



Cisco NCS 560 シリーズルータ（IOS XR リリース 7.1.x）IP アドレスおよびサービスのコンフィギュレーションガイド

初版：2020 年 1 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/>



目次

第 1 章

ネットワーク スタック IPv4 および IPv6 の実装 1

フォールバック VRF の実装 1

ネットワーク スタック IPv4 および IPv6 の例外 2

IPv4 および IPv6 機能 3

Cisco IOS XR ソフトウェアの IPv6 3

ネットワーク スタック IPv4 および IPv6 の実装方法 3

IPv4 アドレス指定の設定 4

IPv6 アドレッシングの設定 5

IPv6 マルチキャスト グループ 5

ネットワーク インターフェイスへの複数の IP アドレスの割り当て 10

IPv4 および IPv6 プロトコル スタックの設定 11

アンナンバード インターフェイス上での IPv4 処理のイネーブル化 13

IPv4 ICMP レート制限 14

IPv6 ICMP レート制限 16

柔軟な送信元 IP の選択 17

IPARM 競合解決の設定 17

静的ポリシー解決 17

最長プレフィックス アドレス競合解決 18

最大 IP アドレス競合解決 19

接続ルートに対する Route-Tag のサポート 19

拡大された IPv6 アドレス空間 20

IPv6 アドレス形式 21

IPv6 アドレス タイプ : ユニキャスト 22

集約可能グローバル アドレス 22

| | |
|----------------------------|----|
| リンクローカル アドレス | 24 |
| IPv4 互換 IPv6 アドレス | 25 |
| 簡易 IPv6 パケット ヘッダー | 25 |
| IPv6 のパス MTU ディスカバリ | 29 |
| IPv6 ネイバー探索 | 29 |
| IPv6 ネイバー送信要求メッセージ | 29 |
| IPv6 ルータ アドバタイズメント メッセージ | 32 |
| IPv6 ネイバー リダイレクト メッセージ | 33 |
| Address Repository Manager | 34 |
| アドレス競合解決 | 34 |

第 2 章

ARP の設定 37

| | |
|---------------------------|----|
| ARP の設定 | 37 |
| ARP キャッシュ エントリ | 38 |
| スタティック ARP キャッシュ エントリの定義 | 38 |
| プロキシ ARP とローカル プロキシ ARP | 38 |
| プロキシ ARP のイネーブル化 | 39 |
| ローカル プロキシ ARP のイネーブル化 | 40 |
| ローカル ARP エントリの学習の設定 | 41 |
| ARP の設定に関する情報 | 42 |
| アドレス解決の概要 | 42 |
| 単一の LAN でのアドレス解決 | 43 |
| ルータによって相互接続されている場合のアドレス解決 | 43 |

第 3 章

シスコ エクスプレス フォワーディングの実装 45

| | |
|------------------------------|----|
| シスコ エクスプレス フォワーディングの実装 | 45 |
| CEF の確認 | 46 |
| フロー単位ロード バランシング | 48 |
| スタティック ルートの設定 | 49 |
| BGP 属性ダウンロード | 52 |
| プロアクティブなアドレス解決プロトコルおよびネイバー探索 | 53 |

第 4 章

ホスト サービスとアプリケーションの実装 55

ホスト サービスとアプリケーションの実装 55

ネットワーク接続性ツール 55

ping 55

ネットワーク接続の確認 56

複数の宛先に対するネットワーク接続性のチェック 57

traceroute 58

パケット ルートのチェック 59

ドメイン サービス 60

ドメイン サービスの設定 60

TFTP サーバ 61

TFTP サーバとしてのルータの設定 61

ファイル転送サービス 62

FTP 63

FTP 接続使用時のルータ設定 63

TFTP 64

TFTP 接続使用時のルータ設定 64

SCP 64

SCP によるファイル転送 65

Cisco inetd 65

Telnet 65

Syslog の送信元インターフェイス 66

第 5 章

ダイナミック ホスト コンフィギュレーション プロトコルの実装 67

回線 ID およびリモート ID を持つ DHCP Option-82 67

DHCP リレー エージェントの設定の前提条件 68

DHCP リレー機能の制限事項 68

DHCP リレー エージェントを設定およびイネーブルにする方法 69

DHCP リレー エージェントの設定およびイネーブル化 69

DHCP リレー Option-82 の設定およびイネーブル化 70

インターフェイスでの DHCPv6 リレー エージェントのイネーブル化 71

| | |
|---|----|
| インターフェイスでの DHCP リレーのディセーブル化 | 72 |
| VRF での DHCP リレーのイネーブル化 | 72 |
| 複数のヘルパー アドレスを使用した DHCP リレー プロファイルの設定 | 72 |
| プレフィックス委任の DHCP リレー エージェント通知 | 73 |
| プレフィックス委任のための DHCP ステートフル リレー エージェントの設定 | 74 |
| IANA アドレス割り当てのための BVI を介した DHCPv6 リレー | 74 |
| DHCP リレー プロファイル：例 | 78 |
| インターフェイス上の DHCP リレー：例 | 78 |
| VRF 上の DHCP リレー：例 | 78 |
| リレー エージェント情報オプションのサポート：例 | 78 |
| リレー エージェント giaddr ポリシー：例 | 79 |
| DHCP プロキシ プロファイルの設定 | 79 |
| DHCP サーバ | 79 |
| DHCP サーバ プロファイルの設定 | 80 |
| プールを使用した複数のクラスの設定 | 81 |
| クラス一致オプションを使用したサーバ プロファイル DAP の設定 | 81 |
| DAP プール一致オプションを使用しないサーバ プロファイルの設定 | 83 |
| DAP での ISP ごとのアドレス プール設定 | 83 |
| DHCP クライアント | 84 |
| インターフェイスでの DHCP クライアントのイネーブル化 | 85 |
| DHCPv6 プロキシ バインディング テーブルのリロード永続性 | 85 |
| システム永続メモリへの DHCP リレー バインディング データベースの書き込みの設定 | 85 |

DHCP リレーの概要 87

| | |
|-------------------------------------|----|
| 回線 ID およびリモート ID を持つ DHCP Option-82 | 88 |
| DHCP リレー エージェントの設定の前提条件 | 89 |
| DHCP リレー機能の制限事項 | 89 |
| DHCP リレー エージェントを設定およびイネーブルにする方法 | 90 |
| DHCP リレー エージェントの設定およびイネーブル化 | 90 |
| DHCP リレー Option-82 の設定およびイネーブル化 | 91 |

| | |
|---|-----|
| インターフェイスでの DHCPv6 リレー エージェントのイネーブル化 | 92 |
| インターフェイスでの DHCP リレーのディセーブル化 | 93 |
| VRF での DHCP リレーのイネーブル化 | 93 |
| 複数のヘルパー アドレスを使用した DHCP リレー プロファイルの設定 | 93 |
| プレフィックス委任の DHCP リレー エージェント通知 | 94 |
| プレフィックス委任のための DHCP ステートフル リレー エージェントの設定 | 95 |
| IANA アドレス割り当てのための BVI を介した DHCPv6 リレー | 95 |
| DHCP リレー プロファイル：例 | 99 |
| インターフェイス上の DHCP リレー：例 | 99 |
| VRF 上の DHCP リレー：例 | 99 |
| リレー エージェント情報オプションのサポート：例 | 99 |
| リレー エージェント giaddr ポリシー：例 | 100 |
| DHCP プロキシ プロファイルの設定 | 100 |
| DHCP サーバ | 100 |
| DHCP サーバ プロファイルの設定 | 101 |
| プールを使用した複数のクラスの設定 | 102 |
| クラス一致オプションを使用したサーバ プロファイル DAP の設定 | 102 |
| DAP プール一致オプションを使用しないサーバ プロファイルの設定 | 104 |
| DAP での ISP ごとのアドレス プール設定 | 104 |
| DHCP クライアント | 105 |
| インターフェイスでの DHCP クライアントのイネーブル化 | 106 |
| DHCPv6 プロキシ バインディング テーブルのリロード永続性 | 106 |
| システム永続メモリへの DHCP リレー バインディング データベースの書き込みの設定 | 106 |

第 7 章

| | |
|---------------------------|-----|
| アクセス リストおよびプレフィックス リストの実装 | 109 |
| アクセス リストの概要 | 109 |
| IPv4 ACL の設定 | 113 |
| IPv6 ACL の設定 | 116 |
| ACL の変更 | 121 |
| ACL ベースの転送の設定 | 122 |

| | |
|--|-----|
| ブリッジ仮想インターフェイスの ACL | 125 |
| フラグメント制御を使用した ACL の設定 | 128 |
| フラグメント タイプでの照合を実行するための IPv4 ACL の設定 | 130 |
| ACL でのフラグメント オフセットによる一致 | 131 |
| フラグメント オフセットによる ACL 照合の設定 | 132 |
| IP パケット長による ACL フィルタリングの設定 | 133 |
| パケット長を使用してフィルタリングするためのシンプルな IPv4 ACL の設定 | 134 |
| パケット長を使用してフィルタリングするための拡張 IPv4 ACL の設定 | 135 |
| パケット長を使用してフィルタリングするための拡張 IPv6 ACL の設定 | 136 |
| オブジェクトグループ ACL の概要 | 137 |
| オブジェクトグループ ACL の設定 | 138 |
| ネットワーク オブジェクトグループ ACL の設定 | 139 |
| ポート オブジェクトグループ ACL の設定 | 140 |
| IPv4 ACL での TTL の照合および書き換えの設定 | 141 |
| IPv6 ACL での TTL の照合および書き換えの設定 | 143 |
| IP アクセス リスト ロギング メッセージの概要 | 144 |
| プレフィックス リストの概要 | 145 |
| プレフィックス リストの設定 | 146 |
| プレフィックス リスト エントリの順序付けとプレフィックス リストの変更 | 147 |

第 8 章

| | |
|-------------------|------------|
| HSRP の実装 | 149 |
| HSRP の実装の前提条件 | 149 |
| HSRP の実装の制約事項 | 149 |
| HSRP の実装に関する情報 | 150 |
| HSRP の概要 | 150 |
| HSRP グループ | 150 |
| HSRP と ARP | 153 |
| プリエンブション | 153 |
| ICMP リダイレクト メッセージ | 153 |
| HSRP の実装方法 | 154 |
| HSRP のイネーブル化 | 154 |

| | |
|-------------------------------------|-----|
| IPv6 の HSRP のイネーブル化 | 155 |
| HSRP グループの属性の設定 | 156 |
| HSRP アクティベーション遅延の設定 | 159 |
| ICMP リダイレクトメッセージの HSRP サポートのディセーブル化 | 160 |
| HSRP のマルチ グループ オプティマイゼーション (MGO) | 162 |
| HSRP のカスタマイズ | 162 |
| プライマリ仮想 IPv4 アドレスの設定 | 164 |
| セカンダリ仮想 IPv4 アドレスの設定 | 165 |
| スレーブ フォローの設定 | 166 |
| スレーブ プライマリ仮想 IPv4 アドレスの設定 | 167 |
| スレーブグループ用セカンダリ仮想 IPv4 アドレスの設定 | 167 |
| スレーブ仮想 MAC アドレスの設定 | 168 |
| HSRP セッション名の設定 | 169 |
| HSRP および IP スタティックの拡張オブジェクト トラッキング | 170 |
| HSRP 用のオブジェクト トラッキングの設定 | 170 |
| HSRP のホット リスタート | 171 |
| ソフトウェアでの HSRP の実装の設定例 | 171 |
| HSRP グループの設定：例 | 171 |
| 複数の HSRP グループ用のルータの設定：例 | 172 |

第 9 章

LPTS の実装 173

| | |
|--|-----|
| LPTS の概要 | 173 |
| LPTS ポリサー | 173 |
| マルチキャストおよびブロードキャストのパントされたパケットにおけるポートごとのレート制限 | 178 |
| マルチキャストおよびブロードキャストのパントされたトラフィックに対するレート制限の設定 | 178 |
| ドメインベースの LPTS ポリサー | 186 |
| ダイナミック LPTS フロー タイプの定義 | 187 |

第 10 章

VRRP の実装 191

| | |
|---------------------------------------|-----|
| VRRP の設定 | 191 |
| VRRP のカスタマイズ | 191 |
| VRRP のイネーブル化 | 193 |
| グローバル仮想 IPv6 アドレスの設定 | 194 |
| プライマリおよびセカンダリの仮想 IPv4 アドレスの設定 | 194 |
| 仮想リンクローカル IPv6 アドレスの設定 | 195 |
| 状態変更ロギングのディセーブル化 | 196 |
| VRRP のマルチ グループ オプティマイゼーション (MGO) の有効化 | 197 |
| VRRP イベントに関する SNMP サーバ通知の設定 | 198 |
| VRRP の概要 | 199 |

第 11 章

| | |
|--------------------------------|-----|
| TCP 転送、UDP 転送の設定に関する情報 | 203 |
| グレースフル リスタート | 203 |
| TCP の概要 | 204 |
| UDP の概要 | 204 |
| NSR のリカバリ アクションとしてのフェールオーバーの設定 | 204 |



第 1 章

ネットワーク スタック IPv4 および IPv6 の実装

ネットワーク スタック IPv4 および IPv6 機能は、インターネット プロトコル バージョン 4 (IPv4) およびインターネット プロトコルバージョン 6 (IPv6) の設定とモニタリングに使用します。

制約事項

IPv6 に対応している Cisco IOS XR ソフトウェア リリースでは、1 つのインターフェイス上に複数の IPv6 グローバル アドレスを設定できます。ただし、1 つのインターフェイス上での複数の IPv6 リンクローカル アドレスはサポートされません。

- [フォールバック VRF の実装 \(1 ページ\)](#)
- [ネットワーク スタック IPv4 および IPv6 の例外 \(2 ページ\)](#)
- [IPv4 および IPv6 機能 \(3 ページ\)](#)
- [Cisco IOS XR ソフトウェアの IPv6, on page 3](#)
- [ネットワーク スタック IPv4 および IPv6 の実装方法, on page 3](#)

フォールバック VRF の実装

仮想ルーティングおよびフォワーディング (VRF) は、同じルータ上にルーティング テーブルの複数のインスタンスが同時に存在できるようにする IP テクノロジーです。ルーティング インスタンスは独立しているため、同じ IP アドレスを競合することなく使用できます。

データ パケットの宛先プレフィックスが、設定されている VRF のどのルートとも一致しない場合、グローバル ルーティング テーブルからデフォルト ルートが識別されます。ただし、デフォルト ルートを使用するには明示的なネクスト ホップが必要なため、効率的でない可能性があります。フォールバック VRF ルートを設定することをお勧めします。宛先が VRF テーブルで一致しない場合は、フォールバック VRF テーブルが使用されます。フォールバック VRF には、グローバル ルーティング テーブルまたは非グローバル VRF テーブルを使用できます。

制約事項

フォールバック VRF ルートを設定する場合は、次の制約事項が適用されます。

- フォールバック VRF ルートは、各プライマリ VRF のアドレス ファミリーごとに 1 つのみ設定できます。
- LPTS 受信トラップはサポート対象外であるため、ping、トレースルート、または低速パス アプリケーションはフォールバック VRF でサポートされません。
- Cisco NCS 560 シリーズ ルータでは、1000 の VRF と 1 つのグローバル テーブルのみがサポートされます。
- VRF へのスタティック デフォルト ルートを設定すると、このスタティック デフォルト ルートがフォールバック VRF よりも優先されます。VRF のデフォルト ルートを設定すると、ルート ルックアップにグローバル ルーティング テーブルが使用されます。デフォルト ルートは、設定済みのネクスト ホップに必ず転送されます。
- プライマリ VRF でパケットのルート ルックアップが失敗した場合、フォールバック VRF でルートルックアップを実行するためにパケットがリサイクルされます。したがって、パケットのルーティング パフォーマンスが最大で 50% 低下します。
- パケットの ACL ベース転送 (ABF) VRF リダイレクトと VRF フォールバックの両方を設定すると、パケットは 2 回リサイクルされます。したがって、パケットのルーティング パフォーマンスが最大で 33% 低下します。
- フォールバック VRF でパケットのルートが見つかった場合、グリーンング IPv4 およびグリーンング IPv6 隣接関係パケットのみが正常にパントされます。
- ループ設定では、パケットのルートがプライマリとフォールバックのどちらの VRF でも見つからない場合、パケットはリサイクルパスでループします。最終的にパケットはリサイクル出力キューにドロップされます。リサイクル キューの優先順位が最も高いため、ループしているトラフィックのレートが高いと、他の正常なリサイクルパケットがドロップされる可能性があります。

ネットワーク スタック IPv4 および IPv6 の例外

Cisco IOS XR ソフトウェアでのネットワーク スタック機能には、次の例外があります。

- Cisco IOS XR ソフトウェアでは、**clear ipv6 neighbors** および **show ipv6 neighbors** コマンドに **location node-id** キーワードが含まれています。場所を指定した場合、指定した場所の隣接エントリのみが表示されます。
- **ipv6 nd scavenge-timeout** コマンドは、stale 状態の隣接エントリの有効期間を設定します。隣接エントリの廃棄タイマーの有効期間が切れると、そのエントリはクリアされます。
- Cisco IOS XR ソフトウェアでは、**show ipv4 interface** および **show ipv6 interface** コマンドに **location node-id** キーワードが含まれています。場所を指定した場合、指定した場所のインターフェイス エントリのみが表示されます。
- Cisco IOS XR ソフトウェアでは、設定時に、競合する IP アドレス エントリが許可されます。アクティブな 2 つのインターフェイスの間に IP アドレス競合が存在する場合、Cisco

IOS XR ソフトウェアは、設定されている競合ポリシーに従って、インターフェイスを停止します（デフォルト ポリシーでは、より高いインターフェイス インスタンスを停止します）。

IPv4 および IPv6 機能

Cisco IOS XR ソフトウェアが IPv4 と IPv6 の両方のアドレスを使用して設定されている場合、インターフェイスは IPv4 と IPv6 の両方のネットワーク上のデータを送受信できます。

IPv6 のアーキテクチャは、エンドツーエンドのセキュリティ、Quality of Service (QoS)、グローバルに一意なアドレスなどのサービスを提供する一方で、既存の IPv4 ユーザが IPv6 に簡単に移行できるように設計されています。拡大された IPv6 アドレス空間により、ネットワークのスケーラビリティが可能となり、グローバルな到達可能性が提供されます。簡素化された IPv6 パケット ヘッダー形式により、パケットの処理効率が向上しています。IPv6 プレフィックス集約、簡略化されたネットワーク リナサンバリング、および IPv6 サイト マルチホーミング機能によって、より効率的なルーティングを実現する IPv6 アドレッシング階層が提供されます。IPv6 は、Open Shortest Path First (OSPF) やマルチプロトコル ボーダー ゲートウェイ プロトコル (BGP) など、広く導入されているルーティング プロトコルをサポートしています。

IPv6 ネイバー探索 (nd) プロセスでは、インターネット制御メッセージ プロトコル (ICMP) および送信要求 ノード マルチキャスト アドレスを使用して、同じネットワーク（ローカル リンク）上のネイバーのリンク層アドレスを判断し、ネイバーに到達可能かどうかを確認し、隣接ルータを追跡します。

Cisco IOS XR ソフトウェアの IPv6

以前は IPng（次世代）と呼ばれていた IPv6 は、インターネット プロトコル (IP) の最新バージョンです。IP は、デジタル ネットワーク上のデータ、音声、およびビデオ トラフィックの交換に使用されるパケットベースのプロトコルです。IP バージョン 4 (IPv4) の 32 ビット アドレッシング方式ではインターネットの成長の需要を十分に満たせないことが明らかになったときに、IPv6 が提案されました。長い議論の後で、IP を IPng のベースにするが、はるかに大きなアドレス空間と、簡略化されたメインヘッダーや拡張ヘッダーなどの改善を追加することが決定されました。IPv6 は、Internet Engineering Task Force (IETF) から発行されている RFC 2460、『*Internet Protocol, Version 6 (IPv6) Specification*』で最初に規定されました。IPv6 でサポートされるアーキテクチャとサービスについては他の RFC で規定されています。

ネットワーク スタック IPv4 および IPv6 の実装方法

ここでは、次の手順について説明します。

IPv4 アドレス指定の設定

IP を設定するための基本的かつ必須のタスクは、IPv4 アドレスをネットワーク インターフェイスに割り当てることです。こうすることで、インターフェイスがイネーブルになり、IPv4 を使用するこれらのインターフェイスでホストとの通信が可能になります。IP アドレスは IP データグラムの送信先を特定します。インターフェイスには、1つのプライマリ IP アドレスと複数のセカンダリアドレスを設定できます。ソフトウェアにより生成されるパケットは、必ずプライマリ IPv4 アドレスを使用します。そのため、セグメントのすべてのネットワーキング デバイスは、同じプライマリ ネットワーク番号を共有する必要があります。

このタスクに関連付けられているのは、IP アドレスのサブネット化およびマスキングに関する決定です。マスクで、IP アドレス中のネットワーク番号を示すビットが識別できます。マスクを使用してネットワークをサブネット化した場合、そのマスクはサブネットマスクと呼ばれます。



- (注) シスコでは、ネットワーク フィールドに対して左寄せの連続ビットを使用するネットワーク マスクのみをサポートしています。

設定例

IPv4 アドレス 192.168.1.27 とネットワーク マスク 「/8」 が、インターフェイス **HundredGigE 0/9/0/1** に割り当てられます。



- (注) 4分割ドット付き 10進表記のアドレスでネットワーク マスクを指定します。たとえば、255.0.0.0 は、1に等しい各ビットが、ネットワーク アドレスに属した対応するアドレス ビットを意味することを示します。ネットワーク マスクは、スラッシュ (/) および数字、つまり、プレフィックス長として示される場合もあります。プレフィックス長は、アドレスの高次の連続ビットのうち、何個がプレフィックス（アドレスのネットワーク部分）を構成しているかを指定する 10進数値です。スラッシュは 10進数値の前に置かれ、IP アドレスとスラッシュの間にスペースは入りません。

```
Router#configure HundredGigE0/9/0/1
Router(config)#interface HundredGigE 0/9/0/1
Router(config-if)#ipv4 address 192.168.1.27/8
Router(config-if)#commit
```

実行コンフィギュレーション

```
Router#show running-config interface HundredGigE0/9/0/1
interface HundredGigE0/9/0/1
  ipv4 address 192.168.1.27 255.0.0.0
!
```

確認

HundredGigE インターフェイスがアクティブであり、IPv4 がイネーブルであることを確認します。

```
Router# show ipv4 interface HundredGigE0/9/0/1
interface HundredGigE0/9/0/1 is Up, ipv4 protocol is Up
Vrf is default (vrfid 0x60000000)
Internet address is 192.168.1.27/8
MTU is 1514 (1500 is available to IP)
Helper address is not set
Multicast reserved groups joined: 224.0.0.2 224.0.0.1
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is disabled
ICMP redirects are never sent
ICMP unreachable are always sent
ICMP mask replies are never sent
Table Id is 0xe0000000
```

関連コマンド

- `ipv4 address`
- `show ipv4 interface`

IPv6 アドレッシングの設定

ルータでの IPv6 トラフィックのグローバル転送を可能にするため、IPv6 アドレスは個々のルータ インターフェイスに設定されます。デフォルトでは、IPv6 アドレスは設定されていません。



(注) **ipv6 address** コマンドの *ipv6-prefix* 引数には、RFC 2373 に記載されている形式を使用する必要があります。コロンで区切った 16 ビット値を使用して 16 進数でアドレスを指定してください。

ipv6 address コマンドの */prefix-length* 引数には、プレフィックスを構成しているアドレスの連続する上位ビットの数（アドレスのネットワーク部）を示す 10 進数の値を指定します。10 進値の前にはスラッシュが必要です。

ipv6 address link-local コマンドの *ipv6-address* 引数には、RFC 2373 に記載されている形式を使用する必要があります。コロンで区切った 16 ビット値を使用して 16 進数でアドレスを指定してください。

IPv6 マルチキャスト グループ

インターフェイスで IPv6 トラフィックを転送できるようにするには、そのインターフェイスで IPv6 アドレスを設定する必要があります。インターフェイスにグローバル IPv6 アドレスを設定すると、リンクローカルアドレスが自動的に設定され、そのインターフェイスに対して IPv6 がアクティブになります。

また、設定されたインターフェイスは、そのリンクに必要な次のマルチキャストグループに自動的に加入します。

- 送信要求ノード マルチキャスト グループ FF02:0:0:0:1:FF00::/104 (インターフェイスに割り当てられた各ユニキャスト アドレス用)
- 全ノード リンクローカル マルチキャスト グループ FF02::1
- 全ルータ リンクローカル マルチキャスト グループ FF02::2



(注) 送信要求ノード マルチキャスト アドレスは、ネイバー探索プロセスで使用されます。

設定例

IPv6 アドレス 2001:0DB8:0:1::1/64 が、インターフェイス **HundredGigE 0/9/0/1** に割り当てられます。

```
Router#configure
Router(config)#interface HundredGigE 0/9/0/1
Router(config-if)#ipv6 address 2001:0DB8:0:1::1/64
Router(config-if)#commit
```

実行コンフィギュレーション

```
Router#show running-config interface HundredGigE0/9/0/1
interface HundredGigE0/9/0/1
  ipv4 address 192.168.1.27 255.0.0.0
  ipv4 address 1.0.0.1 255.255.255.0 secondary
  ipv4 address 2.0.0.1 255.255.255.0 secondary
  ipv6 address 2001:db8:0:1::1/64
!
```

確認

HundredGigE インターフェイスがアクティブであり、IPv6 が有効であることを確認します。

```
Router#show ipv6 interface HundredGigE0/9/0/1
HundredGigE0/9/0/1 is Up, ipv6 protocol is Up, Vrfid is default (0x60000000)
  IPv6 is enabled, link-local address is fe80::c672:95ff:fea6:1c75
    Global unicast address(es):
      2001:db8:0:1::1, subnet is 2001:db8:0:1::/64
    Joined group address(es): ff02::1:ff00:1 ff02::1:ffa6:1c75 ff02::2
      ff02::1
    MTU is 1514 (1500 is available to IPv6)
    ICMP redirects are disabled
    ICMP unreachable are enabled
    ND DAD is enabled, number of DAD attempts 1
    ND reachable time is 0 milliseconds
    ND cache entry limit is 1000000000
    ND advertised retransmit interval is 0 milliseconds
    Hosts use stateless autoconfig for addresses.
    Outgoing access list is not set
    Inbound access list is not set
    Table Id is 0xe0800000
```



```
Complete protocol adjacency: 0
Complete glean adjacency: 0
Incomplete protocol adjacency: 0
Incomplete glean adjacency: 0
Dropped protocol request: 0
Dropped glean request: 0
```

関連コマンド

- ipv6 address
- interface
- show ipv6 interface

設定例

IPv6 アドレス 2001:0DB8:0:1::/64 が、**インターフェイス HundredGigE 0/9/0/1** に割り当てられます。**eui-64** キーワードを指定して、IPv6 アドレスの下位 64 ビットにインターフェイス識別子 (ID) を含むサイトローカルおよびグローバル IPv6 アドレスを設定します。指定する必要があるのはアドレスの 64 ビット ネットワーク プレフィックスだけです。最後の 64 ビットはインターフェイス ID から自動的に計算されます。

```
Router#configure
Router(config)#interface HundredGigE 0/9/0/1
Router(config-if)#ipv6 address 2001:0DB8:0:1::/64 eui-64
Router(config-if)#commit
```

実行コンフィギュレーション

```
Router#show running-config interface HundredGigE0/9/0/1
interface HundredGigE0/9/0/1
  ipv4 address 192.168.1.27 255.0.0.0
  ipv4 address 1.0.0.1 255.255.255.0 secondary
  ipv4 address 2.0.0.1 255.255.255.0 secondary
  ipv6 address 2001:db8:0:1::/64 eui-64
!
```

確認

HundredGigE インターフェイスがアクティブであり、IPv6 が有効であることを確認します。

```
Router#show ipv6 interface HundredGigE0/9/0/1
HundredGigE0/9/0/1 is Up, ipv6 protocol is Up, Vrfid is default (0x60000000)
  IPv6 is enabled, link-local address is fe80::c672:95ff:fea6:1c75
    Global unicast address(es):
      2001:db8:0:1:c672:95ff:fea6:1c75, subnet is 2001:db8:0:1::/64
    Joined group address(es): ff02::1:ffa6:1c75 ff02::2 ff02::1
    MTU is 1514 (1500 is available to IPv6)
    ICMP redirects are disabled
    ICMP unreachable are enabled
    ND DAD is enabled, number of DAD attempts 1
    ND reachable time is 0 milliseconds
    ND cache entry limit is 1000000000
    ND advertised retransmit interval is 0 milliseconds
    Hosts use stateless autoconfig for addresses.
    Outgoing access list is not set
    Inbound access list is not set
    Table Id is 0xe0800000
```

```
Complete protocol adjacency: 0
Complete glean adjacency: 0
Incomplete protocol adjacency: 0
Incomplete glean adjacency: 0
Dropped protocol request: 0
Dropped glean request: 0
```

関連コマンド

- ipv6 address
- interface
- show ipv6 interface

設定例

IPv6 アドレス FE80::260:3EFF:FE11:6770 が、インターフェイス **HundredGigE 0/9/0/1** に割り当てられます。link-local キーワードを指定して、リンクローカルアドレスをインターフェイスに設定します。このアドレスは、IPv6 がインターフェイスでイネーブルになっているときに自動的に設定されるリンクローカルアドレスの代わりに使用されます。

```
Router#configure
Router(config)#interface HundredGigE 0/9/0/1
Router(config-if)#ipv6 address FE80::260:3EFF:FE11:6770 link-local
Router(config-if)#commit
```

実行コンフィギュレーション

```
Router#show running-config interface HundredGigE0/9/0/1

interface HundredGigE0/9/0/1
  ipv6 address fe80::260:3eff:fe11:6770 link-local
!
```

確認

HundredGigE インターフェイスがアクティブであり、IPv6 がリンクローカルアドレスで有効になっていることを確認します。

```
Router#show ipv6 interface HundredGigE0/9/0/1
HundredGigE0/9/0/1 is Up, ipv6 protocol is Up, Vrfid is default (0x60000000)
  IPv6 is enabled, link-local address is fe80::260:3eff:fe11:6770
    Global unicast address(es):
      2001:db8:0:1:260:3eff:fe11:6770, subnet is 2001:db8:0:1::/64
    Joined group address(es): ff02::1:ff11:6770 ff02::2 ff02::1
    MTU is 1514 (1500 is available to IPv6)
    ICMP redirects are disabled
    ICMP unreachable are enabled
    ND DAD is enabled, number of DAD attempts 1
    ND reachable time is 0 milliseconds
    ND cache entry limit is 1000000000
    ND advertised retransmit interval is 0 milliseconds
    Hosts use stateless autoconfig for addresses.
    Outgoing access list is not set
    Inbound access list is not set
    Table Id is 0xe0800000
    Complete protocol adjacency: 0
    Complete glean adjacency: 0
```

```
Incomplete protocol adjacency: 0
Incomplete glean adjacency: 0
Dropped protocol request: 0
Dropped glean request: 0
```

関連コマンド

- `ipv6 address`
- `interface`
- `show ipv6 interface`

設定例

明示的な IPv6 アドレスが設定されていないインターフェイス **HundredGigE 0/9/0/1** での IPv6 の処理を有効にします。

```
Router#configure
Router(config)#interface HundredGigE 0/9/0/1
Router(config-if)#ipv6 enable
Router(config-if)#commit
```

実行コンフィギュレーション

```
Router#show running-config interface HundredGigE0/9/0/1
interface HundredGigE0/9/0/1
ipv6 enable
!
```

確認

HundredGigE インターフェイスがアクティブであり、IPv6 が有効であることを確認します。

```
Router#show ipv6 interface HundredGigE0/9/0/1
HundredGigE0/9/0/1 is Up, ipv6 protocol is Up, Vrfid is default (0x60000000)
IPv6 is enabled, link-local address is fe80::c672:95ff:fea6:1c75
No global unicast address is configured
Joined group address(es): ff02::1:ffa6:1c75 ff02::2 ff02::1
MTU is 1514 (1500 is available to IPv6)
ICMP redirects are disabled
ICMP unreachable are enabled
ND DAD is enabled, number of DAD attempts 1
ND reachable time is 0 milliseconds
ND cache entry limit is 1000000000
ND advertised retransmit interval is 0 milliseconds
Hosts use stateless autoconfig for addresses.
Outgoing access list is not set
Inbound access list is not set
Table Id is 0xe0800000
Complete protocol adjacency: 0
Complete glean adjacency: 0
Incomplete protocol adjacency: 0
Incomplete glean adjacency: 0
Dropped protocol request: 0
Dropped glean request: 0
```

関連コマンド

- ipv6 enable
- interface
- show ipv6 interface

ネットワーク インターフェイスへの複数の IP アドレスの割り当て

Cisco IOS XR ソフトウェアは、インターフェイスごとに複数の IP アドレス（セカンダリ アドレス）をサポートしています。セカンダリ アドレスは無制限に指定できます。セカンダリ IP アドレスは、さまざまな状況で使用できます。次に、一般的な使用状況を示します。

- 特定のネットワーク セグメントに十分なホスト アドレスがない場合があります。たとえば、サブネット化により、論理サブネットあたり最大 254 のホストを使用できますが、1 つの物理サブネットでは、300 のホスト アドレスが必要になるとします。ルータまたはアクセス サーバでセカンダリ IP アドレスを使用すると、2 つの論理サブネットで 1 つの物理サブネットを使用できます。
- 多くの旧式ネットワークは、レベル 2 ブリッジを使用して構築され、サブネット化されませんでした。セカンダリ アドレスは、慎重に使用することで、サブネット化されたルータベース ネットワークへの移行に役立ちます。旧式のブリッジ セグメントのルータで、そのセグメントに複数のサブネットがあることを簡単に認識されるようにできます。
- 1 つのネットワークの 2 つのサブネットは、別の方法で、別のネットワークにより分離できる場合があります。別のネットワークによって物理的に分離された複数のサブネットから、セカンダリ アドレスを使用して、1 つのネットワークを作成できます。このような場合、最初のネットワークは、2 番めのネットワークの上に拡張されます。つまり、上の階層となります。サブネットは、同時に複数のアクティブなインターフェイス上に表示できないことに注意してください。



(注) ネットワーク セグメント上の任意のルータがセカンダリ IPv4 アドレスを使用した場合、同一のセグメント上にある他のルータもすべて、同一のネットワークまたはサブネットからセカンダリ アドレスを使用する必要があります。



注意 ネットワーク セグメント上のセカンダリ アドレスの使用に矛盾があると、ただちにルーティンググループが引き起こされる可能性があります。

設定例

セカンダリ IPv4 アドレス 192.168.1.27 が Hundredgige インターフェイス 0/0/0/1 に割り当てられます。

注：IPv6 の場合は、**secondary** キーワードを指定せずに、インターフェイスに複数の IPv6 アドレスを設定できます。

```
Router# configure
Router(config)# interface HundredGigE 0/9/0/1
Router(config-if)# ipv4 address 192.168.1.27 255.255.255.0 secondary
Router(config-if)#commit
```

実行コンフィギュレーション

```
Router#show running-config interface HundredGigE0/9/0/1
```

```
interface HundredGigE0/9/0/1
  ipv4 address 192.168.1.27 255.255.255.0 secondary
!
```

確認

```
Router#show ipv4 interface HundredGigE0/9/0/1
HundredGigE0/9/0/1 is Up, ipv4 protocol is Up
  Vrf is default (vrfid 0x60000000)
  Internet address is unassigned
  Secondary address 192.168.1.27/24
  MTU is 1514 (1500 is available to IP)
  Helper address is not set
  Multicast reserved groups joined: 224.0.0.2 224.0.0.1
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is disabled
  ICMP redirects are never sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  Table Id is 0xe0000000
```

関連コマンド

- ipv4 address
- show ipv4 interface

IPv4 および IPv6 プロトコル スタックの設定

このタスクでは、IPv4 と IPv6 の両方のプロトコル スタックをサポートするようにシスコのネットワーク デバイスのインターフェイスを設定します。

シスコのネットワーク デバイスのインターフェイスが IPv4 アドレスと IPv6 アドレスの両方で設定されている場合、インターフェイスは IPv4 トラフィックと IPv6 トラフィックの両方を転送します。インターフェイスは、IPv4 ネットワークと IPv6 ネットワークの両方でデータを送受信できます。

設定例

インターフェイス **HundredGigE 0/9/0/1** に IPv4 アドレス 192.168.99.1 と IPv6 アドレス 2001:0DB8:c18:1::3/64 を設定します。

```
Router#configure
Router(config)#interface HundredGigE 0/9/0/1
Router(config-if)#ipv4 address 192.168.99.1 255.255.255.0
Router(config-if)#ipv6 address 2001:0DB8:c18:1::3/64
Router(config-if)#commit
```

実行コンフィギュレーション

```
Router# show running-config interface HundredGigE0/9/0/1
interface HundredGigE0/9/0/1
  ipv4 address 192.168.99.1 255.255.255.0
  ipv6 address 2001:db8:c18:1::3/64
!
```

確認

HundredGigE インターフェイスがアクティブであり、IPv4 と IPv6 が有効になっていることを確認します。

```
Router#show ipv4 interface HundredGigE0/9/0/1
HundredGigE0/9/0/1 is Up, ipv4 protocol is Up
  Vrf is default (vrfid 0x60000000)
  Internet address is 192.168.99.1/24
  MTU is 1514 (1500 is available to IP)
  Helper address is not set
  Multicast reserved groups joined: 224.0.0.2 224.0.0.1
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is disabled
  ICMP redirects are never sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  Table Id is 0xe0000000

Router#show ipv6 interface HundredGigE0/9/0/1
HundredGigE0/9/0/1 is Up, ipv6 protocol is Up, Vrfid is default (0x60000000)
  IPv6 is enabled, link-local address is fe80::c672:95ff:fea6:1c75
  Global unicast address(es):
    2001:db8:c18:1::3, subnet is 2001:db8:c18:1::/64
  Joined group address(es): ff02::1:ff00:3 ff02::1:ffa6:1c75 ff02::2
    ff02::1
  MTU is 1514 (1500 is available to IPv6)
  ICMP redirects are disabled
  ICMP unreachable are enabled
  ND DAD is enabled, number of DAD attempts 1
  ND reachable time is 0 milliseconds
  ND cache entry limit is 1000000000
  ND advertised retransmit interval is 0 milliseconds
  Hosts use stateless autoconfig for addresses.
  Outgoing access list is not set
  Inbound access list is not set
  Table Id is 0xe0800000
  Complete protocol adjacency: 0
  Complete glean adjacency: 0
  Incomplete protocol adjacency: 0
  Incomplete glean adjacency: 0
  Dropped protocol request: 0
  Dropped glean request: 0
```

関連コマンド

- `ipv4 address`
- `ipv6 address`
- `show ipv4 interface`
- `show ipv6 interface`

アンナンバード インターフェイス上での IPv4 処理のイネーブル化

ここでは、明示的な IP アドレスをインターフェイスに割り当てることなく、IPv4 ポイントツーポイント インターフェイスをイネーブルにするプロセスについて説明します。アンナンバード インターフェイスがパケットを生成する場合（たとえば、ルーティング アップデートのため）は必ず、IP パケットの送信元アドレスとして指定したインターフェイスのアドレスが使用されます。また、アンナンバード インターフェイスを介してアップデートを送信するルーティング プロセスを判別する場合、指定されたインターフェイスのアドレスが使用されます。その制限を次に示します。

- High-Level Data Link Control (HDLC)、PPP、およびフレーム リレーのカプセル化を使用するインターフェイスには、アンナンバードを設定できます。フレーム リレー カプセル化を使用するシリアル インターフェイスにもアンナンバードを設定できますが、そのインターフェイスはポイントツーポイント サブインターフェイスでなければなりません。
- インターフェイスには IP アドレスがないため、`ping EXEC` コマンドを使用してインターフェイスがアップ状態かどうかを確認することはできません。簡易ネットワーク管理プロトコル (SNMP) は、インターフェイス ステータスのリモートでのモニタリングに使用できます。
- IP セキュリティ オプションは、アンナンバード インターフェイス上でサポートできません。

Intermediate System-to-Intermediate System (IS-IS) をシリアル回線全体で設定する場合、シリアル インターフェイスをアンナンバードとして設定し、それにより、各インターフェイス上で IP アドレスは必須ではないことを規定している RFC 1195 に準拠することができます。

設定例

明示的な IP アドレスを割り当てることなく、IPv4 ポイントツーポイント インターフェイスをイネーブルにします。

```
Router#configure
Router(config)#interface HundredGigE 0/9/0/1
Router(config-if)#ipv4 unnumbered loopback 0
Router(config-if)#commit
```

実行コンフィギュレーション

```
Router#show running-config interface HundredGigE0/9/0/1
interface HundredGigE0/9/0/1
  ipv4 point-to-point
```

```
ipv4 unnumbered Loopback0
!
```

確認

```
Router#show interface HundredGigE0/9/0/1
HundredGigE0/9/0/1 is up, line protocol is up
  Interface state transitions: 5
  Hardware is HundredGige, address is 00e2.2a33.445b (bia 00e2.2a33.445b)
  Layer 1 Transport Mode is LAN
  Internet address is 10.0.0.2/32
  MTU 1514 bytes, BW 10000000 Kbit (Max: 10000000 Kbit)
    reliability 255/255, txload 194/255, rxload 0/255
  Encapsulation ARPA,
  Full-duplex, 10000Mb/s, link type is force-up
  output flow control is off, input flow control is off
  Carrier delay (up) is 10 msec
  loopback not set,
  Last link flapped 01:38:49
  ARP type ARPA, ARP timeout 04:00:00
  Last input 00:00:00, output 00:00:00
  Last clearing of "show interface" counters 02:34:16
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 7647051000 bits/sec, 12254894 packets/sec
    1061401410 packets input, 82789675614 bytes, 0 total input drops
    0 drops for unrecognized upper-level protocol
    Received 5 broadcast packets, 19429 multicast packets
      0 runts, 0 giants, 0 throttles, 0 parity
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    76895885948 packets output, 6192569128048 bytes, 0 total output drops
    Output 7 broadcast packets, 18916 multicast packets
    0 output errors, 0 underruns, 0 applique, 0 resets
    0 output buffer failures, 0 output buffers swapped out
    2 carrier transitions
```

```
Router #show run int lo 0
interface Loopback0
  ipv4 address 10.0.0.2 255.255.255.255
```

関連コマンド

- ipv4 unnumbered
- show interfaces

IPv4 ICMP レート制限

IPv4 ICMP レート制限機能では、IPv4 ICMP 宛先到達不能メッセージが生成されるレートを制限します。Cisco IOS XR ソフトウェアは、通常の宛先到達不能メッセージ用と DF 宛先到達不能メッセージ用の2つのタイマーを保守します。これらは同じ時間制限およびデフォルトを共有します。DF キーワードが設定されていない場合、icmp ipv4 rate-limit unreachable コマンドによって DF 宛先到達不能メッセージの時間値が設定されます。DF キーワードが設定されている場合、その時間値は、通常の宛先到達不能メッセージの時間値とは無関係のままになります。

設定例

IPv4 ICMP 宛先到達不能メッセージが 1,000 ミリ秒ごとに生成されるレートを制限します。

DF キーワードは、コード 4 フラグメンテーションが必要で、Don't Fragment (DF) が設定されているときに ICMP 宛先到達不能メッセージの IP ヘッダーに指定されているように ICMP 宛先到達不能メッセージを送信するレートを任意で制限します。

```
Router#configure
Router(config)#icmp ipv4 rate-limit unreachable 1000
Router(config)#icmp ipv4 rate-limit unreachable DF 1000
Router(config)#commit
```

実行コンフィギュレーション

```
Router#show running-config | in icmp
Building configuration...
icmp ipv4 rate-limit unreachable DF 1000
icmp ipv4 rate-limit unreachable 1000
```

確認

```
Router#show ipv4 interface HundredGigE0/9/0/1
HundredGigE0/9/0/1 is Up, ipv4 protocol is Up
  Vrf is default (vrfid 0x60000000)
  Internet address is 192.85.1.1/24
  MTU is 1514 (1500 is available to IP)
  Helper address is not set
  Multicast reserved groups joined: 224.0.0.2 224.0.0.1 224.0.0.2
    224.0.0.5 224.0.0.6
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound common access list is not set, access list is not set
  Proxy ARP is disabled
  ICMP redirects are never sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  Table Id is 0xe0000000
```

送信または受信する ICMP 到達不能メッセージの数は、**show ipv4 traffic** コマンドを使用して指定できます。

```
Router# show ipv4 traffic
ICMP statistics:
  Sent: 0 admin unreachable, 5 network unreachable
        0 host unreachable, 0 protocol unreachable
        0 port unreachable, 0 fragment unreachable
        0 time to live exceeded, 0 reassembly ttl exceeded
        0 echo request, 0 echo reply
        0 mask request, 0 mask reply
        0 parameter error, 0 redirects
        5 total
  Rcvd: 0 admin unreachable, 0 network unreachable
        0 host unreachable, 0 protocol unreachable
        0 port unreachable, 0 fragment unreachable
        0 time to live exceeded, 0 reassembly ttl exceeded
        0 echo request, 0 echo reply
        0 mask request, 0 mask reply
        0 redirect, 0 parameter error
        0 source quench, 0 timestamp, 0 timestamp reply
        0 router advertisement, 0 router solicitation
        0 total, 0 checksum errors, 0 unknown
```

関連コマンド

- icmp ipv4 rate-limit unreachable
- show ipv4 traffic

IPv6 ICMP レート制限

IPv6 ICMP レート制限機能によって、IPv6 ICMP エラー メッセージがネットワークへ送信されるレートを制限するためのトークン バケット アルゴリズムが実装されます。IPv6 ICMP レート制限の初期の実装では、エラー メッセージ間に固定の間隔が定義されていましたが、tracertなどの一部のアプリケーションでは、間断なく送信される要求のグループへの返信が必要になる場合があります。エラー メッセージ間の固定間隔は、tracertなどのアプリケーションで動作するのに十分な柔軟性がなく、アプリケーションが失敗する原因となることがあります。トークンバケット方式を実装すると、複数のトークンを仮想バケットに格納できます。トークンごとに1つのエラー メッセージを送信できます。バケットに格納できるトークンの最大数を指定でき、エラー メッセージが送信されるたびに1つのトークンがバケットから削除されます。一連のエラー メッセージが生成された場合は、バケットが空になるまでエラー メッセージを送信できます。トークンのバケットが空になると、新しいトークンがバケットに配置されるまで、IPv6 ICMP エラー メッセージは送信されません。トークンバケットアルゴリズムは、レート制限の平均時間間隔を増やさず、固定時間間隔方式よりも柔軟性が高くなります。

設定例

50 ミリ秒の間隔と、20 トークンのバケット サイズを IPv6 ICMP エラー メッセージに設定します。

- milliseconds 引数では、トークンがバケットに追加される間隔を指定します。
- オプションの bucketsize 引数では、バケットに格納されるトークンの最大数を定義します。

```
Router#configure
Router(config)#ipv6 icmp error-interval 50 20
Router(config)#commit
```

実行コンフィギュレーション

```
Router#show running-config
Building configuration...
!! IOS XR Configuration version = 6.0.0.26I
!! Last configuration change at Mon Dec 14 22:07:35 2015 by root
!
hostname test-83
logging console debugging
username root
  group root-lr
  group cisco-support
  secret 5 $1$d2NC$RbAdqdU7kw/kEJoMP/IJG1
!
cdp
ipv6 icmp error-interval 50 20
icmp ipv4 rate-limit unreachable DF 1000
```

```
icmp ipv4 rate-limit unreachable 1000  
ipv4 conflict-policy static
```

関連コマンド

- ipv6 icmp error-interval

柔軟な送信元 IP の選択

障害に応答する Internet Control Message Protocol (ICMP) 応答パケットで柔軟な送信元 IP アドレスを選択できます。

設定例

送信元アドレスの選択に関する RFC コンプライアンスをイネーブルにします。

```
Router#configure  
Router(config)#icmp ipv4 source rfc  
Router(config)#commit
```

実行コンフィギュレーション

```
Router#show running-config | in source rfc  
Building configuration...  
icmp ipv4 source rfc
```

関連コマンド

IPARM 競合解決の設定

このタスクでは、IP Address Repository Manager (IPARM) アドレス競合解決のパラメータを設定します。

- 静的ポリシー解決
- 最長プレフィックス アドレス競合解決
- 最大 IP アドレス競合解決
- 接続ルートに対する Route-Tag のサポート

静的ポリシー解決

静的ポリシー解決の設定により、新しいアドレス設定が現在実行中のインターフェイスに影響するのを防ぎます。

設定例

競合ポリシーを静的に設定します。つまり、新しいインターフェイスアドレスが現在実行中のインターフェイスに影響するのを防ぎます。

```
Router#configure
Router(config)#ipv4 conflict-policy static
*/For IPv6, use the ipv6 conflict-policy static command/*
Router(config)#commit
```

実行コンフィギュレーション

```
Router#show running-config | in ipv4 config
Building configuration...
!! IOS XR Configuration version = 6.0.0.26I
!! Last configuration change at Mon Dec 14 21:57:27 2015 by root
!
hostname sample-83
logging console debugging
username root
  group root-lr
  group test
  secret 5 $1$d2NC$RbAdqdU7kw/eKJpMo/GJI1
!
cdp
ipv4 conflict-policy static
interface Loopback0
  ipv4 address 1.1.1.1 255.255.255.255
!
....
```

確認

```
Router#show arm ipv4 conflicts
F Forced down
| Down interface & addr                Up interface & addr VRF

F tenGigE 0/11/0/0 192.85.1.2/24    HundredGigE0/9/0/1 192.85.1.1/24 default
```

```
Forced down interface                Up interface                VRF
```

関連コマンド

- ipv4 conflict-policy
- ipv6 conflict-policy

最長プレフィックス アドレス競合解決

この競合解決ポリシーは、プレフィックスが最長の IP アドレスに最も高い優先度を付与することを試みます。つまり、現在実行しているインターフェイスの最長プレフィックスアドレスと競合しない競合セット内のすべてのアドレスが、同様に実行を許可されます。

設定例

最長プレフィックス アドレス競合解決を設定します。

```
Router# configure
Router(config)# ipv4 conflict-policy longest-prefix
*/For IPv6, use the ipv6 conflict-policy command*/
Router(config)# commit
```

実行コンフィギュレーション

```
Router# show running-config | in longest-prefix
Building configuration...
ipv4 conflict-policy longest-prefix
```

確認

```
Router#show arm ipv4 conflicts
F Forced down
| Down interface & addr          Up interface & addr VRF

F tenGigE 0/11/0/0 192.85.1.2/24  HundredGigE0/9/0/1  192.85.1.1/24 default
```

```
Forced down interface          Up interface          VRF
```

最大 IP アドレス競合解決

この競合解決ポリシーは、値が最も高い IP アドレスに最も高い優先度を付与することを試みます。つまり、値が最も高い IP アドレスが優先されます。

設定

最大 IP アドレス競合解決を設定します。

```
Router# configure
Router(config)#ipv4 conflict-policy highest-ip
*/For IPv6, use the ipv6 conflict-policy highest-ip command/*
Router(config)#commit
```

実行コンフィギュレーション

```
Router#show running-config | in highest-ip
Building configuration...
ipv4 conflict-policy highest-ip
```

確認

```
Router#show arm ipv4 conflicts
F Forced down
| Down interface & addr          Up interface & addr VRF

F tenGigE 0/11/0/0 192.85.1.2/24  HundredGigE0/9/0/1  192.85.1.1/24 default
```

```
Forced down interface          Up interface          VRF
```

接続ルートに対する Route-Tag のサポート

接続ルートに対する Route-Tag のサポート機能は、インターフェイスのすべての IPv4 および IPv6 アドレスにタグを付加します。このタグは、IPv4 および IPv6 の管理エージェント（MA）から、IPv4 および IPv6 の Address Repository Manager（ARM）およびルーティングプロトコルに伝搬されるため、ユーザは、Routing Policy Language（RPL）スクリプトを使用してルートタグを調べることで、接続ルートの再配布を制御します。これにより、ルートポリシーのルートタグを確認して、一部のインターフェイスの再配布を回避できます。ルートタグがポリシー

に一致し、再配布を回避できるスタティックルートと接続ルート（インターフェイス）では、このルート タグ機能はすでに利用可能になっています。

設定例

インターフェイス **HundredGigE 0/9/0/1** に対して、ルート タグ 20 が付いた IPv4 アドレス 10.0.54.2/30 を指定します。

```
Router#configure
Router(config)#interface HundredGigE 0/9/0/1
Router(config-if)#ipv4 address 10.0.54.2/30 route-tag 1899
Router(config)#commit
```

実行コンフィギュレーション

```
Router#show running-config interface HundredGigE0/9/0/1

interface HundredGigE0/9/0/1
  ipv4 address 10.0.54.2/30 route-tag 1899
!
```

確認

ルートのパラメータを確認します。

```
Router#show route 10.0.54.2
Routing entry for 10.0.54.2/32
  Known via "local", distance 0, metric 0 (connected)
  Tag 1899
Routing Descriptor Blocks
  directly connected, via HundredGigE0/9/0/1
    Route metric is 0
    No advertising protos.
```

関連コマンド

- route-tag

拡大された IPv6 アドレス空間

グローバルに一意な IP アドレスの需要は今後増加すると予想され、その需要を満たす必要があることが、IPv6 の主な目的です。モバイルインターネット対応デバイス（携帯情報端末（PDA）、電話、車両など）、Home Area Network（HAN）、ワイヤレスデータサービスなどのアプリケーションによって、グローバルに一意な IP アドレスの需要が増大しています。IPv6 は、ネットワーク アドレス ビット数を（IPv4 での）32 ビットの 4 倍の 128 ビットにしているため、地球上のすべてのネットワーク デバイスにグローバルに一意な IP アドレスを十分に提供できます。IPv6 アドレスをグローバルに一意にすることで、ネットワーク デバイスのグローバルな到達可能性とエンドツーエンドのセキュリティが実現されます。これは、アドレスの需要を喚起するアプリケーションとサービスに不可欠な機能です。また、柔軟性の高い IPv6 アドレス空間により、プライベートアドレスの必要性和ネットワーク アドレス変換（NAT）の使用が低減されます。したがって、IPv6 を使用すると、ネットワーク エッジにある境界ルー

タによる特別な処理を必要としない新しいアプリケーションプロトコルがイネーブルになります。

IPv6 アドレス形式

IPv6 アドレスは、x:x:x:x:x:x:x のようにコロン (:) で区切られた一連の 16 ビットの 16 進フィールドで表されます。次に、IPv6 アドレスの例を 2 つ示します。

```
2001:0DB8:7654:3210:FEDC:BA98:7654:3210
```

```
2001:0DB8:0:0:8:800:200C:417A
```

IPv6 アドレスには、通常、連続するゼロの 16 進フィールドが含まれます。IPv6 アドレスを扱いやすくするために、2 つのコロン (::) を使用して、IPv6 アドレスの先頭、中間、最後の部分の連続したゼロの 16 進フィールドを圧縮できます。（これらのコロンは、連続したゼロの 16 進フィールドを表します）。表 1: 圧縮された IPv6 アドレス形式 (21 ページ) に、圧縮された IPv6 アドレス形式を示します。

連続する 16 ビット値がゼロで表されている場合は、`ipv6-address` 引数の一部として 2 つのコロンを使用できます。インターフェイスごとに複数の IPv6 アドレスを設定できますが、設定できるリンクローカルアドレスは 1 つだけです。



(注) IPv6 アドレスでは、最も長く連続するゼロの 16 進フィールドを表すために 2 つのコロン (::) を 1 回だけ使用できます。

IPv6 アドレスの 16 進文字は大文字と小文字が区別されません。

表 1: 圧縮された IPv6 アドレス形式

| IPv6 アドレス タイプ | 優先形式 | 圧縮形式 |
|---------------|-------------------------------|--------------------------|
| ユニキャスト | 2001:0:0:0:0DB8:800:200C:417A | 1080::0DB8:800:200C:417A |
| マルチキャスト | FF01:0:0:0:0:0:0:101 | FF01::101 |
| ループバック | 0:0:0:0:0:0:0:1 | ::1 |
| 未指定 | 0:0:0:0:0:0:0:0 | :: |

ノードは、表 1: 圧縮された IPv6 アドレス形式 (21 ページ) に示されているループバック アドレスを使用して、IPv6 パケットを自身に送信できます。IPv6 のループバック アドレスは、IPv4 のループバック アドレス (127.0.0.1) と同じように機能します。



- (注) IPv6 ループバック アドレスは、物理インターフェイスに割り当てることができません。IPv6 ループバックアドレスを送信元アドレスまたは宛先アドレスとするパケットは、そのパケットを作成したノード内に留まっている必要があります。IPv6 ルータは、IPv6 ループバック アドレスを送信元アドレスまたは宛先アドレスとするパケットを転送しません。

表 1: 圧縮された IPv6 アドレス形式 (21 ページ) に示されている未指定アドレスは、IPv6 アドレスがないことを示します。たとえば、IPv6 ネットワーク上で新しく初期化されたノードは、IPv6 アドレスを受信するまで、パケットで未指定アドレスを送信元アドレスとして使用できます。



- (注) IPv6 未指定アドレスは、インターフェイスに割り当てることができません。未指定 IPv6 アドレスを IPv6 パケットまたは IPv6 ルーティング ヘッダーで宛先アドレスとして使用することはできません。

ipv6-prefix/prefix-length 形式の IPv6 アドレス プレフィックスを使用すると、アドレス空間全体のビット単位の連続ブロックを表現できます。 *ipv6-prefix* 引数には、RFC 2373 に記載されている形式を使用する必要があります。コロンで区切った 16 ビット値を使用して 16 進数でアドレスを指定してください。プレフィックス長は、アドレスの高次の連続ビットのうち、何個がプレフィックス (アドレスのネットワーク部分) を構成しているかを指定する 10 進数値です。たとえば、2001:0DB8:8086:6502::/32 は有効な IPv6 プレフィックスです。

IPv6 アドレス タイプ : ユニキャスト

IPv6 ユニキャストアドレスは、単一ノード上の単一インターフェイスの識別子です。ユニキャストアドレスに送信されるパケットは、そのアドレスで識別されるインターフェイスに配信されます。Cisco IOS XR ソフトウェアでは、次の IPv6 ユニキャスト アドレス タイプがサポートされています。

- 集約可能グローバル アドレス
- サイトローカル アドレス (IETF では廃止を提案しています)
- リンクローカル アドレス
- IPv4 互換 IPv6 アドレス

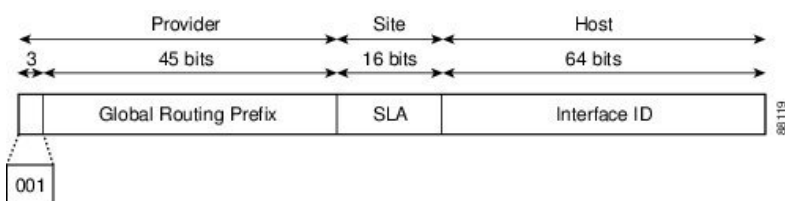
集約可能グローバル アドレス

集約可能グローバル アドレスは、集約可能なグローバル ユニキャスト プレフィックスによる IPv6 アドレスです。集約可能グローバル ユニキャスト アドレスの構造により、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 エントリ数を制限するルーティング プレフィックスの厳密な集約が可能になります。集約可能グローバル アドレスは、組織を上に向

かつて、最終的にインターネットサービスプロバイダー（ISP）まで集約されるリンクで使用されます。

集約可能グローバル IPv6 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 により定義されます。バイナリ 000 から開始するアドレスを除き、すべてのグローバルユニキャストアドレスには 64 ビットのインターフェイス ID があります。現在のグローバルユニキャストアドレスの割り当てには、バイナリ値 001 (2000::/3) から始まるアドレスの範囲が使用されます。次の図は、集約可能グローバルアドレスの構造を示しています。

図 1: 集約可能グローバルアドレス形式



2000::/3 (001) ~ E000::/3 (111) のプレフィックスを持つアドレスには、Extended Universal Identifier (EUI) 64 形式の 64 ビット インターフェイス識別子が必要です。インターネット割り当て番号局 (IANA) は、2000::/16 の範囲の IPv6 アドレス空間を地域レジストリに割り当てます。

集約可能グローバルアドレスは、通常、48 ビットのグローバルルーティングプレフィックスと、16 ビットのサブネット ID またはサイトレベル集約 (SLA) で構成されます。RFC 2374 (IPv6 集約可能グローバルユニキャストアドレス形式に関するドキュメント) では、グローバルルーティングプレフィックスに Top-Level Aggregator (TLA) と Next-Level Aggregator (NLA) という他の 2 つの階層構造フィールドが含まれていました。IETF は、TLS フィールドと NLA フィールドがポリシーベースのフィールドであるため、これらのフィールドを RFC から削除することに決定しました。この変更の前に展開された既存の IPv6 ネットワークの中には、依然として古いアーキテクチャに基づくネットワークを使用しているものもあります。

個々の組織では、サブネット ID と呼ばれる 16 ビットのサブネット フィールドを使用して、独自のローカルアドレスリング階層を作成したり、サブネットを識別したりできます。サブネット ID は IPv4 でのサブネットに似ていますが、IPv6 サブネット ID を持つ組織では最大 65,535 個のサブネットをサポートできるという点が異なります。

インターフェイス ID は、リンク上のインターフェイスの識別に使用されます。インターフェイス ID は、リンク上で一意である必要があります。より広い範囲で一意にすることもできます。多くの場合、インターフェイス ID は、インターフェイスのリンク層アドレスと同じか、リンク層アドレスに基づいています。集約可能グローバルユニキャストおよびその他の IPv6 アドレス タイプで使用するインターフェイス ID は、長さが 64 ビットの変更された EUI-64 形式で構築されている必要があります。

インターフェイス ID は、次のいずれかに該当する変更済みの EUI-64 形式で構築されています。

- すべての IEEE 802 インターフェイス タイプ（イーサネット インターフェイス、FDDI インターフェイスなど）の場合、最初の 3 オクテット（24 ビット）は、そのインターフェイス

スの 48 ビットリンク層アドレス (MAC アドレス) の組織固有識別子 (OUI) から取得され、4 番めと 5 番めのオクテット (16 ビット) は、FFFE の固定 16 進数値です。最後の 3 オクテット (24 ビット) は、MAC アドレスの最後の 3 オクテットから取得されます。インターフェイス ID の構成は、最初のオクテットの 7 番めのビットである Universal/Local (U/L) ビットを 0 または 1 の値に設定することで完成します。値 0 はローカルに管理されている識別子を示し、値 1 はグローバルに一意の IPv6 インターフェイス識別子を示します。

- IPv6 オーバーレイ トンネルで使用されるトンネルインターフェイス タイプの場合、インターフェイス ID は、識別子の上位 32 ビットがすべてゼロであるトンネルインターフェイスに割り当てられた IPv4 アドレスです。



(注) ポイントツーポイントプロトコル (PPP) を使用するインターフェイスの場合は、接続の両端のインターフェイスが同じ MAC アドレスを持つ可能性があるため、接続の両端で使用されるインターフェイス識別子は、両方の識別子が一意になるまでネゴシエーション (ランダムに選択され、必要に応じて再構築) されます。ルータの最初の MAC アドレスが、PPP を使用するインターフェイスの識別子の構築に使用されます。

ルータに IEEE 802 インターフェイス タイプがない場合は、ルータのインターフェイスでリンクローカル IPv6 アドレスが次のシーケンスで生成されます。

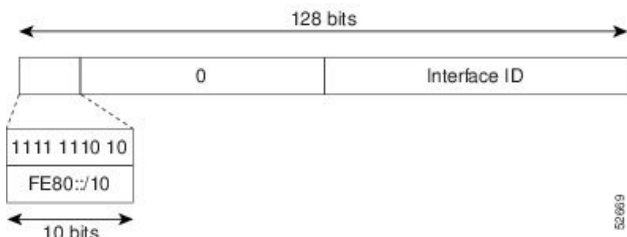
1. ルータに MAC アドレスが (ルータの MAC アドレス プールから) 照会されます。
2. 使用できる MAC アドレスがない場合は、ルート プロセッサ (RP) またはラインカード (LC) のシリアル番号を使用して、リンクローカル アドレスを形成します。

リンクローカルアドレス

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、ネイバー探索プロトコルとステータ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。次の図は、以下のリンクローカルアドレスの構造を示しています。

IPv6 ルータでは、送信元または宛先がリンクローカルアドレスであるパケットを他のリンクに転送できません。

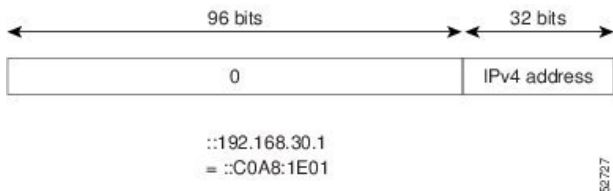
図 2: リンクローカル アドレス形式



IPv4 互換 IPv6 アドレス

IPv4 互換 IPv6 アドレスは、アドレスの上位 96 ビットがゼロであり、アドレスの下位 32 ビットが IPv4 アドレスである IPv6 ユニキャストアドレスです。IPv4 互換 IPv6 アドレスの形式は、0:0:0:0:0:0:A.B.C.D または ::A.B.C.D です。IPv4 互換 IPv6 アドレスの 128 ビット全体がノードの IPv6 アドレスとして使用され、下位 32 ビットに埋め込まれた IPv4 アドレスがノードの IPv4 アドレスとして使用されます。IPv4 互換 IPv6 アドレスは、IPv4 と IPv6 の両方のプロトコルスタックをサポートするノードに割り当てられ、自動トンネルで使用されます。次の図は、IPv4 互換 IPv6 アドレスの構造と、許容されるアドレスフォーマットのいくつかを示しています。

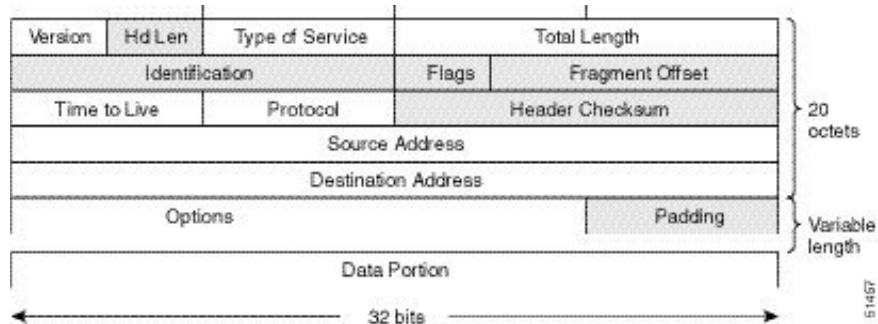
図 3: IPv4 互換 IPv6 アドレス形式



簡易 IPv6 パケット ヘッダー

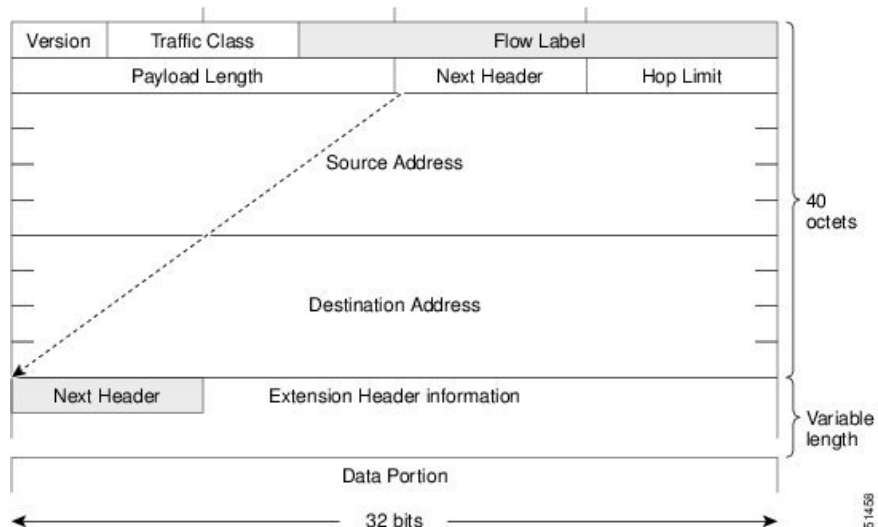
基本 IPv4 パケット ヘッダーには、合計サイズが 20 オクテット（160 ビット）の 12 のフィールドがあります。この 12 個のフィールドの後にはオプションフィールドが続く場合があります、さらにその後に、通常はトランスポートレイヤパケットであるデータ部分が続きます。可変長のオプションフィールドは、IPv4 パケット ヘッダーの合計サイズに加算されます。IPv4 パケット ヘッダーのグレーの部分のフィールドは、IPv6 パケット ヘッダーに含まれません。

図 4: IPv4 パケット ヘッダー形式



基本 IPv6 パケット ヘッダーには、合計サイズが 40 オクテット (320 ビット) の 8 つのフィールドがあります。IPv6 では、フラグメンテーションはルータによって処理されず、チェックサムはネットワーク層で使用されないため、IPv6 ヘッダーからフィールドが除去されました。代わりに、IPv6 のフラグメンテーションはパケットの送信元によって処理され、チェックサムはデータ リンク層とトランスポート層で使用されます (IPv4 では、ユーザ データグラム プロトコル (UDP) トランスポート層でオプションのチェックサムが使用されます。IPv6 では、UDP チェックサムを使用して内部パケットの完全性を確認する必要があります)。また、基本 IPv6 パケット ヘッダーとオプション フィールドは 64 ビットに揃えられています。これにより、IPv6 パケットの処理が容易になります。

図 5: IPv6 パケット ヘッダー形式



次の表に、基本 IPv6 パケット ヘッダーのフィールドをリストします。

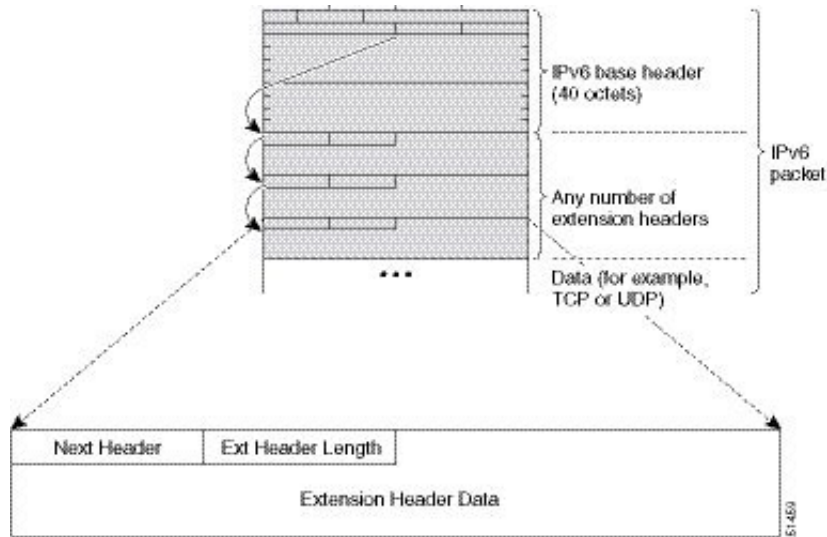
表 2: 基本 IPv6 パケット ヘッダー フィールド

| フィールド | 説明 |
|-------|--|
| バージョン | IPv4 パケット ヘッダーのバージョン フィールドと同様ですが、IPv4 を意味する数字 4 の代わりに IPv6 を意味する数字 6 が示されます。 |

| フィールド | 説明 |
|------------|---|
| トラフィック クラス | IPv4 パケット ヘッダーのタイプ オブ サービス フィールドと同様です。トラフィック クラス フィールドは、差別化されたサービスで使用するトラフィック クラスのタグをパケットに付けます。 |
| フロー ラベル | IPv6 パケット ヘッダーの新しいフィールドです。フロー ラベル フィールドは、ネットワーク層でパケットを差別化する特定のフローのタグをパケットに付けます。 |
| ペイロード長 | IPv4 パケット ヘッダーの合計長フィールドと同様です。ペイロード長 フィールドは、パケットのデータ部分の合計長を示します。 |
| 次ヘッダー | IPv4 パケット ヘッダーのプロトコルフィールドと同様です。次ヘッダー フィールドの値により、基本 IPv6 ヘッダーに続く情報のタイプが決まります。基本 IPv6 ヘッダーの後ろに続く情報のタイプは、TCP や UDP パケットなどのトランスポートレイヤ パケット、または拡張ヘッダーです。 |
| ホップ リミット | IPv4 パケット ヘッダーの存続可能時間フィールドと同様です。ホップ リミット フィールドの値は、IPv6 パケットが無効と見なされる前に通過できるルータの最大数です。各ルータを通過するたびに、この値が 1 つずつ減少します。IPv6 ヘッダーにはチェックサムがないため、ルータは値を減らすたびにチェックサムを再計算する必要がなく、処理リソースが節約されます。 |
| 送信元アドレス | IPv4 パケット ヘッダーの送信元アドレス フィールドと同様ですが、IPv4 の 32 ビット送信元アドレスの代わりに、IPv6 では 128 ビットの送信元アドレスが含まれます。 |
| 宛先アドレス | IPv4 パケット ヘッダーの宛先アドレス フィールドと同様ですが、IPv4 の 32 ビット宛先アドレスの代わりに、IPv6 では 128 ビットの宛先アドレスが含まれます。 |

基本 IPv6 パケット ヘッダーの 8 つのフィールドの後に、オプションの拡張ヘッダーおよびパケットのデータ部分が続きます。存在する場合は、各拡張ヘッダーが 64 ビットに揃えられます。IPv6 パケットの拡張ヘッダーの数は固定されていません。拡張ヘッダーがまとまってヘッダーのチェーンを形成します。各拡張ヘッダーは、前のヘッダーの次ヘッダー フィールドによって識別されます。通常は、最後の拡張ヘッダーに、TCP や UDP などのトランスポートレイヤ プロトコルの次ヘッダー フィールドがあります。次の図は、IPv6 拡張ヘッダーの形式を示しています。

図 6: IPv6 拡張ヘッダー形式



次の表に、拡張ヘッダー タイプとその次ヘッダー フィールド値をリストします。

表 3: IPv6 拡張ヘッダー タイプ

| ヘッダー タイプ | 次ヘッダー の値 | 説明 |
|--------------------|-------------|--|
| ホップバイホップ オプションヘッダー | 0 | このヘッダーは、パケットのパス上のすべてのホップで処理されます。存在する場合、ホップバイホップ オプションヘッダーは、常に基本 IPv6 パケットヘッダーの直後に続きます。 |
| 宛先オプションヘッダー | 60 | 宛先オプションヘッダーは、任意のホップバイホップ オプションヘッダーの後に続くことがあります。その場合、宛先オプションヘッダーは、最終的な宛先と、ルーティングヘッダーで指定された各通過アドレスでも処理されます。また、宛先オプションヘッダーは、任意のカプセル化セキュリティペイロード (ESP) ヘッダーの後に続くこともあります。その場合、宛先オプションヘッダーは、最終的な宛先でだけ処理されます。 |
| ルーティングヘッダー | 43 | ルーティングヘッダーは送信元のルーティングに使用されます。 |
| フラグメントヘッダー | 44 | フラグメントヘッダーは、送信元が、送信元と宛先の間のパスの最大伝送ユニット (MTU) よりも大きいパケットをフラグメント化する必要がある場合に使用されます。フラグメントヘッダーは、フラグメント化された各パケットで使用されます。 |

| ヘッダー タイプ | 次ヘッダー の値 | 説明 |
|---------------------------|-------------------------|---|
| 認証ヘッダー および ESP ヘッダー | 51 50 | 認証ヘッダーと ESP ヘッダーは、パケットの認証、整合性、および機密性を提供するために IP セキュリティ プロトコル (IPSec) 内で使用されます。これらのヘッダーは、IPv4 と IPv6 の両方で同一です。 |
| 上位層ヘッダー | 6 (TCP) 17 (UDP) | 上位層 (トランスポート) ヘッダーは、データを転送するためにパケットの内部で使われる典型的なヘッダーです。2 つの主要なトランスポート プロトコルは TCP と UDP です。 |
| モビリティ ヘッダー | IANA で実 行 | バインディングの作成と管理に関連するすべてのメッセージで、モバイル ノード、通信ノード、およびホーム エージェントによって使用される拡張ヘッダーです。 |

IPv6 のパス MTU ディスカバリ

IPv4 の場合と同様に、IPv6 のパス MTU ディスカバリを使用すると、特定のデータパス上のすべてのリンクの MTU サイズの差をホストが動的に検出し、調整できます。ただし、IPv6 では、特定のデータパス上の 1 つのリンクのパス MTU がパケットのサイズに十分に対応できる大きさでない場合に、フラグメンテーションはパケットの送信元によって処理されます。IPv6 ホストでパケットフラグメンテーションを処理すると、IPv6 ルータの処理リソースが節約され、IPv6 ネットワークの効率が向上します。

IPv4 では、最小リンク MTU が 68 オクテットであるため、特定のデータパスに沿うすべてのリンクの MTU サイズが少なくとも 68 オクテットの MTU サイズをサポートする必要があります。IPv6 では、最小リンク MTU は 1280 オクテットです。IPv6 リンクには、1500 オクテットの MTU 値の使用をお勧めします。



(注) パス MTU ディスカバリは、TCP を使用するアプリケーションでのみサポートされます。

IPv6 ネイバー探索

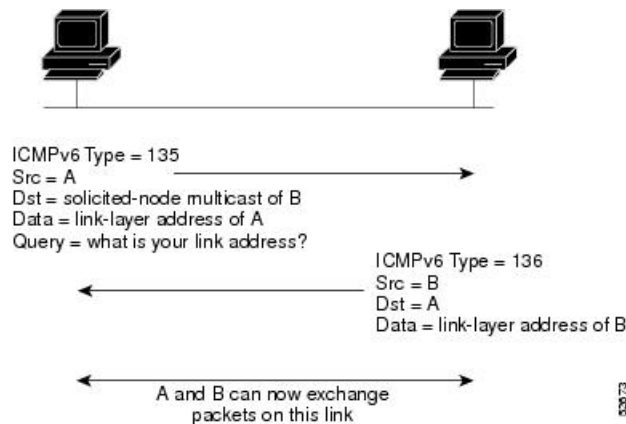
IPv6 のネイバー探索プロセスは、ICMP メッセージと送信要求ノード マルチキャスト アドレスを使用して、同じネットワーク (ローカルリンク) 上のネイバーのリンク層アドレスを判別し、ネイバーの到達可能性を確認して、隣接ルータの状況を把握します。

IPv6 ネイバー送信要求メッセージ

ICMP パケットヘッダーのタイプフィールドの値 135 は、ネイバー送信要求メッセージを示します。ネイバー送信要求メッセージは、ノードが同じローカルリンク上の別のノードのリンク層アドレスを決定するときに、ローカルリンク上で送信されます。ノードが別のノードのリンク

層アドレスを判断する必要がある場合、ネイバー請求メッセージ内の送信元アドレスは、ネイバー請求メッセージを送信するノードの IPv6 アドレスです。ネイバー送信要求メッセージ内の宛先アドレスは、宛先ノードの IPv6 アドレスに対応する送信要求ノードマルチキャストアドレスです。ネイバー送信要求メッセージには、送信元ノードのリンク層アドレスも含まれます。

図 7: IPv6 ネイバー探索 - ネイバー送信要求メッセージ



ネイバー送信要求メッセージを受信した後に、宛先ノードは、ICMP パケットヘッダーのタイプフィールドに値 136 を含むネイバーアドバタイズメントメッセージをローカルリンクに送信することで応答します。ネイバーアドバタイズメントメッセージの送信元アドレスは、ネイバーアドバタイズメントメッセージを送信するノードの IPv6 アドレス（具体的には、ノードインターフェースの IPv6 アドレス）です。ネイバーアドバタイズメントメッセージ内の宛先アドレスは、ネイバー送信要求メッセージを送信したノードの IPv6 アドレスです。ネイバーアドバタイズメントメッセージのデータ部分には、ネイバーアドバタイズメントメッセージを送信するノードのリンク層アドレスが含まれます。

送信元ノードがネイバーアドバタイズメントを受信すると、送信元ノードと宛先ノードが通信できるようになります。

ネイバー送信要求メッセージは、ネイバーのリンク層アドレスが識別された後に、ネイバーの到達可能性の確認にも使用されます。ノードがネイバーの到達可能性を確認するときに、ネイバー送信要求メッセージの宛先アドレスは、ネイバーのユニキャストアドレスです。

ネイバーアドバタイズメントメッセージは、ローカルリンク上のノードのリンク層アドレスが変更されたときにも送信されます。そのような変更があった場合、ネイバーアドバタイズメントの宛先アドレスは全ノードマルチキャストアドレスになります。

ネイバー送信要求メッセージは、ネイバーのリンク層アドレスが識別された後に、ネイバーの到達可能性の確認にも使用されます。ネイバー到達不能検出では、ネイバーの障害またはネイバーへの転送パスの障害が識別されます。この検出は、ホストとネイバーノード（ホストまたはルータ）間のすべてのパスで使用されます。ネイバー到達不能検出は、ユニキャストパケットだけが送信されるネイバーに対して実行され、マルチキャストパケットが送信されるネイバーに対しては実行されません。

ネイバーは、（以前にネイバーに送信されたパケットが受信され、処理されたことを示す）肯定確認応答がネイバーから返された場合に、到達可能と見なされます。上位層プロトコル (TCP

など)からの肯定確認応答は、接続で転送が順調に進行している(宛先に到達しつつある)こと、またはネイバー送信要求メッセージに対する応答でネイバーアドバタイズメントメッセージが受信されたことを示します。パケットがピアに到達している場合、それらのパケットは送信元のネクストホップネイバーにも到達しています。したがって、転送の進行により、ネクストホップネイバーが到達可能であることも確認されます。

ローカルリンク上にない宛先の場合、転送の進行は、ファーストホップルータが到達可能であることを暗に意味します。上位層プロトコルからの確認応答がない場合、ノードは、ユニキャストネイバー送信要求メッセージを使用してネイバーを探し、転送パスがまだ機能していることを確認します。送信要求ネイバーアドバタイズメントメッセージがネイバーから返されることは、転送パスがまだ機能していることを示す肯定確認応答です。(送信要求フラグに値1が設定されているネイバーアドバタイズメントメッセージは、ネイバー送信要求メッセージへの応答でのみ送信されます)。非送信要求メッセージでは、送信元ノードから宛先ノードへの一方向パスだけが確認されます。送信要求ネイバーアドバタイズメントメッセージは、両方向のパスが機能していることを示します。



(注) 送信要求フラグが値0に設定されたネイバーアドバタイズメントメッセージは、転送パスがまだ機能していることを示す肯定確認応答とは見なされません。

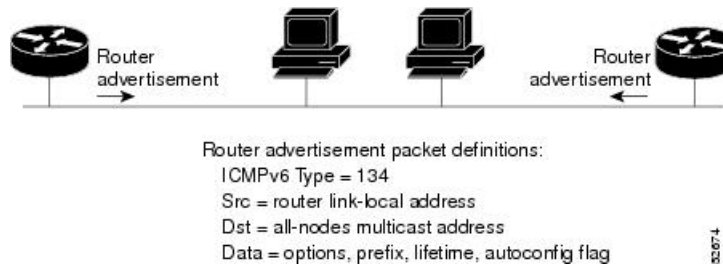
ネイバー送信要求メッセージは、ユニキャストIPv6アドレスがインターフェイスに割り当てられる前にそのアドレスが一意であることを確認するために、ステートレス自動設定プロセスでも使用されます。アドレスがインターフェイスに割り当てられる前に、重複アドレス検出がまず新しいリンクローカルIPv6アドレスで実行されます(重複アドレス検出の実行時、新しいアドレスは暫定的な状態にあります)。具体的には、ノードは未指定の送信元アドレスと一時的なリンクローカルアドレスをメッセージの本文に含むネイバー送信要求メッセージを送信します。そのアドレスが別のノードですでに使用されている場合、ノードは一時的なリンクローカルアドレスを含むネイバーアドバタイズメントメッセージを返します。別のノードが同じアドレスの一意性を同時に検証している場合は、そのノードもネイバー送信要求メッセージを返します。ネイバー送信要求メッセージの返信としてネイバーアドバタイズメントメッセージが受信されず、同じ一時アドレスの検証を試行している他のノードからのネイバー送信要求メッセージも受信されない場合、最初のネイバー送信要求メッセージを送信したノードは、一時的なリンクローカルアドレスを一意であると見なし、そのアドレスをインターフェイスに割り当てます。

IPv6ユニキャストアドレス(グローバルまたはリンクローカル)はすべてリンクでの一意性を確認する必要があります。ただし、リンクローカルアドレスの一意性が確認されるまで、リンクローカルアドレスに関連付けられた他のIPv6アドレスに対して重複アドレス検出は実行されません。Cisco IOS XRソフトウェアでの重複アドレス検出のシスコ実装では、64ビットインターフェイス識別子から生成されるエニキャストアドレスまたはグローバルアドレスの一意性はチェックされません。

IPv6 ルータ アドバタイズメント メッセージ

ルータ アドバタイズメント (RA) メッセージは、ICMP パケット ヘッダーのタイプ フィールドが値 134 であり、IPv6 ルータの設定済みの各インターフェイスへ定期的送信されます。ルータ アドバタイズメント メッセージは全ノードマルチキャストアドレスに送信されます。

図 8: IPv6 ネイバー探索 - ルータ アドバタイズメント メッセージ



ルータ アドバタイズメント メッセージには、通常、次の情報が含まれています。

- ローカル リンク上のノードがその IPv6 アドレスの自動設定に使用できる 1 つ以上のオン リンク IPv6 プレフィックス
- アドバタイズメントに含まれる各プレフィックスのライフタイム情報
- 完成可能な自動設定のタイプ (ステートレスまたはステートフル) を示すフラグのセット
- デフォルト ルータ情報 (アドバタイズメントを送信しているルータをデフォルト ルータとして使用する必要があるかどうか、および、その場合は、ルータがデフォルトルータとして使用される秒単位の時間)
- ホストが発信するパケットで使用する必要のあるホップ リミットや MTU など、ホストに関する詳細情報

ルータ アドバタイズメントは、ルータ送信要求メッセージへの応答としても送信されます。ICMP パケット ヘッダーの Type 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ルータ アドバタイズメント 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。ルータ送信要求メッセージが通常システム起動時にホストによって送信される (ホストにユニキャストアドレスが設定されていない) 場合、ルータ送信要求メッセージの送信元アドレスは、通常は未指定の IPv6 アドレス (0:0:0:0:0:0:0:0) です。ホストに設定済みのユニキャスト アドレスがある場合、ルータ送信要求メッセージを送信するインターフェイスのユニキャストアドレスが、メッセージ内の送信元アドレスとして使用されます。ルータ送信要求メッセージの宛先アドレスは、スコープがリンクである全ルータ マルチキャスト アドレスです。ルータ送信要求に回答してルータ アドバタイズメントが送信される場合、ルータ アドバタイズメント メッセージ内の宛先アドレスはルータ送信要求メッセージの送信元のユニキャスト アドレスです。

次のルータ アドバタイズメント メッセージ パラメータを設定できます。

- ルータ アドバタイズメント メッセージの定期的な時間間隔
- (特定のリンク上のすべてのノードで使用される) デフォルトルータとしてのルータの実用性を示す「ルータ ライフタイム」値

- 特定のリンクで使用されているネットワーク プレフィックス
- (特定のリンクで) ネイバー送信要求メッセージが再送信される時間の間隔
- ノードによってネイバーが到達可能である (特定のリンク上のすべてのノードで使用できる) と見なされるまでの時間

設定されたパラメータはインターフェイスに固有です。ルータ アドバタイズメント メッセージ (デフォルト値を含む) の送信は、イーサネットと FDDI インターフェイス上では自動的にイネーブルになります。その他のインターフェイス タイプの場合、ルータ アドバタイズメント メッセージの送信は、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 suppress-ra** コマンドを使用して手動で設定する必要があります。ルータ アドバタイズメント メッセージの送信を個々のインターフェイスでディセーブルにするには、インターフェイス コンフィギュレーション モードで **ipv6 nd suppress-ra** コマンドを使用します。

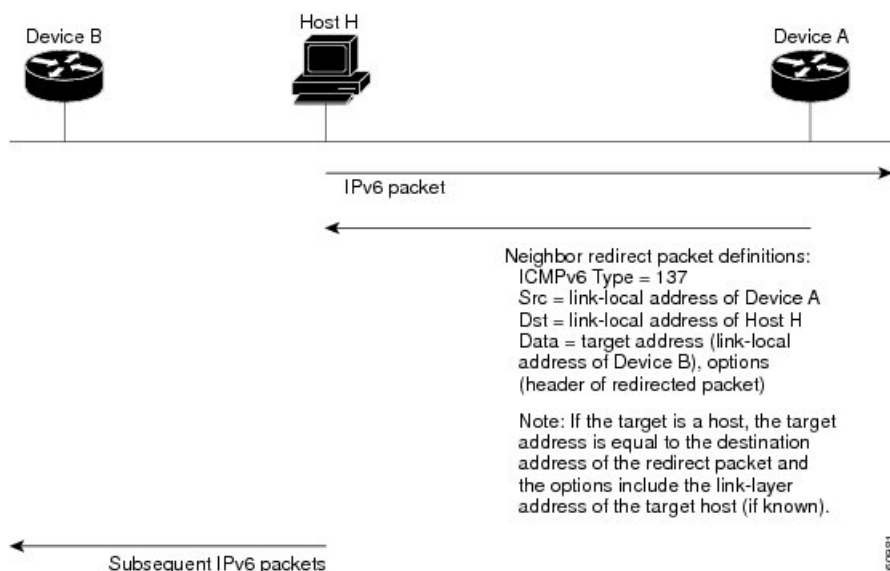


(注) ステートレス自動設定が正しく機能するには、ルータ アドバタイズメント メッセージでアドバタイズされたプレフィックス長が常に 64 ビットである必要があります。

IPv6 ネイバー リダイレクト メッセージ

ICMP パケット ヘッダーのタイプ フィールドの値 137 は、IPv6 ネイバー リダイレクト メッセージを示します。ルータは、ネイバー リダイレクト メッセージを送信して、宛先へのパス上のより適切なファーストホップ ノードをホストに通知します

図 9: IPv6 ネイバー探索 - ネイバー リダイレクト メッセージ





- (注) リダイレクト メッセージ内のターゲット アドレス（最終的な宛先）によって隣接ルータのリンクローカル アドレスが確実に識別されるように、ルータは各隣接ルータのリンクローカル アドレスを判断できる必要があります。スタティック ルーティングの場合、ネクストホップ ルータのアドレスは、ルータのリンクローカルアドレスを使用して指定する必要があります。ダイナミック ルーティングの場合は、すべての IPv6 プロトコルが隣接ルータのリンクローカル アドレスを交換する必要があります。

パケットの転送後に、次の条件が満たされる場合、ルータはパケットの送信元にリダイレクト メッセージを送信する必要があります。

- パケットの宛先アドレスがマルチキャスト アドレスではない。
- パケットがルータにアドレッシングされていなかった。
- パケットが、そのパケットを受信したインターフェイスから送信されようとしている。
- ルータが、パケットにより適したファーストホップ ノードはパケットの送信元と同じリンク上にあると判断した。
- パケットの送信元アドレスが、同じリンク上のネイバーのグローバル IPv6 アドレス、またはリンクローカルアドレスである。

ルータがすべての IPv6 ICMP エラー メッセージ（ネイバー リダイレクト メッセージを含む）を生成するレートを制限するには、**ipv6 icmp error-interval** 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。これにより、リンク層の輻輳が低減されます。



- (注) ルータはネイバー リダイレクト メッセージを受信してもそのルーティング テーブルを更新せず、ホストはネイバー リダイレクト メッセージを発信しません。

Address Repository Manager

IPv4 および IPv6 の Address Repository Manager (IPARM) は、システムで設定されたグローバル IP アドレスの一意性を強制適用し、IP アドレスを消費するアプリケーションプログラム インターフェイス (API) を使用して、グローバル IP アドレス情報（アンナンバード インターフェイス情報を含む）をルート プロセッサ (RP) およびラインカード (LC) 上のプロセスに伝達します。

アドレス競合解決

競合解決には、競合データベースおよび競合セット定義という 2 つの部分があります。

競合データベース

IPARM では、グローバル競合データベースを保持します。互いに競合する IP アドレスは、競合セットと呼ばれるリストに保持されます。これらの競合セットは、グローバル競合データベースを構成します。

IP アドレスのセットは、そのセット内の少なくとも 1 つのプレフィックスが、同じセットに属する他のすべての IP アドレスと競合する場合に、競合セットの一部であると見なされます。たとえば、次の 4 つのアドレスは、単一の競合セットの一部です。

アドレス 1 : 10.1.1.1/16

アドレス 2 : 10.2.1.1/16

アドレス 3 : 10.3.1.1/16

アドレス 4 : 10.4.1.1/8

競合する IP アドレスが競合セットに追加されると、アルゴリズムによってそのセット全体が調べられ、そのセット内の最も優先度の高いアドレスが判別されます。

この競合ポリシーアルゴリズムは決定論的アルゴリズムであり、つまり、ユーザは、インターフェイス上のいずれのアドレスがイネーブルまたはディセーブルであるかがわかります。イネーブルなインターフェイス上のアドレスは、その競合セットの最も優先度の高いアドレスとして宣言されます。

競合ポリシー アルゴリズムは、セット内の最も優先度の高い IP アドレスを判別します。



第 2 章

ARP の設定

- [ARP の設定 \(37 ページ\)](#)
- [ARP の設定に関する情報 \(42 ページ\)](#)

ARP の設定

アドレス解決はネットワーク アドレスをメディアアクセスコントロール (MAC) アドレスにマッピングするプロセスです。通常は、ARP プロトコルを使用してシステムにより動的に実行されますが、スタティック ARP エントリの設定によって実行することもできます。このプロセスを実現するのに使用されるのが、アドレス解決プロトコル (ARP) です。

ARP は、IP アドレスをメディアや MAC アドレスに関連付けるために使用されます。ARP は IP アドレスを入力とし、関連するメディアのアドレスを決定します。メディアまたは MAC アドレスが決定すると、IP アドレスまたはメディアアドレスの関連付けは、すぐ取得できるように ARP のキャッシュに保管されます。その後、IP データグラムがリンク層フレームにカプセル化され、ネットワークを通じて送信されます。

ARP の詳細については、次を参照してください。 [ARP の設定に関する情報 \(42 ページ\)](#)

ARP およびプロキシ ARP

Cisco IOS XR ソフトウェアでは、アドレス解決プロトコル (ARP) とプロキシ ARP という 2 つの形式のアドレス解決がサポートされています。これらのプロトコルは、それぞれ RFC 826 と RFC 1027 で定義されています。Cisco IOS XR ソフトウェアでは、ローカル プロキシ ARP という ARP の形式もサポートされています。

プロキシ ARP とローカル プロキシ ARP の詳細については、次を参照してください。 [プロキシ ARP とローカル プロキシ ARP \(38 ページ\)](#)

制約事項

ARP の設定には、次の制約事項が適用されます。

- 逆アドレス解決プロトコル (RARP) はサポートされません。
- 転送情報ベース (FIB) で ARP パケットのレートを制限する ARP スロットリングはサポートされていません。

ARP キャッシュ エントリ

ARP は、ネットワーク アドレス（IP アドレスなど）とイーサネット ハードウェア アドレスの間の通信を確立します。各通信の記録は、キャッシュ内に事前定義された期間だけ保持された後、廃棄されます。

また、明示的に削除されるまで存続するスタティック（永続）エントリを ARP キャッシュに追加することもできます。

スタティック ARP キャッシュ エントリの定義

ARP をはじめとするアドレス解決プロトコルを使用すると、IP アドレスとメディア アドレスとをダイナミックにマッピングできます。大部分のホストはダイナミック アドレス解決をサポートしているため、通常はスタティック ARP エントリを指定する必要はありません。スタティック ARP キャッシュ エントリを定義する必要がある場合は、グローバルに定義できます。このタスクを実行すると、ARP キャッシュにエントリが永続的にインストールされます。Cisco IOS XR ソフトウェアはこのエントリを使用して、32 ビット IP アドレスを 48 ビットのハードウェア アドレスに変換します。

また、ARP キャッシュにエイリアス エントリを作成することにより、特定の IP アドレスによって識別されたかのように、ARP 要求に応答することもできます。

設定例

キャッシュ エントリを作成して、IP アドレス **203.0.1.2** と MAC アドレス **0010.9400.000c** の間に接続を確立します。さらに、このキャッシュ エントリをエイリアス エントリとして作成すると、エントリに関連付けられているインターフェイスは、エントリ内のデータリンク層アドレスを使って、このネットワーク層アドレスに対する ARP 要求パケットに応答します。

```
Router#config
Router(config)#arp 203.0.1.2 0010.9400.000c arPA
Router(config)#commit
```

実行コンフィギュレーション

```
Router#show run arp 203.0.1.2 0010.9400.000c arPA
arp vrf default 203.0.1.2 0010.9400.000c ARPA
```

確認

[State] が [Static] になっているかをチェックして、適切に機能していることを確認します。

```
Router#show arp location 0/RP0/CPU0
Address      Age      Hardware Addr  State      Type  Interface
203.0.1.1    -        ea28.5f0b.8024 Interface ARPA  HundredGigE0/9/0/0
203.0.1.2    -        0010.9400.000c Static ARPA  HundredGigE0/9/0/0
```

プロキシ ARP とローカル プロキシ ARP

プロキシ ARP がディセーブルされると、ネットワーキング デバイスは、次のいずれかの条件が満たされる場合に限り、インターフェイスに受信された ARP 要求に応答します。

- ARP 要求のターゲット IP アドレスは、要求が受信されたインターフェイス IP アドレスと同じです。
- ARP 要求のターゲット IP アドレスには、静的に設定された ARP エイリアスがあります。

プロキシ ARP がイネーブルになると、ネットワーキング デバイスは、次の条件すべてを満たす ARP 要求にも応答します。

- ターゲット IP アドレスが、要求を受信した同一の物理ネットワーク（LAN）上にない。
- ネットワーキング デバイスに、ターゲット IP アドレスまでのルートが1つ以上存在する。
- ターゲット IP アドレスまでのルートすべてが、要求を受信したインターフェイスとは別のインターフェイスを通過する。

プロキシ ARP がイネーブルになっている場合、ネットワーキング デバイスは、次の条件をすべて満たす ARP 要求に応答します。

- ARP 要求のターゲット IP アドレス、ARP ソースの IP アドレス、および ARP 要求を受信するインターフェイスの IP アドレスが、同じレイヤ 3 ネットワーク上にある。
- ターゲット IP アドレスのネクストホップが、要求を受信するインターフェイスと同じインターフェイスを使用する。

通常、ローカル プロキシ ARP は、同じレイヤ 3 ネットワークで MAC アドレスを IP アドレスに解決するために使用されます。ローカル プロキシ ARP は、ARP でサポートされるあらゆるタイプのインターフェイスに加えて、アンナンバード インターフェイスに対応しています。

プロキシ ARP のイネーブル化

Cisco IOS XR ソフトウェアは（RFC 1027 で定義されている）プロキシ ARP を使用して、ルーティングに必要な情報を持たないホストでも他のネットワークやサブネット上のホストのメディア アドレスを判別できるようにします。たとえば、ARP 要求の送信元と異なるインターフェイス上のホストに宛てた ARP 要求をルータが受信した場合、そのルータに他のインターフェイスを経由してそのホストに至るすべてのルートが格納されていれば、ルータは自身のローカル データ リンク アドレスを示すプロキシ ARP 応答パケットを生成します。ARP 要求を送信したホストはルータにパケットを送信し、ルータはパケットを目的のホストに転送します。プロキシ ARP はデフォルトではディセーブルになっています。このタスクでは、ディセーブルになっているプロキシ ARP をイネーブルにする方法について説明します。

設定例

プロキシ ARP を HundredGigE インターフェイス 0/9/0/0 でイネーブルにします。

```
Router#configure
Router(config)#interface HundredGigE0/9/0/0
Router(config-if)#proxy-arp
Router(config-if)#commit
```

実行コンフィギュレーション

```
Router# show running-config interface HundredGigE0/9/0/0
interface HundredGigE0/9/0/0
  mtu 4000
  ipv4 address 1.0.0.1 255.255.255.0
  proxy-arp
!
```

確認

プロキシ ARP が設定され、イネーブルになっていることを確認します。

```
Router#show arp idb interface HundredGigE0/9/0/0 location 0/RP0/CPU0
  interface HundredGigE0/9/0/0 (0x08000038):
    IPv4 address 1.0.0.1, Vrf ID 0x60000000
    VRF Name default
    Dynamic learning: Enable
    Dynamic entry timeout: 14400 secs
    Purge delay: off
    IPv4 caps added (state up)
    MPLS caps not added
    Interface not virtual, not client fwd ref,
    Proxy arp is configured, is enabled
    Local Proxy arp not configured
    Packet IO layer is NetIO
    Srg Role : DEFAULT
    Idb Flag : 262332
    IDB is Complete
```

ローカル プロキシ ARP のイネーブル化

ローカル プロキシ ARP は、レイヤ 2 で分離されたプライベート VLAN など、同じレイヤ 3 ネットワークで MAC アドレスを IP アドレスに解決するために使用されます。ローカル プロキシ ARP は、ARP でサポートされるあらゆるタイプのインターフェイスに加えて、アンナバードインターフェイスに対応しています。

設定例

ローカル プロキシ ARP を HundredGigE インターフェイス 0/9/0/0 でイネーブルにします。

```
Router#configure
Router(config)#interface HundredGigE0/9/0/0
Router(config-if)#local-proxy-arp
Router(config-if)#commit
```

実行コンフィギュレーション

```
Router#show running-config interface HundredGigE0/9/0/1
  interface HundredGigE0/9/0/0
    ipv4 address 1.0.0.1 255.255.255.0
    local-proxy-arp
!
```

確認

ローカル プロキシ ARP が設定されていることを確認します。

```

Router#show arp idb interface HundredGigE0/9/0/0 location 0/RP0/CPU0
HundredGigE0/9/0/1 (0x08000038):
  IPv4 address 1.0.0.1, Vrf ID 0x60000000
  VRF Name default
  Dynamic learning: Enable
  Dynamic entry timeout: 14400 secs
  Purge delay: off
  IPv4 caps added (state up)
  MPLS caps not added
  Interface not virtual, not client fwd ref,
  Proxy arp not configured, not enabled
  Local Proxy arp is configured
  Packet IO layer is NetIO
  Srg Role : DEFAULT
  IdB Flag : 264332
  IDB is Complete

```

関連コマンド

- [local-proxy-arp](#)
- `show arp idb`

ローカル ARP エントリの学習の設定

インターフェイスまたはサブインターフェイスを設定して、ローカルサブネットから ARP エントリのみを学習することができます。

インターフェイス上にローカル ARP 学習を設定するには、次の手順を実行します。

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。

```
Router(config)# interface TenGigE 0/11/0/0
```

2. インターフェイスの IPv4/IPv6 アドレスを設定します。

```
Router(config-if)# ipv4 address 12.1.3.4 255.255.255.0
```

3. インターフェイス上にローカル ARP インターフェイスの学習を設定します。

```
Router(config-if)# arp learning local
```

4. インターフェイスを有効にし、設定をコミットします。

```

Router(config-if)# no shut
Router(config-if)# commit
RP/0/0/CPU0:Dec 12 13:41:16.580 : ifmgr[397]: %PKT_INFRA-LINK-3-UPDOWN : interface
TenGigE 0/11/0/0, changed state to Down
RP/0/0/CPU0:Dec 12 13:41:16.683 : ifmgr[397]: %PKT_INFRA-LINK-3-UPDOWN : interface
TenGigE 0/11/0/0 changed state to Up

```

5. 設定を確認します。

```

Router(config-if)# show running-configuration
..
Building configuration...
!! IOS XR Configuration 0.0.0
!! Last configuration change at Mon Dec 12 13:41:16 2016
!interface TenGigE 0/11/0/0
  ipv4 address 12.1.3.4 255.255.255.0

```

```
arp learning local
!
```

- ローカル ARP 学習がインターフェイスに設定したとおりに動作していることを確認します。

```
Router(config-if)# do show arp idb TenGigE 0/11/0/0 location 0/RP0/CPU0
Thu Dec 15 10:00:11.733 IST
```

```
TenGigE 0/11/0/0 (0x00000040):
  IPv4 address 12.1.3.4, Vrf ID 0x60000000
  VRF Name default
  Dynamic learning: Local
  Dynamic entry timeout: 14400 secs
  Purge delay: off
  IPv4 caps added (state up)
  MPLS caps not added
  Interface not virtual, not client fwd ref,
  Proxy arp not configured, not enabled
  Local Proxy arp not configured
  Packet IO layer is NetIO
  Srg Role : DEFAULT
  Idb Flag : 2146444
  IDB is Complete
```

- (任意) インターフェイス上で ARP トラフィックをモニタできます。

```
Router(config-if)# do show arp idb TenGigE 0/11/0/0 location 0/RP0/CPU0
Thu Dec 15 10:13:28.964 IST
```

ARP statistics:

```
Recv: 0 requests, 0 replies
Sent: 0 requests, 1 replies (0 proxy, 0 local proxy, 1 gratuitous)
Subscriber Interface:
  0 requests rcvd, 0 replies sent, 0 gratuitous replies sent
Resolve requests rcvd: 0
Resolve requests dropped: 0
Errors: 0 out of memory, 0 no buffers, 0 out of sunbet
```

ARP cache:

```
Total ARP entries in cache: 1
Dynamic: 0, Interface: 1, Standby: 0
Alias: 0, Static: 0, DHCP: 0
```

```
IP Packet drop count for GigabitEthernet0_0_0_1: 0
```

ARP の設定に関する情報

アドレス解決の概要

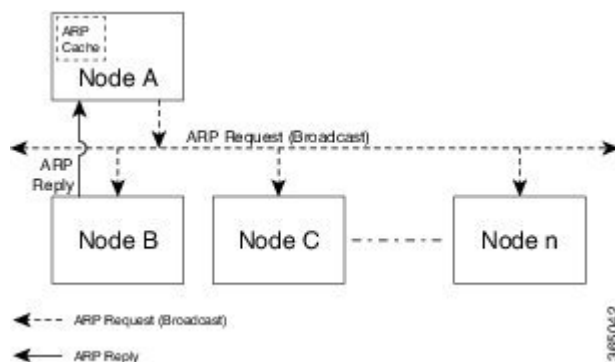
IP のデバイスは、ローカルアドレス（ローカルセグメントまたは LAN のデバイスを一意に識別）とネットワークアドレス（デバイスが属するネットワークを識別）の両方を持つことができます。ローカルアドレスは、より正確にはデータリンク アドレスとして知られています。その理由は、ローカルアドレスはパケットヘッダーのデータリンク層（OSI モデルの第 2 層）の部分にあり、データリンクデバイス（ブリッジやすべてのデバイスインターフェイスなど）

によって読み取られるからです。データリンク層内の MAC 副層がその層用にアドレスを処理するため、技術志向が強い人ほどローカルアドレスを **MAC アドレス** と呼びます。

たとえば、イーサネットではデバイスと通信するには、Cisco IOS XR ソフトウェアがまずそのデバイスの 48 ビットの MAC アドレスまたはローカルデータリンクアドレスを特定する必要があります。IP アドレスからローカルデータリンクアドレスを決定する処理は、アドレス解決と呼ばれています。

単一の LAN でのアドレス解決

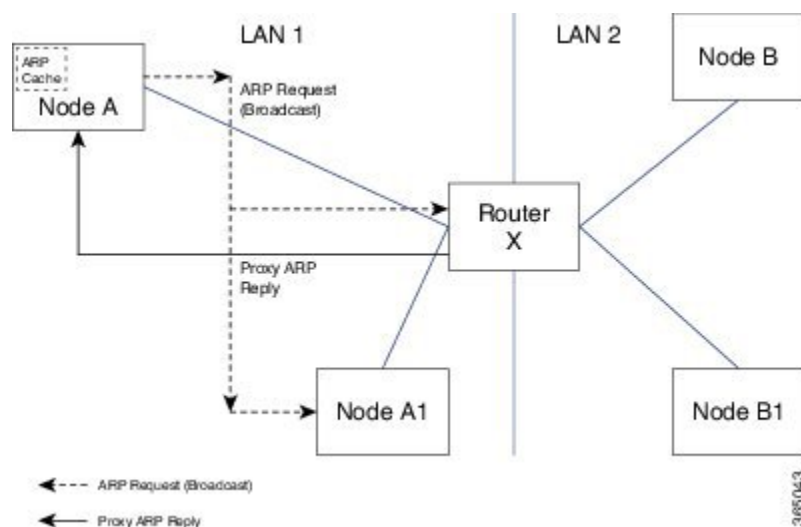
次のプロセスでは、送信元デバイスと宛先デバイスが同じ LAN に接続されている場合のアドレス解決について説明します。



1. エンドシステム A（ノード A）は ARP 要求を LAN にブロードキャストし、エンドシステム B（ノード B）の MAC アドレスの学習を試みます。
2. ブロードキャストは、エンドシステム B を含め LAN 上のすべてのデバイスで受信され、処理されます。
3. エンドシステム B のみが、ARP 要求に応答します。ARP 応答に自身の MAC アドレスを含めてエンドシステム A（ノード A）に送信します。
4. エンドシステム A（ノード A）は応答を受信し、自身の ARP キャッシュにエンドシステム B の MAC アドレスを保存します（ARP キャッシュ内で、ネットワークアドレスが MAC アドレスに関連付けられます）。
5. エンドシステム A（ノード A）はエンドシステム B との通信が必要になるたびに、ARP キャッシュをチェックしてエンドシステム B の MAC アドレスを探し、フレームを直接送信します。最初に ARP 要求を使用する必要はありません。

ルータによって相互接続されている場合のアドレス解決

次のプロセスでは、送信元デバイスと宛先デバイスが、ルータによって相互接続された異なる LAN に接続されている場合のアドレス解決について説明します（プロキシ ARP が有効になっている場合のみ）。



1. エンドシステム Y (ノード A) は ARP 要求を LAN にブロードキャストし、エンドシステム Z (ノード B) の MAC アドレスの学習を試みます。
2. ブロードキャストは、ルータ X を含め LAN 上のすべてのデバイスで受信され、処理されます。
3. ルータ X は、自身のルーティングテーブルをチェックし、エンドシステム Z (ノード B) が別の LAN 上にあることを突き止めます。
4. これにより、ルータ X はエンドシステム Z (ノード B) のプロキシとして動作します。ルータ X はエンドシステム Z (ノード B) に属しているかのように、エンドシステム Y (ノード A) からの ARP 要求に応答し、ARP 応答に自身の MAC アドレスを含めて送信します。
5. エンドシステム Y (ノード A) は ARP 応答を受信し、自身の ARP キャッシュのエンドシステム Z (ノード B) 用エントリにルータ X の MAC アドレスを保存します。
6. エンドシステム Y (ノード A) はエンドシステム Z (ノード B) との通信が必要になると、ARP キャッシュをチェックしてルータ X の MAC アドレスを探し、フレームを直接送信します。ARP 要求は使用されません。
7. ルータ X は、エンドシステム Y (ノード A) からトラフィックを受信し、それを他の LAN 上のエンドシステム Z (ノード B) に転送します。



第 3 章

シスコ エクスプレス フォワーディングの実装

- ・ [シスコ エクスプレス フォワーディングの実装 \(45 ページ\)](#)

シスコ エクスプレス フォワーディングの実装

Cisco Express Forwarding (CEF) は、拡張レイヤ 3 IP スイッチング テクノロジーです。CEF によって、インターネットや、Web ベースのアプリケーションまたは対話型セッションが集中的に使用されるネットワークなどの、大規模でダイナミックなトラフィック パターンを持つネットワークのパフォーマンスおよびスケーラビリティが最適化されます。CEF は内蔵されている機能であり、イネーブルにするために設定を行う必要はありません。必要に応じて、デフォルトのルート パージ遅延とスタティック ルートを変更できます。

コンポーネント

Cisco IOS XR ソフトウェアの CEF は常に、次の 2 種類のコンポーネントとともに CEF モードで動作します。

- ・ 転送情報ベース (FIB) データベース：プロトコル依存の FIB プロセスは、ルート プロセッサに IPv4 および IPv6 ユニキャストの転送テーブルを保持します。各ノード上の FIB はルーティング情報ベース (RIB) を更新し、ルート解決を実行してルートプロセッサに個別に FIB テーブルを保持します。各ノード上の FIB テーブルに格納されている情報は、テーブルによって若干異なることがあります。
- ・ 隣接関係テーブル：プロトコルに依存しない隣接情報ベース (AIB)

CEF は、Cisco IOS XR ソフトウェアのプライマリ IP パケット転送データベースです。CEF の役割は次の機能を果たすことです。

- ・ ソフトウェア スイッチング パス
- ・ ソフトウェアおよびハードウェア転送エンジンの転送テーブルおよび隣接関係テーブルのメンテナンス (AIB によるメンテナンス)

Cisco IOS XR ソフトウェア上の CEF では、次の機能をサポートしています。

- バンドル インターフェイスのサポート
- マルチパス サポート
- ルート整合性
- パッケージング、再起動性、リソース不足（OOR）処理などのハイ アベイラビリティ機能
- OSPFv2 SPF プレフィックス優先順位付け
- BGP 属性ダウンロード

CEF の利点

- パフォーマンス向上：CEF は、高速スイッチング ルート キャッシング よりも CPU を消費しません。より多くの CPU 処理能力を Quality of Service（QoS）や暗号化などのレイヤ 3 サービスに向けることができます。
- スケーラビリティ：CEF では、各ライン カードでスイッチング機能を最大限に活用できます。
- 復元力：CEF では、大規模な動的ネットワーク上で比類ないレベルのスイッチング一貫性と安定性を実現します。動的ネットワークでは、ルーティング変更のために、高速にスイッチングされるキャッシュ エントリが頻繁に無効化されます。ルーティング変更により、ルート キャッシュを使用した高速スイッチングではなく、ルーティング テーブルを使用したトラフィックのプロセススイッチングが行われることがあります。転送情報ベース（FIB）ルックアップテーブルにはルーティングテーブルに存在する既知のルートがすべて含まれているため、ルート キャッシュのメンテナンスが不要になるほか、高速スイッチングまたはプロセススイッチングフォワーディングのシナリオも必要ありません。CEF では、一般的なデマンドキャッシング スキームよりも効率よくトラフィックを切り替えることができます。

Cisco IOS XR ソフトウェアでは、次の CEF 転送テーブルがメンテナンスされます。

- IPv4 CEF データベース：IPv4 ユニキャスト パケット 転送用の IPv4 ユニキャスト ルートが保存されます。
- IPv6 CEF データベース：IPv6 ユニキャスト パケット 転送用の IPv6 ユニキャスト ルートが保存されます。
- MPLS LFD データベース：MPLS パケット 転送用の MPLS ラベル テーブルが保存されます。

CEF の確認

IPv4 または IPv6 CEF テーブルの詳細を表示するには、次のコマンドを使用します。

- `show cef {ipv4 address | ipv6 address} hardware egress`

IPv4 または IPv6 CEF テーブルを表示します。ネクスト ホップおよび転送インターフェイスがプレフィックスごとに表示されます。**show cef** コマンドの出力は、場所によって異なります。

```
Router# show cef 203.0.1.2 hardware egress
 203.0.1.2/32, version 0, internal 0x1020001 0x0 (ptr 0x8d7db7f0) [1], 0x0 (0x8daeedf0),
 0x0 (0x0)
Updated Nov 20 13:33:23.557
local adjacency 203.0.1.2
Prefix Len 32, traffic index 0, Adjacency-prefix, precedence n/a, priority 15
  via 203.0.1.2/32, HundredGigE0/9/0/0, 3 dependencies, weight 0, class 0 [flags 0x0]
    path-idx 0 NHID 0x0 [0x8cfc81a0 0x0]
    next hop 203.0.1.2/32
    local adjacency
```

- **show cef {ipv4 | ipv6} summary**

IPv4 または IPv6 CEF テーブルのサマリーを表示します。

```
Router#show cef ipv4 summary
Fri Nov 20 13:50:45.239 UTC
```

```
Router ID is 216.1.1.1
```

```
IP CEF with switching (Table Version 0) for node0_RP0_CPU0
```

```
Load balancing: L4
Tableid 0xe0000000 (0x8cf5b368), Vrfid 0x60000000, Vrid 0x20000000, Flags 0x1019
Vrfname default, Refcount 4129
56 routes, 0 protected, 0 reresolve, 0 unresolved (0 old, 0 new), 7616 bytes
13 rib, 0 lsd, 0:27 aib, 1 internal, 10 interface, 4 special, 1 default routes
56 load sharing elements, 24304 bytes, 1 references
1 shared load sharing elements, 432 bytes
55 exclusive load sharing elements, 23872 bytes
0 route delete cache elements
13 local route bufs received, 1 remote route bufs received, 0 mix bufs received
13 local routes, 0 remote routes
13 total local route updates processed
0 total remote route updates processed
0 pkts pre-routed to cust card
0 pkts pre-routed to rp card
0 pkts received from core card
0 CEF route update drops, 0 revisions of existing leaves
0 CEF route update drops due to version mis-match
Resolution Timer: 15s
0 prefixes modified in place
0 deleted stale prefixes
0 prefixes with label imposition, 0 prefixes with label information
0 LISP EID prefixes, 0 merged, via 0 rlocs
28 next hops
1 incomplete next hop

0 PD backwalks on LDIs with backup path
```

- **show cef { ipv4 address | ipv6 address } detail**

IPv4 または IPv6 CEF テーブルの詳細を表示します。

```
Router#show cef 203.0.1.2 detail
203.0.1.2/32, version 0, internal 0x1020001 0x0 (ptr 0x8d7db7f0) [1], 0x0 (0x8daeedf0),
 0x0 (0x0)
Updated Nov 20 13:33:23.556
local adjacency 203.0.1.2
```

```

Prefix Len 32, traffic index 0, Adjacency-prefix, precedence n/a, priority 15
gateway array (0x8d84beb0) reference count 1, flags 0x0, source aib (10), 0 backups
[2 type 3 flags 0x8401 (0x8d99a598) ext 0x0 (0x0)]
LW-LDI[type=3, refc=1, ptr=0x8daeef0, sh-ldi=0x8d99a598]
gateway array update type-time 1 Nov 20 13:33:23.556
LDI Update time Nov 20 13:33:23.556
LW-LDI-TS Nov 20 13:33:23.556
via 203.0.1.2/32, HundredGigE0/9/0/0, 3 dependencies, weight 0, class 0 [flags 0x0]
path-idx 0 NHID 0x0 [0x8cfc81a0 0x0]
next hop 203.0.1.2/32
local adjacency
Load distribution: 0 (refcount 2)

Hash OK Interface Address
0 Y HundredGigE0/9/0/0 203.0.1.2

```

• show adjacency detail

インターフェイスごとのレイヤ 2 情報など詳細な隣接情報を表示します。show adjacency コマンドの出力は、場所によって異なります。

Router#show adjacency detail

0/RP0/CPU0

| Interface | Address | Version | Refcount | Protocol |
|-----------|----------------------|---------|----------|----------|
| Hu0/9/0/0 | (interface) | 13 | 1(0) | |
| | (interface entry) | | | |
| | mtu: 1500, flags 1 4 | | | |
| Hu0/9/0/1 | (interface) | 31 | 1(0) | |
| | (interface entry) | | | |
| | mtu: 1500, flags 1 4 | | | |

フロー単位ロード バランシング

システムは基本的に 7 タプル ハッシュ アルゴリズムをサポートしています。ロード バランシングでは、レイヤ 3（ネットワーク層）およびレイヤ 4（トランスポート層）のルーティング情報に基づいてパケットを複数のリンクに分散させるルータ機能について説明します。ルータが宛先に至るパスを複数検出した場合は、その宛先の複数のエントリでルーティングテーブルが更新されます。

フロー単位のロード バランシングでは、以下の機能が実行されます。

- 着信データ トラフィックは、複数の等コスト接続に均等に分散されます。
- 着信データ トラフィックは、バンドル インターフェイス内の複数の等コスト接続メンバーリンクに均等に分散されます。
- レイヤ 2 バンドルとレイヤ 3（ネットワーク レイヤ）のロード バランシングの決定は、IPv4、IPv6、および MPLS フローで行われます。IPv4 または IPv6 のペイロードの場合は、7 タプル ハッシングが実行されます。3 つ以下のラベルが設定された MPLS ペイロードの場合は、ハードウェアが下部のペイロードを解析し、そのペイロードに IPv4 または IPv6 ヘッダーがあるかどうかを特定します。IPv4 または IPv6 ヘッダーの場合は、IP 送信元、

IP 送信先、ルータ ID、およびラベル スタックの基づいて 4 タプル ハッシングが実行されます。それ以外の場合は、MPLS ラベル ベースのハッシングが実行されます。MPLS ラベル ベースのハッシングの場合は、上位 4 ラベルがハッシュの計算に使用されます。ただし、J2 ライン カードの場合は、すべてのラベルが MPLS ラベルベースのハッシングに使用されます。

- 7 タプル ハッシュ アルゴリズムはより細かなロード バランシングを実現し、複数の等コスト レイヤ 3（ネットワーク層）パス全体でのロード バランシングに使用されます。レイヤ 3（ネットワーク層）パスは、物理 インターフェイスまたは バンドル インターフェイス上にあります。また、メンバ リンクに対するロード バランシングが、レイヤ 2 バンドル インターフェイス内で行われることがあります。
- 7 タプル ロード バランス ハッシュ 計算には以下が含まれます。
 - 送信元 IP アドレス
 - 宛先 IP アドレス
 - IP プロトコル タイプ
 - ルータ ID
 - 送信元ポート
 - 宛先ポート
 - 入力 インターフェイス



(注) 入力 インターフェイスはロード バランス ハッシュ 計算のパラメータとして考慮されないため、J2 ライン カードでは、6 タプルのロード バランス ハッシュ 計算がサポートされています。

宛先別ロード バランシング

再帰 MPLS パス（BGP 3107 を通じて学習したパスなど）を介して遷移するパケットには、宛先別ロード バランシングが使用されます。宛先別ロード バランシングとは、ルートの宛先に基づいてルータがパケットを分散します。同じネットワークへのパスが 2 つある場合、そのネットワーク上の宛先 1 へのすべてのパケットが最初のパスを介して移動し、そのネットワーク上の宛先 2 へのすべてのパケットが 2 番目のパスを介して移動するという具合になります。これにより、パケットの順序は保持されますが、リンクの使用が不等になる可能性があります。1 つのホストがトラフィックの大部分を受け取る場合は、すべてのパケットが 1 つのリンクを使用し、他のリンクの帯域幅は使用されないままとなります。宛先アドレスが多数ある場合は、より均等にリンクが使用されます。

スタティック ルートの設定

ルータは、ユーザが手動で設定したルート テーブル エントリのルート情報を使用するか、またはダイナミック ルーティング アルゴリズムで計算されたルート情報を使用して、パケット

を転送します。スタティックルートは、2つのルータ間の明示パスを定義するものであり、自動的にアップデートされません。ネットワークに変更があった場合は、ユーザが手動でスタティックルートを再設定する必要があります。スタティックルートは、ダイナミックルートに比べて使用する帯域幅が少なくなります。スタティックルートは、ネットワークトラフィックが予測可能で、ネットワーク設計がシンプルな環境で使用します。スタティックルートはネットワークの変化に対応できないので、大規模でたえず変化しているネットワークでは、スタティックルートを使用すべきではありません。大部分のネットワークは、ルータ間の通信にダイナミックルートを使用しますが、特殊な状況でスタティックルートを1つか2つ設定する場合があります。スタティックルートは、最終手段としてのゲートウェイ（ルーティング不能なすべてのパケットの送信先となるデフォルトルータ）を指定する場合にも便利です。

設定例

HundredGigE インターフェイスを介してルータ A とルータ B 間にスタティックルートを作成します。宛先 IP アドレスは 203.0.1.2/32、ネクストホップアドレスは 1.0.0.2 です。



```
Router(config)#router static address-family ipv4 unicast
Router(config-static-afi)#203.0.1.2/32 HundredGigE 0/9/0/0 1.0.0.2
Router(config-static-afi)#commit
```

実行コンフィギュレーション

```
Router#show running-config router static address-family ipv4 unicast
router static
  address-family ipv4 unicast
    203.0.1.2/32 HundredGigE 0/9/0/0 1.0.0.2
  !
!
```

確認

Next Hop Flags のフィールドに COMPLETE と表示され、設定が適切に機能していることを確認してください。

プレフィックスが更新された LPM、EXT-TCAM、LEM などのデータベースも、出力を通じて提供されます。プレフィックスのスケーリングを把握できるようになるため、ネットワークリソースを効率的に管理できます。また、デバイスに対する特定の IP アドレスの設定が失敗した理由を理解でき、デバッグが簡単になります。

```
Router#show cef 203.0.1.2/32 hardware egress details location 0/0/CPU0
Wed Nov  6 10:09:23.548 UTC
111.0.0.1/32, version 221, attached, internal 0x1000041 0x0 (ptr 0x8b00ea80) [1], 0x0
(0x8afd9768), 0x0 (0x0)
Updated Nov  6 10:08:07.424
Prefix Len 32, traffic index 0, precedence n/a, priority 2
  gateway array (0x8ae4baf0) reference count 1, flags 0x0, source rib (7), 0 backups
    [2 type 3 flags 0x40008441 (0x8af020c0) ext 0x0 (0x0)]
    LW-LDI[type=3, refc=1, ptr=0x8afd9768, sh-ldi=0x8af020c0]
    gateway array update type-time 1 Nov  6 10:08:07.423
LDI Update time Nov  6 10:08:07.423
LW-LDI-TS Nov  6 10:08:07.424
```

```

via tunnel-ip1, 0 dependencies, recursive [flags 0x8]
path-idx 0 NHID 0x0 [0x8ae0d728 0x0]
local adjacency

LEAF - HAL pd context :
sub-type : IPV4, ecd_marked:0, has_collapsed_ldi:0
collapse_bwalk_required:0, ecdv2_marked:0,
HW Walk:
LEAF:
  PI:0x308b00ea80 PD:0x308b00eb20 rev:293 type: IPV4 (0)
  LEAF location: LEM
  FEC key: 0x1640000dc6

  LWLDI:
    PI:0x308afd9768 PD:0x308afd97a8 rev:292 p-rev:291 ldi type:IP
    FEC key: 0x1640000dc6 fec index: 0x0(0) num paths:1, bkup paths: 0

REC-SHLDI HAL PD context :
ecd_marked:0, collapse_bwalk_required:0, load_shared_lb:0

RSHLDI:
  PI:0x308af020c0 PD:0x308af02190 rev:291 dpa-rev:2448 flag:0x1
  FEC key: 0x1640000dc6 fec index: 0x2001ffd8(131032) num paths: 1
  p-rev:
  Path:0 fec index: 0x2001ffd8(131032) DSP fec index: 0x20000001(1),
  TEP Encap Id: 0x40013801

LEAF - HAL pd context :
sub-type : IPV4, ecd_marked:0, has_collapsed_ldi:0
collapse_bwalk_required:0, ecdv2_marked:0,
HW Walk:
LEAF:
  PI:0x308b00e558 PD:0x308b00e5f8 rev:270 type: IPV4 (0)
  LEAF location: LEM
  FEC key: 0x1240000dc6

  LWLDI:
    PI:0x308afd9128 PD:0x308afd9168 rev:269 p-rev:268 268 ldi type:IP
    FEC key: 0x1240000dc6 fec index: 0x0(0) num paths:2, bkup paths: 0

  SHLDI:
    PI:0x308af00d88 PD:0x308af00e58 rev:268 dpa-rev:2433 cbf_enabled:0
pbts_enabled:0 flag:0x0
    FEC key: 0x1240000dc6 fec index: 0x20000001(1) num paths: 2 bkup paths: 0
    p-rev:265 262
    Path:0 fec index: 0x2001ffdc(131036) DSP:0x15 Dest fec index: 0x0(0)
    Path:1 fec index: 0x2001ffdd(131037) DSP:0x16 Dest fec index: 0x0(0)

TX-NHINFO:
  PI: 0x308c8d8298 PD: 0x308c8d8318 rev:265 dpa-rev:2431 Encap hdl:
0x308c84c350
  Encap id: 0x40010001 Remote: 0 L3 int: 1552 flags: 0x3
  npu_mask: 0x1 DMAC: f0:78:16:62:f6:a7

TX-NHINFO:
  PI: 0x308c8d80b0 PD: 0x308c8d8130 rev:262 dpa-rev:2429 Encap hdl:
0x308c84c968
  Encap id: 0x40010000 Remote: 0 L3 int: 1551 flags: 0x3
  npu_mask: 0x1 DMAC: f0:78:16:62:f6:a6

Load distribution: 0 (refcount 2)

```

| Hash | OK | Interface | Address |
|------|----|------------|------------|
| 0 | Y | tunnel-ip1 | 10.10.10.1 |

関連コマンド

- router static
- [show cef](#)

BGP 属性ダウンロード

BGP 属性ダウンロード機能を使用すると、CEF にインストールした BGP 属性を表示できます。

- **show cef bgp-attribute** コマンドは、CEF にインストールした BGP 属性を表示します。
- 属性 ID とローカル属性 ID で特定の BGP 属性を表示するには、**show cef bgp-attribute attribute-id** コマンドと **show cef bgp-attribute local-attribute-id** コマンドを使用します。

確認

```
Router# show cef bgp-attribute
Router ID is 216.1.1.1
```

```
IP CEF with switching (Table Version 0) for node0_RP0_CPU0
```

```
Load balancing: L4
Tableid 0xe0000000 (0x8cf5b368), Vrfid 0x60000000, Vrid 0x20000000, Flags 0x1019
Vrfname default, Refcount 4129
56 routes, 0 protected, 0 reresolve, 0 unresolved (0 old, 0 new), 7616 bytes
13 rib, 0 lsd, 0:27 aib, 1 internal, 10 interface, 4 special, 1 default routes
56 load sharing elements, 24304 bytes, 1 references
1 shared load sharing elements, 432 bytes
55 exclusive load sharing elements, 23872 bytes
0 route delete cache elements
13 local route bufs received, 1 remote route bufs received, 0 mix bufs received
13 local routes, 0 remote routes
13 total local route updates processed
0 total remote route updates processed
0 pkts pre-routed to cust card
0 pkts pre-routed to rp card
0 pkts received from core card
0 CEF route update drops, 0 revisions of existing leaves
0 CEF route update drops due to version mis-match
Resolution Timer: 15s
0 prefixes modified in place
0 deleted stale prefixes
0 prefixes with label imposition, 0 prefixes with label information
0 LISP EID prefixes, 0 merged, via 0 rlocs
28 next hops
1 incomplete next hop

0 PD backwalks on LDIs with backup path

VRF: default

Table ID: 0xe0000000. Total number of entries: 0
OOR state: GREEN. Number of OOR attributes: 0
```

関連コマンド

- `show cef bgp-attribute`

プロアクティブなアドレス解決プロトコルおよびネイバー探索

CEF は、レイヤ 2 隣接関係情報がないルートをインストールすると、不完全なレイヤ 3 ネクストホップを作成してハードウェアにプログラムします。この不完全なプログラミングが原因となり、最初のパケットはソフトウェア転送パスに転送されます。次に、ソフトウェア転送ではレイヤ 2 隣接関係情報を解決するために、パケットからレイヤ 2 ヘッダーを除去して、ARP（アドレス解決プロトコル）または ND（ネイバー探索）に転送します。このようなパケットでレイヤ 2 ヘッダー内に機能固有の情報が含まれていると、ソフトウェア転送パスがレイヤ 2 ヘッダーを完全に除去できないため、ARP または ND は欠落しているレイヤ 2 隣接関係情報を解決できずに、トラフィックがドロップされる結果になります。

プロアクティブな ARP および ND 機能は、欠落しているレイヤ 2 隣接関係情報を解決するために CEF が ARP または ND をプロアクティブにトリガーするようにし、ネクストホップ情報が解決されるまで 15 秒ごとに再試行することで上記の問題を解決します。したがって、不完全なネクストホップ情報を含むスタティック ルートを設定すると、この機能によって ARP または ND の解決が自動的にトリガーされます。



第 4 章

ホスト サービスとアプリケーションの実装

- [ホスト サービスとアプリケーションの実装 \(55 ページ\)](#)
- [ネットワーク接続性ツール \(55 ページ\)](#)
- [ドメイン サービス \(60 ページ\)](#)
- [TFTP サーバ, on page 61](#)
- [ファイル転送サービス, on page 62](#)
- [Cisco inetd, on page 65](#)
- [Telnet \(65 ページ\)](#)
- [Syslog の送信元インターフェイス \(66 ページ\)](#)

ホスト サービスとアプリケーションの実装

ルータ上の Cisco IOS XR ソフトウェア ホスト サービスおよびアプリケーション機能は主に、ネットワークの接続性とパケットが宛先に達するまでのルートをチェックし、ホスト名を IP アドレスに（または IP アドレスをホスト名に）マッピングして、ルータと UNIX ワークステーション間でファイルを転送するために使用します。

ネットワーク接続性ツール

ネットワーク接続性ツールを使用すると、ネットワーク上のデバイスに対して `traceroute` や `ping` を実行して、デバイスの接続をチェックできます。

ping

`ping` コマンドは、デバイスのアクセシビリティのトラブルシューティングに広く使用されている方法です。これは、2つのインターネット制御メッセージプロトコル (ICMP) クエリーメッセージ、ICMP エコー要求、および ICMP エコー応答を使用して、リモート ホストがアクティブであるかどうかを判断します。`ping` コマンドは、エコー応答を受信するまでにかかる時間も測定します。

ping コマンドは、最初に 1 つのアドレスにエコー要求パケットを送信して応答を待ちます。ping が正常に完了するのは、エコー要求が宛先に届き、定義済みの時間内に宛先が ping の送信元にエコー応答（ホスト名が存続している）を返すことができる場合だけです。

bulk オプションが導入されたため、複数の宛先の到達可能性をチェックできるようになりました。宛先は、CLI から直接入力します。このオプションは、ipv4 の宛先でのみサポートされます。

ネットワーク接続の確認

基本的なネットワーク接続性の診断を支援する手段として、多くのネットワークプロトコルがエコープロトコルをサポートしています。プロトコルでは、宛先ホストに特殊なデータグラムを送信し、そのホストからの応答データグラムを待ちます。このエコープロトコルからの結果は、ホストに至るパスの信頼性、パスの遅延、およびホストに到達できるのか、ホストが機能しているのかを評価するのに役立ちます。

ネットワーク接続を確認するための設定

次の設定は、ルータ A のインターフェイスとルータ B のインターフェイスから送信される拡張 ping コマンドを示しています。この ping が成功する場合、ルーティング上の問題がないことを示します。ルータ A はルータ B のインターフェイスに到達する方法を認識していて、ルータ B はルータ A のインターフェイスに到達する方法を認識しています。また、両方のホストには適切に設定されたデフォルト ゲートウェイがあります。

ルータ A からの拡張 ping コマンドが失敗する場合、ルーティング上の問題があることを意味します。3 つのルータのいずれでもルーティングの問題が発生する可能性があります。ルータ A では、ルータ B のインターフェイスのサブネットへのルートや、ルータ C とルータ B 間のサブネットへのルートが不明になる可能性があります。ルータ B では、ルータ A のサブネットへのルートや、ルータ C とルータ A 間のサブネットへのルートが不明になる可能性があります。ルータ C では、ルータ A またはルータ B のイーサネット セグメントのサブネットへのルートが不明になる可能性があります。ルーティングに関する問題を修正してから、ホスト 1 からホスト 2 への ping を実行する必要があります。ホスト 1 からホスト 2 への ping を実行できない場合は、両方のホストのデフォルト ゲートウェイを確認してください。ルータ A のインターフェイスとルータ B のインターフェイスとの接続は、拡張 ping コマンドを使用してチェックします。

ルータ A からルータ B のインターフェイスへの通常の ping では、ping パケットの送信元アドレスは発信インターフェイスのアドレス、つまり インターフェイスのアドレス (10.0.0.2) になります。ルータ B が ping パケットに応答するとき、送信元アドレス (つまり、10.0.0.2) に応答します。このように、ルータ A のインターフェイス (10.0.0.2) とルータ B の TenGigE インターフェイス (10.0.0.1) 間の接続だけがテストされます。

ルータ A のインターフェイス (10.0.0.2) とルータ B のインターフェイス (10.0.0.1) との接続をテストするには、拡張 ping コマンドを使用します。拡張 ping コマンドには、ping パケットの送信元アドレスを指定するオプションがあります。

設定例

この使用例では、拡張 **ping** コマンドを使用して、2 つの IP アドレス（ルータ A（10.0.0.2）とルータ B（10.0.0.1））間の IP 接続を検証します。

```
Router# ping 10.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5)
Router#!!!!
```

/If you do not enter a hostname or an IP address on the same line as the ping command, the system prompts you to specify the target IP address and several other command parameters. After specifying the target IP address, you can specify alternate values for the remaining parameters or accept the displayed default for each parameter /

```
Router# ping
Protocol [ipv4]:
Target IP address: 10.0.0.1
Repeat count [5]: 5
Datagram size [100]: 1000
Timeout in seconds [2]: 1
Interval in milliseconds [10]: 1
Extended commands? [no]: no
Sweep range of sizes? [no]:
Type escape sequence to abort.
Sending 5, 1000-byte ICMP Echos to 10.0.0.1, timeout is 1 seconds:
!!!!
Success rate is 100 percent (5/5)
Router#!!!!
```

関連コマンド

複数の宛先に対するネットワーク接続性のチェック

bulk オプションを使用すると、複数の宛先への到達可能性をチェックできます。宛先は、CLI から直接入力します。このオプションは、**ipv4** の宛先でのみサポートされます。

設定例

次の IP アドレスを持つ IP ネットワーク上の複数のホストへの到達可能性とネットワーク接続を確認します。

- 1: 1.1.1.1
- 2: 2.2.2.2
- 3: 3.3.3.3

```
Router# ping bulk ipv4 input cli batch
*/You must hit the Enter button and then specify one destination address per line*/
Please enter input via CLI with one destination per line and when done Ctrl-D/(exit) to
initiate pings:
1: 1.1.1.1
2: 2.2.2.2
3: 3.3.3.3
4:
```

```

Starting pings...
Target IP address: 1.1.1.1
Repeat count [5]: 5
Datagram size [100]: 1
% A decimal number between 36 and 18024.
Datagram size [100]: 1
% A decimal number between 36 and 18024.
Datagram size [100]: 1000
Timeout in seconds [2]: 1
Interval in milliseconds [10]: 10
Extended commands? [no]: no
Sweep range of sizes? [no]: q
% Please answer 'yes' or 'no'.
Sweep range of sizes? [no]: q
% Please answer 'yes' or 'no'.
Sweep range of sizes? [no]:
Type escape sequence to abort.
Sending 5, 1000-byte ICMP Echos to 1.1.1.1, vrf is default, timeout is 1 seconds:
!!!!
Success rate is 100 percent (5/5),
Target IP address: 2.2.2.2
Repeat count [5]:
Datagram size [100]: q
% A decimal number between 36 and 18024.
Datagram size [100]:
Timeout in seconds [2]:
Interval in milliseconds [10]:
Extended commands? [no]:
Sweep range of sizes? [no]:
Sending 5, 100-byte ICMP Echos to 1.1.1.1, vrf is default, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5),
Target IP address: 3.3.3.3
Repeat count [5]: 4
Datagram size [100]: 100
Timeout in seconds [2]: 1
Interval in milliseconds [10]: 10
Extended commands? [no]: no
Sweep range of sizes? [no]: no
Sending 4, 100-byte ICMP Echos to 1.1.1.1, vrf is default, timeout is 1 seconds:
!!!!
Success rate is 100 percent (4/5),

```

関連コマンド

tracert

ping コマンドを使用してデバイス間の接続性を検証できる場合は、**tracert** コマンドを使用してパケットがリモート接続先までにたどるパスおよびルーティングに障害がある場所を検出できます。

tracert コマンドは、各 ICMP "time-exceeded" メッセージの送信元を記録して、パケットが宛先に達するまでにたどったパスを示すことができます。IP **tracert** コマンドを使用すると、パケットがネットワーク経由でたどるパスをホップバイホップで特定できます。このコマンドを実行すると、トラフィックが宛先に到達するまでに通過するルータなどのすべてのネットワーク層（レイヤ 3）デバイスが表示されます。

traceroute コマンドは、IP ヘッダーの存続可能時間（TTL）フィールドを使用して、ルータとサーバで特定のリターンメッセージが生成されるようにします。**traceroute** コマンドは、TTL フィールドが 1 に設定されている宛先ホストに、ユーザデータグラムプロトコル（UDP）データグラムを送信します。ルータは 1 または 0 の TTL 値を検出すると、データグラムをドロップし、送信元に ICMP の **time-exceeded** メッセージを戻します。**traceroute** 機能は、ICMP **time-exceeded** メッセージの送信元アドレス フィールドを調べ、最初のホップのアドレスを判別します。

ネクスト ホップを識別するために、**traceroute** コマンドは TTL 値が 2 の UDP パケットを送信します。1 番めのルータは、TTL フィールドの値から 1 を差し引いて次のルータにデータグラムを送信します。2 番めのルータは、TTL 値が 1 の UDP パケットを受け取り、データグラムを廃棄して、送信元に **time-exceeded** メッセージを戻します。このように、データグラムが宛先ホストに到達するまで（または TTL の最大値に達するまで）TTL の値は増分され、処理が続けられます。

データグラムが宛先に到達したことを判断するために、**traceroute** コマンドは、宛先ホストが使用しないと予測される非常に大きな値をデータグラムの UDP 宛先ポートに設定します。ホストは、この未知のポート番号を持つデータグラムを受信すると、送信元に ICMP **port unreachable error** メッセージを戻します。このメッセージにより、宛先に到達したことを **traceroute** 機能に伝えます。

パケットルートのチェック

traceroute コマンドを使用すると、パケットが宛先に到達するまでに実際にたどるルートをトレースできます。

設定例

10.0.0.2 から 20.1.1.1 へのルートをトレースします。

```
Router# traceroute 20.1.1.1
Type escape sequence to abort.
Tracing the route to 20.1.1.1
  1  10.0.0.1 39 msec  *   3 msec
```

/If you do not enter a hostname or an IP address on the same line as the traceroute command, the system prompts you to specify the target IP address and several other command parameters. After specifying the target IP address, you can specify alternate values for the remaining parameters or accept the displayed default for each parameter/

```
Router #traceroute
Protocol [ipv4]:
Target IP address: 20.1.1.1
Source address: 10.0.0.2
Numeric display? [no]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
```

```
Type escape sequence to abort.
```

```
Tracing the route to 20.1.1.1
 0  10.0.0.1 3 msec  *  3 msec
```

関連コマンド

ドメイン サービス

Cisco IOS XR ソフトウェア ドメイン サービスは、Berkeley Standard Distribution (BSD) ドメイン リゾルバとして機能します。ドメイン サービスは、アプリケーション (Telnet など) やコマンド (**ping**、**traceroute** など) で使用される、ホスト名対アドレスのマッピングのローカル キャッシュを保持します。ローカルキャッシュにより、ホスト名からアドレスへの変換の速度が向上します。ローカルキャッシュには、2つのタイプのエントリが存在します。スタティク とダイナミックです。**domain ipv4 host** または **domain ipv6 host** コマンドを使用して設定されたエントリはスタティク エントリとして追加され、ネーム サーバから受信したエントリはダイナミック エントリとして追加されます。

ネーム サーバは、World Wide Web (WWW) でネットワーク ノードの名前をアドレスに変換するために使用されます。ネーム サーバは、DNS サーバから DNS プロトコルを使用して、ホスト名を IP アドレスにマッピングする分散データベースを維持します。**domain name-server** コマンドを使用して、1つ以上のネーム サーバを指定できます。

アプリケーションでホストの IP アドレスまたは IP アドレスのホスト名が必要になると、ドメイン サービスに対してリモート プロシージャ コール (RPC) が実行されます。ドメイン サービスは、キャッシュ内で IP アドレスまたはホスト名を探し、エントリが見つからない場合にはネーム サーバに DNS クエリーを送信します。

ドメイン名要求を完了するために Cisco IOS XR ソフトウェアで使用するデフォルト ドメイン名を指定できます。単一のドメインまたはドメイン名のリストを指定することもできます。IP ホスト名にドメイン名が含まれていない場合には、ホスト テーブルに追加される前に指定のドメイン名が付加されます。1つまたは複数のドメイン名を指定するには、**domain name** コマンドまたは **domain list** コマンドを使用します。

ドメイン サービスの設定

デフォルトでは、DNS によるホスト名からアドレスへの変換がイネーブルになっています。**domain lookup disable** コマンドによってホスト名からアドレスへの変換がディセーブルになっている場合は、**no domain lookup disable** コマンドを使用して変換を再びイネーブルにします。

設定例

スタティク ホスト名とアドレスのマッピングを定義します。IPv4 アドレスを2つのホスト (192.168.7.18 と 10.2.0.2 192.168.7.33) に関連付けます (またはマッピングします)。ホスト名は host1 と host2 です。

```
Defining the Domain Host
=====
Router# configure
Router(config)#domain ipv4 host host1 192.168.7.18
```

```
Router(config)#domain ipv4 host host2 10.2.0.2 192.168.7.33
Router(config)#commit
```

```
Defining the Domain Name
=====
```

```
*/Define cisco.com as the default domain name/*
Router#configure
Router(config)#domain name cisco.com
Router(config)#commit
```

```
Specifying the Addresses of the Name Servers
=====
```

```
*/Specify host 192.168.1.111 as the primary name server
and host 192.168.1.2 as the secondary server/*
Router#configure
Router(config)#domain name-server 192.168.1.111
Router(config)#domain name-server 192.168.1.2
Router(config)#commit
```

確認

```
Router#show hosts
Default domain is cisco.com
Name/address lookup uses domain service
Name servers: 192.168.1.111, 192.168.1.2
```

| Host | Flags | Age(hr) | Type | Address(es) |
|-------|------------|---------|------|--------------------------|
| host2 | (perm, OK) | 0 | IP | 10.2.0.2 192.168.7.33 |
| host1 | (perm, OK) | 0 | IP | 192.168.7.18 |

関連コマンド

TFTP サーバ

サーバとしてのみ機能するマシンをネットワークの各セグメントに配置するのは、コストがかかり、非効率的です。しかし、すべてのセグメントにサーバがあるのではない場合、ネットワークセグメントを超えたネットワークの操作によって相当の遅延が引き起こされることがあります。ルータを TFTP サーバとして機能するように設定すると、ルータの通常の機能を使用しながらコストと遅延時間を削減できます。

通常、TFTP サーバとして設定するルータでは、ルータがクライアントルータからの要求に対応できるようになります。この設定には、フラッシュメモリからのシステムイメージまたはルータのコンフィギュレーションファイルをクライアントルータに提供するなどのサービスが含まれます。他のタイプのサービス要求に応答するようにルータを設定することもできます。

TFTP サーバとしてのルータの設定

TFTP 機能の実装前に、サーバとクライアントルータは互いに到達可能である必要があります。ping コマンドを使用してサーバとクライアントルータ間の接続を（いずれかの方向で）テストして、この接続を検証します。

このタスクを実行すると、ルータを TFTP サーバとして設定できます。これにより、TFTP クライアントとして機能する他のデバイスは、slot0: や /tmp などの特定のディレクトリ（TFTP ホーム ディレクトリ）の下にあるファイルをルータに対して読み書きできます。



(注) セキュリティを確保するため、ファイルがすでに存在していないと、TFTP サーバでは書き込み要求を正常に完了できません。

TFTP 機能の実装前に、サーバとクライアント ルータは互いに到達可能である必要があります。ping コマンドを使用してサーバとクライアント ルータ間の接続を（いずれかの方向で）テストして、この接続を検証します。

設定例

TFTP サーバとしてルータを設定します（ホーム ディレクトリの disk0:）。

```
Router#configure
Router(config)#tftp ipv4 server homedir disk0
Router(config)#commit
```

実行コンフィギュレーション

```
Router#show running-config tftp ipv4 server homedir disk0:
tftp vrf default ipv4 server homedir disk0:
```

確認

```
Router#show cinetd services
Vrf Name Family Service      Proto Port ACL  max_cnt  curr_cnt wait  Program Client Option
default  v4      tftp      udp    69      unlimited 0      wait   tftpd   sysdb  disk0:
default  v4      telnet    tcp    23      10       0      nowait telnetd sysdb
```

関連コマンド

ファイル転送サービス

ファイル転送プロトコル（FTP）、簡易ファイル転送プロトコル（TFTP）、リモート コピー プロトコル（RCP）の各クライアント、およびセキュアコピープロトコル（SCP）はファイル システムまたはリソース マネージャとして実装されます。たとえば、tftp:// で始まるパス名は TFTP リソース マネージャによって処理されます。

ファイルシステムインターフェイスは、URL を使用して、ファイルの場所を指定します。URL は、WWW でファイルまたは場所を指定するのに広く使用されています。ただし、Cisco ルータの URL には、ルータまたはリモート ファイル サーバ上のファイルの場所も指定されます。

ルータがクラッシュしたときは、ルータのメモリ内容全体のコピーを取得するのが便利です（これをコア ダンプと言います）。テクニカル サポート担当者が、クラッシュの原因を特定

するのに使用します。SCP、FTP、TFTP、RCP を使用すると、コア ダンプをリモート サーバに保存できます。

FTP

ファイル転送プロトコル (FTP) は、TCP/IP プロトコルスタックの一部であり、ネットワーク ノード間でファイルを転送するのに使用します。FTP は、RFC 959 で定義されています。

FTP 接続使用時のルータ設定

FTP 接続を使用してネットワーク上のシステム間でファイルを転送するようにルータを設定できます。次の FTP の特性を設定できます。

- パッシブ モード FTP
- パスワード
- IP アドレス

設定例

ルータによる FTP 接続の使用をイネーブルにします。パッシブ FTP 接続を使用するようにソフトウェアを設定し、匿名ユーザのパスワードを設定して、FTP 接続の送信元 IP アドレスも指定します。

```
Router#configure
Router(config)#ftp client passive
(Optional) Router(config)#ftp client vrf vrfA
Router(config)#ftp client anonymous-password xxxx
Router(config)#ftp client source-interface HundredGigE 0/9/0/0
Router(config)#commit
```

実行コンフィギュレーション

```
Router#show running-config ftp client passive
ftp client passive
ftp client vrf vrfA
Router#show running-config ftp client anonymous-password xxxx
ftp client anonymous-password xxxx
Router#show running-config ftp client source-interface HundredGigE 0/9/0/0
ftp client source-interface HundredGigE 0/9/0/0
```

関連コマンド

- ftp client passive
- ftp client anonymous-password
- ftp client source-interface

TFTP

Trivial File Transfer Protocol (TFTP) は FTP の簡易版で、ネットワークを介して 1 つのコンピュータから別のコンピュータにファイルを転送できます。通常は、クライアント認証（ユーザ名とパスワードなど）を使用しません。

TFTP 接続使用時のルータ設定

設定例

TFTP 接続を使用するようにルータを設定し、TFTP 接続の送信元アドレスとして HundredGigE 0/9/0/0 の IP アドレスを設定します。

```
Router#configure
Router(config)#tftp client source-interface HundredGigE 0/9/0/0
Router(config)#commit
```

実行コンフィギュレーション

```
Router#show running-config tftp client source-interface HundredGigE 0/9/0/0
tftp client source-interface HundredGigE 0/9/0/0
```

確認

```
Router#show cinetd services
```

| Vrf | Name | Family | Service | Proto | Port | ACL | max_cnt | curr_cnt | wait | Program | Client | Option |
|---------|------|--------|---------|-------|-----------|-----|---------|----------|-------|---------|--------|--------|
| default | v4 | tftp | udp | 69 | unlimited | 0 | wait | tftpd | sysdb | disk0: | | |
| default | v4 | telnet | tcp | 23 | 10 | 0 | nowait | telnetd | sysdb | | | |

関連コマンド

- tftp client source-interface type
- show cinetd services

SCP

セキュア コピー プロトコル (SCP) は、ファイルを転送するための認証されたセキュアな方式を提供するファイル転送プロトコルです。SCP は SSHv2 に依存して、リモート ロケーションからローカル ロケーションに、またはローカル ロケーションからリモート ロケーションにファイルを転送します。

Cisco IOS XR ソフトウェアは SCP サーバ操作とクライアント操作をサポートしています。デバイスが SCP 要求を受信すると、SSH サーバプロセスはクライアントとやり取りする SCP サーバプロセスを生成します。各着信 SCP サブシステム要求に対して新しい SCP サーバインスタンスが生成されます。デバイスが宛先デバイスにファイル転送要求を送信する場合、そのデバイスはクライアントとして機能します。

デバイスがファイル転送のためにリモート ホストとの SSH 接続を開始すると、リモート デバイスはソース モードまたはシンク モードで要求に応答することができます。ソース モードで

は、デバイスはファイル ソースになります。デバイスはそのローカル ディレクトリからファイルを読み取り、目的の宛先に転送します。シンクモードでは、デバイスは転送するファイルの宛先になります。

SCP を使用して、ローカル デバイスから宛先デバイスに、または宛先デバイスからローカル デバイスにファイルをコピーできます。

SCP では、個々のファイルの転送のみを実行できます。宛先デバイスから別の宛先デバイスにファイルを転送することはできません。

SCP によるファイル転送

セキュア コピー プロトコル (SCP) を使用すると、送信元デバイスと宛先デバイス間でファイルを転送できます。一度に 1 つのファイルを転送できます。宛先がサーバの場合は、SSH サーバ プロセスが実行されている必要があります。

設定例

ファイル「test123.txt」をローカル ディレクトリからリモート ディレクトリに転送します。

```
Router#scp /harddisk:/test123.txt xyz@1.75.55.1:/auto/remote/test123.txt
Connecting to 1.75.55.1...
Password:
Router#commit
```

確認

テキスト「test123.txt」ファイルがコピーされたことを確認します。

```
xyz-lnx-v1:/auto/remote> ls -altr test123.txt
-rw-r--r-- 1 xyz eng 0 Nov 23 09:46 test123.txt
```

関連コマンド

- scp

Cisco inetd

Cisco インターネット サービス プロセス デーモン (Cinetd) は、システムのブート後にシステム マネージャによって開始されるマルチスレッドサーバプロセスです。Cinetd は、Telnet サービスや TFTP サービスなどのインターネット サービスをリッスンします。Cinetd が特定のサービスをリッスンするかどうかは、ルータ コンフィギュレーションによって異なります。たとえば、**tftp server** コマンドを入力すると、Cinetd は TFTP サービスのリッスンを開始します。要求が届くと、Cinetd はサービスに関連付けられたサーバ プログラムを実行します。

Telnet

Telnet をイネーブルにすると、ネットワークング デバイスで着信 Telnet 接続が許可されます。

設定例

Telnetをイネーブルにして、ルータに同時にアクセスできるユーザの数を10人に制限します。

```
Router# configure
Router(config)# telnet ipv4 server max-servers 10
Router(config)# commit
```

確認

```
Router# show cinetd services
Vrf Name  Family  Service  Proto Port ACL max_cnt  curr_cnt  wait  Program Client
Option
default  v4          tftp      udp  69      unlimited  0        wait  tftpd  sysdb
disk0:
default  v4          telnet     tcp  23      10        nowait  telnetd sysdb
```

関連コマンド

Syslog の送信元インターフェイス

ロギング送信元インターフェイスを設定すると、特定のルータから VRF で発信される syslog トラフィックを、単一のデバイスからの着信として識別できます。

設定例

リモート Syslog サーバの送信元インターフェイスをイネーブルにします。デフォルトの vrf のロギング送信元インターフェイスとして loopback 2 を設定します。

```
Router#configure
Router(config)#logging source-interface Loopback2
Router(config)#logging source-interface Loopback3 vrf vrfa
Router(config)#commit
```

実行コンフィギュレーション

```
Router#show running-config logging
/*Logging configuration after changing the source into loopback2 interface.
logging console debugging
logging monitor debugging
logging facility local4
logging 123.100.100.189 vrf default severity info port default
logging source-interface Loopback2
logging source-interface Loopback3 vrf vrfa
```

関連コマンド

- logging source-interface
- show running-configuration logging



第 5 章

ダイナミックホストコンフィギュレーション ンプロトコルの実装

- [回線 ID およびリモート ID を持つ DHCP Option-82](#) (67 ページ)
- [DHCP リレー エージェントの設定の前提条件](#) (68 ページ)
- [DHCP リレー機能の制限事項](#) (68 ページ)
- [DHCP リレー エージェントを設定およびイネーブルにする方法](#) (69 ページ)
- [DHCP プロキシプロファイルの設定](#) (79 ページ)
- [DHCP サーバ](#) (79 ページ)
- [DHCP クライアント](#) (84 ページ)
- [DHCPv6 プロキシバインディング テーブルのリロード永続性](#) (85 ページ)

回線 ID およびリモート ID を持つ DHCP Option-82

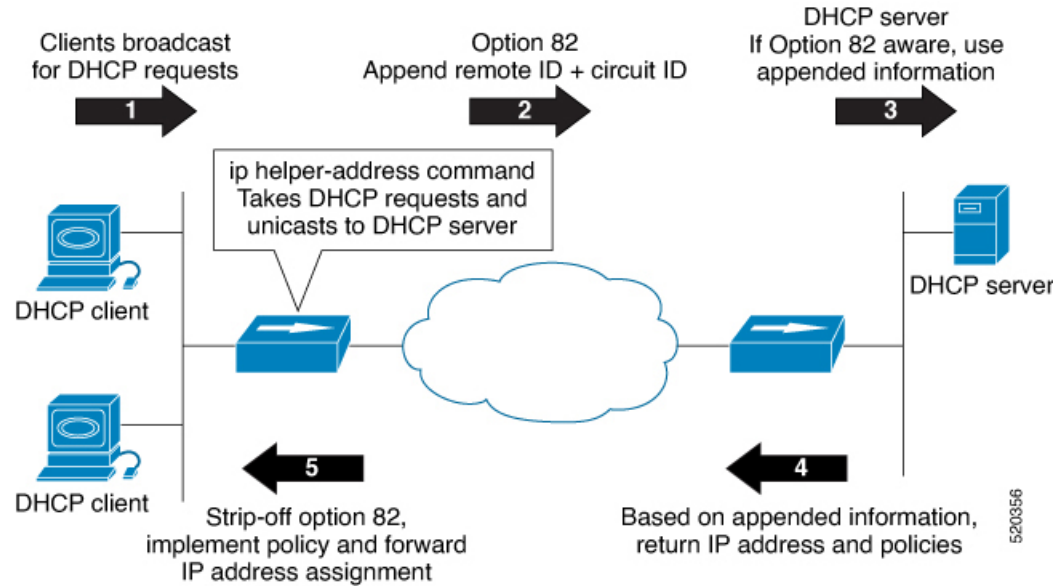
DHCP リレーエージェント情報オプション (Option-82) では、Dynamic Host Configuration Protocol (DHCP) リレーエージェントがクライアントから発信された DHCP パケットを DHCP サーバに転送する際に、エージェント自体の情報をパケットに含めることができます。DHCP サーバでは、この情報を使用して、IP アドレスまたはその他のパラメータ割り当てポリシーを実装します。

この機能は、エージェントリモート ID と呼ばれる DHCP リレーエージェント情報オプションのサブオプションを使用して、DHCP サーバに情報を伝えます。エージェントリモート ID に組み込まれて送信される情報には、リレーエージェントを識別する IP アドレス 1 つと、着信する DHCP 要求が経由する ATM インターフェイスおよび PVC に関する情報が含まれます。DHCP サーバはこの情報を使用して、IP アドレスの割り当てとセキュリティポリシーの決定を行うことができます。

図では、DHCP クライアントが DHCP 要求を生成し、ネットワーク上でブロードキャストする時点を示しています。DHCP リレーエージェントはブロードキャスト DHCP 要求パケットを代行受信し、パケット内にリレーエージェント情報オプション (option-82) を挿入します。リレーエージェント情報オプションには、関連するサブオプションが含まれています。DHCP リレー エージェントは DHCP パケットを DHCP サーバにユニキャストします。DHCP サーバはパケットを受信し、サブオプションを使用して IP アドレスや他の設定パラメータを割り当て、

クライアントに転送します。サブオプションフィールドは、クライアントへの転送の際にリレーエージェントによってパケットから取り除かれます。

図 10: DHCP リレー option-82 を使用したパケットの転送



Cisco IOS XR リリース 7.1.1 より、DHCP IPv4 リレーエージェントには、DHCP IPv4 リレーパケットのリモート ID と回線 ID 情報が含まれています。

BVI インターフェイスを介してリレーされる DHCP IPv4 パケットは、リレーエージェントのリレー情報オプションポリシーを表示します。DHCP IPv4 アプリケーションには、option-82 のリモート ID と回線 ID が含まれており、それらの ID はサーバに転送されます。

DHCP リレー エージェントの設定の前提条件

DHCP リレー エージェントを設定するための前提条件は、次のとおりです。

- 適切なタスク ID を含むタスク グループに関連付けられているユーザグループに属している必要があります。このコマンドリファレンスには、各コマンドに必要なタスク ID が含まれます。ユーザ グループの割り当てが原因でコマンドを使用できないと考えられる場合、AAA 管理者に連絡してください。
- 設定済みで動作している DHCP クライアントおよび DHCP サーバ。
- リレー エージェントと DHCP サーバ間の接続

DHCP リレー機能の制限事項

DHCP リレー機能の実装に関する制限事項は次のとおりです。

- マルチキャストアドレスはサポートされていません。DHCP リレー プロファイル サブモードの **helper-address** コマンドは、ヘルパー アドレスとしてグローバル ユニキャスト IP アドレスのみをサポートします。
- パケットを DHCP サーバに転送するときにリレーエージェントによって追加される DHCP オプション コードは、**interface-id** と **remote-id** のみです。



(注) DHCP リレー プロファイル サブモードでは、DHCP オプション コードの設定はサポートされていません。

DHCP リレー エージェントを設定およびイネーブルにする方法

ここでは、次のタスクについて説明します。

DHCP リレー エージェントの設定およびイネーブル化

設定例

```
Router# configure
/* Enters the global configuration mode */

Router(config)# dhcp ipv4
/* Configures DHCP for IPv4 and enters the DHCPv4 configuration submode. */

Router(config-dhcpv4)# profile r1 relay
/* Enables DHCP relay profile */

Router(config-dhcpv4-relay-profile)# helper-address vrf A 10.10.10.1 giaddr 40.1.1.2
Router(config-dhcpv4-relay-profile)# broadcast-flag policy check
/* Configures VRF addresses for forwarding UDP broadcasts, including DHCP. */

Router(config-dhcpv4-relay-profile)# relay information option vpn
Router(config-dhcpv4-relay-profile)# relay information option vpn-mode rfc
/* Inserts the DHCP relay agent information option (option-82 field) in forwarded
BOOTREQUEST messages to a DHCP server. */

Router(config-dhcpv4-relay-profile)# relay information option allow-untrusted
/* (Optional) Configures the DHCP IPv4 Relay not to discard BOOTREQUEST packets
that have an existing relay information option and the giaddr set to zero. */

Router(config-dhcpv4-relay-profile)# exit
Router(config-dhcpv4)# interface BVI 1 relay profile r1
Router(config-dhcpv4)# commit
/* Configures DHCP relay on a BVI interface and commits the configuration */
```

実行コンフィギュレーション

```
Router#show running-config
Tue May 23 10:56:14.463 IST
Building configuration...
!! IOS XR Configuration 0.0.0
!! Last configuration change at Tue May 23 10:56:08 2017 by annseque
!
dhcp ipv4
  vrf vrf1 relay profile client
  profile r1 relay
    helper-address vrf A 10.10.10.1 giaddr 40.1.1.2
    broadcast-flag policy check
    relay information option vpn
    relay information option vpn-mode rfc
    relay information option allow-untrusted
  !
```

DHCP リレー Option-82 の設定およびイネーブル化

設定例

リモート ID と回線 ID 情報を使用した DHCP IPv4 リレーエージェント設定の例を次に示します。BVI インターフェイスに関連付けられている DHCP IPv4 リレープロファイル設定内のリモート ID 設定を設定します。また、レイヤ 2 トランスポート AC の DHCP IPv4 パケット設定に回線 ID 情報を設定します。

```
Router# configure
/* Enters the global configuration mode */

Router(config)# dhcp ipv4
/* Configures DHCP for IPv4 and enters the DHCPv4 configuration submode. */

Router(config-dhcpv4)# profile test relay
/* Enables DHCP relay profile */

Router(config-dhcpv4-relay-profile)# helper-address vrf1 10.20.0.4 giaddr 10.20.0.1
Router(config-dhcpv4-relay-profile)# broadcast-flag policy check
/* Configures VRF addresses for forwarding UDP broadcasts, including DHCP. */

Router(config-dhcpv4-relay-profile)# relay information option vpn
Router(config-dhcpv4-relay-profile)# relay information check
Router(config-dhcpv4-relay-profile)# relay information option
Router(config-dhcpv4-relay-profile)# relay information policy drop
Router(config-dhcpv4-relay-profile)# relay information option vpn-mode rfc
Router(config-dhcpv4-relay-profile)# relay information option remote-id format-type hex
12
/*Configures the remote ID on DHCP relay */
/* Inserts the DHCP relay agent information option (option-82 field) in forwarded
BOOTREQUEST messages to a DHCP server. */

Router(config-dhcpv4-relay-profile)# relay information option allow-untrusted
/* (Optional) Configures the DHCP IPv4 Relay not to discard BOOTREQUEST packets
that have an existing relay information option and the giaddr set to zero. */

Router(config-dhcpv4-relay-profile)# exit
Router(config-dhcpv4)# interface BVI 1 relay profile test1
Router(config-dhcpv4)# interface Bundle-Ether1.29 relay information option circuit-id
format-type ascii 120
```



```
/*Configures the circuit ID on the DHCP relay */
Router(config-dhcpv4)# commit
/* Configures DHCP relay on a BVI interface and commits the configuration */
```

実行コンフィギュレーション

```
Router#show running-config
dhcp ipv4

!
profile test1 relay
  helper-address vrf vrfl 10.20.0.4 giaddr 10.20.0.1
  relay information option vpn
  relay information check
  relay information option
  relay information policy drop
  relay information option vpn-mode rfc
  relay information option remote-id format-type hex 12
  relay information option allow-untrusted

interface BVI2 relay profile test1
interface Bundle-Ether1.29 relay information option circuit-id format-type ascii 120

interface Bundle-Ether1.29 l2transport
  encapsulation dot1q 29
  rewrite ingress tag pop 1 symmetric
!

l2vpn
  bridge group IRB
  bridge-domain DHCP1
  interface Bundle-Ether1.29
    split-horizon group
  !
```

インターフェイスでの DHCPv6 リレー エージェントのイネーブル化

このタスクでは、インターフェイスで Cisco IOS XR DHCPv6 リレー エージェントをイネーブルにする方法について説明します。



- (注) Cisco IOS XR ソフトウェアでは、DHCPv6 リレー エージェントがデフォルトでディセーブルになっています。

```
RP/0/RP0/CPU0:router# configure terminal
RP/0/RP0/CPU0:router(config)# dhcp ipv6
RP/0/RP0/CPU0:router(config-dhcpv6)# interface type interface-instance relay profile
profile-name
RP/0/RP0/CPU0:router(config-dhcpv6-if)# commit
```

インターフェイスでの DHCP リレーのディセーブル化

このタスクでは、インターフェイスにプロファイルを割り当てないことにより、インターフェイスで DHCP リレーをディセーブルにする方法について説明します。

```
Router# configure terminal
Router(config)# dhcp ipv6
Router(config-dhcpv6)# interface type name none
Router(config-dhcpv6-if)# commit
```

VRF での DHCP リレーのイネーブル化

このタスクでは、VRF で DHCP リレーをイネーブルにする方法について説明します。

```
/CPU0:router# configure terminal
Router(config)# dhcp ipv6
Router(config-dhcpv6)# vrf vrf-name relay profile profile-name
Router(config-dhcpv6-if)# commit
```

複数のヘルパー アドレスを使用した DHCP リレー プロファイルの設定

DHCPv4 または DHCPv6 リレー プロファイルには、最大 16 のヘルパー IPv4 および IPv6 アドレスを設定できます。

1. DHCPv4 または DHCPv6 コンフィギュレーション モードを開始します。

```
Router(config)# dhcp ipv6
```

2. DHCPv4 または DHCPv6 リレー プロファイルを設定します。

```
Router(config-dhcpv6)# profile helper relay
```

3. ヘルパー アドレスを設定します。



(注) 最大 16 の IPv4 および IPv6 アドレスを設定できます。

```
Router(config-dhcpv6-relay-profile)# helper-address vrf default 2001:1:1::2
```

4. 設定を確認します。

```
Router(config-dhcpv6-relay-profile)# show configuration
```

```
!! IOS XR Configuration 0.0.0
dhcp ipv6
  profile helper relay
    helper-address vrf default 2001:1:1::2
  !
!
end
```

5. 設定をコミットします。

```
Router(config-dhcpv6-relay-profile)# commit
```

6. コンフィギュレーション モードを終了し、設定されているヘルパー アドレスを確認します。

```
Router# show dhcp ipv6 relay profile name helper
...
Profile: helper
Helper Addresses:
    2001:1:1::2, vrf default
Information Option: Disabled
Information Option Allow Untrusted: Disabled
Information Option VPN: Disabled
Information Option VPN Mode: RFC
Information Option Policy: Replace
Information Option Check: Disabled
GIADDR Policy: Keep
Broadcast-flag Policy: Ignore
VRF References:
Interface References:
```

DHCPv6 リレー ヘルパー アドレスが正常に設定されています。

プレフィックス委任の DHCP リレー エージェント通知

プレフィックス委任の DHCP リレー エージェント通知を使用すると、DHCPv6 リレー エージェントとして動作するルータは、リレー エージェントからクライアントに中継される DHCP RELAY-REPLY パケットの内容を確認することによって、プレフィックス委任オプションを見つけることができます。リレー エージェントは、プレフィックス委任オプションを検出すると、委任されるプレフィックスに関する情報を抽出し、プレフィックス委任情報と一致する IPv4 または IPv6 加入者ルートをリレー エージェントに挿入します。その後リレー経由でそのプレフィックスに宛てられたパケットは、プレフィックス委任に含まれる情報に基づいて転送されます。IPv4 または IPv6 加入者ルートは、プレフィックス委任のリース期間が経過するか、またはリレー エージェントがプレフィックス委任を解放するクライアントから解放パケットを受信するまで、ルーティング テーブルに保持されます。

リレー エージェントは、自動的に加入者ルート管理を行います。

IPv4 または IPv6 ルートは、リレー エージェントが RELAY-REPLY パケットを中継すると追加され、プレフィックス委任のリース期間が経過するか、リレー エージェントが解放メッセージを受信すると削除されます。プレフィックス委任のリース期間を延長するときに、リレー エージェントのルーティング テーブル内の IPv4 または IPv6 加入者ルートを更新できます。

この機能により、IPv4 または IPv6 ルートはリレー エージェントのルーティング テーブルに保持されます。この登録された IPv4 または IPv6 アドレスを使用すると、ユニキャスト RPF (uRPF) の動作が可能になりますが、そのためには、リバース ルックアップを実行するルータがリレー エージェント上の IPv4 または IPv6 アドレスが正しく、スプーフィングされていないことを確認できるようにします。リレー エージェントのルーティング テーブル内の IPv6 ルートを他のルーティングプロトコルに再配布して、サブネットを他のノードにアドバタイズできます。クライアントが DHCP_DECLINE メッセージを送信すると、ルートは削除されます。

プレフィックス委任のための DHCP ステートフル リレー エージェントの設定

プレフィックス委任用にダイナミック ホスト コンフィギュレーション プロトコル DHCP リレー エージェント通知を設定するには、このタスクを実行します。

設定例

1. DHCP プロファイルの設定
2. DHCP リレー エージェントの設定
3. IPv4 または IPv6 DHCP ステートフル リレー エージェントとして機能する IPv4 または IPv6 DHCP をインターフェイスでイネーブルにします。
4. プロファイル名を設定します。

設定

```
/* Enter the global configuration mode and then enter the DHCPv6 configuration mode. */
Router# config
Router(config)# dhcp ipv6
Router(config-dhcpv6)#

/* Enter the proxy profile configuration mode and configure the DHCPv6 relay agent. */
Router(config-dhcpv6)# profile downstream proxy
Router(config-dhcpv6-profile)# helper-address 2001:db8::1 GigabitEthernet 0/1/0/1

/* Exits from the proxy profile configuration mode and enable IPv6 DHCP on an interface.
*/
Router(config-dhcpv6-profile)# exit
Router(config-dhcpv6-if)# interface GigabitEthernet 0/1/0/0 proxy

/* Configure a profile name. */

Router(config-dhcpv6-if)# profile downstream
Router(config-dhcpv6-if)# commit
```

IANA アドレス割り当てのための BVI を介した DHCPv6 リレー

DHCPv6 リレーエージェントは、DHCPv6 クライアントから送信されるすべてのパケットをアクセスインターフェイス経由で外部 DHCPv6 サーバ向けにリレーし、DHCPv6 クライアントの IANA 割り当てを介して IP アドレス (::/128) を要求します。また、DHCPv6 リレーエージェントは DHCPv6 サーバからの応答パケットを受信し、BVI インターフェイスを介して DHCPv6 クライアントにパケットを転送します。DHCPv6 リレーエージェントは、DHCPv6 バインディングと、割り当てられた IP アドレスの各ルートエントリを維持しません。そのため、デフォルトでは DHCPv6 クライアントに対してステートレスとして機能します。DHCPv6 サーバによって割り当てられた特定の IPv6 アドレスを、インターネット割り当て番号局 (IANA) のアドレス割り当てを介して、ブリッジ仮想インターフェイス (BVI) 経由で DHCPv6 クライアントに取得させることができます。したがって、DHCPv6 リレーエージェントはステートフルリ

レー エージェントとして機能し、DHCPv6 バインディングと、割り当てられた IPv6 アドレスのそれぞれのルートエントリを維持します。

制約事項

- DHCP リレー用に BVI インターフェイス経由で最大 500 のクライアントセッションを設定できます。
- それぞれの DHCPv6 リレープロファイルは、最大 8 つの DHCPv6 サーバアドレスを使用して設定できます。

設定例

IANA アドレス割り当て用に BVI 経由で DHCPv6 リレーを設定するには、次の手順を実行します。

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、BVI インターフェイスを設定します。
2. BVI インターフェイスに IPv6 アドレスを割り当てます。
3. リレーエージェントの L3 BVI インターフェイスに L2 アクセスインターフェイスをルーティングします。
4. DHCP IPv6 コンフィギュレーション モードを開始し、DHCP IPv6 ステートフル リレー プロファイルを作成します。
5. サーバアドレスにリレープロファイルを接続します。
6. IANA 経由のルート割り当てをイネーブルにして、ステートフルリレーエージェントを設定します。
7. DHCPv6 リレープロファイルに BVI インターフェイスを接続します。

設定

```
/* Enter the interface configuration mode and configure a BVI interface. */
Router# configure
Router(config)# interface BVI1

Assign an IPv6 address to the BVI interface.
Router(config-if)# ipv6 address 2001:db8::2/64
Router(config-if)# commit
Router(config-if)# exit

/* Route the L2 access interface to the L3 BVI interface of the relay agent. */
Router(config)# l2vpn bridge group 1
Router(config-l2vpn-bg)# bridge-domain 1
Router(config-l2vpn-bg-bd)# interface hundredGigE 0/0/0/1.100
Router(config-l2vpn-bg-bd-ac)# commit
Router(config-l2vpn-bg-bd-ac)# exit
Router(config-l2vpn-bg-bd)# routed interface BVI1
Router(config-l2vpn-bg-bd)# exit
Router(config-l2vpn-bg)# exit
Router(config-l2vpn-bg)# exit
```

```

Router(config-l2vpn)# exit
Router(config)#

/* Enter the DHCP IPv6 configuration mode and then create a DHCP IPv6 Stateful relay
profile. */
Router(config)# dhcp ipv6
Router(config-dhcpv6)# dhcp ipv6
Router(config-dhcpv6)# profile RELAY1 relay

/* Attach the relay profile to a server address. */
Router(config-dhcpv6-relay-profile)# helper-address vrf default 2001:DB8::1

/* Configure a stateful relay agent by enabling route allocation through IANA. */
Router(config-dhcpv6-relay-profile)# iana-route-add

/* Attach the BVI Interface to the DHCPv6 relay profile. */
Router(config-dhcpv6-relay-profile)# interface BVI1 relay profile RELAY1
Router(config-dhcpv6-relay-profile)# commit

```

実行コンフィギュレーション

```

Router# show running configuration
interface BVI1
  ipv6 address 2001:db8::2/64
!
l2vpn
  bridge group 1
    bridge-domain 1
      interface HundredGigE0/0/0/1.100
      !
      routed interface BVI1
      !
    !
  !
!
dhcp ipv6
  profile RELAY1 relay
    helper-address vrf default 2001:db8::1
    iana-route-add
    !
  interface BVI1 relay profile RELAY1
!

```

確認

次のコマンドを使用して、1つ以上のDHCPクライアントがBVI経由でブリッジされていることを確認します。

```

Router# show dhcp ipv6 relay binding
Thu Nov 21 05:48:38.463 UTC

Summary:
Total number of clients: 500

IPv6 Address: 2000::418f/128 (BVI31)
Client DUID: 000100015dcf28de001094003295
MAC Address: 0010.9400.3295

```

```

IAID: 0x0
VRF: default
Lifetime: 600 secs (00:10:00)
Expiration: 533 secs (00:08:53)
L2Intf AC: Bundle-Ether3.1
SERG State: NONE
SERG Intf State: SERG-NONE
IPv6 Address: 2000::4190/128 (BVI31)
Client DUID: 000100015dcf28de001094003296
MAC Address: 0010.9400.3296
IAID: 0x0
VRF: default
Lifetime: 600 secs (00:10:00)
Expiration: 531 secs (00:08:51)
L2Intf AC: Bundle-Ether3.1
SERG State: NONE
SERG Intf State: SERG-NONE
IPv6 Address: 2000::4191/128 (BVI31)
Client DUID: 000100015dcf28de001094003297
MAC Address: 0010.9400.3297
IAID: 0x0
VRF: default
Lifetime: 600 secs (00:10:00)
Expiration: 448 secs (00:07:28)
L2Intf AC: Bundle-Ether3.1
SERG State: NONE
SERG Intf State: SERG-NONE
IPv6 Address: 2000::4192/128 (BVI31)
Client DUID: 000100015dcf28de001094003298
MAC Address: 0010.9400.3298
IAID: 0x0
VRF: default
Lifetime: 600 secs (00:10:00)
Expiration: 439 secs (00:07:19)
L2Intf AC: Bundle-Ether3.1
SERG State: NONE
SERG Intf State: SERG-NONE

```

次のコマンドを使用して、IANA の割り当てにより、一意の IPv6 アドレスがクライアントに割り当てられていることを確認します。

```

Router# show route ipv6
Mon Oct 21 06:16:43.617 UTC

Codes: C - connected, S - static, R - RIP, B - BGP, (>) - Diversion path
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - ISIS, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, su - IS-IS summary null, * - candidate default
U - per-user static route, o - ODR, L - local, G - DAGR, l - LISP
A - access/subscriber, a - Application route
M - mobile route, r - RPL, t - Traffic Engineering, (!) - FRR Backup path

Gateway of last resort is not set

A    2000::/64
    [1/0] via fe80::1, 00:00:37, BVI700
A    2000::1/128
    [1/0] via fe80::210:94ff:fe00:8, 00:00:12, BVI700
C    2007:3019::/64 is directly connected,
    00:00:37, Loopback1
L    2007:3019::1/128 is directly connected,
    00:00:37, Loopback1

```

```

C    7001:6018::/64 is directly connected,
    00:00:37, BVI700
L    7001:6018::1/128 is directly connected,
    00:00:37, BVI700
C    7001:6019::/64 is directly connected,
    00:00:37, TenGigE0/0/0/2.2
L    7001:6019::1/128 is directly connected,
    00:00:37, TenGigE0/0/0/2.2

```

DHCP リレー プロファイル : 例

次に、DHCP リレー プロファイルを設定する例を示します。

```

dhcp ipv4
  profile client relay
  helper-address vrf foo 10.10.1.1
!
! ...

```

インターフェイス上の DHCP リレー : 例

次に、インターフェイスで DHCP リレー エージェントをイネーブルにする例を示します。

```

dhcp ipv4
  interface GigabitEthernet 0/1/1/0 relay profile client
!

```

VRF 上の DHCP リレー : 例

次に、VRF で DHCP リレー エージェントをイネーブルにする例を示します。

```

dhcp ipv4
  vrf default relay profile client
!

```

リレー エージェント情報オプションのサポート : 例

次に、リレー エージェントと、DHCP リレー 情報オプションの挿入および削除をイネーブルにする例を示します。

```

dhcp ipv4
  profile client relay
  relay information option
!
!

```


リレー エージェント **giaddr** ポリシー : 例

次に、リレー エージェント **giaddr** ポリシーを設定する例を示します。

```
dhcp ipv4
  profile client relay
    giaddr policy drop
  !
!
```

DHCP プロキシ プロファイルの設定

DHC プロキシはすべてのリレー機能を実行し、さらにいくつかの追加機能も提供します。DHCP プロキシは、DHCP クライアントから DHCP サーバの詳細を見えないようにします。DHCP プロキシは、クライアントがプロキシをサーバと見なすように DHCP 応答を変更します。この状態では、クライアントは DHCP サーバに対するようにプロキシと相互作用します。

設定例

1. DHCP IPv4 または DHCP IPv6 プロファイル プロキシ サブモードを開始します。
2. DHCP などの UDP ブロードキャストを転送します。



- (注)
- **address** 引数の値には、特定の DHCP サーバ アドレスまたはネットワーク アドレス（宛先ネットワーク セグメントに他にも DHCP サーバがある場合）を指定できます。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。
 - サーバが複数ある場合は、各サーバにヘルパー アドレスを 1 つ設定してください。

設定

```
/* Enter the DHCP IPv4 profile proxy submode. */
Router(config)# dhcp ipv4
Router(config-dhcpv4)# profile client proxy

/* Forward UDP broadcasts, including DHCP */
Router(config-dhcpv4-proxy-profile)# helper-address vrf vrf1 foo 10.10.1.1
Router(config-dhcpv4-proxy-profile)# commit
```

DHCP サーバ

DHCP サーバはアドレス割り当て要求と更新を受け取り、分散アドレスプール（DAP）内にある定義済みアドレス グループから IP アドレスを割り当てます。サブネット マスク、ドメイン

名、DNS サーバの IP アドレス、デフォルト ルータ、その他の設定パラメータなどの詳細情報を要求元クライアントに提供するように DHCP サーバを設定することもできます。DHCP サーバは、ローカル接続されている LAN セグメントからのブロードキャストや、ネットワークにある他の DHCP リレー エージェントから転送された DHCP 要求のブロードキャストを受け入れることができます。

DHC プロキシはすべてのリレー機能を実行し、さらにいくつかの追加機能も提供します。DHCP プロキシは、DHCP クライアントから DHCP サーバの詳細を見えないようにします。DHCP プロキシは、クライアントがプロキシをサーバと見なすように DHCP 応答を変更します。この状態では、クライアントは DHCP サーバに対するようにプロキシと相互作用します。

DHCP サービスベース モードの選択

DHCP サービスベース モードの選択機能の一部として、DHCP ベースという新しいモードが導入されました。DHCP ベース モードでインターフェイスが設定されている場合、DHCP はクライアント要求のオプション 60 (class-identifier) 値を DHCP ベース プロファイルで設定された値と照合することによって、DHCP プロキシまたは DHCP サーバ モードのいずれかを選択してクライアント要求を処理します。

プールは、サーバプロファイル モードおよびサーバプロファイルクラス サブモードで設定されます。クラスベースのプールの選択は、常にプロファイル プールの選択よりも優先されます。

DHCPv6 サーバプロファイルクラス サブモードは、一部 (0、12、50、52、53、54、58、59、61、82、および 255) を除く DHCP オプションの設定をサポートします。

```
dhcp ipv6
profile DHCP_BASE base
    match option 60 41424344 profile DHCPv6_PROXY proxy
    match option 60 41424355 profile DHCPv6_SERVER server
    default profile DEFAULT_PROFILE server
    relay information authenticate inserted
    !
profile DHCPv6_PROXY proxy
    helper-address vrf default 10.10.10.1 giaddr 0.0.0.0
    !
profile DHCPv6_SERVER server
    lease 1 0 0
    pool IP_POOL
    !
profile DEFAULT_PROFILE server
    lease 1 0 0
    pool IP_POOL
    !
    !
interface TenGigE 0/11/0/0 base profile DHCP_BASE
```

DHCP サーバ プロファイルの設定

ルータは、DHCPv4 または DHCPv6 サーバ プロファイルを使用して設定できます。

DHCPv6 サーバ プロファイルを設定するには、次のタスクを実行します。

```
Router# configure
Router(config)# dhcp ipv6
```

```

Router(config-dhcpv6)# profile profile-name server
Router(config-dhcpv6-server-profile)# bootfile boot-file-name
Router(config-dhcpv6-server-profile)# broadcast-flag policy unicast-always
Router(config-dhcpv6-server-profile)# class class-name
Router(config-dhcpv6-server-profile-class)# exit
Router(config-dhcpv6-server-profile)# default-router address1 address2 ... address8
Router(config-dhcpv6-server-profile)# lease {infinite | days minutes seconds }
Router(config-dhcpv6-server-profile)# limit lease {per-circuit-id | per-interface | per-remote-id} value
Router(config-dhcpv6-server-profile)# netbios-name server address1 address2 ... address8

Router(config-dhcpv6-server-profile)# netbios-node-type {number | b-node | h-node | m-node | p-node}
Router(config-dhcpv6-server-profile)# option option-code {ascii string | hex string | ip address}
Router(config-dhcpv6-server-profile)# pool pool-name
Router(config-dhcpv6-server-profile)# requested-ip-address-check disable
Router(config-dhcpv6-server-profile)# commit

```

プールを使用した複数のクラスの設定

複数のクラスにプールを設定するには、次のタスクを実行します。

```

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# dhcp ipv6
RP/0/RP0/CPU0:router(config-dhcpv6)# profile profile-name server
RP/0/RP0/CPU0:router(config-dhcpv6-server-profile)# pool pool-name
RP/0/RP0/CPU0:router(config-dhcpv6-server-profile)# class class-name
RP/0/RP0/CPU0:router(config-dhcpv6-server-class)# pool pool-name
RP/0/RP0/CPU0:router(config-dhcpv6-server-class)# match option option [ sub-option
sub-option] [ ascii asciiString | hex hexString ]
RP/0/RP0/CPU0:router(config-dhcpv6-server-class)# exit
RP/0/RP0/CPU0:router(config-dhcpv6-server-profile)# class class-name
RP/0/RP0/CPU0:router(config-dhcpv6-server-class)# pool pool-name
RP/0/RP0/CPU0:router(config-dhcpv6-server-class)# match vrf vrf-name
RP/0/RP0/CPU0:router(config-dhcpv6-server-class)# commit

```

クラス一致オプションを使用したサーバ プロファイル DAP の設定

ここでは、クラス一致オプションを使用したサーバ プロファイル DAP の設定について説明します。

設定例

```

router#configure

router(config)#dhcp ipv4
/* The 'dhcp ipv6' command configures DHCP for IPv6 and enters the DHCPv6 configuration
submode. */

router(config-dhcpv4)#profile ISP1 server
/* Enters the server profile configuration mode. */

router(config-dhcpv4-server-profile)#pool ISP1_POOL
/* Configures the DAPS pool name. */

router(config-dhcpv4-server-profile)#class ISP1_CLASS
/* Creates and enters server profile class configuration submode. */

```

```

router(config-dhcpv4-server-profile-class)#pool ISP1_CLASS_POOL
/* Configures the pool name. */

router(config-dhcpv4-server-profile-class)#match option 60 hex PXEClient_1
/* DHCP server selects a pool from a class by matching options in the received DISCOVER
packet with the match option. */

router(config-dhcpv4-server-profile-class)#exit

router(config-dhcpv4-server-profile)#exit

router(config-dhcpv4)#profile ISP2 server
/* Enters the server profile configuration mode. */

router(config-dhcpv4-server-profile)#dns-server 10.20.3.4
/* Configures the name of the DNS server or the IP address. */

router(config-dhcpv4-server-profile)#pool ISP2_POOL
/* Configures the pool name. */

router(config-dhcpv4-server-profile)#class ISP2_CLASS
/* Creates and enters the server profile class. */

router(config-dhcpv4-server-profile-class)#pool ISP2_CLASS_POOL
/* Configures the pool name. */

router(config-dhcpv4-server-profile-class)#match option 60 hex PXEClient_2
/* DHCP server selects a pool from a class by matching options in the received DISCOVER
packet with the match option. */

router(config-dhcpv4-server-profile-class)#exit

router(config-dhcpv4-server-profile)#exit

router(config-dhcpv4)#commit

```

実行コンフィギュレーション

```

Router#show running-config dhcp ipv4
dhcp ipv4
profile ISP1 server
pool ISP1_POOL
class ISP1_CLASS
pool ISP1_CLASS_POOL
match option 60 hex PXEClient_1
exit
exit
profile ISP2 server
dns-server 10.20.3.4
pool ISP2_POOL
class ISP2_CLASS
pool ISP2_CLASS_POOL
match option 60 hex PXEClient_2
exit
exit
!

```

DAP プール一致オプションを使用しないサーバ プロファイルの設定

ここでは、DAP プール一致オプションを使用しないサーバ プロファイルの設定について説明します。

設定例

```
router#configure

router(config)#dhcp ipv4
/* The 'dhcp ipv6' command configures DHCP for IPv6 and enters the DHCPv6 configuration
submode. */

router(config-dhcpv4)#profile ISP1 server
/* Enters the server profile configuration mode. */

router(config-dhcpv4-server-profile)#dns-server ISP1.com
/* Configures the name of the DNS server or IP address. */

router(config-dhcpv4-server-profile)#exit

router(config-dhcpv4)#profile ISP2 server
/* Enters the server profile configuration mode. */

router(config-dhcpv4-server-profile)#dns-server ISP2.com
/* Configures the name of the DNS server or IP address. */

router(config-dhcpv4-server-profile)#exit

router(config-dhcpv4)#commit
```

実行コンフィギュレーション

```
Router#show running-config dhcp ipv4
dhcp ipv4
  profile ISP1 server
    dns-server ISP1.com
  exit
  profile ISP2 server
    dns-server ISP2.com
  exit
!
```

DAP での ISP ごとのアドレス プール設定

ここでは、DAP で ISP ごとにアドレス プールを設定する方法について説明します。

設定例

```
router#configure

router(config)#pool vrf ISP_1 ipv4 ISP1_POOL
/* Configures an IPv4 pool for the specified VRF or all VRFs. Use the 'ipv6' keyword for
IPv6 pool. */

router(config-pool-ipv4)#network 10.10.10.0
```

```

/* Specifies network for allocation. */

router(config-pool-ipv4)#exit

router(config)#pool vrf ISP_2 ipv4 ISP2_POOL
/* Configures an IPv4 pool for the specifed VRF or all VRFs. */

router(config-pool-ipv4)#network 10.20.20.0
/* Specifies network for allocation. */

router(config-pool-ipv4)#exit

router(config-dhcpv4)#commit

```

実行コンフィギュレーション

```

Router#show running-config pool
pool vrf ISP_1 ipv4 ISP1_POOL
  network 10.10.10.0
  exit
pool vrf ISP_2 ipv4 ISP2_POOL
  network 10.20.20.0
!

```

DHCP クライアント

Dynamic Host Configuration Protocol (DHCP) クライアント機能を使用すると、ルータインターフェイスが IPv4、DHCPv4、DHCPv6 サーバのいずれかを動的に取得し、該当するレイヤ 2 アドレスに応答を転送します。これにより、該当するデバイスが適切な設定情報を取得できるようになります。

DHCP は、リース期間と呼ばれる設定可能な期間にのみ IP アドレスを割り当てることができます。クライアントがこの IP アドレスをリース期間を超えて保持する必要がある場合は、IP アドレスが期限切れになる前にリース期間を更新する必要があります。クライアントは、サーバから送信された設定に基づいてリースを更新します。クライアントは、サーバの IP アドレスを使用して REQUEST メッセージをユニキャストします。サーバは REQUEST メッセージを受信すると、ACK メッセージで応答します。クライアントのリース期間が、ACK メッセージに設定されたリース時間で延長されます。

制約事項と制限

- DHCPv4 または DHCPv6 クライアントは、管理インターフェイスでのみイネーブルにできます。
- インターフェイスで設定できるのは、DHCPv4、DHCPv6、スタティック IPv4、スタティック IPv6 のいずれかです。

インターフェイスでの DHCP クライアントのイネーブル化

DHCPv4 または DHCPv6 クライアントは、インターフェイス レベルでイネーブルにできます。インターフェイスで DHCPv4 または DHCPv6 がイネーブル化またはディセーブル化されると、DHCP コンポーネントが通知を受信します。

```
Router# configure
Router(config)# interface MgmtEth rack/slot/CPU0/port
Router(config)# interface interface_name ipv6 address dhcp
```

DHCPv6 プロキシ バインディング テーブルのリロード永続性

Cisco IOS XR Dynamic Host Configuration Protocol (DHCP) アプリケーションは、DHCP アプリケーションによってクライアントに割り当てられた DHCP リースの DHCP バインディング状態を維持する役割を担います。これらのバインディング状態は、DHCP アプリケーション（プロキシ/リレー/スヌーピング）によって学習されます。DHCP クライアントは、DHCP アプリケーションで発生するイベントに関係なく、DHCP リースを維持することを想定しています。



(注) リリース 6.2.2 以降では、DHCPv4 または DHCPv6 を稼動しているプロキシまたはサーバで 200K セッションがサポートされます。

この機能により、DHCP アプリケーションは上記のイベントを介してバインド状態を維持できます。

- プロセスの再起動：ローカル チェックポイント
- RP フェールオーバー：チェックポイントを使用したホットスタンバイ RP
- LC IMDR：ローカル チェックポイント
- LC OIR：RP 上のシャドー テーブル
- システムの再起動：ローカル ディスクに保存されたバインディング

システム永続メモリへの DHCP リレー バインディング データベースの書き込みの設定

システム永続メモリへの DHCP リレー バインディング データベースの書き込みを設定するには、次のタスクを実行します。これは、システムのリロード後に DHCP リレー バインディング テーブルを回復するのに役立ちます。完全な永続ファイルの書き込みに使用されるファイル名は、dhcpv4_srp_{nodeid}_odd or dhcpv6_srp_{nodeid}_odd および dhcpv4_srp_{nodeid}_even or dhcpv6_srp_{nodeid}_even です。nodeid は、ファイルが書き込まれるノードの実際のノード ID です。増分ファイルは完全なファイルと同じ方法で命名され、_inc が付加されます。

```
Router# configure
Router(config)# dhcp ipv6
Router(config-dhcpv6)# database [relay] [full-write-interval full-write-interval]
[incremental-write-interval incremental-write-interval]
Router(config-dhcpv6)# commit
```




第 6 章

DHCP リレーの概要

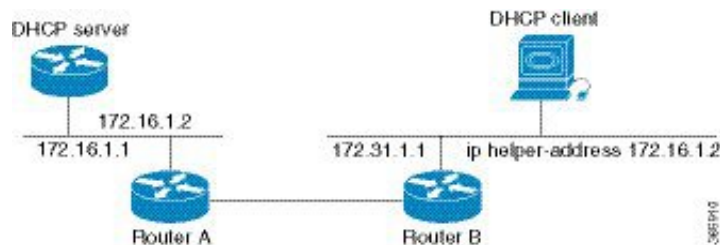
DHCP リレー エージェントは、共有の物理サブネットに存在しないクライアントとサーバとの間で DHCP パケットを転送するホストです。リレー エージェント転送は、IP ルータの通常の転送とは異なります。通常の転送では、IP データグラムがネットワーク間で透過的にスイッチングされます。

DHCP クライアントは、自身の所属先のネットワークに関する情報を保持していないときには、ユーザデータグラムプロトコル (UDP) ブロードキャストを使用して、DHCPDISCOVER メッセージを送信します。

サーバが含まれていないネットワークセグメント上にクライアントがある場合、DHCP パケットが別のネットワークセグメント上のサーバに届くようにするには、そのネットワークセグメントにリレー エージェントが必要です。ほとんどのルータはブロードキャストトラフィックを転送するように設定されていないため、UDP ブロードキャストパケットは転送されません。DHCP リレー プロファイルを設定することにより DHCP パケットをリモートサーバに転送するように DHCP リレー エージェントを設定し、そこに 1 つ以上のヘルパー アドレスを設定できます。プロファイルをインターフェイスまたは VRF に割り当てることができます。

次の図に、このプロセスを示します。DHCP クライアントが、IP アドレスの要求と追加設定パラメータをローカル LAN 上でブロードキャストしています。DHCP リレー エージェントとして機能するルータ B は、ブロードキャストを取得し、宛先アドレスを DHCP サーバのアドレスに変更し、別のインターフェイスにメッセージを送信します。リレー エージェントは、DHCP クライアントのパケットを受け取ったインターフェイスの IP アドレスを DHCP パケットのゲートウェイ アドレス (giaddr) フィールドに挿入します。これにより、DHCP サーバは、どのサブネットがオファーを受信するかを判断し、適切な IP アドレス範囲を特定できます。リレー エージェントは、メッセージを (リレー プロファイルのヘルパー アドレスによって指定される) サーバアドレス、この場合は 172.16.1.2 にユニキャストします。

図 11: ヘルパー アドレスを使用した UDP ブロードキャストの DHCP サーバへの転送



- 回線 ID およびリモート ID を持つ DHCP Option-82 (88 ページ)
- DHCP リレー エージェントの設定の前提条件 (89 ページ)
- DHCP リレー機能の制限事項 (89 ページ)
- DHCP リレー エージェントを設定およびイネーブルにする方法 (90 ページ)
- DHCP プロキシ プロファイルの設定 (100 ページ)
- DHCP サーバ (100 ページ)
- DHCP クライアント (105 ページ)
- DHCPv6 プロキシ バインディング テーブルのリロード永続性 (106 ページ)

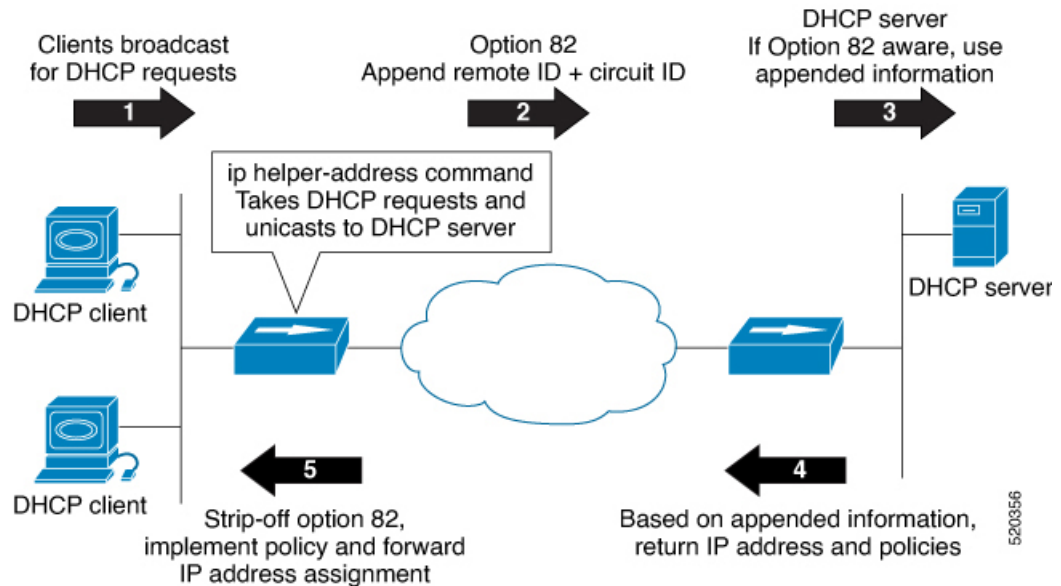
回線 ID およびリモート ID を持つ DHCP Option-82

DHCP リレーエージェント情報オプション (Option-82) では、Dynamic Host Configuration Protocol (DHCP) リレーエージェントがクライアントから発信された DHCP パケットを DHCP サーバに転送する際に、エージェント自体の情報をパケットに含めることができます。DHCP サーバでは、この情報を使用して、IP アドレスまたはその他のパラメータ割り当てポリシーを実装します。

この機能は、エージェントリモート ID と呼ばれる DHCP リレーエージェント情報オプションのサブオプションを使用して、DHCP サーバに情報を伝えます。エージェントリモート ID に組み込まれて送信される情報には、リレーエージェントを識別する IP アドレス 1 つと、着信する DHCP 要求が経由する ATM インターフェイスおよび PVC に関する情報が含まれます。DHCP サーバはこの情報を使用して、IP アドレスの割り当てとセキュリティポリシーの決定を行うことができます。

図では、DHCP クライアントが DHCP 要求を生成し、ネットワーク上でブロードキャストする時点を示しています。DHCP リレーエージェントはブロードキャスト DHCP 要求パケットを代行受信し、パケット内にリレーエージェント情報オプション (option-82) を挿入します。リレーエージェント情報オプションには、関連するサブオプションが含まれています。DHCP リレー エージェントは DHCP パケットを DHCP サーバにユニキャストします。DHCP サーバはパケットを受信し、サブオプションを使用して IP アドレスや他の設定パラメータを割り当て、クライアントに転送します。サブオプションフィールドは、クライアントへの転送の際にリレーエージェントによってパケットから取り除かれます。

図 12: DHCP リレー option-82 を使用したパケットの転送



Cisco IOS XR リリース 7.1.1 より、DHCP IPv4 リレーエージェントには、DHCP IPv4 リレーパケットのリモート ID と回線 ID 情報が含まれています。

BVI インターフェイスを介してリレーされる DHCP IPv4 パケットは、リレーエージェントのリレー情報オプションポリシーを表示します。DHCP IPv4 アプリケーションには、option-82 のリモート ID と回線 ID が含まれており、それらの ID はサーバに転送されます。

DHCP リレー エージェントの設定の前提条件

DHCP リレー エージェントを設定するための前提条件は、次のとおりです。

- 適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。このコマンド リファレンスには、各コマンドに必要なタスク ID が含まれます。ユーザ グループの割り当てが原因でコマンドを使用できないと考えられる場合、AAA 管理者に連絡してください。
- 設定済みで動作している DHCP クライアントおよび DHCP サーバ。
- リレー エージェントと DHCP サーバ間の接続

DHCP リレー機能の制限事項

DHCP リレー機能の実装に関する制限事項は次のとおりです。

- マルチキャストアドレスはサポートされていません。DHCP リレー プロファイル サブモードの **helper-address** コマンドは、ヘルパー アドレスとしてグローバルユニキャスト IP アドレスのみをサポートします。
- パケットを DHCP サーバに転送するときにリレーエージェントによって追加される DHCP オプション コードは、**interface-id** と **remote-id** のみです。



(注) DHCP リレー プロファイル サブモードでは、DHCP オプション コードの設定はサポートされていません。

DHCP リレー エージェントを設定およびイネーブルにする方法

ここでは、次のタスクについて説明します。

DHCP リレー エージェントの設定およびイネーブル化

設定例

```
Router# configure
/* Enters the global configuration mode */

Router(config)# dhcp ipv4
/* Configures DHCP for IPv4 and enters the DHCPv4 configuration submode. */

Router(config-dhcpv4)# profile r1 relay
/* Enables DHCP relay profile */

Router(config-dhcpv4-relay-profile)# helper-address vrf A 10.10.10.1 giaddr 40.1.1.2
Router(config-dhcpv4-relay-profile)# broadcast-flag policy check
/* Configures VRF addresses for forwarding UDP broadcasts, including DHCP. */

Router(config-dhcpv4-relay-profile)# relay information option vpn
Router(config-dhcpv4-relay-profile)# relay information option vpn-mode rfc
/* Inserts the DHCP relay agent information option (option-82 field) in forwarded
BOOTREQUEST messages to a DHCP server. */

Router(config-dhcpv4-relay-profile)# relay information option allow-untrusted
/* (Optional) Configures the DHCP IPv4 Relay not to discard BOOTREQUEST packets
that have an existing relay information option and the giaddr set to zero. */

Router(config-dhcpv4-relay-profile)# exit
Router(config-dhcpv4)# interface BVI 1 relay profile r1
Router(config-dhcpv4)# commit
/* Configures DHCP relay on a BVI interface and commits the configuration */
```

実行コンフィギュレーション

```
Router#show running-config
Tue May 23 10:56:14.463 IST
Building configuration...
!! IOS XR Configuration 0.0.0
!! Last configuration change at Tue May 23 10:56:08 2017 by annseque
!
dhcp ipv4
  vrf vrf1 relay profile client
  profile r1 relay
    helper-address vrf A 10.10.10.1 giaddr 40.1.1.2
    broadcast-flag policy check
    relay information option vpn
    relay information option vpn-mode rfc
    relay information option allow-untrusted
  !
```

DHCP リレー Option-82 の設定およびイネーブル化

設定例

リモート ID と回線 ID 情報を使用した DHCP IPv4 リレーエージェント設定の例を次に示します。BVI インターフェイスに関連付けられている DHCP IPv4 リレープロファイル設定内のリモート ID 設定を設定します。また、レイヤ 2 トランスポート AC の DHCP IPv4 パケット設定に回線 ID 情報を設定します。

```
Router# configure
/* Enters the global configuration mode */

Router(config)# dhcp ipv4
/* Configures DHCP for IPv4 and enters the DHCPv4 configuration submode. */

Router(config-dhcpv4)# profile test relay
/* Enables DHCP relay profile */

Router(config-dhcpv4-relay-profile)# helper-address vrf1 10.20.0.4 giaddr 10.20.0.1
Router(config-dhcpv4-relay-profile)# broadcast-flag policy check
/* Configures VRF addresses for forwarding UDP broadcasts, including DHCP. */

Router(config-dhcpv4-relay-profile)# relay information option vpn
Router(config-dhcpv4-relay-profile)# relay information check
Router(config-dhcpv4-relay-profile)# relay information option
Router(config-dhcpv4-relay-profile)# relay information policy drop
Router(config-dhcpv4-relay-profile)# relay information option vpn-mode rfc
Router(config-dhcpv4-relay-profile)# relay information option remote-id format-type hex
12
/*Configures the remote ID on DHCP relay */
/* Inserts the DHCP relay agent information option (option-82 field) in forwarded
BOOTREQUEST messages to a DHCP server. */

Router(config-dhcpv4-relay-profile)# relay information option allow-untrusted
/* (Optional) Configures the DHCP IPv4 Relay not to discard BOOTREQUEST packets
that have an existing relay information option and the giaddr set to zero. */

Router(config-dhcpv4-relay-profile)# exit
Router(config-dhcpv4)# interface BVI 1 relay profile test1
Router(config-dhcpv4)# interface Bundle-Ether1.29 relay information option circuit-id
format-type ascii 120
```

```
/*Configures the circuit ID on the DHCP relay */
Router(config-dhcpv4)# commit
/* Configures DHCP relay on a BVI interface and commits the configuration */
```

実行コンフィギュレーション

```
Router#show running-config
dhcp ipv4

!
profile test1 relay
  helper-address vrf vrf1 10.20.0.4 giaddr 10.20.0.1
  relay information option vpn
  relay information check
  relay information option
  relay information policy drop
  relay information option vpn-mode rfc
  relay information option remote-id format-type hex 12
  relay information option allow-untrusted

interface BVI2 relay profile test1
interface Bundle-Ether1.29 relay information option circuit-id format-type ascii 120

interface Bundle-Ether1.29 l2transport
  encapsulation dot1q 29
  rewrite ingress tag pop 1 symmetric
!

l2vpn
bridge group IRB
bridge-domain DHCP1
  interface Bundle-Ether1.29
    split-horizon group
  !
```

インターフェイスでの DHCPv6 リレー エージェントのイネーブル化

このタスクでは、インターフェイスで Cisco IOS XR DHCPv6 リレー エージェントをイネーブルにする方法について説明します。



- (注) Cisco IOS XR ソフトウェアでは、DHCPv6 リレー エージェントがデフォルトでディセーブルになっています。

```
RP/0/RP0/CPU0:router# configure terminal
RP/0/RP0/CPU0:router(config)# dhcp ipv6
RP/0/RP0/CPU0:router(config-dhcpv6)# interface type interface-instance relay profile
profile-name
RP/0/RP0/CPU0:router(config-dhcpv6-if)# commit
```

インターフェイスでの DHCP リレーのディセーブル化

このタスクでは、インターフェイスにプロファイルを割り当てないことにより、インターフェイスで DHCP リレーをディセーブルにする方法について説明します。

```
Router# configure terminal
Router(config)# dhcp ipv6
Router(config-dhcpv6)# interface type name none
Router(config-dhcpv6-if)# commit
```

VRF での DHCP リレーのイネーブル化

このタスクでは、VRF で DHCP リレーをイネーブルにする方法について説明します。

```
/CPU0:router# configure terminal
Router(config)# dhcp ipv6
Router(config-dhcpv6)# vrf vrf-name relay profile profile-name
Router(config-dhcpv6-if)# commit
```

複数のヘルパーアドレスを使用した DHCP リレー プロファイルの設定

DHCPv4 または DHCPv6 リレー プロファイルには、最大 16 のヘルパー IPv4 および IPv6 アドレスを設定できます。

1. DHCPv4 または DHCPv6 コンフィギュレーション モードを開始します。

```
Router(config)# dhcp ipv6
```

2. DHCPv4 または DHCPv6 リレー プロファイルを設定します。

```
Router(config-dhcpv6)# profile helper relay
```

3. ヘルパー アドレスを設定します。



(注) 最大 16 の IPv4 および IPv6 アドレスを設定できます。

```
Router(config-dhcpv6-relay-profile)# helper-address vrf default 2001:1:1::2
```

4. 設定を確認します。

```
Router(config-dhcpv6-relay-profile)# show configuration
```

```
!! IOS XR Configuration 0.0.0
dhcp ipv6
  profile helper relay
    helper-address vrf default 2001:1:1::2
  !
!
end
```

5. 設定をコミットします。

```
Router(config-dhcpv6-relay-profile)# commit
```

6. コンフィギュレーション モードを終了し、設定されているヘルパー アドレスを確認します。

```
Router# show dhcp ipv6 relay profile name helper
...
Profile: helper
Helper Addresses:
    2001:1:1::2, vrf default
Information Option: Disabled
Information Option Allow Untrusted: Disabled
Information Option VPN: Disabled
Information Option VPN Mode: RFC
Information Option Policy: Replace
Information Option Check: Disabled
GIADDR Policy: Keep
Broadcast-flag Policy: Ignore
VRF References:
Interface References:
```

DHCPv6 リレー ヘルパー アドレスが正常に設定されています。

プレフィックス委任の DHCP リレー エージェント通知

プレフィックス委任の DHCP リレーエージェント通知を使用すると、DHCPv6 リレーエージェントとして動作するルータは、リレー エージェントからクライアントに中継される DHCP RELAY-REPLY パケットの内容を確認することによって、プレフィックス委任オプションを見つけることができます。リレー エージェントは、プレフィックス委任オプションを検出すると、委任されるプレフィックスに関する情報を抽出し、プレフィックス委任情報と一致する IPv4 または IPv6 加入者ルートをリレー エージェントに挿入します。その後リレー経由でそのプレフィックスに宛てられたパケットは、プレフィックス委任に含まれる情報に基づいて転送されます。IPv4 または IPv6 加入者ルートは、プレフィックス委任のリース期間が経過するか、またはリレーエージェントがプレフィックス委任を解放するクライアントから解放パケットを受信するまで、ルーティング テーブルに保持されます。

リレー エージェントは、自動的に加入者ルート管理を行います。

IPv4 または IPv6 ルートは、リレー エージェントが RELAY-REPLY パケットを中継すると追加され、プレフィックス委任のリース期間が経過するか、リレーエージェントが解放メッセージを受信すると削除されます。プレフィックス委任のリース期間を延長するときに、リレーエージェントのルーティング テーブル内の IPv4 または IPv6 加入者ルートを更新できます。

この機能により、IPv4 または IPv6 ルートはリレー エージェントのルーティング テーブルに保持されます。この登録された IPv4 または IPv6 アドレスを使用すると、ユニキャスト RPF (uRPF) の動作が可能になりますが、そのためには、リバース ルックアップを実行するルータがリレーエージェント上の IPv4 または IPv6 アドレスが正しく、スプーフィングされていないことを確認できるようにします。リレー エージェントのルーティング テーブル内の IPv6 ルートを他のルーティングプロトコルに再配布して、サブネットを他のノードにアドバタイズできます。クライアントが DHCP_DECLINE メッセージを送信すると、ルートは削除されます。

プレフィックス委任のための DHCP ステートフルリレー エージェントの設定

プレフィックス委任用にダイナミック ホスト コンフィギュレーション プロトコル DHCP リレー エージェント通知を設定するには、このタスクを実行します。

設定例

1. DHCP プロファイルの設定
2. DHCP リレー エージェントの設定
3. IPv4 または IPv6 DHCP ステートフルリレー エージェントとして機能する IPv4 または IPv6 DHCP をインターフェイスでイネーブルにします。
4. プロファイル名を設定します。

設定

```
/* Enter the global configuration mode and then enter the DHCPv6 configuration mode. */
Router# config
Router(config)# dhcp ipv6
Router(config-dhcpv6)#

/* Enter the proxy profile configuration mode and configure the DHCPv6 relay agent. */
Router(config-dhcpv6)# profile downstream proxy
Router(config-dhcpv6-profile)# helper-address 2001:db8::1 GigabitEthernet 0/1/0/1

/* Exits from the proxy profile configuration mode and enable IPv6 DHCP on an interface.
*/
Router(config-dhcpv6-profile)# exit
Router(config-dhcpv6-if)# interface GigabitEthernet 0/1/0/0 proxy

/* Configure a profile name. */

Router(config-dhcpv6-if)# profile downstream
Router(config-dhcpv6-if)# commit
```

IANA アドレス割り当てのための BVI を介した DHCPv6 リレー

DHCPv6 リレーエージェントは、DHCPv6 クライアントから送信されるすべてのパケットをアクセスインターフェイス経由で外部 DHCPv6 サーバ向けにリレーし、DHCPv6 クライアントの IANA 割り当てを介して IP アドレス (::/128) を要求します。また、DHCPv6 リレーエージェントは DHCPv6 サーバからの応答パケットを受信し、BVI インターフェイスを介して DHCPv6 クライアントにパケットを転送します。DHCPv6 リレーエージェントは、DHCPv6 バインディングと、割り当てられた IP アドレスの各ルートエントリを維持しません。そのため、デフォルトでは DHCPv6 クライアントに対してステートレスとして機能します。DHCPv6 サーバによって割り当てられた特定の IPv6 アドレスを、インターネット割り当て番号局 (IANA) のアドレス割り当てを介して、ブリッジ仮想インターフェイス (BVI) 経由で DHCPv6 クライアントに取得させることができます。したがって、DHCPv6 リレーエージェントはステートフルリ

レー エージェントとして機能し、DHCPv6 バインディングと、割り当てられた IPv6 アドレスのそれぞれのルートエントリを維持します。

制約事項

- DHCP リレー用に BVI インターフェイス経由で最大 500 のクライアントセッションを設定できます。
- それぞれの DHCPv6 リレープロファイルは、最大 8 つの DHCPv6 サーバアドレスを使用して設定できます。

設定例

IANA アドレス割り当て用に BVI 経由で DHCPv6 リレーを設定するには、次の手順を実行します。

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、BVI インターフェイスを設定します。
2. BVI インターフェイスに IPv6 アドレスを割り当てます。
3. リレーエージェントの L3 BVI インターフェイスに L2 アクセスインターフェイスをルーティングします。
4. DHCP IPv6 コンフィギュレーション モードを開始し、DHCP IPv6 ステートフル リレー プロファイルを作成します。
5. サーバアドレスにリレープロファイルを接続します。
6. IANA 経由のルート割り当てをイネーブルにして、ステートフルリレー エージェントを設定します。
7. DHCPv6 リレープロファイルに BVI インターフェイスを接続します。

設定

```
/* Enter the interface configuration mode and configure a BVI interface. */
Router# configure
Router(config)# interface BVI1

Assign an IPv6 address to the BVI interface.
Router(config-if)# ipv6 address 2001:db8::2/64
Router(config-if)# commit
Router(config-if)# exit

/* Route the L2 access interface to the L3 BVI interface of the relay agent. */
Router(config)# l2vpn bridge group 1
Router(config-l2vpn-bg)# bridge-domain 1
Router(config-l2vpn-bg-bd)# interface hundredGigE 0/0/0/1.100
Router(config-l2vpn-bg-bd-ac)# commit
Router(config-l2vpn-bg-bd-ac)# exit
Router(config-l2vpn-bg-bd)# routed interface BVI1
Router(config-l2vpn-bg-bd)# exit
Router(config-l2vpn-bg)# exit
Router(config-l2vpn-bg)# exit
```

```
Router(config-l2vpn)# exit
Router(config)#

/* Enter the DHCP IPv6 configuration mode and then create a DHCP IPv6 Stateful relay
profile. */
Router(config)# dhcp ipv6
Router(config-dhcpv6)# dhcp ipv6
Router(config-dhcpv6)# profile RELAY1 relay

/* Attach the relay profile to a server address. */
Router(config-dhcpv6-relay-profile)# helper-address vrf default 2001:DB8::1

/* Configure a stateful relay agent by enabling route allocation through IANA. */
Router(config-dhcpv6-relay-profile)# iana-route-add

/* Attach the BVI Interface to the DHCPv6 relay profile. */
Router(config-dhcpv6-relay-profile)# interface BVI1 relay profile RELAY1
Router(config-dhcpv6-relay-profile)# commit
```

実行コンフィギュレーション

```
Router# show running configuration
interface BVI1
  ipv6 address 2001:db8::2/64
!
l2vpn
  bridge group 1
    bridge-domain 1
      interface HundredGigE0/0/0/1.100
      !
      routed interface BVI1
      !
    !
  !
!
dhcp ipv6
  profile RELAY1 relay
    helper-address vrf default 2001:db8::1
    iana-route-add
    !
  interface BVI1 relay profile RELAY1
!
```

確認

次のコマンドを使用して、1つ以上の DHCP クライアントが BVI 経由でブリッジされていることを確認します。

```
Router# show dhcp ipv6 relay binding
Thu Nov 21 05:48:38.463 UTC

Summary:
Total number of clients: 500

IPv6 Address: 2000::418f/128 (BVI31)
Client DUID: 000100015dcf28de001094003295
MAC Address: 0010.9400.3295
```

```

IAID: 0x0
VRF: default
Lifetime: 600 secs (00:10:00)
Expiration: 533 secs (00:08:53)
L2Intf AC: Bundle-Ether3.1
SERG State: NONE
SERG Intf State: SERG-NONE
IPv6 Address: 2000::4190/128 (BVI31)
Client DUID: 000100015dcf28de001094003296
MAC Address: 0010.9400.3296
IAID: 0x0
VRF: default
Lifetime: 600 secs (00:10:00)
Expiration: 531 secs (00:08:51)
L2Intf AC: Bundle-Ether3.1
SERG State: NONE
SERG Intf State: SERG-NONE
IPv6 Address: 2000::4191/128 (BVI31)
Client DUID: 000100015dcf28de001094003297
MAC Address: 0010.9400.3297
IAID: 0x0
VRF: default
Lifetime: 600 secs (00:10:00)
Expiration: 448 secs (00:07:28)
L2Intf AC: Bundle-Ether3.1
SERG State: NONE
SERG Intf State: SERG-NONE
IPv6 Address: 2000::4192/128 (BVI31)
Client DUID: 000100015dcf28de001094003298
MAC Address: 0010.9400.3298
IAID: 0x0
VRF: default
Lifetime: 600 secs (00:10:00)
Expiration: 439 secs (00:07:19)
L2Intf AC: Bundle-Ether3.1
SERG State: NONE
SERG Intf State: SERG-NONE

```

次のコマンドを使用して、IANA の割り当てにより、一意の IPv6 アドレスがクライアントに割り当てられていることを確認します。

```

Router# show route ipv6
Mon Oct 21 06:16:43.617 UTC

Codes: C - connected, S - static, R - RIP, B - BGP, (>) - Diversion path
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - ISIS, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, su - IS-IS summary null, * - candidate default
        U - per-user static route, o - ODR, L - local, G - DAGR, l - LISP
        A - access/subscriber, a - Application route
        M - mobile route, r - RPL, t - Traffic Engineering, (!) - FRR Backup path

Gateway of last resort is not set

A    2000::/64
     [1/0] via fe80::1, 00:00:37, BVI700
A    2000::1/128
     [1/0] via fe80::210:94ff:fe00:8, 00:00:12, BVI700
C    2007:3019::/64 is directly connected,
     00:00:37, Loopback1
L    2007:3019::1/128 is directly connected,
     00:00:37, Loopback1

```

```
C    7001:6018::/64 is directly connected,  
    00:00:37, BVI700  
L    7001:6018::1/128 is directly connected,  
    00:00:37, BVI700  
C    7001:6019::/64 is directly connected,  
    00:00:37, TenGigE0/0/0/2.2  
L    7001:6019::1/128 is directly connected,  
    00:00:37, TenGigE0/0/0/2.2
```

DHCP リレー プロファイル：例

次に、DHCP リレー プロファイルを設定する例を示します。

```
dhcp ipv4  
  profile client relay  
  helper-address vrf foo 10.10.1.1  
!  
! ...
```

インターフェイス上の DHCP リレー：例

次に、インターフェイスで DHCP リレー エージェントをイネーブルにする例を示します。

```
dhcp ipv4  
  interface GigabitEthernet 0/1/1/0 relay profile client  
!
```

VRF 上の DHCP リレー：例

次に、VRF で DHCP リレー エージェントをイネーブルにする例を示します。

```
dhcp ipv4  
  vrf default relay profile client  
!
```

リレー エージェント情報オプションのサポート：例

次に、リレーエージェントと、DHCP リレー情報オプションの挿入および削除をイネーブルにする例を示します。

```
dhcp ipv4  
  profile client relay  
  relay information option  
  
!  
!
```

リレー エージェント **giaddr** ポリシー : 例

次に、リレー エージェント **giaddr** ポリシーを設定する例を示します。

```
dhcp ipv4
  profile client relay
  giaddr policy drop
!
```

DHCP プロキシ プロファイルの設定

DHCプロキシはすべてのリレー機能を実行し、さらにいくつかの追加機能も提供します。DHCP プロキシは、DHCP クライアントから DHCP サーバの詳細を見えないようにします。DHCP プロキシは、クライアントがプロキシをサーバと見なすように DHCP 応答を変更します。この状態では、クライアントは DHCP サーバに対するようにプロキシと相互作用します。

設定例

1. DHCP IPv4 または DHCP IPv6 プロファイル プロキシ サブモードを開始します。
2. DHCP などの UDP ブロードキャストを転送します。



- (注)
- **address** 引数の値には、特定の DHCP サーバアドレスまたはネットワーク アドレス（宛先ネットワーク セグメントに他にも DHCP サーバがある場合）を指定できます。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。
 - サーバが複数ある場合は、各サーバにヘルパー アドレスを 1 つ設定してください。

設定

```
/* Enter the DHCP IPv4 profile proxy submode. */
Router(config)# dhcp ipv4
Router(config-dhcpv4)# profile client proxy

/* Forward UDP broadcasts, including DHCP */
Router(config-dhcpv4-proxy-profile)# helper-address vrf vrf1 foo 10.10.1.1
Router(config-dhcpv4-proxy-profile)# commit
```

DHCP サーバ

DHCP サーバはアドレス割り当て要求と更新を受け取り、分散アドレスプール (DAP) 内にある定義済みアドレス グループから IP アドレスを割り当てます。サブネットマスク、ドメイン

名、DNS サーバの IP アドレス、デフォルト ルータ、その他の設定パラメータなどの詳細情報を要求元クライアントに提供するように DHCP サーバを設定することもできます。DHCP サーバは、ローカル接続されている LAN セグメントからのブロードキャストや、ネットワークにある他の DHCP リレー エージェントから転送された DHCP 要求のブロードキャストを受け入れることができます。

DHC プロキシはすべてのリレー機能を実行し、さらにいくつかの追加機能も提供します。DHCP プロキシは、DHCP クライアントから DHCP サーバの詳細を見えないようにします。DHCP プロキシは、クライアントがプロキシをサーバと見なすように DHCP 応答を変更します。この状態では、クライアントは DHCP サーバに対するようにプロキシと相互作用します。

DHCP サービスベース モードの選択

DHCP サービスベース モードの選択機能の一部として、DHCP ベースという新しいモードが導入されました。DHCP ベース モードでインターフェイスが設定されている場合、DHCP はクライアント要求のオプション 60 (class-identifier) 値を DHCP ベース プロファイルで設定された値と照合することによって、DHCP プロキシまたは DHCP サーバ モードのいずれかを選択してクライアント要求を処理します。

プールは、サーバプロファイル モードおよびサーバプロファイルクラス サブモードで設定されます。クラスベースのプールの選択は、常にプロファイル プールの選択よりも優先されます。

DHCPv6 サーバプロファイルクラス サブモードは、一部 (0、12、50、52、53、54、58、59、61、82、および 255) を除く DHCP オプションの設定をサポートします。

```
dhcp ipv6
profile DHCP_BASE base
  match option 60 41424344 profile DHCPv6_PROXY proxy
  match option 60 41424355 profile DHCPv6_SERVER server
  default profile DEFAULT_PROFILE server
  relay information authenticate inserted
!
profile DHCPv6_PROXY proxy
  helper-address vrf default 10.10.10.1 giaddr 0.0.0.0
!
profile DHCPv6_SERVER server
  lease 1 0 0
  pool IP_POOL
!
profile DEFAULT_PROFILE server
  lease 1 0 0
  pool IP_POOL
!
!
interface TenGigE 0/11/0/0 base profile DHCP_BASE
```

DHCP サーバ プロファイルの設定

ルータは、DHCPv4 または DHCPv6 サーバ プロファイルを使用して設定できます。

DHCPv6 サーバ プロファイルを設定するには、次のタスクを実行します。

```
Router# configure
Router(config)# dhcp ipv6
```

```

Router(config-dhcpv6)# profile profile-name server
Router(config-dhcpv6-server-profile)# bootfile boot-file-name
Router(config-dhcpv6-server-profile)# broadcast-flag policy unicast-always
Router(config-dhcpv6-server-profile)# class class-name
Router(config-dhcpv6-server-profile-class)# exit
Router(config-dhcpv6-server-profile)# default-router address1 address2 ... address8
Router(config-dhcpv6-server-profile)# lease {infinite | days minutes seconds }
Router(config-dhcpv6-server-profile)# limit lease {per-circuit-id | per-interface |
per-remote-id} value
Router(config-dhcpv6-server-profile)# netbios-name server address1 address2 ... address8

Router(config-dhcpv6-server-profile)# netbios-node-type {number | b-node | h-node | m-node
| p-node}
Router(config-dhcpv6-server-profile)# option option-code {ascii string | hex string | ip
address}
Router(config-dhcpv6-server-profile)# pool pool-name
Router(config-dhcpv6-server-profile)# requested-ip-address-check disable
Router(config-dhcpv6-server-profile)# commit

```

プールを使用した複数のクラスの設定

複数のクラスにプールを設定するには、次のタスクを実行します。

```

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# dhcp ipv6
RP/0/RP0/CPU0:router(config-dhcpv6)# profile profile-name server
RP/0/RP0/CPU0:router(config-dhcpv6-server-profile)# pool pool-name
RP/0/RP0/CPU0:router(config-dhcpv6-server-profile)# class class-name
RP/0/RP0/CPU0:router(config-dhcpv6-server-class)# pool pool-name
RP/0/RP0/CPU0:router(config-dhcpv6-server-class)# match option option [ sub-option
sub-option] [ ascii asciiString | hex hexString ]
RP/0/RP0/CPU0:router(config-dhcpv6-server-class)# exit
RP/0/RP0/CPU0:router(config-dhcpv6-server-profile)# class class-name
RP/0/RP0/CPU0:router(config-dhcpv6-server-class)# pool pool-name
RP/0/RP0/CPU0:router(config-dhcpv6-server-class)# match vrf vrf-name
RP/0/RP0/CPU0:router(config-dhcpv6-server-class)# commit

```

クラス一致オプションを使用したサーバ プロファイル DAP の設定

ここでは、クラス一致オプションを使用したサーバ プロファイル DAP の設定について説明します。

設定例

```

router#configure

router(config)#dhcp ipv4
/* The 'dhcp ipv6' command configures DHCP for IPv6 and enters the DHCPv6 configuration
submode. */

router(config-dhcpv4)#profile ISP1 server
/* Enters the server profile configuration mode. */

router(config-dhcpv4-server-profile)#pool ISP1_POOL
/* Configures the DAPS pool name. */

router(config-dhcpv4-server-profile)#class ISP1_CLASS
/* Creates and enters server profile class configuration submode. */

```



```
router(config-dhcpv4-server-profile-class)#pool ISP1_CLASS_POOL
/* Configures the pool name. */

router(config-dhcpv4-server-profile-class)#match option 60 hex PXEClient_1
/* DHCP server selects a pool from a class by matching options in the received DISCOVER
packet with the match option. */

router(config-dhcpv4-server-profile-class)#exit

router(config-dhcpv4-server-profile)#exit

router(config-dhcpv4)#profile ISP2 server
/* Enters the server profile configuration mode. */

router(config-dhcpv4-server-profile)#dns-server 10.20.3.4
/* Configures the name of the DNS server or the IP address. */

router(config-dhcpv4-server-profile)#pool ISP2_POOL
/* Configures the pool name. */

router(config-dhcpv4-server-profile)#class ISP2_CLASS
/* Creates and enters the server profile class. */

router(config-dhcpv4-server-profile-class)#pool ISP2_CLASS_POOL
/* Configures the pool name. */

router(config-dhcpv4-server-profile-class)#match option 60 hex PXEClient_2
/* DHCP server selects a pool from a class by matching options in the received DISCOVER
packet with the match option. */

router(config-dhcpv4-server-profile-class)#exit

router(config-dhcpv4-server-profile)#exit

router(config-dhcpv4)#commit
```

実行コンフィギュレーション

```
Router#show running-config dhcp ipv4
dhcp ipv4
profile ISP1 server
pool ISP1_POOL
class ISP1_CLASS
pool ISP1_CLASS_POOL
match option 60 hex PXEClient_1
exit
exit
profile ISP2 server
dns-server 10.20.3.4
pool ISP2_POOL
class ISP2_CLASS
pool ISP2_CLASS_POOL
match option 60 hex PXEClient_2
exit
exit
!
```

DAP プール一致オプションを使用しないサーバプロファイルの設定

ここでは、DAP プール一致オプションを使用しないサーバプロファイルの設定について説明します。

設定例

```
router#configure

router(config)#dhcp ipv4
/* The 'dhcp ipv6' command configures DHCP for IPv6 and enters the DHCPv6 configuration
submode. */

router(config-dhcpv4)#profile ISP1 server
/* Enters the server profile configuration mode. */

router(config-dhcpv4-server-profile)#dns-server ISP1.com
/* Configures the name of the DNS server or IP address. */

router(config-dhcpv4-server-profile)#exit

router(config-dhcpv4)#profile ISP2 server
/* Enters the server profile configuration mode. */

router(config-dhcpv4-server-profile)#dns-server ISP2.com
/* Configures the name of the DNS server or IP address. */

router(config-dhcpv4-server-profile)#exit

router(config-dhcpv4)#commit
```

実行コンフィギュレーション

```
Router#show running-config dhcp ipv4
dhcp ipv4
  profile ISP1 server
    dns-server ISP1.com
  exit
  profile ISP2 server
    dns-server ISP2.com
  exit
!
```

DAP での ISP ごとのアドレス プール設定

ここでは、DAP で ISP ごとにアドレス プールを設定する方法について説明します。

設定例

```
router#configure

router(config)#pool vrf ISP_1 ipv4 ISP1_POOL
/* Configures an IPv4 pool for the specified VRF or all VRFs. Use the 'ipv6' keyword for
IPv6 pool. */

router(config-pool-ipv4)#network 10.10.10.0
```

```
/* Specifies network for allocation. */

router(config-pool-ipv4)#exit

router(config)#pool vrf ISP_2 ipv4 ISP2_POOL
/* Configures an IPv4 pool for the specifed VRF or all VRFs. */

router(config-pool-ipv4)#network 10.20.20.0
/* Specifies network for allocation. */

router(config-pool-ipv4)#exit

router(config-dhcpv4)#commit
```

実行コンフィギュレーション

```
Router#show running-config pool
pool vrf ISP_1 ipv4 ISP1_POOL
  network 10.10.10.0
  exit
pool vrf ISP_2 ipv4 ISP2_POOL
  network 10.20.20.0
!
```

DHCP クライアント

Dynamic Host Configuration Protocol (DHCP) クライアント機能を使用すると、ルータインターフェイスが IPv4、DHCPv4、DHCPv6 サーバのいずれかを動的に取得し、該当するレイヤ 2 アドレスに応答を転送します。これにより、該当するデバイスが適切な設定情報を取得できるようになります。

DHCP は、リース期間と呼ばれる設定可能な期間にのみ IP アドレスを割り当てることができます。クライアントがこの IP アドレスをリース期間を超えて保持する必要がある場合は、IP アドレスが期限切れになる前にリース期間を更新する必要があります。クライアントは、サーバから送信された設定に基づいてリースを更新します。クライアントは、サーバの IP アドレスを使用して REQUEST メッセージをユニキャストします。サーバは REQUEST メッセージを受信すると、ACK メッセージで応答します。クライアントのリース期間が、ACK メッセージに設定されたリース時間で延長されます。

制約事項と制限

- DHCPv4 または DHCPv6 クライアントは、管理インターフェイスでのみイネーブルにできます。
- インターフェイスで設定できるのは、DHCPv4、DHCPv6、スタティック IPv4、スタティック IPv6 のいずれかです。

インターフェイスでの DHCP クライアントのイネーブル化

DHCPv4 または DHCPv6 クライアントは、インターフェイス レベルでイネーブルにできます。インターフェイスで DHCPv4 または DHCPv6 がイネーブル化またはディセーブル化されると、DHCP コンポーネントが通知を受信します。

```
Router# configure
Router(config)# interface MgmtEth rack/slot/CPU0/port
Router(config)# interface interface_name ipv6 address dhcp
```

DHCPv6 プロキシ バインディング テーブルのリロード 永続性

Cisco IOS XR Dynamic Host Configuration Protocol (DHCP) アプリケーションは、DHCP アプリケーションによってクライアントに割り当てられた DHCP リースの DHCP バインディング状態を維持する役割を担います。これらのバインディング状態は、DHCP アプリケーション（プロキシ/リレー/スヌーピング）によって学習されます。DHCP クライアントは、DHCP アプリケーションで発生するイベントに関係なく、DHCP リースを維持することを想定しています。



(注) リリース 6.2.2 以降では、DHCPv4 または DHCPv6 を稼働しているプロキシまたはサーバで 200K セッションがサポートされます。

この機能により、DHCP アプリケーションは上記のイベントを介してバインド状態を維持できます。

- プロセスの再起動：ローカル チェックポイント
- RP フェールオーバー：チェックポイントを使用したホットスタンバイ RP
- LC IMDR：ローカル チェックポイント
- LC OIR：RP 上のシャドー テーブル
- システムの再起動：ローカル ディスクに保存されたバインディング

システム永続メモリへの DHCP リレー バインディング データベースの書き込みの設定

システム永続メモリへの DHCP リレー バインディング データベースの書き込みを設定するには、次のタスクを実行します。これは、システムのリロード後に DHCP リレー バインディング テーブルを回復するのに役立ちます。完全な永続ファイルの書き込みに使用されるファイル名は、dhcpv4_srp_{nodeid}_odd or dhcpv6_srp_{nodeid}_odd および dhcpv4_srp_{nodeid}_even or dhcpv6_srp_{nodeid}_even です。nodeid は、ファイルが書き込まれるノードの実際のノード ID です。増分ファイルは完全なファイルと同じ方法で命名され、_inc が付加されます。

```
Router# configure
Router(config)# dhcp ipv6
Router(config-dhcpv6)# database [relay] [full-write-interval full-write-interval]
[incremental-write-interval incremental-write-interval]
Router(config-dhcpv6)# commit
```




第 7 章

アクセス リストおよびプレフィックス リストの実装

- [アクセス リストの概要 \(109 ページ\)](#)
- [IPv4 ACL の設定 \(113 ページ\)](#)
- [IPv6 ACL の設定 \(116 ページ\)](#)
- [ACL の変更 \(121 ページ\)](#)
- [ACL ベースの転送の設定 \(122 ページ\)](#)
- [ブリッジ仮想インターフェイスの ACL \(125 ページ\)](#)
- [フラグメント制御を使用した ACL の設定 \(128 ページ\)](#)
- [IP パケット長による ACL フィルタリングの設定 \(133 ページ\)](#)
- [オブジェクトグループ ACL の概要 \(137 ページ\)](#)
- [IPv4 ACL での TTL の照合および書き換えの設定 \(141 ページ\)](#)
- [IPv6 ACL での TTL の照合および書き換えの設定 \(143 ページ\)](#)
- [IP アクセス リスト ロギング メッセージの概要, on page 144](#)
- [プレフィックス リストの概要 \(145 ページ\)](#)
- [プレフィックス リストの設定 \(146 ページ\)](#)
- [プレフィックス リスト エントリの 順序付けとプレフィックス リストの変更 \(147 ページ\)](#)

アクセス リストの概要

アクセス リストは、パケット フィルタリングを実行して、ネットワークを介して移動するパケットとその場所を制御します。この処理は、ネットワークトラフィックを制限したり、ユーザやデバイスによるネットワークへのアクセスを制限したりするのに役立ちます。アクセス リストの用途は多様なので、多くのコマンドの構文でアクセス リストが参照されます。アクセス リストを使用して、次のようなことを実行できます。

アクセス コントロール リスト (ACL) は、ネットワークトラフィック プロファイルをまとめて定義する 1 つ以上のアクセス コントロール エントリ (ACE) です。このプロファイルは、トラフィック フィルタリング、ルート フィルタリング、QoS 分類、アクセス コントロールなど、Cisco IOS XR ソフトウェアの機能で参照できます。次の 2 種類の ACL があります。

- 標準的な ACL：パケットの送信元 IP アドレスのみを確認します。トラフィックは、ACL に設定されたアドレスまたはプレフィックスの比較と、パケットにある送信元アドレスで制御されます。
- 拡張 ACL：パケットの発信元アドレス以外の属性も確認します。確認する属性は、送信先アドレス、特定の IP プロトコル、UDP または TCP ポート番号、DSCP などです。ACL に記載されている属性と、着信パケットまたは発信パケット内の属性を比較することで、トラフィックが制御されます。

Cisco IOS XR は標準アクセス リストと拡張アクセス リストとを区別しません。標準アクセス リストをサポートしているのは、下位互換性を確保するためです。

IP アクセス リストの目的

- インターフェイスで着信パケットまたは発信パケットをフィルタリングします。
- ミラーリングのためにパケットをフィルタリングします。
- 必要に応じて、トラフィックをリダイレクトします。
- ルーティング アップデートの内容の制限
- アドレスまたはプロトコルに基づくデバッグ出力の制限
- vty へのアクセスの制御
- 輻輳回避、輻輳管理、プライオリティ キューイング、カスタム キューイングなどの高度な機能に使用されるトラフィックの特定または分類

IP アクセス リストの機能

アクセス リストは、`permit` ステートメントと `deny` ステートメントで構成される順次リストです。これらのステートメントは、IP アドレス、場合によっては上位層 IP プロトコルに適用されます。アクセス リストには、参照に使用される名前があります。多くのソフトウェア コマンドは、構文の一部としてアクセス リストを受け取ります。

アクセス リストを設定して名前を付けることは可能ですが、アクセス リストを受け取るコマンドによってアクセスリストが参照されるまで、有効にはなりません。複数のコマンドから同じアクセス リストを参照できます。アクセス リストで、ルータに到達するトラフィック、またはルータ経由で送信されるトラフィックは制御できますが、ルータが送信元のトラフィックは制御できません。

送信元アドレスと宛先アドレスは、IP パケットの最も一般的な2つのフィールドで、アクセス リストの基礎となります。送信元アドレスを指定して、特定のネットワーキングデバイスまたはホストからのパケットを制御します。宛先アドレスを指定して、特定のネットワーキングデバイスまたはホストに送信されるパケットを制御します。

また、トランスポート層の情報（パケットが TCP、UDP、ICMP、IGMP のいずれであるかなどの情報）に基づいてパケットをフィルタリングすることもできます。

ACL のワークフロー

次の図に、ACL のワークフローを示します。

IP アクセス リストのプロセスとルール

IP アクセス リストを設定するときは、次のプロセスとルールを使用してください。

- アクセスリストの条件に対してフィルタリングされる各パケットの送信元アドレスや宛先アドレス、またはプロトコルがテストされます。一度に1つの条件（**permit** ステートメントまたは **deny** ステートメント）がテストされます。
- パケットがアクセスリストのステートメントに一致しないと、そのパケットはリスト内の次のステートメントに対してテストされます。
- パケットとアクセスリストのステートメントが一致すると、リスト内の残りのステートメントはスキップされ、パケットは一致したステートメントに指定されたとおりに許可または拒否されます。パケットが許可されるか拒否されるかは、パケットが一致する最初のエントリによって決まります。つまり、一致すると、それ以降のエントリは考慮されません。
- アクセスリストでアドレスまたはプロトコルが拒否されると、パケットは廃棄され、インターネット制御メッセージプロトコル（ICMP）ホスト到達不能メッセージが返されます。ICMP は、Cisco IOS XR ソフトウェアで設定できます。
- 各アクセス リストの最後には暗黙の **deny** ステートメントがあるため、一致する条件がない場合は、パケットはドロップされます。つまり、各ステートメントに対してテストするときまでにパケットを許可または拒否しないと、パケットは拒否されます。
- アクセス リストには **permit** ステートメントを1つ以上含める必要があります。そうしないと、パケットはすべて拒否されます。
- 最初に一致が見つかった後は条件のテストが終了するため、条件の順序は重要です。同じ **permit** ステートメントまたは **deny** ステートメントでも、順序が異なる場合、ある状況では通過し、別の状況では拒否されるパケットが生じる可能性があります。
- 1つのインターフェイス、1つのプロトコル、1つの方向につき、許可されるアクセス リストは1つだけです。
- インバウンドアクセス リストは、ルータに到達するパケットを処理します。着信パケットの処理後に、アウトバウンドインターフェイスへのルーティングが行われます。インバウンドアクセスリストが効率的なのは、フィルタリングテストで拒否されたことでパケットが廃棄される場合、ルーティング検索のオーバーヘッドが抑えられるためです。パケットがテストで許可されると、そのパケットに対してルーティングの処理が実施されます。インバウンドリストの場合、**permit** はインバウンド インターフェイスで受信したパケットが引き続き処理されることを意味し、**deny** はパケットが廃棄されることを意味します。
- アウトバウンドアクセス リストの場合、パケットの処理後にルータから送信されます。着信パケットはアウトバウンドインターフェイスにルーティングされてから、アウトバウ

ンドアクセスリストで処理されます。アウトバウンドリストの場合、許可とは、出力バッファに対して送信されることを示し、拒否とは、パケットが廃棄されることを示します。

- アクセス リストは、使用中のアクセス グループによって適用されている場合には削除できません。アクセス リストを削除するには、まずアクセス リストを参照しているアクセス グループを削除してから、アクセス リストを削除します。
- 特定のトラフィックを拒否する ACL で設定されているインターフェイスを削除する前に、その ACL を削除し、設定をコミットする必要があります。これを実行しないと、**no interface <interface-name>** コマンドが設定され、コミットされるとすぐにインターフェイスを通じて一部のパケットがリークします。
- **ipv4 | ipv6 access group** コマンドを使用するには、アクセス リストが必要です。

ワイルドカード マスクと暗黙的なワイルドカード マスクを使用した ACL フィルタリング

アドレスフィルタリングでは、アクセスリストエントリ内のアドレスビットとアクセスリストに送信されるパケットを比較するときに、ワイルドカード マスクを使用して、対応する IP アドレス ビットを確認するか無視するかを指定します。管理者は、ワイルドカード マスクを慎重に設定することにより、許可または拒否のテストに 1 つまたは複数の IP アドレスを選択できます。

IP アドレス ビット用のワイルドカード マスクでは、数値 1 と数値 0 を使用して、対応する IP アドレス ビットをどのように扱うかを指定します。1 と 0 は、サブネット（ネットワーク）マスクで意味する内容が逆になるため、ワイルドカード マスクは逆マスクとも呼ばれます。

- ワイルドカード マスク ビット 0 は、対応するビット値を確認することを示します。
- ワイルドカード マスクのビット 1 は、対応するビット値を無視することを意味します。

アクセス リスト ステートメントでは、送信元アドレスまたは宛先アドレスにワイルドカード マスクを指定する必要はありません。**host** キーワードを使用すると、ワイルドカード マスクとして 0.0.0.0 を指定したものと見なされます。

サブネットマスクでは、ネットワークとサブネットを示す隣接ビットをマスクにする必要がありますが、それとは異なり、ワイルドカード マスクではマスクに非隣接ビットを使用できます。

ワイルドカード ビットの代わりに、CIDR 形式 (/x) を使用することもできます。たとえば、IPv4 アドレス 1.2.3.4 0.255.255.255 は 1.2.3.4/8 に相当し、IPv6 アドレスの場合、2001:db8:abcd:0012:0000:0000:0000:0000 は 2001:db8:abcd:0012::0/64 に相当します。

アクセス リストのコメントの組み入れ

remark アクセス リスト コンフィギュレーション コマンドを使用すると、名前付き IP アクセス リストにエントリに関するコメント（注釈）を含めることができます。コメントを含めると、ネットワーク管理者がアクセス リストを理解し、精査しやすくなります。1 つのコメント行の最大長は 255 文字です。

コメントは、**permit** ステートメントまたは **deny** ステートメントの前後どちらにでも配置できます。コメントがどの **permit** ステートメントまたは **deny** ステートメントの説明であるのかが明確になるように、コメントの位置に関して一貫性を保つようにしてください。たとえば、一部のコメントが **permit** または **deny** ステートメントの前にあり、他のコメントがステートメントの後ろにあると、混乱を招きます。コメントに順番を付けることができます。

アクセスリストの作成後、アクセスリストをインターフェイスまたは端末回線に適用することを忘れないでください。

IPv4 ACL の設定

この項では、IPv4 の入力 ACL と出力 ACL の基本的な設定について説明します。

IPv4 入力 ACL を設定するための注意事項と制約事項

IPv4 入力 ACL は、次の動作を特徴としています。

- 許可 ACL 一致の統計情報はサポートされていません。
- 入力 IPv4 ACL は、管理インターフェイス以外のすべてのインターフェイスでサポートされています。
- ACL ベースの転送（ABF）は、入力方向でのみサポートされています。
- NPU ごとにデフォルトで許可されている ACL の総数は 32127 です。
- ラインカードごとに許可されている付加された ACE の数は 4,000 です。
- 入力インターフェイスによる ACL ロギング（**log-input** キーワードを使用）はサポートされていません。
- 統計情報を確認するための **show access-lists ipv4 acl_name stats** コマンドは、ログを含む ACE ではサポートされません。したがって、ログを含む ACE の統計情報を確認するには、**show access-lists acl-name hardware [ingress | egress] detail location/loc** コマンドを使用してください。
- **show access-lists ipv4 <ACL name> hardware ingress location 0/RP0/CPU0** コマンドを使用した入力 ACL 一致統計情報は、反映されるまでに遅延（最大 15 秒）が発生する場合があります。

IPv4 出力 ACL を設定するための注意事項と制約事項

IPv4 出力 ACL は、次の動作を特徴としています。

- 出力 IPv4 ACL は、メインの物理インターフェイスとバンドルインターフェイスでサポートされています。



(注) 出力 ACL は、サブインターフェイスでは直接サポートされていません。ただし、サブインターフェイスがあるメインのインターフェイス上に出力 ACL を設定した場合、ACL アクションはサブインターフェイストラフィックにも適用されます。この出力 ACL の動作は、メインのインターフェイスに ACL を適用した後でサブインターフェイスを設定した場合も同じです。

- NPU ごとに許可された出力 ACL の総数は 255 です。
- ACL は、出力方向の管理インターフェイスではサポートされていません。
- ライン カードごとに許可されている付加された ACE の数は 4,000 です。
- ACL ロギング (**log** コマンドを使用) と入力インターフェイスによる ACL ロギング (**log-input** コマンドを使用) はサポートされていません。
- 階層型 QoS がイネーブルの場合、出力 ACL はサブインターフェイスでサポートされます。ただし、メインのインターフェイス上に設定された 出力 ACL はサブインターフェイストラフィックには適用されません。

ギガビットイーサネット インターフェイス上での入力 IPv4 ACL の設定

GigE インターフェイス上で入力 IPv4 ACL を設定するには、次の設定を使用します。

```
/* Configure a GigE interface with an IPv4 address */
Router(config)# interface TenGigE 0/11/0/0
Router(config-if)# ipv4 address 10.1.1.1 255.255.255.0
Router(config-if)# no shut
Router(config-if)# commit
Thu Jan 25 10:07:54.700 IST
Router(config-if)# exit

/* Verify if the interface is up */
Router(config)# do show ipv4 interface brief
Thu Jan 25 10:08:49.087 IST

Interface                               IP-Address      Status          Protocol
Vrf-NameTenGigE0/11/0/0                 10.1.1.1        Up              Up          default

/* Configure an IPv4 ingress ACL */
Router(config)# ipv4 access-list V4-ACL-INGRESS
Router(config-ipv4-acl)# 10 permit tcp 10.2.1.1 0.0.0.255 any
Router(config-ipv4-acl)# 20 deny udp any any
Router(config-ipv4-acl)# 30 permit ipv4 10.2.0.0 0.255.255.255 any
Router(config-ipv4-acl)# commit
Thu Jan 25 10:16:11.473 IST

/* Verify the ingress ACL creation */
Router(config)# do show access-lists ipv4
Thu Jan 25 10:25:19.896 IST
...
ipv4 access-list V4-ACL-INGRESS
  10 permit tcp 10.2.1.0 0.0.0.255 any
  20 deny udp any any
```

```

30 permit ipv4 10.0.0.0 0.255.255.255 any

/* Apply the ingress ACL to the GigE interface */
Router(config)# interface TenGigE0/11/0/0
Router(config-if)# ipv4 access-group V4-ACL-INGRESS ingress
Router(config-if)# commit
Thu Jan 25 10:28:19.671 IST
Router(config-if)# exit

/* Verify if the ingress ACL has been successfully applied to the interface */
Router(config)# do show ipv4 interface
Thu Jan 25 10:29:44.944 IST
TenGigE0/11/0/0 is Up, ipv4 protocol is Up
  Vrf is default (vrfid 0x60000000)
  Internet address is 10.1.1.1/24
  MTU is 1514 (1500 is available to IP)
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound common access list is not set, access list is V4-ACL-INGRESS
  Proxy ARP is disabled
  ICMP redirects are never sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  Table Id is 0xe0000000

```

ギガビットイーサネットインターフェイス上にIPv4入力ACLを正常に設定しました。

ギガビットイーサネットインターフェイス上での出力IPv4 ACLの設定

GigE インターフェイス上で出力IPv4 ACLを設定するには、次の設定を使用します。

```

/* Configure a GigE interface with an IPv4 address */
Router(config)# interface TenGigE 0/11/0/0
Router(config-if)# ipv4 address 20.1.1.1 255.255.255.0
Router(config-if)# no shut
Router(config-if)# commit
Thu Jan 25 10:08:38.767 IST
Router(config-if)# exit

/* Verify if the interface is up */
Router(config)# do show ipv4 interface brief
Thu Jan 25 10:08:49.087 IST

Interface                IP-Address      Status      Protocol Vrf-Name
TenGigE0/11/0/0          10.1.1.1        Up          default
TenGigE0/11/0/1          20.1.1.1        Up          default

/* Configure an IPv4 egress ACL */
Router(config)# ipv4 access-list V4-ACL-EGRESS
Router(config-ipv4-acl)# 10 permit ipv4 10.2.0.0 0.255.255.255 20.2.0.0 0.255.255.255
Router(config-ipv4-acl)# 20 deny ipv4 any any
Router(config-ipv4-acl)# commit
Thu Jan 25 10:25:04.655 IST

/* Verify the egress ACL creation */
Router(config)# do show access-lists ipv4
Thu Jan 25 10:25:19.896 IST
ipv4 access-list V4-ACL-EGRESS
  10 permit ipv4 10.0.0.0 0.255.255.255 20.0.0.0 0.255.255.255
  20 deny ipv4 any any

```

```

...

/* Apply the egress ACL to the GigE interface */
Router(config)# interface TenGigE 0/11/0/1
Router(config-if)# ipv4 access-group V4-ACL-EGRESS egress
Router(config-if)# commit
Thu Jan 25 10:28:45.937 IST
Router(config-if)# exit

/* Verify if the egress ACL has been successfully applied to the interface */
Router(config)# do show ipv4 interface
Thu Jan 25 10:29:44.944 IST
TenGigE 0/11/0/1 is Up, ipv4 protocol is Up
  Vrf is default (vrfid 0x60000000)
  Internet address is 20.1.1.1/24
  MTU is 1514 (1500 is available to IP)
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is V4-ACL-EGRESS
  Inbound common access list is not set, access list is not set
  Proxy ARP is disabled
  ICMP redirects are never sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  Table Id is 0xe0000000
...

```

ギガビット イーサネット インターフェイス上に IPv4 出力 ACL を正常に設定しました。

IPv6 ACL の設定

この項では、ギガビットイーサネットとバンドルイーサネットを介して入力 IPv6 ACL と出力 IPv6 ACL を設定するステップについて説明します。

IPv6 入力 ACL を設定するための注意事項と制約事項

IPv6 入力 ACL は、次の動作を特徴としています。

- 入力 IPv6 ACL はすべてのインターフェイスでサポートされています。
- ACL ベースの転送 (ABF) は、入力方向でのみサポートされています。
- NPU ごとに許可されている ACL の総数は 32127 です。
- ライン カードごとに許可されている付加された ACE の数は 2047 です。
- 入力インターフェイスによる ACL ロギング (**log-input** キーワードを使用) はサポートされていません。
- パケット長 (**pkt-length** キーワードを使用) はサポートされていません。
- 統計情報を確認するための **show access-lists ipv4 acl_name stats** コマンドは、ログを含む ACE ではサポートされません。したがって、ログを含む ACE の統計情報を確認するには、**show access-lists acl-name hardware [ingress | egress] detail location/loc** コマンドを使用してください。

- **show access-lists ipv6 <ACL name> hardware ingress location 0/RP0/CPU0** コマンドを使用した入力 ACL 一致統計情報は、反映されるまでに遅延（最大 15 秒）が発生する場合があります。

IPv6 出力 ACL を設定するための注意事項と制約事項

IPv6 出力 ACL は、次の動作を特徴としています。

- パケット長の設定は、出力 ACL ではサポートされていません。
- TCP フラグは出力 ACL ではサポートされていません。
- 出力 ACL は、BVI インターフェイスおよび L2 インターフェイスではサポートされていません。
- QoS グループの設定は、出力 ACL ではサポートされていません。
- 出力 ACL では、スループットの 50% 以下がサポートされます。
- スループットの制限を除き、ルータによって生成されたトラフィックが出力 IPv6 ACL の影響を受けることはありません。
- NPU ごとに許可された出力 ACL の総数は 255 です。
- ラインカードごとに許可されている付加 ACE の合計数は 2000 です。
- ダイナミック TCAM キーの設定は、出力 ACL ではサポートされていません。
- 出力 IPv6 ACL がリサイクルパスを取得するため、NPU ごとに最大で合計 160GB の IPv6 出力 ACL がサポートされます。
- 階層型 QoS がイネーブルの場合、出力 ACL はサブインターフェイスでサポートされます。ただし、メインのインターフェイス上に設定された出力 ACL はサブインターフェイスのトラフィックには適用されません。

ギガビットイーサネットインターフェイス上での入力 IPv6 ACL の設定

GigE インターフェイス上で入力 IPv6 ACL を設定するには、次の設定を使用します。

```
/* Configure a GigE interface with an IPv6 address */
Router(config)# interface TenGigE 0/11/0/0
Router(config-if)# ipv6 address 1001::1/64
Router(config-if)# no shut
Router(config-if)# commit
Thu Jan 25 10:07:54.700 IST
Router(config-if)# exit

/* Verify if the interface is up */
Router(config)# do show ipv6 interface brief
Thu Jan 25 12:38:35.742 IST
TenGigE 0/11/0/0 [Up/Up]
    fe80::bd:b9ff:fea9:5606
    1001::1
...

/* Configure an IPv6 ingress ACL */
```

```

Router(config)# ipv6 access-list V6-INGRESS-ACL
Router(config-ipv6-acl)# 10 permit ipv6 any any
Router(config-ipv6-acl)# 20 deny udp any any
Router(config-ipv6-acl)# commit
Thu Jan 25 11:31:24.488 IST
Router(config-ipv6-acl)# exit

/* Verify the ingress ACL creation */
Router(config)# do show access-lists ipv6
Thu Jan 25 11:34:56.911 IST
ipv6 access-list V6-INGRESS-ACL
  10 permit ipv6 any any
  20 deny udp any any

/* Apply the ingress ACL to the GigE interface */
Router(config)# interface TenGigE 0/11/0/0
Router(config-if)# ipv6 access-group V6-INGRESS-ACL ingress
Router(config-if)# commit
Thu Jan 25 11:32:55.194 IST
Router(config-if)# exit

/* Verify if the ingress ACL has been successfully applied to the interface */
Router(config)# do show ipv6 interface
Thu Jan 25 11:34:08.028 IST
TenGigE 0/11/0/0 is Up, ipv6 protocol is Up, Vrfid is default (0x60000000)
  IPv6 is enabled, link-local address is fe80::bd:b9ff:fea9:5606
  Global unicast address(es):
    1001::1, subnet is 1001::/64
    Joined group address(es): ff02::1:ff00:1 ff02::1:ffa9:5606 ff02::2
                             ff02::1
    MTU is 1514 (1500 is available to IPv6)
    ICMP redirects are disabled
    ICMP unreachable are enabled
    ND DAD is enabled, number of DAD attempts 1
    ND reachable time is 0 milliseconds
    ND cache entry limit is 1000000000
    ND advertised retransmit interval is 0 milliseconds
    Hosts use stateless autoconfig for addresses.
    Outgoing access list is not set
    Inbound common access list is not set, access list is V6-INGRESS-ACL
    Table Id is 0xe0800000
    Complete protocol adjacency: 0
    Complete glean adjacency: 0
    Incomplete protocol adjacency: 0
    Incomplete glean adjacency: 0
    Dropped protocol request: 0
    Dropped glean request: 0
...

```

ギガビットイーサネットインターフェイス上にIPv6入力ACLを正常に設定しました。

ギガビットイーサネットインターフェイス上での出力IPv6 ACLの設定

GigEインターフェイス上で出力IPv6 ACLを設定するには、次の設定を使用します。

```

/* Configure a GigE interface with an IPv6 address */
Router(config)# interface TenGigE 0/11/0/1
Router(config-if)# ipv6 address 2001::1/64
Router(config-if)# no shut
Router(config-if)# commit

```



```

Thu Jan 25 11:41:25.778 IST
Router(config-if)# exit

/* Verify if the interface is up */
Router(config)# do show ipv6 interface brief
Thu Jan 25 12:38:35.742 IST
TenGigE 0/11/0/0 [Up/Up]
    fe80::bd:b9ff:fea9:5606
    1001::1
TenGigE 0/11/0/1 [Up/Up]
    fe80::23:e9ff:fea8:a44e
    2001::1

/* Configure an IPv6 egress ACL */
Router(config)# ipv6 access-list V6-EGRESS-ACL
Router(config-ipv6-acl)# 10 permit ipv6 any any
Router(config-ipv6-acl)# 20 deny udp any any
Router(config-ipv6-acl)# commit
Thu Jan 25 11:44:03.969 IST
Router(config-ipv6-acl)# exit

/* Verify the egress ACL creation */
Router(config)# do show access-lists ipv6
Thu Jan 25 11:45:53.823 IST
ipv6 access-list V6-EGRESS-ACL
  10 permit ipv6 any any
  20 deny udp any any
...

/* Apply the egress ACL to the GigE interface */
Router(config)# interface TenGigE 0/11/0/1
Router(config-if)# ipv6 access-group V6-EGRESS-ACL egress
Router(config-if)# commit
Thu Jan 25 11:45:12.682 IST
Router(config-if)# exit

/* Verify if the egress ACL has been successfully applied to the interface */
Router(config)# do show ipv6 interface
Thu Jan 25 11:46:43.234 IST
...
TenGigE 0/11/0/1 is Up, ipv6 protocol is Up, Vrfid is default (0x60000000)
  IPv6 is enabled, link-local address is fe80::23:e9ff:fea8:a44e
  Global unicast address(es):
    2001::1, subnet is 2001::/64
  Joined group address(es): ff02::1:ff00:1 ff02::1:ffa8:a44e ff02::2
    ff02::1
  MTU is 1514 (1500 is available to IPv6)
  ICMP redirects are disabled
  ICMP unreachable are enabled
  ND DAD is enabled, number of DAD attempts 1
  ND reachable time is 0 milliseconds
  ND cache entry limit is 1000000000
  ND advertised retransmit interval is 0 milliseconds
  Hosts use stateless autoconfig for addresses.
Outgoing access list is V6-EGRESS-ACL
  Inbound common access list is not set, access list is not set
  Table Id is 0xe0800000
  Complete protocol adjacency: 0
  Complete glean adjacency: 0
  Incomplete protocol adjacency: 0
  Incomplete glean adjacency: 0
  Dropped protocol request: 0
  Dropped glean request: 0

```

...

ギガビットイーサネットインターフェイス上に IPv6 出力 ACL を正常に設定しました。

バンドルインターフェイス上での入力 IPv6 ACL と出力 IPv6 ACL の設定

バンドルインターフェイス上で入力 IPv6 ACL と出力 IPv6 ACL を設定するには、次の設定を使用します。

```
/* Configure a bundle interface with an IPv6 address */
Router(config)# interface Bundle-Ether 1
Router(config-if)# ipv6 address 3001::1/64
Router(config-if)# no shut
Router(config-if)# commit
Thu Jan 25 13:53:47.435 IST
Router(config-if)# exit

/* Configure an IPv6 egress ACL */
Router(config)# ipv6 access-list V6-EGRESS-ACL-bundle interface
Router(config-ipv6-acl)# 100 permit tcp any any eq www
Router(config-ipv6-acl)# 110 permit tcp any any eq https
Router(config-ipv6-acl)# 120 permit tcp any any eq ssh
Router(config-ipv6-acl)# 130 permit udp any any eq snmp
Router(config-ipv6-acl)# commit
Thu Jan 25 13:57:14.960 IST
Router(config-ipv6-acl)# exit

/* Configure an IPv6 ingress ACL to deny ingress traffic on the bundle interface */
Router(config)# ipv6 access-list V6-DENY-INGRESS-ACL
Router(config-ipv6-acl)# 10 deny ipv6 any any
Router(config-ipv6-acl)# commit
Thu Jan 25 13:59:23.198 IST
Router(config-ipv6-acl)# exit

/* Verify the egress and ingress ACL creation */
Router(config)# do show access-lists ipv6
Thu Jan 25 14:00:24.055 IST
ipv6 access-list V6-DENY-INGRESS-ACL
 10 deny ipv6 any any
ipv6 access-list V6-EGRESS-ACL-bundle
 100 permit tcp any any eq www
 110 permit tcp any any eq https
 120 permit tcp any any eq ssh
 130 permit udp any any eq snmp
...

/* Apply the egress and ingress ACLs to the bundle interface */
Router(config)# interface Bundle-Ether 1
Router(config-if)# ipv6 access-group V6-EGRESS-ACL-bundle egress
Router(config-if)# ipv6 access-group V6-DENY-INGRESS-ACL ingress
Router(config-if)# commit
Thu Jan 25 14:04:19.536 IST
Router(config-if)# exit

/* Verify if the ACLs have been successfully applied to the interface */
Router(config)# do show ipv6 interface
Thu Jan 25 11:46:43.234 IST
...
Thu Jan 25 14:04:51.322 IST
Bundle-Ether1 is Down, ipv6 protocol is Down, Vrfid is default (0x60000000)
  IPv6 is enabled, link-local address is fe80::1:10ff:fe87:8d04 [TENTATIVE]
```

```

Global unicast address(es):
  3001::1, subnet is 3001::/64 [TENTATIVE]
Joined group address(es): ff02::2 ff02::1
MTU is 1514 (1500 is available to IPv6)
ICMP redirects are disabled
ICMP unreachable are enabled
ND DAD is enabled, number of DAD attempts 1
ND reachable time is 0 milliseconds
ND cache entry limit is 1000000000
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 160 to 240 seconds
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses.
Outgoing access list is V6-EGRESS-ACL-BI
Inbound common access list is not set, access list is V6-DENY-INGRESS-ACL
Table Id is 0xe0800000
Complete protocol adjacency: 0
Complete glean adjacency: 0
Incomplete protocol adjacency: 0
Incomplete glean adjacency: 0
Dropped protocol request: 0
Dropped glean request: 0

```

バンドル インターフェイス上に入力 IPv6 ACL と出力 IPv6 ACL を正常に設定しました。

ACL の変更

この項では、ACL を変更するための設定の例について説明します。

```

*/ Create an Access List*/
Router(config)#ipv4 access-list acl_1

*/Add entries (ACEs) to the ACL*/
Router(config-ipv4-acl)#10 permit ip host 10.3.3.3 host 172.16.5.34
Router(config-ipv4-acl)#20 permit icmp any any
Router(config-ipv4-acl)#30 permit tcp any host 10.3.3.3
Router(config-ipv4-acl)#end

*/Verify the entries of the ACL*/:
Router#show access-lists ipv4 acl_1
ipv4 access-list acl_1
10 permit ip host 10.3.3.3 host 172.16.5.34
20 permit icmp any any
30 permit tcp any host 10.3.3.3

*/Add new entries, one with a sequence number "15" and another without a sequence number
to the ACL. Delete an entry with the sequence number "30":*/
Router(config)#ipv4 access-list acl_1
Router(config-ipv4-acl)# 15 permit 10.5.5.5 0.0.0.255
Router(config-ipv4-acl)# no 30
Router(config-ipv4-acl)# permit 10.4.4.4 0.0.0.255
Router(config-ipv4-acl)# commit

*/When an entry is added without a sequence number, it is automatically given a sequence
number
that puts it at the end of the access list. Because the default increment is 10, the
entry will have a sequence
number 10 higher than the last entry in the existing access list*/

```

```

*/Verify the entries of the ACL:*/
Router(config)#show access-lists ipv4 acl_1
ipv4 access-list acl_1
 10 permit ipv4 host 10.3.3.3 host 172.16.5.34

15 permit 10.5.5.5 0.0.0.255---*/newly added ACE (with the sequence number)*/
20 permit icmp any any
30 permit ipv4 10.4.4.0 0.0.0.255 any ---*/newly added ACE (without the sequence number)*/

*/The entry with the sequence number 30, that is, "30 permit tcp any host 10.3.3.3" is
deleted from the ACL*/

```

機能中の ACL を正常に変更しました。

ACL ベースの転送の設定

統合ネットワークは、音声、ビデオ、およびデータを伝送します。トラフィックによっては、ルーティングプロトコルが算出したパスを使用するのではなく、特定のパスにルーティングすることが必要になる場合があります。これを実現するには、ACL 設定にネクストホップアドレスを指定します。これで、パケットベースで宛先アドレスをルックアップするのではなく、ACL に設定したネクストホップアドレスを使用して指定の宛先にパケットを転送できるようになります。ACL 設定でネクストホップを使用して転送するというこの機能は、ACL ベース転送 (ABF) と呼ばれます。

ACL ベース転送を使用すると、ブロードキャスト TV over IP、IP テレフォニー、データなどを対象としたサービスを複数のプロバイダーから選択することが可能になり、カフェテリア形式でインターネットにアクセスできます。サービス プロバイダーは、ユーザ トラフィックをさまざまなコンテンツ プロバイダーに迂回させることができます。

機能概要

- ABF は入力 ACL でのみサポートされています。
- ABF はネクストホップの変更をサポートしています。ネクストホップの変更、ネクストホップの削除、または既存のネクストホップ間での変更が可能です。



(注) ネクストホップがデフォルトの VRF 内にある場合を除き、ACE ルールの定義時にすべてのネクストホップの VRF を指定する必要があります。これにより、パケットがネクストホップへの適切なパスを取得できるようになります。

- VRF 認識型 ABF は、最大 3 つのネクストホップがある IPv4 と IPv6 でサポートされています。
- GRE インターフェイスを介してルーティングされた IPv4 ABF のネクストホップがサポートされています。

- ABF は ACL ベースであるため、ACL 内の既存のルール (ACE) に一致しないパケットはデフォルトの ACL ルール (すべてドロップ) に従います。ACL が (セキュリティ上の理由ではなく) ABF リダイレクトにのみ使用されている場合は、ACL の末尾 (最下位のユーザ プライオリティ) に明示的な ACL ルールを組み込んで、すべてのトラフィックを照合して「許可」します。これにより、ABF ルールに一致しないすべてのトラフィックが許可され、通常通りに転送されるようになります。
- ABF は、許可ルールのみでサポートされています。
- VRF-select (ネクストホップに対して VRF のみが設定されている場合) は、IPv4 および IPv6 アドレスの ABF でサポートされ、最大 3 つの VRF ネクストホップが許可されます。
- ABF のデフォルトのルートはサポートされていません。
- 低速パスでは ABF がサポートされないため、NPU からラインカード CPU へと入力方向にパントされたパケットは ABF では処理されません。通常、これらのパケットは、ソフトウェアデータプレーンによる送信先アドレスのルックアップに基づいて転送されます。これらのタイプのパケットには、IPv4 オプション、IPv6 拡張ヘッダー、および収集 (未解決/不完全) 隣接関係宛のパケットなどがありますが、これらに限定されません。
- ローカル IP インターフェイス宛のパケット (「for-us」パケット) は、ABF アクションが含まれているルールに一致した場合はリダイレクトの対象になります。これは、「for-us」パケットへの一致を避けるために十分な具体的なルールを作成するか、または ABF ルールの照合よりも前に (高いプライオリティの) 明確な許可 ACL ルールを ACL に配置することで防ぐことができます。

設定例

ACL ベースの転送を設定するには、次の設定例を使用します。

```
/* Enter IPv4 access list configuration mode and configure an ACL: */
Router# configure
Router(config)# ipv4 access-list abf-acl

/* Set the conditions for the ACL and configure ABF: */
/* The next hop for this entry is specified. */
Router(config-ipv4-acl)# 10 permit ipv4 192.168.18.0 0.255.255.255 any nexthop1 ipv4 192.168.20.2
Router(config-ipv4-acl)# 15 permit ipv4 192.168.21.0 0.0.0.255 any
Router(config-ipv4-acl)# 20 permit ipv4 192.168.22.0 0.0.255.255 any nexthop1 ipv4 192.168.23.2
/* More than two nexthops */
Router(config-ipv4-acl)# 25 permit tcp any range 2000 3000 any range 4000 5000 nexthop1 ipv4 192.168.23.1 nexthop2 ipv4 192.168.24.1 nexthop3 ipv4 192.168.25.1

/* VRF support on ABF */
Router(config-ipv4-acl)# 30 permit tcp any eq www host 192.168.12.2 precedence immediate nexthop1 vrf vrf1_ipv4 ipv4 192.168.13.2 nexthop2 vrf vrf1_ipv4 ipv4 192.168.14.2

Router(config-ipv4-acl)# 35 permit ipv4 any any

Router(config-ipv4-acl)# commit

/* (Optional) Display ACL information: */
Router# show access-lists ipv4 abf-acl
```

実行コンフィギュレーション

```

ipv4 access-list abf-acl
10 permit ipv4 192.168.18.0 0.255.255.255 any nexthop1 192.168.20.2
15 permit ipv4 192.168.21.0 0.0.0.255 any
20 permit ipv4 192.168.22.0 0.0.255.255 any nexthop1 192.168.23.2
25 permit tcp any range 2000 3000 any range 4000 5000 nexthop1 ipv4 192.168.23.1 nexthop2
   ipv4 192.168.24.1 nexthop3 ipv4 192.168.25.1
30 permit tcp any eq www host 192.168.12.2 precedence immediate nexthop1 vrf vrf1_ipv4
   ipv4 192.168.13.2 nexthop2 vrf vrf1_ipv4 ipv4 192.168.14.2
35 permit ipv4 any any
commit
!
```

```

ipv4 access-list TEST
10 permit ipv4 60.1.1.5 0.0.0.255 any nexthop1 vrf VRF1 nexthop2 vrf VRF2 nexthop3 vrf
   VRF3
!
```

確認

ABF 内の IP ネクストホップの状態を確認し、その予想されるネクストホップが起動するようになるには、次のコマンドを使用します。

```

Router# show access-lists ipv4 abf nexthops client pfilter_ea location 0/0/CPU0
Wed Jan 24 14:18:58.667 UTC
```

```

ACL name : abf-acl
ACE seq.  NH-1    NH-2    NH-3
-----
10          192.168.13.2
status      UP
at status   Not Present
exist       No
vrf         default
track
pd          ctx    Present
25  192.168.14.2    192.168.11.1  192.168.12.1
status      UP      Down    Down
at status   Not Present  Not Present  Not Present
exist       No      Yes     Yes
vrf         default  default  default
track
pd ctx      Present  Not present  Not present
30  192.168.15.1    192.168.12.7
status      Unknown  Unknown
at status   Not Present  Not Present
exist       No      Yes
vrf         vrf1_ipv4  vrf1_ipv4
track
pd ctx      Not present  Not present
```

ABF がラインカードのインターフェイスに現在付加されているかどうかを確認するには、次のコマンドを使用します。

```

show access-lists usage pfilter location all
```

ブリッジ仮想インターフェイスの ACL

ブリッジ仮想インターフェイス（BVI）は、ルータ上のルーティングドメインとブリッジングドメイン間にブリッジを提供します。BVIはIPアドレスで設定され、通常のルーテッドインターフェイスとして動作します。BVI上にACLを設定して、そのインターフェイスを使用するネットワークに対するトラフィックをフィルタリングできます。



- (注) BVIインターフェイスがブリッジドメインに含まれていない場合は、BVIインターフェイスに付加されているACLを削除しないでください。後でBVIインターフェイスをブリッジドメインに追加した場合は、トラフィックがドロップされます。

BVI上でのACLの設定によるTCAM消費の増加

BVIにACLが設定されている場合、TCAMリソースの消費は次のように影響されます。

- 入力ACLでは、同じACLのTCAMエントリが同じNPU上のインターフェイス間で共有されます。
- 出力ACLでは、同じACLのTCAMエントリはすべてのインターフェイスに一意です。これにより、TCAMリソースの消費が増加します。

BVI上でのACL設定の制約事項

BVI上でのACLの設定に進む前に、次の制約事項を認識しておく必要があります。

- BVIでは、出力IPv6 ACLはサポートされていません。
- **hw-module** コマンドを使用してBVI上で出力IPv4 ACLを有効にすると、そのACLでは他のインターフェイスタイプがサポートされません（このモードのACLでは、非BVIインターフェイスはサポートされません）。

BVIでのIPv4出力ACL設定の前提条件

デフォルトでは、BVI上のIPv4出力ACLは無効になっており、ACLがBVIに付加されていてもACLのフィルタリングは実行されません。そのため、**hw-module** コマンドを使用して、ラインカードのリロード時にACLを有効にします。



- (注) IPv4とIPv6の入力ACLはこの設定を必要としません。

次の設定を使用して、ハードウェア上のBVIでIPv4出力ACLを有効にし、ラインカードをリロードします。

```
/* Enable an IPv4 egress ACL on BVI */  
Router(config)# hw-module profile acl egress layer3 interface-based
```

```

/* Enable permit statistics for the egress ACL (by default, only deny statistics are
shown) */
Router(config)# hw-module profile stats acl-permit
Router(config)# commit
Router(config)# end
Router# reload location all
Wed Apr 5 23:05:46.193 UTC
Proceed with reload? [confirm]

```

設定

次の項では、BVI 上で IPv4 の入力 ACL と出力 ACL を設定する手順について説明します。

BVI で IPv4 の入力 ACL と出力 ACL を設定するには、次の設定例を使用した手順を実行します。

1. グローバル コンフィギュレーション モードを開始し、IPv4 入力 ACL を設定します。

```

Router(config)# ipv4 access-list v4-acl-ingress
Router(config-ipv4-acl)# 10 permit tcp any 10.1.1.0/24 dscp cs6
Router(config-ipv4-acl)# 20 deny udp any any eq ssh
Router(config-ipv4-acl)# 30 permit ipv4 any any
Router(config-ipv4-acl)# commit
Router(config-ipv4-acl)# exit

```

2. IPv4 出力 ACL を設定します。

```

Router(config)# ipv4 access-list v4-acl-egress
Router(config-ipv4-acl)# 10 deny ipv4 any any fragments log
Router(config-ipv4-acl)# 20 deny tcp any any ack
Router(config-ipv4-acl)# 30 permit ipv4 any any
Router(config-ipv4-acl)# commit
Router(config-ipv4-acl)# exit

```

3. BVI にマップする必要があるギガビット イーサネット インターフェイスを設定し、レイヤ 2 トランSPORT に対して有効にします。

```

Router(config)# interface GigabitEthernet 0/0/0/0
Router(config-if)# l2transport
Router(config-if-l2)# commit

```

4. 入力 ACL と出力 ACL を BVI に付加します。

```

Router(config)# interface BVI1
Router(config-if)# ipv4 access-group v4-acl-ingress ingress
Router(config-if)# ipv4 access-group v4-acl-egress egress
Router(config-if)# commit
Router(config-if)# exit

```

5. ギガビット イーサネット インターフェイスと BVI でブリッジ ドメインを設定します。

```

Router(config)# l2vpn
Router(config-l2vpn)# bridge group BG1
Router(config-l2vpn-bg)# bridge-domain B1
Router(config-l2vpn-bg-bd)# interface GigabitEthernet 0/0/0/0
Router(config-l2vpn-bg-bd-ac)# routed interface BVI1
Router(config-l2vpn-bg-bd)# commit

```



```
Router(config-l2vpn-bg-bd)# exit
Router(config-l2vpn-bg)# exit
Router(config-l2vpn)# exit
```

6. 設定が正常にコミットされていることを確認します。

```
Router(config)# show run
...
!
!
ipv4 access-list v4-acl-egress
  10 deny ipv4 any any fragments log
  20 deny tcp any any ack
  30 permit ipv4 any any
!
ipv4 access-list v4-acl-ingress
  10 permit tcp any 10.1.1.0/24 dscp cs6
  20 deny udp any any eq ssh
  30 permit ipv4 any any
!
interface GigabitEthernet0/0/0/0
  l2transport
!
!
interface BVII1
ipv4 address 209.165.200.224/27
  ipv4 access-group v4-acl-ingress ingress
  ipv4 access-group v4-acl-egress egress
!
l2vpn
  bridge group BG1
    bridge-domain B1
      interface GigabitEthernet0/0/0/0
        !
        routed interface BVII1
      !
    !
  !
end
```

7. エグゼクティブ特権モードに移行して、ACL が機能していることを確認します。

```
Router# show access-lists interface bvii1
Tue May 9 10:01:25.732 EDT
Input ACL (common): GigabitEthernet 0/0/0/0 (interface): v4-acl-ingress
Output ACL: v4-acl-egress

Router# show access-lists summary
Tue May 9 10:02:01.167 EDT
ACL Summary:
Total ACLs configured: 2
Total ACEs configured: 6

Router# show access-lists ipv4 v4-acl-egress hardware egress location 0/0/CPU0
ipv4 access-list v4-acl-egress
10 deny ipv4 any any fragments log (15214 matches)
20 deny tcp any any ack (15214 matches)
30 permit ipv4 any any (15214 matches)
```

設定した ACL、ACE の総数（ACL ごとに 3 つ）、およびハードウェア内の ACE の一致も出力に明確に表示されます。

IPv4 の入力および出力 ACL が BVI 上に正常に設定されました。

フラグメント制御を使用した ACL の設定

非フラグメント パケットとパケットの先頭フラグメントは、IP 拡張アクセス リストで処理されていましたが（このアクセス リストを適用した場合）、先頭以外のフラグメントはデフォルトで許可されていました。しかし、現在では、フラグメント制御機能付きの IP 拡張アクセス リストによって、パケットの先頭以外のフラグメントもさらにきめ細かく制御できるようになりました。この機能を使用すると、IP 拡張アクセス リストを適用するときに、パケットの先頭以外の IP フラグメントを調べるかどうかを指定できます。

先頭以外のフラグメントにはレイヤ 3 情報だけしか含まれていないので、レイヤ 3 情報のみを含んでいるアクセスリスト エントリを先頭以外のフラグメントに適用できるようになりました。フラグメントにはフィルタリングに必要な情報がすべて含まれているため、アクセスリスト エントリをパケットのフラグメントに適用できるのです。

この機能により、オプションの **fragments** キーワードが、IP アクセスリスト コマンドの **deny** と **permit** に追加されます。アクセスリスト エントリに **fragments** キーワードを指定すると、その特定のアクセスリスト エントリはパケットの先頭以外のフラグメントにのみ適用され、指定に応じてフラグメントが許可または拒否されます。

fragments キーワードの有無に応じたアクセスリスト エントリの動作の概要は、以下のとおりです。

| アクセスリストエントリの状態 | 結果 |
|--|--|
| fragments キーワードがなく、すべてのアクセスリストエントリ情報が一致する | <p>アクセス リスト エントリにレイヤ 3 情報のみが含まれている場合：</p> <ul style="list-style-type: none"> • エントリは、非フラグメント パケット、先頭フラグメント、先頭以外のフラグメントに適用されます。 <p>アクセス リスト エントリにレイヤ 3 情報とレイヤ 4 情報が含まれている場合：</p> <ul style="list-style-type: none"> • エントリは、非フラグメント パケットと先頭フラグメントに適用されます。 • エントリが一致し、かつ permit ステートメントである場合、パケットまたはフラグメントは許可されます。 • エントリが一致し、かつ deny ステートメントである場合、パケットまたはフラグメントは拒否されます。 • エントリは、次の方法で先頭以外のフラグメントにも適用されます。先頭以外のフラグメントにはレイヤ 3 情報のみが含まれているため、アクセスリスト エントリのレイヤ 3 部分のみが適用されます。アクセス リスト エントリのレイヤ 3 の部分が一致し、 <ul style="list-style-type: none"> • エントリが permit ステートメントの場合、先頭以外のフラグメントが許可されます。 • エントリが deny ステートメントの場合は、次のアクセス リスト エントリが処理されます。 <p>(注) 先頭以外のフラグメントと、非フラグメントまたは先頭フラグメントとでは、deny ステートメントの処理方法が異なります。</p> |
| fragments キーワードがあり、すべてのアクセスリストエントリ情報が一致する | <p>アクセスリスト エントリは、先頭以外のフラグメントにのみ適用されます。</p> <p>(注) レイヤ 4 情報を含むアクセスリスト エントリに fragments キーワードは設定できません。</p> |

すべてのアクセスリストエントリに **fragments** キーワードを追加しないでください。IP パケットの先頭フラグメントは非フラグメントと見なされ、それ以降のフラグメントとは独立して扱われるためです。先頭フラグメントは、**fragments** キーワードが含まれているアクセス リストの **permit** または **deny** エントリとは一致しないため、パケットは次のアクセスリスト エントリと比較されます。この比較は、**fragments** キーワードが含まれていないアクセスリスト エントリ

リによってパケットが許可または拒否されるまで続きます。したがって、deny エントリごとに、2つのアクセス リスト エントリが必要になる場合があります。ペアの最初の deny エントリは **fragments** キーワードを含んでおらず、先頭フラグメントに適用されます。ペアの2番目の deny エントリは **fragments** キーワードを含んでおり、以降のフラグメントに適用されます。同じホストに対して複数の deny アクセスリスト エントリがあり、それぞれのレイヤ 4 ポートが異なる場合は、そのホスト用として、**fragments** キーワードを含む deny アクセスリスト エントリを 1 つだけ追加する必要があります。このように、パケットのすべてのフラグメントは、アクセス リストによって同様に扱われます。

IP データグラムのパケット フラグメントは個々のパケットと見なされ、各フラグメントはアクセス リスト アカウンティングとアクセス リスト違反カウントの 1 つのパケットとして個別にカウントされます。



(注) アクセス リストおよび IP フラグメントに関するあらゆるケースを **fragments** キーワードで解決できるわけではありません。



(注) ACL 処理の範囲内で、レイヤ 3 情報は IPv4 ヘッダー内のフィールド（送信元、宛先、プロトコルなど）を参照します。レイヤ 4 情報は、TCP または UDP の送信元ポートと宛先ポート、TCP のフラグ、ICMP のタイプとコードなど、IPv4 ヘッダーの後ろに含まれるその他のデータを参照します。

フラグメント タイプでの照合を実行するための IPv4 ACL の設定

ほとんどの DoS（サービス妨害）攻撃は、フラグメント化されたパケットでネットワークをフラッドさせることで機能します。ネットワーク内のパケットの着信フラグメントをフィルタリングすることで、このような攻撃に対する保護レイヤを余分に追加できます。

フラグメント タイプを照合する IPv4 ACL を設定し、適切なアクションを実行できます。次の設定例ではさまざまなフラグメント オプションで使用できます。

```
/* Enter the global configuration mode and configure an IPv4 access list */
Router# config
Router(config)# ipv4 access-list TEST
Router(config-ipv4-acl)# 10 permit tcp any any

/* Configure an ACE to match on the dont-fragment flag (indicates a non-fragmented packet)
and forward the packet to the default (pre-configured) next hop */
Router(config-ipv4-acl)# 20 permit tcp any any fragment-type dont-fragment default

/* Configure an ACE to match on the is-fragment flag (indicates a fragmented packet)
and forward the packet to a next hop of 10.10.10.1 */
Router(config-ipv4-acl)# 30 permit udp any any fragment-type is-fragment nexthop1 ipv4
10.10.10.1

/* Configure an ACE to match on the first-fragment flag (indicates the first fragment
of a fragmented packet)
```

```
and forward the packet to a next hop of 20.20.20.1 */
Router(config-ipv4-acl)# 40 permit ospf any any fragment-type first-fragment nexthop1
ipv4 20.20.20.1

/* Configure an ACE to match on the last-fragment flag (indicates the last fragment of
a fragmented packet)
and forward the packet to a next hop of 30.30.30.1 */
Router(config-ipv4-acl)# 50 permit icmp any any fragment-type last-fragment nexthop1
ipv4 30.30.30.1
Router(config-ipv4-acl)# commit
```

使用例：最初のフラグメントと最後のフラグメントを照合する IPv4 ACL の設定

この項では、パケットの最初のフラグメントの場合はそのフラグメントを転送し、パケットの最後のフラグメントの場合はそのフラグメントを破棄するように ACL を設定する使用例について説明します。

この設定では、ACLがフラグメントオフセット値（最初のフラグメントの場合は「0」）を確認します。そのフラグメントがパケットの最初のフラグメントの場合は、パケットが転送されます。そのフラグメントがパケットの最後のフラグメントの場合は、インターフェイスでドロップされます。

```
/* Enter the global configuration mode and configure an IPv4 access list */
Router# config
Thu Jan 11 11:56:27.221 IST
Router(config)# ipv4 access-list ACLFIRSTFRAG

/* Configure an ACE to match on the first fragment.
If the fragment offset value equals 0, the fragment is forwarded to the 192.168.1.2 next
hop */
Router(config-ipv4-acl)# 10 permit tcp any any fragment-type first-fragment nexthop1
ipv4 192.168.1.2

/* Configure an ACE to match on the last fragment, and drop the fragment at the interface.
*/
Router(config-ipv4-acl)# 20 deny tcp any any fragment-type last-fragment
Router(config-ipv4-acl)# commit
Thu Jan 11 12:01:33.297 IST

/* Validate the configuration */
Router(config-ipv4-acl)# do show access-lists
Thu Jan 11 12:05:23.646 IST
ipv4 access-list ACLFIRSTFRAG
 10 permit tcp any any fragment-type first-fragment nexthop1 ipv4 192.168.1.20
 20 deny tcp any any fragment-type last-fragment
```

フラグメント タイプを照合する IPv4 ACL を正常に設定しました。

ACLでのフラグメントオフセットによる一致

フラグメント オフセット値でパケットをフィルタリングするようにアクセス コントロール リスト (ACL) のルールを作成できます。パケットが permit ステートメントまたは deny ステートメントの条件に一致するかどうかにより、パケットはインターフェイスでそれぞれ処理され

るか、またはドロップされます。フラグメント オフセット フィルタリングは、圧縮モードの ACL を使用して入力方向でのみサポートされています。

この機能の詳細については、『*IP Addresses and Services Configuration Guide for Cisco NCS 560 Series Routers*』の「*Implementing Access Lists and Prefix Lists*」の章を参照してください。詳細なコマンド リファレンスについては、『*IP Addresses and Services Command Reference for Cisco NCS 5500 Series and NCS 540 and NCS 560 Series Routers*』の「*Access List Commands*」の章を参照してください。

フラグメント オフセットによる ACL 照合の設定

ACL でフラグメント オフセット一致を設定するには、IPv4 または IPv6 アクセスリスト コンフィギュレーション モードの **permit** コマンドまたは **deny** コマンドで **fragment-offset** オプションを使用します。

設定

次に、IPv4 ヘッダーごとのフラグメント オフセットに基づいて ACL ルールを設定する例を示します。ここでは、パケットの IPv4 ヘッダー内のフラグメント オフセットが 300 ～ 400 の範囲内にある場合にのみ、パケットが許可されます。値 300 ～ 400 は 8 バイトの単位に基づいており、これは 2400 ～ 3200 バイトのフラグメント オフセットと同じです。

```
/* Configure ACL */
Router# configure
Router(config)# ipv4 access-list fragment-offset-acl
Router(config-ipv4-acl)# 10 permit ipv4 any any fragment-offset range 300 400
Router# commit
```

実行コンフィギュレーション

```
ipv4 access-list fragment-offset-acl
 10 permit ipv4 any any fragment-offset range 300 400
!
```

ACL でのフラグメント オフセットの一致の確認

```
Router#
show access-lists ipv4 fragment-offset-acl usage pfilter loc 0/0/CPU0

Wed Apr 12 19:49:54.457 UTC
Interface : Bundle-Ether70
  Input  ACL : Common-ACL : N/A  ACL : fragment-offset-acl  (comp-lvl 3)
  Output ACL : N/A

Router#
show access-lists ipv4 fragment-offset-acl hardware ing int Bundle-Ether70 loc 0/0/CPU0

Wed Apr 12 19:51:07.837 UTC
```

```
ipv4 access-list fragment-offset-acl
10 permit ipv4 any any fragment-offset range 300 400
```

関連コマンド

- `ipv4 access-list`
- `ipv6 access-list`
- `deny` (IPv4)
- `deny` (IPv6)
- `fragment-offset`
- `permit` (IPv4)
- `permit` (IPv6)

IP パケット長による ACL フィルタリングの設定

入力インターフェイスでパケット長を使用してパケットをフィルタリングするようにアクセスコントロール リストを設定できます。パケットが `permit` ステートメントまたは `deny` ステートメントのパケット長条件と一致するかどうかに応じて、パケットはインターフェイスでそれぞれ処理またはドロップされます。

ACL でパケット長フィルタリングを設定するには、IPv4 または IPv6 アクセスリスト コンフィギュレーション モードの `permit` コマンドまたは `deny` コマンドで `packet-length` オプションを使用します。

制約事項

ACL でのパケット長フィルタリング機能には次の制約事項があります。

- パケット長フィルタリングは、シンプル（非圧縮）ACL とハイブリッド（圧縮）ACL の両方で入力方向のみがサポートされています。
- IPv6 のパケット長フィルタリングは、ハイブリッド ACL でのみサポートされています。シンプル ACL ではサポートされていません。
- IPv4 のシンプル ACL でサポートされているのは、量子化された（16 で割り切れる値）パケット長フィルタリングのみです。
- パケット長のフィルタリングはデフォルトの TCAM キーではサポートされていないため、「設定」の項で説明されているように、`hw-module profile tcam format` コマンドを使用するユーザ定義の TCAM キー（UDK）が必要です。

パケット長を使用してフィルタリングするためのシンプルな IPv4 ACL の設定

シンプルな ACL を設定して IPv4 ネットワーク内のパケット長でフィルタリングするには、次のステップを実行します。

1. `hw-module` コマンドを使用して、グローバル コンフィギュレーション モードでパケット長のフィルタリングをイネーブルにします。

```
Router# config
Router(config)# hw-module profile tcam format access-list ipv4 dst-addr dst-port
proto packet-length frag-bit port-range
```

2. グローバル コンフィギュレーション モードを開始し、パケット長値でパケットをフィルタリングするシンプルな IPv4 アクセス リストを設定します。

次の特定の例では、指定したパケット長の条件に一致するパケットのみを処理する一連のステートメントを設定します。その他のパケットは、この ACL が入力インターフェイスに適用された時点でドロップされます。

```
Router# config
Router(config)# ipv4 access-list pktlen-v4
Router(config-ipv4-acl)# 10 permit tcp any any packet-length eq 1664
Router(config-ipv4-acl)# 20 permit udp any any packet-length range 1600 2000
Router(config-ipv4-acl)# 30 deny ipv4 any any
```

3. ACL をコミットし、IPv4 ACL コンフィギュレーション モードを終了します。

```
Router(config-ipv4-acl)# commit
Router(config-ipv4-acl)# end
```

4. 必要なイーサネット インターフェイスに ACL を適用します。

```
Router(config)# interface Te0/0/0/0
Router(config-if)# ipv4 access-group pktlen-v4 ingress
```

5. 設定をコミットし、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。

```
Router(config-if)# commit
Router(config-if)# end
```

6. 設定を確認します。

```
Router# show access-lists pktlen-v4

ipv4 access-list pktlen-v4
10 permit ipv4 host 10.0.0.10 any packet-length lt 1008
20 permit ipv4 host 10.0.0.9 any packet-length gt 992
```

7. ハードウェアで ACL の一致を確認します。

```
Router# show access-lists pktlen-v4 hardware ingress location 0/0/CPU0

ipv4 access-list pklen-v4
```



```
10 permit ipv4 host 10.0.0.10 any packet-length lt 1008
20 permit ipv4 host 10.0.0.9 any packet-length gt 992
```

パケット長でフィルタリングするためのシンプルな IPv4 ACL を正常に設定しました。

パケット長を使用してフィルタリングするための拡張 IPv4 ACL の設定

拡張 ACL を設定して IPv4 ネットワーク内のパケット長でフィルタリングするには、次のステップを実行します。

1. `hw-module` コマンドを使用して、グローバル コンフィギュレーション モードでパケット長のフィルタリングをイネーブルにします。

```
Router# config
Router (/config) # hw-module profile tcam format access-list ipv4 dst-addr dst-port
proto packet-length frag-bit port-range
```

2. グローバル コンフィギュレーション モードを開始し、拡張 ACL を設定するオブジェクトグループを作成します。

```
Router (config) # object-group network ipv4 netobject1
Router (config-object-group-ipv4) # 50.0.0.0/24
Router (config-object-group-ipv4) # commit
```

3. グローバル コンフィギュレーション モードから、パケット長値でパケットをフィルタリングする IPv4 アクセス リストを設定します。

次の特定の例では、指定したパケット長の条件に一致するパケットのみを処理するステートメントを設定します。その他のパケットは、この ACL が入力インターフェイスに適用された時点でドロップされます。

```
Router# configure
Router (config) # ipv4 access-list scaled_acl1
Router (config-ipv4-acl) # 10 permit ipv4 net-group netobject1 any packet-length eq
1000
```

4. ACL をコミットし、IPv4 ACL コンフィギュレーション モードを終了します。

```
Router (config-ipv4-acl) # commit
Router (config-ipv4-acl) # end
```

5. 必要なギガビット イーサネット インターフェイスに ACL を適用します。

```
Router (config) # interface Te0/0/0/3
Router (config-if) # ipv4 access-group scaled_acl1 ingress
```

6. 設定をコミットし、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。

```
Router (config-if) # commit
Router (config-if) # end
```

7. 設定を確認します。

```
Router# show access-lists scaled_acl1
```

```
ipv4 access-list scaled_acl1
10 permit ipv4 net-group netobject1 any packet-length eq 1000
```

- ハードウェアで ACL の一致を確認します。

```
Router# show access-lists scaled_acl1 hardware ingress location 0/0/CPU0
ipv4 access-list scaled_acl1
10 permit ipv4 net-group netobject1 any packet-length eq 1000 (1500 hw matches)
```

パケット長でフィルタリングするための拡張 IPv4 ACL を正常に設定しました。

パケット長を使用してフィルタリングするための拡張 IPv6 ACL の設定

拡張 ACL を設定して IPv6 ネットワーク内のパケット長でフィルタリングするには、次のステップを実行します。

- hw-module コマンドを使用して、グローバル コンフィギュレーション モードでパケット長のフィルタリングをイネーブルにします。

```
Router# config
Router(/config)# hw-module profile tcam format access-list ipv4 dst-addr dst-port
proto packet-length frag-bit port-range
```

- グローバル コンフィギュレーション モードを開始し、拡張 ACL を設定するオブジェクトグループを作成します。

```
Router(config)# object-group network ipv6 netobject2
Router(config-object-group-ipv6)# 2001::0/128
Router(config-object-group-ipv6)# commit
```

- グローバル コンフィギュレーション モードから、パケット長値でパケットをフィルタリングする拡張 IPv6 アクセス リストを設定します。

次の特定の例では、指定したパケット長の条件に一致するパケットのみを処理するステートメントを設定します。その他のパケットは、この ACL が入力インターフェイスに適用された時点でドロップされます。

```
Router(config)# ipv6 access-list scaled_acl2
Router(config-ipv6-acl)# 10 permit ipv6 net-group netobject2 any packet-length eq 1000
Router(config-ipv6-acl)# commit
```

- ACL をコミットし、IPv6 ACL コンフィギュレーション モードを終了します。

```
Router(config-ipv6-acl)# commit
Router(config-ipv6-acl)# end
```

- 必要なギガビット イーサネット インターフェイスに ACL を適用します。

```
Router# config
Router(config)# interface Te/0/0/0/3
Router(config-if)# ipv6 access-group scaled_acl2 ingress
```

- 設定をコミットし、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。

```
Router(config-if)# commit
Router(config-if)# end
```

7. 設定を確認します。

```
Router# show access-lists ipv6 scaled_acl2
ipv6 access-list scaled_acl2
10 permit ipv6 net-group netobject2 any packet-length eq 1000
```

8. ハードウェアで ACL の一致を確認します。

```
Router# show access-lists ipv6 scaled_acl2 hardware ingress location 0/0/CPU0
ipv6 access-list scaled_acl2
10 permit ipv6 net-group netobject2 any packet-length eq 1000 (2000 hw matches)
```

パケット長でフィルタリングするための拡張 IPv6 ACL を正常に設定しました。

オブジェクトグループ ACL の概要

オブジェクトグループ ACL を使用すると、ユーザ、デバイス、またはプロトコルをグループに分類できるため、グループレベルのアクセスコントロールポリシーを設定できます。個別の IP アドレス、プロトコル、およびポート番号を複数の ACE に指定する代わりに、単一の ACL にオブジェクトグループを指定できます。

この機能は、現在、数百もの ACL が含まれている大規模なネットワークには非常に有益です。オブジェクトグループ ACL 機能を使用することで、ACL あたりの ACE の数が大幅に削減します。また、オブジェクトグループ ACL は判読性が高く、従来の ACL よりも簡単に管理できます。従来の ACL の代わりにオブジェクトグループ ACL を使用することで、TCAM に必要なストレージが最適化されます。

オブジェクトグループ ACL のタイプ

Cisco IOS XR では 2 つのタイプの オブジェクトグループ ACL を作成できます。

- **ネットワーク オブジェクトグループ ACL** : ホスト IP アドレスとネットワーク IP アドレスから構成されます。
- **ポート オブジェクトグループ ACL** : ポートとサポートしているレイヤ 3/レイヤ 4 プロトコルのグループから構成されます。

ACL の圧縮

オブジェクトグループ ACL は圧縮を使用して多数の ACE に対応します。圧縮は、ACE の次の 3 つのフィールドを圧縮することで実行されます。

- 送信元 IP プレフィックス
- 送信先 IP プレフィックス
- 送信元ポート番号

入力インターフェイス上の ACL のアクセスグループ設定には、次の 2 つの圧縮レベルしかありません。

- **圧縮レベル 0** : 圧縮は ACE フィールドでは実行されません。

このモードでは、オブジェクトグループ ACL は従来の ACL のように動作します。内部 TCAM リソースを利用するため、ACL の処理に必要なシステム リソースと時間に膨大な影響を与えます。

- **圧縮レベル 3** : ACE の 3 つフィールド（送信元 IP、送信先 IP、および送信元ポート）すべてが圧縮されます。

このモードでは、プレフィックスのルックアップには外部 TCAM、ACE のルックアップには内部 TCAM を使用します。このモードは、16 ビット ベースの packets 長フィルタリングとフラグメント オフセット フィルタリングをサポートしています。



(注) Cisco NCS 540 シリーズ ルータには外部 TCAM がいないため、圧縮レベル 3 はサポートされません。

オブジェクトグループ ACL の設定

はじめる前に

オブジェクトグループ ACL に適用される次の情報を把握しておく必要があります。

- 従来の ACL とオブジェクトグループ ACL の両方を含む ACL を設定できます。
- オブジェクト グループや、そのオブジェクト グループを参照する ACE を定義し直すことなく、オブジェクト グループ内のオブジェクトをダイナミックに変更できます。
- オブジェクトグループ ACL は、送信元グループまたは送信先グループ、あるいは送信元と送信先のグループの両方を使用して複数回設定できます。

制約事項

オブジェクトグループ ACL の設定には、次の制約事項があります。

- オブジェクトグループ ACL は、インターフェイスにのみ設定できます。SSH、SNMP、NTP などのアプリケーションで使用または参照することはできません。
- オブジェクトグループを削除するには、最初にすべての ACL から削除する必要があります。
- QoS ポリシーとともにオブジェクトグループ ACL を設定することはできません。
- オブジェクトグループ ACL は、ポリシー ベースの設定ではサポートされません。
- リリース 6.2.1 以降、ネストされたオブジェクトグループはサポートされていません。

ネットワークオブジェクトグループACLの設定

ネットワークオブジェクトグループには単一または複数のネットワークオブジェクトを含めることができます。

設定

次の一連の設定ステートメントを使用して、IPv4アドレスのネットワークオブジェクトグループACLを設定します。

```
/* From the global configuration mode, create a network object group. */
Router(config)# object-group network ipv4 netobj1
Router(config-object-group-ipv4)# description my-network-object
Router(config-object-group-ipv4)# host 10.1.1.1
Router(config-object-group-ipv4)# 10.2.1.0 255.255.255.0
Router(config-object-group-ipv4)# range 10.3.1.10 10.3.1.50

/* Create an access list referencing the object group. */
Router(config)# ipv4 access-list network-object-acl permit ipv4 net-group netobj1 any

/* Apply the access list containing the object group to the desired interface and commit
your configuration. */
Router(config)# interface TenGigE0/0/0/10/3
Router(config-if)# ipv4 address 1.1.1.1/24
Router(config-if)# no shut
Router(config-if)# ipv4 access-group network-object-acl ingress compress level 0
Router(config-if)# commit
Tue Mar 28 10:23:34.106 IST

RP/0/0/CPU0:Mar 28 10:37:48.570 : ifmgr[397]: %PKT_INFRA-LINK-3-UPDOWN : Interface
TenGigE0/0/0/10/3 , changed state to Down
RP/0/0/CPU0:Mar 28 10:37:48.608 : ifmgr[397]: %PKT_INFRA-LINK-3-UPDOWN : Interface
TenGigE0/0/0/10/3 , changed state to Up

Router(config-if)# exit
```

次の一連の設定ステートメントを使用して、IPv6アドレスのネットワークオブジェクトグループACLを設定します。

```
/* From the global configuration mode, create a network object group. */
Router(config)# object-group network ipv6 netobj1
Router(config-object-group-ipv6)# description my-network-object
Router(config-object-group-ipv6)# host 2001:DB8:1::1
Router(config-object-group-ipv6)# 2001:DB8::1 2001:DB8:0:ABCD::1
Router(config-object-group-ipv6)# range 2001:DB8::2 2001:DB8::5

/* Create an access list referencing the object group. */
Router(config)# ipv6 access-list network-object-acl permit ipv6 net-group netobj1 any

/* Apply the access list containing the object group to the desired interface and commit
your configuration. */
Router(config)# interface TenGigE0/0/0/10/3
Router(config-if)# ipv6 address 2001:DB8::1/32
Router(config-if)# no shut
Router(config-if)# ipv6 access-group network-object-acl ingress compress level 0
Router(config-if)# commit
Tue Mar 28 10:23:34.106 IST
```

ポートオブジェクトグループ ACL の設定

```
RP/0/0/CPU0:Mar 28 10:37:48.570 : ifmgr[397]: %PKT_INFRA-LINK-3-UPDOWN : Interface
TenGigE0/0/0/10/3 , changed state to Down
RP/0/0/CPU0:Mar 28 10:37:48.608 : ifmgr[397]: %PKT_INFRA-LINK-3-UPDOWN : Interface
TenGigE0/0/0/10/3 , changed state to Up

Router(config-if)# exit
```

実行コンフィギュレーション

設定を確認します。

```
Router(config)# show run
Tue Mar 28 10:37:55.737 IST

Building configuration...
!! IOS XR Configuration 0.0.0
...

!
object-group network ipv4 netobj1
 10.2.1.0/24
 host 10.1.1.1
 range 10.3.1.10 10.3.1.50
 description my-network-object
!
!
ipv4 access-list network-object-acl
 10 permit ipv4 net-group netobj1 any
!
```

ネットワーク オブジェクトグループ ACL は正常に設定されました。

ポートオブジェクトグループ ACL の設定

ポートオブジェクトグループには単一または複数のポートオブジェクトを含めることができます。

設定

次の一連の設定ステートメントを使用して、ポートオブジェクトグループ ACL を設定します。

```
/* From the global configuration mode, create a port object group, and commit your
configuration. */
RP/0/RP0/cpu 0: router(config)# object-group port portobj1
RP/0/RP0/cpu 0: router(config-object-group-ipv4)# description my-port-object
RP/0/RP0/cpu 0: router(config-object-group-ipv4)# eq bgp
RP/0/RP0/cpu 0: router(config-object-group-ipv4)# range 100 200
RP/0/RP0/cpu 0: router(config-object-group-ipv4)# commit
RP/0/RP0/cpu 0: router(config-object-group-ipv4)# exit

/* Create an access list referencing the object group. */
RP/0/RP0/cpu 0: router(config)# ipv4 access-list port-object-acl permit ipv4 net-group
portobj1

/* Apply the access list containing the object group to the desired interface and commit
your configuration. */
RP/0/RP0/cpu 0: router(config)# interface Te0/0/0/3
```

```
RP/0/RP0/cpu 0: router(config-if)# ipv4 address 2.2.2.2/24

RP/0/RP0/cpu 0: router(config-if)# no shut
RP/0/RP0/cpu 0: router(config-if)# commit
Tue Mar 28 10:23:34.106 IST

RP/0/0/CPU0:Mar 28 10:37:48.570 : ifmgr[397]: %PKT_INFRA-LINK-3-UPDOWN : Interface
TenGigE0/0/0/10/3 , changed state to Down
RP/0/0/CPU0:Mar 28 10:37:48.608 : ifmgr[397]: %PKT_INFRA-LINK-3-UPDOWN : Interface
TenGigE0/0/0/10/3 , changed state to Up

RP/0/RP0/cpu 0: router(config-if)# exit
```

実行コンフィギュレーション

設定を確認します。

```
RP/0/RP0/cpu 0: router(config)# show run
Tue Mar 28 10:37:55.737 IST

Building configuration...
!! IOS XR Configuration 0.0.0
...
object-group port portobj1
  eq bgp
  range 100 200
!

ipv4 access-list port-object-acl
  10 permit tcp net-group portobj1
!
interface Te/0/0/0/3

!
end
!
```

ポート オブジェクトグループ ACL が正常に設定されました。

IPv4 ACL での TTL の照合および書き換えの設定

IPv4 ヘッダーに指定されている TTL 値で照合するように ACL を設定できます。TTL 一致条件を単一の値か、または複数の値に基づくように指定できます。また、**set ttl** コマンドを使用して、IPv4 ヘッダー内の TTL 値を書き換えることもできます。

IPv4 ACL での TTL の照合および書き換えの使用に関する制限事項

IPv4 ACL での TTL の照合および書き換えの使用には、次の制限事項があります。

- TTL の照合は、入力 ACL でのみサポートされています。
- ユーザ定義の TCAM キー (UDK) に **enable set ttl** オプションを設定すると、入力 ACL で ACL ロギングがサポートされません。

- TTL の書き換えを IP-in-IP ヘッダーの外側の IPv4 ヘッダーに適用する場合は、GRE カプセル化解除により外側の IPv4 ヘッダーのカプセル化が解除されると、内部 IPv4 ヘッダーにも TTL の書き換えが適用されます。
- TTL の照合はデフォルトの TCAM キーではサポートされていないため、「設定」の項で説明されているように、**hw-module profile tcam format** コマンドを使用するユーザ定義の TCAM キー（UDK）が必要です。

設定

IPv4 ACL に TTL の照合および書き換えを設定するには、次のステップを実行します。

```
/* Enable TTL matching and rewriting in the global configuration mode by using the
hw-module command */
Router(config)# hw-module profile tcam format access-list ipv4 dst-addr dst-port proto
port-range enable-set-ttl ttl-match

/* Configure an IPv4 ACL with the TTL parameters */
Router(config)# ipv4 access-list acl-v4
Router(config-ipv4-acl)# 10 deny tcp any any ttl eq 100
Router(config-ipv4-acl)# 20 permit tcp any any ttl range 1 50 set ttl 200
Router(config-ipv4-acl)# 30 permit tcp any any ttl neq 100 set ttl 255
Router(config-ipv4-acl)# commit
Thu Nov  2 12:22:58.948 IST

/* Attach the IPv4 ACL to the GigE interface */
Router(config)# interface Te0/0/0/0
Router(config-if)# ipv4 address 15.1.1.1 255.255.255.0
Router(config-if)# ipv4 access-group acl-v4 ingress
Router(config-if)# commit
```

実行コンフィギュレーション

show run コマンドを使用して設定を検証します。

```
Router(config)# show run
Thu Nov  2 14:01:53.376 IST
Building configuration...
!! IOS XR Configuration 0.0.0
!! Last configuration change at Thu Nov  2 12:22:59 2017 by annseque
!
hw-module profile tcam format access-list ipv4 dst-addr dst-port proto port-range
enable-set-ttl ttl-match
!
ipv4 access-list acl-v4
  10 deny tcp any any ttl eq 100
  20 permit tcp any any ttl range 1 50 set ttl 200
  30 permit tcp any any ttl neq 100 set ttl 255
!
interface Te0/0/0/0
  ipv4 address 15.1.1.1 255.255.255.0
  ipv4 access-group acl-v4 ingress
!
```

IPv4 ACL に TTL の照合および書き換えが正常に設定されています。

IPv6 ACL での TTL の照合および書き換えの設定

IPv6 ヘッダーに指定されている TTL 値で照合するように ACL を設定できます。TTL 一致条件を単一の値か、または複数の値に基づくように指定できます。また、**set ttl** コマンドを使用して、IPv6 ヘッダー内の TTL 値を書き換えることもできます。



(注) **hw-module profile** コマンドを入力した後は、コマンドをアクティブにするためにラインカードを再起動する必要があります。

IPv6 ACL での TTL の照合および書き換えの使用に関する制限

IPv6 ACL での TTL の照合および書き換えの使用には、次の制限事項があります。

- TTL の照合は、入力 ACL でのみサポートされています。
- ユーザ定義の TCAM キー（UDK）に **enable set ttl** オプションを設定すると、入力 ACL で ACL ロギングがサポートされません。
- TTL の書き換えを IP-in-IP ヘッダーの外側の IPv6 ヘッダーに適用する場合は、GRE カプセル化解除により外側の IPv6 ヘッダーのカプセル化が解除されると、内部 IPv6 ヘッダーにも TTL の書き換えが適用されます。
- TTL の照合はデフォルトの TCAM キーではサポートされていないため、「設定」の項で説明されているように、**hw-module profile tcam format** コマンドを使用するユーザ定義の TCAM キー（UDK）が必要です。

設定

IPv6 ACL に TTL の照合および書き換えを設定するには、次のステップを実行します。

```
/* Enable TTL matching and rewriting in the global configuration mode by using the
hw-module command */
Router(config)# hw-module profile tcam format access-list ipv6 dst-addr dst-port src-port
next-hdr enable-set-ttl ttl-match

/* Configure an IPv6 ACL with the TTL parameters */
Router(config)# ipv6 access-list acl-v6
Router(config-ipv6-acl)# 10 deny tcp any any ttl eq 50
Router(config-ipv6-acl)# 20 permit tcp any any ttl lt 50 set ttl 255
Router(config-ipv6-acl)# 30 permit tcp any any ttl gt 50 set ttl 200
Router(config-ipv6-acl)# commit
Thu Nov 2 12:22:58.948 IST

/* Attach the IPv6 ACL to the GigE interface */
Router(config)# interface Te0/0/0/0
Router(config-if)# ipv6 address 2001:2:1::1/64
Router(config-if)# ipv6 access-group acl-v6 ingress
Router(config-if)# commit
```

実行コンフィギュレーション

show run コマンドを使用して設定を検証します。

```
Router(config)# show run
Thu Nov  2 14:01:53.376 IST
Building configuration...
!! IOS XR Configuration 0.0.0
!! Last configuration change at Thu Nov  2 12:22:59 2017 by annseque
!hw-module profile tcam format access-list ipv6 dst-addr dst-port src-port next-hdr
enable-set-ttl ttl-match
!
ipv6 access-list acl-v6
  10 deny tcp any any ttl eq 50
  20 permit tcp any any ttl lt 50 set ttl 255
  30 permit tcp any any ttl gt 50 set ttl 200
!
interface Te0/0/0/0
  ipv6 address 2001:2::1/64
  ipv6 access-group acl-v6 ingress
!
```

IPv6 ACL に TTL の照合および書き換えが正常に設定されています。

IP アクセス リスト ロギング メッセージの概要

Cisco IOS XR ソフトウェアでは、標準 IP アクセス リストで許可または拒否されたパケットに関するログメッセージが表示されます。つまり、パケットがアクセス リストに一致すると、そのパケットに関するログメッセージ情報がコンソールに送信されます。ログをコンソールに送信するメッセージのレベルは、グローバルコンフィギュレーションモードの **logging console** コマンドで制御します。

最初にパケットがアクセス リストをトリガーすると、すぐにログメッセージが生成されます。その後、5分間隔でパケットが収集されて表示または記録されます。ログメッセージにはアクセス リスト番号、パケットの許可または拒否に関する状況、パケットの送信元 IP アドレス、および直前の 5 分間に許可または拒否された送信元からのパケット数が示されます。

ただし、**{ ipv4 | ipv6 } access-list log-update threshold** コマンドを使用すれば、アクセス リストに一致する（許可または拒否される）場合にシステムでログメッセージを生成するパケットの数を設定できます。この手順は、5分間隔よりも短い頻度でログメッセージを受信する場合に実行することを推奨します。



Caution

number-of-matches 引数を 1 に設定すると、ログメッセージはキャッシュされずにただちに送信されます。この場合、アクセス リストに一致するすべてのパケットについてログメッセージが生成されます。大量のログメッセージでシステムが過負荷になる可能性があるため、1 に設定することは推奨されません。

{ ipv4 | ipv6 } access-list log-update threshold コマンドを使用する場合も 5 分タイマーは有効なままなので、各キャッシュのメッセージ数に関係なく、5 分が経過すると各キャッシュは空に

なります。ログメッセージを送信するタイミングに関係なく、しきい値が指定されていない場合と同様に、ログメッセージのキャッシュは消去され、カウンタは0にリセットされます。

**Note**

ログメッセージが多すぎて処理できない場合や、1秒以内に2つ以上のログメッセージを処理した場合には、ログメッセージパケットの一部がドロップされることがあります。この動作により、ログを生成するパケットの数が増えても、ルータがCPUサイクルを過度に使用することはありません。したがって、ロギング機能は課金ツールや、アクセスリストとの一致数を正確に把握するための情報源として使用しないでください。

プレフィックス リストの概要

プレフィックス リストはルート マップおよびルート フィルタリング操作に使用されるほか、ボーダー ゲートウェイ プロトコル (BGP) の多くのルート フィルタリング コマンドではアクセス リストの代わりに使用できます。プレフィックスはIP アドレスの一部であり、左端のオクテットの左端のビットから始まります。アドレスの何ビットがプレフィックスに属するかを正確に指定すると、プレフィックスを使用してアドレスを集約し、そのアドレスに対して再配布 (フィルタ ルーティング アップデート) などの機能を実行できるようになります。

プレフィックス リストを使用した BGP フィルタリング

プレフィックス リストは、BGP ルート フィルタリング コマンドの多くでアクセス リストの代わりに使用できます。これは BGP プロトコルのグローバル コンフィギュレーションで設定されます。プレフィックス リストを使用した場合の利点は次のとおりです。

- サイズの大きなリストをロードしてルート ルックアップを実施する場合のパフォーマンスが大幅に向上します。
- 差分更新がサポートされます。
- CLI の使い勝手が向上します。アクセス リストを使用して BGP 更新をフィルタリングするための CLI は、パケット フィルタリング形式を使用しているため、わかりやすく使い勝手もよくありません。
- 柔軟性が高まります。

コマンドでプレフィックス リストを使用するには、あらかじめプレフィックス リストをセットアップしておく必要があります。プレフィックス リストのエントリには、シーケンス番号を割り当ててください。

プレフィックス リストでトラフィックをフィルタリングする仕組み

プレフィックス リストによるフィルタリングでは、ルートのプレフィックスが、プレフィックス リストに記載されているプレフィックスと照合されます。一致すると、一致したルートが使用されます。具体的には、プレフィックスを許可するか、拒否するかは次のルールに基づきます。

- 空のプレフィックスリストはすべてのプレフィックスを許可します。
- 特定のプレフィックスがプレフィックスリストのどのエントリとも一致しなかった場合、暗黙の **deny** が適用されます。
- プレフィックスリストの複数のエントリが特定のプレフィックスと一致したときは、最も長く、最も具体的な一致が選択されます。

シーケンス番号は自動的に生成されます。ただし、この自動生成をディセーブルにしている場合を除きます。シーケンス番号の自動生成をディセーブルにしている場合は、IPv4またはIPv6のプレフィックスリスト コンフィギュレーション コマンドで、**permit** と **deny** コマンドの *sequence-number* 引数を使用して、各エントリのシーケンス番号を指定する必要があります。プレフィックスリストのエントリを削除するには、**permit** または **deny** コマンドの **no** 形式を使用して、*sequence-number* 引数を指定します。

show コマンドの出力には、シーケンス番号が含まれます。

プレフィックス リストの設定

設定例

「Deny all routes with a prefix of 10/8」というコメントが付いたプレフィックスリスト「pfx_2」を作成します。このプレフィックスリストは、128.0.0.0/8 の /24 に一致するプレフィックスをすべて拒否します。

```
Router#configure
Router(config)#ipv4 prefix-list pfx_2
/* Use the ipv6 access-list command to create an IPv6 access list */

Router(config-ipv4_pfx)#10 remark Deny all routes with a prefix of 10/8
Router(config-ipv4_pfx)#20 deny 128.0.0.0/8 eq 24
/* Repeat the above step as necessary. Use the no sequence-number command to delete an entry. */

Router(config-ipv4_pfx)#commit
```

実行コンフィギュレーション

```
Router#show running-config ipv4 prefix-list pfx_2
ipv4 prefix-list pfx_2
  10 remark Deny all routes with a prefix of 10/8
  20 deny 128.0.0.0/8 eq 24
!
```

確認

許可とコメントの設定が設定されているコンフィギュレーションに合致していることを確認します。

```
Router# show prefix-list pfx_2
ipv4 prefix-list pfx_2
  10 remark Deny all routes with a prefix of 10/8
```

```
20 deny 128.0.0.0/8 eq 24
RP/0/RP0/CPU0:ios#
```

関連コマンド

プレフィックスリストエントリの順序付けとプレフィックスリストの変更

設定例

名前付きプレフィックスリストのエントリにシーケンス番号を割り当て、プレフィックスリストに対してエントリを追加または削除する方法を示します。プレフィックスリストを変更することを前提に説明します。プレフィックスリストの並べ替えは任意です。

```
Router#config
Router(config)#ipv4 prefix-list cl_1
/* Use the ipv6 prefix-list command to create an IPv6 prefix-list */

Router(config)#10 permit 172.16.0.0 0.0.255.255
/* Repeat the above step as necessary adding statements by sequence number where you
planned; use the no sequence-number command to delete an entry */

Router(config)#commit
end
Router#resequence prefix-list ipv4 cl_1 20 15
/* Use the resequence prefix-list ipv6 to resequence IPv6 prefix list */
```

実行コンフィギュレーション

```
/*Before resequencing*/
Router#show running-config ipv4 prefix-list cl_1
ipv4 prefix-list cl_1
 10 permit 172.16.0.0/16
!
/* After resequencing using the resequence prefix-list ipv4 cl_1 20 15 command: */
Router#show running-config ipv4 prefix-list cl_1
ipv4 prefix-list cl_1
 35 permit 172.16.0.0/16
!
```

確認

プレフィックスリストが並べ替えられたことを確認します。

```
Router#show prefix-list cl_1
ipv4 prefix-list cl_1
 35 permit 172.16.0.0/16
```

関連コマンド



CHAPTER 8

HSRP の実装

ホットスタンバイ ルータ プロトコル (HSRP) は、ファーストホップ IP ルータで透過的にフェールオーバーが発生する事態を考慮するように設計された IP ルーティング冗長プロトコルです。ネットワーク上のホストからの IP トラフィックをルーティングするときに単一ルータの可用性に依存しないため、HSRP では、高度なネットワーク可用性が提供されます。ルータのグループで HSRP を使用して、アクティブ ルータとスタンバイ ルータを選択します (アクティブ ルータとは、パケット転送用に選択されているルータのことです。スタンバイ ルータとは、アクティブ ルータで障害が発生したときや、プリセット条件が満たされたときに、ルーティング処理を引き継ぐルータのことです)。

HSRP の実装の機能履歴

- [HSRP の実装の前提条件](#), on page 149
- [HSRP の実装の制約事項](#), on page 149
- [HSRP の実装に関する情報](#), on page 150
- [HSRP の実装方法](#), on page 154
- [HSRP および IP スタティックの拡張オブジェクト トラッキング](#) (170 ページ)
- [HSRP のホット リスタート](#), on page 171
- [ソフトウェアでの HSRP の実装の設定例](#), on page 171

HSRP の実装の前提条件

適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。このコマンドリファレンスには、各コマンドに必要なタスク ID が含まれます。ユーザ グループの割り当てが原因でコマンドを使用できないと考えられる場合、AAA 管理者に連絡してください。

HSRP の実装の制約事項

HSRP は、イーサネットインターフェイス、イーサネットサブインターフェイス、イーサネットリンクバンドル、およびブリッジ仮想インターフェイス (BVI) でサポートされています。

HSRPの実装に関する情報

Cisco IOS XR ソフトウェアのソフトウェアに HSRP を実装するには、次の概念を理解する必要があります。

HSRP の概要

HSRP は、ルータ ディスカバリ プロトコル (Internet Control Message Protocol [ICMP] Router Discovery Protocol [IRDP] など) をサポートしないホスト、および選択したルータがリロードしたときやルータの電源が失われたときに新しいルータに切り替えることができないホストに便利です。また、既存の TCP セッションはフェールオーバーが発生しても存続するため、このプロトコルでは IP トラフィックをルーティングするためにネクスト ホップを動的に選択するホストの回復をさらに透過的に実行できます。

HSRP をネットワーク セグメントに設定すると、HSRP が動作するルータのグループで仮想 MAC アドレスと IP アドレスを共有できるようになります。この HSRP ルータ グループのアドレスが仮想 IP アドレスと呼ばれます。このようなデバイスの 1 つが、アクティブルータとしてプロトコルによって選択されます。アクティブルータは、グループの MAC アドレス宛のパケットを受信して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。

HSRP が指定アクティブルータの障害を検出すると、選択されているスタンバイルータが HSRP グループの MAC アドレスと 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 を実行しているルータは、ユーザデータグラム プロトコル (UDP) ベースのマルチキャスト hello パケットを送受信して、ルータの障害を検出したり、アクティブルータとスタンバイルータを指定したりします。

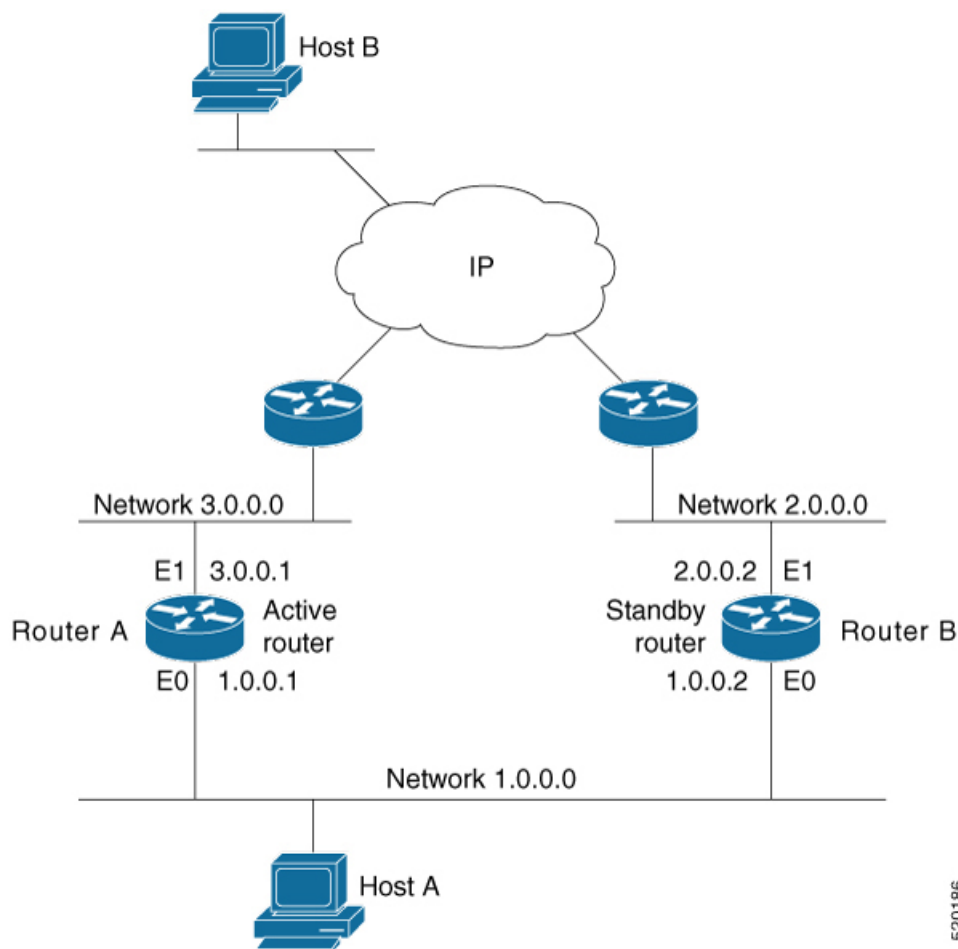
HSRP グループ

HSRP グループは、HSRP を実行し、かつ互いにホットスタンバイ サービスを提供するように設定されている複数のルータで構成されています。HSRP は、プライオリティスキームを使用して、HSRP によって設定されたどのルータをデフォルトのアクティブルータにするかを決定します。ルータをアクティブルータとして設定するには、他のすべての HSRP 設定済みルータのプライオリティよりも高いプライオリティをそのルータに割り当てます。デフォルトのプライオリティは 100 です。したがって、100 よりも高いプライオリティを持つルータを 1 つだけ設定した場合、そのルータがデフォルトのアクティブルータになります。

HSRP は、HSRP グループ間でプライオリティをアドバタイズするマルチキャストメッセージを交換することによって機能します。アクティブルータが設定された時間内に hello メッセージを送信できなかった場合は、最高のプライオリティのスタンバイルータがアクティブルータになります。このようにパケット転送機能が別のルータに移行しても、ネットワークのいずれのホストにもまったく影響はありません。

次の図に、単一の HSRP グループのメンバとして設定されたルータを示します。

Figure 13: HSRP グループとして設定されたルータ

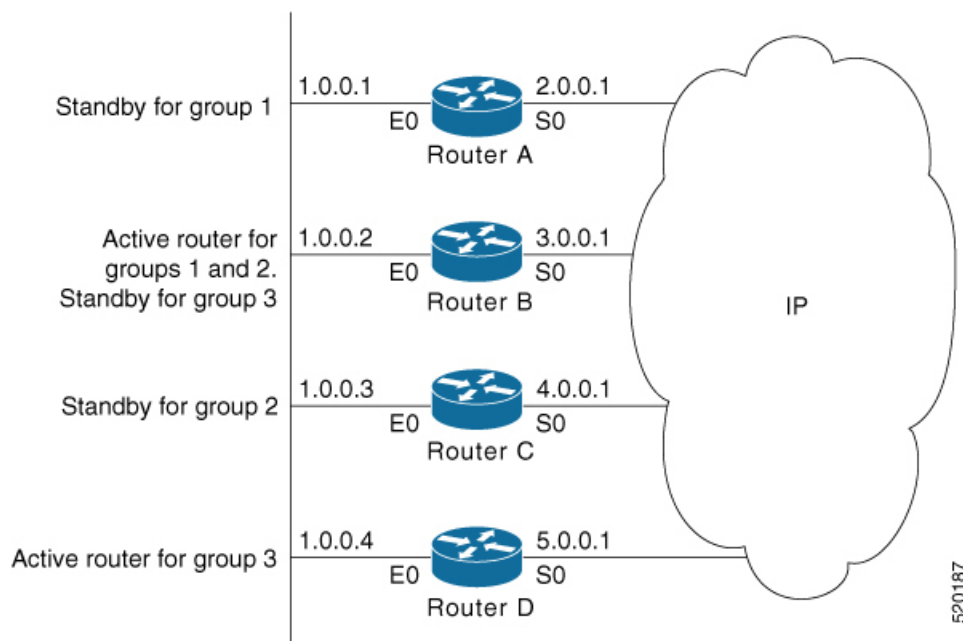


520186

ネットワーク上のホストはすべて、仮想ルータの IP アドレス（この場合 1.0.0.3）をデフォルトゲートウェイとして使用するよう設定されています。

1つのルータインターフェイスを複数の HSRP グループに属するように設定することもできます。次の図に、複数の HSRP グループのメンバとして設定されたルータを示します。

Figure 14: 複数の HSRP グループのメンバとして設定されたルータ



上の図では、ルータ A のイーサネット インターフェイス 0 は、グループ 1 に属します。ルータ B のイーサネット インターフェイス 0 は、グループ 1、2、および 3 に属します。ルータ C のイーサネット インターフェイス 0 は、グループ 2、ルータ D のイーサネット インターフェイス 0 はグループ 3 に属します。グループを作成するときは、部門の編成に従うことをお勧めします。この場合、グループ 1 はエンジニアリング部門、グループ 2 は製造部門、グループ 3 は財務部門をサポートします。

ルータ B は、グループ 1 と 2 のアクティブ ルータ、およびグループ 3 のスタンバイ ルータとして設定されています。ルータ D は、グループ 3 のアクティブ ルータとして設定されています。何らかの理由でルータ D で障害が発生すると、ルータ B がルータ D のパケット転送機能を引き継ぐため、財務部門のユーザは引き続き他のサブネット上のデータにアクセスできます。



Note サブインターフェイスごとに異なる仮想 MAC アドレス (VMAC) が必要になります。VMAC は、グループ ID に基づいて決定されます。このため、VMAC を明示的に設定する場合を除いて、設定するサブインターフェイスごとに固有のグループ ID が必要です。



Note 仮想ルータが接続されているスイッチ ポートでは、スパニング ツリー プロトコル (STP) を無効にすることをお勧めします。スイッチがこれらのプロトコルをサポートしている場合に、RSTP または rapid-PVST を有効にします。

HSRP と ARP

HSRP グループのルータは、アクティブになると、仮想 IP アドレスと仮想 MAC アドレスが含まれている ARP 応答を数多く送信します。このような ARP 応答は、スイッチおよびラーニングブリッジが自身のポートと MAC のマッピングを更新するのに役立ちます。このような ARP 応答により、（事前に割り当てられた MAC アドレスまたは機能アドレスではなく）インターフェイスのバーンドインアドレスを仮想 MAC アドレスとして使用するようルータを設定できます。これは、仮想 IP アドレスの ARP エントリを更新するための手段となります。インターフェイスがアップ状態になったときにそのインターフェイス IP アドレスを特定するために送信される Gratuitous ARP 応答と異なり、HSRP ルータ ARP 応答パケットはパケット ヘッダーで仮想 MAC アドレスを伝送します。IP アドレスおよびメディア アドレスの ARP データフィールドには、仮想 IP アドレスおよび仮想 MAC アドレスが含まれています。

プリエンプション

HSRP プリエンプション機能を使用すると、プライオリティの最も高いルータがただちにアクティブルータになることができます。プライオリティはまず設定したプライオリティ値に従って決定され、次に IP アドレスに従って決定されます。どちらの場合も、値の大きい方がプライオリティが高くなります。

プライオリティの高いルータが、プライオリティの低いルータをプリエンプション処理すると、**coup** メッセージを送信します。プライオリティの低いアクティブルータが、プライオリティの高いアクティブルータから **coup** メッセージまたは **hello** メッセージを受信すると、スピーク状態に変わり、**resign** メッセージを送信します。

ICMP リダイレクト メッセージ

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 は多くの診断機能を備えており、ホストへのエラーパケットの送信およびリダイレクトが可能です。HSRP を実行しているときは、HSRP グループに属するルータのインターフェイス（または実際の）MAC アドレスをホストが検出しないようにすることが重要です。ICMP によってホストがルータの実際の MAC アドレスへリダイレクトされて、そのルータに障害が発生した場合、ホストからのパケットは消失します。

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。この機能は、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ことのある HSRP で発信 ICMP リダイレクト メッセージをフィルタリングすることによって効果を発揮します。

ICMP リダイレクトをサポートするために、HSRP 経由で **redirect** メッセージがフィルタリングされます。これにより、ネクストホップ IP アドレスが HSRP 仮想アドレスに変更されます。HSRP リダイレクトが有効になっていると、HSRP が動作する ICMP インターフェイスはこのフィルタリングを行います。HSRP は、アドバタイズメントを送信し、実 IP アドレスと仮想 IP アドレスのマッピングを維持してリダイレクトのフィルタリングを実行することにより、すべての HSRP ルータの状況を把握します。

HSRP の実装方法

ここでは、次のタスクの手順を示します。

HSRP のイネーブル化

hsrp ipv4 コマンドは、設定済みの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 アドレスが指定されていない場合は、仮想アドレスがアクティブ ルータから学習されます。HSRP が指定ルータを選択できるようにするには、ホットスタンバイ グループ内の少なくとも1つのルータに指定アドレスを指定しておくか、またはルータが指定アドレスを学習する必要があります。アクティブルータ上の指定アドレスを設定すると、常に現在使用されている指定アドレスが上書きされます。

設定手順

1. 特定のインターフェイスで HSRP インターフェイス コンフィギュレーション モードをイネーブルにします。
2. 特定のインターフェイスで HSRP アドレス ファミリ コンフィギュレーション モードをイネーブルにします。
3. HSRP グループサブモードをイネーブルにします。



Note

バージョンキーワードは、IPv4 アドレスファミリが選択されている場合にのみ使用できます。デフォルトでは、IPv6 アドレスファミリのバージョンは 2 に設定されています。

4. 設定済みのインターフェイスで HSRP をアクティブにします。



Note

- 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 アドレスが指定されていない場合は、仮想アドレスがアクティブ ルータから学習されます。
- IPv6 の HSRP を設定する場合は、リンクローカル IPv6 アドレスを設定するか、**autoconfig** キーワードを使用してリンクローカル IPv6 アドレスをイネーブルにする必要があります。リンクローカル IPv6 アドレスを設定しない場合、**commit** キーワードを使用して変更をコミットしても、ルータは設定を受け入れません。

設定

```
/* Enable HSRP interface configuration mode on a specific interface. */
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface <type> <interface-path-id>
```

```
/* Enable HSRP address-family configuration mode on a specific interface. */
Router(config-hsrp-if) # address-family ipv4

/* Enable HSRP group submode. */
Router(config-hsrp-ipv4) # hsrp <group-number> version <version-no>

/* Activate HSRP on the configured interface. */
Router(config-hsrp-gp) # address {learn|address[secondary]}
Router(config-hsrp-gp) # commit
```

実行コンフィギュレーション

```
Router# show running-configuration
router hsrp
interface GigabitEthernet0/2/0/1
  address-family ipv4
    hsrp 1 version 1
    address learn
!
```

IPv6 の HSRP のイネーブル化

IPv6 の HSRP をイネーブルにするには、次の手順を使用します。

1. 特定のインターフェイスで HSRP インターフェイス コンフィギュレーション モードをイネーブルにします。
2. 特定のインターフェイスで HSRP アドレス ファミリ コンフィギュレーション モードをイネーブルにします。
3. HSRP グループサブモードをイネーブルにします。



(注) バージョンキーワードは、IPv4 アドレスファミリが選択されている場合にのみ使用できます。デフォルトでは、IPv6 アドレスファミリのバージョンは 2 に設定されています。

4. 設定されたインターフェイスで HSRP をアクティブにし、リンクローカル IPv6 アドレスを割り当てます。



(注)

- 仮想リンクローカルアドレスは、別のグループに対してすでに設定されている他の仮想リンクローカルアドレスと一致するべきではありません。
- 仮想リンクローカルアドレスは、インターフェイスのリンクローカル IPv6 アドレスと一致するべきではありません。
- **autoconfig** キーワードを使用すると、リンクローカルアドレスは EUI-64 形式を使用して計算されます。
- Cisco IOS およびその他のレガシー シスコ デバイスと互換性のある **legacy-compatible** キーワードを使用します。

5. 設定されたインターフェイスで HSRP をアクティブにし、グローバル IPv6 アドレスを割り当てます。



- (注) IPv6 の HSRP を設定する場合は、**autoconfig** キーワードを使用して、リンクローカル IPv6 アドレスを設定するか、イネーブルにする必要があります。リンクローカル IPv6 アドレスを設定しない場合、**commit** キーワードを使用して変更をコミットしても、ルータは設定を受け入れません。

設定

```
/* Enable HSRP interface configuration mode on a specific interface. */
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface <type> <interface-path-id>

/* Enable HSRP address-family configuration mode on a specific interface. */
Router(config-hsrp-if)# address-family ipv4

/* Enable HSRP group submode. */
Router(config-hsrp-ipv4)# hsrp <group-number>

/* Activate HSRP on the configured interface. */
Router(config-hsrp-gp)# address global <ipv6-address>
Router(config-hsrp-gp)# commit
```

実行コンフィギュレーション

```
Router# show running-configuration
configure
router hsrp
interface GigabitEthernet0/2/0/1
address-family ipv4
hsrp 1
address linklocal autoconfig
address global 2001:DB8:A:B::1
!
```

HSRP グループの属性の設定

ローカル ルータが HSRP に関与する仕組みに影響を与える他のホットスタンバイ グループ属性を設定するには、必要に応じてインターフェイス コンフィギュレーション モードで次の手順を使用します。

設定例

1. HSRP コンフィギュレーション モードをイネーブルにします。
2. 特定のインターフェイスで HSRP インターフェイス コンフィギュレーション モードをイネーブルにします。
3. 特定のインターフェイスで HSRP アドレス ファミリ コンフィギュレーション モードをイネーブルにします。

4. HSRP グループサブモードをイネーブルにします。

**Note**

バージョンキーワードは、IPv4 アドレスファミリが選択されている場合にのみ使用できます。デフォルトでは、IPv6 アドレスファミリのバージョンは 2 に設定されています。

5. (任意) HSRP プライオリティを設定します。

- 割り当てられたプライオリティは、アクティブ ルータとスタンバイ ルータを選択するために使用されます。プリエンプションがイネーブルである場合は、プライオリティが最高のルータが指定されたアクティブ ルータになります。プライオリティが等しい場合、プライマリ IP アドレスが比較され、大きい IP アドレスが優先されます。
- インターフェイスが **track** コマンドによって設定されている場合、デバイス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。
- **preempt** コマンドを使用してプリエンプションをイネーブルにしていない場合、ルータは他の HSRP ルータよりもプライオリティが高い場合でもアクティブにならないことがあります。
- デフォルトの HSRP プライオリティ値を復元するには、**no priority** コマンドを使用します。

6. (任意) 他のインターフェイスの可用性に基づいてホットスタンバイ プライオリティが変わるように、インターフェイスを設定します。

- トラッキング対象のインターフェイスがダウンすると、ホットスタンバイ プライオリティが 10 だけ減少します。インターフェイスがトラッキングされていなければ、ステートが変化した場合でもホット スタンバイ プライオリティに影響することはありません。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、トラッキングするインターフェイスのリストを個別に設定できます。
- オプションの *priority-decrement* 引数には、トラッキング対象のインターフェイスがダウンした場合にホットスタンバイ プライオリティをどれだけ減らすかを指定します。トラッキング対象のインターフェイスが再びアップ状態になると、プライオリティは同じ値だけ段階的に増えていきます。
- トラッキング対象の複数のインターフェイスがダウンした場合、*priority-decrement* 引数が設定されていれば、設定されているプライオリティの減分値が累積されます。トラッキング対象のインターフェイスがダウンし、どのオブジェクトにもプライオリティの減分値が設定されていなければ、デフォルトの減分値は 10 で、累積されます。
- 常に最適なルータを使用してパケットが転送されるようにするには、グループ内のすべてのルータ上でこのコマンドとともに **preempt** コマンドを使用する必要があります。**preempt** コマンドを使用しないと、他の HSRP ルータの現在のプライオリティに関係なく、アクティブルータがアクティブのままになります。
- トラッキングを削除するには、**no preempt** コマンドを使用します。

7. (任意) 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。

- **preempt** コマンドでプリエンプションおよびプリエンプション遅延を設定した場合、ローカルルータに現在のアクティブルータよりも高いホットスタンバイ プライオリティが設定されているときには、そのローカルルータはアクティブルータとして制御を引き継ごうとします。**preempt** コマンドを設定していない場合、ローカルルータは、(指定ルータとして機能する) 現在アクティブ状態のルータがないことを示す情報を受信した場合にのみ、アクティブルータとして制御を引き継ぎます。
- ルータが最初に起動したとき、ルータのルーティング テーブルは完全ではありません。プリエンプション処理するように設定されている場合にはアクティブルータになりますが、まだ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、プリエンプション処理する側のルータが現在アクティブなルータを実際にプリエンプション処理するまでの遅延を設定します。
- 現在アクティブ状態のルータがない場合は、プリエンプションの *delay seconds* の値は適用されません。この場合、ローカルルータは、プリエンプション遅延の秒数に関係なく、該当するタイムアウトが経過した後 (**timers** コマンドを参照)、アクティブになります。
- HSRP プリエンプションおよびプリエンプション遅延値をデフォルトに戻すには、**no preempt** コマンドを使用します。

8. (任意) ホットスタンバイ ルータ プロトコル (HSRP) 用の認証ストリングを設定します。

- 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。相互運用性を確保するには、LAN 上の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、デバイスは、HSRP で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 アドレスおよびホットスタンバイ タイマー値を学習できません。
- 認証ストリングが一致しないと、あるルータが指定ルータを引き継ぐというようなプロトコル イベントを回避できません。
- 認証ストリングを削除するには、**no authentication** コマンドを使用します。

設定

```
/* Enable HSRP configuration mode. */
Router# configure
Router(config)# router hsrp

/* Enable HSRP interface configuration mode on a specific interface. */
Router(config-hsrp)# interface <type> <interface-path-id>

/* Enable HSRP address-family configuration mode on a specific interface. */
Router(config-hsrp-if)# address-family ipv4

/* Enable HSRP group submode. */
Router(config-hsrp-ipv4)# hsrp <group-number> version <version-no>
```



```
/* (Optional) Configure HSRP priority. */
Router(config-hsrp-gp) # priority <priority>

/* (Optional) Configure an interface so that the Hot Standby priority changes on the
basis of the availability of other interfaces. */
Router(config-hsrp-gp) # track <type> instance <priority-decrement>

/* (Optional) Configure an authentication string for the Hot Standby Router Protocol
(HSRP). */
Router(config-hsrp-gp) # authentication <string>
```

実行コンフィギュレーション

```
Router# show running-configuration
configure
router hsrp
interface TenGigE0/2/0/1
address-family ipv4
hsrp 1 version 1
priority 100
track TenGigE0/3/0/1
preempt
authentication company1
!
!
!
```

HSRP アクティベーション遅延の設定

HSRP のアクティベーション遅延は、インターフェイスがアップ状態になったときに、ステートマシンの起動を遅らせることを目的としています。これにより、ネットワーク タイムが安定し、リンクがアップ状態になったあとの早い段階で不必要に状態が変化するのを防ぐことができます。

設定例

1. HSRP コンフィギュレーション モードをイネーブルにします。
2. 特定のインターフェイスで HSRP インターフェイス コンフィギュレーション モードをイネーブルにします。
3. ステートマシンの起動の遅延を設定します。



Note

リロード遅延は、最初のインターフェイス起動イベント後に適用される遅延です。最小遅延は、後続の（インターフェイスがフラップする場合の）インターフェイス起動イベントに適用される遅延です。

4. 特定のインターフェイスで HSRP アドレス ファミリ コンフィギュレーション モードをイネーブルにします。
5. HSRP グループサブモードをイネーブルにします。
6. 設定済みのインターフェイスで HSRP をアクティブにします。

**Note**

- 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 アドレスが指定されていない場合は、仮想アドレスがアクティブ ルータから学習されます。
- IPv6 の HSRP を設定する場合は、**autoconfig** キーワードを使用して、リンクローカル IPv6 アドレスを設定するか、イネーブルにする必要があります。リンクローカル IPv6 アドレスを設定しない場合、**commit** キーワードを使用して変更をコミットしても、ルータは設定を受け入れません。

設定

```

/* Enable HSRP configuration mode. */
Router# configure
Router(config)# router hsrp

/* Enable HSRP interface configuration mode on a specific interface. */
Router(config-hsrp)# interface <type> <interface-path-id>

/* Configure the delay of startup of the state machine. */
Router(config-hsrp-if)# hsrp delay minimum <seconds> reload <seconds>

/* Enable HSRP address-family configuration mode on a specific interface. */
Router(config-hsrp-if)# address-family ipv4

/* Enable HSRP group submode. */
Router(config-hsrp-ipv4)# hsrp <group-number> version <version-no>

/* Activate HSRP on the configured interface. */
Router(config-hsrp-gp)# address { learn | address [secondary] }
Router(config-hsrp-gp)# commit

```

実行コンフィギュレーション

```

Router# show running-configuration
configure
router hsrp
  interface TenGigE0/2/0/1
    hsrp delay minimum 2 reload 10
    address-family ipv4
      hsrp 1
      address learn
    !

```

ICMP リダイレクトメッセージの HSRP サポートのディセーブル化

デフォルトでは、ICMP リダイレクト メッセージの HSRP フィルタリングは、HSRP が実行されているルータでイネーブルになっています。

ディセーブルになっているこの機能の再イネーブル化をルータに設定するには、インターフェイス コンフィギュレーション モードで **hsrp redirects** コマンドを使用します。

設定例

1. 特定のインターフェイスで HSRP インターフェイス コンフィギュレーション モードをイネーブルにします。
2. 特定のインターフェイスで HSRP アドレス ファミリ コンフィギュレーション モードをイネーブルにします。
3. HSRP グループサブモードをイネーブルにします。

**Note**

バージョンキーワードは、IPv4 アドレスファミリが選択されている場合にのみ使用できます。デフォルトでは、IPv6 アドレスファミリのバージョンは 2 に設定されています。

4. 設定済みのインターフェイスで HSRP をアクティブにします。

**Note**

- 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 アドレスが指定されていない場合は、仮想アドレスがアクティブ ルータから学習されます。
 - IPv6 の HSRP を設定する場合は、**autoconfig** キーワードを使用して、リンクローカル IPv6 アドレスを設定するか、イネーブルにする必要があります。リンクローカル IPv6 アドレスを設定しない場合、**commit** キーワードを使用して変更をコミットしても、ルータは設定を受け入れません。
5. インターフェイスにホットスタンバイ ルータ プロトコル (HSRP) が設定されているときに送信する Internet Control Message Protocol (ICMP) リダイレクトメッセージを設定します。

**Note**

- **hsrp redirects** コマンドは、インターフェイスごとに設定できます。インターフェイス上で最初に HSRP を設定する場合、このインターフェイスの設定ではグローバル値を継承します。ICMP リダイレクトをインターフェイスで明示的にディセーブルにしている場合は、グローバル コマンドではその機能を再びイネーブルにすることができません。
- **hsrp redirects** コマンドがイネーブルである場合、リダイレクトパケットのネクストホップ アドレスの実 IP アドレスが仮想 IP アドレスに置き換えられて（それが HSRP に認識されている場合）、ICMP リダイレクトメッセージがフィルタリングされます。
- デフォルト (ICMP メッセージがイネーブル) に戻すには、**no hsrp redirects** コマンドを使用します。

設定

```
/* Enable HSRP interface configuration mode on a specific interface. */
Router# configure
Router(config)# router hsrp
```

```

Router(config-hsrp)# interface <type> <interface-path-id>

/* Configure Internet Control Message Protocol (ICMP) redirect messages to be sent when
the Hot Standby Router Protocol (HSRP) is configured on an interface. */
Router(config-hsrp-gp)# hsrp redirects disable

/* Enable HSRP address-family configuration mode on a specific interface. */
Router(config-hsrp-if)# address-family ipv4

/* Enable HSRP group submode. */
Router(config-hsrp-ipv4)# hsrp <group-number> version <version-no>

/* Activate HSRP on the configured interface. */
Router(config-hsrp-gp)# address {learn|address[secondary]}

```

実行コンフィギュレーション

```

Router# show running-configuration
router hsrp
  interface TenGigE 0/2/0/1
    address-family ipv4
      hsrp 1 version 1
      address learn
    !
  !
  hsrp redirects disable
  !
!

```

HSRP のマルチ グループ オプティマイゼーション (MGO)

マルチ グループ オプティマイゼーションは、多くのサブインターフェイスで構成される配置で制御トラフィックを削減するためのソリューションです。HSRP 制御トラフィックの実行をセッションの 1 つに限ることにより、冗長性要件が同じサブインターフェイスでは制御トラフィックが減少します。他のすべてのセッションはこのプライマリセッションのスレーブになり、プライマリ セッションから状態を継承します。

HSRP のカスタマイズ

HSRP 動作のカスタマイズは任意です。HSRP グループをイネーブルにすると、そのグループはすぐに動作します。

設定例

1. 特定のインターフェイスで HSRP インターフェイス コンフィギュレーション モードをイネーブルにします。
2. 特定のインターフェイスで HSRP アドレス ファミリ コンフィギュレーション モードをイネーブルにします。
3. HSRP グループサブモードをイネーブルにします。



(注) バージョンキーワードは、IPv4 アドレスファミリが選択されている場合にのみ使用できます。デフォルトでは、IPv6 アドレスファミリのバージョンは 2 に設定されています。

4. HSRP セッション名を設定します。
5. IP のホットスタンバイ プロトコルをイネーブルにします。



(注) 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 アドレスが指定されていない場合は、仮想アドレスがアクティブ ルータから学習されます。

6. ルータのセカンダリ仮想 IPv4 アドレスを設定します。
7. ホットスタンバイ ルータ プロトコル (HSRP) 用の認証ストリングを設定します。
8. 特定のインターフェイスで HSRP スレーブ コンフィギュレーションモードをイネーブルにします。
9. 指定のグループから状態を継承するようにスレーブグループを設定します。
10. スレーブグループ用にプライマリ仮想 IPv4 アドレスを設定します。

設定

```
/* Enable HSRP interface configuration mode on a specific interface. */
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface <type> <interface-path-id>

/* Enable HSRP address-family configuration mode on a specific interface. */
Router(config-hsrp-if)# address-family ipv4

/* Enable HSRP group configuration mode on a specific interface. */
Router(config-hsrp-ipv4)# hsrp <group-no> version <version-no>

/* Configure an HSRP session name. */
Router(config-hsrp-gp)# name <name>

/* Enable hot standby protocol for IP. */
Router(config-hsrp-gp)# address { learn | address}

/* Configure the secondary virtual IPv4 address for a router. */
Router(config-hsrp-gp)# address <address> secondary

/* Configures an authentication string for the Hot Standby Router Protocol (HSRP). */
Router(config-hsrp-gp)# authentication <string>

/* Enables HSRP slave configuration mode on a specific interface. */
Router(config-hsrp-gp)# hsrp <group-no> slave

/* Configure the slave group to inherit its state from a specified group. */
Router(config-hsrp-slave)# follow mgo-session-name
```

```
/* Configure the primary virtual IPv4 address for the slave group.
Router(config-hsrp-slave)# address <ip-address>
```

実行コンフィギュレーション

```
Router# show running-configuration
router hsrp
  interface TenGigE0/2/0/1
    address-family ipv4
      hsrp 1 version 1
        name s1
        address learn
        address 1198.51.100.1 secondary
        authentication company1
      hsrp 2 slave
        follow s1
        address 192.0.2.1
    !
  !
!
!
```

プライマリ仮想 IPv4 アドレスの設定

IP のホットスタンバイプロトコルをイネーブルにするには、HSRP グループサブモードで **address (hsrp)** コマンドを使用します。

設定例

1. 特定のインターフェイスで HSRP インターフェイス コンフィギュレーション モードをイネーブルにします。
2. 特定のインターフェイスで HSRP アドレス ファミリ コンフィギュレーション モードをイネーブルにします。
3. 特定のインターフェイスで HSRP グループ コンフィギュレーション モードをイネーブルにします。



- (注)
- バージョンキーワードは、IPv4 アドレスファミリが選択されている場合にのみ使用できます。デフォルトでは、IPv6 アドレスファミリのバージョンは 2 に設定されています。
 - HSRP バージョン 2 では、0 ～ 4095 の拡張グループ範囲が提供されます。

4. IP のホットスタンバイプロトコルをイネーブルにします。

設定

```
/* Enable HSRP interface configuration mode on a specific interface. */
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface <type> <interface-path-id>

/* Enable HSRP address-family configuration mode on a specific interface. */
```

```
Router(config-hsrp-if)# address-family ipv4

/* Enable HSRP group configuration mode on a specific interface. */
Router(config-hsrp-ipv4)# hsrp <group-number> version <version-no>

/* Enable hot standby protocol for IP. */
Router(config-hsrp-ipv4)# address { learn | address }
```

実行コンフィギュレーション

```
Router# show running-configuration
router hsrp
 interface TenGigE 0/2/0/1
   address-family ipv4
     hsrp 1 version 1
     address learn
   !
 !
 !
 !
```

セカンダリ仮想 IPv4 アドレスの設定

ルータのセカンダリ仮想 IPv4 アドレスを設定するには、ホットスタンバイ ルータ プロトコル (HSRP) 仮想ルータサブモードで **address secondary** コマンドを使用します。

設定例

1. 特定のインターフェイスで HSRP インターフェイス コンフィギュレーション モードをイネーブルにします。
2. 特定のインターフェイスで HSRP アドレス ファミリ コンフィギュレーション モードをイネーブルにします。
3. 特定のインターフェイスで HSRP グループ コンフィギュレーション モードをイネーブルにします。



- (注)
- バージョンキーワードは、IPv4 アドレスファミリが選択されている場合にのみ使用できます。デフォルトでは、IPv6 アドレスファミリのバージョンは 2 に設定されています。
 - HSRP バージョン 2 では、0 ～ 4095 の拡張グループ範囲が提供されます。

4. ルータのセカンダリ仮想 IPv4 アドレスを設定します。

設定

```
/* Enable HSRP interface configuration mode on a specific interface. */
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface <type> <interface-path-id>

/* Enable HSRP address-family configuration mode on a specific interface. */
Router(config-hsrp-if)# address-family ipv4

/* Enable HSRP group configuration mode on a specific interface. */
```

```
Router(config-hsrp-ipv4)# hsrp <group-number> version <version-no>

/* Configure the secondary virtual IPv4 address for a router. */
Router(config-hsrp-ipv4)# address <address> secondary
```

実行コンフィギュレーション

```
Router# show running-configuration
router hsrp
  interface TenGigE 0/2/0/1
    address-family ipv4
      hsrp 1 version 1
      192.0.2.1
    !
  !
!
```

スレーブ フォローの設定

指定のグループから状態を継承するようにスレーブグループに指示するには、HSRP スレーブ サブモードモードで **slave follow** コマンドを使用します。

設定例

1. 特定のインターフェイスで HSRP インターフェイス コンフィギュレーション モードをイネーブルにします。
2. 特定のインターフェイスで HSRP アドレス ファミリ コンフィギュレーション モードをイネーブルにします。
3. 特定のインターフェイスで HSRP スレーブ コンフィギュレーション モードをイネーブルにします。
4. 指定のグループから状態を継承するようにスレーブグループを設定します。

Configuration

```
/* Enable HSRP interface configuration mode on a specific interface. */
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface <type> <interface-path-id>

/* Enable HSRP address-family configuration mode on a specific interface. */
Router(config-hsrp-if)# address-family ipv4

/* Enable HSRP slave configuration mode on a specific interface. */
Router(config-hsrp-ipv4)# hsrp <group-no> slave

/* Configure the slave group to inherit its state from a specified group. */
Router(config-hsrp-slave)# address <ip-address>
```

Running Configuration

```
Router# show running-configuration
router hsrp
  interface TenGigE 0/2/0/1
    address-family ipv4
      hsrp 1 slave
      address 192.0.2.1
    !
```



```
!
!
!
```

スレーブ プライマリ仮想 IPv4 アドレスの設定

スレーブグループのプライマリ仮想 IPv4 アドレスを設定するには、HSRP スレーブサブモードで **slave primary virtual IPv4 address** コマンドを使用します。

設定例

1. 特定のインターフェイスで HSRP インターフェイス コンフィギュレーション モードをイネーブルにします。
2. 特定のインターフェイスで HSRP アドレス ファミリ コンフィギュレーション モードをイネーブルにします。
3. 特定のインターフェイスで HSRP スレーブ コンフィギュレーション モードをイネーブルにします。
4. スレーブグループ用にプライマリ仮想 IPv4 アドレスを設定します。

Configuration

```
/* Enable HSRP interface configuration mode on a specific interface. */
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface <type> <interface-path-id>

/* Enable HSRP address-family configuration mode on a specific interface. */
Router(config-hsrp-if)# address-family ipv4

/* Enable HSRP slave configuration mode on a specific interface. */
Router(config-hsrp-ipv4)# hsrp <group-no> slave

/* Configure the primary virtual IPv4 address for the slave group. */
Router(config-hsrp-slave)# address <ip-address>
```

Running Configuration

```
Router# show running-configuration
router hsrp
  interface TenGigE 0/2/0/1
    address-family ipv4
      hsrp 1 slave
      address 192.0.2.1
    !
  !
!
```

スレーブグループ用セカンダリ仮想 IPv4 アドレスの設定

次のタスクを実行して、スレーブグループのセカンダリ仮想 IPv4 アドレスを設定します。

設定例

1. 特定のインターフェイスで HSRP インターフェイス コンフィギュレーション モードをイネーブルにします。
2. 特定のインターフェイスで HSRP アドレス ファミリ コンフィギュレーション モードをイネーブルにします。
3. 特定のインターフェイスで HSRP スレーブ コンフィギュレーション モードをイネーブルにします。
4. ルータのセカンダリ仮想 IPv4 アドレスを設定します。

Configuration

```
/* Enable HSRP interface configuration mode on a specific interface. */
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface <type> <interface-path-id>

/* Enable HSRP address-family configuration mode on a specific interface. */
Router(config-hsrp-if)# address-family ipv4

/* Enable HSRP slave configuration mode on a specific interface. */
Router(config-hsrp-ipv4)# hsrp <group-no> slave

/* Configure the secondary virtual IPv4 address for the slave group. */
Router(config-hsrp-slave)# address <ip-address> secondary
```

Running Configuration

```
Router# show running-configuration
router hsrp
  interface TenGigE 0/2/0/1
    address-family ipv4
      hsrp 1 slave
      address 192.0.2.1 secondary
    !
  !
!
```

スレーブ仮想 MAC アドレスの設定

スレーブグループの仮想 MAC アドレスを設定するには、HSRP スレーブサブモードで **slave virtual mac address** コマンドを使用します。

設定例

1. 特定のインターフェイスで HSRP インターフェイス コンフィギュレーション モードをイネーブルにします。
2. 特定のインターフェイスで HSRP アドレス ファミリ コンフィギュレーション モードをイネーブルにします。
3. 特定のインターフェイスで HSRP スレーブ コンフィギュレーション モードをイネーブルにします。

Configuration

```

/* Enable HSRP interface configuration mode on a specific interface. */
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface <type> <interface-path-id>

/* Enable HSRP address-family configuration mode on a specific interface. */
Router(config-hsrp-if)# address-family ipv4

/* Enable HSRP slave configuration mode on a specific interface. */
Router(config-hsrp-ipv4)# hsrp <group-no> slave

```

Running Configuration

```

Router# show running-configuration
router hsrp
  interface TenGigE 0/2/0/1
    address-family ipv4
      hsrp 1 slave
    !
  !
!
!

```

HSRP セッション名の設定

HSRP セッション名を設定するには、HSRP グループサブモードで **session name** コマンドを使用します。

設定例

1. 特定のインターフェイスで HSRP インターフェイス コンフィギュレーション モードをイネーブルにします。
2. 特定のインターフェイスで HSRP アドレス ファミリ コンフィギュレーション モードをイネーブルにします。
3. 特定のインターフェイスで HSRP グループ コンフィギュレーション モードをイネーブルにします。



- (注)
- バージョンキーワードは、IPv4 アドレスファミリが選択されている場合にのみ使用できます。デフォルトでは、IPv6 アドレスファミリのバージョンは 2 に設定されています。
 - HSRP バージョン 2 では、0 ～ 4095 の拡張グループ範囲が提供されます。

4. 指定のグループから状態を継承するようにスレーブグループを設定します。

Configuration

```

/* Enable HSRP interface configuration mode on a specific interface. */
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface <type> <interface-path-id>

/* Enable HSRP address-family configuration mode on a specific interface. */
Router(config-hsrp-if)# address-family ipv4

```

```
/* Enable HSRP group configuration mode on a specific interface. */
Router(config-hsrp-ipv4)# hsrp <group-no> hsrp <version-no>

/* Configure the slave group to inherit its state from a specified group. */
Router(config-hsrp-ipv4)# name <name>
```

Running Configuration

```
Router# show running-configuration
router hsrp
 interface TenGigE 0/2/0/1
   address-family ipv4
     hsrp 1 version 2
     name s1
   !
 !
 !
```

HSRP および IP スタティックの拡張オブジェクトトラッキング

標準の HSRP 障害検出メカニズムでは、アクティブルータとコア ネットワークとの間の障害を検出できません。オブジェクトトラッキングは、そのような障害を検出するために使用します。そのような障害が発生すると、アクティブルータはプライオリティの減分値をその HSRP セッションに適用します。この結果、プライオリティがスタンバイルータのプライオリティを下回った場合には、このことを HSRP 制御トラフィックから検出し、これをアクティブなロールをプリエンプション処理して引き継ぐためのトリガーとして使用します。

Cisco IOS XR ソフトウェアは、最大 512 のトラッキングオブジェクトをサポートします。

HSRP および IP スタティック機能の拡張オブジェクトトラッキングを使用すると、IP サービス レベル契約 (IPSLA) に基づいて、ファーストホップの冗長性を確保し、デフォルトゲートウェイを選択できます。

スタティックルートの拡張されたオブジェクトトラッキングの詳細については、*Routing Configuration Guide for Cisco NCS 560 Series Routers* を参照してください。

HSRP 用のオブジェクトトラッキングの設定

名前付きオブジェクトのトラッキングを、減分値を指定してイネーブルにするには、HSRP グループサブモードで次の設定を使用します。

設定例

1. 特定のインターフェイスで HSRP インターフェイス コンフィギュレーション モードをイネーブルにします。
2. 特定のインターフェイスで HSRP アドレス ファミリ コンフィギュレーション モードをイネーブルにします。
3. 特定のインターフェイスで HSRP グループサブモードをイネーブルにします。



(注) バージョンキーワードは、IPv4 アドレスファミリが選択されている場合にのみ使用できます。デフォルトでは、IPv6 アドレスファミリのバージョンは 2 に設定されています。

4. 名前付きオブジェクトのトラッキングを、減分値を指定してイネーブルにします。

Configuration

```
/* Enable HSRP interface configuration mode on a specific interface. */
Router# configure
Router(config)# router hsrp
Router(config-hsrp)# interface <type> <interface-path-id>

/* Enable HSRP address-family configuration mode on a specific interface. */
Router(config-hsrp-if)# address-family ipv4

/* Enable HSRP group sub-mode on a specific interface. */
Router(config-hsrp-ipv4)# hsrp <group-no> hsrp <version-no>

/* Enable tracking of the named object with the specified decrement. */
Router(config-hsrp-gp)# track object <name> [priority-decrement]
```

Running Configuration

```
Router# show running-configuration
router hsrp
  interface TenGigE 0/2/0/1
    address-family ipv4
      hsrp 1 version 1
      track object t1 2
    !
  !
!
```

HSRP のホット リスタート

1 つのアクティブ グループで HSRP プロセスの障害が発生した場合には、ピア HSRP アクティブ ルータ グループで強制的にフェールオーバーが行われなくする必要があります。ホット リスタートはウォーム RP フェールオーバーをサポートしており、ピア HSRP アクティブ ルータ グループへの強制的なフェールオーバーは発生しません。

ソフトウェアでの HSRP の実装の設定例

ここでは、次の HSRP 設定例について説明します。

HSRP グループの設定：例

次に、インターフェイスで HSRP をイネーブルにし、HSRP グループ属性を設定する例を示します。

```
configure
router hsrp
interface 0/2/0/1
hsrp 1 ipv4 1.0.0.5
commit
hsrp 1 timers 100 200
hsrp 1 preempt delay 500
hsrp priority 20
hsrp track 0/2/0/2
hsrp 1 authentication company0
hsrp use-bia
commit
```

複数の HSRP グループ用のルータの設定 : 例

次に、複数の HSRP グループ用にルータを設定する例を示します。

```
configure
router hsrp
interface 0/2/0/3
hsrp 1 ipv4 1.0.0.5
hsrp 1 priority 20
hsrp 1 preempt
hsrp 1 authentication sclara
hsrp 2 ipv4 1.0.0.6
hsrp 2 priority 110
hsrp 2 preempt
hsrp 2 authentication mtview
hsrp 3 ipv4 1.0.0.7
hsrp 3 preempt
hsrp 3 authentication svale
commit
```



第 9 章

LPTS の実装

- [LPTS の概要 \(173 ページ\)](#)
- [LPTS ポリサー \(173 ページ\)](#)
- [マルチキャストおよびブロードキャストのパントされたパケットにおけるポートごとのレート制限 \(178 ページ\)](#)
- [ドメインベースの LPTS ポリサー \(186 ページ\)](#)
- [ダイナミック LPTS フロー タイプの定義 \(187 ページ\)](#)

LPTS の概要

Local Packet Transport Services (LPTS) では、セキュア ドメイン ルータ (SDR) 宛てのすべてのパケットフローを記述するテーブルを保持し、これにより、意図した宛先に確実にパケットが配信されます。

LPTS では、ポート アービトラータおよびフロー マネージャという 2 つのコンポーネントを使用して、このタスクを実行します。ポート アービトラータおよびフロー マネージャは、Internal Forwarding Information Base (IFIB) と呼ばれる、論理ルータ用のパケット フローを記述するテーブルを保持するプロセスです。IFIBは、受信したパケットを適切なルートプロセッサにルーティングして処理するために使用します。

LPTS は、ルータ外からパケットを受信するすべてのアプリケーションと内部的にインターフェイスします。LPTS は、カスタマー設定の必要なく機能します。ただし、ポリサー値は、必要に応じてカスタマイズできます。カスタマーが LPTS フロー マネージャとポート アービトラータのアクティビティやパフォーマンスをモニタリングできるように、LPTS の show コマンドが用意されています。

LPTS ポリサー

Cisco IOS XR では、ルート プロセッサ (RP) 宛ての制御パケットは、着信ポートで一連の入力ポリサーを使用してポリシングされます。これらのポリサーは、ブートアップ時に LPTS コンポーネントによって静的にプログラミングされます。これらのポリサーは、着信制御トラフィックのフロー タイプに基づいて適用されます。フロー タイプは、パケット ヘッダーを調

べることで決定されます。これらの静的入力ポリサーのポリサー レートは、コンフィギュレーションファイルで定義され、ブートアップ時にルートプロセッサにプログラミングされます。これらの一連の入力ポリサーのフロータイプに基づいて、ポリサー値を変更できます。各ノードのポリサーごとにレートを設定できます。



- (注) • デフォルトのポリサー値とフロー タイプの現在のレートは、次の **show** コマンドの出力で確認できます。

```
show lpts pifib hardware police
```

- データポートを介したファイル転送を高速化するために、SSH フローの LPTS ポリサー レートを設定できます。

show lpts pifib hardware entry brief location node-id |inc SSH コマンドを使用して、LPTS のドロップを確認します。LPTS ドロップがある場合は、最大 50000 pps までレートを増やします。

pps が高いと CPU サイクルの使用率が増加するため、必要な場合にのみ値を最大にします。

次に例を示します。

```
Router#configure
Router(config)#lpts pifib hardware police location 0/0/CPU0
Router(config-pifib-policer-per-node)# flow ssh known rate 50000
Router(config-pifib-policer-per-node)#commit
```

設定例

次の値をすべてのノードにグローバルに使用して、OSPF および BGP フロータイプに LPTS ポリサーを設定します。

- ospf unicast default rate 3000
- bgp default rate 4000

```
Router#configure
Router(config)#lpts pifib hardware police
Router(config-pifib-policer-global)#flow ospf unicast default rate 3000
Router(config-pifib-policer-global)#flow bgp default rate 4000
Router (config-pifib-policer-global)#commit
```

実行コンフィギュレーション

```
lpts pifib hardware police
flow ospf unicast default rate 3000
flow bgp default rate 4000
!
```

確認

```
Router#show run lpts pifib hardware police
lpts pifib hardware police
```



```
flow ospf unicast default rate 3000
flow bgp default rate 4000
```

設定例

次の値を個々のノード 0/RP0/CPU0 に使用して、OSPF および BGP フロー タイプに LPTS ポリサーを設定します。

- ospf unicast default rate 3000
- flow bgp default rate 4000

```
Router#configure
Router(config)#lpts pifib hardware police location 0/RP0/CPU0
Router(config-pifib-policer-per-node)#flow ospf unicast default rate 3000
Router(config-pifib-policer-per-node)#flow bgp default rate 4000
Router(config-pifib-policer-per-node)#commit
```

実行コンフィギュレーション

```
lpts pifib hardware police location 0/RP0/CPU0
flow ospf unicast default rate 3000
flow bgp default rate 4000
```

確認

show lpts pifib hardware police location 0/RP0/CPU0 コマンドは、指定したノードの Pre-Internal Forwarding Information Base (IFIB) 情報を表示します。

```
Router#show lpts pifib hardware police location 0/RP0/CPU0
```

```
-----
Node 0/RP0/CPU0:
-----
Burst = 100ms for all flow types
-----
```

| FlowType | Policer | Type | Cur. Rate | Burst | npu |
|-----------------|---------|------|-----------|-------|-----|
| OSPF-uc-default | 32106 | np | 3000 | 1000 | 0 |
| BGP-default | 32118 | np | 4000 | 1250 | 0 |

確認

show controllers npu stats traps-all instance all location 0/RP0/CPU0 コマンドは、ローカルで処理されたパケットと、CPU によってドロップされたパケットを表示します。

```
Router# show controllers npu stats traps-all instance all location 0/RP0/CPU0
```

| Trap Type | NPU | Trap | TrapStats | Policer | Packet |
|---|-----|------|-----------|---------|----------|
| Packet | ID | ID | ID | | Accepted |
| Dropped | | | | | |
| RxTrapMimSaMove (CFM_DOWM_MEP_DMM) | 0 | 6 | 0x6 | 32037 | 0 |
| RxTrapMimSaUnknown (RCY_CFM_DOWN_MEP_DMM) | 0 | 7 | 0x7 | 32037 | 0 |
| RxTrapAuthSaLookupFail (IPMC default) | 0 | 8 | 0x8 | 32033 | 0 |
| RxTrapSaMulticast | 0 | 11 | 0xb | 32018 | 0 |

| | | | | | | |
|---|---|----|------|-------|---------|---|
| RxTrapArpMyIp | 0 | 13 | 0xd | 32001 | 0 | 0 |
| RxTrapArp | 0 | 14 | 0xe | 32001 | 11 | 0 |
| RxTrapDhcpv4Server | 0 | 18 | 0x12 | 32022 | 0 | 0 |
| RxTrapDhcpv4Client | 0 | 19 | 0x13 | 32022 | 0 | 0 |
| RxTrapDhcpv6Server | 0 | 20 | 0x14 | 32022 | 0 | 0 |
| RxTrapDhcpv6Client | 0 | 21 | 0x15 | 32022 | 0 | 0 |
| RxTrapL2Cache_LACP | 0 | 23 | 0x17 | 32003 | 0 | 0 |
| RxTrapL2Cache_LLDP1 | 0 | 24 | 0x18 | 32004 | 0 | 0 |
| RxTrapL2Cache_LLDP2 | 0 | 25 | 0x19 | 32004 | 1205548 | 0 |
| RxTrapL2Cache_LLDP3 | 0 | 26 | 0x1a | 32004 | 0 | 0 |
| RxTrapL2Cache_ELMI | 0 | 27 | 0x1b | 32005 | 0 | 0 |
| RxTrapL2Cache_BPDU | 0 | 28 | 0x1c | 32027 | 0 | 0 |
| RxTrapL2Cache_BUNDLE_BPDU | 0 | 29 | 0x1d | 32027 | 0 | 0 |
| RxTrapL2Cache_CDP | 0 | 30 | 0x1e | 32002 | 0 | 0 |
| RxTrapHeaderSizeErr | 0 | 32 | 0x20 | 32018 | 0 | 0 |
| RxTrapIpCompMcInvalidIp | 0 | 35 | 0x23 | 32018 | 0 | 0 |
| RxTrapMyMacAndIpDisabled | 0 | 36 | 0x24 | 32018 | 0 | 0 |
| RxTrapMyMacAndMplsDisable | 0 | 37 | 0x25 | 32018 | 0 | 0 |
| RxTrapArpReply | 0 | 38 | 0x26 | 32001 | 2693 | 0 |
| RxTrapFibDrop | 0 | 41 | 0x29 | 32018 | 0 | 0 |
| RxTrapMTU | 0 | 42 | 0x2a | 32020 | 0 | 0 |
| RxTrapMiscDrop | 0 | 43 | 0x2b | 32018 | 0 | 0 |
| RxTrapL2AclDeny | 0 | 44 | 0x2c | 32034 | 0 | 0 |
| Rx_UNKNOWN_PACKET | 0 | 46 | 0x2e | 32018 | 0 | 0 |
| RxTrapL3AclDeny | 0 | 47 | 0x2f | 32034 | 0 | 0 |
| RxTrapOamY1731MplsTp (OAM_SWOFF_DN_CCM) | 0 | 57 | 0x39 | 32029 | 0 | 0 |
| RxTrapOamY1731Pwe (OAM_SWOFF_DN_CCM) | 0 | 58 | 0x3a | 32030 | 0 | 0 |
| RxTrapOamLevel | 0 | 64 | 0x40 | 32023 | 0 | 0 |
| RxTrapRedirectToCpuOamPacket | 0 | 65 | 0x41 | 32025 | 0 | 0 |
| RxTrapOamPassive | 0 | 66 | 0x42 | 32024 | 0 | 0 |
| RxTrap1588 | 0 | 67 | 0x43 | 32038 | 0 | 0 |
| RxTrapExternalLookupError | 0 | 72 | 0x48 | 32018 | 0 | 0 |

| | | | | | | |
|--|---|-----|------|-------|-----------|---|
| RxTrapArplookupFail | 0 | 73 | 0x49 | 32001 | 0 | 0 |
| RxTrapUcLooseRpfFail | 0 | 84 | 0x54 | 32035 | 0 | 0 |
| RxTrapMplsControlWordTrap | 0 | 88 | 0x58 | 32015 | 0 | 0 |
| RxTrapMplsControlWordDrop | 0 | 89 | 0x59 | 32015 | 0 | 0 |
| RxTrapMplsUnknownLabel | 0 | 90 | 0x5a | 32018 | 0 | 0 |
| RxTrapIpv4VersionError | 0 | 98 | 0x62 | 32018 | 0 | 0 |
| RxTrapIpv4ChecksumError | 0 | 99 | 0x63 | 32018 | 0 | 0 |
| RxTrapIpv4HeaderLengthError | 0 | 100 | 0x64 | 32018 | 0 | 0 |
| RxTrapIpv4TotalLengthError | 0 | 101 | 0x65 | 32018 | 0 | 0 |
| RxTrapIpv4Ttl0 | 0 | 102 | 0x66 | 32008 | 0 | 0 |
| RxTrapIpv4Ttl1 | 0 | 104 | 0x68 | 32008 | 0 | 0 |
| RxTrapIpv4DipZero | 0 | 106 | 0x6a | 32018 | 0 | 0 |
| RxTrapIpv4SipIsMc | 0 | 107 | 0x6b | 32018 | 0 | 0 |
| RxTrapIpv6VersionError | 0 | 109 | 0x6d | 32018 | 0 | 0 |
| RxTrapIpv6HopCount0 | 0 | 110 | 0x6e | 32011 | 0 | 0 |
| RxTrapIpv6LoopbackAddress | 0 | 113 | 0x71 | 32018 | 0 | 0 |
| RxTrapIpv6MulticastSource | 0 | 114 | 0x72 | 32018 | 0 | 0 |
| RxTrapIpv6NextHeaderNull | 0 | 115 | 0x73 | 32010 | 0 | 0 |
| RxTrapIpv6Ipv4CompatibleDestination | 0 | 121 | 0x79 | 32018 | 0 | 0 |
| RxTrapMplsTtl1 | 0 | 125 | 0x7d | 32012 | 316278 | |
| 2249 RxTrapUcStrictRpfFail | 0 | 137 | 0x89 | 32035 | 0 | 0 |
| RxTrapMcExplicitRpfFail | 0 | 138 | 0x8a | 32033 | 0 | 0 |
| RxTrapOamp (OAM_BDL_DN_NON_CCM) | 0 | 141 | 0x8d | 32031 | 0 | 0 |
| RxTrapOamEthUpAccelerated (OAM_BDL_UP_NON_CCM) | 0 | 145 | 0x91 | 32032 | 0 | 0 |
| RxTrapReceive | 0 | 150 | 0x96 | 32017 | 125266112 | 0 |
| RxTrapUserDefine_FIB_IPV4_NULL0 | 0 | 151 | 0x97 | 32018 | 0 | 0 |
| RxTrapUserDefine_FIB_IPV6_NULL0 | 0 | 152 | 0x98 | 32018 | 0 | 0 |
| RxTrapUserDefine_FIB_IPV4_GLEAN | 0 | 153 | 0x99 | 32016 | 0 | 0 |
| RxTrapUserDefine_FIB_IPV6_GLEAN | 0 | 154 | 0x9a | 32016 | 0 | 0 |
| RxTrapUserDefine_IPV4_OPTIONS | 0 | 155 | 0x9b | 32006 | 0 | 0 |
| RxTrapUserDefine_IPV4_RSVP_OPTIONS | 0 | 156 | 0x9c | 32007 | 0 | 0 |
| RxTrapUserDefine | 0 | 157 | 0x9d | 32026 | 0 | 0 |

| | | | | | | |
|---|---|-----|------|-------|---|---|
| RxTrapUserDefine_BFD | 0 | 163 | 0xa3 | 32028 | 0 | 0 |
| RxTrapMC | 0 | 181 | 0xb5 | 32033 | 0 | 0 |
| RxNetflowSnoopTrap0 | 0 | 182 | 0xb6 | 32018 | 0 | 0 |
| RxNetflowSnoopTrap1 | 0 | 183 | 0xb7 | 32018 | 0 | 0 |
| RxTrapMimSaMove (CFM_DOWM_MEP_DMM) | 1 | 6 | 0x6 | 32037 | 0 | 0 |
| RxTrapMimSaUnknown (RCY_CFM_DOWN_MEP_DMM) | 1 | 7 | 0x7 | 32037 | 0 | 0 |
| RxTrapAuthSaLookupFail (IPMC default) | 1 | 8 | 0x8 | 32033 | 0 | 0 |
| RxTrapSaMulticast | 1 | 11 | 0xb | 32018 | 0 | 0 |
| RxTrapArpMyIp | 1 | 13 | 0xd | 32001 | 0 | 0 |

関連コマンド

- lpts pifib hardware police
- flow ospf
- flow bgp
- show lpts pifib hardware police

マルチキャストおよびブロードキャストのパントされたパケットにおけるポートごとのレート制限

この機能により、インターフェイスレベルでのマルチキャストおよびブロードキャストのパントされたトラフィックのレート制限がイネーブルになります。現在は NPU レベルごとのレート制限がサポートされています。この機能は、パントされたトラフィックのマルチキャストおよびブロードキャストストームの受信からポートを保護するため、インターフェイスレベルでのレート制限をサポートします。すべての L3 プロトコルパントパケットおよび L2 プロトコルパケット（ERPS および DOT1x のみ）のレート制限は、物理およびバンドルのメインインターフェイスでサポートされています。

マルチキャストおよびブロードキャストのパントされたトラフィックに対するレート制限の設定

マルチキャストおよびブロードキャストのレート制限は、次の 3 つのレベルで設定できます。

- インターフェイス レベル
- グローバル レベル
- ドメインレベル

マルチキャストおよびブロードキャストのパントされたトラフィックをレート制限するとともに、次のプロトコルのパントされたトラフィックに対してレート制限を設定できます。

- ARP
- CDP
- LACP

プロトコル固有の設定については、以下のセクションで説明します。

制限事項

ブロードキャストとマルチキャストのレート制限が **ARP** のレート制限とともに設定されている場合、ARP パケットによってブロードキャストカウンタとマルチキャストカウンタが増加します。

インターフェイス レベル

TenGig インターフェイスでマルチキャストおよびブロードキャストのパントされたトラフィックのレート制限を 1000 pps に設定する例を示します。



(注) インターフェイスレベルのレート制限の設定は、グローバルレベルおよびドメインレベルの設定よりも優先されます。

1. Router# configure
 コンフィギュレーション モードを開始します。
2. Router(config)# lpts punt police
 パント コンフィギュレーション モードを開始します。
3. Router(config-lpts-punt-policer)# interface TenGigE0/0/0/8/0
 インターフェイスレベルのポリサー設定ごとに開始します。
4. Router(config-lpts-punt-policer-global-if)# mcast rate 1000
 マルチキャストのパントされたトラフィックのレート制限を 1000 pps に設定します。
5. Router(config-lpts-punt-policer-global-if)# bcast rate 1000
 ブロードキャストのパントされたトラフィックのレート制限を 1000 pps に設定します。
6. Router(config-lpts-punt-policer-global-if)# commit
 設定をコミットします。

グローバルレベル

レート制限を設定する例を示します。

- マルチキャストおよびブロードキャストのパントされたトラフィックに 1000 pps

1. Router# configure
コンフィギュレーション モードを開始します。
2. Router(config)# lpts punt police
パント コンフィギュレーション モードを開始します。
3. Router(config-punt-policer-global)# mcast rate 1000
マルチキャストレート制限を 1000 pps に設定します。
4. Router(config-punt-policer-global)# bcast rate 1000
ブロードキャストレート制限を 1000 pps に設定します。
5. Router(config-punt-policer-global)# commit
設定をコミットします。

ドメインレベル

LPTS ドメインを設定し、レート制限を適用する例を示します。

- マルチキャストおよびブロードキャストのパントされたトラフィックに 1000 pps

1. Router# configure
コンフィギュレーション モードを開始します。
2. Router(config)# lpts punt police domain ACCESS
LPTS パント ドメイン コンフィギュレーション モードを開始します。
3. Router(config-lpts-punt-policer-global-ACCESS)# mcast 5000
マルチキャストレート制限を 5000 pps に設定します。
4. Router(config-lpts-punt-policer-global-ACCESS)# bcast 5000
ブロードキャストレート制限を 5000 pps に設定します。
5. Router(config-lpts-punt-policer-global-ACCESS)# exit
ドメインアクセスモードを終了します。
6. Router(config-lpts-punt-policer)# exit
LPTS パント コンフィギュレーション モードを終了します。
7. Router(config)# lpts pifib hardware domain ACCESS
LPTS ハードウェア ドメイン コンフィギュレーション モードを開始します。
8. Router(config-pifib-domain-ACCESS)# interface TenGigE0/0/0/8/1
TenGigE0/0/0/8/1 インターフェイスノードに、ドメインアクセスを適用します。
9. Router(config-pifib-domain-ACCESS)# exit
LPTS ドメインモードを終了します。

10. Router(config)# lpts punt police location 0/0/CPU0
LPTS パント ポリサー コンフィギュレーション モードを開始します。
11. Router(config-lpts-punt-policer)# protocol arp rate 500
ARP プロトコルパケットに 500 pps のレート制限を設定します。
12. Router(config-lpts-punt-policer)# protocol cdp rate 500
CDP プロトコルパケットに 500 pps のレート制限を設定します。
13. Router(config-lpts-punt-policer)# exit
LPTS パント ポリサー コンフィギュレーション モードを終了します。
14. Router(config)# lpts punt police location 0/4/CPU0
ノードロケーション 0/4/CPU0 で LPTS パントポリサーを設定します。
15. Router(config)# commit
設定をコミット



(注) 設定をコミットした後、マルチキャストおよびブロードキャストのレート制限に関して、syslog でエラーメッセージがキャプチャされているかどうかを確認します。

プロトコルのパントされたトラフィック

プロトコルのパントされたトラフィック（ARP、CDP、LACP）に対してレート制限を設定できます。

グローバルレベルでのプロトコルのパントされたトラフィックに対し、次のレート制限を設定する例を示します。

- ARP および CDP プロトコルに 500 pps

1. Router(config-punt-policer-global)# protocol arp rate 500
ARP プロトコルパケットに 500 pps のレート制限を設定します。
2. Router(config-punt-policer-global)# protocol cdp rate 500
CDP プロトコルパケットに 500 pps のレート制限を設定します。
3. Router(config-punt-policer-global)# commit
設定をコミットします。

ドメインレベルでのプロトコルのパントされたトラフィックに対し、次のレート制限を設定する例を示します。

- ARP および CDP プロトコルに 500 pps

1. Router(config)# lpts pifib hardware domain ACCESS

LPTS ハードウェア ドメイン コンフィギュレーション モードを開始します。

2. Router(config-pifib-domain-ACCESS)# interface TenGigE0/0/0/8/1
TenGigE0/0/0/8/1 インターフェイスノードに、ドメインアクセスを適用します。
3. Router(config-pifib-domain-ACCESS)# exit
LPTS ドメインモードを終了します。
4. Router(config)# lpts punt police location 0/0/CPU0
LPTS パント ポリサー コンフィギュレーション モードを開始します。
5. Router(config-lpts-punt-policer)# protocol arp rate 500
ARP プロトコルパケットに 500 pps のレート制限を設定します。
6. Router(config-lpts-punt-policer)# protocol cdp rate 500
CDP プロトコルパケットに 500 pps のレート制限を設定します。
7. Router(config-lpts-punt-policer)# exit
LPTS パント ポリサー コンフィギュレーション モードを終了します。
8. Router(config)# lpts punt police location 0/4/CPU0
ノードロケーション 0/4/CPU0 で LPTS パントポリシングを設定します。
9. Router(config)# commit
設定をコミット

ランニング コンフィギュレーション

```
lpts punt police
interface TenGigE0/0/0/8/0
  mcast rate 1000
  bcast rate 1000
!
mcast rate 1000
bcast rate 1000
protocol arp rate 700
protocol cdp rate 700
domain ACCESS
  mcast rate 5000
  bcast rate 5000
!
!
lpts pifib hardware domain ACCESS
interface TenGigE0/0/0/8/1
!
lpts punt police location 0/0/CPU0
protocol arp rate 500
protocol cdp rate 500
!
lpts punt police location 0/4/CPU0
!
```


確認

次の show コマンドの出力では、ドメインでのレート制限の設定を確認するための強調表示されたフィールドと、インターフェイスレベルを確認する必要があります。

```
Router# show lpts punt statistics location 0/0/CPU0
Fri Nov 15 06:23:20.410 UTC

Lpts Punt Policer Statistics:
-----
Punt_Reason - Ingress Packets type to be Punt policed
Scope      - Configured scope - Global/Domain/IFH
State      - Current config state
Rate       - Policer rate in PPS
Accepted   - No of Packets Accepted
Dropped    - No of Packets Dropped
Domain     - Domain name
-----

Interface Name      : any
Punt Reason       : ARP
Domain           : ACCESS
Scope              : Default
State              : Active
Configured Rate   : 1000
Operational Rate   : 986
Accepted           : 0
Dropped            : 0
Last Update (if any):
Punt Type          : ARP
Interface Handle    : 0x00000000
Is Virtual          : 0
Is Enabled          : 1
Packet Rate        : 1000
Domain              : 1
CreateTime         : Fri Nov 15 2019 06:22:42.237.188
Platform:
  PolicerID        : 32398
  NPU: TCAM-entry   StatsID
    0:              172 0x80001d54
    1:              297 0x80001dd0
    2:              172 0x80001d54
    3:              172 0x80001d54
    4:              172 0x80001d54
    5:              172 0x80001d54
-----

Interface Name      : any
Punt Reason       : CDP
Domain           : ACCESS
Scope              : Default
State              : Active
Configured Rate   : 1000
Operational Rate   : 986
Accepted           : 0
Dropped            : 0
Last Update (if any):
Punt Type          : CDP
Interface Handle    : 0x00000000
Is Virtual          : 0
Is Enabled          : 1
Packet Rate        : 1000
Domain              : 1
CreateTime         : Fri Nov 15 2019 06:22:42.258.192
```

```

Platform:
  PolicerID      : 32404
  NPU: TCAM-entry  StatsID
    0:           173 0x80001d55
    1:           298 0x80001dd1
    2:           173 0x80001d55
    3:           173 0x80001d55
    4:           173 0x80001d55
    5:           173 0x80001d55
-----
Interface Name      : any
Punt Reason       : ARP
Domain              : default
Scope               : Local
State               : Active
Configured Rate    : 500
Operational Rate    : 515
Accepted            : 980
Dropped             : 0
Last Update (if any):
Punt Type           : ARP
Interface Handle     : 0x00000000
Is Virtual          : 0
Is Enabled           : 1
Packet Rate         : 500
Domain              : 0
CreateTime          : Tue Nov 12 2019 06:31:25.136.800
Platform:
  PolicerID      : 32306
  NPU: TCAM-entry  StatsID
    0:           41 0x80001cd2
    1:           41 0x80001cd2
    2:           41 0x80001cd2
    3:           41 0x80001cd2
    4:           41 0x80001cd2
    5:           41 0x80001cd2
-----
Interface Name      : any
Punt Reason       : CDP
Domain              : default
Scope               : Local
State               : Active
Configured Rate     : 500
Operational Rate    : 515
Accepted            : 4292
Dropped             : 0
Last Update (if any):
Punt Type         : CDP
Interface Handle     : 0x00000000
Is Virtual          : 0
Is Enabled           : 1
Packet Rate       : 500
Domain              : 0
CreateTime          : Tue Nov 12 2019 06:31:25.513.897
Platform:
  PolicerID      : 32312
  NPU: TCAM-entry  StatsID
    0:           42 0x80001cd3
    1:           42 0x80001cd3
    2:           42 0x80001cd3
    3:           42 0x80001cd3
    4:           42 0x80001cd3
    5:           42 0x80001cd3
-----

```

```

-----
Interface Name      : TenGigE0
Punt Reason         : MCAST
Domain              : default
Scope               : Global
State               : Active
Configured Rate     : 1000
Operational Rate    : 986
Accepted            : 0
Dropped             : 0
Last Update (if any):
Punt Type           : MCAST
Interface Handle    : 0x0800001c
Is Virtual          : 1
Is Enabled          : 1
Packet Rate         : 1000
Domain              : 0
CreateTime          : Tue Nov 12 2019 06:32:43.210.014
Platform:
  PolicerID         : 32396
  NPU: TCAM-entry   StatsID
    0:               170 0x80001d52
    1:               172 0x80001d53
    2:               170 0x80001d52
    3:               170 0x80001d52
    4:               170 0x80001d52
    5:               170 0x80001d52
-----
Interface Name      : TenGigE0
Punt Reason         : BCAST
Domain              : default
Scope               : Global
State               : Active
Configured Rate     : 1000
Operational Rate    : 986
Accepted            : 0
Dropped             : 0
Last Update (if any):
Punt Type           : BCAST
Interface Handle    : 0x0800001c
Is Virtual          : 1
Is Enabled          : 1
Packet Rate         : 1000
Domain              : 0
CreateTime          : Tue Nov 12 2019 06:32:43.227.279
Platform:
  PolicerID         : 32397
  NPU: TCAM-entry   StatsID
    0:               171 0x80001d53
    1:               173 0x80001d54
    2:               171 0x80001d53
    3:               171 0x80001d53
    4:               171 0x80001d53
    5:               171 0x80001d53
-----

```

ドメインベースの LPTS ポリサー

単一ドメインの LPTS ポリサーを使用して、ルータの特定のポート、ポートのグループ、またはラインカードを設定できます。特定のドメインに属するポートベースのポリサーを設定すると、さまざまなタイプの入力トラフィックの適切な分類および制御が可能になります。たとえば、iBGP トラフィックはトラフィックフローのレートが高いため、iBGP トラフィックを処理するポートは、eBGP トラフィックを処理するポートに比べて高いポリサーレートで設定できます。

制約事項

- ポートまたはラインカードに対して設定されたポリサーレートは、ドメインの一部としてポートまたはラインカードが設定された後に、ドメインのポリサーレートとして転送されます。たとえば、ポート `hundredGigE 0/0/0/1` およびポート `hundredGigE 0/0/0/2` に `ospf` ユニキャストの既知のフローとしてポリサーレート 3000 が設定され、ポートがドメインコアの一部として設定されている場合、`ospf` ユニキャストの既知のフローにおけるドメインコアのポリサーレートは、特に設定されていない限り 3000 です。
- ルータごとに 1 つのドメインのみを設定できます。
- ドメイン名には任意の単語を使用できますが、最大 32 文字までです。

設定例

LPTS のドメインベースのポリサーを設定するには、次の手順を実行します。

1. LPTS ハードウェア コンフィギュレーション モードを開始し、ドメインを作成します。
2. ドメインのインターフェイスを設定します。
3. ドメインコアの LPTS ハードウェア コンフィギュレーション モードを開始し、グローバルレベルでドメインコアの入力ポリサーレートを設定します。
4. ドメインコアの LPTS ハードウェア コンフィギュレーション モードを開始し、ラインカードレベルでドメインコアの入力ポリサーレートを設定します。

設定

```
/* Enter the LPTS hardware ingress policer configuration mode and create a domain named CORE. */
Router# config
Router(config)# lpts pifib hardware domain CORE

/* Configure the interfaces for the domain CORE. */
Router(config-lpts-domains-CORE)# interface hundredGigE 0/0/0/1
Router(config-lpts-domains-CORE)# interface hundredGigE 0/0/0/2
Router(config-lpts-domains-CORE)# commit
Router(config-lpts-domains-CORE)# exit

/* Enter the LPTS hardware configuration mode for the domain CORE, and then configure the ingress policer rates for the domain CORE at the global level. */
```

```

Router(config)# lpts pifib hardware police domain CORE
Router(config-lpts-policer-global-CORE)# flow ospf unicast known rate 6000
Router(config-lpts-policer-global-CORE)# flow ospf unicast default rate 7000
Router(config-lpts-policer-global-CORE)# commit
Router(config-lpts-policer-global-CORE)# exit
Router(config-lpts-policer-global)# exit

/* Enter the LPTS hardware configuration mode for the domain CORE, and then configure
the ingress policer rates for the domain CORE at the line card level. */
Router(config)# lpts pifib hardware police location 0/0/CPU0 domain CORE
Router(config-lpts-policer-global-CORE)# flow ospf unicast known rate 7000
Router(config-lpts-policer-global-CORE)# flow ospf unicast default rate 8000
Router(config-lpts-policer-global-CORE)# commit

```

実行コンフィギュレーション

```

lpts pifib hardware domain CORE
  interface HundredGigE0/0/0/1
  interface HundredGigE0/0/0/2
!
lpts pifib hardware police
  domain CORE
    flow ospf unicast known rate 6000
    flow ospf unicast default rate 7000
!

lpts pifib hardware police location 0/0/CPU0 domain CORE
  flow ospf unicast known rate 7000
  flow ospf unicast default rate 8000
!

```

確認

設定された LPTS ドメインの情報を確認するには、次のコマンドを使用します。

```

Router# show lpts pifib domains
Thu Nov 21 15:49:31.334 IST

Domains Information: 1 Configured
-----
Domain: [1] CORE
-----
interface [-----] HundredGigE0/0/0/1
interface [-----] HundredGigE0/0/0/2
                  0 local of total 2 interfaces

```

ダイナミック LPTS フロー タイプの定義

ダイナミック LPTS フロー タイプ機能を使用すると、LPTS フロー タイプを設定できるとともに、TCAM 内の各フロー タイプの最大 LPTS エントリ数を定義できます。ダイナミック LPTS フロー タイプの設定はラインカードごとに行うため、複数のラインカードにわたって複数のプロファイルを設定できます。

ルータが起動すると、デフォルトの LPTS フロータイプが TCAM でプログラミングされます。フロータイプそれぞれに、最大フロー エントリ数が事前に定義されています。後で、実行時にネットワーク要件に基づいてフロータイプを選択し、最大フロー エントリ値も設定するオ

プシオンがあります。最大フロー エントリ値ゼロは、フロー タイプが設定されていないことを示します。



- (注) 設定可能なフローと設定不能なフローの両方のデフォルト最大フロー値は、次の show コマンドの出力で確認できます。

```
show lpts pifib dynamic-flows statistics location <location specification>
```

設定可能なフロー タイプと設定不能なフロー タイプのリストを次の表に示します。また、設定可能なフロー タイプと設定不能なフロー タイプのリストを表示するには、**show lpts pifib dynamic-flows statistics location** コマンドも使用できます。



- (注) すべてのフロー タイプに設定される最大 LPTS エントリの総数は、ライン カードあたり 8,000 エントリを超えないものとします。

設定例

次の例では、TCAM に BGP-known と ISIS-known の LPTS フロー タイプを設定し、ノード ロケーション 0/1/CPU0 に最大フロー エントリ 1800 と 500 を定義します。新しい最大値がデフォルト値を超えているため、他のフロー タイプを無効にして TCAM 内にスペースを作成し、ラインカードあたりのすべてのフロー タイプの最大エントリ総数を 8,000 エントリを超えないようにする必要があります。そのため、次の例では RSVP-known フロー タイプがゼロに設定されています。

```
Router#configure
Router(config)#lpts pifib hardware dynamic-flows location 0/1/CPU0
Router(config-pifib-flows-per-node)#flow bgp-known max 1800
Router(config-pifib-flows-per-node)#flow ISIS-known max 500
Router(config-pifib-flows-per-node)#flow RSVP-known max 0
Router(config-pifib-flows-per-node)#commit
```

実行コンフィギュレーション

```
Router#show run lpts pifib hardware dynamic-flows location 0/1/CPU0
flow bgp known max 1800
flow isis-known 500
flow RSVP-known 0
```

確認

次の show コマンドは、ダイナミック フローの統計情報を表示します。フロー タイプの BGP-known と ISIS-known が新たに設定した最大フロー エントリ値で TCAM に設定されていることを確認できます。また、RSVP-known フロー タイプが無効になっていることも確認できます。

```
Router#show lpts pifib dynamic-flows statistics location 0/1/CPU0
```

```
Dynamic-flows Statistics:
-----
```

(C - Configurable, T - TRUE, F - FALSE, * - Configured)

Def_Max - Default Max Limit

Conf_Max - Configured Max Limit

HWCnt - Hardware Entries Count

ActLimit - Actual Max Limit

SWCnt - Software Entries Count

P, (+) - Pending Software Entries

| FLOW-TYPE | C | Def_Max | Conf_Max | HWCnt/ActLimit | SWCnt P |
|-------------------|----------|------------|-------------|-----------------|----------|
| Fragment | F | 2 | -- | 2/2 | 2 |
| OSPF-mc-known | T | 600 | -- | 2/600 | 2 |
| OSPF-mc-default | F | 4 | -- | 4/4 | 4 |
| OSPF-uc-known | T | 300 | -- | 1/300 | 1 |
| OSPF-uc-default | F | 2 | -- | 2/2 | 2 |
| ISIS-known | T | 300 | 500 | 500/300 | 0 |
| ISIS-default | F | 1 | -- | 1/1 | 1 |
| BGP-known | T | 900 | 1800 | 1800/900 | 0 |
| BGP-cfg-peer | T | 900 | -- | 0/900 | 0 |
| BGP-default | F | 4 | -- | 4/4 | 4 |
| PIM-mcast-default | F | 40 | -- | 0/40 | 0 |
| PIM-mcast-known | T | 300 | -- | 0/300 | 0 |
| PIM-ucast | F | 40 | -- | 2/40 | 2 |
| IGMP | T | 1200 | -- | 0/1200 | 0 |
| ICMP-local | F | 4 | -- | 4/4 | 4 |
| ICMP-control | F | 5 | -- | 5/5 | 5 |
| ICMP-default | F | 9 | -- | 9/9 | 9 |
| ICMP-app-default | F | 2 | -- | 2/2 | 2 |
| LDP-TCP-known | T | 300 | -- | 0/300 | 0 |
| LDP-TCP-cfg-peer | T | 300 | -- | 0/300 | 0 |
| LDP-TCP-default | F | 40 | -- | 0/40 | 0 |
| LDP-UDP | T | 300 | -- | 0/300 | 0 |
| All-routers | T | 300 | -- | 0/300 | 0 |
| RSVP-default | F | 4 | -- | 1/4 | 1 |
| RSVP-known | T | 300 | 0 | 0/300 | 0 |
| SNMP | T | 300 | -- | 0/300 | 0 |
| SSH-known | T | 150 | -- | 0/150 | 0 |
| SSH-default | F | 40 | -- | 0/40 | 0 |
| TELNET-known | T | 150 | -- | 0/150 | 0 |
| TELNET-default | F | 4 | -- | 0/4 | 0 |
| UDP-default | F | 2 | -- | 2/2 | 2 |
| TCP-default | F | 2 | -- | 2/2 | 2 |
| Raw-default | F | 2 | -- | 2/2 | 2 |
| GRE | F | 4 | -- | 0/4 | 0 |
| VRRP | T | 150 | -- | 150/150 | 0 |
| DNS | T | 40 | -- | 0/40 | 0 |
| NTP-default | F | 4 | -- | 0/4 | 0 |
| NTP-known | T | 150 | -- | 0/150 | 0 |
| TPA | T | 5 | -- | 0/5 | 0 |

Local Limit : **7960**/8000 /*The sum of maximum flow entries configured for all flow types

per line card is less than 8000*/

HWCnt/SWCnt : 45/51

上記の show コマンド出力では、最後の列の **P** でそのフロー タイプの保留中ソフトウェアフロー エントリを指定します。



第 10 章

VRRP の実装

- [VRRP の設定 \(191 ページ\)](#)
- [VRRP のマルチ グループ オプティマイゼーション \(MGO\) の有効化 \(197 ページ\)](#)
- [VRRP イベントに関する SNMP サーバ通知の設定 \(198 ページ\)](#)
- [VRRP の概要 \(199 ページ\)](#)

VRRP の設定

仮想ルータ冗長プロトコル (VRRP) 機能を使用すると、ファーストホップ IP ルータでの透過的なフェールオーバーが可能になり、ルータ グループが単一の仮想ルータを形成できるようになります。VRRP と関連する概念の詳細については、次を参照してください。 [VRRP の概要 \(199 ページ\)](#)

VRRP 設定の制約事項

- VRRP を介した Bidirectional Forwarding Detection (BFD) はサポートされていません。
- ICMP リダイレクトはサポートされていません。
- サポートされている VRRP の最大数は 16 のみですが、このスケール数は、BFD、BVIV4、および V6 の設定に基づいて、さらに変化したり減少したりする場合があります。たとえば、BFD が設定されている場合、値は $16 - 1 = 15$ になります。BVI v4 と BVI v6 も BFD とともに設定されている場合、値は $16 - 3 = 13$ のみです。

VRRP のカスタマイズ

設定例

VRRP の動作のカスタマイズはオプションです。VRRP グループをイネーブルにするとすぐに、そのグループは動作を開始することに注意してください。VRRP をカスタマイズする前に、VRRP グループをイネーブルにした場合、機能のカスタマイズが完了しないうちに、ルータがそのグループの制御をテイクオーバーし、マスター仮想ルータになる可能性があります。この

ため、VRRPをカスタマイズする場合には、カスタマイズを行ってからVRRPをイネーブルにすることを推奨します。

```
Router#configure
Router(config)#router vrrp
router(config-vrrp)#interface TenGigE 0/0/0/2

router(config-vrrp)#delay minimum 2 reload 10
/* (Optional) Delays the startup of the state machine when an interface comes up. */

router(config-vrrp-if)#address-family ipv6
router(config-vrrp-address-family)#vrrp 3
/* The version keyword is available only if IPv4 address-family is selected. */

router(config-vrrp-virtual-router)#text-authentication text1
/* (Optional) Configures the simple text authentication used for VRRP packets received
from other routers running VRRP. */

router(config-vrrp-virtual-router)#accept-mode disable
/* Disables the installation of routes for the VRRP virtual addresses. */

router(config-vrrp-virtual-router)#priority 254
/* (Optional) Sets the priority of the virtual router. */

router(config-vrrp-virtual-router)#preempt delay 15
/* (Optional) Controls which router becomes the master router. */

router(config-vrrp-virtual-router)#timer 4
/* (Optional) Configures the interval between successive advertisements by the master
router in a VRRP virtual router. */

router(config-vrrp-virtual-router)#track interface TenGigE 0/0/0/2 30
/* (Optional) Configures the VRRP to track an interface. */

router(config-vrrp-virtual-router)#commit
```

実行コンフィギュレーション

```
Router#show running-config router vrrp
router vrrp
interface TenGigE 0/0/0/2
delay minimum 2 reload 10
address-family ipv6
vrrp 3
text-authentication
accept-mode disable
priority 254
preempt delay 15
timer 4
track interface TenGigE 0/0/0/2 30
!
```

確認

```
Router#show vrrp detail

TenGigE0/0/0/2 - IPv4 vrID 3
  State is Master, IP address owner
    1 state changes, last state change 00:01:00
  State change history:
    May 19 12:28:59.825 UTC  Init      -> Master  Virtual IP configured
```

```

Last resign sent:      Never
Last resign received: Never
Virtual IP address is 10.0.0.1
Virtual MAC address is 0000.5E00.0103, state is active
Master router is local
Version is 2
Advertise time 4 secs
Master Down Timer 12.015 (3 x 4 + (1 x 4/256))
Minimum delay 2 sec, reload delay 10 sec
Current priority 255
Configured priority 254, may preempt
minimum delay 15 secs
Authentication enabled, string "text1"
Tracked items: 1/1 up: 30 decrement

```

| Object name | State | Decrement |
|----------------|-------|-----------|
| TenGigE0/0/0/2 | Up | 30 |

VRRPのイネーブル化

設定例

```

Router#configure
Router(config)#router vrrp
router(config-vrrp)#interface TenGigE 0/0/0/2
router(config-vrrp-if)#address-family ipv4
router(config-vrrp-address-family)#vrrp 3 version 3
/* The version keyword is available only if IPv4 address-family is selected. */

router(config-vrrp-virtual-router)#address 10.20.30.1
/* Enables VRRP on an interface and specifies the IP address of the virtual router. */

router(config-vrrp-virtual-router)#commit

```

実行コンフィギュレーション

```

Router#show running-config router vrrp
router vrrp
interface TenGigE 0/0/0/2
address-family ipv4
vrrp 3 version 3
address 10.20.30.1
!

```

確認

```

Router#show vrrp detail

TenGigE0/0/0/2 - IPv4 vrID 3
State is Master, IP address owner
1 state changes, last state change 00:01:00
State change history:
May 19 12:28:59.825 UTC Init -> Master Virtual IP configured
Last resign sent:      Never
Last resign received: Never
Virtual IP address is 10.20.30.1
Virtual MAC address is 0000.5E00.0103, state is active
Master router is local

```

```

Version is 2
Advertise time 4 secs
  Master Down Timer 12.015 (3 x 4 + (1 x 4/256))
Current priority 255

```

VRRP 統計情報のクリア

指定の仮想ルータの全ソフトウェア カウンタを消去します。

```

Router#clear vrrp statistics
/* If no interface is specified, statistics of all virtual routers are removed. */

```

グローバル仮想 IPv6 アドレスの設定

設定例

仮想ルータのグローバル仮想 IPv6 アドレスを設定します。

```

Router#configure
Router(config)#router vrrp
router(config-vrrp)#interface TenGigE 0/0/0/2
router(config-vrrp-if)#address-family ipv6
router(config-vrrp-address-family)#vrrp 3
/* The version keyword is available only if IPv4 address-family is selected. */

router(config-vrrp-if-virtual-router)#address global 2001:db8::/32
router(config-vrrp-virtual-router)#commit

```

実行コンフィギュレーション

```

Router#show running-config router vrrp
router vrrp
interface TenGigE 0/0/0/2
address-family ipv6
vrrp 3
address global 2001:db8::/32
!

```

プライマリおよびセカンダリの仮想 IPv4 アドレスの設定

設定例

```

Router#configure
Router(config)#router vrrp
router(config-vrrp)#interface TenGigE 0/0/0/2
router(config-vrrp-if)#address-family ipv4
router(config-vrrp-address-family)#vrrp 3 version 3
/* The version keyword is available only if IPv4 address-family is selected. */

router(config-vrrp-if-virtual-router)#address 10.20.30.1
/* Configures primary virtual IPv4 address for a virtual router. */

router(config-vrrp-if-virtual-router)#address 10.20.30.2 secondary

```

```
/* Configures secondary virtual IPv4 address for a virtual router. */  
  
router(config-vrrp-virtual-router)#commit
```

実行コンフィギュレーション

```
Router#show running-config router vrrp  
router vrrp  
interface TenGigE 0/0/0/2  
address-family ipv4  
vrrp 3 version 3  
address 10.20.30.1  
address 10.20.30.2 secondary  
!
```

確認

```
Router#show vrrp detail  
  
TenGigE0/0/0/2 - IPv4 vrID 3  
State is Master, IP address owner  
  1 state changes, last state change 00:01:00  
State change history:  
  May 19 12:28:59.825 UTC  Init      -> Master   Virtual IP configured  
Last resign sent:      Never  
Last resign received: Never  
Virtual IP address is 10.20.30.1  
Virtual MAC address is 0000.5E00.0103, state is active  
Master router is local  
Virtual secondary IP address is 10.20.30.2  
Version is 2  
Advertise time 4 secs  
  Master Down Timer 12.015 (3 x 4 + (1 x 4/256))  
Current priority 255
```

仮想リンクローカル IPv6 アドレスの設定

仮想ルータの仮想リンクローカル IPv6 アドレスを設定するか、または仮想リンクローカル IPv6 アドレスが有効になっており、仮想ルータの仮想 MAC アドレスから自動的に計算されることを指定します。

IPv6 アドレス空間は、IPv4 に比べて異なる構造になっています。リンクローカルアドレスは、ローカルネットワーク上の各インターフェイスを識別するために使用します。これらのアドレスは、インターフェイスのリンクローカル（ハードウェア）アドレス（イーサネットインターフェイスの MAC アドレス）を使用して、標準の方法で設定または決定されます。リンクローカルアドレスは、標準の形式を持ち、ローカルネットワークでのみ有効です（複数ホップ先とのルーティングは実行できません）。

グローバルユニキャスト IPv6 アドレスは、IPv6 アドレス空間で、リンクローカルアドレスから分離したサブセットを占有します。これらは、複数ホップ先と相互にルーティングでき、関連付けられたプレフィックス長（0 ～ 128 ビット）を持ちます。

各 VRRP 仮想ルータには、関連付けられた仮想リンクローカルアドレスがあります。これは、仮想ルータの仮想 MAC アドレスから自動的に設定および決定されます。仮想 MAC アドレスは、ローカル ネットワークで一意である必要があります。仮想リンクローカルアドレスは、スコープがローカルのアドレスでは重複アドレス検出が不要であるため、その仮想 IP (VIP) 状態がアップであることが常に考慮される点を除き、IPv4 仮想ルータのプライマリ仮想 IPv4 アドレスに似ています。

設定例

```
Router#configure
Router(config)#router vrrp
router(config-vrrp)#interface TenGigE 0/0/0/2
router(config-vrrp-if)#address-family ipv6

/* Use one of the following address linklocal commands: */
router(config-vrrp-address-family)#vrrp 1 address linklocal FE80::260:3EFF:FE11:6770
/* Configures the virtual link-local IPv6 address for the virtual router. */

router(config-vrrp-address-family)#vrrp 1 address linklocal autoconfigure
/* Specifies that the virtual link-local IPv6 address should be enabled and calculated
automatically
from the virtual router virtual MAC address. */

router(config-vrrp-virtual-router)#commit
```

実行コンフィギュレーション

```
Router#show running-config router vrrp
router vrrp
interface TenGigE 0/0/0/2
address-family ipv6
vrrp 1 address linklocal FE80::260:3EFF:FE11:6770
!
```

状態変更ロギングのディセーブル化

設定例

syslog を介して VRRP 状態変更イベントをロギングするタスクをディセーブルにします。

```
Router#configure
Router(config)#router vrrp
router(config-vrrp)#message state disable
router(config-vrrp)#commit
```

VRRPのマルチグループオプティマイゼーション (MGO) の有効化

設定例

Virtual Router Redundancy Protocol (VRRP) のマルチ グループ オプティマイゼーションは、多くのサブインターフェイスから構成される導入環境で制御トラフィックを削減するためのソリューションです。VRRP 制御トラフィックの実行を1つのセッションに制限することにより、冗長性要求が同一のサブインターフェイスに対して制御トラフィックが減少します。他のすべてのセッションはこのプライマリ セッションのスレーブになり、プライマリ セッションから状態を継承します。

VRRP セッション名

```
Router#configure
Router(config)#router vrrp
router(config-vrrp)#interface TenGigE 0/0/0/2
router(config-vrrp-if)#address-family ipv4
router(config-vrrp-address-family)#vrrp 1
/* Enables VRRP group configuration mode on a specific interface. */

router(config-vrrp-vritual-router)#name s1
/* Specifies the VRRP session name. */

router(config-vrrp-gp)#commit
```

Slave Follow

```
Router#configure
Router(config)#router vrrp
router(config-vrrp)#interface TenGigE 0/0/0/2
router(config-vrrp-if)#address-family ipv4

router(config-vrrp-address-family)#vrrp 2 slave
/* Enables VRRP slave configuration mode on a specific interface. */

router(config-vrrp-slave)#follow m1
/* Configures a slave follow. Instructs the slave group to inherit its state from the
specified group, m1 (MGO session name). */

router(config-vrrp-slave)#address 10.2.3.2
/* Specifies the primary virtual IPv4 address for slave group. */

router(config-vrrp-slave)#address 10.2.3.3 secondary
/* Specifies the secondary virtual IPv4 address for slave group. */

router(config-vrrp-gp)#commit
```

スレーブ グループのライマリおよびセカンダリの仮想 IPv4 アドレス

```
Router#configure
Router(config)#router vrrp
router(config-vrrp)#interface TenGigE 0/0/0/2
router(config-vrrp-if)#address-family ipv4

router(config-vrrp-address-family)#vrrp 2 slave
```

```

/* Enables VRRP slave configuration mode on a specific interface. */

router(config-vrrp-slave)#address 10.2.3.2
/* Specifies the primary virtual IPv4 address for slave group. */

router(config-vrrp-slave)#address 10.2.3.3 secondary
/* Specifies the secondary virtual IPv4 address for slave group. */

router(config-vrrp-slave)#commit

```

実行コンフィギュレーション

```

Router#show running-config router vrrp 1
router vrrp
interface TenGigE 0/0/0/2
address-family ipv4
vrrp 1
name s1
!

/* Slave group */
Router#show running-config router vrrp 2
router vrrp
interface TenGigE 0/0/0/2
address-family ipv4
vrrp 2 slave
follow m1
address 10.2.3.2
address 10.2.3.3 secondary
!

```

VRRP イベントに関する SNMP サーバ通知の設定

MIB の VRRP サポート

VRRPを使用すると、障害が発生したとき、ルータが1つ以上のIPアドレスを引き継ぐことができます。たとえば、障害の発生したルータがデフォルトゲートウェイであったために、ホストからのIPトラフィックがそのルータに到達した場合、そのトラフィックは制御を引き継いだVRRPルータによって透過的に転送されます。VRRPを使用する場合、ダイナミックルーティングやルータディスカバリプロトコルの設定を各エンドホストで行う必要はありません。仮想ルータに割り当てるIPアドレスを制御するVRRPルータはマスターと呼ばれ、送信されたパケットをそれらのIPアドレスに転送します。この選択プロセスにより、マスターが使用不可になった場合の転送責任のダイナミックフェールオーバー（スタンバイ）が提供されます。これにより、LAN上の仮想ルータIPアドレスをデフォルトの最初のホップルータとしてエンドホストが使用するようにできます。

VRRPを使用することで得られるメリットは、ダイナミックルーティングやRouter Discovery Protocolをエンドホストごとに設定する必要なく、デフォルトパスの可用性が向上することです。Simple Network Management Protocol (SNMP)トラップは、仮想ルータ（スタンバイ）がマスター状態に移行した場合、またはスタンバイルータがマスターになった場合に、状態変更に関する情報を提供します。

設定例

VRRP に対して SNMP サーバ通知（トラップ）を有効にします。

```
Router#configure
Router(config)#snmp-server traps vrrp events
router(config)#commit
```

SNMP サーバ通知の詳細を表示するには、**show snmp traps details** コマンドを使用します。

VRRP の概要

仮想ルータ冗長プロトコル（VRRP）機能を使用すると、ファーストホップ IP ルータでの透過的なフェールオーバーが可能になり、ルータグループが単一の仮想ルータを形成できるようになります。



(注) VRRP は VRF でサポートされています。

VRRP の概要

LAN クライアントは、動的プロセスまたは静的設定を使用して、特定のリモート宛先への最初のホップとなるルータを決定します。次に、ダイナミック ルータ ディスカバリのクライアント例を示します。

- プロキシ ARP：クライアントはアドレス解決プロトコル（ARP）を使用して到達すべき宛先を取得します。ルータは独自の MAC アドレスで ARP 要求に応答します。
- ルーティング プロトコル：クライアントはダイナミック ルーティング プロトコルのアップデートを（ルーティング情報プロトコル（RIP）などから）受信し、独自のルーティング テーブルを形成します。
- IRDP（ICMP Router Discovery Protocol）クライアント：クライアントはインターネット制御メッセージ プロトコル（ICMP）ルータ ディスカバリ クライアントを実行します。

ダイナミック ディスカバリ プロトコルには、LAN クライアントにおいて、設定および処理のオーバーヘッドが発生するという短所があります。また、ルータが機能を停止したときに、別のルータへの切り替え処理が遅くなる可能性があります。

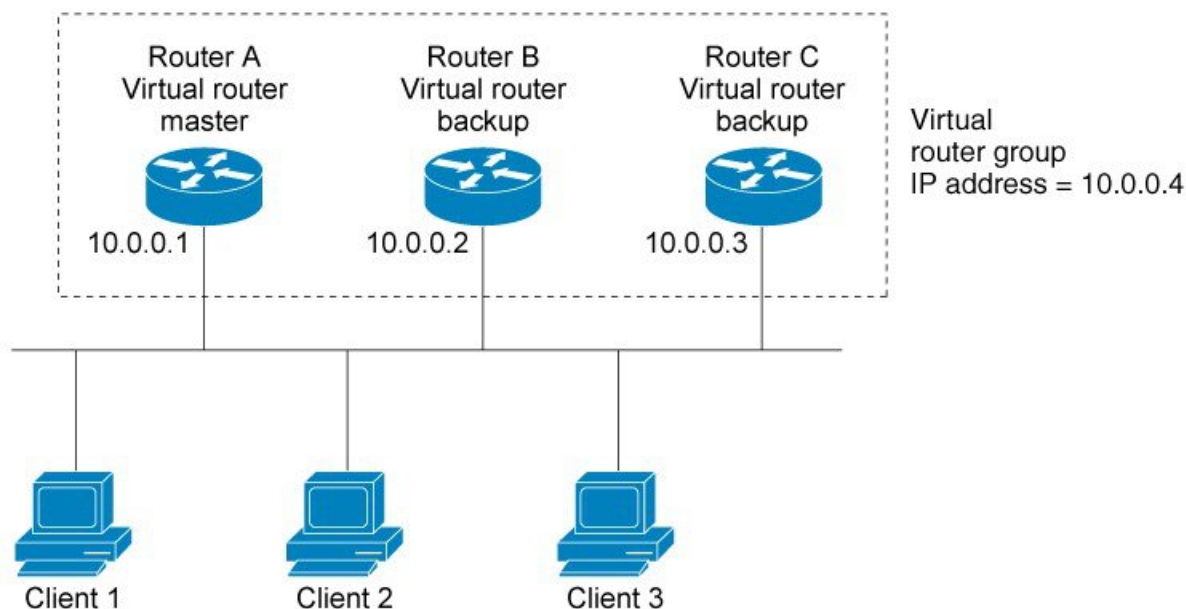
ダイナミック ディスカバリ プロトコルの代わりに、クライアント上でデフォルト ルータをスタティックに設定することもできます。このアプローチでは、クライアントの設定と処理は簡略化されますが、単一障害点が生じます。デフォルト ゲートウェイで障害が発生した場合、LAN クライアントの通信はローカル IP ネットワーク セグメントに限定され、ネットワークの他の部分から切り離されます。

仮想ルータ冗長プロトコル（VRRP）機能により、この静的設定の問題を解決できます。VRRP は、ファーストホップ IP ルータの透過的なフェールオーバーを可能にするように設計された IP ルーティング冗長プロトコルです。VRRP を使用すると、ルータのグループで 1 つの仮想ルータを形成できます。これにより、仮想ルータをデフォルト 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。ルータのグループを表す仮想ルータは、**VRRP** グループとも呼ばれます。

例として、[図 15: 基本的な VRRP トポロジ \(200 ページ\)](#) に、VRRP が設定された LAN トポロジを示します。この例では、ルータ A、B、および C は仮想ルータで構成される **VRRP** ルータ (VRRP を実行するルータ) です。仮想ルータの IP アドレスは、ルータ A のインターフェイスに設定されたアドレス (10.0.0.1) と同じです。

図 15: 基本的な VRRP トポロジ



仮想ルータはルータ A の物理インターフェイスの IP アドレスを使用するため、ルータ A はマスター仮想ルータのロールを担い、**IP** アドレス所有者とも呼ばれます。ルータ A は、マスター仮想ルータとして、仮想ルータの IP アドレスを管理し、この IP アドレスに送信されたパケットの転送を行います。クライアント 1～3 には、デフォルトゲートウェイの IP アドレス 10.0.0.1 が設定されています。

ルータ B および C は、バックアップ仮想ルータとして機能します。マスター仮想ルータに障害が発生すると、高いプライオリティが設定されているルータがマスター仮想ルータになり、LAN ホストに対して中断なくサービスが提供されます。ルータ A は、回復すると、再びマスター仮想ルータになります。



(注) 仮想ルータが接続されているスイッチポートでは、スパニングツリープロトコル (STP) を無効にすることをお勧めします。スイッチがこれらのプロトコルをサポートしている場合に、RSTP または rapid-PVST を有効にします。

複数の仮想ルータのサポート

ルータ インターフェイスには、最大 100 の仮想ルータを設定できます。ルータ インターフェイスには、最大 256 の仮想ルータを設定できます。ルータ インターフェイスがサポートできる実際の仮想ルータの数は、次の要因によって異なります。

- ルータの処理能力
- ルータのメモリの能力
- 複数の MAC アドレスのルータ インターフェイス サポート

1つのルータ インターフェイス上に複数の仮想ルータが設定されているトポロジでは、そのインターフェイスは 1 つ以上の仮想ルータのマスター、および 1 つ以上の仮想ルータのバックアップとして動作することができます。

VRRP ルータ プライオリティ

VRRP 冗長性スキームの重要な一面に、VRRP ルータ プライオリティがあります。プライオリティにより、各 VRRP ルータが果たすロールと、マスター仮想ルータ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。

VRRP ルータが仮想ルータの 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、このルータがマスター仮想ルータとして機能します。

IP アドレスのオーナーである VRRP ルータが存在しない場合は、VRRP ルータのプライオリティおよびプリエンプション設定の組み合わせにより、VRRP ルータがマスターとして機能するか、またはバックアップ仮想ルータとして機能するかが決まります。デフォルトでは、最高のプライオリティを持つ VRRP ルータがマスターとして機能し、その他のすべてがバックアップとして機能します。プライオリティにより、マスター仮想ルータが機能を停止した場合にマスター仮想ルータになる優先順位も決まります。vrrp priority コマンドを使用して 1 ～ 254 の値を設定し、各バックアップ仮想ルータのプライオリティを設定できます。

たとえば、LAN トポロジのマスター仮想ルータであるルータ A が機能を停止した場合、選択プロセスが実行されて、バックアップ仮想ルータ B または C が引き継ぐかどうか決定されます。ルータ B とルータ C がそれぞれプライオリティ 101 と 100 に設定されている場合、プライオリティの高いルータ B がマスター仮想ルータになります。ルータ B とルータ C が両方ともプライオリティ 100 に設定されている場合、IP アドレスがより高いバックアップ仮想ルータが選択されてマスター仮想ルータになります。

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おり、使用可能になった高いプライオリティのバックアップ仮想ルータが、現在のマスター仮想ルータから引き継ぎます。このプリエンプティブスキームを無効にするには、vrrp preempt disable コマンドを使用します。プリエンプションが無効になっている場合、元のプライオリティがより高いマスターの障害時にマスターになるように選択されたバックアップ仮想ルータは、元のマスター仮想ルータが回復して再び使用可能になっても、マスターのままとなります。

VRRPのアドバタイズメント

マスター仮想ルータは、同じグループ内の他のVRRPルータに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、マスター仮想ルータのプライオリティと状態を伝えます。VRRPアドバタイズメントはIP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IPバージョン4マルチキャストアドレスに送信されます。アドバタイズメントは、デフォルトで1秒に1回送信されますが、この間隔は設定可能です。

VRRPの利点

VRRPの利点は、次のとおりです。

- 冗長性：VRRPにより、複数のルータをデフォルトゲートウェイルータとして設定できるようになるため、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クライアントとの間のトラフィックを複数のルータで共有するようにVRRPを設定できるため、利用可能なルータ間でより均等にトラフィックの負荷を分散できます。
- 複数の仮想ルータ：プラットフォームが複数のMACアドレスをサポートする場合、VRRPは、ルータのインターフェイス上で最大100の仮想ルータ（VRRPグループ）をサポートします。ルータインターフェイスには、最大256の仮想ルータを設定できます。複数の仮想ルータ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。
- 複数のIPアドレス：仮想ルータは、セカンダリIPアドレスを含む、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。
- プリエンプション：VRRPの冗長性スキームにより、障害が発生したマスター仮想ルータを引き継いだバックアップ仮想ルータを、使用可能になった高いプライオリティのバックアップ仮想ルータに切り替えることができます。
- テキスト認証：簡易テキストパスワードを設定して、仮想ルータを構成しているVRRPルータから受信したVRRPメッセージが認証されたことを確認できます。
- アドバタイズメントプロトコル：VRRPでは、VRRPアドバタイズメントに、専用のインターネット割り当て番号局（IANA）規格マルチキャストアドレス（224.0.0.18）を使用します。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ルータ数が最小限になり、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を割り当てています。

VRRPのホットリスタート

1つのグループでVRRPプロセスの障害が発生した場合には、ピアVRRPマスタールータグループで強制的にフェールオーバーが行われないようにする必要があります。ホットリスタートはウォームRPフェールオーバーをサポートしており、ピアVRRPルータへの強制的なフェールオーバーは発生しません。



第 11 章

TCP 転送、UDP 転送の設定に関する情報

TCP 転送、UDP 転送、および RAW 転送を設定するには、次の概念を理解しておく必要があります。

- [グレースフル リスタート \(203 ページ\)](#)
- [TCP の概要 \(204 ページ\)](#)
- [UDP の概要 \(204 ページ\)](#)
- [NSR のリカバリ アクションとしてのフェールオーバーの設定 \(204 ページ\)](#)

グレースフル リスタート

BGP ルーティングプロトコル情報がフェールオーバー後に復元されている間に、転送情報ベース (FIB) 内の既知のルートでデータパケットを転送するように、BGP の無停止フォワーディング (NSF) を使用できます。NSF では、BGP ピアはルーティング フラップと無縁です。フェールオーバー時に、データトラフィックはインテリジェントモジュール経由で転送され、スタンバイ スーパーバイザがアクティブになります。

シスコ ルータでコールドリブートが発生した場合、ネットワークはルータへのトラフィック転送を中止し、ネットワーク トポロジからルータを削除します。この状況では、BGP は非グレースフル リスタートになり、すべてのルートが削除されます。シスコ オペレーティング システムがスタートアップ コンフィギュレーションを適用すると、BGP はピアリング セッションを再確立して、ルートを再学習します。

デュアル スーパーバイザ構成のシスコ ルータでは、ステートフル スーパーバイザ スイッチオーバーが実行されます。スイッチオーバーの間、BGP は無停止フォワーディングを使用し、FIB の情報に基づいてトラフィックを転送します。システムがネットワーク トポロジから取り除かれることはありません。ネイバーが再起動しているルータは、「ヘルパー」と呼ばれます。スイッチオーバー後、グレースフルリスタート動作が開始されます。この処理が進行中の際、2 つのルータはネイバー関係を再確立し、これらの BGP ルートを交換します。このネイバー関係が再起動中でも、ヘルパーは再起動中のピアを指すプレフィックスの転送を続け、再起動中のルータはピアにトラフィックを転送し続けます。再起動中のルータがグレースフルリスタート可能なすべての BGP ピアを持つ場合、グレースフルリスタートが完了し、BGP は再び動作可能なネイバーを通知します。

TCP の概要

TCP は、2つのコンピュータシステムがデータを転送するために交換する、データおよび確認応答の形式が指定されたコネクション型プロトコルです。また、TCP では、データを正しく到達させるために、コンピュータが使用する手順も指定されています。TCP では、アプリケーション プログラム間の着信トラフィックのすべての逆多重化を処理するため、TCP を使用すると、1つのシステム上の複数のアプリケーションが同時に通信できます。

UDP の概要

ユーザ データグラム プロトコル (UDP) は、IP ファミリに属するコネクションレス型トランスポートレイヤプロトコルです。UDP は、ネットワーク ファイル システム (NFS)、簡易ネットワーク管理プロトコル (SNMP)、ドメイン ネーム システム (DNS)、TFTP などの一般的なアプリケーション層プロトコルのための、トランスポートプロトコルです。

TCP および UDP 以外のすべての IP プロトコルは、RAW プロトコルと考えられています。

ほとんどのサイトでは、TCP、UDP、および RAW トランスポートのデフォルト設定を変更する必要はありません。

NSR のリカバリ アクションとしてのフェールオーバーの設定

アクティブな TCP、またはアクティブな TCP の NSR クライアントが終了または再起動すると、TCP セッションはダウンします。NSR の提供を継続するには、リカバリ アクションとしてフェールオーバーを設定する必要があります。フェールオーバーが設定されている場合、アクティブな TCP またはアクティブなアプリケーション (LDP、OSPF など) が再起動または終了すると、スイッチオーバーが開始されます。

NSR に MPLS Label Distribution Protocol (LDP) を設定する方法については、『*MPLS Configuration Guide for Cisco NCS 540 Series Routers*』を参照してください。

各プロセスにプロセスごとのレベルで NSR を設定する方法については、『*Routing Configuration Guide for Cisco NCS 540 Series Routers*』を参照してください。

設定例

ノンストップルーティングを維持するために、アクティブなインスタンスをスタンバイに切り替えるリカバリ アクションとしてフェールオーバーを設定します。

```
Router#configure
Router(config)#nsr process-failures switchover
Router(config)#commit
```

実行コンフィギュレーション

```
Router#show running-configuration nsr process-failures switchover  
nsr process-failures switchover
```

関連コマンド

- nsr process-failures switchover

