ仮想デバイスの優先順位と状態が伝達されます。VRRP アドバタイズメントは、（VRRP グループ設定に基づいて）IPv4 または IPv6 パケットにカプセル化され、VRRP グループに割り当てられた適切なマルチキャストアドレスに送信されます。IPv4 では、マルチキャスト アドレスは 224.0.0.18 です。IPv6 では、マルチキャスト アドレスは FF02:0:0:0:0:0:0:12 です。アドバタイズメントは、デフォルトでは 1 秒に 1 回送信されますが、この間隔は設定可能です。

シスコ デバイスでは、VRRPv2 からの変更点であるミリ秒タイマーを設定できます。ミリ秒タイマー値は、プライマリ デバイスとバックアップ デバイスの両方に手動で設定する必要があります。バックアップデバイス上の **show vrrp** コマンド出力に表示されるプライマリ アドバタイズメント値は、常に 1 秒です。これはバックアップデバイス上のパケットでミリ秒値が受け入れられないためです。

ミリ秒タイマーは、絶対に必要な場合以外は使用しないようにし、使用する場合は慎重な検討とテストが必要です。ミリ秒の値は望ましい状況でのみ動作します。ミリ秒のタイマー値の使用は、VRRPv3 も含めてサポートしている限り、サードパーティ ベンダーと互換性があります。タイマー値は 100 ～ 40000 ミリ秒の範囲で指定できます。

VRRPv3 プロトコル サポートの設定方法

VRRP グループの作成とカスタマイズ

VRRP グループを作成するには、次の手順を実行します。ステップ 6 ～ 14 はそのグループのカスタマイズ オプションで、これらは省略可能です。

手順の概要

1. **enable**
2. **configure terminal**
3. **fhrp version vrrp v3**
4. **interface** *type number*
5. **vrrp** *group-id* **address-family** {**ipv4** | **ipv6**}
6. **address** *ip-address* [**primary** | **secondary**]
7. **description** *group-description*
8. **match-address**
9. **preempt delay minimum** *seconds*
10. **priority** *priority-level*
11. **timers advertise** 間隔
12. **vrrpv2**
13. **vrrs leader** *vrrs-leader-name*
14. **shutdown**
15. **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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**fhrp version vrrp v3** 例： `Device(config)# fhrp version vrrp v3`	VRRPv3 および VRRS を設定する機能をイネーブルにします。 （注） VRRPv3 が使用中の場合、VRRPv2 は使用できません。 **fhrp version vrrp v2** コマンドは設定可能ですが、サポートされていません。
ステップ 4	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/0/0`	インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**vrrp** *group-id* **address-family** {**ipv4** | **ipv6**} 例： `Device(config-if)# vrrp 3 address-family ipv4`	VRRP グループを作成し、VRRP 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	**address** *ip-address* [**primary** | **secondary**] 例： `Device(config-if-vrrp)# address 100.0.1.10 primary`	VRRP グループのプライマリ アドレスまたはセカンダリ アドレスを指定します。 （注） IPv6 の VRRPv3 では、グループを動作可能にするため、プライマリ仮想リンクローカル IPv6 アドレスが設定されている必要があります。プライマリ リンクローカル IPv6 アドレスがグループに確立されると、セカンダリ グローバルアドレスを追加できます。
ステップ 7	**description** *group-description* 例： `Device(config-if-vrrp)# description group 3`	（任意）VRRP グループの説明を指定します。
ステップ 8	**match-address** 例： `Device(config-if-vrrp)# match-address`	（任意）アドバタイズメント パケットのセカンダリ アドレスを設定したアドレスと照合します。 • セカンダリ アドレスの照合は、デフォルトで有効になっています。
ステップ 9	**preempt delay minimum** *seconds* 例： `Device(config-if-vrrp)# preempt delay minimum 30`	（任意）優先順位の低いプライマリデバイスのプリエンプションは、オプションの遅延時間を指定して有効にします。 • プリエンプションはデフォルトでイネーブルです。
ステップ 10	**priority** *priority-level* 例： `Device(config-if-vrrp)# priority 3`	（任意）VRRP グループのプライオリティを指定します。 • VRRP グループの優先度はデフォルトで 100 です。
ステップ 11	**timers advertise** 間隔 例： `Device(config-if-vrrp)# timers advertise 1000`	（任意）アドバタイズメント タイマーをミリ秒で設定します。 • アドバタイズメント タイマーはデフォルトで 1000 ミリ秒に設定されています。

	コマンドまたはアクション	目的
ステップ 12	**vrrpv2** 例： `Device(config-if-vrrp)# vrrpv2`	（任意）互換モードで VRRPv2 設定デバイスのサポートを有効にします。 • VRRPv2 はサポートされていません。
ステップ 13	**vrrs leader** *vrrs-leader-name* 例： `Device(config-if-vrrp)# vrrs leader leader-1`	（任意）VRRS に登録され、フォロワーに使用されるリーダーの名前を指定します。 • 登録済みの VRRS 名はデフォルトで使用不可になっています。
ステップ 14	**shutdown** 例： `Device(config-if-vrrp)# shutdown`	（任意）VRRP グループの VRRP 設定をディセーブルにします。 • VRRP の設定は、VRRP グループに対してはデフォルトでイネーブルになっています。
ステップ 15	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

FHRP クライアントの初期化前の遅延時間の設定

インターフェイス上のすべての FHRP クライアントの初期化の前に遅延期間を設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **fhrp version vrrp v3**
4. **interface** *type number*
5. **fhrp delay** {[**minimum**] [**reload**] *seconds*}
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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**fhrp version vrrp v3** 例： `Device(config)# fhrp version vrrp v3`	VRRPv3 および VRRS を設定する機能をイネーブルにします。 （注） VRRPv3 が使用中の場合、VRRPv2 は使用できません。
ステップ 4	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/0/0`	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 5	**fhrp delay** {[**minimum**] [**reload**] *seconds*} 例： `Device(config-if)# fhrp delay minimum 5`	インターフェイスの起動後に、FHRP クライアントの初期化の遅延期間を指定します。 • 範囲は 0 ～ 3600 秒です。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

VRRPv3 プロトコル サポートの設定例

例：デバイス上の VRRPv3 のイネーブル化

次の例は、デバイスで VRRPv3 をイネーブルにする方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
Device(config-if-vrrp)# end
```

例：VRRP グループの作成とカスタマイズ

次に、VRRP グループを作成およびカスタマイズする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# vrrp 3 address-family ipv4
Device(config-if-vrrp)# address 100.0.1.10 primary
Device(config-if-vrrp)# description group 3
Device(config-if-vrrp)# match-address
Device(config-if-vrrp)# preempt delay minimum 30
Device(config-if-vrrp)# end
```

（注） 上の例では、グローバル コンフィギュレーション モードで **fhrp version vrrp v3** コマンドが使用されています。

例：FHRP クライアントの初期化前の遅延時間の設定

次の例は、FHRP クライアントの初期化前の遅延時間の設定方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# fhrp delay minimum 5
Device(config-if-vrrp)# end
```

（注） 上記の例では、インターフェイスが表示されてから FHRP クライアントの初期化に 5 秒間の遅延時間が指定されています。遅延時間は 0 ～ 3600 秒の範囲で指定できます。

例：VRRP ステータス、設定、および統計情報の詳細

以下は、VRRP グループのステータス、設定、および統計情報の詳細の出力例です。

```
Device> enable
Device# show vrrp detail

 GigabitEthernet1/0/1 - Group 3 - Address-Family IPv4
  Description is "group 3"
  State is MASTER
  State duration 53.901 secs
  Virtual IP address is 100.0.1.10
  Virtual MAC address is 0000.5E00.0103
  Advertisement interval is 1000 msec
  Preemption enabled, delay min 30 secs (0 msec remaining)
  Priority is 100
  Master Router is 10.21.0.1 (local), priority is 100
  Master Advertisement interval is 1000 msec (expires in 832 msec)
  Master Down interval is unknown
```

```
  VRRPv3 Advertisements: sent 61 (errors 0) - rcvd 0
  VRRPv2 Advertisements: sent 0 (errors 0) - rcvd 0
  Group Discarded Packets: 0
    VRRPv2 incompatibility: 0
    IP Address Owner conflicts: 0
    Invalid address count: 0
    IP address configuration mismatch : 0
    Invalid Advert Interval: 0
    Adverts received in Init state: 0
    Invalid group other reason: 0
  Group State transition:
    Init to master: 0
    Init to backup: 1 (Last change Sun Mar 13 19:52:56.874)
    Backup to master: 1 (Last change Sun Mar 13 19:53:00.484)
    Master to backup: 0
    Master to init: 0
    Backup to init: 0

Device# 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
FHRP コマンド	『First Hop Redundancy Protocols Command Reference』
VRRPv2 の設定	『*Configuring VRRP*』
VRRPv3 コマンド	この章で使用するコマンドの完全な構文および使用方法の詳細。

標準および RFC

標準/RFC	タイトル
RFC5798	『*Virtual Router Redundancy Protocol*』

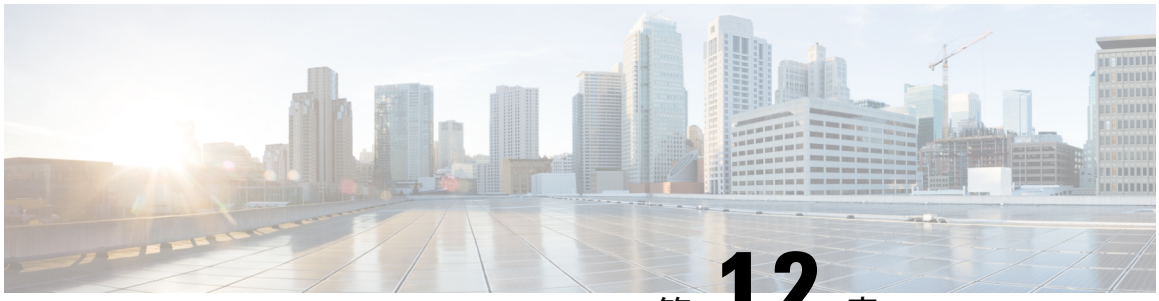
VRRPv3 プロトコルのサポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

けを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *14 : VRRPv3* プロトコルのサポートの機能情報

機能名	リリース	機能情報
VRRPv3 プロトコルのサポート	Cisco IOS XE Fuji 16.9.1	VRRP は、デバイスのグループを使用して単一の仮想デバイスを形成し、冗長性を実現します。これにより、仮想デバイスをデフォルト ゲートウェイとして使用するように、LAN クライアントを設定できます。デバイスのグループを表す仮想デバイスは、「VRRP グループ」とも呼ばれます。VRRPv3 プロトコルのサポート機能は、IPv4 と IPv6 アドレスをサポートするための機能を提供します。 この機能が導入されました。



第 12 章

拡張オブジェクト トラッキングの設定

拡張オブジェクト トラッキングに関する情報

拡張オブジェクト トラッキングの概要

拡張オブジェクト トラッキング機能が導入される前は、ホットスタンバイ ルータ プロトコル（HSRP）に単純なトラッキング メカニズムが内蔵されていますた。このメカニズムでは、インターフェイスのラインプロトコルのステートしか追跡することができませんでした。インターフェイスのラインプロトコル ステートがダウンになった場合、ルータのHSRP優先度は削減され、より高い優先度のもう 1 つの HSRP ルータがアクティブになることができます。

拡張オブジェクトトラッキング機能は、HSRPからトラッキング メカニズムを分離させて、独立したトラッキング プロセスを別途生成します。これにより、HSRP以外のプロセスがこのトラッキング プロセスを使用できます。この機能を使用すると、インターフェイスのラインプロトコルのステートに加えて他のオブジェクトも追跡できます。

HSRP、仮想ルータ冗長プロトコル（VRRP）、Gateway Load Balancing Protoco（GLBP）などのクライアント プロセスで、トラッキング オブジェクトに対する興味を登録し、追跡対象オブジェクトの状態が変化したときに通知を受け取るようにすることができます。

各追跡対象オブジェクトには、トラッキング コマンドライン インターフェイス（CLI）で指定される一意の番号があります。クライアント プロセスは、この番号を使用して特定のオブジェクトを追跡します。トラッキング プロセスは、追跡対象オブジェクトに値の変化がないかどうかを定期的にポーリングし、（アップまたはダウン値など）変化があれば登録されているクライアント プロセスに通知します。ただちに通知する場合と、指定された時間遅延後に通知する場合があります。同じオブジェクトを複数のクライアントが追跡して、オブジェクトのステートが変化した場合に、それぞれが異なるアクションを実行できます。

複数のオブジェクトを組み合わせて1つのリストにして追跡することもできます。このリストの状態判定には、重みしきい値またはパーセンテージを使用します。オブジェクトの組み合わせには、ブールロジックを使用できます。「AND」ブール関数を使用する追跡リストの場合、リスト内の各オブジェクトがアップ ステートでないと追跡対象オブジェクトはアップになりません。「OR」ブール関数を使用する追跡リストの場合、リスト内の 1 つのオブジェクトだけがアップ ステートであれば追跡対象オブジェクトはアップになります。

インターフェイス ラインプロトコルまたは IP ルーティング ステートのトラッキング

インターフェイス ラインプロトコル ステートまたはインターフェイス IP ルーティング ステートのいずれかを追跡できます。IP ルーティング ステートを追跡する場合、オブジェクトをアップするには次の 3 つの条件が必要です。

- インターフェイス上で IP ルーティングがイネーブル、かつアクティブになっている。
- インターフェイス ラインプロトコル ステートが使用可能な状態（アップ）にある。
- 既知のインターフェイス IP アドレスを使用している。

この 3 つの条件がすべて合致しないと、IP ルーティング ステートはダウンになります。

追跡リスト

オブジェクトの追跡リストは、ブール式、重みしきい値、またはパーセントしきい値を使用して設定できます。トラッキング対象リストには1つまたは複数のオブジェクトが含まれます。オブジェクトは存在していないと追跡リストに追加できません。

- 設定にブール式による演算を指定する場合は、「AND」または「OR」演算子を使用します。
- 追跡リストのステートを重みしきい値で判定する場合は、追跡リスト内の各オブジェクトに重み番号を割り当てます。追跡リストのステートは、このしきい値に合致したかどうかで判定されます。各オブジェクトのステートは、すべてのオブジェクトの重みの合計と各オブジェクトのしきい値の重みを比較して判定されます。
- 追跡リストをパーセントしきい値で判定する場合は、追跡リスト内のすべてのオブジェクトにパーセントしきい値を割り当てます。各オブジェクトのステートは、各オブジェクトに割り当てたパーセンテージとリストを比較して判定されます。

他の特性のトラッキング

拡張オブジェクト トラッキングを使用して他の特性を追跡することもできます。

- **track ip route reachability** グローバル コンフィギュレーション コマンドを使用すると、IP ルートの到達可能性を追跡できます。

- **track ip route metric threshold** グローバル コンフィギュレーション コマンドを使用すると、ルートがしきい値を超えているか下回っているかを確認できます。
- **track resolution** グローバル コンフィギュレーション コマンドを使用すると、ルーティングプロトコルのメトリック解決のデフォルト値を変更できます。
- **track timer tracking** コンフィギュレーション コマンドを使用すると、トラッキング対象オブジェクトを定期的にポーリングするようにトラッキングプロセスを設定できます。

拡張オブジェクトトラッキング設定を確認する場合は、 **show track** 特権 EXEC コマンドを使用してください。

IP SLA オブジェクト トラッキング

Cisco IOS IP サービス レベル契約（SLA）は、ネットワーク パフォーマンスの測定と診断を行うツールです。ネットワーク パフォーマンスを測定するためのトラフィック生成には、アクティブ モニタリングが使用されます。Cisco IP SLA 動作は、ネットワークのトラブルシューティングや設計、分析に使用できるリアルタイム メトリックを収集します。

IP SLA 動作のオブジェクト トラッキングを活用すると、クライアントは IP SLA オブジェクトの出力を追跡して、その情報をアクションのトリガーに使用できます。各 IP SLA 動作は、OK または OverThreshold のような簡易ネットワーク管理プロトコル（SNMP）動作の戻りコード値を保持しているため、トラッキング プロセス側で解釈できます。ステートと到達可能性という IP SLA 動作の 2 つの側面をトラッキングできます。ステートの場合、戻りコードが OK のとき、トラック ステートがアップします。リターン コードが OK ではないとき、トラック ステートはダウンします。到達可能性の場合、戻りコードが OK または OverThreshold のとき、到達可能性がアップします。リターン コードが OK ではないとき、到達可能性はダウンします。

スタティック ルート オブジェクト トラッキング

拡張オブジェクトトラッキングを使用したスタティック ルーティング サポートにより、デバイスで ICMP ping を使用して、設定済みのスタティックルートまたは DHCP ルートがダウンしていることを認識できます。トラッキングを有効にしている場合、システムはルート ステートを追跡し、ステートの変化をクライアントに通知できます。スタティック ルート オブジェクト トラッキングは、プライマリ ゲートウェイへの接続状態をモニタするために、Cisco IP SLA を使用して ICMP ping を生成します。

拡張オブジェクト トラッキングの設定方法

インターフェイスでのライン ステート プロトコルまたは IP ルーティング ステートのトラッキングの設定

インターフェイスのラインプロトコル ステートまたは IP ルーティング ステートを追跡するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **track** *object-number***interface** *interface-id***line-protocol**
4. **delay** { *object-number***up***seconds*[**down***seconds*]|[**up***seconds*]**down***seconds*}
5. **exit**
6. **track** *object-number***interface** *interface-id***ip routing**
7. **delay** { *object-number***up***seconds*[**down***seconds*]|[**up***seconds*]**down***seconds*}
8. **end**
9. **show track***object-number*

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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**track** *object-number***interface** *interface-id***line-protocol** 例： `Device(config)# track 33 interface gigabitethernet 1/0/1 line-protocol`	（任意）インターフェイスのラインプロトコル ステートを追跡するための追跡リストを作成し、トラッキング コンフィギュレーション モードを開始します。 • object-number：追跡対象オブジェクトの番号です。指定できる範囲は 1 ～ 500 です。

	コマンドまたはアクション	目的
		• **interface** interface-id は、追跡されるインターフェイスです。
ステップ 4	**delay** { *object-number***up***seconds*[**down***seconds*][**up***seconds*]**down***seconds*}	（任意）追跡対象オブジェクトのステート変更の通信を遅延させる時間（秒）を指定します。指定できる範囲は 1 ～ 180 秒です。
ステップ 5	**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	**track** *object-number***interface** *interface-id***ip routing** 例： `Device(config)# track 33 interface gigabitethernet 1/0/1 ip routing`	（任意）インターフェイスの IP ルーティング ステートを追跡するための追跡リストを作成し、トラッキング コンフィギュレーション モードを開始します。IP ルート追跡では、ルーティング テーブル内の IP ルートおよびインターフェイスの IP パケット ルーティング機能を追跡します。 • object-number：追跡対象オブジェクトの番号です。指定できる範囲は 1 ～ 500 です。 • **interface** interface-id は、追跡されるインターフェイスです。
ステップ 7	**delay** { *object-number***up***seconds*[**down***seconds*][**up***seconds*]**down***seconds*}	（任意）追跡対象オブジェクトのステート変更の通信を遅延させる時間（秒）を指定します。指定できる範囲は 1 ～ 180 秒です。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show track***object-number*	指定したオブジェクトが追跡されているかどうかを確認します。

追跡リストの設定

重みしきい値による追跡リストの設定

重みしきい値による追跡を行うには、複数オブジェクトを含んだ追跡リストを作成し、重みをしきい値として使用することを指定したあと、各オブジェクトに重み値を設定します。各オブジェクトのステートは、アップであるすべてのオブジェクトの重み合計と各オブジェクトのしきい値の重みを比較して判定されます。

重みしきい値のリストには、「NOT」ブール演算子を使用できません。

重みしきい値を使用してオブジェクトの追跡リストを作成し、各オブジェクトに重み値を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **track** *track-number***list threshold** {**weight**}
4. **object** *object-number*[**weight***weight-number*]
5. **threshold weight** {**up***number*|[**down***number*]}
6. **delay** { **up***seconds*[**down***seconds*]|[**up***seconds*]**down***seconds*}
7. **end**
8. **show track***object-number*
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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**track** *track-number***list threshold** {**weight**} 例： `Device(config)# track 4 list threshold weight`	トラッキング対象リスト オブジェクトを設定し、トラッキング コンフィギュレーション モードを開始します。指定できる track-number の範囲は 1 ～ 500 です。 • **threshold—**追跡リストのステートがしきい値に基づくことを指定します。 • **weight—** しきい値が重みに基づくことを指定します。
ステップ 4	**object** *object-number*[**weight***weight-number*] 例： `Device(config)#object 2 weight 15`	追跡対象のオブジェクトを指定します。指定できる範囲は 1 ～ 500 です。任意の **weight***weight-number* には、オブジェクトのしきい値の重みを指定します。範囲は 1 ～ 255 です。 （注） オブジェクトは存在していないと追跡リストに追加できません。
ステップ 5	**threshold weight** {**up***number*|[**down***number*]} 例：	（任意）重みしきい値を指定します。

	コマンドまたはアクション	目的
	`Device(config-track)# threshold weight up 30 down 10`	• **up***number*：範囲は 1 ～ 255 です。 • **down***number*：（任意）範囲は **up***number* で選択した数値によって異なります。**up***number* を 25 に設定すると、down number の範囲は 0 ～ 24 になります。
ステップ 6	**delay** { **up***seconds*[**down***seconds*]|[**up***seconds*]**down***seconds*}	（任意）追跡対象オブジェクトのステート変更の通信を遅延させる時間（秒）を指定します。指定できる範囲は 1 ～ 180 秒です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show track***object-number*	指定したオブジェクトが追跡されているかどうかを確認します。
ステップ 9	**copy running-config startup-config** 例： `Device# 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。

パーセントしきい値による追跡リストの設定

パーセントしきい値による追跡を行うには、複数オブジェクトを含んだ追跡リストを作成し、パーセンテージをしきい値として使用することを指定したあと、リスト内のすべてのオブジェクトにパーセンテージを指定します。リストのステートは、各オブジェクトに割り当てたパーセンテージとリストを比較して判定されます。

パーセントしきい値のリストには、「NOT」ブール演算子を使用できません。

パーセントしきい値を使用してオブジェクトの追跡リストを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **track** *track-number***list threshold** {**percentage**}
4. **object** *object-number*
5. **threshold percentage** {**up***number*|[**down***number*]}
6. **delay** { **up***seconds*[**down***seconds*]|[**up***seconds*]**down***seconds*}
7. **end**
8. **show track***object-number*
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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**track** *track-number***list threshold** {**percentage**} 例： `Device(config)# track 4 list threshold percentage`	トラッキング対象リスト オブジェクトを設定し、トラッキング コンフィギュレーション モードを開始します。指定できる track-number の範囲は 1 ～ 500 です。 • **threshold—**追跡リストのステートがしきい値に基づくことを指定します。 • **percentage—** しきい値がパーセンテージに基づくことを指定します。
ステップ 4	**object** *object-number* 例： `Device(config)# object 1`	追跡対象のオブジェクトを指定します。指定できる範囲は 1 ～ 500 です。 （注） オブジェクトは存在していないと追跡リストに追加できません。
ステップ 5	**threshold percentage** {**up***number*|[**down***number*]} 例： `Device(config)# threshold percentage up 51 down 10`	（任意）パーセントしきい値を指定します。 • **up***number*：範囲は 1 ～ 100 です。 • **down***number*：（任意）範囲は **up***number* で選択した数値によって異なります。**up***number* を 25 に設定すると、down number の範囲は 0 ～ 24 になります。
ステップ 6	**delay** { **up***seconds*[**down***seconds*]|[**up***seconds*]**down***seconds*}	（任意）追跡対象オブジェクトのステート変更の通信を遅延させる時間（秒）を指定します。指定できる範囲は 1 ～ 180 秒です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show track***object-number*	指定したオブジェクトが追跡されているかどうかを確認します。

	コマンドまたはアクション	目的
ステップ 9	**copy running-config startup-config** 例： `Device# 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。

HSRP オブジェクト トラッキングの設定

特定のオブジェクトを追跡し、そのオブジェクトのステートに基づいてHSRPプライオリティを変更できるようにスタンバイ HSRP グループを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **track** *object-number*{**interface** *interface-id*{**line-protocol**|**ip routing**}|**ip route***ip address/prefix-length*{**metric threshold**|**reachability**}**list**{**boolean**{**and**|**or**}}|{**threshold**{**weight**|**percentage**}}}
4. **exit**
5. **interface** { *interface-id*
6. **standby**[*group-number*]**ip**[*ip-address***secondary**]]
7. **standby**[*group-number*]**track**[*object-number*[**decrement** *priority-decrement*]]
8. **end**
9. **show standby**
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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**track** *object-number*{**interface** *interface-id*{**line-protocol**|**ip routing**}|**ip route***ip address/prefix-length*{**metric threshold**|**reachability**}**list**{**boolean**{**and**|**or**}}|{**threshold**{**weight**|**percentage**}}}	（任意）設定されたステートを追跡するための追跡リストを作成し、トラッキング 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
		• object-number：追跡対象オブジェクトの番号です。指定できる範囲は 1 ～ 500 です。 • 追跡するインターフェイスを指定するには、**interface** *interface-id* を入力します。 • インターフェイス ライン プロトコルの状態を追跡するには **line-protocol** を入力します。また、インターフェイス IP ルーティングの状態を追跡するには、**ip routing** を入力します。 • IP ルートの状態を追跡するには、**ip route***ip-address/prefix-length* を入力します。 • しきい値メトリックを追跡する場合は **metric threshold**、ルートが到達可能かどうかを追跡するには **reachability** を入力します。 デフォルトの up しきい値は 254、デフォルトの down しきい値は 255 です。 • リスト内の一連のオブジェクトを追跡するには、**list** を入力します。 （注） 追跡するインターフェイスごとにこの手順を繰り返してください。
ステップ 4	**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 5	**interface** { *interface-id*	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 6	**standby**[*group-number*]**ip**[*ip-address***secondary**]]	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成（またはイネーブルに）します。 • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号を入力します。指定できる範囲は 0 ～ 255 です。デフォルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • （1 つのインターフェイスで必須、それ以外は任意）*ip-address*：ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対し

	コマンドまたはアクション	目的
		て仮想IPアドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 • （任意）**secondary**：IP アドレスがセカンダリ ホット スタンバイ ルータ インターフェイスであることを指定します。このキーワードが省略された場合、設定されたアドレスはプライマリ IP アドレスになります。
ステップ 7	**standby**[*group-number*]**track**[*object-number*[**decrement** *priority-decrement*]]	特定のオブジェクトを追跡し、そのオブジェクト ステートに基づいてホットスタンバイ プライオリティを変更できるように HSRP を設定します。 • （任意）*group-number*：追跡が適用されるグループ番号を入力します。 • *object-number*：追跡対象のオブジェクト番号を入力します。指定できる範囲は1～500で、デフォルトは 1 です。 • （任意）**secondary**：IP アドレスがセカンダリ ホット スタンバイ ルータ インターフェイスであることを指定します。このキーワードが省略された場合、設定されたアドレスはプライマリ IP アドレスになります。 • （任意）**decrement***priority-decrement*：追跡対象のオブジェクトがダウンになった場合（またはアップに戻った場合）に、ルータのホットスタンバイの優先順位を減少（または増加）させる幅を指定します。指定できる範囲は 1 ～ 255 で、デフォルトは 10 です。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show standby**	スタンバイ ルータの IP アドレスおよび追跡ステートを確認します。
ステップ 10	**copy running-config startup-config** 例： `Device# 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。

IP SLA オブジェクト トラッキングの設定

IP SLA 動作のステートまたは IP SLA IP ホストの到達可能性を追跡するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **track** *object-number* **ip sla** *operation-number* {**state | reachability**}
4. **delay** { **up***seconds*[**down***seconds*]|[**up***seconds*]**down***seconds*}
5. **end**
6. **show track***object-number*
7. **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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**track** *object-number* **ip sla** *operation-number* {**state	reachability**} 例： `Device(config)# track 2 ip sla 123 state`	トラッキング コンフィギュレーション モードを開始し、IP SLA 動作のステートを追跡します。 • *object-number* の範囲は 1 ～ 500 です。 • *operation-number* の範囲は 1 ～ 2147483647 です。
ステップ 4	**delay** { **up***seconds*[**down***seconds*]|[**up***seconds*]**down***seconds*}	（任意）追跡対象オブジェクトのステート変更の通信を遅延させる時間（秒）を指定します。指定できる範囲は 1 ～ 180 秒です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show track***object-number*	指定したオブジェクトが追跡されているかどうかを確認します。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： `Device# 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 ルート オブジェクト トラッキングの設定

スタティック ルーティング用のプライマリ インターフェイスの設定

スタティック ルーティングのプライマリ 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。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface***interface-id*
4. **description***string*
5. **ip address***ip-address mask*[**secondary**]
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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id*	プライマリまたはセカンダリ インターフェイスを選択し、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	**description***string*	インターフェイスに説明を追加します。
ステップ 5	**ip address***ip-address mask*[**secondary**]	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 6	**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。

DHCP のプライマリ インターフェイスの設定

DHCP のプライマリ 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。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface***interface-id*
4. **description***string*
5. **ip dhcp client route track***number*
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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***interface-id*	プライマリまたはセカンダリ インターフェイスを選択し、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	**description***string*	インターフェイスに説明を追加します。
ステップ 5	**ip dhcp client route track***number*	DHCP クライアントを設定し、追加されたルートを指定の追跡番号に関連付けます。有効な数値は 1 ～ 500 です。
ステップ 6	**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。

IP SLA モニタリング エージェントの設定

プライマリ インターフェイスおよびエージェント状態をモニタするトラック オブジェクトを使用して、IP アドレスの ping を実行するように IP SLA エージェントを設定することができます。

Cisco IP SLA でネットワーク モニタリ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. **ip sla***operation number*
4. **icmp-echo**{ *destination ip-address*|*destination hostname*[**source - ipaddr**{*ip-address*|*hostname***source-interface***interface-id*]
5. **timeout***milliseconds*
6. **frequency***seconds*
7. **threshold***milliseconds*
8. **exit**
9. **ip sla schedule** *operation-number*[**life** {**forever**|*seconds*}]**start-time***time*|**pending**|**now**|**after***time*]**ageout***seconds*][**recurring**]
10. **track** *object-number***rtr** *operation-number***statereachability**
11. **end**
12. **show track***object-number*
13. **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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip sla***operation number*	Cisco IP SLA 動作の設定を開始し、IP SLA 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	**icmp-echo**{ *destination ip-address*|*destination hostname*[**source - ipaddr**{*ip-address*|*hostname***source-interface***interface-id*]	Cisco IP SLA エンドツーエンド ICMP エコー応答時間動作を設定し、IP SLA ICMP エコー コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**timeout***milliseconds*	要求パケットの応答に対する動作の待機時間を設定します。
ステップ 6	**frequency***seconds*	動作がネットワークに送信される頻度を設定します。
ステップ 7	**threshold***milliseconds*	反応イベントを生成し、その動作の履歴情報を保存するしきい値（ヒステリシス）の上限を設定します。
ステップ 8	**exit**	IP SLA ICMP エコー コンフィギュレーション モードを終了します。
ステップ 9	**ip sla schedule** *operation-number*[**life** {**forever**|*seconds*}]**start-time***time*|**pending**|**now**|**after***time*][**ageout***seconds*][**recurring**] 例： `Device(config)# track 2 200 state`	単一の IP SLA 動作のスケジューリング パラメータを設定します。 • *object-number* の範囲は 1 ～ 500 です。 • *operation-number* の範囲は 1 ～ 2147483647 です。
ステップ 10	**track** *object-number***rtr** *operation-number***statereachability**	Cisco IOS IP SLA 動作の状態を追跡し、トラッキング コンフィギュレーション モードを開始します。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show track***object-number*	指定したオブジェクトが追跡されているかどうかを確認します。
ステップ 13	**copy running-config startup-config** 例： `Device# 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。

ルーティング ポリシーおよびデフォルト ルートの設定

オブジェクト トラッキングを使用してバックアップ スタティック ルーティングのルーティング 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. **access-list***access-list-number*
4. **route-map***map tag*[**permit**|**deny**][*sequence-number*]
5. **match ip address**{*access-list number*[**permit**|**deny**][*sequence-number*]

6. **set ip next-hop dynamic dhcp**
7. **set interface***interface-id*
8. **exit**
9. **ip local policy route-map***map tag*
10. **ip route***prefix mask*{*ip address*|*interface-id*[*ip address*]}[*distance*][*name*][**permanent**|**track***track-number*][*tag tag*]
11. **end**
12. **show ip route track table**
13. **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： `Device> 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： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**access-list***access-list-number*	拡張 IP アクセス リストを定義します。オプションの文字を設定します。
ステップ 4	**route-map***map tag*[**permit**|**deny**][*sequence-number*]	ルートマップ コンフィギュレーション モードを開始し、特定のルーティングから別のルーティングへの再配信ルートの条件を定義します。
ステップ 5	**match ip address**{*access-list number*[**permit**|**deny**][*sequence-number*]	標準または拡張アクセス リストに許可された宛先ネットワーク番号アドレスを持つルートを配信し、パケットのポリシー ルーティングを実行します。複数の番号または名前を入力できます。
ステップ 6	**set ip next-hop dynamic dhcp**	DHCP ネットワーク専用。DHCP クライアントが学んだ最新のゲートウェイへのネクスト ホップを設定します。
ステップ 7	**set interface***interface-id*	スタティック ルーティング ネットワーク専用。ポリシー ルーティングのルート マップ一致条件をパスした出力パケットの送信場所を指定します。
ステップ 8	**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。

	コマンドまたはアクション	目的
ステップ 9	**ip local policy route-map***map tag*	ルート マップを特定し、ローカル ポリシー ルーティングに使用します。
ステップ 10	**ip route***prefix mask*{*ip address*|*interface-id*[*ip address*]}[*distance*][*name*][**permanent**|**track***track-number*][*tag tag*]	スタティック ルーティング ネットワーク専用。スタティック ルートを確立します。**track***track-number* を入力し、設定したトラックオブジェクトがアップの場合に限り、静的ルートがインストールされるように指定します。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show ip route track table**	IP ルート トラック テーブルの情報を表示します。
ステップ 13	**copy running-config startup-config** 例： `Device# 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。

拡張オブジェクト トラッキングのモニタリング

下の表に示す特権EXECコマンドまたはユーザEXECコマンドを使用して、拡張オブジェクトの追跡情報を表示します。

。

表 *15 :* 追跡情報を表示するコマンド

コマンド	目的
show ip route track table	IPルート トラック テーブルの情報を表示します。
show track [*object-number*]	すべての追跡リストまたは指定リストの情報を表示します。
show track brief	すべてのインターフェイスまたは指定されたインターフェイスに対するVTPのステータスおよび設定を表示します。
show track interface [brief]	追跡対象のインターフェイス オブジェクトに関する情報を表示します。
show track ip [*object-number*][**brief**]**route**	追跡対象IPルート オブジェクトの情報を表示します。

コマンド	目的
show track resolution	追跡対象パラメータの解像度を表示します。
show track timer	追跡対象のポーリング インターバル タイマーを表示します。

その他の参考資料

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

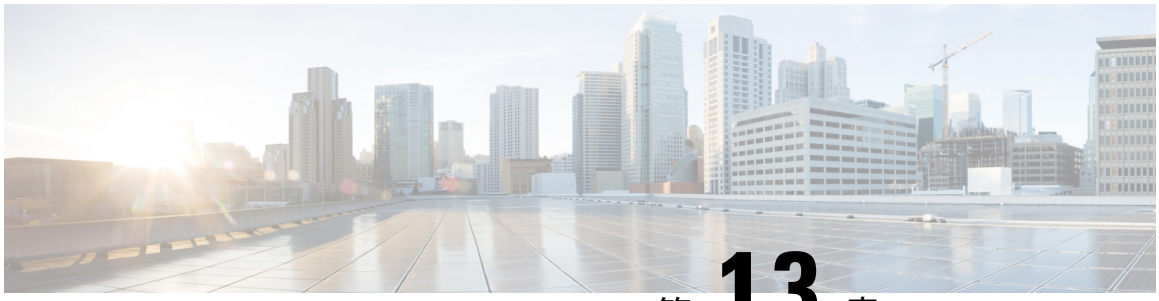
拡張オブジェクト トラッキングの機能情報

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

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

表 *16* : 拡張オブジェクト トラッキングの機能情報

機能名	リリース	機能情報
拡張オブジェクト トラッキング	Cisco IOS XE Fuji 16.9.1	この機能が導入されました。



第 13 章

TCP MSS 調整の設定

TCP MSS 調整に関する情報

トランスミッション コントロール プロトコル（TCP）最大セグメントサイズ（MSS）調整機能では、ルータを通過する一時的なパケット（特に SYN ビットが設定された TCP セグメント）の最大セグメントサイズを設定することができるようになります。切り捨てを回避するために、SYN パケットの中間ルータで MSS 値を指定するには、インターフェイス コンフィギュレーション モードで ip tcp adjust-mss コマンドを使用します。

ホスト（通常は PC）がサーバと TCP セッションを開始するときは、TCP SYN パケットの MSS オプション フィールドを使って IP セグメント サイズをネゴシエートします。MSS フィールドの値は、ホスト上の MTU 設定によって決まります。PC のデフォルト MSS 値は 1500 バイトです。

PPP over Ethernet（PPPoE）標準は、1,492 バイトのみの MTU をサポートします。ホストと PPPoE での MTU サイズの不一致は、ホストとサーバの間にあるルータで 1500 バイトのパケットが損失し、PPPoE を介した TCP セッションが終了する原因となる場合があります。ホストでパス MTU（パス全体で正しい MTU を検出）が有効になっていても、システム管理者がパス MTU を機能させるためにホストからリレーする必要がある ICMP エラーメッセージを無効にすることがあるため、セッションがドロップされることがあります。

ip tcp adjust-mss コマンドで TCP SYN パケットの MSS 値を調整すると、TCP セッション損失防止の役に立ちます。

ip tcp adjust-mss コマンドは、ルータを通過する TCP 接続に対してのみ有効です。

ほとんどの場合、ip tcp adjust-mss コマンドの max-segment-size 引数の最適値は 1,452 バイトです。この値に、20 バイトの IP ヘッダー、20 バイトの TCP ヘッダー、および 8 バイトの PPPoE

ヘッダーが追加されて、イーサネット リンクの MTU サイズと同じ 1500 バイトのパケットになります。

サポートされるインターフェイス

TCP MSS 調整は、次のインターフェイスでのみサポートされます。

- 物理層 3 インターフェイス
- SVI
- レイヤ 3 ポートチャネル
- レイヤ 3 GRE トンネル

（注） サブインターフェイスは TCP MSS 調整をサポートしません。

一時的な TCP SYN パケットの MSS 値の設定

始める前に

ルータを通過する一時的なパケット（特に SYN ビットが設定された TCP セグメント）の MSS を設定するには、この作業を実行します。

シスコでは、次のコマンドと値を使用することをお勧めしています。

- **ip tcp adjust-mss 1452**

手順の概要

1. **enable**
2. **configure terminal**
3. **interface***type number*
4. **ip tcp adjust-mss***max-segment-size*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device>enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device#config terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***type number* 例： `Device(config)#interface GigabitEthernet 1/0/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip tcp adjust-mss***max-segment-size* 例： `Device(config-if)#ip tcp adjust-mss 1452`	ルータを通過する TCP SYN パケットの MSS 値を調整します。 • max-segment-size 引数には、MSS をバイト単位で指定します。範囲は 500 ～ 1460 です。
ステップ 5	**end** 例： `Device(config-if)#end`	グローバル コンフィギュレーション モードに戻ります。

IPv6 トラフィックの MSS 値の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface***type number*
4. **ipv6 tcp adjust-mss***max-segment-size*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device>enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device#config 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：	インターフェイス タイプを設定し、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。

	コマンドまたはアクション	目的
	`Device(config)#interface GigabitEthernet 1/0/0`	
ステップ 4	**ipv6 tcp adjust-mss***max-segment-size* 例： `Device(config-if)#ipv6 tcp adjust-mss 1440`	デバイスを通過する TCP DF パケットの MSS 値を調整します。 • max-segment-size 引数には、MSS をバイト単位で指定します。指定できる範囲は 40 ～ 1440 です。
ステップ 5	**end** 例： `Device(config-if)#end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

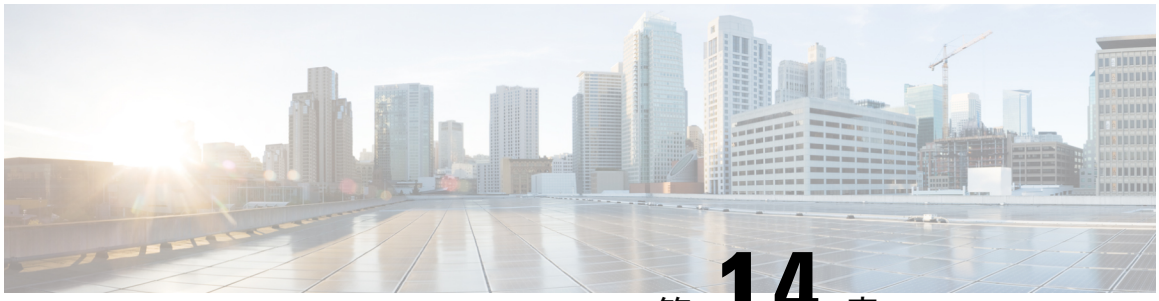
例：IPv6 トラフィックの TCP MSS 調整の設定

```
Device>enable
Device#configure terminal
Device(config)#interface GigabitEthernet 0/0/0
Device(config)#ipv6 tcp adjust-mss 1440
Device(config)#end
```

TCP MSS 調整の機能履歴と情報

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。

機能名	リリース	機能説明
トランスミッション コントロール プロトコル（TCP）最大セグメントサイズ（MSS）調整	Cisco IOS XE Fuji 16.9.1	TCP MSS 調整機能では、ルータを通過する一時的なパケット（特に SYN ビットが設定された TCP セグメント）の最大セグメントサイズを設定することができるようになります。この機能は、TCP SYN パケットの MSS 値を調整することで TCP セッション損失防止の役に立ちます。



第 14 章

IPv6 の拡張ネイバー探索キャッシュ管理

IPv6 の拡張ネイバー探索キャッシュ管理

ネイバー探索プロトコルは、障害のあるノードまたはデバイス、およびリンク層アドレスの変更を検出できるネイバー到達不能検出を実行します。ネイバー到達不能検出プロセスは、ホストからホスト、ホストからデバイス、デバイスからホストへの通信など、ホストとネイバーノード間の全パスの到達可能性情報を保持します。

ネイバーキャッシュは、リンクレイヤアドレスへの IPv6 リンクローカルアドレスまたはグローバルアドレスに関するマッピング情報を保持します。ネイバーキャッシュは、ネイバー到達不能検出プロセスを使用して、ネイバーの到達可能性の状態に関する情報も保持します。ネイバーは、次の 5 つのうちいずれかの状態になります。

- DELAY：ネイバーの解決は保留になっており、トラフィックがこのネイバーに流れる可能性があります。
- INCOMPLETE：アドレスの解決中であり、リンク層アドレスはまだ不明です。
- PROBE：ネイバーの解決中であり、トラフィックがこのネイバーに流れる可能性があります。
- REACHABLE：最後の到達可能時間間隔内でネイバーに到達可能であることがわかっています。
- STALE：ネイバーは解決を必要としており、トラフィックがこのネイバーに流れる可能性があります。

非送信要求ネイバーアドバタイズメントからエントリを収集するネイバー探索プロトコルを設定するには、**ipv6 nd na glean** コマンドを使用します。

ネットワークの中断時にネイバーのネイバー探索キャッシュエントリを保持するようにネイバー探索プロトコルを設定するには、**ipv6 nd nud retry** コマンドを使用します。

ネイバーへのトラフィックフローがない場合でも、ネイバー探索キャッシュエントリを保持するようにネイバー探索プロトコルを設定するには、**ipv6 nd cache expire refresh** コマンドを使用します。

IPv6 ネイバー探索のパラメータのカスタマイズ

IPv6 ネイバー探索のパラメータをカスタマイズするには、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： `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 1/1/4`	インターフェイスタイプと ID を指定します。インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 nd nud retry** *base interval max-attempts* [*final-wait-time*] 例： `Device(config-if)# ipv6 nd nud retry 1 1000 3`	ネイバー到達不能検出でネイバー送信要求を再送信する回数を設定します。
ステップ 5	**ipv6 nd cache expire** *expire-time-in-seconds* [**refresh**] 例： `Device(config-if)# ipv6 nd cache expire 7200`	IPv6 ネイバー探索キャッシュエントリの期限が切れるまでの時間を設定します。
ステップ 6	**ipv6 nd na glean** 例： `Device(config-if)# ipv6 nd na glean`	IPv6 ネイバー探索キャッシュエントリの期限が切れるまでの時間を設定します。
ステップ 7	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 8	**show ipv6 interface** 例： `Device# show ipv6 interface`	（任意）ネイバー探索キャッシュ管理と IPv6 用に設定されたインターフェイスのユーザビリティのステータスを表示します。

例：IPv6 ネイバー探索のパラメータのカスタマイズ

次の例では、IPv6 ネイバーアドバタイズメントの収集が有効になっており、IPv6 ネイバー探索キャッシュの有効期限は 7200 秒（2 時間）に設定されています。

```
Device> enable
Device# configure terminal
Device(config)# interface Port-channel 189
Device(config-if)# no ip address
Device(config-if)# ipv6 address 2001:BD8::/64
Device(config-if)# ipv6 nd reachable-time 2700000
Device(config-if)# ipv6 nd na glean
Device(config-if)# ipv6 nd cache expire 7200
Device(config-if)# no ipv6 redirects
Device(config-if)# end
```

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
この章で使用するコマンドの完全な構文および使用方法の詳細。	「*IP* アドレッシングサービス」のセクションを参照 *Command Reference (Catalyst 9200 Series Switches)*
IPv6 ネイバー探索インスペクションの詳細	「セキュリティ」のセクションを参照*Software Configuration Guide (Catalyst 9200 Switches)*

IPv6 ネイバー探索に関する機能情報

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。

表 *17 : IPv6* ネイバー探索に関する機能情報

機能名	リリース	機能情報
IPv6 の拡張ネイバー探索キャッシュ管理	Cisco IOS XE Fuji 16.9.2	ネイバー探索プロトコルは、障害のあるノードまたはルータ、およびリンク層アドレスの変更を検出できるネイバー到達不能検出を実行します。