IPv6 コンフィギュレーション ガイド、Cisco IOS Release 15.1S

IPv6 Configuration Guide, Cisco IOS Release 15.1S

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco IOS IPv6 コンフィギュレーション ガイド

はじめに：IPv6 機能に対応する Cisco IOS ソフトウェア リリースの詳細

このマニュアルでは、Cisco IOS ソフトウェア リリースのうち、12.0S、12.*x*T、12.2S ファミリ、12.3、12.4、15.0、および 15.1 のリリース トレインでサポートされている IP バージョン 6（IPv6）の機能について説明します。

IPv6 for Cisco IOS ソフトウェア機能のマニュアルには、Cisco IOS ソフトウェアでサポートされている IPv6 機能の実装およびコマンド リファレンスの情報が記載されています。このマニュアルでは、IPv6 機能に対応する Cisco IOS ソフトウェア リリースの詳細だけを取り上げています。ご使用の Cisco IOS ソフトウェア リリースによっては、一部の IPv6 機能がサポートされていない場合もあります。他の IPv6 for Cisco IOS ソフトウェア機能のマニュアルを読む前に、このマニュアルを通して読んでおくことを強く推奨します。

機能情報の確認

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

『*Cisco IOS IPv6 Configuration Guide*』は、次の Web サイトにあります。

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide

『*Cisco IOS IPv6 Command Reference*』は、次の Web サイトにあります。

http://www.cisco.com/en/US/docs/ios/ipv6/command/reference

目次

このマニュアルは、次の各項で構成されています。

Cisco IOS ソフトウェアのプラットフォーム依存関係および制約事項

IPv6 機能は、12.0S、12.*x*T、12.2S、12.2SB、12.2SE、12.2SG、12.2SR、12.2SX、12.3、12.4、および 15.0M の Cisco IOS ソフトウェア リリース トレインでサポートされています。これらの一連のソフトウェア リリースはそれぞれ、Cisco IOS Release 12.0(22)S、12.2(2)T、12.2(14)S、12.2(28)SB、12.2(25)SEA、12.2(33)SRA、12.2(17a)SX1、12.3、12.4、および 15.0(1)M から開始されます。Cisco IOS ソフトウェア トレインの各リリースでサポートされている IPv6 機能を調べるには、表 1 を参照してください。

- IPv6 は、12.0(21)ST Cisco IOS ソフトウェア リリース トレインで導入され、Cisco IOS Release 12.0(22)S からは、12.0S Cisco IOS ソフトウェア リリース トレインとマージされました。12.0S Cisco IOS ソフトウェア リリース トレインは、Cisco 12000 シリーズ インターネット ルータおよび Cisco 10720 インターネット ルータにかぎり、IPv6 サポートを提供しています。
- 12.2S Cisco IOS リリース トレインは、次のように、それぞれ異なるプラットフォームをサポートするリリース トレイン ファミリで構成されています。
  - 12.2SB Cisco IOS リリース トレインには、Cisco 10000、7304、7301、および 7200 シリーズが含まれます。Cisco IOS Release 12.2(33)SB 以降、12.2SB リリース トレインでは、Cisco 7200 および 7301 シリーズはサポートされていません。
  - 12.2SE Cisco IOS リリース トレインは、Cisco Catalyst 3560、3750、3560E、および 3750E シリーズで構成されます。
  - 12.2SG Cisco IOS リリース トレインは、Cisco Catalyst 4500 および Cisco Catalyst 4900 シリーズで構成されます。
  - 12.2SR Cisco IOS リリース トレインは、Cisco 7600 および 7200 シリーズ ルータで構成されます。
  - 12.2SX Cisco IOS リリース トレインは、Cisco Catalyst 6500 で構成されます。12.2SR Cisco IOS リリース トレイン以前は、Cisco 7600 シリーズも 12.2SX リリース トレインに含まれていました。
- 15.0MS Cisco IOS リリース トレインは、12.2、12.3、および 12.4 の Cisco IOS リリース トレインで構成されます。
- また、IPv6 は、一部の特殊なソフトウェア リリース トレインでもサポートされています。

Cisco IOS IPv6 機能およびサポートされているソフトウェア リリース

表 1 に、12.0S、12.*x*T、12.2S、12.2SB、12.2SR、12.2SX、12.3、12.4、および 15.0M Cisco IOS ソフトウェア リリース トレインでサポートされている IPv6 機能を示します。

（注） 表 1 は、ソフトウェア リリース トレインごとに、この機能が使用可能になった最初のリリースを示しています。表 1 で特に明記していないかぎり、その機能は、それ以降の Cisco IOS ソフトウェア リリース トレインでもサポートされます。

表 1　サポートされている IPv6 機能

機能	説明している章	12.0S リリース	12.*x*T/15.*x*T リリース	12.*x*/15.*x* リリース	12.2SB リリース	12.2SE リリース	12.2SG リリース	12.2SR リリース	12.2SX リリース
IPv6									
IPv6 アドレス タイプ：ユニキャスト	「Implementing IPv6 Addressing and Basic Connectivity」	(22)	12.2(2)	12.3	(28)	(25)SEA	—	(33)SRA	(17a)SX1
IPv6：uRPF	「Implementing IPv6 Addressing and Basic Connectivity」	(31)	—	—	—	—	—	—	—
IPv6：ICMPv6	「Implementing IPv6 Addressing and Basic Connectivity」	(22)	12.2(2)	12.3	(28)[1]	(25)SEA	(25)	(33)SRA	(17a)SX1
IPv6：IPv6 ネイバー探索	「Implementing IPv6 Addressing and Basic Connectivity」	(22)	12.2(2)	12.3	(28)	(25)SEA	(25)	(33)SRA	(17a)SX1
IPv6：IPv6 ステートレス自動設定	「Implementing IPv6 Addressing and Basic Connectivity」	(22)	12.2(2)	12.3	(28)	(25)SEA	(25)	(33)SRA	(17a)SX1
IPv6：IPv6 MTU パス ディスカバリ	「Implementing IPv6 Addressing and Basic Connectivity」	(22)	12.2(2)	12.3	(28)	(25)SEA	(25)	(33)SRA	(17a)SX1
IPv6：ping	「Implementing IPv6 for Network Management」	(22)	12.2(2)	12.3	(28)	(25)SEA	(25)	(33)SRA	(17a)SX1
IPv6：Telnet、DNS、TFTP クライアント、traceroute	「Implementing IPv6 Addressing and Basic Connectivity」、「Implementing IPv6 for Network Management」	(22)	12.2(2)	12.3	(28)	(25)SEA	(25)	(33)SRA	(17a)SX1

機能	説明している章	12.0S リリース	12.*x*T/ 15.*x*T リリース	12.*x*/15.*x* リリース	12.2SB リリース	12.2SE リリース	12.2SG リリース	12.2SR リリース	12.2SX リリース
IPv6：ICMPv6 リダイレクト	「Implementing IPv6 Addressing and Basic Connectivity」	(22)	12.2(4)	12.3	(28)	(25)SEA	(25)	(33)SRA	(17a)SX1
IPv6：ICMP レート制限	「Implementing IPv6 Addressing and Basic Connectivity」	—	12.2(8)	12.3	—	(25)	(25)	(33)SRA	(17a)SX1
IPv6：ネイバー探索重複アドレス検出	「Implementing IPv6 Addressing and Basic Connectivity」	(22)	12.2(4)	12.3	(28)	(25)SEA	(25)	(33)SRA	(17a)SX1
IPv6：ネイバー探索用の IPv6 スタティック キャッシュ エントリ	「Implementing IPv6 Addressing and Basic Connectivity」	(22)	12.2(8)	12.3	(28)	(25)SEA	(25)	(33)SRA	(17a)SX1
IPv6：Per-Interface ネイバー探索キャッシュ制限	『Implementing IPv6 Addressing and Basic Connectivity』	—	15.1(3)	—	—	—	—	—	—
IPv6 アドレス タイプ：エニーキャスト	「Implementing IPv6 Addressing and Basic Connectivity」	—	12.3(4)	12.4	(28)	(25)SEA	(25)	(33)SRA	(33)SXH
IPv6：NetFlow for IPv6 ユニキャスト トラフィック	「Implementing NetFlow for IPv6」	—	12.3(7)	12.4	—	—	—	(33)SRB	(33)SXH
IPv6：NetFlow：IPv6 NetFlow に置き換わる Flexible NetFlow for IPv6	「Implementing NetFlow for IPv6」	—	12.4(20)	15.0	—	—	—	—	—
IPv6：モバイル IPv6 ホーム エージェント	「Implementing Mobile IPv6」	—	12.3(14)	12.4	—	—	—	—	—

機能	説明している章	12.0S リリース	12.xT/15.xT リリース	12.x/15.x リリース	12.2SB リリース	12.2SE リリース	12.2SG リリース	12.2SR リリース	12.2SX リリース
IPv6：IPv6 デフォルト ルータ プリファレンス	「Implementing IPv6 Addressing and Basic Connectivity」	—	12.4(2)	15.0	(33)	(46)	(46)	(33)SRA	(33)SXH
IPv6：モバイル IPv6 の IPv6 ACL 拡張	「Implementing Mobile IPv6」	—	12.4(2)	—	—	—	—	(33)SRB	(33)SXI
IPv6：モバイル IP - モバイル v6 - 基本 NEMO	「Implementing Mobile IPv6」	—	12.4(20)	15.0	—	—	—	—	—
IPv6：IPv6 トラフィックの IP 受信 ACL	「IP Receive ACL」	(32)	—	—	—	—	—	—	—
IPv6：IPv6 での syslog	「Implementing IPv6 for Network Management」	—	12.4(4)	15.0	(33)	(44)	(44)	(33)SRB	(33)SXI
IPv6：IPv6 VPN over MPLS	「Implementing IPv6 VPN over MPLS」	—	12.4(20)	15.0	(33)	—	—	(33)SRB	(33)SXI
IPv6：IP トンネルを介した MPLS VPN 6VPE サポート	「Implementing IPv6 VPN over MPLS (6VPE)」	—	—	—	—	—	—	(33)SRB1	(33)SXI
IPv6：IPv6 の CNS エージェント	「Implementing IPv6 for Network Management」	—	12.4(20)	15.0	(33)	—	(50)	(33)SRC	—
IPv6：IPv6 の IP SLA	「Implementing IPv6 for Network Management」	—	12.4(20)	15.0	(33)	—	(50)	(33)SRC	—
IPv6：config ロガーでの IPv6	「Implementing IPv6 for Network Management」	—	12.4(20)	15.0	(33)	—	(50)	(33)SRC	—
IPv6：IPv6 Netconf サポート	「Implementing IPv6 for Network Management」	—	12.4(20)	15.0	(33)	—	(50)	(33)SRC	—
IPv6：IPv6 での TCL のサポート	「Implementing IPv6 for Network Management」	—	12.4(20)	15.0	—	—	(50)	(33)SRC	—

機能	説明している章	12.0S リリース	12.*x*T/15.*x*T リリース	12.*x*/15.*x* リリース	12.2SB リリース	12.2SE リリース	12.2SG リリース	12.2SR リリース	12.2SX リリース
IPv6：SOAP での IPv6 サポート	「Implementing IPv6 for Network Management」	—	12.4(20)	15.0	(33)	—	(50)	(33)SRC	—
IPv6：HTTP(S) IPv6 サポート（インフラストラクチャ）	「Implementing IPv6 for Network Management」	—	12.4(20)	15.0	(33)	(44)	(44)	(33)SRC	—
IPv6：no ipv6 source-route コマンド	『Cisco IOS IPv6 Command Reference』	—	12.3(4)	12.4	—	—	—	(33)SRB1	—
IPv6 RA ガード	『Implementing First Hop Security in IPv6』	—	—	—	—	—	(54)	—	(33)SXI4
IPv6 PACL サポート	『Implementing First Hop Security in IPv6』	—	—	—	—	(46)	(54)	—	(33)SXI4
IPv6 選択的パケット廃棄	『Implementing Selective Packet Discard in IPv6』	—	—	15.0(1)S	—	—	—	(33)SRC	(33)SXH
IPv6：完全な選択的パケット廃棄サポート	『Implementing Selective Packet Discard in IPv6』	—	15.1(3)	—	—	—	—	—	—
BVI インターフェイス上での IPv6 サポート	『Implementing IPv6 Addressing and Basic Connectivity』	—	15.1(2)	—	—	—	—	—	—
IPv6 スイッチング サービス									
IPv6 スイッチング：シスコ エクスプレス フォワーディング/分散型シスコ エクスプレス フォワーディングのサポート	「Implementing IPv6 Addressing and Basic Connectivity」	(22)	12.2(13)	12.3	(28)	(25)SEA	(25)	(33)SRA	(17a)SX1

機能	説明している章	12.0S リリース	12.xT/15.xT リリース	12.x/15.x リリース	12.2SB リリース	12.2SE リリース	12.2SG リリース	12.2SR リリース	12.2SX リリース
IPv6 スイッチング：設定済みの CEFv6 スイッチド IPv6 over IPv4 トンネル	「Implementing Tunneling for IPv6」	—	12.2(13)	12.4	(28)	—	—	(33)SRA	(18)SXE
IPv6 スイッチング：MPLS を介するプロバイダー エッジ ルータ (6PE)[2] [3]	「Implementing IPv6 over MPLS」	(22)	12.2(15)	12.3	(31)	—	—	(33)SRA	(17b)SXA
IPv6 スイッチング：CEFv6 スイッチド ISATAP	「Implementing Tunneling for IPv6」	—	12.3(2)	12.4	(28)	—	(25)	(33)SRA	(17a)SX1
IPv6 スイッチング：CEFv6 スイッチド自動 IPv4 互換トンネル	「Implementing Tunneling for IPv6」	—	12.3(2)	12.4	(28)	—	—	(33)SRA	(17a)SX1
IPv6 ルーティング									
IPv6 ルーティング：RIP for IPv6（RIPng）	「Implementing RIP for IPv6」	(22)	12.2(2)[4]	12.3	(28)	(25)SEA	(25)	(33)SRA	(17a)SX1
IPv6 ルーティング：スタティック ルーティング	「Implementing Static Routes for IPv6」	(22)	12.2(2)	12.3	(28)	(25)SEA	(25)	(33)SRA	(17a)SX1
IPv6 ルーティング：ルート再配布	「Implementing IS-IS for IPv6」、「Implementing RIP for IPv6」	(22)	12.2(2)	12.3	(28)	(25)SEA	(25)	(33)SRA	(18)SXE
IPv6 ルーティング：マルチプロトコル BGP for IPv6 拡張	「Implementing Multiprotocol BGP for IPv6」	(22)	12.2(2)[5]	12.3	(28)	—	(25)	(33)SRA	(17a)SX1
IPv6 ルーティング：マルチプロトコル BGP リンクローカル アドレス ピアリング	「Implementing Multiprotocol BGP for IPv6」	(22)	12.2(4)	12.3	(28)	—	(25)	(33)SRA	(17a)SX1

機能	説明している章	12.0S リリース	12.*x*T/ 15.*x*T リリース	12.*x*/15.*x* リリース	12.2SB リリース	12.2SE リリース	12.2SG リリース	12.2SR リリース	12.2SX リリース
IPv6 ルーティング：IPv6 の IS-IS サポート	「Implementing IS-IS for IPv6」	(22)	12.2(8)	12.3	(28)	—	(25)	(33)SRA	(17a)SX1
IPv6 ルーティング：IPv6 の IS-IS マルチトポロジ サポート	「Implementing IS-IS for IPv6」	(26)	12.2(15)	12.3	(28)	—	(25)	(33)SRA	(18)SXE
IPv6 ルーティング：OSPF for IPv6（OSPFv3）	「Implementing OSPF for IPv6」	(24)	12.2(15)	12.3	(28)	(25)SEA	(25)	(33)SRA	(17a)SX1
IPv6 ルーティング：IPsec を使用した OSPF for IPv6 の認証サポート	「Implementing OSPF for IPv6」	—	12.3(4)	12.4	—	—	—	—	—
IPv6 ルーティング：OSPF IPv6（OSPFv3）IPsec ESP 暗号化および認証	「Implementing OSPF for IPv6」	—	12.4(9)	15.0	—	—	—	—	—
OSPFv3 ダイナミック インターフェイス コスト サポート	「Implementing OSPF for IPv6」	—	12.4(15)	15.0	—	—	—	—	—
IPv6 ルーティング：IPv6 ポリシーベース ルーティング	「Implementing Policy-Based Routing for IPv6」	—	12.3(7)	12.4	—	—	—	—	(33)SXI4
IPv6 ルーティング：EIGRP サポート	「Implementing EIGRP for IPv6」	—	12.4(6)	—	—	(40)	(40)	(33)SRB	(33)SXI
EIGRP IPv6 VRF-Lite	「Implementing EIGRP for IPv6」			15.1(1)S					
IPv6 ルーティング：OSPFv3 高速コンバージェンス - LSA および SPF スロットリング	「Implementing OSPF for IPv6」	—	—	15.0(1)M	(33)	—	—	(33)SRC	—

機能	説明している章	12.0S リリース	12.*x*T/ 15.*x*T リリース	12.*x*/15.*x* リリース	12.2SB リリース	12.2SE リリース	12.2SG リリース	12.2SR リリース	12.2SX リリース
OSPFv3 for BFD	「Implementing OSPF for IPv6」、「Implementing Bidirectional Forwarding Detection for IPv6」	—	15.1(2)	—	—	—	—	(33)SRE	—
BFD IPv6 カプセル化サポート	『Implementing Bidirectional Forwarding Detection for IPv6』	—	15.1(2)	—	—	—	—	(33)SRE	—
IPv6 での BFD に対するスタティック ルート サポート	「Implementing Bidirectional Forwarding Detection for IPv6」	—	15.1(2)	—	—	—	—	—	—
IPv6 サービスおよび管理									
IPv6 サービス：IPv4 トランスポートでの AAAA DNS ルックアップ	「Implementing IPv6 Addressing and Basic Connectivity」	(22)	12.2(2)	12.3	(28)	(25)SEA	(25)	(33)SRA	(17a)SX1
IPv6 サービス：標準アクセス コントロール リスト	「Implementing Traffic Filters and Firewalls for IPv6 Security」	(22)	12.2(2)	12.3	(28)	(25)SED	(25)	(33)SRA	(17a)SX1
IPv6 サービス：IPsec 認証ヘッダーのための IPv6 ACL 拡張	「Implementing Traffic Filters and Firewalls for IPv6 Security」	—	12.4(20)	15.0	—	—	—	—	—
IPv6 サービス：IPv6 トランスポートでの DNS ルックアップ	「Implementing IPv6 Addressing and Basic Connectivity」	(22)	12.2(8)	12.3	(28)	(25)SED	(25)	(33)SRE2	(17a)SX1
IPv6 サービス：IPv6 での Secure Shell（SSH; セキュア シェル）サポート	「Implementing IPv6 for Network Management」	(22)	12.2(8)	12.3	(28)	(25)SEE	(25)	(33)SRA	(17a)SX1

機能	説明している章	12.0S リリース	12.*x*T/ 15.*x*T リリース	12.*x*/15.*x* リリース	12.2SB リリース	12.2SE リリース	12.2SG リリース	12.2SR リリース	12.2SX リリース
IPv6 サービス：シスコ検出プロトコル：ネイバー情報の IPv6 アドレス ファミリ サポート	「Implementing IPv6 Addressing and Basic Connectivity」	—	12.2(8)	12.3	(28)	(25)SEE	(25)	(33)SRA	(18)SXE
IPv6 サービス：CISCO-IP-MIB サポート	「Implementing IPv6 for Network Management」	(22)	12.2(15)	12.3	(28)	(25)SEE	(25)	(33)SRA	(18)SXE
IPv6 サービス：CISCO-IP-FORWARDING-MIB サポート	「Implementing IPv6 for Network Management」	(22)	12.2(15)	12.3	(28)	(25)SEE	(25)	(33)SRA	(18)SXE
IPv6 サービス：RFC 4293 IP-MIB（IPv6 専用）および RFC 4292 IP-FORWARD-MIB（IPv6 専用）	「Implementing IPv6 for Network Management」	—	15.1(3)	—	(33)	—	(54)	(33)SRC	—
IPv6 サービス：拡張アクセス コントロール リスト[3]	「Implementing Traffic Filters and Firewalls for IPv6 Security」	(23)	12.2(13)	12.3	(28)	(25)SED	(25)	(33)SRA	(17a)SX1
IPv6 サービス：汎用プレフィクス	「Implementing IPv6 Addressing and Basic Connectivity」	—	12.3(4)	12.4	—	—	—	—	—
IPv6 サービス：SNMP over IPv6[6]	「Implementing IPv6 for Network Management」	(27)	12.3(14)	12.4	(33)	(44)	(44)	(33)SRB	(33)SXI
SNMPv3：3DES および AES 暗号化のサポート	「Implementing IPv6 for Network Management」	—	12.4(2)	15.0	(33)	(52)	(50)	(33)SRB	(33)SXI
IPv6 サービス：IPv6 IOS ファイア ウォール	「Implementing Traffic Filters and Firewalls for IPv6 Security」	—	12.3(7)	12.4	—	—	—	—	—

機能	説明している章	12.0S リリース	12.xT/15.xT リリース	12.x/15.x リリース	12.2SB リリース	12.2SE リリース	12.2SG リリース	12.2SR リリース	12.2SX リリース
IPv6 サービス：IPv6 IOS ファイアウォール FTP アプリケーション サポート	「Implementing Traffic Filters and Firewalls for IPv6 Security」	—	12.3(11)	—	—	—	—	—	—
IPv6 サービス：IPv6 IPSec VPN	「Implementing IPSec in IPv6 Security」	—	12.4(4)	15.0	—	—	—	—	—
IPsec IPv6 フェーズ 2 サポート	「Implementing IPSec in IPv6 Security」	—	12.4(4)	15.0	—	—	—	—	—
IPv6 Secure Neighbor Discovery (SeND; セキュア ネイバー探索)	『Implementing First Hop Security in IPv6』	—	12.4(24)	15.0	—	—	—	—	—
IPv6 サービス：IPv6 over DMVPN	「Implementing Dynamic Multipoint VPN over IPv6」	—	12.4(20)	15.0	—	—	—	—	—
IPv6 サービス：HSRP for IPv6	「Configuring First Hop Redundancy Protocols in IPv6」	—	12.4(4)	15.0	—	(46)	(52)	(33)SRB	(33)SXI
HSRP：グローバル IPv6 アドレス	「Configuring First Hop Redundancy Protocols in IPv6」	—	—	—	—	—	—	—	(33)SXI4
IPv6 サービス：FHRP - GLBP for IPv6	「Configuring First Hop Redundancy Protocols in IPv6」	—	12.4(6)	15.0	—	—	—	—	(33)SXI
IPv6 over Frame Relay	「Implementing IPv6 over Frame Relay」	(33)	—	—	—	—	—	—	—
NTPv4 in IPv6	「Implementing NTPv4 in IPv6」	—	12.4(20)	—	—	—	—	—	—

機能	説明している章	12.0S リリース	12.*x*T/15.*x*T リリース	12.*x*/15.*x* リリース	12.2SB リリース	12.2SE リリース	12.2SG リリース	12.2SR リリース	12.2SX リリース
IPv6 サービス：IOS ゾーンベース ファイアウォール	「Implementing Traffic Filters and Firewalls for IPv6 Security」	—	15.1(2)	—	—	—	—	—	—
NBAR IPv6 移行メカニズム検出		—	15.1(3)	—	—	—	—	—	—
IPv6 ブロードバンド アクセス									
IPv6 アクセス サービス：PPPoA	「Implementing ADSL and Deploying Dial Access for IPv6」	—	12.2(13)	12.3	—	—	—	(33)SRC[7]	—
IPv6 アクセス サービス：PPPoE	「Implementing ADSL and Deploying Dial Access for IPv6」	—	12.2(13)	12.3	—	—	—	(33)SRC[7]	—
IPv6 アクセス サービス：プレフィクス プール	「Implementing ADSL and Deploying Dial Access for IPv6」	—	12.2(13)	12.3	—	—	—	(33)SRC[7]	—
IPv6 アクセス サービス：AAA での Cisco VSA IPv6 アトリビュートのサポート	「Implementing ADSL and Deploying Dial Access for IPv6」	—	12.2(13)	12.3	—	—	—	(33)SRC[7]	—
IPv6 アクセス サービス：リモート ブリッジ型のカプセル化	「Implementing IPv6 Addressing and Basic Connectivity」	—	12.3(4)	12.4	—	—	—	(33)SRC[7]	—
IPv6 アクセス サービス：AAA での RFC 3162 IPv6 RADIUS アトリビュートのサポート	「Implementing ADSL and Deploying Dial Access for IPv6」	—	12.3(4)	12.4	—	—	—	(33)SRC[7]	—
DHCP for IPv6									

機能	説明している章	12.0S リリース	12.xT/15.xT リリース	12.x/15.x リリース	12.2SB リリース	12.2SE リリース	12.2SG リリース	12.2SR リリース	12.2SX リリース
IPv6 アクセス サービス：ステートレス DHCPv6	「Implementing DHCP for IPv6」	(32)[8]	12.3(4)	12.4	(28)	—	—	(33)SRA	(18)SXE
IPv6 アクセス サービス：DHCPv6 プレフィクス委任	「Implementing DHCP for IPv6」、「Implementing ADSL and Deploying Dial Access for IPv6」	(32)[8]	12.3(4)	12.4	(28)	—	—	(33)SRA	(18)SXE
IPv6 アクセス サービス：DHCP for IPv6 リレー エージェント	「Implementing DHCP for IPv6」	—	12.3(11)	12.4	(28)	(46)	(50)	(33)SRC	(33)SXI
IPv6 アクセス サービス：AAA を介する DHCPv6 プレフィクス委任	「Implementing ADSL and Deploying Dial Access for IPv6」	—	12.3(14)	12.4	(28)[9]	—	—	—	—
IPv6 アクセス サービス：DHCPv6 サーバ ステートレス自動設定	「Implementing DHCP for IPv6」	—	12.4(15)	—	(28)	(46)	(52)	(33)SRC	(33)SXI
IPv6 アクセス サービス：DHCPv6 クライアント情報リフレッシュ オプション	「Implementing DHCP for IPv6」	—	12.4(15)	15.0	—	—	—	—	—
IPv6 アクセス サービス：プレフィクス委任のための DHCPv6 リレー エージェント通知[10]	「Implementing DHCP for IPv6」	—	—	—	—	(46)	(52)	(33)SRC	(33)SXI
IPv6 アクセス サービス：DHCPv6 リレー - リロード永続インターフェイス ID オプション	「Implementing DHCP for IPv6」	—	—	—	(33)	(46)	(52)	(33)SRC	(33)SXI

機能	説明している章	12.0S リリース	12.*x*T/ 15.*x*T リリース	12.*x*/15.*x* リリース	12.2SB リリース	12.2SE リリース	12.2SG リリース	12.2SR リリース	12.2SX リリース
IPv6 アクセス サービス：DHCPv6 イーサネット リモート ID オプション	「Implementing DHCP for IPv6」	—	—	—	—	(46)	(52)	(33)SRC	(33)SXI
DHCP：DHCPv6 個別アドレス割り当て	「Implementing DHCP for IPv6」	—	12.4(24)	—	—	(46)	—	—	—
DHCP：DHCPv6 リレーの SSO/ISSU	「Implementing DHCP for IPv6」	—	—	—	—	—	—	(33)SRE	—
DHCPv6 リレー：送信元設定	「Implementing DHCP for IPv6」	—	—	—	—	—	—	(33)SRE	—
DHCPv6 Bulk Lease クエリー	「Implementing DHCP for IPv6」	—	—	15.1(1)S	—	—	—	—	—
IPv6 マルチキャスト									
IPv6 マルチキャスト：Multicast Listener Discovery（MLD; マルチキャスト リスナー ディスカバリ）プロトコル（バージョン 1 および 2）	「Implementing IPv6 Multicast」	(26)[11]	12.3(2)	12.4	(28)	—	(40)	(33)SRA	(18)SXE
IPv6 マルチキャスト：PIM Sparse Mode（PIM-SM; PIM 希薄モード）	「Implementing IPv6 Multicast」	(26)[11]	12.3(2)	12.4	(28)	—	(40)	(33)SRA	(18)SXE

機能	説明している章	12.0S リリース	12.*x*T/ 15.*x*T リリース	12.*x*/15.*x* リリース	12.2SB リリース	12.2SE リリース	12.2SG リリース	12.2SR リリース	12.2SX リリース
IPv6 マルチキャスト：PIM Source Specific Multicast（PIM-SSM; PIM 送信元固有マルチキャスト）	「Implementing IPv6 Multicast」	(26)[11]	12.3(2)	12.4	(28)	—	(40)	(33)SRA	(18)SXE
IPv6 マルチキャスト：スコープ境界	「Implementing IPv6 Multicast」	(26)[11]	12.3(2)	12.4	(28)	—	(40)	(33)SRA	(18)SXE
IPv6 マルチキャスト：MLD アクセス グループ	「Implementing IPv6 Multicast」	(26)[11]	12.3(4)	12.4	(28)	—	(40)	(33)SRA	(33)SXH
IPv6 マルチキャスト：PIM accept register	「Implementing IPv6 Multicast」	(26)[11]	12.3(4)	12.4	(28)	—	(40)	(33)SRA	(33)SXH
IPv6 マルチキャスト：PIM 組み込み RP サポート	「Implementing IPv6 Multicast」	(26)[11]	12.3(4)	12.4	(28)	—	(40)	(33)SRA	(33)SXH
IPv6 マルチキャスト：Bootstrap Router（BSR; ブートストラップ ルータ）パケットの RPF フラッディング	「Implementing IPv6 Multicast」	(26)[11]	12.3(4)	12.4	(28)	—	(40)	(33)SRA	(33)SXH
IPv6 マルチキャスト：ルーティング可能アドレスの hello オプション	「Implementing IPv6 Multicast」	(26)[11]	12.3(4)	12.4	(28)	—	(40)	(33)SRA	(33)SXH
IPv6 マルチキャスト：スタティック マルチキャスト ルーティング（mroute）	「Implementing IPv6 Multicast」	(26)[11]	12.3(4)	12.4	(28)	—	(40)	(33)SRA	(33)SXH

機能	説明している章	12.0S リリース	12.*x*T/ 15.*x*T リリース	12.*x*/15.*x* リリース	12.2SB リリース	12.2SE リリース	12.2SG リリース	12.2SR リリース	12.2SX リリース
IPv6 マルチキャスト：Multiprotocol Border Gateway Protocol（MBGP; マルチプロトコル ボーダー ゲートウェイ プロトコル）のアドレス ファミリ サポート	「Implementing IPv6 Multicast」	(26)[11]	12.3(4)	12.4	(28)	—	—	(33)SRA	(33)SXH
IPv6 マルチキャスト：受信側の明示的トラッキング	「Implementing IPv6 Multicast」	—	12.3(7)	12.4	(28)	—	(40)	(33)SRA	(33)SXH
IPv6 マルチキャスト：IPv6 双方向 PIM	「Implementing IPv6 Multicast」	—	12.3(7)	12.4	(28)	—	(40)	(33)SRA	—
IPv6 マルチキャスト：MFIB 表示機能拡張	「Implementing IPv6 Multicast」	—	12.3(7)	12.4	—	—	(40)	—	—
IPv6 マルチキャスト：IPv6 BSR	「Implementing IPv6 Multicast」	(28)	12.3(11)	12.4	(28)	—	(40)	(33)SRA	(18)SXE
IPv6 マルチキャスト：IPv6 BSR 双方向サポート	「Implementing IPv6 Multicast」	—	12.3(14)	12.4	—	—	(40)	(33)SRE	—
IPv6 マルチキャスト：IPv6 BSR 限定スコープ ゾーン サポート	「Implementing IPv6 Multicast」	—	12.3(14)	12.4	—	—	(40)	—	—
IPv6 マルチキャスト：MLDv1 SSM 用の SSM マッピング	「Implementing IPv6 Multicast」	—	12.4(2)	—	—	—	(40)	(33)SRA	(18)SXE

機能	説明している章	12.0S リリース	12.xT/15.xT リリース	12.x/15.x リリース	12.2SB リリース	12.2SE リリース	12.2SG リリース	12.2SR リリース	12.2SX リリース
IPv6 マルチキャスト：RP マッピングを設定するための IPv6 BSR 機能	「Implementing IPv6 Multicast」	—	12.4(2)	—	—	—	(40)	(33)SRE	—
IPv6 マルチキャスト：MLD グループ制限	「Implementing IPv6 Multicast」	—	12.4(2)	—	—	—	(40)	(33)SRE	—
IPv6 マルチキャスト：マルチキャスト ユーザ認証およびプロファイル サポート	「Implementing IPv6 Multicast」	—	12.4(4)	—	—	—	(40)	—	—
IPv6 マルチキャスト：MLD スヌーピング	「Implementing IPv6 Multicast」	—	—	—	—	(25)SED	(40)	(33)SRB	(18)SXE
IPv6 マルチキャスト：アドレス グループ範囲のサポート	「Implementing IPv6 Multicast」	—	—	15.0(1)M	—	—	(40)	(33)SRE	(33)SXI
IPv6 マルチキャスト：帯域幅ベースの Call Admission Control（CAC; コール アドミッション制御）	「Implementing IPv6 Multicast」	—	—	—	—	—	(40)	(33)SRE	—
IPv6 マルチキャスト：MLD プロキシ	「Implementing IPv6 Multicast」	—	15.1(2)	—	—	—	—	—	—
NAT Protocol Translation（NAT-PT; NAT プロトコル変換）		—	12.2(13)	12.3	—	—	—	—	—
NAT-PT：DNS ALG のサポート	「Implementing NAT Protocol Translation」	—	12.2(13)	12.3	—	—	—	—	—
NAT-PT：過負荷（PAT）のサポート	「Implementing NAT Protocol Translation」	—	12.3(2)	12.4	—	—	—	—	—

機能	説明している章	12.0S リリース	12.*x*T/ 15.*x*T リリース	12.*x*/15.*x* リリース	12.2SB リリース	12.2SE リリース	12.2SG リリース	12.2SR リリース	12.2SX リリース
NAT-PT：FTP ALG のサポート	「Implementing NAT Protocol Translation」	—	12.3(2)	12.4	—	—	—	—	—
NAT-PT：フラグメンテーションのサポート	「Implementing NAT Protocol Translation」	—	12.3(2)	12.4	—	—	—	—	—
IPv6 トンネル サービス									
IPv6 トンネリング：自動 6to4 トンネル	「Implementing Tunneling for IPv6」	(22)	12.2(2)	12.3	(28)	—	(25)	(33)SRA	(18)SXE
IPv6 トンネリング：CEF スイッチド自動 6to4 トンネル	「Implementing Tunneling for IPv6」	(22)	12.3(2)	12.3	(28)	—	(25)	(33)SRA	(18)SXE
IPv6 トンネリング：自動 IPv4 互換トンネル	「Implementing Tunneling for IPv6」	(22)	12.2(2)	12.3	(28)	—	(25)	(33)SRA	(18)SXE
IPv6 トンネリング：手動で設定された IPv6 over IPv4 トンネル	「Implementing Tunneling for IPv6」	(23)[12]	12.2(2)	12.3	(28)	—	(25)	(33)SRA	(17a)SX1
IPv6 トンネリング：IPv6 over IPv4 GRE トンネル	「Implementing Tunneling for IPv6」	(22)[13]	12.2(4)	12.3	(28)	—	—	(33)SRA	(17a)SX1
IPv6 トンネリング：トンネル ラインカードを使用する IPv6 over UTI[14]	「Implementing Tunneling for IPv6」	(23)[12]	—	—	—	—	—	—	—
IPv6 トンネリング：ISATAP トンネル サポート	「Implementing Tunneling for IPv6」	—	12.2(15)	12.3	(28)SB	—	(25)	(33)SRA	(17a)SX1
IPv6 トンネリング：IPv6 over IPv6 トンネル	「Implementing Tunneling for IPv6」	—	12.3(7)	12.4	—	—	—		—
IPv6 トンネリング：IP over IPv6 GRE トンネル	「Implementing Tunneling for IPv6」	—	12.3(7)	12.4	—	—	—	—	—

機能	説明している章	12.0S リリース	12.*x*T/ 15.*x*T リリース	12.*x*/15.*x* リリース	12.2SB リリース	12.2SE リリース	12.2SG リリース	12.2SR リリース	12.2SX リリース
IPv6 トンネリング：GRE IPv6 および IPv4 トンネルの CLNS サポート	「Implementing Tunneling for IPv6」	—	12.3(7)	12.4	(28)SB	—	—	(33)SRA	(33)SXH
IPv6 Rapid Deployment	「Implementing Tunneling for IPv6」	—	15.1(3)	—	—	—	—	—	—
IPv6 Quality of Service（QoS; サービス品質）									
IPv6 QoS：MQC パケット分類	「Implementing QoS for IPv6」	—	12.2(13)	12.3	—	—	(50)	(33)SRA	(18)SXE
IPv6 QoS：MQC トラフィック シェーピング	「Implementing QoS for IPv6」	(28)	12.2(13)	12.3	—	—	(50)	(33)SRA	(18)SXE
IPv6 QoS：MQC トラフィック ポリシング	「Implementing QoS for IPv6」	(28)	12.2(13)	12.3	—	—	(50)	(33)SRA	(18)SXE
IPv6 QoS：MQC パケット マーキング/再マーキング	「Implementing QoS for IPv6」	(28)	12.2(13)	12.3	—	—	(50)	(33)SRA	(18)SXE
IPv6 QoS：キューイング	「Implementing QoS for IPv6」	—	12.2(13)	12.3	—	—	(50)	(33)SRA	(18)SXE
IPv6 QoS：MQC Weighted Random Early Detection（WRED; 重み付けランダム早期検出）ベースのドロップ	「Implementing QoS for IPv6」	(28)	12.2(13)	12.3	—	—	(50)	(33)SRA	(18)SXE
IPv6：QoS トラスト	「Configuring QoS」	—	—	—	—	(52)	(50)	—	—
IPv6 ハイ アベイラビリティ									
IPv6：基本プロトコル ハイ アベイラビリティ	「Implementing IPv6 Addressing and Basic Connectivity」	—	—	—	—	—	—	(33)SRE	—

機能	説明している章	12.0S リリース	12.*x*T/ 15.*x*T リリース	12.*x*/15.*x* リリース	12.2SB リリース	12.2SE リリース	12.2SG リリース	12.2SR リリース	12.2SX リリース
IPv6 ルーティング：RIPng ノンストップ フォワーディング	「Implementing RIP for IPv6」	—	—	—	—	—	—	(33)SRE	—
IPv6 ルーティング：MP-BGP IPv6 アドレス ファミリ用の NSF およびグレースフル リスタート	「Implementing Multiprotocol BGP for IPv6」	—	—	—	—	—	—	(33)SRE	—
OSPFv3 グレースフル リスタート	「Implementing OSPF for IPv6」	—	—	15.0(1)M	—	—	—	(33)SRE	—
NSF/SSO - IPv6 マルチキャスト	「Implementing IPv6 Multicast」	—	—	—	—	—	—	(33)SRE	—
IPv6 音声									
RTP/RTCP over IPv6	「Implementing Voice over IPv6」	—	12.4(22)	—	—	—	—	—	—
IPv6 データ リンク レイヤ									
IPv6 データ リンク：ATM PVC および ATM LANE	「Implementing IPv6 Addressing and Basic Connectivity」	(22)[15]	12.2(2)	12.3	(28)	—	—	(33)SRA	—
IPv6 データ リンク：イーサネット、ファスト イーサネット、ギガビット イーサネット、および 10- ギガビット イーサネット	「Implementing IPv6 Addressing and Basic Connectivity」	(22)	12.2(2)	12.3	(28)	(25)SEA	(25)	(33)SRA	—
IPv6 データ リンク：フレーム リレー PVC	「Implementing IPv6 Addressing and Basic Connectivity」	(22)[16]	12.2(2)	12.3	(28)	—	—	(33)SRA	—

機能	説明している章	12.0S リリース	12.xT/15.xT リリース	12.x/15.x リリース	12.2SB リリース	12.2SE リリース	12.2SG リリース	12.2SR リリース	12.2SX リリース
IPv6 データ リンク：ハイレベル データリンク コントロール	「Implementing IPv6 Addressing and Basic Connectivity」	(22)	12.2(2)	12.3	(28)	—	—	(33)SRA	—
IPv6 データ リンク：PPP service over Packet over SONET、ISDN、およびシリアル（非同期および同期）インターフェイス	「Implementing IPv6 Addressing and Basic Connectivity」	(22)	12.2(2)	12.3	(28)[17]	—	—	(33)SRA	—
IPv6 データ リンク：IEEE 802.1Q カプセル化を使用した VLAN	「Implementing IPv6 Addressing and Basic Connectivity」	(22)	12.2(2)	12.3	(28)	(25)SEA	(25)	(33)SRA	(18)SXE
IPv6 データ リンク：Cisco Inter-Switch Link（ISL; スイッチ間リンク）を使用した VLAN	「Implementing IPv6 Addressing and Basic Connectivity」	(22)	12.2(2)	12.3	(28)	(25)SEA	(25)	(33)SRA	(18)SXE
IPv6 データ リンク：Dynamic Packet Transport（DPT; ダイナミック パケット トランスポート）	「Implementing IPv6 Addressing and Basic Connectivity」	(23)	—	—	—	—	—	—	—

1. ファストパス モードでの ping はサポートされていません。サポート レートは、インターフェイスあたり毎秒 10 ping に制限されています。
2. Cisco 10720 インターネット ルータは、Cisco IOS Release 12.0(26)S でサポートされています。
3. IPv6 拡張アクセス コントロール リストおよび MPLS を介する IPv6 プロバイダー エッジ ルータは、Cisco IOS Release 12.0(25)S 以降のリリースが稼動する Cisco IOS ルータの Cisco 12000 シリーズ インターネット ルータ IP Service Engine（ISE; IP サービス エンジン）ライン カード上に、IPv6 ハードウェア アクセラレーションとともに実装されています。
4. RIP for IPv6 機能は、Cisco IOS Release 12.2(13)T で更新されました。
5. いくつかのマルチプロトコル BGP コマンドが機能拡張されました。
6. SNMP バージョン 1、2、および 3 は、IPv6 トランスポートを介してサポートされます。
7. IPv6 ブロードバンド アクセス機能は、12.2(33) SRC リリースにかぎり Cisco IOS 7200 シリーズ ルータで使用できます。

8. Cisco IOS Release 12.0(32)S では、IPv6 プレフィクス委任のための Dynamic Host Configuration Protocol（DHCP）は、Cisco 12000 シリーズ インターネット ルータの 10G エンジン 5 SPA Interface Processor（SIP; SPA インターフェイス プロセッサ）の Shared Port Adaptor（SPA; 共有ポート アダプタ）で、ステートレス アドレス割り当てに対してだけサポートされています。
9. この機能は、IPv6 over PPPoE 機能か IPv6 over PPPoA 機能のいずれかがないと使用できない場合があります。また、IPv6 over PPPoE 機能または IPv6 over PPPoA 機能は、Cisco IOS Release 12.2(28)SB ではサポートされていません。
10. この機能のサポートは、Cisco IOS Release 12.2(33)SCA で提供されています（表 3 を参照）。
11. この機能は、Cisco IOS Release 12.0(26)S が稼動する Cisco 12000 シリーズ インターネット ルータ上でサポートされます。
12. Cisco IOS Release 12.0(23)S の場合、Cisco 12000 シリーズ インターネット ルータでは、トラフィックをラインカード上で処理することで、手動で設定された IPv6 トンネルのパフォーマンスを強化しています。
13. IPv6 over IPv4 GRE トンネルは、Cisco 12000 シリーズのインターネット ルータではサポートされていません。
14. 機能は、Cisco 12000 シリーズのインターネット ルータだけでサポートされています。
15. Cisco IOS 2.0S ソフトウェア リリース トレインでは、ATM PVC だけがサポートされています。ATM LANE はサポートされていません。
16. フレーム リレー PVC は、12.0S Cisco IOS ソフトウェア トレインでは、IPv6 の分散型シスコ エクスプレス フォワーディング スイッチングによってサポートされていません。Cisco 12000 シリーズ インターネット ルータでは、フレーム リレー カプセル化 IPv6 パケットは、ルート プロセッサ上でプロセス スイッチングが行われます。
17. 12.2(28)SB では、PPPoA、PPPoE、および VLAN を介する PPP はサポートされていません。シリアル リンクを介する PPP はサポートされています。

IPv6 ハードウェア フォワーディングをサポートしているシスコのプラットフォーム

サポートされているプラットフォーム

表 1 に、IPv6 ハードウェア フォワーディングに対応しているシスコのプラットフォームと、この機能を導入している Cisco IOS ソフトウェア リリース トレインを示します。

（注） 表 2 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。表 2 で特に明記していないかぎり、その機能は、それ以降の Cisco IOS ソフトウェア リリース トレインでもサポートされます。

表 2　IPv6 ハードウェア フォワーディングをサポートしているシスコ プラットフォームの最小リリース要件

ハードウェアおよび機能	Cisco IOS ソフトウェア リリース
Cisco 12000 シリーズ	
IP ISE ラインカード IPv6 フォワーディング	12.0(23)S
IP ISE ラインカード拡張 ACL	12.0(25)S
IP ISE ラインカード IPv6 over MPLS（6PE）	12.0(25)S
IP ISE ラインカード IPv6 マルチキャスト アシスト	12.0(26)S
IP ISE ラインカード IPv6 QoS	12.0(28)S
エンジン 5 ラインカード IPv6 ハードウェア フォワーディング	12.0(31)S
IPv6 トラフィックの IP 受信 ACL	12.0(32)S
Cisco 10000 シリーズ	
Cisco 10000 シリーズ Performance Routing Engine 2（PRE-2）	12.2(28)SB

表 2　IPv6 ハードウェア フォワーディングをサポートしているシスコ プラットフォームの最小リリース要件 （続き）

ハードウェアおよび機能	Cisco IOS ソフトウェア リリース
Cisco 10000 シリーズ PRE-3	12.2(31)SB
Cisco 10000 シリーズ 6PE サポート	12.2(31)SB
Cisco 10000 シリーズ PRE-4	12.2(33)SB
Cisco 10720 シリーズ	
IPv6 フォワーディングのために加速された PxF	12.0(26)S、12.2(28)SB
IPv6 拡張 ACL のために加速された PxF	12.0(26)S
IPv6 over MPLS（6PE）のために加速された PxF	12.0(26)S
PRE-2 ハードウェア フォワーディング	12.2(28)SB
Cisco 7600 Series、Cisco Catalyst 6500、Cisco Catalyst 3700、および Cisco Catalyst 3500	
IPv6：Express setup	12.2(35)SE
Cisco Catalyst 3560 シリーズ	12.2(25)SEA
Cisco Catalyst 3750 シリーズ	12.2(25)SEA
IPv6：IPv6 および IPv4 TCAM テンプレート	12.2(25)SEA
IPv6：IPv6 ネイバー探索スロットリング	12.2(25)SEA
Cisco Catalyst 3560E シリーズ	12.2(35)SE2
Cisco Catalyst 3570E シリーズ	12.2(35)SE2
Cisco Catalyst 3560 シリーズ：IPv6 マルチキャスト ハードウェア レイヤ	12.2(25)SED
Supervisor Engine 720 および 720-3bxl	12.2(33)SRA
Cisco 7600 シリーズでのルート/スイッチ プロセッサ 720	12.2(33)SRB
Supervisor Engine 720 IPv6 フォワーディング	12.2(17a)SX1
Supervisor Engine 720 IPv6 拡張 ACL	12.2(17a)SX1
Supervisor Engine 720 IPv6 over MPLS（6PE）	12.2(17b)SXA
Supervisor Engine 720 IPv6 マルチキャスト ハードウェア フォワーディング	12.2(18)SXE
Supervisor Engine 720 IPv6 マルチキャスト RPR/RPR+ サポート	12.2(18)SXE
Supervisor Engine 720 IPv6 マルチキャスト ハードウェアアシスト出力レプリケーション	12.2(18)SXE
Supervisor Engine 32/MSFC2A	12.2(18)SXF

その他の 12.2S リリース トレイン

初期導入 Cisco IOS ソフトウェア Release 12.2S トレインのいくつかは、Cisco IOS ソフトウェア メインライン Release 12.2S トレインに同期します。次の表に、IPv6 ハードウェアが使用されているリリース トレインの情報を示します。

表 3　初期導入 12.2S Cisco IOS ソフトウェア リリース トレインでの IPv6 ハードウェアの最小リリース要件

初期導入 Cisco IOS ソフトウェア リリースおよびハードウェア	リリースの説明
Cisco 10000 シリーズでの 12.2(28)SB および 12.2(33)SB	Cisco IOS Release 12.2(28)SB または Cisco IOS Release 12.2(33)SB の機能の一部は、Cisco 10000 シリーズ ルータでサポートされていません。Cisco IOS Release 12.2(28)SB または Cisco IOS Release 12.2(33)SB の詳細については、http://www.cisco.com/en/US/docs/ios/12_2sb/release/notes/122SB.html の URL にあるリリース ノートを参照してください。
Cisco Catalyst 3560 および 3570 シリーズでの 12.2(25)SEA	12.2(25)SEA では、12.2S IPv6 機能セットのサブセットがサポートされます。IPv6 マルチキャストはサポートされません。
Cisco 7600 シリーズでの 12.2(33)SRA	12.2(33)SRA には、Cisco IOS ソフトウェア Release 12.2S および 12.2SX のすべての IPv6 機能が含まれています。
Cisco Catalyst 6500 での 12.2SX	12.2(17)SX には、Cisco IOS ソフトウェア Release 12.2(14)S 機能セット全部と OSPFv3 が含まれています。
Cisco Catalyst 6500 Supervisor Engine 2/MSFC2 での 12.2(17d)SXB	Cisco Catalyst 6500 Supervisor Engine 2/MSFC2 では、12.2(17)SXB に対して IPv6 がサポートされています。
Cisco Catalyst 6500 および Cisco 7600 シリーズでの 12.2(18)SXE	12.2(18)SXE では、IPv6 マルチキャスト ハードウェア フォワーディングがサポートされています。
Supervisor Engine 32/MSFC2A での 12.2(18)SXF	
Cisco Catalyst 3560E および 3570E シリーズでの 12.2(35)SE2	
Cisco Catalyst 2960 での 12.2(40)SE	MLD スヌーピングのために提供された IPv6 サポート。
UBR での 12.2(33)SCA	プレフィクス委任のために DHCPv6 リレー エージェント通知のサポートが提供されています。

その他の関連資料

ここでは、Cisco IOS IPv6 機能に関する関連資料について説明します。

関連資料

関連項目	参照先
IPv6 コマンド：コマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS IPv6 Command Reference*』

RFC

RFC	タイトル
RFC 1886	『*DNS Extensions to Support IP version 6*』
RFC 1981	『*Path MTU Discovery for IP version 6*』
RFC 2080	『*RIPng for IPv6*』
RFC 2373	『*IP Version 6 Addressing Architecture*』
RFC 2374	『*An Aggregatable Global Unicast Address Format*』
RFC 2375	『*IPv6 Multicast Address Assignments*』
RFC 2401	『*Security Architecture for the Internet Protocol*』
RFC 2402	『*IP Authentication Header*』
RFC 2404	『*The Use of Hash Message Authentication Code Federal Information Processing Standard 180-1 within Encapsulating Security Payload and Authentication Header*』
RFC 2406	『*IP Encapsulating Security Payload (ESP)*』
RFC 2407	『*The Internet Security Domain of Interpretation for ISAKMP*』
RFC 2408	『*Internet Security Association and Key Management Protocol*』
RFC 2409	『*Internet Key Exchange (IKE)*』
RFC 2460	『*Internet Protocol, Version 6 (IPv6) Specification*』
RFC 2461	『*Neighbor Discovery for IP Version 6 (IPv6)*』
RFC 2462	『*IPv6 Stateless Address Autoconfiguration*』
RFC 2463	『*Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*』
RFC 2464	『*Transmission of IPv6 Packets over Ethernet*』
RFC 2467	『*Transmission of IPv6 Packets over FDDI*』
RFC 2472	『*IP Version 6 over PPP*』
RFC 2474	『*Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*』
RFC 2475	『*An Architecture for Differentiated Services Framework*』
RFC 2492	『*IPv6 over ATM*』
RFC 2545	『*Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*』
RFC 2590	『*Transmission of IPv6 Packets over Frame Relay Specification*』
RFC 2597	『*Assured Forwarding PHB*』
RFC 2598	『*An Expedited Forwarding PHB*』
RFC 2697	『*A Single Rate Three Color Marker*』
RFC 2698	『*A Two Rate Three Color Marker*』
RFC 2710	『*Multicast Listener Discovery (MLD) for IPv6*』
RFC 2711	『*IPv6 Router Alert Option*』
RFC 2740	『*OSPF for IPv6*』
RFC 2766	『*Network Address Translation–Protocol Translation (NAT-PT)*』

RFC	タイトル
RFC 2858	『*Multiprotocol Extensions for BGP-4*』
RFC 2893	『*Transition Mechanisms for IPv6 Hosts and Routers*』
RFC 3056	『*Connection of IPv6 Domains via IPv4 Clouds*』
RFC 3068	『*An Anycast Prefix for 6to4 Relay Routers*』
RFC 3147	『*Generic Routing Encapsulation over CLNS*』
RFC 3152	『*Delegation of IP6.ARPA*』
RFC 3162	『*RADIUS and IPv6*』
RFC 3315	『*Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*』
RFC 3319	『*Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiated Protocol (SIP) Servers*』
RFC 3392	『*Capabilities Advertisement with BGP-4*』
RFC 3484	『*Default Address Selection for Internet Protocol version 6 (IPv6)*』
RFC 3513	『*Internet Protocol Version 6 (IPv6) Addressing Architecture*』
RFC 3576	『*Change of Authorization*』
RFC 3587	『*IPv6 Global Unicast Address Format*』
RFC 3590	『*Source Address Selection for the Multicast Listener Discovery (MLD) Protocol*』
RFC 3596	『*DNS Extensions to Support IP Version 6*』
RFC 3633	『*DHCP IPv6 Prefix Delegation*』
RFC 3646	『*DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*』
RFC 3697	『*IPv6 Flow Label Specification*』
RFC 3736	『*Stateless DHCP Service for IPv6*』
RFC 3756	『*IPv6 Neighbor Discovery (ND) Trust Models and Threats*』
RFC 3775	『*Mobility Support in IPv6*』
RFC 3810	『*Multicast Listener Discovery Version 2 (MLDv2) for IPv6*』
RFC 3879	『*Deprecating Site Local Addresses*』
RFC 3898	『*Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*』
RFC 3954	『*Cisco Systems NetFlow Services Export Version 9*』
RFC 3956	『*Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address*』
RFC 3963	『*Network Mobility (NEMO) Basic Support Protocol*』
RFC 3971	『*SEcure Neighbor Discovery (SEND)*』
RFC 3972	『*Cryptographically Generated Addresses (CGA)*』
RFC 4007	『*IPv6 Scoped Address Architecture*』
RFC 4075	『*Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6*』
RFC 4087	『*IP Tunnel MIB*』
RFC 4109	『*Algorithms for Internet Key Exchange version 1 (IKEv1)*』
RFC 4191	『*Default Router Preferences and More-Specific Routes*』

RFC	タイトル
RFC 4193	『*Unique Local IPv6 Unicast Addresses*』
RFC 4214	『*Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)*』
RFC 4242	『*Information Refresh Time Option for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*』
RFC 4283	『*Mobile Node Identifier Option for Mobile IPv6*』
RFC 4291	『*IP Version 6 Addressing Architecture*』
RFC 4292	『*IP Forwarding Table MIB*』
RFC 4293	『*Management Information Base for the Internet Protocol (IP)*』
RFC 4302	『*IP Authentication Header*』
RFC 4306	『*Internet Key Exchange (IKEv2) Protocol*』
RFC 4308	『*Cryptographic Suites for IPsec*』
RFC 4364	『*BGP MPLS/IP Virtual Private Networks (VPNs)*』
RFC 4382	『*MPLS/BGP Layer 3 Virtual Private Network (VPN) Management Information Base*』
RFC 4443	『*Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*』
RFC 4552	『*Authentication/Confidentiality for OSPFv3*』
RFC 4601	『*Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification*』
RFC 4649	『*Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option*』
RFC 4659	『*BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*』
RFC 4724	『*Graceful Restart Mechanism for BGP*』
RFC 4798	『*Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)*』
RFC 4862	『*IPv6 Stateless Address Autoconfiguration*』
RFC 4884	『*Extended ICMP to Support Multi-Part Messages*』
RFC 5059	『*Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)*』
RFC 5072	『*IPv6 over PPP*』
RFC 5095	『*Deprecation of Type 0 Routing Headers in IPv6*』
RFC 5120	『*M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)*』
RFC 5187	『*OSPFv3 Graceful Restart*』
RFC 5308	『*Routing IPv6 with IS-IS*』
RFC 5969	『*IPv6 Rapid Deployment on IPv4 Infrastructures (6RD) — Protocol Specification*』
draft-ietf-bfd-v4v6-1hop	『*BFD for IPv4 and IPv6 (Single Hop)*』

MIB

MIB	MIB リンク
• CISCO-CONFIG-COPY-MIB • CISCO-CONFIG-MAN-MIB • CISCO-DATA-COLLECTION-MIB • CISCO-FLASH-MIB • CISCO-IETF-IP-FORWARDING-MIB（Cisco IOS Release 12.2(33)SRC 以降使用不能） • CISCO-IETF-IP-MIB（Cisco IOS Release 12.2(33)SRC 以降使用不能） • CISCO-IP-FORWARD-MIB • CISCO-IP-MIB • CISCO-RTTMON-IPv6-MIB • CISCO-SNMP-TARGET-EXT-MIB • ENTITY-MIB • NOTIFICATION-LOG-MIB • SNMP-TARGET-MIB • TUNNEL-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

IPv6 アドレッシングと基本接続の実装

Cisco IOS ソフトウェアでの基本的な IPv6 接続の実装は、個々のルータ インターフェイスへの IPv6 アドレスの割り当てで構成されます。IPv6 トラフィックの転送はグローバルにイネーブルにでき、IPv6 のシスコ エクスプレス フォワーディング スイッチングをイネーブルにすることもできます。基本接続は、Domain Name System（DNS; ドメイン ネーム システム）の名前からアドレスおよびアドレスから名前のルックアップ プロセスで AAAA レコード タイプのサポートを設定し、IPv6 ネイバー探索を管理することで拡張できます。

この章では、IPv6 アドレッシングおよび基本 IPv6 接続の作業について説明します。

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「IPv6 アドレッシングと基本接続の実装の機能情報」（P.63）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

IPv6 アドレッシングと基本接続の実装の前提条件

- このマニュアルでは、IPv4 に精通していることを前提としています。IPv4 の設定およびコマンド リファレンス情報については、「その他の関連資料」に示されている資料を参照してください。
- Cisco Express Forwarding for IPv6 および分散型 Cisco Express Forwarding for IPv6 には、次の前提条件が適用されます。
  - シスコ エクスプレス フォワーディングまたは分散型シスコ エクスプレス フォワーディングを使用して IPv6 トラフィックを転送するには、**ipv6 unicast-routing** コマンドを使用してルータ上で IPv6 ユニキャスト データグラムの転送をグローバルに設定するか、**ipv6 address** コマンドを使用してインターフェイスに IPv6 アドレスを設定する必要があります。
  - **ipv6 cef** コマンドを使用してルータ上で Cisco Express Forwarding for IPv6 をグローバルにイネーブルにする前に、**ip cef** コマンドを使用してルータ上で Cisco Express Forwarding for IPv4 をグローバルにイネーブルにする必要があります。
  - Cisco 7500 シリーズ ルータなど、シスコ エクスプレス フォワーディングと分散型シスコ エクスプレス フォワーディングの両方をサポートする分散型アーキテクチャ プラットフォームでは、**ipv6 cef distributed** コマンドを使用してルータ上で分散型 Cisco Express Forwarding for IPv6 をグローバルにイネーブルにする前に、**ip cef distributed** コマンドを使用してルータ上で分散型 Cisco Express Forwarding for IPv4 をグローバルにイネーブルにする必要があります。

（注） デフォルトでは、Gigabit Switch Router（GSR; ギガビット スイッチ ルータ）では分散型シスコ エクスプレス フォワーディングだけがサポートされます。

  - ユニキャスト Reverse Path Forwarding（RPF）を使用するには、ルータでシスコ エクスプレス フォワーディング スイッチングまたは分散型シスコ エクスプレス フォワーディング スイッチングをイネーブルにします。シスコ エクスプレス フォワーディング スイッチングの入力インターフェイスを設定する必要はありません。シスコ エクスプレス フォワーディングがルータ上で実行されているかぎり、個々のインターフェイスは他のスイッチング モードで設定できます。

（注） ユニキャスト RPF が機能するためには、ルータでシスコ エクスプレス フォワーディングがグローバルに設定されている必要があります。ユニキャスト RPF は、シスコ エクスプレス フォワーディングがないと動作しません。

IPv6 アドレッシングと基本接続の実装の制約事項

- Cisco IOS Release 12.2(11)T またはそれ以前のリリースでは、IPv6 はパケット転送に対してプロセス スイッチングだけをサポートします。IPv6 のシスコ エクスプレス フォワーディング スイッチングおよび分散型シスコ エクスプレス フォワーディング スイッチングは、Cisco IOS Release 12.2(13)T でサポートされています。IPv6 の分散型シスコ エクスプレス フォワーディング スイッチングは、Cisco IOS Release 12.0(21)ST でサポートされています。
- レイヤ 2 LAN スイッチは IPv6 フレームを転送する前にレイヤ 3 パケット情報を調べないため、IPv6 パケットはレイヤ 2 LAN スイッチに対して透過的です。したがって、IPv6 ホストをレイヤ 2 LAN スイッチに直接接続できます。

- IPv6 がサポートされている任意の Cisco IOS リリースでは、1 つのインターフェイス上で同じプレフィクス内に複数の 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。1 つのインターフェイス上での同じプレフィクス内の複数の IPv6 グローバル アドレスの設定については、「例：IPv6 アドレッシングと IPv6 ルーティングの設定」を参照してください。
- RFC 3879 ではサイトローカル アドレスの使用が廃止されたため、プライベート IPv6 アドレスの設定は、RFC 4193 の Unique Local Addressing（ULA）に関する推奨事項に従って行う必要があります。
- IPv6 での Bridge-Group Virtual Interface（BVI; ブリッジ グループ仮想インターフェイス）は、NAT-PT およびワイヤレス インターフェイス Dot11Radio でサポートされません。

IPv6 アドレッシングと基本接続の実装に関する情報

Cisco IOS ソフトウェアの IPv6

以前は IPng（次世代）と呼ばれていた IPv6 は、Internet Protocol（IP; インターネット プロトコル）の最新バージョンです。IP は、デジタル ネットワーク上でデータ、音声、およびビデオ トラフィックの交換に使用するパケットベースのプロトコルです。IP Version 4（IPv4; IP バージョン 4）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。長い議論のあとで、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 は当初、Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）によって発行された RFC 2460『*Internet Protocol, Version 6 (IPv6) Specification*』に規定されていました。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。

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; サービス品質）、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。より大きな IPv6 アドレス空間により、ネットワークが拡張可能になり、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 プレフィクス集約、簡略化されたネットワーク リナンバリング、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 では、Routing Information Protocol（RIP; ルーティング情報プロトコル）、Integrated Intermediate System-to-Intermediate System（IS-IS）、Open Shortest Path First for IPv6、マルチプロトコル Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）などの広く導入されているルーティング プロトコルがサポートされます。使用可能なその他の機能として、ステートレス自動設定、拡張されたモバイル IPv6 のサポート、および増やされたマルチキャスト アドレス数があります。

一意のアドレスを確保するための大きな IPv6 アドレス空間

IPv6 の主な開発動機は、将来的に予想されるグローバルに一意な IP アドレスの需要を満たす必要性です。モバイル インターネット対応デバイス（Personal Digital Assistants（PDA）、電話、カードなど）、Home-Area Networks（HAN; ホームエリア ネットワーク）、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加しています。IPv6 は、ネットワーク アドレス ビット数を 32 ビット（IPv4）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 アドレスの必要性と Network Address Translation（NAT; ネットワーク アドレス変換）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 アドレスの形式

IPv6 アドレスは、x: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、中央、または末尾にある連続するゼロの 16 進フィールドを圧縮できます（コロンは連続するゼロの 16 進フィールドを表します）。表 1 に、圧縮された IPv6 アドレスの形式をリストします。

連続する 16 ビット値がゼロとして指定されている場合は、2 つのコロンを *ipv6-address* 引数の一部として使用できます。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	2001::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 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 アドレスを物理インターフェイスに割り当てることはできません。送信元または宛先のアドレスとして IPv6 ループバック アドレスを含むパケットは、そのパケットを作成したノードの外には転送できません。IPv6 ルータは、送信元または宛先のアドレスとして IPv6 ループバック アドレスを含むパケットを転送しません。

表 1 にリスト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 ネットワーク上の新規に初期化されたノードは、IPv6 アドレスを受け取るまで、パケット内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 未指定アドレスをインターフェイスに割り当てることはできません。未指定 IPv6 アドレスは、IPv6 パケット内の宛先アドレスまたは IPv6 ルーティング ヘッダーとして使用しないでください。

ipv6-prefix/*prefix-length* の形式の IPv6 アドレス プレフィクスを使用して、アドレス空間全体のビット単位の連続ブロックを表すことができます。*ipv6-prefix* は、RFC 2373 に記載された形式で指定する必要があります。この形式では、アドレスは、16 進数値を 16 ビット単位でコロンで区切って指定します。プレフィクス長は、アドレスのうち連続する上位何ビットがプレフィクス（アドレスのネットワーク部）を構成するかを示す 10 進数値です。たとえば、2001:0DB8:8086:6502::/32 は有効な IPv6 プレフィクスです。

IPv6 アドレス タイプ：ユニキャスト

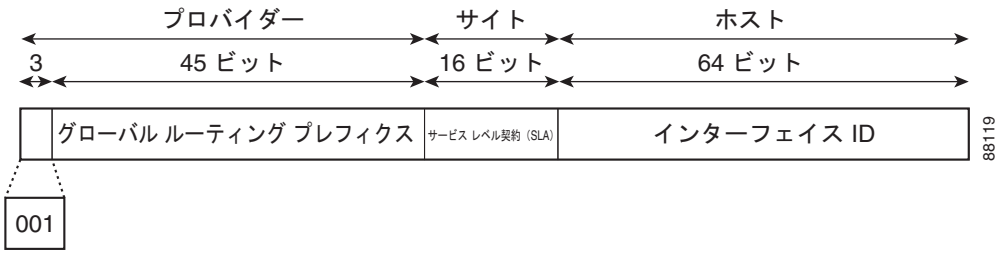
IPv6 ユニキャスト アドレスは、単一ノード上の単一インターフェイスの識別子です。ユニキャスト アドレスに送信されたパケットは、そのアドレスが示すインターフェイスに配信されます。Cisco IOS ソフトウェアでは、次の IPv6 ユニキャスト アドレス タイプがサポートされます。

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、集約可能グローバル ユニキャスト プレフィクスによる 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、組織を上に向かって、最終的に Internet Service Provider（ISP; インターネット サービス プロバイダー）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。IPv6 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。図 1 に、集約可能グローバル アドレスの構造を示します。

図 1　　集約可能グローバル アドレスの形式



2000::/3（001）～ E000::/3（111）のプレフィクスを持つアドレスには、Extended Universal Identifier（EUI; 拡張ユニバーサル識別子）64 形式の 64 ビット インターフェイス識別子が必要です。Internet Assigned Numbers Authority（IANA; インターネット割り当て番号局）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 プレフィクスと、16 ビットのサブネット ID または Site-Level Aggregator（SLA; サイトレベル集約）で構成されます。IPv6 集約可能グローバル ユニキャスト アドレス形式の文書（RFC 2374）では、グローバル ルーティング プレフィクスには、Top-Level Aggregator（TLA; 最上位レベル集約）および Next-Level Aggregator（NLA; 次レベル集約）という他の 2 つの階層構造フィールドが含まれるとされていました。TLS フィールドと NLA フィールドはポリシーベースであるため、IETF はこれらのフィールドを RFC から削除することを決定しました。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 アドレッシ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レイヤ アドレスと同じか、リンクレイヤ 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 タイプで使用され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された EUI-64 形式で構築されます。

- すべての IEEE 802 インターフェイス タイプ（イーサネット、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の 48 ビット リンクレイヤ アドレス（Media Access Control（MAC; メディア アクセス制御）アドレス）の Organizational Unique Identifier（OUI; 組織固有識別子）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; ユニバーサル/ローカル）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。
- その他のすべてのインターフェイス タイプ（シリアル ループバック、ATM、フレーム リレー、トンネル インターフェイスタイプなど。ただし、IPv6 オーバーレイ トンネルで使用されるトンネル インターフェイスを除く）の場合、インターフェイス ID は IEEE 802 インターフェイス タイプのインターフェイス ID と同じように構築されますが、識別子の構築にはルータの MAC アドレス プールの最初の MAC アドレスが使用されます（インターフェイスには MAC アドレスがないため）。
- 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） Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）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。

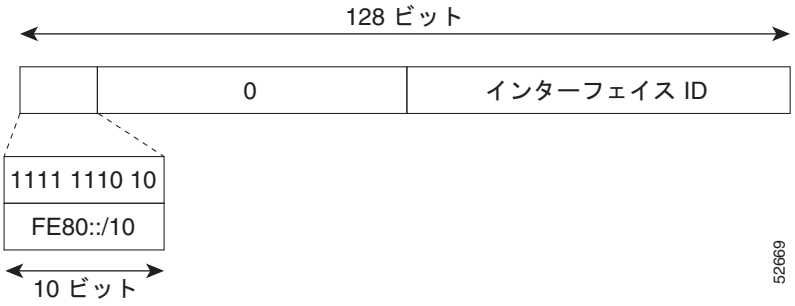
1. ルータに MAC アドレスが（ルータの MAC アドレス プールから）照会されます。
2. 使用可能な MAC アドレスがルータにない場合は、ルータのシリアル番号を使用してリンクローカル アドレスが作成されます。
3. リンクローカル アドレスの作成にルータのシリアル番号を使用できない場合、ルータは Message Digest Algorithm 5（MD5）ハッシュを使用して、ルータのホスト名からルータの MAC アドレスを決定します。

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どのインターフェイスでも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トレス自動設定プロセスで使用されます。ローカル リンク上のノードは、リンクローカル アドレスを使用して通信できます。ノードの通信にグローバルに一意のアドレスは不要です。図 2 に、リンクローカル アドレスの構造を示します。

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。

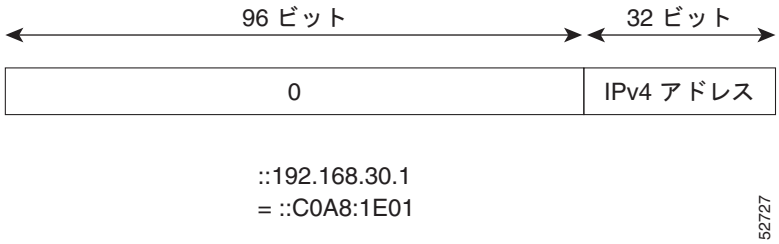
図 2　　リンクローカル アドレスの形式



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。図 3 に、IPv4 互換 IPv6 アドレスの構造と、許容されるいくつかのアドレス形式を示します。

図 3　　IPv4 互換 IPv6 アドレスの形式



一意のローカル アドレス

一意のローカル アドレスは、グローバルに一意であり、ローカル通信を目的とした IPv6 ユニキャスト アドレスです。グローバル インターネット上でのルーティングには対応しておらず、サイトなどの限定されたエリア内でルーティング可能です。限定された複数のサイト間でルーティングされることもあります。

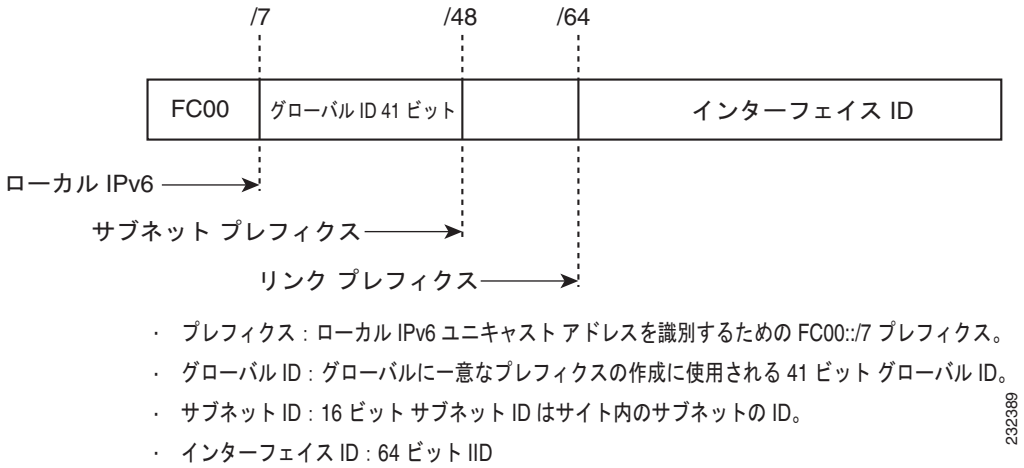
一意のローカル アドレスには、次の特性があります。

- グローバルに一意のプレフィクスがある（一意である可能性が高い）。
- 既知のプレフィクスがあるため、サイト境界で簡単にフィルタリングできる。
- アドレス競合を発生させたり、これらのプレフィクスを使用するインターフェイスのリナンバリングを必要としたりすることなく、サイトを結合またはプライベートに相互接続できる。
- ISP に依存せず、永続的または断続的なインターネット接続がなくてもサイト内での通信に使用できる。

- ルーティングまたは DNS により誤ってサイト外にリークされた場合でも、他のアドレスと競合しない。
- アプリケーションは、一意のローカル アドレスをグローバル スコープのアドレスのように扱うことができる。

図 4 に、一意のローカル アドレスの構造を示します。

図 4　一意のローカル アドレスの構造



サイトローカル アドレス

RFC 3879 ではサイトローカル アドレスの使用が廃止されたため、プライベート IPv6 アドレスの設定は、RFC 4193 の Unique Local Addressing（ULA）に関する推奨事項に従って行う必要があります。

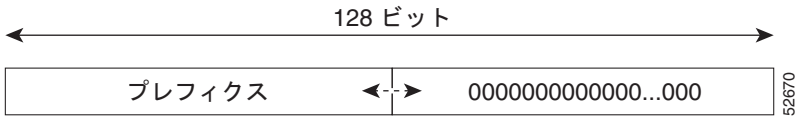
IPv6 アドレス タイプ：エニーキャスト

エニーキャスト アドレスは、通常は異なるノードに属するインターフェイスのセットに割り当てられます。エニーキャスト アドレスに送信されたパケットは、使用しているルーティング プロトコルの定義に従って、そのエニーキャスト アドレスが示す最も近いインターフェイスに送信されます。エニーキャスト アドレスは、ユニキャスト アドレス空間から割り当てられるため、その構文ではユニキャスト アドレスと区別できません。ユニキャスト アドレスを複数のインターフェイスに割り当てると、ユニキャスト アドレスがエニーキャスト アドレスになります。エニーキャスト アドレスが割り当てられたノードは、アドレスがエニーキャスト アドレスであることを認識するように明示的に設定されている必要があります。

（注） エニーキャスト アドレスを使用できるのはルータだけです。ホストでは使用できません。エニーキャスト アドレスは、IPv6 パケットの送信元アドレスとして使用できません。

図 5 に、サブネット ルータ エニーキャスト アドレスの形式を示します。アドレスには、連続するゼロで連結されたプレフィクス（インターフェイス ID）があります。サブネット ルータ エニーキャスト アドレスを使用すると、サブネット ルータ エニーキャスト アドレスのプレフィクスが示すリンク上のルータに到達できます。

図 5　サブネット ルータ エニーキャスト アドレスの形式



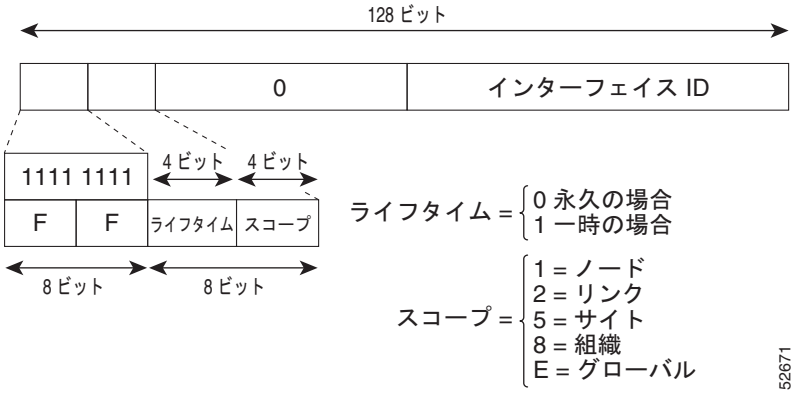
次に、6to4 リレー ルータのエニーキャスト プレフィクスの設定を示します。

```
interface Tunnel0
no ip address
ipv6 address 2001:0DB8:A00:1::1/64
ipv6 address 2001:oDB8:c058:6301::/128 anycast
tunnel source Ethernet0
tunnel mode ipv6ip 6to4
!
interface Ethernet0
ip address 10.0.0.1 255.255.255.0
ip address 192.88.99.1 255.255.255.0 secondary
!
ipv6 route 2001:0DB8::/16 Tunnel0
!
```

IPv6 アドレス タイプ：マルチキャスト

IPv6 マルチキャスト アドレスは、FF00::/8（1111 1111）というプレフィクスを持つ IPv6 マルチキャスト アドレスです。IPv6 マルチキャスト アドレスは、通常は異なるノードに属するインターフェイスのセットの識別子です。マルチキャスト アドレスに送信されたパケットは、マルチキャスト アドレスが示すすべてのインターフェイスに配信されます。プレフィクスに続く 2 番めのオクテットで、マルチキャスト アドレスのライフタイムとスコープが定義されます。永続マルチキャスト アドレスはライフタイム パラメータが 0 と等しく、一時マルチキャスト アドレスはライフタイム パラメータが 1 と等しくなっています。ノード、リンク、サイト、または組織のスコープ、またはグローバル スコープを持つマルチキャスト アドレスのスコープ パラメータは、それぞれ 1、2、5、8、E です。たとえば、プレフィクスが FF02::/16 のマルチキャスト アドレスは、リンク スコープを持つ永続マルチキャスト アドレスです。図 6 に、IPv6 マルチキャスト アドレスの形式を示します。

図 6　IPv6 マルチキャスト アドレスの形式



IPv6 ノード（ホストとルータ）は、（受信パケットの宛先となる）次のマルチキャスト グループに加入する必要があります。

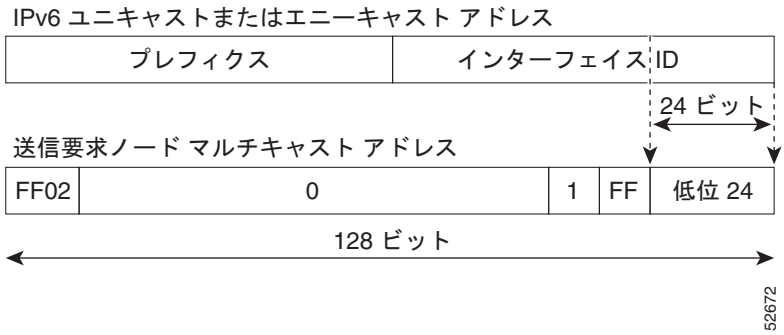
- 全ノード マルチキャスト グループ FF02:0:0:0:0:0:0:1（スコープはリンクローカル）

- 割り当てられたユニキャスト アドレスおよびエニーキャスト アドレスごとの請求ノード マルチキャスト グループ FF02:0:0:0:0:1:FF00:0000/104

IPv6 ルータは、全ルータ マルチキャスト グループ FF02:0:0:0:0:0:0:2（スコープはリンクローカル）にも加入する必要があります。

請求ノード マルチキャスト アドレスは、IPv6 ユニキャスト アドレスまたはエニーキャスト アドレスに対応するマルチキャスト グループです。IPv6 ノードは、割り当てられているユニキャスト アドレスおよびエニーキャスト アドレスごとに、関連付けられた請求ノード マルチキャスト グループに加入する必要があります。IPv6 請求ノード マルチキャスト アドレスには、対応する IPv6 ユニキャスト アドレスまたは IPv6 エニーキャスト アドレスの下位 24 ビットに連結されたプレフィクス FF02:0:0:0:0:1:FF00:0000/104 があります（図 7 を参照）。たとえば、IPv6 アドレス 2037::01:800:200E:8C6C に対応する請求ノード マルチキャスト アドレスは FF02::1:FF0E:8C6C です。請求ノード アドレスは、ネイバー請求メッセージで使用されます。

図 7　　IPv6 請求ノード マルチキャスト アドレスの形式



（注）　IPv6 にはブロードキャスト アドレスがありません。IPv6 マルチキャスト アドレスがブロードキャスト アドレスの代わりに使用されます。

IPv6 マルチキャスト グループ

インターフェイスが IPv6 トラフィックを転送するためには、そのインターフェイス上に 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。

- インターフェイスに割り当てられたユニキャスト アドレスおよびエニーキャスト アドレスごとの請求ノード マルチキャスト グループ FF02:0:0:0:0:1:FF00::/104
- 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）　請求ノード 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。

IPv6 マルチキャストの詳細については、「*Implementing IPv6 Multicast*」を参照してください。

IPv6 アドレスの出力表示

IPv6 または IPv4 コマンドの出力に IPv6 アドレスが表示される場合、長い IPv6 アドレスが隣接フィールドにオーバーフローし、出力が読みにくくなることがあります。出力フィールドは、考えられる最長の IPv4 アドレス（15 文字）に対応するように設計されました。IPv6 アドレスは最大 39 文字です。適切な長さの IPv6 アドレスを表示し、必要に応じて以降のフィールドを次の行に移動するために、以下の方式が IPv4 および IPv6 コマンドに採用されました。移動されるフィールドは、ヘッダー行に位置揃えされます。

たとえば、**where** コマンドからの出力表示を使用すると、8 の接続が表示されます。最初の 6 つの接続には IPv6 アドレスを使用し、最後の 2 つの接続には IPv4 アドレスを使用しています。

```
Router# where

Conn Host                 Address             Byte  Idle Conn Name
   1 test5                2001:0DB8:3333:4::5    6    24 test5
   2 test4                2001:0DB8:3333:44::5
                                                 6    24 test4
   3 2001:0DB8:3333:4::5 2001:0DB8:3333:4::5    6    24 2001:0DB8:3333:4::5
   4 2001:0DB8:3333:44::5
                          2001:0DB8:3333:44::5
                                                 6    23 2001:0DB8:3333:44::5
   5 2001:0DB8:3000:4000:5000:6000:7000:8001
                          2001:0DB8:3000:4000:5000:6000:7000:8001
                                                 6    20 2001:0DB8:3000:4000:5000:6000:
   6 2001:0DB8:1::1       2001:0DB8:1::1         0     1 2001:0DB8:1::1
   7 10.1.9.1             10.1.9.1               0     0 10.1.9.1
   8 10.222.111.222       10.222.111.222         0     0 10.222.111.222
```

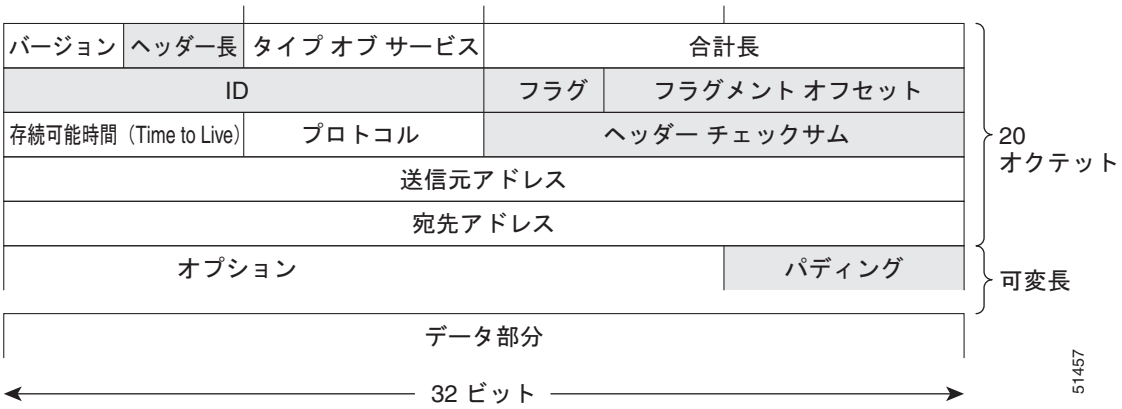
接続 1 には、アドレス フィールドの最大アドレス長を使用する IPv6 アドレスが含まれます。接続 2 では、IPv6 アドレスによってアドレス フィールドがオーバーフローし、以降のフィールドが次の行に移動されますが、適切なヘッダーに位置揃えされていることが示されています。接続 3 には、どの行もラップせずにホスト名フィールドとアドレス フィールドの最大長を充てんする IPv6 が含まれます。接続 4 は、ホスト名フィールドとアドレス フィールドの両方に長い IPv6 アドレスが含まれる場合の結果を示しています。出力は、適切な見出し位置を維持したまま、3 行にわたって表示されています。接続 5 は、接続 4 と同様の結果を示していますが、ホスト名フィールドとアドレス フィールドに非常に長い IPv6 アドレスがあります。実際には、接続名フィールドは切り捨てられています。接続 6 では、表示の変更が不要な非常に短い IPv6 アドレスが表示されます。接続 7 および 8 では、短い IPv4 アドレスと長い IPv4 アドレスが表示されます。

（注） IPv6 アドレスの出力表示は、IPv6 アドレスを表示するすべてのコマンドに適用されます。

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（図 8 を参照）。この 12 個のフィールドのあとにはオプション フィールドが続く場合があり、さらにそのあとに、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。図 8 に示す IPv4 パケット ヘッダーのグレーのフィールドは、IPv6 パケット ヘッダーに含まれません。

図 8　IPv4 パケット ヘッダーの形式



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（図 9 を参照）。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 レイヤ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 レイヤとトランスポート レイヤで使用されます（IPv4 では、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）トランスポート レイヤでオプションのチェックサムが使用されます。IPv6 では、内部パケットの整合性をチェックするために UDP チェックサムを使用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 ビットに揃えられるため、IPv6 パケットの処理が簡単になります。

図 9　IPv6 パケット ヘッダーの形式

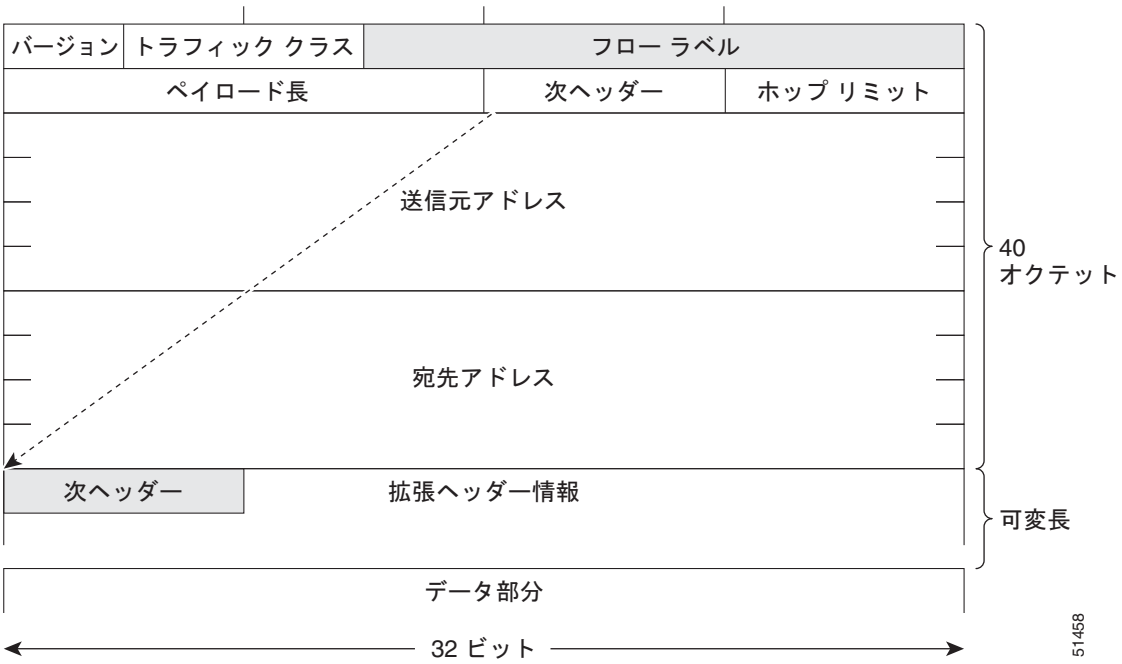


表 2 に、IPv6 パケット ヘッダーのフィールドをリストします。

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。
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されるトラフィック 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 レイヤ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 ヘッダーに続く情報のタイプは、図 9 に示すように、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 つのフィールドのあとに、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。拡張ヘッダーが存在する場合は、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。図 10 に、IPv6 拡張ヘッダー形式を示します。

図 10　　IPv6 拡張ヘッダーの形式

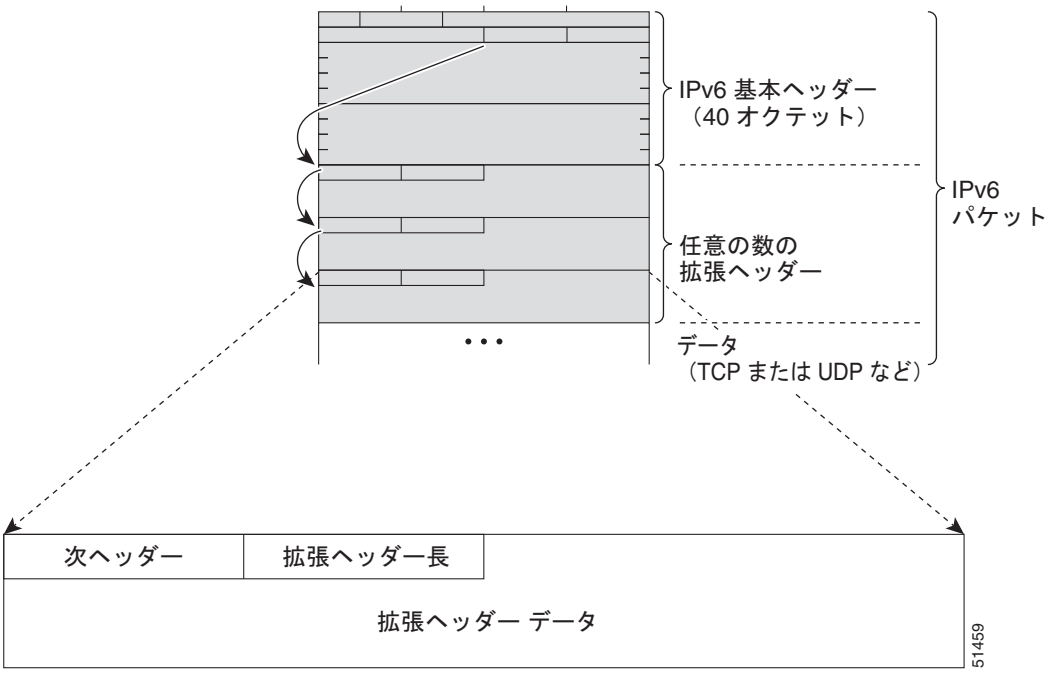


表 3 に、拡張ヘッダー タイプとその次ヘッダー フィールド値をリストします。

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 ヘッダーのあと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 Encapsulating Security Payload（ESP; カプセル化セキュリティ ペイロード）ヘッダーのあと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 Maximum Transmission Unit（MTU; 最大伝送ユニット）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。
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 Security Protocol（IPsec; IP セキュリティ プロトコル）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用さ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	135	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、対応ノード、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。

IPv6 のシスコ エクスプレス フォワーディング スイッチングと分散型シスコ エクスプレス フォワーディング スイッチング

シスコ エクスプレス フォワーディングは、IPv6 パケットを転送するための高度なレイヤ 3 IP スイッチング テクノロジーです。分散型シスコ エクスプレス フォワーディングは、シスコ エクスプレス フォワーディングと同じ機能を実行しますが、GSR や Cisco 7500 シリーズ ルータなどの分散型アーキテクチャ プラットフォーム用です。分散型 Cisco Express Forwarding for IPv6 および Cisco Express Forwarding for IPv6 は、分散型 Cisco Express Forwarding for IPv4 および Cisco Express Forwarding for IPv4 と同じ機能と利点を提供します。使用しているルーティング プロトコルの指示に従って追加、削除、または変更された IPv6 Routing Information Base（RIB; ルーティング情報ベース）のネットワーク エントリが Forwarding Information Bases（FIB; 転送情報ベース）に反映され、IPv6 隣接関係テーブルによって各 FIB のすべてのエントリのレイヤ 2 ネクストホップ アドレスが管理されます。

（注） デフォルトでは、GSR では、分散型シスコ エクスプレス フォワーディングだけがサポートされます（シスコ エクスプレス フォワーディング スイッチングはライン カードによって実行されます）。Cisco 7500 シリーズ ルータでは、シスコ エクスプレス フォワーディングと分散型シスコ エクスプレス フォワーディングの両方がサポートされます。シスコ エクスプレス フォワーディングが Cisco 7500 シリーズ ルータ上に設定されている場合、シスコ エクスプレス フォワーディング スイッチングは Route Processor（RP; ルート プロセッサ）によって実行されます。分散型シスコ エクスプレス フォワーディングが設定されている場合、シスコ エクスプレス フォワーディング スイッチングはライン カードによって実行されます。

Cisco IOS Release 12.0(21)ST では、分散型 Cisco Express Forwarding には IPv6 アドレスおよびプレフィクスのサポートが含まれていました。Cisco IOS Release 12.0(22)S またはそれ以降のリリース、および Cisco IOS Release 12.2(13)T またはそれ以降のリリースでは、分散型シスコ エクスプレス フォワーディングとシスコ エクスプレス フォワーディングが拡張され、IPv6 のグローバル アドレスおよびリンクローカル アドレス用に別々の FIB がサポートされるようになりました。

各 IPv6 ルータ インターフェイスには、1 つの IPv6 グローバル FIB と 1 つの IPv6 リンクローカル FIB への関連付けがあります（複数のインターフェイスが同じ FIB への関連付けを持つことができます）。同じ IPv6 リンクに接続されているすべての IPv6 ルータ インターフェイスが、同じ IPv6 リンクローカル FIB を共有します。IPv6 グローバル宛先アドレスを持つ IPv6 パケットは IPv6 グローバル FIB によって処理されますが、IPv6 グローバル宛先アドレスと IPv6 リンクローカル送信元アドレスを持つパケットは、プロセス スイッチングとスコープエラー処理のために RP に送信されます。リンクローカル送信元アドレスを持つパケットはローカル リンクの外部に転送されず、プロセス スイッチングとスコープエラー処理のために RP に送信されます。

ユニキャスト Reverse Path Forwarding

ユニキャスト RPF 機能を使用すると、IPv6 ルータを経由する不正形式または偽造（スプーフィング）IPv6 送信元アドレスを原因とする問題が軽減されます。不正形式または偽造送信元アドレスは、送信元 IPv6 アドレス スプーフィングに基づく Denial-of-Service（DoS; サービス拒絶）攻撃を示すことがあります。

インターフェイスでユニキャスト RPF がイネーブルになっている場合、ルータはそのインターフェイスで受信したすべてのパケットを調べます。ルータは、送信元アドレスがルーティング テーブルにあり、パケットを受信したインターフェイスと一致することを確認します。ルックアップは FIB の存在に依存するため、この「後方参照」機能はシスコ エクスプレス フォワーディングがルータでイネーブルになっている場合にだけ使用可能です。シスコ エクスプレス フォワーディングでは、その動作の一部として FIB が生成されます。

（注） ユニキャスト RPF は入力機能であり、接続のアップストリーム エンドのルータの入力インターフェイスだけに適用されます。

ユニキャスト RPF 機能では、ルータ インターフェイスで受信されたパケットが、パケットの送信元への最良リターン パスの 1 つで着信するかどうかが検証されます。この機能では、シスコ エクスプレス フォワーディング テーブルのリバース ルックアップが実行されます。ユニキャスト RPF がパケットのリバース パスを見つけることができない場合、ユニキャスト RPF は、Access Control List（ACL; アクセス コントロール リスト）が指定されているかどうかに応じてパケットをドロップまたは転送できます。ACL が指定されている場合は、パケットがユニキャスト RPF チェックに失敗した場合にだけ、パケットが（ACL の deny 文を使用して）ドロップされる必要があるか、（ACL の permit 文を使用して）転送される必要があるかを確認するために ACL がチェックされます。パケットがドロップされるか転送されるかにかかわらず、パケットは、ユニキャスト RPF ドロップのグローバル IP トラフィック統計情報とユニキャスト RPF のインターフェイス統計情報でカウントされます。

ACL が指定されていない場合、ルータは偽造または不正形式のパケットを即時にドロップし、ACL ロギングは行われません。ルータおよびインターフェイス ユニキャスト RPF カウンタが更新されます。

RPF イベントは、ACL エントリのロギング オプションを指定することでロギングできます。ログ情報を使用して、送信元アドレスや時間など、攻撃に関する情報を収集できます。

（注） ユニキャスト RPF では、コストが等しいすべての「最良」リターン パスが有効と見なされます。複数のリターン パスが存在していても、各パスのルーティング コスト（ホップ数や加重など）が他のパスと等しく、そのルートが FIB 内にあるかぎり、ユニキャスト RPF は機能します。

IPv6 の DNS

IPv6 では、DNS の名前からアドレスおよびアドレスから名前のルックアップ プロセスでサポートされる DNS レコード タイプがサポートされます。DNS レコード タイプでは、IPv6 アドレスがサポートされます。IPv6 では、IPv6 アドレスから DNS 名への逆マッピングもサポートされます。

ネーム サーバを使用して、ドメイン名に関連付けられている情報を追跡します。ネーム サーバでは、ホスト名からアドレスへのマッピングのデータベースを維持できます。各名前は、1 つ以上の IPv4 アドレス、IPv6 アドレス、または両方のアドレス タイプにマッピングできます。このサービスを使用してドメイン名を IPv6 アドレスにマッピングするには、ネーム サーバを指定し、DNS をイネーブルにする必要があります。

Cisco IOS ソフトウェアは、**connect**、**telnet**、**ping** の各コマンド、関連する Telnet サポート操作、およびコマンド出力を生成する他の多くのコマンドで使用するために、ホスト名からアドレスへのマッピングのキャッシュを維持します。このキャッシュによって、名前からアドレスへの変換が高速になります。

IPv4 と同様に、IPv6 で使用されるネーミング方式では、ドメインに対して提供する階層名前空間内の場所によってネットワーク デバイスを識別できます。ドメイン名は、ピリオド（.）を区切り文字として結合されます。たとえば、シスコは com ドメイン名で識別される商業組織であるため、ドメイン名は cisco.com です。このドメイン内の特定のデバイス、たとえば FTP サーバは、ftp.cisco.com として識別されます。

（注） IP6.ARPA サポートは、Cisco IOS Release 12.3(11)T で追加されました。IP6.ARPA は、Cisco IOS Release 12.3(11)T よりも前のリリースではサポートされていません。

表 4 に、IPv6 DNS レコード タイプをリストします。

表 4　IPv6 DNS レコード タイプ

レコード タイプ	説明	形式
AAAA	ホスト名を IPv6 アドレスにマッピングします(IPv4 の A レコードと同等)。 （注） IPv6 トランスポートまたは IPv4 トランスポートでの AAAA レコードと A レコードは、Cisco IOS Release 12.2(8)T またはそれ以降のリリースでサポートされます。	www.abc.test AAAA 3FFE:YYYY:C18:1::2
PTR	IPv6 アドレスをホスト名にマッピングします（IPv4 の PTR レコードと同等)。 （注） Cisco IOS ソフトウェアでは、IP6.INT ドメインの PTR レコードの解決がサポートされます。	2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.1.c.0.y.y.y.y.e.f.f.3.ip6.int PTR www.abc.test

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。

（注） 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 値の使用が推奨されます。

シスコ検出プロトコル IPv6 アドレスのサポート

ネイバー情報機能向けのシスコ検出プロトコル IPv6 アドレス サポートにより、2 台のシスコ デバイス間で IPv6 アドレッシング情報を転送できます。IPv6 アドレス向けシスコ検出プロトコル サポートでは、ネットワーク管理製品とトラブルシューティング ツールに IPv6 情報が提供されます。

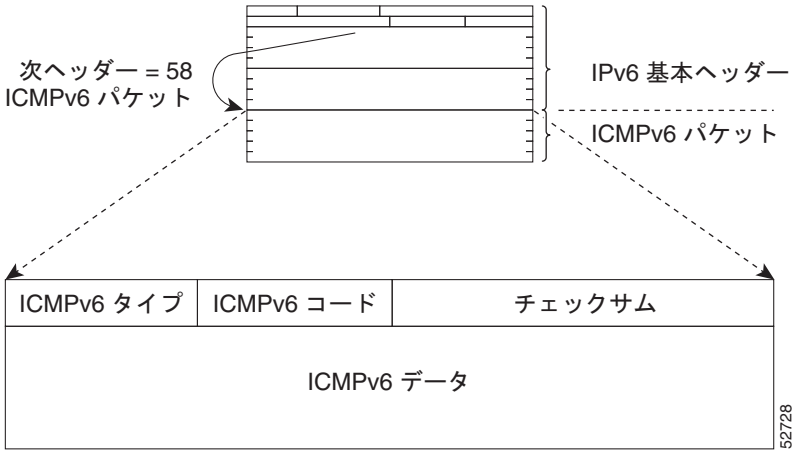
IPv6 の ICMP

IPv6 の Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）の機能は、IPv4 の ICMP と同じです。ICMP は、ICMP 宛先到達不能メッセージなどのエラー メッセージと、ICMP エコー要求および応答メッセージなどの情報メッセージを生成します。また、IPv6 の ICMP パケットは、IPv6 ネイバー探索プロセス、パス MTU ディスカバリ、および Multicast Listener Discovery（MLD; マルチキャスト リスナー ディスカバリ）プロトコル for IPv6 で使用されます。MLD は、直接接続リンク上でマルチキャスト リスナー（特定のマルチキャスト アドレス宛てのマルチキャスト パケットを受信するノード）を検出するために IPv6 によって使用されます。MLD は、バージョン 2 の Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）for IPv4 をベースとしています。

基本 IPv6 パケット ヘッダーの次ヘッダー フィールドの値 58 は、IPv6 ICMP パケットを示します。IPv6 の ICMP パケットは、ICMP パケットがすべての拡張ヘッダーのあとに続き、IPv6 パケット内の最後の情報部分であるという点で、トランスポートレイヤ パケットと同様です。IPv6 ICMP パケット

内の ICMPv6 タイプ フィールドと ICMPv6 コード フィールドは、ICMP メッセージ タイプなどの IPv6 ICMP パケットの詳細を示します。チェックサム フィールドの値は、（送信側で計算し、受信側がチェックすることにより）IPv6 ICMP パケットと IPv6 擬似ヘッダーのフィールドから抽出されます。ICMPv6 データ フィールドには、IP パケット処理に関連するエラー情報または診断情報が含まれます。図 11 に、IPv6 ICMP パケット ヘッダーの形式を示します。

図 11　　IPv6 ICMP パケット ヘッダーの形式



IPv6 ICMP レート制限

Cisco IOS Release 12.2(8)T またはそれ以降のリリースでは、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、traceroute 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、traceroute 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。

IPv6 ネイバー探索

IPv6 ネイバー探索プロセスでは、ICMP メッセージおよび請求ノード マルチキャスト アドレスを使用して、同じネットワーク（ローカル リンク）上のネイバーのリンクレイヤ 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、ネイバー ルータを追跡します。

ネイバー探索機能の IPv6 スタティック キャッシュ エントリにより、IPv6 ネイバー キャッシュ内にスタティック エントリを作成できます。スタティック ルーティングでは、管理者が、各ルータの各インターフェイスの IPv6 アドレス、サブネット マスク、ゲートウェイ、および対応する MAC アドレスをテーブルに入力する必要があります。スタティック ルーティングによって、より詳細な制御が可能になりますが、テーブルの保守作業が増えます。ルートが追加または変更されるたびにテーブルを更新する必要があります。

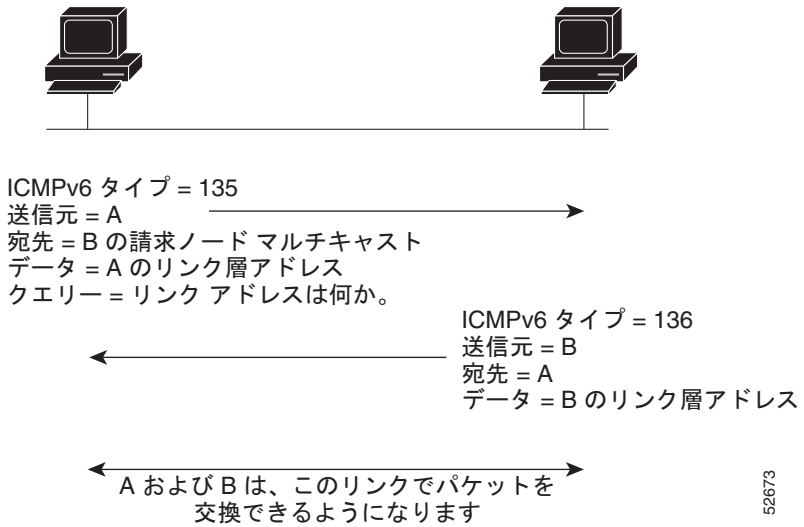
ステートフル スイッチオーバー

IPv6 ネイバー探索では、シスコ エクスプレス フォワーディングを使用した Stateful Switchover（SSO; ステートフル スイッチオーバー）がサポートされます。スイッチオーバーが行われると、（チェックポイントされる）シスコ エクスプレス フォワーディングの隣接状態を使用して、ネイバー探索キャッシュが再構築されます。

IPv6 ネイバー請求メッセージ

ICMP パケット ヘッダーのタイプ フィールドの値 135 は、ネイバー請求メッセージを示します。ネイバー請求メッセージは、ノードが同じローカル リンク上の別のノードのリンクレイヤ アドレスを判断する必要がある場合にローカル リンクに送信されます（図 12 を参照）。ノードが別のノードのリンクレイヤ 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。ネイバー請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請求ノード マルチキャスト アドレスです。ネイバー請求メッセージには、送信元ノードのリンクレイヤ アドレスも含まれます。

図 12　　IPv6 ネイバー探索：ネイバー請求メッセージ



ネイバー請求メッセージを受信したあと、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 インターフェイスの 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、ネイバー請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レイヤ 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。

ネイバー請求メッセージは、ネイバーのリンクレイヤ アドレスが識別されたあとに、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、ネイバー請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レイヤ アドレスが変更されたときにも送信されます。このような変更がある場合、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 アドレスです。

ネイバー請求メッセージは、ネイバーのリンクレイヤ アドレスが識別されたあとに、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、またはネイバー請求メッセージに対してネイバー 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 ネイバー請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。

ネイバーから返信された請求ネイバー 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という肯定確認応答です（請求フラグが値 1 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、ネイバー請求メッセージへの返信としてだけ送信されます）。非請求メッセージでは、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。請求ネイバー 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） 請求フラグが値 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。

ネイバー請求メッセージは、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。新規のリンクローカル IPv6 アドレスに対しては、アドレスがインターフェイスに割り当てられる前に、最初に重複アドレス検出が実行されます（重複アドレス検出の実行中、新規アドレスは一時的な状態のままです）。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請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請求メッセージを返します。ネイバー請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請求メッセージも受信されない場合、最初のネイバー請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。

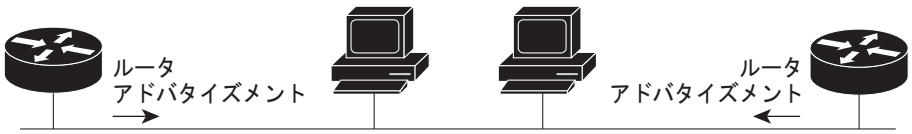
リンク上のすべての IPv6 ユニキャスト アドレス（グローバルまたはリンクローカル）が一意であることを検証する必要がありますが、リンクローカル アドレスの一意性が確認されるまでは、リンクローカル アドレスに関連付けられている他の IPv6 アドレスに対して重複アドレス検出は実行されません。Cisco IOS ソフトウェアでの重複アドレス検出のシスコ実装では、64 ビット インターフェイス識別子から生成されるエニーキャスト アドレスまたはグローバル アドレスの一意性は確認されません。

IPv6 ルータ アドバタイズメント メッセージ

Router Advertisement（RA; ルータ アドバタイズメント）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に送信されます。ステートレス自動設定が正しく機能するには、RA メッセージでアドバタイズされるプレフィクス長が常に 64 ビットである必要があります。

RA 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 13 を参照）。

図 13　IPv6 ネイバー探索：RA メッセージ



ルータ アドバタイズメント パケット定義：
ICMPv6 タイプ = 134
送信元 = ルータ リンクローカル アドレス
宛先 = すべてのノードのマルチキャスト アドレス
データ = オプション、プレフィクス、有効期間、自動設定フラグ
52674

通常、RA メッセージには次の情報が含まれます。

- 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 プレフィクス
- アドバタイズメントに含まれる各プレフィ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、また使用する必要がある場合はルータをデフォルト ルータとして使用する必要のある秒単位での時間）
- 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

RA は、ルータ請求メッセージへの返信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 であるルータ請求メッセージは、システム始動時にホストによって送信されるため、ホストは次のスケジュールされた RA メッセージを待機することなくすぐに自動設定できます。ルータ請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、ルータ請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。ホストにユニキャスト アドレスが設定されている場合は、ルータ請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、メッセージで送信元アドレスとして使用されます。ルータ請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。RA がルータ請求への返信として送信される場合、RA メッセージ内の宛先アドレスは、ルータ請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 RA メッセージ パラメータを設定できます。

- RA メッセージが定期的に送信される時間の間隔
- （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 プレフィクス
- （特定のリンクで）ネイバー請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。RA メッセージ（デフォルト値を含む）の送信は、**ipv6 unicast-routing** コマンドの設定時にイーサネットおよび FDDI インターフェイスで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 タイプの場合は、**no ipv6 nd ra suppress** コマンドを使用して、RA メッセージの送信を手動で設定する必要があります。個々のインターフェイスで、**ipv6 nd ra suppress** コマンドを使用して、RA メッセージの送信をディセーブルにできます。

トラフィック エンジニアリングのデフォルト ルータ プリファレンス

ホストは、RA をリスニングすることでデフォルト ルータを検出し、選択します。通常のデフォルト ルータ選択メカニズムは、トラフィック エンジニアリングが必要な場合など、特定のケースでは次善のメカニズムです。たとえば、リンク上の 2 台のルータが、同等だが等しくはないコストのルーティングを提供している場合や、ポリシーによってルータの一方を優先することが指示されている場合があります。次に例をいくつか示します。

- 異なるプレフィクス セットへルーティングする複数のルータ：リダイレクト（宛先に対して最適でないルータによって送信される）は、ホストが任意のルータを選択でき、システムが機能することを意味します。ただし、トラフィック パターンは、ルータの 1 つを選択すると、リダイレクトがかなり少なくなることを意味する場合があります。
- 新しいルータの誤った展開：新しいルータを完全に設定する前に展開すると、ホストによって新しいルータがデフォルト ルータとして採用され、トラフィックが消える可能性があります。ネットワーク管理者は、一部のルータが他のルータよりも優先されることを指定できます。
- マルチホーム環境：複数の物理リンクと IPv6 トランスポートでのトンネリングの使用により、マルチホーム環境はより一般的になる可能性があります。一部のルータは、6-to-4 プレフィクスにだけルーティングするか、企業イントラネットにだけルーティングするため、完全なデフォルト ルーティングを提供しないことがあります。このような状況は、単一リンク上でだけ機能するリダイレクトでは解決できません。

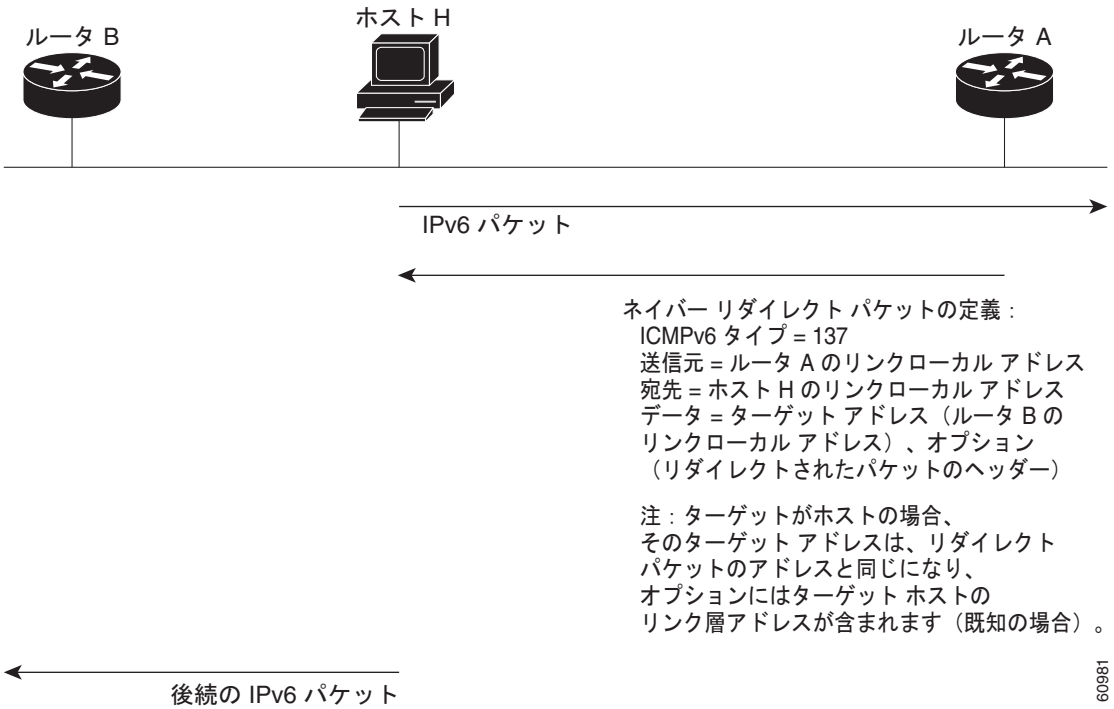
Default Router Preference（DRP; デフォルト ルータ プリファレンス）拡張は、大まかなプリファレンス メトリック（低、中、高）をデフォルト ルータに提供します。デフォルト ルータの DRP は、RA メッセージ内の未使用ビットで通知されます。この拡張は、ルータ（DRP ビットの設定）とホスト（DRP ビットの解釈）の両方に対して下位互換性があります。これらのビットは、DRP 拡張を実装しないホストでは無視されます。同様に、DRP 拡張を実装しないルータによって送信される値は、DRP 拡張を実装するホストによって「中」のプリファレンスが指定されたものと解釈されます。

DRP は手動で設定する必要があります。オプションの DRP 拡張の設定については、「トラフィック エンジニアリングの DRP 拡張の設定」を参照してください。

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 14 を参照）。

図 14　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）によってネイバー 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、ルータは各ネイバー 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 プロトコルがネイバー 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。

ネイバー リダイレクト メッセージなどのすべての IPv6 ICMP エラー メッセージをルータが生成するレートを制限するには、**ipv6 icmp error-interval** コマンドを使用します。これにより、リンクレイヤの輻輳が最終的に低減されます。

（注）　ルータは、ネイバー リダイレクト メッセージの受信後はルーティング テーブルを更新できず、ホストはネイバー リダイレクト メッセージを発信できません。

Per-Interface ネイバー探索キャッシュ制限

ネイバー探索キャッシュ内のエントリ数は、インターフェイスごとに制限できます。この制限に達すると、新しいエントリは追加されなくなります。Per-Interface ネイバー探索キャッシュ制限機能を使用すれば、インターフェイスに接続された特定のお客様がネイバー探索キャッシュに過剰な負荷を与えることを、それが意図的かどうかにかかわらず防ぐことができます。

この機能をグローバルにイネーブルにすると、ルータ上のすべてのインターフェイスに、共通のインターフェイス単位のキャッシュ サイズ制限が設定されます。この機能をインターフェイスごとにイネーブルにすると、キャッシュ サイズ制限はそれに対応するインターフェイス上で設定されます。インターフェイスごとの制限は、グローバルに設定された制限よりも優先されます。

リンク、サブネット、およびサイト アドレッシングの変更

ここでは、リンク、サブネット、およびサイト アドレッシングの変更の管理に使用できる IPv6 ステートレス自動設定および汎用プレフィクスの機能について説明します。

IPv6 ステートレス自動設定

IPv6 ノード上のすべてのインターフェイスには、通常はインターフェイスの識別子とリンクローカル プレフィクス FE80::/10 から自動的に設定されるリンクローカル アドレスが必要です。リンクローカル アドレスを使用すると、ノードがリンク上の他のノードと通信できます。また、リンクローカル アドレスを使用して、ノードをさらに設定することもできます。

ノードは、手動の設定や Dynamic Host Configuration Protocol（DHCP）サーバなどのサーバの支援を必要とすることなく、ネットワークに接続し、グローバル IPv6 アドレスを自動的に生成できます。IPv6 では、リンク上のルータは、RA メッセージ内で、任意のグローバル プレフィクスと、リンクのデフォルト ルータとして機能する旨をアドバタイズします。RA メッセージは、定期的に送信される場合と、システム始動時にホストから送信されるルータ請求メッセージに対する応答として送信される場合があります。

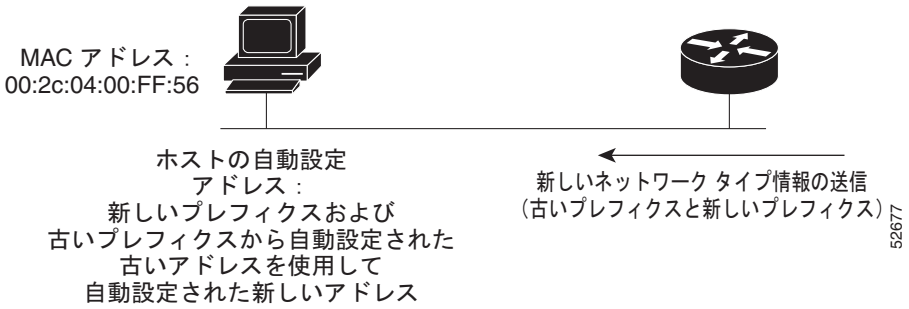
リンク上のノードは、RA メッセージに含まれるプレフィクス（64 ビット）にインターフェイス識別子（64 ビット）を付加することで、グローバル IPv6 アドレスを自動的に設定できます。ノードによって設定された 128 ビットの IPv6 アドレスは、重複アドレス検出の対象となり、リンク上での一意性が確保されます。RA メッセージでアドバタイズされたプレフィクスがグローバルに一意である場合、ノードによって設定された IPv6 アドレスもグローバルに一意になります。ICMP パケット ヘッダーの Type フィールドの値が 133 であるルータ請求メッセージは、システム始動時にホストによって送信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

IPv6 ホストの簡易ネットワーク リナンバリング

グローバル ルーティング テーブルの厳格な集約では、ネットワークのサービス プロバイダーが変更された場合にネットワークをリナンバリングする必要があります。IPv6 のステートレス自動設定機能を使用してネットワークをリナンバリングする場合は、新しいサービス プロバイダーからのプレフィクスが、リンク上に送信される RA メッセージに追加されます（RA メッセージには、古いサービス プロバイダーからのプレフィクスと新しいサービス プロバイダーからのプレフィクスの両方が含まれます）。リンク上のノードは、新しいサービス プロバイダーからのプレフィクスを使用して追加アドレスを自動的に設定します。ノードは、新しいプレフィクスから作成されたアドレスとリンク上の古いプレフィクスから作成された既存のアドレスを使用できます。古いプレフィクスと新しいプレフィクスに関連付けられているライフタイム パラメータの設定は、リンク上のノードが、新しいプレフィクスから

作成されたアドレスだけを使用するように移行できることを意味します。移行期間中は、古いプレフィクスが RA メッセージから削除され、新しいプレフィクスを含むアドレスだけがリンク上で使用されます（リナンバリングが完了します）（図 15 を参照）。

図 15　ステートレス自動設定を使用したホストの IPv6 ネットワーク リナンバリング



IPv6 の汎用プレフィクス

IPv6 アドレスの上位 64 ビットは、RFC 3513 で定義されているように、グローバル ルーティング プレフィクスとサブネット ID から構成されます。汎用プレフィクス（/48 など）には、短いプレフィクスが保持されます。このプレフィクスに基づいて、より長く詳細な複数のプレフィクス（/64 など）を定義できます。汎用プレフィクスが変更されると、そのプレフィクスに基づくより詳細なプレフィクスもすべて変更されます。この機能により、ネットワーク リナンバリングが大幅に簡略化され、自動化されたプレフィクス定義が可能になります。

たとえば、汎用プレフィクスは 48 ビットの長さ（/48）で、そのプレフィクスから生成されるより詳細なプレフィクスは 64 ビットの長さ（/64）の場合があります。次の例では、すべての詳細プレフィクスの一番左の 48 ビットが同じになります。これは汎用プレフィクス自体と同じです。次の 16 ビットはすべて異なります。

- 汎用プレフィクス：2001:0DB8:2222::/48
- 詳細プレフィクス：2001:0DB8:2222:0000::/64
- 詳細プレフィクス：2001:0DB8:2222:0001::/64
- 詳細プレフィクス：2001:0DB8:2222:4321::/64
- 詳細プレフィクス：2001:0DB8:2222:7744::/64

汎用プレフィクスは、次のようないくつかの方法で定義できます。

- 手動で定義する
- 6to4 インターフェイスに基づいて定義する
- DHCP for IPv6 プレフィクス委任クライアントによって受信されたプレフィクスから動的に定義する

汎用プレフィクスに基づくより詳細なプレフィクスは、インターフェイスに IPv6 を設定する場合に使用できます。

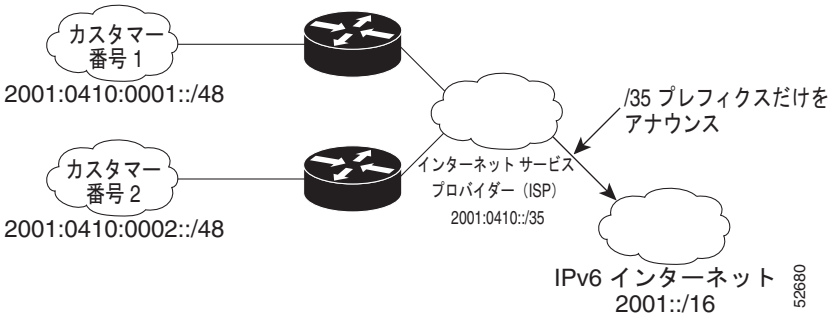
DHCP for IPv6 プレフィクス委任

DHCP for IPv6 を環境で使用して、ステートフルおよびステートレス情報を配信できます。この機能の詳細については、「*Implementing DHCP for IPv6*」を参照してください。

IPv6 プレフィクス集約

IPv6 アドレス空間の集約可能な特性により、IPv6 アドレッシング階層がイネーブルになります。たとえば、企業はサービス プロバイダーの単一の IPv6 プレフィクスを複数のより長いプレフィクスに分割して、社内ネットワーク内で使用できます。反対に、サービス プロバイダーは、カスタマーのすべてのプレフィクスを、サービス プロバイダーが IPv6 インターネット上でアドバタイズできる単一のより短いプレフィクスに集約できます（図 16 を参照）。

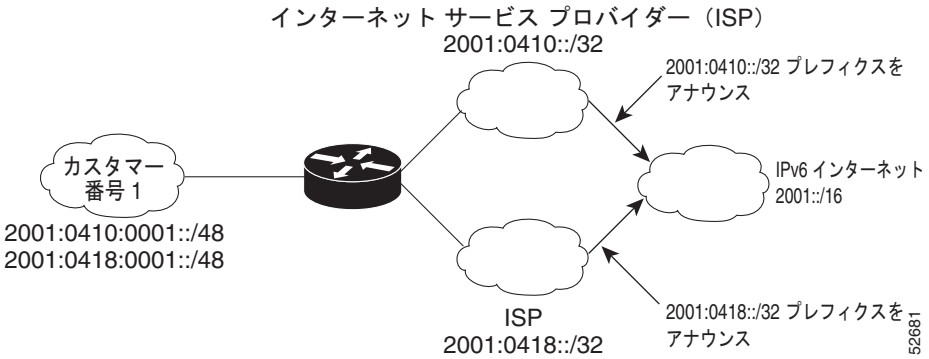
図 16　　IPv6 プレフィクス集約



IPv6 サイト マルチホーミング

複数の IPv6 プレフィクスをネットワークとホストに割り当てることができます。複数のプレフィクスをネットワークに割り当てると、グローバル ルーティング テーブルを壊すことなくネットワークを複数の ISP に簡単に接続できるようになります（図 17 を参照）。

図 17　　IPv6 サイト マルチホーミング



IPv6 データ リンク

IPv6 ネットワークでは、データ リンクは特定のリンクローカル プレフィクスを共有するネットワークです。データ リンクは、接続しているネットワークのアドレッシングの複雑さをサブネットワークから隠しながらマルチレベルの階層ルーティング構造を提供するために、ネットワーク管理者によって任意にセグメント化されるネットワークです。IPv6 のサブネットワークの機能は、IPv4 のサブネットワークと同様です。サブネットワーク プレフィクスは 1 つのデータ リンクに関連付けられ、複数のサブネットワーク プレフィクスを同じデータ リンクに割り当てることができます。

IPv6 では、ATM Permanent Virtual Circuit（PVC; 相手先固定接続）および ATM LANE、イーサネット、ファスト イーサネット、ギガビット イーサネット、FDDI、フレーム リレー PVC、Cisco High-Level Data Link Control（HDLC; ハイレベル データリンク コントロール）、PPP over Packet over SONET（PoS）、ISDN、シリアル インターフェイス、Dynamic Packet Transport（DPT; ダイナミック パケット トランスポート）の各データ リンクがサポートされます。

Cisco IOS ソフトウェアの IPv6 でのワイドエリア ネットワーク テクノロジーのサポート

Cisco IOS ソフトウェアの IPv6 では、Cisco HDLC、PoS、ISDN、シリアル（同期および非同期）インターフェイス タイプ、ATM PVC、フレーム リレー PVC などのワイドエリア ネットワーク テクノロジーがサポートされます。これらのテクノロジーは、IPv6 でも IPv4 と同様に動作します。IPv6 での機能強化はありません。

IPv6 アドレスと PVC

LAN では、プロトコル（ネットワークレイヤ）アドレスをリモート ノード（ホストおよびルータ）のハードウェア アドレスにマッピングするために、ブロードキャストとマルチキャストが使用されます。ブロードキャストおよびマルチキャストを使用した、ATM ネットワークやフレーム リレー ネットワークなどの回線ベースの WAN のハードウェア アドレスへのネットワークレイヤ アドレスのマッピングは実装が難しいため、これらのネットワークでは、リモート ノードのネットワークレイヤ アドレスおよびアドレスへの到達に使用される PVC に暗黙のマッピング、明示的なマッピング、およびダイナミック マッピングを利用します。

ipv6 address コマンドを使用した、インターフェイスへの IPv6 アドレスの割り当てでは、インターフェイスおよびインターフェイスに直接接続されているネットワークの IPv6 アドレスを定義します。インターフェイスで 1 つの PVC だけが終端されている（インターフェイスがポイントツーポイント インターフェイスである）場合は、ネットワーク上のすべての IPv6 アドレスとアドレスへの到達に使用される PVC 間に暗黙のマッピングがあります（追加のアドレス マッピングは不要です）。インターフェイスで複数の PVC が終端されている（インターフェイスがポイントツーマルチポイント インターフェイスである）場合は、**protocol ipv6** コマンド（ATM ネットワークの場合）または **frame-relay map ipv6** コマンド（フレーム リレー ネットワークの場合）を使用して、リモート ノードの IPv6 アドレスとアドレスへの到達に使用される PVC との間に明示的なマッピングを設定します。

（注） IPv6 では複数のアドレス タイプがサポートされるため、ポイントツーマルチポイント インターフェイスに設定されるアプリケーションまたはプロトコルによっては、インターフェイスの IPv6 アドレスとアドレスへの到達に使用される PVC との間に複数の明示的なマッピングを設定することが必要な場合があります。たとえば、ポイントツーマルチポイント インターフェイスのリンクローカルとグローバルの両方の IPv6 アドレスを、インターフェイスが終端する PVC に明示的にマッピングすると、インターフェイスに設定された Interior Gateway Protocol（IGP; 内部ゲートウェイ プロトコル）が PVC との間でトラフィックを正しく転送することが保証されます。

IPv6 のルーテッド ブリッジ カプセル化

Routed Bridge Encapsulation（RBE; ルーテッド ブリッジ カプセル化）は、ブリッジ インターフェイスから別のルーテッド インターフェイスまたはブリッジ インターフェイスにプロトコルをルーティングするメカニズムを提供します。IPv6 の RBE は、IPv6 ハーフブリッジング用に設定された ATM ポイントツーポイント サブインターフェイス上で使用できます。IP パケットと IPv6 ハーフブリッジング、ブリッジング、PPP over Ethernet（PPPoE）、またはその他のイーサネット 802.3 カプセル化プロトコルのルーティングを同じサブインターフェイス上で設定できます。

IPv6 リダイレクト メッセージ

IPv6 リダイレクト メッセージ機能により、ルータは ICMP IPv6 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（ルータまたはホスト）をホストに通知できます。

ブリッジングおよびルーティングのための BVI インターフェイス上での IPv6

Integrated Routing and Bridging（IRB）により、ユーザは、ルーテッド インターフェイスとブリッジ グループの間またはブリッジ グループ間で所定のプロトコルをルーティングできるようになります。具体的には、ローカル トラフィックまたはルーティング不可能なトラフィックは同じブリッジ グループ内のブリッジ インターフェイス間でブリッジされ、ルーティング可能なトラフィックは他のルーテッド インターフェイスまたはブリッジ グループにルーティングされます。

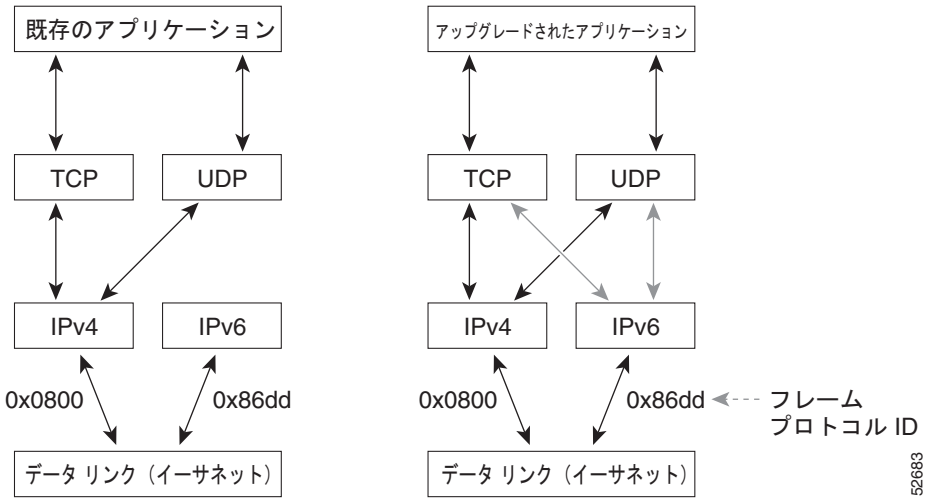
IPv6 は、BVI でサポートされています。BVI は、ブリッジ インターフェイス用の IPv4 インターフェイスです。ブリッジングはデータリンク レイヤで実行され、ルーティングはネットワーク レイヤで実行されるため、それぞれ異なるプロトコル設定モデルに従います。基本的な IPv4 モデルでは、たとえば、すべてのブリッジ インターフェイスは同じネットワークに属している必要があり、それに対してルーテッド インターフェイスはそれぞれ別個のネットワークを表します。ルーティングされるトラフィックの宛先はルータになりますが、ブリッジされるトラフィックの宛先はルータになることはありません。BVI を使用すると、同じブリッジ グループ内で所定のプロトコルのブリッジングおよびルーティングを両方実行するとき、どのプロトコル設定モデルを使用するか混乱することはなくなります。

（注） IPv6 での Bridge-Group Virtual Interface（BVI; ブリッジ グループ仮想インターフェイス）は、NAT-PT およびワイヤレス インターフェイス Dot11Radio でサポートされません。

デュアル IPv4 および IPv6 プロトコル スタック

デュアル IPv4 および IPv6 プロトコル スタック手法を使用して IPv6 に移行できます。これにより、ノードで稼動しているアプリケーションに対する段階的な 1 つずつのアップグレードが可能になります。ノードで稼動しているアプリケーションは、IPv6 プロトコル スタックを使用するようにアップグレードされます。アップグレードされない（IPv4 プロトコル スタックだけをサポートする）アプリケーションは、ノード上のアップグレードされたアプリケーションと共存できます。新しいアプリケーションとアップグレードされたアプリケーションでは、IPv4 と IPv6 の両方のプロトコル スタックを使用します（図 18 を参照）。

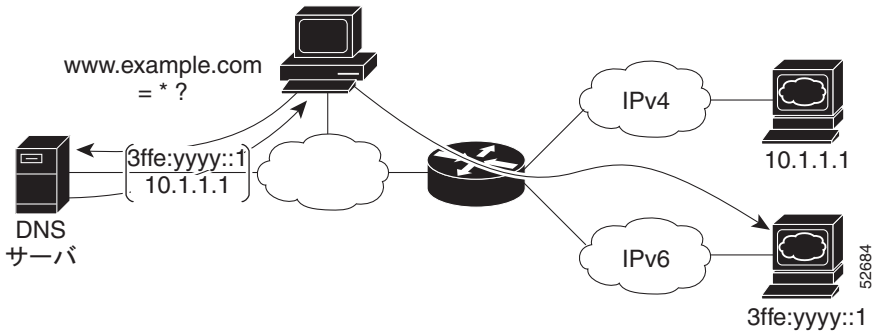
図 18　デュアル IPv4 および IPv6 プロトコル スタック手法



1 つの Application Program Interface（API; アプリケーション プログラム インターフェイス）で、IPv4 アドレスと IPv6 アドレスの両方および DNS 要求がサポートされます。アプリケーションを新しい API にアップグレードしても、依然として IPv4 プロトコル スタックだけを使用できます。Cisco IOS ソフトウェアでは、デュアル IPv4 および IPv6 プロトコル スタック手法がサポートされます。IPv4 アドレスと IPv6 アドレスの両方でインターフェイスが設定されている場合、インターフェイスは IPv4 と IPv6 両方のトラフィックを転送します。

図 19 では、デュアル IPv4 および IPv6 プロトコル スタックをサポートするアプリケーションは、宛先ホスト名 www.a.com で使用可能なすべてのアドレスを DNS サーバに要求します。DNS サーバは、www.example.com で使用可能なすべてのアドレス（IPv4 アドレスと IPv6 アドレスの両方）で返信します。アプリケーションはアドレスを選択し（ほとんどの場合、IPv6 アドレスがデフォルトの選択肢です）、IPv6 プロトコル スタックを使用して送信元ノードを宛先に接続します。

図 19　デュアル IPv4 および IPv6 プロトコル スタック アプリケーション



IPv6 アドレッシングと基本接続の実装方法

- 「IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル」（P.32）
- 「IPv6 汎用プレフィクスの定義と使用」（P.35）
- 「IPv4 および IPv6 プロトコル スタックをサポートするためのインターフェイスの設定」（P.37）
- 「IPv6 ICMP レート制限の設定」（P.38）

IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル

IPv6 アドレスを個々のルータ インターフェイスに割り当て、IPv6 トラフィックの転送をルータ上でグローバルにイネーブルにするには、次の作業を実行します。デフォルトでは、IPv6 アドレスは設定されず、IPv6 ルーティングはディセーブルになります。

（注） **ipv6 address** コマンドの *ipv6-address* 引数は、RFC 2373 に記載された形式にする必要があり、16 ビット値をコロンで区切った 16 進でアドレスを指定します。

ipv6 address コマンドの *ipv6-prefix* 引数は、RFC 2373 に記載された形式にする必要があり、16 ビット値をコロンで区切った 16 進でアドレスを指定します。

ipv6 address コマンドの */prefix-length* キーワードおよび引数は、アドレスのうち連続する上位何ビットがプレフィクス（アドレスのネットワーク部）を構成するかを示す 10 進数値です。10 進数値の前にスラッシュ記号が必要です。

制約事項

Cisco IOS Release 12.2(4)T またはそれ以降のリリース、Cisco IOS Release 12.0(21)ST、および Cisco IOS Release 12.0(22)S またはそれ以降のリリースでは、**ipv6 address** または **ipv6 address eui-64** コマンドを使用して、インターフェイス上の同じプレフィクス内に複数の IPv6 グローバル アドレスを設定できます。1 つのインターフェイス上で複数の IPv6 リンクローカル アドレスはサポートされません。

Cisco IOS Releases 12.2(4)T、12.0(21)ST、および 12.0(22)S よりも前のリリースでは、インターフェイス上の同じプレフィクス内に複数の IPv6 アドレスが設定されていると、Cisco IOS Command-Line Interface（CLI; コマンドライン インターフェイス）に次のエラー メッセージが表示されます。

```
Prefix <prefix-number> already assigned to <interface-type>
```

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 address** *ipv6-prefix*/*prefix-length* **eui-64**
   または
   ipv6 address *ipv6-address*/*prefix-length* **link-local**
   または
   ipv6 address *ipv6-prefix*/*prefix-length* **anycast**
   または
   ipv6 enable

5. **exit**
6. **ipv6 unicast-routing**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface ethernet 0/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。

ステップ 4	**ipv6 address** *ipv6-prefix*/*prefix-length* **eui-64**
	または
	ipv6 address *ipv6-address*/*prefix-length* **link-local**
	または
	ipv6 address *ipv6-prefix*/*prefix-length* **anycast**
	または
	ipv6 enable
	
	例：
	`Router(config-if)# ipv6 address 2001:0DB8:0:1::/64 eui-64`
	
	または
	
	例：
	`Router(config-if)# ipv6 address FE80::260:3EFF:FE11:6770 link-local`
	
	または
	
	例：
	`Router(config-if) ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64 anycast`
	
	または
	
	例：
	`Router(config-if)# ipv6 enable`
		インターフェイスに割り当てられている IPv6 ネットワークを指定し、インターフェイスで IPv6 処理をイネーブルにします。
		または
		インターフェイスに割り当てられている IPv6 アドレスを指定し、そのインターフェイスで IPv6 処理をイネーブルにします。
		または
		インターフェイスで IPv6 リンクローカル アドレスを自動的に設定し、インターフェイスで IPv6 処理もイネーブルにします。リンクローカル アドレスは、同じリンク上のノードとの通信にだけ使用できます。
		• **ipv6 address eui-64** コマンドを指定して、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）を持つグローバル 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。
		• **ipv6 address link-local** コマンドを指定して、IPv6 がインターフェイスでイネーブルになっている場合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るリンクローカル アドレスを、インターフェイスに設定します。
		• **ipv6 address anycast** コマンドを指定して、IPv6 エニーキャスト アドレスを追加します。

	コマンドまたはアクション	目的
ステップ 5	**exit** **例：** `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 6	**ipv6 unicast-routing** **例：** `Router(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。

ネイバー探索キャッシュ制限の設定

ネイバー探索キャッシュ制限をインターフェイスごとまたはグローバルに設定するには、次の作業を実行します。

- 「指定したルータ インターフェイス上でのネイバー探索キャッシュ制限の設定」（P.34）
- 「すべてのルータ インターフェイス上でのネイバー探索キャッシュ制限の設定」（P.35）

指定したルータ インターフェイス上でのネイバー探索キャッシュ制限の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 nd cache interface-limit** *size* [**log** *rate*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface GigabitEthernet 1/0/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 nd cache interface-limit** *size* [**log** *rate*] **例：** `Router(config-if)# ipv6 nd cache interface-limit 1`	ルータ上の指定したインターフェイスにネイバー探索キャッシュ制限を設定します。 • このコマンドを実行すると、グローバル コンフィギュレーション モードで **ipv6 nd cache interface-limit** を実行して作成されている設定が上書きされます。

すべてのルータ インターフェイス上でのネイバー探索キャッシュ制限の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 nd cache interface-limit** *size* [**log** *rate*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 nd cache interface-limit** *size* [**log** *rate*] **例：** `Router(config)# ipv6 nd cache interface-limit 4`	ルータ上のすべてのインターフェイスにネイバー探索キャッシュ制限を設定します。

IPv6 汎用プレフィクスの定義と使用

汎用プレフィクスは、次のようないくつかの方法で定義できます。

- 手動で定義する
- 6to4 インターフェイスに基づいて定義する
- DHCP for IPv6 プレフィクス委任クライアントによって受信されたプレフィクスから動的に定義する

汎用プレフィクスに基づくより詳細なプレフィクスは、インターフェイスに IPv6 を設定する場合に使用できます。

次の作業では、IPv6 汎用プレフィクスを定義および使用する方法を示します。

- 「汎用プレフィクスの手動定義」（P.35）
- 「6to4 インターフェイスに基づく汎用プレフィクスの定義」（P.36）
- 「DHCP for IPv6 プレフィクス委任クライアント機能での汎用プレフィクスの定義」（P.37）
- 「IPv6 での汎用プレフィクスの使用」（P.37）

汎用プレフィクスの手動定義

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 general-prefix** *prefix-name* [*ipv6-prefix*/*prefix-length*] [**6to4** *interface-type interface-number*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 general-prefix** *prefix-name* {*ipv6-prefix*/*prefix-length* | **6to4** *interface-type interface-number*} **例：** `Router(config)# ipv6 general-prefix my-prefix 2001:0DB8:2222::/48`	IPv6 アドレスの汎用プレフィクスを定義します。 汎用プレフィクスを手動で定義する場合は、*ipv6-prefix* 引数と */prefix-length* 引数の両方を指定します。

6to4 インターフェイスに基づく汎用プレフィクスの定義

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 general-prefix** *prefix-name* [*ipv6-prefix*/*prefix-length*] [**6to4** *interface-type interface-number*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 general-prefix** *prefix-name* {*ipv6-prefix*/*prefix-length* | **6to4** *interface-type interface-number*} **例：** `Router(config)# ipv6 general-prefix my-prefix 6to4 ethernet 0`	IPv6 アドレスの汎用プレフィクスを定義します。 6to4 インターフェイスに基づく汎用プレフィクスを定義する場合は、**6to4** キーワードと *interface-type interface-number* 引数を指定します。 6to4 トンネリングに使用するインターフェイスに基づく汎用プレフィクスを定義する場合、汎用プレフィクスは 2001:a.b.c.d::/48 の形式になります。「a.b.c.d」は、参照されるインターフェイスの IPv4 アドレスです。

DHCP for IPv6 プレフィクス委任クライアント機能での汎用プレフィクスの定義

DHCP for IPv6 プレフィクス委任クライアント機能を使用して、汎用プレフィクスを動的に定義できます。この作業の実行方法については、「*DHCP for IPv6 の実装*」の章を参照してください。

IPv6 での汎用プレフィクスの使用

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface ethernet 0/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*} **例：** `Router(config-if) ipv6 address my-prefix 2001:0DB8:0:7272::/64`	IPv6 アドレスの IPv6 プレフィクス名を設定し、インターフェイスで IPv6 処理をイネーブルにします。

IPv4 および IPv6 プロトコル スタックをサポートするためのインターフェイスの設定

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。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するには、次の作業を実行します。

手順の概要

1. **enable**

2. **configure terminal**
3. **ipv6 unicast-routing**
4. **interface** *type number*
5. **ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
6. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*}

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 unicast-routing** **例：** `Router(config)# ipv6 unicast routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。
ステップ 4	**interface** *type number* **例：** `Router(config)# interface ethernet 0`	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]] **例：** `Router(config-if)# ip address 192.168.99.1 255.255.255.0`	インターフェイスに対するプライマリ IPv4 アドレスまたはセカンダリ IPv4 アドレスを指定します。
ステップ 6	**ipv6 address** {*ipv6-address*/*prefix-length*	*prefix-name sub-bits*/*prefix-length*} **例：** `Router(config-if)# ipv6 address 2001:0DB8:c18:1::3/64`	インターフェイスに割り当てられている IPv6 ネットワークを指定し、インターフェイスで IPv6 処理をイネーブルにします。 **（注）** IPv6 アドレスの設定の詳細については、「IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル」を参照してください。

IPv6 ICMP レート制限の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 icmp error-interval** *milliseconds* [*bucketsize*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 icmp error-interval** *milliseconds* [*bucketsize*] **例：** `Router(config)# ipv6 icmp error-interval 50 20`	IPv6 ICMP エラー メッセージの間隔とバケット サイズを設定します。 • *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。

トラフィック エンジニアリングの DRP 拡張の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 nd router-preference** {**high** | **medium** | **low**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface ethernet 0`	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 nd router-preference** {**high** | **medium** | **low**} **例：** `Router(config-if)# ipv6 nd router-preference high`	特定のインターフェイス上のルータに DRP を設定します。

IPv6 のシスコ エクスプレス フォワーディング スイッチングと分散型シスコ エクスプレス フォワーディング スイッチングの設定

IPv6 のシスコ エクスプレス フォワーディング スイッチングと分散型シスコ エクスプレス フォワーディング スイッチングを設定するには、次の作業を実行します。

- 「分散型および非分散型アーキテクチャ プラットフォームでのシスコ エクスプレス フォワーディング スイッチングの設定」（P.40）
- 「ユニキャスト RPF の設定」（P.44）

分散型および非分散型アーキテクチャ プラットフォームでのシスコ エクスプレス フォワーディング スイッチングの設定

シスコ エクスプレス フォワーディングは、Cisco 7200 シリーズ ルータなどの非分散型アーキテクチャ プラットフォーム用に設計されています。分散型シスコ エクスプレス フォワーディングは、GSR や Cisco 7500 シリーズ ルータなどの分散型アーキテクチャ プラットフォーム用に設計されています。非分散型プラットフォームでは、分散型シスコ エクスプレス フォワーディングはサポートされませんが、Cisco 7500 シリーズ ルータなどの一部の分散型プラットフォームでは、シスコ エクスプレス フォワーディングと分散型シスコ エクスプレス フォワーディングの両方がサポートされます。

シスコ エクスプレス フォワーディングが Cisco 7500 シリーズ ルータ上に設定されている場合、シスコ エクスプレス フォワーディング スイッチングは RP によって実行されます。分散型シスコ エクスプレス フォワーディングが設定されている場合、シスコ エクスプレス フォワーディング スイッチングはライン カードによって実行されます。デフォルトでは、GSR では、分散型シスコ エクスプレス フォワーディングだけがサポートされます（シスコ エクスプレス フォワーディング スイッチングはライン カードによって実行されます）。

前提条件

ルータでシスコ エクスプレス フォワーディング トラフィックおよび分散型シスコ エクスプレス フォワーディング トラフィックの転送をイネーブルにするには、**ipv6 unicast-routing** コマンドを使用してルータ上に IPv6 ユニキャスト データグラムの転送をグローバルに設定し、**ipv6 address** コマンドを使用してインターフェイス上に IPv6 アドレスおよび IPv6 処理を設定します。

ルータ上で Cisco Express Forwarding for IPv6 をグローバルにイネーブルにする前に、**ip cef** コマンドを使用してルータ上で Cisco Express Forwarding for IPv4 をグローバルにイネーブルにする必要があります。

分散型 Cisco Express Forwarding for IPv6 をイネーブルにする前に、**ip cef distributed** コマンドを使用して分散型 Cisco Express Forwarding for IPv4 をイネーブルにする必要があります。

制約事項

GSR は分散型シスコ エクスプレス フォワーディング モードでだけ動作するため、この分散型プラットフォームでは **ipv6 cef** コマンドと **ipv6 cef distributed** コマンドはサポートされません。

Cisco IOS Release 12.0(22)S またはそれ以降のリリースでは、シスコ エクスプレス フォワーディングと分散型シスコ エクスプレス フォワーディングに設定されている非分散型および分散型アーキテクチャ プラットフォームに次の制約が適用されます。

（注） デフォルトでは、GSR では、分散型シスコ エクスプレス フォワーディングだけがサポートされます（シスコ エクスプレス フォワーディング スイッチングはライン カードによって実行されます）。

- グローバルな送信元および宛先アドレスを持つ IPv6 パケットは、シスコ エクスプレス フォワーディングまたは分散型シスコ エクスプレス フォワーディングでスイッチングされる。
- リンクローカルの送信元アドレスと宛先アドレスを持つ IPv6 パケットは、プロセスでスイッチングされる。
- 手動で設定した IPv6 トンネル内でトンネリングされる IPv6 パケットは、シスコ エクスプレス フォワーディングでスイッチングされる。
- 次のインターフェイスおよびカプセル化タイプだけがサポートされる。
  - ATM PVC および ATM LANE
  - Cisco HDLC
  - イーサネット、ファスト イーサネット、およびギガビット イーサネット
  - FDDI
  - フレーム リレー PVC
  - PPP over Packet over SONET、ISDN、およびシリアル（同期および非同期）インターフェイス タイプ
- 次のインターフェイスおよびカプセル化タイプはサポートされない。
  - HP 100VG-AnyLAN
  - Switched Multimegabit Data Service（SMDS; スイッチド マルチメガビット データ サービス）
  - トークンリング
  - X.25

（注） シスコ エクスプレス フォワーディングおよび分散型シスコ エクスプレス フォワーディングの詳細なハードウェア制約については、製品を購入されたシスコシステムズ代理店へお問い合せください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 cef**
   または
   ipv6 cef distributed
4. **ipv6 cef accounting** [**non-recursive** | **per-prefix** | **prefix-length**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 3	**ipv6 cef**
	または
	ipv6 cef distributed
	
	例：
	`Router(config)# ipv6 cef`
	または
	
	例：
	`Router(config)# ipv6 cef distributed`
		ルータでシスコ エクスプレス フォワーディングをグローバルにイネーブルにします。
		または
		ルータで分散型シスコ エクスプレス フォワーディングをグローバルにイネーブルにします。

ステップ 4	**ipv6 cef accounting** [**non-recursive** | **per-prefix** | **prefix-length**] **例：** `Router(config)# ipv6 cef accounting`	ルータで、シスコ エクスプレス フォワーディングおよび分散型シスコ エクスプレス フォワーディングのネットワーク アカウンティングをグローバルにイネーブルにします。 • シスコ エクスプレス フォワーディングおよび分散型シスコ エクスプレス フォワーディングのネットワーク アカウンティングにより、シスコ エクスプレス フォワーディングおよび分散型シスコ エクスプレス フォワーディングのトラフィックに固有の統計情報を収集することで、ネットワーク内のシスコ エクスプレス フォワーディング トラフィック パターンをよりよく理解できます。たとえば、シスコ エクスプレス フォワーディングおよび分散型シスコ エクスプレス フォワーディングのネットワーク アカウンティングにより、宛先にスイッチングされたパケット数とバイト数や、宛先を経由してスイッチングされたパケット数などの情報を収集できます。 • オプションの **per-prefix** キーワードでは、IPv6 宛先（または IPv6 プレフィクス）にエクスプレス フォワーディングされたパケット数とバイト数の収集をイネーブルにします。 • オプションの **prefix-length** キーワードでは、IPv6 プレフィクス長にエクスプレス フォワーディングされたパケット数とバイト数の収集をイネーブルにします。 **（注）** シスコ エクスプレス フォワーディングがルータでグローバルにイネーブルになっている場合、アカウンティング情報は RP で収集されます。分散型シスコ エクスプレス フォワーディングがルータでグローバルにイネーブルになっている場合、アカウンティング情報はライン カードで収集されます。

ユニキャスト RPF の設定

前提条件

ユニキャスト RPF を使用するには、ルータでシスコ エクスプレス フォワーディング スイッチングまたは分散型シスコ エクスプレス フォワーディング スイッチングをイネーブルにします。シスコ エクスプレス フォワーディング スイッチングの入力インターフェイスを設定する必要はありません。シスコ エクスプレス フォワーディングがルータ上で実行されているかぎり、個々のインターフェイスは他のスイッチング モードで設定できます。

（注） ルータでシスコ エクスプレス フォワーディングをグローバルに設定することが非常に重要です。ユニキャスト RPF は、シスコ エクスプレス フォワーディングがないと動作しません。

制約事項

ユニキャスト RPF は、ネットワーク内部のインターフェイスでは使用できません。内部インターフェイスは、ルーティングを非対称にする可能性が高く、パケットの送信元へのルートが複数存在する場合が多いからです。ユニキャスト RPF は、元々対称であるか、対称に設定されている場合にだけ適用してください。

たとえば、ISP のネットワークのエッジにあるルータは、ISP ネットワークのコアにあるルータよりも対称リバース パスを持つ可能性が高くなります。ISP ネットワークのコアにあるルータでは、ルータからの最良の転送パスがルータへ返されるパケットに対して選択されるパスとなることが保証されません。したがって、非対称ルーティングの可能性があるユニキャスト RPF の適用は推奨されません。ネットワークのエッジにだけ、または ISP の場合はネットワークのカスタマー エッジにだけユニキャスト RPF を配置するのが最も単純です。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 verify unicast source reachable-via** {**rx** | **any**} [**allow-default**] [**allow-self-ping**] [*access-list-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* **例：** `Router(config)# interface atm 0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 verify unicast source reachable-via** {**rx** | **any**} [**allow-default**] [**allow-self-ping**] [*access-list-name*] **例：** `Router(config-if)# ipv6 verify unicast source reachable-via any`	送信元アドレスが FIB テーブルに存在していることを確認し、ユニキャスト RPF をイネーブルにします。

IPv6 アドレスへのホスト名のマッピング

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 host** *name* [*port*] *ipv6-address1* [*ipv6-address2...ipv6-address4*]
4. **ip domain name** [**vrf** *vrf-name*] *name*
   または
   ip domain list [**vrf** *vrf-name*] *name*
5. **ip name-server** [**vrf** *vrf-name*] *server-address1* [*server-address2...server-address6*]
6. **ip domain-lookup**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 host** *name* [*port*] *ipv6-address1* [*ipv6-address2...ipv6-address4*] **例：** `Router(config)#  ipv6 host cisco-sj 2001:0DB8:20:1::12`	ホスト名からアドレスへのスタティック マッピングをホスト名キャッシュに定義します。 • 通常は、数字のアドレスではなくシンボリック名でネットワーク デバイスを参照する方が簡単です（Telnet などのサービスでは、ホスト名またはアドレスを使用できます）。ホスト名と IPv6 アドレスは、静的または動的な手段で相互に関連付けることができます。 • ダイナミック マッピングが使用可能でない場合は、ホスト名をアドレスに手動で割り当てると便利です。

	コマンドまたはアクション	目的

ステップ 4	**ip domain name** [**vrf** *vrf-name*] *name*
	または
	ip domain list [**vrf** *vrf-name*] *name*
	
	例：
	`Router(config)# ip domain-name cisco.com`
	または
	
	例：
	`Router(config)# ip domain list cisco1.com`
		（任意）非修飾ホスト名を完成させるために Cisco IOS ソフトウェアで使用されるデフォルトのドメイン名を定義します。
		または
		（任意）非修飾ホスト名を完成させるためのデフォルト ドメイン名のリストを定義します。
		• ドメイン名要求を完成させるために Cisco IOS ソフトウェアで使用されるデフォルトのドメイン名を指定できます。単一のドメイン名またはドメイン名のリストを指定できます。完全なドメイン名を含まないホスト名では、名前が検索される前に、指定したデフォルトドメイン名が付加されます。
		（注） **ip domain name** コマンドと **ip domain list** コマンドは、IPv4 と IPv6 の両方で使用できるデフォルトドメイン名の指定に使用されます。

ステップ 5	**ip name-server** [**vrf** *vrf-name*] *server-address1* [*server-address2...server-address6*] **例：** `Router(config)# ip name-server 2001:0DB8::250:8bff:fee8:f800 2001:0DB8:0:f004::1`	名前情報を提供する 1 つ以上のホストを指定します。 • DNS に名前情報を提供するネーム サーバとして機能できる 1 つ以上（6 つまで）のホストを指定します。 **（注）** *server-address* 引数には、IPv4 アドレスまたは IPv6 アドレスを指定できます。
ステップ 6	**ip domain-lookup** **例：** `Router(config)# ip domain-lookup`	DNS ベースのアドレス変換をイネーブルにします。 • DNS はデフォルトでイネーブルになっています。

IPv6 アドレスから IPv6 ATM およびフレーム リレー インターフェイスへのマッピング

IPv6 アドレスを ATM PVC およびフレーム リレー PVC にマッピングするには、次の作業を実行します。具体的には、この項の手順では、アドレスに到達するために使用される ATM PVC およびフレーム リレー PVC に IPv6 アドレスを明示的にマッピングする方法について説明します。

（注） この作業では、ATM PVC とフレーム リレー PVC の両方の設定方法を示します。多くのネットワークで設定する必要がある PVC のタイプは 1 つだけであるため、手順の多くには任意というラベルが付いています。この項の手順は、ATM LANE には適用されません。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **pvc** [*name*] *vpi*/*vci* [**ces** | **ilmi** | **qsaal** | **smds** | **l2transport**]
5. **protocol ipv6** *ipv6-address* [[**no**] **broadcast**]

6. **exit**
7. **ipv6 address** *ipv6-address*/*prefix-length* **link-local**
8. **exit**
9. **interface** *type number*
10. **frame-relay map ipv6** *ipv6-address dlci* [**broadcast**] [**cisco**] [**ietf**] [**payload-compression** {**packet-by-packet** | **frf9 stac** [*hardware-options*] | **data-stream stac** [*hardware-options*]}]
11. **ipv6 address** *ipv6-address*/*prefix-length* **link-local**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface atm 0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**pvc** [*name*] *vpi*/*vci* [**ces** | **ilmi** | **qsaal** | **smds** | **l2transport**] **例：** `Router(config-if)# pvc 1/32`	（任意）ATM PVC に名前を割り当てるかまたは名前を作成し、ルータを ATM VC コンフィギュレーション モードにします。
ステップ 5	**protocol ipv6** *ipv6-address* [[**no**] **broadcast**] **例：** `Router(config-if-atm-vc)# protocol ipv6 2001:0DB8:2222:1003::45`	（任意）リモート ノードの IPv6 アドレスを、アドレスへの到達に使用する PVC にマッピングします。 • *ipv6-address* 引数は、RFC 2373 に記載された形式で指定する必要があります。この形式では、アドレスは、16 進数値を 16 ビット単位でコロンで区切って指定します。 • オプションの [**no**] **broadcast** キーワードは、IPv6 マルチキャスト パケット（ブロードキャスト パケットではない）がインターフェイスに送信される場合にマップ エントリを使用する必要があるかどうかを示します。擬似ブロードキャストがサポートされます。**protocol ipv6** コマンドの [**no**] **broadcast** キーワードは、同じ ATM PVC に設定された **broadcast** コマンドよりも優先されます。
ステップ 6	**exit** **例：** `Router(config-if-atm-vc)# exit`	ATM VC コンフィギュレーション モードを終了し、ルータをインターフェイス コンフィギュレーション モードに戻します。

	コマンドまたはアクション	目的
ステップ 7	**ipv6 address** *ipv6-address*/*prefix-length* **link-local** **例：** `Router(config-if)# ipv6 address 2001:0DB8:2222:1003::72/64 link-local`	インターフェイスに割り当てられている IPv6 ネットワークを指定し、インターフェイスで IPv6 処理をイネーブルにします。 • この作業のコンテキストでは、リンクの反対側のノードのリンクローカル アドレスは、ネットワークで使用される IGP に必要です。 • **ipv6 address link-local** コマンドを指定して、IPv6 がインターフェイスでイネーブルになっている場合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るリンクローカル アドレスを、インターフェイスに設定します。
ステップ 8	**exit** **例：** `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 9	**interface** *type number* **例：** `Router(config)# interface serial 3`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 10	**frame-relay map ipv6** *ipv6-address dlci* [**broadcast**] [**cisco**] [**ietf**] [**payload-compression** {**packet-by-packet** | **frf9 stac** [*hardware-options*] | **data-stream stac** [*hardware-options*]}] **例：** `Router(config-if)# frame-relay map ipv6 FE80::E0:F727:E400:A 17 broadcast`	（任意）リモート ノードの IPv6 アドレスを、アドレスへの到達に使用する PVC の Data-Link Connection Identifier（DLCI; データリンク接続識別子）にマッピングします。
ステップ 11	**ipv6 address** *ipv6-address*/*prefix-length* **link-local** **例：** `Router(config-if)# ipv6 address 2001:0DB8:2222:1044::46/64 link-local`	インターフェイスに割り当てられている IPv6 ネットワークを指定し、インターフェイスで IPv6 処理をイネーブルにします。 • この作業のコンテキストでは、リンクの反対側のノードのリンクローカル アドレスは、ネットワークで使用される IGP に必要です。 • **ipv6 address link-local** コマンドを指定して、IPv6 がインターフェイスでイネーブルになっている場合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るリンクローカル アドレスを、インターフェイスに設定します。

IPv6 リダイレクト メッセージの表示

IPv6 リダイレクト メッセージを表示するには、次の作業を実行します。示されているコマンドはオプションであり、任意の順序で入力できます。

手順の概要

1. **enable**

2. **show ipv6 interface** [**brief**] [*type number*] [**prefix**]
3. **show ipv6 neighbors** [*interface-type interface-number* | *ipv6-address* | *ipv6-hostname* | **statistics**]
4. **show ipv6 route** [*ipv6-address* | *ipv6-prefix*/*prefix-length* | *protocol* | *interface-type interface-number*]
5. **show ipv6 traffic**
6. **show frame-relay map** [**interface** *type number*] [*dlci*]
7. **show atm map**
8. **show hosts** [**vrf** *vrf-name* | **all** | *hostname* | **summary**]
9. **show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router# enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**show ipv6 interface** [**brief**] [*type number*] [**prefix**] **例：** `Router# show ipv6 interface ethernet 0`	IPv6 用に設定されたインターフェイスが使用可能かどうかのステータスを表示します。 • IPv6 ネイバー リダイレクト メッセージ、IPv6 ネイバー探索メッセージ、およびステートレス自動設定のステータスに関する情報を表示します。
ステップ 3	**show ipv6 neighbors** [*interface-type interface-number* | *ipv6-address* | *ipv6-hostname* | **statistics**] **例：** `Router# show ipv6 neighbors ethernet 2`	IPv6 ネイバー探索キャッシュ情報を表示します。
ステップ 4	**show ipv6 route** [*ipv6-address* | *ipv6-prefix*/*prefix-length* | *protocol* | *interface-type interface-number*] **例：** `Router# show ipv6 route`	IPv6 ルーティング テーブルの現在の内容を表示します。
ステップ 5	**show ipv6 traffic** **例：** `Router# show ipv6 traffic`	IPv6 トラフィックに関する統計情報を表示します。
ステップ 6	**show frame-relay map** [**interface** *type number*] [*dlci*] **例：** `Router# show frame-relay map`	フレーム リレー接続に関する現在のマップ エントリと情報を表示します。
ステップ 7	**show atm map** **例：** `Router# show atm map`	ATM ネットワークおよび ATM バンドル マップのリモート ホストに対して設定されたすべての ATM スタティック マップのリストを表示します。

	コマンドまたはアクション	目的
ステップ 8	**show hosts** [**vrf** *vrf-name* | **all** | *hostname* | **summary**] **例：** `Router# show hosts`	デフォルトのドメイン名、名前ルックアップ サービス、ネーム サーバ ホストのリスト、およびホスト名とアドレスのキャッシュされたリストを表示します。
ステップ 9	**show running-config** **例：** `Router# show running-config`	ルータで実行されている現在の設定を表示します。

例

ここでは、次の出力例について説明します。

- 「show ipv6 interface コマンドの出力例」
- 「ipv6 neighbors コマンドの出力例」
- 「show ipv6 route コマンドの出力例」
- 「show ipv6 traffic コマンドの出力例」
- 「show frame-relay map コマンドの出力例」
- 「show atm map コマンドの出力例」
- 「show hosts コマンドの出力例」
- 「show running-config コマンドの出力例」

show ipv6 interface コマンドの出力例

次の例では、**show ipv6 interface** コマンドを使用して、IPv6 アドレスがイーサネット インターフェイス 0 に対して正しく設定されていることを確認します。IPv6 ネイバー リダイレクト メッセージ、IPv6 ネイバー探索メッセージ、およびステートレス自動設定のステータスに関する情報も表示されます。

```
Router# show ipv6 interface ethernet 0

Ethernet0 is up, line protocol is up
  IPv6 is stalled, link-local address is FE80::1
  Global unicast address(es):
    2001:0DB8:2000::1, subnet is 2001:0DB8:2000::/64
    2001:0DB8:3000::1, subnet is 2001:0DB8:3000::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
```

ipv6 neighbors コマンドの出力例

次の例では、**show ipv6 neighbors** コマンドを使用して、IPv6 ネイバー探索キャッシュ情報を表示します。コマンド出力の Age フィールドのハイフン（-）は、スタティック エントリを示します。次の例は、イーサネット インターフェイス 2 に対する IPv6 ネイバー探索キャッシュ情報を表示します。

```
Router# show ipv6 neighbors ethernet 2

IPv6 Address                                Age Link-layer Addr State Interface
2001:0DB8:0:4::2                              0 0003.a0d6.141e  REACH Ethernet2
FE80::XXXX:A0FF:FED6:141E                     0 0003.a0d6.141e  REACH Ethernet2
2001:0DB8:1::45a                              - 0002.7d1a.9472  REACH Ethernet2
```

show ipv6 route コマンドの出力例

ipv6-address 引数または *ipv6-prefix*/*prefix-length* 引数が指定されている場合は、そのアドレスまたはネットワークのルート情報だけが表示されます。次に、IPv6 プレフィクス 2001:0DB8::/35 を指定して入力した **show ipv6 route** コマンドの出力例を示します。

```
Router# show ipv6 route 2001:0DB8::/35

IPv6 Routing Table - 261 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea

B 2001:0DB8::/35 [20/3]
  via FE80::60:5C59:9E00:16, Tunnel1
```

show ipv6 traffic コマンドの出力例

次の例では、**show ipv6 traffic** コマンドを使用して、ICMP レート制限カウンタを表示します。

```
Router# show ipv6 traffic

ICMP statistics:
  Rcvd: 188 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        1 router solicit, 175 router advert, 0 redirects
        0 neighbor solicit, 12 neighbor advert
  Sent: 7376 output, 56 rate-limited
        unreach: 0 routing, 15 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        15 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 7326 router advert, 0 redirects
        2 neighbor solicit, 22 neighbor advert
```

show frame-relay map コマンドの出力例

次の例では、**show frame-relay map** コマンドを使用して、リモート ノードの IPv6 アドレスがアドレスへの到達に使用される PVC の DLCI にマッピングされていることを確認します。次の例は、2 つのリモート ノードのリンクローカル IPv6 アドレスおよびグローバル IPv6 アドレス（FE80::E0:F727:E400:A と 2001:0DB8:2222:1044::73、FE80::60:3E47:AC8:8 と 2001.0DB8:2222:1044::72）がそれぞれ DLCI 17 と DLCI 19 に明示的にマッピングされていることを示しています。DLCI 17 と DLCI 19 の両方が、このノードのインターフェイス シリアル 3 で終端されているため、このノードのインターフェイス シリアル 3 はポイントツーマルチポイント インターフェイスです。

```
Router# show frame-relay map

Serial3 (up): ipv6 FE80::E0:F727:E400:A dlci 17(0x11,0x410), static,
              broadcast, CISCO, status defined, active
Serial3 (up): ipv6 2001:0DB8:2222:1044::72 dlci 19(0x13,0x430), static,
              CISCO, status defined, active
Serial3 (up): ipv6 2001:0DB8:2222:1044::73 dlci 17(0x11,0x410), static,
              CISCO, status defined, active
Serial3 (up): ipv6 FE80::60:3E47:AC8:8 dlci 19(0x13,0x430), static,
              broadcast, CISCO, status defined, active
```

show atm map コマンドの出力例

次の例では、**show atm map** コマンドを使用して、リモート ノードの IPv6 アドレスがアドレスへの到達に使用される PVC にマッピングされていることを確認します。次の例は、リモート ノードのリンクローカル IPv6 アドレスおよびグローバル IPv6 アドレス（それぞれ FE80::60:3E47:AC8:C と 2001:0DB8:2222:1003::72）が ATM インターフェイス 0 の PVC 1/32 に明示的にマッピングされていることを示しています。

```
Router# show atm map

Map list ATM0pvc1 : PERMANENT
ipv6 FE80::60:3E47:AC8:C maps to VC 1, VPI 1, VCI 32, ATM0
       , broadcast
ipv6 2001:0DB8:2222:1003::72 maps to VC 1, VPI 1, VCI 32, ATM0
```

show hosts コマンドの出力例

DHCP for IPv6 クライアントの名前ルックアップ システムの状態は、**show hosts** コマンドで表示できます。

```
Router# show hosts

Default domain is not set
Domain list:example.com
Name/address lookup uses domain service
Name servers are 2001:0DB8:A:B::1, 2001:0DB8:3000:3000::42

Codes:UN - unknown, EX - expired, OK - OK, ?? - revalidate
       temp - temporary, perm - permanent
       NA - Not Applicable None - Not defined

Host                      Port  Flags      Age Type   Address(es)
sdfasfd                   None  (temp, UN)  0  IPv6
```

show running-config コマンドの出力例

次の例では、**show running-config** コマンドを使用して、パケットの IPv6 処理がルータと該当インターフェイス上でグローバルにイネーブルになっていることと、IPv6 アドレスが該当インターフェイスで設定されていることを確認します。

```
Router# show running-config

Building configuration...

Current configuration : 22324 bytes
!
! Last configuration change at 14:59:38 PST Tue Jan 16 2001
! NVRAM config last updated at 04:25:39 PST Tue Jan 16 2001 by bird
!
hostname Router
!
ipv6 unicast-routing
!
```

```
interface Ethernet0
 no ip route-cache
 no ip mroute-cache
 no keepalive
 media-type 10BaseT
    ipv6 address 2001:0DB8:0:1::/64 eui-64
!
```

次の例では、**show running-config** コマンドを使用して、シスコ エクスプレス フォワーディングとシスコ エクスプレス フォワーディングのネットワーク アカウンティングが非分散型アーキテクチャ プラットフォームでグローバルにイネーブルになっていることと、シスコ エクスプレス フォワーディングが IPv6 インターフェイスでイネーブルになっていることを確認します。次の出力は、シスコ エクスプレス フォワーディングとシスコ エクスプレス フォワーディングのネットワーク アカウンティングの両方がルータでグローバルにイネーブルになっており、シスコ エクスプレス フォワーディングがイーサネット インターフェイス 0 でもイネーブルになっていることを示しています。

```
Router# show running-config

Building configuration...

Current configuration : 22324 bytes
!
! Last configuration change at 14:59:38 PST Tue Jan 16 2001
! NVRAM config last updated at 04:25:39 PST Tue Jan 16 2001 by bird
!
hostname Router
!
ip cef
ipv6 unicast-routing
ipv6 cef
ipv6 cef accounting prefix-length
!
!
interface Ethernet0
 ip address 10.4.9.11 255.0.0.0
 media-type 10BaseT
 ipv6 address 2001:0DB8:C18:1::/64 eui-64
!
```

次の例では、**show running-config** コマンドを使用して、分散型シスコ エクスプレス フォワーディングと分散型シスコ エクスプレス フォワーディングのネットワーク アカウンティングが Cisco 7500 シリーズ ルータなどの分散型アーキテクチャ プラットフォームでグローバルにイネーブルになっていることを確認します。次の例は、分散型シスコ エクスプレス フォワーディングと分散型シスコ エクスプレス フォワーディングのネットワーク アカウンティングの両方がルータでグローバルにイネーブルになっていることを示しています。

（注） 分散型シスコ エクスプレス フォワーディングは、GSR ではデフォルトでイネーブルになり、Cisco 7500 シリーズ ルータではデフォルトでディセーブルになります。したがって、GSR での **show running-config** コマンドの出力には、分散型シスコ エクスプレス フォワーディングがルータでグローバルに設定されているかどうかは表示されません。次に、Cisco 7500 シリーズ ルータからの出力を示します。

```
Router# show running-config

Building configuration...

Current configuration : 22324 bytes
!
! Last configuration change at 14:59:38 PST Tue Jan 16 2001
! NVRAM config last updated at 04:25:39 PST Tue Jan 16 2001 by bird
```

```
!
hostname Router
!
ip cef distributed
ipv6 unicast-routing
ipv6 cef distributed
ipv6 cef accounting prefix-length
```

次の例では、**show running-config** コマンドを使用して、ホスト名からアドレスへのマッピング、デフォルト ドメイン名、およびホスト名キャッシュ内のネーム サーバを確認し、DNS サービスがイネーブルになっていることを確認します。

```
Router# show running-config

Building configuration...
!
ipv6 host cisco-sj 2001:0DB8:20:1::12
!
ip domain-name cisco.com
ip domain-lookup
ip name-server 2001:0DB8:C01F:768::1
```

IPv6 アドレッシングと基本接続の実装の設定例

例：IPv6 アドレッシングと IPv6 ルーティングの設定

次の例では、IPv6 は、ルータ上で IPv6 プレフィクス 2001:0DB8:c18:1::/64 に基づくリンクローカル アドレスとグローバル アドレスの両方でイネーブルになっています。EUI-64 インターフェイス ID が、両方のアドレスの下位 64 ビットで使用されます。**show ipv6 interface** コマンドからの出力は、インターフェイス ID（260:3EFF:FE47:1530）がイーサネット インターフェイス 0 のリンクローカル プレフィクス FE80::/64 にどのように追加されるかを示します。

```
ipv6 unicast-routing

interface ethernet 0
  ipv6 address 2001:0DB8:c18:1::/64 eui-64

Router# show ipv6 interface ethernet 0

Ethernet0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::260:3EFF:FE47:1530
  Global unicast address(es):
    2001:0DB8:C18:1:260:3EFF:FE47:1530, subnet is 2001:0DB8:C18:1::/64
  Joined group address(es):
    FF02::1
    FF02::2
```

```
    FF02::1:FF47:1530
    FF02::9
  MTU is 1500 bytes
  ICMP error messages limited to one every 500 milliseconds
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
```

次の例では、プレフィクス 2001:0DB8::/64 内の複数の IPv6 グローバル アドレスがイーサネット インターフェイス 0 に設定されています。

```
interface ethernet 0
 ipv6 address 2001:0DB8::1/64
 ipv6 address 2001:0DB8::/64 eui-64
```

例：デュアル プロトコル スタックの設定

次の例では、ルータで IPv6 ユニキャスト データグラムの転送をグローバルにイネーブルにし、IPv4 アドレスと IPv6 アドレスの両方でイーサネット インターフェイス 0 を設定します。

```
ipv6 unicast-routing

interface Ethernet0
 ip address 192.168.99.1 255.255.255.0
 ipv6 address 2001:0DB8:c18:1::3/64
```

例：IPv6 ICMP レート制限の設定

次の例は、50 ミリ秒の間隔と 20 トークンのバケット サイズが IPv6 ICMP エラー メッセージに対して設定されていることを示します。

```
ipv6 icmp error-interval 50 20
```

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

次の例では、Cisco Express Forwarding for IPv6 および Cisco Express Forwarding for IPv6 のネットワーク アカウンティングの両方が非分散型アーキテクチャ ルータでグローバルにイネーブルになっていて、Cisco Express Forwarding for IPv6 がイーサネット インターフェイス 0 でイネーブルになっています。例では、**ipv6 unicast-routing** コマンドを使用して IPv6 ユニキャスト データグラムの転送がルータ上でグローバルに設定されていること、**ipv6 address** コマンドを使用して IPv6 アドレスがイーサネット インターフェイス 0 に設定されていること、および **ip cef** コマンドを使用して Cisco Express Forwarding for IPv4 がルータでグローバルに設定されていることも示されています。

```
ip cef
ipv6 unicast-routing
ipv6 cef
ipv6 cef accounting prefix-length

interface Ethernet0
 ip address 10.4.9.11 255.0.0.0
 media-type 10BaseT
 ipv6 address 2001:0DB8:C18:1::/64 eui-64
```

次の例では、分散型 Cisco Express Forwarding for IPv6 および分散型 Cisco Express Forwarding for IPv6 のネットワーク アカウンティングの両方が分散型アーキテクチャ ルータでグローバルにイネーブルになっています。**ipv6 unicast-routing** コマンドで IPv6 ユニキャスト データグラムの転送がルータでグローバルに設定され、**ip cef distributed** コマンドで分散型 Cisco Express Forwarding for IPv4 がルータでグローバルに設定されています。

```
ip cef distributed
ipv6 unicast-routing
ipv6 cef distributed
ipv6 cef accounting prefix-length
```

例：ホスト名からアドレスへのマッピングの設定

次の例では、ホスト名キャッシュに 2 つの静的なホスト名からアドレスへのマッピングを定義し、未修飾のホスト名を完成させるための複数の代替ドメイン名でドメイン リストを設定します。また、ホスト 2001:0DB8::250:8bff:fee8:f800 とホスト 2001:0DB8:0:f004::1 をネーム サーバとして指定し、DNS サービスを再びイネーブルにします。

```
ipv6 host cisco-sj 2001:0DB8:700:20:1::12
ipv6 host cisco-hq 2001:0DB8:768::1 2001:0DB8:20:1::22
ip domain list example1.com
ip domain list example2.com
ip domain list example3.edu
ip name-server 2001:0DB8::250:8bff:fee8:f800 2001:0DB8:0:f004::1
ip domain-lookup
```

例：IPv6 アドレスから ATM PVC およびフレーム リレー PVC へのマッピングの設定

- 「例：IPv6 ATM PVC マッピングの設定：ポイントツーポイント インターフェイス」
- 「例：IPv6 ATM PVC マッピングの設定：ポイントツーマルチポイント インターフェイス」
- 「例：IPv6 フレーム リレー PVC マッピングの設定：ポイントツーポイント インターフェイス」
- 「例：IPv6 フレーム リレー PVC マッピングの設定：ポイントツーマルチポイント インターフェイス」

例：IPv6 ATM PVC マッピングの設定：ポイントツーポイント インターフェイス

次の例では、ルータ 1 およびルータ 2 という名前の 2 つのノードが単一の PVC で接続されています。ポイントツーポイント サブインターフェイス ATM0.132 が、PVC を終端するために両方のノードで使用されています。したがって、両方のノードの IPv6 アドレスと PVC との間のマッピングは暗黙的です（追加のマッピングは不要です）。

ルータ 1 の設定

```
interface ATM 0
 no ip address
!
interface ATM 0.132 point-to-point
 pvc 1/32
 encapsulation aal5snap
 !
 ipv6 address 2001:0DB8:2222:1003::72/64
```

ルータ 2 の設定

```
interface ATM 0
 no ip address
!
interface ATM 0.132 point-to-point
 pvc 1/32
 encapsulation aal5snap
 !
 ipv6 address 2001:0DB8:2222:1003::45/64
```

例：IPv6 ATM PVC マッピングの設定：ポイントツーマルチポイント インターフェイス

次の例では、前の例と同じ 2 つのノード（ルータ 1 とルータ 2）が同じ PVC で接続されています。ただし、この例では、PVC を終端するために両方のノードでポイントツーマルチポイント インターフェイス ATM0 が使用されています。したがって、両方のノードのインターフェイス ATM0 のリンクローカル IPv6 アドレスおよびグローバル IPv6 アドレスと PVC との間には明示的なマッピングが必要です。また、両方のノードのインターフェイス ATM0 のリンクローカル アドレスで ATM 擬似ブロードキャストがイネーブルになっています。ここで指定したリンクローカル アドレスは、PVC のもう一方の側のリンクローカル アドレスです。

ルータ 1 の設定

```
interface ATM 0
 no ip address
 pvc 1/32
 protocol ipv6 2001:0DB8:2222:1003::45
 protocol ipv6 FE80::60:2FA4:8291:2 broadcast
 encapsulation aal5snap
 !
 ipv6 address 2001:0DB8:2222:1003::72/64
```

ルータ 2 の設定

```
interface ATM 0
 no ip address
 pvc 1/32
 protocol ipv6 FE80::60:3E47:AC8:C broadcast
 protocol ipv6 2001:0DB8:2222:1003::72
 encapsulation aal5snap
 !
 ipv6 address 2001:0DB8:2222:1003::45/64
```

例：IPv6 フレーム リレー PVC マッピングの設定：ポイントツーポイント インターフェイス

次の例では、ルータ A、ルータ B、およびルータ C という 3 つのノードが完全メッシュ ネットワークを構成します。各ノードは、他の 2 つの各ノードへの個別の接続を提供する 2 つの PVC で設定されています。各 PVC は異なるポイントツーポイント サブインターフェイスに設定され、3 つの固有な IPv6 ネットワーク（2001:0DB8:2222:1017:/64、2001:0DB8:2222:1018::/64、および 2001:0DB8:2222:1019::/64）を作成します。したがって、各ノードの IPv6 アドレスとアドレスへの到達に使用される PVC の DLCI（DLCI 17、18、19）との間のマッピングは暗黙的です（追加のマッピングは不要です）。

（注） 次の例の各 PVC が異なるポイントツーポイント サブインターフェイスに設定されている場合、次の例の設定は、完全メッシュでないネットワークでも使用できます。また、各 PVC を異なるポイントツーポイント サブインターフェイスに設定すると、ルーティング プロトコル設定を簡略化できます。ただし、次の例の設定では複数の IPv6 ネットワークが必要ですが、各 PVC をポイントツーマルチポイント インターフェイスに設定するために必要な IPv6 ネットワークは 1 つだけです。

ルータ A の設定

```
interface Serial 3
 encapsulation frame-relay
!
interface Serial3.17 point-to-point
 description to Router B
 ipv6 address 2001:0DB8:2222:1017::46/64
 frame-relay interface-dlci 17
!
interface Serial 3.19 point-to-point
 description to Router C
 ipv6 address 2001:0DB8:2222:1019::46/64
 frame-relay interface-dlci 19
```

ルータ B の設定

```
interface Serial 5
 encapsulation frame-relay
!
interface Serial5.17 point-to-point
 description to Router A
 ipv6 address 2001:0DB8:2222:1017::73/64
 frame-relay interface-dlci 17
!
interface Serial5.18 point-to-point
 description to Router C
 ipv6 address 2001:0DB8:2222:1018::73/64
 frame-relay interface-dlci 18
```

ルータ C の設定

```
interface Serial 0
 encapsulation frame-relay
!
interface Serial0.18 point-to-point
 description to Router B
 ipv6 address 2001:0DB8:2222:1018::72/64
 frame-relay interface-dlci 18
!
interface Serial0.19 point-to-point
 description to Router A
 ipv6 address 2001:0DB8:2222:1019::72/64
 frame-relay interface-dlci 19
```

例：IPv6 フレーム リレー PVC マッピングの設定：ポイントツーマルチポイント インターフェイス

次の例では、前の例と同じ 3 つのノード（ルータ A、ルータ B、およびルータ C）が完全メッシュ ネットワークを構成し、各ノードに 2 つの PVC が設定されています（これにより、他の 2 つの各ノードへの個別の接続が提供されます）。ただし、次の例の各ノード上の 2 つの PVC は、単一のインターフェイス（それぞれ、シリアル 3、シリアル 5、およびシリアル 10）に設定されています。これによ

り、各インターフェイスはポイントツーマルチポイント インターフェイスになります。したがって、3 つのノードすべての各インターフェイスのリンクローカル IPv6 アドレスおよびグローバル IPv6 アドレスと、アドレスへの到達に使用される PVC の DLCI（DLCI 17、18、19）との間には、明示的なマッピングが必要です。

ルータ A の設定

```
interface Serial 3
 encapsulation frame-relay
 ipv6 address 2001:0DB8:2222:1044::46/64
 frame-relay map ipv6 FE80::E0:F727:E400:A 17 broadcast
 frame-relay map ipv6 FE80::60:3E47:AC8:8 19 broadcast
 frame-relay map ipv6 2001:0DB8:2222:1044::72 19
 frame-relay map ipv6 2001:0DB8:2222:1044::73 17
```

ルータ B の設定

```
interface Serial 5
 encapsulation frame-relay
 ipv6 address 2001:0DB8:2222:1044::73/64
 frame-relay map ipv6 FE80::60:3E59:DA78:C 17 broadcast
 frame-relay map ipv6 FE80::60:3E47:AC8:8 18 broadcast
 frame-relay map ipv6 2001:0DB8:2222:1044::46 17
 frame-relay map ipv6 2001:0DB8:2222:1044::72 18
```

ルータ C の設定

```
interface Serial 10
 encapsulation frame-relay
 ipv6 address 2001:0DB8:2222:1044::72/64
 frame-relay map ipv6 FE80::60:3E59:DA78:C 19 broadcast
 frame-relay map ipv6 FE80::E0:F727:E400:A 18 broadcast
 frame-relay map ipv6 2001:0DB8:2222:1044::46 19
 frame-relay map ipv6 2001:0DB8:2222:1044::73 18
```

関連情報

IPv6 ルーティング プロトコルを実装する場合は、「*Implementing RIP for IPv6*」、「*Implementing IS-IS for IPv6*」、または「*Implementing Multiprotocol BGP for IPv6*」の章を参照してください。

その他の関連資料

関連資料

関連項目	参照先
IPv6 のサポート機能リスト	『*Cisco IOS IPv6 Configuration Guide*』の「Start Here: Cisco IOS Software Release Specifics for IPv6 Features」
IPv6 コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト、使用に関する注意事項、および例	『*Cisco IOS IPv6 Command Reference*』
IPv6 DHCP の説明と設定	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing DHCP for IPv6」
IPv4 アドレッシングの設定作業	『*Cisco IOS IP Addressing Services Configuration Guide*』の「Configuring IPv4 Addresses」
IPv4 サービスの設定作業	『*Cisco IOS IP Application Services Configuration Guide*』の「Configuring IP Services」
IPv4 アドレッシング コマンド	『*Cisco IOS IP Addressing Services Command Reference*』
IPv4 IP サービス コマンド	『*Cisco IOS IP Application Services Command Reference*』
ステートフル スイッチオーバー	『*Cisco IOS High Availability Configuration Guide*』の「Stateful Switchover」
スイッチングの設定作業	『*Cisco IOS IP Switching Configuration Guide*』の「Cisco IOS IP Switching Features Roadmap」
スイッチング コマンド	『*Cisco IOS IP Switching Command Reference*』

規格

規格	タイトル
この機能によってサポートされる新しい規格または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 1981	『*Path MTU Discovery for IP version 6*』
RFC 2373	『*IP Version 6 Addressing Architecture*』
RFC 2374	『*An Aggregatable Global Unicast Address Format*』
RFC 2460	『*Internet Protocol, Version 6 (IPv6) Specification*』
RFC 2461	『*Neighbor Discovery for IP Version 6 (IPv6)*』
RFC 2462	『*IPv6 Stateless Address Autoconfiguration*』
RFC 2463	『*Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*』
RFC 2464	『*Transmission of IPv6 Packets over Ethernet Networks*』
RFC 2467	『*Transmission of IPv6 Packets over FDDI Networks*』
RFC 2472	『*IP Version 6 over PPP*』
RFC 2492	『*IPv6 over ATM Networks*』
RFC 2590	『*Transmission of IPv6 Packets over Frame Relay Networks Specification*』
RFC 3152	『*Delegation of IP6.ARPA*』
RFC 3162	『*RADIUS and IPv6*』
RFC 3513	『*Internet Protocol Version 6 (IPv6) Addressing Architecture*』
RFC 3596	『*DNS Extensions to Support IP version 6*』
RFC 3879	『*Deprecating Site Local Addresses*』
RFC 4193	『*Unique Local IPv6 Unicast Addresses*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 アドレッシングと基本接続の実装の機能情報

表 5 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どのソフトウェア イメージが特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 5 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 5　IPv6 アドレッシングと基本接続の実装の機能情報

機能名	リリース	機能情報
IPv6：エニーキャスト アドレス	12.2(25)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(33)SXH 12.3(4)T 12.4 12.4(2)T	エニーキャスト アドレスは、通常は異なるノードに属するインターフェイスのセットに割り当てられます。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 アドレス タイプ：エニーキャスト」（P.9） • 「IPv6 アドレス タイプ：マルチキャスト」（P.10） • 「IPv6 マルチキャスト グループ」（P.11） • 「IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル」（P.32）
IPv6：基本プロトコル ハイ アベイラビリティ	12.2(33)SRE	IPv6 ネイバー探索では SSO がサポートされます。 この機能に関する詳細については、次の項を参照してください。 • 「ステートフル スイッチオーバー」（P.21）
IPv6：ICMPv6	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(17a)SX1 12.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T	ICMP for IPv6 は、ICMP 宛先到達不能メッセージなどのエラー メッセージと、ICMP エコー要求および応答メッセージなどの情報メッセージを生成します。また、IPv6 の ICMP パケットは、IPv6 ネイバー探索プロセス、パス MTU 探索、および IPv6 の MLD プロトコルで使用されます。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 の ICMP」（P.19） • 「IPv6 ネイバー探索」（P.20） • 「IPv6 ネイバー請求メッセージ」（P.21） • 「IPv6 ルータ アドバタイズメント メッセージ」（P.22） • 「IPv6 ステートレス自動設定」（P.26） • 「IPv6 ICMP レート制限の設定」（P.38） • 「例：IPv6 ICMP レート制限の設定」（P.55）

表 5　IPv6 アドレッシングと基本接続の実装の機能情報 （続き）

機能名	リリース	機能情報
IPv6：ICMPv6 リダイレクト	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(17a)SX1 12.2(4)T 12.3 12.3(2)T 12.4 12.4(2)T	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。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 ネイバー リダイレクト メッセージ」（P.24） • 「IPv6 リダイレクト メッセージ」（P.30）
IPv6：ICMP レート制限	12.2(8)T 12.3 12.3(2)T 12.4 12.4(2)T	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。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 ICMP レート制限の設定」（P.38） • 「IPv6 ICMP レート制限」（P.20） • 「例：IPv6 ICMP レート制限の設定」（P.55）
IPv6：IPv6 デフォルト ルータ プリファレンス	12.2(33)SB 12.2(33)SRA 12.4(2)T 12.2(33)SXH 15.0(1)S	DRP 拡張は、大まかなプリファレンス メトリック（低、中、高）をデフォルト ルータに提供します。 この機能に関する詳細については、次の各項を参照してください。 • 「トラフィック エンジニアリングのデフォルト ルータ プリファレンス」（P.24） • 「トラフィック エンジニアリングの DRP 拡張の設定」（P.39）
IPv6：IPv6 MTU パス ディスカバリ	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(17a)SX1 12.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	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。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 のパス MTU ディスカバリ」（P.19） • 「IPv6 の ICMP」（P.19）

表 5　IPv6 アドレッシングと基本接続の実装の機能情報 （続き）

機能名	リリース	機能情報
IPv6：IPv6 ネイバー探索	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(17a)SX1 12.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	IPv6 ネイバー探索プロセスでは、ICMP メッセージおよび請求ノード マルチキャスト アドレスを使用して、同じネットワーク（ローカル リンク）上のネイバーのリンク レイヤ 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、ネイバー ルータを追跡します。 この機能に関する詳細については、次の各項を参照してください。 • 「リンクローカル アドレス」（P.7） • 「IPv6 の ICMP」（P.19） • 「IPv6 ネイバー探索」（P.20） • 「IPv6 マルチキャスト グループ」（P.11）
IPv6：IPv6 ネイバー探索重複アドレス検出	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(17a)SX1 12.2(4)T 12.3 12.3(2)T 12.4 12.4(2)T	新規のリンクローカル IPv6 アドレスに対しては、アドレスがインターフェイスに割り当てられる前に、最初に IPv6 ネイバー探索重複アドレス検出が実行されます（重複アドレス検出の実行中、新規アドレスは一時的な状態のままです）。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 ネイバー請求メッセージ」（P.21） • 「IPv6 ステートレス自動設定」（P.26）
IPv6：IPv6 ステートレス自動設定	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(17a)SX1 12.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	IPv6 ステートレス自動設定機能を使用して、リンク、サブネット、およびサイト アドレッシングの変更を管理できます。 この機能に関する詳細については、次の各項を参照してください。 • 「リンクローカル アドレス」（P.7） • 「IPv6 ネイバー請求メッセージ」（P.21） • 「IPv6 ルータ アドバタイズメント メッセージ」（P.22） • 「IPv6 ステートレス自動設定」（P.26） • 「IPv6 ホストの簡易ネットワーク リナンバリング」（P.26）
IPv6：ネイバー探索用の IPv6 スタティック キャッシュ エントリ	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(33)SRA 12.2(17a)SX1 12.2(8)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	ネイバー探索用の IPv6 スタティック キャッシュ エントリ機能により、IPv6 ネイバー キャッシュ内にスタティック エントリを作成できます。 この機能に関する詳細については、次の項を参照してください。 • 「IPv6 ネイバー探索」（P.20）

表 5　IPv6 アドレッシングと基本接続の実装の機能情報 （続き）

機能名	リリース	機能情報
IPv6：Per-Interface ネイバー探索キャッシュ制限	15.1(3)T	Per-Interface ネイバー探索キャッシュ制限機能により、インターフェイス単位でネイバー探索キャッシュのエントリ数を制限できます。この機能に関する詳細については、次の各項を参照してください。 • 「Per-Interface ネイバー探索キャッシュ制限」（P.26） • 「ネイバー探索キャッシュ制限の設定」（P.34） **ipv6 nd cache interface-limit**（グローバル）、**ipv6 nd cache interface-limit**（インターフェイス）、**show ipv6 neighbors** の各コマンドがこの機能のために導入または修正されました。
IPv6 アクセス サービス：Routed Bridged Encapsulation（RBE; ルーテッド ブリッジ カプセル化）	12.3(4)T 12.4 12.4(2)T	RBE は、ブリッジ インターフェイスから別のルーテッド インターフェイスまたはブリッジ インターフェイスにプロトコルをルーティングするメカニズムを提供します。 この機能に関する詳細については、次の項を参照してください。 • 「IPv6 のルーテッド ブリッジ カプセル化」（P.29）
IPv6 アドレス タイプ：ユニキャスト	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(33)SRA 12.2(17a)SX1 12.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T	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。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 アドレスの形式」（P.4） • 「IPv6 アドレス タイプ：ユニキャスト」（P.6） • 「IPv6 アドレス タイプ：エニーキャスト」（P.9） • 「IPv6 アドレス タイプ：マルチキャスト」（P.10） • 「IPv6 ネイバー請求メッセージ」（P.21） • 「IPv6 ルータ アドバタイズメント メッセージ」（P.22） • 「IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル」（P.32）
IPv6 データ リンク：ATM PVC および ATM LANE	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(33)SRA 12.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T	IPv6 ネットワークでは、データ リンクは特定のリンク ローカル プレフィクスを共有するネットワークです。ATM PVC および ATM LANE は、IPv6 でサポートされるデータ リンクです。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 データ リンク」（P.28） • 「IPv6 のシスコ エクスプレス フォワーディング スイッチングと分散型シスコ エクスプレス フォワーディング スイッチングの設定」（P.40） • 「IPv6 アドレスから IPv6 ATM およびフレーム リレー インターフェイスへのマッピング」（P.46）

表 5　IPv6 アドレッシングと基本接続の実装の機能情報 （続き）

機能名	リリース	機能情報
IPv6 データ リンク：Cisco High-Level Data Link Control（HDLC; ハイ レベル データリンク コントロール）	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(33)SRA 12.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T	IPv6 ネットワークでは、データ リンクは特定のリンク ローカル プレフィクスを共有するネットワークです。HDLC は、IPv6 でサポートされるデータ リンクのタイプです。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 データ リンク」（P.28） • 「IPv6 のシスコ エクスプレス フォワーディング スイッチングと分散型シスコ エクスプレス フォワーディング スイッチングの設定」（P.40） • 「IPv6 アドレスから IPv6 ATM およびフレーム リレー インターフェイスへのマッピング」（P.46）
IPv6 データ リンク：Dynamic Packet Transport（DPT; ダイナミック パケット トランスポート）	12.0(23)S	IPv6 ネットワークでは、データ リンクは特定のリンク ローカル プレフィクスを共有するネットワークです。DPT は、IPv6 でサポートされるデータ リンクのタイプです。 この機能に関する詳細については、次の項を参照してください。 • 「IPv6 データ リンク」（P.28）
IPv6 データ リンク：イーサネット、ファスト イーサネット、ギガビット イーサネット、および 10- ギガビット イーサネット	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(33)SRA1 2.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T	IPv6 ネットワークでは、データ リンクは特定のリンク ローカル プレフィクスを共有するネットワークです。イーサネット、ファスト イーサネット、ギガビット イーサネット、および 10- ギガビット イーサネットは、IPv6 でサポートされるデータ リンクです。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 データ リンク」（P.28） • 「IPv6 のシスコ エクスプレス フォワーディング スイッチングと分散型シスコ エクスプレス フォワーディング スイッチングの設定」（P.40）
IPv6 データ リンク：FDDI	12.2(14)S 12.2(28)SB 12.2(33)SRA 12.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T	IPv6 ネットワークでは、データ リンクは特定のリンクローカル プレフィクスを共有するネットワークです。FDDI は、IPv6 でサポートされるデータ リンクのタイプです。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 データ リンク」（P.28） • 「IPv6 のシスコ エクスプレス フォワーディング スイッチングと分散型シスコ エクスプレス フォワーディング スイッチングの設定」（P.40）

表 5　IPv6 アドレッシングと基本接続の実装の機能情報 （続き）

機能名	リリース	機能情報
IPv6 データ リンク：フレーム リレー PVC	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(33)SRA 12.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T	IPv6 ネットワークでは、データ リンクは特定のリンク ローカル プレフィクスを共有するネットワークです。フレーム リレー PVC は、IPv6 でサポートされるデータ リンクのタイプです。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 データ リンク」（P.28） • 「IPv6 のシスコ エクスプレス フォワーディング スイッチングと分散型シスコ エクスプレス フォワーディング スイッチングの設定」（P.40） • 「IPv6 アドレスから IPv6 ATM およびフレーム リレー インターフェイスへのマッピング」（P.46）
IPv6 データ リンク：PPP service over Packet over SONET、ISDN、およびシリアル（非同期および同期）インターフェイス	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(33)SRA 12.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T	IPv6 ネットワークでは、データ リンクは特定のリンク ローカル プレフィクスを共有するネットワークです。PPP service over Packet over SONET、ISDN、およびシリアル インターフェイスは、IPv6 でサポートされるデータ リンクのタイプです。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 データ リンク」（P.28） • 「IPv6 のシスコ エクスプレス フォワーディング スイッチングと分散型シスコ エクスプレス フォワーディング スイッチングの設定」（P.40） • 「IPv6 アドレスから IPv6 ATM およびフレーム リレー インターフェイスへのマッピング」（P.46）
IPv6 データ リンク：Cisco Inter-Switch Link（ISL; スイッチ間リンク）を使用した VLAN	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(18)SXE 12.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	IPv6 ネットワークでは、データ リンクは特定のリンク ローカル プレフィクスを共有するネットワークです。Cisco ISL を使用した VLAN は、IPv6 でサポートされるデータ リンクのタイプです。 この機能に関する詳細については、次の項を参照してください。 • 「IPv6 データ リンク」（P.28）

表 5　IPv6 アドレッシングと基本接続の実装の機能情報 （続き）

機能名	リリース	機能情報
IPv6 データ リンク：IEEE 802.1Q カプセル化を使用した VLAN	12.0(22)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(18)SXE 12.2(14)S 12.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	IPv6 ネットワークでは、データ リンクは特定のリンク ローカル プレフィクスを共有するネットワークです。IEEE 802.1Q カプセル化を使用した VLAN は、IPv6 でサポートされるデータ リンクのタイプです。 この機能に関する詳細については、次の項を参照してください。 • 「IPv6 データ リンク」（P.28）
IPv6 サービス：IPv4 トランスポートでの AAAA DNS ルックアップ	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(17a)SX1 12.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	IPv6 基本接続は、DNS の名前からアドレスおよびアドレスから名前のルックアップ プロセスで AAAA レコード タイプのサポートを設定することで拡張できます。 この機能に関する詳細については、次の項を参照してください。 • 「IPv6 の DNS」（P.18）
IPv6 サービス：シスコ検出プロトコル：ネイバー情報の IPv6 アドレス ファミリ サポート	12.2(14)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(18)SXE 12.2(8)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	ネイバー情報のシスコ検出プロトコル IPv6 アドレス サポート機能により、2 台のシスコ デバイス間で IPv6 アドレッシング情報を転送する機能が追加されます。 この機能に関する詳細については、次の項を参照してください。 • 「シスコ検出プロトコル IPv6 アドレスのサポート」（P.19）
IPv6 サービス：IPv6 トランスポートでの DNS ルックアップ	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(25)SG 12.2(33)SRE2 12.2(8)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	IPv6 では、DNS の名前からアドレスおよびアドレスから名前のルックアップ プロセスでサポートされる DNS レコード タイプがサポートされます。 この機能に関する詳細については、次の項を参照してください。 • 「IPv6 の DNS」（P.18）

表 5　IPv6 アドレッシングと基本接続の実装の機能情報 （続き）

機能名	リリース	機能情報
IPv6 サービス：汎用プレフィクス	12.3(4)T 12.4 12.4(2)T	IPv6 アドレスの上位 64 ビットは、グローバル ルーティング プレフィクスとサブネット ID から構成されます。汎用プレフィクス（/48 など）には、短いプレフィクスが保持されます。このプレフィクスに基づいて、より長く詳細な複数のプレフィクス（/64 など）を定義できます。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 の汎用プレフィクス」（P.27） • 「IPv6 汎用プレフィクスの定義と使用」（P.35）
IPv6 スイッチング：シスコ エクスプレス フォワーディングと分散型シスコ エクスプレス フォワーディングのサポート	12.0(21)ST 12.0(22)S 12.2(14)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(17a)SX1 12.2(13)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	Cisco Express Forwarding for IPv6 は、IPv6 パケットを転送するための高度なレイヤ 3 IP スイッチング テクノロジーです。分散型 Cisco Express Forwarding for IPv6 は、CEFv6 と同じ機能を実行しますが、GSR や Cisco 7500 シリーズ ルータなどの分散型アーキテクチャ プラットフォーム用です。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 のシスコ エクスプレス フォワーディング スイッチングと分散型シスコ エクスプレス フォワーディング スイッチング」（P.16） • 「IPv6 のシスコ エクスプレス フォワーディング スイッチングと分散型シスコ エクスプレス フォワーディング スイッチングの設定」（P.40）
BVI インターフェイス上での IPv6 サポート	15.1(2)T	この機能により、IPv6 コマンドが BVI 上でサポートされます。それにより、ユーザが IPv6 アドレスを BVI に割り当て、IPv6 パケットをルーティングできるようになります。 この機能に関する詳細については、次の各項を参照してください。 • 「ブリッジングおよびルーティングのための BVI インターフェイス上での IPv6」（P.30）
IPv6 のユニキャスト Reverse Path Forwarding	12.0(31)S	ユニキャスト RPF 機能により、IPv6 ルータを経由する不正形式または偽造（スプーフィング）IPv6 送信元アドレスを原因とする問題が軽減されます。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 アドレッシングと基本接続の実装の前提条件」（P.2） • 「ユニキャスト Reverse Path Forwarding」（P.17）

Bidirectional Forwarding Detection for IPv6 の実装

このマニュアルでは、Bidirectional Forwarding Detection for IPv6（BFDv6）プロトコルを実装する方法について説明します。BFD はあらゆるメディア タイプ、カプセル化、トポロジ、およびルーティング プロトコルの高速転送パス障害検出回数を提供するように設計された検出プロトコルです。高速転送パス障害検出に加えて、BFD はネットワーク管理者に整合性のある障害検出方法を提供します。BFDv6 は、IPv6 アドレスに対応することで IPv6 サポートを提供します。また、BFDv6 セッションを作成する機能も提供します。

ネットワーク管理者は BFD を使用して、さまざまなルーティング プロトコルの hello メカニズムで、変動速度ではなく一定速度で転送パスの障害を検出できるため、ネットワーク プロファイリングおよびプランニングが容易になります。また、再コンバージェンス時間の整合性が保たれ、予測可能になります。

機能情報の確認

お使いのソフトウェア リリースが、このモジュールで説明されている機能の一部をサポートしていないことがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「Bidirectional Forwarding Detection for IPv6 の実装の機能情報」（P.15）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

目次

Bidirectional Forwarding Detection for IPv6 の実装の前提条件

参加するすべてのルータ上で IPv6 シスコ エクスプレス フォワーディングおよび IPv6 ユニキャスト ルーティングがイネーブルになっている必要があります。

Bidirectional Forwarding Detection for IPv6 の実装の制約事項

- グローバル IPv6 アドレスがインターフェイス上で設定されている場合、BFDv6 はグローバル IPv6 ネイバー アドレスだけをサポートします。
- 非同期モードのみがサポートされます。非同期モードでは、どちらの BFDv6 ピアも BFDv6 セッションを開始できます。

Bidirectional Forwarding Detection for IPv6 の実装に関する情報

BFDv6 プロトコルの概要

ここでは、BFDv6 プロトコル、IPv4 用の BFD との違い、および IPv4 用の BFD との協調動作について説明します。BFD はあらゆるメディア タイプ、カプセル化、トポロジ、およびルーティング プロトコルの高速転送パス障害検出回数を提供するように設計された検出プロトコルです。高速転送パス障害検出に加えて、BFD はネットワーク管理者に整合性のある障害検出方法を提供します。BFDv6 は、IPv6 アドレスに対応することで IPv6 サポートを提供します。また、BFDv6 セッションを作成する機能も提供します。

BFDv6 登録

BFD クライアントは、レジストリ Application Program Interface（API; アプリケーション プログラム インターフェイス）を使用して BFD に登録します。レジストリ引数には、プロトコル タイプ、監視するルートのアドレスと Interface Description Block（IDB; インターフェイス記述ブロック）などがあります。これらの API と引数は、BFD によってすべて IPv4 であると仮定されます。

BFDv6 には、これらの引数を削除したレジストリがあります。プロトコルおよびカプセル化は、セッション情報構造内に記述されます。これらのセッション情報構造は、サポートされているプロトコルに対して BFDv6 によって定義されます。BFDv6 は、セッション情報構造の情報を使用して、そのセッション上の BFDv6 パケットに対する正しいカプセル化を決定します。

BFDv6 のグローバルおよびリンクローカル アドレス

BFDv6 では、ネイバーの作成に、グローバルとリンクローカルの両方のアドレスがサポートされています。BFDv6 セッションでは、ネイバーのアドレス タイプと一致するように送信元アドレスが選択されます（たとえば、グローバル IPv6 アドレスのネイバーはグローバル IPv6 送信元アドレスと、リンクローカル IPv6 アドレスのネイバーはリンクローカル IPv6 送信元アドレスとペアになる必要があります）。表 1 に、BFDv6 でサポートされるアドレスのペアを示します。

表 1　　ネイバー作成のための BFDv6 アドレスのペア

送信元アドレス	宛先アドレス	ステータス
グローバル	グローバル	サポートあり
グローバル	リンク ローカル	サポートなし
リンク ローカル	グローバル	サポートなし
リンク ローカル	リンク ローカル	サポートあり

すべての IPv6 対応インターフェイスにはリンクローカル アドレスがあり、BFDv6 によって送信元アドレスが選択されるため、常にリンクローカル アドレス ネイバーがリンクローカル インターフェイス アドレスとペアになります。グローバル宛先アドレスとリンクローカル送信元アドレスの組み合わせは、シスコ エクスプレス フォワーディングではサポートされていません。そのため、グローバル アドレス ネイバーとのセッションを BFDv6 で確立するには、インターフェイス上でグローバル IPv6 アドレスを設定する必要があります。BFDv6 では、ネイバー アドレスがグローバルなのに、グローバル アドレスがインターフェイス上に設定されていないセッションは、すべて拒否されます。

（注） BFDv6 での Unique Local Address（ULA; 一意のローカル アドレス）の動作は、グローバル アドレスと同じです。

同じインターフェイス上での IPv4 用と IPv6 用の BFD

BFD では、インターフェイスごとに複数の IPv4 および IPv6 セッションがサポートされます。これらのセッションのプロトコルに制約はありません。

IPv6 での BFD に対するスタティック ルート サポート

スタティック ルート ネクスト ホップに到達するために BFDv6 プロトコルを使用すると、ネクスト ホップ ネイバーが到達可能なとき、IPv6 スタティック ルートは IPv6 Routing Information Base（RIB; ルーティング情報ベース）にだけ挿入されることが保証されます。また、BFDv6 プロトコルを使用すると、ネクスト ホップが到達不能になったとき、IPv6 スタティック ルートを IPv6 RIB から削除することもできます。

ユーザは、IPv6 スタティック BFDv6 ネイバーを設定できます。これらのネイバーは、associated（デフォルト）モードと unassociated モードのいずれかで動作できます。ネイバーは、自身が関連している BFDv6 セッションを中断させずに、これら 2 つのモードの間を遷移できます。

BFDv6 associated モード

BFDv6 associated モードでは、スタティック ルート ネクスト ホップがスタティック BFDv6 ネイバーと完全に一致すれば、IPv6 スタティック ルートが IPv6 スタティック BFDv6 ネイバーと自動的に関連付けられます。

IPv6 スタティック ルートは、1 つ以上の IPv6 スタティック ルートが関連付けられているスタティック BFDv6 ネイバーごとに BFDv6 セッションを要求し、BFD が設定されているインターフェイス上で設定されます。BFDv6 セッションの状態は、関連付けられた IPv6 スタティック ルートを IPv6 RIB に挿入するかどうかを決定するために使用されます。たとえば、スタティック ルートは、BFDv6 ネイバーが到達可能な場合にだけ、IPv6 RIB に挿入されます。またその後に、BFDv6 ネイバーが到達不能になると、そのスタティック ルートは IPv6 RIB から削除されます。

BFDv6 associated モードでは、BFD-monitored スタティック ルートを必要とするルータとネイバー ルータの両方で、BFD ネイバーとスタティック ルートをユーザが設定する必要があります。

BFDv6 unassociated モード

IPv6 スタティック BFD ネイバーは、unassociated として設定できます。このモードでは、ネイバーはスタティック ルートと関連付けられません。また、インターフェイスが BFDv6 用に設定されていると、ネイバーは常に BFDv6 セッションを要求します。

unassociated モードは、次の状況で役に立ちます。

- IPv6 スタティック ルートがない状態での BFDv6 セッションの構築：これは、スタティック ルートがルータ A 上にあり、ルータ B がネクスト ホップのときに起こります。associated モードでは、ルータ B からルータ A への BFDv6 セッションを構築するために、ユーザが両方のルータ上でスタティック BFD ネイバーとスタティック ルートの両方を作成する必要があります。ルータ B 上でスタティック BFD ネイバーを unassociated モードで指定すると、不要なスタティック ルートを設定する必要がなくなります。
- スタティック ルートの BFD モニタリングへの移行：これは、既存の IPv6 スタティック ルートが IPv6 RIB に挿入されているときに起こります。ユーザは、トラフィックを中断させずに、これらのスタティック ルートの BFD モニタリングを有効にする必要があります。接続されている IPv6 スタティック BFD ネイバーをユーザが設定すると、スタティック ルートは、新しいスタティック BFD ネイバーに即座に関連付けられます。しかし、スタティック BFD ネイバーはダウン状態で始まるため、関連付けられたスタティック ルートは IPv6 RIB から一旦削除され、BFDv6 セッションが確立されたときに再挿入されます。したがって、ユーザはトラフィックの中断を経験することになります。この中断は、スタティック BFD ネイバーを unassociated として設定し、BFDv6 セッションが確立するまで待機して、確立後にスタティック BFD ネイバーを associated として再設定することで回避できます。
- スタティック ルートの BFD モニタリングからの移行：この場合、IPv6 スタティック ルートは、BFD によってモニタされ、RIB に挿入されています。ユーザは、トラフィック フローを中断させずに、スタティック ルートの BFD モニタリングを無効にする必要があります。このシナリオは、最初にスタティック BFD ネイバーを非接続として再設定し（つまり、スタティック ルートからネイバーの関連付けを解除）、その後にスタティック BFD ネイバーの設定を解除することで実現できます。

OSPFv3 に対する BFD サポート

BFD では、ダイナミック ルーティング プロトコル OSPF for IPv6（OSPFv3）がサポートされています。OSPFv3 の設定方法については、「OSPFv3 に対する BFD サポートの設定」を参照してください。

Bidirectional Forwarding Detection for IPv6 の設定方法

BFDv6 は、IPv4 用の BFD とほぼ同じ方法で設定されます。BFDv6 の設定方法については、『*Cisco IOS IP Routing Protocols Configuration Guide*』の「Bidirectional Forwarding Detection」を参照してください。

ここでは、次の BFDv6 の作業について説明します。

スタティック BFDv6 ネイバーの指定

IPv6 スタティック BFDv6 ネイバーは、IPv6 スタティック ルートとは別に指定されます。IPv6 スタティック BFDv6 ネイバーは、インターフェイスとネイバー アドレスで完全に設定される必要があり、ローカル ルータに直接接続されている必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 route static bfd** [**vrf** *vrf-name*] *interface-type interface-number ipv6-address* [**unassociated**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 route static bfd** [**vrf** *vrf-name*] *interface-type interface-number ipv6-address* [**unassociated**] **例：** `Router(config)# ipv6 route static bfd ethernet 0/0 2001::1`	スタティック ルート IPv6 BFDv6 ネイバーを指定します。

BFDv6 ネイバーとの IPv6 スタティック ルートの関連付け

IPv6 スタティック ルートは、スタティック BFDv6 ネイバーと自動的に関連付けされます。スタティック ネイバーは、スタティック ネクストホップが BFDv6 ネイバーと明確に一致すると、その BFDv6 ネイバーと関連付けられます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 route static bfd** [**vrf** *vrf-name*] *interface-type interface-number ipv6-address* [**unassociated**]
4. **ipv6 route** [**vrf** *vrf-name*] *ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [**nexthop-vrf** [*vrf-name1* | **default**]] [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [*next-hop-address*] [**tag** *tag*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 route static bfd** [**vrf** *vrf-name*] *interface-type interface-number ipv6-address* [**unassociated**] **例：** `Router(config)# ipv6 route static bfd ethernet 0/0 2001::1`	スタティック ルート BFDv6 ネイバーを指定します。
ステップ 4	**ipv6 route** [**vrf** *vrf-name*] *ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [**nexthop-vrf** [*vrf-name1* | **default**]] [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [*next-hop-address*] [**tag** *tag*] **例：** `Router(config)# ipv6 route 2001:0DB8::/64 ethernet 0/0 2001::1`	スタティック IPv6 ルートを確立します。

OSPFv3 に対する BFD サポートの設定

ここでは、OSPFv3 が BFD の登録プロトコルとなり、BFD から転送パスの検出障害メッセージを受信するように、OSPFv3 に対する BFD サポートを設定する手順について説明します。すべてのインターフェイスでグローバルに OSPFv3 に対する BFD を設定するか、または 1 つ以上のインターフェイスで選択的に設定することができます。

OSPFv3 に対する BFD サポートをイネーブルにするには、2 つの方法があります。

- ルータ コンフィギュレーション モードで **bfd all-interfaces** コマンドを使用して、OSPFv3 がルーティングしているすべてのインターフェイスに対して BFD をイネーブルにできます。インターフェイス コンフィギュレーション モードで **ipv6 ospf bfd disable** コマンドを使用して、個々のインターフェイス上で BFD サポートをディセーブルにできます。

- インターフェイス コンフィギュレーション モードで **ipv6 ospf bfd** コマンドを使用して、OSPFv3 がルーティングしているインターフェイスのサブセットに対して BFD をイネーブルにできます。

OSPFv3 に対する BFD サポートの設定作業については、次の各項を参照してください。

- 「インターフェイスでの BFD セッション パラメータの設定」（P.7）
- 「すべてのインターフェイスの OSPFv3 に対する BFD サポートの設定」（P.7）
- 「1 つ以上のインターフェイスの OSPFv3 に対する BFD サポートの設定」（P.9）

インターフェイスでの BFD セッション パラメータの設定

この手順では、インターフェイスで基本 BFD セッション パラメータを設定することによって、インターフェイスで BFD を設定する方法を示します。BFD ネイバーに対して BFD セッションを実行するインターフェイスごとに、この手順を繰り返します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface ethernet 0/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier* **例：** `Router(config-if)# bfd interval 50 min_rx 50 multiplier 5`	インターフェイスで BFD をイネーブルにします。

すべてのインターフェイスの OSPFv3 に対する BFD サポートの設定

すべての OSPFv3 インターフェイスに BFD を設定するには、この項の手順に従います。

すべての OSPFv3 インターフェイスに対して BFD を設定するのではなく、特定の 1 つ以上のインターフェイスに対して BFD サポートを設定する場合は、「1 つ以上のインターフェイスの OSPFv3 に対する BFD サポートの設定」を参照してください。

前提条件

OSPFv3 は、関連するすべてのルータで実行する必要があります。BFD セッションを BFD ネイバーに対して実行するインターフェイスで、BFD セッションの基本パラメータを設定する必要があります。詳細については、「インターフェイスでの BFD セッション パラメータの設定」を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **bfd all-interfaces**
5. **exit**（このコマンドを 2 回入力します）
6. **show bfd neighbors** [**vrf** *vrf-name*] [**client** {**bgp** | **eigrp** | **isis** | **ospf** | **rsvp** | **te-frr**}] [*ip-address* | **ipv6** *ipv6-address*] [**details**]
7. **show ipv6 ospf** [*process-id*] [*area-id*] [**rate-limit**]
8. **show ipv6 ospf** [*process-id*] [*area-id*] **interface** [*type number*] [**brief**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 router ospf** *process-id* **例：** `Router(config)# ipv6 router ospf 2`	OSPFv3 ルーティング プロセスを設定します。
ステップ 4	**bfd all-interfaces** **例：** `Router(config-router)# bfd all-interfaces`	ルーティング プロセスに参加するすべてのインターフェイスに対して BFD をイネーブルにします。
ステップ 5	**exit** **例：** `Router(config-router)# exit`	このコマンドを 2 回入力して、特権 EXEC モードにします。

	コマンドまたはアクション	目的
ステップ 6	**show bfd neighbors** [**vrf** *vrf-name*] [**client** {**bgp** | **eigrp** | **isis** | **ospf** | **rsvp** | **te-frr**}] [*ip-address* | **ipv6** *ipv6-address*] [**details**] **例：** `Router# show bfd neighbors details`	（任意）既存の BFD 隣接関係の行単位のリストを表示します。
ステップ 7	**show ipv6 ospf** [*process-id*] [*area-id*] [**rate-limit**] **例：** `Router# show ipv6 ospf`	（任意）OSPFv3 ルーティング プロセスに関する一般情報を表示します。
ステップ 8	**show ipv6 ospf** [*process-id*] [*area-id*] **interface** [*type number*] [**brief**] **例：** `Router# show ipv6 ospf interface`	（任意）OSPF 関連のインターフェイス情報を表示します。

1 つ以上のインターフェイスの OSPFv3 に対する BFD サポートの設定

1 つ以上の OSPFv3 インターフェイスで BFD を設定するには、この項の手順に従います。

前提条件

OSPFv3 は、関連するすべてのルータで実行する必要があります。BFD セッションを BFD ネイバーに対して実行するインターフェイスで、BFD セッションの基本パラメータを設定する必要があります。詳細については、「インターフェイスでの BFD セッション パラメータの設定」を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 ospf bfd** [**disable**]
5. **exit**
6. **show bfd neighbors** [**vrf** *vrf-name*] [**client** {**bgp** | **eigrp** | **isis** | **ospf** | **rsvp** | **te-frr**}] [*ip-address* | **ipv6** *ipv6-address*] [**details**]
7. **show ipv6 ospf** [*process-id*] [*area-id*] [**rate-limit**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface ethernet 0/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 ospf bfd** [**disable**] **例：** `Router(config-if)# ipv6 ospf bfd`	OSPFv3 ルーティング プロセスに関連付けられた 1 つ以上のインターフェイスに対して、インターフェイスごとに BFD をイネーブルにします。
ステップ 5	**exit** **例：** `Router(config-router)# exit`	このコマンドを 2 回入力して、特権 EXEC モードにします。
ステップ 6	**show bfd neighbors** [**vrf** *vrf-name*] [**client** {**bgp** | **eigrp** | **isis** | **ospf** | **rsvp** | **te-frr**}] [*ip-address* | **ipv6** *ipv6-address*] [**details**] **例：** `Router# show bfd neighbors detail`	（任意）既存の BFD 隣接関係の行単位のリストを表示します。
ステップ 7	**show ipv6 ospf** [*process-id*] [*area-id*] [**rate-limit**] **例：** `Router# show ipv6 ospf`	（任意）OSPFv3 ルーティング プロセスに関する一般情報を表示します。

BFDv6 の監視とトラブルシューティング

手順の概要

1. **enable**
2. **monitor event ipv6 static** [**enable** | **disable**]
3. **show ipv6 static** [*ipv6-address* | *ipv6-prefix*/*prefix-length*] [**interface** *type number* | **recursive**] [**vrf** *vrf-name*] [**bfd**] [**detail**]
4. **debug bfd** {**event** | **packet** [*ip-address* | *ipv6-address*]}
5. **debug ipv6 static**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**monitor event ipv6 static** [**enable** | **disable**] **例：** `Router# monitor event ipv6 static enable`	イベント トレースの使用をイネーブルにして、IPv6 スタティック ネイバーと IPv6 スタティック BFDv6 ネイバーの動作をモニタします。
ステップ 3	**show ipv6 static** [*ipv6-address* | *ipv6-prefix*/*prefix-length*] [**interface** *type number* | **recursive**] [**vrf** *vrf-name*] [**bfd**] [**detail**] **例：** `Router# show ipv6 static vrf vrf1 bfd`	スタティック BFDv6 ネイバーおよび関連付けられたスタティック ルートを表示します。
ステップ 4	**debug bfd** {**event** | **packet** [*ip-address* | *ipv6-address*]} **例：** `Router# debug bfd`	BFD に関するデバッグ メッセージを表示します。
ステップ 5	**debug ipv6 static** **例：** `Router# debug ipv6 static`	BFDv6 デバッグをイネーブルにします。

Bidirectional Forwarding Detection for IPv6 の設定例

ここでは、次の BFD 設定例について説明します。

- 「例：IPv6 スタティック BFDv6 ネイバーの指定」（P.11）
- 「例：BFDv6 ネイバーとの IPv6 スタティック ルートの関連付け」（P.11）

例：IPv6 スタティック BFDv6 ネイバーの指定

次に、完全に設定された IPv6 スタティック BFDv6 ネイバーを指定する例を示します。インターフェイスはイーサネット 0/0、ネイバー アドレスは 2001::1 です。

```
Router(config)# ipv6 route static bfd ethernet 0/0 2001::1
```

例：BFDv6 ネイバーとの IPv6 スタティック ルートの関連付け

この例では、IPv6 スタティック ルート 2001:0DB8::/32 がイーサネット 0/0 インターフェイス上の BFDv6 ネイバー 2001::1 と関連付けられます。

```
Router(config)# ipv6 route static bfd ethernet 0/0 2001::1
Router(config)# ipv6 route 2001:0DB8::/32 ethernet 0/0 2001::1
```

例：BFD に関する OSPF インターフェイス情報の表示

次の表示例は、OSPF インターフェイスが BFD に対してイネーブルになっていることを示しています。

```
Router# show ipv6 ospf interface

Serial10/0 is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE00:6500, Interface ID 42
  Area 1, Process ID 1, Instance ID 0, Router ID 10.0.0.1
  Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT, BFD enabled
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.0.1
  Suppress hello for 0 neighbor(s)
```

その他の参考資料

関連資料

関連項目	参照先
OSPF for IPv6	『*Cisco IOS IPv6 Configuration Guide*』の「*Implementing OSPF for IPv6*」
IPv6 スタティック ルート	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing Static Routes for IPv6」
IPv6 のサポート機能リスト	『*Cisco IOS IPv6 Configuration Guide*』の「Start Here: Cisco IOS Software Release Specifics for IPv6 Features」
IPv6 コマンド：コマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS IPv6 Command Reference*』
IPv4 用 BFD	『*Cisco IOS IP Routing Protocols Configuration Guide*』の「Bidirectional Forwarding Detection」
IPv4 用 BFD のコマンド	『*Cisco IOS IP Routing Protocols Command Reference*』の「IP Routing Protocol-Independent Commands」

規格

規格	タイトル
この機能によってサポートされる新しい規格または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
•	選択したプラットフォーム、Cisco ソフトウェア リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
draft-ietf-bfd-v4v6-1hop-07.txt	『*BFD for IPv4 and IPv6 (Single Hop)*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

Bidirectional Forwarding Detection for IPv6 の実装の機能情報

表 2 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どのソフトウェア イメージが特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 2 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 2　Bidirectional Forwarding Detection for IPv6 の実装の機能情報

機能名	リリース	機能情報
BFD 用の OSPFv3	12.2(33)SRE 15.0(1)S 15.1(2)T	BFD では、ダイナミック ルーティング プロトコル OSPF for IPv6（OSPFv3）がサポートされています。 この機能に関する詳細については、次の項を参照してください。 • 「OSPFv3 に対する BFD サポート」（P.4） • 「OSPFv3 に対する BFD サポートの設定」（P.6） • 「BFDv6 の監視とトラブルシューティング」（P.10） **bfd**、**bfd all-interfaces**、**debug bfd**、**ipv6 router ospf**、**show bfd neighbors**、**show ipv6 ospf**、**show ipv6 ospf interface** の各コマンドが導入または修正されました。

表 2　Bidirectional Forwarding Detection for IPv6 の実装の機能情報 （続き）

機能名	リリース	機能情報
BFD IPv6 カプセル化サポート	12.2(33)SRE 15.1(2)T	BFDv6 カプセル化は、セッション情報構造内に記述されます。これらのセッション情報構造は、サポートされているプロトコルに対して BFDv6 によって定義されます。BFDv6 は、セッション情報構造の情報を使用して、そのセッション上の BFDv6 パケットに対する正しいカプセル化を決定します。 この機能に関する詳細については、次の項を参照してください。 • 「BFDv6 登録」（P.2）
IPv6 での BFD に対するスタティック ルート サポート	15.1(2)T	スタティック ルート ネクスト ホップに到達するために BFDv6 プロトコルを使用すると、ネクストホップ ネイバーが到達可能なとき、IPv6 スタティック ルートは IPv6 Routing Information Base（RIB; ルーティング情報ベース）にだけ挿入されることが保証されます。また、BFDv6 プロトコルを使用すると、ネクスト ホップが到達不能になったとき、IPv6 スタティック ルートを IPv6 RIB から削除することもできます。 この機能に関する詳細については、次の項を参照してください。 • 「IPv6 での BFD に対するスタティック ルート サポート」（P.3） • 「スタティック BFDv6 ネイバーの指定」（P.5） • 「BFDv6 ネイバーとの IPv6 スタティック ルートの関連付け」（P.5） • 「BFDv6 の監視とトラブルシューティング」（P.10） • 「例：IPv6 スタティック BFDv6 ネイバーの指定」（P.11） • 「例：BFDv6 ネイバーとの IPv6 スタティック ルートの関連付け」（P.11） **debug bfd**、**debug ipv6 static**、**ipv6 route**、**ipv6 route static bfd**、**monitor event ipv6 static**、**show ipv6 static** の各コマンドが導入または修正されました。

マルチプロトコル BGP for IPv6 の実装

この章では、マルチプロトコル Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）for IPv6 を設定する方法について説明します。BGP は、独立したルーティング ポリシーを持つ個別のルーティング ドメイン（自律システム）を接続する場合に主に使用される Exterior Gateway Protocol（EGP; 外部ゲートウェイ プロトコル）です。BGP の一般的な用途は、サービス プロバイダーに接続してインターネットにアクセスすることです。BGP は、自律システム内で使用することもできます。このタイプの BGP は、internal BGP（iBGP; 内部 BGP）と呼ばれます。マルチプロトコル BGP は、複数のネットワーク レイヤ プロトコル アドレス ファミリ（IPv6 アドレス ファミリなど）、および IP マルチキャスト ルートに関するルーティング情報を伝送する拡張 BGP です。すべての BGP コマンドおよびルーティング ポリシー機能をマルチプロトコル BGP で使用できます。

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「マルチプロトコル BGP for IPv6 の実装の機能情報」（P.34）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

マルチプロトコル BGP for IPv6 の実装の前提条件

- この章では、IPv6 アドレッシングおよび基本設定に精通していることを前提としています。詳細については、「*IPv6 アドレッシングと基本接続の実装*」の章を参照してください。
- この章では、IPv4 に精通していることを前提としています。IPv4 の設定およびコマンド リファレンス情報については、「関連資料」の関連資料を参照してください。
- VPN for IPv6（VPNv6）は、IPv6 VPN over MPLS（6VPE）を介してサポートされています。

マルチプロトコル BGP for IPv6 の実装に関する情報

マルチプロトコル BGP for IPv6 拡張

マルチプロトコル BGP は、IPv6 用にサポートされている EGP です。マルチプロトコル BGP for IPv6 拡張では、IPv4 BGP と同じ機能および機能性がサポートされています。マルチプロトコル BGP に対する IPv6 拡張には、IPv6 アドレス ファミリ、Network Layer Reachability Information（NLRI; ネットワーク レイヤ到達可能性情報）、および IPv6 アドレスを使用するネクストホップ（宛先へのパス内の次のルータ）アトリビュートのサポートが含まれています。

IPv6 マルチキャスト アドレス ファミリのマルチプロトコル BGP

IPv6 マルチキャスト アドレス ファミリのマルチプロトコル BGP 機能では、マルチプロトコル BGP for IPv6 拡張を提供し、IPv4 BGP と同じ機能と機能性をサポートします。マルチキャスト BGP に対する IPv6 拡張には、IPv6 マルチキャスト アドレス ファミリ、Network Layer Reachability Information（NLRI; ネットワーク レイヤ到達可能性情報）、および IPv6 アドレスを使用するネクストホップ（宛先へのパス内の次のルータ）アトリビュートのサポートが含まれています。

マルチキャスト BGP は、ドメイン間 IPv6 マルチキャストの配布を可能にする、拡張された BGP です。マルチプロトコル BGP では、複数のネットワーク レイヤ プロトコル アドレス ファミリ（IPv6 アドレス ファミリなど）および IPv6 マルチキャスト ルートに関するルーティング情報を伝送します。IPv6 マルチキャスト アドレス ファミリには、IPv6 PIM プロトコルによる RPF ルックアップに使用される複数のルートが含まれており、マルチキャスト BGP IPV6 は、同じドメイン間転送を提供します。ユニキャスト BGP が学習したルートは IPv6 マルチキャストには使用されないため、ユーザは、BGP で IPv6 マルチキャストを使用する場合は、マルチプロトコル BGP for IPv6 マルチキャストを使用する必要があります。

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

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

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

MP-BGP IPv6 アドレス ファミリのノンストップ フォワーディングおよびグレースフル リスタート

グレースフル リスタート機能は、IPv6 BGP ユニキャスト、IPv6 BGP マルチキャスト、および VPNv6 アドレス ファミリでサポートされており、BGP IPv6 用の Cisco NonStop Forwarding（NSF; ノンストップ フォワーディング）機能をイネーブルにします。BGP グレースフル リスタート機能を使用すると、TCP 状態を維持することなく、BGP ルーティング テーブルをピアから回復できます。

NSF では、ルーティング プロトコルのコンバージェンス時にも引き続きパケットが転送されるため、スイッチオーバー時のルート フラップが回避されます。転送は、アクティブ RP とスタンバイ RP 間で FIB を同期することで維持されます。スイッチオーバー時、転送は FIB を使用して維持されます。RIB の同期は維持されないため、RIB はスイッチオーバー時に空になります。RIB は、ルーティング プロトコルによって再入力され、次に、NSF_RIB_CONVERGED レジストリ コールを使用して RIB コンバージェンスに関する情報を FIB に伝えます FIB テーブルは、RIB から更新され、古いエントリが削除されます。RIB は、ルーティング プロトコルが RIB のコンバージェンスの通知に失敗した場合、RP スイッチオーバー時にフェールセーフ タイマーを開始します。

Cisco BGP Address Family Identifier（AFI）モデルは、モジュラ式でスケーラブルな設計となっており、複数の AFI 設定および Subsequent Address Family Identifier（SAFI）設定をサポートするように設計されています。

6PE マルチパス

IPv6 の内部および外部 BGP マルチパスによって、IPv6 ルータは、宛先に到達するために複数のパス（同じネイバー自律システムやサブ自律システム、または同じメトリックなど）間のロード バランシングを行うことができます。6PE マルチパス機能では、Multiprotocol internal BGP（MP-iBGP; マルチプロトコル内部 BGP）を使用して、MPLS IPv4 コア ネットワークを介して IPv6 ルートを配布し、MPLS ラベルを各ルートに付加します。

MP-iBGP マルチパスが 6PE ルータでイネーブルになっていると、MPLS 情報が使用できる場合は、MPLS 情報（ラベル スタック）を使用して、ラベルの付いたすべてのパスが、転送テーブルにインストールされます。この機能によって、6PE はロード バランシングを実行できます。

マルチプロトコル BGP for IPv6 の実装方法

マルチプロトコル BGP for IPv6 拡張を設定する場合は、BGP ルーティング プロセスを作成し、ピアリング関係を設定し、特定のネットワーク用に BGP をカスタマイズする必要があります。

（注） 次の各項では、IPv6 マルチプロトコル BGP ルーティング プロセスの作成、そのルーティング プロセスへのピア、ピア グループ、およびネットワークの関連付けに関する設定作業について説明します。次の各項では、マルチプロトコル BGP のカスタマイズについては詳しく説明していません。IPv6 でのプロトコルの機能は、IPv4 の場合と同じであるためです。BGP とマルチプロトコル BGP の設定およびコマンド リファレンス情報の詳細については、「関連資料」の項を参照してください。

次の各項の作業では、マルチプロトコル BGP for IPv6 拡張の設定方法について説明します。一覧内の各作業は、必須と任意に分けています。

IPv6 BGP ルーティング プロセスおよび BGP ルータ ID の設定

IPv6 BGP ルーティング プロセスを設定し、オプションの BGP スピーキング ルータ用 BGP ルータ ID を設定するには、次の作業を実行します。

前提条件

BGP for IPv6 を実行するようにルータを設定する前に、**ipv6 unicast-routing** コマンドを使用して、IPv6 ルーティングをグローバルにイネーブルにする必要があります。基本的な IPv6 の接続作業の詳細については、「*Implementing Basic Connectivity for IPv6*」の章を参照してください。

IPv6 の BGP ルータ ID

BGP では、ルータ ID を使用して、BGP スピーキング ピアを識別します。BGP ルータ ID は、32 ビット値であり、多くの場合、IPv4 アドレスで表されます。デフォルトでは、Cisco IOS ソフトウェアによって、ルータ ID がルータ上のループバック インターフェイスの IPv4 アドレスに設定されます。ルータ上でループバック インターフェイスが設定されていない場合は、BGP ルータ ID を表すためにルータ上の物理インターフェイスに設定されている最上位の IPv4 アドレスがソフトウェアによって選択されます。IPv6 だけがイネーブルになっているルータ（IPv4 アドレスを持っていないルータ）で BGP を設定する場合、そのルータの BGP ルータ ID を手動で設定する必要があります。IPv4 アドレス構文を使用して 32 ビット値で表される BGP ルータ ID は、ルータの BGP ピアで一意である必要があります。

手順の概要

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

3. **router bgp** *as-number*
4. **no bgp default ipv4-unicast**
5. **bgp router-id** *ip-address*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* **例：** `Router(config)# router bgp 65000`	BGP ルーティング プロセスを設定し、指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**no bgp default ipv4-unicast** **例：** `Router(config-router)# no bgp default ipv4-unicast`	前の手順で指定した BGP ルーティング プロセスの IPv4 ユニキャスト アドレス ファミリをディセーブルにします。 **（注）** IPv4 ユニキャスト アドレス ファミリのルーティング情報が、**neighbor remote-as** コマンドを使用して設定した各 BGP ルーティング セッションにデフォルトでアドバタイズされます。ただし、**neighbor remote-as** コマンドを設定する前に **no bgp default ipv4-unicast** コマンドを設定している場合は除きます。
ステップ 5	**bgp router-id** *ip-address* **例：** `Router(config-router)# bgp router-id 192.168.99.70`	（任意）固定 32 ビット ルータ ID を、BGP を実行するローカル ルータの ID として設定します。 **（注）** **bgp router-id** コマンドを使用してルータ ID を設定すると、アクティブな BGP ピアリング セッションがすべてリセットされます。

IPv6 マルチプロトコル BGP ピアの設定

制約事項

デフォルトでは、ルータ コンフィギュレーション モードで **neighbor remote-as** コマンドを使用して定義したネイバーは、IPv4 ユニキャスト アドレス プレフィクスだけを交換します。IPv6 プレフィクスなどの他のアドレス プレフィクス タイプを交換するには、その他のプレフィクス タイプ（IPv6 プレフィクスなど）のアドレス ファミリ コンフィギュレーション モードで **neighbor activate** コマンドを使用して、ネイバーをアクティブ化する必要もあります。

手順の概要

1. **enable**

2. **configure terminal**
3. **router bgp** *as-number*
4. **neighbor** {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number ...*]
5. **address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast** | **vpnv6**]
6. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address***%**} **activate**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* **例：** `Router(config)# router bgp 65000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number ...*] **例：** `Router(config-router)# neighbor 2001:0DB8:0:CC00::1 remote-as 64600`	指定した自律システム内のネイバーの IPv6 アドレスを、ローカル ルータの IPv6 マルチプロトコル BGP ネイバー テーブルに追加します。
ステップ 5	**address-family ipv6** [**unicast** | **multicast**] **例：** `Router(config-router)# address-family ipv6`	IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードでは、IPv6 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv6** コマンドで **unicast** キーワードが指定されていない場合、ルータは IPv6 ユニキャスト アドレス ファミリのコンフィギュレーション モードになります。 • **multicast** キーワードでは、IPv6 マルチキャスト アドレス プレフィクスを指定します。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address***%**} **activate** **例：** `Router(config-router-af)# neighbor 2001:0DB8:0:CC00::1 activate`	ローカル ルータとの間で IPv6 アドレス ファミリを交換できるようにネイバーを設定します。

リンクローカル アドレスを使用した IPv6 マルチプロトコル BGP ピアの設定

リンクローカル アドレスを使用したマルチプロトコル BGP ピアリング

リンクローカル アドレスを使用して 2 台の IPv6 ルータ（ピア）間に IPv6 マルチプロトコル BGP を設定する場合は、ネイバーのインターフェイスが **update-source** コマンドを使用して識別され、IPv6 グローバル ネクストホップを設定するようにルート マップが設定されている必要があります。

制約事項

- デフォルトでは、ルータ コンフィギュレーション モードで **neighbor remote-as** コマンドを使用して定義したネイバーは、IPv4 ユニキャスト アドレス プレフィクスだけを交換します。IPv6 プレフィクスなどの他のアドレス プレフィクス タイプを交換するには、その他のプレフィクス タイプ（IPv6 プレフィクスなど）のアドレス ファミリ コンフィギュレーション モードで **neighbor activate** コマンドを使用して、ネイバーをアクティブ化する必要もあります。
- デフォルトでは、**neighbor route-map** コマンドを使用してルータ コンフィギュレーション モードで適用されるルート マップは、IPv4 ユニキャスト アドレス プレフィクスだけに適用されます。IPv6 アドレス ファミリなどのその他のアドレス ファミリのルート マップは、**neighbor route-map** コマンドを使用してアドレス ファミリ コンフィギュレーション モードで適用される必要があります。ルート マップは、指定したアドレス ファミリの下にあるネイバーの着信ルーティング ポリシーまたは発信ルーティング ポリシーとして適用されます。各アドレス ファミリ タイプで個別のルート マップを設定すると、各アドレス ファミリの複雑なポリシーまたはさまざまなポリシーを簡単に管理できるようになります。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number ...*]
5. **neighbor** {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **update-source** *interface-type interface-number*
6. **address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast** | **vpnv6**]
7. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address***%**} **activate**
8. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address* [**%**]} **route-map** *map-name* {**in** | **out**}
9. **exit**
10. ステップ 9 を繰り返します。
11. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
12. **match ipv6 address** {**prefix-list** *prefix-list-name* | *access-list-name*}
13. **set ipv6 next-hop** *ipv6-address* [*link-local-address*] [**peer-address**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 65000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number* ...] **例：** `Router(config-router)# neighbor FE80::XXXX:BFF:FE0E:A471% remote-as 64600`	指定したリモート自律システム内のネイバーのリンクローカル IPv6 アドレスをローカル ルータの IPv6 マルチプロトコル BGP ネイバーテーブルに追加します。 • 省略可能な **%** キーワードは、IPv6 リンクローカル アドレス ID です。このキーワードは、リンクローカル IPv6 アドレスがそのインターフェイスのコンテキスト外で使用される場合は、追加する必要があります。
ステップ 5	**neighbor** {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **update-source** *interface-type interface-number* **例：** `Router(config-router)# neighbor FE80::XXXX:BFF:FE0E:A471% update-source fastethernet0`	ピアリングが発生するリンクローカル アドレスを指定します。 • 省略可能な **%** キーワードは、IPv6 リンクローカル アドレス ID です。このキーワードは、リンクローカル IPv6 アドレスがそのインターフェイスのコンテキスト外で使用される場合は、追加する必要があります。 • ネイバーへの接続が複数存在し、**neighbor update-source** コマンドで *interface-type* 引数と *interface-number* 引数を使用してネイバー インターフェイスを指定していない場合は、リンクローカル アドレスを使用してネイバーとの TCP 接続を確立することはできません。
ステップ 6	**address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast** | **vpnv6**] **例：** `Router(config-router)# address-family ipv6`	IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードでは、IPv6 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv6** コマンドで **unicast** キーワードが指定されていない場合、ルータは IPv6 ユニキャスト アドレス ファミリのコンフィギュレーション モードになります。 • **multicast** キーワードでは、IPv6 マルチキャスト アドレス プレフィクスを指定します。

	コマンドまたはアクション	目的
ステップ 7	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address***%**} **activate** **例：** `Router(config-router-af)# neighbor FE80::XXXX:BFF:FE0E:A471% activate`	ネイバーが、指定したリンクローカル アドレスを使用して IPv6 アドレス ファミリのプレフィクスをローカル ルータと交換できるようにします。 • 省略可能な **%** キーワードは、IPv6 リンクローカル アドレス ID です。このキーワードは、リンクローカル IPv6 アドレスがそのインターフェイスのコンテキスト外で使用される場合は、追加する必要があります。
ステップ 8	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*[**%**]} **route-map** *map-name* {**in** | **out**} **例：** `Router(config-router-af)# neighbor FE80::XXXX:BFF:FE0E:A471% route-map nh6 out`	着信ルートまたは発信ルートにルート マップを適用します。 • 省略可能な **%** キーワードは、IPv6 リンクローカル アドレス ID です。このキーワードは、リンクローカル IPv6 アドレスがそのインターフェイスのコンテキスト外で使用される場合は、追加する必要があります。
ステップ 9	**exit** **例：** `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了し、ルータをルータ コンフィギュレーション モードに戻します。
ステップ 10	ステップ 9 を繰り返します。 **例：** `Router(config-router)# exit`	ルータ コンフィギュレーション モードを終了し、ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 11	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] **例：** `Router(config)# route-map nh6 permit 10`	ルート マップを定義し、ルート マップ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 12	**match ipv6 address** {**prefix-list** *prefix-list-name* | *access-list-name*} **例：** `Router(config-route-map)# match ipv6 address prefix-list cisco`	プレフィクス リストで許可されている宛先 IPv6 ネットワーク番号アドレスを持つすべてのルートを配布するか、パケットに対してポリシー ルーティングを実行します。
ステップ 13	**set ipv6 next-hop** *ipv6-address* [*link-local-address*] [**peer-address**] **例：** `Router(config-route-map)# set ipv6 next-hop 2001:0DB8::1`	ポリシー ルーティング用のルート マップの match 句を渡す IPv6 パケットのピアにアドバタイズされるネクストホップを上書きします。 • *ipv6-address* 引数では、ネクストホップの IPv6 グローバル アドレスを指定します。隣接ルータである必要はありません。 • *link-local-address* 引数では、ネクストホップの IPv6 リンクローカル アドレスを指定します。隣接ルータである必要があります。 **（注）** ルート マップによって、BGP アップデートに IPv6 ネクストホップ アドレス（グローバルおよびリンクローカル）が設定されます。ルート マップが設定されていない場合、BGP アップデートのネクストホップ アドレスは、未指定 IPv6 アドレス（::）にデフォルト設定され、ピアによって拒否されます。 ステップ 5 において **neighbor update-source** コマンドでネイバー インターフェイス（*interface-type* 引数）を指定したあとに、**set ipv6 next-hop** コマンドでグローバル IPv6 ネクストホップ アドレス（*ipv6-address* 引数）だけを指定している場合は、*interface-type* 引数で指定したインターフェイスのリンクローカル アドレスが、BGP アップデートのネクストホップとして含まれています。したがって、リンクローカル アドレスを使用する複数の BGP ピアに必要となるのは、BGP アップデートにグローバル IPv6 ネクストホップ アドレスを設定する 1 つのルート マップだけとなります。

トラブルシューティングのヒント

この作業でピアリングが確立されなかった場合、ルート マップの **set ipv6 next-hop** コマンドの欠落が原因である可能性があります。**debug bgp ipv6 update** コマンドを使用して、アップデートに関するデバッグ情報を表示し、ピアリングの状態の識別に役立てます。

IPv6 マルチプロトコル BGP ピア グループの設定

制約事項

- デフォルトでは、ルータ コンフィギュレーション モードで **neighbor remote-as** コマンドを使用して定義したネイバーは、IPv4 ユニキャスト アドレス プレフィクスだけを交換します。IPv6 プレフィクスなどの他のアドレス プレフィクス タイプを交換するには、その他のプレフィクス タイプ（IPv6 プレフィクスなど）のアドレス ファミリ コンフィギュレーション モードで **neighbor activate** コマンドを使用して、ネイバーをアクティブ化する必要もあります。
- デフォルトでは、**neighbor peer-group** コマンドを使用してルータ コンフィギュレーション モードで定義されたピア グループは、IPv4 ユニキャスト アドレス プレフィクスだけを交換します。IPv6 プレフィクスなどの他のプレフィクス タイプを交換するには、その他のプレフィクス タイプ（IPv6 プレフィクスなど）のアドレス ファミリ コンフィギュレーション モードで **neighbor activate** コマンドを使用して、ピア グループをアクティブ化する必要があります。
- ピア グループのメンバは、そのピア グループのアドレス プレフィクス設定を自動的に継承します。
- アクティブな IPv4 ネイバーは、アクティブな IPv6 ネイバーと同じピア グループに存在することはできません。IPv4 ピアと IPv6 ピア用に個別のピア グループを作成します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **neighbor** *peer-group-name* **peer-group**
5. **neighbor** {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number ...*]
6. **address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast** | **vpnv6**]
7. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address***%**} **activate**
8. **neighbor** {*ip-address* | *ipv6-address*} **send-label**
9. **neighbor** {*ip-address* | *ipv6-address*} **peer-group** *peer-group-name*
10. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* **例：** `Router(config)# router bgp 65000`	指定した BGP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** *peer-group-name* **peer-group** **例：** `Router(config-router)# neighbor group1 peer-group`	マルチプロトコル BGP ピア グループを作成します。
ステップ 5	**neighbor** {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number* ...] **例：** `Router(config-router)# neighbor 2001:0DB8:0:CC00::1 remote-as 64600`	指定した自律システム内のネイバーの IPv6 アドレスを、ローカル ルータの IPv6 マルチプロトコル BGP ネイバー テーブルに追加します。 • **neighbor remote-as** コマンドの *ipv6-address* 引数は、RFC 2373 に記載された形式にする必要があり、16 ビット値をコロンで区切った 16 進でアドレスを指定します。
ステップ 6	**address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast** | **vpnv6**] **例：** `Router(config-router)# address-family ipv6 unicast`	IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードでは、IPv6 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv6** コマンドで **unicast** キーワードが指定されていない場合、ルータは IPv6 ユニキャスト アドレス ファミリのコンフィギュレーション モードになります。 • **multicast** キーワードでは、IPv6 マルチキャスト アドレス プレフィクスを指定します。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address***%**} **activate** **例：** `Router(config-router-af)# neighbor 2001:0DB8:0:CC00::1 activate`	ネイバーが、指定したファミリ タイプのプレフィクスをネイバーおよびローカル ルータと交換できるようにします。 • 各ネイバーでの追加の設定手順を回避するために、この手順の代替として、*peer-group-name* 引数を指定して **neighbor activate** コマンドを使用します。
ステップ 8	**neighbor** {*ip-address* | *ipv6-address*} **send-label** **例：** `Router(config-router-af)# neighbor 192.168.99.70 send-label`	BGP ルートとともに MPLS ラベルを送信するルータの機能をアドバタイズします。 • IPv6 アドレス ファミリ コンフィギュレーション モードでは、このコマンドによって、BGP の IPv6 プレフィクスのアドバタイズ時に集約ラベルをバインドおよびアドバタイズできるようになります。

	コマンドまたはアクション	目的
ステップ 9	**neighbor** {*ip-address* | *ipv6-address*} **peer-group** *peer-group-name* **例：** `Router(config-router-af)# neighbor 2001:0DB8:0:CC00::1 peer-group group1`	BGP ネイバーの IPv6 アドレスをピア グループに割り当てます。
ステップ 10	**exit** **例：** `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了し、ルータをルータ コンフィギュレーション モードに戻します。 • このステップを繰り返して、ルータ コンフィギュレーション モードを終了し、ルータをグローバル コンフィギュレーション モードに戻します。

IPv6 マルチプロトコル BGP へのルートのアドバタイズ

制約事項

デフォルトでは、**network** コマンドを使用してルータ コンフィギュレーション モードで定義されたネットワークは、IPv4 ユニキャスト データベースに挿入されます。ネットワークを IPv6 BGP データベースなどの他のデータベースに挿入するには、他のデータベース（IPv6 BGP データベースなど）のアドレス ファミリ コンフィギュレーション モードで **network** コマンドを使用して、ネットワークを定義する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast** | **vpnv6**]
5. **network** {*network-number* [**mask** *network-mask*] | *nsap-prefix*} [**route-map** *map-tag*]
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**router bgp** *as-number* **例：** `Router(config)# router bgp 65000`	指定した BGP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast** | **vpnv6**] **例：** `Router(config-router)# address-family ipv6 unicast`	IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードでは、IPv6 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv6** コマンドで **unicast** キーワードが指定されていない場合、ルータは IPv6 ユニキャスト アドレス ファミリのコンフィギュレーション モードになります。 • **multicast** キーワードでは、IPv6 マルチキャスト アドレス プレフィクスを指定します。
ステップ 5	**network** {*network-number* [**mask** *network-mask*] | *nsap-prefix*} [**route-map** *map-tag*] **例：** `Router(config-router-af)# network 2001:0DB8::/24`	指定したプレフィクスを IPv6 BGP データベースにアドバタイズ（挿入）します（ルートは、まず IPv6 ユニキャスト ルーティング テーブルで検索される必要があります）。 • 具体的には、前の手順で指定したアドレス ファミリのデータベースにプレフィクスが挿入されます。 • ルートには指定したプレフィクスによって「local origin」のタグが付けられます。 • **network** コマンドの *ipv6-prefix* 引数は、RFC 2373 に記載された形式にする必要があり、16 ビット値をコロンで区切った 16 進でアドレスを指定します。 • *prefix-length* 引数は、アドレスのうち連続する上位何ビットがプレフィクス（アドレスのネットワーク部）を構成するかを示す 10 進数値です。10 進数値の前にスラッシュ記号が必要です。
ステップ 6	**exit** **例：** `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了し、ルータをルータ コンフィギュレーション モードに戻します。 • この手順を繰り返して、ルータ コンフィギュレーション モードを終了し、ルータをグローバル コンフィギュレーション モードに戻します。

IPv6 マルチプロトコル BGP プレフィクスのルート マップの設定

制約事項

- デフォルトでは、ルータ コンフィギュレーション モードで **neighbor remote-as** コマンドを使用して定義したネイバーは、IPv4 ユニキャスト アドレス プレフィクスだけを交換します。IPv6 プレフィクスなどの他のアドレス プレフィクス タイプを交換するには、その他のプレフィクス タイプ（IPv6 プレフィクスなど）のアドレス ファミリ コンフィギュレーション モードで **neighbor activate** コマンドを使用して、ネイバーをアクティブ化する必要もあります。
- デフォルトでは、**neighbor route-map** コマンドを使用してルータ コンフィギュレーション モードで適用されるルート マップは、IPv4 ユニキャスト アドレス プレフィクスだけに適用されます。IPv6 アドレス ファミリなどのその他のアドレス ファミリのルート マップは、**neighbor route-map** コマンドを使用してアドレス ファミリ コンフィギュレーション モードで適用される必要があります。ルート マップは、指定したアドレス ファミリの下にあるネイバーの着信ルーティング ポリシーまたは発信ルーティング ポリシーとして適用されます。各アドレス ファミリ タイプで個別のルート マップを設定すると、各アドレス ファミリの複雑なポリシーまたはさまざまなポリシーを簡単に管理できるようになります。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **neighbor** {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number ...*]
5. **address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast** | **vpnv6**]
6. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address***%**} **activate**
7. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address* [**%**]} **route-map** *map-name* {**in** | **out**}
8. **exit**
9. ステップ 8 を繰り返します。
10. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
11. **match ipv6 address** {**prefix-list** *prefix-list-name* | *access-list-name*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**router bgp** *as-number* **例：** `Router(config)# router bgp 65000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number* ...] **例：** `Router(config-router)# neighbor 2001:0DB8:0:cc00::1 remote-as 64600`	指定したリモート自律システム内のネイバーのリンクローカル IPv6 アドレスをローカル ルータの IPv6 マルチプロトコル BGP ネイバーテーブルに追加します。
ステップ 5	**address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast** | **vpnv6**] **例：** `Router(config-router)# address-family ipv6`	IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードでは、IPv6 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv6** コマンドで **unicast** キーワードが指定されていない場合、ルータは IPv6 ユニキャスト アドレス ファミリのコンフィギュレーション モードになります。 • **multicast** キーワードでは、IPv6 マルチキャスト アドレス プレフィクスを指定します。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address***%**} **activate** **例：** `Router(config-router-af)# neighbor 2001:0DB8:0:cc00::1 activate`	ネイバーが、指定したリンクローカル アドレスを使用して IPv6 アドレス ファミリのプレフィクスをローカル ルータと交換できるようにします。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address* [**%**]} **route-map** *map-name* {**in** | **out**} **例：** `Router(config-router-af)# neighbor 2001:0DB8:0:cc00::1 route-map rtp in`	着信ルートまたは発信ルートにルート マップを適用します。 • ルート マップへの変更は、ピアリングがリセットされるまで、またはソフト リセットが実行されるまで、現在のピアでは有効になりません。**soft** キーワードと **in** キーワードを指定して **clear bgp ipv6** コマンドを使用すると、ソフト リセットが実行されます。
ステップ 8	**exit** **例：** `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了し、ルータをルータ コンフィギュレーション モードに戻します。
ステップ 9	ステップ 8 を繰り返します。 **例：** `Router(config-router)# exit`	ルータ コンフィギュレーション モードを終了し、ルータをグローバル コンフィギュレーション モードに戻します。

	コマンドまたはアクション	目的
ステップ 10	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] **例：** `Router(config)# route-map rtp permit 10`	ルート マップを定義し、ルート マップ コンフィギュレーション モードを開始します。 • **match** コマンドを使用して、この手順を実行します。
ステップ 11	**match ipv6 address** {**prefix-list** *prefix-list-name* | *access-list-name*} **例：** `Router(config-route-map)# match ipv6 address prefix-list cisco`	プレフィクス リストで許可されている宛先 IPv6 ネットワーク番号アドレスを持つすべてのルートを配布するか、パケットに対してポリシー ルーティングを実行します。

IPv6 マルチプロトコル BGP へのプレフィクスの再配布

IPv6 用の再配布

再配布は、あるルーティング プロトコルから別のルーティング プロトコルにプレフィクスを再配布（挿入）するプロセスです。ここでは、あるルーティング プロトコルのプレフィクスを IPv6 マルチプロトコル BGP に挿入する方法について説明します。具体的には、**redistribute** ルータ コンフィギュレーション コマンドを使用して IPv6 マルチプロトコル BGP に再配布されたプレフィクスが、IPv6 ユニキャスト データベースに挿入されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast** | **vpnv6**]
5. **redistribute bgp** [*process-id*] [**metric** *metric-value*] [**route-map** *map-name*] [*source-protocol-options*]
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* **例：** `Router(config)# router bgp 65000`	指定した BGP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast** | **vpnv6**] **例：** `Router(config-router)# address-family ipv6`	IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードでは、IPv6 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv6** コマンドで **unicast** キーワードが指定されていない場合、ルータは IPv6 ユニキャスト アドレス ファミリのコンフィギュレーション モードになります。 • **multicast** キーワードでは、IPv6 マルチキャスト アドレス プレフィクスを指定します。
ステップ 5	**redistribute bgp** [*process-id*] [**metric** *metric-value*] [**route-map** *map-name*] [*source-protocol-options*] **例：** `Router(config-router-af)# redistribute bgp 64500 metric 5 metric-type external`	あるルーティング ドメインから別のルーティング ドメインへ IPv6 ルートを再配布します。
ステップ 6	**exit** **例：** `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了し、ルータをルータ コンフィギュレーション モードに戻します。 • このステップを繰り返して、ルータ コンフィギュレーション モードを終了し、ルータをグローバル コンフィギュレーション モードに戻します。

IPv6 BGP ピア間での IPv4 ルートのアドバタイズ

IPv6 ピア間で IPv4 ルートをアドバタイズするには、次の作業を実行します。IPv6 ネットワークが 2 つの個別の IPv4 ネットワークに接続されている場合、IPv6 を使用して IPv4 ルートをアドバタイズできます。IPv4 アドレス ファミリ内で IPv6 アドレスを使用してピアリングを設定します。アドバタイズされるネクストホップは、通常、到着不能であるため、スタティック ルートまたはインバウンド ルート マップを使用してネクストホップを設定します。2 つの IPv4 ピア間での IPv6 ルートのアドバタイズでは、同じモデルを使用することもできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **neighbor** *peer-group-name* **peer-group**
5. **neighbor** {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number ...*]
6. **address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*]
7. **neighbor** *ipv6-address* **peer-group** *peer-group-name*
8. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address* [**%**]} **route-map** *map-name* {**in** | **out**}
9. **exit**

10. ステップ 11 を繰り返します。
11. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
12. **set ip next-hop** *ip-address* [*... ip-address*] [**peer-address**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* **例：** `Router(config)# router bgp 65000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**neighbor** *peer-group-name* **peer-group** **例：** `Router(config-router)# neighbor 6peers peer-group`	マルチプロトコル BGP ピア グループを作成します。
ステップ 5	**neighbor** {*ip-address* | *ipv6-address*[**%**] | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number* ...] **例：** `Router(config-router)# neighbor 6peers remote-as 65002`	指定した自律システム内のネイバーの IPv6 アドレスを、ローカル ルータの IPv6 マルチプロトコル BGP ネイバーテーブルに追加します。
ステップ 6	**address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] **例：** `Router(config-router)# address-family ipv4`	アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィクスを使用するルーティング セッションを設定します。
ステップ 7	**neighbor** *ipv6-address* **peer-group** *peer-group-name* **例：** `Router(config-router-af)# neighbor 2001:0DB8:yyyy::2 peer-group 6peers`	BGP ネイバーの IPv6 アドレスをピア グループに割り当てます。
ステップ 8	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address* [**%**]} **route-map** *map-name* {**in** | **out**} **例：** `Router(config-router-af)# neighbor 6peers route-map rmap out`	着信ルートまたは発信ルートにルート マップを適用します。 • ルート マップへの変更は、ピアリングがリセットされるまで、またはソフト リセットが実行されるまで、現在のピアでは有効になりません。**soft** キーワードと **in** キーワードを指定して **clear bgp ipv6** コマンドを使用すると、ソフト リセットが実行されます。

	コマンドまたはアクション	目的
ステップ 9	**exit** **例：** `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了し、ルータをルータ コンフィギュレーション モードに戻します。
ステップ 10	ステップ 11 を繰り返します。 **例：** `Router(config-router)# exit`	ルータ コンフィギュレーション モードを終了し、ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 11	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] **例：** `Router(config)# route-map rmap permit 10`	ルート マップを定義し、ルート マップ コンフィギュレーション モードを開始します。
ステップ 12	**set ip next-hop ip-address** [... *ip-address*] [*peer-address*] **例：** `Router(config-route-map)# set ip next-hop 10.21.8.10`	ピアにアドバタイズされる IPv4 パケットのネクストホップを上書きします。

BGP の管理ディスタンスの割り当て

RPF ルックアップでユニキャスト ルートとの比較に使用されるマルチキャスト BGP ルートの管理ディスタンスを指定するには、次の作業を実行します。

注意 BGP 内部ルートの管理ディスタンスを変更することは、推奨されません。発生する可能性のある 1 つの問題は、ルーティング テーブルの不整合が累積され、それによってルーティングが中断する可能性があることです。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast** | **vpnv6**]
5. **distance bgp** *external-distance internal-distance local-distance*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* **例：** `Router(config)# router bgp 65000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast** | **vpnv6**] **例：** `Router(config-router)# address-family ipv6`	IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードでは、IPv6 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv6** コマンドで **unicast** キーワードが指定されていない場合、ルータは IPv6 ユニキャスト アドレス ファミリのコンフィギュレーション モードになります。 • **multicast** キーワードでは、IPv6 マルチキャスト アドレス プレフィクスを指定します。
ステップ 5	**distance bgp** *external-distance internal-distance local-distance* **例：** `Router(config-router-af)# distance bgp 10 50 100`	BGP ルートの管理ディスタンスを設定します。

IPv6 マルチキャスト BGP の変換アップデートの生成

ピアから受信したユニキャスト IPv6 アップデートに対応する IPv6 マルチキャスト BGP アップデートを生成するには、次の作業を実行します。

MBGP 変換アップデート機能は、一般に、BGP 対応ルータだけを持つカスタマー サイト（つまり、ルータを MBGP 対応イメージにアップグレードしていない、またはアップグレードできないカスタマー サイト）とピアリングする MBGP 対応ルータで使用されます。そのカスタマー サイトでは MBGP アドバタイズメントを発信できないため、カスタマー サイトがピアリングするルータは、BGP プレフィクスを、マルチキャスト ソース Reverse Path Forwarding（RPF）ルックアップに使用される MBGP プレフィクスに変換します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*

4. **address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast** | **vpnv6**]
5. **neighbor** *ipv6-address* **translate-update ipv6 multicast** [**unicast**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* **例：** `Router(config)# router bgp 65000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast** | **vpnv6**] **例：** `Router(config-router)# address-family ipv6`	IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードでは、IPv6 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv6** コマンドで **unicast** キーワードが指定されていない場合、ルータは IPv6 ユニキャスト アドレス ファミリのコンフィギュレーション モードになります。 • **multicast** キーワードでは、IPv6 マルチキャスト アドレス プレフィクスを指定します。
ステップ 5	**neighbor** *ipv6-address* **translate-update ipv6 multicast** [**unicast**] **例：** `Router(config-router-af)# neighbor 7000::2 translate-update ipv6 multicast`	ピアから受信したユニキャスト IPv6 アップデートに対応するマルチプロトコル IPv6 BGP アップデートを生成します。

IPv6 BGP グレースフル リスタート機能の設定

IPv6 BGP グレースフル リスタート機能を設定することで、NSF 機能をイネーブルにするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast** | **vpnv6**]
5. **bgp graceful-restart** [**restart-time** *seconds* | **stalepath-time** *seconds*] [**all**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* **例：** `Router(config)# router bgp 65000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast** | **vpnv6**] **例：** `Router(config-router)# address-family ipv6`	IPv6 アドレス ファミリを指定します。
ステップ 5	**bgp graceful-restart** [**restart-time** *seconds* | **stalepath-time** *seconds*] [**all**] **例：** `Router(config-router)# bgp graceful-restart`	BGP グレースフル リスタート機能をイネーブルにします。

BGP セッションのリセット

手順の概要

1. **enable**
2. **clear bgp ipv6** {**unicast** | **multicast**} {***** | *autonomous-system-number* | *ip-address* | *ipv6-address* | *peer-group-name*} [**soft**] [**in** | **out**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**clear bgp ipv6** {**unicast** | **multicast**} {***** | *autonomous-system-number* | *ip-address* | *ipv6-address* | *peer-group-name*} [**soft**] [**in** | **out**] **例：** `Router# clear bgp ipv6 unicast peer-group marketing soft out`	IPv6 BGP セッションをリセットします。

外部 BGP ピアのクリア

手順の概要

1. **enable**
2. **clear bgp ipv6** {**unicast** | **multicast**} **external** [**soft**] [**in** | **out**]
3. **clear bgp ipv6** {**unicast** | **multicast**} **peer-group** [*name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**clear bgp ipv6** {**unicast** | **multicast**} **external** [**soft**] [**in** | **out**] **例：** `Router# clear bgp ipv6 unicast external soft in`	外部 IPv6 BGP ピアをクリアします。
ステップ 3	**clear bgp ipv6** {**unicast** | **multicast**} **peer-group** [*name*] **例：** `Router# clear bgp ipv6 unicast peer-group`	IPv6 BGP ピア グループのすべてのメンバをクリアします。

IPv6 BGP ルート減衰情報のクリア

IPv6 BGP ルート減衰情報をクリアするには、次の作業を実行します。また、抑制されたルートの抑制を解除する方法も示します。

手順の概要

1. **enable**
2. **clear bgp ipv6** {**unicast** | **multicast**} **dampening** [*ipv6-prefix*/*prefix-length*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**clear bgp ipv6** {**unicast** | **multicast**} **dampening** [*ipv6-prefix*/*prefix-length*] **例：** `Router# clear bgp ipv6 unicast dampening 2001:0DB8::/64`	IPv6 BGP ルート減衰情報をクリアし、抑制ルートの抑制を解除します。

IPv6 BGP フラップ統計情報のクリア

手順の概要

1. **enable**
2. **clear bgp ipv6** {**unicast** | **multicast**} **flap-statistics** [*ipv6-prefix*/*prefix-length* | **regexp** *regexp* | **filter-list** *list*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**clear bgp ipv6** {**unicast** | **multicast**} **flap-statistics** [*ipv6-prefix*/*prefix-length* | **regexp** *regexp* | **filter-list** *list*] **例：** `Router# clear bgp ipv6 unicast flap-statistics filter-list 3`	IPv6 BGP フラップ統計情報をクリアします。

IPv6 マルチプロトコル BGP の設定および動作の確認

手順の概要

1. **show bgp ipv6** {**unicast** | **multicast**} [*ipv6-prefix*/*prefix-length*] [**longer-prefixes**] [**labels**]
2. **show bgp ipv6** {**unicast** | **multicast**} **summary**
3. **show bgp ipv6** {**unicast** | **multicast**} **dampening dampened-paths**
4. **enable**
5. **debug bgp ipv6** {**unicast** | **multicast**} **dampening** [**prefix-list** *prefix-list-name*]

6. **debug bgp ipv6** {**unicast** | **multicast**} **updates** [*ipv6-address*] [**prefix-list** *prefix-list-name*] [**in** | **out**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show bgp ipv6** {**unicast**	**multicast**} [*ipv6-prefix*/*prefix-length*] [**longer-prefixes**] [**labels**] **例：** `Router> show bgp ipv6 unicast`	（任意）IPv6 BGP ルーティング テーブルのエントリを表示します。
ステップ 2	**show bgp ipv6** {**unicast**	**multicast**} **summary** **例：** `Router> show bgp ipv6 unicast summary`	（任意）すべての IPv6 BGP 接続のステータスを表示します。
ステップ 3	**show bgp ipv6** {**unicast**	**multicast**} **dampening dampened-paths** **例：** `Router> show bgp ipv6 unicast dampening dampened-paths`	（任意）IPv6 BGP 減衰ルートを表示します。
ステップ 4	**enable** **例：** `Router> enable`	特権 EXEC モードなど、高位の権限レベルをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 5	**debug bgp ipv6** {**unicast**	**multicast**} **dampening** [**prefix-list** *prefix-list-name*] **例：** `Router# debug bgp ipv6 unicast dampening`	（任意）IPv6 BGP 減衰パケットのデバッグ情報を表示します。 • プレフィクス リストが指定されていない場合は、すべての IPv6 BGP 減衰パケットのデバッグ メッセージが表示されます。
ステップ 6	**debug bgp ipv6** {**unicast**	**multicast**} **updates** [*ipv6-address*] [**prefix-list** *prefix-list-name*] [**in**	**out**] **例：** `Router# debug bgp ipv6 unicast updates`	（任意）IPv6 BGP アップデート パケットのデバッグ情報を表示します。 • *ipv6-address* 引数が指定されている場合は、指定したネイバーへの IPv6 BGP アップデートのデバッグ メッセージが表示されます。 • **in** キーワードを使用して、インバウンド アップデートのデバッグ メッセージだけを表示するようにします。 • **out** キーワードを使用して、アウトバウンド アップデートのデバッグ メッセージだけを表示するようにします。

例

- 「show bgp ipv6 コマンドの出力例」
- 「show bgp ipv6 summary コマンドの出力例」
- 「show bgp ipv6 dampened-paths コマンドの出力例」
- 「debug bgp ipv6 dampening コマンドの出力例」

show bgp ipv6 コマンドの出力例

次の例では、IPv6 BGP ルーティング テーブルのエントリが、**show bgp ipv6** コマンドを使用して表示されています。

```
Router> show bgp ipv6 unicast

BGP table version is 12612, local router ID is 192.168.99.70
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>                  2001:0DB8:E:C::2                       0 3748 4697 1752 i
*                   2001:0DB8:0:CC00::1
                                                           0 1849 1273 1752 i
*  2001:618:3::/48  2001:0DB8:E:4::2          1             0 4554 1849 65002 i
*>                  2001:0DB8:0:CC00::1
                                                           0 1849 65002 i
*> 2001:620::/35    2001:0DB8:0:F004::1
                                                           0 3320 1275 559 i
*                   2001:0DB8:E:9::2                       0 1251 1930 559 i
*                   2001:0DB8::A                           0 3462 10566 1930 559 i
*                   2001:0DB8:20:1::11
                                                           0 293 1275 559 i
*                   2001:0DB8:E:4::2          1            0 4554 1849 1273 559 i
*                   2001:0DB8:E:B::2                       0 237 3748 1275 559 i
*                   2001:0DB8:E:C::2                       0 3748 1275 559 i
```

show bgp ipv6 summary コマンドの出力例

次の例では、すべての IPv6 BGP 接続のステータスが、**unicast** キーワードを指定した **show bgp ipv6 summary** コマンドを使用して表示されています。

```
Router# show bgp ipv6 unicast summary

BGP router identifier 172.30.4.4, local AS number 200
BGP table version is 1, main routing table version 1

Neighbor           V    AS  MsgRcvd  MsgSent   TblVer  InQ  OutQ  Up/Down   State/PfxRcd
2001:0DB8:101::2   4    200    6869     6882        0    0     0  06:25:24  Active
```

show bgp ipv6 dampened-paths コマンドの出力例

次の例では、IPv6 BGP 減衰ルートが、**unicast** キーワードを指定した **show bgp ipv6 dampened-paths** コマンドを使用して表示されています。

```
Router# show bgp ipv6 unicast dampening dampened-paths

BGP table version is 12610, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From             Reuse    Path
*d 3FFE:1000::/24   3FFE:C00:E:B::2  00:00:10 237 2839 5609 i
*d 2001:228::/35    3FFE:C00:E:B::2  00:23:30 237 2839 5609 2713 i
```

debug bgp ipv6 dampening コマンドの出力例

次の例では、IPv6 BGP 減衰パケットのデバッグ メッセージが、**unicast** キーワードを指定した **debug bgp ipv6 dampening** コマンドを使用して表示されています。

（注） デフォルトでは、**debug** コマンドからの出力、およびシステム エラー メッセージがコンソールに送信されます。デバッグ出力をリダイレクトするには、コンフィギュレーション モードで **logging** コマンド オプションを使用します。指定できる宛先として、コンソール、仮想端末、内部バッファ、および syslog サーバを実行している UNIX ホストがあります。**debug** コマンドおよびデバッグ出力のリダイレクトの詳細については、『*Cisco IOS Debug Command Reference*, Release 12.4』を参照してください。

```
Router# debug bgp ipv6 unicast dampening

00:13:28:BGP(1):charge penalty for 2001:0DB8:0:1::/64 path 2 1 with halflife-time 15
reuse/suppress 750/2000
00:13:28:BGP(1):flapped 1 times since 00:00:00. New penalty is 1000
00:13:28:BGP(1):charge penalty for 2001:0DB8:0:1:1::/80 path 2 1 with halflife-time 15
reuse/suppress 750/2000
00:13:28:BGP(1):flapped 1 times since 00:00:00. New penalty is 1000
00:13:28:BGP(1):charge penalty for 2001:0DB8:0:5::/64 path 2 1 with halflife-time 15
reuse/suppress 750/2000
00:13:28:BGP(1):flapped 1 times since 00:00:00. New penalty is 1000
00:16:03:BGP(1):charge penalty for 2001:0DB8:0:1::/64 path 2 1 with halflife-time 15
reuse/suppress 750/2000
00:16:03:BGP(1):flapped 2 times since 00:02:35. New penalty is 1892
00:18:28:BGP(1):suppress 2001:0DB8:0:1:1::/80 path 2 1 for 00:27:30 (penalty 2671)
00:18:28:halflife-time 15, reuse/suppress 750/2000
00:18:28:BGP(1):suppress 2001:0DB8:0:1::/64 path 2 1 for 00:27:20 (penalty 2664)
00:18:28:halflife-time 15, reuse/suppress 750/2000
```

debug bgp ipv6 updates コマンドの出力例

次の例では、IPv6 BGP アップデート パケットのデバッグ メッセージが、**unicast** キーワードを指定した **debug bgp ipv6 updates** コマンドを使用して表示されています。

```
Router# debug bgp ipv6 unicast updates

14:04:17:BGP(1):2001:0DB8:0:2::2 computing updates, afi 1, neighbor version 0, table
version 1, starting at ::
14:04:17:BGP(1):2001:0DB8:0:2::2 update run completed, afi 1, ran for 0ms, neighbor
version 0, start version 1, throttled to 1
14:04:19:BGP(1):sourced route for 2001:0DB8:0:2::1/64 path #0 changed (weight 32768)
14:04:19:BGP(1):2001:0DB8:0:2::1/64 route sourced locally
14:04:19:BGP(1):2001:0DB8:0:2:1::/80 route sourced locally
14:04:19:BGP(1):2001:0DB8:0:3::2/64 route sourced locally
14:04:19:BGP(1):2001:0DB8:0:4::2/64 route sourced locally
14:04:22:BGP(1):2001:0DB8:0:2::2 computing updates, afi 1, neighbor version 1, table
version 6, starting at ::
14:04:22:BGP(1):2001:0DB8:0:2::2 send UPDATE (format) 2001:0DB8:0:2::1/64, next
2001:0DB8:0:2::1, metric 0, path
14:04:22:BGP(1):2001:0DB8:0:2::2 send UPDATE (format) 2001:0DB8:0:2:1::/80, next
2001:0DB8:0:2::1, metric 0, path
14:04:22:BGP(1):2001:0DB8:0:2::2 send UPDATE (prepend, chgflags:0x208)
2001:0DB8:0:3::2/64, next 2001:0DB8:0:2::1, metric 0, path
14:04:22:BGP(1):2001:0DB8:0:2::2 send UPDATE (prepend, chgflags:0x208)
2001:0DB8:0:4::2/64, next 2001:0DB8:0:2::1, metric 0, path
```

マルチプロトコル BGP for IPv6 の設定例

- 「例：BGP プロセス、BGP ルータ ID、および IPv6 マルチプロトコル BGP ピアの設定」（P.29）
- 「例：リンクローカル アドレスを使用した IPv6 マルチプロトコル BGP ピアの設定」（P.29）
- 「例：IPv6 マルチプロトコル BGP ピア グループの設定」（P.30）

例：BGP プロセス、BGP ルータ ID、および IPv6 マルチプロトコル BGP ピアの設定

次の例では、IPv6 をグローバルにイネーブルにし、BGP プロセスを設定して BGP ルータ ID を確立します。また、IPv6 マルチプロトコル BGP ピア 2001:0DB8:0:CC00:: が設定およびアクティブ化されます。

```
ipv6 unicast-routing
!
router bgp 65000
no bgp default ipv4-unicast
bgp router-id 192.168.99.70
neighbor 2001:0DB8:0:CC00::1% remote-as 64600

address-family ipv6 unicast
  neighbor 2001:0DB8:0:CC00::1% activate
```

例：リンクローカル アドレスを使用した IPv6 マルチプロトコル BGP ピアの設定

次の例では、ファスト イーサネット インターフェイス 0 上で IPv6 マルチプロトコル BGP ピア FE80::XXXX:BFF:FE0E:A471 を設定し、ファスト イーサネット インターフェイス 0 の IPv6 ネクストホップ グローバル アドレスを BGP アップデートに含めるために nh6 という名前のルート マップを設定します。IPv6 ネクストホップ リンクローカル アドレスは、nh6 ルート マップ（次の例では示されていません）によって、または **neighbor update-source** コマンド（次の例で示しています）で指定したインターフェイスから設定できます。

```
router bgp 65000
 neighbor FE80::XXXX:BFF:FE0E:A471 remote-as 64600
 neighbor FE80::XXXX:BFF:FE0E:A471 update-source fastethernet 0

address-family ipv6
 neighbor FE80::XXXX:BFF:FE0E:A471 activate
 neighbor FE80::XXXX:BFF:FE0E:A471 route-map nh6 out

route-map nh6 permit 10
 match ipv6 address prefix-list cisco
 set ipv6 next-hop 2001:0DB8:5y6::1

ipv6 prefix-list cisco permit 2001:0DB8:2Fy2::/48 le 128
ipv6 prefix-list cisco deny ::/0
```

（注） **neighbor update-source** コマンドでネイバー インターフェイス（*interface-type* 引数）を指定したあとに、**set ipv6 next-hop** コマンドでグローバル IPv6 ネクストホップ アドレス（*ipv6-address* 引数）だけを指定している場合は、*interface-type* 引数で指定したインターフェイスのリンクローカル アドレスが BGP アップデートのネクストホップとして含まれています。したがって、リンクローカル アドレスを使用する複数の BGP ピアに必要となるのは、BGP アップデートにグローバル IPv6 ネクストホップ アドレスを設定する 1 つのルート マップだけとなります。

例：IPv6 マルチプロトコル BGP ピア グループの設定

次に、group1 という名前の IPv6 マルチプロトコル BGP ピア グループを設定する例を示します。

```
router bgp 65000
no bgp default ipv4-unicast
neighbor group1 peer-group
neighbor 2001:0DB8:0:CC00::1 remote-as 64600

address-family ipv6 unicast
 neighbor group1 activate
 neighbor 2001:0DB8:0:CC00::1 peer-group group1
```

例：IPv6 マルチプロトコル BGP へのルートのアドバタイズ

次の例では、IPv6 ネットワーク 2001:0DB8::/24 をローカル ルータの IPv6 ユニキャスト データベースに挿入します（BGP は、ネットワークをアドバタイズする前に、ネットワークのルートがローカル ルータの IPv6 ユニキャスト データベースに存在することを確認します）。

```
router bgp 65000
 no bgp default ipv4-unicast

address-family ipv6 unicast
  network 2001:0DB8::/24
```

例：IPv6 マルチプロトコル BGP プレフィクスのルート マップの設定

次の例では、ネットワーク 2001:0DB8::/24 からの IPv6 ユニキャスト ルートが、cisco という名前のプレフィクス リストに一致する場合は許可するように、rtp という名前のルート マップを設定します。

```
router bgp 64900
no bgp default ipv4-unicast
neighbor 2001:0DB8:0:CC00::1 remote-as 64700

address-family ipv6 unicast
 neighbor 2001:0DB8:0:CC00::1 activate
 neighbor 2001:0DB8:0:CC00::1 route-map rtp in

ipv6 prefix-list cisco seq 10 permit 2001:0DB8::/24

route-map rtp permit 10
 match ipv6 address prefix-list cisco
```

例：IPv6 マルチプロトコル BGP へのプレフィクスの再配布

次の例では、RIP ルートをローカル ルータの IPv6 ユニキャスト データベースに再配布しています。

```
router bgp 64900
no bgp default ipv4-unicast
address-family ipv6 unicast
 redistribute rip
```

例：IPv6 ピア間での IPv4 ルートのアドバタイズ

次の例では、IPv6 ネットワークが 2 つの個別 IPv4 ネットワークに接続している場合に、IPv6 ピア間で IPv4 ルートをアドバタイズしています。ピアリングは、IPv4 アドレス ファミリ コンフィギュレーション モードで IPv6 アドレスを使用して設定されています。アドバタイズされたネクストホップは到達不能である可能性があるため、rmap という名前のインバウンド ルート マップによってネクストホップが設定されます。

```
router bgp 65000
!
 neighbor 6peers peer-group
 neighbor 2001:0DB8:yyyy::2 remote-as 65002
 address-family ipv4
 neighbor 6peers activate
 neighbor 6peers soft-reconfiguration inbound
 neighbor 2001:0DB8:yyyy::2 peer-group 6peers
 neighbor 2001:0DB8:yyyy::2 route-map rmap in
!
route-map rmap permit 10
 set ip next-hop 10.21.8.10
```

その他の関連資料

関連資料

関連項目	参照先
IPv4 BGP の設定作業	『*Cisco* IOS IP Routing Protocols Configuration Guide』の「BGP Features Roadmap」
マルチプロトコル BGP の設定作業	『*Cisco IOS IP Routing Protocols Configuration Guide*』の「BGP Features Roadmap」
BGP およびマルチプロトコル BGP コマンド：complete コマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS IP Routing Protocols Command Reference*』の「BGP Commands」
Cisco ノンストップ フォワーディング	『*Cisco IOS High Availability Configuration Guide*』の「Cisco Nonstop Forwarding」
IPv6 のサポート機能リスト	『*Cisco IOS IPv6 Configuration Guide*』の「Start Here: Cisco IOS Software Release Specifics for IPv6 Features」
IPv6 コマンド：コマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS IPv6 Command Reference*』

規格

規格	タイトル
この機能によってサポートされる新しい規格または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2545	『*Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*』
RFC 2858	『*Multiprotocol Extensions for BGP-4*』
RFC 4007	『*IPv6 Scoped Address Architecture*』
RFC 4364	『*BGP MPLS/IP Virtual Private Networks (VPNs)*』

RFC	タイトル
RFC 4382	『*MPLS/BGP Layer 3 Virtual Private Network (VPN) Management Information Base*』
RFC 4659	『*BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*』
RFC 4724	『*Graceful Restart Mechanism for BGP*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

マルチプロトコル BGP for IPv6 の実装の機能情報

表 1 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どのソフトウェア イメージが特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1　マルチプロトコル BGP for IPv6 の実装の機能情報

機能名	リリース	機能情報
IPv6 ルーティング：マルチプロトコル BGP for IPv6 拡張	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(17a)SX1 12.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	マルチプロトコル BGP for IPv6 拡張では、IPv4 BGP と同じ機能および機能性がサポートされています。 この機能に関する詳細については、次の各項を参照してください。 • 「マルチプロトコル BGP for IPv6 拡張」（P.2） • 「マルチプロトコル BGP for IPv6 の実装方法」（P.3）
IPv6 ルーティング：マルチプロトコル BGP リンクローカル アドレス ピアリング	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(17a)SX1 12.2(4)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	IPv6 では、マルチプロトコル BGP リンクローカル アドレス ピアリングをサポートしています。 この機能に関する詳細については、次の各項を参照してください。 • 「リンクローカル アドレスを使用した IPv6 マルチプロトコル BGP ピアの設定」（P.7） • 「リンクローカル アドレスを使用したマルチプロトコル BGP ピアリング」（P.7）
IPv6 マルチプロトコル BGP へのルートのアドバタイズ	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T	ユーザは、プレフィクスを IPv6 マルチプロトコル BGP にアドバタイズ（挿入）します。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 マルチプロトコル BGP へのルートのアドバタイズ」（P.13） • 「例：IPv6 マルチプロトコル BGP へのルートのアドバタイズ」（P.30）

表 1　マルチプロトコル BGP for IPv6 の実装の機能情報 （続き）

機能名	リリース	機能情報
IPv6 マルチプロトコル BGP プレフィクスのルート マップの設定	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T	ユーザは、IPv6 マルチプロトコル BGP プレフィクスのルート マップを設定できます。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 マルチプロトコル BGP プレフィクスのルート マップの設定」（P.15） • 「例：IPv6 マルチプロトコル BGP プレフィクスのルート マップの設定」（P.30）
IPv6 マルチプロトコル BGP へのプレフィクスの再配布	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T	ユーザは、別のルーティング プロトコルから IPv6 マルチプロトコル BGP にプレフィクスを再配布（挿入）できます。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 マルチプロトコル BGP へのプレフィクスの再配布」（P.17） • 「例：IPv6 マルチプロトコル BGP へのプレフィクスの再配布」（P.30）
IPv6 マルチキャスト アドレス ファミリでのマルチプロトコル BGP のサポート	12.0(26)S 12.2(25)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(33)SXH 12.3(4)T 12.4 12.4(2)T	IPv6 マルチキャスト アドレス ファミリのマルチプロトコル BGP 機能では、マルチプロトコル BGP for IPv6 拡張を提供し、IPv4 BGP と同じ機能と機能性をサポートします。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 マルチキャスト アドレス ファミリのマルチプロトコル BGP」（P.2） • 「マルチプロトコル BGP for IPv6 の実装方法」（P.3）

表 1　マルチプロトコル BGP for IPv6 の実装の機能情報 （続き）

機能名	リリース	機能情報
6PE マルチパス	12.2(25)S 12.2(28)SB 12.2(33)SRA 12.2(33)SXI1 12.4(6)T	6PE マルチパス機能では、Multiprotocol internal BGP（MP-iBGP; マルチプロトコル内部 BGP）を使用して、MPLS IPv4 コア ネットワークを介して IPv6 ルートを配布し、MPLS ラベルを各ルートに付加します。 この機能に関する詳細については、次の各項を参照してください。 • 「6PE マルチパス」（P.3）
IPv6：MP-BGP IPv6 アドレス ファミリ用の NSF およびグレースフル リスタート	12.2(33)SRE 12.2(33)XNE	グレースフル リスタート機能は、IPv6 BGP ユニキャスト、IPv6 BGP マルチキャスト、および VPNv6 アドレス ファミリでサポートされており、BGP IPv6 用の Cisco NonStop Forwarding（NSF; ノンストップ フォワーディング）機能をイネーブルにします。BGP グレースフル リスタート機能を使用すると、TCP 状態を維持することなく、BGP ルーティング テーブルをピアから回復できます。 この機能に関する詳細については、次の項を参照してください。 • 「MP-BGP IPv6 アドレス ファミリのノンストップ フォワーディングおよびグレースフル リスタート」（P.3） • 「IPv6 BGP グレースフル リスタート機能の設定」（P.22）

DHCP for IPv6 の実装

この章では、ネットワーク デバイス上で Dynamic Host Configuration Protocol（DHCP）for IPv6 プレフィクス委任を設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「DHCP for IPv6 の実装の機能情報」（P.42）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

DHCP for IPv6 の実装の前提条件

このマニュアルでは、IPv6 と IPv4 に精通していることを前提としています。IPv6 と IPv4 の設定およびコマンド リファレンス情報については、「その他の関連資料」に記載されている資料を参照してください。

DHCP for IPv6 の実装の制約事項

- Cisco IOS Release 12.0S は、Gigabit Switch Router（GSR; ギガビット スイッチ ルータ）および Cisco 10720 インターネット ルータにかぎり、IPv6 サポートを提供しています。
- イーサネット インターフェイスの DHCPv6 Remote-ID 機能は、Cisco IOS Release 12.2(33)SRC のイーサネット インターフェイスに対してだけ機能します。
- Cisco IOS Release 12.3(4)T、Cisco IOS Release 12.0(32)S、および Cisco IOS 12.2(33)SRC における DHCPv6 の実装では、ステートレス アドレス割り当てだけがサポートされています。

DHCP for IPv6 の実装に関する情報

- 「DHCPv6 プレフィクス委任」（P.2）

DHCPv6 プレフィクス委任

DHCPv6 プレフィクス委任機能を使用すると、リンク、サブネット、およびサイト アドレッシングの変更を管理できます。環境で DHCPv6 を使用して、ステートフル情報やステートレス情報を配布できます。

- ステートフル：アドレス割り当ては一元管理され、クライアントは、アドレス自動設定やネイバー探索などのプロトコルを通じて入手できない設定情報を取得する必要があります。
- ステートレス：Domain Name System（DNS; ドメイン ネーム システム）サーバのアドレスやドメイン検索リスト オプションなど、ステートレス設定パラメータでは、個々のクライアントのダイナミック状態をサーバで保持する必要がありません。

DHCPv6 の機能拡張により、プレフィクス委任も可能になります。Internet Service Provider（ISP; インターネット サービス プロバイダー）はプレフィクス委任を使用して、カスタマーのネットワーク内で使用するプレフィクスをカスタマーに割り当てる処理を自動化できます。プレフィクス委任は、DHCPv6 プレフィクス委任オプションを使用して、Provider Edge（PE; プロバイダー エッジ）デバイスと Customer Premises Equipment（CPE; 宅内装置）の間で行われます。ISP によってプレフィクスがカスタマーに委任されると、カスタマーはさらにプレフィクスをサブネット化してカスタマーのネットワーク内のリンクに割り当てます。

プレフィクス委任のないノード設定

ステートレス DHCPv6 では、DHCPv6 を使用して、サーバによるノードのダイナミック状態の保持を必要としないパラメータをノードに設定できます。ステートレス DHCP の使用は、ルータによってマルチキャストされた Router Advertisement（RA; ルータ アドバタイズメント）メッセージで制御されます。Cisco IOS DHCPv6 クライアントは、適切な RA を受け取るとステートレス DHCPv6 を呼び出します。Cisco IOS DHCPv6 サーバは、DNS サーバやドメイン検索リスト オプションなどの適切な設定パラメータが指定されたステートレス DHCPv6 要求に応答します。

クライアントとサーバの識別

各 DHCPv6 クライアントとサーバは、DHCP Unique Identifier（DUID; DHCP 固有識別子）によって識別されます。DUID は、クライアント識別子およびサーバ識別子オプションで伝送されます。DUID はすべての DHCP クライアントとサーバで一意であり、特定のクライアントまたはサーバに固定されます。DHCPv6 では、クライアントとサーバの両方の識別子にリンク層アドレスに基づく DUID を使用します。デバイスは、最も小さい番号のインターフェイスの MAC アドレスを使用して DUID を形成します。ネットワーク インターフェイスは、デバイスに永続的に接続されていると見なされます。

IPv6 DHCP クライアントが 2 つのプレフィクスを要求し、そのプレフィクスの DUID が同じで IAID が 2 つの異なるインターフェイス上で異なる場合、これらのプレフィクスは 2 つの異なるクライアント用と見なされ、両方のインターフェイス情報が保持されます。

迅速なコミット

DHCPv6 クライアントは、迅速な 2 つのメッセージ交換（請求、応答）または通常の 4 つのメッセージ交換（請求、アドバタイズ、要求、応答）によって、サーバから設定パラメータを取得できます。デフォルトでは、4 つのメッセージ交換が使用されます。rapid-commit オプションをクライアントとサーバの両方でイネーブルにすると、2 つのメッセージ交換が使用されます。

DHCPv6 クライアント、サーバ、およびリレーの機能

DHCPv6 クライアント、サーバ、およびリレーの機能は、インターフェイス上で相互排他的です。これらの機能の 1 つがすでにイネーブルになっている場合、ユーザが同じインターフェイスに別の機能を設定しようとすると、「Interface is in DHCP client mode」、「Interface is in DHCP server mode」、または「Interface is in DHCP relay mode」のいずれかのメッセージが表示されます。

ここでは、次の機能について説明します。

- 「クライアント機能」（P.3）
- 「サーバ機能」（P.4）
- 「DHCP リレー エージェント」（P.7）

クライアント機能

DHCPv6 クライアント機能は、個々の IPv6 対応インターフェイスに対してイネーブルにすることができます。

DHCPv6 クライアントは、DNS サーバのアドレスやドメイン検索リスト オプションなど、個々のクライアントのダイナミック状態をサーバで保持する必要がない設定パラメータを要求したり、受け入れたりできます。DHCPv6 クライアントは、受信した情報でローカルの Cisco IOS スタックを設定します。

DHCPv6 クライアントは、プレフィクスの委任を要求することもできます。委任ルータから取得したプレフィクスは、ローカルの IPv6 の一般的なプレフィクス プールに格納されます。一般的なプレフィクス プールに格納されたプレフィクスは、他のアプリケーションから参照できます。たとえば、一般的なプレフィクス プールを使用して、ルータのダウンストリーム インターフェイスに番号を割り当てることができます。

サーバの選択

DHCPv6 クライアントは、請求メッセージを送信し、サーバからアドバタイズ メッセージの応答を収集することによって、サーバのリストを作成します。これらのメッセージには、優先度の値に基づいてランクが付けられます。サーバは、優先度の値を明示的に指定してアドバタイズ メッセージに優先度オプションを追加できます。クライアントがサーバからプレフィクスを取得する必要がある場合は、プレフィクスをアドバタイズしたサーバだけが考慮されます。

IAPD と IAID

Identity Association for Prefix Delegation（IAPD）は、要求側ルータに割り当てられたプレフィクスの集まりです。要求側ルータには、インターフェイスごとに 1 つずつなど、複数の IAPD が存在する可能性があります。

各 IAPD は、Identity Association Identification（IAID）によって識別されます。IAID は、要求側ルータによって選択され、要求側ルータ上の IAPD IAID で一意です。IAID は、デバイスに永続的に接続されていると見なされる、関連付けられたネットワーク インターフェイスの情報を使用するため、ルータをリブートしても変わりません。

サーバ機能

DHCPv6 サーバ機能は、個々の IPv6 対応インターフェイスに対してイネーブルにすることができます。

DHCPv6 サーバは、DNS サーバのアドレスやドメイン検索リスト オプションなど、個々のクライアントのダイナミック状態をサーバで保持する必要がない設定パラメータを提供できます。プレフィクス委任を実行するように DHCPv6 サーバを設定できます。

クライアントのすべての設定パラメータはそれぞれ独立して DHCPv6 設定プールに設定され、それらのプールは NVRAM に格納されます。設定プールには、起動時にインターフェイス上の特定の DHCPv6 サーバに関連付けることができます。クライアントに委任されるプレフィクスは、特定のクライアントに対してあらかじめ割り当てられたプレフィクスのリストとして指定するか、または NVRAM にも格納される IPv6 ローカル プレフィクス プールとして指定できます。手動で設定したプレフィクスのリストまたは IPv6 ローカル プレフィクス プールは、DHCPv6 設定プールによって参照および使用できます。

DHCPv6 サーバは、自動バインディング テーブルをメモリに保持して、サーバとクライアント間のプレフィクスなどの設定パラメータの割り当てをトラッキングします。自動バインディングは、データベース エージェントに永続的に格納できます。このようなデータベース エージェントには、リモート TFTP サーバやローカル NVRAM ファイル システムなどがあります。

設定情報プール

DHCPv6 設定情報プールは名前付きエンティティであり、プールからクライアントへのパラメータの割り当てを制御する、使用可能な設定パラメータやポリシーに関する情報が格納されます。プールは DHCPv6 サービスとは無関係に設定され、Command-Line Interface（CLI; コマンドライン インターフェイス）を使用して DHCPv6 サービスに関連付けられます。

各設定プールには、次の設定パラメータと動作情報を格納できます。

- 次のようなプレフィクス委任情報
  - プレフィクス プール名および関連付けられている推奨期間と有効期間
  - 特定のクライアントの使用可能なプレフィクスのリストおよび関連付けられている推奨期間と有効期間
- DNS サーバの IPv6 アドレスのリスト
- ドメイン検索リスト（DNS 解決のためのドメイン名を含む文字列）

DHCP for IPv6 アドレスの割り当て

DHCPv6 を使用すると、DHCP サーバは IPv6 ネットワーク アドレスなどの設定パラメータを IPv6 クライアントに渡すことができます。DHCPv6 個別アドレス割り当て機能は、ホストが接続されているネットワークに基づいた正しいプレフィクス内で、重複しないようにアドレス割り当てを管理します。アドレスは、1 つまたは複数のプレフィクス プールから割り当てることができます。デフォルト ドメインや DNS ネーム サーバ アドレスなどの追加オプションをクライアントに戻すことができます。アドレス プールを特定のインターフェイスまたは複数のインターフェイスで使用するように割り当てるか、サーバで自動的に適切なプールを検索するように設定できます。

プレフィクスの割り当て

プレフィクス委任ルータ（DHCPv6 サーバ）は、クライアントから要求を受信するときに、要求側ルータ（DHCPv6 クライアント）に割り当てるプレフィクスを選択します。サーバは、スタティック割り当てとダイナミック割り当てのメカニズムを使用して、要求側クライアントのプレフィクスを選択できます。管理者は、DUID によって識別される特定クライアントの IAPD について、プレフィクスのリストおよび関連付けられている推奨期間と有効期間を手動で設定できます。

委任ルータはクライアントから要求を受信すると、クライアントのメッセージに IAPD に対して設定されたスタティック バインディングがあるかどうかをチェックします。スタティック バインディングがある場合、バインディングのプレフィクスがクライアントに返されます。そのようなバインディングが見つからない場合、サーバは他のソースからクライアントのプレフィクスを割り当てようとします。

Cisco IOS DHCPv6 サーバは、IPv6 ローカル プレフィクス プールからダイナミックにプレフィクスを割り当てることができます。サーバはクライアントからプレフィクス要求を受信すると、割り当てられていないプレフィクスをプールから取得しようとします。クライアントが前に割り当てられたプレフィクスを解放すると、サーバはそれらのプレフィクスを再割り当てできるようにプールに戻します。

IPv6 プレフィクス委任ルータは、Framed-IPv6-Prefix アトリビュートを使用する RADIUS サーバなどの外部装置に基づいて要求側ルータのプレフィクスを選択することもできます。この機能の詳細については、「*Implementing ADSL and Deploying Dial Access for IPv6*」の章を参照してください。

自動バインディング

各 DHCPv6 設定プールには、バインディング テーブルが関連付けられています。バインディング テーブルには、明示的にクライアントに委任された設定プール内のすべてのプレフィクスに関するレコードが格納されます。バインディング テーブル内の各エントリに含まれる情報は次のとおりです。

- クライアントの DUID
- クライアントの IPv6 アドレス
- クライアントに関連付けられた IAPD のリスト
- 各 IAPD に委任されたプレフィクスのリスト
- 各プレフィクスの推奨期間と有効期間
- このバインディング テーブルが属している設定プール
- プールを使用するサーバが実行されるネットワーク インターフェイス

バインディング テーブルのエントリは、プレフィクスが設定プールからクライアントに委任されるたびに自動的に作成され、クライアントはプレフィクス委任を更新、再バインディング、または確認すると更新されます。また、クライアントが自発的にバインディング内のすべてのプレフィクスを解放したとき、すべてのプレフィクスの有効期間が経過したとき、または管理者が **clear ipv6 dhcp binding** コマンドを実行したときに削除されます。

バインディング データベース

自動バインディングは RAM に保持され、永続的なストレージに保存できます。これにより、システムのリロード後や電源切断後でも、クライアントに割り当てられたプレフィクスなどの設定に関する情報が失われなくなります。バインディングはテキスト レコードとして格納されるため、メンテナンスが容易です。各レコードには、次の情報が格納されます。

- クライアントに割り当てられた設定の DHCPv6 プール名
- クライアントが要求を受信したインターフェイスの ID
- クライアントの IPv6 アドレス
- クライアントの DUID
- IAPD の IAID

- クライアントに委任されたプレフィクス
- プレフィクス長
- プレフィクスの推奨期間（秒単位）
- プレフィクスの有効期間（秒単位）
- プレフィクスの期限切れタイム スタンプ
- 割り当てられたプレフィクスのオプションのローカル プレフィクス プール名

ファイルの先頭（テキスト レコードの前）には、データベースが作成された時間を記録するタイム スタンプと、新しいデータベースと古いデータベースの区別に役立つバージョン番号があります。ファイルの最後（テキスト レコードのあと）には、ファイルの切り捨てを検出するための「*end*」というテキスト文字列が格納されています。

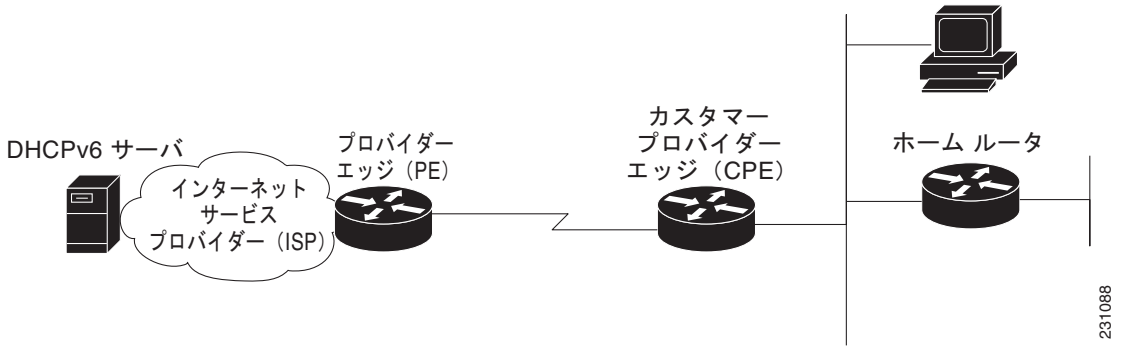
バインディング データベースが保存される永続的なストレージのことをデータベース エージェントと呼びます。データベース エージェントには、FTP サーバや TFTP サーバ、RCP、フラッシュ ファイル システム、NVRAM などがあります。

DHCPv6 サーバ ステートレス自動設定

ステートレス設定パラメータの階層型 DHCPv6 により、ステートレスまたはステートフル DHCPv6 クライアントは、設定パラメータ（DHCPv6 オプション）をローカル DHCPv6 サーバ プールにエクスポートできます。ローカル DHCPv6 サーバは、インポートされた設定パラメータを他の DHCPv6 クライアントに提供できます。

図 1 に、一般的なブロードバンドの配置を示します。

図 1　　ブロードバンド トポロジ



PE 方向の CPE インターフェイスは、ステートレスまたはステートフル DHCPv6 クライアントにすることができます。どちらの場合も、ISP 側の DHCPv6 サーバは、DNS サーバ アドレス、ドメイン名、Simple Network Time Protocol（SNTP; 簡易ネットワーク タイム プロトコル）サーバなどの設定パラメータを CPE 上の DHCP クライアントに提供できます。これらの情報は ISP に固有であり、変更される可能性があります。

CPE は、DHCPv6 クライアント（たとえば、ISP に対するクライアント）であるだけでなく、ホーム ネットワークに対する DHCPv6 サーバとして機能する場合もあります。たとえば、CPE とホーム デバイス（ホーム ルータや PC など）間のリンク上では、ネイバー探索のあとにステートレスまたはステートフル DHCPv6 が動作することがあります。また、ホーム ネットワークに提供される情報は、ISP 側の DHCPv6 サーバから取得された情報と同じであることもあります。この情報はダイナミックに変更される可能性があるため、CPE の設定にハード設定することはできません。そのため、CPE 上の DHCPv6 コンポーネントでは、設定パラメータを DHCPv6 クライアントから DHCPv6 サーバ プールに自動的にインポートできます。

DHCPv6 は、次の項で説明されている、サーバ上の IPv6 のオプションをサポートします。

情報リフレッシュ サーバ オプション

DHCPv6 情報リフレッシュ オプションでは、クライアントが DHCPv6 から取得した情報をリフレッシュするまで待機する時間の長さの上限を指定できます。DHCPv6 サーバにアクセスして設定をリフレッシュするタイミングをクライアントに通知できる、期間が設定されたアドレスまたはその他のエンティティが存在しないため、このオプションは、ステートレス DHCPv6 で使用します。

NIS- および NIS+ 関連のサーバ オプション

NIS- および NIS+ 関連のオプションを使用して Network Information Service（NIS）アドレスや NIS プラス（NIS+）アドレス、または DHCPv6 サーバのドメイン名を設定し、その情報を DHCPv6 クライアントにインポートできます。

SIP サーバ オプション

Session Initiation Protocol（SIP）サーバ オプションには、1 つ以上の SIP アウトバウンド プロキシ サーバにマッピングできるドメイン名または IPv6 アドレスのリストが含まれます。一方のオプションでドメイン名のリストを伝送し、もう一方のオプションで 128 ビットの IPv6 アドレスのリストを伝送します。

SIP は、マルチメディア セッションまたはコールを確立、変更、および終了できるアプリケーション レイヤ制御プロトコルです。SIP システムには、ユーザ エージェント、プロキシ サーバ、リダイレクト サーバ、レジストラなどのいくつかの論理コンポーネントがあります。ユーザ エージェントには SIP クライアントが含まれ、プロキシ サーバには常に SIP クライアントが含まれます。

SNTP サーバ オプション

SNTP サーバ オプションは、クライアントで同期に使用できる SNTP サーバの 1 つ以上の IPv6 アドレスのリストを提供します。クライアントはこれらの SNTP サーバを使用して、システム時刻を標準時刻サーバのシステム時刻に同期します。サーバは、SNTP サーバのリストを優先度の降順に示す場合がありますが、クライアントは SNTP サーバのリストを順序指定されたリストとして処理する必要があります。

DHCP リレー エージェント

クライアントのリンク上に常駐する DHCP リレー エージェントは、クライアントとサーバ間のメッセージの中継に使用されます。DHCP リレー エージェントの動作は、クライアントに対して透過的です。クライアントは、リンクスコープを持つ予約済みのマルチキャスト アドレスを使用して DHCP サーバを探します。したがって、クライアントとサーバの間で直接通信するために、クライアントとサーバを同じリンクに接続する必要があります。ただし、容易な管理、節約、またはスケーラビリティに懸念があるような場合には、DHCP クライアントから同じリンクに接続されていない DHCP サーバにメッセージを送信できるようにする必要があります。

プレフィクス委任の DHCPv6 リレー エージェント通知

プレフィクス委任の DHCPv6 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 DHCPv6 RELAY-REPLY パケットの内容を確認することによって、プレフィ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クス委任オプションを見つけると、委任されるプレフィクスに関する情報を抽出し、その情報に一致する IPv6 スタティック 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クスに宛てられたパケットは、プレフィクス委任に含

まれる情報に基づいて転送されます。IPv6 スタティック ルートは、プレフィ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は、ルーティング テーブルに保持されます。

この機能を使用するためにユーザ設定は必要ありません。スタティック ルートの管理は、リレー エージェントによって自動的に行われます。

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、プレフィクス委任のリース期限が経過するか、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。リレー エージェントのルーティング テーブル内の IPv6 スタティック ルートは、プレフィクス委任のリース期間を延長すると更新できます。

この機能により、IPv6 スタティック 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 IPv6 アドレスを使用すると、unicast Reverse Packet Forwarding（uRPF; ユニキャスト RPF）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 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 テーブル内のスタティック 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。スタティック ルートは、クライアントから DHCP_DECLINE メッセージが送信されると削除されます。

DHCPv6 Bulk-Lease クエリー

DHCPv6 では、クライアントが DHCPv6 バインディングに関する情報を要求できる Bulk-Lease クエリーがサポートされています。この機能により、新しいクエリー タイプが追加され、TCP を使用した DHCPv6 バインディング データのバルク転送が可能になります。

DHCPv6 リレー エージェントがイネーブルの場合、Bulk-Lease クエリーはデフォルトでイネーブルになります。Bulk-Lease クエリーは、リロードにより失われたバインディング情報を取得するために、リレー エージェントの始動時にトリガーされます。DHCPv6 リレー宛先がインターフェイス上で設定されると、Bulk-Lease クエリーは、DHCPv6 リレーがイネーブルにされているインターフェイスの IPv6 アドレスで実行されます。Bulk-Lease クエリーは、リレー エージェント プロセスから独立したプロセスです。

DHCPv6 リレー送信元設定

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

図 2 に、1 つのクライアント、リレー、およびサーバで構成される簡単なネットワークを示します。リレーとサーバは 2001:0DB8:1::/64 を介して通信し、リレーには 2001:0DB8:2::/64 に対するクライアント方向インターフェイスがあります。リレーには、アドレス 2001:0DB8:3:1/64 が設定されたループバック インターフェイスもあります。

図 2　DHCPv6 リレー送信元設定 - 簡単なネットワーク

DHCPv6 リレー

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

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

DHCPv6 リレーの SSO と ISSU

二重 RP をサポートしているシスコの特定のネットワーク デバイスでは、Stateful Switchover（SSO; ステートフル スイッチオーバー）は RP 冗長性を活用してネットワークのアベイラビリティを向上させます。この機能は RP の一方をアクティブ プロセッサとして設定し、もう一方の RP をスタンバイ プロセッサとして指定したあと、これらの RP の間で重要なステート情報を同期します。2 つのプロセッサの初回同期後、SSO はこれらの間の RP ステート情報をダイナミックに維持します。

Cisco IOS In Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）プロセスを使用すると、パケット転送中に Cisco IOS ソフトウェアを更新または変更できます。ほとんどのネットワークでは、計画的なソフトウェア アップグレードがダウンタイムの大きな原因になっています。ISSU を使用すると、パケット転送中に Cisco IOS ソフトウェアを変更できるため、ネットワークのアベイラビリティが向上し、計画的なソフトウェア アップグレードによるダウンタイムを短縮できます。

SSO と ISSU は冗長ハードウェアを使用し、アクティブ RP とスタンバイ RP がそれぞれ DHCP リレー エージェントのインスタンスを実行します。両方のインスタンスは実行時の状態データを交換します。

SSO と ISSU の詳細については、『*Cisco IOS High Availability Configuration Guide* 』の「Stateful Switchover」と「Cisco IOS In Service Software Upgrade Process」の章を参照してください。

DHCPv6 リレー オプション：イーサネット インターフェイスの Remote-ID

この機能は、リモート ID（remote-ID）オプションを中継される（RELAY-FORWARD）DHCPv6 パケットに追加します。

remote-ID オプションによって、ポート情報、システムの DUID、VLAN ID などの情報が DHCPv6 サーバに提供されます。この情報は、クライアントのパケットが到達時に経由するリレー上のポートとリレーの両方を一意に識別するために使用できます。DHCPv6 サーバはこの情報を使用して、特定のユーザ、ホスト、または加入者モデムに固有のパラメータを選択します。この機能は、現時点ではイーサネット インターフェイスに対してだけ機能します。

この機能によってユーザ設定が追加されることはありません。remote-ID オプションは RELAY-FORWARD パケットに自動的に追加されるため、ユーザ設定は必要ありません。

DHCPv6 サーバは、RELAY-REPLY パケットで remote-ID オプションをエコーする必要はありません。リレー エージェントの remote-ID オプションには、Internet Assigned Numbers Authority（IANA; インターネット割り当て番号局）によって DHCPv6 オプション コード 37 が割り当てられています。

remote-ID オプションが RELAY-REPLY パケットに含まれている場合、パケットがクライアントに中継される前に、オプションはパケットから取り除かれます。

DHCPv6 リレー オプション：リロード永続 Interface-ID

この機能により、interface-ID オプションが永続化されます。interface-ID オプションは、RELAY-REPLY パケットの転送時に使用するインターフェイスを決定するために、リレー エージェントによって使用されます。永続 interface-ID オプションは、リレー エージェントとして機能するルータがオフライン（リロード時や停電時など）になっても変わりません。リレー エージェントとして機能するルータがオンラインに戻ったときに、リレー エージェントの内部インターフェイス インデックスに変更が加えられている可能性があります。たとえば、リレー エージェントがリブートし、インターフェイス インデックスのインターフェイスの数が変更されている場合、またはリレー エージェントが起動し、リブート前よりも仮想インターフェイスの数が増えている場合などです。この機能を使用すると、このような場合に問題が発生するのを防ぐことができます。

この機能は、単純にインターフェイス名の短縮形として表現されるように DHCPv6 interface-ID オプションを変更します。この構文により、リロード後にリレー エージェント上で物理インターフェイスまたは論理インターフェイスが変更されたことが原因で発生する可能性がある問題を回避できます。

DHCP for IPv6 の実装方法

DHCPv6 サーバ機能の設定

次の各項の作業では、DHCPv6 サーバ機能の設定方法を示します。

DHCPv6 設定プールの設定

DHCPv6 設定プールを作成して設定し、そのプールをインターフェイス上のサーバに関連付けるには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **domain-name** *domain*
5. **dns-server** *ipv6-address*
6. **prefix-delegation** *ipv6-prefix*/*prefix-length client-duid* [**iaid** *iaid*] [*lifetime*]
7. **prefix-delegation pool** *poolname* [**lifetime** *valid-lifetime preferred-lifetime*]
8. **exit**
9. **interface** *type number*
10. **ipv6 dhcp server** *poolname* [**rapid-commit**] [**preference** *value*] [**allow-hint**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 dhcp pool** *poolname* **例：** `Router(config)# ipv6 dhcp pool pool1`	DHCPv6 設定情報プールを設定し、DHCPv6 プール コンフィギュレーション モードを開始します。
ステップ 4	**domain-name** *domain* **例：** `Router(config-dhcp)# domain-name example.com`	DHCPv6 クライアントのドメイン名を設定します。
ステップ 5	**dns-server** *ipv6-address* **例：** `Router(config-dhcp)# dns-server 2001:0DB8:3000:3000::42`	DHCPv6 クライアントで使用できる DNS IPv6 サーバを指定します。
ステップ 6	**prefix-delegation** *ipv6-prefix*/*prefix-length client-duid* [**iaid** *iaid*] [*lifetime*] **例：** `Router(config-dhcp)# prefix-delegation 2001:0DB8:1263::/48 0005000400F1A4D070D03`	指定したクライアントの IAPD に委任する、手動設定済みの数値プレフィクスを指定します。

	コマンドまたはアクション	目的
ステップ 7	**prefix-delegation pool** *poolname* [**lifetime** *valid-lifetime preferred-lifetime*] **例：** `Router(config-dhcp)# prefix-delegation pool pool1 lifetime 1800 60`	DHCPv6 クライアントに委任するプレフィクスの名前付き IPv6 ローカル プレフィクス プールを指定します。
ステップ 8	**exit** **例：** `Router(config-dhcp)# exit`	DHCPv6 プール コンフィギュレーション モードを終了し、ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 9	**interface** *type number* **例：** `Router(config)# interface serial 3`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 10	**ipv6 dhcp server** *poolname* [**rapid-commit**] [**preference** *value*] [**allow-hint**] **例：** `Router(config-if)# ipv6 dhcp server pool1`	インターフェイスに対して DHCPv6 をイネーブルにします。

サーバ機能のバインディング データベース エージェントの設定

バインディング テーブルのエントリは、プレフィクスが設定プールからクライアントに委任されるたびに自動的に作成され、クライアントがプレフィクス委任を更新、再バインディング、または確認すると更新されます。また、クライアントが自発的にバインディング内のすべてのプレフィクスを解放したとき、すべてのプレフィクスの有効期間が経過したとき、または管理者が **clear ipv6 dhcp binding** コマンドをイネーブルにしたときに削除されます。これらのバインディングは RAM に保持され、*agent* 引数を使用して永続的なストレージに保存できます。これにより、システムのリロード後や電源切断後でも、クライアントに割り当てられたプレフィクスなどの設定に関する情報が失われなくなります。バインディングはテキスト レコードとして格納されるため、メンテナンスが容易です。

バインディング データベースが保存される永続的な各ストレージのことをデータベース エージェントと呼びます。データベース エージェントには、FTP サーバなどのリモート ホストや NVRAM などのローカル ファイル システムがあります。

サーバ機能の DHCPv6 バインディング データベース エージェントを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp database** *agent* [**write-delay** *seconds*] [**timeout** *seconds*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 dhcp database** *agent* [**write-delay** *seconds*] [**timeout** *seconds*] **例：** `Router(config)# ipv6 dhcp database tftp://10.0.0.1/dhcp-binding`	DHCPv6 バインディング データベース エージェントのパラメータを指定します。

DHCPv6 クライアント機能の設定

一般的なプレフィクスは、DHCPv6 プレフィクス委任クライアントが受信したプレフィクスからダイナミックに定義できます。インターフェイス上で DHCPv6 クライアント機能を設定し、インターフェイス上でプレフィクス委任をイネーブルにするには、次の作業を実行します。委任されたプレフィクスは、一般的なプレフィクスに格納されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 dhcp client pd** {*prefix-name* | **hint** *ipv6-prefix*} [**rapid-commit**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface ethernet 0/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 dhcp client pd** {*prefix-name* | **hint** *ipv6-prefix*} [**rapid-commit**] **例：** `Router(config-if)# ipv6 dhcp client pd dhcp-prefix`	DHCPv6 クライアント プロセスをイネーブルにし、指定したインターフェイスを経由するプレフィクス委任の要求をイネーブルにします。

DHCPv6 リレー エージェントの設定

DHCPv6 リレー エージェント機能をイネーブルにし、インターフェイス上でリレー宛先アドレスを指定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 dhcp relay destination** *ipv6-address* [*interface-type interface-number*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* **例：** `Router(config)# interface ethernet 4/2`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 dhcp relay destination** *ipv6-address* [*interface-type interface-number*] **例：** `Router(config-if) ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 ethernet 4/3`	クライアント パケットを転送する宛先アドレスを指定し、インターフェイスに対して DHCPv6 リレー サービスをイネーブルにします。

DHCPv6 リレー送信元の設定

DHCPv6 リレー送信元を設定するには、次の作業を実行します。

- 「インターフェイスに対する DHCPv6 リレー送信元の設定」（P.15）
- 「DHCPv6 リレー送信元のグローバルな設定」（P.16）
- 「DHCPv6 Bulk-Lease クエリー パラメータの設定」（P.17）

DHCPv6 リレー送信元の設定の制限事項

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

インターフェイスに対する DHCPv6 リレー送信元の設定

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

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 dhcp relay source-interface** *interface-type interface-number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface loopback 0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 dhcp relay source-interface** *interface-type interface-number* **例：** `Router(config-if)# ipv6 dhcp relay source-interface loopback 0`	このインターフェイスで受信したメッセージの中継時に送信元として使用するインターフェイスを設定します。

DHCPv6 リレー送信元のグローバルな設定

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

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp-relay source-interface** *interface-type interface-number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 dhcp-relay source-interface** {*interface-type interface-number*} **例：** `Router(config)# ipv6 dhcp-relay source-interface loopback 0`	メッセージの中継時に送信元として使用するインターフェイスを設定します。

DHCPv6 Bulk-Lease クエリー パラメータの設定

DHCPv6 リレー エージェントがイネーブルの場合、DHCPv6 Bulk-Lease クエリー機能は自動的にイネーブルになります。Bulk-Lease クエリー パラメータを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp-relay bulk-lease** {**data-timeout** *seconds* | **retry** *number*} [**disable**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 dhcp-relay bulk-lease** {**data-timeout** *seconds* | **retry** *number*} [**disable**] **例：** `Router(config)# ipv6 dhcp-relay bulk-lease data-timeout 60`	Bulk-Lease クエリー パラメータを設定します。

DHCP for IPv6 アドレス割り当ての設定

DHCPv6 アドレス割り当てを設定するには、次の作業を実行します。

- 「インターフェイスに対する DHCPv6 サーバ機能のイネーブル化」（P.18）（必須）
- 「インターフェイスに対する DHCPv6 クライアント機能のイネーブル化」（P.20）（必須）

DHCPv6 アドレス割り当ての設定の前提条件

デフォルトでは、DHCPv6 機能はルータで設定されていません。

DHCPv6 アドレス割り当てを設定する場合は、指定したインターフェイスが次のレイヤ 3 インターフェイスのいずれかである必要があります。

- Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）：**interface vlan** *vlan-id* コマンドを使用して作成された VLAN インターフェイス。
- レイヤ 3 モードの EtherChannel ポート チャネル：**interface port-channel port-channel-number** コマンドを使用して作成されたポートチャネル論理インターフェイス。

インターフェイスに対する DHCPv6 サーバ機能のイネーブル化

インターフェイスに対して DHCPv6 サーバ機能をイネーブルにするには、次の作業を実行します。

（注） DHCPv6 プールを削除するには、**no ipv6 dhcp pool** *poolname* 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。DHCPv6 プールの特性を変更するには、**no** 形式の DHCP プール コンフィギュレーション モード コマンドを使用します。インターフェイスに対して DHCPv6 サーバ機能をディセーブルにするには、**no ipv6 dhcp server** インターフェイス コンフィギュレーション コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **address prefix** *ipv6-prefix* [**lifetime** {*valid-lifetime preferred-lifetime* | **infinite**}]
5. **link-address** *ipv6-prefix*
6. **vendor-specific** *vendor-id*
7. **suboption** *number* {**address** *ipv6-address* | **ascii** *ascii-string* | **hex** *hex-string*}
8. **exit**
9. **exit**
10. **interface** *type number*
11. **ipv6 dhcp server** [*poolname* | **automatic**] [**rapid-commit**] [**preference value**] [**allow-hint**]
12. **end**
13. **show ipv6 dhcp pool**
    または
    show ipv6 dhcp interface
14. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router(config)# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 dhcp pool** *poolname* **例：** `Router(config)# ipv6 dhcp pool engineering`	DHCP プール コンフィギュレーション モードを開始し、IPv6 DHCP プールの名前を定義します。

	コマンド	目的
ステップ 4	**address prefix** *ipv6-prefix* [**lifetime** {*valid-lifetime preferred-lifetime* | **infinite**}] **例：** `Router(config-dhcpv6)# address prefix 2001:1000::0/64 lifetime infinite`	（任意）アドレス割り当て用のアドレス プレフィクスを指定します。 • このアドレスは、16 ビット値をコロンで区切った 16 進数で指定する必要があります。 • **lifetime** *valid-lifetime preferred-lifetime* ：IPv6 アドレス プレフィクスが有効な状態を維持する時間間隔（秒単位）を指定します。
ステップ 5	**link-address** *ipv6-prefix* **例：** `Router(config-dhcpv6)# link-address 2001:1001::0/64`	（任意）link-address IPv6 プレフィクスを指定します。 • 着信インターフェイス上のアドレスまたはパケット内のリンク アドレスが指定した IPv6 プレフィクスに一致しない場合、サーバは設定情報プールを使用します。
ステップ 6	**vendor-specific** *vendor-id* **例：** `Router(config-dhcpv6)# vendor-specific 9`	（任意）ベンダー固有の識別番号を指定して、ベンダー固有のコンフィギュレーション モードを開始します。
ステップ 7	**suboption** *number* {**address** *ipv6-address* | **ascii** *ascii-string* | **hex** *hex-string*} **例：** `Router(config-dhcpv6-vs)# suboption 1 address 1000:235D::1`	（任意）ベンダー固有のサブオプション番号を入力します。
ステップ 8	**exit** **例：** `Router(config-dhcpv6-vs)# exit`	DHCP プール コンフィギュレーション モードに戻ります。
ステップ 9	**exit** **例：** `Router(config-dhcpv6)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**interface** *type number* **例：** `Router(config)# interface fastethernet 0/0`	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 11	**ipv6 dhcp server** [*poolname* | **automatic**] [**rapid-commit**] [**preference** *value*] [**allow-hint**] **例：** `Router(config-if)# ipv6 address dhcp server rapid-commit`	インターフェイスに対して DHCPv6 サーバ機能をイネーブルにします。
ステップ 12	**end** **例：** `Router(config-if)# end`	特権 EXEC モードに戻ります。

	コマンド	目的

ステップ 13	**show ipv6 dhcp pool**
	または
	show ipv6 dhcp interface
	
	例：
	`Router# show ipv6 dhcp pool`
	または
	
	例：
	`Router# show ipv6 dhcp interface`
		DHCPv6 プール設定を確認するか、または DHCPv6 サーバ機能がインターフェイスでイネーブルになっていることを確認します。

ステップ 14	**copy running-config startup-config** **例：** `Router# copy running-config startup-config`	（任意）エントリをコンフィギュレーション ファイルに保存します。

インターフェイスに対する DHCPv6 クライアント機能のイネーブル化

インターフェイスに対して DHCPv6 クライアント機能をイネーブルにするには、次の作業を実行します。

（注） DHCPv6 クライアント機能をディセーブルにするには、**no ipv6 address dhcp** インターフェイス コンフィギュレーション コマンドを使用します。DHCPv6 クライアント要求を削除するには、**no ipv6 address dhcp client request vendor** インターフェイス コンフィギュレーション コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 address dhcp** [**rapid-commit**]
5. **ipv6 address dhcp client request vendor**
6. **end**
7. **show ipv6 dhcp interface**

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface fastethernet 0/0`	インターフェイス コンフィギュレーション モードを開始し、設定するインターフェイスを指定します。
ステップ 4	**ipv6 address dhcp** [**rapid-commit**] **例：** `Router(config-if)# ipv6 address dhcp rapid-commit`	インターフェイスで DHCPv6 サーバから IPv6 アドレスを取得できるようにします。
ステップ 5	**ipv6 address dhcp client request vendor** **例：** `Router(config-if)# ipv6 dhcp client request vendor-specific`	（任意）インターフェイスでベンダー固有のオプションを要求できるようにします。
ステップ 6	**end** **例：** `Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show ipv6 dhcp interface** **例：** `Router# show ipv6 dhcp interface`	DHCPv6 クライアントがインターフェイスでイネーブルになっていることを確認します。

ステートレス DHCPv6 機能の設定

DHCPv6 機能を使用してクライアントに名前ルックアップ システムに関する情報を設定するには、次の作業を実行します。サーバは、クライアントに関連する状態を保持しません。たとえば、割り当てのプレフィクス プールやレコードは保持されません。したがって、この機能は「ステートレス」DHCPv6 です。

- 「ステートレス DHCPv6 サーバの設定」（P.21）（必須）
- 「ステートレス DHCPv6 クライアントの設定」（P.23）（必須）
- 「送信元ルーティング ヘッダー オプションを使用したパケットの処理のイネーブル化」（P.23）（必須）

ステートレス DHCPv6 サーバの設定

ステートレス DHCPv6 サーバを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **dns-server** *ipv6-address*
5. **domain-name** *domain*
6. **exit**
7. **interface** *type number*
8. **ipv6 dhcp server** *poolname* [**rapid-commit**] [**preference** *value*] [**allow-hint**]
9. **ipv6 nd other-config-flag**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 dhcp pool** *poolname* **例：** `Router(config)# ipv6 dhcp pool dhcp-pool`	DHCPv6 設定情報プールを設定し、DHCPv6 プール コンフィギュレーション モードを開始します。
ステップ 4	**dns-server** *ipv6-address* **例：** `Router(config-dhcp) dns-server 2001:0DB8:3000:3000::42`	DHCPv6 クライアントで使用できる DNS IPv6 サーバを指定します。
ステップ 5	**domain-name** *domain* **例：** `Router(config-dhcp)# domain-name domain1.com`	DHCPv6 クライアントのドメイン名を設定します。
ステップ 6	**exit** **例：** `Router(config-dhcp)# exit`	DHCPv6 プール コンフィギュレーション モードを終了し、ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 7	**interface** *type number* **例：** `Router(config)# interface serial 3`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。

	コマンドまたはアクション	目的
ステップ 8	**ipv6 dhcp server** *poolname* [**rapid-commit**] [**preference** *value*] [**allow-hint**] **例：** `Router(config-if)# ipv6 dhcp server dhcp-pool`	インターフェイスに対して DHCPv6 をイネーブルにします。
ステップ 9	**ipv6 nd other-config-flag** **例：** `Router(config-if)# ipv6 nd other-config-flag`	IPv6 RA に「別のステートフル設定」フラグを設定します。

ステートレス DHCPv6 クライアントの設定

ステートレス DHCPv6 クライアントを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 address autoconfig** [**default**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface serial 3`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 address autoconfig** [**default**] **例：** `Router(config-if)# ipv6 address autoconfig`	インターフェイスに対してステートレス自動設定を使用した IPv6 アドレスの自動設定をイネーブルにし、インターフェイスにおける IPv6 処理をイネーブルにします。

送信元ルーティング ヘッダー オプションを使用したパケットの処理のイネーブル化

送信元ルーティング ヘッダー オプションを使用したパケットの処理をイネーブルにするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 source-route**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 source-route** **例：** `Router(config)# ipv6 source-route`	IPv6 タイプ 0 ルーティング ヘッダーの処理をイネーブルにします。

DHCPv6 サーバ オプションの設定

DHCPv6 サーバでステートレス オプションを設定し、それらのオプションを DHCPv6 クライアントにインポートするには、次の作業を実行します。

- 「情報リフレッシュ サーバ オプションの設定」（P.24）（任意）
- 「情報リフレッシュ サーバ オプションのインポート」（P.25）（任意）
- 「NIS- および NISP 関連のサーバ オプションの設定」（P.26）（任意）
- 「NIS- および NIS+ 関連のサーバ オプションのインポート」（P.27）（任意）
- 「SIP サーバ オプションのインポート」（P.28）（任意）
- 「SNTP サーバ オプションの設定」（P.29）（任意）
- 「SNTP サーバ オプションのインポート」（P.29）（任意）
- 「ステートレス DHCPv6 サーバ オプションのインポート」（P.30）（任意）

情報リフレッシュ サーバ オプションの設定

情報リフレッシュ サーバ オプションを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **information refresh** {*days* [*hours minutes*] | **infinity**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 dhcp pool** *poolname* **例：** `Router(config)# ipv6 dhcp pool pool1`	DHCPv6 設定情報プールを設定し、DHCPv6 プール コンフィギュレーション モードを開始します。
ステップ 4	**information refresh** {*days* [*hours minutes*] | **infinity**} **例：** `Router(config-dhcp)# information refresh 1 1 1`	クライアントに送信する情報リフレッシュ タイムを指定します。

情報リフレッシュ サーバ オプションのインポート

情報リフレッシュ サーバ オプションを DHCPv6 クライアントにインポートするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **import information refresh**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 dhcp pool** *poolname* **例：** `Router(config)# ipv6 dhcp pool pool1`	DHCPv6 設定情報プールを設定し、DHCPv6 プール コンフィギュレーション モードを開始します。
ステップ 4	**import information refresh** **例：** `Router(config-dhcp)# import information refresh`	情報リフレッシュ タイム オプションを DHCPv6 クライアントにインポートします。

NIS- および NISP 関連のサーバ オプションの設定

NIS- および NIS+ 関連のサーバ オプションを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **nis address** *ipv6-address*
5. **nis domain-name** *domain-name*
6. **nisp address** *ipv6-address*
7. **nisp domain-name** *domain-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 dhcp pool** *poolname* **例：** `Router(config)# ipv6 dhcp pool pool1`	DHCPv6 設定情報プールを設定し、DHCPv6 プール コンフィギュレーション モードを開始します。
ステップ 4	**nis address** *ipv6-address* **例：** `Router(config-dhcp)# nis address 2001:0DB8:1000:1000::30`	クライアントに送信する IPv6 サーバの NIS アドレスを指定します。

	コマンドまたはアクション	目的
ステップ 5	**nis domain-name** *domain-name* **例：** `Router(config-dhcp)# nis domain-name domain1`	サーバがクライアントの NIS ドメイン名情報をクライアントに伝送できるようにします。
ステップ 6	**nisp address** *ipv6-address* **例：** `Router(config-dhcp)# nisp address 2001:0DB8:3000:3000::42`	DHCPv6 クライアントに送信する IPv6 サーバの NIS+ アドレスを指定します。
ステップ 7	**nisp domain-name** *domain-name* **例：** `Router(config-dhcp)# nisp domain-name domain2`	サーバがクライアントの NIS+ ドメイン名情報を DHCPv6 クライアントに伝送できるようにします。

NIS- および NIS+ 関連のサーバ オプションのインポート

NIS- および NIS+ 関連のサーバ オプションをインポートするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **import nis address**
5. **import nis domain-name**
6. **import nisp address**
7. **import nisp domain-name**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 dhcp pool** *poolname* **例：** `Router(config)# ipv6 dhcp pool pool1`	DHCPv6 設定情報プールを設定し、DHCPv6 プール コンフィギュレーション モードを開始します。
ステップ 4	**import nis address** **例：** `Router(config-dhcp)# import nis address`	NIS サーバ オプションを DHCPv6 クライアントにインポートします。

	コマンドまたはアクション	目的
ステップ 5	**import nis domain-name** **例：** `Router(config-dhcp)# import nis domain-name`	NIS ドメイン名オプションを DHCPv6 クライアントにインポートします。
ステップ 6	**import nisp address** **例：** `Router(config-dhcp)# import nisp address`	NISP アドレス オプションを DHCPv6 クライアントにインポートします。
ステップ 7	**import nisp domain-name** **例：** `Router(config-dhcp)# import nisp domain-name`	NISP ドメイン名オプションを DHCPv6 クライアントにインポートします。

SIP サーバ オプションのインポート

SIP サーバ オプションをアウトバウンド SIP プロキシ サーバにインポートするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **import sip address**
5. **import sip domain-name**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 dhcp pool** *poolname* **例：** `Router(config)# ipv6 dhcp pool pool1`	DHCPv6 設定情報プールを設定し、DHCPv6 プール コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**import sip address** **例：** `Router(config-dhcp)# import sip address`	SIP サーバの IPv6 アドレス リスト オプションをアウトバウンド SIP プロキシ サーバにインポートします。
ステップ 5	**import sip domain-name** **例：** `Router(config-dhcp)# import sip domain-name`	SIP サーバのドメイン名リスト オプションをアウトバウンド SIP プロキシ サーバにインポートします。

SNTP サーバ オプションの設定

SNTP サーバ オプションを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **sntp address** *ipv6-address*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 dhcp pool** *poolname* **例：** `Router(config)# ipv6 dhcp pool pool1`	DHCPv6 設定情報プールを設定し、DHCPv6 プール コンフィギュレーション モードを開始します。
ステップ 4	**sntp address** *ipv6-address* **例：** `Router(config-dhcp)# sntp address 2001:0DB8:2000:2000::33`	クライアントに送信する SNTP サーバ リストを指定します。

SNTP サーバ オプションのインポート

SNTP サーバ オプションをインポートするには、次の作業を実行します。

手順の概要

1. **enable**

2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **import sntp address** *ipv6-address*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 dhcp pool** *poolname* **例：** `Router(config)# ipv6 dhcp pool pool1`	DHCPv6 設定情報プールを設定し、DHCPv6 プール コンフィギュレーション モードを開始します。
ステップ 4	**import sntp address** *ipv6-address* **例：** `Router(config-dhcp)# import sntp address 2001:0DB8:2000:2000::33`	SNTP サーバ オプションを DHCPv6 クライアントにインポートします。

ステートレス DHCPv6 サーバ オプションのインポート

ステートレス DHCPv6 サーバ オプションをインポートするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **import dns-server**
5. **import domain-name**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 dhcp pool** *poolname* **例：** `Router(config)# ipv6 dhcp pool pool1`	DHCPv6 設定情報プールを設定し、DHCPv6 プール コンフィギュレーション モードを開始します。
ステップ 4	**import dns-server** **例：** `Router(config-dhcp)# import dns-server`	DNS 再帰名サーバ オプションを DHCPv6 クライアントにインポートします。
ステップ 5	**import domain-name** **例：** `Router(config-dhcp)# import domain-name`	ドメイン検索リスト オプションを DHCPv6 クライアントにインポートします。

DHCPv6 プレフィクス委任クライアント機能による一般的なプレフィクスの定義

インターフェイス上で DHCPv6 クライアント機能を設定し、インターフェイス上でプレフィクス委任をイネーブルにするには、次の作業を実行します。委任されたプレフィクスは、一般的なプレフィクスに格納されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 dhcp client pd** {*prefix-name* | **hint** *ipv6-prefix*} [**rapid-commit**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* **例：** `Router(config)# interface ethernet 0/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 dhcp client pd** {*prefix-name* | **hint** *ipv6-prefix*} [**rapid-commit**] **例：** `Router(config-if)# ipv6 dhcp client pd dhcp-prefix`	DHCPv6 クライアント プロセスをイネーブルにし、指定したインターフェイスを経由するプレフィクス委任の要求をイネーブルにします。 • 委任されたプレフィクスは、一般的なプレフィクスの *prefix-name* 引数に格納されます。

インターフェイス上の DHCPv6 クライアントの再起動

まず以前に取得したプレフィクスとその他の設定オプションを解放して設定を解除したあとで、指定したインターフェイス上の DHCPv6 クライアントを再起動するには、次の作業を実行します。

手順の概要

1. **enable**
2. **clear ipv6 dhcp client** *interface-type interface-number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**clear ipv6 dhcp client** *interface-type interface-number* **例：** `Router# clear ipv6 dhcp client Ethernet 1/0`	インターフェイス上の DHCPv6 クライアントを再起動します。

DHCPv6 バインディング テーブルからの自動クライアント バインディングの削除

DHCPv6 バインディング テーブルから自動クライアント バインディングを削除するには、次の作業を実行します。

手順の概要

1. **enable**
2. **clear ipv6 dhcp binding** [*ipv6-address*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**clear ipv6 dhcp binding** [*ipv6-address*] **例：** `Router# clear ipv6 dhcp binding`	DHCPv6 バインディング テーブルから自動クライアント バインディングを削除します。

DHCPv6 のトラブルシューティング

この作業では、DHCPv6 設定のトラブルシューティング時に必要に応じて使用できるコマンドを示します。

手順の概要

1. **enable**
2. **debug ipv6 dhcp** [**detail**]
3. **debug ipv6 dhcp database**
4. **debug ipv6 dhcp relay**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**debug ipv6 dhcp** [**detail**] **例：** `Router# debug ipv6 dhcp`	DHCPv6 のデバッグをイネーブルにします。
ステップ 3	**debug ipv6 dhcp database** **例：** `Router# debug ipv6 dhcp database`	DHCPv6 バインディング データベースのデバッグをイネーブルにします。
ステップ 4	**debug ipv6 dhcp relay** **例：** `Router# debug ipv6 dhcp relay`	DHCPv6 リレー エージェントのデバッグをイネーブルにします。

DHCPv6 の設定と動作の確認

DHCPv6 の設定と動作を確認するために情報を表示するには、次の作業を実行します。これらのコマンドは、任意の順序で入力できます。

手順の概要

1. **enable**
2. **show ipv6 dhcp**
3. **show ipv6 dhcp binding** [*ipv6-address*]
4. **show ipv6 dhcp database** [*agent-url*]
5. **show ipv6 dhcp interface** [*type number*]
6. **show ipv6 dhcp pool** [*poolname*]
7. **show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router# enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**show ipv6 dhcp** **例：** `Router# show ipv6 dhcp`	指定したデバイスの DUID を表示します。
ステップ 3	**show ipv6 dhcp binding** [*ipv6-address*] **例：** `Router# show ipv6 dhcp binding`	DHCPv6 データベース内の自動クライアント バインディングを表示します。
ステップ 4	**show ipv6 dhcp database** [*agent-url*] **例：** `Router# show ipv6 dhcp database`	DHCPv6 バインディング データベース エージェントの情報を表示します。
ステップ 5	**show ipv6 dhcp interface** [*type number*] **例：** `Router# show ipv6 dhcp interface`	DHCPv6 インターフェイスの情報を表示します。
ステップ 6	**show ipv6 dhcp pool** [*poolname*] **例：** `Router# show ipv6 dhcp pool`	DHCPv6 設定プールの情報を表示します。
ステップ 7	**show running-config** **例：** `Router# show running-config`	ルータで実行されている現在の設定を表示します。

例

ここでは、次の出力例について説明します。

show ipv6 dhcp コマンドの出力例

次の **show ipv6 dhcp** コマンドの例は、デバイスの DUID を示しています。

```
Router# show ipv6 dhcp

This device's DHCPv6 unique identifier(DUID): 000300010002FCA5DC1C
```

show ipv6 dhcp binding コマンドの出力例

次の **show ipv6 dhcp binding** コマンドの例は、2 つのクライアントに関する情報（DUID、IAPD、プレフィクス、推奨期間と有効期間など）を示しています。

```
Router# show ipv6 dhcp binding

Client: FE80::202:FCFF:FEA5:DC39 (Ethernet2/1)
  DUID: 000300010002FCA5DC1C
  IA PD: IA ID 0x00040001, T1 0, T2 0
    Prefix: 3FFE:C00:C18:11::/68
            preferred lifetime 180, valid lifetime 12345
            expires at Nov 08 2002 02:24 PM (12320 seconds)
Client: FE80::202:FCFF:FEA5:C039 (Ethernet2/1)
  DUID: 000300010002FCA5C01C
  IA PD: IA ID 0x00040001, T1 0, T2 0
    Prefix: 3FFE:C00:C18:1::/72
            preferred lifetime 240, valid lifetime 54321
            expires at Nov 09 2002 02:02 AM (54246 seconds)
    Prefix: 3FFE:C00:C18:2::/72
            preferred lifetime 300, valid lifetime 54333
            expires at Nov 09 2002 02:03 AM (54258 seconds)
    Prefix: 3FFE:C00:C18:3::/72
            preferred lifetime 280, valid lifetime 51111
```

show ipv6 dhcp database コマンドの出力例

次の **show ipv6 dhcp database** コマンドの例は、バインディング データベース エージェントである TFTP、NVRAM、およびフラッシュに関する情報を示しています。

```
Router# show ipv6 dhcp database

Database agent tftp://172.19.216.133/db.tftp:
  write delay: 69 seconds, transfer timeout: 300 seconds
  last written at Jan 09 2003 01:54 PM,
     write timer expires in 56 seconds
  last read at Jan 06 2003 05:41 PM
  successful read times 1
  failed read times 0
  successful write times 3172
  failed write times 2
Database agent nvram:/dhcpv6-binding:
  write delay: 60 seconds, transfer timeout: 300 seconds
  last written at Jan 09 2003 01:54 PM,
```

```
     write timer expires in 37 seconds
  last read at never
  successful read times 0
  failed read times 0
  successful write times 3325
  failed write times 0
Database agent flash:/dhcpv6-db:
  write delay: 82 seconds, transfer timeout: 3 seconds
  last written at Jan 09 2003 01:54 PM,
    write timer expires in 50 seconds
  last read at never
  successful read times 0
  failed read times 0
  successful write times 2220
  failed write times 614
```

show ipv6 dhcp interface コマンドの出力例

次に、**show ipv6 dhcp interface** コマンドの出力例を示します。最初の例では、DHCPv6 サーバとして機能するインターフェイスを持つルータでコマンドを使用しています。2 番めの例では、DHCPv6 クライアントとして機能するインターフェイスを持つルータでコマンドを使用しています。

```
Router1# show ipv6 dhcp interface

Ethernet2/1 is in server mode
  Using pool: svr-p1
  Preference value: 20
  Rapid-Commit is disabled

Router2# show ipv6 dhcp interface

Ethernet2/1 is in client mode
  State is OPEN (1)
  List of known servers:
    Address: FE80::202:FCFF:FEA1:7439, DUID 000300010002FCA17400
    Preference: 20
      IA PD: IA ID 0x00040001, T1 120, T2 192
        Prefix: 3FFE:C00:C18:1::/72
                preferred lifetime 240, valid lifetime 54321
                expires at Nov 08 2002 09:10 AM (54319 seconds)
        Prefix: 3FFE:C00:C18:2::/72
                preferred lifetime 300, valid lifetime 54333
                expires at Nov 08 2002 09:11 AM (54331 seconds)
        Prefix: 3FFE:C00:C18:3::/72
                preferred lifetime 280, valid lifetime 51111
                expires at Nov 08 2002 08:17 AM (51109 seconds)
      DNS server: 2001:0DB8:1001::1
      DNS server: 2001:0DB8:1001::2
      Domain name: example1.net
      Domain name: example2.net
      Domain name: example3.net
    Prefix name is cli-p1
    Rapid-Commit is enabled
```

show ipv6 dhcp pool コマンドの出力例

次の **show ipv6 dhcp pool** コマンドの例は、svr-p1 という名前の設定プールに関する情報（svr-p1 プールで見つかったスタティック バインディング、プレフィクス情報、DNS サーバ、ドメイン名など）を示しています。

```
Router# show ipv6 dhcp pool

DHCPv6 pool: svr-p1
  Static bindings:
```

```
    Binding for client 000300010002FCA5C01C
      IA PD: IA ID 00040002,
        Prefix: 3FFE:C00:C18:3::/72
                preferred lifetime 604800, valid lifetime 2592000
      IA PD: IA ID not specified; being used by 00040001
        Prefix: 3FFE:C00:C18:1::/72
                preferred lifetime 240, valid lifetime 54321
        Prefix: 3FFE:C00:C18:2::/72
                preferred lifetime 300, valid lifetime 54333
        Prefix: 3FFE:C00:C18:3::/72
                preferred lifetime 280, valid lifetime 51111
  Prefix from pool: local-p1, Valid lifetime 12345, Preferred lifetime 180
  DNS server: 2001:0DB8:1001::1
  DNS server: 2001:0DB8:1001::2
  Domain name: example1.net
  Domain name: example2.net
  Domain name: example3.net
Active clients: 2
Current configuration : 22324 bytes
!
! Last configuration change at 14:59:38 PST Tue Jan 16 2001
! NVRAM config last updated at 04:25:39 PST Tue Jan 16 2001 by bird
!
hostname Router
!
ip cef
ipv6 unicast-routing
ipv6 cef
ipv6 cef accounting prefix-length
!
!
interface Ethernet0
 ip address 10.4.9.11 255.0.0.0
 media-type 10BaseT
 ipv6 address 2001:0DB8:C18:1::/64 eui-64
```

DHCP for IPv6 の実装の設定例

ここでは、次の DHCPv6 マッピングの設定例について説明します。

- 「例：DHCPv6 サーバ機能の設定」（P.37）
- 「例：DHCPv6 クライアント機能の設定」（P.38）
- 「例：サーバ機能のデータベース エージェントの設定」（P.38）
- 「例：DHCP for IPv6 アドレス割り当ての設定」（P.38）
- 「例：ステートレス DHCPv6 機能の設定」（P.39）

例：DHCPv6 サーバ機能の設定

DHCPv6 クライアントは、イーサネット インターフェイス 0/0 上でこのサーバに接続されています。サーバは、dhcp-pool という名前の DHCP プール内のパラメータを使用するように設定されています。このプールは、DNS サーバの IPv6 アドレスと使用するドメイン名をクライアントに提供します。また、プレフィクスを client-prefix-pool1 という名前のプレフィクス プールから委任できるように指定しています。委任されたプレフィクスの有効期間と推奨期間はそれぞれ 1800 秒と 600 秒に設定されています。client-prefix-pool1 という名前のプレフィクス プールには、長さが /40 のプレフィクスがあり、そのプレフィクスから長さが /48 の（サブ）プレフィクスが委任されます。

```
ipv6 dhcp pool dhcp-pool
 prefix-delegation pool client-prefix-pool1 lifetime 1800 600
 dns-server 2001:0DB8:3000:3000::42
 domain-name example.com
!
interface Ethernet0/0
 description downlink to clients
 ipv6 address FEC0:240:104:2001::139/64
 ipv6 dhcp server dhcp-pool
!
ipv6 local pool client-prefix-pool1 2001:0DB8:1200::/40 48
```

例：DHCPv6 クライアント機能の設定

この DHCPv6 クライアントには、3 つのインターフェイスがあります。イーサネット インターフェイス 0/0 は、DHCPv6 サーバ機能がイネーブルになっているサービス プロバイダーへのアップストリーム リンクです。FastEthernet インターフェイス 0/0 と 0/1 は、ローカル ネットワークへのリンクです。

アップストリーム インターフェイスであるイーサネット インターフェイス 0/0 では、DHCPv6 クライアント機能がイネーブルになっています。プロバイダーによって委任されたプレフィクスは、prefix-from-provider という名前の一般的なプレフィクスに格納されます。

ローカル ネットワークである FastEthernet インターフェイス 0/0 と 0/1 は、両方とも prefix-from-provider という名前の一般的なプレフィクスに基づいてインターフェイス アドレスを割り当てます。アドレスの左端のビットは一般的なプレフィクスに基づき、右端のビットはスタティックに指定されます。

```
interface Ethernet 0/0
 description uplink to provider DHCP IPv6 server
 ipv6 dhcp client pd prefix-from-provider
!
interface FastEthernet 0/0
 description local network 0
 ipv6 address prefix-from-provider ::5:0:0:0:100/64
!
interface FastEthernet 0/1
 description local network 1
 ipv6 address prefix-from-provider ::6:0:0:0:100/64
```

例：サーバ機能のデータベース エージェントの設定

DHCPv6 サーバは、TFTP プロトコルを使用して、アドレス 10.0.0.1 のサーバ上にある dhcp-binding という名前のファイルにテーブル バインディングを格納するように設定されています。バインディングは 120 秒ごとに保存されます。

```
ipv6 dhcp database tftp://10.0.0.1/dhcp-binding write-delay 120
```

次の例では、DHCP for IPv6 バインディング データベース エージェントのパラメータを指定し、バインディング エントリをブートフラッシュに格納しています。

```
ipv6 dhcp database bootflash
```

例：DHCP for IPv6 アドレス割り当ての設定

次に、1 つの IPv6 アドレス プレフィクスを含む engineering という名前のプールを設定する例を示します。

```
ipv6 dhcp pool engineering
address prefix 2001:1000::0/64 lifetime infinite
```

次に、3 つのリンク アドレスと 1 つの IPv6 アドレス プレフィクスを含む testgroup という名前のプールを設定する例を示します。

```
ipv6 dhcp pool testgroup
link-address 2001:1001::0/64
link-address 2001:1002::0/64
link-address 2001:2000::0/48
address prefix 2001:1000::0/64 lifetime infinite
end
```

次に、ベンダー固有オプションを含む 350 という名前のプールを設定する例を示します。

```
ipv6 dhcp pool 350
address prefix 2001:1000::0/64 lifetime infinite
vendor-specific 9
suboption 1 address 1000:235D::1
suboption 2 ascii "IP-Phone"
end
```

例：ステートレス DHCPv6 機能の設定

この例では、DHCPv6 機能を使用して、クライアントに名前ルックアップ システムに関する情報を設定しています。サーバには、クライアントに渡される名前ルックアップ情報を含む DHCP プールが設定されています。プレフィクス プールを含める必要はありません。この DHCP プールは、**ipv6 dhcp server** コマンドを使用して、カスタマー（イーサネット 0/0）へのアクセス リンクに接続されています。このアクセス リンクでは、**ipv6 nd other-config-flag** コマンドもイネーブルになっています。このインターフェイスから送信された RA メッセージは、「別の」（たとえば、アドレス以外の）設定情報に DHCPv6 を使用する必要があることをクライアントに通知します。

```
ipv6 dhcp pool dhcp-pool
 dns-server 2001:0DB8:A:B::1
 dns-server 2001:0DB8:3000:3000::42
 domain-name example.com
!
interface Ethernet0/0
 description Access link down to customers
 ipv6 address 2001:0DB8:1234:42::1/64
 ipv6 nd other-config-flag
 ipv6 dhcp server dhcp-pool
```

クライアントには DHCPv6 設定はありません。ただし、サービス プロバイダーへのアップリンク（イーサネット 0/0）に対して **ipv6 address autoconfig** コマンドを発行すると、2 つのイベントが発生します。

- アドレスは、サーバから受信した RA メッセージ内のプレフィクスに基づいてインターフェイスに自動設定されます。
- 受信した RA メッセージに「別の設定」フラグが設定されている場合、インターフェイスは DHCPv6 サーバから別の（たとえばアドレス以外の）設定を取得しようとします。

その他の関連資料

関連資料

関連項目	参照先
IPv6 のサポート機能リスト	『*Cisco IOS IPv6 Configuration Guide*』の「Start Here: Cisco IOS Software Release Specifics for IPv6 Features」
IPv6 基本接続	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing IPv6 Addressing and Basic Connectivity」
IPv6 プレフィクス委任	• 『*Cisco IOS IPv6 Configuration Guide*』の「Implementing IPv6 Addressing and Basic Connectivity」 • 『*Cisco IOS IPv6 Configuration Guide*』の「Implementing ADSL and Deploying Dial Access for IPv6」
IPv6 コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト、使用に関する注意事項、および例	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS DHCP リレー エージェント	『*Configuring the Cisco IOS DHCP Relay Agent*』

規格

規格	タイトル
この機能によってサポートされる新しい規格または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 3315	『*Dynamic Host Configuration Protocol for IPv6*』
RFC 3319	『*Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers*』
RFC 3633	『*IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) Version 6*』

RFC	タイトル
RFC 3646	『*DNS Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*』
RFC 3898	『*Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*』
RFC 4075	『*Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6*』
RFC 4242	『*Information Refresh Time Option for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*』
RFC 4649	『*Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option*』
RFC 5460	『*DHCPv6 Bulk Leasequery*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

DHCP for IPv6 の実装の機能情報

表 1 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どのソフトウェア イメージが特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1　DHCP for IPv6 の実装の機能情報

機能名	リリース	機能情報
IPv6 アクセス サービス：DHCPv6 プレフィクス委任	12.0(32)S 12.2(28)SB 12.2(33)SRA 12.2(18)SXE 12.3(4)T 12.4 12.4(2)T 15.0(1)S	DHCPv6 プレフィクス委任機能を使用すると、リンク、サブネット、およびサイト アドレッシングの変更を管理できます。環境で DHCPv6 を使用して、ステートフル情報やステートレス情報を配布できます。 この機能に関する詳細については、次の各項を参照してください。 • 「DHCPv6 プレフィクス委任」（P.2） • 「DHCPv6 サーバ機能の設定」（P.10） • 「DHCPv6 クライアント機能の設定」（P.13） • 「例：DHCPv6 サーバ機能の設定」（P.37） • 「例：DHCPv6 クライアント機能の設定」（P.38）
IPv6 アクセス サービス：ステートレス DHCPv6	12.2(33)SRA 12.2(18)SXE 12.3(4)T 12.4 12.4(2)T	ステートレス DHCPv6 では、DHCPv6 を使用して、サーバによるノードのダイナミック状態の保持を必要としないパラメータをノードに設定できます。 この機能に関する詳細については、次の各項を参照してください。 • 「DHCPv6 プレフィクス委任」（P.2） • 「プレフィクス委任のないノード設定」（P.2） • 「ステートレス DHCPv6 機能の設定」（P.21） • 「例：ステートレス DHCPv6 機能の設定」（P.39）
IPv6 アクセス サービス：DHCP for IPv6 リレー エージェント	12.2(28)SB 12.2(33)SRC 12.2(33)SXI 12.3(11)T 12.4 12.4(2)T	クライアントのリンク上に常駐する DHCP リレー エージェントは、クライアントとサーバ間のメッセージの中継に使用されます。 この機能に関する詳細については、次の各項を参照してください。 • 「DHCP for IPv6 の実装方法」（P.10） • 「DHCPv6 リレー エージェントの設定」（P.14）

表 1　DHCP for IPv6 の実装の機能情報 （続き）

機能名	リリース	機能情報
IPv6 アクセス サービス：DHCPv6 サーバ ステートレス自動設定	12.4(15)T	ステートレス設定パラメータの階層型 DHCPv6 により、ステートレスまたはステートフル DHCPv6 クライアントは、設定パラメータ（DHCPv6 オプション）をローカル DHCPv6 サーバ プールにエクスポートできます。 この機能に関する詳細については、次の各項を参照してください。 • 「DHCPv6 サーバ ステートレス自動設定」（P.6） • 「DHCPv6 サーバ オプションの設定」（P.24）
IPv6 アクセス サービス：DHCPv6 クライアント情報リフレッシュ オプション	12.4(15)T	DHCPv6 情報リフレッシュ オプションでは、クライアントが DHCPv6 から取得した情報をリフレッシュするまで待機する時間の長さの上限を指定できます。 この機能に関する詳細については、次の各項を参照してください。 • 「DHCPv6 サーバ ステートレス自動設定」（P.6） • 「DHCPv6 サーバ オプションの設定」（P.24）
DHCP：DHCPv6 サーバ SNTP、NIS、NIS+、リフレッシュ タイマー オプション	12.4(15)T	DHCPv6 サーバ オプションは、DHCP ステートレス自動設定の一部です。 この機能に関する詳細については、次の各項を参照してください。 • 「DHCPv6 サーバ ステートレス自動設定」（P.6） • 「DHCPv6 サーバ オプションの設定」（P.24）
DHCP：プレフィクス委任の DHCPv6 リレー エージェント通知	12.2(33)SCA 12.2(33)SRC 12.2(33)SXI 15.0(1)S	プレフィクス委任の DHCPv6 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 DHCPv6 パケットの内容を確認することによって、プレフィクス委任オプションを見つけることができます。 この機能に関する詳細については、次の項を参照してください。 • 「プレフィクス委任の DHCPv6 リレー エージェント通知」（P.7）
DHCPv6 イーサネット Remote-ID オプション	12.2(33)SRC 12.2(33)SXI 15.0(1)S	この機能を使用すると、中継される（RELAY-FORWARD）DHCPv6 パケットに remote-ID オプションが追加されます。 この機能に関する詳細については、次の項を参照してください。 • 「DHCPv6 リレー オプション：イーサネット インターフェイスの Remote-ID」（P.9）

表 1　DHCP for IPv6 の実装の機能情報 （続き）

機能名	リリース	機能情報
DHCPv6 リレー：リロード永続インターフェイス ID オプション	12.2(33)SB 12.2(33)SRC 12.2(33)SXI 15.0(1)S	この機能により、interface-ID オプションが永続化されます。interface-ID オプションは、RELAY-REPLY パケットの転送時に使用するインターフェイスを決定するために、リレー エージェントによって使用されます。 この機能に関する詳細については、次の項を参照してください。 • 「DHCPv6 リレー オプション：リロード永続 Interface-ID」（P.10）
DHCP：DHCPv6 個別アドレス割り当て	12.4(24)T	この機能は、ホストが接続されているネットワークに基づいて、正しいプレフィクス内で重複しないようにアドレス割り当てを管理します。 この機能に関する詳細については、次の項を参照してください。 • 「DHCP for IPv6 アドレスの割り当て」（P.4） • 「DHCP for IPv6 アドレス割り当ての設定」（P.17）
DHCP：DHCPv6 リレーの SSO/ISSU	12.2(33)SRE	SSO と ISSU は冗長ハードウェアを使用し、アクティブ RP とスタンバイ RP がそれぞれ DHCP リレー エージェントのインスタンスを実行します。 この機能に関する詳細については、次の項を参照してください。 • 「DHCPv6 リレーの SSO と ISSU」（P.9）
DHCPv6 リレー送信元設定	12.2(33)SRE	DHCPv6 を使用する一部のネットワークでは、より安定したアドレス（ループバック インターフェイスなど）を設定し、そのインターフェイスを中継されたメッセージの送信元アドレスとしてリレーで使用することが望ましい場合があります。DHCPv6 リレー送信元設定機能には、この機能が用意されています。 この機能に関する詳細については、次の各項を参照してください。 • 「DHCPv6 リレー送信元設定」（P.8） • 「DHCPv6 リレー送信元の設定」（P.15）

表 1　DHCP for IPv6 の実装の機能情報 （続き）

機能名	リリース	機能情報
DHCPv6 再パッケージ化	12.2(33)SRE 12.2(33)XNE	DHCPv6 再パッケージ化機能は、DHCPv6 個別アドレス割り当てとステートレス DHCPv6 で構成されています。 DHCPv6 個別アドレス割り当て機能は、ホストが接続されているネットワークに基づいて、正しいプレフィクス内で重複しないようにアドレス割り当てを管理します。 この機能に関する詳細については、次の各項を参照してください。 • 「DHCP for IPv6 アドレスの割り当て」（P.4） • 「DHCP for IPv6 アドレス割り当ての設定」（P.17） ステートレス DHCPv6 機能では、DHCPv6 を使用して、サーバによるノードのダイナミック状態の保持を必要としないパラメータをノードに設定できます。 この機能に関する詳細については、次の各項を参照してください。 • 「DHCPv6 プレフィクス委任」（P.2） • 「プレフィクス委任のないノード設定」（P.2） • 「ステートレス DHCPv6 機能の設定」（P.21） • 「例：ステートレス DHCPv6 機能の設定」（P.39）
DHCPv6 Bulk-Lease クエリー	15.1(1)S	Cisco IOS DHCPv6 リレー エージェントでは、RFC 5460 に準拠した Bulk-Lease クエリーがサポートされています。 この機能に関する詳細については、次の各項を参照してください。 • 「DHCPv6 Bulk-Lease クエリー」（P.8） • 「DHCPv6 Bulk-Lease クエリー パラメータの設定」（P.17） **debug ipv6 dhcp relay**、**ipv6 dhcp-relay bulk-lease** の各コマンドがこの機能のために導入されました。

EIGRP for IPv6 の実装

カスタマーは、IPv6 プレフィクスをルーティングするように Enhanced Interior Gateway Routing Protocol（EIGRP）を設定できます。EIGRP IPv4 は IPv4 トランスポート上で動作し、IPv4 ピアとだけ通信したり、IPv4 ルートだけをアドバタイズしたりします。EIGRP for IPv6 はこれと同じモデルに従います。EIGRP for IPv4 と EIGRP for IPv6 は別々に設定および管理します。ただし、EIGRP for IPv4 と EIGRP for IPv6 の設定は似ているため、動作はわかりやすく、矛盾がありません。

このマニュアルでは、EIGRP for IPv6 の設定と実装について説明します。

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「EIGRP for IPv6 の実装の機能情報」（P.20）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

EIGRP for IPv6 の実装の前提条件

- このマニュアルでは、EIGRP IPv4 に精通していることを前提としています。
- このマニュアルでは、IPv6 アドレッシングについての基本知識があることを前提としています。

EIGRP for IPv6 の実装の制約事項

ここでは、EIGRP for IPv6 と EIGRP IPv4 の違いおよび EIGRP for IPv6 の制約事項を示します。

- EIGRP for IPv6 は、それが実行されるインターフェイスに直接設定します。この機能により、グローバル IPv6 アドレスを使用しないで EIGRP for IPv6 を設定できます。EIGRP for IPv6 にはネットワーク文はありません。

  システム始動時のインターフェイスごとの設定で、インターフェイスに EIGRP が設定されている場合は、EIGRP ルータ モード コマンドが実行される前に EIGRP プロトコルが実行を開始します。
- EIGRP for IPv6 プロトコル インスタンスが実行を開始するには、ルータ ID が必要です。
- EIGRP for IPv6 にはシャットダウン機能があります。実行を開始するには、ルーティング プロセスを「no shut」モードにする必要があります。
- passive-interface 設定を使用する場合、パッシブにするインターフェイスに EIGRP for IPv6 を設定する必要はありません。
- EIGRP for IPv6 では、**distribute-list prefix-list** コマンドを使用してルートをフィルタリングできます。配布リストによるルート フィルタリングでは、**route-map** コマンドの使用はサポートされません。

EIGRP for IPv6 の実装に関する情報

- 「Cisco EIGRP for IPv6 の実装」（P.2）

Cisco EIGRP for IPv6 の実装

EIGRP は、シスコが開発した IGRP の拡張バージョンです。EIGRP では、IGRP と同じ距離ベクトル型アルゴリズムや距離情報が使用されます。ただし、EIGRP のコンバージェンス特性と動作効率は、IGRP よりも大幅に改善されています。

コンバージェンス テクノロジーは、SRI International で実施された研究に基づいており、Diffusing Update Algorithm（DUAL; 拡散更新アルゴリズム）というアルゴリズムを採用しています。このアルゴリズムは、ルート計算中のどの時点でもループが発生しないようにし、トポロジ変更に関与するすべてのデバイスを同時に同期できるようにします。トポロジ変更の影響を受けないルータは、再計算に含まれません。DUAL によるコンバージェンス時間は、他の既存のルーティング アルゴリズムのコンバージェンス時間に匹敵します。

EIGRP には次の機能があります。

- ネットワーク幅の拡大：Routing Information Protocol（RIP; ルーティング情報プロトコル）では、ネットワークの最大可能幅は 15 ホップです。EIGRP をイネーブルにすると、最大可能幅は 224 ホップになります。EIGRP メトリックは数千のホップをサポートできるほど大きいため、ネットワークの拡大の障害となるのは、トランスポート レイヤのホップ カウンタだけです。シスコでは、この制限を回避するために、IPv4 または IPv6 パケットが 15 台のルータを通過し、宛先へのネク

ストホップが EIGRP によって学習された場合にだけトランスポート制御フィールドを増やします。RIP ルートが宛先へのネクストホップとして使用される場合、トランスポート制御フィールドは通常どおりに増加します。

- 高速コンバージェンス：DUAL アルゴリズムにより、他のルーティング プロトコルと同じくらいすばやくルーティング情報をコンバージできます。
- 部分アップデート：宛先の状態が変化した場合、EIGRP は、ルーティング テーブルの内容全体を送信するのではなく、差分アップデートを送信します。この機能により、EIGRP パケットに必要な帯域幅が最小限に抑えられます。
- ネイバー探索メカニズム：ネイバー ルータの学習に使用される簡単な hello メカニズムです。この機能はプロトコルに依存しません。
- 任意のルート集約。
- スケーリング：EIGRP は大規模なネットワークに合わせて拡張します。
- ルート フィルタリング：EIGRP for IPv6 では、**distribute-list prefix-list** コマンドを使用してルートをフィルタリングできます。配布リストによるルート フィルタリングでは、**route-map** コマンドの使用はサポートされません。

EIGRP には、次の 4 つの基本コンポーネントがあります。

- ネイバー探索：直接接続されたネットワーク上の他のルータをダイナミックに学習するために、ルータによって使用されるプロセスです。ルータは、ネイバーが到達不能または動作不能になったことも検出する必要があります。EIGRP ネイバー探索では、小さな hello パケットを定期的に送信するため、オーバーヘッドが低く抑えられます。回復したネイバーは hello パケットを送信するため、EIGRP ネイバーは、停止後に回復したネイバーを検出することもできます。hello パケットを受信するかぎり、Cisco IOS ソフトウェアはネイバーがアライブ状態で動作していることを確認できます。このステータスが確認されると、ネイバー ルータはルーティング情報を交換できます。

（注） Cisco IOS Release 12.2(33)SRD では、EIGRP IPv6 ルータ プロセスをイネーブルにする場合、**no shut** コマンドを明示的に設定する必要があります。**no shut** コマンドが設定されていない場合、IPv6 EIGRP ネイバーは失われます。

- 信頼性の高いトランスポート プロトコル：信頼性の高いトランスポート プロトコルでは、EIGRP パケットがすべてのネイバーに順序正しく確実に配布されます。マルチキャスト パケットとユニキャスト パケットが混在した伝送もサポートされます。EIGRP パケットには、確実に送信する必要があるものと、その必要がないものがあります。効率を高めるため、信頼性は必要な場合にだけ確保されます。たとえば、マルチキャスト機能（GigabitEthernet など）を持つマルチアクセス ネットワークでは、すべてのネイバーのそれぞれに hello パケットを確実に送信する必要はありません。そのため、EIGRP は、1 つのマルチキャスト hello を送信し、パケットに確認応答が必要ないという通知をそのパケットに含めます。その他のタイプのパケット（アップデートなど）には、確認応答が必要であり、そのことをパケットで示します。信頼性の高い転送では、確認応答のないパケットの保留中にすばやくマルチキャスト パケットを送信できます。これにより、速度が変化するリンクが存在する場合でも短いコンバージェンス時間を維持できます。
- DUAL 有限状態マシン：DUAL 有限状態マシンには、すべてのルート計算の決定プロセスが組み込まれています。すべてのネイバーによってアドバタイズされたすべてのルートをトラッキングします。DUAL では、距離情報やコスト情報などのいくつかのメトリックを使用して、効率的なループフリー パスを選択します。ネイバーへの複数のルートが存在する場合、DUAL は最小メトリック（到達可能距離と呼ばれる）のルートを特定し、このルートをルーティング テーブルに挿入します。このネイバーへの他のルートを受信し、そのメトリックの方が大きい場合、DUAL はこのネットワークへの報告距離を決定します。報告距離は、宛先へのパスのアップストリーム ネイバーによってアドバタイズされた合計メトリックとして定義されます。DUAL は、報告距離を到達可能距離と比較し、報告距離が到達可能距離よりも小さい場合、そのルートを到達可能後継

ルートと見なしてトポロジ テーブルに挿入します。現在のルートで障害が発生した場合、メトリックが最小である到達可能後継ルータのルートが現在のルートの後継ルートになります。ルーティングのループを回避するために、DUAL では、報告距離が常に到達可能距離よりも小さいことを確認し、ネイバー ルータが宛先ネットワークに到達できるようにします。それ以外の場合、ネイバーへのルートはローカル ルータにループバックする可能性があります。

- プロトコル依存モジュール：障害が発生したルートへの到達可能後継ルータが存在せず、ルートをアドバタイズするネイバーが存在する場合は、再計算が必要になります。このプロセスによって、DUAL は新しい後継ルータを決定します。ルートの再計算に必要な時間は、コンバージェンス時間に影響します。再計算は、プロセッサに高い負荷を与えます。したがって、不要な再計算を行わないことを推奨します。トポロジが変更されると、DUAL は到達可能後継ルータをテストします。到達可能後継ルータがある場合、DUAL は不要な再計算を行わないためにそれらのルータを使用します。

  プロトコル依存モジュールは、ネットワーク レイヤ プロトコル固有のタスクを実行します。たとえば、EIGRP モジュールは、IPv4 または IPv6 でカプセル化された EIGRP パケットを送受信します。また、EIGRP パケットを解析したり、DUAL に受信した新しい情報を通知したりします。EIGRP は、DUAL にルーティングの決定を要求しますが、その結果は IPv4 または IPv6 ルーティングに格納されます。さらに、EIGRP は、他の IPv4 または IPv6 ルーティング プロトコルによって学習されたルートを再配布します。

EIGRP for IPv6 の実装方法

インターフェイスに対する EIGRP for IPv6 のイネーブル化

指定したインターフェイスの EIGRP for IPv6 をイネーブルにするには、次の作業を実行します。EIGRP for IPv6 は、それが実行されるインターフェイスに直接設定します。これにより、グローバル IPv6 アドレスを使用しないで EIGRP for IPv6 を設定できます。

手順の概要

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

4. **interface** *type number*
5. **ipv6 enable**
6. **ipv6 eigrp** *as-number*
7. **ipv6 router eigrp** *as-number*
8. **eigrp router-id** *ip-address*
9. **exit**
10. **show ipv6 eigrp** [*as-number*] **interfaces** [*type number*] [**detail**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 unicast-routing** **例：** `Router(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。
ステップ 4	**interface** *type number* **例：** `Router(config)# interface FastEthernet 0/0`	EIGRP を設定するインターフェイスを指定します。
ステップ 5	**ipv6 enable** **例：** `Router(config-if)# ipv6 enable`	明示的な IPv6 アドレスが設定されていないインターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 6	**ipv6 eigrp** *as-number* **例：** `Router(config-if)# ipv6 eigrp 1`	指定したインターフェイスに対して、EIGRP for IPv6 をイネーブルにします。
ステップ 7	**ipv6 router eigrp** *as-number* **例：** `Router(config-if)# ipv6 router eigrp 1`	ルータ コンフィギュレーション モードを開始し、EIGRP IPv6 ルーティング プロセスを作成します。
ステップ 8	**eigrp router-id** *ip-address* **例：** `Router(config-router)# eigrp router-id 10.1.1.1`	固定ルータ ID の使用をイネーブルにします。 このコマンドは、ルータ ID を設定するルータで IPv4 アドレスが定義されていない場合だけ使用します。

	コマンドまたはアクション	目的
ステップ 9	**exit** **例：** `Router(config-router) exit`	3 回入力して特権 EXEC モードに戻ります。
ステップ 10	**show ipv6 eigrp** [*as-number*] **interfaces** [*type number*] [**detail**] **例：** `Router# show ipv6 eigrp interfaces`	EIGRP for IPv6 用に設定されたインターフェイスに関する情報を表示します。

EIGRP によるリンク帯域幅の使用率の設定

デフォルトでは、EIGRP パケットはリンク帯域幅の最大 50% を使用します。この値は、**bandwidth interface** コマンドで設定されます。異なるレベルのリンク使用率が必要な場合、または設定されている帯域幅が実際のリンク帯域幅と一致しない場合は（ルート メトリックの計算に影響するように設定されている場合があります）、この値を変更できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 bandwidth-percent eigrp** *as-number percent*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface FastEthernet 0/0`	EIGRP を設定するインターフェイスを指定します。
ステップ 4	**ipv6 bandwidth-percent eigrp** *as-number percent* **例：** `Router(config-if)# ipv6 bandwidth-percent eigrp 1 75`	インターフェイスで EIGRP for IPv6 が使用できる帯域幅の割合を設定します。

サマリー アドレスの設定

指定したインターフェイスのサマリー アドレスを設定するには、次の作業を実行します。より限定されたルートがルーティング テーブルにある場合、EIGRP for IPv6 はそれらのすべてのルートの最小値に等しいメトリックを持つインターフェイスからサマリー アドレスをアドバタイズします。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 summary-address eigrp** *as-number ipv6-address* [*admin-distance*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface FastEthernet 0/0`	EIGRP を設定するインターフェイスを指定します。
ステップ 4	**ipv6 summary-address eigrp** *as-number ipv6-address* [*admin-distance*] **例：** `Router(config-if)# ipv6 summary-address eigrp 1 2001:0DB8:0:1::/64`	指定されたインターフェイスのサマリー集約アドレスを設定します。

EIGRP ルート認証の設定

EIGRP ルート認証では、EIGRP ルーティング プロトコルからのルーティング アップデートについて Message Digest Algorithm 5（MD5）認証を実行します。各 EIGRP パケット内の MD5 キー付きダイジェストによって、承認されていない送信元からの未認証のルーティング メッセージや不正なルーティング メッセージの送信を防止します。

各キーには、ローカルに格納される独自のキー識別子があります。キー識別子とメッセージに関連付けられたインターフェイスの組み合せによって、使用中の認証アルゴリズムと MD5 認証キーが一意に識別されます。

複数のキーにライフタイムを設定できます。存在する有効なキーの数にかかわらず、送信される認証パケットは 1 つだけです。最小の番号から順にキー番号が調べられ、最初に見つかった有効なキーが使用されます。ルータは時刻を把握する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 authentication mode eigrp** *as-number* **md5**
5. **ipv6 authentication key-chain eigrp** *as-number key-chain*
6. **exit**
7. **key chain** *name-of-chain*
8. **key** *key-id*
9. **key-string** *text*
10. **accept-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}
11. **send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface FastEthernet 0/0`	EIGRP を設定するインターフェイスを指定します。
ステップ 4	**ipv6 authentication mode eigrp** *as-number* **md5** **例：** `Router(config-if)# ipv6 authentication mode eigrp 1 md5`	EIGRP for IPv6 パケットで使用する認証タイプを指定します。
ステップ 5	**ipv6 authentication key-chain eigrp** *as-number key-chain* **例：** `Router(config-if)# ipv6 authentication key-chain eigrp 1 chain1`	EIGRP for IPv6 パケットの認証をイネーブルにします。
ステップ 6	**exit** **例：** `Router(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**key chain** *name-of-chain* **例：** `Router(config)# key chain chain1`	認証キーのグループを指定します。 • 手順 5 で指定した名前を使用します。

	コマンドまたはアクション	目的
ステップ 8	**key** *key-id* **例：** `Router(config-keychain)# key 1`	キー チェーンの認証キーを識別します。
ステップ 9	**key-string** *text* **例：** `Router(config-keychain-key)# key-string chain 1`	キーの認証文字列を指定します。
ステップ 10	**accept-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*} **例：** `Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 10 2006 duration 7200`	キー チェーンの認証キーが有効として受信される期間を設定します。
ステップ 11	**send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*} **例：** `Router(config-keychain-key)# send-lifetime 15:00:00 Jan 10 2006 duration 3600`	キー チェーンの認証キーが有効に送信される期間を設定します。

EIGRP のネクストホップの上書き

デフォルトでは、EIGRP は、ルートを学習したインターフェイスと同じインターフェイス上でルートをアドバタイズする場合も、アドバタイズするルートの IPv6 ネクストホップ値として自身を設定します。このデフォルトを変更するには、次の作業を実行して、ルートのアドバタイズ時に受信したネクストホップ値を使用するように EIGRP に指示します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no ipv6 next-hop-self eigrp** *as-number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* **例：** `Router(config)# interface FastEthernet 0/0`	EIGRP を設定するインターフェイスを指定します。
ステップ 4	**no ipv6 next-hop-self eigrp** *as-number* **例：** `Router(config-if)# no ipv6 next-hop-self eigrp 1`	デフォルトの IPv6 ネクストホップ値を変更し、受信したネクストホップ値を使用するように EIGRP に指示します。

EIGRP for IPv6 における Hello パケットの間隔の調整

ルーティング デバイスは、定期的に hello パケットを相互に送信して、直接接続されたネットワーク上の他のルータをダイナミックに学習します。この情報は、ネイバーを検出したり、ネイバーが到達不能または動作不能になったことを学習したりするために使用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 hello-interval eigrp** *as-number seconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface FastEthernet 0/0`	EIGRP を設定するインターフェイスを指定します。
ステップ 4	**ipv6 hello-interval eigrp** *as-number seconds* **例：** `Router(config)# ipv6 hello-interval eigrp 1 10`	自律システム番号によって指定された EIGRP for IPv6 ルーティング プロセスの hello 間隔を設定します。

EIGRP for IPv6 における保留時間の調整

非常に輻輳した大規模なネットワークでは、デフォルトの保留時間では、全ルータがネイバーから hello パケットを受信するまでに十分な時間がない場合もあります。この場合、ホールド タイムを増やすこともできます。

自律システム番号によって指定された特定の EIGRP ルーティング プロセスの保留時間を、指定したインターフェイスに対して設定できます。保留時間は、hello パケットでアドバタイズされ、送信元を有効と見なす時間の長さをネイバーに示します。デフォルトの保留時間は、hello 間隔の 3 倍または 15 秒です。低速の NonBroadcast MultiAccess（NBMA; 非ブロードキャスト マルチアクセス）ネットワークでは、デフォルトの保留時間は 180 秒です。hello 間隔の値を変更した場合は、保留時間を変更する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 hold-time eigrp** *as-number seconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface FastEthernet 0/0`	EIGRP を設定するインターフェイスを指定します。
ステップ 4	**ipv6 hold-time eigrp** *as-number seconds* **例：** `Router(config)# ipv6 hold-time eigrp 1 40`	自律システム番号によって指定された特定の EIGRP for IPv6 ルーティング プロセスの保留時間を設定します。

EIGRP for IPv6 におけるスプリット ホライズンのディセーブル化

スプリット ホライズンは、EIGRP のアップデート パケットとクエリー パケットの送信を制御します。スプリット ホライズンがインターフェイスでイネーブルになっている場合、アップデート パケットとクエリー パケットは、このインターフェイスがネクスト ホップである宛先に送信されません。この方法でアップデート パケットとクエリー パケットを制御すると、ルーティング ループが発生する可能性が低くなります。

デフォルトでは、スプリット ホライズンはすべてのインターフェイスでイネーブルになっています。

スプリット ホライズンは、ルート情報がルータによってその情報の送信元であるインターフェイスからアドバタイズされるのを防ぎます。通常、特にリンクが切断された場合には、この動作によって複数のルーティング デバイス間の通信が最適化されます。ただし、非ブロードキャスト ネットワーク（マルチポイント GRE など）では、この動作が適切ではない状況が発生する場合があります。このような状況では（EIGRP が設定されているネットワークなど）、スプリット ホライズンをディセーブルにすることもできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no ipv6 split-horizon eigrp** *as-number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface FastEthernet 0/0`	EIGRP を設定するインターフェイスを指定します。
ステップ 4	**no ipv6 split-horizon eigrp** *as-number* **例：** `Router(config-if)# no ipv6 split-horizon eigrp 101`	指定したインターフェイスの EIGRP for IPv6 スプリット ホライズンをディセーブルにします。

ネットワークの安定性を向上させる EIGRP スタブ ルーティングの設定

EIGRP スタブ ルーティング機能は、ネットワークの安定性の向上に役立ちます。ネットワークが不安定になったときに、EIGRP クエリーが非中継ルータへの制限された帯域幅リンクを介して送信されるのを防ぎます。代わりに、スタブ ルータの接続先の分散型ルータがスタブ ルータに代わってクエリーに応答します。この機能により、輻輳している、または問題のある WAN リンクによってネットワークが不安定になる可能性が低減されます。また、EIGRP スタブ ルーティング機能を使用すると、ハブアンドスポーク ネットワークの設定とメンテナンスが簡略化されます。スタブ ルーティングをデュアルホーム接続のリモート設定でイネーブルにすると、リモート ルータがハブ ルータへの中継パスとして表示されないようにリモート ルータでフィルタリングを設定する必要がなくなります。

注意 EIGRP スタブ ルーティングは、スタブ ルータ上でだけ使用してください。スタブ ルータは、コア中継トラフィックが通過しないネットワーク コアまたは分散型レイヤに接続されたルータとして定義されます。スタブ ルータが分散型ルータ以外の EIGRP ネイバーを持つことはできません。

- 「EIGRP スタブ ルーティング用のルータの設定」（P.13）
- 「EIGRP スタブ ルーティングの確認」（P.13）

EIGRP スタブ ルーティング用のルータの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router eigrp** *as-number*
4. **eigrp stub** [**receive-only** | **leak-map** | **connected** | **static** | **summary** | **redistributed**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 router eigrp** *as-number* **例：** `Router(config)# ipv6 router eigrp 1`	設定する EIGRP for IPv6 ルーティング プロセスを指定します。
ステップ 4	**eigrp stub** [**receive-only** | **leak-map** | **connected** | **static** | **summary** | **redistributed**] **例：** `Router(config-router)# eigrp stub`	ルータを EIGRP を使用するスタブとして設定します。

EIGRP スタブ ルーティングの確認

手順の概要

1. **enable**
2. **show ipv6 eigrp neighbors detail** [*interface-type* | *as-number* | **static**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**show ipv6 eigrp neighbors detail** [*interface-type* | *as-number* | **static**] **例：** `Router# show ipv6 eigrp neighbors detail`	EIGRP for IPv6 によって検出されたネイバーを表示します。 リモートのステータスを表示するには、このコマンドを分散型レイヤ ルータで実行します。

EIGRP for IPv6 ルーティング プロセスのカスタマイズ

特定のインターフェイスに対して EIGRP for IPv6 をイネーブルにしたら、EIGRP for IPv6 ルーティング プロセスを設定できます。次の任意の作業では、ニーズに合わせて EIGRP for IPv6 ルーティング プロセスを設定する方法を示します。

- 「EIGRP ネイバー ルータとの隣接関係の変更のロギング」（P.14）
- 「ネイバー警告の間隔の設定」（P.15）
- 「EIGRP for IPv6 メトリック ウェイトの調整」（P.16）

EIGRP ネイバー ルータとの隣接関係の変更のロギング

ルーティング システムの安定性を監視し、問題を検出しやすくするために、ネイバー ルータとの隣接関係の変更のロギングをイネーブルにすることができます。デフォルトでは、隣接関係の変更はロギングされます。このロギングを必要な場合にイネーブルにするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router eigrp** *as-number*
4. **eirgp log-neighbor-changes**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 router eigrp** *as-number* **例：** `Router(config)# ipv6 router eigrp 1`	設定する EIGRP for IPv6 ルーティング プロセスを指定します。
ステップ 4	**eigrp log-neighbor-changes** **例：** `Router(config-router)# eigrp log-neighbor-changes`	EIGRP for IPv6 ネイバー隣接関係の変更のロギングをイネーブルにします。

ネイバー警告の間隔の設定

ネイバー警告メッセージが発生した場合は、デフォルトでログに記録されます。ネイバー警告メッセージの間隔を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router eigrp** *as-number*
4. **eigrp log-neighbor-warnings** [*seconds*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 router eigrp** *as-number* **例：** `Router(config)# ipv6 router eigrp 1`	設定する EIGRP for IPv6 ルーティング プロセスを指定します。
ステップ 4	**eigrp log-neighbor-warnings** [*seconds*] **例：** `Router(config-router)# eigrp log-neighbor-warnings 300`	EIGRP ネイバー警告メッセージのロギング間隔を設定します。

EIGRP for IPv6 メトリック ウェイトの調整

EIGRP for IPv6 では、宛先ネットワークへのパスの最小帯域幅と遅延の合計を使用して、ルーティング メトリックを計算します。**metric weights** コマンドを使用すると、EIGRP for IPv6 ルーティングのデフォルト動作とメトリック計算を調整できます。EIGRP for IPv6 メトリックのデフォルトは、ほとんどのネットワークでパフォーマンスが最適になるように、慎重に選択されています。

（注） EIGRP メトリック ウェイトを調整すると、ネットワーク パフォーマンスに大きな影響を及ぼす可能性があります。この作業は複雑であるため、デフォルト値の変更は、経験豊富なネットワーク設計者からのアドバイスがある場合にかぎり行うことを推奨します。

デフォルトでは、EIGRP 複合メトリックは、特定のルートのセグメント遅延と（拡張およびインバートされた）最小セグメント帯域幅の合計である 32 ビットになります。同種メディアのネットワークでは、このメトリックは 1 ホップ カウントまで減少します。混合メディア（GigabitEthernet、FastEthernet、イーサネットなど）のネットワークでは、メトリックが最小のルートが宛先への最適なパスになります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router eigrp** *as-number*
4. **metric weights** *tos k1 k2 k3 k4 k5*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 router eigrp** *as-number* **例：** `Router(config)# ipv6 router eigrp 1`	設定する EIGRP for IPv6 ルーティング プロセスを指定します。
ステップ 4	**metric weights** *tos k1 k2 k3 k4 k5* **例：** `Router(config-router)# metric weights 0 2 0 2 0 0`	EIGRP メトリック計算を調整します。

EIGRP の監視および維持

• 「EIGRP for IPv6 ルーティング テーブルからのエントリの削除」（P.17）

EIGRP for IPv6 ルーティング テーブルからのエントリの削除

手順の概要

1. **enable**
2. **clear ipv6 eigrp** [*as-number*] [**neighbor** [*ipv6-address* | *interface-type interface-number*]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**clear ipv6 eigrp** [*as-number*] [**neighbor** [*ipv6-address* | *interface-type interface-number*]] **例：** `Router# clear ipv6 eigrp neighbor 3FEE:12E1:2AC1:EA32`	EIGRP for IPv6 ルーティング テーブルからエントリを削除します。 削除されるのは、指定したルータによって学習されたルートです。

EIGRP for IPv6 の実装の設定例

例：インターフェイス上での隣接関係を確立する EIGRP の設定

EIGRP for IPv6 は、それが実行されるインターフェイスに直接設定します。この例では、EIGRP for IPv6 で hello パケットを送信してイーサネット 0 上に隣接を確立するのに必要な最小限の設定を示します。

```
ipv6 unicast-routing
interface gigabitethernet0/0
  ipv6 enable
  ipv6 eigrp 1
  no shut
!
ipv6 router eigrp 1
  eigrp router-id 10.1.1.1
```

関連情報

他の IPv6 内部ゲートウェイ ルーティング プロトコルを実装する場合は、「*Implementing RIP for IPv6*」または「*Implementing IS-IS for IPv6*」の章を参照してください。外部ゲートウェイ ルーティング プロトコルの Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）を実装する場合は、「*Implementing Multiprotocol BGP for IPv6*」の章を参照してください。

その他の関連資料

関連資料

関連項目	参照先
IPv6 のサポート機能リスト	「*Start Here: Cisco IOS Software Release Specifics for IPv6 Features*」
IS-IS for IPv6 の実装	「*Implementing IS-IS for IPv6*」
マルチプロトコル BGP for IPv6 の実装	「*Implementing Multiprotocol BGP for IPv6*」
RIP for IPv6 の実装	「*Implementing RIP for IPv6*」
EIGRP for IPv4	『*Cisco IOS IP Routing Protocols Configuration Guide*』の「Configuring EIGRP」
EIGRP for IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
EIGRP for IPv4 コマンド	『*Cisco IOS IP Routing Protocols Command Reference*』の「EIGRP Commands」

規格

規格	タイトル
この機能によってサポートされる新しい規格または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によってサポートされる新しい RFC または変更された RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

EIGRP for IPv6 の実装の機能情報

表 1 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どのソフトウェア イメージが特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1　EIGRP for IPv6 の実装の機能情報

機能名	リリース	機能情報
IPv6 ルーティング - EIGRP サポート	12.4(6)T 12.2(33)SRB 12.2(33)SXI 15.0(1)S	カスタマーは、IPv6 プレフィクスをルーティングするように EIGRP を設定できます。EIGRP for IPv4 と EIGRP for IPv6 の間に関連はありません。これらは別々に設定および管理します。ただし、EIGRP for IPv4 と EIGRP for IPv6 の設定は似ているため、動作はわかりやすく、矛盾がありません。 この機能に関する詳細については、次の各項を参照してください。 • 「EIGRP for IPv6 の実装に関する情報」（P.2） • 「EIGRP for IPv6 の実装方法」（P.4） • 「EIGRP for IPv6 の実装の設定例」（P.17） この機能のために次のコマンドが導入または変更されました。**accept-lifetime**、**clear ipv6 eigrp**、**eirgp log-neighbor-changes**、**eigrp log-neighbor-warnings**、**eigrp router-id**、**eigrp stub**、**ipv6 authentication key-chain eigrp**、**ipv6 authentication mode eigrp**、**ipv6 bandwidth-percent eigrp**、**ipv6 eigrp**、**ipv6 hello-interval eigrp**、**ipv6 hold-time eigrp**、**ipv6 next-hop-self eigrp**、**ipv6 router eigrp**、**ipv6 split-horizon eigrp**、**ipv6 summary-address eigrp**、**ipv6 unicast-routing**、**key**、**key chain**、**key-string**、**metric weights**、**send-lifetime**、**show ipv6 eigrp**、**show ipv6 eigrp neighbors**

表 1　EIGRP for IPv6 の実装の機能情報 （続き）

機能名	リリース	機能情報
EIGRP IPv6 VRF-Lite	15.1(1)S	EIGRP IPv6 VRF-Lite 機能により、複数の VRF に対する EIGRP IPv6 サポートが提供されます。EIGRP for IPv6 は、VRF のコンテキスト内で動作します。EIGRP IPv6 VRF-Lite 機能では、ルーティングと転送が分離され、異なる VRF に属するデバイス間の通信は明示的に設定しなければ許可されないため、セキュリティが強化されます。EIGRP IPv6 VRF-Lite 機能により、特定の VRF に属しているトラフィックの管理とトラブルシューティングが簡素化されます。 EIGRP IPv6 VRF-Lite 機能は、EIGRP 名前付きコンフィギュレーションでのみ使用できます。 この機能により、新規追加または変更されたコマンドはありません。

IPv6 における First Hop Redundancy Protocol の設定

IPv6 ルーティング プロトコルは、ルータ間の復元力とフェールオーバーを提供します。ただし、ホストとファーストホップ ルータ間のパスで障害が発生した場合、またはファーストホップ ルータで障害が発生した場合は、First Hop Redundancy Protocol（FHRP）によってホストとルータ間の復元力とフェールオーバーが確保されます。

Gateway Load Balancing Protocol（GLBP; ゲートウェイ ロード バランシング プロトコル）FHRP は、障害が発生したルータまたは回線からデータ トラフィックを保護し、冗長ルータ間でパケットのロード シェアリングを実行できるようにします。Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）は、ゲートウェイで障害が発生した場合にデータ トラフィックを保護します。

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「IPv6 における First Hop Redundancy Protocol の機能情報」（P.28）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

IPv6 における First Hop Redundancy Protocol の前提条件

- GLBP を設定する前に、ルータが物理インターフェイス上の複数の MAC アドレスをサポートできることを確認してください。設定される GLBP フォワーダごとに、追加の MAC アドレスが使用されます。
- GLBP が設定されたインターフェイスでは、スタティック リンクローカル アドレッシングを使用しないでください。
- HSRP IPv6 を設定する前に、インターフェイスに対して HSRP バージョン 2 をイネーブルにする必要があります。

IPv6 における First Hop Redundancy Protocol に関する情報

GLBP for IPv6

GLBP for IPv6 の概要

ゲートウェイ ロード バランシング プロトコル機能は、IEEE 802.3 LAN 上の 1 つのデフォルト ゲートウェイが設定された IPv6 ホストに対して自動ルータ バックアップを提供します。LAN 上にある複数のファーストホップ ルータの組み合せによって、1 つの仮想ファーストホップ IPv6 ルータが提供され、IPv6 パケット転送のロード シェアリングが実行されます。GLBP では、HSRP と同様のユーザ用機能を実行します。HSRP では、仮想 IPv6 アドレスが設定された仮想ルータ グループに複数のルータが参加できます。1 つのメンバがアクティブ ルータとして選択され、グループの仮想 IPv6 アドレスに送信されたパケットを転送します。グループ内の他のルータは、アクティブ ルータで障害が発生するまでは冗長ルータです。これらのスタンバイ ルータには、プロトコルによって使用されていない未使用帯

域幅があります。同じルータ セットに対して複数の仮想ルータ グループを設定できますが、ホストは異なるデフォルト ゲートウェイに対して設定する必要があります。その結果、管理上の負担が大きくなります。GLBP の利点は、1 つの仮想 IPv6 アドレスと複数の仮想 MAC アドレスを使用して、複数のルータ（ゲートウェイ）に対するロード バランシングが可能なことです。転送負荷は、GLBP グループ内のすべてのルータ間に分散されるため、単一のルータだけが処理して残りのルータがアイドルのままになるようなことはありません。各ホストに同じ仮想 IPv6 アドレスが設定され、仮想ルータ グループ内のすべてのルータがパケットの転送に関与します。

GLBP の利点

GLBP for IPv6 には、次の利点があります。

ロード シェアリング

LAN クライアントからのトラフィックを複数のルータに公平に分散するように GLBP を設定できます。

複数の仮想ルータ

GLBP では、ルータの各物理インターフェイス上に最大 1024 台の仮想ルータ（GLBP グループ）とグループごとに最大 4 つの仮想フォワーダがサポートされます。

プリエンプション

GLBP の冗長性スキームにより、使用可能になっているプライオリティの高いバックアップ仮想ゲートウェイをアクティブ仮想ゲートウェイにすることができます。フォワーダ プリエンプションも同じように機能しますが、フォワーダ プリエンプションはプライオリティの代わりに重み付けを使用し、デフォルトでイネーブルになっている点が異なります。

認証

業界標準の Message Digest Algorithm 5（MD5）アルゴリズムを使用して、信頼性、セキュリティ、および GLBP スプーフィング ソフトウェアからの保護を向上させることもできます。GLBP グループ内のルータの認証文字列が他のルータとは異なる場合、そのルータは他のグループ メンバによって無視されます。GLBP グループ メンバ間で簡単なテキスト パスワード認証方式を使用して、設定エラーを検出することもできます。

GLBP アクティブ仮想ゲートウェイ

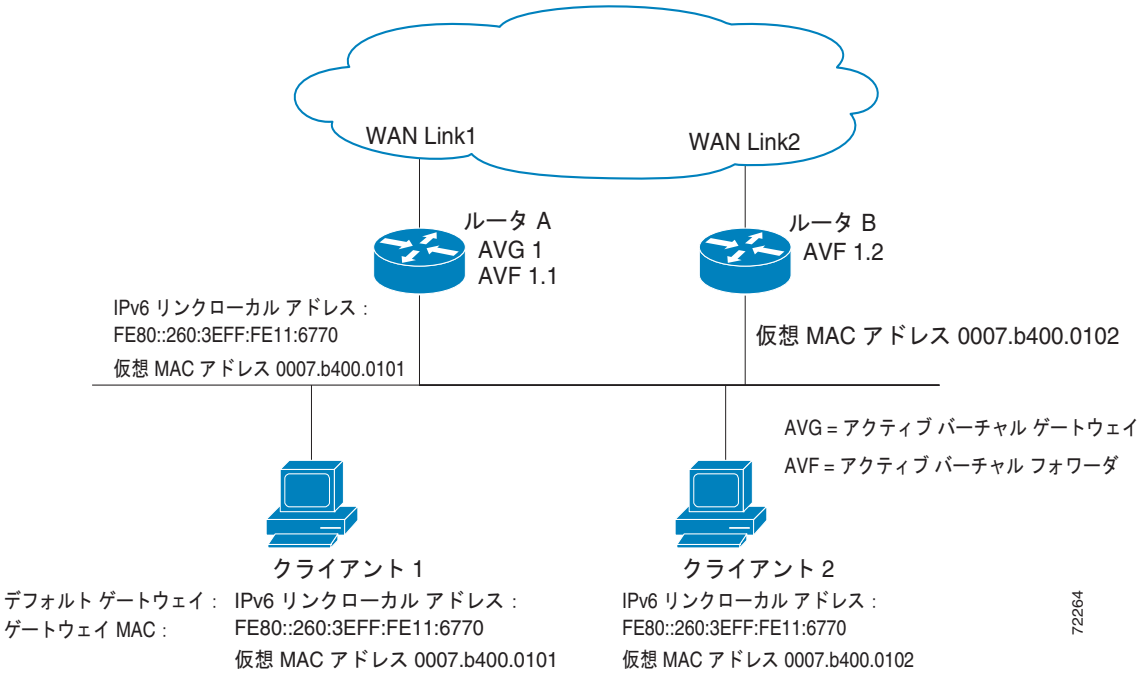
GLBP グループのメンバは、1 つのゲートウェイをそのグループの Active Virtual Gateway（AVG; アクティブ仮想ゲートウェイ）として選択します。他のグループ メンバは、AVG が使用できなくなった場合のバックアップとなります。AVG の機能は、仮想 MAC アドレスを GLBP グループの各メンバに割り当てることです。各ゲートウェイは、AVG によって割り当てられている仮想 MAC アドレスに送信されたパケットを転送する役割を引き継ぎます。これらのゲートウェイは、仮想 MAC アドレスの Active Virtual Forwarder（AVF; アクティブ仮想フォワーダ）と呼ばれます。

AVG は、仮想 IPv6 アドレスに対する Address Resolution Protocol（ARP; アドレス解決プロトコル）要求への応答も行います。ロード シェアリングは、AVG が異なる仮想 MAC で ARP 要求に応答することによって行われます。

図 1 では、ルータ A が GLBP グループの AVG であり、IPv6 リンクローカル アドレス FE80::260:3EFF:FE11:6770 を担当します。ルータ A は、仮想 MAC アドレス 0007.b400.0101 の AVF でもあります。ルータ B は同じ GLBP グループのメンバであり、仮想 MAC アドレス 0007.b400.0102 の AVF として指定されています。クライアント 1 には、デフォルト ゲートウェイ IPv6 アドレス

FE80::260:3EFF:FE11:6770 とゲートウェイ MAC アドレス 0007.b400.0101 が設定されています。クライアント 2 は、同じデフォルト ゲートウェイ IP アドレスを共有しますが、ルータ B がルータ A とトラフィック負荷を分担するため、ゲートウェイ MAC アドレス 0007.b400.0102 が与えられます。

図 1　　GLBP トポロジ



ルータ A が使用できなくなった場合でも、クライアント 1 は WAN にアクセスできます。これは、ルータ B がルータ A の仮想 MAC アドレスに送信されたパケットの転送を引き継ぎ、ルータ B 自身の仮想 MAC アドレスに送信されたパケットに応答するからです。ルータ B は、GLBP グループ全体の AVG の役割も引き継ぎます。GLBP メンバの通信は、GLBP グループ内のルータで障害が発生しても継続されます。

GLBP 仮想 MAC アドレスの割り当て

GLBP グループごとに最大 4 つの仮想 MAC アドレスを設定できます。AVG は、仮想 MAC アドレスをグループの各メンバに割り当てます。他のグループ メンバは、hello メッセージを通じて AVG を検出したあとで仮想 MAC アドレスを要求します。ゲートウェイには、シーケンスにおける次の MAC アドレスが割り当てられます。AVG によって仮想 MAC アドレスが割り当てられた仮想フォワーダは、プライマリ仮想フォワーダと呼ばれます。GLBP グループの他のメンバは、hello メッセージから仮想 MAC アドレスを学習します。仮想 MAC アドレスを学習した仮想フォワーダは、セカンダリ仮想フォワーダと呼ばれます。

GLBP 仮想ゲートウェイの冗長性

GLBP では、HSRP と同じ方法で仮想ゲートウェイの冗長性が実現されます。1 つのゲートウェイが AVG として選択され、もう 1 つのゲートウェイがスタンバイ仮想ゲートウェイとして選択されます。残りのゲートウェイはリッスン状態になります。

AVG で障害が発生すると、スタンバイ仮想ゲートウェイが仮想 IPv6 アドレスの役割を引き継ぎます。その後、リッスン状態のゲートウェイから新しいスタンバイ仮想ゲートウェイが選択されます。

GLBP 仮想フォワーダの冗長性

GLBP 仮想フォワーダの冗長性は、AVF による仮想ゲートウェイの冗長性と似ています。AVF で障害が発生すると、リッスン状態のセカンダリ 仮想フォワーダの 1 つが仮想 MAC アドレスの役割を引き継ぎます。

新しい AVF は、別のフォワーダ番号のプライマリ仮想フォワーダでもあります。GLBP は、ゲートウェイがアクティブ仮想フォワーダ状態に変わるとすぐに始動する 2 つのタイマーを使用して、古いフォワーダ番号からホストを移行します。GLBP は hello メッセージを使用してタイマーの現在の状態を通信します。

リダイレクト時間は、AVG がホストを古い仮想フォワーダ MAC アドレスにリダイレクトし続ける時間です。リダイレクト時間が経過すると、AVG は ARP 応答で古い仮想フォワーダの MAC アドレスを使用するのを中止しますが、仮想フォワーダは古い仮想フォワーダの MAC アドレスに送信されたパケットの転送を続行します。

セカンダリ保留時間は、仮想フォワーダが有効である時間です。セカンダリ保留時間を経過すると、仮想フォワーダは GLBP グループ内のすべてのゲートウェイから削除されます。期限切れになった仮想フォワーダ番号は、AVG による再割り当てが可能になります。

GLBP ゲートウェイのプライオリティ

GLBP ゲートウェイのプライオリティによって、各 GLBP ゲートウェイの役割と AVG で障害が発生した場合の結果が決まります。

また、GLBP ルータがバックアップ仮想ゲートウェイとして機能するかどうか、および現在の AVG で障害が発生した場合に AVG になる順番も決まります。各バックアップ仮想ゲートウェイのプライオリティには、**glbp priority** コマンドを使用して 1 ～ 255 の値を設定できます。

図 1 では、LAN トポロジ内の AVG であるルータ A で障害が発生すると、選択プロセスが実行され、処理を引き継ぐバックアップ仮想ゲートウェイが決定されます。この例では、ルータ B がグループ内の唯一の他のメンバであるため、ルータ B が自動的に新しい AVG になります。同じ GLBP グループ内にプライオリティの高い別のルータが存在していた場合は、そのプライオリティの高いルータが選択されます。両方のルータでプライオリティが同じ場合は、高い方の IPv6 アドレスを持つバックアップ仮想ゲートウェイがアクティブ仮想ゲートウェイとして選択されます。

デフォルトでは、GLBP 仮想ゲートウェイのプリエンプティブ方式はディセーブルになっています。バックアップ仮想ゲートウェイが AVG になるのは、仮想ゲートウェイに割り当てられているプライオリティにかかわらず、現在の AVG で障害が発生した場合だけです。**glbp preempt** コマンドを使用すると、GLBP 仮想ゲートウェイのプリエンプティブ方式をイネーブルにすることができます。プリエンプションを使用すると、バックアップ仮想ゲートウェイに現在の AVG よりも高いプライオリティが割り当てられている場合に、そのバックアップ仮想ゲートウェイを AVG にすることができます。

GLBP ゲートウェイの重み付けとトラッキング

GLBP では、重み付けによって GLBP グループ内の各ルータの転送容量を決定します。GLBP グループ内のルータに割り当てられた重み付けを使用して、そのルータがパケットを転送するかどうか、転送する場合はパケットを転送する LAN 内のホストの比率を決定できます。しきい値を設定すると、重み付けが特定の値を下回ったときに転送をディセーブルにすることができます。重み付けがもう一方のしきい値を上回ると、転送は自動的に再びイネーブルになります。

GLBP グループの重み付けは、ルータ内のインターフェイス状態のトラッキングによって自動的に調整できます。追跡対象のインターフェイスがダウンした場合、GLBP グループの重み付けは指定された値だけ小さくなります。GLBP の重み付けの減少値は、追跡対象のインターフェイスごとに変えることができます。

デフォルトでは、GLBP 仮想フォワーダのプリエンプティブ方式はイネーブルになっており、遅延は 30 秒です。現在の AVF の重み付けが下限しきい値を下回り、その状態で 30 秒経過すると、バックアップ仮想フォワーダが AVF になります。GLBP フォワーダのプリエンプティブ方式をディセーブルにするには **no glbp forwarder preempt** コマンドを使用し、遅延を変更するには **glbp forwarder preempt delay minimum** コマンドを使用します。

HSRP for IPv6

HSRP for IPv6 の概要

HSRP 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 FHRP です。デフォルト ゲートウェイの IP アドレスが設定されたイーサネット上の IP ホストにファーストホップのルーティング冗長性を確保することによって、高いネットワーク アベイラビリティを提供します。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。ルータ インターフェイスのグループ内では、アクティブ ルータはパケットをルーティングするルータです。スタンバイ ルータは、アクティブ ルータで障害が発生した場合、またはプリセットされた条件が満たされた場合に処理を引き継ぐルータです。

IPv6 ホストは、IPv6 ネイバー探索の RA メッセージを通じて使用可能な IPv6 ルータを学習します。これらのメッセージは定期的にマルチキャストされるか、またはホストによって請求されることもあります。HSRP は、IPv6 ホストに仮想ファースト ホップだけを提供するように設計されています。

HSRP IPv6 グループには、HSRP グループ番号に基づく仮想 MAC アドレスと、デフォルトでは HSRP 仮想 MAC アドレスに基づく仮想 IPv6 リンクローカル アドレスが割り当てられます。HSRP グループがアクティブな場合、定期的な RA が HSRP 仮想 IPv6 リンクローカル アドレス宛てに送信されます。これらの RA は、グループがアクティブ状態ではなくなるときに最後の RA が送信されると停止します。

インターフェイスのリンクローカル アドレスに対する定期的な RA は、少なくとも 1 つの仮想 IPv6 リンクローカル アドレスがインターフェイスに設定されているときに最後の RA が送信されると停止します。インターフェイスの IPv6 リンクローカル アドレスには、RA について説明したこと以外に制約事項はありません。他のプロトコルは、このアドレスへのパケットを送受信し続けます。

HSRP では、プライオリティ メカニズムを使用して、デフォルトのアクティブ ルータにする HSRP 設定済みルータを決定します。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 IPv6 仮想 MAC アドレスの範囲

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

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

HSRP IPv6 UDP ポート番号

HSRP IPv6 には、ポート番号 2029 が割り当てられています。

HSRP グローバル IPv6 アドレス

HSRP グローバル IPv6 アドレス機能では、ユーザが複数の非リンク ローカル アドレスを仮想アドレスとして設定できます。また、既存のプライマリ リンクローカル アドレスに加えて、複数のグローバル IPv6 仮想アドレスを保管し、管理できます。IPv6 アドレスを使用する場合、そのアドレスに IPv6 プレフィクス長を含める必要があります。リンクローカル アドレスを使用する場合は、プレフィクスを与えてはいけません。

図 2 に、HSRP IPv6 グローバル仮想インターフェイスを使用した展開シナリオを示します。

図 2　　HSRP 展開シナリオ

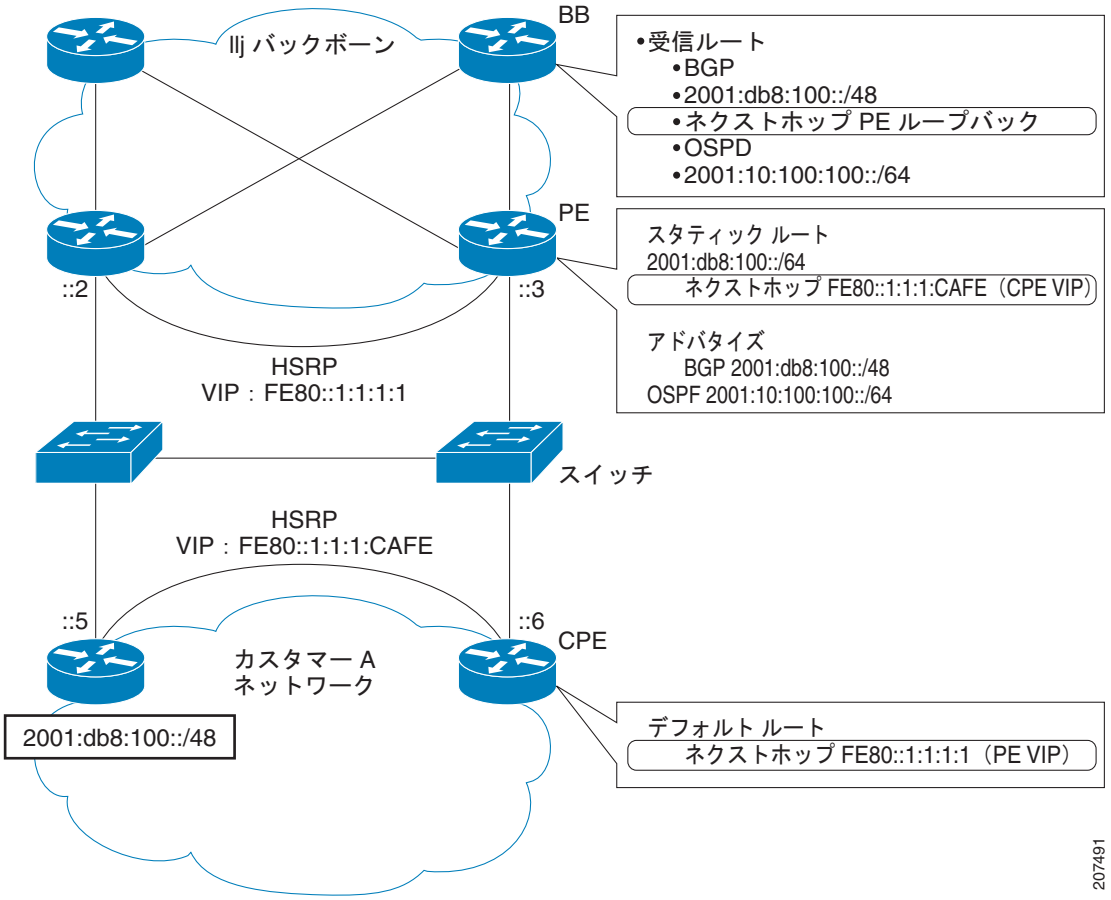


図 2 の場合、Provider Equipment（PE）ルータは、バックボーン ルータから Customer Premises Equipment（CPE; 宅内装置）に到達するためのルートを挿入する必要があります。2 台の CPE が存在するため、HSRP を使用すると便利です。スタティック ルートは、リンクローカル ネクスト ホップ（FE80::1:1:1:CAFE）で設定されます。リンクローカル アドレスはレイヤ 2 ローカル LAN 空間内のスコープしか持たないため、このアドレスがバックボーンに挿入されても、リンクローカル ネクスト ホップのままではこのルートは役に立ちません。この問題に対処するには、バックボーン ルータがパケットを PE ルータにルーティングできるように、仮想アドレスへのスタティック ルートのネクスト

ホップを非リンクローカル アドレスに設定する必要があります。ネクストホップのアドレス解決時、アクティブ HSRP グループ メンバが、非リンクローカル アドレスへ送信された Neighbor Solicitation（NS; ネイバー請求）メッセージに応答します。

IPv6 における First Hop Redundancy Protocol の設定方法

GLBP の設定とカスタマイズ

GLBP 動作のカスタマイズは任意です。GLBP 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。GLBP グループをイネーブルにしてから GLBP をカスタマイズすると、機能のカスタマイズを完了する前にルータがグループの制御を引き継ぎ、AVG になる可能性があります。したがって、GLBP をカスタマイズする場合は、GLBP をイネーブルにする前に行うことを推奨します。

ここでは、次の任意の手順について説明します。

GLBP のカスタマイズ

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 address** {*ipv6-global-address* | *prefix-name ipv6-prefix/prefix-length* | **autoconfig** [*default-route*]}
5. **glbp** *group* **timers** [**msec**] *hellotime* [**msec**] *holdtime*
6. **glbp** *group* **timers redirect** *redirect timeout*
7. **glbp** *group* **load-balancing** [**host-dependent** | **round-robin** | **weighted**]
8. **glbp** *group* **priority** *level*
9. **glbp** *group* **preempt** [**delay minimum** *seconds*]
10. **glbp** *group* **name** *redundancy-name*
11. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface fastethernet 0/0`	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name ipv6-prefix*/*prefix-length* | **autoconfig** [*default-route*]} **例：** `Router(config-if)# ipv6 address 2001:0DB8:0:7272::72/64`	IPv6 の一般的なプレフィクスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 5	**glbp** *group* **timers** [**msec**] *hellotime* [**msec**] *holdtime* **例：** `Router(config-if)# glbp 10 timers 5 18`	GLBP グループ内の AVG によって連続的に送信される hello パケットの間隔を設定します。 • *holdtime* 引数には、hello パケット内の仮想ゲートウェイと仮想フォワーダの情報が無効と見なされるまでの時間を秒数で指定します。 • オプションの **msec** キーワードは、そのあとに続く引数がデフォルトの秒単位ではなくミリ秒単位であることを指定します。
ステップ 6	**glbp** *group* **timers redirect** *redirect timeout* **例：** `Router(config-if)# glbp 10 timers redirect 600 7200`	AVG がクライアントを AVF にリダイレクトし続ける時間を設定します。 • *timeout* 引数には、セカンダリ仮想フォワーダが無効になるまでの時間を秒数で指定します。
ステップ 7	**glbp** *group* **load-balancing** [**host-dependent** | **round-robin** | **weighted**] **例：** `Router(config-if)# glbp 10 load-balancing host-dependent`	GLBP AVG で使用するロード バランシングの方式を指定します。
ステップ 8	**glbp** *group* **priority** *level* **例：** `Router(config-if)# glbp 10 priority 254`	GLBP グループ内のゲートウェイのプライオリティ レベルを設定します。 • デフォルト値は 100 です。

	コマンドまたはアクション	目的
ステップ 9	**glbp** *group* **preempt** [**delay minimum** *seconds*] **例：** `Router(config-if)# glbp 10 preempt delay minimum 60`	ルータのプライオリティが現在の AVG よりも高い場合に、GLBP グループの AVG として処理を引き継ぐようにルータを設定します。 • このコマンドは、デフォルトでディセーブルになっています。 • オプションの **delay** キーワードと **minimum** キーワードおよび *seconds* 引数を使用して、AVG のプリエンプションが実行されるまでの最小遅延時間を秒数で指定します。
ステップ 10	**glbp** *group* **name** *redundancy-name* **例：** `Router(config-if)# glbp 10 name abcompany`	GLBP グループに名前を割り当てることによって、IPv6 冗長性をイネーブルにします。 • 冗長クライアントと GLBP グループを接続できるように、GLBP 冗長クライアントに同じ GLBP グループ名を設定する必要があります。
ステップ 11	**exit** **例：** `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、ルータをグローバル コンフィギュレーション モードに戻します。

GLBP 認証の設定

ここでは、GLBP 認証の設定作業について説明します。実行する作業は、認証にテキスト認証、簡単な MD5 キー ストリング、または MD5 キー チェーンのどの方法を使用するかによって異なります。

- 「キー ストリングを使用した GLBP MD5 認証の設定」（P.11）
- 「キー チェーンを使用した GLBP MD5 認証の設定」（P.12）
- 「GLBP テキスト認証の設定」（P.14）

GLBP MD5 認証の動作

GLBP MD5 認証を使用すると、別のプレーン テキスト認証方式よりもセキュリティを強化できます。MD5 認証では、各 GLBP グループ メンバが秘密キーを使用して、発信パケットに含まれるキー付き MD5 ハッシュを生成できます。着信パケットのキー付きハッシュが生成され、着信パケット内のハッシュが生成されたハッシュに一致しない場合、そのパケットは無視されます。

MD5 ハッシュのキーは、キー ストリングを使用して設定で直接指定するか、またはキー チェーンを使用して間接的に指定できます。

ルータは、GLBP グループに対する認証設定と異なる設定を持つルータからの着信 GLBP パケットを無視します。GLBP には、次の 3 つの認証方式があります。

- 認証なし
- プレーン テキスト認証
- MD5 認証

GLBP パケットは、次のいずれかの場合に拒否されます。

- 認証方式がルータと着信パケットで異なる。
- MD5 ダイジェストがルータと着信パケットで異なる。
- テキスト認証文字列がルータと着信パケットで異なる。

キー ストリングを使用した GLBP MD5 認証の設定

GLBP MD5 認証を設定すると、ルータをスプーフィング ソフトウェアから保護し、業界標準の MD5 アルゴリズムによって信頼性とセキュリティを向上できます。キー ストリングを使用した GLBP MD5 認証を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name ipv6-prefix*/*prefix-length* | **autoconfig** [*default-route*]}
5. **glbp** *group-number* **authentication md5 key-string** [**0** | **7**] *key*
6. **glbp** *group* **ipv6** [*ipv6-address* | **autoconfig**]
7. 通信する各ルータに対してステップ 1 ～ 6 を繰り返します。
8. **end**
9. **show glbp**

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface Ethernet 0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name ipv6-prefix*/*prefix-length* | **autoconfig** [*default-route*]} **例：** `Router(config-if)# ipv6 address 2001:0DB8:0:7272::72/64`	IPv6 の一般的なプレフィクスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。

	コマンド	目的
ステップ 5	**glbp** *group-number* **authentication md5 key-string** [**0** | **7**] *key* **例：** `Router(config-if)# glbp 1 authentication md5 key-string d00b4r987654321a`	GLBP MD5 認証の認証キーを設定します。 • コマンドとキー ストリングの文字数が 255 文字を超えないようにします。 • *key* 引数の前にキーワードを指定しないか、または **0** を指定した場合、キーは暗号化されません。 • **7** を指定すると、キーは暗号化されます。**service password-encryption** グローバル コンフィギュレーション コマンドがイネーブルになっている場合、key-string 認証キーは自動的に暗号化されます。
ステップ 6	**glbp** *group* **ipv6** [*ipv6-address* | **autoconfig**] **例：** `Router(config-if)# glbp 1 ipv6 FE80::260:3EFF:FE11:6770`	IPv6 の GLBP をイネーブルにします。
ステップ 7	通信する各ルータに対してステップ 1 ～ 6 を繰り返します。	—
ステップ 8	**end** **例：** `Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show glbp** **例：** `Router# show glbp`	（任意）GLBP の情報を表示します。 • このコマンドを使用して、設定を確認します。設定されている場合はキー ストリングと認証タイプが表示されます。

キー チェーンを使用した GLBP MD5 認証の設定

キー チェーンを使用した GLBP MD5 認証を設定するには、次の作業を実行します。キー チェーンを使用すると、キー チェーン設定に従って異なる時点で異なるキー ストリングを使用できます。GLBP は、適切なキー チェーンを照会して、指定されたキー チェーンの現在アクティブなキーとキー ID を取得します。

手順の概要

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *string*
6. **exit**
7. **exit**
8. **interface** *type number*
9. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name ipv6-prefix*/*prefix-length* | **autoconfig** [*default-route*]}

10. **glbp** *group-number* **authentication md5 key-chain** *name-of-chain*
11. **glbp** *group* **ipv6** [*ipv6-address* | **autoconfig**]
12. 通信する各ルータに対してステップ 1 ～ 11 を繰り返します。
13. **end**
14. **show glbp**
15. **show key chain**

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**key chain** *name-of-chain* **例：** `Router(config)# key chain glbp2`	ルーティング プロトコルの認証をイネーブルにし、認証キーのグループを識別します。
ステップ 4	**key** *key-id* **例：** `Router(config-keychain)# key 100`	キー チェーンの認証キーを識別します。 • *key-id* は数字である必要があります。
ステップ 5	**key-string** *string* **例：** `Router(config-keychain-key)# key-string string1`	キーの認証文字列を指定します。 • *string* は、1 ～ 80 文字の大文字または小文字の英数字である必要があります。最初の文字には数字を使用できません。
ステップ 6	**exit** **例：** `Router(config-keychain-key)# exit`	キーチェーン コンフィギュレーション モードに戻ります。
ステップ 7	**exit** **例：** `Router(config-keychain)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**interface** *type number* **例：** `Router(config)# interface Ethernet 0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 9	**ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name ipv6-prefix*/*prefix-length* | **autoconfig** [*default-route*]} **例：** `Router(config-if)# ipv6 address 2001:0DB8:0:7272::72/64`	IPv6 の一般的なプレフィクスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 10	**glbp** *group-number* **authentication md5 key-chain** *name-of-chain* **例：** `Router(config-if)# glbp 1 authentication md5 key-chain glbp2`	GLBP MD5 認証の認証 MD5 キー チェーンを設定します。 • キー チェーン名は、ステップ 3 で指定した名前に一致する必要があります。
ステップ 11	**glbp** *group* **ipv6** [*ipv6-address* | **autoconfig**] **例：** `Router(config-if)# glbp 1 ipv6 FE80::E0:F727:E400:A`	IPv6 の GLBP をイネーブルにします。
ステップ 12	通信する各ルータに対してステップ 1 ～ 11 を繰り返します。	—
ステップ 13	**end** **例：** `Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 14	**show glbp** **例：** `Router# show glbp`	（任意）GLBP の情報を表示します。 • このコマンドを使用して、設定を確認します。設定されている場合はキー チェーンと認証タイプが表示されます。
ステップ 15	**show key chain** **例：** `Router# show key chain`	（任意）認証キー情報を表示します。

GLBP テキスト認証の設定

GLBP テキスト認証を設定するには、次の作業を実行します。この認証方式では、最小限のセキュリティが確保されます。セキュリティが必須の場合は、MD5 認証を使用してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name ipv6-prefix*/*prefix-length* | **autoconfig** [*default-route*]}
5. **glbp** *group-number* **authentication text** *string*
6. **glbp** *group* **ipv6** [*ipv6-address* | **autoconfig**]
7. 通信する各ルータに対してステップ 1 ～ 6 を繰り返します。
8. **end**

9. **show glbp**

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface Ethernet 0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name ipv6-prefix*/*prefix-length* | **autoconfig** [*default-route*]} **例：** `Router(config-if)# ipv6 address 2001:0DB8:0:7272::72/64`	IPv6 の一般的なプレフィクスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 5	**glbp** *group-number* **authentication text** *string* **例：** `Router(config-if)# glbp 10 authentication text stringxyz`	グループ内の他のルータから受信した GLBP パケットを認証します。 • 認証を設定する場合は、GLBP グループ内のすべてのルータで同じ認証文字列を使用する必要があります。
ステップ 6	**glbp** *group* **ipv6** [*ipv6-address* | **autoconfig**] **例：** `Router(config-if)# glbp 1 ipv6 FE80::60:3E47:AC8:8`	IPv6 の GLBP をイネーブルにします。
ステップ 7	通信する各ルータに対してステップ 1 ～ 6 を繰り返します。	—
ステップ 8	**end** **例：** `Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show glbp** **例：** `Router# show glbp`	（任意）GLBP の情報を表示します。 • このコマンドを使用して、設定を確認します。

GLBP の重み付けの値とオブジェクト トラッキング

GLBP の重み付けは、ルータを仮想フォワーダとして動作できるようにするかどうかを決定するために使用します。重み付けの初期値を設定したり、オプションのしきい値を指定したりできます。インターフェイスの状態を追跡し、インターフェイスがダウンした場合に重み付けの値を減らすための減少値を

設定できます。GLBP ルータの重み付けが指定した値を下回ると、ルータはアクティブ仮想フォワーダではなくなります。重み付けが指定した値を上回ると、ルータはアクティブ仮想フォワーダとしての役割を再開できます。

GLBP の重み付けの値とオブジェクト トラッキングを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**}
4. **interface** *type number*
5. **glbp** *group* **weighting** *maximum* [**lower** *lower*] [**upper** *upper*]
6. **glbp** *group* **weighting track** *object-number* [**decrement** *value*]
7. **glbp** *group* **forwarder preempt** [**delay minimum** *seconds*]
8. **end**
9. **show track** [*object-number* | **brief**] [**interface** [**brief**] | **ip route** [**brief**] | **resolution** | **timers**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**} **例：** `Router(config)# track 2 interface POS 6/0 ip routing`	GLBP ゲートウェイの重み付けに影響する状態変化を追跡するインターフェイスを設定し、トラッキング コンフィギュレーション モードを開始します。 • このコマンドでは、インターフェイス、および **glbp weighting track** コマンドで使用する、そのインターフェイスに対応するオブジェクト番号を設定します。 • **line-protocol** キーワードを指定すると、インターフェイスがアップ状態かどうかが追跡されます。**ip routing** キーワードを指定すると、インターフェイスで IPv6 ルーティングがイネーブルになっているかどうか、および IPv6 アドレスが設定されているかどうかがチェックされます。
ステップ 4	**interface** *type number* **例：** `Router(config)# interface fastethernet 0/0`	インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**glbp** *group* **weighting** *maximum* [**lower** *lower*] [**upper** *upper*] **例：** `Router(config-if)# glbp 10 weighting 110 lower 95 upper 105`	GLBP ゲートウェイの重み付けの初期値、上限しきい値、および下限しきい値を指定します。
ステップ 6	**glbp** *group* **weighting track** *object-number* [**decrement** *value*] **例：** `Router(config-if)# glbp 10 weighting track 2 decrement 5`	GLBP ゲートウェイの重み付けに影響する、追跡対象のオブジェクトを指定します。 • *value* 引数には、追跡対象のオブジェクトで障害が発生した場合に GLBP ゲートウェイの重み付けを減らす量を指定します。
ステップ 7	**glbp** *group* **forwarder preempt** [**delay minimum** *seconds*] **例：** `Router(config-if)# glbp 10 forwarder preempt delay minimum 60`	GLBP グループの現在の AVF で重み付けがしきい値を下回った場合に、ルータが GLBP グループの AVF の役割を引き継ぐように設定します。 • このコマンドは、デフォルトでイネーブルになっており、遅延は 30 秒です。 • オプションの **delay** キーワードと **minimum** キーワードおよび *seconds* 引数を使用して、AVF のプリエンプションが実行されるまでの最小遅延時間を秒数で指定します。
ステップ 8	**end** **例：** `Router(config-if)# exit`	特権 EXEC モードに戻ります。
ステップ 9	**show track** [*object-number* | **brief**] [**interface** [**brief**]| **ip route** [**brief**] | **resolution** | **timers**] **例：** `Router# show track 2`	トラッキング情報を表示します。

GLBP のイネーブル化と確認

この作業では、インターフェイスに対して GLBP をイネーブルにし、その設定と動作を確認する方法を示します。GLBP は、簡単に設定できる設計になっています。GLBP グループ内の各ゲートウェイには同じグループ番号を設定し、GLBP グループ内の少なくとも 1 つのゲートウェイにグループで使用する仮想 IPv6 アドレスを設定する必要があります。その他のすべての必須パラメータは学習できます。

前提条件

インターフェイスで VLAN が使用されている場合、GLBP グループ番号は VLAN ごとに異なる値にする必要があります。

手順の概要

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

4. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name ipv6-prefix*/*prefix-length* | **autoconfig** [*default-route*]}
5. **glbp** *group* **ipv6** [*ipv6-address* | **autoconfig**]
6. **exit**
7. **show glbp** [*interface-type interface-number*] [*group*] [*state*] [**brief**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface fastethernet 0/0`	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name ipv6-prefix*/*prefix-length* | **autoconfig** [*default-route*]} **例：** `Router(config-if)# ipv6 address 2001:0DB8:0:7262::62/64`	IPv6 の一般的なプレフィクスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 5	**glbp** *group* **ipv6** [*ipv6-address* | **autoconfig**] **例：** `Router(config-if)# glbp 1 ipv6 FE80::60:3E47:AC8:8`	IPv6 の GLBP をイネーブルにします。
ステップ 6	**exit** **例：** `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 7	**show glbp** [*interface-type interface-number*] [*group*] [*state*] [**brief**] **例：** `Router(config)# show glbp 10`	（任意）ルータ上の GLBP グループに関する情報を表示します。 • オプションの **brief** キーワードを使用すると、各仮想ゲートウェイまたは仮想フォワーダに関する情報が 1 行表示されます。

GLBP のトラブルシューティング

debug glbp コマンドを使用した場合の影響を最小限に抑えるには、次の作業を実行します。

前提条件

この作業では、コンソールに直接接続された GLBP を実行しているルータが必要です。

手順の概要

1. **enable**
2. **configure terminal**
3. **no logging console**
4. Telnet を使用してルータ ポートにアクセスし、ステップ 1 と 2 を繰り返します。
5. **end**
6. **terminal monitor**
7. **debug condition glbp** *interface-type interface-number group* [*forwarder*]
8. **terminal no monitor**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no logging console** **例：** `Router(config)# no logging console`	コンソール端末へのすべてのロギングをディセーブルにします。 • コンソールへのロギングを再度イネーブルにするには、グローバル コンフィギュレーション モードで **logging console** コマンドを使用します。
ステップ 4	Telnet を使用してルータ ポートにアクセスし、ステップ 1 と 2 を繰り返します。	再帰 Telnet セッションでグローバル コンフィギュレーション モードを開始します。これにより、出力をコンソール ポートからリダイレクトできます。
ステップ 5	**end** **例：** `Router(config)# end`	終了して、特権 EXEC モードに戻ります。
ステップ 6	**terminal monitor** **例：** `Router# terminal monitor`	仮想端末でのロギング出力をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 7	**debug condition glbp** *interface-type interface-number group* [*forwarder*] **例：** `Router# debug condition glbp fastethernet 0/0 10 1`	GLBP 状態に関するデバッグ メッセージを表示します。 • 特定の **debug condition glbp** または **debug glbp** コマンドだけを入力して、出力を特定のサブコンポーネントに分離し、プロセッサの負荷を最小限に抑えます。適切な引数とキーワードを使用して、指定したサブコンポーネント上に詳細なデバッグ情報を生成します。 • 終了したら、特定の **no debug condition glbp** または **no debug glbp** コマンドを入力します。
ステップ 8	**terminal no monitor** **例：** `Router# terminal no monitor`	仮想端末でのロギングをディセーブルにします。

IPv6 用 HSRP グループの動作のイネーブル化

HSRP IPv6 を設定する前に、インターフェイスに対して HSRP バージョン 2 をイネーブルにする必要があります。次の作業では、IPv6 用 HSRP グループをイネーブルにし、確認する方法を示します。

- 「HSRP バージョン 2 のイネーブル化」（P.20）
- 「IPv6 用 HSRP グループの動作のイネーブル化と確認」（P.21）

HSRP バージョン 2 のイネーブル化

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **standby version** {**1** | **2**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* **例：** `Router(config)# interface ethernet 0/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**standby version** {**1** | **2**} **例：** `Router(config-if)# standby version 2`	HSRP のバージョンを変更します。 • デフォルトはバージョン 1 です。

IPv6 用 HSRP グループの動作のイネーブル化と確認

この作業では、**standby ipv6** コマンドを入力すると、変更された EUI-64 形式のインターフェイス ID が生成されます。このインターフェイス ID は、関連する HSRP 仮想 MAC アドレスに基づいて作成されます。

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

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

次の作業では、IPv6 用 HSRP グループの動作をイネーブルにし、HSRP 情報を確認する方法を示します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **interface** *type number*
5. **standby** [*group-number*] **ipv6** {*ipv6-global-address* | *ipv6-address*/*prefix-length* | *ipv6-prefix*/*prefix-length* | *link-local-address* | **autoconfig**}
6. **standby** [*group-number*] **preempt** [**delay** {**minimum** *seconds* | **reload** *seconds* | **sync** *seconds*}]
7. **standby** [*group-number*] **priority** *priority*
8. **exit**
9. **show standby** [*type number* [*group*]] [**all** | **brief**]
10. **show ipv6 interface** [**brief**] [*interface-type interface-number*] [**prefix**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 unicast-routing** **例：** `Router(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。 • HSRP for IPv6 を機能させるには、**ipv6 unicast-routing** コマンドをイネーブルにする必要があります。
ステップ 4	**interface** *type number* **例：** `Router(config)# interface ethernet 0/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 5	**standby** [*group-number*] **ipv6** {*ipv6-global-address* | *ipv6-address*/*prefix-length* | *ipv6-prefix*/*prefix-length* | *link-local-address* | **autoconfig**} **例：** `Router(config-if)# standby 1 ipv6 autoconfig`	IPv6 の HSRP をアクティブにします。 IPv6 アドレスを使用する場合、そのアドレスに IPv6 プレフィクス長を含める必要があります。リンクローカル アドレスを使用する場合は、プレフィクスを与えてはいけません。
ステップ 6	**standby** [*group-number*] **preempt** [**delay** {**minimum** *seconds* | **reload** *seconds* | **sync** *seconds*}] **例：** `Router(config-if)# standby 1 preempt`	HSRP プリエンプションとプリエンプション遅延を設定します。
ステップ 7	**standby** [*group-number*] **priority** *priority* **例：** `Router(config-if)# standby 1 priority 110`	HSRP プライオリティを設定します。
ステップ 8	**exit** **例：** `Router(config-if)# exit`	ルータを特権 EXEC モードに戻します。
ステップ 9	**show standby** [*type number* [*group*]] [**all** | **brief**] **例：** `Router# show standby`	HSRP 情報を表示します。
ステップ 10	**show ipv6 interface** [**brief**] [*interface-type interface-number*] [**prefix**] **例：** `Router# show ipv6 interface ethernet 0/0`	IPv6 用に設定されたインターフェイスが使用可能かどうかのステータスを表示します。

IPv6 における First Hop Redundancy Protocol の設定例

例：GLBP 設定のカスタマイズ

次の例では、図 1 で示したルータ A に複数の GLBP コマンドが設定されています。

```
interface fastethernet 0/0
 ipv6 address 2001:0DB8:0001:0001:/64
 glbp 10 timers 5 18
 glbp 10 timers redirect 600 7200
 glbp 10 load-balancing host-dependent
 glbp 10 priority 254
 glbp 10 preempt delay minimum 60
```

例：キー ストリングを使用した GLBP MD5 認証

次に、キー ストリングを使用した GLBP MD5 認証を設定する例を示します。

```
!
interface Ethernet 0/1
 ipv6 address 2001:0DB8:0001:0001:/64
 glbp 2 authentication md5 key-string ThisStringIsTheSecretKey
 glbp 2 ipv6 FE80::260:3EFF:FE11:6770
```

例：キー チェーンを使用した GLBP MD5 認証

次に、GLBP がキー チェーン「AuthenticateGLBP」を照会して、指定されたキー チェーンの現在アクティブなキーとキー ID を取得する例を示します。

```
key chain AuthenticateGLBP
 key 1
  key-string ThisIsASecretKey
interface Ethernet 0/1
 ipv6 address 2001:0DB8:0001:0001:/64
 glbp 2 authentication md5 key-chain AuthenticateGLBP
 glbp 2 ipv6 FE80::E0:F727:E400:A
```

例：GLBP テキスト認証

次に、テキスト文字列を使用した GLBP テキスト認証を設定する例を示します。

```
interface fastethernet 0/0
 ipv6 address 2001:0DB8:0001:0001:/64
```

```
 glbp 10 authentication text stringxyz
 glbp 10 ipv6 FE80::60:3E47:AC8:8
```

例：GLBP の重み付け

次に、図 1 で示したルータ A を POS インターフェイス 5/0 と 6/0 の IP ルーティング状態を追跡するように設定し、GLBP の重み付けの初期値、上限しきい値、下限しきい値、および重み付けの減少値 10 を設定する例を示します。POS インターフェイス 5/0 と 6/0 がダウンすると、ルータの重み付けの値が小さくなります。

```
track 1 interface POS 5/0 ip routing
track 2 interface POS 6/0 ip routing
interface fastethernet 0/0
 glbp 10 weighting 110 lower 95 upper 105
 glbp 10 weighting track 1 decrement 10
 glbp 10 weighting track 2 decrement 10
 glbp 10 forwarder preempt delay minimum 60
```

例：GLBP 設定のイネーブル化

次に、GLBP をイネーブルにするようにルータを設定し、GLBP グループ 10 に仮想 IPv6 アドレス 2001:0DB8:0002:0002:/64 を指定する例を示します。

```
interface fastethernet 0/0
ipv6 address 2001:0DB8:0001:0001:/64
 glbp 10 ipv6 FE80::60:3E47:AC8:8
```

次に、GLBP グループ 15 に対して GLBP for IPv6 をイネーブルにする例を示します。

```
interface fastethernet 0/0
 ipv6 address 2001:0DB8:0001:0001:/64
 glbp 10 ipv6
```

例：IPv6 用 HSRP グループの動作のイネーブル化と確認

ここでは、次の例を示します。

- 「例：HSRP グループの設定と確認」（P.24）
- 「例：HSRP グローバル IPv6 アドレスの設定」（P.26）

例：HSRP グループの設定と確認

次に、ルータ 1 とルータ 2 で構成される IPv6 用 HSRP グループの設定および確認の例を示します。ルータの設定を確認するために、各ルータに対して **show standby** コマンドが発行されています。

ルータ 1 設定

```
interface FastEthernet0/0.100
description DATA VLAN for PCs
encapsulation dot1Q 100
ipv6 address 2001:DB8:CAFE:2100::BAD1:1010/64
standby version 2
standby 101 priority 120
standby 101 preempt delay minimum 30
standby 101 authentication ese
```

```
standby 101 track Serial0/1/0.17 90
standby 201 ipv6 autoconfig
standby 201 priority 120
standby 201 preempt delay minimum 30
standby 201 authentication ese
standby 201 track Serial0/1/0.17 90

Router1# show standby

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

ルータ 2 設定

```
interface FastEthernet0/0.100
description DATA VLAN for Computers
encapsulation dot1Q 100
ipv6 address 2001:DB8:CAFE:2100::BAD1:1020/64
standby version 2
standby 101 preempt
standby 101 authentication ese
standby 201 ipv6 autoconfig
standby 201 preempt
standby 201 authentication ese

Router2# show standby

FastEthernet0/0.100 - Group 101 (version 2)
State is Standby
7 state changes, last state change 5w5d
Active virtual MAC address is 0000.0c9f.f065
Local virtual MAC address is 0000.0c9f.f065 (v2 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.936 secs
Authentication text "ese"
Preemption enabled
MAC address is 0012.7fc6.8f0c
Standby router is local
```

```
Priority 100 (default 100)
IP redundancy name is "hsrp-Fa0/0.100-101" (default)
FastEthernet0/0.100 - Group 201 (version 2)
State is Standby
7 state changes, last state change 5w5d
Virtual IP address is FE80::5:73FF:FEA0:C9
Active virtual MAC address is 0005.73a0.00c9
Local virtual MAC address is 0005.73a0.00c9 (v2 IPv6 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.936 secs
Authentication text "ese"
Preemption enabled
Active router is FE80::212:7FFF:FEC6:8F0C, priority 120 (expires in 7.548 sec)
MAC address is 0012.7fc6.8f0c
Standby router is local
Priority 100 (default 100)
IP redundancy name is "hsrp-Fa0/0.100-201" (default)
```

例：HSRP グローバル IPv6 アドレスの設定

次に、明示的に設定された 1 つのリンクローカル アドレスと 3 つの HSRP グローバル IPv6 アドレスの例を示します。

```
interface Ethernet0/0
 no ip address
 ipv6 address 2001::0DB8:1/64
 standby version 2
 standby 1 ipv6 FE80::1:CAFÉ
 standby 1 ipv6 2001::0DB8:2/64
 standby 1 ipv6 2001:0DB8::3/64
 standby 1 ipv6 2001:0DB8::4/64
end
```

その他の関連資料

関連資料

関連項目	参照先
IPv6 リンクローカル アドレスとステートレス自動設定	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing IPv6 Addressing and Basic Connectivity」
IPv6 コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト、使用上のガイドライン、および例	『*Cisco IOS IPv6 Command Reference*』
IPv4 における HSRP の設定	『*Cisco IOS IP Application Services Configuration Guide*』の「Configuring HSRP」

規格

規格	タイトル
この機能によってサポートされる新しい規格または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2281	『*Cisco Hot Standby Router Protocol (HSRP)*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 における First Hop Redundancy Protocol の機能情報

表 1 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どのソフトウェア イメージが特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1　IPv6 における First Hop Redundancy Protocol の機能情報

機能名	リリース	機能設定情報
FHRP：IPv6 用 GLBP のサポート	12.2(33)SXI 12.4(6)T	GLBP は、障害が発生したルータまたは回線からデータ トラフィックを保護し、冗長ルータ間でパケットのロード シェアリングを実行できるようにします。 この機能に関する詳細については、次の項を参照してください。 • 「GLBP for IPv6」（P.2） • 「GLBP の設定とカスタマイズ」（P.8） • 「GLBP のトラブルシューティング」（P.18） • 「例：GLBP 設定のカスタマイズ」（P.23） • 「例：GLBP の重み付け」（P.24） • 「例：GLBP 設定のイネーブル化」（P.24） **glbp forwarder preempt**、**glbp ipv6**、**glbp load-balancing**、**glbp preempt**、**glbp priority**、**glbp name**、**glbp timers**、**glbp timers redirect**、**glbp weighting**、**glbp weighting track**、**track interface** の各コマンドがこの機能のために導入または修正されました。
GLBP MD5 認証	12.2(18)S 12.3(2)T	MD5 認証を使用すると、別のプレーン テキスト認証方式よりもセキュリティを強化できます。MD5 認証では、各 GLBP グループ メンバが秘密キーを使用して、発信パケットに含まれるキー付き MD5 ハッシュを生成できます。着信パケットのキー付きハッシュが生成され、着信パケット内のハッシュが生成されたハッシュに一致しない場合、そのパケットは無視されます。 この機能に関する詳細については、次の項を参照してください。 • 「GLBP 認証の設定」（P.10） • 「例：キー ストリングを使用した GLBP MD5 認証」（P.23） • 「例：キー チェーンを使用した GLBP MD5 認証」（P.23） • 「例：GLBP テキスト認証」（P.23） **glbp authentication**、**key**、**key chain**、**key-string**（認証）、**show glbp**、**show key chain** の各コマンドがこの機能のために導入または修正されました。

表 1　IPv6 における First Hop Redundancy Protocol の機能情報 （続き）

機能名	リリース	機能設定情報
IPv6 サービス：HSRP for IPv6	12.4(4)T 12.2(33)SRB 12.2(33)SXI	HSRP は、ファーストホップ IPv6 ルータの透過的なフェールオーバーを可能にする FHRP です。 この機能に関する詳細については、次の各項を参照してください。 • 「HSRP for IPv6」（P.6） • 「IPv6 用 HSRP グループの動作のイネーブル化」（P.20） • 「例：IPv6 用 HSRP グループの動作のイネーブル化と確認」（P.24） **show standby**、**standby ipv6**、**standby preempt**、**standby priority** の各コマンドがこの機能によって導入または修正されました。
HSRP：グローバル IPv6 アドレス	12.2(33)SXI4	HSRP グローバル IPv6 アドレス機能では、ユーザが複数の非リンク ローカル アドレスを仮想アドレスとして設定できます。 この機能に関する詳細については、次の各項を参照してください。 • 「HSRP グローバル IPv6 アドレス」（P.7） • 「IPv6 用 HSRP グループの動作のイネーブル化と確認」（P.21） • 「例：HSRP グローバル IPv6 アドレスの設定」（P.26） **standby ipv6** コマンドが、この機能によって修正されました。

用語集

- **CPE**：Customer Premises Equipment（CPE; 宅内装置）
- **FHRP**：First Hop Redundancy Protocol（FHRP）
- **GLBP**：Gateway Load Balancing Protocol（GLBP; ゲートウェイ ロード バランシング プロトコル）
- **HSRP**：Hot Standby Routing Protocol（HSRP）
- **NA**：Neighbor Advertisement（NA; ネイバー アドバタイズメント）
- **ND**：Neighbor Discovery（ND; ネイバー探索）
- **NS**：Neighbor Solicitation（NS; ネイバー請求）
- **PE**：Provider Equipment（PE）
- **RA**：Router Advertisement（RA; ルータ アドバタイズメント）
- **RS**：Router Solicitation（RS; ルータ請求）

IS-IS for IPv6 の実装

この章では、Integrated Intermediate System-to-Intermediate System（IS-IS）for IPv6 を設定する方法について説明します。IS-IS は、ネットワーク全体にリンクステート情報をアドバタイズしてネットワーク トポロジの全体像を作成する Interior Gateway Protocol（IGP; 内部ゲートウェイ プロトコル）です。IS-IS は、中継システムをレベル 1 またはレベル 2 デバイスとして指定する Open Systems Interconnection（OSI; オープン システム インターコネクション）階層型ルーティング プロトコルです。レベル 2 デバイスは、レベル 1 エリア間でルーティングを実行してドメイン内ルーティング バックボーンを作成します。統合 IS-IS は、1 つのルーティング アルゴリズムを使用して複数のネットワーク アドレス ファミリ（IPv6、IPv4、OSI など）をサポートします。

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「IS-IS for IPv6 の実装に関する機能情報」（P.22）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

IS-IS for IPv6 の実装の前提条件

- この章では、IPv4 に精通していることを前提としています。IPv4 の設定およびコマンド リファレンス情報については、「関連資料」の関連資料を参照してください。
- この章では、IPv6 アドレッシングおよび基本設定に精通していることを前提としています。詳細については、「*Implementing IPv6 Addressing and Basic Connectivity*」を参照してください。

IS-IS for IPv6 の実装の制約事項

Cisco IOS Release 12.0(22)S 以降のリリースおよび Cisco IOS Release 12.2(8)T 以降のリリースでは、IPv6 の IS-IS サポートによって、IETF IS-IS WG *draft-ietf-isis-ipv6.txt* に基づくシングルトポロジの IPv6 IS-IS 機能が実装されます。レベルごとに 1 つの Shortest Path First（SPF）を使用して、OSI、IPv4（設定されている場合）、および IPv6 のルートが計算されます。1 つの SPF が使用されるため、IPv4 IS-IS と IPv6 IS-IS の両方のルーティング プロトコルで共通のネットワーク トポロジを共有する必要があります。IPv4 および IPv6 ルーティングに IS-IS を使用するには、IPv4 IS-IS 用に設定されたインターフェイスを IPv6 IS-IS 用にも設定する必要があり、その逆の設定も必要です。また、IS-IS エリア（レベル 1 ルーティング）またはドメイン（レベル 2 ルーティング）内のすべてのルータで同じアドレス ファミリ セット（IPv4 だけ、IPv6 だけ、または IPv4 と IPv6 の両方）をサポートする必要があります。

Cisco IOS Release 12.2(15)T 以降のリリースでは、IPv6 の IS-IS サポートが拡張され、IETF IS-IS WG *draft-ietf-isis-wg-multi-topology.txt* に規定されているマルチトポロジの IPv6 もサポートされるようになりました。マルチトポロジの IPv6 IS-IS サポートにより、複数の SPF を使用してルートが計算されるため、すべてのインターフェイスですべての設定済みアドレス ファミリをサポートしたり、IS-IS エリアまたはドメイン内のすべてのルータで同じアドレス ファミリ セットをサポートしたりする必要がなくなります。

次の IS-IS ルータ コンフィギュレーション コマンドは IPv4 に固有であり、IPv6 IS-IS ではサポートされません。使用すると IPv6 IS-IS に影響します。

- **mpls**
- **traffic-share**

IS-IS for IPv6 の実装に関する情報

- 「IPv6 の IS-IS 機能拡張」（P.2）

IPv6 の IS-IS 機能拡張

IPv6 における IS-IS は、IPv4 における IS-IS と同じように機能し、同じ利点が多数あります。IS-IS への IPv6 の機能拡張により、IS-IS は IPv4 および OSI ルートに加えて IPv6 プレフィクスをアドバタイズできます。また、IS-IS Command-Line Interface（CLI; コマンドライン インターフェイス）の機能拡張により、IPv6 固有のパラメータを設定できます。IPv6 IS-IS では、IS-IS によってサポートされるアドレス ファミリが、OSI や IPv4 に加えて IPv6 も含まれるように拡張されています。

IPv6 における IS-IS は、シングルトポロジ モードまたはマルチトポロジ モードをサポートします。

IPv6 の IS-IS シングルトポロジ サポート

IPv6 のシングルトポロジ サポートにより、IS-IS for IPv6 を他のネットワーク プロトコル（たとえば、IPv4 や Connectionless Network Service（CLNS; コネクションレス型ネットワーク サービス））とともにインターフェイスに設定できます。すべてのインターフェイスに同じネットワーク アドレス ファミリのセットを設定する必要があります。さらに、IS-IS エリア（レベル 1 ルーティングの場合）またはドメイン（レベル 2 ルーティングの場合）内のすべてのルータがすべてのインターフェイス上で同じネットワーク レイヤ アドレス ファミリのセットをサポートする必要があります。

IPv6 のシングルトポロジ サポートを使用する場合、旧スタイルまたは新スタイルの TLV を使用できます。ただし、IPv6 プレフィクスへの到達可能性のアドバタイズに使用される TLV では、拡張メトリックを使用します。Cisco ルータでは、IPv4 用の新スタイルの TLV だけをサポートするように設定されていない場合、インターフェイス メトリックを 63 よりも大きい値に設定できません。シングルトポロジの IPv6 モードでは、設定されたメトリックは IPv4 と IPv6 の両方で常に同じです。

IPv6 の IS-IS マルチトポロジ サポート

IPv6 の IS-IS マルチトポロジ サポートにより、IS-IS は単一エリアまたはドメイン内で独立したトポロジのセットを維持できます。このモードを使用すると、IS-IS が設定されているすべてのインターフェイスで同じネットワーク アドレス ファミリのセットをサポートする必要がなくなります。また、IS-IS エリア（レベル 1 ルーティングの場合）またはドメイン（レベル 2 ルーティングの場合）内のすべてのルータで同じネットワーク レイヤ アドレス ファミリのセットをサポートする必要がなくなります。複数の SPF が設定済みのトポロジごとに 1 つずつ実行されるため、特定のネットワーク アドレス ファミリをルーティング可能にするには、エリアまたはドメイン内のルータのサブセットに接続が存在するだけで十分です。

isis ipv6 metric コマンドを使用して、IPv6 用のインターフェイスと IPv4 用のインターフェイスに異なるメトリックを設定できます。

IPv6 のマルチトポロジ サポートを使用する場合は、**metric-style wide** コマンドを使用して、新スタイルの TLV を使用するように IS-IS を設定します。これは、Link-State Packet（LSP; リンクステート パケット）で IPv6 情報をアドバタイズするために使用される TLV は、拡張メトリックだけを使用するように定義されているからです。

IPv6 のシングルトポロジ サポートからマルチトポロジ サポートへの移行

エリアまたはドメイン内のすべてのルータは、同じタイプの IPv6 サポート（シングルトポロジまたはマルチトポロジ）を使用する必要があります。マルチトポロジ モードで動作しているルータは、シングルトポロジ モードのルータが IPv6 トラフィックをサポートできるかどうかを認識できないため、IPv6 トポロジに欠陥が生じます。シングルトポロジのサポートから柔軟性の高いマルチトポロジのサポートに移行するために、マルチトポロジ移行モードが用意されています。

マルチトポロジ移行モードでは、シングルトポロジの IS-IS IPv6 サポート モードで動作しているネットワークは、ルータをマルチトポロジの IS-IS IPv6 サポートに対応するようにアップグレードしている間でも動作を継続できます。移行モードでは、両方のタイプの TLV（シングルトポロジとマルチトポロジ）はすべての設定済み IPv6 アドレスについて LSP で送信されますが、ルータはシングルトポロジ モードで動作し続けます（つまり、シングルトポロジ モードのトポロジに関する制約事項が適用されます）。エリアまたはドメイン内のすべてのルータをマルチトポロジ IPv6 に対応するようにアップグレードし、移行モードで動作させたあとで、移行モードを設定から削除できます。エリアまたはドメイン内のすべてのルータがマルチトポロジ IPv6 モードで動作すると、シングルトポロジ モードのトポロジに関する制約事項は適用されなくなります。

IPv6 IS-IS のローカル RIB

IS-IS IPv6 を実行しているルータは、ローカル RIB を保持します。このローカル RIB には、ネイバーから学習した宛先へのすべてのルートが格納されています。各 SPF の最後に、IS-IS はローカル RIB に存在する宛先への最良（つまり、最小コストの）ルートをグローバル IPv6 ルーティング テーブルにインストールしようとします。

IPv6 IS-IS のローカル RIB の詳細については、「IPv6 IS-IS の設定と動作の確認」の項を参照してください。

IS-IS for IPv6 の実装方法

サポートされているルーティング プロトコルを IPv6 で設定する場合は、ルーティング プロセスを作成し、そのルーティング プロセスをインターフェイスに対してイネーブルにして、特定のネットワークに合せてルーティング プロトコルをカスタマイズする必要があります。

（注） ここでは、IPv6 IS-IS ルーティング プロセスの作成とインターフェイスに対するルーティング プロセスのイネーブル化の設定作業について説明します。IPv6 におけるプロトコルの動作は IPv4 と同じであるため、IS-IS のカスタマイズについては詳しく説明しません。IPv4 と IPv6 の設定の詳細およびコマンド リファレンス情報については、「関連資料」に記載されている資料を参照してください。

次の各項の作業では、IPv6 IS-IS の設定方法を示します。一覧内の各作業は、必須と任意に分けています。

- 「シングルトポロジ IS-IS for IPv6 の設定」（P.4）（必須）
- 「マルチトポロジ IS-IS for IPv6 の設定」（P.6）（任意）
- 「IPv6 IS-IS のカスタマイズ」（P.7）（任意）
- 「IPv6 IS-IS ルーティング プロセスへのルートの再配布」（P.10）（任意）
- 「IS-IS レベル間での IPv6 IS-IS ルートの再配布」（P.11）（任意）
- 「IPv6 プロトコル サポートの整合性検査のディセーブル化」（P.12）（任意）
- 「IPv6 IS-IS の設定と動作の確認」（P.14）（任意）

シングルトポロジ IS-IS for IPv6 の設定

IPv6 IS-IS プロセスを作成し、インターフェイスに対して IPv6 IS-IS サポートをイネーブルにするには、次の作業を実行します。

IS-IS の設定では、2 つの作業を実行します。まず、IS-IS ルーティング プロセスを作成します。この作業では、プロトコルに依存しない IS-IS コマンドを使用します。次に、インターフェイスにおける IS-IS プロトコルの動作を設定します。

前提条件

IPv6 IS-IS を実行するようにルータを設定する前に、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 をグローバルにイネーブルにします。基本的な IPv6 接続作業の詳細については、「*Implementing IPv6 Addressing and Basic Connectivity*」を参照してください。

制約事項

IPv6、IPv4、または IPv6 と IPv4 の両方の IS-IS シングルトポロジ サポートを使用する場合は、IPv6 と IPv4 の両方をレベル 1、レベル 2、またはレベル 1 とレベル 2 の両方の IS-IS インターフェイスに設定できます。ただし、IPv6 と IPv4 の両方を同じインターフェイスに設定する場合は、両方で同じ IS-IS レベルを実行する必要があります。つまり、指定したイーサネット インターフェイス上で IS-IS レベル 2 だけを実行するように IPv6 が設定されている場合、IPv4 を同じインターフェイス上で IS-IS レベル 1 だけを実行するように設定することはできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **router isis** *area-tag*
4. **net** *network-entity-title*
5. **exit**
6. **interface** *type number*
7. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*}
8. **ipv6 router isis** *area-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router isis** *area-tag* **例：** `Router(config)# router isis area2`	指定した IS-IS ルーティング プロセスの IS-IS をイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**net** *network-entity-title* **例：** `Router(config-router)# net 49.0001.0000.0000.000c.00`	ルーティング プロセスの IS-IS Network Entity Title（NET）を設定します。 • *network-entity-title* 引数には、IS-IS エリアのエリア アドレスとルータのシステム ID を指定します。 **（注）** *network-entity-title* 引数の形式の詳細については、『*Cisco IOS ISO CLNS Configuration Guide*』の「Configuring ISO CLNS」の章を参照してください。
ステップ 5	**exit** **例：** `Router(config-router)# exit`	ルータ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**interface** *type number* **例：** `Router(config)# interface Ethernet 0/0/1`	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*} **例：** `Router(config-if)# ipv6 address 2001:0DB8::3/64`	インターフェイスに割り当てられている IPv6 ネットワークを指定し、インターフェイスで IPv6 処理をイネーブルにします。 **（注）** IPv6 アドレスの設定の詳細については、「*Implementing IPv6 Addressing and Basic Connectivity*」を参照してください。
ステップ 8	**ipv6 router isis** *area-name* **例：** `Router(config-if)# ipv6 router isis area2`	指定した IPv6 IS-IS ルーティング プロセスをインターフェイスに対してイネーブルにします。

マルチトポロジ IS-IS for IPv6 の設定

IPv6 でマルチトポロジ IS-IS を設定するには、次の作業を実行します。

マルチトポロジ IS-IS for IPv6 を設定するときに **transition** キーワードを使用すると、IS-IS IPv6 のシングルトポロジ SPF モードで作業しているユーザは、マルチトポロジ IS-IS へのアップグレード中でも作業を継続できます。すべてのルータに **transition** キーワードを設定したら、各ルータで **transition** キーワードを削除できます。移行モードがイネーブルになっていない場合、シングルトポロジ モードで動作しているルータとマルチトポロジ モードで動作しているルータ間の IPv6 接続は確立できません。

マルチトポロジ IS-IS へのアップグレード中は既存の IPv6 トポロジを引き続き使用できます。オプションの **isis ipv6 metric** コマンドを使用すると、マルチトポロジ モードでの動作時に IPv6 トラフィックと IPv4 トラフィックのリンクコストを区別できます。

前提条件

IS-IS for IPv6 の設定後、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router isis** *area-tag*
4. **metric-style wide** [**transition**] [**level-1** | **level-2** | **level-1-2**]
5. **address-family ipv6** [**unicast** | **multicast**]
6. **multi-topology** [**transition**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router isis** *area-tag* **例：** `Router(config)# router isis area2`	指定した IS-IS ルーティング プロセスの IS-IS をイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**metric-style wide** [**transition**] [**level-1** | **level-2** | **level-1-2**] **例：** `Router(config-router)# metric-style wide level-1`	IS-IS を実行しているルータを、新スタイルの TLV だけを生成して受け入れるように設定します。
ステップ 5	**address-family ipv6** [**unicast** | **multicast**] **例：** `Router(config-router)# address-family ipv6`	IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードには、IPv6 ユニキャスト アドレス ファミリを指定します。**address-family ipv6** コマンドで **unicast** キーワードが指定されていない場合、ルータはデフォルトでユニキャスト IPv6 アドレス ファミリのコンフィギュレーション モードになります。
ステップ 6	**multi-topology** [**transition**] **例：** `Router(config-router-af)# multi-topology`	マルチトポロジ IS-IS for IPv6 をイネーブルにします。 • オプションの **transition** キーワードを指定すると、IS-IS IPv6 ユーザはマルチトポロジ モードへのアップグレード中に引き続きシングルトポロジ モードを使用できます。

IPv6 IS-IS のカスタマイズ

IPv6 IS-IS の新しい管理ディスタンス、IPv6 IS-IS でサポートされる等価コスト パスの最大数、IPv6 IS-IS のサマリー プレフィクス、およびデフォルトの IPv6 ルート（::/0）をアドバタイズする IS-IS インスタンスを設定するには、次の作業を実行します。Partial Route Calculation（PRC; 部分的なルート計算）間のホールドダウン時間と、マルチトポロジ IS-IS の使用時に Cisco IOS ソフトウェアが SPF 計算を実行する頻度の設定方法についても説明します。

ネットワークに合せて IPv6 の IS-IS マルチトポロジをカスタマイズできますが、多くの場合、その必要はありません。この機能のデフォルトは、ほとんどのカスタマーや機能の要件を満たすように設定されています。デフォルトを変更する場合は、IPv4 のコンフィギュレーション ガイドや IPv6 コマンド リファレンスを参照して、該当する構文を探してください。

手順の概要

1. **enable**

2. **configure terminal**
3. **router isis** *area-tag*
4. **address-family ipv6** [**unicast** | **multicast**]
5. **default-information originate** [**route-map** *map-name*]
6. **distance** *value*
7. **maximum-paths** *number-paths*
8. **summary-prefix** *ipv6-prefix*/*prefix-length* [**level-1** | **level-1-2** | **level-2**]
9. **prc-interval** *seconds* [*initial-wait*] [*secondary-wait*]
10. **spf-interval** [**level-1** | **level-2**] *seconds* [*initial-wait*] [*secondary-wait*]
11. **exit**
12. **interface** *type number*
13. **isis ipv6 metric** *metric-value* [**level-1** | **level-2** | **level-1-2**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router isis** *area-tag* **例：** `Router(config)# router isis area2`	指定した IS-IS ルーティング プロセスの IS-IS をイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv6** [**unicast** | **multicast**] **例：** `Router(config-router)# address-family ipv6`	IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードには、IPv6 ユニキャスト アドレス ファミリを指定します。**address-family ipv6** コマンドで **unicast** キーワードが指定されていない場合、ルータはデフォルトでユニキャスト IPv6 アドレス ファミリのコンフィギュレーション モードになります。
ステップ 5	**default-information originate** [**route-map** *map-name*] **例：** `Router(config-router-af)# default-information originate`	（任意）デフォルトの IPv6 ルートを IS-IS ルーティング ドメインに挿入します。 • **route-map** キーワードと *map-name* 引数には、IPv6 デフォルト ルートがアドバタイズされる条件を指定します。 • **route map** キーワードを省略すると、IPv6 デフォルト ルートは無条件にレベル 2 でアドバタイズされます。

	コマンドまたはアクション	目的
ステップ 6	**distance** *value* **例：** `Router(config-router-af)# distance 90`	（任意）IPv6 ルーティング テーブル内の IPv6 IS-IS ルートの管理ディスタンスを定義します。 • *value* 引数は、10 ～ 254 の整数です（値 0 ～ 9 は、内部で使用するために予約されています）。
ステップ 7	**maximum-paths** *number-paths* **例：** `Router(config-router-af)# maximum-paths 3`	（任意）IPv6 IS-IS がサポートできる等価コスト ルートの最大数を定義します。 • このコマンドは、IPv6 Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）と Routing Information Protocol（RIP; ルーティング情報プロトコル）もサポートしています。 • *number-paths* 引数は、1 ～ 64 の整数です。BGP のデフォルトは 1 本のパス、IS-IS と RIP のデフォルトは 16 本のパスです。
ステップ 8	**summary-prefix** *ipv6-prefix/prefix-length* [**level-1** | **level-1-2** | **level-2**] **例：** `Router(config-router-af)# summary-prefix 2001:0DB8::/24`	（任意）レベル 1-2 ルータがサマリーをアドバタイズするときに直接レベル 1 プレフィクスをアドバタイズするのではなく、レベル 1 プレフィクスをレベル 2 で集約できるようにします。 • **summary-prefix** コマンドの *ipv6-prefix* 引数は、RFC 2373 に記載された形式にする必要があり、16 ビット値をコロンで区切った 16 進でアドレスを指定します。 • *prefix-length* 引数は、アドレスのうち連続する上位何ビットがプレフィクス（アドレスのネットワーク部）を構成するかを示す 10 進数値です。10 進数値の前にスラッシュ記号が必要です。
ステップ 9	**prc-interval** *seconds* [*initial-wait*] [*secondary-wait*] **例：** `Router(config-router-af)# prc-interval 20`	（任意）マルチトポロジ IS-IS for IPv6 の PRC 間のホールドダウン時間を設定します。
ステップ 10	**spf-interval** [**level-1** | **level-2**] *seconds* [*initial-wait*] [*secondary-wait*] **例：** `Router(config-router-af)# spf-interval 30`	（任意）Cisco IOS ソフトウェアがマルチトポロジ IS-IS for IPv6 の SPF 計算を実行する頻度を設定します。
ステップ 11	**exit** **例：** `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了し、ルータをルータ コンフィギュレーション モードに戻します。 • この手順を繰り返して、ルータ コンフィギュレーション モードを終了し、ルータをグローバル コンフィギュレーション モードに戻します。

	コマンドまたはアクション	目的
ステップ 12	**interface** *type number* **例：** `Router(config-router)# interface Ethernet 0/0/1`	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 13	**isis ipv6 metric** *metric-value* [**level-1** | **level-2** | **level-1-2**] **例：** `Router(config-if)# isis ipv6 metric 20`	（任意）マルチトポロジ IS-IS for IPv6 メトリックの値を設定します。

IPv6 IS-IS ルーティング プロセスへのルートの再配布

手順の概要

1. **enable**
2. **configure terminal**
3. **router isis** *area-tag*
4. **address-family ipv6** [**unicast** | **multicast**]
5. **redistribute** *source-protocol* [*process-id*] [**include-connected**] [*target-protocol-options*] [*source-protocol-options*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router isis** *area-tag* **例：** `Router(config)# router isis area2`	指定した IS-IS ルーティング プロセスの IS-IS をイネーブルにし、ルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**address-family ipv6** [**unicast** | **multicast**] **例：** `Router(config-router)# address-family ipv6`	IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードには、IPv6 ユニキャスト アドレス ファミリを指定します。**address-family ipv6** コマンドで **unicast** キーワードが指定されていない場合、ルータはデフォルトでユニキャスト IPv6 アドレス ファミリのコンフィギュレーション モードになります。
ステップ 5	**redistribute** *source-protocol* [*process-id*] [**include-connected**] [*target-protocol-options*] [*source-protocol-options*] **例：** `Router(config-router-af)# redistribute bgp 64500 metric 100 route-map isismap`	ルートを指定したプロトコルから IS-IS プロセスに再配布します。 • *source-protocol* 引数には、**bgp**、**connected**、**isis**、**rip**、または **static** のいずれかのキーワードを指定できます。 • ここでは、この作業に関連する引数およびキーワードだけを指定しています。

IS-IS レベル間での IPv6 IS-IS ルートの再配布

この作業では、ある IS-IS レベルで学習した IPv6 ルートを別のレベルに再配布する方法を示します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router isis** *area-tag*
4. **address-family ipv6** [**unicast** | **multicast**]
5. **redistribute isis** [*process-id*] {**level-1** | **level-2**} **into** {**level-1** | **level-2**} **distribute-list** *list-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router isis** *area-tag* **例：** `Router(config)# router isis area2`	指定した IS-IS ルーティング プロセスの IS-IS をイネーブルにし、ルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**address-family ipv6** [**unicast** | **multicast**] **例：** `Router(config-router)# address-family ipv6`	IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードには、IPv6 ユニキャスト アドレス ファミリを指定します。**address-family ipv6** コマンドで **unicast** キーワードが指定されていない場合、ルータはデフォルトでユニキャスト IPv6 アドレス ファミリのコンフィギュレーション モードになります。
ステップ 5	**redistribute isis** [*process-id*] {**level-1** | **level-2**} **into** {**level-1** | **level-2**} **distribute-list** *list-name* **例：** `Router(config-router-af)# redistribute isis level-1 into level-2`	IPv6 ルートをある IS-IS レベルから別の IS-IS レベルに再配布します。 • デフォルトでは、レベル 1 のインスタンスによって学習されたルートは、レベル 2 のインスタンスによって再配布されます。 （注） **redistribute** コマンドのこの設定では、*protocol* 引数を **isis** にする必要があります。ここでは、この作業に関連する引数とキーワードだけを指定します。

IPv6 プロトコル サポートの整合性検査のディセーブル化

IPv6 シングルトポロジ モードでプロトコルサポートの整合性検査をディセーブルにするには、次の作業を実行します。

シングルトポロジの IS-IS IPv6 では、同じアドレス ファミリ セットを実行するようにルータを設定する必要があります。IS-IS は hello パケットに対して整合性検査を実行し、設定されているアドレス ファミリのセットが異なる hello パケットを拒否します。たとえば、IPv4 と IPv6 の両方の IS-IS を実行しているルータは、IPv4 または IPv6 だけの IS-IS を実行しているルータとの隣接を形成しません。アドレス ファミリが一致しないネットワークで隣接を形成できるようにするには、IPv6 アドレス ファミリ コンフィギュレーション モードで **adjacency-check** コマンドをディセーブルにする必要があります。このコマンドは、特殊な状況でだけ使用する設計になっています。この作業を設定する前に、次の注意事項をお読みください。

（注） **no adjacency-check** コマンドを入力すると、ネットワーク設定に悪影響が及ぶ可能性があります。**no adjacency-check** コマンドは、すべてのルータ上で IPv4 IS-IS を実行し、IPv6 IS-IS をネットワークに追加して、移行中にすべての隣接を保持する必要がある場合にだけ入力してください。IPv6 IS-IS の設定が完了したら、設定から **no adjacency-check** コマンドを削除してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **router isis** *area-tag*
4. **address-family ipv6** [**unicast** | **multicast**]
5. **no adjacency-check**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router isis** *area-tag* **例：** `Router(config)# router isis area2`	指定した IS-IS ルーティング プロセスの IS-IS をイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv6** [**unicast** | **multicast**] **例：** `Router(config-router)# address-family ipv6`	IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードには、IPv6 ユニキャスト アドレス ファミリを指定します。**address-family ipv6** コマンドで **unicast** キーワードが指定されていない場合、ルータはデフォルトでユニキャスト IPv6 アドレス ファミリのコンフィギュレーション モードになります。
ステップ 5	**no adjacency-check** **例：** `Router(config-router-af)# no adjacency-check`	hello パケットに対して実行される IPv6 プロトコル サポートの整合性検査をディセーブルにし、既存の隣接を保持したまま IPv6 を IPv4 だけのネットワークに導入できるようにします。 • **adjacency-check** コマンドはデフォルトでイネーブルになっています。

IPv4 サブネットの整合性検査のディセーブル化

隣接の形成時に IPv4 サブネットの整合性検査をディセーブルにするには、次の作業を実行します。Cisco IOS ソフトウェアは、以前から hello パケットに対する検査を実行し、IPv4 アドレスが存在することと、そのサブネットが hello パケットの送信元のネイバーと一致することを確認しています。この検査をディセーブルにするには、ルータ コンフィギュレーション モードで **no adjacency-check** コマンドを使用します。ただし、マルチトポロジ IS-IS が設定されている場合、この検査は自動的に抑制されます。これは、マルチトポロジ IS-IS では、LAN 上のすべてのルータで共通のプロトコルがサポートされているかどうかに関係なく、ルータによって隣接が形成されることが必要となるためです。

手順の概要

1. **enable**
2. **configure terminal**
3. **router isis** *area-tag*
4. **no adjacency-check**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router isis** *area-tag* **例：** `Router(config)# router isis area2`	指定した IS-IS ルーティング プロセスの IS-IS をイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**no adjacency-check** **例：** `Router(config-router-af)# no adjacency-check`	hello パケットに対して実行される IPv6 プロトコル サポートの整合性検査をディセーブルにし、既存の隣接を保持したまま IPv6 を IPv4 だけのネットワークに導入できるようにします。 • **adjacency-check** コマンドはデフォルトでイネーブルになっています。

IPv6 IS-IS の設定と動作の確認

手順の概要

1. **enable**
2. **show ipv6 protocols** [**summary**]
3. **show isis** [*process-tag*] [**ipv6** | *****] **topology**
4. **show clns** [*process-tag*] **neighbors** [*interface-type interface-number*] [**area**] [**detail**]
5. **show clns** *area-tag* **is-neighbors** [*type number*] [**detail**]
6. **show isis** [*process-tag*] **database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [**lspid**]
7. **show isis ipv6 rib** [*ipv6-prefix*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**show ipv6 protocols** [**summary**] **例：** `Router# show ipv6 protocols`	アクティブな IPv6 ルーティング プロセスのパラメータと現在の状態を表示します。

	コマンドまたはアクション	目的
ステップ 3	**show isis** [*process-tag*] [**ipv6** | *****] **topology** **例：** `Router# show isis topology`	すべてのエリア内の IS-IS を実行しているすべての接続済みルータのリストを表示します。
ステップ 4	**show clns** [*process-tag*] **neighbors** [*interface-type interface-number*] [**area**] [**detail**] **例：** `Router# show clns neighbors detail`	End System（ES; エンド システム）、Intermediate System（IS; 中継システム）、および Multitopology IS-IS（M-ISIS; マルチトポロジ IS-IS）ネイバーを表示します。
ステップ 5	**show clns** *area-tag* **is-neighbors** [*type number*] [**detail**] **例：** `Router# show clns is-neighbors detail`	IS-IS ネイバーの IS-IS 隣接情報を表示します。 • **detail** キーワードを使用すると、ネイバーの IPv6 リンクローカル アドレスが表示されます。
ステップ 6	**show isis** [*process-tag*] **database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [**lspid**] **例：** `Router# show isis database detail`	IS-IS リンクステート データベースを表示します。 • この例では、**detail** キーワードを使用して、各 LSP の内容を表示します。
ステップ 7	**show isis ipv6 rib** [*ipv6-prefix*] **例：** `Router# show isis ipv6 rib`	IPv6 のローカル RIB を表示します。

例

show ipv6 protocols コマンドの出力例

次の例では、**show ipv6 protocols** コマンドを使用して、アクティブな IPv6 ルーティング プロセスのパラメータと現在の状態に関する出力情報を表示しています。

```
Router# show ipv6 protocols

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "isis"
  Interfaces:
    Ethernet0/0/3
    Ethernet0/0/1
    Serial1/0/1
    Loopback1 (Passive)
    Loopback2 (Passive)
    Loopback3 (Passive)
    Loopback4 (Passive)
```

```
    Loopback5 (Passive)
  Redistribution:
    Redistributing protocol static at level 1
  Address Summarization:
    L2: 2001:0DB8:33::/16  advertised with metric 0
    L2: 2001:0DB8:44::/16  advertised with metric 20
    L2: 2001:0DB8:66::/16  advertised with metric 10
    L2: 2001:0DB8:77::/16  advertised with metric 10
```

show isis topology コマンドの出力例

次の例では、**show isis topology** コマンドを使用して、すべてのエリア内の IS-IS を実行しているすべての接続済みルータに関する出力情報を表示しています。

```
Router# show isis topology

IS-IS paths to level-1 routers
System Id       Metric  Next-Hop        Interface       SNPA
0000.0000.000C
0000.0000.000D  20      0000.0000.00AA  Se1/0/1         *HDLC*
0000.0000.000F  10      0000.0000.000F  Et0/0/1         0050.e2e5.d01d
0000.0000.00AA  10      0000.0000.00AA  Se1/0/1         *HDLC*

IS-IS paths to level-2 routers
System Id       Metric  Next-Hop        Interface       SNPA
0000.0000.000A  10      0000.0000.000A  Et0/0/3         0010.f68d.f063
0000.0000.000B  20      0000.0000.000A  Et0/0/3         0010.f68d.f063
0000.0000.000C  --
0000.0000.000D  30      0000.0000.000A  Et0/0/3         0010.f68d.f063
0000.0000.000E  30      0000.0000.000A  Et0/0/3         0010.f68d.f063
```

show clns is-neighbors コマンドの出力例

次の例では、**show clns is-neighbors** コマンドを使用して、ローカル ルータによって他の IS-IS ネイバーとの必要なすべての IS-IS 隣接が形成されていることを確認するための出力情報を表示しています。ネイバーの IPv6 リンクローカル アドレスを表示するには、**detail** キーワードを指定します。

```
Router# show clns is-neighbors detail

System Id      Interface   State  Type Priority  Circuit Id         Format
0000.0000.00AA Se1/0/1     Up     L1   0         00                 Phase V
  Area Address(es): 49.0001
  IPv6 Address(es): FE80::YYYY:D37C:C854:5
  Uptime: 17:21:38
0000.0000.000F Et0/0/1     Up     L1   64        0000.0000.000C.02  Phase V
  Area Address(es): 49.0001
  IPv6 Address(es): FE80::XXXX:E2FF:FEE5:D01D
  Uptime: 17:21:41
0000.0000.000A Et0/0/3     Up     L2   64        0000.0000.000C.01  Phase V
  Area Address(es): 49.000b
  IPv6 Address(es): FE80::ZZZZ:F6FF:FE8D:F063
  Uptime: 17:22:06
```

show clns neighbors コマンドの出力例

次の例では、**show clns neighbors** コマンドに **detail** キーワードを指定して、End System（ES; エンドシステム）ネイバーと Intermediate System（IS; 中継システム）ネイバーの両方に関する詳細な出力情報を表示しています。

```
Router# show clns neighbors detail

System Id          Interface    SNPA            State  Holdtime  Type Protocol
0000.0000.0007     Et3/3        aa00.0400.6408  UP     26        L1   IS-IS
Area Address(es): 20
```

```
IP Address(es): 172.16.0.42*
Uptime: 00:21:49
0000.0C00.0C35     Et3/2        0000.0c00.0c36  Up     91         L1   IS-IS
Area Address(es): 20
IP Address(es): 192.168.0.42*
Uptime: 00:21:52
0800.2B16.24EA     Et3/3        aa00.0400.2d05  Up     27         L1   M-ISIS
Area Address(es): 20
IP Address(es): 192.168.0.42*
IPv6 Address(es): FE80::2B0:8EFF:FE31:EC57
Uptime: 00:00:27
0800.2B14.060E     Et3/2        aa00.0400.9205  Up     8          L1   IS-IS
Area Address(es): 20
IP Address(es): 192.168.0.30*
Uptime: 00:21:52
```

show isis database コマンドの出力例

次の例では、**show isis database** コマンドに **detail** キーワードを指定して、他のルータから受信した LSP とそれらのルータがアドバタイズしている IPv6 プレフィクスに関する詳細な出力情報を表示しています。

```
Router# show isis database detail

IS-IS Level-1 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.0C35.00-00  0x0000000C   0x5696        325           0/0/0
  Area Address: 47.0004.004D.0001
  Area Address: 39.0001
  Metric: 10   IS 0000.0C00.62E6.03
  Metric: 0    ES 0000.0C00.0C35
 --More--
0000.0C00.40AF.00-00* 0x00000009   0x8452        608           1/0/0
  Area Address: 47.0004.004D.0001
  Topology: IPv4 (0x0) IPv6 (0x2)
  NLPID: 0xCC 0x8E
  IP Address: 172.16.21.49
  Metric: 10   IS 0800.2B16.24EA.01
  Metric: 10   IS 0000.0C00.62E6.03
  Metric: 0    ES 0000.0C00.40AF
  IPv6 Address: 2001:0DB8::/32
  Metric: 10   IPv6 (MT-IPv6) 2001:0DB8::/64
  Metric: 5    IS-Extended cisco.03
  Metric: 10   IS-Extended cisco1.03
  Metric: 10    IS (MT-IPv6) cisco.03

IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.000A.00-00  0x00000059   0x378A        949               0/0/0
  Area Address: 49.000b
  NLPID:        0x8E
  IPv6 Address: 2001:0DB8:1:1:1:1:1:1
  Metric: 10         IPv6 2001:0DB8:2:YYYY::/64
  Metric: 10         IPv6 2001:0DB8:3:YYYY::/64
  Metric: 10         IPv6 2001:0DB8:2:YYYY::/64
  Metric: 10         IS-Extended 0000.0000.000A.01
  Metric: 10         IS-Extended 0000.0000.000B.00
  Metric: 10         IS-Extended 0000.0000.000C.01
  Metric: 0          IPv6 11:1:YYYY:1:1:1:1:1/128
  Metric: 0          IPv6 11:2:YYYY:1:1:1:1:1/128
  Metric: 0          IPv6 11:3:YYYY:1:1:1:1:1/128
  Metric: 0          IPv6 11:4:YYYY:1:1:1:1:1/128
  Metric: 0          IPv6 11:5:YYYY:1:1:1:1:1/128
0000.0000.000A.01-00  0x00000050   0xB0AF        491               0/0/0
  Metric: 0          IS-Extended 0000.0000.000A.00
  Metric: 0          IS-Extended 0000.0000.000B.00
```

show isis ipv6 rib コマンドの出力例

次の例では、**show isis ipv6 rib** コマンドの出力を示しています。アスタリスク（*）は、IS-IS ルートとしてマスター IPv6 RIB にインストールされているプレフィクスを示します。各プレフィクスのあとにすべてのパスが優先順に表示されています。つまり、先頭に最適なパス、そのあとに次善パスが表示されています。

```
Router# show isis ipv6 rib

IS-IS IPv6 process "", local RIB
  2001:0DB8:88:1::/64
    via FE80::210:7BFF:FEC2:ACC9/Ethernet2/0, type L2  metric 20 LSP [3/7]
    via FE80::210:7BFF:FEC2:ACCC/Ethernet2/1, type L2  metric 20 LSP [3/7]
* 2001:0DB8:1357:1::/64
    via FE80::202:7DFF:FE1A:9471/Ethernet2/1, type L2  metric 10 LSP [4/9]
* 2001:0DB8:45A::/64
    via FE80::210:7BFF:FEC2:ACC9/Ethernet2/0, type L1  metric 20 LSP [C/6]
    via FE80::210:7BFF:FEC2:ACCC/Ethernet2/1, type L1  metric 20 LSP [C/6]
    via FE80::210:7BFF:FEC2:ACC9/Ethernet2/0, type L2  metric 20 LSP [3/7]
    via FE80::210:7BFF:FEC2:ACCC/Ethernet2/1, type L2  metric 20 LSP [3/7]
```

IPv6 IS-IS の設定例

例：シングルトポロジ IS-IS for IPv6 の設定

次に、シングルトポロジ モードをイネーブルにし、IS-IS プロセスの作成、NET の定義、インターフェイスの IPv6 アドレスの設定、およびインターフェイスによる IPv6 IS-IS の実行の設定を行う例を示します。

```
ipv6 unicast-routing
!
router isis
 net 49.0001.0000.0000.000c.00
 exit
interface Ethernet0/0/1
 ipv6 address 2001:0DB8::3/64
 ipv6 router isis area2
```

例：IPv6 IS-IS のカスタマイズ

次に、イーサネット インターフェイス 0/0/1 上で送信されるルータ アップデートで、他のすべてのルートとともに、イーサネット インターフェイス 0/0/1 を起点とする IPv6 デフォルト ルート（::/0）をアドバタイズする例を示します。また、この例では、IPv6 IS-IS の管理ディスタンスを 90 に、IPv6 IS-IS がサポートする等価コスト パスの最大数を 3 に設定し、IPv6 IS-IS にサマリー プレフィクス 2001:0DB8::/24 を設定しています。

```
router isis
 address-family ipv6
 default-information originate
 distance 90
 maximum-paths 3
 summary-prefix 2001:0DB8::/24
 exit
```

例：IPv6 IS-IS ルーティング プロセスへのルートの再配布

次に、IPv6 BGP ルートを IPv6 IS-IS レベル 2 ルーティング プロセスに再配布する例を示します。

```
router isis
 address-family ipv6
 redistribute bgp 64500 metric 100 route-map isismap
 exit
```

例：IS-IS レベル間での IPv6 IS-IS ルートの再配布

次に、IPv6 IS-IS レベル 1 ルートを IPv6 IS-IS レベル 2 ルーティング プロセスに再配布する例を示します。

```
router isis
 address-family ipv6
 redistribute isis level-1 into level-2
```

例：IPv6 プロトコルサポートの整合性検査のディセーブル化

次に、**adjacency-check** コマンドをディセーブルにして、ネットワーク管理者が既存の隣接を保持したままルータに IPv6 IS-IS を設定できるようにする例を示します。

```
router isis
 address-family ipv6
 no adjacency-check
```

例：マルチトポロジ IS-IS for IPv6 の設定

次に、IS-IS for IPv6 の設定後、IPv6 におけるマルチトポロジ IS-IS を設定する例を示します。

```
router isis
 metric-style wide
 address-family ipv6
 multi-topology
```

例：マルチトポロジ IS-IS の IS-IS IPv6 メトリックの設定

次に、IS-IS IPv6 メトリックの値を 20 に設定する例を示します。

```
interface Ethernet 0/0/1
 isis ipv6 metric 20
```

その他の関連資料

関連資料

関連項目	参照先
IPv6 のサポート機能リスト	『*Cisco IOS IPv6 Configuration Guide*』の「Start Here: Cisco IOS Software Release Specifics for IPv6 Features」
IPv6 コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト、使用上のガイドライン、および例	『*Cisco IOS IPv6 Command Reference*』
IS-IS の設定作業	『*Cisco IOS IP Routing Protocols Configuration Guide*』の「Integrated IS-IS Feature Roadmap」
IS-IS コマンド：コマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS IP Routing Protocols Command Reference*』

規格

規格	タイトル
この機能によってサポートされる新しい規格または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
• CISCO-IETF-IP-FORWARD-MIB • CISCO-IETF-IP-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 1195	『*Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*』
RFC 5120	『*M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)*』
RFC 5308	『*Routing IPv6 with IS-IS*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IS-IS for IPv6 の実装に関する機能情報

表 1 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どのソフトウェア イメージが特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1　IS-IS for IPv6 の実装に関する機能情報

機能名	リリース	機能情報
IPv6 ルーティング：ルート再配布	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	IS-IS for IPv6 では、IPv6 IS-IS ルーティング プロセスへのルートの再配布と IS-IS レベル間での IPv6 IS-IS ルートの再配布がサポートされています。 この機能に関する詳細については、次の各項を参照してください。 • 「IS-IS for IPv6 の実装に関する情報」（P.2） • 「IPv6 IS-IS ルーティング プロセスへのルートの再配布」（P.10） • 「IS-IS レベル間での IPv6 IS-IS ルートの再配布」（P.11）
IPv6 ルーティング：IPv6 の IS-IS サポート	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(8)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	IS-IS への IPv6 の機能拡張により、IS-IS は IPv4 および OSI ルートに加えて IPv6 プレフィクスをアドバタイズできます。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 の IS-IS 機能拡張」（P.2） • 「シングルトポロジ IS-IS for IPv6 の設定」（P.4） • 「IPv6 IS-IS のカスタマイズ」（P.7） • 「IPv6 IS-IS ルーティング プロセスへのルートの再配布」（P.10） • 「IS-IS レベル間での IPv6 IS-IS ルートの再配布」（P.11）

表 1　IS-IS for IPv6 の実装に関する機能情報 （続き）

機能名	リリース	機能情報
IPv6 ルーティング：IPv6 の IS-IS マルチトポロジ サポート	12.0(26)S 12.2(18)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA1 2.2(15)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	IPv6 の IS-IS マルチトポロジ サポートにより、IS-IS は単一エリアまたはドメイン内で独立したトポロジのセットを維持できます。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 の IS-IS 機能拡張」（P.2） • 「IPv6 の IS-IS マルチトポロジ サポート」（P.3） • 「IPv6 のシングルトポロジ サポートからマルチトポロジ サポートへの移行」（P.3） • 「マルチトポロジ IS-IS for IPv6 の設定」（P.6）
IPv6 ルーティング：IS-IS のローカル RIB	12,2(22)S 12.2(33)SRA 12.2(33)SXH	IS-IS IPv6 を実行しているルータは、ローカル RIB を保持します。このローカル RIB には、ネイバーから学習した宛先へのすべてのルートが格納されています。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 IS-IS のローカル RIB」（P.4） • 「IPv6 IS-IS の設定と動作の確認」（P.14）

ネットワーク管理用 IPv6 の実装

このマニュアルでは、IPv6 でのシスコ アプリケーションの管理およびネットワーク管理用 IPv6 の実装の概念とコマンドについて説明します。IPv6 に管理機能を提供するために、**copy**、**ping**、**telnet**、および **traceroute** コマンドが変更されました。Secure Shell（SSH; セキュア シェル）の拡張により、IPv6 アドレスがサポートされるため、Cisco ルータは IPv6 トランスポートを介してリモート IPv6 ノードとのセキュアな暗号化された接続を受け入れたり、確立したりできます。

Cisco IOS IPv6 組み込み管理コンポーネントは、IPv6 ネットワークおよび IPv6 と IPv4 のハイブリッド ネットワークにおいて IPv6 に対応した操作性を実現します。Cisco IOS 組み込み管理コンポーネントとして、system message logging（syslog; システム メッセージ ロギング）、Cisco Networking Services（CNS）エージェント、設定ロガー、Hypertext Transfer Protocol server（HTTP(S); ハイパーテキスト転送プロトコル サーバ）、Tool Command Language（TCL; ツール コマンド言語）、Network Configuration Protocol（NETCONF）、Service-Oriented Access Protocol（SOAP）、および IP Service Level Agreements（SLA; サービス レベル契約）があります。

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「ネットワーク管理用 IPv6 の実装の機能情報」（P.21）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

ネットワーク管理用 IPv6 の実装の前提条件

- デフォルトでは、IPv6 ルーティングは Cisco IOS ソフトウェアでディセーブルになっています。IPv6 ルーティングをイネーブルにするには、まずルータで IPv6 トラフィックの転送をイネーブルにし、IPv6 アドレスをルータの個々のインターフェイスに割り当てる必要があります。少なくとも 1 つのインターフェイスに IPv6 を設定する必要があります。
- ルータへの Telnet アクセスをイネーブルにするには、vty インターフェイスとパスワードを作成する必要があります。
- このマニュアルでは、IPv4 に精通していることを前提としています。IPv4 の設定およびコマンドリファレンス情報については、「その他の関連資料」に記載されている資料を参照してください。

ネットワーク管理用 IPv6 の実装に関する情報

IPv6 を介した Telnet アクセス

Cisco IOS ソフトウェアの Telnet クライアントとサーバでは、IPv6 接続がサポートされています。IPv6 Telnet クライアントを使用してルータへの Telnet セッションを直接確立するか、またはルータから IPv6 Telnet 接続を開始できます。IPv6 ルータへの Telnet アクセスをイネーブルにするには、vty インターフェイスとパスワードを作成する必要があります。

IPv6 での TFTP ファイルのダウンロード

IPv6 では、**copy** コマンドを使用した TFTP ファイルのダウンロードとアップロードがサポートされています。次に示すように、**copy** コマンドは、引数として宛先の IPv6 アドレスまたは IPv6 ホスト名を受け入れ、ルータの実行コンフィギュレーションを IPv6 TFTP サーバに保存します。

```
Router# copy running-config tftp://[3ffe:xxxx:c18:1:290:27ff:fe3a:9e9a]/running-config
```

（注） Cisco IOS Release 12.2(8)T 以降のリリースでは、ポート番号とともに指定されたリテラル IPv6 アドレスを TFTP の送信元または宛先 URL で使用する場合、角カッコ（[ ]）で囲む必要があります。ポート番号のないリテラル IPv6 アドレスは、角カッコで囲む必要はありません。URL でリテラル IPv6 アドレスに角カッコを使用する方法の詳細については、RFC 2732 の『*Format for Literal IPv6 Addresses in URLs*』を参照してください。

IPv6 における ping および traceroute コマンド

ping コマンドは、引数として宛先の IPv6 アドレスまたは IPv6 ホスト名を受け入れ、Internet Control Message Protocol version 6（ICMPv6; インターネット制御メッセージ プロトコル バージョン 6）エコー要求メッセージを指定された宛先に送信します。ICMPv6 エコー応答メッセージは、コンソールに表示されます。拡張 ping 機能も IPv6 でサポートされています。

traceroute コマンドは、引数として宛先の IPv6 アドレスまたは IPv6 ホスト名を受け入れ、IPv6 トラフィックを生成して、宛先アドレスに到達するために使用された各 IPv6 ホップを報告します。

IPv6 トランスポートを介した SSH

IPv6 における SSH は、IPv4 における SSH と同じように機能し、同じ利点があります。SSH サーバ機能を使用すると、SSH クライアントは Cisco ルータへのセキュアな暗号化された接続を確立できます。SSH クライアント機能を使用すると、Cisco ルータは別の Cisco ルータまたは SSH サーバが稼動する他のデバイスへのセキュアな暗号化された接続を確立できます。SSH への IPv6 の機能拡張により、IPv6 アドレスがサポートされるため、Cisco ルータは IPv6 トランスポートを介してリモート IPv6 ノードとのセキュアな暗号化された接続を受け入れたり、確立したりできます。

IPv6 トランスポートを介した SNMP

IPv6 ホストが SNMP クエリーを実行したり、Cisco IOS IPv6 を実行しているデバイスから SNMP 通知を受信したりできるように、IPv6 トランスポートを介した Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）を設定できます。SNMP エージェントおよび関連する MIB が拡張され、IPv6 アドレッシングがサポートされるようになりました。

SNMP for IPv6 は、メッセージの暗号化用に 3DES と AES を提供します。

Cisco IOS IPv6 MIB

シスコは長い間 IPv4 の IP-MIB と IP-FORWARD-MIB をサポートしてきました。CISCO-IETF-IP-MIB と CISCO-IETF-IP-FORWARDING-MIB は、プロトコルに依存しない MIB として定義されている IPv6 MIB ですが、IPv6 オブジェクトとテーブルについてだけ実装されています。Cisco IOS Release 12.2(33)SRC では、IP-MIB と IP-FORWARD-MIB が RFC 4293 および RFC 4292 標準に準拠するように更新されました。

- アップグレードには下位互換性があります。つまり、すべての IP-MIB と IP-FORWARD-MIB のオブジェクトやテーブルは引き続き表示されます。
- IP-MIB と IP-FORWARD-MIB には、新しい IPv6 専用、IPv4 専用、および Protocol-Version Independent（PVI）のオブジェクトとテーブルの定義が含まれます。ただし、これらの MIB の中で新しい IPv6 専用オブジェクトとテーブルおよび PVI オブジェクトとテーブルの新しい IPv6 部分に対してのみサポートが追加されます。

新しい標準が適用されている Cisco IOS リリースからは、CISCO-IETF-IP-MIB と CISCO-IETF-IP-FORWARDING-MIB が削除されています。これらの MIB 内の情報は、新しい MIB の IP-MIB と IP-FORWARD-MIB に含まれるようになりました。これらのリリースについては、「ネットワーク管理用 IPv6 の実装の機能情報」（P.21）を参照してください。

IPv6 でサポートされる MIB

IPv6 では、次の MIB がサポートされます。

- CISCO-CONFIG-COPY-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-DATA-COLLECTION-MIB
- CISCO-FLASH-MIB
- CISCO-IETF-IP-FORWARDING-MIB（Cisco IOS Release 12.2(33)SRC 以降使用不能）
- CISCO-IETF-IP-MIB（Cisco IOS Release 12.2(33)SRC 以降使用不能）
- IP-FORWARD-MIB
- IP-MIB
- ENTITY-MIB
- NOTIFICATION-LOG-MIB
- SNMP-TARGET-MIB

TFTP、remote copy protocol（rcp; リモート コピー プロトコル）、または FTP が使用されている場合、CISCO-CONFIG-COPY-MIB と CISCO-FLASH-MIB では IPv6 アドレッシングがサポートされます。

SNMP を介した IPv6 をサポートするために、次の MIB が追加されました。

- CISCO-SNMP-TARGET-EXT-MIB

SNMP を介した IPv6 をサポートするために、次の MIB が変更されました。

- CISCO-FLASH-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-CONFIG-COPY-MIB

Cisco IOS IPv6 組み込み管理コンポーネント

ここでは、IPv6 ネットワークおよび IPv6 と IPv4 のハイブリッド ネットワークで IPv6 に対応した操作性を実現する Cisco IOS 組み込み管理コンポーネントについて説明します。ここで説明する Cisco IOS 組み込み管理コンポーネントには、次の IPv6 機能があります。

- 「syslog」（P.4）
- 「CNS エージェント」（P.5）
- 「設定ロガー」（P.6）
- 「HTTP(S) の IPv6 サポート」（P.6）
- 「TCL」（P.6）
- 「NETCONF」（P.6）
- 「SOAP メッセージ フォーマット」（P.7）
- 「IP SLA for IPv6」（P.7）

syslog

IPv6 における Cisco IOS system message logging（syslog; システム メッセージ ロギング）プロセスを使用すると、ユーザは IPv6 アドレスを指定して syslog メッセージを外部の syslog サーバやホストに記録できます。この実装では、ホストの IP アドレスを IPv4 形式（たとえば、192.168.0.0）または IPv6 形式（たとえば、2001:0DB8:A00:1::1/64）で指定して、IPv4 ベースのロギング ホスト（syslog サーバ）を指定できます。

Cisco IOS Release 12.4(4)T および 12.2(33)SRC 以降では、この機能は既存の IPv4 および新しい IPv6 のアドレスやホスト名と下位互換性があります。

CNS エージェント

Cisco Networking Services（CNS）サブシステムでは、IPv6 アドレッシングがサポートされています。CNS は、ユーザをネットワーク サービスにリンクするための基盤テクノロジーであり、多数のネットワーク デバイスの自動設定に対応するインフラストラクチャを提供します。多くの IPv6 ネットワークは複雑で多くのデバイスが存在し、各デバイスを個別に設定する必要があります。標準設定が存在しない場合、または変更されている場合は、初期インストールとその後のアップグレードにかなりの時間がかかります。Internet Service Providers（ISP; インターネット サービス プロバイダー）には、部分的な設定を送信して新しいサービスを導入するための手段が必要です。

これらのすべての問題に対処するために、CNS は、中央のディレクトリ サービスと分散型エージェントを使用した「プラグアンドプレイ」ネットワーク サービスを提供するように設計されました。CNS 機能には、CNS エージェントとフロースルー プロビジョニング構造が含まれます。CNS フロースルー プロビジョニングは、CNS の設定エージェントとイベント エージェントを使用してワークフローを自動化するため、オンサイト技術者は必要なくなります。

IPv6 アドレッシングでは、ここで説明する CNS エージェントがサポートされます。

- 「CNS 設定エージェント」（P.5）
- 「CNS イベント エージェント」（P.5）
- 「CNS EXEC エージェント」（P.5）
- 「CNS イメージ エージェント」（P.5）

CNS 設定エージェント

CNS 設定エージェントは、Cisco IOS デバイスにおける初期設定とその後の部分的な設定に関与します。CNS 設定エンジンを使用して、Cisco IOS デバイスの初期設定、増分設定、および同期された設定アップデートを自動化するための手段を提供します。設定エンジンは、設定のロード ステータスをイベントとして報告し、ネットワーク モニタリングまたはワークフロー アプリケーションはそのイベントをサブスクライブできます。

CNS イベント エージェント

CNS イベント エージェントは、他のすべての CNS エージェントに対して CNS イベント バスへのトランスポート接続を提供します。CNS イベント エージェントが動作し、設定エンジンとルータ間の接続が正常に確立されるまでは、イベントを設定エンジンによってルータに送信できません。

イベント エージェントは CNS 設定エンジンを使用して、Cisco IOS デバイスの初期設定、増分設定、および同期された設定アップデートを自動化するための手段を提供します。

CNS EXEC エージェント

CNS EXEC エージェントを使用すると、リモート アプリケーションは、コマンドが含まれるイベント メッセージを送信することによって、Cisco IOS デバイス上で CLI コマンドを EXEC モードで実行できます。

CNS イメージ エージェント

Cisco IOS デバイスの大規模なネットワークを保持する管理者には、イメージ ファイルを多数のリモート デバイスにロードするための自動化されたメカニズムが必要です。ネットワーク管理アプリケーションを使用すると、実行するイメージやシスコ オンライン ソフトウェア センターから受信したイ

メージの管理方法を決定できます。他のイメージ配布ソリューションは、数千のデバイスに対応するように拡張されず、ファイアウォールの背後にあるデバイスや Network Address Translation（NAT; ネットワーク アドレス変換）を使用したデバイスにイメージを配布できません。CNS イメージ エージェントを使用すると、管理対象デバイスは、ネットワーク接続を開始したり、イメージ ダウンロードを要求したりできるため、NAT を使用したデバイスやファイアウォールの背後にあるデバイスはイメージ サーバにアクセスできます。

CNS イメージ エージェントは、CNS イベント バスを使用するように設定できます。CNS イベント バスを使用するには、CNS 設定エンジンで CNS イベント エージェントをイネーブルにし、CNS イベント ゲートウェイに接続する必要があります。CNS イメージ エージェントは、CNS イメージ エージェント プロトコルを認識する HTTP サーバを使用することもできます。CNS イメージ エージェント動作の展開では、CNS イベント バスと HTTP サーバの両方を使用できます。

CNS エージェントの詳細については、『*Cisco IOS Network Management Configuration Guide*』の「Cisco Networking Services」を参照してください。

設定ロガー

設定ロガーは、変更を追跡したり報告したりします。設定ロガーでは、次の 2 つのコンテンツ タイプがサポートされています。

- プレーン テキスト：プレーン テキスト形式を使用すると、設定ロガーは設定変更だけを報告します。
- XML：設定ロガーは、Extensible Markup Language（XML; 拡張マークアップ言語）を使用して設定変更の詳細（変更内容、変更者、変更日時、Parser Return Code（PRC）値、増分の NVGEN 結果など）を報告します。

HTTP(S) の IPv6 サポート

この機能は、IPv6 アドレスをサポートするように HTTP(S) クライアントとサーバを拡張します。Cisco IOS ソフトウェアの HTTP サーバは、IPv6 と IPv4 の両方の HTTP クライアントからの要求を処理できます。Cisco IOS ソフトウェアの HTTP クライアントは、IPv4 と IPv6 の両方の HTTP サーバへの要求の送信をサポートします。HTTP クライアントを使用する場合、リテラル IPv6 アドレスを含む URL を RFC 2732 のルールに従った形式にする必要があります。

TCL

Tool Command Language（TCL; ツール コマンド言語）は、Embedded Syslog Manager（ESM）、Embedded Event Manager（EEM）、Interactive Voice Response（IVR; 自動音声応答）、tclsh パーサー モードなどの機能をサポートするために Cisco IOS IPv6 で使用されます。TCL では、送信側（クライアント）と受信側（サーバ）の両方のソケットがサポートされています。

NETCONF

Network Configuration Protocol（NETCONF）では、ネットワーク デバイスの管理、設定データ情報の取得、および新しい設定データのアップロードと操作に使用できるメカニズムが定義されています。NETCONF は、設定データとプロトコル メッセージに XML ベースのデータ符号化を使用します。

NETCONF の詳細については、『*Cisco IOS Network Management Configuration Guide*』の「Network Configuration Protocol」を参照してください。

SOAP メッセージ フォーマット

Service-Oriented Access Protocol（SOAP）を使用すると、CNS メッセージのレイアウトを一貫性のある形式でフォーマットできます。SOAP は、非集中型の分散型環境で構造化された情報を交換するためのプロトコルです。XML テクノロジーを使用して、基礎となるさまざまなプロトコルを介して交換できるメッセージ フォーマットを提供する拡張メッセージ フレームワークを定義します。

SOAP メッセージ構造内にはセキュリティ ヘッダーがあり、CNS 通知メッセージによってユーザ クレデンシャルを認証できます。

CNS メッセージは、要求、応答、および通知の 3 つのメッセージ タイプに分類されます。SOAP の詳細については、『*Cisco IOS Network Management Configuration Guide*』の「Cisco Networking Services」を参照してください。

IP SLA for IPv6

Cisco IOS IP Service Level Agreement（SLA; サービス レベル契約）は、Cisco IOS ソフトウェアを実行するほとんどのデバイスに組み込まれているテクノロジーのポートフォリオであり、シスコのカスタマーは IPv6 アプリケーションやサービスの IPv6 サービス レベルの分析、生産性の向上、運用コストの削減、およびネットワーク停止頻度の低減が可能になります。IP SLA では、ネットワーク パフォーマンスの測定にアクティブなトラフィック モニタリング（継続的で信頼性のある予測可能な方法によるトラフィックの生成）を使用します。

IPv6 では、次の Cisco IOS IP SLA がサポートされています。

- Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）エコー動作：IPv4 または IPv6 を使用する Cisco ルータとデバイス間でエンドツーエンドの応答時間を監視するために使用されます。ICMP エコーは、ネットワーク接続問題のトラブルシューティングに役立ちます。
- TCP 接続動作：IPv4 または IPv6 を使用する Cisco ルータとデバイス間で TCP 接続動作の実行にかかった応答時間を測定するために使用されます。
- User Datagram Protocol（UDP; ユーザ データグラム プロトコル）エコー動作：IPv4 または IPv6 を使用する Cisco ルータとデバイス間でエンドツーエンドの応答時間を監視するために使用されます。
- UDP ジッタ動作：IPv4 または IPv6 ネットワークで UDP トラフィックを伝送するネットワークのラウンドトリップ遅延、一方向遅延、一方向ジッタ、一方向パケット損失、および接続を分析するために使用されます。
- UDP ジッタ動作：ネットワークにおける VoIP 品質レベルを予防的に監視するために使用されます。これにより、IPv4 または IPv6 ネットワーク内のユーザに対して VoIP 品質レベルを保証できます。

ネットワーク管理用 IPv6 の実装方法

- 「IPv6 ルータへの Telnet アクセスのイネーブル化と Telnet セッションの確立」（P.8）（任意）
- 「IPv6 ルータでの SSH のイネーブル化」（P.9）（任意）
- 「IPv6 を介した SNMP 通知サーバの設定」（P.11）（任意）
- 「Cisco IOS IPv6 組み込み管理コンポーネントの設定」（P.13）（任意）

IPv6 ルータへの Telnet アクセスのイネーブル化と Telnet セッションの確立

IPv6 ルータへの Telnet アクセスをイネーブルにし、Telnet セッションを確立するには、次の作業を実行します。IPv4 または IPv6 トランスポートを使用すると、Telnet を使用して、ホストからルータ、ルータからルータ、およびルータからホストに接続できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 host** *name* [*port*] *ipv6-address1* [*ipv6-address2...ipv6-address4*]
4. **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]
5. **password** *password*
6. **login** [**local** | **tacacs**]
7. **ipv6 access-class** *ipv6-access-list-name* {**in** | **out**}
8. **telnet** *host* [*port*] [*keyword*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 host** *name* [*port*] *ipv6-address1* [*ipv6-address2...ipv6-address4*] **例：** `Router(config)# ipv6 host cisco-sj 2001:0DB8:20:1::12`	ホスト名からアドレスへのスタティック マッピングをホスト名キャッシュに定義します。
ステップ 4	**line** [**aux**	**console**	**tty**	**vty**] *line-number* [*ending-line-number*] **例：** `Router(config)# line vty 0 4`	**vty** キーワードを指定して vty インターフェイスを作成します。
ステップ 5	**password** *password* **例：** `Router(config)# password hostword`	Telnet をイネーブルにするパスワードを作成します。
ステップ 6	**login** [**local**	**tacacs**] **例：** `Router(config)# login tacacs`	（任意）ログイン時のパスワード チェックをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 7	**ipv6 access-class** *ipv6-access-list-name* {**in** | **out**} **例：** `Router(config)# ipv6 access-list hostlist`	（任意）回線インターフェイスに IPv6 アクセス リストを追加します。 • このコマンドを使用すると、アクセス リストに一致するセッションへのリモート アクセスが制限されます。
ステップ 8	**telnet** *host* [*port*] [*keyword*] **例：** `Router(config)# telnet cisco-sj`	ホスト名または IPv6 アドレスを使用して、ルータからリモート ホストへの Telnet セッションを確立します。 • Telnet セッションは、ルータ名または IPv6 アドレスに対して確立できます。

IPv6 ルータでの SSH のイネーブル化

IPv6 トランスポート上で使用するために SSH をイネーブルにするには、次の作業を実行します。SSH パラメータを設定しない場合は、デフォルト値が使用されます。

前提条件

IPv6 トランスポートを介した SSH を設定する前に、次の条件が満たされていることを確認してください。

- Cisco IOS Release 12.2(8)T 以降のリリースまたは Cisco IOS Release 12.0(22)S 以降のリリースの IPsec（Data Encryption Standard（DES; データ暗号規格）または 3DES）暗号化ソフトウェア イメージがルータにロードされている。SSH サーバと SSH クライアントの IPv6 トランスポートには、IPsec 暗号化ソフトウェア イメージが必要です。
- ルータにホスト名とホスト ドメインが設定されている。IPv6 アドレスへのホスト名の割り当ておよび IPv4 と IPv6 の両方で使用できるデフォルト ドメイン名の指定については、「*Implementing IPv6 Addressing and Basic Connectivity*」の章の「Mapping Host Names to IPv6 Addresses」の項を参照してください。
- SSH を自動的にイネーブルにする Rivest, Shamir, and Adelman（RSA; Rivest、Shamir、および Adelman）キー ペアがルータに生成されている。

  （注） RSA は公開キー暗号化システムで、Ron Rivest、Adi Shamir、Leonard Adelman の 3 名によって開発されました。RSA キーは、1 つの公開キーと 1 つの秘密キーのペアになっています。

- ルータでローカル アクセスまたはリモート アクセスのユーザ認証メカニズムが設定されている。

制約事項

『*Cisco IOS Security Configuration Guide*』の「Configuring Secure Shell」に記載されている、IPv4 トランスポートを介した SSH の基本的な制約事項は、IPv6 トランスポートを介した SSH にも適用されます。その章に記載されている制約事項以外に、ローカルに格納されているユーザ名とパスワードを使用できるのは、IPv6 トランスポートを介した SSH によってサポートされているユーザ認証メカニズムだけです。IPv6 トランスポートを介した TACACS+ および RADIUS ユーザ認証メカニズムはサポートされません。

（注） SSH クライアントを認証するには、IPv4 トランスポートを介した TACACS+ または RADIUS を設定し、IPv6 トランスポートを介した SSH サーバに接続します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip ssh** [**timeout** *seconds* | **authentication-retries** *integer*]
4. **exit**
5. **ssh** [**-v 1** | **2**] [**-c** {**3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc**}] [**-l** *userid* | **-l** *userid*:*number ip-address* | **-l** *userid*:**rotary** *number ip-address*] [**-m** {**hmac-md5 | hmac-md5-96 | hmac-sha1 | hmac-sha1-96**}] [**-o numberofpasswordprompts** *n*] [**-p** *port-num*] {*ip-addr* | *hostname*} [*command*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip ssh** [**timeout** *seconds* | **authentication-retries** *integer*] **例：** `Router(config)# ip ssh timeout 100 authentication-retries 2`	ルータに SSH 制御変数を設定します。 • 120 秒以内のタイムアウトを秒数で指定できます。デフォルトは 120 です。この設定は、SSH ネゴシエーション フェーズに適用されます。EXEC セッションが開始すると、vty に設定された標準のタイムアウトが適用されます。 デフォルトでは、5 本の vty 回線（0 ～ 4）が定義されています。したがって、5 本のターミナル セッションを確立できます。SSH でシェルが実行されると、vty タイムアウトが始動します。vty タイムアウトのデフォルトは 10 分です。 • 認証の再試行回数（5 回以内）も指定できます。デフォルトは 3 です。

	コマンドまたはアクション	目的
ステップ 4	**exit** **例：** `Router(config)# exit`	コンフィギュレーション モードを終了し、ルータを特権 EXEC モードに戻します。
ステップ 5	**ssh** [**-v** {**1** | **2**}] [**-c** {**3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc**}] [**-l** *userid* | **-l** *userid*:*number ip-address* | **-l** *userid*:**rotary***number ip-address*] [**-m** {**hmac-md5** | **hmac-md5-96** | **hmac-sha1** | **hmac-sha1-96**}] [**-o numberofpasswordprompts** *n*] [**-p** *port-num*] {*ip-addr* | *hostname*} [*command*] **例：** `Router# ssh`	リモート ネットワーク デバイスとの暗号化されたセッションを開始します。

IPv6 を介した SNMP 通知サーバの設定

SNMP マネージャとエージェントとの関係を定義するには、SNMP コミュニティ ストリングを使用します。コミュニティ ストリングは、パスワードと同じように機能して、ルータ上でのエージェントへのアクセスを制限します。ストリングに関連付ける特性を次の中から 1 つ以上指定することもできます。

- コミュニティ ストリングを使用したエージェントへのアクセスが許可される SNMP マネージャの IP アドレスのアクセス リスト
- 特定のコミュニティへのアクセスが可能なすべての MIB オブジェクトのサブセットを定義する MIB ビュー
- コミュニティへのアクセスが可能な MIB オブジェクトに対する読み書きアクセス権または読み取り専用アクセス権

1 つ以上のコミュニティ ストリングを設定できます。特定のコミュニティ ストリングを削除するには、**no snmp-server community** コマンドを使用します。

snmp-server host コマンドでは、SNMP 通知を受信するホスト、および通知をトラップまたは応答要求として送信するかどうかを指定します。**snmp-server enable traps** コマンドでは、指定された通知タイプの生成メカニズム（Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）トラップ、設定トラップ、エンティティ トラップ、Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）トラップなど）をグローバルにイネーブルにします。

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [**ipv6** *nacl*] [*access-list-number*]
4. **snmp-server engineID remote** {*ipv4-ip-address* | *ipv6 address*} [**udp-port** *udp-port-number*] [**vrf** *vrf-name*] *engineid-string*
5. **snmp-server group** *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**context** *context-name*] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** [**ipv6** *named-access-list*]{*acl-number* | *acl-name*}]
6. **snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]

7. **snmp-server user** *username group-name* [**remote** *host* [**udp-port** *port*]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** [**ipv6** *nacl*] [**priv** {**des** | **3des** | **aes** {**128** | **192** |**256**}} *privpassword*] {*acl-number* | *acl-name*}]
8. **snmp-server enable traps** [*notification-type*] [**vrrp**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-server community** *string* [**view** *view-name*] [**ro**	**rw**] [**ipv6** *nacl*] [*access-list-number*] **例：** `Router(config)# snmp-server community mgr view restricted rw ipv6 mgr2`	コミュニティ アクセス ストリングを定義します。
ステップ 4	**snmp-server engineID remote** {*ipv4-ip-address*	*ipv6-address*} [**udp-port** *udp-port-number*] [**vrf** *vrf-name*] *engineid-string* **例：** `Router(config)# snmp-server engineID remote 3ffe:b00:c18:1::3/127 remotev6`	（任意）リモート SNMP エンジン（または SNMP のコピー）の名前を指定します。
ステップ 5	**snmp-server group** *group-name* {**v1**	**v2c**	**v3** {**auth**	**noauth**	**priv**}} [**context** *context-name*] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** [**ipv6** *named-access-list*]{*acl-number*	*acl-name*}] **例：** `Router(config)# snmp-server group public v2c access ipv6 public2`	（任意）新しい SNMP グループ、または SNMP ユーザを SNMP ビューにマッピングするテーブルを設定します。
ステップ 6	**snmp-server host** {*hostname*	*ip-address*} [**vrf** *vrf-name*] [**traps**	**informs**] [**version** {**1**	**2c**	**3** [**auth**	**noauth**	**priv**]}] *community-string* [**udp-port** *port*] [*notification-type*] **例：** `Router(config)# snmp-server host host1.com 2c vrf trap-vrf`	SNMP 通知動作の受信者を指定します。 • SNMP 通知をトラップまたは応答要求として送信するかどうか、使用する SNMP のバージョン、通知のセキュリティ レベル（SNMPv3 の場合）、および通知の受信者（ホスト）を指定します。

	コマンドまたはアクション	目的
ステップ 7	**snmp-server user** *username group-name* [**remote** *host* [**udp-port** *port*]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** [**ipv6** *nacl*] [**priv** {**des** | **3des** | **aes** {**128** | **192** | **256**}} *privpassword*] {*acl-number* | *acl-name*}] **例：** `Router(config)# snmp-server user user1 bldg1 remote 3ffe:b00:c18:1::3/127 v2c access ipv6 public2`	（任意）既存の SNMP グループの新しいユーザを設定します。 **（注）** アドレスのリモート ユーザを設定するには、まずそのリモート ホストのエンジン ID を設定する必要があります。これは、これらのコマンドの設計に適用される制限事項です。ホストよりも前にユーザを設定しようとすると、警告メッセージが表示され、コマンドは実行されません。
ステップ 8	**snmp-server enable traps** [*notification-type*] [**vrrp**] **例：** `Router(config)# snmp-server enable traps bgp`	トラップと応答要求の送信をイネーブルにし、送信する通知のタイプを指定します。 • *notification-type* が指定されていない場合は、サポートされているすべての通知がルータでイネーブルになります。 • ルータで使用可能な通知を確認するには、**snmp-server enable traps ?** コマンドを入力します。

Cisco IOS IPv6 組み込み管理コンポーネントの設定

IPv6 をイネーブルにすると、ほとんどの IPv6 組み込み管理コンポーネントは自動的にイネーブルになり、それ以上の設定は必要ありません。IPv6 を介した syslog を設定したり、ルータへの HTTP アクセスをディセーブルにしたりする場合は、次の各項で説明する作業を参照してください。

- 「IPv6 を介した syslog の設定」（P.13）
- 「IPv6 ルータへの HTTP アクセスのディセーブル化」（P.14）

IPv6 を介した syslog の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **logging host** {{*ip-address* | *hostname*} | {**ipv6** *ipv6-address* | *hostname*}} [**transport** {**udp** [**port** *port-number*] | **tcp** [**port** *port-number*] [**audit**]}] [**xml** | **filtered** [**stream** *stream-id*]] [**alarm** [*severity*]]

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**logging host** {{*ip-address* | *hostname*} | {**ipv6** *ipv6-address* | *hostname*}} [**transport** {**udp** [**port** *port-number*] | **tcp** [**port** *port-number*] [**audit**]}] [**xml** | **filtered** [**stream** *stream-id*]] [**alarm** [*severity*]] **例：** `Router(config)# logging host ipv6 AAAA:BBBB:CCCC:DDDD::FFFF`	システム メッセージとデバッグ出力をリモート ホストに記録します。

IPv6 ルータへの HTTP アクセスのディセーブル化

HTTP サーバをイネーブルにし、ルータに IPv6 アドレスが設定されている場合、IPv6 を介した HTTP アクセスは自動的にイネーブルになります。HTTP サーバが必要ない場合は、この項の説明に従ってディセーブルにしてください。

手順の概要

1. **enable**
2. **configure terminal**
3. **no ip http server**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no ip http server** **例：** `Router(config)# no ip http server`	HTTP アクセスをディセーブルにします。

ネットワーク管理用 IPv6 の実装の設定例

例：IPv6 ルータ設定への Telnet アクセスのイネーブル化

次に、Telnet をイネーブルにし、IPv6 ルータとの間のセッションを開始する例を示します。次の例では、IPv6 アドレス 2001:0db8:20:1::12 とホスト名 cisco-sj が指定されています。この情報を確認するために、**show host** コマンドが使用されています。

```
Router# configure terminal
Router(config)# ipv6 host cisco-sj 2001:0db8:20:1::12
Router(config)# end
Router# show host

Default domain is not set
Name/address lookup uses static mappings

Codes:UN - unknown, EX - expired, OK - OK, ?? - revalidate
       temp - temporary, perm - permanent
       NA - Not Applicable None - Not defined

Host                 Port  Flags      Age Type   Address(es)
cisco-sj             None  (perm, OK)  0  IPv6 2001:0db8:20:1::12
```

ルータへの Telnet アクセスをイネーブルにするには、vty インターフェイスとパスワードを作成します。

```
Router(config)# line vty 0 4

password lab
login
```

Telnet を使用してルータにアクセスするには、パスワードを入力する必要があります。

```
Router# telnet cisco-sj

Trying cisco-sj (2001:0db8:20:1::12)... Open

User Access Verification

Password:
cisco-sj
.
.
.
verification
```

telnet コマンドを使用する必要はありません。次の例に示すように、ホスト名またはアドレスを指定するだけで十分です。

```
Router# cisco-sj
```

または

```
Router# 2001:0db8:20:1::12
```

接続先ルータ上の IPv6 接続ユーザ（回線 130）を表示するには、**show users** コマンドを使用します。

```
Router# show users

    Line       User       Host(s)              Idle       Location
*  0 con 0                 idle                 00:00:00
 130 vty 0                 idle                 00:00:22   8800::3
```

表示されるアドレスは、接続元の IPv6 アドレスです。Domain Name Server（DNS; ドメイン ネーム サーバ）またはローカルのホスト キャッシュで接続元のホスト名が既知の場合は、代わりにホスト名が表示されます。

```
Router# show users

    Line       User       Host(s)              Idle       Location
*  0 con 0                 idle                 00:00:00
 130 vty 0                 idle                 00:02:47   cisco-sj
```

接続ルータのユーザが ^6x とのセッションを一時停止して **show sessions** コマンドを入力すると、IPv6 接続が表示されます。

```
Router# show sessions

Conn Host                Address             Byte  Idle Conn Name
*  1 cisco-sj 2001:0db8:20:1::12      0     0 cisco-sj
```

Conn Name フィールドには、宛先のホスト名（既知の場合だけ）が表示されます。ホスト名が不明な場合、出力は次のようになります。

```
Router# show sessions

Conn Host                Address             Byte  Idle Conn Name
*  1 2001:0db8:20:1::12 2001:0db8:20:1::12      0     0 2001:0db8:20:1::12
```

例：ルータへの HTTP アクセスのディセーブル化

次の例では、**show running-config** コマンドを使用すると、ルータで HTTP アクセスがディセーブルになっていることが示されています。

```
Router# show running-config

Building configuration...
!
Current configuration : 1490 bytes
!
version 12.2
!
hostname Router
!
no ip http server
!
line con 0
line aux 0
line vty 0 4
```

例：IPv6 を介した SNMP 通知サーバの設定

次に、コミュニティ ストリング public を使用して、SNMP が読み取り専用アクセス権ですべてのオブジェクトにアクセスすることを許可する例を示します。また、ルータは、BGP トラップを SNMPv1 を使用して IPv4 ホスト 172.16.1.111 と IPv6 ホスト 3ffe:b00:c18:1::3/127 に送信し、SNMPv2c を使用してホスト 172.16.1.27 に送信します。トラップとともにコミュニティ ストリング public が送信されます。

```
Router(config)# snmp-server community public
Router(config)# snmp-server enable traps bgp
Router(config)# snmp-server host 172.16.1.27 version 2c public
Router(config)# snmp-server host 172.16.1.111 version 1 public
Router(config)# snmp-server host 3ffe:b00:c18:1::3/127 public
```

SNMP サーバ グループを指定したビューに関連付ける例

次に、SNMP コンテキスト A を SNMPv2c グループ GROUP1 のビューと IPv6 の名前付きアクセス リスト public2 に関連付ける例を示します。

```
Router(config)# snmp-server context A
Router(config)# snmp mib community-map commA context A target-list commAVpn
Router(config)# snmp mib target list commAVpn vrf CustomerA
Router(config)# snmp-server view viewA ciscoPingMIB included
Router(config)# snmp-server view viewA ipForward included
Router(config)# snmp-server group GROUP1 v2c context A read viewA write viewA notify
  access ipv6 public2
```

SNMP 通知サーバの作成例

次に、IPv6 ホストを通知サーバとして設定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# snmp-server community mgr view restricted rw ipv6 mgr2
Router(config)# snmp-server engineID remote 3ffe:b00:c18:1::3/127 remotev6
Router(config)# snmp-server group public v2c access ipv6 public2
Router(cofig)# snmp-server host host1.com 2c vrf trap-vrf
Router(cofig)# snmp-server user user1 bldg1 remote 3ffe:b00:c18:1::3/127 v2c access ipv6
public2
Router(config)# snmp-server enable traps bgp
Router(config)# exit
```

関連情報

IPv6 ルーティング プロトコルを実装する場合は、「*Implementing RIP for IPv6*」、「*Implementing IS-IS for IPv6*」、または「*Implementing Multiprotocol BGP for IPv6*」の章を参照してください。

その他の関連資料

関連資料

関連項目	参照先
IPv6 でサポートされる機能	『*Cisco IOS IPv6 Configuration Guide*』の「Start Here: Cisco IOS Software Release Specifics for IPv6 Features」
基本的な IPv6 の設定作業	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing IPv6 Addressing and Basic Connectivity」
IPv6 コマンド：コマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS IPv6 Command Reference*』
SSH 設定情報	『*Cisco IOS Security Command Reference*』
IPv4 CNS、SOAP	『*Cisco IOS Network Management Configuration Guide*』の「Cisco Networking Services」
NETCONF	『*Cisco IOS Network Management Configuration Guide*』の「Network Configuration Protocol」
IP SLA for IPv6	• 『*IP SLAs—Analyzing IP Service Levels Using the ICMP Echo Operation*』 • 『*IP SLAs—Analyzing IP Service Levels Using the TCP Connect Operation*』 • 『*IP SLAs—Analyzing IP Service Levels Using the UDP Echo Operation*』 • 『*IP SLAs—Analyzing IP Service Levels Using the UDP Jitter Operation*』 • 『*IP SLAs—Analyzing VoIP Service Levels Using the UDP Jitter Operation*』

規格

規格	タイトル
この機能によってサポートされる新しい規格または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
• CISCO-CONFIG-COPY-MIB • CISCO-CONFIG-MAN-MIB • CISCO-DATA-COLLECTION-MIB • CISCO-FLASH-MIB • CISCO-RTTMON-IPv6-MIB • CISCO-SNMP-TARGET-EXT-MIB • ENTITY-MIB • IP-FORWARD-MIB • IP-MIB • NOTIFICATION-LOG-MIB • SNMP-TARGET-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2732	『*Format for Literal IPv6 Addresses in URLs*』
RFC 3414	『*User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*』
RFC 3484	『*Default Address Selection for Internet Protocol version 6 (IPv6)*』
RFC 4292	『*IP Forwarding Table MIB*』
RFC 4293	『*Management Information Base for the Internet Protocol (IP)*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ネットワーク管理用 IPv6 の実装の機能情報

表 1 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どのソフトウェア イメージが特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1　IPv6 を介した Cisco IOS アプリケーションの管理の機能情報

機能名	リリース	機能情報
IPv6 を介した Telnet アクセス	12.0(22)S 12.2(2)T 12.2(14)S 12.2(28)SB 12.3 12.3(2)T 12.4 12.4(2)T	Cisco IOS ソフトウェアの Telnet クライアントとサーバでは、IPv6 接続がサポートされています。IPv6 Telnet クライアントを使用してルータへの Telnet セッションを直接確立するか、またはルータから IPv6 Telnet 接続を開始できます。 この機能に関する詳細については、次の各項を参照してください。 • 「ネットワーク管理用 IPv6 の実装の前提条件」（P.2） • 「IPv6 を介した Telnet アクセス」（P.2） • 「IPv6 ルータへの Telnet アクセスのイネーブル化と Telnet セッションの確立」（P.8） • 「例：IPv6 ルータ設定への Telnet アクセスのイネーブル化」（P.15）
IPv6 での TFTP ファイルのダウンロード	12.0(22)S 12.2(2)T 12.2(14)S 12.2(28)SB 12.3 12.3(2)T 12.4 12.4(2)T	IPv6 では、TFTP ファイルのダウンロードとアップロードがサポートされています。 この機能に関する詳細については、次の項を参照してください。 • 「IPv6 での TFTP ファイルのダウンロード」（P.2）

表 1　IPv6 を介した Cisco IOS アプリケーションの管理の機能情報 （続き）

機能名	リリース	機能情報
IPv6 トランスポートを介した SSH	12.0(22)S 12.2(8)T 12.2(14)S 12.2(28)SB 12.2(33)SRA 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	IPv6 における SSH は、IPv4 における SSH と同じように機能し、同じ利点があります。SSH サーバ機能を使用すると、SSH クライアントは Cisco ルータへのセキュアな暗号化された接続を確立できます。SSH クライアント機能を使用すると、Cisco ルータは別の Cisco ルータまたは SSH サーバが稼動する他のデバイスへのセキュアな暗号化された接続を確立できます。 この機能に関する詳細については、次の項を参照してください。 • 「IPv6 トランスポートを介した SSH」（P.3） • 「IPv6 ルータでの SSH のイネーブル化」（P.9）
IPv6 を介した SNMP	12.0(27)S 12.2(33)SRB 12.2(33)SXI 12.3(14)T 12.4 12.4(2)T	IPv6 ホストが SNMP クエリーを実行したり、Cisco IOS IPv6 を実行しているデバイスから SNMP 通知を受信したりできるように、IPv6 トランスポートを介した SNMP を設定できます。 この機能に関する詳細については、次の項を参照してください。 • 「IPv6 トランスポートを介した SNMP」（P.3） • 「IPv6 を介した SNMP 通知サーバの設定」（P.11） • 「例：IPv6 を介した SNMP 通知サーバの設定」（P.17）
IPv6 サービス：IP-FORWARD-MIB のサポート	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(33)SRA 12.2(15)T 12.3 12.3(2)T 12.4 12.4(2)T	MIB は、デバイス上の管理可能なオブジェクトのデータベースです。管理対象オブジェクト、つまり変数を設定したり読み取ったりして、ネットワーク デバイスやインターフェイスに関する情報を提供できます。 この機能に関する詳細については、次の項を参照してください。 • 「IPv6 トランスポートを介した SNMP」（P.3）
IPv6 サービス：IP-MIB のサポート	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(33)SRA 12.2(15)T 12.3 12.3(2)T 12.4 12.4(2)T	MIB は、デバイス上の管理可能なオブジェクトのデータベースです。管理対象オブジェクト、つまり変数を設定したり読み取ったりして、ネットワーク デバイスやインターフェイスに関する情報を提供できます。 この機能に関する詳細については、次の項を参照してください。 • 「IPv6 トランスポートを介した SNMP」（P.3）
SNMPv3：3DES および AES 暗号化のサポート	12.2(33)SB 12.2(33)SRB 12.2(33)SXI 12.4(2)T	SNMP for IPv6 では、3DES および AES 暗号化がサポートされています。 この機能に関する詳細については、次の項を参照してください。 • 「IPv6 トランスポートを介した SNMP」（P.3） • 「IPv6 ルータでの SSH のイネーブル化」（P.9）

表 1　IPv6 を介した Cisco IOS アプリケーションの管理の機能情報 （続き）

機能名	リリース	機能情報
IPv6 サービス：RFC 4293 IP-MIB（IPv6 専用）および RFC 4292 IP-FORWARD-MIB（IPv6 専用）	12.2(33)SB 12.2(54)SG 12.2(33)SRC 15.1(3)T	IP-FORWARD-MIB と IP-MIB は、それぞれ RFC 4292 標準と RFC 4293 標準に準拠するように更新されました。 この機能に関する詳細については、次の項を参照してください。 • 「Cisco IOS IPv6 MIB」（P.3）
IPv6：IPv6 での syslog	12.2(33)SB 12.2(33)SRC 12.2(33)SXI 12.4(4)T	IPv6 における Cisco IOS syslog プロセスを使用すると、ユーザは IPv6 アドレスを指定して syslog メッセージを外部の syslog サーバやホストに記録できます。 この機能に関する詳細については、次の項を参照してください。 • 「syslog」（P.4）
IPv6 の CNS エージェント	12.2(33)SB 12.2(33)SRC 12.4(20)T	CNS 設定エージェントとイベント エージェントは、CNS 設定エンジンを使用して、Cisco IOS デバイスの初期設定、増分設定、および同期された設定アップデートを自動化するための手段を提供します。設定エンジンは、設定のロード ステータスをイベントとして報告し、ネットワーク モニタリングまたはワークフロー アプリケーションはそのイベントをサブスクライブできます。 この機能に関する詳細については、次の項を参照してください。 • 「CNS エージェント」（P.5）
設定ロガーでの IPv6	12.2(33)SB 12.2(33)SRC 12.4(20)T	設定ロガーは、変更を追跡したり報告したりします。 この機能に関する詳細については、次の項を参照してください。 • 「設定ロガー」（P.6）
HTTP(S) の IPv6 サポート	12.2(33)SB 12.2(33)SRC 12.4(20)T	この機能は、IPv6 アドレスをサポートするように HTTP(S) クライアントとサーバを拡張します。 この機能に関する詳細については、次の項を参照してください。 • 「HTTP(S) の IPv6 サポート」（P.6）
IPv6 での TCL のサポート	12.2(33)SRC 12.4(20)T	IPv6 では、TCL がサポートされています。 この機能に関する詳細については、次の項を参照してください。 • 「TCL」（P.6）
IPv6 NETCONF のサポート	12.2(33)SB 12.2(33)SRC 12.4(20)T	Network Configuration Protocol（NETCONF）では、ネットワーク デバイスの管理、設定データ情報の取得、および新しい設定データのアップロードと操作に使用できる簡単なメカニズムが定義されています。 この機能に関する詳細については、次の項を参照してください。 • 「NETCONF」（P.6）

表 1　IPv6 を介した Cisco IOS アプリケーションの管理の機能情報 （続き）

機能名	リリース	機能情報
SOAP での IPv6 のサポート	12.2(33)SB 12.2(33)SRC 12.4(20)T	SOAP は、非集中型の分散型環境で構造化された情報を交換するためのプロトコルです。この機能に関する詳細については、次の項を参照してください。 • 「SOAP メッセージ フォーマット」（P.7）
IP SLA for IPv6	12.2(33)SB 12.2(33)SRC 12.4(20)T 15.0(1)S	IPv6 では IP SLA がサポートされています。 この機能に関する詳細については、次の項を参照してください。 • 「IP SLA for IPv6」（P.7）

モバイル IPv6 の実装

モバイル IP は、IPv4 と IPv6 の両方の規格の一部として含まれています。モバイル IP を使用すると、ホスト デバイスが物理的な接続ポイントをあるネットワークから別のネットワークに移動する可能性がある場合でも、そのデバイスを単一の IP アドレスで識別できます。異なるネットワーク間での移動にかかわらず、異なるポイントでの接続は、ユーザの介入なくシームレスに行われます。有線ネットワークからワイヤレス ネットワークまたはワイドエリア ネットワークへのローミングも簡単に行われます。モバイル IP は、ユーザが企業ネットワーク内にいるか自宅から離れているかにかかわらず、ユーザにユビキタス接続を提供します。

このマニュアルでは、モバイル IPv6 に関する情報を説明します。

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「モバイル IPv6 の実装の機能情報」（P.29）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

モバイル IPv6 の実装の制約事項

Network Mobility（NEMO; ネットワーク モビリティ）基本サポート プロトコル機能を使用する場合、ユーザはどのローミング インターフェイスでも IPv6 ルーティング プロトコルをイネーブルにしてはなりません。

モバイル IPv6 の実装に関する情報

モバイル IPv6 の概要

モバイル IPv4 は、ネットワーク間を移動するときに、同じ IPv4 アドレスを保持し、中断のないネットワークおよびアプリケーション接続を維持する機能を IPv4 ノードに提供します。モバイル IPv6 では、IPv6 アドレス空間によって、任意の種類の大規模環境へのモバイル IP の展開がイネーブルになります。モバイル IPv6 を使用するために外部エージェントは不要です。

モバイル IPv6 ノードを受け入れるためにシステム インフラストラクチャをアップグレードする必要はありません。IPv6 自動設定によって、Mobile Node（MN; モバイル ノード）Care of Address（CoA; 気付アドレス）の割り当てが簡略化されます。

モバイル IPv6 は IPv6 プロトコルのメリットを利用します。たとえば、モバイル IPv6 では、IPv6 オプション ヘッダー（ルーティング、宛先、およびモビリティ）を使用し、ネイバー探索のメリットを利用します。

モバイル IPv6 は、三角ルーティングの回避に役立つ最適化されたルーティングを提供します。モバイル IPv6 ノードは、モビリティをサポートしないノードでも透過的に動作します（ただし、これらのノードはルートの最適化を行いません）。

モバイル IPv6 は、既存の IPv6 仕様との完全な下位互換性があります。したがって、新しいモバイル メッセージを認識しない既存のホストは、直接ルーティング最適化は行いませんが、エラー メッセージを送信し、モバイル ノードとの通信を継続できます。

モバイル IPv6 の機能

モバイル IPv6 を実装するには、モバイル ノードのホーム アドレスが存在するホーム サブネット上にホーム エージェントが必要です。IPv6 Home Address（HA; ホーム アドレス）がモバイル ノードに割り当てられます。モバイル ノードは、接続先のネットワーク上で新しい IPv6 アドレス（CoA）を取得します。ホーム エージェントは、モバイル ノードの場所をエージェントに通知する BU をモバイル ノードから受け入れます。ホーム エージェントは、モバイル ノードのプロキシとして機能し、モバイル ノードのホーム アドレスへのトラフィックを代行受信して、モバイル ノードにトンネリングします。

モバイル ノードは、元のホーム ネットワーク上のホーム エージェントに新しいアドレスを通知し、対応ノードはモバイル ノードに CoA について通知します。入力フィルタリングを使用しているため、モバイル ノードはホーム エージェントへのトンネル リターン トラフィックを反転させ、モバイル ノードの送信元アドレス（ホーム アドレス）が常に地理的に正しくなるようにします。

モバイル IPv6 とは、対応ノードへの IP パケットの送信時にモバイル ノードがホーム エージェントをバイパスする機能です。オプションの拡張によってモバイル IPv6 での直接ルーティングが可能になりますが、拡張は一部のモバイル IPv6 の展開では実装されない場合があります。

直接ルーティングはモバイル IPv6 に組み込まれており、直接ルーティング機能では IPv6 ルーティング ヘッダーと IPv6 宛先オプション ヘッダーが使用されます。ルーティング ヘッダーは現在の CoA を使用したモバイル ノードへのパケットの送信に使用され、現在の CoA はパケットの送信元アドレスであるため、新しいホーム アドレス宛先オプションがモバイル ノードのホーム アドレスを含めるために使用されます。

IPv6 NEMO

NEMO 基本サポート プロトコルにより、モバイル IPv6 ネットワークをインターネット上の異なるポイントに接続できます。このプロトコルはモバイル IPv6 の拡張であり、ネットワークが移動するときに、モバイル ネットワーク内のすべてのノードでセッションを継続できます。NEMO を使用すると、ユーザの移動中もモバイル ネットワーク内のすべてのノードが到達可能になります。ネットワークをインターネットに接続するモバイル ルータは、NEMO 基本サポート プロトコルをその Home Agent（HA; ホーム エージェント）で実行します。NEMO を使用すると、ネットワーク モビリティがモバイル ネットワークの内部のノードに対して透過的になります。

NEMO ルータは、ローミング インターフェイスを介した IPv6 のデフォルト ルートであるモバイル ルートを維持します。

モバイル IPv6 ホーム エージェント

ホーム エージェントは、モバイル IPv6 の 3 つの主要コンポーネントの 1 つです。ホーム エージェントは、対応ノードおよびモバイル ノードと連携して、モバイル IPv6 機能をイネーブルにします。

- ホーム エージェント：ホーム エージェントは、モバイル モードのホーム IPv4 または IPv6 アドレスと、外部ネットワーク上のその CoA（貸与アドレス）との間の関連付けを維持します。
- 対応ノード：対応ノードは、モバイル ノードとのセッションでの宛先 IPv4 または IPv6 ホストです。
- モバイル ノード：接続先のリンク（またはネットワーク）に関係なく、ホーム IPv4 または IPv6 アドレスを使用してネットワーク接続を維持する IPv4 ホストまたは IPv6 ホストです。

ここでは、モバイル IPv6 ホーム エージェントの機能について説明します。

- 「モバイル IPv6 ホーム エージェントのバインディング キャッシュ」（P.3）
- 「モバイル IPv6 ホーム エージェントのバインディング アップデート リスト」（P.4）
- 「ホーム エージェント リスト」（P.4）
- 「NEMO 対応ホーム エージェント」（P.4）

モバイル IPv6 ホーム エージェントのバインディング キャッシュ

各 IPv6 ノードによって、その IPv6 アドレスごとに個別のバインディング キャッシュが維持されます。ルータは、パケットの送信時に、ネイバー探索の概念的な宛先キャッシュを検索する前に IPv6 アドレスのバインディング キャッシュを検索します。

ノードのいずれの IPv6 アドレスのバインディング キャッシュにも、モバイル ノード ホーム アドレスごとに 1 つのエントリを含めることができます。ノードのすべてのバインディング キャッシュ エントリの内容は、再起動時にクリアされます。

バインディング キャッシュ エントリは、ホーム登録エントリまたは対応登録エントリとしてマークされます。ホーム登録エントリは、バインディング ライフタイムの期限が切れると削除されます。その他のエントリは、ローカル キャッシュ置換ポリシーを通じていつでも置換できます。

モバイル IPv6 ホーム エージェントのバインディング アップデート リスト

Binding Update（BU; バインディング アップデート）リストは、各モバイル ノードによって維持されます。BU リストには、ライフタイムがまだ期限切れになっていない、このモバイル ノードによって送信された各 BU の情報が記録されます。BU リストには、モバイル ノードによって送信されたすべての BU（対応ノードに送信されたバインディング、およびモバイル ノードのホーム エージェントに送信されたバインディング）が含まれます。

モビリティ拡張ヘッダーには、新しいルーティング ヘッダー タイプと新しい宛先オプションがあり、BU プロセス中に使用されます。このヘッダーは、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、対応ノード、およびホーム エージェントによって使用されます。

ホーム エージェント リスト

ホーム エージェント リストは、各ホーム エージェントと各モバイル ノードによって維持されます。ホーム エージェント リストには、このノードが最近受信した、ホーム エージェント（H）ビットが設定されたルータ アドバタイズメントの送信元の各ホーム エージェントに関する情報が記録されます。

各ホーム エージェントでは、ホーム エージェントが機能するリンクごとに別々のホーム エージェント リストが維持されます。このリストは、動的ホーム エージェント アドレス検出メカニズムでホーム エージェントによって使用されます。各ローミング モバイル ノードでは、新しいリンクに移動したときに前のリンク上のホーム エージェントに通知できるようにするホーム エージェント リストも維持されます。

NEMO 対応ホーム エージェント

モバイル IPv6 のプロトコル拡張を使用して、ネットワーク モビリティのサポートをイネーブルにします。拡張は、既存のモバイル IPv6 機能との下位互換性があります。NEMO 対応ホーム エージェントは、モバイル IPv6 ホーム エージェントとして動作できます。

Dynamic Home Agent Address Discovery（DHAAD; 動的ホーム エージェント アドレス検出）メカニズムにより、モバイル ノードはそのホーム リンク上のホーム エージェントのアドレスを検出できます。次のリストでは、DHAAD の機能について説明します。

- モバイル ルータは、Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）ホーム エージェント アドレス検出要求をモバイル IPv6 ホーム エージェントのホーム サブネット プレフィクスのエニーキャスト アドレスに送信する。
- モバイル ルータをサポートするホーム エージェントを検出することを指定する新しいフラグ（R）が DHAAD 要求メッセージに導入されている。このフラグは、DHAAD 返信メッセージにも追加されています。
- ホーム エージェント アドレス検出の返信メッセージを受信すると、モバイル ルータはホーム リンクで稼動しているホーム エージェントを検出する。
- モバイル ルータは、登録が受け入れられるまで、各ホーム エージェントへのホーム登録を試行する。モバイル ルータは、ホーム登録試行のたびに、ホーム登録試行間の推奨時間が経過するまで待機します。

暗黙のプレフィクス登録

暗黙のプレフィクス登録を使用している場合、モバイル ルータはホーム エージェントでのバインディング アップデートの一部としてプレフィクスを登録しません。この機能には、ホーム エージェントでの静的な設定が必要であり、ルート転送を設定するには、ホーム エージェントに、特定のモバイル ルータに関連付けられたプレフィクスに関する情報が必要です。

明示的なプレフィクス登録

明示的なプレフィクス登録を使用する場合、モバイル ルータは、バインディング アップデート手順の一部として、プレフィクスのリストをホーム エージェントに提示します。ホーム エージェントは、モバイル ルータがこれらのプレフィクスの使用を承認されていると判断した場合に、バインド確認応答メッセージを送信します。

モバイル IPv6 のパケット ヘッダー

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 レイヤで使用されないため、IPv4 ヘッダーと比べると、IPv6 ヘッダーからは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 レイヤとトランスポート レイヤで使用されます また、基本 IPv6 パケット ヘッダーおよびオプション 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。

モバイル IPv6 では、モバイル ノードと対応ノード間の通信にルーティングおよび宛先オプション ヘッダーが使用されます。新しいモビリティ オプション ヘッダーは、BU プロセスにだけ使用されます。

モバイル IPv6 をサポートするために、いくつかの ICMP メッセージ タイプが定義されています。IPv6 アクセス リストを設定して、モバイル IPv6 固有の ICMP メッセージと一致する IPv6 アクセス リスト エントリを設定したり、モバイル IPv6 拡張ヘッダーを含むパケットに一致するエントリを定義したりできます。

IPv6 パケット ヘッダーの詳細については、「*Implementing IPv6 Addressing and Basic Connectivity*」の章を参照してください。

モバイル IPv6 での IPv6 ネイバー探索

IPv6 ネイバー探索機能は、モバイル IPv6 で動作するように次の変更が加えられています。

- 変更されたルータ アドバタイズメント メッセージ形式：ホーム エージェント サービスを示す単一のフラグ ビットがあります。
- 変更されたプレフィクス情報オプション形式：ルータがグローバル アドレスをアドバタイズできます。
- 新しいアドバタイズメント間隔オプション形式
- 新しいホーム エージェント情報オプション形式
- ルータ アドバタイズメントの送信に対する変更
- モバイル ノードのタイムリーな移動検出

NEMO での IPv6 ネイバー探索重複アドレス検出

IPv6 ルータは、ステートレスおよびステートフル自動設定モードで取得された IPv6 アドレスをいずれかのインターフェイスに割り当てる前に、すべての IPv6 アドレスに対して Duplicate Address Detection（DAD; 重複アドレス検出）を実行する必要があります。モバイル ルータがローミングして IPv6 アドレスを取得するたびに、モバイル ルータは、アドレスの衝突を回避するために、新規に取得した気付アドレスとそのリンクローカル アドレスに対して DAD を実行する必要があります。

ただし、DAD 機能は、特定のレイヤ 2 環境で大きなハンドオフ遅延を発生させます。これらの遅延は、オプティミスティック DAD 手法を使用して回避できます。NEMO では、気付アドレスまたは気付アドレスとリンクローカル アドレスの両方で DAD を省略するための最適化オプションがサポートされます。

IPv6 ネイバー探索の詳細については、「*IPv6 アドレッシングと基本接続の実装*」の章を参照してください。

モバイル IPv6 トンネルの最適化

モバイル IPv6 トンネルの最適化により、ネイティブ IPv6 トンネル インフラストラクチャ上でのルーティングがイネーブルになり、モバイル IPv6 は、シスコ エクスプレス フォワーディング スイッチング サポートなどのすべての IPv6 トンネリング インフラストラクチャ機能を使用できます。

ホーム エージェントは、モバイル ノードから有効な BU 要求を受信したあとで、双方向トンネルのエンドポイントを設定します。このプロセスには、カプセル化モードが IPv6/IPv6 に設定された論理インターフェイス、モバイル ノードのホーム リンク上のホーム エージェントのアドレスへのトンネル ソース、およびモバイル ノードの登録済み気付アドレスに設定されたトンネル宛先の作成が関係します。ルートは、トンネルを介してモバイル ノードのホーム アドレスのルーティング テーブルに挿入されます。

IPv6 ホスト グループの設定

ユーザは、IPv6 ホスト グループ設定を使用してモバイル ユーザ ポリシーまたはモバイル グループ ポリシーを作成できます。ホスト グループ プロファイル ルックアップ インターフェイスにより、任意の検索キーを使用して、BU の送信元に関連付けられているプロファイルをルックアップできます。

- プロファイル名
- IPv6 アドレス
- Network Address Identifier（NAI; ネットワーク アドレス識別子）

ホスト プロファイル ルックアップ インターフェイスでは、単一方向または双方向 Security Parameter Index（SPI; セキュリティ パラメータ インデックス）を作成することにより、IPv6 モバイル ノードの認証プロパティも指定されます。

グループ プロファイルは、SPI オプションが設定され、NAI または IPv6 アドレスが設定されたあとでアクティブになります。また、必要な最小限のオプションが設定されていない場合は、プロファイルが非アクティブになります。アクティブ バインディングを持ついずれかのアクティブ プロファイルが非アクティブ化または削除された場合は、そのプロファイルに関連付けられているすべてのバインディングが無効になります。

NAI に基づくモバイル IPv6 ノードの識別

モバイル ノードは、ホーム アドレスを識別子として使用して自身を識別できます。モバイル IPv6 プロトコル メッセージでは、登録メッセージでこの識別子を使用します。ただし、特定の展開では、モバイル ノードに、ネットワーク アドレスではなく NAI などの論理識別子を使用して自身を識別する機能

が必要です。モバイル IPv6 のモバイル ノード識別子オプションにより、IPv6 アドレスではなく NAI によってモバイル ノードを識別できます。この機能により、ネットワークはモバイル ノードに動的 IPv6 アドレスを付与したり、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）を使用してモバイル ノードを認証したりできます。このオプションは、Internet Key Exchange（IKE; インターネット キー エクスチェンジ）または IPsec が BU または Binding Acknowledgments（BA; バインディング確認応答）の保護に使用されていない場合に使用する必要があります。

ローミング サービスを提供するために、NAI やモバイル ノード ホーム アドレスなど、ユーザを識別するための標準化された方法が必要です。ローミングとは、1 つの Internet Service Providers（ISP; インターネット サービス プロバイダー）との正式なカスタマー/ベンダー関係を維持したまま、複数の ISP のいずれか 1 つを使用できる機能として大まかに定義できます。ローミング機能が必要になる例として、ISP 連合および ISP が提供する企業ネットワーク アクセス サポートがあります。ローミング機能に関心を持つその他のエンティティは次のとおりです。

- より広いエリアでダイヤルアップ サービスを提供するために他の地域プロバイダーとの協力を望む、特定の州や地域で営業している地域 ISP。
- 別の国の 1 つ以上の ISP と事業を連合して、複数の国や 1 つの大陸でより包括的なダイヤルアップ サービスを提供することを望む国内 ISP。
- 1 つ以上の ISP にサービスを提供するワイヤレス LAN ホット スポット。
- 世界規模で従業員にダイヤルアップ サービスの包括的なパッケージを提供することを望む企業。これらのサービスには、インターネット アクセスや、VPN を使用した企業イントラネットへのセキュア アクセスがあります。

モバイル IPv6 の認証プロトコル

モバイル IPv6 サポートの認証プロトコルでは、MN-HA モビリティ メッセージ認証オプションを使用してモバイル ノードとホーム エージェントのシグナリングが保護されます。このオプションは、共有キーに基づく Mobile Node（MN; モバイル ノード）と HA 間のセキュリティ アソシエーションに基づいて、BU および BA メッセージを認証します。この機能により、非 IPsec 認証方式が必要な実稼動環境にモバイル IPv6 を展開できます。MN-HA は、モビリティ SPI、共有キー、認証アルゴリズム、およびモビリティ メッセージ リプレイ保護オプションから構成されます。

モビリティ SPI は、256 ～ 4,294,967,296 の数値です。キーは、任意の値から構成され、16 オクテットの長さです。使用される認証アルゴリズムは HMAC_SHA1 です。リプレイ保護メカニズムでは、シーケンス番号オプションまたはタイムスタンプ オプションを使用できます。MN-HA モビリティ メッセージ認証オプションは、メッセージ内の唯一のモビリティ メッセージ認証オプションである場合には、モビリティ ヘッダーを持つメッセージの最後のオプションである必要があります。

BU または BA メッセージが MN-HA オプションなしで受信され、そのメッセージを受信したエンティティが MN-HA オプションを使用するように設定されているか、モビリティ メッセージ認証オプションの共有キーに基づくモビリティ セキュリティ アソシエーションを持つ場合は、エンティティによって受信メッセージが廃棄されます。

モビリティ メッセージ リプレイ保護オプションにより、ホーム エージェントは、BU がモバイル ノードによって新規に生成されたものであり、攻撃者によって以前の BU からリプレイされていないことを確認できます。この機能は、バインディング エントリが削除されたあとでホーム エージェントがモバイル ノードに関するステートフル情報を維持しない場合に特に役立ちます。ホーム エージェントは、BU が認証されたあとでリプレイ保護チェックを実行します。モビリティ メッセージ リプレイ保護オプションは、BA を BU と照合するためにモバイル ノードによって使用されます。ホーム エージェントは、モビリティ メッセージ リプレイ保護オプションを BU で受信した場合に、BA にモビリティ メッセージ リプレイ保護オプションを含める必要があります。

モバイル IPv6 の実装方法

ルータでのモバイル IPv6 のイネーブル化

指定したインターフェイスでモバイル IPv6 をイネーブルにし、モバイル IPv6 情報を表示するには、次の作業を実行します。モバイル IPv6 を開始する前（「インターフェイスでのモバイル IPv6 のカスタマイズ」（P.19）を参照）またはモバイル IPv6 が稼動しているときに、インターフェイス コンフィギュレーション パラメータをカスタマイズできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 mobile home-agent** [**preference** *preference-value*]
5. **exit**
6. **exit**
7. **show ipv6 mobile globals**
8. **show ipv6 mobile home-agent** [*interface-type interface-number* [*prefix*]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* **例：** `Router(config)# interface Ethernet 2`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 mobile home-agent** [**preference** *preference-value*] **例：** `Router(config-if)# ipv6 mobile home-agent`	特定のインターフェイスでモバイル IPv6 ホーム エージェントを初期化し、起動します。
ステップ 5	**exit** **例：** `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 6	**exit** **例：** `Router(config)# exit`	グローバル コンフィギュレーション モードを終了し、ルータを特権 EXEC モードに戻します。
ステップ 7	**show ipv6 mobile globals** **例：** `Router# show ipv6 mobile globals`	グローバル モバイル IPv6 パラメータを表示します。
ステップ 8	**show ipv6 mobile home-agent** [*interface-type interface-number* [*prefix*]] **例：** `Router# show ipv6 mobile home-agent`	ローカルおよび検出済みのネイバー ホーム エージェントを表示します。

モバイル IPv6 のバインディング情報の設定

指定したインターフェイスでモバイル IPv6 を開始する前に、ルータでバインディング情報を設定できます。IPv6 ルータでバインディング情報を設定および検証するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 mobile home-agent**
4. **binding** [**access** *access-list-name* | *auth-option* | *seconds* | *maximum* | *refresh*]
5. **exit**
6. **exit**
7. **show ipv6 mobile binding** [**care-of-address** *address* | **home-address** *address* | *interface-type interface-number*]
8. **show ipv6 mobile traffic**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 mobile home-agent** **例：** `Router(config)# ipv6 mobile home-agent`	ルータをホームエージェント コンフィギュレーション モードにします。
ステップ 4	**binding** [**access** *access-list-name* | *auth-option* | *seconds* | *maximum* | *refresh*] **例：** `Router(config-ha)# binding`	モバイル IPv6 ホーム エージェント機能のバインディング オプションを設定します。
ステップ 5	**exit** **例：** `Router(config-ha)# exit`	ホームエージェント コンフィギュレーション モードを終了し、ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 6	**exit** **例：** `Router(config)# exit`	グローバル コンフィギュレーション モードを終了し、ルータを特権 EXEC モードに戻します。
ステップ 7	**show ipv6 mobile binding** [**care-of-address** *address* | **home-address** *address* | *interface-type interface-number*] **例：** `Router# show ipv6 mobile binding`	バインディング キャッシュに関する情報を表示します。
ステップ 8	**show ipv6 mobile traffic** **例：** `Router# show ipv6 mobile traffic`	受信した BU および送信した BA に関する情報を表示します。

IPv6 モバイル ルータでの NEMO のイネーブルと設定

NEMO 基本サポート プロトコルにより、モバイル IPv6 ネットワークをインターネット上の異なるポイントに接続できます。IPv6 モバイル ルータで NEMO をイネーブルにし、設定するには、次の作業を実行します。また、NEMO 設定を検証する方法も示します。

手順の概要

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

3. **ipv6 mobile router**
4. **eui-interface** *interface-type interface-number*
5. **home-network** *ipv6-prefix*
6. **home-address** {**home-network** | *ipv6-address-identifier* | *interface*}
7. **explicit-prefix**
8. **register** {**extend expire** *seconds* **retry** *number* **interval** *seconds* | **lifetime** *seconds* | **retransmit initial** *milliseconds* **maximum** *milliseconds* **retry** *number*}
9. **exit**
10. **exit**
11. **show ipv6 mobile router** [**running-config** | **status**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 mobile router** **例：** `Router(config)# ipv6 mobile router`	ルータで IPv6 NEMO 機能をイネーブルにし、ルータを IPv6 モバイル ルータ コンフィギュレーション モードにします。
ステップ 4	**eui-interface** *interface-type interface-number* **例：** `Router(IPv6-mobile-router)# eui-interface Ethernet0/0`	IPv6 モバイル ホーム アドレスを取得するために、指定したインターフェイスの Media Access Control（MAC; メディア アクセス制御）アドレスを使用します。
ステップ 5	**home-network** *ipv6-prefix* **例：** `Router(IPv6-mobile-router)# home-network 2001:0DB1:1/64`	モバイル ルータにホーム ネットワークの IPv6 プレフィクスを指定します。 • ユーザは、最大 10 個のホームネットワーク エントリを設定できます。これらのエントリは優先度の順に使用されます。プレフィクスは、モバイル ルータのホーム ネットワークを識別し、モバイル ルータがいつ自宅にあるかを検出するために使用されます。
ステップ 6	**home-address** {**home-network** | *ipv6-address-identifier* | *interface*} **例：** `Router(IPv6-mobile-router)# home-address home-network eui-64`	IPv6 アドレスまたはインターフェイス識別子を使用して、モバイル ルータ ホーム アドレスを指定します。 • 複数のホーム ネットワークが設定されている場合は、モバイル ルータが登録先のホーム ネットワークに一致するホーム アドレスを構築するように、**home-address home-network** コマンド構文を使用することを推奨します。

	コマンドまたはアクション	目的
ステップ 7	**explicit-prefix** **例：** `Router(IPv6-mobile-router)# explicit-prefix`	IPv6 モバイル ルータに接続されている IPv6 プレフィクスを登録します。
ステップ 8	**register** {**extend expire** *seconds* **retry** *number* **interval** *seconds* | **lifetime** *seconds* | **retransmit initial** *milliseconds* **maximum** *milliseconds* **retry** *number*} **例：** `Router(IPv6-mobile-router)# register lifetime 600`	IPv6 モバイル ルータの登録パラメータを制御します。
ステップ 9	**exit** **例：** `Router(IPv6-mobile-router)# exit`	IPv6 モバイル ルータ コンフィギュレーション モードを終了し、ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 10	**exit** **例：** `Router(config)# exit`	グローバル コンフィギュレーション モードを終了し、ルータを特権 EXEC モードに戻します。
ステップ 11	**show ipv6 mobile router** [**running-config** | **status**] **例：** `Router# show ipv6 mobile router`	IPv6 モバイル ルータに関する設定情報と監視統計情報を表示します。

IPv6 モバイル ルータ ホーム エージェントでの NEMO のイネーブル化

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router nemo**
4. **distance** [*mobile-distance*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 router nemo** **例：** `Router(config)# ipv6 router nemo`	ホーム エージェントで NEMO ルーティング プロセスをイネーブルにし、ルータをルータ コンフィギュレーション モードにします。
ステップ 4	**distance** [*mobile-distance*] **例：** `Router(config-rtr)# distance 10`	NEMO ルートの管理ディスタンスを定義します。

IPv6 モバイル ルータ インターフェイスでのローミングのイネーブル

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 mobile router-service roam** [**bandwidth-efficient** | **cost-efficient** | **priority** *value*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface ethernet 0/0`	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 mobile router-service roam** [**bandwidth-efficient** | **cost-efficient** | **priority** *value*] **例：** `Router(config-if)# ipv6 mobile router-service roam`	IPv6 モバイル ルータ インターフェイスのローミングをイネーブルにします。

モバイル IPv6 プロトコル ヘッダーおよびオプションのフィルタリング

IPv6 拡張ヘッダーは、モバイル IPv6 に固有のオプション ヘッダーの使用をサポートするために開発されました。IPv6 モビリティ ヘッダー、タイプ 2 ルーティング ヘッダー、および宛先オプション ヘッダーにより、モバイル IPv6 固有の ICMPv6 メッセージと一致する IPv6 アクセス リスト エントリの設定と、新規および変更された IPv6 拡張ヘッダーを含むパケットと一致するエントリの定義が可能になります。

モバイル IPv6 プロトコル ヘッダーおよびオプションのフィルタリングをイネーブルにするには、次の作業を実行します。IPv6 アクセス リストの作成、設定、および適用方法については、「*Implementing Traffic Filters and Firewalls for IPv6 Security*」の章を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *access-list-name*
4. **permit icmp** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [*icmp-type* [*icmp-code*] | *icmp-message*] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
   または
   deny icmp {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [*icmp-type* [*icmp-code*] | *icmp-message*] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 access-list** *access-list-name* **例：** `Router(config)# ipv6 access-list list1`	IPv6 アクセス リストを定義し、ルータを IPv6 アクセス リスト コンフィギュレーション モードにします。

ステップ 4	**permit icmp** {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [*icmp-type* [*icmp-code*] | *icmp-message*] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
	
	または
	
	deny icmp {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [*icmp-type* [*icmp-code*] | *icmp-message*] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
	
	例：
	`Router(config-ipv6-acl)# permit icmp host 2001:0DB8:0:4::32 any routing-type 2`
	
	または
	
	`Router(config-ipv6-acl)# deny icmp host 2001:0DB8:0:4::32 any routing-type 2`
		IPv6 アクセス リストにモバイル IPv6 固有オプション ヘッダーの許可または拒否条件を指定します。
		• *icmp-type* 引数には、次のモバイル IPv6 固有オプションのいずれかを指定できます（ただし、これらに限定されません）。
		– dhaad-request：数値は 144 です。
		– dhaad-reply：数値は 145 です。
		– mpd-solicitation：数値は 146 です。
		– mpd-advertisement：数値は 147 です。
		• *doh-number* または *doh-type* 引数とともに **dest-option-type** キーワードを使用する場合、IPv6 パケットは、各 IPv6 パケット ヘッダー内の宛先オプション拡張ヘッダーと照合されます。
		• **mobility** キーワードが使用される場合、IPv6 パケットは、各 IPv6 パケット ヘッダー内のモビリティ拡張ヘッダーと照合されます。
		• *mh-number* または *mh-type* 引数とともに **mobility-type** キーワードを使用する場合、IPv6 パケットは各 IPv6 パケット ヘッダー内のモビリティタイプ オプション拡張ヘッダーと照合されます。
		• **routing-type** キーワードと *routing-number* 引数を使用する場合、IPv6 パケットは、各 IPv6 パケット ヘッダー内のルーティングタイプ オプション拡張ヘッダーと照合されます。

ICMP 到達不能メッセージの制御

IPv6 は、パケットをルーティングできない場合に、パケットの送信元に誘導される適切な ICMP 到達不能メッセージを生成します。指定したインターフェイスに到着したパケットの ICMP 到達不能メッセージを制御するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 unreachables**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface ethernet 0/0`	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 unreachables** **例：** `Router(config-if)# ipv6 unreachables`	指定したインターフェイスに到着したパケットの ICMPv6 到達不能メッセージの生成をイネーブルにします。

モバイル IPv6 のネイティブ IPv6 トンネリングの検証

モバイル IPv6 の IPv6 トンネル情報を検証するには、次の作業を実行します。

ネイティブ IPv6 トンネリング（または Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化））インフラストラクチャを使用すると、ホーム エージェントのスケーラビリティとスイッチングのパフォーマンスが向上します。ホーム エージェントがモバイル ノードから BU を送信したあとで、カプセル化モードが IPv6/IPv6 に設定され、送信元アドレスがモバイル ノードのホーム インターフェイスのホーム エージェント アドレスの送信元アドレスに設定され、トンネル宛先がモバイル ノードの CoA の宛先に設定されたトンネル インターフェイスが作成されます。

これらの機能は透過的であり、モバイル IPv6 で動作するために設定する必要はありません。IPv6 トンネリングの詳細と IPv6 で GRE トンネリングを実装する方法については、「*トンネリング for IPv6 の実装*」の章を参照してください。

手順の概要

1. **enable**
2. **show ipv6 mobile tunnels** [**summary** | **tunnel** *if-number*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**show ipv6 mobile tunnels** [**summary** | **tunnel** *if-number*] **例：** `Router# show ipv6 mobile tunnels`	ホーム エージェントのモバイル IPv6 トンネルをリストします。

モバイル IPv6 のホスト グループの設定と検証

モバイル IPv6 のホスト グループ情報を設定および検証するには、次の作業を実行します。

ユーザは、ホスト グループ設定を使用してモバイル ユーザ ポリシーまたはモバイル グループ ポリシーを作成できます。ホスト グループ プロファイル ルックアップ インターフェイスにより、送信元のプロファイル名、IPv6 アドレス、または NAI を使用して、BU の送信元に関連付けられているプロファイルをルックアップできます。ホスト プロファイル ルックアップ インターフェイスでは、単一方向または双方向 SPI を作成することにより、IPv6 モバイル ノードの認証プロパティも指定されます。

モバイル ノードは、プロファイル名またはホーム アドレスを識別子として自身を識別できます。モバイル IPv6 プロトコル メッセージは、この識別子を登録メッセージの識別子として使用します。ただし、特定の展開では、モバイル ノードに、ネットワーク アドレスではなく NAI などの論理識別子を使用して自身を識別する機能が必要です。

制約事項

- IPv6 アドレス オプションを使用している場合は、同じ IPv6 アドレスを持つ 2 つのホスト グループ プロファイルを設定できません。
- NAI オプションがレルム名に設定され、アドレス オプションが特定の IPv6 アドレスに設定されたプロファイルは設定できません。NAI オプションを削除するか、NAI オプションに完全修飾ユーザ名を指定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 mobile home-agent**
4. **binding** [**access** *access-list-name* | *auth-option* | *seconds* | *maximum* | *refresh*]
5. **host group** *profile-name*
6. **address** {*ipv6-address* | **autoconfig**}
7. **nai** [**realm** | **user** | **macaddress**] {*user@realm* | *@realm*}
8. **authentication** {**inbound-spi** {*hex-in* | **decimal** *decimal-in*} **outbound-spi** {*hex-out* | **decimal** *decimal-out*} | **spi** {*hex-value* | **decimal** *decimal-value*}} **key** {**ascii** *string* | **hex** *string*} [**algorithm** *algorithm-type*] [**replay within** *seconds*]
9. **exit**
10. **exit**
11. **show ipv6 mobile host groups** [*profile-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 mobile home-agent** **例：** `Router(config)# ipv6 mobile home-agent`	ルータをホームエージェント コンフィギュレーション モードにします。
ステップ 4	**binding** [**access** *access-list-name* | *auth-option* | *seconds* | *maximum* | *refresh*] **例：** `Router(config-ha)# binding 15`	モバイル IPv6 ホーム エージェント機能のバインディング オプションを設定します。
ステップ 5	**host group** *profile-name* **例：** `Router(config-ha)# host group profile1`	モバイル IPv6 にホスト設定を作成します。 • プロファイル名が異なる複数のインスタンスを作成および使用できます。
ステップ 6	**address** {*ipv6-address* | **autoconfig**} **例：** `Router(config-ha)# address baba 2001:0DB8:1`	IPv6 モバイル ノードのホーム アドレスを指定します。
ステップ 7	**nai** [**realm** | **user** | **macaddress**] {*user*@*realm* | @*realm*} **例：** `Router(config-ha)# nai @cisco.com`	IPv6 モバイル ノードの NAI を指定します。
ステップ 8	**authentication** {**inbound-spi** {*hex-in* | **decimal** *decimal-in*} **outbound-spi** {*hex-out* | **decimal** *decimal-out*} | **spi** {*hex-value* | **decimal** *decimal-value*}} **key** {**ascii** *string* | **hex** *string*}[**algorithm** *algorithm-type*] [**replay within** *seconds*] **例：** `Router(config-ha)# authentication spi 500 key ascii cisco`	単一方向または双方向 SPI を作成することにより、IPv6 モバイル ノードの認証プロパティを指定します。
ステップ 9	**exit** **例：** `Router(config-ha)# exit`	ホームエージェント コンフィギュレーション モードを終了し、ルータをグローバル コンフィギュレーション モードに戻します。

	コマンドまたはアクション	目的
ステップ 10	**exit** **例：** `Router(config)# exit`	グローバル コンフィギュレーション モードを終了し、ルータを特権 EXEC モードに戻します。
ステップ 11	**show ipv6 mobile host groups** [*profile-name*] **例：** `Router# show ipv6 mobile host groups`	モバイル IPv6 ホスト グループに関する情報を表示します。

インターフェイスでのモバイル IPv6 のカスタマイズ

この作業では、次のような、ルータ設定のインターフェイス設定パラメータをカスタマイズするいくつかの方法について説明します。

- Router Advertisement（RA; ルータ アドバタイズメント）で送信されるアドバタイズメントの間隔オプションの設定
- IPv6 RA にどの IPv6 プレフィクスが含まれるかの設定
- インターフェイス上の IPv6 RA 送信間隔の設定

これらのインターフェイス設定パラメータは、モバイル IPv6 を開始する前またはモバイル IPv6 が稼動しているときに設定できます。これらのパラメータのいずれも必要に応じてカスタマイズできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 mobile home-agent** [**preference** *preference-value*]
5. **ipv6 nd advertisement-interval**
6. **ipv6 nd prefix** {*ipv6-prefix*/*prefix-length* | **default**} [[*valid-lifetime preferred-lifetime* | **at** *valid-date preferred-date*] | **infinite** | **no-advertise** | **off-link** | **no-rtr-address** | **no-autoconfig**]
7. **ipv6 nd ra interval** {*maximum-secs* [*minimum-secs*] | **msec** *maximum-msecs* [*minimum-msecs*]}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* **例：** `Router(config)# interface serial 3`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 mobile home-agent** [**preference** *preference-value*] **例：** `Router(config-if)# ipv6 mobile home-agent preference 10`	インターフェイスでモバイル IPv6 ホーム エージェント プリファレンス値を設定します。
ステップ 5	**ipv6 nd advertisement-interval** **例：** `Router(config-if)# ipv6 nd advertisement-interval`	RA で送信されるアドバタイズメントの間隔オプションを設定します。
ステップ 6	**ipv6 nd prefix** {*ipv6-prefix*/*prefix-length* | **default**} [[*valid-lifetime preferred-lifetime* | **at** *valid-date preferred-date*] | **infinite** | **no-advertise** | **off-link** | **no-rtr-address** | **no-autoconfig**] **例：** `Router(config-if)# ipv6 nd prefix 2001:0DB8::/35 1000 900`	IPv6 RA にどの IPv6 プレフィクスが含まれるかを設定します。
ステップ 7	**ipv6 nd ra interval** {*maximum-secs* [*minimum-secs*] | **msec** *maximum-msecs* [*minimum-msecs*]} **例：** `Router(config-if)# ipv6 nd ra interval 201`	インターフェイス上の IPv6 RA 送信間隔を設定します。

ルータでのモバイル IPv6 の監視および保守

手順の概要

1. **enable**
2. **clear ipv6 mobile binding** [**care-of-address** *prefix* | **home-address** *prefix* | *interface-type interface-number*]
3. **clear ipv6 mobile home-agents** [*interface-type interface-number*]
4. **clear ipv6 mobile traffic**
5. **debug ipv6 mobile** {**binding-cache** | **forwarding** | **home-agent** | **registration**}
6. **debug ipv6 mobile networks**
7. **debug ipv6 mobile router** [**detail**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**clear ipv6 mobile binding** [**care-of-address** *prefix* | **home-address** *prefix* | *interface-type interface-number*] **例：** `Router# clear ipv6 mobile binding`	ルータのモバイル IPv6 バインディング キャッシュをクリアします。
ステップ 3	**clear ipv6 mobile home-agents** [*interface-type interface-number*] **例：** `Router# clear ipv6 mobile home-agents`	ネイバー ホーム エージェント リストをクリアします。
ステップ 4	**clear ipv6 mobile traffic** **例：** `Router# clear ipv6 mobile traffic`	モバイル IPv6 に関連付けられているカウンタをクリアします。
ステップ 5	**debug ipv6 mobile** {**binding-cache** | **forwarding** | **home-agent** | **registration**} **例：** `Router# debug ipv6 mobile registration`	モバイル IPv6 のデバッグ情報の表示をイネーブルにします。
ステップ 6	**debug ipv6 mobile networks** **例：** `Router# debug ipv6 mobile networks`	IPv6 モバイル ネットワークのデバッグ メッセージを表示します。
ステップ 7	**debug ipv6 mobile router** [**detail**] **例：** `Router# debug ipv6 mobile router`	IPv6 モバイル ルータのデバッグ メッセージを表示します。

例

show ipv6 mobile binding コマンドの出力例

```
Router # show ipv6 mobile binding
```

```
Mobile IPv6 Binding Cache Entries:
2001:DB8:2000::1111/64
via care-of address 2001:DB8::A8BB:CCFF:FE01:F611
home-agent 2001:DB8:2000::2001
Prefix 2001:DB8:8000::/64
Prefix 2001:DB8:2000::1111/128
Prefix 2001:DB8:1000::1111/128 installed
state ACTIVE, sequence 23, flags AHRlK
lifetime: remaining 44 (secs), granted 60 (secs), requested 60 (secs)
interface Ethernet0/2
tunnel interface Tunnel0
0 tunneled, 0 reversed tunneled
Selection matched 1 bindings
```

show ipv6 mobile globals コマンドの出力例

次の例では、**show ipv6 mobile globals** コマンドによってバインディング パラメータが表示されます。

```
Router# show ipv6 mobile globals

Mobile IPv6 Global Settings:

  1 Home Agent service on following interfaces:
    Ethernet1/2
  Bindings:
    Maximum number is unlimited.
    1 bindings are in use
    1 bindings peak
    Binding lifetime permitted is 262140 seconds
    Recommended refresh time is 300 seconds
```

show ipv6 mobile home-agent コマンドの出力例

次の例では、ネイバー モバイル ホーム エージェントが見つからなかったことが表示されます。

```
Router# show ipv6 mobile home-agent

Home Agent information for Ethernet1/3
  Configured:
    FE80::20B:BFFF:FE33:501F
    preference 0 lifetime 1800
      global address 2001:0DB8:1::2/64
  Discovered Home Agents:
    FE80::4, last update 0 min
    preference 0 lifetime 1800
      global address 2001:0DB8:1::4/64
```

show ipv6 mobile host groups コマンドの出力例

次の例では、localhost という名前のホスト グループに関する情報が表示されます。

```
Router# show ipv6 mobile host groups

Mobile IPv6 Host Configuration
Mobile Host List:

Host Group Name: localhost
    NAI: sai@cisco.com
    Address: CAB:C0:CA5A:CA5A::CA5A

    Security Association Entry:
      SPI: (Hex: 501) (Decimal Int: 1281)
      Key Format: Hex    Key: baba
      Algorithm: HMAC_SHA1
      Replay Protection: On    Replay Window: 6 secs
```

show ipv6 mobile router コマンドの出力例

次の例では、ルータで IPv6 NEMO が設定されている場合の IPv6 モバイル ルータ ステータスに関する情報が表示されます。

```
Router# show ipv6 mobile router

Mobile Reverse Tunnel established
---------------------------------
using Nemo Basic mode
Home Agent: 2001:DB8:2000::2001
CareOf Address: 2001:DB8::A8BB:CCFF:FE01:F611
Attachment Router: FE80::A8BB:CCFF:FE01:F511
Attachment Interface: Ethernet1/1
Home Network: 2001:DB8:2000:0:FDFF:FFFF:FFFF:FFFE/64
Home Address: 2001:DB8:2000::1111/64
```

show ipv6 mobile traffic コマンドの出力例

次の例では、モバイル IPv6 トラフィックに関する情報が表示されます。

```
Router# show ipv6 mobile traffic

    MIPv6 statistics:
      Rcvd: 6477 total
          0 truncated, 0 format errors
          0 checksum errors
        Binding Updates received:6477
          0 no HA option, 0 BU's length
          0 options' length, 0 invalid CoA
      Sent: 6477 generated
        Binding Acknowledgements sent:6477
          6477 accepted (0 prefix discovery required)
          0 reason unspecified, 0 admin prohibited
          0 insufficient resources, 0 home reg not supported
          0 not home subnet, 0 not home agent for node
          0 DAD failed, 0 sequence number
        Binding Errors sent:0
          0 no binding, 0 unknown MH

  Home Agent Traffic:
    6477 registrations, 0 deregistrations
    00:00:23 since last accepted HA registration
    unknown time since last failed HA registration
    unknown last failed registration code
    Traffic forwarded:
      0 tunneled, 0 reversed tunneled
    Dynamic Home Agent Address Discovery:
      1 requests received, 1 replies sent
    Mobile Prefix Discovery:
      0 solicitations received, 0 advertisements sent
```

show ipv6 mobile tunnels コマンドの出力例

次の例では、ホーム エージェント上のモバイル IPv6 トンネルに関する情報が表示されます。

```
Router# show ipv6 mobile tunnels

Tunnel1:
 Source: 2001:0DB1:1:1
 Destination: 2001:0DB1:2:1
 Encapsulation Mode: IPv6/IPv6
 Egress Interface: Ethernet 1/0
 Switching Mode: Process
 Keep-Alive: Not Supported
 Path MTU Discovery: Enabled
 Input: 20 packets, 1200 bytes, 0 drops
 Output: 20 packets, 1200 bytes, 0 drops
 NEMO Options: Not Supported
```

モバイル IPv6 の実装の設定例

例：ルータでのモバイル IPv6 のイネーブル化

次の例では、指定したインターフェイスでモバイル IPv6 を設定し、イネーブルにする方法を示します。

```
Router> enable
Router# config terminal
Router(config)# interface Ethernet 1
Router(config-if)# ipv6 mobile home-agent
```

例：IPv6 モバイル ルータでの NEMO のイネーブル化と設定

次の例では、IPv6 モバイル ルータで NEMO をイネーブルにし、設定する方法を示します。/128 サブネットを使用する必要があります。そうしないと、IPv6 モバイル ルータはホーム ネットワークがローカルに接続されていると想定するため、登録に失敗します。

```
ipv6 unicast-routing
!
interface ethernet0/0
no ip address
ipv6 address 2001:0DB8:2000::1111/128
ipv6 nd ra mtu suppress
!
interface ethernet0/1
no ip address
ipv6 address 2001:0DB8:1000::1111/128
ipv6 nd ra mtu suppress
!
interface Ethernet0/0
description Roaming Interface to AR2
```

```
no ip address
ipv6 address autoconfig
ipv6 enable
ipv6 nd ns-interval 5000
ipv6 mobile router-service roam
ipv6 rip home enable
!
interface Ethernet0/1
description Mobile Network Interface
no ip address
ipv6 address 2001:0DB8:8000::8001/64
ipv6 enable
ipv6 nd advertisement-interval
ipv6 nd ra interval msec 1000
ipv6 rip home enable
!
interface Ethernet1/1
description Roaming Interface to AR1
no ip address
ipv6 address autoconfig
ipv6 enable
ipv6 nd ns-interval 5000
ipv6 mobile router-service roam priority 99
ipv6 rip home enable
!
ipv6 router rip home
!
ipv6 mobile router
host group mr-host-group
nai mr1@cisco.com
address 2001:0DB8:2000::1112/128
authentication spi hex 100 key ascii hi
exit
home-network 2001:0DB8:2000::/64 discover priority 127
home-network 2001:0DB8:1000::/64 discover
home-address home-network eui-64
explicit-prefix
register lifetime 60
register retransmit initial 1000 maximum 1000 retry 1
register extend expire 20 retry 1 interval 1
```

例 : IPv6 モバイル ルータ ホーム エージェントでの NEMO のイネーブル化

次の例では、IPv6 モバイル ルータ ホーム エージェントで NEMO をイネーブルにし、設定する方法を示します。DHAAD が動作するためにはエニーキャスト アドレスが必要です。**redistribute nemo** コマンドは、NEMO ルートをルーティング プロトコルに再配布します。

```
ipv6 unicast-routing
!
interface Ethernet0/2
description To Network
no ip address
no ipv6 address
ipv6 address 2001:0DB8:2000::2001/64
ipv6 address 2001:0DB8:2000::FDFF:FFFF:FFFF:FFFE/64 anycast
ipv6 enable
ipv6 nd advertisement-interval
ipv6 nd ra lifetime 2
ipv6 nd ra interval msec 1000
ipv6 mobile home-agent preference 100
ipv6 mobile home-agent
```

```
ipv6 rip home enable
!
interface Ethernet2/2
description To CN2
no ip address
no ipv6 address
ipv6 address 2001:0DB8:3000::3001/64
ipv6 enable
ipv6 rip home enable
!
ipv6 router nemo
!
ipv6 router rip home
redistribute nemo
poison-reverse
!
ipv6 mobile home-agent
host group mr-host-group
nai mr1@cisco.com
address 2001:0DB8:2000::1112/64
authentication spi hex 100 key ascii hi
exit
host group mr2-host-group
nai mr2@cisco.com
address 2001:0DB8:2000::2222
authentication spi decimal 512 key hex 12345678123456781234567812345678
exit
```

例：IPv6 モバイル ルータ インターフェイスでのローミングのイネーブル化

次の例では、IPv6 モバイル ルータ インターフェイスでローミングをイネーブルにする方法を示します。

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 mobile router-service roam
```

例：モバイル IPv6 のホスト グループの設定

次の例では、group1 という名前のモバイル IPv6 ホスト グループを設定する方法を示します。

```
ipv6 mobile host group group1
  nai sri@cisco.com
  address autoconfig
  authentication spi 500 key ascii cisco
```

その他の関連資料

関連資料

関連項目	参照先
IPv6 のサポート機能リスト	「*Start Here: Cisco IOS Software Release Specifics for IPv6 Features*」
IPv6 コマンド：コマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS IPv6 Command Reference*』
IPv6 簡易パケット ヘッダー、IPv6 ネイバー探索、IPv6 ステートレス自動設定、IPv6 ステートフル自動設定	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing IPv6 Addressing and Basic Connectivity」
IPv6 アクセス リスト	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing Traffic Filters and Firewalls for IPv6 Security」
IPv6 トンネリング	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing Tunneling for IPv6」
IPv4 モビリティの設定とコマンド	• 『*Cisco IOS IP Mobility Configuration Guide*』 • 『*Cisco IOS IP Mobility Command Reference*』

規格

規格	タイトル
この機能によってサポートされる新しい規格または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 3775	『*Mobility Support in IPv6*』
RFC 3846	『*Mobile IPv4 Extension for Carrying Network Access Identifiers*』
RFC 3963	『*Network Mobility (NEMO) Basic Support Protocol*』
RFC 4282	『*The Network Access Identifier*』
RFC 4283	『*Mobile Node Identifier Option for Mobile IPv6 (MIPv6)*』
RFC 4285	『*Authentication Protocol for Mobile IPv6*』
draft-ietf-nemo-terminology	『*Network Mobility Support Terminology*』
draft-ietf-nemo-home-network-models	『*NEMO Home Network Models* 』
draft-thubert-nemo-ipv4-traversal	『*IPv4 Traversal for MIPv6 Mobile Routers*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

モバイル IPv6 の実装の機能情報

表 1 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どのソフトウェア イメージが特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1　モバイル IPv6 の実装の機能情報

機能名	リリース	機能情報
モバイル IPv6 ホーム エージェント	12.3(14)T 12.4	モバイル IPv6 機能では、IPv6 アドレス空間を使用して、任意の種類の大規模環境でのモバイル IP 展開をイネーブルにします。モバイル IPv6 を使用するために外部エージェントは不要です。 この機能に関する詳細については、次の各項を参照してください。 • 「モバイル IPv6 ホーム エージェント」（P.3） • 「ルータでのモバイル IPv6 のイネーブル化」（P.8） • 「モバイル IPv6 のバインディング情報の設定」（P.9） • 「インターフェイスでのモバイル IPv6 のカスタマイズ」（P.19） • 「例：ルータでのモバイル IPv6 のイネーブル化」（P.24）
モバイル IPv6 の IPv6 ACL 拡張	12.4(2)T 12.2(33)SRB 12.2(33)SXI 15.0(1)S	IPv6 アクセス リストを設定して、モバイル IPv6 固有の ICMP メッセージと一致する IPv6 アクセス リスト エントリを設定したり、モバイル IPv6 拡張ヘッダーを含むパケットに一致するエントリを定義したりできます。 この機能に関する詳細については、次の各項を参照してください。 • 「モバイル IPv6 のパケット ヘッダー」（P.5） • 「モバイル IPv6 プロトコル ヘッダーおよびオプションのフィルタリング」（P.14） • 「ICMP 到達不能メッセージの制御」（P.15）

表 1　モバイル IPv6 の実装の機能情報 （続き）

機能名	リリース	機能情報
モバイル IP：モバイル IPv6 HA フェーズ 2	12.4(11)T	モバイル IPv6 のこの開発フェーズには、NAI、代替認証、およびネイティブ IPv6 トンネル インフラストラクチャのサポートが含まれます。 これらの機能に関する詳細については、次の各項を参照してください。 • 「モバイル IPv6 トンネルの最適化」（P.6） • 「IPv6 ホスト グループの設定」（P.6） • 「NAI に基づくモバイル IPv6 ノードの識別」（P.6） • 「モバイル IPv6 の認証プロトコル」（P.7） • 「モバイル IPv6 のネイティブ IPv6 トンネリングの検証」（P.16） • 「モバイル IPv6 のホスト グループの設定と検証」（P.17） • 「例：モバイル IPv6 のホスト グループの設定」（P.26）
モバイル ネットワーク v6：基本 NEMO	12.4(20)T	Network Mobility（NEMO; ネットワーク モビリティ）基本サポート プロトコルにより、モバイル IPv6 ネットワークをインターネット上の異なるポイントに接続できます。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 NEMO」（P.3） • 「NEMO 対応ホーム エージェント」（P.4） • 「NEMO での IPv6 ネイバー探索重複アドレス検出」（P.6） • 「IPv6 モバイル ルータでの NEMO のイネーブルと設定」（P.10） • 「IPv6 モバイル ルータ ホーム エージェントでの NEMO のイネーブル化」（P.12） • 「IPv6 モバイル ルータ インターフェイスでのローミングのイネーブル」（P.13） • 「例：IPv6 モバイル ルータでの NEMO のイネーブル化と設定」（P.24） • 「例：IPv6 モバイル ルータ ホーム エージェントでの NEMO のイネーブル化」（P.25） • 「例：IPv6 モバイル ルータ インターフェイスでのローミングのイネーブル化」（P.26）

IPv6 マルチキャストの実装

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

この章では、ネットワークに IPv6 マルチキャストを実装するときに必要な概念と作業について説明します。

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「IPv6 マルチキャストの実装の機能情報」（P.79）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

IPv6 マルチキャストの実装の前提条件

- ルータで IPv6 マルチキャスト ルーティングをイネーブルにするためには、そのルータで最初に IPv6 ユニキャスト ルーティングをイネーブルにする必要があります。ルータで IPv6 ユニキャスト ルーティングをイネーブルにする方法については、「*Implementing IPv6 Addressing and Basic Connectivity*」を参照してください。
- すべてのインターフェイスで IPv6 ユニキャスト ルーティングをイネーブルにする必要があります。
- この章では、IPv6 アドレッシングおよび基本設定に精通していることを前提としています。詳細については、「*Implementing IPv6 Addressing and Basic Connectivity*」の章を参照してください。
- この章では、IPv4 に精通していることを前提としています。IPv4 の設定およびコマンド リファレンス情報については、「その他の関連資料」に記載されている資料を参照してください。

IPv6 マルチキャストの実装の制約事項

- Cisco IOS ソフトウェアの IPv6 マルチキャストでは、MLD バージョン 2 が使用されます。この MLD バージョンは、MLD バージョン 1 と完全な下位互換性があります（RFC 2710 で規定）。MLD バージョン 1 だけをサポートするホストは、MLD バージョン 2 を実行しているルータと相互運用します。MLD バージョン 1 ホストと MLD バージョン 2 ホストの両方が混在する LAN もサポートされています。
- Cisco IOS Release 12.3(2)T、Cisco IOS Release 12.2(18)S、および Cisco IOS Release 12.0(26)S では、IPv6 マルチキャストは IPv4 トンネルだけでサポートされています。
- ネットワークで双方向（bidir）範囲が使用されている場合は、そのネットワーク内のすべてのルータが Bootstrap Message（BSM; ブートストラップ メッセージ）内の双方向範囲を理解できる必要があります。
- **ipv6 unicast-routing** コマンドを設定すると、IPv6 マルチキャスト ルーティングがデフォルトでディセーブルになります。Cisco Catalyst 6500 および Cisco 7600 シリーズ ルータで IPv6 ユニキャスト ルーティングを使用するためには、**ipv6 multicast-routing** もイネーブルにする必要があります。

プラットフォーム固有の情報および制約事項

Cisco IOS Release 12.0(26)S では、IPv6 マルチキャストは次のラインカードの Cisco 12000 シリーズ インターネット ルータだけでサポートされています。

- IP Service Engine（ISE; IP サービス エンジン）：
  - 4 ポート ギガビット イーサネット ISE
  - 4 ポート OC-3c/STM-1c POS/SDH ISE
  - 8 ポート OC-3c/STM-1c POS/SDH ISE
  - 16 ポート OC-3c/STM-1c POS/SDH ISE
  - 4 ポート OC-12c/STM-4c POS/SDH ISE
  - 1 ポート OC-48c/STM-16c POS/SDH ISE
- Engine 4 Plus（E4+）Packet-over-SONET（POS）：
  - 4 ポート OC-48c/STM-16c POS/SDH
  - 1 ポート OC-192c/STM-64c POS/SDH

Cisco 12000 シリーズ ラインカードでは、IPv6 マルチキャスト機能には、Protocol Independent Multicast Sparse Mode（PIM-SM; PIM 希薄モード）、Multicast Listener Discovery（MLDv2; マルチキャスト リスナー ディスカバリ）、スタティック mroute、および IPv6 分散型 Multicast Forwarding Information Base（MFIB; マルチキャスト転送情報ベース）のサポートが含まれています。

IPv6 マルチキャスト トラフィックの転送は、IPv6 マルチキャストをサポートする Cisco 12000 シリーズ IP Service Engine（ISE; IP サービス エンジン）ラインカードではハードウェアベースであり、サポートされている他のすべての Cisco 12000 シリーズ ラインカードではソフトウェアベースです。

Cisco 12000 シリーズ ISE ラインカードでの IPv6 マルチキャストの実装では、IPv6 マルチキャスト ルートの数が Ternary Content Addressable Memory（TCAM）のハードウェア容量を超える場合に、IPv6 マルチキャスト ルートの TCAM ハードウェア容量を増やす方法を示す次のエラー メッセージが表示されます。

```
EE48-3-IPV6_TCAM_CAPACITY_EXCEEDED: IPv6 multicast pkts will be software switched.
To support more IPv6 multicast routes in hardware:
 Get current TCAM usage with: show controllers ISE <slot> tcam
 In config mode, reallocate TCAM regions e.g. reallocate Netflow TCAM to IPv6 Mcast
  hw-module slot <num> tcam carve rx_ipv6_mcast <v6-mcast-percent>
  hw-module slot <num> tcam carve rx_top_nf <nf-percent>
 Verify with show command that sum of all TCAM regions = 100%
 Reload the linecard for the new TCAM carve config to take effect
WARNING: Recarve may affect other input features(ACL,CAR,MQC,Netflow)
```

TCAM は IPv6 マルチキャスト転送ルックアップで使用されます。IPv6 マルチキャスト ルートを処理するための TCAM 容量を増やすには、特権 EXEC モードで **hw-module slot** *number* **tcam carve rx_ipv6_mcast** *v6-mcast-percentage* コマンドを使用する必要があります。*v6-mcast-percentage* では、IPv6 マルチキャスト プレフィクスで使用される TCAM ハードウェアの割合を指定します。

たとえば、次のように、NetFlow リージョンを 35%（デフォルト）から 20% に再割り当てすることによって、TCAM ハードウェアの IPv6 マルチキャスト リージョンを 1%（デフォルト）から 16% に変更できます。

```
Router# hw-module slot 3 tcam carve rx_ipv6_mcast 16
Router# hw-module slot 3 tcam carve rx_nf  20
```

IPv6 マルチキャストをイネーブルにした Cisco 12000 シリーズ ルータでは、IPv6 が設定されたサブインターフェイスを削除した場合、またはサブインターフェイス上で IPv6 をディセーブルにした場合、関連するメイン インターフェイスがリセットされます。

（注） Cisco IOS Release 12.0(32)SY11 および 12.0(33)S7 からは、サブインターフェイスを削除したり、サブインターフェイス上で IPv6 をディセーブルにしたりしても、そのサブインターフェイスに関連するメイン インターフェイスにまだ IPv6 が設定されているサブインターフェイスがある場合は、そのメイン インターフェイスはリセットされません。

IPv6 マルチキャスト ハードウェア転送は、Cisco IOS Release 12.2(18)SXE の Cisco Catalyst 6500 および 7600 シリーズでサポートされています。

IPv6 マルチキャストの実装に関する情報

IPv6 マルチキャストの概要

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

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

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

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

マルチキャスト グループ内の受信側に対して、1 つのマルチキャスト アドレスが選択されます。送信側は、グループのすべてのメンバに到達するために、そのアドレスをデータグラムの宛先アドレスとして使用します。

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

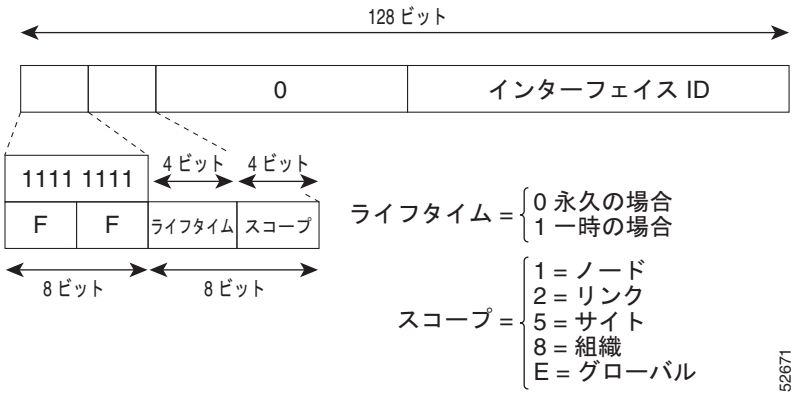
マルチキャスト グループがどの程度アクティブであるか、その期間、およびメンバシップはグループおよび状況によって異なります。メンバが存在するグループに、アクティビティがないこともあります。

IPv6 マルチキャスト アドレッシング

IPv6 マルチキャスト アドレスは、FF00::/8（1111 1111）というプレフィクスを持つ IPv6 マルチキャスト アドレスです。IPv6 マルチキャスト アドレスは、通常は異なるノードに属するインターフェイスのセットの識別子です。マルチキャスト アドレスに送信されたパケットは、マルチキャスト アドレスが示すすべてのインターフェイスに配信されます。プレフィクスに続く 2 番めのオクテットで、マルチキャスト アドレスのライフタイムとスコープが定義されます。永続マルチキャスト アドレスはライフタイム パラメータが 0 と等しく、一時マルチキャスト アドレスはライフタイム パラメータが 1 と等しくなっています。ノード、リンク、サイト、または組織のスコープ、またはグローバル スコープを持

つマルチキャスト アドレスのスコープ パラメータは、それぞれ 1、2、5、8、E です。たとえば、プレフィクスが FF02::/16 のマルチキャスト アドレスは、リンク スコープを持つ永続マルチキャスト アドレスです。図 1 に、IPv6 マルチキャスト アドレスの形式を示します。

図 1　　IPv6 マルチキャスト アドレスの形式



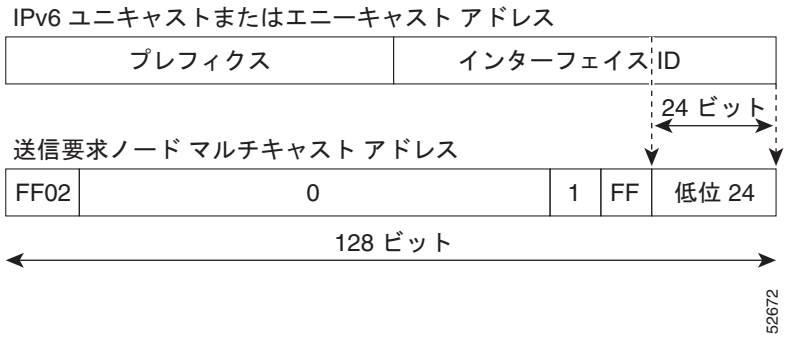
IPv6 ノード（ホストとルータ）は、（受信パケットの宛先となる）次のマルチキャスト グループに加入する必要があります。

- 全ノード マルチキャスト グループ FF02:0:0:0:0:0:0:1（スコープはリンクローカル）
- 割り当てられたユニキャスト アドレスおよびエニーキャスト アドレスごとの請求ノード マルチキャスト グループ FF02:0:0:0:0:1:FF00:0000/104

IPv6 ルータは、全ルータ マルチキャスト グループ FF02:0:0:0:0:0:0:2（スコープはリンクローカル）にも加入する必要があります。

請求ノード マルチキャスト アドレスは、IPv6 ユニキャスト アドレスまたはエニーキャスト アドレスに対応するマルチキャスト グループです。IPv6 ノードは、割り当てられているユニキャスト アドレスおよびエニーキャスト アドレスごとに、関連付けられた請求ノード マルチキャスト グループに加入する必要があります。IPv6 請求ノード マルチキャスト アドレスには、対応する IPv6 ユニキャスト アドレスまたは IPv6 エニーキャスト アドレスの下位 24 ビットに連結されたプレフィクス FF02:0:0:0:0:1:FF00:0000/104 があります（図 2 を参照）。たとえば、IPv6 アドレス 2037::01:800:200E:8C6C に対応する請求ノード マルチキャスト アドレスは FF02::1:FF0E:8C6C です。請求ノード アドレスは、ネイバー請求メッセージで使用されます。

図 2　　IPv6 請求ノード マルチキャスト アドレスの形式



（注） IPv6 にはブロードキャスト アドレスはありません。IPv6 マルチキャスト アドレスがブロードキャスト アドレスの代わりに使用されます。

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。インターフェイスでサイトローカルまたはグローバル 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。

- インターフェイスに割り当てられたユニキャスト アドレスおよびエニーキャスト アドレスごとの請求ノード マルチキャスト グループ FF02:0:0:0:0:1:FF00::/104
- 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） 請求ノード 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。

IPv6 アドレスの設定の詳細については、「*Implementing IPv6 Addressing and Basic Connectivity*」を参照してください。

限定スコープ アドレス アーキテクチャ

IPv6 では、グローバル アドレスと非グローバル アドレスがサポートされています。ここでは、異なるスコープの IPv6 アドレスの使用方法について説明します。

スコープ ゾーン（簡単にはゾーン）とは、特定のスコープのトポロジの、接続されているリージョンです。たとえば、特定のサイト内のルータが接続しているリンクのセット、およびこれらのリンクに接続されているインターフェイスは、サイトローカル スコープの単一のゾーンを構成します。

ゾーンはトポロジ リージョンの特定のインスタンス（たとえば、ゾーン 1 のサイトまたはゾーン 2 のサイト）であるのに対し、スコープはトポロジ リージョンの規模（たとえば、サイトまたはリンク）です。特定の非グローバル アドレスに関連するゾーンは、アドレス自体では符号化されません。ただし、その代わりに、その送受信を行うインターフェイスなどのコンテキストによって判別されます。したがって、特定の非グローバル スコープのアドレスは、そのスコープの別々のゾーンで再利用される場合があります。たとえば、ゾーン 1 のサイトとゾーン 2 のサイトのそれぞれに、サイトローカル アドレス FEC0::1 を持つノードが含まれている場合があります。

異なるスコープのゾーンは、次のようにインスタンス化されます。

- 各リンク、およびそのリンクに接続されているインターフェイスは、リンクローカル スコープの単一のゾーン（ユニキャストおよびマルチキャストの両方に使用）を構成します。
- インターネットのすべてのリンクおよびインターフェイスで構成されるグローバル スコープの単一のゾーン（ユニキャストおよびマルチキャストの両方に使用）もあります。
- インターフェイスローカル、リンクローカル、およびグローバル以外のスコープのゾーンの境界については、ネットワーク管理者が定義および設定する必要があります。ユニキャストおよびマルチキャストの両方で、サイト境界が境界として機能します。

ゾーン境界は、比較的スタティックな機能であり、トポロジにおける短期的な変更に応じて変化することはありません。したがって、ゾーン内のトポロジが「接続されている必要がある」という要件は、一時的にだけ接続されることがあるリンクとインターフェイスを含めるためのものです。たとえば、ダイ

ヤルアップにより従業員のサイトへのインターネット アクセスを取得するレジデンシャル ノードまたはネットワークは、ダイヤルアップ リンクが切断された場合でも、従業員のサイトローカル ゾーンの一部として扱われることがあります。同様に、ゾーンのパーティション化を引き起こすルータ、インターフェイス、またはリンクの障害が発生しても、そのゾーンが複数のゾーンに分割されることはありません。厳密には、別個のパーティションが引き続き同じゾーンに属しているものと見なされます。

ゾーンには、他にも次の特性があります。

- ゾーン境界はリンクではなくノードを横断します（グローバル ゾーンには境界はなく、インターフェイスローカル ゾーンの境界には 1 つのインターフェイスだけが含まれています）。
- 同じスコープのゾーンは重なることができません。つまり、共通するリンクまたはインターフェイスを持つことはできません。
- （グローバルより小さい）特定のスコープのゾーンは、それより大きいスコープのゾーン内に完全に含まれます。つまり、小さいスコープのゾーンには、リンクまたはインターフェイスを共有する大きいスコープのゾーンを超えるトポロジを含めることはできません。
- 各インターフェイスは、それぞれのスコープの 1 つのゾーンに厳密に属しています。

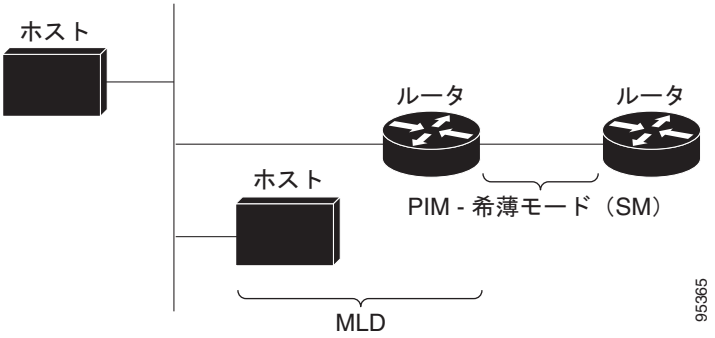
IPv6 マルチキャスト ルーティングの実装

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

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

図 3 に、IPv6 マルチキャスト環境で MLD と PIM-SM が動作する場所を示します。

図 3　IPv6 でサポートされている IPv6 マルチキャスト ルーティング プロトコル



マルチキャスト リスナー ディスカバリ プロトコル for IPv6

キャンパス ネットワークでマルチキャストの実装を開始するには、最初にマルチキャストの受信対象を定義する必要があります。MLD プロトコルは、直接接続されているリンク上のマルチキャスト リスナーの存在（たとえば、マルチキャスト パケットの受信を希望するノード）を検出したり、これらのネイバー ノードが対象としているマルチキャスト アドレスを具体的に検出したりするために IPv6 ルータで使用されます。また、ローカル グループおよび送信元固有のグループ メンバシップを検出するためにも使用されます。MLD プロトコルは、特別なマルチキャスト クエリアおよびホストを使用して、ネットワーク全体でマルチキャスト トラフィックのフローを自動的に制御および制限する手段を提供します。

マルチキャスト クエリアおよびホストの違いは次のとおりです。

- クエリアは、クエリー メッセージを送信して、特定のマルチキャスト グループのメンバであるネットワーク デバイスを検出するネットワーク デバイス（ルータなど）です。
- ホストは、レポート メッセージを送信して、クエリアにホスト メンバシップを通知する受信側（ルータを含む）です。

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

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

MLD では、次の 3 種類のメッセージが使用されます。

- クエリー：一般、グループ固有、およびマルチキャスト アドレス固有のクエリーです。MLD から一般クエリーが送信されるとき、クエリー メッセージ内のマルチキャスト アドレス フィールドは 0 に設定されます。一般クエリーでは、接続されているリンク上にリスナーが存在するマルチキャスト アドレスを学習します。

  グループ固有のクエリーおよびマルチキャスト アドレス固有のクエリーは同じです。グループ アドレスはマルチキャスト アドレスです。

- レポート：レポート メッセージでは、マルチキャスト アドレス フィールドは、送信側がリッスンしている特定の IPv6 マルチキャスト アドレスのフィールドになります。
- 完了：完了メッセージでは、マルチキャスト アドレス フィールドは、MLD メッセージの送信元が今後リッスンしない特定の IPv6 マルチキャスト アドレスのフィールドになります。

MLD レポートの送信には、有効な IPv6 リンクローカル送信元アドレスを使用するか、または送信側インターフェイスが有効なリンクローカル アドレスをまだ取得していない場合は未指定アドレス（::）を使用する必要があります。ネイバー探索プロトコルでの IPv6 マルチキャストの使用をサポートするために、未指定アドレスを使用してレポートを送信できるようになっています。

ステートレス自動設定で Duplicate Address Detection（DAD; 重複アドレス検出）を実行するためには、ノードは複数の IPv6 マルチキャスト グループに加入する必要があります。DAD よりも前に、レポート ノードで送信側インターフェイス用として使用される唯一のアドレスは暫定的なものであり、通信には使用できません。そのため、未指定アドレスを使用する必要があります。

MLD バージョン 2 または MLD バージョン 1 のメンバシップ レポートから生成される MLD ステートは、グローバルに、またはインターフェイス単位で制限できます。MLD グループ制限機能は、MLD パケットによって生じる Denial of Service（DoS; サービス拒絶）攻撃に対する保護を提供します。設定されている制限を超過するメンバシップ レポートは MLD キャッシュには格納されず、これらの超過メンバシップ レポートのトラフィックは転送されません。

MLD では、送信元フィルタリングがサポートされています。送信元フィルタリングにより、特定の送信元アドレスからのパケット（SSM をサポートするのに必要）、または特定の送信元アドレスを除くすべてのアドレスから特定のマルチキャスト アドレスに送信されたパケットをリッスンする対象をノードがレポートできるようになります。

MLD バージョン 1 を使用するホストが脱退メッセージを送信した場合、ルータはクエリー メッセージを送信することによって、このホストがグループに加入している最後の MLD バージョン 1 ホストであることを再確認する必要があります。再確認後、トラフィックの転送を停止できます。この処理には約 2 秒かかります。この「脱退遅延」は、IPv4 マルチキャスト対応 IGMP バージョン 2 にも存在します。

MLD アクセス グループ

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

受信側の明示的トラッキング

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

マルチキャスト ユーザ認証およびプロファイル サポート

IPv6 マルチキャストは、ネットワーク内の任意のホストがマルチキャスト グループの受信側または送信元になれる設計になっています。したがって、ネットワークのマルチキャスト トラフィックを制御するには、マルチキャスト アクセス コントロールが必要です。アクセス コントロール機能は、主に、送信元のアクセス コントロールとアカウンティング、受信側のアクセス コントロールとアカウンティング、およびこのアクセス コントロール メカニズムのプロビジョニングで構成されます。

マルチキャスト アクセス コントロールは、マルチキャストと Authentication, Authorization, Accounting（AAA; 認証、認可、アカウンティング）の間のインターフェイスを提供し、ラストホップ ルータ、マルチキャストにおける受信側アクセス コントロール機能、およびマルチキャストにおけるグループまたはチャネル ディセーブル化機能でのプロビジョニング、認可、およびアカウンティングを実現します。

新しいマルチキャスト サービス環境を展開する場合、ユーザ認証を追加し、インターフェイス単位でユーザ プロファイルのダウンロードを行う必要があります。AAA と IPv6 マルチキャストを使用すると、マルチキャスト環境でのユーザ認証とユーザ プロファイルのダウンロードがサポートされます。

RADIUS サーバからアクセス ルータへのマルチキャスト キャスト アクセス コントロール プロファイルのダウンロードをトリガーするイベントは、アクセス ルータへの MLD join の着信です。このイベントが発生すると、ユーザはタイムアウトする認可キャッシュを調べ、ダウンロードを定期的に要求したり、適切なマルチキャスト クリア コマンドを使用して、プロファイルが変更された場合に新しいダウンロードをトリガーしたりできるようになります。

アカウンティングは RADIUS アカウンティングを使用して行われます。開始および停止アカウンティング レコードは、アクセス ルータから RADIUS サーバに送信されます。リソースの消費をストリーム単位で追跡できるように、これらのアカウンティング レコードには、マルチキャスト送信元およびグループに関する情報が含まれています。ラストホップ ルータが新しい MLD レポートを受信すると、開始レコードが送信され、MLD leave を受信するか、何らかの理由によりグループまたはチャネルが削除されると、停止レコードが送信されます。

MLD プロキシ

MLD プロキシ機能は、ルータのアップストリーム インターフェイス上のすべての（*, G）/（S, G）エントリまたはこれらのエントリのユーザ定義のサブセットについてルータが MLD メンバシップ レポートを生成するメカニズムを提供します。MLD プロキシ機能により、デバイスは、プロキシ グループ メンバシップ情報を学習し、その情報に基づいてマルチキャスト パケットを転送できるようになります。

ルータが mroute プロキシ エントリの RP として動作する場合、これらのエントリの MLD メンバシップ レポートを、ユーザが指定したプロキシ インターフェイス上で生成できます。

プロトコル独立マルチキャスト

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

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

PIM 希薄モード

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

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

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

PIM join がツリーの上位方向に送信されると、要求されたマルチキャスト トラフィックがツリーの下位方向に転送されるように、パス上のルータがマルチキャスト転送ステートを設定します。マルチキャスト トラフィックが今後不要になると、ルータは PIM prune をルート ノードに向けてツリーの上位方向に送信し、不要なトラフィックを削除します（脱退処理）。この PIM prune がツリーの上位方向にホップバイホップで送信されると、各ルータはその転送ステートを適切にアップデートします。最終的に、マルチキャスト グループまたは送信元に関連付けられている転送ステートは削除されます。

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

代表ルータ

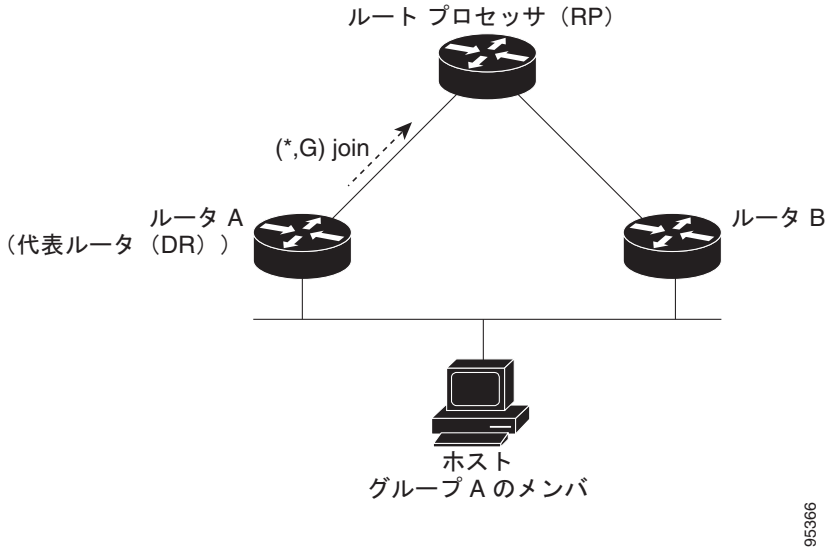
Cisco ルータは、LAN セグメント上に複数のルータが存在する場合、PIM-SM を使用してマルチキャスト トラフィックを転送し、選択プロセスに従って代表ルータを選択します。

代表ルータは、PIM register と PIM join および prune メッセージを RP に向けて送信し、ホスト グループ メンバシップについて通知します。

LAN 上に複数の PIM-SM ルータが存在する場合は、代表ルータを選択して、接続されているホストに対するマルチキャスト トラフィックの重複を回避する必要があります。**ipv6 pim dr-priority** コマンドを使用して DR の選択を強制しないかぎり、最上位 IPv6 アドレスを持つ PIM ルータが LAN の DR になります。このコマンドでは、LAN セグメント上の各ルータの DR プライオリティ（デフォルトのプライオリティ = 1）を指定して、最もプライオリティの高いルータが DR として選択されるようにすることができます。LAN セグメント上のすべてのルータのプライオリティが同じ場合にも、最上位 IPv6 アドレスを持つルータが選択されます。

図 4 に、マルチアクセス セグメントでの動作を示します。ルータ A およびルータ B は、ホスト A をグループ A のアクティブな受信側として使用する共通のマルチアクセス イーサネット セグメントに接続されます。DR として動作するルータ A だけが join を RP に送信して、グループ A の共有ツリーを構築します。ルータ B も RP への（*, G）join の送信を許可されている場合は、パラレル パスが作成され、ホスト A が重複マルチキャスト トラフィックを受信します。ホスト A がグループにマルチキャスト トラフィックを送信し始めたら、DR は register メッセージを RP に送信する役割を担います。両方のルータに役割が割り当てられている場合は、RP が重複マルチキャスト パケットを受信します。

図 4　マルチアクセス セグメントでの代表ルータの選択



DR で障害が発生した場合、PIM-SM はルータ A の障害を検出し、フェールオーバー DR を選択する手段を提供します。DR（ルータ A）が動作不能になると、ルータ A とのネイバー ルータとの隣接関係がタイムアウトしたときに、ルータ B はその状況を検出します。ルータ B はホスト A から MLD メンバシップ レポートを受けているため、このインターフェイスでグループ A の MLD ステートをすでに持ち、新しい DR になると即座に RP に join を送信します。この段階で、ルータ B を経由する共有ツリーの新しいブランチの下位方向へのトラフィック フローが再び確立されます。また、ホスト A がトラフィックを送信していた場合、ルータ B は、ホスト A から次のマルチキャスト パケットを受信した直後に、新しい登録プロセスを開始します。このアクションがトリガーとなって、RP は、ルータ B を経由する新しいブランチを介して、ホスト A への SPT に加入します。

ヒント　2 つの PIM ルータが直接接続されている場合、これらのルータはネイバーになります。PIM ネイバーを表示するには、特権 EXEC モードで **show ipv6 pim neighbor** コマンドを使用します。

（注）　DR 選択プロセスは、マルチアクセス LAN でだけ必要になります。ホストに直接接続されているラストホップ ルータが DR になります。

ランデブー ポイント

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

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

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

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

- データは register パケットにカプセル化され、DR として動作するファーストホップ ルータによって RP に直接ユニキャストされます。
- RP 自身が送信元ツリーに加入している場合は、「PIM 希薄モード」で説明したように、RPF 転送アルゴリズムに従ってマルチキャスト転送されます。

RP アドレスは、パケットをグループに送信するホストの代わりに、ファーストホップ ルータで PIM register メッセージを送信するために使用されます。また、ラストホップ ルータでも、PIM join および prune メッセージを RP に送信してグループ メンバシップについて通知するために使用されます。すべてのルータ（RP ルータを含む）で RP アドレスを設定する必要があります。

1 つの PIM ルータを複数のグループの RP にすることができます。特定のグループの PIM ドメイン内で一度に使用できる RP アドレスは 1 つだけです。アクセス リストで指定されている条件によって、ルータがどのグループの RP であるかが判別されます。

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

IPv6 BSR

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

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

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

RP マッピングを設定するための IPv6 BSR 機能を使用すると、スコープと RP のマッピングを候補 RP メッセージから学習する代わりに、BSR から直接アナウンスするように、IPv6 マルチキャスト ルータをスタティックに設定できます。BSR から RP マッピングをアナウンスすると、次のいくつかの状況で役立ちます。

- RP が 1 つしか存在しないか、またはグループ範囲でエニーキャスト RP が使用されているために、RP アドレスが変わらない場合、候補 BSR で RP アドレス通知をスタティックに設定することは容易になります。
- RP アドレスが仮想 RP アドレスである場合（双方向 PIM を使用している場合など）、BSR はそのアドレスを候補 RP から学習できません。その代わりに、候補 BSR で仮想 RP アドレスをアナウンス対象 RP として設定する必要があります。

Cisco IOS IPv6 ルータでは、BSM のフローを妨げることがないように、BSR パケットの RPF フラッディングがサポートされています。ルータは、BSM を十分に認識および解析して、BSR アドレスを識別します。ルータは、この BSR アドレスの RPF チェックを実行し、RPF インターフェイスで受信したパケットだけを転送します。また、RPF 情報を含む BSR エントリを作成し、同じ BSR からの今後の BSM に使用できるようにします。特定の BSR から BSM を今後受信しなくなると、BSR エントリはタイムアウトします。

双方向 BSR がサポートされているため、双方向 RP を C-RP メッセージおよび BSM の双方向範囲でアドバタイズできます。システム内のすべてのルータが BSM の双方向範囲を使用できる必要があります。そうでないと、双方向 RP 機能は動作しません。

BSR では、管理用スコープのマルチキャストを使用してネットワークでグループと RP のマッピングを配布することによって、限定スコープ ゾーンをサポートしています。ユーザは、ドメイン内の管理用スコープ領域ごとに候補 BSR と一連の候補 RP を設定できます。

管理用スコープで BSR が正しく機能するようにするには、BSR と少なくとも 1 つの C-RP がすべての管理用スコープ領域内に存在している必要があります。管理用スコープ ゾーンの境界は、Zone Border Router（ZBR; ゾーン境界ルータ）で設定する必要があります。これは、エラー条件が原因で境界を間違って越える可能性がある PIM join メッセージをフィルタリングする必要があるためです。また、管理用スコープ ゾーン内の少なくとも 1 つの C-BSR が、管理用スコープ ゾーンのアドレス範囲の C-BSR になるように設定する必要があります。

これにより、BSR 選択は、（BSM を使用して）管理用スコープ範囲ごとに 1 回、およびグローバル範囲に対して 1 回行われるようになります。管理用スコープ範囲は BSM で識別されます。これは、特定の RP セットで処理するように設定されている範囲だけでなく、管理用スコープ範囲であることを示すように、グループ範囲がマーク付けされているためです。

C-RP にスコープが設定されていない場合、その C-RP は、スコープ ゾーンのグループ範囲を含む選択 BSR から BSM を受信することによって、管理用スコープ ゾーンの有無およびそのグループ範囲を検出します。C-RP には、各選択 BSR のアドレスとその BSM に含まれる管理用スコープ範囲が格納されます。C-RP は、RP として動作する意思のある管理用スコープ範囲ごとに C-RP-Adv メッセージを適切な BSR に個別にユニキャストします。

管理用スコープ範囲が使用中の PIM ブートストラップ ドメイン内のすべての PIM ルータが、BSM を受信し、該当するすべての管理用スコープ ゾーンに対する選択 BSR と RP のセットを格納できる必要があります。

PIM 送信元固有マルチキャスト

PIM-SSM は、SSM の実装をサポートするルーティング プロトコルであり、PIM-SM から派生したものです。ただし、PIM-SM では PIM join を受けてすべてのマルチキャスト送信元からデータが送信されるのに対し、SSM 機能では、受信側が明示的に加入しているマルチキャスト送信元だけからその受信側にデータグラム トラフィックが転送されます。これにより、帯域利用率が最適化され、不要なインターネット ブロードキャスト トラフィックが拒否されます。さらに、SSM では、RP と共有ツリーを使用する代わりに、マルチキャスト グループの送信元アドレスで見つかった情報を使用します。こ

の情報は、MLD メンバシップ レポートによってラストホップ ルータにリレーされる送信元アドレスを通して受信側から提供されます。その結果として、送信元に直接つながる最短パス ツリーが得られます。

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

SSM を動作させるには、MLD バージョン 2 が必要です。MLD を使用すると、ホストが送信元の情報を提供できるようになります。MLD を使用して SSM を動作させるには、Cisco IOS IPv6 ルータ、アプリケーションが実行されているホスト、およびアプリケーション自体で SSM がサポートされている必要があります。

IPv6 用の SSM マッピング

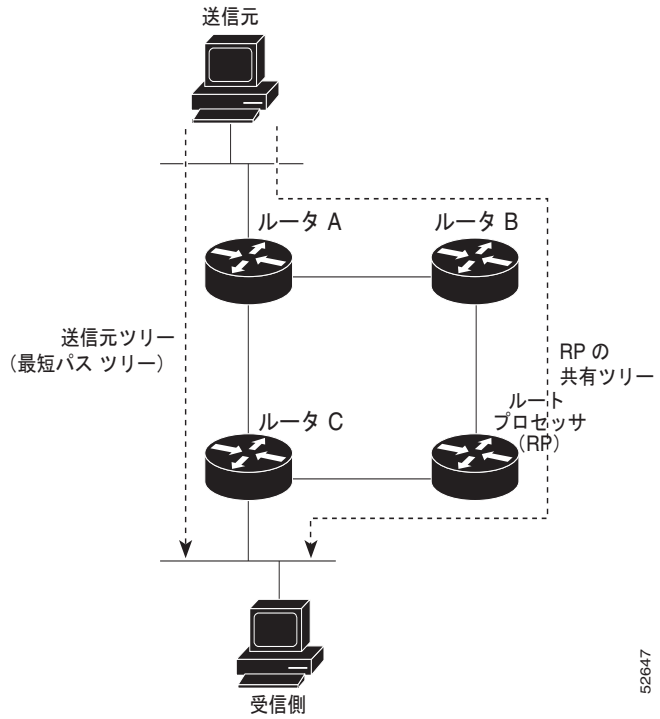
IPv6 用の SSM マッピングでは、MLD バージョン 1 の受信側用にスタティックとダイナミックの両方の Domain Name System（DNS; ドメイン ネーム システム）マッピングがサポートされています。この機能を使用すると、TCP/IP ホスト スタックおよび IP マルチキャスト受信アプリケーションで MLD バージョン 2 サポートを提供できないホストで IPv6 SSM を展開できます。

SSM マッピングにより、ルータは実行コンフィギュレーションまたは DNS サーバのいずれかでマルチキャスト MLD バージョン 1 レポートの送信元を検索できるようになります。そのあと、ルータは送信元に対する（S, G）join を開始できます。

PIM 共有ツリーおよび送信元ツリー（最短パス ツリー）

デフォルトでは、グループのメンバは、RP をルートとする単一のデータ配布ツリーを通じて、送信側からグループへのデータを受信します。このタイプの配布ツリーは、共有ツリーまたは Rendezvous Point Tree（RPT; ランデブー ポイント ツリー）と呼ばれます（図 5 を参照）。送信側からのデータは、RP に配信され、その共有ツリーに加入しているグループ メンバに配布されます。

図 5　　共有ツリーおよび送信元ツリー（最短パス ツリー）



データしきい値で保証される場合、共有ツリー上のリーフ ルータは、送信元をルートとするデータ配布ツリーへの切り替えを開始できます。このタイプの配布ツリーは、最短パス ツリーまたは送信元ツリーと呼ばれます。デフォルトでは、Cisco IOS ソフトウェアは、送信元から最初のデータ パケットを受信した時点で、送信元ツリーへの切り替えを行います。

次に、共有ツリーから送信元ツリーに切り替わるプロセスの詳細を示します。

1. 受信側がグループに加入します。リーフ ルータ C が RP に join メッセージを送信します。
2. RP がルータ C へのリンクを発信インターフェイス リストに登録します。
3. 送信元がデータを送信します。ルータ A が register にデータをカプセル化し、それを RP に送信します。
4. RP が共有ツリーの下位方向のルータ C にデータを転送し、送信元に join メッセージを送信します。この時点で、データはルータ C に 2 回（カプセル化された状態で 1 回、ネイティブの状態で 1 回）着信する可能性があります。
5. データがネイティブの（カプセル化されていない）状態で RP に着信すると、RP はルータ A に register-stop メッセージを送信します。
6. デフォルトでは、ルータ C は、最初のデータ パケットを受信した時点で、送信元に join メッセージを送信します。
7. ルータ C が（S, G）でデータを受信すると、ルータ C は共有ツリーの上位方向にある送信元に prune メッセージを送信します。
8. RP が（S, G）の発信インターフェイスからルータ C へのリンクを削除します。
9. RP が送信元への prune メッセージをトリガーします。

送信元および RP に join および prune メッセージが送信されます。これらのメッセージはホップバイホップで送信され、送信元または RP に向かうパス上の各 PIM ルータによって処理されます。register および register-stop メッセージは、ホップバイホップで送信されません。これらのメッセージは、送信元に直接接続されている代表ルータによって送信され、グループの RP によって受信されます。

Reverse Path Forwarding

Reverse Path Forwarding は、マルチキャスト データグラムの転送に使用されます。これは、次のように機能します。

- ルータで送信元へのユニキャスト パケットの送信に使用しているインターフェイスでデータグラムを受信すると、パケットは RPF インターフェイスに着信しています。
- パケットが RPF インターフェイスに着信した場合、ルータは、マルチキャスト ルーティング テーブル エントリの発信インターフェイス リストに存在するインターフェイスにパケットを転送します。
- パケットが RPF インターフェイスに着信しない場合、パケットはループを回避するためにサイレントにドロップされています。

PIM では、送信元ツリーと RP をルートとする共有ツリーの両方を使用してデータグラムを転送します。RPF チェックは、次のようにそれぞれ異なる方法で実行されます。

- PIM ルータが送信元ツリー ステートである場合（つまり、(S, G）エントリがマルチキャスト ルーティング テーブル内にある場合)、マルチキャスト パケットの送信元の IPv6 アドレスに対して RPF チェックが実行されます。
- PIM ルータが共有ツリー ステートである場合（および送信元ツリー ステートが明示されていない場合)、(メンバがグループに加入している場合は既知である）RP のアドレスに対して RPF チェックが実行されます。

空間モード PIM では、RPF ルックアップ機能を使用して、join および prune の送信先を決定します。(S, G）join（送信元ツリー ステート）は送信元に向けて送信されます。(*, G）join（共有ツリー ステート）は RP に向けて送信されます。

ルーティング可能アドレスの hello オプション

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

2 つの典型的な状況により、IPv6 のこの状況が生じる可能性があります。1 つめの状況は、ユニキャスト ルーティング テーブルが IPv6 内部ゲートウェイ プロトコル（マルチキャスト BGP など）によって構築されない場合に発生します。2 つめの状況は、RP のアドレスがダウンストリーム ルータとサブネット プレフィクスを共有している場合に発生します（RP ルータ アドレスはドメインワイドにする必要があるため、リンクローカル アドレスにはできないことに注意してください)。

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

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

双方向 PIM

双方向 PIM を使用すると、マルチキャスト ルータは、PIM-SM の単一方向共有ツリーと比べて縮小されたステート情報を維持できるようになります。双方向共有ツリーは、送信元から RP にデータを伝送し、それらを RP から受信側に配布します。PIM-SM とは異なり、双方向 PIM は送信元ツリーへの切り替えは実行しません。また、送信元から RP へのデータの登録カプセル化は行われません。

双方向 PIM は、中レートまたは低レートの送信元が多数存在する場合に役立ちます。ただし、双方向送信元ツリーは、PIM-SM で構築された送信元ツリーよりも、遅延特性が劣ります。

IPv6 では、双方向 RP のスタティック設定だけがサポートされています。

スタティック mroute

IPv6 スタティック mroute は、IPv6 スタティック ルートとほぼ同じように動作します。IPv6 スタティック mroute は、IPv6 スタティック ルートと同じデータベースを共有し、スタティック ルート サポートを拡張することによって実装されます。スタティック mroute では、等価コスト マルチパス mroute がサポートされています。また、ユニキャスト専用スタティック ルートもサポートされています。

IPv6 スタティック ルートの詳細については、「*Implementing Static Routes for IPv6*」を参照してください。

MRIB

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

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

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

MFIB

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

ネットワーク内でルーティングまたはトポロジが変更されると、IPv6 ルーティング テーブルがアップデートされ、これらの変更が MFIB に反映されます。MFIB は、IPv6 ルーティング テーブル内の情報に基づいて、ネクストホップ アドレス情報を管理します。MFIB エントリとルーティング テーブル エ

ントリの間には 1 対 1 の相互関係があるため、MFIB には既知のすべてのルートが含まれ、ファスト スイッチングや最適スイッチングなどのスイッチング パスに関連付けられているルート キャッシュ管理の必要がなくなります。

分散型 MFIB

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

dMFIB は、次の機能を実装します。

- ラインカードに MFIB のコピーを配布します。
- ラインカードで生成されたデータ駆動型プロトコル イベントを PIM にリレーします。
- ハードウェア アクセラレーション エンジンをプログラミングするためのプラットフォーム固有のコードに MFIB の変更を伝播する MFIB プラットフォーム Application Program Interface（API; アプリケーション プログラム インターフェイス）を提供します。また、この API には、ソフトウェアでパケットをスイッチングしたり（パケットがデータ駆動型イベントのトリガーとなっている場合に必要）、ソフトウェアにトラフィックの統計情報をアップロードしたりするエントリ ポイントも含まれています。
- RP に存在するクライアントがオンデマンドでトラフィックの統計情報を読み取れるようにするフックを提供します（dMFIB はこれらの統計情報を RP に定期的にアップロードすることはありません）。

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

IPv6 マルチキャストのプロセス スイッチングおよびファスト スイッチング

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

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

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

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

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

IPv6 マルチキャスト アドレス ファミリのマルチプロトコル BGP

IPv6 マルチキャスト アドレス ファミリのマルチキャスト BGP 機能では、マルチキャスト BGP for IPv6 拡張を提供し、IPv4 BGP と同じ機能と機能性をサポートします。マルチキャスト BGP に対する IPv6 拡張には、IPv6 マルチキャスト アドレス ファミリ、Network Layer Reachability Information（NLRI; ネットワーク レイヤ到達可能性情報）、および IPv6 アドレスを使用するネクストホップ（宛先へのパス内の次のルータ）アトリビュートのサポートが含まれています。

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

マルチキャスト BGP 機能は、個別のアドレス ファミリ コンテキストを介して提供されます。Subsequent Address Family Identifier（SAFI）では、アトリビュートで伝送されるネットワーク レイヤ到達可能性情報のタイプに関する情報を提供します。マルチプロトコル BGP ユニキャストでは SAFI 1 メッセージを使用し、マルチプロトコル BGP マルチキャストでは SAFI 2 メッセージを使用します。

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

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

IPv6 マルチキャストでの NSF と SSO のサポート

IPv6 マルチキャストでは、Nonstop Forwarding（NSF; ノンストップ フォワーディング）および Stateful Switchover（SSO; ステートフル スイッチオーバー）がサポートされています。NSF と SSO の詳細については、『*Cisco IOS High Availability Configuration Guide*』の「Stateful Switchover」および「Cisco Nonstop Forwarding」を参照してください。

IPv6 マルチキャストの帯域幅ベースの CAC

IPv6 マルチキャストの帯域幅ベースの Call Admission Control（CAC; コール アドミッション制御）機能は、コスト乗数を使用してインターフェイス単位の mroute ステート リミッタをカウントする手段を実装します。この機能を使用すると、マルチキャスト フローで異なる量の帯域幅が利用されるネットワーク環境で、インターフェイス単位の帯域幅ベースの CAC を提供できます。

この機能では、IPv6 マルチキャスト ステートを詳細に制限および考慮します。この機能を設定すると、IPv6 マルチキャスト PIM トポロジの着信インターフェイスまたは発信インターフェイスとして使用できる回数にインターフェイスを制限できます。

この機能を使用すると、ルータ管理者はアクセス リストと一致するステートに対してグローバル制限コスト コマンドを設定して、インターフェイス制限に対してこのようなステートを考慮するときに使用するコスト乗数を指定できます。この機能では、異なる帯域幅要件に応じてコスト乗数を適切に調整することによって、帯域幅ベースのローカル CAC ポリシーを柔軟に実装できます。

IPv6 マルチキャストの実装方法

IPv6 マルチキャスト ルーティングのイネーブル化

この作業では、すべてのインターフェイスで IPv6 マルチキャスト ルーティングをイネーブルにする方法、およびイネーブルになっているすべてのルータ インターフェイスで PIM および MLD に対してマルチキャスト転送をイネーブルにする方法を示します。

前提条件

ルータで IPv6 マルチキャスト ルーティングをイネーブルにするためには、そのルータで最初に IPv6 ユニキャスト ルーティングをイネーブルにする必要があります。ルータで IPv6 ユニキャスト ルーティングをイネーブルにする方法については、「*Implementing IPv6 Addressing and Basic Connectivity*」を参照してください。

IPv6 ユニキャスト ルータをすでに使用している場合に、IPv6 マルチキャスト ルーティングをイネーブルにし、IPv6 マルチキャスト ルーティング オプションを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 multicast-routing**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 multicast-routing** **例：** `Router(config)# ipv6 multicast-routing`	すべての IPv6 対応インターフェイスでマルチキャスト ルーティングをイネーブルにし、イネーブルになっているすべてのルータ インターフェイスで PIM および MLD に対してマルチキャスト転送をイネーブルにします。

MLD プロトコルのカスタマイズおよび確認

インターフェイスでの MLD のカスタマイズおよび確認

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 mld join-group** [*group-address*] [**include** | **exclude**] {*source-address* | **source-list** [*acl*]}
5. **ipv6 mld access-group** *access-list-name*
6. **ipv6 mld static-group** [*group-address*] [**include** | **exclude**] {*source-address* | **source-list** [*acl*]}
7. **ipv6 mld query-max-response-time** *seconds*
8. **ipv6 mld query-timeout** *seconds*

9. **ipv6 mld query-interval** *seconds*
10. **exit**
11. **show ipv6 mld groups** [**link-local**] [*group-name* | *group-address*] [*interface-type interface-number*] [**detail** | **explicit**]
12. **show ipv6 mld groups summary**
13. **show ipv6 mld interface** [*type number*]
14. **debug ipv6 mld** [*group-name* | *group-address* | *interface-type*]
15. **debug ipv6 mld explicit** [*group-name* | *group-address*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface FastEthernet 1/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 mld join-group** [*group-address*] [**include** | **exclude**] {*source-address* | **source-list** [*acl*]} **例：** `Router(config-if)# ipv6 mld join-group FF04::10`	指定したグループおよび送信元に対して MLD レポートを設定します。
ステップ 5	**ipv6 mld access-group** *access-list-name* **例：** `Router(config-if)# ipv6 access-list acc-grp-1`	ユーザに IPv6 マルチキャストの受信側アクセス コントロールの実行を許可します。
ステップ 6	**ipv6 mld static-group** [*group-address*] [**include** | **exclude**] {*source-address* | **source-list** [*acl*]} **例：** `Router(config-if)# ipv6 mld static-group ff04::10 include 100::1`	指定したインターフェイスにマルチキャスト グループのトラフィックをスタティックに転送し、MLD ジョイナがインターフェイスに存在するかのようにインターフェイスが動作するようにします。
ステップ 7	**ipv6 mld query-max-response-time** *seconds* **例：** `Router(config-if)# ipv6 mld query-max-response-time 20`	MLD キューにアドバタイズされる最大応答時間を設定します。

	コマンドまたはアクション	目的
ステップ 8	**ipv6 mld query-timeout** *seconds* **例：** `Router(config-if)# ipv6 mld query-timeout 130`	ルータがインターフェイスのクエリアを継承するまでのタイムアウト値を設定します。
ステップ 9	**ipv6 mld query-interval** *seconds* **例：** `Router(config-if)# ipv6 mld query-interval 60`	Cisco IOS ソフトウェアが MLD ホストクエリー メッセージを送信する頻度を設定します。 **注意** この値を変更すると、マルチキャスト転送に深刻な影響が及ぶ可能性があります。
ステップ 10	**exit** **例：** `Router(config-if)# exit`	このコマンドを 2 回入力して、インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 11	**show ipv6 mld groups** [**link-local**] [*group-name* | *group-address*] [*interface-type interface-number*] [**detail** | **explicit**] **例：** `Router# show ipv6 mld groups FastEthernet 2/1`	ルータに直接接続されており、MLD を介して学習したマルチキャスト グループを表示します。
ステップ 12	**show ipv6 mld groups summary** **例：** `Router# show ipv6 mld groups summary`	MLD キャッシュに存在する (*, G) および (S, G) メンバシップ レポートの番号を表示します。
ステップ 13	**show ipv6 mld interface** [*type number*] **例：** `Router# show ipv6 mld interface FastEthernet 2/1`	インターフェイスのマルチキャスト関連情報を表示します。

ステップ 14	`debug ipv6 mld [group-name | group-address | interface-type]`
	
	例：
	`Router# debug ipv6 mld`
		MLD プロトコル アクティビティに対するデバッグをイネーブルにします。

ステップ 15	**debug ipv6 mld explicit** [*group-name* | *group-address*] **例：** `Router# debug ipv6 mld explicit`	ホストの明示的トラッキングに関連する情報を表示します。

MLD グループ制限の実装

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

次の各作業では、MLD バージョン 2 または MLD バージョン 1 メンバシップ レポートから生じる MLD ステートをグローバルに、またはインターフェイス単位で制限する方法を示します。

- 「MLD グループ制限のグローバルな実装」（P.25）
- 「MLD インターフェイス カウンタのクリア」（P.32）

MLD グループ制限のグローバルな実装

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 mld state-limit** *number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 mld state-limit** *number* **例：** `Router(config)# ipv6 mld state-limit 300`	MLD ステートの数をグローバルに制限します。

MLD グループ制限のインターフェイス単位での実装

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface FastEthernet 1/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 mld limit** *number* [**except** *access-list*] **例：** `Router(config-if)# ipv6 mld limit 100`	MLD ステートの数をインターフェイス単位で制限します。

受信側の明示的トラッキングによってホストの動作を追跡するための設定

この作業では、受信側機能の明示的トラッキングをイネーブルにします。明示的トラッキング機能を使用すると、ルータが IPv6 ネットワーク内のホストの動作を追跡できるようになります。また、高速脱退メカニズムを MLD バージョン 2 のホスト レポートで使用できるようになります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 mld explicit-tracking** *access-list-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* **例：** `Router(config)# interface FastEthernet 1/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 mld explicit-tracking** *access-list-name* **例：** `Router(config-if)# ipv6 mld explicit-tracking list1`	ホストの明示的トラッキングをイネーブルにします。

マルチキャスト ユーザ認証およびプロファイル サポートの設定

ここでは、マルチキャスト ユーザ認証およびプロファイル サポート機能をイネーブルにして設定するためのいくつかの作業について説明します。

前提条件

マルチキャスト ユーザ認証およびプロファイル サポートを設定する前に、IPv6 マルチキャストで次の受信側アクセス コントロール機能を設定できます。

- MLD グループをグローバルに制限するには、「MLD グループ制限のグローバルな実装」（P.25）を参照してください。
- MLD グループをインターフェイス単位で制限するには、「MLD グループ制限のインターフェイス単位での実装」（P.25）を参照してください。
- インターフェイスで許可する MLD グループおよび送信元を指定するには、「インターフェイスでの MLD のカスタマイズおよび確認」（P.22）のステップ 5 を参照してください。

制約事項

マルチキャスト ユーザ認証およびプロファイル サポートを設定する前に、次の制約事項を認識しておく必要があります。

- ポート、インターフェイス、VC、または VLAN ID がユーザまたは加入者アイデンティティになります。ホスト名、ユーザ ID、またはパスワードを使用したユーザ アイデンティティはサポートされていません。

マルチキャスト ユーザ認証およびプロファイル サポートを設定するには、次の各作業を実行します。

- 「IPv6 マルチキャストに対する AAA アクセス コントロールのイネーブル化」（P.27）
- 「方式リストの指定およびマルチキャスト アカウンティングのイネーブル化」（P.28）
- 「ルータでの未認証マルチキャスト トラフィックの受信のディセーブル化」（P.29）
- 「MLD インターフェイスでの認可ステータスのリセット」（P.31）

IPv6 マルチキャストに対する AAA アクセス コントロールのイネーブル化

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** **例：** `Router(config)# aaa new-model`	AAA アクセス コントロール システムをイネーブルにします。

方式リストの指定およびマルチキャスト アカウンティングのイネーブル化

次の作業では、AAA 認可およびアカウンティングに使用される方式リストを指定する方法、およびインターフェイス上の指定したグループまたはチャネルでマルチキャスト アカウンティングをイネーブルにする方法を示します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa authorization multicast default** [*method1* | *method2*]
4. **aaa accounting multicast default** [**start-stop** | **stop-only**] [**broadcast**] [*method3*] [*method4*] [*method3*] [*method4*]
5. **interface** *type number*
6. **ipv6 multicast aaa account receive** *access-list-name* [**throttle** *throttle-number*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**aaa authorization multicast default** [*method3* | *method4*] **例：** `Router(config)# aaa authorization multicast default`	AAA 認可をイネーブルにし、IPv6 マルチキャスト ネットワークへのユーザ アクセスを制限するパラメータを設定します。
ステップ 4	**aaa accounting multicast default** [**start-stop** | **stop-only**] [**broadcast**] [*method1*] [*method2*] [*method3*] [*method4*] **例：** `Router(config)# aaa accounting multicast default`	課金、または RADIUS を使用する際のセキュリティのために、IPv6 マルチキャスト サービスの AAA アカウンティングをイネーブルにします。
ステップ 5	**interface** *type number* **例：** `Router(config)# interface FastEthernet 1/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 6	**ipv6 multicast aaa account receive** *access-list-name* [**throttle** *throttle-number*] **例：** `Router(config-if)# ipv6 multicast aaa account receive list1`	指定したグループまたはチャネルで AAA アカウンティングをイネーブルにします。

ルータでの未認証マルチキャスト トラフィックの受信のディセーブル化

状況によっては、アクセス コントロール プロファイルに従って加入者の認証とチャネルの認可が行われていないかぎり、マルチキャスト トラフィックの受信を防止することが必要となる場合があります。つまり、アクセス コントロール プロファイルで特に指定がなければ、トラフィックを完全になくす必要があります。

次の作業では、未認証グループまたは未認可チャネルからのマルチキャスト トラフィックをルータで受信しないようにする方法を示します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 multicast group-range** [*access-list-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 multicast group-range** [*access-list-name*] **例：** `Router(config)# ipv6 multicast group-range`	ルータのすべてのインターフェイスで未認可グループまたはチャネルのマルチキャスト プロトコル アクションおよびトラフィック転送をディセーブルにします。

IPv6 での MLD プロキシのイネーブル化

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 mld host-proxy** [*group-acl*]
4. **ipv6 mld host-proxy interface** [*group-acl*]
5. **show ipv6 mld host-proxy** [*interface-type interface-number*] [**group** [*group-address*]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 mld host-proxy** [*group-acl*] **例：** `Router(config)# ipv6 mld host-proxy proxy-group`	MLD プロキシ機能をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**ipv6 mld host-proxy interface** [*group-acl*] **例：** `Router(config)# ipv6 mld host-proxy interface Ethernet 0/0`	RP 上の指定したインターフェイス上で MLD プロキシ機能をイネーブルにします。
ステップ 5	**show ipv6 mld host-proxy** [*interface-type interface-number*] [**group** [*group-address*]] **例：** `Router# show ipv6 mld host-proxy Ethernet0/0`	IPv6 MLD ホスト プロキシ情報を表示します。

MLD インターフェイスでの認可ステータスのリセット

次の作業では、インターフェイスの認可ステータスをリセットする方法を示します。インターフェイスを指定しない場合は、すべての MLD インターフェイスで認可がリセットされます。

手順の概要

1. **enable**
2. **clear ipv6 multicast aaa authorization** [*interface-type interface-number*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**clear ipv6 multicast aaa authorization** [*interface-type interface-number*] **例：** `Router# clear ipv6 multicast aaa authorization FastEthernet 1/0`	IPv6 マルチキャスト ネットワークへのユーザ アクセスを制限するパラメータをクリアします。

MLD トラフィック カウンタのリセット

手順の概要

1. **enable**
2. **clear ipv6 mld traffic**
3. **show ipv6 mld traffic**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**clear ipv6 mld traffic** **例：** `Router# clear ipv6 mld traffic`	すべての MLD トラフィック カウンタをリセットします。
ステップ 3	**show ipv6 mld traffic** **例：** `Router# show ipv6 mld traffic`	MLD トラフィック カウンタを表示します。

MLD インターフェイス カウンタのクリア

手順の概要

1. **enable**
2. **clear ipv6 mld counters** [*interface-type*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**clear ipv6 mld counters** [*interface-type*] **例：** `Router# clear ipv6 mld counters Ethernet1/0`	MLD インターフェイス カウンタをクリアします。

PIM の設定

PIM-SM の設定およびグループ範囲の PIM-SM 情報の表示

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 pim rp-address** *ipv6-address* [*group-access-list*] [**bidir**]
4. **exit**
5. **show ipv6 pim interface** [**state-on**] [**state-off**] [*type number*]
6. **show ipv6 pim group-map** [*group-name* | *group-address*] | [*group-range* | *group-mask*] [**info-source** {**bsr** | **default** | **embedded-rp** | **static**}]
7. **show ipv6 pim neighbor** [**detail**] [*interface-type interface-number* | **count**]
8. **show ipv6 pim range-list** [**config**] [*rp-address* | *rp-name*]
9. **show ipv6 pim tunnel** [*interface-type interface-number*]
10. **debug ipv6 pim** [*group-name* | *group-address* | *interface-type* | **neighbor** | **bsr**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 pim rp-address** *ipv6-address* [*group-access-list*] [**bidir**] **例：** `Router(config)# ipv6 pim rp-address 2001:0DB8::01:800:200E:8C6C acc-grp-1`	特定のグループ範囲の PIM RP のアドレスを設定します。
ステップ 4	**exit** **例：** `Router(config-if)# exit`	グローバル コンフィギュレーション モードを終了し、ルータを特権 EXEC モードに戻します。
ステップ 5	**show ipv6 pim interface** [**state-on**] [**state-off**] [*type number*] **例：** `Router# show ipv6 pim interface`	PIM に対して設定されたインターフェイスに関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 6	**show ipv6 pim group-map** [*group-name* | *group-address*] | [*group-range* | *group-mask*] [**info-source** {**bsr** | **default** | **embedded-rp** | **static**}] **例：** Router# show ipv6 pim group-map	IPv6 マルチキャスト グループ マッピング テーブルを表示します。
ステップ 7	**show ipv6 pim neighbor** [**detail**] [*interface-type interface-number* | **count**] **例：** Router# show ipv6 pim neighbor	Cisco IOS ソフトウェアで検出された PIM ネイバーを表示します。
ステップ 8	**show ipv6 pim range-list** [**config**] [*rp-address* | *rp-name*] **例：** Router# show ipv6 pim range-list	IPv6 マルチキャスト範囲リストに関する情報を表示します。
ステップ 9	**show ipv6 pim tunnel** [*interface-type interface-number*] **例：** Router# show ipv6 pim tunnel	インターフェイス上の PIM レジスタのカプセル化およびカプセル化解除トンネルに関する情報を表示します。
ステップ 10	**debug ipv6 pim** [*group-name* | *group-address* | *interface-type* | **neighbor** | **bsr**] **例：** Router# debug ipv6 pim	PIM プロトコル アクティビティに対するデバッグをイネーブルにします。

PIM オプションの設定

次の作業では、一般的なインターフェイスまたは指定したインターフェイスの両方で PIM-SM および PIM-SSM の設定を細かく調整するために使用できるコマンドを示します。また、PIM の設定と情報を確認するために使用できる各種コマンドについても示します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 pim spt-threshold infinity** [**group-list** *access-list-name*]
4. **ipv6 pim accept-register** {**list** *access-list* | **route-map** *map-name*}
5. **interface** *type number*
6. **ipv6 pim dr-priority** *value*
7. **ipv6 pim hello-interval** *seconds*
8. **ipv6 pim join-prune-interval** *seconds*
9. **exit**
10. **show ipv6 pim join-prune statistic** [*interface-type*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 pim spt-threshold infinity** [**group-list** *access-list-name*] **例：** `Router(config)# ipv6 pim spt-threshold infinity group-list acc-grp-1`	PIM リーフ ルータが指定したグループの SPT に加入するタイミングを設定します。
ステップ 4	**ipv6 pim accept-register** {**list** *access-list* | **route-map** *map-name*} **例：** `Router(config)# ipv6 pim accept-register route-map reg-filter`	RP のレジスタを許可または拒否します。
ステップ 5	**interface** *type number* **例：** `Router(config)# interface FastEthernet 1/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 6	**ipv6 pim dr-priority** *value* **例：** `Router(config-if)# ipv6 pim dr-priority 3`	PIM ルータの DR プライオリティを設定します。
ステップ 7	**ipv6 pim hello-interval** *seconds* **例：** `Router(config-if)# ipv6 pim hello-interval 45`	インターフェイスにおける PIM hello メッセージの頻度を設定します。
ステップ 8	**ipv6 pim join-prune-interval** *seconds* **例：** `Router(config-if)# ipv6 pim join-prune-interval 75`	指定したインターフェイスに対して join および prune の定期的な通知間隔を設定します。
ステップ 9	**exit** **例：** `Router(config-if)# exit`	このコマンドを 2 回入力して、インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 10	**show ipv6 pim join-prune statistic** [*interface-type*] **例：** `Router# show ipv6 pim join-prune statistic`	各インターフェイスの最後の集約パケットに関する平均 join-prune 集約を表示します。

双方向 PIM の設定および双方向 PIM 情報の表示

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 pim rp-address** *ipv6-address* [*group-access-list*] [**bidir**]
4. **exit**
5. **show ipv6 pim df** [*interface-type interface-number*] [*rp-address*]
6. **show ipv6 pim df winner** [*interface-type interface-number*] [*rp-address*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 pim rp-address** *ipv6-address* [*group-access-list*] [**bidir**] **例：** `Router(config)# ipv6 pim rp-address 2001:0DB8::01:800:200E:8C6C bidir`	特定のグループ範囲の PIM RP のアドレスを設定します。**bidir** キーワードを使用すると、そのグループ範囲が双方向共有ツリー転送に使用されるようになります。
ステップ 4	**exit** **例：** `Router(config-if)# exit`	グローバル コンフィギュレーション モードを終了し、ルータを特権 EXEC モードに戻します。
ステップ 5	**show ipv6 pim df** [*interface-type interface-number*] [*rp-address*] **例：** `Router# show ipv6 pim df`	RP の各インターフェイスの Designated Forwarder（DF）選択ステートを表示します。
ステップ 6	**show ipv6 pim df winner** [*interface-type interface-number*] [*rp-address*] **例：** `Router# show ipv6 pim df winner ethernet 1/0 200::1`	各 RP の各インターフェイスの DF 選択ウィナーを表示します。

PIM トラフィック カウンタのリセット

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

この作業では、PIM トラフィック カウンタをリセットし、PIM トラフィック情報を確認する方法を示します。

手順の概要

1. **enable**
2. **clear ipv6 pim counters**
3. **show ipv6 pim traffic**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**clear ipv6 pim counters** **例：** `Router# clear ipv6 pim counters`	PIM トラフィック カウンタをリセットします。
ステップ 3	**show ipv6 pim traffic** **例：** `Router# show ipv6 pim traffic`	PIM トラフィック カウンタを表示します。

PIM トポロジ テーブルをクリアすることによる MRIB 接続のリセット

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

手順の概要

1. **enable**
2. **clear ipv6 pim topology** [*group-name* | *group-address*]
3. **show ipv6 mrib client** [**filter**] [**name** {*client-name* | *client-name*:*client-id*}]
4. **show ipv6 mrib route** [**link-local** | **summary** | *source-address* | *source-name* | *****] [*group-name* | *group-address* [*prefix-length*]]
5. **show ipv6 pim topology** [**link-local** | **route-count** | *group-name* | *group-address*] [*source-address* | *source-name*]
6. **debug ipv6 mrib client**
7. **debug ipv6 mrib io**

8. **debug ipv6 mrib proxy**
9. **debug ipv6 mrib route** [*group-name* | *group-address*]
10. **debug ipv6 mrib table**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**clear ipv6 pim topology** [*group-name* | *group-address*] **例：** `Router# clear ipv6 pim topology FF04::10`	PIM トポロジ テーブルをクリアします。
ステップ 3	**show ipv6 mrib client** [**filter**] [**name** {*client-name* | *client-name*:*client-id*}] **例：** `Router# show ipv6 mrib client`	インターフェイスのマルチキャスト関連情報を表示します。
ステップ 4	**show ipv6 mrib route** [**link-local** | **summary** | *source-address* | *source-name* | *****] [*group-name* | *group-address* [*prefix-length*]] **例：** `Router# show ipv6 mrib route`	MRIB ルート情報を表示します。
ステップ 5	**show ipv6 pim topology** [**link-local** | **route-count** | *group-name* | *group-address*] [*source-address* | *source-name*] **例：** `Router# show ipv6 pim topology`	特定のグループまたはすべてのグループの PIM トポロジ テーブル情報を表示します。
ステップ 6	**debug ipv6 mrib client** **例：** `Router# debug ipv6 mrib client`	MRIB クライアント管理アクティビティに対するデバッグをイネーブルにします。
ステップ 7	**debug ipv6 mrib io** **例：** `Router# debug ipv6 mrib io`	MRIB I/O イベントに対するデバッグをイネーブルにします。
ステップ 8	**debug ipv6 mrib proxy** **例：** `Router# debug ipv6 mrib proxy`	分散型ルータ プラットフォームにおけるルート プロセッサとラインカード間の MRIB プロキシ アクティビティに対するデバッグをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 9	**debug ipv6 mrib route** [*group-name* | *group-address*] **例：** `Router# debug ipv6 mrib route`	MRIB ルーティング エントリ関連のアクティビティに関する情報を表示します。
ステップ 10	**debug ipv6 mrib table** **例：** `Router# debug ipv6 mrib table`	MRIB テーブル管理アクティビティに対するデバッグをイネーブルにします。

BSR の設定

BSR の設定および BSR 情報の確認

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 pim bsr candidate bsr** *ipv6-address* [*hash-mask-length*] [**priority** *priority-value*]
4. **interface** *type number*
5. **ipv6 pim bsr border**
6. **exit**
7. **show ipv6 pim bsr** {**election** | **rp-cache** | **candidate-rp**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 pim bsr candidate bsr** *ipv6-address* [*hash-mask-length*] [**priority** *priority-value*] **例：** `Router(config)# ipv6 pim bsr candidate bsr 2001:0DB8:3000:3000::42 124 priority 10`	候補 BSR になるようにルータを設定します。
ステップ 4	**interface** *type number* **例：** `Router(config)# interface FastEthernet 1/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 5	**ipv6 pim bsr border** **例：** `Router(config-if)# ipv6 pim bsr border`	指定したインターフェイスの任意のスコープの全 BSM に対して境界を設定します。
ステップ 6	**exit** **例：** `Router(config-if)# exit`	このコマンドを 2 回入力して、インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 7	**show ipv6 pim bsr** {**election** | **rp-cache** | **candidate-rp**} **例：** `Router# show ipv6 pim bsr election`	PIM BSR プロトコル処理に関連する情報を表示します。

BSR への PIM RP アドバタイズメントの送信

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 pim bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*] [**scope** *scope-value*] [**bidir**]
4. **interface** *type number*
5. **ipv6 pim bsr border**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 pim bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*] [**scope** *scope-value*] [**bidir**] **例：** `Router(config)# ipv6 pim bsr candidate rp 2001:0DB8:3000:3000::42 priority 0`	BSR に PIM RP アドバタイズメントを送信します。
ステップ 4	**interface** *type number* **例：** `Router(config)# interface FastEthernet 1/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 5	**ipv6 pim bsr border** **例：** `Router(config-if)# ipv6 pim bsr border`	指定したインターフェイスの任意のスコープの全 BSM に対して境界を設定します。

限定スコープ ゾーン内で BSR を使用できるようにするための設定

次の作業では、限定スコープ ゾーン内で BSR を使用できるようにします。ユーザは、ドメイン内の管理用スコープ領域ごとに候補 BSR と一連の候補 RP を設定できます。

候補 RP でスコープが指定されている場合、このルータは指定されたスコープの BSR に自身を C-RP 専用としてアドバタイズします。スコープとともにグループ リストが指定されている場合は、そのグループ リストと同じスコープが指定されたアクセス リスト内のプレフィクスだけがアドバタイズされます。

ブートストラップ ルータでスコープが指定されている場合、その BSR はそのスコープに関連付けられているグループ範囲を含む BSM の起点となり、指定されたスコープに属するグループに対する C-RP 通知を受け入れます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 pim bsr candidate bsr** *ipv6-address* [*hash-mask-length*] [**priority** *priority-value*]
4. **ipv6 pim bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*] [**scope** *scope-value*] [**bidir**]
5. **interface** *type number*
6. **ipv6 multicast boundary scope** *scope-value*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 pim bsr candidate bsr** *ipv6-address* [*hash-mask-length*] [**priority** *priority-value*] **例：** `Router(config)# ipv6 pim bsr candidate bsr 2001:0DB8:1:1:4`	候補 BSR になるようにルータを設定します。
ステップ 4	**ipv6 pim bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*] [**scope** *scope-value*] [**bidir**] **例：** `Router(config)# ipv6 pim bsr candidate rp 2001:0DB8:1:1:1 group-list list scope 6`	BSR に PIM RP アドバタイズメントを送信するように候補 RP を設定します。
ステップ 5	**interface** *type number* **例：** `Router(config)# interface FastEthernet 1/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 6	**ipv6 multicast boundary scope** *scope-value* **例：** `Router(config-if)# ipv6 multicast boundary scope 6`	指定されたスコープのインターフェイスでマルチキャスト境界を設定します。

BSR ルータにスコープと RP のマッピングをアナウンスさせるための設定

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

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 pim bsr announced rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**bidir**] [**scope** *scope-value*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 pim bsr announced rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**bidir**] [**scope** *scope-value*] **例：** `Router(config)# ipv6 pim bsr announced rp 2001:0DB8:3000:3000::42 priority 0`	指定した候補 RP の BSR からスコープと RP のマッピングを直接アナウンスします。

SSM マッピングの設定

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

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

この作業では、SSM マッピングをイネーブルにし、DNS ベースのマッピングをディセーブルにし、スタティック SSM マッピングを設定する方法について説明します。

制約事項

DNS ベースの SSM マッピングを使用するには、ルータは正しく設定されている DNS サーバを少なくとも 1 つ見つける必要があります。ルータは、その DNS サーバに直接接続される可能性があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 mld ssm-map enable**
4. **no ipv6 mld ssm-map query dns**
5. **ipv6 mld ssm-map static** *access-list source-address*
6. **exit**
7. **show ipv6 mld ssm-map** [*source-address*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 mld ssm-map enable** **例：** `Router(config)# ipv6 mld ssm-map enable`	設定済みの SSM 範囲内のグループに対して SSM マッピング機能をイネーブルにします。
ステップ 4	**no ipv6 mld ssm-map query dns** **例：** `Router(config)# no ipv6 mld ssm-map query dns`	DNS ベースの SSM マッピングをディセーブルにします。
ステップ 5	**ipv6 mld ssm-map static** *access-list source-address* **例：** `Router(config)# ipv6 mld ssm-map static SSM_MAP_ACL_2 2001:0DB8:1::1`	スタティック SSM マッピングを設定します。
ステップ 6	**exit** **例：** `Router(config-if)# exit`	グローバル コンフィギュレーション モードを終了し、ルータを特権 EXEC モードに戻します。
ステップ 7	**show ipv6 mld ssm-map** [*source-address*] **例：** `Router# show ipv6 mld ssm-map`	SSM マッピング情報を表示します。

スタティック mroute の設定

この作業では、スタティック マルチキャスト ルートを設定し、スタティック mroute 情報を確認する方法を示します。IPv6 のスタティック マルチキャスト ルート（mroute）は、IPv6 スタティック ルートの拡張として実装できます。ルータを設定する際には、ユニキャスト ルーティング専用としてスタティック ルートを使用するか、マルチキャスト RPF 選択専用としてスタティック マルチキャスト ルートを使用するか、またはユニキャスト ルーティングとマルチキャスト RPF 選択の両方にスタティック ルートを使用するように設定できます。

手順の概要

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

3. **ipv6 route** *ipv6-prefix/prefix-length* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [**tag** *tag*]
4. **exit**
5. **show ipv6 mroute** [**link-local** [*group-name* | *group-address* [*source-address* | *source-name*]] [**summary**] [**count**]
6. **show ipv6 mroute** [**link-local** | *group-name* | *group-address*] **active** [*kbps*]
7. **show ipv6 rpf** *ipv6-prefix*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 route** *ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [**tag** *tag*] **例：** `Router(config)# ipv6 route 2001:0DB8::/64 6::6 100`	スタティック IPv6 ルートを確立します。この例は、ユニキャスト ルーティングとマルチキャスト RPF 選択の両方に使用されるスタティック ルートを示しています。
ステップ 4	**exit** **例：** `Router(config-if)# exit`	グローバル コンフィギュレーション モードを終了し、ルータを特権 EXEC モードに戻します。
ステップ 5	**show ipv6 mroute** [**link-local** [*group-name* | *group-address* [*source-address* | *source-name*]] [**summary**] [**count**] **例：** `Router# show ipv6 mroute ff07::1`	IPv6 マルチキャスト ルーティング テーブルの内容を表示します。
ステップ 6	**show ipv6 mroute** [**link-local** | *group-name* | *group-address*] a**ctive** [*kbps*] **例：** `Router# show ipv6 mroute active`	ルータ上のアクティブなマルチキャスト ストリームを表示します。
ステップ 7	**show ipv6 rpf** *ipv6-prefix* **例：** `Router# show ipv6 rpf 2001:0DB8::1:1:2`	特定のユニキャスト ホスト アドレスおよびプレフィクスの RPF 情報を確認します。

IPv6 マルチプロトコル BGP の設定

次の各作業では、マルチキャスト ルーティングを実行するように IPv6 マルチプロトコル BGP を設定する方法を示します。IPv6 マルチキャストに関連するこれらのマルチキャスト BGP 作業は、IPv6 ユニキャスト用のマルチキャスト BGP 作業と類似していることに注意してください。

IPv6 ピア グループでマルチキャスト BGP ルーティングを実行するための設定

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **neighbor** *peer-group-name* **peer-group**
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number*
6. **address-family ipv6** [**unicast** | **multicast**]
7. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
8. **neighbor** {*ip-address* | *ipv6-address*} **peer-group** *peer-group-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* **例：** `Router(config)# router bgp 65000`	指定した BGP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**neighbor** *peer-group-name* **peer-group** **例：** `Router(config-router)# neighbor group1 peer-group`	マルチキャスト BGP ピア グループを作成します。
ステップ 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number* **例：** `Router(config-router)# neighbor 2001:0DB8:0:CC00::1 remote-as 64600`	指定した自律システムにおけるネイバーの IPv6 アドレスをローカル ルータの IPv6 マルチキャスト BGP ネイバー テーブルに追加します。 • **neighbor remote-as** コマンドの *ipv6-address* 引数は、RFC 2373 に記載された形式にする必要があり、16 ビット値をコロンで区切った 16 進でアドレスを指定します。
ステップ 6	**address-family ipv6** [**unicast** | **multicast**] **例：** `Router(config-router)# address-family ipv6 multicast`	IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードでは、IPv6 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv6** コマンドで **unicast** キーワードが指定されていない場合、ルータは IPv6 ユニキャスト アドレス ファミリのコンフィギュレーション モードになります。 • **multicast** キーワードでは、IPv6 マルチキャスト アドレス プレフィクスを指定します。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** **例：** `Router(config-router-af)# neighbor 2001:0DB8:0:CC00::1 activate`	ネイバーが、指定したファミリ タイプのプレフィクスをネイバーおよびローカル ルータと交換できるようにします。 • 各ネイバーでの追加の設定手順を回避するために、この手順の代替として、*peer-group-name* 引数を指定して **neighbor activate** コマンドを使用します。
ステップ 8	**neighbor** {*ip-address* | *ipv6-address*} **peer-group** *peer-group-name* **例：** `Router(config-router-af)# neighbor 2001:0DB8:0:CC00::1 peer-group group1`	BGP ネイバーの IPv6 アドレスをピア グループに割り当てます。

この次の手順

ピア グループにオプションを割り当てて、BGP またはマルチキャスト BGP ネイバーをピア グループのメンバにする方法の詳細については、「*Implementing Multiprotocol BGP for IPv6*」の「Configuring an IPv6 Multiprotocol BGP Peer Group」および『*Cisco IOS IP Routing Configuration Guide*』の「BGP Features Roadmap」の章を参照してください。

IPv6 マルチプロトコル BGP へのルートのアドバタイズ

この作業では、IPv6 マルチキャスト BGP にプレフィクスをアドバタイズ（挿入）する方法を示します。IPv6 マルチキャストに関連するこの作業および他のマルチキャスト BGP 作業は、IPv6 ユニキャスト用のマルチキャスト BGP 作業と類似していることに注意してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv6** [**unicast** | **multicast**]
5. **network** *ipv6-address*/*prefix-length*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* **例：** `Router(config)# router bgp 65000`	指定した BGP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv6** [**unicast** | **multicast**] **例：** `Router(config-router)# address-family ipv6 multicast`	IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードでは、IPv6 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv6** コマンドで **unicast** キーワードを指定しない場合、ルータは IPv6 ユニキャスト アドレス ファミリのコンフィギュレーション モードになります。 • **multicast** キーワードでは、IPv6 マルチキャスト アドレス プレフィクスを指定します。
ステップ 5	**network** *ipv6-address*/*prefix-length* **例：** `Router(config-router-af)# network 2001:0DB8::/24`	指定したプレフィクスを IPv6 BGP データベースにアドバタイズ（挿入）します（ルートは、まず IPv6 ユニキャスト ルーティング テーブルで検索される必要があります）。 • 具体的には、前の手順で指定したアドレス ファミリのデータベースにプレフィクスが挿入されます。 • ルートには指定したプレフィクスによって「local origin」のタグが付けられます。 • **network** コマンドの *ipv6-prefix* 引数は、RFC 2373 に記載された形式にする必要があり、16 ビット値をコロンで区切った 16 進でアドレスを指定します。 • *prefix-length* 引数は、アドレスのうち連続する上位何ビットがプレフィクス（アドレスのネットワーク部）を構成するかを示す 10 進数値です。10 進数値の前にスラッシュ記号が必要です。

この次の手順

ピア グループにオプションを割り当てて、BGP またはマルチキャスト BGP ネイバーをピア グループのメンバにする方法の詳細については、「*Implementing Multiprotocol BGP for IPv6*」実装ガイドの「Advertising Routes into IPv6 Multiprotocol BGP」の項を参照してください。

IPv6 マルチプロトコル BGP へのプレフィクスの再配布

この作業では、別のルーティング プロトコルからプレフィクスを IPv6 マルチキャスト BGP に再配布（注入）する方法を示します。IPv6 マルチキャストに関連するこの作業および他のマルチキャスト BGP 作業は、IPv6 ユニキャスト用のマルチキャスト BGP 作業と類似していることに注意してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv6** [**unicast** | **multicast**]
5. **redistribute** *protocol* [*process-id*] [**level-1** | **level-1-2** | **level-2**] [**metric** *metric-value*] [**metric-type** {**internal** | **external**}] [**route-map** *map-name*]
6. **exit**
7. **debug bgp ipv6** {**unicast** | **multicast**} **dampening** [**prefix-list** *prefix-list-name*]
8. **debug bgp ipv6** {**unicast** | **multicast**} **updates** [*ipv6-address*] [**prefix-list** *prefix-list-name*] [**in** | **out**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* **例：** `Router(config)# router bgp 65000`	指定した BGP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**address-family ipv6** {**unicast** | **multicast**} **例：** `Router(config-router)# address-family ipv6 multicast`	IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードでは、IPv6 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv6** コマンドで **unicast** キーワードを指定しない場合、ルータは IPv6 ユニキャスト アドレス ファミリのコンフィギュレーション モードになります。 • **multicast** キーワードでは、IPv6 マルチキャスト アドレス プレフィクスを指定します。
ステップ 5	**redistribute** *protocol* [*process-id*] [**level-1** | **level-1-2** | **level-2**] [**metric** *metric-value*] [**metric-type** {**internal** | **external**}] [**route-map** *map-name*] **例：** `Router(config-router-af)# redistribute rip`	どのルーティング プロトコルからプレフィクスを IPv6 マルチキャスト BGP に再配布するかを指定します。 • *protocol* 引数は、**bgp**、**connected**、**isis**、**rip**、または **static** キーワードのいずれかにすることができます。 （注） **connected** キーワードは、インターフェイスでイネーブルになっている IPv6 によって自動的に確立されるルートを示します。
ステップ 6	**exit** **例：** `Router(config-router-af)# exit`	このコマンドを 3 回入力して、アドレス ファミリ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 7	**debug bgp ipv6** {**unicast** | **multicast**} **dampening** [**prefix-list** *prefix-list-name*] **例：** `Router# debug bgp ipv6 multicast`	IPv6 BGP 減衰のデバッグ メッセージを表示します。
ステップ 8	**debug bgp ipv6** {**unicast** | **multicast**} **updates** [*ipv6-address*] [**prefix-list** *prefix-list-name*] [**in** | **out**] **例：** `Router# debug bgp ipv6 multicast updates`	IPv6 BGP アップデート パケットのデバッグ メッセージを表示します。

この次の手順

ピア グループにオプションを割り当てて、BGP またはマルチキャスト BGP ネイバーをピア グループのメンバにする方法の詳細については、「*Implementing Multiprotocol BGP for IPv6*」実装ガイドの「Redistributing Prefixes into IPv6 Multiprotocol BGP」の項を参照してください。

BGP の管理ディスタンスの割り当て

この作業では、RPF ルックアップでユニキャスト ルートとの比較に使用されるマルチキャスト BGP ルートの管理ディスタンスを指定する方法を示します。IPv6 マルチキャストに関連するこの作業および他のマルチキャスト BGP 作業は、IPv6 ユニキャスト用のマルチキャスト BGP 作業と類似していることに注意してください。

注意 BGP 内部ルートの管理ディスタンスを変更することは危険と見なされ、推奨されません。発生する可能性のある 1 つの問題は、ルーティング テーブルの不整合が累積され、それによってルーティングが中断する可能性があることです。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv6** [**unicast** | **multicast**}
5. **distance bgp** *external-distance internal-distance local-distance*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* **例：** `Router(config)# router bgp 100`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv6** [**unicast** | **multicast**} **例：** `Router(config-router)# address-family ipv6 multicast`	標準 IPv6 アドレス プレフィクスを使用する BGP などのルーティング セッションを設定するために、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**distance bgp** *external-distance internal-distance local-distance* **例：** `Router(config-router)# distance bgp 20 20 200`	BGP 管理ディスタンスを割り当てます。

IPv6 マルチキャスト BGP の変換アップデートの生成

ここでは、ピアから受信したユニキャスト IPv6 アップデートに対応する IPv6 マルチキャスト BGP アップデートを生成する方法を示します。

一般的に、マルチキャスト BGP 変換アップデート機能は、BGP 対応ルータだけが存在するカスタマー サイトとピアであるマルチキャスト BGP 対応ルータで使用されます。カスタマー サイトは、ルータをマルチキャスト BGP 対応イメージにアップグレードしません（できません）。カスタマー サイトはマルチキャスト BGP アドバタイズメントの起点となることはできないため、そのピアであるルータが BGP プレフィクスをマルチキャスト BGP プレフィクスに変換します。この変換後のプレフィクスがマルチキャスト送信元の RPF ルックアップで使用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv6** [**unicast** | **multicast**}
5. **neighbor** *ipv6-address* **translate-update ipv6 multicast** [**unicast**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* **例：** `Router(config)# router bgp 100`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv6** [**unicast**	**multicast**} **例：** `Router(config-router)# address-family ipv6 multicast`	標準 IPv6 アドレス プレフィクスを使用する BGP などのルーティング セッションを設定するために、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**neighbor** *ipv6-address* **translate-update ipv6 multicast** [**unicast**] **例：** `Router(config-router)# neighbor 2001:0DB8:7000::2 translate-update ipv6 multicast`	ピアから受信したユニキャスト IPv6 アップデートに対応するマルチプロトコル IPv6 BGP アップデートを生成します。

BGP セッションのリセット

手順の概要

1. **enable**
2. **clear bgp ipv6** {**unicast** | **multicast**} {***** | *autonomous-system-number* | *ip-address* | *ipv6-address* | *peer-group-name*} [**soft**] [**in** | **out**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**clear bgp ipv6** {**unicast** | **multicast**} {***** | *autonomous-system-number* | *ip-address* | *ipv6-address* | *peer-group-name*} [**soft**] [**in** | **out**] **例：** `Router# clear bgp ipv6 unicast peer-group marketing soft out`	IPv6 BGP セッションをリセットします。

外部 BGP ピアのクリア

手順の概要

1. **enable**
2. **clear bgp ipv6** {**unicast** | **multicast**} **external** [**soft**] [**in** | **out**]
3. **clear bgp ipv6** {**unicast** | **multicast**} **peer-group** [*name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**clear bgp ipv6** {**unicast** | **multicast**} **external** [**soft**] [**in** | **out**] **例：** `Router# clear bgp ipv6 unicast external soft in`	外部 IPv6 BGP ピアをクリアします。
ステップ 3	**clear bgp ipv6** {**unicast** | **multicast**} **peer-group** [*name*] **例：** `Router# clear bgp ipv6 unicast peer-group`	IPv6 BGP ピア グループのすべてのメンバをクリアします。

IPv6 BGP ルート減衰情報のクリア

手順の概要

1. **enable**
2. **clear bgp ipv6** {**unicast** | **multicast**} **dampening** [*ipv6-prefix*/*prefix-length*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**clear bgp ipv6** {**unicast** | **multicast**} **dampening** [*ipv6-prefix*/*prefix-length*] **例：** `Router# clear bgp ipv6 unicast dampening 2001:0DB8:7000::/64`	IPv6 BGP ルート減衰情報をクリアし、抑制ルートの抑制を解除します。

IPv6 BGP フラップ統計情報のクリア

手順の概要

1. **enable**
2. **clear bgp ipv6** {**unicast** | **multicast**} **flap-statistics** [*ipv6-prefix*/*prefix-length* | **regexp** *regexp* | **filter-list** *list*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**clear bgp ipv6** {**unicast** | **multicast**} **flap-statistics** [*ipv6-prefix*/*prefix-length* | **regexp** *regexp* | **filter-list** *list*] **例：** `Router# clear bgp ipv6 multicast flap-statistics`	IPv6 BGP フラップ統計情報をクリアします。

IPv6 の帯域幅ベースの CAC の設定

次の各作業では、IPv6 の帯域幅ベースの CAC を設定する方法を示します。

- 「IPv6 の帯域幅ベースの CAC で使用するインターフェイス制限の設定」（P.54）
- 「IPv6 の帯域幅ベースの CAC で使用するアクセス リストの設定」（P.55）
- 「IPv6 の帯域幅ベースの CAC で使用するグローバル制限の設定」（P.56）

IPv6 の帯域幅ベースの CAC で使用するインターフェイス制限の設定

IPv6 の帯域幅ベースの CAC では、コスト乗数を使用してインターフェイス単位の IPv6 mroute ステートをカウントします。この機能を使用すると、ルータ管理者はインターフェイス制限に対してこのようなステートを考慮するときに使用するコスト乗数を指定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*}
5. **ipv6 multicast limit** [**connected** | **rpf** | **out**] *limit-acl max*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface FastEthernet 1/3`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*} **例：** `Router(config-if)# ipv6 address FE80::40:1:3 link-local`	IPv6 の一般的なプレフィクスに基づいて IPv6 アドレスを設定します。
ステップ 5	**ipv6 multicast limit** [**connected** | **rpf** | **out**] *limit-acl max* **例：** `Router (config-if)# ipv6 multicast limit out acl1 10`	IPv6 のインターフェイス単位の mroute ステート リミッタを設定します。

IPv6 の帯域幅ベースの CAC で使用するアクセス リストの設定

IPv6 の帯域幅ベースの CAC では、ルータ管理者はアクセス リストと一致するステートに対してグローバル制限コスト コマンドを設定できます。この作業では、アクセス リストを設定して、そのアクセス リストと一致するステートを設定できるようにする方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *access-list-name*
4. **permit**

または

deny

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 access-list** *access-list-name* **例：** `Router(config)# ipv6 access-list costlist1`	IPv6 アクセス リストを定義し、ルータを IPv6 アクセス リスト コンフィギュレーション モードにします。
ステップ 4	**permit** または **deny** **例：** `Router(config-ipv6-acl)# permit any ff03::1/64`	**permit** または **deny** コマンドを使用して、IPv6 アクセス リストの条件を設定します。

IPv6 の帯域幅ベースの CAC で使用するグローバル制限の設定

ルータ管理者は、アクセス リストと一致するステートに対してグローバル制限コスト コマンドを設定できます。この作業では、IPv6 の帯域幅ベースの CAC で使用するグローバル制限を設定する方法を示します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 multicast limit cost** *access-list cost-multiplier*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 multicast limit cost** *access-list cost-multiplier* **例：** `Router (config)# ipv6 multicast limit cost costlist1 2`	IPv6 のインターフェイス単位の mroute ステート リミッタと一致する mroute にコストを適用します。

IPv6 マルチキャストでの MFIB の使用

IPv6 マルチキャスト ルーティングをイネーブルにすると、マルチキャスト転送が自動的にイネーブルになります。次の各作業では、必要に応じて MFIB の設定と動作を確認するための情報を表示し、MFIB をリセットする方法を示します。

- 「IPv6 マルチキャストでの MFIB の動作の確認」（P.57）
- 「MFIB トラフィック カウンタのリセット」（P.58）
- 「IPv6 マルチキャストのデフォルトの機能のディセーブル化」（P.59）

IPv6 マルチキャストでの MFIB の動作の確認

手順の概要

1. **enable**
2. **show ipv6 mfib** [**link-local** | *ipv6-prefix/prefix-length* | *group-name* | *group-address* [*source-name* | *source-address*]] [**verbose**]
3. **show ipv6 mfib** [**link-local** | *group-name* | *group-address*] **active** [*kbps*]
4. **show ipv6 mfib** [**link-local** | *group-name* | *group-address* [*source-name* | *source-address*]] **count**
5. **show ipv6 mfib interface**
6. **show ipv6 mfib status**
7. **show ipv6 mfib summary**
8. **debug ipv6 mfib** [*group-name* | *group-address*] [**adjacency** | **signal** | **db** | **init** | **mrib** | **pak** | **ps**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**show ipv6 mfib** [**link-local** | *ipv6-prefix*/*prefix-length* | *group-name* | *group-address* [*source-name* | *source-address*]] [**verbose**] **例：** `Router# show ipv6 mfib`	IPv6 MFIB での転送エントリおよびインターフェイスを表示します。
ステップ 3	**show ipv6 mfib** [**link-local** | *group-name* | *group-address*] **active** [*kbps*] **例：** `Router# show ipv6 mfib active`	アクティブな送信元からマルチキャスト グループへの送信レートを表示します。
ステップ 4	**show ipv6 mfib** [**link-local** | *group-name* | *group-address* [*source-name* | *source-address*]] **count** **例：** `Router# show ipv6 mfib count`	MFIB からのグループおよび送信元に関するサマリー トラフィック統計情報を表示します。
ステップ 5	**show ipv6 mfib interface** **例：** `Router# show ipv6 mfib interface`	IPv6 マルチキャスト対応インターフェイスとその転送ステータスに関する情報を表示します。
ステップ 6	**show ipv6 mfib status** **例：** `Router# show ipv6 mfib status`	一般的な MFIB 設定と動作ステータスを表示します。
ステップ 7	**show ipv6 mfib summary** **例：** `Router# show ipv6 mfib summary`	IPv6 MFIB エントリおよびインターフェイスの数に関するサマリー情報を表示します。
ステップ 8	**debug ipv6 mfib** [*group-name* | *group-address*] [**adjacency** | **signal** | **db** | **init** | **mrib** | **pak** | **ps**] **例：** `Router# debug ipv6 mfib FF04::10 pak`	IPv6 MFIB に対するデバッグ出力をイネーブルにします。

MFIB トラフィック カウンタのリセット

手順の概要

1. **enable**
2. **clear ipv6 mfib counters** [*group-name* | *group-address* [*source-address* | *source-name*]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**clear ipv6 mfib counters** [*group-name* | *group-address* [*source-address* | *source-name*]] **例：** `Router# clear ipv6 mfib counters FF04::10`	アクティブなすべての MFIB トラフィック カウンタをリセットします。

IPv6 マルチキャストのデフォルトの機能のディセーブル化

IPv6 マルチキャストを使用すると、いくつかの機能が自動的にイネーブルになります。ただし、状況に合わせて一部の機能をディセーブルにできます。次の各作業では、このような状況と特定の IPv6 マルチキャスト機能をディセーブルにする方法を示します。

- 「IPv6 PIM での組み込み RP サポートのディセーブル化」（P.59）
- 「指定したインターフェイスでの IPv6 PIM のオフ」（P.60）
- 「MLD ルータ側処理のディセーブル化」（P.61）
- 「ルータでの MFIB のディセーブル化」（P.61）
- 「分散型プラットフォームでの MFIB のディセーブル化」（P.62）
- 「MFIB 割り込みレベル IPv6 マルチキャスト転送のディセーブル化」（P.63）

IPv6 PIM での組み込み RP サポートのディセーブル化

ドメイン内のすべてのルータが組み込み RP をサポートしていない場合、必要に応じて、インターフェイスで組み込み RP サポートをディセーブルにできます。この作業では、IPv6 PIM での組み込み RP サポートをディセーブルにする方法を示します。

（注） この作業では、IPv6 PIM での組み込み RP サポートだけでなく、PIM を完全にディセーブルにします。

手順の概要

1. **enable**
2. **configure terminal**
3. **no ipv6 pim rp embedded**
4. **interface** *type number*
5. **no ipv6 pim**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no ipv6 pim rp embedded** **例：** `Router(config)# no ipv6 pim rp embedded`	IPv6 PIM での組み込み RP サポートをディセーブルにします。
ステップ 4	**interface** *type number* **例：** `Router(config)# interface FastEthernet 1/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 5	**no ipv6 pim** **例：** `Router(config-if)# no ipv6 pim`	指定したインターフェイスで IPv6 PIM をオフにします。

指定したインターフェイスでの IPv6 PIM のオフ

特定のインターフェイスだけで IPv6 マルチキャストを実行する必要がある場合、指定したインターフェイスで PIM をオフにすることができます。この作業では、指定したインターフェイスで PIM をオフにする方法を示します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no ipv6 pim**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* **例：** `Router(config)# interface FastEthernet 1/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**no ipv6 pim** **例：** `Router(config-if)# no ipv6 pim`	指定したインターフェイスで IPv6 PIM をオフにします。

MLD ルータ側処理のディセーブル化

特定のインターフェイスだけで IPv6 マルチキャストを実行する必要がある場合、指定したインターフェイスで MLD ルータ側処理をオフにすることができます。指定したインターフェイスで MLD ルータ側処理をディセーブルにするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no ipv6 mld router**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface FastEthernet 1/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**no ipv6 mld router** **例：** `Router(config-if)# no ipv6 mld router`	指定したインターフェイスで MLD ルータ側処理をディセーブルにします。

ルータでの MFIB のディセーブル化

IPv6 マルチキャスト ルーティングをイネーブルにすると、マルチキャスト転送が自動的にイネーブルになります。ただし、必要に応じて、ルータでマルチキャスト転送をディセーブルにできます。次の作業では、ルータでマルチキャスト転送をディセーブルにする方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no ipv6 mfib**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no ipv6 mfib** **例：** `Router(config)# no ipv6 mfib`	ルータで IPv6 マルチキャスト転送をディセーブルにします。

分散型プラットフォームでの MFIB のディセーブル化

IPv6 マルチキャスト ルーティングをイネーブルにすると、マルチキャスト転送が自動的にイネーブルになります。ただし、必要に応じて、分散型プラットフォームでマルチキャスト転送をディセーブルにできます。次の作業では、分散型プラットフォームでマルチキャスト転送をディセーブルにする方法を示します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 mfib-mode centralized-only**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 mfib-mode centralized-only** **例：** `Router(config)# ipv6 mfib-mode centralized-only`	分散型プラットフォームで分散転送をディセーブルにします。

MFIB 割り込みレベル IPv6 マルチキャスト転送のディセーブル化

特定のインターフェイスでの発信パケットの MFIB 割り込みレベル IPv6 マルチキャスト転送は、シスコ エクスプレス フォワーディングをサポートするインターフェイスでイネーブルになります。ただし、必要に応じて、指定したインターフェイスで MFIB 割り込みレベル転送をディセーブルにできます。次の作業では、この機能をディセーブルにする方法を示します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no ipv6 mfib cef output**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* **例：** `Router(config)# interface FastEthernet 1/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**no ipv6 mfib cef output** **例：** `Router(config-if)# no ipv6 mfib cef output`	特定のインターフェイスで発信パケットの MFIB 割り込みレベル IPv6 マルチキャスト転送をディセーブルにします。

例

ここでは、次の出力例について説明します。

show ipv6 mfib コマンドの出力例

次に、MFIB での転送エントリおよびインターフェイスを表示する例を示します。ルータはファストスイッチング用に設定されており、受信側はイーサネット 1/1 の FF05::1 に加入し、送信元（2001:0DB8:1:1:20）はイーサネット 1/2 で送信しています。

```
Router# show ipv6 mfib

IP Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,FF00::/8) Flags: C
   Forwarding: 0/0/0/0, Other: 0/0/0
   Tunnel0 Flags: NS
(*,FF00::/15) Flags: D
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,FF05::1) Flags: C
   Forwarding: 2/0/100/0, Other: 0/0/0
   Tunnel0 Flags: A NS
   Ethernet1/1 Flags: F NS
     Pkts: 0/2
(2001:0DB8:1:1:200,FF05::1) Flags:
   Forwarding: 5/0/100/0, Other: 0/0/0
   Ethernet1/2 Flags: A
   Ethernet1/1 Flags: F NS
     Pkts: 3/2
(*,FF10::/15) Flags: D
   Forwarding: 0/0/0/0, Other: 0/0/0
```

show ipv6 mfib active コマンドの出力例

次に、アクティブな IP マルチキャスト送信元による情報の送信レートに関する統計情報を表示する例を示します。ルータは、トラフィックを 2001:0DB8:1:1:200 から FF05::1 にスイッチングしています。

```
Router# show ipv6 mfib active

Active IPv6 Multicast Sources - sending >= 4 kbps
Group: FF05::1
  Source: 2001:0DB8:1:1:200
    Rate: 20 pps/16 kbps(1sec), 0 kbps(last 128 sec)
```

show ipv6 mfib count コマンドの出力例

次に、MFIB からのグループおよび送信元に関する統計情報を表示する例を示します。ルータは、トラフィックを 2001:0DB8:1:1:200 から FF05::1 にスイッチングしています。

```
Router# show ipv6 mfib count

IP Multicast Statistics
54 routes, 7 groups, 0.14 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Group: FF00::/8
  RP-tree:    Forwarding: 0/0/0/0, Other: 0/0/0
Group: FF00::/15
  RP-tree:    Forwarding: 0/0/0/0, Other: 0/0/0
Group: FF05::1
  RP-tree:    Forwarding: 2/0/100/0, Other: 0/0/0
  Source: 10::1:1:200,   Forwarding: 367/10/100/7, Other: 0/0/0
```

```
  Tot. shown: Source count: 1, pkt count: 369
Group: FF10::/15
  RP-tree:    Forwarding: 0/0/0/0, Other: 0/0/0
Group: FF20::/15
  RP-tree:    Forwarding: 0/0/0/0, Other: 0/0/0
```

show ipv6 mfib interface コマンドの出力例

次に、IPv6 マルチキャスト対応インターフェイスとその転送ステータスに関する情報を表示する例を示します。ルータはファスト スイッチング用に設定されています。

```
Router# show ipv6 mfib interface

IPv6 Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running

MFIB interface       status    CEF-based output
                               [configured,available]
Ethernet1/1          up      [yes       ,yes      ]
Ethernet1/2          up      [yes       ,?        ]
Tunnel0              up      [yes       ,?        ]
Tunnel1              up      [yes       ,?        ]
```

show ipv6 mfib summary コマンドの出力例

次に、IPv6 MFIB エントリおよびインターフェイスの数に関するサマリー情報を表示する例を示します。

```
Router# show ipv6 mfib summary

IPv6 MFIB summary:
  54     total entries [1 (S,G), 7 (*,G), 46 (*,G/m)]
  17     total MFIB interfaces
```

show ipv6 mld groups コマンドの出力例

次に、**show ipv6 mld groups** コマンドの出力例を示します。この例では、ネットワーク プロトコルで使用されているリンクローカル グループを含め、ファスト イーサネット インターフェイス 2/1 が加入しているすべてのグループが示されています。

```
Router# show ipv6 mld groups FastEthernet 2/1

MLD Connected Group Membership
Group Address           Interface           Uptime        Expires
FF02::2                 FastEthernet2/1     3d18h         never
FF02::D                 FastEthernet2/1     3d18h         never
FF02::16                FastEthernet2/1     3d18h         never
FF02::1:FF00:1          FastEthernet2/1     3d18h         00:00:27
FF02::1:FF00:79         FastEthernet2/1     3d18h         never
FF02::1:FF23:83C2       FastEthernet2/1     3d18h         00:00:22
FF02::1:FFAF:2C39       FastEthernet2/1     3d18h         never
FF06:7777::1            FastEthernet2/1     3d18h         00:00:26
```

show ipv6 mld groups summary コマンドの出力例

次に、**show ipv6 mld groups summary** コマンドの出力例を示します。

```
Router# show ipv6 mld groups summary

MLD Route Summary
  No. of (*,G) routes = 5
  No. of (S,G) routes = 0
```

show ipv6 mld interface コマンドの出力例

次に、ファスト イーサネット インターフェイス 2/1 に対する **show ipv6 mld interface** コマンドの出力例を示します。

```
Router# show ipv6 mld interface FastEthernet 2/1

FastEthernet2/1 is up, line protocol is up
Internet address is FE80::205:5FFF:FEAF:2C39/10
MLD is enabled in interface
Current MLD version is 2
MLD query interval is 125 seconds
MLD querier timeout is 255 seconds
MLD max query response time is 10 seconds
Last member query response interval is 1 seconds
MLD activity: 25 joins, 17 leaves
MLD querying router is FE80::205:5FFF:FEAF:2C39 (this system)
```

show ipv6 mld ssm-map コマンドの出力例

次に、送信元アドレス 2001:0DB8::1 に対する SSM マッピングの例を示します。

```
Router# show ipv6 mld ssm-map 2001:0DB8::1

 Group address  : 2001:0DB8::1
 Group mode ssm : TRUE
 Database       : STATIC
 Source list    : 2001:0DB8::2
                  2001:0DB8::3

Router# show ipv6 mld ssm-map 2001:0DB8::2

 Group address  : 2001:0DB8::2
 Group mode ssm : TRUE
 Database       : DNS
 Source list    : 2001:0DB8::3
                  2001:0DB8::1
```

show ipv6 mld traffic コマンドの出力例

次に、送受信された MLD プロトコル メッセージを表示する例を示します。

```
Router# show ipv6 mld traffic

MLD Traffic Counters
Elapsed time since counters cleared:00:00:21

                                Received     Sent
Valid MLD Packets                 3           1
Queries                           1           0
Reports                           2           1
Leaves                            0           0
Mtrace packets                    0           0

Errors:
Malformed Packets                             0
Bad Checksums                                 0
Martian source                                0
Packets Received on MLD-disabled Interface    0
```

show ipv6 mrib client コマンドの出力例

次に、**show ipv6 mrib client** コマンドの出力例を示します。

```
Router# show ipv6 mrib client
```

```
IP MRIB client-connections
igmp:145        (connection id 0)
pim:146 (connection id 1)
mfib ipv6:3     (connection id 2)
slot 3  mfib ipv6 rp agent:16   (connection id 3)
slot 1  mfib ipv6 rp agent:16   (connection id 4)
slot 0  mfib ipv6 rp agent:16   (connection id 5)
slot 4  mfib ipv6 rp agent:16   (connection id 6)
slot 2  mfib ipv6 rp agent:16   (connection id 7)
```

show ipv6 mrib route コマンドの出力例

次に、**show ipv6 mrib route** コマンドで **summary** キーワードを指定した場合の出力例を示します。

```
Router# show ipv6 mrib route summary

MRIB Route-DB Summary
  No. of (*,G) routes = 52
  No. of (S,G) routes = 0
  No. of Route x Interfaces (RxI) = 10
```

show ipv6 mroute コマンドの出力例

show ipv6 mroute コマンドの使用は、マルチキャスト IPv6 データが流れていることをダイナミックに確認するのに適しています。次に、**show ipv6 mroute** コマンドの出力例を示します。

```
Router# show ipv6 mroute ff07::1

Multicast Routing Table
Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers:Uptime/Expires
Interface state:Interface, State

(*, FF07::1), 00:04:45/00:02:47, RP 2001:0DB8:6::6, flags:S
  Incoming interface:Tunnel5
  RPF nbr:6:6:6::6
  Outgoing interface list:
    POS4/0, Forward, 00:04:45/00:02:47

(2001:0DB8:999::99, FF07::1), 00:02:06/00:01:23, flags:SFT
  Incoming interface:POS1/0
  RPF nbr:2001:0DB8:999::99
  Outgoing interface list:
    POS4/0, Forward, 00:02:06/00:03:27
```

show ipv6 mroute active コマンドの出力例

次に、**show ipv6 mroute active** コマンドの出力例を示します。

```
Router# show ipv6 mroute active

Active IPv6 Multicast Sources - sending >= 4 kbps
Group:FF05::1
 Source:2001:0DB8:1:1:1
   Rate:11 pps/8 kbps(1sec), 8 kbps(last 8 sec)
```

show ipv6 pim bsr コマンドの出力例

次に、BSR 選択情報を表示する例を示します。

```
Router# show ipv6 pim bsr election

PIMv2 BSR information
```

```
BSR Election Information
Scope Range List: ff00::/8
This system is the Bootstrap Router (BSR)
BSR Address: 2001:0DB8:1:1:4
Uptime: 00:11:55, BSR Priority: 0, Hash mask length: 126
RPF: FE80::A8BB:CCFF:FE03:C400,Ethernet0/0
BS Timer: 00:00:07
This system is candidate BSR
Candidate BSR address: 2001:0DB8:1:1:4, priority: 0, hash mask length: 126
```

show ipv6 pim group-map コマンドの出力例

次に、**show ipv6 pim group-map** コマンドの出力例を示します。

```
Router# show ipv6 pim group-map

FF33::/32*
      SSM
      Info source:Static
      Uptime:00:08:32, Groups:0
  FF34::/32*
      SSM
      Info source:Static
      Uptime:00:09:42, Groups:0
```

show ipv6 pim interface コマンドの出力例

次に、**show ipv6 pim interface** コマンドで **state-on** キーワードを指定した場合の出力例を示します。

```
Router# show ipv6 pim interface state-on

Interface          PIM  Nbr   Hello  DR
                        Count Intvl  Prior

Ethernet0          on   0     30     1
    Address:FE80::208:20FF:FE08:D7FF
    DR     :this system
POS1/0             on   0     30     1
    Address:FE80::208:20FF:FE08:D554
    DR     :this system
POS4/0             on   1     30   1
    Address:FE80::208:20FF:FE08:D554
    DR     :FE80::250:E2FF:FE8B:4C80
POS4/1             on   0     30   1
    Address:FE80::208:20FF:FE08:D554
    DR     :this system
Loopback0          on   0     30     1
    Address:FE80::208:20FF:FE08:D554
    DR     :this system
```

show ipv6 pim join-prune statistic コマンドの出力例

次に、イーサネット インターフェイス 0/0/0 での join/prune 集約の例を示します。

```
Router# show ipv6 pim join-prune statistic Ethernet0/0/0

PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface             Transmitted             Received

Ethernet0/0/0      0    / 0    / 0         1    / 0    / 0
```

show ipv6 pim neighbor コマンドの出力例

次に、**show ipv6 pim neighbor** コマンドで **detail** キーワードを指定して、ルーティング可能アドレスの hello オプションを通して学習されたネイバーの追加アドレスを識別する場合の出力例を示します。

```
Router# show ipv6 pim neighbor detail

Neighbor Address(es)       Interface          Uptime    Expires DR pri Bidir

FE80::A8BB:CCFF:FE00:401   Ethernet0/0        01:34:16  00:01:16 1      B
60::1:1:3

FE80::A8BB:CCFF:FE00:501   Ethernet0/0        01:34:15  00:01:18 1      B
60::1:1:4
```

show ipv6 pim range-list コマンドの出力例

次に、**show ipv6 pim range-list** コマンドの出力例を示します。

```
Router# show ipv6 pim range-list

config SSM Exp:never Learnt from :::
 FF33::/32 Up:00:26:33
 FF34::/32 Up:00:26:33
 FF35::/32 Up:00:26:33
 FF36::/32 Up:00:26:33
 FF37::/32 Up:00:26:33
 FF38::/32 Up:00:26:33
 FF39::/32 Up:00:26:33
 FF3A::/32 Up:00:26:33
 FF3B::/32 Up:00:26:33
 FF3C::/32 Up:00:26:33
 FF3D::/32 Up:00:26:33
 FF3E::/32 Up:00:26:33
 FF3F::/32 Up:00:26:33
config SM RP:40::1:1:1 Exp:never Learnt from :::
 FF13::/64 Up:00:03:50
config SM RP:40::1:1:3 Exp:never Learnt from :::
 FF09::/64 Up:00:03:50
```

show ipv6 pim topology コマンドの出力例

次に、**show ipv6 pim topology** コマンドの出力例を示します。

```
Router# show ipv6 pim topology

IP PIM Multicast Topology Table
Entry state:(*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags:KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR - Sending Registers, E - MSDP External,
    DCC - Don't Check Connected
Interface state:Name, Uptime, Fwd, Info
Interface flags:LI - Local Interest, LD - Local Dissinterest,
II - Internal Interest, ID - Internal Dissinterest,
LH - Last Hop, AS - Assert, AB - Admin Boundary

(*,FF05::1)
SM UP:02:26:56 JP:Join(now) Flags:LH
RP:2001:0DB8:1:1:2
RPF:Ethernet1/1,FE81::1
  Ethernet0/1          02:26:56  fwd LI LH

(2001:0DB8:1:1:200,FF05::1)
SM UP:00:00:07 JP:Null(never) Flags:
RPF:Ethernet1/1,FE80::30:1:4
  Ethernet1/1          00:00:07  off LI
```

show ipv6 pim traffic コマンドの出力例

次に、送受信された PIM プロトコル メッセージの数を表示する例を示します。

```
Router# show ipv6 pim traffic

PIM Traffic Counters
Elapsed time since counters cleared:00:05:29

                              Received     Sent
Valid PIM Packets               22          22
Hello                           22          22
Join-Prune                      0           0
Register                        0           0
Register Stop                   0           0
Assert                          0           0
Bidir DF Election               0           0

Errors:
Malformed Packets                           0
Bad Checksums                               0
Send Errors                                 0
Packet Sent on Loopback Errors              0
Packets Received on PIM-disabled Interface  0
Packets Received with Unknown PIM Version   0
```

show ipv6 pim tunnel コマンドの出力例

次に、RP での **show ipv6 pim tunnel** コマンドの出力例を示します。

```
Router# show ipv6 pim tunnel

Tunnel0*
 Type  :PIM Encap
 RP    :100::1
 Source:100::1
Tunnel0*
 Type  :PIM Decap
 RP    :100::1
 Source: -
```

次に、非 RP での **show ipv6 pim tunnel** コマンドの出力例を示します。

```
Router# show ipv6 pim tunnel

Tunnel0*
 Type  :PIM Encap
 RP    :100::1
 Source:2001::1:1:1
```

show ipv6 rpf コマンドの出力例

次に、IPv6 アドレスが 2001:0DB8:1:1:2 のユニキャスト ホストの RPF 情報を表示する例を示します。

```
Router# show ipv6 rpf 2001:0DB8:1:1:2

RPF information for 2001:0DB8:1:1:2
  RPF interface:Ethernet3/2
  RPF neighbor:FE80::40:1:3
  RPF route/mask:20::/64
  RPF type:Unicast
  RPF recursion count:0
  Metric preference:110
  Metric:30
```

IPv6 マルチキャストの実装の設定例

ここでは、次の設定例について説明します。

例：IPv6 マルチキャスト ルーティングのイネーブル化

次に、すべてのインターフェイスでマルチキャスト ルーティングをイネーブルにする例を示します。また、このコマンドを入力すると、イネーブルになっているすべてのルータ インターフェイスで PIM および MLD に対してマルチキャスト転送がイネーブルになります。

```
Router> enable
Router# configure terminal
Router(config)# ipv6 multicast-routing
```

例：MLD プロトコルの設定

次に、ファスト イーサネット インターフェイス 1/0 でクエリー最大応答時間、クエリー タイムアウト、およびクエリー間隔を設定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface FastEthernet 1/0
Router(config-if)# ipv6 mld query-max-response-time 20
Router(config-if)# ipv6 mld query-timeout 130
Router(config-if)# ipv6 mld query-interval 60
```

次に、ファスト イーサネット インターフェイス 1/0 で、指定したグループおよび送信元に対して MLD レポートを設定し、ユーザに IPv6 マルチキャストの受信側アクセス コントロールの実行を許可し、マルチキャスト グループのトラフィックをスタティックに転送する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface FastEthernet 1/0
```

```
Router(config)# ipv6 mld join-group FF04::10
Router(config)# ipv6 mld static-group FF04::10 100::1
Router(config)# ipv6 mld access-group acc-grp-1
```

例：受信側の明示的トラッキングの設定

次に、受信側の明示的トラッキングを設定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface FastEthernet 1/0
Router(config-if)# ipv6 mld explicit-tracking list1
```

例：MLD プロキシの設定

次に、イーサネット 0/0 インターフェイスの IPv6 MLD プロキシ情報を設定し、設定したインターフェイスに関する情報を表示する例を示します。

```
Router(config)# ipv6 mld host-proxy Ethernet0/0
Router(config)# exit
Router# show ipv6 mld host-proxy Ethernet0/0

Ethernet0/0 is up, line protocol is up
  Internet address is FE80::34/64
MLD is enabled on interface
  MLD querying router is FE80::12, Version: MLDv2
  Current MLD host version is 2
  MLD max query response time is 10 seconds
Number of MLD Query sent on interface : 10
Number of MLD Query received on interface : 20
Number of MLDv1 report sent : 5
Number of MLDv2 report sent : 10
Number of MLDv1 leave sent : 0
Number of MLDv2 leave sent : 1
```

次に、イーサネット 0/0 プロキシ インターフェイスのグループ エントリを設定し、それらのグループ エントリに関する情報を表示する例を示します。

```
Router# show ipv6 mld host-proxy Ethernet0/0 group

Group:               FF5E::12
Uptime:             00:00:07
Group mode:     INCLUDE
Version             MLDv2
Group source list:
  Source Address        Uptime
            5000::2                     00:00:07
            2000::2                     00:01:15

Group:               FF7E::21
Uptime:             00:02:07
Group mode:     EXCLUDE
Version             MLDv2
Group source list: Empty
```

例：PIM の設定

次に、20010DB8::1 を RP として使用して、PIM-SM を使用するようにルータを設定する例を示します。次の例では、SPT しきい値を infinity（無制限）に設定して、送信元がトラフィックの送信を開始したときに送信元ツリーへの切り替えが起こらないようにしています。また、ローカル マルチキャスト BGP プレフィクスを持たないすべての送信元でフィルタを設定しています。

```
Router(config)# ipv6 multicast-routing
Router(config)# ipv6 pim rp-address 2001:0DB8::1
Router(config)# ipv6 pim spt-threshold infinity
Router(config)# ipv6 pim accept-register route-map reg-filter
```

例：PIM オプションの設定

次に、イーサネット インターフェイス 0/0 で DR プライオリティ、PIM hello 間隔、および join/prune の定期的な通知間隔を設定する例を示します。

```
Router(config)# interface Ethernet0/0
Router(config)# ipv6 pim hello-interval 60
Router(config)# ipv6 pim dr-priority 3
Router(config)# ipv6 pim join-prune-interval 75
```

例：mroute の設定

次に、スタティック マルチキャスト ルートをマルチキャスト RPF 選択専用として使用するように設定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# ipv6 route 2001:0DB8::/64 7::7 100 multicast
```

例：IPv6 マルチプロトコル BGP ピア グループの設定

次に、group1 という名前の IPv6 マルチプロトコル BGP ピア グループを設定する例を示します。

```
router bgp 65000
no bgp default ipv4-unicast
neighbor group1 peer-group
neighbor 2001:0DB8:0:CC00::1 remote-as 64600

address-family ipv6 multicast
 neighbor 3FFE:C00:0:1:A8BB:CCFF:FE00:8200 activate
 no auto-summary
 no synchronization
 exit-address-family
```

例：IPv6 マルチプロトコル BGP へのルートのアドバタイズ

次に、ローカル ルータの IPv6 マルチキャスト データベースに IPv6 ネットワーク 2001:0DB8::/24 を注入する例を示します（BGP は、ネットワークをアドバタイズする前に、そのネットワークのルートがローカル ルータの IPv6 マルチキャスト データベースに存在することを確認します）。

```
router bgp 65000
 no bgp default ipv4-unicast
```

```
address-family ipv6 multicast
  network 2001:0DB8::/24
```

例：IPv6 マルチプロトコル BGP へのプレフィクスの再配布

次に、ローカル ルータの IPv6 マルチキャスト データベースに BGP ルートを再配布する例を示します。

```
router bgp 64900
 no bgp default ipv4-unicast
address-family ipv6 multicast
 redistribute BGP
```

例：IPv6 マルチキャスト BGP の変換アップデートの生成

次に、ユニキャスト IPv6 アップデートに対応する IPv6 マルチキャスト BGP アップデートを生成する例を示します。

```
router bgp 64900
 no bgp default ipv4-unicast
address-family ipv6 multicast
 neighbor 2001:0DB8:7000::2 translate-update ipv6 multicast
```

例：IPv6 の帯域幅ベースの CAC の設定

次の各例では、IPv6 の帯域幅ベースの CAC を設定する方法を示します。

- 「例：IPv6 の帯域幅ベースの CAC で使用するインターフェイス制限の設定」（P.75）
- 「例：IPv6 の帯域幅ベースの CAC で使用するアクセス リストの設定」（P.75）
- 「例：帯域幅ベースの CAC で使用するグローバル制限の設定」（P.75）

例：IPv6 の帯域幅ベースの CAC で使用するインターフェイス制限の設定

次に、送信元ルータの発信インターフェイス イーサネット 1/3 でインターフェイス制限を設定する例を示します。

```
interface Ethernet1/3
ipv6 address FE80::40:1:3 link-local
 ipv6 address 2001:0DB8:1:1:3/64
 ipv6 multicast limit out acl1 10
```

例：IPv6 の帯域幅ベースの CAC で使用するアクセス リストの設定

次に、帯域幅ベースの CAC で使用するアクセス リストを設定する例を示します。

```
ipv6 access-list cost-list
   permit any ff03::1/64
```

例：帯域幅ベースの CAC で使用するグローバル制限の設定

次に、送信元ルータでグローバル制限を設定する例を示します。

```
ipv6 multicast limit cost cost-list 2
```

例：IPv6 PIM での組み込み RP サポートのディセーブル化

次に、IPv6 PIM での組み込み RP サポートをディセーブルにする例を示します。

```
Router(config)# ipv6 multicast-routing
Router(config)# no ipv6 pim rp embedded
```

例：指定したインターフェイスでの IPv6 PIM のオフ

次に、ファスト イーサネット インターフェイス 1/0 で IPv6 PIM をオフにする例を示します。

```
Router(config)# ipv6 multicast-routing
Router(config)# interface FastEthernet 1/0
Router(config)# no ipv6 pim
```

例：MLD ルータ側処理のディセーブル化

次に、ファスト イーサネット インターフェイス 1/0 で MLD ルータ側処理をオフにする例を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface FastEthernet 1/0
Router(config-if)# no ipv6 mld router
```

例：MFIB のディセーブル化と再イネーブル化

IPv6 マルチキャスト ルーティングをイネーブルにすると、マルチキャスト転送が自動的にイネーブルになります。ただし、必要に応じて、ルータでマルチキャスト転送をディセーブルにできます。次に、ルータでマルチキャスト転送をディセーブルにし、必要に応じて再度イネーブルにする例を示します。この例では、ファスト イーサネット インターフェイス 1/0 で発信パケットの MFIB 割り込みレベル IPv6 マルチキャスト転送をディセーブルにする方法についても示しています。

```
Router> enable
Router# configure terminal
Router(config) no ipv6 mfib
Router(config) ipv6 mfib-mode centralized-only
Router(config) interface FastEthernet 1/0
Router(config-if) no ipv6 mfib cef output
```

その他の関連資料

関連資料

関連項目	参照先
IPv6 マルチキャスト アドレス	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing IPv6 Addressing and Basic Connectivity」
IPv6 のサポート機能リスト	『*Cisco IOS IPv6 Configuration Guide*』の「Start Here: Cisco IOS Software Release Specifics for IPv6 Features」

関連項目	参照先
IPv6 対応マルチキャスト BGP	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing Multiprotocol BGP for IPv6」
IPv6 スタティック ルート	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing Static Routes for IPv6」
IPv6 トンネル	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing Tunneling for IPv6」
IPv6 コマンド：コマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS IPv6 Command Reference*』
MFIB：IPv4 SSO/ISSU	『*Monitoring and Maintaining Multicast HA Operations (NSF/SSO and ISSU)*』
IPv4 設定情報	『*Cisco IOS IP Multicast Configuration Guide*』の「IP Multicast Features Roadmap」
IPv4 コマンド リファレンス	『*Cisco IOS IP Multicast Command Reference*』
すべてのリリースの IPv6 および IPv4 コマンド	『*Cisco IOS Master Command List*』

規格

規格	タイトル
draft-ietf-pim-sm-v2-new	『*Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)*』（2003 年 3 月 6 日）
draft-savola-mboned-mcast-rpaddr	『*Embedding the Address of RP in IPv6 Multicast Address*』(2003 年 5 月 23 日)
draft-suz-pim-upstream-detection	『*PIM Upstream Detection Among Multiple Addresses*』（2003 年 2 月）
draft-ietf-pim-bidir-05	『*Bi-directional Protocol Independent Multicast (BIDIR-PIM)*』（2003 年 6 月 20 日）
draft-ietf-pim-sm-bsr-03.txt	『*Bootstrap Router (BSR) Mechanism for PIM Sparse Mode*』（2003 年 2 月 25 日）

MIB

MIB	MIB リンク
•	選択したプラットフォーム、Cisco ソフトウェア リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2373	『*IP Version 6 Addressing Architecture*』
RFC 2460	『*Internet Protocol, Version 6 (IPv6) Specification*』

RFC	タイトル
RFC 2461	『*Neighbor Discovery for IP version 6 (IPv6)*』
RFC 2462	『*IPv6 Stateless Address Autoconfiguration*』
RFC 3576	『*Change of Authorization*』
RFC 3590	『*Source Address Selection for the Multicast Listener Discovery (MLD) Protocol*』
RFC 3810	『*Multicast Listener Discovery Version 2 (MLDv2) for IPv6*』
RFC 4007	『*IPv6 Scoped Address Architecture*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

IPv6 マルチキャストの実装の機能情報

表 1 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どのソフトウェア イメージが特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1　IPv6 マルチキャストの実装の機能情報

機能名	リリース	機能情報
IPv6 マルチキャスト	12.0(26)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(18)SXE 12.3(2)T 12.4 12.4(2)T	IPv6 マルチキャストを使用すると、ホストがすべてのホストのサブセットに同時に単一のデータ ストリームを送信できるようになります。 このマニュアルでは、この機能について説明しています。
IPv6 マルチキャスト：Multicast Listener Discovery（MLD; マルチキャスト リスナー ディスカバリ）プロトコル（バージョン 1 および 2）	12.0(26)S 12.2(18)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA1 2.3(2)T 12.4 12.4(2)T 15.0(1)S	MLD は、直接接続されているリンク上のマルチキャスト リスナー（特定のマルチキャスト アドレスを宛先としたマルチキャスト パケットを受信するために使用するノード）を検出するために IPv6 ルータで使用されます。MLD には 2 つのバージョンがあります。MLD バージョン 1 はバージョン 2 の IGMP for IPv4 をベースとしています。MLD バージョン 2 はバージョン 3 の IGMP for IPv4 をベースとしています。Cisco IOS ソフトウェアの IPv6 マルチキャストでは、MLD バージョン 2 と MLD バージョン 1 の両方が使用されます。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 マルチキャストの実装の制約事項」（P.2）

表 1　IPv6 マルチキャストの実装の機能情報 （続き）

機能名	リリース	機能情報
		• 「IPv6 マルチキャストの概要」（P.4） • 「IPv6 マルチキャスト ルーティングの実装」（P.7） • 「マルチキャスト リスナー ディスカバリ プロトコル for IPv6」（P.8） • 「プロトコル独立マルチキャスト」（P.10） • 「MRIB」（P.18） • 「IPv6 マルチキャスト ルーティングのイネーブル化」（P.21） • 「MLD プロトコルのカスタマイズおよび確認」（P.22） • 「SSM マッピングの設定」（P.43） • 「MLD ルータ側処理のディセーブル化」（P.61）
IPv6 マルチキャスト：PIM Sparse Mode（PIM-SM; PIM 希薄モード）	12.0(26)S 12.2(18)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.3(2)T 12.4 12.4(2)T 15.0(1)S	PIM-SM は、ユニキャスト ルーティングを使用して、マルチキャスト ツリー構築用のリバースパス情報を提供します。PIM-SM は、トラフィックに対して明示的な要求がある場合を除いて、各マルチキャストに関与しているルータの数が比較的少なく、これらのルータがグループのマルチキャスト パケットを転送しないときに、マルチキャスト ネットワークで使用されます。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 マルチキャストの実装の制約事項」（P.2） • 「IPv6 マルチキャスト ルーティングの実装」（P.7） • 「プロトコル独立マルチキャスト」（P.10） • 「IPv6 マルチキャストのプロセス スイッチングおよびファスト スイッチング」（P.19） • 「IPv6 マルチキャスト アドレス ファミリのマルチプロトコル BGP」（P.20） • 「IPv6 マルチキャスト ルーティングのイネーブル化」（P.21） • 「PIM の設定」（P.32） • 「BSR の設定および BSR 情報の確認」（P.39） • 「IPv6 PIM での組み込み RP サポートのディセーブル化」（P.59） • 「指定したインターフェイスでの IPv6 PIM のオフ」（P.60）

表 1　IPv6 マルチキャストの実装の機能情報 （続き）

機能名	リリース	機能情報
IPv6 マルチキャスト：PIM Source Specific Multicast（PIM-SSM; PIM 送信元固有マルチキャスト）	12.0(26)S 12.2(18)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.3(2)T 12.4 12.4(2)T 15.0(1)S	PIM-SSM は、PIM-SM から派生したものであり、SSM の実装をサポートしています。SSM 機能では、受信側が明示的に加入しているマルチキャスト送信元だけからその受信側にデータグラム トラフィックが転送されます。これにより、帯域利用率が最適化され、不要なインターネット ブロードキャスト トラフィックが拒否されます。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 マルチキャスト ルーティングの実装」（P.7） • 「プロトコル独立マルチキャスト」（P.10） • 「PIM 送信元固有マルチキャスト」（P.14） • 「IPv6 マルチキャストのプロセス スイッチングおよびファスト スイッチング」（P.19） • 「PIM の設定」（P.32）
IPv6 マルチキャスト：スコープ境界	12.0(26)S 12.2(18)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.3(2)T 12.4 12.4(2)T 15.0(1)S	IPv6 では、グローバル アドレスと非グローバル アドレスがサポートされています。ここでは、異なるスコープの IPv6 アドレスの使用方法について説明します。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 マルチキャスト アドレッシング」（P.4） • 「限定スコープ アドレス アーキテクチャ」（P.6） • 「IPv6 BSR」（P.13） • 「BSR の設定」（P.39）
IPv6 マルチキャスト：MLD アクセス グループ	12.0(26)S 12.3(4)T 12.2(25)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA1 2.2(33)SXH 12.4 12.4(2)T 15.0(1)S	MLD アクセス グループは、Cisco IOS IPv6 マルチキャスト ルータでの受信側アクセス コントロールを実現します。 この機能に関する詳細については、次の各項を参照してください。 • 「MLD アクセス グループ」（P.9） • 「インターフェイスでの MLD のカスタマイズおよび確認」（P.22）
IPv6 マルチキャスト：PIM accept register	12.0(26)S 12.3(4)T 12.2(25)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(33)SXH 12.4 12.4(2)T 15.0(1)S	PIM accept register は、RP で PIM-SM register メッセージのフィルタリングを実行するための機能です。 この機能に関する詳細については、次の各項を参照してください。 • 「PIM 希薄モード」（P.10） • 「PIM オプションの設定」（P.34）

表 1　IPv6 マルチキャストの実装の機能情報 （続き）

機能名	リリース	機能情報
IPv6 マルチキャスト：PIM 組み込み RP サポート	12.0(26)S 12.3(4)T 12.2(25)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(33)SXH 12.4 12.4(2)T 15.0(1)S	組み込み RP サポートを利用すると、ルータは、スタティックに設定されている RP の代わりに、マルチキャスト グループ宛先アドレスを使用して RP 情報を学習できるようになります。 この機能に関する詳細については、次の各項を参照してください。 • 「PIM 希薄モード」（P.10） • 「IPv6 PIM での組み込み RP サポートのディセーブル化」（P.59）
IPv6 マルチキャスト：BSR パケットの RPF フラッディング	12.0(26)S 12.3(4)T 12.2(25)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(33)SXH 12.4 12.4(2)T 15.0(1)S	BSR パケットの RPF フラッディングを使用すると、Cisco IOS IPv6 ルータが BSM のフローを妨げることがなくなります。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 BSR」（P.13）
IPv6 マルチキャスト：ルーティング可能アドレスの hello オプション	12.0(26)S 12.3(4)T 12.2(25)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(33)SXH 12.4 12.4(2)T 15.0(1)S	ルーティング可能アドレスの hello オプションを使用すると、PIM hello メッセージがアドバタイズされるインターフェイス上のすべてのアドレスを含む PIM hello メッセージ オプションが追加されます。 この機能に関する詳細については、次の各項を参照してください。 • 「ルーティング可能アドレスの hello オプション」（P.17） • 「PIM オプションの設定」（P.34）
IPv6 マルチキャスト：スタティック マルチキャスト ルーティング（mroute）	12.0(26)S 12.3(4)T 12.2(25)S 12.2(28)SB 12.2(33)SRA 12.2(33)SXH 12.4 12.4(2)T 15.0(1)S	IPv6 スタティック mroute は、IPv6 スタティック ルートと同じデータベースを共有し、スタティック ルート サポートを拡張することによって実装されます。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 マルチキャストの実装の制約事項」（P.2） • 「スタティック mroute」（P.18） • 「スタティック mroute の設定」（P.44）

表 1　IPv6 マルチキャストの実装の機能情報 （続き）

機能名	リリース	機能情報
IPv6 マルチキャスト：マルチプロトコル BGP 用のアドレス ファミリ サポート	12.0(26)S 12.2(25)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(33)SXH 12.3(4)T 12.4 12.4(2)T 15.0(1)S	この機能は、IPv6 のマルチキャスト BGP 拡張を提供し、IPv4 BGP と同じ機能をサポートしています。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 マルチキャスト アドレス ファミリのマルチプロトコル BGP」（P.20） • 「IPv6 マルチプロトコル BGP の設定」（P.46）
IPv6 マルチキャスト：受信側の明示的トラッキング	12.2(25)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(33)SXH 12.3(7)T 12.4 12.4(2)T 15.0(1)S	この機能を使用すると、ルータが IPv6 ネットワーク内のホストの動作を追跡できるようになります。 この機能に関する詳細については、次の各項を参照してください。 • 「受信側の明示的トラッキング」（P.9） • 「受信側の明示的トラッキングによってホストの動作を追跡するための設定」（P.26）
IPv6 マルチキャスト：IPv6 双方向 PIM	12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(25)S 12.3(7)T 12.4 12.4(2)T 15.0(1)S	双方向 PIM を使用すると、マルチキャスト ルータが縮小ステート情報を維持できるようになります。双方向共有ツリーは、送信元から RP にデータを伝送し、それらを RP から受信側に配布します。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 マルチキャストの実装の制約事項」（P.2） • 「双方向 PIM」（P.18） • 「双方向 PIM の設定および双方向 PIM 情報の表示」（P.36）
IPv6 マルチキャスト：MRIB	12.0(26)S 12.2(18)S 12.2(25)SG 12.3(2)T 12.4 12.4(2)T	MRIB は、マルチキャスト ルーティング プロトコル（ルーティング クライアント）によってインスタンス化されるマルチキャスト ルーティング エントリのプロトコル非依存リポジトリです。 この機能に関する詳細については、次の各項を参照してください。 • 「MRIB」（P.18） • 「分散型 MFIB」（P.19） • 「PIM トポロジ テーブルをクリアすることによる MRIB 接続のリセット」（P.37）

表 1　IPv6 マルチキャストの実装の機能情報 （続き）

機能名	リリース	機能情報
IPv6 マルチキャスト：MFIB および MFIB 表示の拡張	12.0(26)S 12.2(18)S 12.3(2)T 12.4 12.4(2)T	MFIB は、IPv6 ソフトウェア用のプラットフォーム非依存およびルーティング プロトコル非依存ライブラリです。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 マルチキャストの実装の制約事項」（P.2） • 「MFIB」（P.18） • 「IPv6 マルチキャストのプロセス スイッチングおよびファスト スイッチング」（P.19） • 「IPv6 マルチキャストでの MFIB の使用」（P.57） • 「ルータでの MFIB のディセーブル化」（P.61） • 「MFIB 割り込みレベル IPv6 マルチキャスト転送のディセーブル化」（P.63）
IPv6 マルチキャスト：Bootstrap Router（BSR; ブートストラップ ルータ）	12.0(28)S 12.2(25)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(33)SXH 12.3(11)T 12.4 12.4(2)T 15.0(1)S	この機能を使用すると、到達不能になった RP が検出され、マッピング テーブルが変更されます。これにより、到達不能な RP が今後使用されなくなり、新しいテーブルがドメイン全体に迅速に配布されるようになります。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 BSR」（P.13） • 「BSR の設定」（P.39）
IPv6 マルチキャスト：IPv6 BSR 双方向サポート	12.2(33)SRE 12.3(14)T 12.4 12.4(2)T 15.0(1)S	双方向 BSR がサポートされているため、双方向 RP を C-RP メッセージおよび BSM の双方向範囲でアドバタイズできます。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 BSR」（P.13）
IPv6 マルチキャスト：IPv6 BSR 限定スコープ ゾーン サポート	12.2(18)SXE 12.2(28)SB	BSR では、管理用スコープ マルチキャストを使用してネットワークでグループと RP のマッピングを配布することによって、限定スコープ ゾーンをサポートしています。ユーザは、ドメイン内の管理用スコープ領域ごとに候補 BSR と一連の候補 RP を設定できます。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 BSR」（P.13） • 「限定スコープ ゾーン内で BSR を使用できるようにするための設定」（P.41） • 「BSR ルータにスコープと RP のマッピングをアナウンスさせるための設定」（P.42）

表 1　IPv6 マルチキャストの実装の機能情報 （続き）

機能名	リリース	機能情報
IPv6 マルチキャスト：SSM マッピング	12.2(28)SB 12.2(33)SRA 12.2(18)SXE 12.4(2)T 15.0(1)S	この機能を使用すると、TCP/IP ホスト スタックおよび IP マルチキャスト受信アプリケーションで MLD バージョン 2 サポートを提供できないホストで IPv6 SSM を展開できます。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 用の SSM マッピング」（P.15） • 「SSM マッピングの設定」（P.43）
IPv6 マルチキャスト：IPv6 BSR：RP マッピングを設定	12.2(33)SRE 12.4(2)T 15.0(1)S	この機能を使用すると、スコープと RP のマッピングを候補 RP メッセージから学習する代わりに、BSR から直接アナウンスするように、IPv6 マルチキャスト ルータをスタティックに設定できます。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 BSR」（P.13） • 「BSR ルータにスコープと RP のマッピングをアナウンスさせるための設定」（P.42）
IPv6 マルチキャスト：MLD グループ制限	12.2(33)SRE 12.4(2)T 15.0(1)S	MLD グループ制限機能は、MLD パケットによって生じる Denial of Service（DoS; サービス拒絶）攻撃に対する保護を提供します。 この機能に関する詳細については、次の各項を参照してください。 • 「マルチキャスト リスナー ディスカバリ プロトコル for IPv6」（P.8） • 「MLD グループ制限の実装」（P.24）
IPv6 マルチキャスト：マルチキャスト ユーザ認証およびプロファイル サポート	12.4(4)T	マルチキャスト アクセス コントロールは、マルチキャストと AAA の間のインターフェイスを提供し、ラストホップ ルータ、マルチキャストにおける受信側アクセス コントロール機能、およびマルチキャストにおけるグループまたはチャネル ディセーブル化機能でのプロビジョニング、認可、およびアカウンティングを実現します。 この機能に関する詳細については、次の各項を参照してください。 • 「マルチキャスト ユーザ認証およびプロファイル サポート」（P.9） • 「マルチキャスト ユーザ認証およびプロファイル サポートの設定」（P.27）

表 1　IPv6 マルチキャストの実装の機能情報 （続き）

機能名	リリース	機能情報
IPv6 マルチキャスト：プロセス スイッチングおよびファスト スイッチング	12.0(26)S 12.2(18)S 12.3(2)T 12.4 12.4(2)T	IPv6 マルチキャストのプロセス スイッチングでは、ルートプロセッサが各パケットの調査、書き換え、および転送を行う必要があります。IPv6 マルチキャストのファスト スイッチングを使用すると、ルータはプロセス スイッチングよりも高いパケット転送パフォーマンスを実現できます。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 マルチキャストのプロセス スイッチングおよびファスト スイッチング」（P.19）
Distributed MFIB（dMFIB; 分散型 MFIB）	12.0(26)S 12.2(25)S 12.2(28)SB 12.3(4)T 12.4 12.4(2)T	Distributed MFIB（dMFIB; 分散型 MFIB）は、分散型プラットフォーム上でマルチキャスト IPv6 パケットをスイッチングするために使用されます。 この機能に関する詳細については、次の各項を参照してください。 • 「分散型 MFIB」（P.19） • 「分散型プラットフォームでの MFIB のディセーブル化」（P.62）
IPv6：マルチキャスト アドレス グループ範囲のサポート	12.2(33)SRE 12.2(33)SXI 15.0(1)M 15.0(1)S	この機能を使用すると、未認証グループまたは未認可チャネルからのマルチキャスト トラフィックをルータで受信しないようにすることができます。 この機能に関する詳細については、次の各項を参照してください。 • 「ルータでの未認証マルチキャスト トラフィックの受信のディセーブル化」（P.29）
IPv6 マルチキャスト：帯域幅ベースの Call Admission Control（CAC; コール アドミッション制御）	12.2(33)SRE 15.0(1)S	IPv6 マルチキャストの帯域幅ベースの Call Admission Control（CAC; コール アドミッション制御）機能は、インターフェイス単位およびマルチキャスト グループ単位で帯域幅を監視して、マルチキャスト サービスによる加入過多を避ける手段を実装します。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 マルチキャストの帯域幅ベースの CAC」（P.21） • 「IPv6 の帯域幅ベースの CAC の設定」（P.54） • 「例：IPv6 の帯域幅ベースの CAC の設定」（P.75）
NSF/SSO：IPv6 マルチキャスト	12.2(33)SRE	この機能は Cisco IOS Release 12.2(33)SRE でサポートされています。 この機能に関する詳細については、次の項を参照してください。 • 「IPv6 マルチキャストでの NSF と SSO のサポート」（P.20）

表 1　IPv6 マルチキャストの実装の機能情報 （続き）

機能名	リリース	機能情報
MFIB：IPv4 SSO/ISSU	12.2(33)SRE	この機能は Cisco IOS Release 12.2(33)SRE でサポートされています。
MLD プロキシ	15.1(2)T	MLD プロキシ機能により、デバイスは、プロキシ グループ メンバシップ情報を学習し、その情報に基づいてマルチキャスト パケットを転送できるようになります。 この機能に関する詳細については、次の各項を参照してください。 • 「MLD プロキシ」（P.10） • 「IPv6 での MLD プロキシのイネーブル化」（P.30） • 「例：MLD プロキシの設定」（P.73）

Netflow v9 for IPv6

この章では、NetFlow バージョン 9（v9）エクスポート フォーマットを使用して、IP バージョン 6（IPv6）トラフィック フローからデータをキャプチャしてエクスポートするために NetFlow および NetFlow Data Export（NDE; ネットフロー データ エクスポート）を設定する手順と設定の概要を示します。

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「Netflow v9 for IPv6 の機能情報」（P.9）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

Netflow v9 for IPv6 の前提条件

Netflow v9 for IPv6 機能を設定するには、ルータで Cisco IOS release 12.2(33)SRB 以降が実行されている必要があります。

Netflow v9 for IPv6 に関する情報

PFC での NetFlow および NDE

PFC での NetFlow キャッシュは、ハードウェア内でルーティングされたフローに対する統計情報をキャプチャします。

PFC は、次のいずれかのフロー マスクを使用して、NetFlow エントリを作成します。

- **source-only**：キャッシュには、送信元 IP アドレスごとに 1 つずつのエントリが含まれます。1 つの送信元 IP アドレスからのすべてのフローで、このエントリが使用されます。
- **destination**：キャッシュには、宛先 IP アドレスごとに 1 つずつのエントリが含まれます。1 つの宛先 IP アドレスへのすべてのフローで、このエントリが使用されます。
- **destination-source**：キャッシュには、送信元 IP アドレスと宛先 IP アドレスのペアごとに 1 つずつのエントリが含まれます。同じ送信元 IP アドレスと宛先 IP アドレス間のすべてのフローで、このエントリが使用されます。
- **destination-source-interface**：**destination-source** フロー マスク内の情報に、送信元 VLAN SNMP ifIndex が追加されます。
- **full**：IP フローごとに個別のキャッシュ エントリが作成されます。完全なエントリには、送信元 IP アドレス、宛先 IP アドレス、プロトコル、およびプロトコル インターフェイスが含まれます。
- **full-interface**：**full** フロー マスク内の情報に、送信元 VLAN SNMP ifIndex が追加されます。

NetFlow フロー マスクおよびフロー レコードの詳細については、『*Cisco 7600 Series Cisco IOS Software Configuration Guide, Release 12.2SR*』の「Configuring NetFlow and NDE」の章を参照してください。

NetFlow エクスポート フォーマット バージョン 9

どの NetFlow エクスポート バージョンでも、NetFlow エクスポート データグラムは、1 つのヘッダーと一連のフロー レコードで構成されます。ヘッダーには、シーケンス番号、レコード カウント、システム動作時間などの情報が含まれています。フロー レコードには、IP アドレス、ポート、ルーティング情報などのフロー情報が含まれています。

NetFlow バージョン 9 エクスポート フォーマットは、最新の NetFlow エクスポート フォーマットです。NetFlow バージョン 9 エクスポート フォーマットの他と異なる特徴は、テンプレート ベースであるということです。テンプレートにより、レコード フォーマットが拡張可能になります。NetFlow バージョン 9 エクスポート フォーマットを使用すると、将来的に、基本的なフローレコード フォーマットに並列的な変更を加えなくても NetFlow を拡張できます。

NetFlow バージョン 9 エクスポートのレコード フォーマットは、従来の NetFlow 固定フォーマット エクスポート レコードとは異なります。NetFlow バージョン 9 では、テンプレートにより NetFlow データが説明され、フロー セットに実際のデータが含まれます。このような配置によって、フレキシブルなエクスポートを可能にしています。

NetFlow バージョン 9 エクスポート フォーマットでテンプレートを使用すると、他にも次のような主要な利点があります。

- ルータまたはスイッチから、ほとんどすべての情報（レイヤ 2 ～ 7 の情報、ルーティング情報、IP バージョン 6（IPv6）、IP バージョン 4（IPv4）、マルチキャスト、および Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）情報を含む）をエクスポートできる。この新しい情報により、新たなエクスポート データの活用とネットワーク動作の表示が可能になります。
- NetFlow コレクタや NetFlow 向け表示サービスを提供するアプリケーションを製造するサードパーティのビジネス パートナーは、新しい NetFlow エクスポート フィールドが追加されるたびにアプリケーションをリコンパイルする必要がない。そうしなくても、既知のテンプレート フォーマットを説明する外部データ ファイルを使用できます。
- 現在の実装を中断することなく、より短時間で NetFlow に新しい機能を追加できる。
- NetFlow は、将来的に新しいプロトコルまたは開発中のプロトコルに対しても使用できる。バージョン 9 エクスポート フォーマットは、これらのプロトコルや、データ収集に対する NetFlow ベースでないアプローチをサポートするように調整できるためです。

表 1 に、NetFlow バージョン 9 エクスポート パケット ヘッダー フォーマットを示します。

表 1　NetFlow バージョン 9 エクスポート パケット ヘッダーのフィールド名および説明

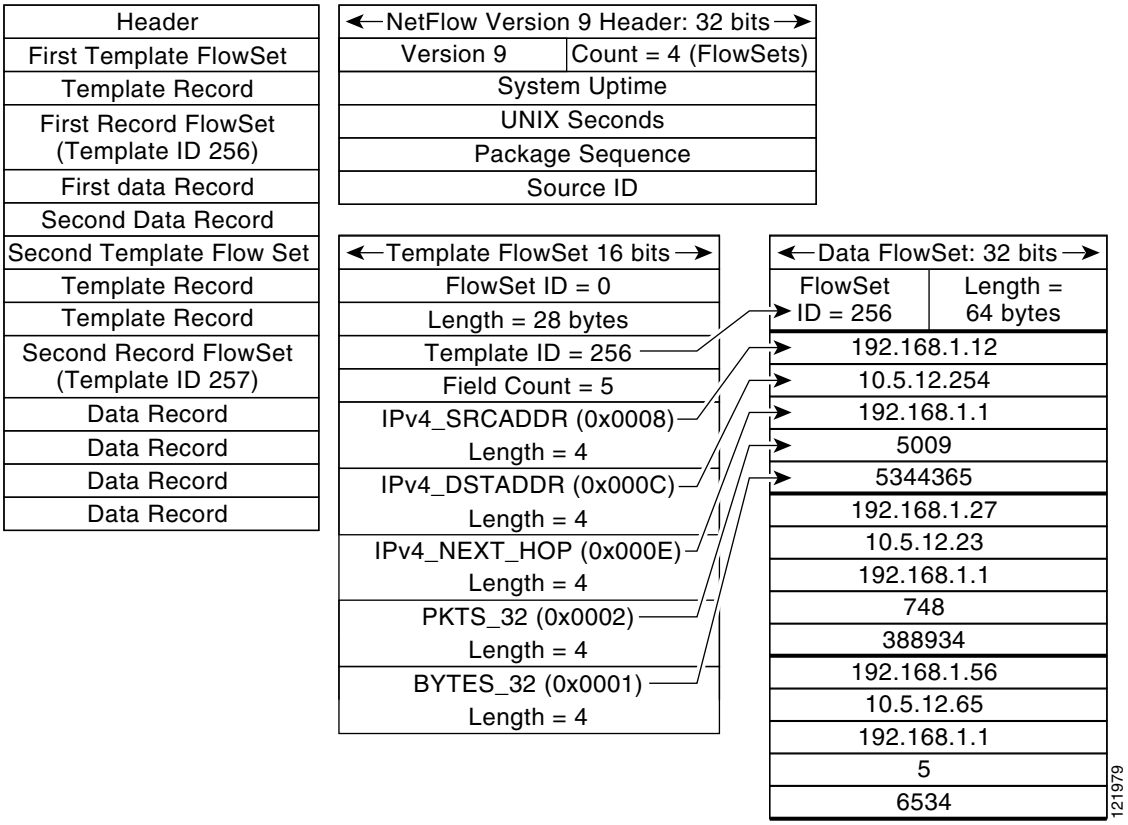
バイト	フィールド名	説明
0 ～ 1	Version	このパケット内にエクスポートされた NetFlow レコードのバージョン。バージョン 9 の場合、この値は 0x0009 です。
2 ～ 3	Count	このパケット内に含まれる FlowSet レコード（テンプレートおよびデータ）の数。
4 ～ 7	System Uptime	このデバイスが最初に起動されてからの経過時間（ミリ秒）。
8 ～ 11	UNIX Seconds	0000 Coordinated Universal Time（UTC; 協定世界時）1970 以降の秒数。

表 1　NetFlow バージョン 9 エクスポート パケット ヘッダーのフィールド名および説明 （続き）

バイト	フィールド名	説明
12 ～ 15	Sequence Number	このエクスポート デバイスにより送信されたすべてのエクスポート パケットのインクリメンタル シーケンス カウンタ。この値は累積値であり、ミスされたエクスポート パケットがあるか調べるために使用できます。 これは NetFlow バージョン 5 およびバージョン 8 のヘッダーから変更された点です。NetFlow バージョン 5 およびバージョン 8 では、この数値は「合計のフロー」を表していました。
16 ～ 19	Source ID	Source ID フィールドは 32 ビットの値であり、特定のデバイスからエクスポートされた各フローの固有性を保証するために使用されます（Source ID フィールドは、NetFlow バージョン 5 およびバージョン 8 のヘッダーでの engine type フィールドおよび engine ID フィールドに相当します）。このフィールドのフォーマットは、ベンダーに固有です。シスコの実装においては、最初の 2 つのバイトは将来の拡張用に予約されており、常に 0 となります。バイト 3 は、エクスポート側デバイスのルーティング エンジンに関する固有性を提供します。バイト 4 は、エクスポート側デバイスの特定のラインカードまたは Versatile Interface Processor に関する固有性を提供します。コレクタ デバイスは、送信元 IP アドレスと Source ID フィールドを組み合せて使用して、着信した NetFlow エクスポート パケットを特定デバイス上の NetFlow の固有インスタンスと関連付ける必要があります。

図 1 に、NetFlow バージョン 9 エクスポート フォーマットを使用してデータをエクスポートする一般的な例を示します。

図 1　NetFlow バージョン 9 エクスポート フォーマット パケットの例



NetFlow エクスポート フォーマット バージョン 9 およびエクスポート フォーマット アーキテクチャの詳細については、『*NetFlow version 9 Flow-Record Format*』を参照してください。

Netflow v9 for IPv6 の設定方法

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **mls flow** {**ip** | **ipv6**} {**destination** | **destination-source** | **full** | **interface-destination-source** | **interface-full** | **source**}
5. **mls nde sender**
6. **ip flow-export version 9**
7. **ip flow-export destination** {*ip-address* | *hostname*} *udp-port*
8. **interface** *type number*
9. **ipv6 address** *ip-address/mask*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 unicast-routing** **例：** `Router(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。
ステップ 4	**mls flow** {**ip** | **ipv6**} {**destination** | **destination-source** | **full** | **interface-destination-source** | **interface-full** | **source**} **例：** `Router(config)# mls flow ipv6 interface-full`	IPv6 トラフィックの NetFlow フロー マスクを指定します。
ステップ 5	**mls nde sender** **例：** `Route(config)# mls nde sender`	ルータでグローバルに NDE をイネーブルにします。 **（注）** エクスポートされるトラフィックの宛先を指定するまで、NDE はデータのエクスポートを開始しません。エクスポートされるトラフィックの宛先は、手順 7 で指定します。
ステップ 6	**ip flow-export version 9** **例：** `Router(config)# ip flow-export version 9`	NetFlow バージョン 9 エクスポート フォーマットを使用するように NDE を設定します。
ステップ 7	**ip flow-export destination** {*ip-address* | *hostname*} *udp-port* **例：** `Router(config)# ip flow-export destination 172.16.10.2 88`	NetFlow コレクタの IP アドレスまたはホスト名と、NetFlow コレクタがリスニングする UDP ポートを指定します。
ステップ 8	**interface** *type number* **例：** `Router(config)# interface fastethernet 1/1`	NetFlow をイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**ipv6 address** *ip-address/mask* **例：** `Router(config-if)# ipv6 address 2001:0DB8:AB::2/64`	インターフェイスで IPv6 アドレスを設定します。

例

show mls nde コマンドの次の出力により、ルータで NDE がイネーブルになっていることを確認できます。

```
Router# show mls nde

 NetFlow Data Export enabled
 Exporting flows to 10.30.30.2 (12345)  172.16.10.2 (88)
 Exporting flows from 10.4.9.149 (58970)
 Version: 9
 Layer2 flow creation is disabled
 Layer2 flow export is disabled
 Include Filter not configured
 Exclude Filter not configured
 Total NetFlow Data Export Packets are:
    0 packets, 0 no packets, 0 records
 Total NetFlow Data Export Send Errors:
        IPWRITE_NO_FIB = 0
        IPWRITE_ADJ_FAILED = 0
        IPWRITE_PROCESS = 0
        IPWRITE_ENQUEUE_FAILED = 0
        IPWRITE_IPC_FAILED = 0
        IPWRITE_OUTPUT_FAILED = 0
        IPWRITE_MTU_FAILED = 0
        IPWRITE_ENCAPFIX_FAILED = 0
 NetFlow Aggregation Disabled
```

Netflow v9 for IPv6の設定例

ここでは、次の設定例を示します。

- 「例：NetFlow v9 for IPv6 機能の設定」（P.7）

例：NetFlow v9 for IPv6 機能の設定

次に、NetFlow エクスポート フォーマット バージョン 9 を使用して、IPv6 トラフィックに NetFlow および NDE のルータを設定する例を示します。

```
ipv6 unicast-routing
mls flow ipv6 interface-full
mls nde sender
ip flow-export version 9
ip flow-export destination 172.16.10.2 88
interface FastEthernet1/1
ipv6 address 2001:0DB8::1/64
```

その他の関連資料

関連資料

関連項目	参照先
プラットフォームに依存しない NetFlow コマンド、完全なコマンド構文、コマンド モード、デフォルト、コマンド履歴、使用上のガイドライン、および例	『*Cisco IOS NetFlow Command Reference*』
Cisco 7600 シリーズ ルータのコマンド リファレンス	『*Cisco 7600 Series Cisco IOS Command Reference*』

規格

規格	タイトル
この機能に関連付けられている規格はありません。	—

MIB

MIB	MIB リンク
•	選択したプラットフォーム、Cisco ソフトウェア リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 3954	『*Cisco Systems NetFlow Services Export Version 9*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

Netflow v9 for IPv6の機能情報

表 2 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どのソフトウェア イメージが特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 2には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 2　Netflow v9 for IPv6 の機能情報

機能名	リリース	機能情報
Netflow v9 for IPv6	12.2(33)SRB 15.0(1)S	Netflow v9 for IPv6 機能を使用すると、IPv6 トラフィックの NetFlow フロー情報のエクスポートが可能になります。 この機能のサポートは、12.2(33)SRB で Cisco 7600 シリーズ ルータに追加されました。

OSPF for IPv6 の実装

「*OSPF for IPv6 の実装*」の章では、Open Shortest Path First（OSPF）が拡張され、IPv6 ルーティング プレフィクスのサポートが提供されています。この章では、ネットワークで OSPF for IPv6 を実装するために必要な概念と作業について説明します。

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「OSPF for IPv6 の実装の機能情報」（P.32）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

OSPF for IPv6 の実装の前提条件

インターフェイスで OSPF for IPv6 をイネーブルにする前に、次の作業を実行する必要があります。

- OSPF ネットワーク方針と IPv6 ネットワークの計画を完了する。たとえば、複数のエリアが必要かどうかを決定する必要があります。
- IPv6 ユニキャスト ルーティングをイネーブルにする。
- インターフェイスで IPv6 をイネーブルにする。
- 認証および暗号化をイネーブルにするために、OSPF for IPv6 に対して IP Security（IPSec; IP セキュリティ）セキュア ソケット Application Program Interface（API; アプリケーション プログラム インターフェイス）を設定する。

このマニュアルでは、IPv4 に精通していることを前提としています。IPv4 の設定およびコマンド リファレンス情報については、「関連資料」の関連資料を参照してください。

OSPF for IPv6 の実装の制約事項

- OSPF バージョン 2 for IPv4 および OSPF for IPv6 を使用してデュアルスタック IP ネットワークを実行している場合、OSPF for IPv6 のイネーブル化に使用するコマンドのデフォルトを変更する際は、注意してください。これらのデフォルトを変更すると、OSPF for IPv6 ネットワークに悪影響を及ぼすことがあります。
- 認証は、Cisco IOS Release 12.3(4)T 以降でサポートされています。
- ESP 認証および暗号化は、Cisco IOS Release 12.4(9)T 以降でサポートされています。
- あるルータ上のインターフェイスで見つかった IPv6 アドレスから発信されたパケットは、そのルータ上では拒否されます。

OSPF for IPv6 の実装に関する情報

OSPF for IPv6 の機能

OSPF は、IP 用のルーティング プロトコルです。OSPF は、距離ベクトル型プロトコルではなく、リンクステート型プロトコルです。リンクを、ネットワーキング デバイス上のインターフェイスとして考えます。リンクステート型プロトコルは、送信元マシンと宛先マシンを接続するリンクのステートに基づいて、ルーティングの決定を行います。リンク ステートは、インターフェイスと、その隣接ネットワーキング デバイスとの関係を説明するものです。インターフェイス情報には、インターフェイスの IPv6 プレフィクス、ネットワーク マスク、接続先のネットワークのタイプ、そのネットワークに接続されているルータなどが含まれます。この情報は、さまざまなタイプの Link-State Advertisement（LSA; リンクステート アドバタイズメント）で伝播されます。

ルータの LSA データの集まりは、リンクステート データベースに格納されます。ダイクストラ アルゴリズムが採用されている場合、データベースの内容に基づいて OSPF ルーティング テーブルが作成されます。データベースとルーティング テーブルの違いは、データベースには raw データの完全な集まりが含まれるのに対し、ルーティング テーブルには特定のルータ インターフェイス ポートを経由する既知の宛先への最短パスのリストが含まれることです。

（RFC 2740 で説明されている）OSPF バージョン 3 は、IPv6 をサポートしています。

OSPF for IPv6 と OSPF バージョン 2 の比較

OSPF for IPv6 機能のほとんどは、OSPF バージョン 2 の機能と同じです。（RFC 2740 で説明されている）OSPF バージョン 3 for IPv6 では、OSPF バージョン 2 が拡張され、IPv6 ルーティング プレフィクスと、より大きなサイズの IPv6 アドレスに対するサポートが提供されています。

OSPF for IPv6 では、ルーティング プロセスを明示的に作成する必要はありません。インターフェイスで OSPF for IPv6 をイネーブルにすると、ルーティング プロセスおよびそれに関連する設定が作成されます。

OSPF for IPv6 では、インターフェイス コンフィギュレーション モードでコマンドを使用して、各インターフェイスをイネーブルにする必要があります。この機能は、ルータ コンフィギュレーション モードを使用してインターフェイスが間接的にイネーブルになる OSPF バージョン 2 とは異なっています。

OSPF for IPv6 で NonBroadcast MultiAccess（NBMA; 非ブロードキャスト マルチアクセス）を使用する場合、ユーザはネイバー リストを使用してルータを手動で設定する必要があります。ネイバー ルータは、それぞれのルータ ID によって識別されます。

IPv6 では、ユーザは 1 つのインターフェイス上に多数のアドレス プレフィクスを設定できます。OSPF for IPv6 には、デフォルトで、1 つのインターフェイス上のすべてのアドレス プレフィクスが組み込まれます。OSPF for IPv6 にインポートするアドレス プレフィクスをユーザが選択することはできません。1 つのインターフェイス上のすべてのアドレス プレフィクスがインポートされるか、1 つのインターフェイス上のいずれのアドレス プレフィクスもインポートされないかのどちらかです。

OSPF バージョン 2 とは異なり、1 つのリンクで OSPF for IPv6 の複数のインスタンスを実行できます。

OSPF for IPv6 では、インターフェイスに IPv4 アドレスを設定しないことが可能です。この場合、ユーザは、OSPF プロセスの開始前に、**router-id** コマンドを使用してルータ ID を設定する必要があります。ルータ ID は、32 ビットの不透明な番号です。OSPF バージョン 2 は、32 ビット IPv4 アドレスを利用して、ルータ ID としての IPv4 アドレスを選択します。インターフェイスで OSPF for IPv6 がイネーブルになっている場合、IPv4 アドレスが存在していると、その IPv4 アドレスがルータ ID として使用されます。複数の IPv4 アドレスが使用可能な場合、OSPF バージョン 2 と同じルールを使用してルータ ID が選択されます。

OSPF では、自動的にループバック インターフェイスが他よりも優先されます。また、すべてのループバック インターフェイスの中で最も高位の IP アドレスが選択されます。ループバック インターフェイスが存在しない場合、ルータ内で最も高位の IP アドレスが選択されます。特定のインターフェイスを使用するように OSPF に指示することはできません。

IPv6 の LSA タイプ

次に、それぞれ用途の異なる LSA タイプを示します。

- ルータ LSA（タイプ 1）：エリアへのルータのリンクのリンク ステートとコストが説明されます。これらの LSA は、エリア内部でだけフラッディングされます。この LSA は、ルータが Area Border Router（ABR; エリア境界ルータ）か Autonomous System Boundary Router（ASBR; 自律システム境界ルータ）か、およびそのルータが仮想リンクの一端であるかどうかを示します。また、タイプ 1 の LSA は、スタブ ネットワークへのアドバタイズにも使用されます。OSPF for IPv6 では、これらの LSA はアドレス情報を持たず、ネットワークプロトコルに依存しません。OSPF for IPv6 では、ルータ インターフェイス情報は複数のルータ LSA に分配されます。受信者は、SPF 計算の実行時に、特定のルータから発信されたすべてのルータ LSA を連結する必要があります。
- ネットワーク LSA（タイプ 2）：ネットワークに接続されているすべてのルータのリンクステートおよびコスト情報が説明されます。この LSA は、ネットワーク内のすべてのリンクステートおよびコスト情報を集約したものです。代表ルータだけがこの情報を追跡し、ネットワーク LSA を生成できます。OSPF for IPv6 では、ネットワーク LSA はアドレス情報を持たず、ネットワークプロトコルに依存しません。
- ABR のエリア間プレフィクス LSA（タイプ 3）：他のエリア内のルータ（エリア間ルート）に内部ネットワークがアドバタイズされます。タイプ 3 の LSA は、単一のネットワークを表すことも、1 つのアドバタイズメントとして集約された一連のネットワークを表すこともあります。集約 LSA を生成するのは、ABR だけです。OSPF for IPv6 では、これらの LSA のアドレスは、*address*, *mask* ではなく、*prefix*, *prefix length* として表現されます。デフォルト ルートは、長さが 0 のプレフィクスとして表現されます。
- ASBR のエリア間ルータ LSA（タイプ 4）：ASBR のロケーションがアドバタイズされます。外部ネットワークにアクセスしようとするルータは、これらのアドバタイズメントを使用して、ネクストホップへの最良パスを決定します。タイプ 4 の LSA は、ASBR によって生成されます。
- 自律システム外部 LSA（タイプ 5）：別の AS から（通常は別のルーティング プロトコルから OSPF に）ルートを再分配します。OSPF for IPv6 では、これらの LSA のアドレスは、*address*, *mask* ではなく、*prefix*, *prefix length* として表現されます。デフォルト ルートは、長さが 0 のプレフィクスとして表現されます。
- リンク LSA（タイプ 8）：ローカルリンク フラッディング スコープを持ちます。関連付けられているリンクを越えてフラッディングされることはありません。リンク LSA は、リンクに接続されている他のすべてのルータに対してルータのリンクローカル アドレスを提供し、リンクに接続されている他のルータに、そのリンクに関連付ける IPv6 プレフィクスのリストを通知します。また、ルータが Options ビットの集まりをアサートして、リンクの起点となるネットワーク LSA と関連付けできるようにします。
- エリア内プレフィクス LSA（タイプ 9）：ルータは、ルータまたは中継ネットワークごとに、それぞれ固有のリンクステート ID を持つ複数のエリア内プレフィクス LSA を発信できます。各エリア内プレフィクス LSA のリンクステート ID は、ルータ LSA またはネットワーク LSA とのアソシエーションを説明するもので、スタブおよび中継ネットワークのプレフィクスを含んでいます。

新しく定義された LSA のほとんどすべてに、アドレス プレフィクスが存在します。プレフィクスは、PrefixLength、PrefixOptions、および Address Prefix の 3 つのフィールドで表現されます。OSPF for IPv6 では、これらの LSA のアドレスは、*address*, *mask* ではなく、*prefix*, *prefix length* として表現されます。デフォルト ルートは、長さが 0 のプレフィクスとして表現されます。タイプ 3 およびタイプ 9 の LSA は、IPv4 ではルータ LSA とネットワーク LSA に含まれているすべての IPv6 プレフィクス情報を伝送します。特定の LSA（ルータ LSA、ネットワーク LSA、エリア間ルータ LSA、およびリンク LSA）の Options フィールドは、OSPF in IPv6 をサポートするために 24 ビットに拡張されました。

OSPF for IPv6 では、エリア間プレフィクス LSA、エリア間ルータ LSA、および自律システム外部 LSA のリンクステート ID の機能は、リンクステート データベースの個々の部分を識別することだけです。OSPF バージョン 2 でリンクステート ID で表されたアドレスまたはルータ ID はすべて、OSPF for IPv6 では LSA の本体で伝送されます。

ネットワーク LSA およびリンク LSA のリンクステート ID は常に、説明されているリンク上の送信元ルータのインターフェイス ID となります。このため、ネットワーク LSA およびリンク LSA は、サイズ制限ができない LSA だけになりました。ネットワーク LSA は、リンクに接続されているすべてのルータをリストする必要があります。リンク LSA は、リンクのルータのアドレス プレフィクスのすべてをリストする必要があります。

OSPF for IPv6 での NBMA

NBMA ネットワークでは、Designated Router（DR; 代表ルータ）または Backup DR（BDR）が LSA フラッディングを実行します。ポイントツーポイントネットワークでは、フラッディングはインターフェイスからネイバーに直接送信されるだけです。

共通セグメントを共有するルータ（2 つのインターフェイス間のレイヤ 2 リンク）は、そのセグメント上でネイバー同士となります。OSPF では、Hello プロトコルを使用して、各インターフェイスから定期的に Hello パケットを送信します。ルータがネイバーの Hello パケット内に自身がリストされていることを認識すると、それらのルータはネイバー同士となります。2 つのルータがネイバーになると、データベースの交換や同期化を行うことができるようになります。これにより、隣接が作成されます。すべてのネイバー ルータが隣接を持っているわけではありません。

ポイントツーポイント ネットワークおよびポイントツーマルチポイント ネットワーク上では、ソフトウェアによってルーティング アップデートがすぐ隣のネイバーにフラッディングされます。DR も BDR もないため、すべてのルーティング情報が各ネットワーキング デバイスにフラッディングされます。

ブロードキャストまたは NBMA セグメントの場合にかぎり、OSPF では、DR と BDR として 1 つずつルータを選択することにより、セグメント上で交換される情報の量を最小限にします。このため、セグメント上の各ルータには、情報交換のための中央接続ポイントがあります。各ルータは、セグメント上の他のルータそれぞれとルーティング アップデートを交換するのではなく、DR および BDR と情報を交換します。DR および BDR は、情報を他のルータに中継します。

ソフトウェアによってセグメント上の各ルータのプライオリティが確認され、DR および BDR となるルータが決定されます。最も高いプライオリティのルータが DR として選択されます。プライオリティが同じ場合、より高位のルータ ID を持つルータが優先されます。DR が選択されると、BDR が同様の方法で選択されます。プライオリティが 0 に設定されているルータは、DR または BDR になる資格がありません。

OSPF for IPv6 で NBMA を使用する場合、ネイバーを自動的に検出することはできません。NBMA インターフェイスで、インターフェイス コンフィギュレーション モードを使用して、手動でネイバーを設定する必要があります。

OSPF for IPv6 での SPF の強制実行

clear ipv6 ospf コマンドとともに **process** キーワードが使用されている場合、OSPF データベースがクリアされて値が再入力されてから、SPF アルゴリズムが実行されます。**clear ipv6 ospf** コマンドとともに **force-spf** キーワードが使用されている場合、SPF アルゴリズムの実行前に OSPF データベースはクリアされません。

高速コンバージェンス - LSA および SPF スロットリング

OSPF for IPv6 の LSA および SPF スロットリング機能は、ネットワークが不安定な間、OSPF でのリンクステート アドバタイズメント アップデートを低速化するためのダイナミック メカニズムを提供します。また、ミリ秒単位の LSA レート制限を提供することにより、より高速な OSPF コンバージェンスを可能にしています。

以前は、OSPF for IPv6 では、レート制限の SPF 計算および LSA 生成にスタティック タイマーを使用していました。これらのタイマーも設定可能ですが、使用される値を秒単位で指定するため、OSPF for IPv6 コンバージェンスに制約が生まれます。LSA および SPF スロットリングは、すばやく応答できる高度な SPF および LSA レート制限メカニズムを提供することにより、1 秒未満単位でのコンバージェンスを実現し、長引く不安定期間中にも安定性および保護を提供します。

OSPF for IPv6 でのロード バランシング

ルータは、複数のルーティング プロセス（またはルーティング プロトコル）を介して特定のネットワークへの複数のルートを認識すると、最短の管理ディスタンスを持つルートをルーティング テーブルにインストールします。同じ管理ディスタンスを持つ同じルーティング プロセスを介して認識された多数のルートから、1 つのルートを選択する必要があることもあります。この場合、ルータは宛先へのコスト（またはメトリック）が最小のパスを選択します。各ルーティング プロセスにより、そのコストが別々に計算されます。また、ロード バランシングを実現するために、コストを操作する必要がある場合もあります。

OSPF では、次のようにしてロード バランシングを自動的に実行します。OSPF で複数のインターフェイスを介して宛先に到達できることが確認されたが、各パスのコストが同じである場合、各パスがルーティング テーブルにインストールされます。同じ宛先へのパスの数は、**maximum-paths** コマンドを指定しないかぎり制限されません。デフォルトの最大パスは 16 です。有効範囲は 1 ～ 64 です。

OSPF for IPv6 へのアドレス インポート

OSPF for IPv6 が実行されているインターフェイス上で指定されているアドレス セットを OSPF for IPv6 にインポートするときに、インポートする特定のアドレスをユーザが選択することはできません。すべてのアドレスがインポートされるか、いずれのアドレスもインポートされないかのどちらかです。

OSPF for IPv6 のカスタマイズ

ご使用のネットワークに対して OSPF for IPv6 をカスタマイズすることもできますが、通常はその必要はありません。OSPF in IPv6 のデフォルトは、ほとんどのカスタマーおよび機能の要件を満たすように設定されています。デフォルトを変更する必要がある場合は、IPv6 コマンド リファレンスを参照して、適切な構文を確認してください。

注意 デフォルトを変更する際は、注意してください。デフォルトを変更すると、OSPF for IPv6 ネットワークに悪影響を及ぼすことがあります。

IPsec を使用した OSPF for IPv6 認証サポート

OSPF for IPv6 パケットが変更されてルータに再送信されることにより、ルータが管理者にとって望ましくない動作をすることにならないように、OSPF for IPv6 パケットを認証する必要があります。OSPF for IPv6 では、IP Security（IPSec; IP セキュリティ）セキュア ソケット Application Program Interface（API; アプリケーション プログラム インターフェイス）を使用して、OSPF for IPv6 パケットに認証を追加します。この API は、IPv6 をサポートするように拡張されています。

OSPF for IPv6 では、認証をイネーブルにするために IPsec を使用する必要があります。認証を使用するには、暗号イメージが必要です。これは、OSPF for IPv6 での使用に必要な IPsec API は、暗号イメージにしか含まれていないためです。

OSPF for IPv6 では、認証フィールドが OSPF ヘッダーから削除されています。OSPF が IPv6 上で動作するとき、ルーティング交換の整合性、認証、および機密性を保証するために、OSPF に IPv6 Authentication Header（AH; 認証ヘッダー）または IPv6 ESP ヘッダーが必要となります。IPv6 AH および ESP 拡張ヘッダーを使用すると、OSPF for IPv6 に認証および機密性を提供できます。

IPsec AH を使用するには、**ipv6 ospf authentication** コマンドをイネーブルにする必要があります。IPsec ESP を使用するには、**ipv6 ospf encryption** コマンドをイネーブルにする必要があります。ESP ヘッダーは、単独で適用することも、AH と組み合せて適用することもできます。ESP を使用した場合、暗号化と認証の両方が提供されます。セキュリティ サービスは、通信する 1 組のホスト、通信する 1 組のセキュリティ ゲートウェイ、またはセキュリティ ゲートウェイとホストの間に提供できます。

IPsec を設定するために、ユーザはセキュリティ ポリシーを設定できます。これは、Security Policy Index（SPI）とキーの組み合せです（このキーはハッシュ値の作成および検証に使用されます）。OSPF for IPv6 の IPsec は、インターフェイスまたは OSPF エリアに対して設定できます。セキュリティを強化するには、ユーザは、IPsec を設定する各インターフェイスで異なるポリシーを設定する必要があります。ユーザが OSPF エリアに対して IPsec を設定した場合、ポリシーはそのエリア内のすべてのインターフェイス（IPsec が直接設定されているインターフェイスを除く）に適用されます。OSPF for IPv6 に対して設定された IPsec は、ユーザには不可視です。

トラフィックを保護するために、アプリケーションによりセキュア ソケット API が使用されます。この API によって、アプリケーションによるセキュア ソケットのオープン、リッスン、およびクローズを許可する必要があります。また、アプリケーションと Secure Socket Layer の間のバインディングにより、Secure Socket Layer は、接続のオープンやイベントのクローズなど、ソケットへの変更をアプリケーションに通知できます。セキュア ソケット API は、ソケットを識別できます。つまり、セキュリティを必要とするトラフィックを伝送するローカルおよびリモートのアドレス、マスク、ポート、およびプロトコルを識別できます。

各インターフェイスのセキュア ソケット ステートは、次のいずれかになります。

- NULL：エリアに対して認証が設定されていれば、インターフェイスに対してセキュア ソケットを作成しません。
- DOWN：インターフェイス（またはインターフェイスが含まれるエリア）に対して IPsec は設定されていますが、OSPF for IPv6 がこのインターフェイスに対するセキュア ソケットの作成を IPsec に要求していないか、またはエラー条件が存在します。
- GOING UP：OSPF for IPv6 は IPsec からのセキュア ソケットを要求したあと、IPsec からの CRYPTO_SS_SOCKET_UP メッセージを待機中です。
- UP：OSPF は、IPsec から CRYPTO_SS_SOCKET_UP メッセージを受信していません。
- CLOSING：インターフェイスのセキュア ソケットはクローズされています。インターフェイスに対して新しいソケットがオープンされることがあります。この場合、現在のセキュア ソケットは DOWN ステートに移行します。オープンされない場合、インターフェイスは UNCONFIGURED となります。
- UNCONFIGURED：インターフェイス上に認証は設定されていません。

OSPF は、DOWN ステートの間、パケットの送信や受け入れを行いません。

IPsec の詳細については、「*IPv6 セキュリティへの IPsec の実装*」を参照してください。

OSPF for IPv6 の仮想リンク

仮想リンクごとに、マスター セキュリティ情報データブロックが作成されます。各インターフェイスでセキュア ソケットをオープンする必要があるため、トランジット エリア内のインターフェイスごとに、対応するセキュリティ情報データブロックが存在することになります。セキュア ソケット ステートは、インターフェイスのセキュリティ情報データブロック内に保持されます。マスター セキュリティ情報データブロック内のステート フィールドは、仮想リンクに対してオープンされたすべてのセキュア ソケットのステータスを反映しています。すべてのセキュア ソケットが UP の場合、仮想リンクのセキュリティ ステートは UP に設定されます。

IPsec が設定された仮想リンク上を送信されるパケットは、事前に決定された送信元アドレスと宛先アドレスを使用する必要があります。エリアのルータのエリア内プレフィクス LSA で見つかった最初のローカル エリア アドレスが、送信元アドレスとして使用されます。この送信元アドレスはエリア データ構造で保存され、セキュア ソケットがオープンされ、パケットが仮想リンク上を送信されるときに使用されます。送信元アドレスが選択されるまで、仮想リンクはポイントツーポイント ステートに移行しません。また、送信元アドレスまたは宛先アドレスが変更された場合は、以前のセキュア ソケットをクローズして、新しいセキュア ソケットをオープンする必要があります。

OSPF コスト計算

コスト コンポーネントは急速に変更される可能性があるため、変更量を抑えてネットワーク全体の変動を小さくする必要があることがあります。S2、S3、および S4 の推奨値は、ネットワークの変更率を抑えるためのネットワーク シミュレーションに基づいています。S1 の推奨値は 0 です。この変数がルート コスト計算から除外されるようにするためです。

全体のリンク コストは、図 1 に示した式を使用して計算されます。

図 1　　全体のリンク コストの式

$$\text{LinkCost} = \text{OC} + \text{①}\,\text{BW}\left(\frac{\text{Throughput\_weight}}{100}\right) + \text{②}\,\text{Resources}\left(\frac{\text{Resources\_weight}}{100}\right) + \text{③}\,\text{Latency}\left(\frac{\text{Latency\_weight}}{100}\right) + \text{④}\,\text{L2\_factor}\left(\frac{\text{L2\_weight}}{100}\right)$$

$$\text{OC} = \left[\frac{(\text{ospf\_reference\_bw})}{(\text{MDR})(1000)}\right] \qquad \text{ospf\_reference\_bw} = 10 \wedge 8$$

$$\text{①}\ \text{BW} = \frac{(65536)\left(100 - \frac{\text{CDR}}{\text{MDR}}(100)\right)}{100}$$

$$\text{②}\ \text{Resources} = \frac{(100 - \text{resources})^3\,(65536)}{1000000}$$

$$\text{③}\ \text{Latency} = \text{latency}$$

$$\text{④}\ \text{L2\_factor} = \frac{(100 - \text{RLQ})(65536)}{100}$$

231048

表 1 に、OSPF コスト計算で使用される記号を定義します。

表 1　　OSPF コスト計算の定義

コスト コンポーネント	コンポーネント定義
OC	デフォルトの OSPF コスト。reference_bw / (MDR*1000)（reference_bw=10^8）を使用して、参照帯域幅から計算されます。
A ～ D	ラジオ固有のデータベースのさまざまな式。0 ～ 64,000 の範囲の結果が生成されます。
A	CDR 関連および MDR 関連の式： (2^16 * (100 – (CDR * 100 / MDR)))/100
B	リソース関連の式： ((100 – RESOURCES)^3 * 2^16 / 10^6)
C	ラジオにより報告される遅延。報告される時点で、すでに 0 ～ 64K の範囲です（LATENCY）。
D	RLF 関連の式： ((100 – RLF) * 2^16)/100
S1 ～ S4	Command-Line Interface（CLI; コマンドライン インターフェイス）からのスカラ重み付け係数入力。これらのスカラは、A ～ D により計算された値を縮小します。 0 の値は、あるコンポーネントに対して 0 ～ 64,000 の全範囲をディセーブルにし、100 の値はイネーブルにします。

各ネットワークに固有の特性があり、実際のネットワーク パフォーマンスを最適化するために異なる設定が必要となることもあるため、これらの推奨値は、OSPFv3 ネットワークを最適化するための開始点として捉えてください。表 2 に、OSPF コスト メトリックの推奨値設定を示します。

表 2　　OSPF コスト メトリックの推奨値

設定	メトリックの説明	デフォルト値	推奨値
S1	ipv6 ospf dynamic weight throughout	100	0
S2	ipv6 ospf dynamic weight resources	100	29
S3	ipv6 ospf dynamic weight latency	100	29
S4	ipv6 ospf dynamic weight L2 factor	100	29

次のリストで示すように、この式を使用してデフォルトのパス コストが計算されています。これらの値が使用しているネットワークに適していない場合は、独自のパス コストの計算方法を使用できます。

- 56-kbps シリアル リンク：デフォルトのコストは 1785 です。
- 64-kbps シリアル リンク：デフォルトのコストは 1562 です。
- T1（1.544-Mbps シリアル リンク）：デフォルトのコストは 64 です。
- E1（2.048-Mbps シリアル リンク）：デフォルトのコストは 48 です。
- 4-Mbps トークン リング：デフォルトのコストは 25 です。
- イーサネット：デフォルトのコストは 10 です。
- 16-Mbps トークン リング：デフォルトのコストは 6 です。
- FDDI：デフォルトのコストは 1 です。

- X25：デフォルトのコストは 5208 です。
- 非同期：デフォルトのコストは 10,000 です。
- ATM：デフォルトのコストは 1 です。

これらの設定を示すために、ここでは、VMI インターフェイスに対して OSPF コスト メトリックを定義する例を示します。

```
interface vmi1
 ipv6 ospf cost dynamic weight throughput 0
 ipv6 ospf cost dynamic weight resources 29
 ipv6 ospf cost dynamic weight latency 29
 ipv6 ospf cost dynamic weight L2-factor 29
```

OSPFv3 グレースフル リスタート

OSPFv3 でグレースフル リスタート機能を使用すると、OSPFv3 ルーティング プロトコル情報の復元中も、既知のルートを使用してノンストップ データ フォワーディングを実行できます。ルータは、再起動モード（グレースフルリスタート対応ルータなど）か、ヘルパー モード（グレースフル リスタート認識ルータなど）のいずれかで、グレースフル リスタートに参加できます。

グレースフル リスタート機能を実行するには、ルータが High Availability（HA; ハイ アベイラビリティ）Stateful Switchover（SSO; ステートフル スイッチオーバー）モード（つまり、デュアル RP）になっている必要があります。グレースフル リスタート機能を備えたルータは、次の場合に、グレースフル リスタート機能を実行します。

- Route Processor（RP; ルート プロセッサ）障害が発生し、スタンバイ RP へのスイッチオーバーが行われた場合
- スタンバイ RP への計画的な RP スイッチオーバーが行われた場合

グレースフル リスタート機能を使用するには、ネイバー ルータがグレースフルリスタート認識ルータであることが必要です。

SSO および Nonstop Forwarding（NSF; ノンストップ フォワーディング）の詳細については、「*Stateful Switchover*」および「*Cisco Nonstop Forwarding*」を参照してください。

BFD での OSPFv3 のサポート

Bidirectional Forwarding Detection（BFD; 双方向フォワーディング検出）では、OSPFv3 をサポートしています。OSPFv3 に対する BFD の設定方法については、『*Implementing Bidirectional Forwarding Detection for IPv6*』の章を参照してください。

OSPF for IPv6 の実装方法

ここでは、次の各手順について説明します。

- 「インターフェイスでの OSPF for IPv6 のイネーブル化」（P.11）（必須）
- 「OSPF for IPv6 のエリア範囲の定義」（P.11）（任意）
- 「OSPF for IPv6 での IPsec の設定」（P.12）（任意）
- 「OSPF for IPv6 での NBMA インターフェイスの設定」（P.17）（任意）
- 「OSPF for IPv6 高速コンバージェンスに対する LSA および SPF スロットリングの設定」（P.19）（任意）

- 「OSPFv3 グレースフル リスタートのイネーブル化」（P.21）（任意）
- 「SPF 計算の強制実行」（P.23）（任意）
- 「OSPF for IPv6 の設定および動作の確認」（P.23）（任意）

インターフェイスでの OSPF for IPv6 のイネーブル化

ここでは、OSPF for IPv6 をイネーブルにし、各インターフェイスで OSPF for IPv6 を設定する方法について説明します。デフォルトでは、OSPF for IPv6 ルーティングはディセーブルになっており、インターフェイス上に OSPF for IPv6 は設定されていません。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 ospf** *process-id* **area** *area-id* [**instance** *instance-id*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface ethernet 0/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 ospf** *process-id* **area** *area-id* [**instance** *instance-id*] **例：** `Router(config-if)# ipv6 ospf 1 area 0`	インターフェイスで OSPF for IPv6 をイネーブルにします。

OSPF for IPv6 のエリア範囲の定義

集約されたルートのコストは、集約されるルートの最高コストとなります。たとえば、次のルートが集約されるとします。

```
OI  2001:0DB8:0:7::/64 [110/20]
     via FE80::A8BB:CCFF:FE00:6F00, Ethernet0/0
OI  2001:0DB8:0:8::/64 [110/100]
     via FE80::A8BB:CCFF:FE00:6F00, Ethernet0/0
OI  2001:0DB8:0:9::/64 [110/20]
```

```
     via FE80::A8BB:CCFF:FE00:6F00, Ethernet0/0
```

これらは、次のように 1 つの集約されたルートとなります。

```
OI  2001:0DB8::/48 [110/100]
     via FE80::A8BB:CCFF:FE00:6F00, Ethernet0/0
```

ここでは、OSPF エリアのルートを統合または集約する方法について説明します。

前提条件

OSPF for IPv6 ルーティングがイネーブルになっている必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **area** *area-id* **range** *ipv6-prefix*/*prefix-length* [**advertise** | **not-advertise**] [**cost** *cost*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 router ospf** *process-id* **例：** `Router(config)# ipv6 router ospf 1`	OSPF ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**area** *area-id* **range** *ipv6-prefix*/*prefix-length* [**advertise** | **not-advertise**] [**cost** *cost*] **例：** `Router(config-rtr)# area 1 range 2001:0DB8::/48`	エリア境界でルートを統合および集約します。

OSPF for IPv6 での IPsec の設定

OSPF for IPv6 の設定を完了し、認証について決定したあとは、グループ内の各ルータでセキュリティ ポリシーを定義する必要があります。セキュリティ ポリシーは、キーと SPI の組み合せで構成されます。セキュリティ ポリシーを定義するには、SPI およびキーを定義する必要があります。

認証ポリシーまたは暗号化ポリシーは、インターフェイスで、または OSPF エリアに対して設定できます。セキュリティ ポリシーは、エリアに対して設定した場合、エリア内のすべてのインターフェイスに適用されます。セキュリティを強化する場合は、各インターフェイスで異なるポリシーを使用してください。

認証および暗号化は、仮想リンク上に設定できます。

ここでは、認証および暗号化を、インターフェイスまたは OSPF エリア、および仮想リンク上に設定する方法について説明します。

- 「インターフェイスでの認証の定義」（P.13）
- 「インターフェイスでの暗号化の定義」（P.14）
- 「OSPF エリア内の認証の定義」（P.15）
- 「OSPF エリア内の暗号化の定義」（P.16）
- 「OSPF エリア内の仮想リンクに対する認証および暗号化の定義」（P.16）

インターフェイスでの認証の定義

ここでは、インターフェイスで認証を定義する方法について説明します。

前提条件

インターフェイスで IPsec を設定する前に、そのインターフェイスで OSPF for IPv6 を設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 ospf authentication ipsec spi** *spi* **md5** [*key-encryption-type* {*key* | **null**}]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* **例：** `Router(config)# interface ethernet 0/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 ospf authentication ipsec spi** *spi* **md5** [*key-encryption-type* {*key* | **null**}] **例：** `Router(config-if)# ipv6 ospf authentication ipsec spi 500 md5 1234567890abcdef1234567890abcdef`	インターフェイスに認証タイプを指定します。

インターフェイスでの暗号化の定義

前提条件

インターフェイスで IPsec を設定する前に、そのインターフェイスで OSPF for IPv6 を設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 ospf encryption** {**ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key* | **null**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* **例：** `Router(config)# interface ethernet 0/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 ospf encryption** {**ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key* | **null**} **例：** `Router(config-if) ipv6 ospf encryption ipsec spi 1001 esp null sha1 123456789A123456789B123456789C123456789D`	インターフェイスに暗号化タイプを指定します。

OSPF エリア内の認証の定義

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **area** *area-id* **authentication ipsec spi** *spi* **md5** [*key-encryption-type*] *key*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 router ospf** *process-id* **例：** `Router(config)# ipv6 router ospf 1`	OSPF ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**area** *area-id* **authentication ipsec spi** *spi* **md5** [*key-encryption-type*] *key* **例：** `Router(config-rtr)# area 1 authentication ipsec spi 678 md5 1234567890ABCDEF1234567890ABCDEF`	OSPF エリア内の認証をイネーブルにします。

OSPF エリア内の暗号化の定義

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **area** *area-id* **encryption ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 router ospf** *process-id* **例：** `Router(config)# ipv6 router ospf 1`	OSPF ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**area** *area-id* **encryption ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key* **例：** `Router(config-rtr)# area 1 encryption ipsec spi 500 esp null md5 1aaa2bbb3ccc4ddd5eee6fff7aaa8bbb`	OSPF エリア内の暗号化をイネーブルにします。

OSPF エリア内の仮想リンクに対する認証および暗号化の定義

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **area** *area-id* **virtual-link** *router-id* **authentication ipsec spi** *spi authentication-algorithm* [*key-encryption-type*] *key*
5. **area** *area-id* **virtual-link** *router-id* **encryption ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 router ospf** *process-id* **例：** `Router(config)# ipv6 router ospf 1`	OSPF ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**area** *area-id* **virtual-link** *router-id* **authentication ipsec spi** *spi authentication-algorithm* [*key-encryption-type*] *key* **例：** `Router(config-rtr)# area 1 virtual-link 10.0.0.1 authentication ipsec spi 940 md5 1234567890ABCDEF1234567890ABCDEF`	OSPF エリア内の仮想リンクに対して認証をイネーブルにします。
ステップ 5	**area** *area-id* **virtual-link** *router-id* **encryption ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key* **例：** `Router(config-rtr)# area 1 virtual-link 10.1.0.1 hello-interval 2 dead-interval 10 encryption ipsec spi 3944 esp null sha1 123456789A123456789B123456789C123456789D`	OSPF エリア内の仮想リンクに対して暗号化をイネーブルにします。

OSPF for IPv6 での NBMA インターフェイスの設定

NBMA インターフェイスを使用するようにネットワーク内の OSPF for IPv6 をカスタマイズできます。OSPF for IPv6 は、NBMA インターフェイスを介してネイバーを自動的に検出することはできません。NBMA インターフェイスで、インターフェイス コンフィギュレーション モードを使用して、手動でネイバーを設定する必要があります。ここでは、NBMA インターフェイスの設定方法について説明します。

前提条件

NBMA インターフェイスを設定する前に、次の作業を実行する必要があります。

- ネットワークを NBMA ネットワークとして設定する。
- 各ネイバーを識別する。

制約事項

- NBMA インターフェイスの使用時に、ネイバーを自動的に検出することはできません。NBMA インターフェイスの使用時には、ネイバーを検出するようにルータを手動で設定する必要があります。
- **ipv6 ospf neighbor** コマンドを設定するときに使用する IPv6 アドレスは、ネイバーのリンクローカル アドレスにする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **frame-relay map ipv6** *ipv6-address dlci* [**broadcast**] [**cisco**] [**ietf**] [**payload-compression** {**packet-by-packet** | **frf9 stac** [*hardware-options*] | **data-stream stac** [*hardware-options*]}]
5. **ipv6 ospf neighbor** *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface serial 0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**frame-relay map ipv6** *ipv6-address dlci* [**broadcast**] [**cisco**] [**ietf**] [**payload-compression** {**packet-by-packet** | **frf9 stac** [*hardware-options*] | **data-stream stac** [*hardware-options*]}] **例：** `Router(config-if)#  frame-relay map ipv6 FE80::A8BB:CCFF:FE00:C01 120`	宛先アドレスへの接続に使用する宛先 IPv6 アドレスと Data-Link Connection Identifier（DLCI; データリンク接続識別子）との間のマッピングを定義します。 • この例では、NBMA リンクはフレーム リレーです。他の種類の NBMA リンクに対しては、別のマッピング コマンドを使用します。
ステップ 5	**ipv6 ospf neighbor** *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**] **例：** `Router(config-if) ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01`	OSPF for IPv6 ネイバー ルータを設定します。

OSPF for IPv6 高速コンバージェンスに対する LSA および SPF スロットリングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **timers throttle spf** *spf-start spf-hold spf-max-wait*
5. **timers throttle lsa** *start-interval hold-interval max-interval*
6. **timers lsa arrival** *milliseconds*
7. **timers pacing flood** *milliseconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 router ospf** *process-id* **例：** `Router(config)# ipv6 router ospf 1`	OSPF ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**timers throttle spf** *spf-start spf-hold spf-max-wait* **例：** `Router(config-rtr)# timers throttle spf 200 200 200`	SPF スロットリングをオンにします。
ステップ 5	**timers throttle lsa** *start-interval hold-interval max-interval* **例：** `Router(config-rtr)# timers throttle lsa 300 300 300`	OSPF for IPv6 の LSA 生成に対してレート制限値を設定します。

	コマンドまたはアクション	目的
ステップ 6	**timers lsa arrival** *milliseconds* **例：** `Router(config-rtr)# timers lsa arrival 300`	ソフトウェアが OSPF ネイバーから同じ LSA を受信する最小間隔を設定します。
ステップ 7	**timers pacing flood** *milliseconds* **例：** `Router(config-rtr)# timers pacing flood 30`	LSA フラッド パケット ペーシングを設定します。

LSA および SPF レート制限に対するイベント ロギングのイネーブル化

OSPF for IPv6 イベント ログは、OSPF for IPv6 インスタンスごとに保持されます。ここでは、LSA および SPF レート制限機能に対してイベント ロギングをイネーブルにする方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **event-log** [**size** [*number of events*]] [**one-shot**] [**pause**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 router ospf** *process-id* **例：** `Router(config)# ipv6 router ospf 1`	OSPF ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**event-log** [**size** [*number of events*]] [**one-shot**] [**pause**] **例：** `Router(config-rtr)# event-log size 10000 one-shot`	イベント ロギングをイネーブルにします。

イベント ログの内容のクリア

手順の概要

1. **enable**
2. **clear ipv6 ospf** [*process-id*] **events**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 必要に応じてパスワードを入力します。
ステップ 2	**clear ipv6 ospf** [*process-id*] **events** **例：** `Router# clear ipv6 ospf 1 events`	OSPF ルーティング プロセス ID に基づいて、OSPF for IPv6 イベント ログの内容をクリアします。

OSPFv3 グレースフル リスタートのイネーブル化

グレースフル リスタート機能は、グレースフルリスタート対応ルータおよびグレースフルリスタート認識ルータに対してイネーブルにできます。ここでは、OSPFv3 グレースフル リスタートをイネーブルにする方法について説明します。

- 「グレースフルリスタート対応ルータでの OSPFv3 グレースフル リスタートのイネーブル化」（P.21）
- 「グレースフルリスタート認識ルータでの OSPFv3 グレースフル リスタートのイネーブル化」（P.22）

グレースフルリスタート対応ルータでの OSPFv3 グレースフル リスタートのイネーブル化

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **graceful-restart** [**restart-interval** *interval*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 router ospf** *process-id* **例：** `Router(config)# ipv6 router ospf 1`	OSPF ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**graceful-restart** [**restart-interval** *interval*] **例：** `Router(config-rtr)# graceful-restart`	グレースフルリスタート対応ルータで OSPFv3 グレースフル リスタート機能をイネーブルにします。

グレースフルリスタート認識ルータでの OSPFv3 グレースフル リスタートのイネーブル化

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **graceful-restart helper** {**disable** | **strict-lsa-checking**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 router ospf** *process-id* **例：** `Router(config)# ipv6 router ospf 1`	OSPF ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**graceful-restart helper** {**disable** | **strict-lsa-checking**} **例：** `Router(config-rtr)# graceful-restart helper strict-lsa-checking`	グレースフルリスタート認識ルータで OSPFv3 グレースフル リスタート機能をイネーブルにします。

SPF 計算の強制実行

手順の概要

1. **enable**
2. **clear ipv6 ospf** [*process-id*] {**process** | **force-spf** | **redistribution**}

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**clear ipv6 ospf** [*process-id*] {**process** | **force-spf** | **redistribution**} **例：** `Router# clear ipv6 ospf force-spf`	OSPF ルーティング プロセス ID に基づいて OSPF ステートをクリアし、SPF アルゴリズムを強制的に開始します。

OSPF for IPv6 の設定および動作の確認

手順の概要

1. **enable**
2. **show ipv6 ospf** [*process-id*] [*area-id*] **interface** [*interface-type interface-number*]
3. **show ipv6 ospf** [*process-id*] [*area-id*]
4. **show crypto ipsec policy** [**name** *policy-name*]
5. **show crypto ipsec sa** [**map** *map-name* | **address** | **identity** | **interface** *type number* | **peer** [**vrf** *fvrf-name*] **address** | **vrf** *ivrf-name* | **ipv6** [*interface-type interface-number*]] [**detail**]
6. **show ipv6 ospf** [*process-ID*] **event** [**generic** | **interface** | **lsa** | **neighbor** | **reverse** | **rib** | **spf**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**show ipv6 ospf** [*process-id*] [*area-id*] **interface** [*interface-type interface-number*] **例：** `Router# show ipv6 ospf interface`	OSPF 関連のインターフェイス情報を表示します。
ステップ 3	**show ipv6 ospf** [*process-id*] [*area-id*] **例：** `Router# show ipv6 ospf`	OSPF ルーティング プロセスに関する一般情報を表示します。
ステップ 4	**show crypto ipsec policy** [**name** *policy-name*] **例：** `Router# show crypto ipsec policy`	各 IPsec パラメータのパラメータを表示します。
ステップ 5	**show crypto ipsec sa** [**map** *map-name* | **address** | **identity** | **interface** *type number* | **peer** [**vrf** *fvrf-name*] **address** | **vrf** *ivrf-name* | **ipv6** [*interface-type interface-number*]] [**detail**] **例：** `Router# show crypto ipsec sa ipv6`	現在の Security Association（SA; セキュリティ アソシエーション）によって使用されている設定を表示します。
ステップ 6	**show ipv6 ospf** [*process-ID*] **event** [**generic** | **interface** | **lsa** | **neighbor** | **reverse** | **rib** | **spf**] **例：** `Router# show ipv6 ospf event spf`	OSPF for IPv6 イベントに関する詳細情報を表示します。

例

- 「show ipv6 ospf interface コマンドの出力例」（P.24）
- 「show ipv6 ospf コマンドの出力例」（P.26）
- 「show crypto ipsec policy コマンドの出力例」（P.26）
- 「show crypto ipsec sa ipv6 コマンドの出力例」（P.26）
- 「show ipv6 ospf graceful-restart コマンドの出力例」（P.27）

show ipv6 ospf interface コマンドの出力例

次に、暗号化および認証によって保護された通常のインターフェイスおよび仮想リンクを使用した、**show ipv6 ospf interface** コマンドの出力例を示します。

```
Router# show ipv6 ospf interface

OSPFv3_VL1 is up, line protocol is up
   Interface ID 69
```

```
   Area 0, Process ID 1, Instance ID 0, Router ID 10.0.0.1
   Network Type VIRTUAL_LINK, Cost: 64
   Configured as demand circuit.
   Run as demand circuit.
   DoNotAge LSA allowed.
   NULL encryption SHA-1 auth SPI 3944, secure socket UP (errors: 0)
   Transmit Delay is 1 sec, State POINT_TO_POINT,
   Timer intervals configured, Hello 2, Dead 10, Wait 40, Retransmit 5
     Hello due in 00:00:00
   Index 1/3/5, flood queue length 0
   Next 0x0(0)/0x0(0)/0x0(0)
   Last flood scan length is 1, maximum is 1
   Last flood scan time is 0 msec, maximum is 0 msec
   Neighbor Count is 1, Adjacent neighbor count is 1
     Adjacent with neighbor 10.2.0.1  (Hello suppressed)
   Suppress hello for 1 neighbor(s)
OSPFv3_VL0 is up, line protocol is up
   Interface ID 67
   Area 0, Process ID 1, Instance ID 0, Router ID 10.0.0.1
   Network Type VIRTUAL_LINK, Cost: 128
   Configured as demand circuit.
   Run as demand circuit.
   DoNotAge LSA allowed.
   MD5 authentication SPI 940, secure socket UP (errors: 0)
   Transmit Delay is 1 sec, State POINT_TO_POINT,
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
     Hello due in 00:00:09
   Index 1/2/4, flood queue length 0
   Next 0x0(0)/0x0(0)/0x0(0)
   Last flood scan length is 1, maximum is 10
   Last flood scan time is 0 msec, maximum is 0 msec
   Neighbor Count is 1, Adjacent neighbor count is 1
     Adjacent with neighbor 10.1.0.1  (Hello suppressed)
   Suppress hello for 1 neighbor(s)
Ethernet1/0 is up, line protocol is up
   Link Local Address FE80::A8BB:CCFF:FE00:6601, Interface ID 6
   Area 0, Process ID 1, Instance ID 0, Router ID 10.0.0.1
   Network Type BROADCAST, Cost: 10
   Transmit Delay is 1 sec, State DR, Priority 1
   Designated Router (ID) 10.0.0.1, local address FE80::A8BB:CCFF:FE00:6601
   No backup designated router on this network
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
     Hello due in 00:00:09
   Index 1/1/1, flood queue length 0
   Next 0x0(0)/0x0(0)/0x0(0)
   Last flood scan length is 0, maximum is 0
   Last flood scan time is 0 msec, maximum is 0 msec
   Neighbor Count is 0, Adjacent neighbor count is 0
   Suppress hello for 0 neighbor(s)
Serial12/0 is up, line protocol is up
   Link Local Address FE80::A8BB:CCFF:FE00:6600, Interface ID 50
   Area 1, Process ID 1, Instance ID 0, Router ID 10.0.0.1
   Network Type POINT_TO_POINT, Cost: 64
   AES-CBC encryption SHA-1 auth SPI 2503, secure socket UP (errors: 0)
   authentication NULL
   Transmit Delay is 1 sec, State POINT_TO_POINT,
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
     Hello due in 00:00:09
   Index 1/2/3, flood queue length 0
   Next 0x0(0)/0x0(0)/0x0(0)
   Last flood scan length is 1, maximum is 5
   Last flood scan time is 0 msec, maximum is 0 msec
   Neighbor Count is 1, Adjacent neighbor count is 1
     Adjacent with neighbor 10.2.0.1
```

```
   Suppress hello for 0 neighbor(s)
Serial11/0 is up, line protocol is up
   Link Local Address FE80::A8BB:CCFF:FE00:6600, Interface ID 46
   Area 1, Process ID 1, Instance ID 0, Router ID 10.0.0.1
   Network Type POINT_TO_POINT, Cost: 64
   MD5 authentication (Area) SPI 500, secure socket UP (errors: 0)
   Transmit Delay is 1 sec, State POINT_TO_POINT,
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
     Hello due in 00:00:09
   Index 1/1/2, flood queue length 0
   Next 0x0(0)/0x0(0)/0x0(0)
   Last flood scan length is 1, maximum is 5
   Last flood scan time is 0 msec, maximum is 0 msec
   Neighbor Count is 1, Adjacent neighbor count is 1
     Adjacent with neighbor 10.0.0.1
   Suppress hello for 0 neighbor(s)
```

show ipv6 ospf コマンドの出力例

次に、**show ipv6 ospf** コマンドの出力例を示します。

```
Router# show ipv6 ospf

Routing Process "ospfv3 1" with ID 172.16.3.3
 It is an autonomous system boundary router
 Redistributing External Routes from,
    static
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 1. Checksum Sum 0x218D
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
    Area 1
        Number of interfaces in this area is 2
        SPF algorithm executed 9 times
        Number of LSA 15. Checksum Sum 0x67581
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

show crypto ipsec policy コマンドの出力例

次に、**show crypto ipsec policy** コマンドの出力例を示します。

```
Router# show crypto ipsec policy

Crypto IPsec client security policy data

Policy name:     OSPFv3-1-1000
Policy refcount: 1
Inbound  AH SPI: 1000 (0x3E8)
Outbound AH SPI: 1000 (0x3E8)
Inbound  AH Key: 1234567890ABCDEF1234567890ABCDEF
Outbound AH Key: 1234567890ABCDEF1234567890ABCDEF
Transform set:   ah-md5-hmac
```

show crypto ipsec sa ipv6 コマンドの出力例

次に、**show crypto ipsec sa ipv6** コマンドの出力例を示します。

```
Router# show crypto ipsec sa ipv6
```

```
IPv6 IPsec SA info for interface Ethernet0/0

   protected policy name:OSPFv3-1-1000
   IPsec created ACL name:Ethernet0/0-ipsecv6-ACL

   local  ident (addr/prefixlen/proto/port):(FE80::/10/89/0)
   remote ident (addr/prefixlen/proto/port):(::/0/89/0)
   current_peer:::
     PERMIT, flags={origin_is_acl,}
    #pkts encaps:21, #pkts encrypt:0, #pkts digest:21
    #pkts decaps:20, #pkts decrypt:0, #pkts verify:20
    #pkts compressed:0, #pkts decompressed:0
    #pkts not compressed:0, #pkts compr. failed:0
    #pkts not decompressed:0, #pkts decompress failed:0
    #send errors 0, #recv errors 0

    local crypto endpt. ::, remote crypto endpt. ::
    path mtu 1500, media mtu 1500
    current outbound spi:0x3E8(1000)

     inbound ESP SAs:

     inbound AH SAs:
      spi:0x3E8(1000)
        transform:ah-md5-hmac ,
        in use settings ={Transport, }
        slot:0, conn_id:2000, flow_id:1, crypto map:N/R
        no sa timing (manual-keyed)
        replay detection support:N

     inbound PCP SAs:

     outbound ESP SAs:

     outbound AH SAs:
      spi:0x3E8(1000)
        transform:ah-md5-hmac ,
        in use settings ={Transport, }
        slot:0, conn_id:2001, flow_id:2, crypto map:N/R
        no sa timing (manual-keyed)
        replay detection support:N

     outbound PCP SAs:
```

show ipv6 ospf graceful-restart コマンドの出力例

次に、**show ipv6 ospf graceful-restart** コマンドの出力例を示します。

```
Router# show ipv6 ospf graceful-restart

Routing Process "ospf 1"
 Graceful Restart enabled
    restart-interval limit: 120 sec, last restart 00:00:15 ago (took 36 secs)
  Graceful Restart helper support enabled
  Router status : Active
  Router is running in SSO mode
  OSPF restart state : NO_RESTART
  Router ID 10.1.1.1, checkpoint Router ID 10.0.0.0
```

OSPF for IPv6 を実装するための設定例

例：インターフェイス設定での OSPF for IPv6 のイネーブル化

次に、OSPF ルーティング プロセス 109 をインターフェイス上で動作するように設定し、エリア 1 に配置する例を示します。

```
ipv6 ospf 109 area 1
```

例：OSPF for IPv6 のエリア範囲の定義

次に、OSPF for IPv6 のエリア範囲を指定する例を示します。

```
interface Ethernet7/0
 ipv6 address 2001:0DB8:0:7::/64 eui-64
 ipv6 enable
 ipv6 ospf 1 area 1
!
interface Ethernet8/0
 ipv6 address 2001:0DB8:0:8::/64 eui-64
 ipv6 enable
 ipv6 ospf 1 area 1
!
interface Ethernet9/0
 ipv6 address 2001:0DB8:0:9::/64 eui-64
 ipv6 enable
 ipv6 ospf 1 area 1
!
ipv6 router ospf 1
 router-id 10.11.11.1
 area 1 range 2001:0DB8::/48
```

例：インターフェイスでの認証の定義

次に、イーサネット 0/0 インターフェイスで認証を定義する例を示します。

```
interface Ethernet0/0
 ipv6 enable
 ipv6 ospf 1 area 0
 ipv6 ospf authentication ipsec spi 500 md5 1234567890ABCDEF1234567890ABCDEF

interface Ethernet0/0
 ipv6 enable
 ipv6 ospf authentication null
 ipv6 ospf 1 area 0
```

例：OSPF エリア内の認証の定義

次に、OSPF エリア 0 で認証を定義する例を示します。

```
ipv6 router ospf 1
 router-id 10.11.11.1
 area 0 authentication ipsec spi 1000 md5 1234567890ABCDEF1234567890ABCDEF
```

例：NBMA インターフェイスの設定

次に、Ipv6 アドレスが FE80::A8BB:CCFF:FE00:C01 の OSPF ネイバー ルータを設定する例を示します。

```
interface serial 0
 ipv6 enable
 ipv6 ospf 1 area 0
 encapsulation frame-relay
 frame-relay map ipv6 FE80::A8BB:CCFF:FE00:C01 120
 ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C0
```

例：OSPF for IPv6 高速コンバージェンスに対する LSA および SPF スロットリングの設定

次に、SPF および LSA スロットル タイマーの設定値を表示する例を示します。

```
Router# show ipv6 ospf

 Routing Process "ospfv3 1" with ID 10.9.4.1
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 It is an autonomous system boundary router
 Redistributing External Routes from,
    ospf 2
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
```

例：SPF 設定の強制実行

次に、SPF をトリガーして、SPF を再実行し、ルーティング テーブルに値を再入力する例を示します。

```
clear ipv6 ospf force-spf
```

その他の関連資料

関連資料

関連項目	参照先
OSPF でのルータ ID の設定	• 『*Cisco IOS IP Routing Protocols Configuration Guide*』の「Configuring OSPF」 • 『*Cisco IOS IP Routing Protocols Command Reference*』
OSPF for IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
IPv6 のサポート機能リスト	『*Cisco IOS IPv6 Configuration Guide*』の「Start Here: Cisco IOS Software Release Specifics for IPv6 Features」
基本的な IPv6 接続の実装	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing IPv6 Addressing and Basic Connectivity」
IPsec for IPv6	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing IPsec for IPv6 Security」
OSPFv3 に対する BFD サポート	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing Bidirectional Forwarding Detection for IPv6」
ステートフル スイッチオーバー	『*Cisco IOS High Availability Configuration Guide*』の「Stateful Switchover」
Cisco ノンストップ フォワーディング	『*Cisco* IOS High Availability Configuration Guide』の「Cisco Nonstop Forwarding」

規格

規格	タイトル
この機能によってサポートされる新しい規格または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
• CISCO-IETF-IP-FORWARD-MIB • CISCO-IETF-IP-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2401	『*Security Architecture for the Internet Protocol*』
RFC 2402	『*IP Authentication Header*』
RFC 2406	『*IP Encapsulating Security Payload (ESP)*』
RFC 2740	『*OSPF for IPv6*』
RFC 4552	『*Authentication/Confidentiality for OSPFv3*』
RFC 5187	『*OSPFv3 Graceful Restart*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

OSPF for IPv6 の実装の機能情報

表 3 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どのソフトウェア イメージが特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 3 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 3　OSPF for IPv6 の実装の機能情報

機能名	リリース	機能情報
IPv6 ルーティング：OSPF for IPv6（OSPFv3）	12.0(24)S 12.2(18)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(15)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)M 15.0(1)S	OSPF バージョン 3 for IPv6 では、OSPF バージョン 2 が拡張され、IPv6 ルーティング プレフィクスと、より大きなサイズの IPv6 アドレスに対するサポートが提供されています。 このマニュアルでは、この機能について説明しています。
IPv6 ルーティング：OSPF for IPv6 での LSA タイプ	12.0(24)S 12.2(18)S 12.2(28)SB 12.2(15)T 12.3 12.3(2)T 12.4 12.4(2)T	ルータの LSA データの集まりは、リンクステート データベースに格納されます。ダイクストラ アルゴリズムが採用されている場合、データベースの内容に基づいて OSPF ルーティング テーブルが作成されます。 この機能に関する詳細については、次の各項を参照してください。 • 「OSPF for IPv6 の機能」（P.3） • 「IPv6 の LSA タイプ」（P.4）

表 3　OSPF for IPv6 の実装の機能情報 （続き）

機能名	リリース	機能情報
IPv6 ルーティング：高速コンバージェンス - LSA および SPF スロットリング	12.2(33)SB 12.2(33)SRC 12.2(33)XNE 15.0(1)M	OSPF for IPv6 の LSA および SPF スロットリング機能は、ネットワークが不安定な間、OSPF でのリンクステート アドバタイズメント アップデートを低速化するためのダイナミック メカニズムを提供します。 この機能に関する詳細については、次の各項を参照してください。 • 「高速コンバージェンス - LSA および SPF スロットリング」（P.6） • 「OSPF for IPv6 高速コンバージェンスに対する LSA および SPF スロットリングの設定」（P.19） • 「LSA および SPF レート制限に対するイベント ロギングのイネーブル化」（P.20） • 「イベント ログの内容のクリア」（P.21） • 「例：OSPF for IPv6 高速コンバージェンスに対する LSA および SPF スロットリングの設定」（P.29）
IPv6 ルーティング：OSPF for IPv6 での NBMA インターフェイス	12.0(24)S 12.2(18)S 12.2(28)SB 12.2(15)T 12.3 12.3(2)T 12.4 12.4(2)T	NBMA ネットワークでは、DR またはバックアップ DR が LSA フラッディングを実行します。 この機能に関する詳細については、次の各項を参照してください。 • 「OSPF for IPv6 での NBMA」（P.5） • 「OSPF for IPv6 での NBMA インターフェイスの設定」（P.17）
IPv6 ルーティング：OSPF for IPv6 での SPF の強制実行	12.0(24)S 12.2(18)S 12.2(28)SB 12.2(15)T 12.3 12.3(2)T 12.4 12.4(2)T	この機能により、OSPF データベースのクリアおよび再入力が可能になります。そのあとで、SPF アルゴリズムが実行されます。 この機能に関する詳細については、次の各項を参照してください。 • 「OSPF for IPv6 での SPF の強制実行」（P.5） • 「OSPFv3 グレースフル リスタートのイネーブル化」（P.21）
IPv6 ルーティング：OSPF for IPv6 でのロード バランシング	12.0(24)S 12.2(18)S 12.2(28)SB 12.2(15)T 12.3 12.3(2)T 12.4 12.4(2)T	OSPF for IPv6 では、自動的にロード バランシングが実行されます。 この機能に関する詳細については、次の項を参照してください。 • 「OSPF for IPv6 でのロード バランシング」（P.6）

表 3　OSPF for IPv6 の実装の機能情報 （続き）

機能名	リリース	機能情報
IPv6 ルーティング：IPsec を使用した OSPF for IPv6 の認証サポート	12.3(4)T 12.4 12.4(2)T	OSPF for IPv6 では、IPsec セキュア ソケット API を使用して、OSPF for IPv6 パケットに認証を追加しています。 この機能に関する詳細については、次の各項を参照してください。 • 「IPsec を使用した OSPF for IPv6 認証サポート」（P.7） • 「OSPF for IPv6 での IPsec の設定」（P.12） • 「インターフェイスでの認証の定義」（P.13） • 「OSPF エリア内の認証の定義」（P.15）
IPv6 ルーティング：OSPF IPv6（OSPFv3）IPsec ESP 暗号化および認証	12.4(9)T	IPv6 ESP 拡張ヘッダーを使用すると、OSPF for IPv6 に認証および機密性を提供できます。 この機能に関する詳細については、次の各項を参照してください。 • 「OSPF for IPv6 の実装の制約事項」（P.2） • 「IPsec を使用した OSPF for IPv6 認証サポート」（P.7） • 「インターフェイスでの暗号化の定義」（P.14） • 「OSPF エリア内の暗号化の定義」（P.16） • 「OSPF エリア内の仮想リンクに対する認証および暗号化の定義」（P.16）
OSPFv3 ダイナミック インターフェイス コスト サポート	12.4(15)T	OSPFv3 ダイナミック インターフェイス コスト サポートでは、OSPF for IPv6 コスト メトリックを拡張して、Mobile Ad Hoc Networking のサポートを提供しています。 この機能に関する詳細については、次の項を参照してください。 • 「OSPF コスト計算」（P.8）
OSPFv3 グレースフル リスタート	12.2(33)SRE 12.2(33)XNE 15.0(1)M	OSPFv3 でグレースフル リスタート機能を使用すると、OSPFv3 ルーティング プロトコル情報の復元中も、既知のルートを使用してノンストップ データ フォワーディングを実行できます。 この機能に関する詳細については、次の各項を参照してください。 • 「OSPFv3 グレースフル リスタート」（P.10） • 「OSPFv3 グレースフル リスタートのイネーブル化」（P.21）
OSPFv3 for BFD	12.2(33)SRE 15.0(1)S 15.1(2)T	BFD は、ダイナミック ルーティング プロトコル OSPF for IPv6（OSPFv3）をサポートしています。 この機能に関する詳細については、次の項を参照してください。 • 「BFD での OSPFv3 のサポート」（P.10）

IPv6 over MPLS の実装

Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）は、多くのサービス プロバイダーによって、その IPv4 ネットワークに展開されています。サービス プロバイダーは、IPv6 サービスをカスタマーに提供しようと考えていますが、既存の IPv4 インフラストラクチャを変更するのは非常にコストがかかり、IPv6 トラフィックが少量であることを考えると、費用対効果は妥当なものとはなりません。既存の IPv4 MPLS インフラストラクチャを活用し、ネットワーク バックボーンに変更を加えることなく IPv6 サービスを追加するために、複数の統合シナリオが開発されています。このマニュアルでは、IPv6 over MPLS を実装する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「IPv6 over MPLS の実装の機能情報」（P.19）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

IPv6 over MPLS の実装の前提条件

- この章では、IPv4 に精通していることを前提としています。IPv4 の設定およびコマンド リファレンス情報については、「関連資料」の関連資料を参照してください。
- MPLS を介した IPv6 プロバイダー エッジ ルータ（6PE）機能を実装する前に、MPLS がコア IPv4 ネットワーク上で実行されている必要があります。Cisco ルータが使用されている場合は、シスコ エクスプレス フォワーディングまたは分散型シスコ エクスプレス フォワーディングが、IPv4 プロトコルと IPv6 プロトコルの両方でイネーブルになっている必要があります。この章では、MPLS に精通していることを前提としています。

IPv6 over MPLS の実装に関する情報

IPv6 over MPLS を設定するには、次の概念を理解する必要があります。

- 「IPv6 over MPLS バックボーンの展開の利点」（P.2）
- 「回線トランスポートを介した IPv6 over MPLS」（P.2）
- 「カスタマー エッジ ルータでトンネルを使用する IPv6」（P.3）
- 「IPv6 プロバイダー エッジ ルータ（6PE）」（P.4）

IPv6 over MPLS バックボーンの展開の利点

IPv6 over MPLS バックボーンを使用すると、孤立した複数の IPv6 ドメインが、MPLS IPv4 コア ネットワークを介して互いに通信できます。この実装では、転送が IP ヘッダー自体ではなくラベルに基づいて行われるため、バックボーン インフラストラクチャのアップグレードは少量で済み、コア ルータの再設定は必要ないため、非常にコスト効率の高い IPv6 の展開計画が提供されます。

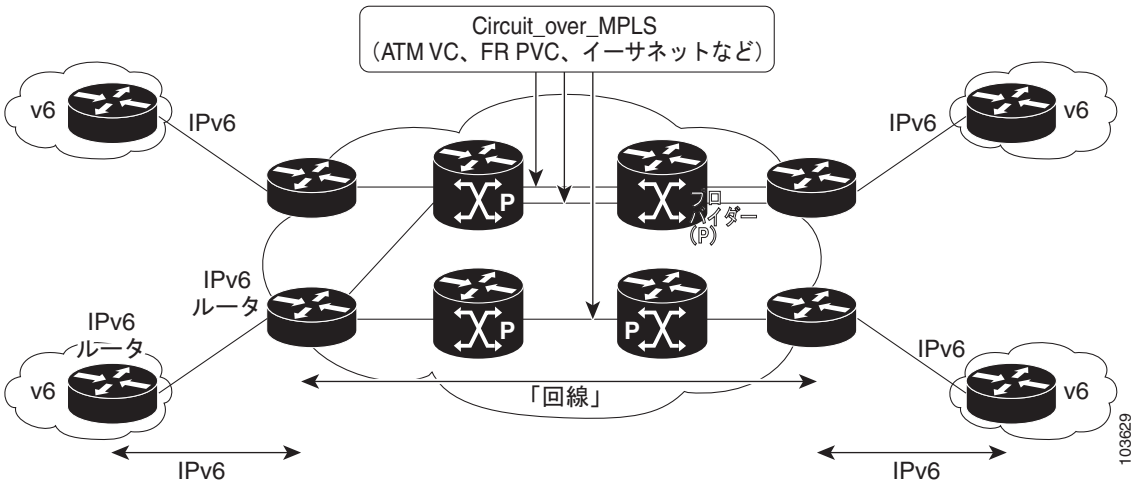
また、MPLS 環境で本来提供されている Virtual Private Network（VPN; バーチャル プライベート ネットワーク）サービスおよび MPLS Traffic Engineering（MPLS TE; MPLS トラフィック エンジニアリング）サービスを使用して、IPv4 VPN および MPLS-TE をサポートするインフラストラクチャを介して IPv6 ネットワークを IPv4 VPN やエクストラネットに組み込むことができます。

回線トランスポートを介した IPv6 over MPLS

いずれの回線トランスポートを IPv6 over MPLS ネットワークの展開に使用しても、MPLS の動作またはインフラストラクチャに影響はなく、コア ルータまたはプロバイダー エッジ ルータの設定を変更する必要もありません。リモート IPv6 ドメイン間の通信では、専用リンクを介してネイティブ IPv6 プロトコルを実行します。この場合、基礎となるメカニズムは IPv6 に対して完全に透過的です。IPv6 トラフィックは、ATM OC-3 またはイーサネット インターフェイスを介してそれぞれ接続されているルータで Any Transport over MPLS（MPLS/AToM）または Ethernet over MPLS（EoMPLS）機能を使用してトンネル化されます。

図 1 に、任意の回線トランスポートを介した IPv6 over MPLS の設定を示します。

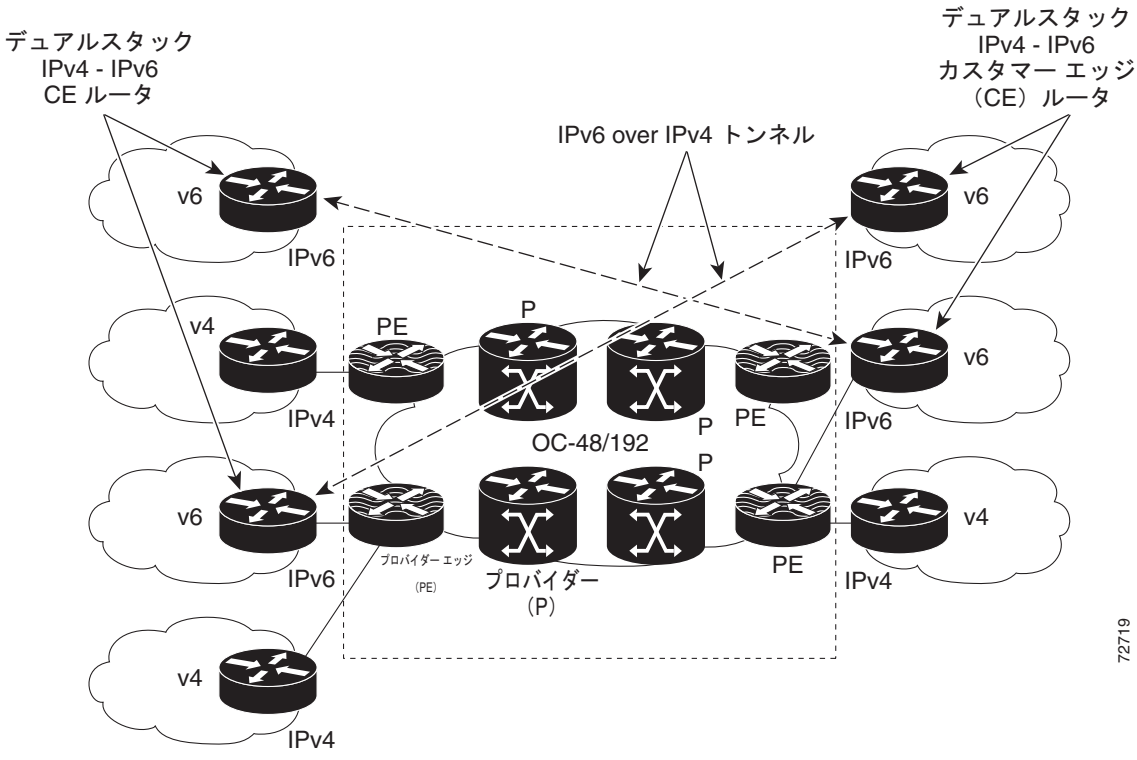
図 1　回線トランスポートを介した IPv6 over MPLS



カスタマー エッジ ルータでトンネルを使用する IPv6

Customer Edge（CE; カスタマー エッジ）ルータでのトンネルの使用が、IPv6 over MPLS ネットワークを最も簡単に展開できる方法です。この方法では、MPLS の動作およびインフラストラクチャには影響を与えず、コア ルータやプロバイダー エッジ ルータの設定を変更する必要もありません。リモート IPv6 ドメイン間の通信では、標準のトンネリング メカニズムが使用され、デュアル IPv4 および IPv6 プロトコル スタックを実行するように CE ルータを設定する必要があります。図 2 に、CE ルータでトンネルを使用する設定を示します。

図 2　CE ルータでトンネルを使用する IPv6



手動で設定されたトンネル、自動トンネル、および 6to4 トンネルに関する設定情報については、「*Implementing Tunneling for IPv6*」を参照してください。

トンネルを使用する場合、CE ルータでトンネルのメッシュを手動で設定するという制限があるため、大規模ネットワークではスケーリング上の問題となります。

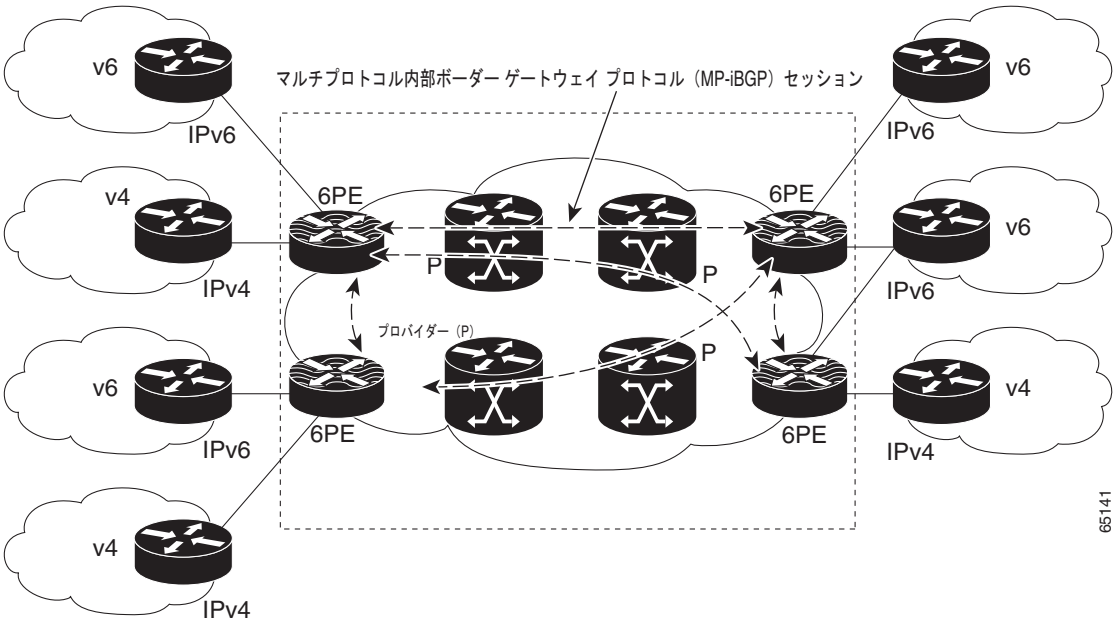
IPv6 プロバイダー エッジ ルータ（6PE）

MPLS を介した IPv6 プロバイダー エッジ ルータのシスコ実装は 6PE と呼ばれ、これにより、IPv6 サイトは、MPLS Label Switched Path（LSP; ラベル スイッチド パス）を使用して MPLS IPv4 コア ネットワークを介して互いに通信できます。この機能は、Provider Edge（PE; プロバイダー エッジ）ルータ上の IPv4 ネットワーク設定のマルチプロトコル Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）拡張に依存して、IPv6 到達可能性情報、およびアドバタイズされる各 IPv6 アドレス プレフィクスに関する MPLS ラベルを交換します。エッジ ルータは、IPv4 と IPv6 の両方を実行するデュアル スタックとして設定され、IPv4 マッピング IPv6 アドレスを使用して IPv6 プレフィクスの到達可能性情報を交換します。

IPv6 トラフィックの透過性をすべてのコア ルータに対して維持するために、ラベルの階層が 6PE 出力ルータでインポーズされています。最上位ラベルは、IPv4 MPLS コア ネットワーク内での接続を提供し、Label Distribution Protocol（LDP; ラベル配布プロトコル）、Tag Distribution Protocol（TDP; タグ配布プロトコル）、または Resource Reservation Protocol（RSVP; リソース予約プロトコル）によってラベルが配布されます。TDP と LDP の両方をラベル配布に使用できますが、RSVP は、MPLS-TE ラベル交換のコンテキストでだけ使用されます。宛先の IPv6 プレフィクスに自動的に割り当てられる一番下のラベルは、マルチプロトコル BGP によって配布され、各 6PE 出力ルータで IPv6 転送のために使用されます。

図 3 では、6PE ルータが IPv4 と IPv6 の両方のトラフィックをルーティングできるデュアル スタック ルータとして設定されています。各 6PE ルータは、LDP、TDP、または RSVP（トラフィック エンジニアリングが設定されている場合）を実行して IPv4 ラベルをバインドするように設定されています。6PE ルータでは、マルチプロトコル BGP を使用して、MPLS ドメイン内の他の 6PE デバイスとの間で到着可能性情報を交換し、IPv6 集約ラベルを配布します。MPLS ドメイン内のすべての 6PE ルータとコア ルータ（図 3 の P ルータ）は、Open Shortest Path First（OSPF）や統合 Intermediate System-to-Intermediate System（IS-IS）などの一般的な IPv4 Interior Gateway Protocol（IGP; 内部ゲートウェイ プロトコル）を共有します。

図 3　6PE ルータ トポロジ



CE ルータに接続している 6PE ルータ上のインターフェイスは、カスタマーの要件に基づいて IPv6 トラフィック、IPv4 トラフィック、または両方のタイプのトラフィックを転送するように設定できます。6PE ルータは、MPLS クラウドを介して 6PE ピアから学習した IPv6 到達可能性情報をアドバタイズします。サービス プロバイダーは、6PE インフラストラクチャを介して、登録済み IPv6 プレフィクスから IPv6 プレフィクスを委任できます。それ以外の場合は、CE ルータに対する影響はありません。

ネットワークのコア内にある P ルータは、P ルータ自身が IPv6 パケットをスイッチングしていることを認識しません。コア ルータは、MPLS クラウド内の内部到達可能性情報を確立するために MPLS および PE ルータと同じ IPv4 IGP をサポートするように設定されています。コア ルータでは、IPv4 ラベルをバインドするために、LDP、TDP、または RSVP も使用されています。Cisco 6PE 機能の実装による MPLS コア デバイスへの影響はありません。

MPLS ネットワークでは、IPv6 トラフィックがラベル スイッチングを使用して転送され、IPv6 トラフィックを MPLS ネットワークのコアに対して透過的にします。IPv6 over IPv4 トンネルまたはレイヤ 2 カプセル化の手法は必要ありません。

6PE マルチパス

IPv6 の内部および外部 Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）マルチパスによって、IPv6 ルータは、複数のパス（同じネイバー Autonomous System（AS; 自律システム）やサブ AS、または同じメトリックなど）間のロード バランシングを行って、宛先に到達できます。6PE マルチパス機能では、Multiprotocol internal BGP（MP-iBGP; マルチプロトコル内部 BGP）を使用して、MPLS IPv4 コア ネットワークを介して IPv6 ルートを配布し、MPLS ラベルを各ルートに付加します。

MP-iBGP マルチパスが 6PE ルータでイネーブルになっていると、MPLS 情報が使用できる場合は、MPLS 情報（ラベル スタック）を使用して、ラベルの付いたすべてのパスが、転送テーブルにインストールされます。この機能によって、6PE はロード バランシングを実行できます。

IPv6 over MPLS の実装方法

ここでは、IPv6 over MPLS を設定する方法について説明します。

回線トランスポートを介した IPv6 over MPLS の展開

回線トランスポートを介した IPv6 over MPLS を展開するには、IPv6 ルータが IPv6 接続用に設定されている必要があります。基本的な IPv6 設定の詳細については、「*Implementing IPv6 Addressing and Basic Connectivity*」を参照してください。MPLS ルータの設定では、AToM 設定または EoMPLS 設定が必要です。

IPv6 プロバイダー エッジ ルータ（6PE）の展開

プロバイダー エッジ ルータ上に IPv6 を実装するには、2 つの作業を実行する必要があります。最初の作業では、ローカルに生成されたパケットが送信元 IPv6 アドレスを取得する元となるインターフェイスを指定します。2 番めの作業では、集約ラベルをバインドおよびアドバタイズします。

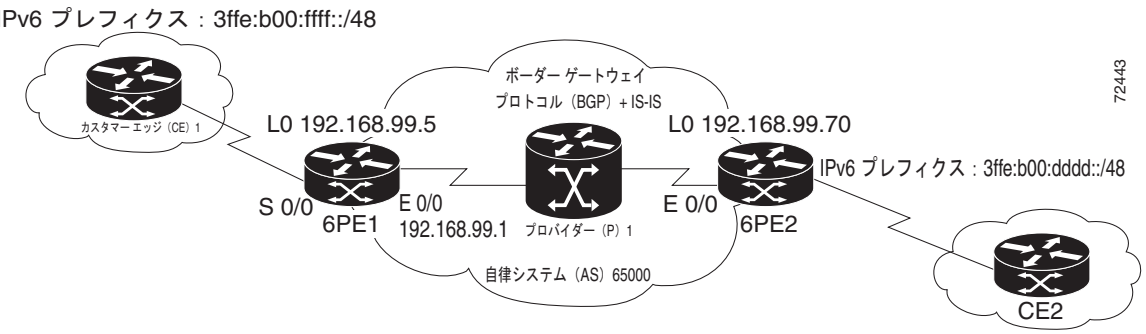
各 6PE ルータ（図 4 の 6PE1 と 6PE2）は、IPv4 ルーティングおよびシスコ エクスプレス フォワーディングを実行していると想定しています。

6PE ネットワーク設定

図 4 に示すネットワークを使用する 2 つの設定作業は、6PE 機能をイネーブルにするために、6PE1 ルータでは必須です。

カスタマー エッジ ルータ（図 4 の CE1）は、その IPv6 トラフィックを 6PE1 ルータに転送するように設定されています。ネットワークのコア内の P1 ルータは、MPLS、ラベル配布プロトコル、IPv4 IGP、およびシスコ エクスプレス フォワーディングか分散型シスコ エクスプレス フォワーディングを実行していると想定されるため、6PE 機能をイネーブルにするための新しい設定は必要ありません。CE1 ルータおよび P1 ルータでは新たな設定作業は必要ありませんが、参照用として設定例を「IPv6 over MPLS の設定例」（P.14）に示します。

図 4　　6PE の設定例



前提条件

- 6PE ルータ（図 4 の 6PE1 ルータと 6PE2 ルータ）は、コア IPv4 ネットワークのメンバである必要があります。コア ネットワークに接続されている 6PE ルータ インターフェイスは、MPLS、およびコア ネットワークと同じラベル配布プロトコルおよび IPv4 IGP を実行している必要があります。
- 6PE ルータは、IPv4 と IPv6 の両方を実行するデュアル スタックとして設定されている必要もあります。

制約事項

（注） Cisco IOS Release 12.2(22)S 時点では、次の制約事項は Cisco IOS 12.2 S リリースには適用されません。

次の制約事項は、IPv6 プロバイダー エッジ ルータ over MPLS（6PE）機能を実装している場合に適用されます。

- コア MPLS ルータは、MPLS と IPv4 だけをサポートしているため、IPv6 Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）メッセージの転送または作成を行うことはできません。
- Cisco 6PE では、MPLS パスと IPv6 パス間のロード バランシング機能が提供されません。両方が使用可能な場合は、MPLS パスが常に優先されます。2 つの MPLS パス間のロード バランシングは実行できます。
- BGP マルチパスは、Cisco 6PE ルータではサポートされていません。2 つの BGP ピアが等価コストで同じプレフィクスをアドバタイズする場合、Cisco 6PE では、最後のルートを使用して MPLS コアを通過します。
- 6PE 機能は、RSVP-TE トンネル以外のトンネルではサポートされていません。

6PE ルータでの送信元アドレス インターフェイスの指定

ここでは、ローカルで生成されたパケットがその送信元 IPv6 アドレスを取得する元となるインターフェイスを指定する方法について説明します。これは、6PE を展開するために実行する必要がある 2 つの作業のうちの最初の作業です。6PE を実装するために必要な 2 番めの作業の詳細については、「プレフィクスをアドバタイズするための 6PE ラベルのバインドおよびアドバタイズ」を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **ipv6 cef**
5. **interface** *type number*
6. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 unicast-routing** **例：** `Router(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。
ステップ 4	**ipv6 cef** **例：** `Router(config)# ipv6 cef`	IPv6 シスコ エクスプレス フォワーディングをイネーブルにします。
ステップ 5	**interface** *type number* **例：** `Router(config)# interface Serial 0/0`	インターフェイスのタイプと番号を指定し、インターフェイス コンフィギュレーション モードを開始します。 • この機能のコンテキストでは、設定されるインターフェイスは、CE ルータと通信するインターフェイスとなります。
ステップ 6	**ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*} **例：** `Router(config-if)# ipv6 address 2001:0DB8:FFFF::2/64`	IPv6 の一般的なプレフィクスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。

プレフィクスをアドバタイズするための 6PE ラベルのバインドおよびアドバタイズ

ここでは、指定した BGP ネイバーに IPv6 プレフィクスをアドバタイズするときに、集約ラベルのバインドとアドバタイズをイネーブルにする方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **no bgp default ipv4-unicast**
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number*
6. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number*
7. **address-family ipv6** [**unicast**]
8. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**

9. **neighbor** {*ip-address* | *ipv6-address*} **send-label**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* **例：** `Router(config)# router bgp 65000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**no bgp default ipv4-unicast** **例：** `Router(config-router)# no bgp default ipv4-unicast`	前の手順で指定した BGP ルーティング プロセスの IPv4 ユニキャスト アドレス ファミリをディセーブルにします。 **（注）** IPv4 ユニキャスト アドレス ファミリのルーティング情報が、**neighbor remote-as** コマンドを使用して設定した各 BGP ルーティング セッションにデフォルトでアドバタイズされます。ただし、**neighbor remote-as** コマンドを設定する前に **no bgp default ipv4-unicast** コマンドを設定している場合は除きます。
ステップ 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number* **例：** `Router(config-router)# neighbor 192.168.99.70 remote-as 65000`	指定した自律システムのネイバーの IP アドレスをローカル ルータの BGP ネイバーテーブルに追加します。
ステップ 6	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number* **例：** `Router(config-router)# neighbor 192.168.99.70 update-source Loopback 0`	IPv4 アドレスがピアリングの送信元アドレスとして使用されるインターフェイスを指定します。 • この作業のコンテキストでは、このインターフェイスは、32 ビットのマスクが設定された IPv4 アドレスを持っている必要があります。ループバック インターフェイスを使用することを推奨します。このアドレスを使用して、IPv6 ネクストホップがピア 6PE によって決定されます。
ステップ 7	**address-family ipv6** [**unicast**] **例：** `Router(config-router)# address-family ipv6`	IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • **unicast** キーワードでは、IPv6 ユニキャスト アドレス ファミリを指定します。デフォルトでは、**address-family ipv6** コマンドで **unicast** キーワードが指定されていない場合、ルータは IPv6 ユニキャスト アドレス ファミリのコンフィギュレーション モードになります。

	コマンドまたはアクション	目的
ステップ 8	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** **例：** `Router(config-router-af)# neighbor 192.168.99.70 activate`	ローカル ルータとの間で IPv6 アドレス ファミリを交換できるようにネイバーを設定します。
ステップ 9	**neighbor** {*ip-address* | *ipv6-address*} **send-label** **例：** `Router(config-router-af)# neighbor 192.168.99.70 send-label`	BGP ルートとともに MPLS ラベルを送信するルータの機能をアドバタイズします。 • IPv6 アドレス ファミリ コンフィギュレーション モードでは、このコマンドによって、BGP での IPv6 プレフィクスのアドバタイズ時に集約ラベルをバインドおよびアドバタイズできるようになります。

iBGP マルチパス ロード シェアリングの設定

ここでは、iBGP マルチパス ロード シェアリングを設定し、ルーティング テーブルにインストールできる並列 iBGP ルートの最大数を制御する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **maximum-paths ibgp** *number-of-paths*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *as-number* **例：** `Router(config)# router bgp 65000`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 4	**maximum-paths ibgp** *number-of-paths* **例：** Router(config-router)# maximum-paths ibgp 3	ルーティング テーブルにインストールできる並列 iBGP ルートの最大数を制御します。

6PE の設定および動作の確認

6PE が実行されている場合は、次のコンポーネントを監視できます。

- マルチプロトコル BGP
- MPLS
- Cisco Express Forwarding for IPv6
- IPv6 ルーティング テーブル

この任意の作業では、6PE の設定および動作を確認するためにさまざまなコンポーネントに関する情報を表示する方法について説明します。

手順の概要

1. **show bgp ipv6** {**unicast** | **multicast**} [*ipv6-prefix*/*prefix-length*] [**longer-prefixes**] [**labels**]
2. **show bgp ipv6** {**unicast** | **multicast**} **neighbors** [*ipv6-address*] [**received-routes** | **routes** | **flap-statistics** | **advertised-routes** | **paths** *regular-expression* | **dampened-routes**]
3. **show mpls forwarding-table** [*network* {*mask* | *length*} | **labels** *label* [**-***label*] | **interface** *interface* | **next-hop** *address* | **lsp-tunnel** [*tunnel-id*]] [**vrf** *vrf-name*] [**detail**]
4. **show ipv6 cef** [*ipv6-prefix*/*prefix-length*] | [*interface-type interface-number*] [**longer-prefixes** | **similar-prefixes** | **detail** | **internal** | **platform** | **epoch** | **source**]]
5. **show ipv6 route** [*ipv6-address* | *ipv6-prefix*/*prefix-length* | *protocol* | *interface-type interface-number*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show bgp ipv6** {**unicast** | **multicast**} [*ipv6-prefix*/*prefix-length*] [**longer-prefixes**] [**labels**] **例：** `Router> show bgp ipv6 unicast 2001:0DB8:DDDD::/48`	（任意）IPv6 BGP ルーティング テーブルのエントリを表示します。 • この例では、プレフィクス 2001:0DB8:DDDD::/48 の IPv6 ルートに関する情報が表示されます。
ステップ 2	**show bgp ipv6** {**unicast** | **multicast**} **neighbors** [*ipv6-address*] [**received-routes** | **routes** | **flap-statistics** | **advertised-routes** | **paths** *regular-expression* | **dampened-routes**] **例：** `Router> show bgp ipv6 neighbors unicast 192.168.99.70`	（任意）ネイバーへの IPv6 BGP 接続に関する情報が表示されます。 • この例では、IPv6 ラベル機能などの情報が、192.168.99.70 の BGP ピアに表示されます。
ステップ 3	**show mpls forwarding-table** [*network* {*mask* | *length*} | **labels** *label* [**-***label*] | **interface** *interface* | **nexthop** *address* | **lsp-tunnel** [*tunnel-id*]] [**vrf** *vrf-name*] [**detail**] **例：** `Router> show mpls forwarding-table`	（任意）MPLS Forwarding Information Base（FIB; 転送情報ベース）の内容を表示します。 • この例では、MPLS ラベルを IPv6 プレフィクスにリンクする情報が表示され、そこではラベルは集約で示され、プレフィクスは IPv6 で示されます。

	コマンドまたはアクション	目的
ステップ 4	**show ipv6 cef** [*ipv6-prefix/prefix-length*]	[*interface-type interface-number*] [**longer-prefixes** | **similar-prefixes** | **detail** | **internal** | **platform** | **epoch** | **source**]] **例：** `Router> show ipv6 cef 2001:0DB8:DDDD::/64`	（任意）IPv6 アドレス情報に基づく FIB エントリを表示します。 • この例では、シスコ エクスプレス フォワーディング テーブルからのプレフィクス 2001:0DB8:DDDD::/64 のラベル情報が表示されます。
ステップ 5	**show ipv6 route** [*ipv6-address* | *ipv6-prefix/prefix-length* | *protocol* | *interface-type interface-number*] **例：** `Router> show ipv6 route`	（任意）IPv6 ルーティング テーブルの現在の内容を表示します。

出力例

ここでは、次の出力例について説明します。

show bgp ipv6 コマンドの出力例

次の例では、IPv6 プレフィクスを指定した **show bgp ipv6** コマンドを使用して、IPv6 ルートに関する出力情報が表示されています。

```
Router# show bgp ipv6 2001:0DB8:DDDD::/48

BGP routing table entry for 2001:0DB8:DDDD::/48, version 15
Paths: (1 available, best #1, table Global-IPv6-Table)
  Not advertised to any peer
  Local
    ::FFFF:192.168.99.70 (metric 20) from 192.168.99.70 (192.168.99.70)
      Origin IGP, localpref 100, valid, internal, best
```

show bgp ipv6 neighbors コマンドの出力例

次の例では、IP アドレスを指定した **show bgp ipv6 neighbors** コマンドを使用して、「IPv6 ラベル」機能を含む、BGP ピアに関する出力情報が表示されています。

```
Router# show bgp ipv6 neighbors 192.168.99.70

BGP neighbor is 192.168.99.70, remote AS 65000, internal link
  BGP version 4, remote router ID 192.168.99.70
  BGP state = Established, up for 00:05:17
  Last read 00:00:09, hold time is 0, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received
    Address family IPv6 Unicast: advertised and received
    ipv6 MPLS Label capability: advertised and received
  Received 54 messages, 0 notifications, 0 in queue
  Sent 55 messages, 1 notifications, 0 in queue
```

```
  Default minimum time between advertisement runs is 5 seconds

 For address family: IPv6 Unicast
  BGP table version 21880, neighbor version 21880
  Index 1, Offset 0, Mask 0x2
  Route refresh request: received 0, sent 0
  77 accepted prefixes consume 4928 bytes
  Prefix advertised 4303, suppressed 0, withdrawn 1328
  Number of NLRIs in the update sent: max 1, min 0
```

show mpls forwarding-table コマンドの出力例

次の例では、**show mpls forwarding-table** コマンドを使用して、MPLS ラベルをプレフィクスにリンクする出力情報が表示されています。6PE 機能が設定されている場合、ラベルは集約されます。これは、1 つのローカル ラベルに対して複数のプレフィクスが存在し、プレフィクスのカラムにはターゲットのプレフィクスではなく「IPv6」が含まれているためです。

```
Router# show mpls forwarding-table

Local Outgoing      Prefix            Bytes tag Outgoing       Next Hop
tag   tag or VC     or Tunnel Id      switched  interface
16    Aggregate     IPv6              0
17    Aggregate     IPv6              0
18    Aggregate     IPv6              0
19    Pop tag       192.168.99.64/30  0         Se0/0          point2point
20    Pop tag       192.168.99.70/32  0         Se0/0          point2point
21    Pop tag       192.168.99.200/32 0         Se0/0          point2point
22    Aggregate     IPv6              5424
23    Aggregate     IPv6              3576
24    Aggregate     IPv6              2600
```

show bgp ipv6 コマンドの出力例

次の例では、**labels** キーワードを指定した **show bgp ipv6** コマンドを使用して、ラベル スイッチング情報とともに最上位のスタック ラベルに関する出力情報が表示されています。

```
Router# show bgp ipv6 labels

Network              Next Hop               In tag/Out tag
2001:0DB8:DDDD::/64  ::FFFF:192.168.99.70   notag/20
```

show ipv6 cef コマンドの出力例

次の例では、IPv6 プレフィクスを指定した **show ipv6 cef** コマンドを使用して、シスコ エクスプレス フォワーディング テーブルのラベルに関する出力情報が表示されています。

```
Router# show ipv6 cef 2001:0DB8:DDDD::/64

2001:0DB8:DDDD::/64
      nexthop ::FFFF:192.168.99.70
      fast tag rewrite with Se0/0, point2point, tags imposed {19 20}
```

show ipv6 route コマンドの出力例

次の例では、**show ipv6 route** コマンドを使用して、IPv6 ルーティング テーブルの出力情報が表示されています。この出力では、IPv6 MPLS 仮想インターフェイスが、MPLS クラウドを介して転送される IPv6 ルートの出力インターフェイスとして示されています。図 4 のルータを使用するこの例では、出力は 6PE1 ルータから得られます。

6PE2 ルータは、CE2 ルータに設定された IPv6 プレフィクス 2001:0DB8:dddd::/48 をアドバタイズし、ネクストホップ アドレスは IPv4 互換 IPv6 アドレス ::ffff:192.168.99.70 です。ここで、192.168.99.70 は、6PE2 ルータの IPv4 アドレスです。

```
Router# show ipv6 route
```

```
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
B 2001:0DB8:DDDD::/64 [200/0]
  via ::FFFF:192.168.99.70, IPv6-mpls
B 2001:0DB8:DDDD::/64 [200/0]
  via ::FFFF:192.168.99.70, IPv6-mpls
L 2001:0DB8:FFFF::1/128 [0/0]
  via ::, Ethernet0/0
C 2001:0DB8:FFFF::/64 [0/0]
  via ::, Ethernet0/0
S 2001:0DB8:FFFF::/48 [1/0]
  via 2001:0DB8:B00:FFFF::2, Ethernet0/0
```

IPv6 over MPLS の設定例

次の例では、図 4 で示し、「6PE ルータでの送信元アドレス インターフェイスの指定」および「プレフィクスをアドバタイズするための 6PE ラベルのバインドおよびアドバタイズ」の項で使用している 3 台のルータの 6PE 設定例を示します。

- 「カスタマー エッジ ルータ：例」（P.14）
- 「プロバイダー エッジ ルータ：例」（P.14）
- 「コア ルータ：例」（P.16）

カスタマー エッジ ルータ：例

次の例では、カスタマー エッジ ルータ（図 4 の CE1）のシリアル インターフェイス 0/0 が、サービス プロバイダーに接続され、IPv6 アドレスを割り当てられています。IPv6 がイネーブルになっており、デフォルトのスタティック ルートが、6PE1 ルータのシリアル インターフェイス 0/0 の IPv6 アドレスを使用してインストールされています。

```
ip cef
!
ipv6 unicast-routing
!
interface Serial 0/0
 description to_6PE1_router
 no ip address
 ipv6 address 2001:0DB8:FFFF::2/64
!
ipv6 route ::/0 Serial 0/0 FE80::210:XXXX:FEE1:1001
```

プロバイダー エッジ ルータ：例

6PE ルータ（図 4 の 6PE1）は、IPv4 と IPv6 の両方のトラフィック用に設定されています。イーサネット インターフェイス 0/0 は、IPv4 アドレスを使用して設定され、ネットワークのコア内のルータ（図 4 のルータ P1）に接続されています。このルータ上の統合 IS-IS および TDP の設定は、P1 ルータと似ています。

ルータ 6PE1 は、IPv4 接続を介して確立された internal BGP（iBGP; 内部 BGP）を使用して、別の 6PE（図 4 のルータ 6PE2）と IPv6 ルーティング情報を交換することから、すべての **neighbor** コマンドで 6PE2 ルータの IPv4 アドレスが使用されます。すべての BGP ピアは自律システム 65000 内に存在するため、IGP との同期は、IPv4 の場合はオフになっています。IPv6 アドレス ファミリ コンフィギュレーション モードでは、同期はデフォルトでディセーブルになっています。

IPv6 および Cisco Express Forwarding for IPv6 はイネーブルであり、6PE2 ネイバーはアクティブ化されており、IPv6 プレフィクスの集約ラベルのバインディングとアドバタイズメントは **neighbor send-label** コマンドを使用してイネーブルになっています。接続されているスタティックな IPv6 ルートは、BGP を使用して再配布されます。IPv6 パケットがローカル ルータで生成される場合、MPLS 処理用の IPv6 アドレスは、ループバック インターフェイス 0 のアドレスになります。

次の例では、シリアル インターフェイス 0/0 がカスタマーに接続され、カスタマーに委任された IPv6 プレフィクスは、サービス プロバイダーの IPv6 プレフィクスから決定された 2001:0DB8:ffff::/48 となっています。スタティック ルートは、IPv6 パケットを 6PE ルートと CE ルータ間でルーティングするように設定されています。

```
ip cef
ipv6 cef
ipv6 unicast-routing
!
mpls ipv6 source-interface Loopback0
tag-switching tdp router-id Loopback0
!
interface Loopback0
 ip address 192.168.99.5 255.255.255.255
 ipv6 address 2001:0DB8:1000:1::1/64
!
interface Ethernet0/0
 description to_P_router
 ip address 192.168.99.1 255.255.255.252
 ip router isis
 tag-switching ip
!
interface Serial0/0
 description to_CE_router
 no ip address
 ipv6 address 2001:0DB8:FFFF::1/64
!
router isis
 passive-interface Loopback0
 net 49.0001.1921.6809.9005.00
!
router bgp 65000
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 192.168.99.70 remote-as 65000
 neighbor 192.168.99.70 description to_6PE2
 neighbor 192.168.99.70 update-source Loopback0
 !
 address-family ipv6
 neighbor 192.168.99.70 activate
 neighbor 192.168.99.70 send-label
 network 2001:0DB8:FFFF::/48
 exit-address-family
!
ipv6 route 2001:0DB8:FFFF::/48 Ethernet0/0 2001:0DB8:FFFF::2
```

コア ルータ：例

次の例では、ネットワークのコア内のルータ（図 4 のルータ P）は、MPLS、IS-IS、および IPv4 だけを実行しています。イーサネット インターフェイスは、IPv4 アドレスを使用して設定されており、6PE ルータに接続されています。IS-IS は、ネットワークの IGP であり、P1 ルータと 6PE ルータは、同じ IS-IS エリア 49.0001 に存在します。TDP およびタグ スイッチングが、両方のイーサネット インターフェイスでイネーブルになっています。シスコ エクスプレス フォワーディングが、グローバル コンフィギュレーション モードでイネーブルになっています。

```
ip cef
!
tag-switching tdp router-id Loopback0
!
interface Loopback0
 ip address 192.168.99.200 255.255.255.255
!
interface Ethernet0/0
 description to_6PE1
 ip address 192.168.99.2 255.255.255.252
 ip router isis
 tag-switching ip
!
interface Ethernet0/1
 description to_6PE2
 ip address 192.168.99.66 255.255.255.252
 ip router isis
 tag-switching ip

router isis
 passive-interface Loopback0
 net 49.0001.1921.6809.9200.00
```

関連情報

MPLS ネットワークをさらにカスタマイズする場合は、『*Cisco IOS IP Switching Configuration Guide*』を参照してください。

その他の関連資料

ここでは、IPv6 over MPLS の実装機能に関する関連資料について説明します。

関連資料

関連項目	参照先
CE ルータでトンネルを使用する IPv6	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing Tunneling for IPv6」
IPv6 のサポート機能リスト	『*Cisco IOS IPv6 Configuration Guide*』の「Start Here: Cisco IOS Software Release Specifics for IPv6 Features」
IPv6 コマンド：コマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS IPv6 Command Reference*』

関連項目	参照先
MPLS の設定作業	『*Cisco IOS Multiprotocol Label Switching Configuration Guide*』の「Multiprotocol Label Switching Overview」
MPLS コマンド：コマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS Multiprotocol Label Switching Command Reference*』

規格

規格	タイトル
Draft-ietf-ngtrans-bgp-tunnel-04.txt	『*Connecting IPv6 Islands Across IPv4 Clouds with BGP*』

MIB

MIB	MIB リンク
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によってサポートされる新しい RFC または変更された RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

IPv6 over MPLS の実装の機能情報

表 1 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。この表には、Cisco IOS Release 12.3(14)T 以降のリリースで導入または変更された機能だけを示します。

ここに記載されていないこのテクノロジーの機能情報については、「*Start Here: Cisco IOS Software Release Specifies for IPv6 Features*」を参照してください。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　IPv6 over MPLS の実装の機能情報

機能名	リリース	機能情報
回線トランスポートを介した IPv6 over MPLS	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(15)T 12.3 12.3(2)T 12.4 12.4(2)T	この機能では、リモート IPv6 ドメイン間の通信は、専用リンクを介してネイティブ IPv6 プロトコルを実行します。この場合、基礎となるメカニズムは IPv6 に対して完全に透過的です。 この機能に関する詳細については、次の各項を参照してください。 • 「回線トランスポートを介した IPv6 over MPLS」（P.2） • 「回線トランスポートを介した IPv6 over MPLS の展開」（P.6）
カスタマー エッジ ルータでトンネルを使用する IPv6	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(15)T 12.3 12.3(2)T 12.4 12.4(2)T	CE ルータでトンネルを使用することが、MPLS の動作またはインフラストラクチャに影響を与えることなく、IPv6 over MPLS ネットワークを最も簡単に展開できる方法です。 この機能に関する詳細については、次の各項を参照してください。 • 「カスタマー エッジ ルータでトンネルを使用する IPv6」（P.3）

表 1　IPv6 over MPLS の実装の機能情報 （続き）

機能名	リリース	機能情報
IPv6 スイッチング：MPLS を介するプロバイダー エッジ ルータ（6PE）	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(33)SRA 12.2(15)T 12.3 12.3(2)T 12.4 12.4(2)T	MPLS を介した IPv6 プロバイダー エッジ ルータのシスコ実装によって、IPv6 サイトは、MPLS LSP を使用して、MPLS IPv4 コア ネットワークを介して互いに通信できます。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 プロバイダー エッジ ルータ（6PE）」（P.4） • 「IPv6 プロバイダー エッジ ルータ（6PE）の展開」（P.6） • 「6PE ルータでの送信元アドレス インターフェイスの指定」（P.7） • 「プレフィクスをアドバタイズするための 6PE ラベルのバインドおよびアドバタイズ」（P.8） • 「IPv6 over MPLS の設定例」（P.14）
6PE マルチパス	12.2(25)S 12.2(28)SB 12.2(33)SRA 12.4(6)T	6PE マルチパス機能では、Multiprotocol internal BGP（MP-iBGP; マルチプロトコル内部 BGP）を使用して、MPLS IPv4 コア ネットワークを介して IPv6 ルートを配布し、MPLS ラベルを各ルートに付加します。 この機能に関する詳細については、次の各項を参照してください。 • 「6PE マルチパス」（P.5） • 「iBGP マルチパス ロード シェアリングの設定」（P.10）

IPv6 VPN over MPLS の実装

Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）- Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）の Virtual Private Network（VPN; バーチャル プライベート ネットワーク）機能は、Provider Edge（PE; プロバイダー エッジ）ベースの VPN モデルの実装を表します。このマニュアルでは、IPv6 VPN over MPLS（6VPE）機能について説明します。

原則として、IPv4 VPN と IPv6 VPN との間に相違点はありません。IPv4 と IPv6 のどちらにおいても、マルチプロトコル BGP が MPLS VPN for IPv6（VPNv6）アーキテクチャの中心的存在となります。サービス プロバイダー バックボーンを介して IPv6 ルートを配布するために使用され、同じ手順を使用して、重複するアドレス、再配布ポリシー、およびスケーラビリティの問題が処理されます。

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「IPv6 VPN over MPLS の実装の機能情報」（P.56）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

IPv6 VPN over MPLS を実装するための前提条件

IPv6 VPN の動作を設定する前に、ネットワークで次の Cisco IOS サービスが稼動している必要があります。

- プロバイダー バックボーン ルータにおける MPLS
- VPN PE ルータがあるプロバイダー ルータにおける VPN コード付き MPLS
- VPN サービスを提供するすべてのルータにおける BGP
- すべての MPLS 対応ルータにおけるシスコ エクスプレス フォワーディング スイッチング
- Class of Service（CoS; サービス クラス）機能

IPv6 VPN over MPLS を実装するための制約事項

6VPE は、MPLS IPv4 シグナリング コアをサポートします。MPLS IPv6 シグナリング コアはサポートされません。

IPv6 VPN over MPLS の実装に関する情報

マルチプロトコル BGP は、IPv4 と IPv6 の両方において MPLS IPv6 VPN アーキテクチャの中心的存在です。サービス プロバイダー バックボーンを介して IPv6 ルートを配布するために使用され、同じ手順を使用して、重複するアドレス、再配布ポリシー、およびスケーラビリティの問題が処理されます。

IPv6 には重複するアドレス空間はありませんが、IPv6 アドレスの先頭には Route Distinguisher（RD; ルート識別子）が付加されます。Network Layer Reachability Information（NLRI; ネットワーク レイヤ到達可能性情報）の 3 タプル形式（長さ、IPv6 プレフィクス、およびラベルを含む）は、マルチプロトコル BGP を使用してこれらのルートを配布するように定義されます。拡張コミュニティ アトリビュート（ルート ターゲット）は、エクスポートされたルートにタグを付け、インポートされたルートをフィルタリングすることによって、ルーティング情報の再配布を制御するために使用されます。

スケーラビリティを実現するために、ルート リフレクタを使用してルーティング パスを集中させ、完全 PE メッシュを回避することができます。ルート リフレッシュ、自動ルート フィルタリング、アウトバウンド ルート フィルタリングなどの IPv6 の BGP 機能は、各 PE に保持されるルートの数を削減するのに役立ちます。

このマニュアルでは、IPv4 と IPv6 間の次の相違点を中心に説明します。

- 新しいマルチプロトコル BGP IPv6 VPN アドレス ファミリの作成と IPv6 VPN アドレス形式の仕様
- 新しい IPv6 VPN NLRI の仕様
- ルータに IPv4 ベースの MPLS コアがある場合の BGP ネクストホップ符号化の仕様

プロバイダー間トポロジおよび Carrier Supporting Carrier（CSC）トポロジなどの一部の IPv6 VPN 機能は、BGP-MPLS IPv6 VPN に固有です。たとえば、Autonomous System Boundary Router（ASBR; 自律システム境界ルータ）間のリンクは、転送されるアドレス ファミリとは関係なく、IPv4 だけ、IPv6 だけ、または両方をサポートすることがあります。

IPv6 VPN over MPLS を設定するには、次の概念を理解する必要があります。

- 「IPv6 VPN over MPLS（6VPE）のアドレッシングに関する考慮事項」（P.3）
- 「IPv6 VPN over MPLS の基本的な機能」（P.3）
- 「IPv6 MPLS VPN の高度な機能」（P.7）

IPv6 VPN over MPLS（6VPE）のアドレッシングに関する考慮事項

配置されている VPN モデル（Customer Edge（CE; カスタマー エッジ）ベース、PE ベースなど）に関係なく、ホストが 1 つの VPN 内の 1 つのサイトを使用して他のサイトやパブリック リソースと通信できるように、VPN のアドレッシング計画を定義する必要があります。

VPN IPv4 サイトは、多くの場合、アドレッシング計画にプライベート アドレッシングを使用します。これらのアドレスは、登録の必要はありませんが、パブリック ネットワーク上ではルーティング不可になります。プライベート サイト内のホストでパブリック ドメインにアクセスする必要がある場合、ホストは常に、そのホストの代わりにパブリック アドレスを検出するデバイスを通過します。IPv4 では、このデバイスに、ネットワーク アドレス変換またはアプリケーション プロキシを指定できます。

IPv6 ではより大きいアドレス空間を使用できるため、IPv6 アドレッシングを実現する最も簡単なアプローチは、プライベート アドレッシング計画に IPv6 グローバル アドレスを使用することです。また別のアプローチとして、Unique Local Address（ULA; ユニーク ローカル アドレス）を使用することもできます。ULA は、それらのスコープに基づいてサイト境界で簡単にフィルタリングできます。また、ULA は Internet Service Provider（ISP; インターネット サービス プロバイダー）非依存であり、永続的または間欠的なインターネット接続がないサイト内での通信に使用できます。

6VPE では、ULA は通常のグローバル アドレスとして処理されます。ULA プレフィクスは、パブリック ドメイン内に表示されないように、ルータ設定によってフィルタリングされます。ピア上のリンク ローカル アドレスが、BGP（IPv6 または IPv6 VPN）スピーカーによってアナウンスされることはありません。

パブリック ドメインにアクセスする必要があるプライベート サイト内のホストは、ルーティング可能なグローバル アドレスを使用してホストの代わりにパブリック リソースにアクセスする IPv6 アプリケーション プロキシ（Web ページにアクセスするための Web プロキシなど）を介して、これを行うことができます。または、ホスト自身のパブリック アドレスを使用することもできます。後者の場合、ULA が配置されているときには、IPv6 ホストもまたルーティング可能なグローバル アドレスを使用して設定されます。送信元アドレスの選択アルゴリズムを使用して、宛先アドレスを基にどちらか片方が選択されます。

IPv6 VPN over MPLS の基本的な機能

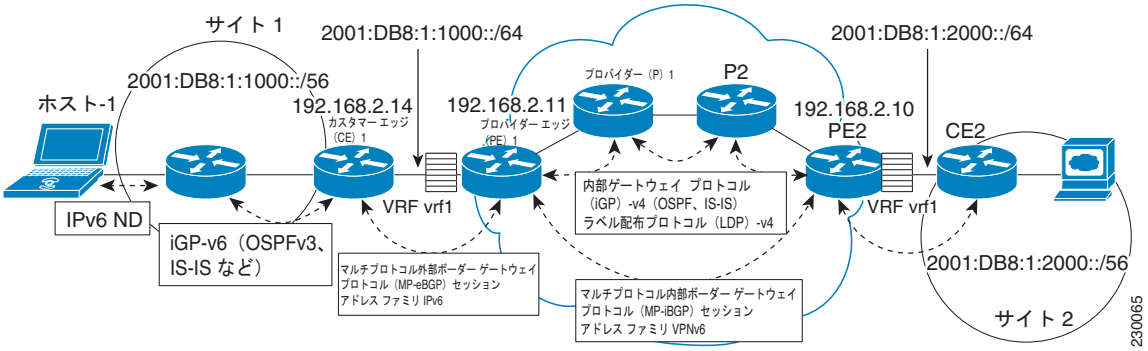
IPv6 への移行により、IPv4 と IPv6 の共存が長期間続くことになると予想されます。IPv6 VPN の配置方式では、既存の MPLS IPv4 コア ネットワークを活用することによってこの共存をうまく利用します。このアプローチを 6VPE と呼びます。

ここでは、基本的な IPv6 MPLS VPN 機能の概念について説明します。

IPv6 VPN アーキテクチャの概要

図 1 に、IPv6 VPN アーキテクチャの重要な特徴を示します。

図 1　簡単な IPv6 VPN アーキテクチャ



CE ルータは、PE ルータを使用して、プロバイダーのバックボーンに接続されます。PE ルータは、プロバイダー（図 1 の P1 および P2）ルータを使用して接続されます。プロバイダー（P）ルータは VPN ルートを認識せず、6VPE の場合は、IPv4 しかサポートしていないこともあります。PE ルータだけが VPN 固有の作業を実行します。6VPE の場合、PE ルータはデュアル スタック（IPv4 および IPv6）ルータになります。

VPN 動作のルーティング コンポーネントは、コア ルーティングとエッジ ルーティングに分けられます。PE ルータと P ルータを含むコア ルーティングは、一般的に Open Shortest Path First（OSPF）または Intermediate System-to-Intermediate System（IS-IS）などの IPv4 Interior Gateway Protocol（IGP; 内部ゲートウェイ プロトコル）によって実行されます。図 1 の場合、IGP は内部ルートだけをプロバイダーの自律システムに配布します。コア ルーティングにより、P および PE ルータ間の接続が可能になります。

エッジ ルーティングは、PE ペア間のルーティングと PE と CE 間のルーティングの 2 方向で発生します。PE ペア間のルーティングは、IPv6 VPN アドレス ファミリを使用したマルチプロトコル internal BGP（iBGP; 内部 BGP）を使用して実行されます。この方式は、入力 PE ルータでは適切なルート エクスポート ポリシーを、出力 PE ルータでは適切なルート インポート ポリシーを使用して、PE-CE ルーティングを介して CE から学習したルートを配布します。

CE とその PE 間のルーティングは、VRF 対応のルーティング プロトコルを使用して実行されます。スタティック ルート、external BGP（eBGP; 外部 BGP）、および Enhanced Interior Gateway Routing Protocol（EIGRP）は、VPN Routing and Forwarding（VRF; VPN ルーティングおよび転送）インスタンス対応です。図 1 の場合、CE（CE1）と PE（PE1）間で eBGP が使用されます。同時に、VPN サイト（図 1 のサイト 1）内では、CE によって IPv6 IGP（IPv6 用の OSPFv3 または IS-IS など）が実行されます。CE は、IGP ルートをマルチプロトコル eBGP アドレス ファミリ IPv6 に再配布します。これらのルートは、PE で vrf1 という名前の VRF にインストールされ、この VRF に定義されているエクスポート ポリシーに応じて、リモート PE（図 1 の PE2）に転送されます。

IPv6 VPN ネクストホップ

ルータが MP_REACH_NLRI アトリビュートを使用してプレフィクスをアナウンスすると、1 つの PE で稼動している MP-BGP が、リモート PE に送信されるアップデート メッセージ内に BGP ネクストホップを挿入します。このネクストホップは、受信されたアップデートから伝播されるか（たとえば、PE がルート リフレクタの場合など）、またはアップデート メッセージを送信する PE（出力 PE）のアドレスになります。

IPv6 VPN アドレス ファミリの場合、PE スピーカー間のネットワークの特性に関係なく、ネクストホップは IPv6 VPN アドレスである必要があります。RD は意味を持たないため（アドレスは VPN の一部ではない）、0 に設定されます。プロバイダー ネットワークがネイティブ IPv6 ネットワークの場

合、ネクストホップの残りの部分は出力 PE の IPv6 アドレスになります。それ以外の場合は、IPv6 マッピング アドレスとして使用される IPv4 アドレスになります（たとえば、::FFFF:*IPv4-address* など）。

IPv6 VPN ネクストホップの設定例については、「例：IPv4 ネクストホップを使用した IPv6 VPN の設定」（P.53）を参照してください。

MPLS 転送

1 つのカスタマー サイトから IPv6 トラフィックを受信すると、入力 PE ルータは MPLS を使用して、BGP ネクストホップとして識別された出力 PE ルータに向けて、バックボーンを介して IPv6 VPN パケットをトンネリングします。入力 PE ルータは、一般的に IPv6 パケットの先頭に外部ラベルおよび内部ラベルを付加してから、出力インターフェイスにパケットを配置します。

通常の動作では、転送パス上の P ルータは最初のラベルの先にあるフレームの内部を調べません。P ルータは着信ラベルを発信ラベルと交換するか、または次のルータが PE ルータの場合には着信ラベルを削除します。着信ラベルの削除は、最後から 2 番めのホップのポッピングと呼ばれます。残りのラベル（BGP ラベル）は、カスタマー サイトへの出力 PE インターフェイスを識別するために使用されます。また、このラベルは、プロトコル バージョン（IPv6）を最後の P ルータから隠します。このようにしなかった場合、最後の P ルータで IPv6 パケットを転送する必要があります。

P ルータは IPv6 VPN ルートを認識しません。IPv6 ヘッダーは 1 つ以上の MPLS ラベルの下に隠されたままになります。P ルータで、送達できない MPLS カプセル化 IPv6 パケットを受信した場合のオプションは 2 つあります。P ルータが IPv6 対応の場合、IPv6 ヘッダーを公開し、IPv6 メッセージ用の Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）を構築して、MPLS カプセル化メッセージを元のパケットの送信元に送信します。P ルータが IPv6 対応ではない場合、パケットはドロップされます。

GRE トンネルを介した 6VPE

一部の Cisco IOS リリースでは、入力 PE ルータは、MPLS を介した 6VPE と組み合せた IPv4 Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）トンネルを使用して、BGP ネクストホップとして識別された出力 PE ルータに向けて、バックボーンを介して IPv6 VPN パケットをトンネリングします。

VRF の概念

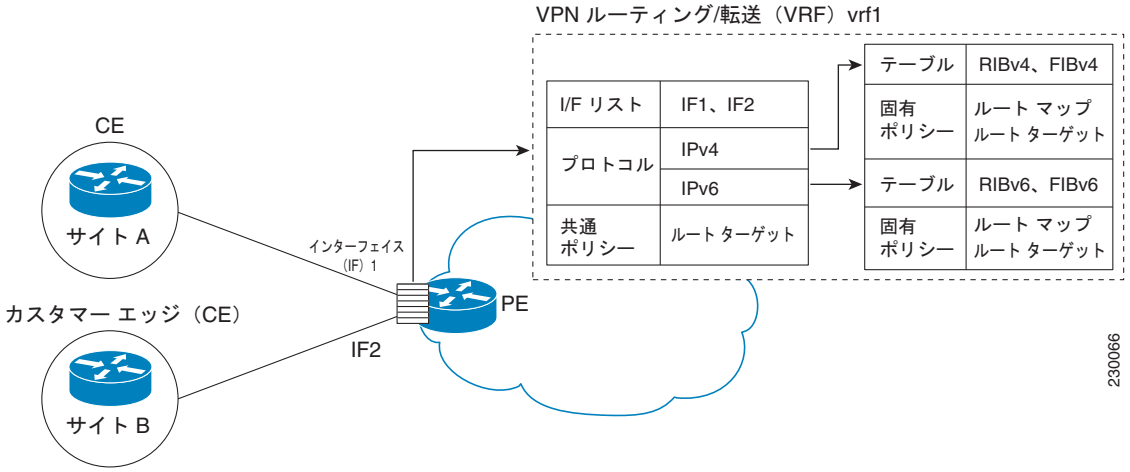
VRF は、プライベートなカスタマー固有の Routing Information Base（RIB; ルーティング情報ベース）および Forwarding Information Base（FIB; 転送情報ベース）とともに動作する仮想ルーティングおよび転送エンティティです。IPv4 ルーティング テーブルと IPv6 ルーティング テーブルは区別されますが、2 つのプロトコルで特定のカスタマーの同じ VRF を共有すると便利です。

IPv6 VPN カスタマーは、デュアル スタック ホストとルータを配置しているか、または IPv4 インフラストラクチャの一部を IPv6 ノードで覆っている既存の VPNv4 カスタマーである可能性があります。複数の配置モデルが可能です。一部のカスタマーは、IPv4 と IPv6 に別々の論理インターフェイスを使用して、それぞれに異なる VRF を定義しています。このアプローチでは IPv4 および IPv6 に別々のポリシーを設定できる柔軟性が提供されますが、同じポリシーを共有することはできなくなります。もう 1 つのアプローチのマルチプロトコル VRF では、PE-CE インターフェイス上で単一の VRF を保持し、IPv4、IPv6、または両方に対してイネーブルにします。これにより、共通または別々のポリシーを IP バージョンごとに定義できるようになります。このアプローチを使用すると、VRF は、PE で検出されるテーブル、インターフェイス、およびポリシーのセットとしてより適切に定義され、この PE に接続されている特定の VPN のサイトによって使用されます。

図 2 に、マルチプロトコル VRF を示します。ここでは、vrf1 という名前の VRF が IPv4 と IPv6 の両方に対してイネーブルになっており、2 つのインターフェイス（IF1、IF2）、2 つのテーブル セット（IPv4 RIB と FIB、IPv6 RIB と FIB）、および共通または個別のポリシー セットに関連付けられています。

IPv6 の VRF を設定する方法については、「IPv6 用の仮想ルーティングおよび転送インスタンスの設定」（P.10）を参照してください。

図 2　　マルチプロトコル VRF



IPv6 VPN スケーラビリティ

BGP-MPLS IPv6 VPN などの PE ベースの VPN は、CE ベースの VPN よりもスケーラビリティが高くなります。ネットワーク設計者は、ネットワークの設計時にスケーリングを考慮する必要があります。BGP-MPLS IPv6 VPN のスケーリングは、BGP-MPLS IPv4 VPN のスケーリングと似ています。次の点について考慮する必要があります。

- VRF テーブル サイズおよび BGP テーブル サイズなどのルーティング テーブル サイズ
- PE の平方数として増加する BGP セッション数

ルーティング テーブル サイズに関する問題は、多数のカスタマー サイトを処理する PE で発生します。これらの PE は、接続されているカスタマーごとに 1 つの RIB および FIB を持つだけではなく、PE の BGP テーブル（個々の VRF のすべてのエントリが統合される）もそれに応じて増加します。もう 1 つのスケーラビリティの問題は、プロバイダー ネットワーク内の PE の数が一定のレベル以上に増加したときに発生します。同じ VPN に属する多くのサイトが多数の PE に広がっていると想定した場合、マルチプロトコル BGP セッションの数は $(n–1) \times n/2$ のように急速に増加します。ここで、n は PE の数です。

IPv6 VPN over MPLS には、次の機能が含まれています。

- ルート リフレッシュおよび自動ルート フィルタリング：VRF にインポートされたルートだけがローカルに保持されるため、ルーティング テーブルのサイズが制限されます。インポート ポリシーが変更された場合は、ルート リフレッシュを送信して、ルーティング アップデートの再送信を照会できます。
- Outbound Route Filtering（ORF; アウトバウンド ルート フィルタリング）：アップデートがネットワーク上に不必要に送信されないように、入力 PE が出力 PE にフィルタをアドバタイズできるようにします。
- ルート リフレクタ：Route Reflector（RR; ルート リフレクタ）は、他の iBGP ピアから学習した iBGP ルートを伝播する iBGP ピアです。RR は iBGP セッションを集中させるために使用されます。

IPv6 MPLS VPN の高度な機能

IPv4 用の VPN からインターネットへのアクセス、マルチ自律システム バックボーン、CSC などの高度な MPLS 機能は、一般的に IPv6 でも IPv4 でも同じです。ただし、アドレッシングと、IPv4 バックボーンを介した 6VPE の動作方法には相違点があります。

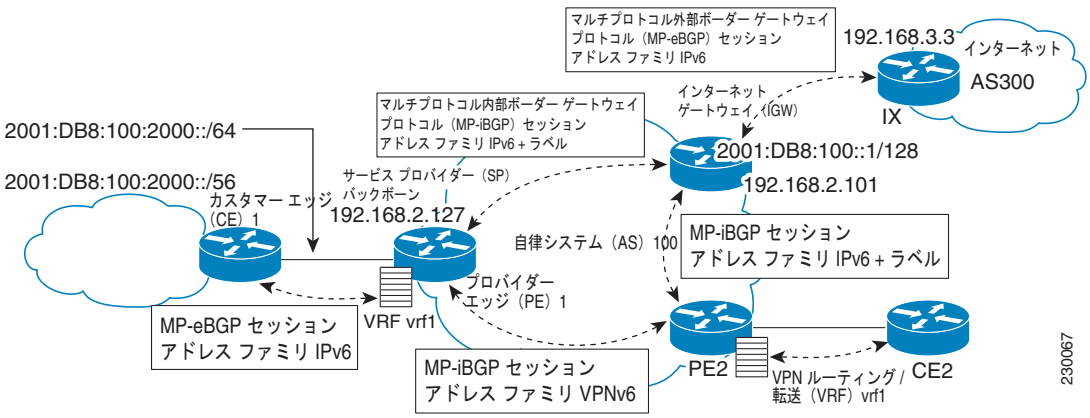
ここでは、高度な IPv6 MPLS VPN 機能の概念について説明します。

内部アクセス

大部分の VPN サイトでインターネットへのアクセスが必要になります。RFC 4364 には、インターネットへの VPN アクセスをイネーブルにするモデル セットが記載されています。これらすべてのモデルが IPv6 VPN にも適用されます。あるアプローチでは、1 つのインターフェイスがインターネットに接続するために CE によって使用され、別のインターフェイスが VRF に接続するために使用されます。別のモデルでは、すべてのインターネット ルートが VRF に再配布されます。このアプローチには、VRF ごとにインターネット ルートを複製する必要があるというデメリットがあります。

あるシナリオでは、IPv6 デフォルト テーブルで見つかったインターネット ゲートウェイを指すネクストホップとともに、スタティック ルートが VRF テーブルに挿入されます。図 3 に、このシナリオを示します。ここでは、インターネット アクセスが vrf1 という名前の VRF 内のカスタマーに提供されます。

図 3　　インターネット アクセス トポロジ



カスタマー サイト（図 3 のサイト 1）がインターネット経由でパブリック リソースにアクセスするには、このサイトがパブリック プレフィクスによって認識されている必要があります。IPv4 とは異なり、IPv6 では、サイト境界から発信されたときにプライベート アドレスをパブリック アドレスに変換できるようにする Network Address Translation（NAT; ネットワーク アドレス変換）メカニズムは提供されません。これは、サイト内のホストがパブリック アドレスを使用して発信することだけではなく、これらのアドレス（またはそれらが属するプレフィクス）がパブリック ドメイン内に表示される必要があることも意味します。

発信トラフィックの場合、入力 PE（PE1）の VRF テーブルに設定されているデフォルト ルートは、VPN 外の宛先に向かうトラフィックをインターネット ゲートウェイに誘導します。

着信トラフィックの場合、カスタマー サイトに向かうトラフィックを接続 PE（図 3 の PE1）経由で誘導するためのルートが、インターネット ゲートウェイに存在している必要があります。このルートは、入力 PE（PE1）により、（IPv6 アドレス ファミリ設定を含む）マルチプロトコル iBGP を使用して配布されます。そのため、インターネット ゲートウェイの VPN PE ごとに特別な設定を行う必要はありません。それでもなお、PE1 の着信トラフィックの場合は、サイトの VRF を指すカスタマー サイト グローバル プレフィクスのデフォルト テーブルに、ルートが存在している必要があります。

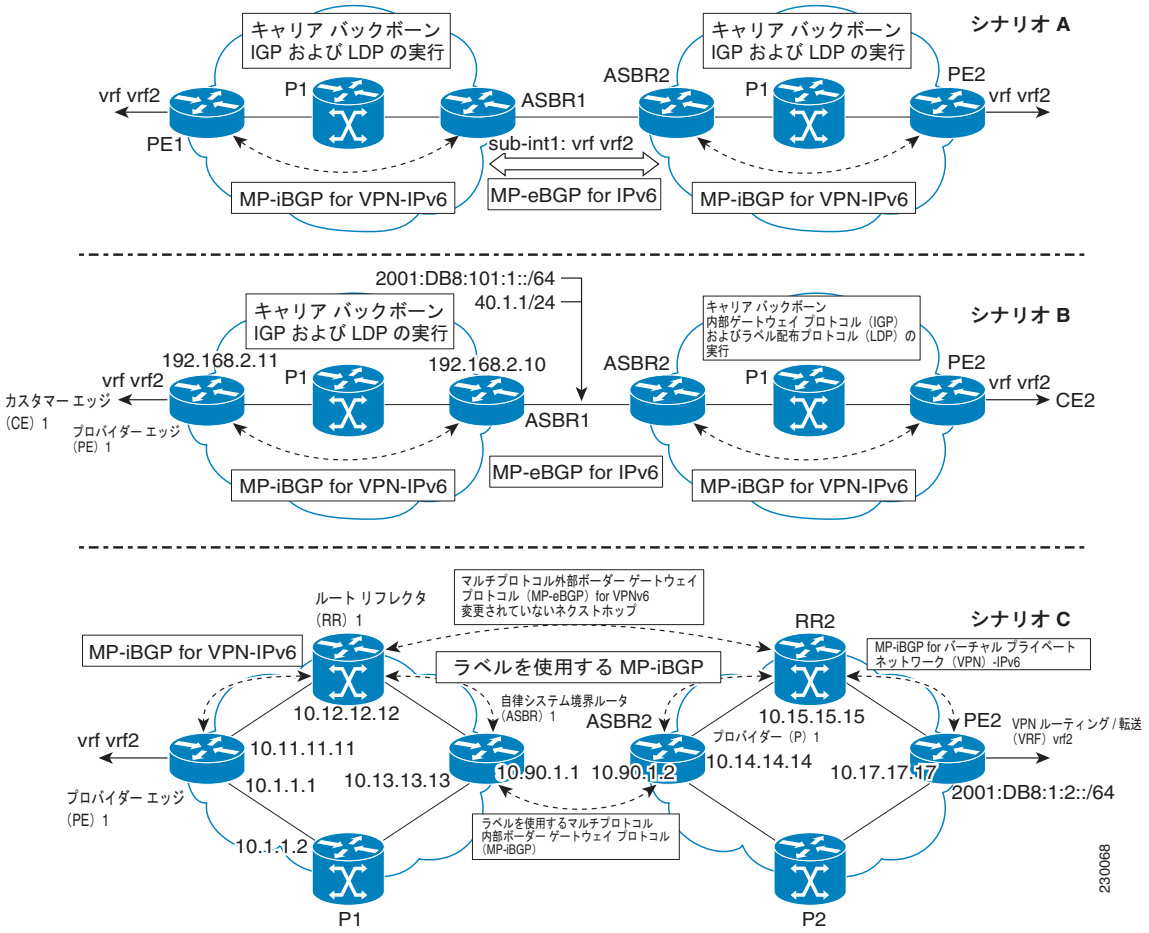
マルチ自律システム バックボーン

IPv4 が配置されていたすべての場所に IPv6 が配置されていると想定した場合、プロバイダー間 VPN の問題は、IPv6 および IPv4 で似ています。

自律システム境界を横断する IPv6 配置の場合、プロバイダーはピアリング モデルを入手するか、または VPNv4 用に設置されているピアリング モデルを使用する必要があることがあります。

図 4 に、IPv6 VPN のプロバイダー間シナリオを示します。

図 4　　プロバイダー間シナリオ



ASBR 間で使用されるネットワーク プロトコルに応じて、図 4 の 3 つのシナリオで複数の実装オプションを使用できます。たとえば、ASBR 間のマルチプロトコル eBGP IPv6 VPN ピアリングを提案しているシナリオ B では、IPv6 または IPv4 リンクのどちらでも使用できます。

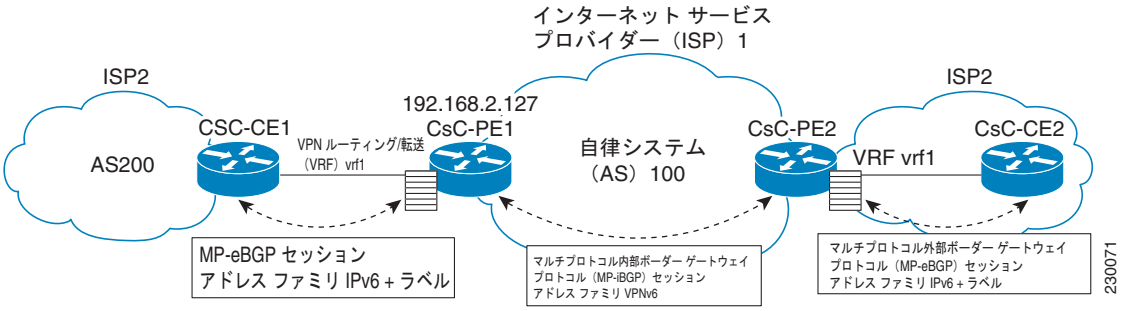
シナリオ C の場合、マルチホップ マルチプロトコル eBGP は、個々の自律システムのルート リフレクタ全体に IPv6 VPN ルートを再配布します。PE へのラベル付き IPv4 ルートは（6VPE の場合）、完全なラベル付きスイッチ パスがエンドツーエンドで設定されるように、ASBR 全体にアドバタイズされる必要があります。

Carrier Supporting Carrier

CSC 機能はカスタマー サービス プロバイダーに VPN アクセスを提供します。そのため、このサービスでは ISP MPLS バックボーンを介してルートを交換し、トラフィックを送信する必要があります。通常の PE との唯一の違いは、CSC-CE から CSC-PE へのインターフェイス上に、IP から MPLS への転送ではなく MPLS から MPLS への転送を提供することです。

図 5 に、2 つの ISP のインターフェイスの重要点を示します。

図 5　　CSC 6VPE の設定例



IPv6 用の BGP-MPLS VPN に CSC を設定する方法については、「IPv6 VPN 用の CSC の設定」（P.45）を参照してください。

IPv6 VPN over MPLS の実装方法

IPv6 用の仮想ルーティングおよび転送インスタンスの設定

VRF は、サポートされているアドレス ファミリごとにイネーブルにしたり設定したりできる、アドレス ファミリ非依存のオブジェクトです。VRF の設定は、次の 3 つの手順で構成されています。

1. VRF のアドレス ファミリ非依存部分の設定
2. VRF を使用するための IPv4 のイネーブル化および設定
3. VRF を使用するための IPv6 のイネーブル化および設定

VRF には名前および RD が与えられます。RD は特定の BGP アドレス ファミリのコンテキスト内にある重複するアドレスを区別するために使用されるものですが、アドレス ファミリのコンテキスト外で設定されます。IPv4 VPN アドレスと IPv6 VPN アドレスとで別々の RD を持っていても問題はありません。Cisco ルータでは、設定および VPN 管理を簡素化するために RD は同じになっています。

アドレス ファミリ コンテキストを使用していない場合、ユーザは IPv4 と IPv6 間で共通のポリシーを設定できます。この機能はルート ターゲット（インポートおよびエクスポート）共有であり、IPv4 ポリシーがすでに設定済みで、IPv6 ポリシーを IPv4 ポリシーと同じようにする必要がある移行シナリオで役立ちます。

IPv4 および IPv6 アドレス ファミリは、それぞれ個別にイネーブル化したり設定したりできます。このレベルで入力したルート ターゲット ポリシーは、アドレス ファミリ非依存の設定時に指定されている可能性のあるグローバル ポリシーに優先することに注意してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **mls ipv6 vrf**
4. **vrf definition** *vrf-name*
5. **rd** *route-distinguisher*
6. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
7. **address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*]
8. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
9. **exit**
10. **address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast**]
11. **route-target** {**import** | **export** | **both**} *route-target-ext-community*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**mls ipv6 vrf** **例：** `Router(config)# mls ipv6 vrf`	VRF 内で IPv6 をグローバルにイネーブルにします。
ステップ 4	**vrf definition** *vrf-name* **例：** `Router(config)# vrf definition vrf1`	VPN VRF ルーティング テーブルを設定し、VRF コンフィギュレーション モードを開始します。
ステップ 5	**rd** *route-distinguisher* **例：** `Router(config-vrf)# rd 100:1`	VRF の RD を指定します。
ステップ 6	**route-target** {**import** | **export** | **both**} *route-target-ext-community* **例：** `Router(config-vrf)# route target import 100:10`	IPv4 と IPv6 の両方のルート ターゲット VPN 拡張コミュニティを指定します。
ステップ 7	**address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] **例：** `Router(config)# address-family ipv4`	アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィクスを使用するルーティング セッションを設定します。
ステップ 8	**route-target** {**import** | **export** | **both**} *route-target-ext-community* **例：** `Router(config-vrf-af)# route target import 100:11`	IPv4 固有のルート ターゲット VPN 拡張コミュニティを指定します。
ステップ 9	**exit** **例：** `Router(config-vrf-af)# exit`	この VRF のアドレス ファミリ コンフィギュレーション モードを終了します。
ステップ 10	**address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast**] **例：** `Router(config-vrf)# address-family ipv6`	標準 IPv6 アドレス プレフィクスを使用する BGP などのルーティング セッションを設定するために、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 11	**route-target** {**import** | **export** | **both**} *route-target-ext-community* **例：** `Router(config-vrf-af)# route target import 100:12`	IPv6 固有のルート ターゲット VPN 拡張コミュニティを指定します。

インターフェイスへの VRF のバインド

次の作業では、VRF をインターフェイスにバインドする方法を示します。どのインターフェイスがどの VRF に属するかを指定するために、IPv4 と IPv6 の両方に対して **vrf forwarding** コマンドを使用します。インターフェイスは、複数の VRF に属すことはできません。インターフェイスが VRF にバインドされると、以前に設定したアドレス（IPv4 および IPv6）は削除されるため、再設定が必要になります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **vrf forwarding** *vrf-name*
5. **ip address** *ip-address mask* [**secondary**]
6. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface Ethernet 0/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**vrf forwarding** *vrf-name* **例：** `Router(config-if)# vrf forwarding vrf1`	VPN VRF をインターフェイスまたはサブインターフェイスに関連付けます。 このコマンドを入力する前に設定されていたアドレス（IPv4 または IPv6）はすべて削除されることに注意してください。
ステップ 5	**ip address** *ip-address mask* [**secondary**] **例：** `Router(config-if)# ip address 10.10.10.1 255.255.255.0`	インターフェイスに IPv4 アドレスを設定します。
ステップ 6	**ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*} **例：** `Router(config-if)# ipv6 address 2001:DB8:100:1::1/64`	インターフェイスに IPv6 アドレスを設定します。

PE から CE へのルーティングのためのスタティック ルートの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 route** [**vrf** *vrf-name*] *ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [**nexthop-vrf** [*vrf-name1* | **default**]] [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [*next-hop-address*] [**tag** *tag*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 route** [**vrf** *vrf-name*] *ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [**nexthop-vrf** [*vrf-name1* | **default**]] [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [*next-hop-address*] [**tag** *tag*] **例：** `Router(config)# ipv6 route vrf vrf1 ::/0 2001:DB8:200::1 nexthop-vrf default`	指定したネクストホップを使用して、指定した IPv6 スタティック ルートをインストールします。

eBGP の PE から CE へのルーティング セッションの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast**]
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number*
6. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 100`	BGP ルーティング プロセスを設定します。
ステップ 4	**address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast**] **例：** `Router(config-router)# address-family ipv6 vrf vrf1`	アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number* **例：** `Router(config-router-af)# neighbor 2001:DB8:100:1::2 remote-as 200`	マルチプロトコル BGP ネイバーテーブルにエントリを追加します。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** **例：** `Router(config-router-af)# neighbor 2001:DB8:100:1::2 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。

iBGP 用の IPv6 VPN アドレス ファミリの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number*
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number*
6. **address-family vpnv6** [**unicast**]
7. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**

8. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]
9. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 100`	BGP ルーティング プロセスを設定します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number* **例：** `Router(config-router)# neighbor 192.168.2.11 remote-as 100`	マルチプロトコル BGP ネイバーテーブルにエントリを追加します。 • IPv6 VPN の場合、BGP セッションを IPv4 ベースのコア ネットワークで転送できるようにするために、ピア アドレスは一般的に IPv4 アドレスになります。
ステップ 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number* **例：** `Router(config-router)# neighbor 192.168.2.11 update-source Loopback 0`	BGP セッションで、指定したインターフェイスの送信元アドレスを使用できるようにします。
ステップ 6	**address-family vpnv6** [**unicast**] **例：** `Router(config-router)# address-family vpnv6`	ルーティング セッションを設定するために、ルータをアドレス ファミリ コンフィギュレーション モードに設定します。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** **例：** `Router(config-router-af)# neighbor 192.168.2.11 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。

	コマンドまたはアクション	目的
ステップ 8	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**] **例：** `Router(config-router-af)# neighbor 192.168.2.11 send-community extended`	コミュニティ アトリビュートを BGP ネイバーに送信する必要があることを指定します。
ステップ 9	**exit** **例：** `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了します。

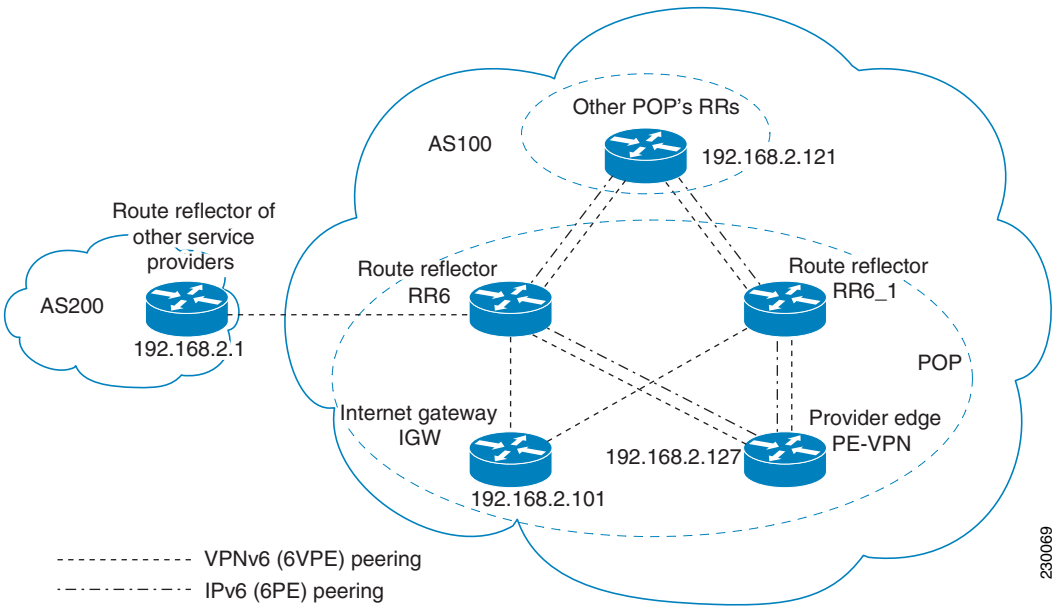
スケーラビリティ向上のためのルート リフレクタの設定

RR を配置すると、BGP セッションの数が大幅に削減され、これによりスケーラビリティが向上します。通常、1 つの RR が多数の iBGP スピーカーとピアリングして、BGP セッションの完全メッシュが防止されます。

MPLS ベースのコアの場合、RR はラベル スイッチ パスの一部ではないため、ネットワーク内の任意の場所に配置できます。たとえば、フラットな RR 設計では、RR はレベル 1 の Point of Presence（POP）に配置でき、完全メッシュ トポロジで互いにピアリングします。階層型の RR 設計では、RR はレベル 1 とレベル 2 の POP に配置でき、レベル 1 POP で互いにピアリングし、レベル 2 の RR ともピアリングします。

既存の MPLS ネットワーク（つまり、VPNv4 サービスを提供するネットワーク）に 6VPE を配置する一般的なケースでは、一部の RR 設計がすでに実施されている可能性が高く、IPv6 VPN サービス用に同様の RR インフラストラクチャを配置できます。図 6 に、ISP POP 内の RR とその RR クライアント セット間の主なピアリング ポイントを示します。

図 6　　ルート リフレクタのピアリング設計



この作業では、冗長性の理由から 2 つの RR が設定されていることに注意してください。

次のリストの BGP RR クライアントを、各 POP の IPv6 RR（図 6 の RR6 および RR6_1）ルータごとに設定する必要があります。

- ISP カスタマーに IPv6 VPN アクセスを提供する POP の PE ルータ（PE-VPN）。これには、カスタマー サイトを相互接続するための IPv6 VPN（6VPE）ピアリングと、VPN カスタマーにインターネット アクセスを提供するための IPv6 ピアリング（6PE）の両方が含まれます（「インターネット アクセスの設定」（P.22）を参照）。
- PE カスタマーに IPv6 インターネットへのアクセスを提供するために、POP 内に配置される Internet Gateway（IGW; インターネット ゲートウェイ）（「インターネット アクセスの設定」（P.22）を参照）。
- 他のサービス プロバイダーの RR。この機能は、相互自律システムの接続を提供するために使用されるもので、IPv6 と IPv6 VPN ピアリングの両方が含まれます。このサービスについては、「IPv6 VPN 用のマルチ自律システム バックボーンの設定」（P.30）で説明しています。
- 他の POP 内の RR。IPv6 と IPv6 VPN の両方のアドレス ファミリがイネーブルになっている場合、すべての RR が互いにピアリングします。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number*
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number*
6. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number*
7. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number*
8. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number*
9. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number*
10. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number*
11. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number*
12. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **ebgp-multihop** [*ttl*]
13. **address-family ipv6**
14. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
15. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label**
16. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client**
17. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
18. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label**
19. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client**
20. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
21. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label**
22. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client**

23. **exit**
24. **address-family vpnv6** [**unicast**]
25. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
26. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]
27. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client**
28. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
29. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]
30. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client**
31. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
32. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]
33. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client**
34. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **next-hop-unchanged** [**allpaths**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 100`	BGP ルーティング プロセスを設定します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number* **例：** `Router(config-router)# neighbor 192.168.2.101 remote-as 100`	マルチプロトコル BGP ネイバーテーブルにエントリを追加して、インターネット アクセスを提供するためにインターネット ゲートウェイとのピアリングを提供します。
ステップ 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number* **例：** `Router(config-router)# neighbor 192.168.2.101 update-source Loopback 0`	BGP セッションで、指定したインターフェイスの送信元アドレスを使用できるようにします。

	コマンドまたはアクション	目的
ステップ 6	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number* **例：** `Router(config-router)# neighbor 192.168.2.121 remote-as 100`	マルチプロトコル BGP ネイバーテーブルにエントリを追加して、他の POP の RR とのピアリングを提供します。
ステップ 7	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number* **例：** `Router(config-router)# neighbor 192.168.2.121 update-source Loopback 0`	BGP セッションで、指定したインターフェイスの送信元アドレスを使用できるようにします。
ステップ 8	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number* **例：** `Router(config-router)# neighbor 192.168.2.127 remote-as 100`	マルチプロトコル BGP ネイバーテーブルにエントリを追加します。
ステップ 9	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number* **例：** `Router(config-router)# neighbor 192.168.2.127 update-source Loopback 0`	BGP セッションで、指定したインターフェイスの送信元アドレスを使用できるようにします。
ステップ 10	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number* **例：** `Router(config-router)# neighbor 192.168.2.1 remote-as 200`	（任意）マルチプロトコル BGP ネイバーテーブルにエントリを追加して、VPN 間サービスを提供するためにピア ISP の RR とのピアリングを提供します。
ステップ 11	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number* **例：** `Router(config-router)# neighbor 192.168.2.1 update-source Loopback 0`	（任意）BGP セッションで、指定したインターフェイスの送信元アドレスを使用できるようにします。
ステップ 12	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **ebgp-multihop** [*ttl*] **例：** `Router(config-router)# neighbor 192.168.2.1 ebgp-multihop`	（任意）直接接続されていないネットワーク上の外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。
ステップ 13	**address-family ipv6** **例：** `Router(config-router)# address-family ipv6`	（任意）インターネット アクセス サービスを提供するために、アドレス ファミリ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 14	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** **例：** `Router(config-router-af)# neighbor 192.168.2.101 activate`	（任意）このアドレス ファミリの情報を、指定したネイバーと交換できるようにします。
ステップ 15	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** **例：** `Router(config-router-af)# neighbor 192.168.2.101 send-label`	（任意）BGP ルートとともに MPLS ラベルをネイバー BGP ルータに送信できるように BGP ルータを設定します。
ステップ 16	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client** **例：** `Router(config-router-af)# neighbor 192.168.2.101 route-reflector-client`	（任意）ルータを BGP ルート リフレクタとして設定し、指定したネイバーをそのクライアントとして設定します。
ステップ 17	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** **例：** `Router(config-router-af)# neighbor 192.168.2.121 activate`	（任意）このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 18	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** **例：** `Router(config-router-af)# neighbor 192.168.2.121 send-label`	（任意）BGP ルートとともに MPLS ラベルをネイバー BGP ルータに送信できるように BGP ルータを設定します。
ステップ 19	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client** **例：** `Router(config-router-af)# neighbor 192.168.2.121 route-reflector-client`	（任意）指定したネイバーをルート リフレクタ クライアントとして設定します。
ステップ 20	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** **例：** `Router(config-router-af)# neighbor 192.168.2.127 activate`	（任意）このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 21	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** **例：** `Router(config-router-af)# neighbor 192.168.2.127 send-label`	（任意）BGP ルートとともに MPLS ラベルをネイバー BGP ルータに送信できるように BGP ルータを設定します。

	コマンドまたはアクション	目的
ステップ 22	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client** **例：** Router(config-router-af)# neighbor 192.168.2.127 route-reflector-client	（任意）指定したネイバーをルート リフレクタ クライアントとして設定します。
ステップ 23	**exit** **例：** Router(config-router-af)# exit	（任意）アドレス ファミリ コンフィギュレーション モードを終了します。
ステップ 24	**address-family vpnv6** [**unicast**] **例：** Router(config-router)# address-family vpnv6	ルーティング セッションを設定するために、ルータをアドレス ファミリ コンフィギュレーション モードに設定します。
ステップ 25	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** **例：** Router(config-router-af)# neighbor 192.168.2.121 activate	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 26	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**] **例：** Router(config-router-af)# neighbor 192.168.2.21 send-community extended	コミュニティ アトリビュートを BGP ネイバーに送信する必要があることを指定します。
ステップ 27	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client** **例：** Router(config-router-af)# neighbor 192.168.2.121 route-reflector-client	指定したネイバーをルート リフレクタ クライアントとして設定します。
ステップ 28	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** **例：** Router(config-router-af)# neighbor 192.168.2.127 activate	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 29	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**] **例：** Router(config-router-af)# neighbor 192.168.2.127 send-community extended	コミュニティ アトリビュートを BGP ネイバーに送信する必要があることを指定します。
ステップ 30	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client** **例：** Router(config-router-af)# neighbor 192.168.2.127 route-reflector-client	指定したネイバーをルート リフレクタ クライアントとして設定します。

	コマンドまたはアクション	目的
ステップ 31	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** **例：** `Router(config-router-af)# neighbor 192.168.2.1 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 32	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**] **例：** `Router(config-router-af)# neighbor 192.168.2.1 send-community extended`	コミュニティ アトリビュートを BGP ネイバーに送信する必要があることを指定します。
ステップ 33	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client** **例：** `Router(config-router-af)# neighbor 192.168.2.1 route-reflector-client`	指定したネイバーをルート リフレクタ クライアントとして設定します。
ステップ 34	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **next-hop-unchanged** [**allpaths**] **例：** `Router(config-router-af)# neighbor 192.168.2.1 next-hop-unchanged allpaths`	EBGP マルチホップ ピアで、パスのネクストホップを変更せずに伝播できるようにします。

インターネット アクセスの設定

大部分の VPN カスタマーは IPv4 インターネットにアクセスできます。IPv6 VPN にアクセスするカスタマーの場合は、IPv6 インターネットにアクセスできる必要があります。このサービスの設計は、グローバル インターネット アクセス サービスと似ています。レベル 1 POP に配置されている 6VPE ルータ（IGW ルータと共存）はネイティブに IGW にアクセスできますが、レベル 2 およびレベル 3 POP に配置されている、IGW に直接アクセスできない 6VPE ルータは、6PE を介して最も近いレベル 1 POP の IGW にアクセスできます。

このような 6VPE ルータで VPN インターネット アクセスを設定するには、IGW との BGP ピアリングの設定が必要になります（多くの場合、「スケーラビリティ向上のためのルート リフレクタの設定」の項で説明したように、IPv6 RR を使用します）。次に、ユーザは、プライベート ドメイン（VRF）とパブリック ドメイン（インターネット）間の通信をイネーブルにするように、相互テーブル ルーティングを設定する必要があります。

図 3 に、次の設定作業が示されています。

- 「インターネット ゲートウェイの設定」（P.22）
- 「IPv6 VPN PE の設定」（P.26）

インターネット ゲートウェイの設定

インターネット アクセス用のインターネット ゲートウェイの設定は、次の作業で構成されます。

- 「VPN PE への iBGP 6PE ピアリングの設定」（P.23）

- 「パブリック ドメインへのゲートウェイとしてのインターネット ゲートウェイの設定」（P.24）
- 「インターネットへの eBGP ピアリングの設定」（P.25）

VPN PE への iBGP 6PE ピアリングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number*
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number*
6. **address-family ipv6**
7. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
8. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 100`	BGP ルーティング プロセスを設定します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number* **例：** `Router(config-router)# neighbor 192.168.2.127 remote-as 100`	マルチプロトコル BGP ネイバーテーブルにエントリを追加して、VPN PE とのピアリングを提供します。
ステップ 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number* **例：** `Router(config-router)# neighbor 192.168.2.127 update-source Loopback 0`	BGP セッションで、指定したインターフェイスの送信元アドレスを使用できるようにします。

	コマンドまたはアクション	目的
ステップ 6	**address-family ipv6** **例：** `Router(config-router)# address-family ipv6`	グローバル テーブルの到達可能性を交換するために、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** **例：** `Router(config-router-af)# neighbor 192.168.2.127 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 8	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** **例：** `Router(config-router-af)# neighbor 192.168.2.127 send-label`	BGP ルートとともに MPLS ラベルをネイバー BGP ルータに送信できるように BGP ルータを設定して、PE VPN が MPLS を介してインターネット ゲートウェイに到達できるようにします。

パブリック ドメインへのゲートウェイとしてのインターネット ゲートウェイの設定

次の作業は、「VPN PE への iBGP 6PE ピアリングの設定」（P.23）で確立した 6PE ピアリング設定を使用して、パブリック ドメインへのゲートウェイになるようにゲートウェイを設定する方法を示しています。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv6**
5. **network** *ipv6-address*/*prefix-length*
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 100`	BGP ルーティング プロセスを設定します。

	コマンドまたはアクション	目的
ステップ 4	**address-family ipv6** **例：** `Router(config-router)# address-family ipv6`	グローバル テーブルの到達可能性を交換するために、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**network** *ipv6-address*/*prefix-length* **例：** `Router(config-router-af)# network 2001:DB8:100::1/128`	PE VPN によって使用されるネクストホップのネットワーク ソースを設定します。
ステップ 6	**exit** **例：** `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了します。

インターネットへの eBGP ピアリングの設定

次の作業では、グローバル テーブルに値を格納するようにインターネットへの eBGP ピアリングを設定する方法を示します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number*
5. **address-family ipv6**
6. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
7. **aggregate-address** *address mask* [**as-set**] [**summary-only**] [**suppress-map** *map-name*] [**advertise-map** *map-name*] [**attribute-map** *map-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 100`	BGP ルーティング プロセスを設定します。

	コマンドまたはアクション	目的
ステップ 4	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number* **例：** `Router(config-router)# neighbor FE80::300::1%Ethernet0/0 remote-as 300`	マルチプロトコル BGP ネイバーテーブルにエントリを追加して、PE（PE-VPN）とのピアリングを提供します。 • ピアリングは、リンクローカル アドレス経由で行われることに注意してください。
ステップ 5	**address-family ipv6** **例：** `Router(config-router)# address-family ipv6`	グローバル テーブルの到達可能性を交換するために、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** **例：** `Router(config-router-af)# neighbor FE80::300::1%Ethernet0/0 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 7	**aggregate-address** *address mask* [**as-set**] [**summary-only**] [**suppress-map** *map-name*] [**advertise-map** *map-name*] [**attribute-map** *map-name*] **例：** `Router(config-router-af)# aggregate-address 2001:DB8::/32 summary-only`	集約プレフィクスを作成してから、インターネットにアドバタイズします。

IPv6 VPN PE の設定

インターネット アクセス用の IPv6 VPN PE の設定は、次の作業で構成されます。

- 「VRF からインターネット ゲートウェイへのデフォルト スタティック ルートの設定」（P.26）
- 「デフォルト テーブルから VRF へのスタティック ルートの設定」（P.27）
- 「インターネット ゲートウェイへの iBGP 6PE ピアリングの設定」（P.28）

VRF からインターネット ゲートウェイへのデフォルト スタティック ルートの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 route** [**vrf** *vrf-name*] *ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [**nexthop-vrf** [*vrf-name1* | **default**]] [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [*next-hop-address*] [**tag** *tag*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 route** [**vrf** *vrf-name*] *ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [**nexthop-vrf** [*vrf-name1* | **default**]] [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [*next-hop-address*] [**tag** *tag*] **例：** `Router(config)# ipv6 route vrf vrf1 ::/0 2001:DB8:100::1 nexthop-vrf default`	発信トラフィックを VRF から発信できるようにするために、VRF からインターネット ゲートウェイへのデフォルト スタティック ルートを設定します。

デフォルト テーブルから VRF へのスタティック ルートの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 route** [**vrf** *vrf-name*] *ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [**nexthop-vrf** [*vrf-name1* | **default**]] [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [*next-hop-address*] [**tag** *tag*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 route** [**vrf** *vrf-name*] *ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [**nexthop-vrf** [*vrf-name1* | **default**]] [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [*next-hop-address*] [**tag** *tag*] **例：** `Router(config)# ipv6 route 2001:DB8:100:2000::/64 nexthop-vrf vrf1`	着信トラフィックが VRF に到達できるようにするために、デフォルト テーブルから VRF へのスタティック ルートを設定します。

インターネット ゲートウェイへの iBGP 6PE ピアリングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number*
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number*
6. **address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast**]
7. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
8. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label**
9. **network** *ipv6-address*/*prefix-length*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 100`	BGP ルーティング プロセスを設定します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number* **例：** `Router(config-router)# neighbor 192.168.2.101 remote-as 100`	インターネット ゲートウェイとピアリングするために、マルチプロトコル BGP ネイバーテーブルにエントリを追加します。
ステップ 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number* **例：** `Router(config-router)# neighbor 192.168.2.101 update-source Loopback 0`	BGP セッションで、指定したインターフェイスの送信元アドレスを使用できるようにします。
ステップ 6	**address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast**] **例：** `Router(config-router)# address-family ipv6`	グローバル テーブルの到達可能性を交換するために、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** **例：** `Router(config-router-af)# neighbor 192.168.2.101 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 8	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** **例：** `Router(config-router-af)# neighbor 192.168.2.101 send-label`	VPN PE が MPLS を介してインターネット ゲートウェイに到達できるようにするために、このネイバーに対するこのアドレス ファミリのラベル交換をイネーブルにします。
ステップ 9	**network** *ipv6-address*/*prefix-length* **例：** `Router(config-router-af)# network 2001:DB8:100:2000::/64`	VRF プレフィクスをインターネット ゲートウェイに提供します。

IPv6 VPN 用のマルチ自律システム バックボーンの設定

たとえば、VPN の 2 つのサイトが異なるサービス プロバイダーに接続されているために、それぞれ別の自律システムに接続されることがあります。この場合、その VPN に接続されている PE ルータは、iBGP 接続を互いに維持したり、共通のルート リフレクタを使用して維持したりすることはできません。このような状況では、eBGP を使用して VPN-IPv6 アドレスを配布するには、何らかの方法が必要となります。

次に、2 つのシナリオでの設定例を示します。1 つは、ASBR 間のマルチプロトコル eBGP-IPv6 VPN ピアリングで IPv4 リンクを使用し、もう 1 つは同じピアリングで IPv6 リンクを使用します。ASBR 間のピアリングが IPv4 リンク経由で実行される場合、ASBR1 の BGP 設定は次のようになります。

```
router bgp 1001
 no bgp default ipv4-unicast
 no bgp default route-target filter
 neighbor 192.1.1.1 remote-as 1002
 neighbor 192.168.2.11 remote-as 1001
 neighbor 192.168.2.11 update-source Loopback1
 !
 address-family vpnv6
!Peering to ASBR2 over an IPv4 link
 neighbor 192.1.1.1 activate
 neighbor 192.1.1.1 send-community extended
!Peering to PE1 over an IPv4 link
 neighbor 192.168.2.11 activate
 neighbor 192.168.2.11 next-hop-self
 neighbor 192.168.2.11 send-community extended
```

ASBR 間のピアリングが IPv6 リンク経由で実行される場合、ASBR1 の BGP 設定は次のようになります。

```
router bgp 1001
neighbor 2001:DB8:101::72d remote-as 1002
!
 address-family vpnv6
!Peering to ASBR2 over an IPv6 link
 neighbor 2001:DB8:101::72d activate
 neighbor 2001:DB8:101::72d send-community extended
```

次の複数の作業は、マルチホップ マルチプロトコル eBGP を使用して個々の自律システムの RR 全体に VPN ルートを再配布する、マルチ自律システム バックボーン用の PE VPN を設定する方法を示しています。PE へのラベル付き IPv4 ルートは、完全な Label Switch Path（LSP; ラベル スイッチ パス）がエンドツーエンドで設定されるように、ASBR 全体にアドバタイズされます。

このシナリオでは、ASBR は VPN 対応ではなく、RR だけが VPN 対応になっています。次の設定を有効にし、かつ理解しておく必要があります。

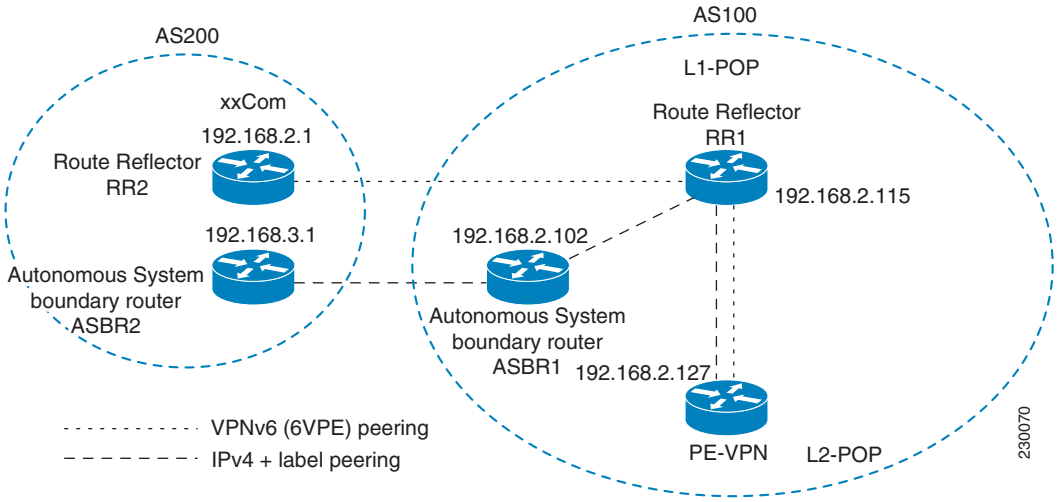
- ASBR では、ピアリングするサービス プロバイダーに PE のループバック アドレスを提供しています。提供される内容は次のとおりです。
  - リモート サービス プロバイダーのロケーションでネクストホップ解決をイネーブルにするための、VPN PE の IPv4 ループバック アドレス（/32）
  - プロバイダー間（RR 間）eBGP ピアリングをイネーブルにするための、VPN RR の IPv4 ループバック アドレス（/32）
- VPN PE の IPv4 ループバック アドレスの場合、ラベルがエンドツーエンド LSP を確立するように、アドレス提供は、ラベルとともにリモート PE までマルチプロトコル BGP を介して実行されます。そのため、次の MP-BGP ピアリングが VPNv4 用に設定されています。
  - VPN PE は VPN RR と iBGP ピアリングする。
  - ASBR は VPN RR と iBGP ピアリングする。

  - ASBR はリモート サービス プロバイダーの ASBR と eBGP ピアリングする。
- 各サービス プロバイダーの VPN RR は、eBGP を介して互いにピアリングして、VPN ルートを交換します。エンドツーエンド LSP が RR 経由にならないように、ネクストホップは変更せずに転送されます。

このシナリオで IPv6 VPN 相互自律システム アクセスをイネーブルにするには、ISP 側で PE VPN および RR での設定を変更する必要があります。同様のサービスを VPNv4 に提供するには、同じ RR を設定します。この場合、RR と ASBR 間のピアリングおよび ASBR 間のピアリングは IPv4 VPN と IPv6 VPN の両方で使用される IPv4 ネクストホップのラベルを交換するだけなので、ASBR は完全に IPv6 非対応のままであり、ここで必要な設定変更はありません。

図 7 に、PE-VPN ルータ（IPv6 VPN アクセスを提供）から xxCom ネットワークへの IPv6 プロバイダー間接続をイネーブルにするために必要な BGP ピアリング ポイントを示します。

図 7　　InterAS シナリオ C をイネーブルにするための BGP ピアリング ポイント



次に、レベル 2 POP に配置されている IPv6 VPN PE からの相互自律システム通信をイネーブルにするために必要となる、その他の BGP ピアリングのリストを示します。

- PE VPN から RR1 という名前のルート リフレクタへの、ラベルを伴う IPv4 ピアリング（VPNv4 interAS が、同じ LSP を使用して同じノードに配置されている場合は、すでに設定済み）
- RR1 から ASBR1 への、ラベルを伴う IPv4 ピアリング
- ASBR1 と ASBR1 間の、ラベルを伴う IPv4 ピアリング
- IPv6 VPN ルートを交換するための、RR1 と RR2（他の自律システムのルート リフレクタ）間の IPv6 VPN ピアリング
- RR1 との IPv6 VPN ピアリング IPv6 VPN サービスを拡張するために使用されているそのルート リフレクタが自律システム機能に使用されている場合、この機能もまたすでに設定済みである可能性があります（「スケーラビリティ向上のためのルート リフレクタの設定」（P.16）を参照）。

IPv6 VPN 用のマルチ自律システム バックボーンの設定は、次の手順で構成されます。

1. 「マルチ自律システム バックボーン用の PE VPN の設定」（P.32）
2. 「マルチ自律システム バックボーン用のルート リフレクタの設定」（P.34）
3. 「ASBR の設定」（P.42）

マルチ自律システム バックボーン用の PE VPN の設定

マルチ自律システム バックボーン用の PE VPN の設定は、次の作業で構成されます。

- 「ルート リフレクタへの iBGP IPv6 VPN ピアリングの設定」（P.32）
- 「ルート リフレクタへの IPv4 とラベルの iBGP ピアリングの設定」（P.33）

ルート リフレクタへの iBGP IPv6 VPN ピアリングの設定

次の作業では、RR1 という名前のルート リフレクタへの iBGP IPv6 VPN ピアリングを設定する方法を示します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number*
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number*
6. **address-family vpnv6** [**unicast**]
7. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
8. **neighbor** {*ip-address* | *ipv6-address* | **peer-group-name**} **send-community** [**both** | **standard** | **extended**]
9. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 100`	BGP ルーティング プロセスを設定します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number* **例：** `Router(config-router)# neighbor 192.168.2.115 remote-as 100`	相互自律システム機能を備えたルート リフレクタとピアリングするために、マルチプロトコル BGP ネイバーテーブルにエントリを追加します。

	コマンドまたはアクション	目的
ステップ 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number* **例：** `Router(config-router)# neighbor 192.168.2.115 update-source Loopback 0`	BGP セッションで、指定したインターフェイスの送信元アドレスを使用できるようにします。
ステップ 6	**address-family vpnv6** [**unicast**] **例：** `Router(config-router)# address-family vpnv6`	（任意）ルーティング セッションを設定するために、ルータをアドレス ファミリ コンフィギュレーション モードに設定します。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** **例：** `Router(config-router-af)# neighbor 192.168.2.115 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 8	**neighbor** {*ip-address* | *ipv6-address* | ***peer-group-name***} **send-community** [**both** | **standard** | **extended**] **例：** `Router(config-router-af)# neighbor 192.168.2.115 send-community extended`	コミュニティ アトリビュートを BGP ネイバーに送信する必要があることを指定します。
ステップ 9	**exit** **例：** `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了します。

ルート リフレクタへの IPv4 とラベルの iBGP ピアリングの設定

次の作業では、RR1 という名前のルート リフレクタへの IPv4 とラベルの iBGP ピアリングを設定する方法を示します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*]
5. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
6. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 100`	BGP ルーティング プロセスを設定します。
ステップ 4	**address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] **例：** `Router(config-router)# address-family ipv4`	アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィクスを使用するルーティング セッションを設定します。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** **例：** `Router(config-router-af)# neighbor 192.168.2.115 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 6	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** **例：** `Router(config-router-af)# neighbor 192.168.2.115 send-label`	エンドツーエンド LSP を設定するためのラベルとともにリモート PE ピア IPv4 ループバックを RR1 経由で受信するために、このネイバーに対するこのアドレス ファミリのラベル交換をイネーブルにします。

マルチ自律システム バックボーン用のルート リフレクタの設定

- 「PE VPN へのピアリングの設定」（P.34）
- 「ルート リフレクタの設定」（P.36）
- 「自律システム境界ルータへのピアリングの設定」（P.38）
- 「別の ISP のルート リフレクタへのピアリングの設定」（P.40）

PE VPN へのピアリングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number*

5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number*
6. **address-family vpnv6** [**unicast**]
7. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
8. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]
9. **exit**
10. **address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*]
11. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
12. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label**
13. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 100`	BGP ルーティング プロセスを設定します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number* **例：** `Router(config-router)# neighbor 192.168.2.115 remote-as 100`	InterAS 用のルート リフレクタとピアリングするために、マルチプロトコル BGP ネイバーテーブルにエントリを追加します。
ステップ 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number* **例：** `Router(config-router)# neighbor 192.168.2.115 update-source Loopback 0`	BGP セッションで、指定したインターフェイスの送信元アドレスを使用できるようにします。
ステップ 6	**address-family vpnv6** [**unicast**] **例：** `Router(config-router)# address-family vpnv6`	（任意）ルータをアドレス ファミリ コンフィギュレーション モードに設定します。

	コマンドまたはアクション	目的
ステップ 7	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** **例：** `Router(config-router-af)# neighbor 192.168.2.115 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 8	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**] **例：** `Router(config-router-af)# neighbor 192.168.2.115 send-community extended`	コミュニティ アトリビュートを BGP ネイバーに送信する必要があることを指定します。
ステップ 9	**exit** **例：** `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了します。
ステップ 10	**address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] **例：** `Router(config-router)# address-family ipv4`	アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィクスを使用するルーティング セッションを設定します。
ステップ 11	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** **例：** `Router(config-router-af)# neighbor 192.168.2.115 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 12	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** **例：** `Router(config-router-af)# neighbor 192.168.2.115 send-label`	エンドツーエンド LSP を設定するためのラベルとともにリモート PE IPv4 ループバックをローカル PE に送信するために、このネイバーに対するこのアドレス ファミリのラベル交換をイネーブルにします。
ステップ 13	**exit** **例：** `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了します。

ルート リフレクタの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number*
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number*

6. **address-family vpnv6** [**unicast**]
7. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
8. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]
9. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client**
10. **exit**
11. **address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*]
12. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
13. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label**
14. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 100`	BGP ルーティング プロセスを設定します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number* **例：** `Router(config-router)# neighbor 192.168.2.127 remote-as 100`	InterAS 用の VPN PE とピアリングするために、マルチプロトコル BGP ネイバーテーブルにエントリを追加します。
ステップ 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number* **例：** `Router(config-router)# neighbor 192.168.2.127 update-source Loopback 0`	BGP セッションで、指定したインターフェイスの送信元アドレスを使用できるようにします。
ステップ 6	**address-family vpnv6** [**unicast**] **例：** `Router(config-router)# address-family vpnv6`	（任意）ルータをアドレス ファミリ コンフィギュレーション モードに設定します。

	コマンドまたはアクション	目的
ステップ 7	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** **例：** `Router(config-router-af)# neighbor 192.168.2.127 activate`	このアドレス ファミリの情報を、指定したネイバーと交換できるようにします。
ステップ 8	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**] **例：** `Router(config-router-af)# neighbor 192.168.2.127 send-community extended`	コミュニティ アトリビュートを BGP ネイバーに送信する必要があることを指定します。
ステップ 9	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client** **例：** `Router(config-router-af)# neighbor 192.168.2.127 route-reflector-client`	指定したネイバーをルート リフレクタ クライアントとして設定します。
ステップ 10	**exit** **例：** `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了します。
ステップ 11	**address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] **例：** `Router(config-router)# address-family ipv4`	アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィクスを使用するルーティング セッションを設定します。
ステップ 12	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** **例：** `Router(config-router-af)# neighbor 192.168.2.127 activate`	このアドレス ファミリの情報を、指定したネイバーと交換できるようにします。
ステップ 13	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** **例：** `Router(config-router-af)# neighbor 192.168.2.127 send-label`	エンドツーエンド LSP を設定するためのラベルとともにリモート PE IPv4 ループバックをローカル PE に送信するために、このネイバーに対するこのアドレス ファミリのラベル交換をイネーブルにします。
ステップ 14	**exit** **例：** `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了します。

自律システム境界ルータへのピアリングの設定

次の作業では、ASBR1 という名前の Autonomous System Boundary Router（ASBR; 自律システム境界ルータ）へのピアリングを設定する方法を示します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number*
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number*
6. **address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*]
7. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
8. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label**
9. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 100`	BGP ルーティング プロセスを設定します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number* **例：** `Router(config-router)# neighbor 192.168.2.102 remote-as 100`	ASBR1 とピアリングするために、マルチプロトコル BGP ネイバーテーブルにエントリを追加します。
ステップ 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number* **例：** `Router(config-router)# neighbor 192.168.2.102 update-source Loopback 0`	BGP セッションで、指定したインターフェイスの送信元アドレスを使用できるようにします。
ステップ 6	**address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] **例：** `Router(config-router)# address-family ipv4`	アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィクスを使用するルーティング セッションを設定します。

	コマンドまたはアクション	目的
ステップ 7	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** **例：** `Router(config-router-af)# neighbor 192.168.2.102 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 8	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** **例：** `Router(config-router-af)# neighbor 192.168.2.102 send-label`	エンドツーエンド LSP を設定するラベルとともにリモート PE IPv4 ループバックを受信するために、このネイバーに対するこのアドレス ファミリのラベル交換をイネーブルにします。
ステップ 9	**exit** **例：** `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了します。

別の ISP のルート リフレクタへのピアリングの設定

次の作業では、RR2 という名前の別の ISP のルート リフレクタへのピアリングを設定する方法を示します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number*
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number*
6. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **ebgp-multihop** [*ttl*]
7. **address-family vpnv6** [**unicast**]
8. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
9. **neighbor** {*ip-address* | *ipv6-address* | **peer-group-name**} **send-community** [**both** | **standard** | **extended**]
10. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **next-hop-unchanged** [**allpaths**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 100`	BGP ルーティング プロセスを設定します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number* **例：** `Router(config-router)# neighbor 192.168.2.1 remote-as 100`	RR2 と eBGP ピアリングするために、マルチプロトコル BGP ネイバーテーブルにエントリを追加します。
ステップ 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number* **例：** `Router(config-router)# neighbor 192.168.2.1 update-source Loopback 0`	BGP セッションで、指定したインターフェイスの送信元アドレスを使用できるようにします。
ステップ 6	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **ebgp-multihop** [*ttl*] **例：** `Router(config-router)# neighbor 192.168.2.1 ebgp-multihop`	（任意）直接接続されていないネットワーク上の外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。
ステップ 7	**address-family vpnv6** [**unicast**] **例：** `Router(config-router)# address-family vpnv6`	（任意）ルーティング セッションを設定するために、ルータをアドレス ファミリ コンフィギュレーション モードに設定します。
ステップ 8	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** **例：** `Router(config-router-af)# neighbor 192.168.2.1 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。

	コマンドまたはアクション	目的
ステップ 9	**neighbor** {*ip-address* | *ipv6-address* | ***peer-group-name***} **send-community** [**both** | **standard** | **extended**] **例：** `Router(config-router-af)# neighbor 192.168.2.1 send-community extended`	コミュニティ アトリビュートを BGP ネイバーに送信する必要があることを指定します。
ステップ 10	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **next-hop-unchanged** [**allpaths**] **例：** `Router(config-router-af)# neighbor 192.168.2.1 next-hop-unchanged allpaths`	eBGP マルチホップ ピアで、パスのネクストホップを変更せずに伝播できるようにします。

ASBR の設定

MultiAS バックボーン用の ASBR の設定は、次の作業で構成されます。

- 「ルート リフレクタ RR1 とのピアリングの設定」（P.42）
- 「他の ISP の ASBR2 とのピアリングの設定」（P.44）

ルート リフレクタ RR1 とのピアリングの設定

次の作業では、RR1 という名前のルート リフレクタとのピアリングを設定する方法を示します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number*
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number*
6. **address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*]
7. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
8. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label**
9. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 100`	BGP ルーティング プロセスを設定します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number* **例：** `Router(config-router)# neighbor 192.168.2.115 remote-as 100`	RR1 とピアリングするために、マルチプロトコル BGP ネイバーテーブルにエントリを追加します。
ステップ 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number* **例：** `Router(config-router)# neighbor 192.168.2.115 update-source Loopback 0`	BGP セッションで、指定したインターフェイスの送信元アドレスを使用できるようにします。
ステップ 6	**address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] **例：** `Router(config-router)# address-family ipv4`	アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィクスを使用するルーティング セッションを設定します。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** **例：** `Router(config-router-af)# neighbor 192.168.2.115 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 8	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** **例：** `Router(config-router-af)# neighbor 192.168.2.115 send-label`	エンドツーエンド LSP を設定するためのラベルとともにリモート PE IPv4 ループバックをローカル PE に送信するために、このネイバーに対するこのアドレス ファミリのラベル交換をイネーブルにします。

ステップ 9	`exit`
	
	例：
	`Router(config-router-af)# exit`
		アドレス ファミリ コンフィギュレーション モードを終了します。

他の ISP の ASBR2 とのピアリングの設定

次の作業では、他の ISP の ASBR（ASBR2）とのピアリングを設定する方法を示します。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number*
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number*
6. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **ebgp-multihop** [*ttl*]
7. **address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*]
8. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
9. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label**
10. **network** {*network-number* [**mask** *network-mask*] | *nsap-prefix*} [**route-map** *map-tag*]
11. **network** {*network-number* [**mask** *network-mask*] | *nsap-prefix*} [**route-map** *map-tag*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 100`	BGP ルーティング プロセスを設定します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number* **例：** `Router(config-router)# neighbor 192.168.3.1 remote-as 100`	ASBR2 とピアリングするために、マルチプロトコル BGP ネイバーテーブルにエントリを追加します。
ステップ 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number* **例：** `Router(config-router)# neighbor 192.168.3.1 update-source Loopback 0`	BGP セッションで、指定したインターフェイスの送信元アドレスを使用できるようにします。

	コマンドまたはアクション	目的
ステップ 6	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **ebgp-multihop** [*ttl*] **例：** `Router(config-router)# neighbor 192.168.3.1 ebgp-multihop`	直接接続されていないネットワーク上の外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。
ステップ 7	**address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] **例：** `Router(config-router)# address-family ipv4`	アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィクスを使用するルーティング セッションを設定します。
ステップ 8	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** **例：** `Router(config-router-af)# neighbor 192.168.3.1 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 9	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** **例：** `Router(config-router-af)# neighbor 192.168.3.1 send-label`	エンドツーエンド LSP を設定するためのラベルとともにリモート PE IPv4 ループバックを受信するために、このネイバーに対するこのアドレス ファミリのラベル交換をイネーブルにします。
ステップ 10	**network** {*network-number* [**mask** *network-mask*] | *nsap-prefix*} [**route-map** *map-tag*] **例：** `Router(config-router-af)# network 192.168.2.27 mask 255.255.255.255`	ネットワークをこの自律システムにローカルとしてフラグして、ネットワークを BGP テーブルに入力します。この設定は PE VPN ループバック用です。
ステップ 11	**network** {*network-number* [**mask** *network-mask*] | *nsap-prefix*} [**route-map** *map-tag*] **例：** `Router(config-router-af)# network 192.168.2.15 mask 255.255.255.255`	ネットワークをこの自律システムにローカルとしてフラグして、ネットワークを BGP テーブルに入力します。この設定は RR1 ループバック用です。

IPv6 VPN 用の CSC の設定

次の作業は、CsC-PE1 の CsC-CE1 とのピアリング設定を指定する方法を示します。

手順の概要

1. **enable**
2. **configure terminal**
3. **hostname** *name*
4. **router bgp** *autonomous-system-number*
5. **address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast**]
6. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number*

7. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
8. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**hostname** *name* **例：** `Router(config)# hostname CSC-PE1`	ネットワーク サーバのホスト名を指定または変更します。
ステップ 4	**router bgp** *autonomous-system-number* **例：** `Router(config)# router bgp 100`	BGP ルーティング プロセスを設定します。
ステップ 5	**address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast**] **例：** `Router(config-router)# address-family ipv6 vrf ISP2`	アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 6	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as** *as-number* **例：** `Router(config-router-af)# neighbor FE80::866C:99%Serial0/0 remote-as 200`	マルチプロトコル BGP ネイバーテーブルにエントリを追加します。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** **例：** `Router(config-router-af)# neighbor FE80::866C:99%Serial0/0 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 8	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** **例：** `Router(config-router-af)# neighbor FE80::866C:99%Serial0/0 send-label`	このネイバーに対するこのアドレス ファミリのラベル交換をイネーブルにします。

IPv6 VPN の確認とトラブルシューティング

ユーザが IPv6 をトラブルシューティングする場合、VPNv4 と同様の働きをする機能は、IPv6 でも機能する可能性が高いため、新しい IPv6 ユーザの学習曲線は最小限に抑えられます。6PE および 6VPE のトラブルシューティングに使用される一部のツールおよびコマンドだけが、IPv6 に固有です。より正確に言うと、トラブルシューティング方法論は IPv4 も IPv6 も同じであり、多くの場合、コマンドおよびツールで異なるのは 1 つのキーワードだけです。

次の作業は、特定のシナリオで IPv6 VPN を確認して問題をトラブルシューティングする方法を示しています。

- 「ルーティングの確認とトラブルシューティング」（P.47）
- 「転送の確認とトラブルシューティング」（P.48）
- 「ルーティングおよび転送のデバッグ」（P.53）

ルーティングの確認とトラブルシューティング

6PE および 6VPE の配置には、主として BGP が関係します。VPNv4 に使用されているコマンド セットと同じコマンドセットを IPv6 にも使用可能であり（引数セットは異なる）、また、同様の出力が得られます。

次の例を使用すると、BGP 配置を確認およびトラブルシューティングできます。

- 「BGP IPv6 アクティビティ サマリー」（P.47）
- 「BGP IPv6 テーブルのダンプ」（P.47）
- 「IPv6 ルーティング テーブルのダンプ」（P.48）

BGP IPv6 アクティビティ サマリー

次に、BGP IPv6 アクティビティのサマリーを表示する例を示します。

```
Router# show bgp ipv6 summary

For address family: IPv6 Unicast
BGP router identifier 192.168.2.126, local AS number 33751
BGP table version is 15, main routing table version 15
12 network entries using 1692 bytes of memory
22 path entries using 1672 bytes of memory
5/4 BGP path/bestpath attribute entries using 580 bytes of memory
14 BGP rrinfo entries using 336 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 4328 total bytes of memory
Dampening enabled. 0 history paths, 0 dampened paths
BGP activity 13/1 prefixes, 23/1 paths, scan interval 60 secs
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.2.146     4 33751     991     983       15    0    0 16:26:21        10
192.168.2.147     4 33751     991     983       15    0    0 16:26:22        10
FE80::4F6B:44%Serial1/0
                4 20331     982     987       15    0    0 14:55:52         1
```

BGP IPv6 テーブルのダンプ

次の例に示すように、各テーブル（BGP IPv6、BGP IPv6 VPN など）を個別に確認できます。

```
Router# show bgp ipv6 unicast
```

```
BGP table version is 15, local router ID is 192.168.2.126
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric    LocPrf Weight Path
* i2001:DB8:100::/48 ::FFFF:192.168.2.101     0    100      0 10000 ?
*>i                  ::FFFF:192.168.2.101     0    100      0 10000 ?
* i2001:DB8::1/128   ::FFFF:192.168.2.101     0    100      0  i
*>i                  ::FFFF:192.168.2.101     0    100      0  i
```

IPv6 ルーティング テーブルのダンプ

次の例に示すように、IPv6 ルーティング テーブルを表示して、ルーティング可能なエントリを導出した各ルーティング プロトコルを確認できます。

```
Router# show ipv6 route

IPv6 Routing Table - default - 13 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
B   2001:DB8:100::/48 [200/0]
     via 192.168.2.101%Default-IP-Routing-Table, indirectly connected
B   2001:DB8::1/128 [200/0]
     via 192.168.2.101%Default-IP-Routing-Table, c
LC  2001:DB8::26/128 [0/0]
     via Loopback0, receive
```

IPv6 ルーティングの観点から見ると、MPLS バックボーンを介して到達可能なエントリが、間接的に接続されているものとしてリストされることに注意してください。これは、MPLS がレイヤ 2 トンネル メカニズムを提供しているためです。

転送の確認とトラブルシューティング

ユーザがトラブルシューティングを実行できるように、転送の異常を検出して、理解しておく必要があります。**ping ipv6** および **traceroute ipv6** などのコマンドを使用して、データプレーン接続を検証し、トラフィックのブラックホール化を検出します。**traceroute mpls** および **show mpls forwarding** などのコマンドでは、障害の発生しているノード、インターフェイス、および Forwarding Error Correction（FEC; 転送エラー訂正）を特定できます。エッジでの特定の IPv6 宛先の転送障害のトラブルシューティングでは、一般的に、再帰的解決が基本構成要素に分割されます。この作業は、IPv6 ルーティング（iBGP または eBGP）、IP ルーティング（IS-IS または OSPF）、ラベル配布（BGP、LDP、または RSVP）、および解決の中断を検出する隣接解決の分析を組み合せて実行する必要があります。

次の例では、IPv6 VPN を確認して、さまざまな IPv6 VPN 転送状況をトラブルシューティングする方法を示します。

- 「PE-CE 接続」（P.48）
- 「PE インポジション パス」（P.50）
- 「PE ディスポジション パス」（P.51）
- 「ラベル スイッチ パス」（P.51）

PE-CE 接続

ipv6 ping および **traceroute** コマンドは、ローカルに接続されている場合でも、MPLS バックボーンを介してリモートで接続されている場合でも、PE から CE への接続を確認するのに役立ちます。

ルータがローカルに接続されている場合は、次の例に示すように、CE のリンクローカル アドレス（eBGP ピアリングに使用される）を指定して、**ipv6 ping** コマンドを使用できます。

```
Router# ping FE80::4F6B:44%Serial1/0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FE80::4F6B:44, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/33/48 ms
```

また、**ipv6 ping** コマンドを使用すると、リモート PE または CE の到達可能性もテストできますが、使用できるのは IPv6 グローバル アドレスだけです（リンクローカル アドレスはリンクの向こう側にはアドバタイズされません）。

```
Router# ping 2001:DB8:1120:1::44

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:1120:1:44::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/33/48 ms
```

MPLS を介した **ping ipv6** および **traceroute** コマンド機能は、PE および CE に対して 1 つの IPv6 グローバル プレフィクスをアナウンスするように要求することに注意してください。各 6PE ルータは、自律システムのエッジでフィルタリングされる 2001:DB8::PE#/128 をアナウンスします。各 IPv6 CE は 2001:DB8:*prefix*:CE#/128 を設定し、これを特定的でないプレフィクスの一部としてアナウンスします（2001:DB8:*prefix*::/n）。

リモート PE および CE の到達可能性は、**traceroute** コマンドを使用してテストできます。すべての PE を **no mpls ip propagate-ttl forwarded** コマンドで設定してある場合、**traceroute** コマンドを CE から実行すると、その出力には IPv6 ノードだけが表示されます。

```
Router# traceroute 2001:DB8::1

Type escape sequence to abort.
Tracing the route to 2001:DB8::1
  1 2001:DB8::26 [AS 33751] 32 msec 32 msec 20 msec
  2 2001:DB8::1 [AS 33751] [MPLS: Label 73 Exp 0] 20 msec 20 msec 20 msec
  3 2001:DB8::1 [AS 33751] 28 msec 20 msec 20 msec
```

P ルータが ICMPv6 をサポートしているイメージでアップグレードされたあとに PE ルータで **traceroute** コマンドを実行すると（このとき、Time to Live（TTL; 存続可能時間）が伝播される）、次の例に示すように、P ルータの応答も表示されます。

```
Router# traceroute 2001:DB8::1

Type escape sequence to abort.
Tracing the route to 2001:DB8::1
  1 ::FFFF:172.20.25.1 [MPLS: Labels 38/73 Exp 0] 40 msec 32 msec 32 msec
  2 ::FFFF:172.20.10.1 [MPLS: Labels 30/73 Exp 0] 60 msec 32 msec 32 msec
  3 2001:DB8::1 [MPLS: Label 73 Exp 0] 32 msec 32 msec 16 msec
```

ping ipv6 コマンドと **traceroute** コマンドを 6VPE ルータから実行すると、どちらのコマンドも VPNv4 の場合とまったく同様に *vrf* 引数を受け付けます。

traceroute コマンドは MPLS バックボーン全体のパスの評価には役立ちますが、データプレーン障害のトラブルシューティングには役立たないことに注意してください。P ルータは IPv6 対応ではないため（VPNv4 対応でもない）、**traceroute** コマンドに応答して生成された ICMPv6 メッセージは、受信されたラベル スタックを使用して出力 PE に転送されます。出力 PE は ICMPv6 メッセージを traceroute の送信元にルーティングできます。MPLS パスが切断されている場合は ICMP メッセージからも切断されるため、ICMP メッセージは出力 PE に到達できません。

PE インポジション パス

Cisco ルータで、IPv6 のインポジション パスのトラブルシューティングに最も役立つツールは、**show ipv6 cef** コマンドです。

IPv6 転送テーブルのダンプ

次の例に示すように、**show ipv6 cef** コマンドを使用すると、各宛先プレフィクスに使用される転送テーブルとラベル スタックが表示されます。

```
Router# show ipv6 cef

2001:DB8:100::/48
  nexthop 172.20.25.1 Serial0/0 label 38 72
2001:DB8::1/128
  nexthop 172.20.25.1 Serial0/0 label 38 73
2001:DB8::26/128
  attached to Loopback0, receive
```

転送テーブル内の IPv6 エントリの詳細

次の例に示すように、**show ipv6 cef** コマンドを使用すると、特定のエントリの詳細を表示したり、宛先の解決方法やラベル スタックの計算方法を分析したりできます。

```
Router# show ipv6 cef 2001:DB8:100::/48 internal

2001:DB8:100::/48, epoch 0, RIB[B], refcount 4
  sources: RIB
..
  recursive via 192.168.2.101[IPv4:Default] label 72, fib 0252B1F8, 1 terminal fib
    path 024F56A8, path list 024F0BA8, share 0/1, type attached nexthop
    ifnums: (none)
     path_list contains at least one resolved destination(s). HW IPv4 notified.
    nexthop 172.20.25.1 Serial0/0 label 38, adjacency IP adj out of Serial0/0 0289BEF0
  output chain: label 72 label 38 TAG adj out of Serial0/0 0289BD80
```

BGP テーブル内の BGP エントリの詳細

前述の例の詳細出力には、ラベル スタックを構成している各ラベルに、個別に追跡できる発信元がそれぞれ含まれていることが示されています。次の例に示すように、BGP テーブルには一番下のラベルが格納されています。

```
Router# show bgp ipv6 unicast 2001:DB8:100::/48

BGP routing table entry for 2001:DB8:100::/48, version 2
Paths: (2 available, best #2, table default)
  Advertised to update-groups:
     1
  10000
    ::FFFF:192.168.2.101 (metric 30) from 192.168.2.147 (192.168.2.147)
      Origin incomplete, metric 0, localpref 100, valid, internal
      Originator: 192.168.2.101, Cluster list: 192.168.2.147,
      mpls labels in/out nolabel/72
  10000
    ::FFFF:192.168.2.101 (metric 30) from 192.168.2.146 (192.168.2.146)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Originator: 192.168.2.101, Cluster list: 192.168.2.146,
      mpls labels in/out nolabel/72
```

次の例に示すように、LDP ではその他のラベルが表示されます。

```
Router# show mpls ldp bindings 192.168.2.101 32

  lib entry: 192.168.2.101/32, rev 56
```

```
        local binding:  label: 40
        remote binding: lsr: 192.168.2.119:0, label: 38

Router# show mpls ldp bindings 172.20.25.0 24

  lib entry: 172.20.25.0/24, rev 2
        local binding: label: imp-null
        remote binding: lsr: 192.168.2.119:0, label: imp-null
```

PE ディスポジション パス

次の例を使用して、ディスポジション パスをトラブルシューティングします。

- 「MPLS 転送テーブルのダンプ」（P.51）
- 「BGP ラベル分析」（P.51）

MPLS 転送テーブルのダンプ

次に、ディスポジション パスをトラブルシューティングするための MPLS 転送テーブル情報の例を示します。

```
Router# show mpls forwarding-table

Local  Outgoing      Prefix            Bytes Label   Outgoing   Next Hop
Label  Label or VC   or Tunnel Id      Switched      interface
16     Pop Label     192.168.2.114/32    0             Se0/0      point2point
17     26            192.168.2.146/32    0             Se0/0      point2point
..
72     No Label      2001:DB8:100::/48     63121         Se1/0      point2point
73     Aggregate     2001:DB8::1/128   24123
```

BGP ラベル分析

次に、スイッチングに使用されるラベルの例を示します。ラベルは iBGP（この例では 6PE）によってアナウンスされており、確認が可能です。

```
Router# show bgp ipv6 2001:DB8:100::/48

BGP routing table entry for 2001:DB8:100::/48, version 2
Paths: (1 available, best #1, table default)
  Advertised to update-groups:
     2
  10000
    FE80::2710:2 (FE80::2710:2) from FE80::2710:2%Serial1/0 (192.168.2.103)
      Origin incomplete, metric 0, localpref 100, valid, external, best,
```

ラベル スイッチ パス

6PE および 6VPE LSP エンドポイントは IPv4 アドレスであるため、LSP をトラブルシューティングする IPv4 ツールが、IPv6 トラフィックのブラックホール化につながるデータプレーン障害の検出に役立ちます。

ラベル スイッチ パスの分析

次に、LSP IPv4 エンドを表示する例を示します。

```
Router# show ipv6 route 2001:DB8::1/128

Routing entry for 2001:DB8::1/128
  Known via "bgp 33751", distance 200, metric 0, type internal
  Route count is 1/1, share count 0
  Routing paths:
    192.168.2.101%Default-IP-Routing-Table indirectly connected
```

```
      MPLS Required
      Last updated 02:42:12 ago
```

traceroute LSP の例

次に、traceroute LSP の例を示します。

```
Router# traceroute mpls ipv4 192.168.2.101/32 verbose

Tracing MPLS Label Switched Path to 192.168.2.101/32, timeout is 2 seconds
Codes: '!' - success, 'Q' - request not transmitted,
       '.' - timeout, 'U' - unreachable,
       'R' - downstream router but not target,
       'M' - malformed request
Type escape sequence to abort.
  0 172.20.25.2 0.0.0.0 MRU 1500 [Labels: 38 Exp: 0]
R 1 172.20.25.1 0.0.0.0 MRU 1500 [Labels: 30 Exp: 0] 40 ms, ret code 6
R 2 172.20.10.1 0.0.0.0 MRU 1504 [Labels: implicit-null Exp: 0] 60 ms, ret code 6
! 3 172.20.40.1 48 ms
```

VRF 情報

次のコマンド入力では、6VPE の VRF 情報が表示されます。

show ipv6 cef vrf

次に、cisco1 という名前の VRF に関連付けられているシスコ エクスプレス フォワーディング FIB からの出力例を示します。

```
Router# show ipv6 cef vrf cisco1

 2001:8::/64
  attached to FastEthernet0/0
 2001:8::3/128
  receive
 2002:8::/64
  nexthop 10.1.1.2 POS4/0 label 22 19
 2010::/64
  nexthop 2001:8::1 FastEthernet0/0
 2012::/64
  attached to Loopback1
 2012::1/128
  receive
```

show ipv6 route vrf

次に、cisco1 という名前の VRF に関連付けられている IPv6 ルーティング テーブルに関する出力例を示します。

```
Router# show ipv6 route vrf cisco1

IPv6 Routing Table cisco1 - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
C   2001:8::/64 [0/0]
     via ::, FastEthernet0/0
L   2001:8::3/128 [0/0]
     via ::, FastEthernet0/0
B   2002:8::/64 [200/0]
     via ::FFFF:192.168.1.4,
B   2010::/64 [20/1]
     via 2001:8::1,
```

```
C   2012::/64 [0/0]
     via ::, Loopback1
L   2012::1/128 [0/0]
     via ::, Loopback1
```

ルーティングおよび転送のデバッグ

ルーティングおよび転送の異常をトラブルシューティングする場合、デバッグ コマンドをイネーブルにすると役立つ可能性がありますが、いくつかのデバッグ メッセージはルータの動作を遅くし、このようなツールの有用性を損なう可能性があります。そのため、**debug** コマンドは注意して使用する必要があります。**debug ipv6 cef**、**debug mpls packet**、および **debug ipv6 packet** コマンドは、転送パスのトラブルシューティングに役立ち、**debug bgp ipv6** および **debug bgp vpnv6** コマンドはコントロール プレーンのトラブルシューティングに役立ちます。

IPv6 VPN over MPLS を実装するための設定例

例：IPv4 ネクストホップを使用した IPv6 VPN の設定

次に、6VPE ネクストホップの例を示します。

```
interface Loopback0
 ip address 192.168.2.11 255.255.255.255
!
router bgp 100
 neighbor 192.168.2.10 remote-as 100
 neighbor 192.168.2.10 update-source Loopback0
!
 address-family vpnv6
 neighbor 192.168.2.10 activate
 neighbor 192.168.2.10 send-community extended
 exit-address-family
```

デフォルトでは、アドバタイズされるネクストホップは IPv6 VPN アドレスになります。

```
[0:0]::FFFF:192.168.2.10
```

[*RD*]::FFFF:*IPv4-address* の形式の 192 ビット アドレスであることに注意してください。

BGP IPv6 VPN ピアが共通サブネットを共有する場合、MP_REACH_NLRI アトリビュートには、グローバル アドレス ネクストホップに加えてリンクローカル アドレス ネクストホップも含まれます。この状況は、一般的に、ASBR が互いに向き合っている相互自律システム トポロジで発生します。この場合、リンクローカル ネクストホップがローカルに使用され、グローバル ネクストホップは BGP によって再アドバタイズされます。

BGP ネクストホップは、ラベル スタックを構築する場合の中心要素です。内部ラベルは BGP NLRI から取得され、外部ラベルは BGP ネクストホップに埋め込まれた IPv4 アドレスに到達する Label Distribution Protocol（LDP; ラベル配布プロトコル）ラベルになります。

その他の関連資料

関連資料

関連項目	参照先
IPv6 マルチプロトコル BGP	『*Implementing Multiprotocol BGP for IPv6*』
IPv6 EIGRP	『*Implementing EIGRP for IPv6*』
IPv6 MPLS	『*Implementing IPv6 over MPLS*』
IPv6 スタティック ルート	『*Implementing Static Routes for IPv6*』
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』

規格

規格	タイトル
draft-bonica-internet-icmp	『*ICMP Extensions for Multiprotocol Label Switching*』
draft-ietf-idr-bgp-ext-communities-0*x*.txt	『*Cooperative Route Filtering Capability for BGP-4*』

MIB

MIB	MIB リンク
•	選択したプラットフォーム、Cisco ソフトウェア リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 1267	『*A Border Gateway Protocol 3 (BGP-3)*』
RFC 1772	『*Application of the Border Gateway Protocol in the Internet*』
RFC 1918	『*Address Allocation for Private Internets*』
RFC 2858	『*Multiprotocol Extensions for BGP-4*』
RFC 3107	『*Carrying Label Information in BGP-4*』
RFC 3392	『*Capabilities Advertisement with BGP-4*』
RFC 3513	『*Internet Protocol Version 6 (IPv6) Addressing Architecture*』
RFC 4007	『*IPv6 Scoped Address Architecture*』
RFC 4193	『*Unique Local IPv6 Unicast Addresses*』
RFC 4364	『*BGP MPLS/IP Virtual Private Networks (VPNs)*』

RFC	タイトル
RFC 4382	『*MPLS/BGP Layer 3 Virtual Private Network (VPN) Management Information Base*』
RFC 4659	『*BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

IPv6 VPN over MPLS の実装の機能情報

表 1 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どのソフトウェア イメージが特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1　IPv6 VPN over MPLS の実装の機能情報

機能名	リリース	機能情報
IPv6 VPN over MPLS（6VPE）	12.2(28)SB 12.2(33)SRB 12.2(33)SXI 12.4(20)T 15.0(1)S	MPLS を介した IPv6 VPN（6VPE）の IPv4 コア インフラストラクチャ機能を使用すると、ISP はカスタマーに IPv6 VPN サービスを提供できます。 このマニュアルでは、この機能について説明しています。
IP トンネルを介した MPLS VPN 6VPE サポート	12.2(33)SRB1 12.2(33)SXI	この機能では、IPv4 GRE トンネルを使用して、BGP ネクストホップに到達するための IPv6 VPN over MPLS 機能を提供できます。 この機能に関する詳細については、次の各項を参照してください。 • 「MPLS 転送」（P.5）

用語集

- **6VPE ルータ**：IPv4 ベースの MPLS コア上に BGP-MPLS IPv6 VPN サービスを提供するプロバイダー エッジ ルータ。コア方向のインターフェイスで 6PE 概念を実装する IPv6 VPN PE のデュアル スタック ルータです。
- **Customer Edge（CE; カスタマー エッジ）ルータ**：VPN カスタマー サイトに接続するサービス プロバイダー ルータ。
- **Forwarding Information Base（FIB; 転送情報ベース）**：IP データグラムの転送に必要な情報を含むテーブル。FIB には、少なくとも、到達可能な宛先ネットワーク プレフィクスごとにインターフェイス識別子とネクストホップ情報が格納されます。
- **Inbound Route Filtering（IRF; インバウンド ルート フィルタリング）**：受信側 PE ルータによってインポートされない着信 BGP アップデートをフィルタリングするために使用される BGP 機能。
- **IPv6 Provider Edge（6PE; IPv6 プロバイダー エッジ）ルータ**：BGP ベースのメカニズムを実行して、MPLS 対応の IPv4 クラウド上で IPv6 アイランドを相互接続するルータ。
- **IPv6 VPN アドレス**：IPv6 VPN アドレスは、8 バイトの Route Distinguisher（RD; ルート識別子）で始まり、16 バイトの IPv6 アドレスで終わる、24 バイトの識別子です。IPv6 VPN アドレスと呼ばれることもあります。
- **IPv6 VPN アドレス ファミリ**：Address-Family Identifier（AFI; アドレス ファミリ識別子）は特定のネットワーク レイヤ プロトコルを識別し、Subsequent AFI（SAFI; 後続 AFI）は追加情報を提供します。AFI IPv6 SAFI VPN（AFI=2、SAFI=128）は、IPv6 VPN アドレス ファミリと呼ばれます。IPv6 VPN アドレス ファミリと呼ばれることもあります。同様に、AFI IPv4 SAFI VPN は VPNv4 アドレス ファミリと呼ばれます。
- **Network Layer Reachability Information（NLRI; ネットワーク レイヤ到達可能性情報）**：BGP では、ルートおよびそのルートへのアクセス方法を記述した NLRI を含むルーティング アップデート メッセージが送信されます。この場合、NLRI がプレフィクスとなります。BGP アップデート メッセージでは、1 つ以上の NLRI プレフィクス、および NLRI プレフィクスのルートのアトリビュートが伝送されます。ルート アトリビュートには、BGP ネクストホップ ゲートウェイ アドレスおよびコミュニティ値が含まれています。
- **Outbound Route Filtering（ORF; アウトバウンド ルート フィルタリング）**：発信 BGP ルーティング アップデートのフィルタリングに使用される BGP 機能。
- **Point of Presence（POP）**：装置にインストールされている中継キャリアが、地域通信事業者と相互接続する物理的なロケーション。
- **Provider Edge（PE; プロバイダー エッジ）ルータ**：VPN カスタマー サイトに接続されるサービス プロバイダー ルータ。
- **Route Distinguisher（RD; ルート識別子）**：グローバルに一意な IPv6 VPN アドレスを形成するために、IPv6 プレフィクスの先頭に付加される 64 ビットの値。
- **Routing Information Base（RIB; ルーティング情報ベース）**：ルーティング テーブルとも呼ばれます。
- **Virtual routing and forwarding（VRF; 仮想ルーティングおよび転送）**：PE 内の VPN ルーティングおよび転送インスタンス。
- **VRF テーブル**：VRF に関連付けられているルーティングおよび転送テーブル。これは、PE ルータがカスタマーごとに独立したルーティング状態を維持できるようにするカスタマー固有のテーブルです。

QoS for IPv6 の実装

この章では、IPv6 環境に Quality of Service（QoS; サービス品質）機能を実装するための情報および作業について説明します。具体的には、IPv6 パケットへの Differentiated Service（DiffServ; ディファレンシエーテッド サービス）QoS 機能の適用について説明します。

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「QoS for IPv6 を実装するための機能情報」（P.17）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

QoS for IPv6 の実装の前提条件

このマニュアルでは、IPv4 に精通していることを前提としています。IPv4 の設定およびコマンド リファレンス情報については、「その他の関連資料」の関連資料を参照してください。

QoS for IPv6 の実装の制約事項

次の QoS 機能は、IPv6 トラフィックの管理ではサポートされません。

- Compressed Real-Time Protocol（CRTP）
- Network-Based Application Recognition（NBAR）
- Committed Access Rate（CAR; 専用アクセス レート）
- Priority Queueing（PQ; プライオリティ キューイング）
- Custom Queueing（CQ）

プラットフォーム固有の情報および制約事項

IPv6 QoS は、Cisco IOS Release 12.0(28)S が稼動する Cisco 12000 シリーズ インターネット ルータ上でサポートされます。IPv6 QoS の機能の中には、Release 12.0(28)S でサポートされない機能もあります。これには、パケット分類などがあります。

QoS for IPv6 の実装に関する情報

IPv6 トラフィックの管理に使用できる QoS 機能に関する詳細については、次の各項を参照してください。

- 「QoS for IPv6 の実装方針」（P.2）
- 「IPv6 でのパケット分類」（P.3）
- 「IPv6 ネットワークでのポリシーおよびクラスベース パケット マーキング」（P.3）
- 「IPv6 ネットワークでの輻輳管理」（P.4）
- 「IPv6 トラフィックの輻輳回避」（P.4）
- 「IPv6 環境でのトラフィック ポリシング」（P.4）

QoS for IPv6 の実装方針

IPv6 パケットは、IPv4 パケットとは別のパスで転送されます。IPv6 環境でサポートされている QoS 機能には、パケット分類、キューイング、トラフィック シェーピング、Weighted Random Early Detection（WRED; 重み付けランダム早期検出）、クラスベース パケット マーキング、および IPv6 パケットのポリシングが含まれます。これらの機能は、IPv6 のプロセス スイッチング パスとシスコ エクスプレス フォワーディング スイッチング パスのどちらでも使用できます。

IPv6 環境で使用可能な QoS 機能はすべて、Modular QoS Command-Line Interface（CLI; コマンドライン インターフェイス）から管理します。Modular QoS CLI を使用すると、トラフィック クラスを定義し、トラフィック ポリシー（ポリシー マップ）を作成および設定してから、それらのトラフィック ポリシーをインターフェイスに対応付けることができます。

IPv6 が稼動しているネットワークに QoS を実装するには、IPv4 だけが稼動しているネットワークに QoS を実装する手順に従ってください。高度なレベルで QoS を実装するための基本手順は、次のとおりです。

1. QoS を必要とするネットワーク内のアプリケーションを特定します。
2. どの QoS 機能が適切であるかを判断するために、アプリケーションの特性を理解します。
3. 変更と転送がリンク レイヤ ヘッダー サイズに及ぼす影響を理解するために、ネットワーク トポロジについて理解します。
4. ネットワークに確立する基準に基づいて、クラスを作成します。具体的には、同じネットワークで IPv6 トラフィックとともに IPv4 トラフィックも伝送されている場合、IPv6 トラフィックと IPv4 トラフィックを同様に処理するか、それとも別の方法で処理し、それぞれに応じた一致基準を指定するかを決定します。両者を同様に処理する場合は、**match precedence**、**match dscp**、**set precedence**、**set dscp** などの match 文を使用します。両者を別の方法で処理する場合は、match-all クラス マップ内に **match protocol ip** や **match protocol ipv6** などの一致基準を追加します。
5. 各クラスにマーキングするためのポリシーを作成します。
6. QoS 機能を適用する際は、エッジからコアに向かって作業します。
7. トラフィックを処理するためのポリシーを構築します。
8. ポリシーを適用します。

IPv6 でのパケット分類

パケット分類は、プロセス スイッチング パスとシスコ エクスプレス フォワーディング スイッチング パスの両方で使用可能です。分類は、IPv6 precedence、Differentiated Services Control Point（DSCP）、および IPv6 アクセス リスト内に指定可能なその他の IPv6 プロトコル固有値に基づいて行うことができます。また、COS、パケット長、QOS グループなどのその他の IPv6 プロトコル固有でない値に基づいて行うこともできます。QoS を必要とするアプリケーションを決定したあとは、アプリケーションの特性に基づいてクラスを作成できます。さまざまな一致基準を使用して、トラフィックを分類できます。さまざまな一致基準を組み合せて、トラフィックを隔離、分離、および区別できます。

Modular QoS CLI（MQC）の機能拡張によって、IPv4 パケットと IPv6 パケットのどちらにも、precedence、DSCP、および IPv6 アクセス グループ値に基づく一致を作成できます。**match** コマンドを使用すると、IPv4 パケットと IPv6 パケットのどちらにも、DSCP 値および precedence に基づいて一致を作成できます。設定のガイドライン、および **match dscp** コマンドと **match precedence** コマンドの説明については、「IPv6 トラフィック フローを管理するための一致基準の使用」（P.6）を参照してください。

IPv6 ネットワークでのポリシーおよびクラスベース パケット マーキング

DSCP か precedence のどちらかを使用して、各トラフィック クラスを適切なプライオリティ値でマーキングするためのポリシーを作成できます。クラスベース マーキングを使用すると、トラフィック管理に対して IPv6 precedence および DSCP の値を設定できます。トラフィックは、ルータの入力インターフェイスに入るときにマーキングされます。このマーキングは、トラフィックがルータの出力インターフェイスを出るときに、トラフィックを処理（転送やキューイング）するために使用されます。トラフィックのマーキングと処理は、できるだけ送信元の近くで行ってください。

パケット マーキングには、**set dscp** コマンドおよび **set precedence** コマンドを使用します。これらのコマンドは、IPv4 トラフィックと IPv6 トラフィックの両方を処理するように変更されています。これらのコマンドを使用する際の設定ガイドラインについては、「IPv6 パケットのマーキング基準の指定」（P.5）を参照してください。

IPv6 ネットワークでの輻輳管理

トラフィックをマーキングしたあとは、そのマーキングを使用してポリシーを構築し、残りのネットワーク セグメントのトラフィックを分類できます。ポリシーを簡潔にしておく（4 クラスを越えないようにする）と、管理が容易になります。IPv6 では、クラスベース キューイングとフローベース キューイングがサポートされています。各種のキューイング オプションを設定するためにプロセスおよびタスクで使用されるコマンドおよび引数は、IP と IPv6 のどちらでも同じです。キューイング機能の設定および使用の手順については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』を参照してください。

IPv6 トラフィックの輻輳回避

WRED は、Class-Based Weighted Fair Queueing（CBWFQ; クラスベース均等化キューイング）の制限を超える可能性のあるパケットに対して RED ベースのドロップ ポリシーを実装します。WRED では、（DSCP または precedence の値を使用する）クラスベース キューイングとフローベース キューイングをサポートしています。WRED コマンドは、何も変更しなくても IPv4 と IPv6 の両方に適用されます。

IPv6 環境でのトラフィック ポリシング

IPv6 での輻輳管理は、IP パケットでの輻輳管理の実装と似ています。また、IPv6 環境でキューイングおよびトラフィック シェーピング機能の設定に使用するコマンドは、IP で使用するコマンドと同じです。トラフィック シェーピングを行うと、トラフィック シェーピング機能に対して設定したパラメータで指定されているとおりに追加のパケットをキューに格納してから転送することで、パケット デキュー レートを制限できます。トラフィック シェーピングでは、デフォルトでフローベース キューイングが使用されます。パケットの分類およびプライオリティ設定には、CBWFQ を使用できます。トラフィックのコンディショニングおよびポリシングには、Class-Based Policer と Generic Traffic Shaping（GTS）、または Frame Relay Traffic Shaping（FRTS; フレーム リレー トラフィック シェーピング）を使用できます。

IPv6 環境で使用するために、ポリシングの既存の設定やコマンド使用法を変更する必要はありませんが、**police** コマンドが拡張されたため、確認アクション、超過アクション、および違反アクションで次のキーワード オプションが使用されているとき、IPv4 パケットと IPv6 パケットの両方がマーキングされるようになりました。

- **set-dscp-transmit**
- **set-precedence-transmit**

QoS for IPv6 の実装方法

ここでは、一致基準を使用したトラフィックの分類方法と、一致基準を使用したトラフィック フローの管理方法について説明します。次の各項で構成されます。

- 「IPv6 ネットワークでのトラフィック分類の制約事項」（P.5）（必須）

- 「IPv6 パケットのマーキング基準の指定」（P.5）（必須）
- 「IPv6 トラフィック フローを管理するための一致基準の使用」（P.6）（必須）
- 「パケット マーキング基準の確認」（P.8）（任意）
- 「サービス ポリシーの確認」（P.13）（任意）

IPv6 ネットワークでのトラフィック分類の制約事項

match dscp コマンドと **match precedence** コマンドが変更されたこと、および IPv6 固有の **match access-group name** コマンドが追加されたことを除いて、**match** コマンドの機能は IPv4 と IPv6 のどちらでも同じです。

802.1Q（dot1Q）インターフェイス用の **set cos** コマンドと **match cos** コマンドは、シスコ エクスプレス フォワーディング スイッチド パケットに対してだけサポートされます。これらのオプションが使用されている場合、プロセス スイッチド パケット（ルータ生成パケットなど）はマーキングされません。

IPv6 パケットのマーキング基準の指定

ここでは、ネットワーク トラフィックを分類するためにあとでパケットのマッチングに使用される一致基準を確立します（つまり、パケットをマーキングします）。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy map** *policy-map-name*
4. **class** {*class-name* | **class-default**}
5. **set precedence** {*precedence-value* | *from-field* [**table** *table-map-name*]}

   または

   set [**ip**] **dscp** {*dscp-value* | *from-field* [**table** *table-map-name*]}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy map** *policy-map-name* **例：** `Router(config)# policy map policy1`	指定された名前を使用してポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。 • 作成するポリシー マップの名前を入力します。

	コマンドまたはアクション	目的
ステップ 4	**class** {*class-name* | **class-default**} **例：** `Router(config-pmap)# class class-default`	指定されたクラス（またはデフォルト クラス）のトラフィックの処理を指定し、QoS ポリシーマップ コンフィギュレーション モードを開始します。

ステップ 5	**set precedence** {*precedence-value* | *from-field* [**table** *table-map-name*]}
	
	または
	
	set [**ip**] **dscp** {*dscp-value* | *from-field* [**table** *table-map-name*]}
	
	例：
	`Router(config-pmap-c)# set dscp cos table table-map1`
	
	または
	
	`Router(config-pmap-c)# set precedence cos table table-map1`
		precedence 値を設定します。
		• この例は、指定したテーブル マップ内で定義されている CoS 値（およびアクション）に基づいています。
		• 同じパケット内で precedence と DSCP の両方を変更することはできません。
		• 指定したテーブル マップ内で定義されている CoS 値（およびアクション）に基づいて、DSCP 値を設定します。

トラブルシューティングのヒント

シスコ エクスプレス フォワーディングがイネーブルになっていることを確認する

show cef interface、**show ipv6 cef**、**show ipv6 interface neighbors**、および **show interface statistics** コマンドを使用して、シスコ エクスプレス フォワーディングがイネーブルになっていることと、パケットがシスコ エクスプレス フォワーディングでスイッチングされていることを確認します。

パケットがシスコ エクスプレス フォワーディングでスイッチングされていることを確認する

show policy-map interface コマンドを使用して、インターフェイスごと、ポリシーごとのシスコ エクスプレス フォワーディングによるスイッチング統計情報を表示します。

IPv6 トラフィック フローを管理するための一致基準の使用

次の作業では、**match** コマンドを使用して、トラフィックを、確立したポリシーとマッチングする方法を示します。複数の match 文を使用できます。クラスのタイプに応じて、すべてのクラスとマッチングするか、それともいずれかのクラスとマッチングするかを指定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map** {*class-name* | **class-default**}
4. **match precedence** *precedence-value* [*precedence-value precedence-value*]

   または

   match access-group name *ipv6-access-group*

   または

match [**ip**] **dscp** *dscp-value* [*dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map** {*class-name* | **class-default**} **例：** `Router(config-pmap-c)# class cls1`	指定されたクラスを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。

ステップ 4	**match precedence** *precedence-value* [*precedence-value precedence-value*]
	
	または
	
	match access-group name *ipv6-access-group*
	
	または
	
	match [ip] dscp *dscp-value* [*dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value*]
	
	例：
	`Router(config-pmap-c)# match precedence 5`
	
	または
	
	`Router(config-pmap-c)# match access-group name ipv6acl`
	
	または
	
	`Router(config-pmap-c)# match ip dscp 15`
		precedence 値とマッチングします。precedence は、IPv4 パケットと IPv6 パケットの両方に適用されます。
		
		または
		
		コンテンツ パケットがトラフィック クラスに属しているかどうかをチェックする IPv6 アクセス リストの名前を指定します。
		
		または
		
		特定の IP DSCP 値を一致基準として識別します。

例

次に、**match precedence** コマンドを使用して IPv6 トラフィック フローを管理する例を示します。

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
 Router(config)# class-m c1
  Router(config-cmap)# match precedence 5
  Router(config-cmap)# end
Router#
 Router(config)# policy p1
  Router(config-pmap)# class c1
  Router(config-pmap-c)# police 10000 conform set-prec-trans 4
```

パケット マーキング基準の確認

パケット マーキングが正常に行われることを確認するには、show policy コマンドを使用します。このコマンドの出力の注目すべき情報は、合計のパケット数とマーキングされたパケット数の差です。

```
Router# show policy p1

  Policy Map p1
    Class c1
      police 10000 1500 1500 conform-action set-prec-transmit 4 exceed-action drop

Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface serial 4/1
Router(config-if)# service out p1
Router(config-if)# end

Router# show policy interface s4/1

 Serial4/1
  Service-policy output: p1
    Class-map: c1 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: precedence 5
      police:
        10000 bps, 1500 limit, 1500 extended limit
        conformed 0 packets, 0 bytes; action: set-prec-transmit 4
        exceeded 0 packets, 0 bytes; action: drop
        conformed 0 bps, exceed 0 bps violate 0 bps

    Class-map: class-default (match-any)
      10 packets, 1486 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

show policy-map interface コマンド出力内のパケット カウンタの解釈

発信インターフェイスでの送信輻輳中、パケットは、インターフェイスが送信可能な速度より速く到達します。シスコの Modular QoS CLI で作成されたサービスポリシーの結果を監視する場合に役立つ **show policy-map interface** コマンドの出力の解釈方法を理解しておくと便利です。

輻輳は通常、高速な入力インターフェイスが相対的に低速な出力インターフェイスに供給する場合に発生します。一般的な輻輳ポイントは、LAN に面したイーサネット ポートおよび WAN に面したシリアル ポートを持つブランチオフィス ルータです。LAN セグメントのユーザが 10 Mbps のトラフィックを生成すると、それが 1.5 Mbps の帯域幅を持つ T1 に供給されます。

機能的には、輻輳の定義は、インターフェイス上で送信リングがいっぱいになることです（リングとは、特殊なバッファ制御構造のことです）。それぞれのインターフェイスは、1 対のリング、つまりパケット受信用の受信リングとパケット送信用の送信リングをサポートしています。リングのサイズは、インターフェイス コントローラやインターフェイスまたは Virtual Circuit（VC; 仮想回線）の帯域幅によって異なります。次の例に示すように、**show atm vc** *vcd* コマンドを使用して、PA-A3 ATM ポートアダプタ上の送信リングの値を表示します。

```
Router# show atm vc 3

ATM5/0.2: VCD: 3, VPI: 2, VCI: 2
VBR-NRT, PeakRate: 30000, Average Rate: 20000, Burst Cells: 94
AAL5-LLC/SNAP, etype:0x0, Flags: 0x20, VCmode: 0x0
```

```
OAM frequency: 0 second(s)
PA TxRingLimit: 10
InARP frequency: 15 minutes(s)
Transmit priority 2
InPkts: 0, OutPkts: 0, InBytes: 0, OutBytes: 0
InPRoc: 0, OutPRoc: 0
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
InPktDrops: 0, OutPktDrops: 0
CrcErrors: 0, SarTimeOuts: 0, OverSizedSDUs: 0
OAM cells received: 0
OAM cells sent: 0
Status: UP
```

Cisco IOS（レイヤ 3 プロセッサとも呼ばれる）およびインターフェイス ドライバは、パケットを物理メディアに移動する際に送信リングを使用します。この 2 つのプロセッサは、次のように連携します。

- インターフェイスは、インターフェイス レートまたはシェイプド レートに応じてパケットを送信します。
- インターフェイスは、物理ワイヤへの送信を待機するパケットの格納場所であるハードウェア キューまたは送信リングを維持します。
- ハードウェア キューまたは送信リングがいっぱいになると、インターフェイスはレイヤ 3 プロセッサ システムへの明示的なバック プレッシャを提供します。インターフェイスは、送信リングがいっぱいになっているためインターフェイスの送信リングへのパケットのデキューを停止するようレイヤ 3 プロセッサに通知します。レイヤ 3 プロセッサは、超過パケットをレイヤ 3 キューに格納します。
- インターフェイスが送信リング上のパケットを送信してリングを空にすると、パケットを格納するために十分なバッファが再び利用可能になります。インターフェイスはバック プレッシャを解放し、レイヤ 3 プロセッサはインターフェイスへの新しいパケットをデキューします。

この通信システムの最も重要な側面は、インターフェイスが送信リングがいっぱいであることを認識し、レイヤ 3 プロセッサ システムからの新しいパケットの受信を制限するということです。したがって、インターフェイスが輻輳状態になった場合、ドロップの決定は、送信リングの First In, First Out（FIFO; 先入れ先出し）キュー内のランダムな後入れ先ドロップ決定から、レイヤ 3 プロセッサによって実装される IP レベルのサービス ポリシーに基づいたディファレンシエーテッド決定に移行されます。

パケット数および一致パケット数

サービス ポリシーは、レイヤ 3 キューに格納されているパケットにだけ適用されます。表 1 に、レイヤ 3 キューに格納されるパケットを示します。ローカルに生成されたパケットは常にプロセス スイッチド パケットとなり、インターフェイス ドライバに渡される前にまずレイヤ 3 キューに送信されます。ファスト スイッチド パケットおよびシスコ エクスプレス フォワーディング スイッチド パケットは、送信リングに直接送信され、送信リングがいっぱいになったときにだけレイヤ 3 キューに入れられます。

表 1　パケット タイプおよびレイヤ 3 キュー

パケット タイプ	輻輳	非輻輳
ローカルに生成されたパケット（Telnet パケットおよび ping を含む）	あり	あり
プロセス スイッチングが行われる他のパケット	あり	あり
シスコ エクスプレス フォワーディング スイッチングまたはファストスイッチングが行われるパケット	あり	なし

次の例では、これらのガイドラインが **show policy-map interface** コマンド出力に適用されています。4 つの主要なカウンタを太字で示しています。

```
Router# show policy-map interface atm 1/0.1

ATM1/0.1: VC 0/100 -
 Service-policy output: cbwfq (1283)
   Class-map: A (match-all) (1285/2)
    28621 packets, 7098008 bytes
     5 minute offered rate 10000 bps, drop rate 0 bps
     Match: access-group 101 (1289)
     Weighted Fair Queueing
       Output Queue: Conversation 73
       Bandwidth 500 (kbps) Max Threshold 64 (packets)
       (pkts matched/bytes matched) 28621/7098008
       (depth/total drops/no-buffer drops) 0/0/0
   Class-map: B (match-all) (1301/4)
     2058 packets, 148176 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
     Match: access-group 103 (1305)
     Weighted Fair Queueing
       Output Queue: Conversation 75
       Bandwidth 50 (kbps) Max Threshold 64 (packets)
       (pkts matched/bytes matched) 0/0
       (depth/total drops/no-buffer drops) 0/0/0
   Class-map: class-default (match-any) (1309/0)
     19 packets, 968 bytes
     5 minute offered rate 0 bps, drop rate 0 bps
     Match: any  (1313)
```

表 2 に、例に太字で示されているカウンタを定義します。

表 2　show policy-map interface 出力内のパケット カウンタ

カウンタ	説明
28621 packets, 7098008 bytes	クラスの基準に一致するパケットの数。このカウンタは、インターフェイスが輻輳しているかどうかにかかわらず、増分します。
(pkts matched/bytes matched) 28621/709800	インターフェイスが輻輳していたときの、クラスの基準に一致するパケットの数。つまり、インターフェイスの送信リングがいっぱいになり、ドライバと L3 プロセッサ システムが連携して、サービス ポリシーが適用される L3 キューに超過パケットを入れました。プロセス スイッチド パケットは常に L3 キューイング システムを通過するため、「一致パケット」カウンタが増分することになります。

表 2　show policy-map interface 出力内のパケット カウンタ （続き）

カウンタ	説明
Class-map: B (match-all) (1301/4)	これらの番号は、CISCO-CLASS-BASED-QOS-MIB Management Information Base（MIB; 管理情報ベース）で使用される内部 ID を定義します。現行リリースの Cisco IOS では、この値は **show policy-map** コマンド出力に表示されません。
5 minute offered rate 0 bps, drop rate 0 bps	この値を変更し、より瞬間的な値にするには、**load-interval** コマンドを使用します。最小値は 30 秒ですが、**show policy-map interface** コマンド出力に表示される統計情報は、10 秒ごとに更新されます。このコマンドは特定の瞬間におけるスナップショットを提供するため、統計情報はキュー サイズの一時的な変更を反映していないことがあります。

輻輳がない場合、超過パケットをキューイングする必要はありません。輻輳が発生した場合、パケット（シスコ エクスプレス フォワーディング スイッチド パケットおよびファスト スイッチド パケットを含む）は、レイヤ 3 キューに入れられる可能性があります。輻輳管理機能を使用する場合、インターフェイスに累積されるパケットは、インターフェイスがそれらのパケットを送信するように解放されるまでキューイングされます。そのあと、割り当てられた優先順位およびインターフェイスに対して設定されたキューイング メカニズムに従ってスケジュールされます。

通常、パケット カウンタの方が、一致パケット カウンタよりもはるかに大きくなります。2 つのカウンタの値がほぼ等しい場合、インターフェイスが大量のプロセス スイッチド パケットを受信しているか、または重度に輻輳しています。確実に最適なパケット転送を行うために、この両方の条件を調査する必要があります。

カンバセーション番号の割り当て

ルータは、サービス ポリシーが適用されたときに作成されたキューに対してカンバセーション番号を割り当てます。次に、キューおよび関連情報を表示する例を示します。

```
Router# show policy-map interface s1/0.1 dlci 100

      Serial1/0.1: DLCI 100 -
      output : mypolicy
       Class voice
        Weighted Fair Queueing
            Strict Priority
            Output Queue: Conversation 72
              Bandwidth 16 (kbps) Packets Matched 0
             (pkts discards/bytes discards) 0/0
       Class immediate-data
        Weighted Fair Queueing
            Output Queue: Conversation 73
              Bandwidth 60 (%) Packets Matched 0
              (pkts discards/bytes discards/tail drops) 0/0/0
              mean queue depth: 0
              drops: class  random   tail     min-th   max-th   mark-prob
                     0      0        0        64       128      1/10
                     1      0        0        71       128      1/10
                     2      0        0        78       128      1/10
                     3      0        0        85       128      1/10
                     4      0        0        92       128      1/10
```

```
                5       0         0         99        128       1/10
                6       0         0         106       128       1/10
                7       0         0         113       128       1/10
                rsvp    0         0         120       128       1/10
Class priority-data
 Weighted Fair Queueing
     Output Queue: Conversation 74
       Bandwidth 40 (%) Packets Matched 0 Max Threshold 64 (packets)
       (pkts discards/bytes discards/tail drops) 0/0/0
Class class-default
 Weighted Fair Queueing
     Flow Based Fair Queueing
     Maximum Number of Hashed Queues 64  Max Threshold 20 (packets)
```

各クラスに対して報告される情報には、次のものが含まれます。

- クラス定義
- 適用されるキューイング方式
- 出力キュー カンバセーション番号
- 使用されている帯域幅
- 廃棄されたパケット数
- 廃棄されたバイト数
- ドロップされたパケット数

class-default クラスは、トラフィックが、ポリシー マップ内にポリシーが定義されている他のクラスの一致基準を満たしていない場合に、そのトラフィックが誘導される宛先のデフォルト クラスです。**fair-queue** コマンドを使用すると、IP フローをソートおよび分類するダイナミック キューの数を指定できます。あるいは、ルータは、インターフェイスまたは VC 上の帯域幅から導出したデフォルトのキュー数を割り当てます。いずれの場合も、サポートされる値は 2 の累乗（16 ～ 4096 の範囲）です。

表 3 に、インターフェイスおよび ATM Permanent Virtual Circuit（PVC; 相手先固定接続）のデフォルト値を示します。

表 3　インターフェイス帯域幅の関数としてのデフォルトのダイナミック キュー数

帯域幅範囲	ダイナミック キューの数
64 kbps 以下	16
64 kbps より大きく、128 kbps 以下	32
128 kbps より大きく、256 kbps 以下	64
256 kbps より大きく、512 kbps 以下	128
512 kbps より大きい	256

表 4 に、ATM PVC 帯域幅に関連するデフォルトのダイナミック キュー数を示します。

表 4　ATM PVC 帯域幅の関数としてのデフォルトのダイナミック キュー数

帯域幅範囲	ダイナミック キューの数
128 kbps 以下	16
128 kbps より大きく、512 kbps 以下	32
512 kbps より大きく、2000 kbps 以下	64

表 4　ATM PVC 帯域幅の関数としてのデフォルトのダイナミック キュー数 （続き）

帯域幅範囲	ダイナミック キューの数
2000 kbps より大きく、8000 kbps 以下	128
8000 kbps より大きい	256

WFQ に予約されているキューの数に基づいて、Cisco IOS ソフトウェアは、表 5 に示すようにカンバセーションまたはキューの番号を割り当てます。

表 5　キューに割り当てられるカンバセーション番号

番号	トラフィックのタイプ
1 ～ 256	一般的なフローベースのトラフィック キュー。ユーザが作成したクラスに一致しないトラフィックは、class-default およびフローベースのキューの 1 つに一致します。
257 ～ 263	Cisco Discovery Protocol（CDP; シスコ検出プロトコル）および内部の高優先順位フラグでマーク付けされたパケット用に予約されています。
264	プライオリティ クラス（priority コマンドで設定されたクラス）用に予約されているキュー。**show policy-map interface** の出力でクラスの「Strict Priority」値を探してください。プライオリティ キューでは、ダイナミック キューに 8 を加算した数値に等しいカンバセーション ID が使用されます。
265 以上	ユーザ作成クラス用のキュー。

サービス ポリシーの確認

この作業では、一致パケット カウンタおよびサービス ポリシーをテストします。トラフィック フローがポリシーの入力パラメータまたは出力パラメータに一致することを確認します。たとえば、FTP サーバからファイルをダウンロードすると、受信方向に輻輳が発生します。これは、サーバが大きい MTU サイズのフレームを送信し、クライアント PC が小さい Acknowledgment（ACK; 確認応答）を返すためです。

この作業の開始前に、大きいサイズの ping および多数の ping を使用した拡張 ping で輻輳をシミュレートします。また、FTP サーバから大きいサイズのファイルのダウンロードを試行します。そのファイルは「障害となる」データであり、インターフェイス帯域幅をいっぱいにします。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface atm slot/0.***subinterface-number* **{multipoint | point-to-point}**
4. **ip address ip-address mask** [*secondary*]
5. **pvc** [*name*] *vpi/vci* [**ces** | **ilmi** | **qsaal** | **smds**]
6. **tx-ring-limit** *ring-limit*

7. **service-policy** {**input** | **output**} *policy-map-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface atm slot/0.** *subinterface-number* {**multipoint** | **point-to-point**} **例：** `Router(config)# interface atm 1/0.1 point-to-point}`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address ip-address mask** [*secondary*] **例：** `Router(config-if)# ip address 10.1.1.1 255.255.255.0`	テストするインターフェイスの IP アドレスを指定します。
ステップ 5	**pvc** [*name*] *vpi*/*vci* [**ces** | **ilmi** | **qsaal** | **smds**] **例：** `Router(config-if)# pvc cisco 0/5`	ATM PVC に名前を作成または割り当てます。任意で、ATM PVC にカプセル化タイプを指定し、インターフェイス ATM-VC コンフィギュレーション モードを開始します。
ステップ 6	**tx-ring-limit** *ring-limit* **例：** `Router(config-if-atm-vc)# tx-ring-limit 10`	インターフェイスの送信リングのサイズを縮小します。この値を小さくすると、Cisco IOS ソフトウェアでの QoS の使用が加速されます。 • 2600 および 3600 シリーズ ルータの場合は、リング制限をパケット数として指定します。7200 および 7500 シリーズ ルータの場合は、メモリ パーティクル数として指定します。
ステップ 7	**service-policy** {**input** | **output**} *policy-map-name* **例：** `Router(config-if-atm-vc)# service-policy output policy9`	入力インターフェイスまたは VC、あるいは出力インターフェイスまたは VC に、そのインターフェイスまたは VC のサービス ポリシーとして使用するポリシー マップを対応付けます。 • 一致パケット カウンタはキューイング機能の一部であり、出力方向に対応付けられたサービス ポリシーに対してだけ使用できることに注意してください。

QoS for IPv6 を実装するための設定例

ここでは、次の設定例について説明します。

• 「シスコ エクスプレス フォワーディング スイッチングの確認：例」（P.15）

- 「DSCP 値のマッチング：例」（P.15）

シスコ エクスプレス フォワーディング スイッチングの確認：例

次に、イーサネット インターフェイス 1/0/0 の **show cef interface detail** コマンドの出力例を示します。このコマンドを使用して、ポリシー決定が行われるようにシスコ エクスプレス フォワーディング スイッチングがイネーブルになっていることを確認します。シスコ エクスプレス フォワーディング スイッチングがイネーブルになっていることが示されます。

```
Router# show cef interface Ethernet 1/0/0 detail

Ethernet1/0/0 is up (if_number 9)
  Corresponding hwidb fast_if_number 9
  Corresponding hwidb firstsw->if_number 9
  Internet address is 10.2.61.8/24
  ICMP redirects are always sent
  Per packet load-sharing is disabled
  IP unicast RPF check is disabled
  Inbound access list is not set
  Outbound access list is not set
  IP policy routing is disabled
  Hardware idb is Ethernet1/0/0
  Fast switching type 1, interface type 5
  IP Distributed CEF switching enabled
  IP Feature Fast switching turbo vector
  IP Feature CEF switching turbo vector
  Input fast flags 0x0, Output fast flags 0x0
  ifindex 7(7)
  Slot 1 Slot unit 0 VC -1
  Transmit limit accumulator 0x48001A82 (0x48001A82)
  IP MTU 1500
```

DSCP 値のマッチング：例

次に、priority50 という名前のサービス ポリシーを設定してインターフェイスに対応付ける例を示します。この例では、**match dscp** コマンドに、任意のキーワード **ip** が含まれています。これは、IPv4 パケットに対してだけマッチングを行うという意味です。ipdscp15 という名前のクラス マップによって、インターフェイス ファスト イーサネット 1/0/0 に入ってくるすべてのパケットが評価されます。パケットが IPv4 パケットであり、その DSCP 値が 15 の場合、そのパケットはプライオリティ トラフィックとして処理され、50 kbps の帯域幅が割り当てられます。

```
Router(config)# class-map ipdscp15
Router(config-cmap)# match ip dscp 15
Router(config)# exit
Router(config)# policy-map priority50
Router(config-pmap)# class ipdscp15
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fa1/0/0
Router(config-if)# service-policy input priority55
```

IPv6 パケットに対してだけマッチングを行う場合は、**match protocol** コマンドに続けて、**ip** キーワードを指定せずに **match dscp** コマンドを使用します。クラス マップが **match-all** アトリビュートを持つこと（デフォルト）を確認します。

```
Router(config)# class-map ipdscp15
Router(config-cmap)# match protocol ipv6
```

```
Router(config-cmap)# match dscp 15
Router(config)# exit
```

IPv4 プロトコルと IPv6 プロトコルの両方に対してパケットをマッチングする場合は、**match dscp** コマンドを使用します。

```
Router(config)# class-map ipdscp15
Router(config-cmap)# match dscp 15
Router(config)# exit
```

その他の関連資料

ここでは、QoS for IPv6 機能の実装に関する関連資料について説明します。

関連資料

関連項目	参照先
IPv6 のサポート機能リスト	『*Cisco IOS IPv6 Configuration Guide*』の「Start Here: Cisco IOS Software Release Specifics for IPv6 Features」
IPv6 コマンド：コマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS IPv6 Command Reference*』

規格

規格	タイトル
この機能によってサポートされる新しい規格または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2474	『*Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*』
RFC 2475	『*An Architecture for Differentiated Services Framework*』
RFC 2597	『*Assured Forwarding PHB*』

RFC	タイトル
RFC 2598	『*An Expedited Forwarding PHB*』
RFC 2640	『*Internet Protocol, Version 6 Specification*』
RFC 2697	『*A Single Rate Three Color Marker*』
RFC 2698	『*A Two Rate Three Color Marker*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

QoS for IPv6 を実装するための機能情報

表 6 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。この表には、Cisco IOS Release 12.2(2)T 以降のリリースで導入または変更された機能だけを示します。

ここに記載されていないこのテクノロジーの機能情報については、「*Start Here: Cisco IOS Software Release Specifics for IPv6 Features*」を参照してください。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 6 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 6　QoS for IPv6 を実装するための機能情報

機能名	リリース	機能情報
IPv6 Quality of Service（QoS; サービス品質）	12.0(28)S[1] 12.2(33)SRA 12.2(18)SXE[2] 12.2(13)T 12.3 12.3(2)T 12.4 12.4(2)T	IPv6 環境でサポートされている QoS 機能には、パケット分類、キューイング、トラフィック シェーピング、WRED、クラスベース パケット マーキング、および IPv6 パケットのポリシングが含まれます。
IPv6 QoS：MQC パケット分類	12.2(33)SRA 12.2(18)SXE[2] 12.2(13)T 12.3 12.3(2)T 12.4 12.4(2)T	Modular QoS CLI を使用すると、トラフィック クラスを定義し、トラフィック ポリシー（ポリシー マップ）を作成および設定してから、それらのトラフィック ポリシーをインターフェイスに対応付けることができます。 この機能に関する詳細については、次の各項を参照してください。 • 「QoS for IPv6 の実装方針」（P.2） • 「IPv6 でのパケット分類」（P.3） • 「IPv6 パケットのマーキング基準の指定」（P.5）
IPv6 QoS：MQC トラフィック シェーピング	12.0(28)S[1] 12.2(33)SRA 12.2(18)SXE[2] 12.2(13)T 12.3 12.3(2)T 12.4 12.4(2)T	トラフィック シェーピングを行うと、トラフィック シェーピング機能に対して設定したパラメータで指定されているとおりに追加のパケットをキューに格納してから転送することで、パケット デキュー レートを制限できます。 この機能に関する詳細については、次の各項を参照してください。 • 「QoS for IPv6 の実装方針」（P.2） • 「IPv6 環境でのトラフィック ポリシング」（P.4） • 「show policy-map interface コマンド出力内のパケット カウンタの解釈」（P.8）
IPv6 QoS：MQC トラフィック ポリシング	12.0(28)S[1] 12.2(33)SRA 12.2(18)SXE[2] 12.2(13)T 12.3 12.3(2)T 12.4 12.4(2)T	IPv6 環境でのポリシングの設定またはコマンド使用法は、IPv4 環境の場合と同じです。 この機能に関する詳細については、次の各項を参照してください。 • 「QoS for IPv6 の実装方針」（P.2） • 「IPv6 環境でのトラフィック ポリシング」（P.4）

表 6　QoS for IPv6 を実装するための機能情報 （続き）

機能名	リリース	機能情報
IPv6 QoS：MQC パケット マーキング/再マーキング	12.0(28)S[1] 12.2(33)SRA 12.2(18)SXE[2] 12.2(13)T 12.3 12.3(2)T 12.4 12.4(2)T	クラスベース マーキングを使用すると、トラフィック管理に対して IPv6 precedence および DSCP の値を設定できます。 この機能に関する詳細については、次の各項を参照してください。 • 「QoS for IPv6 の実装方針」（P.2） • 「IPv6 ネットワークでのポリシーおよびクラスベース パケット マーキング」（P.3） • 「IPv6 環境でのトラフィック ポリシング」（P.4）
IPv6 QoS：キューイング	12.2(33)SRA 12.2(18)SXE[2] 12.2(13)T 12.3 12.3(2)T 12.4 12.4(2)T	IPv6 では、クラスベース キューイングとフローベース キューイングがサポートされています。 この機能に関する詳細については、次の各項を参照してください。 • 「QoS for IPv6 の実装方針」（P.2） • 「IPv6 ネットワークでの輻輳管理」（P.4） • 「IPv6 環境でのトラフィック ポリシング」（P.4） • 「show policy-map interface コマンド出力内のパケット カウンタの解釈」（P.8）
IPv6 QoS：MQC WRED ベース ドロップ	12.0(28)S[1] 12.2(33)SRA 12.2(18)SXE[2] 12.2(13)T 12.3 12.3(2)T 12.4 12.4(2)T	WRED は、CBWFQ の制限を超える可能性のあるパケットに対して RED ベースのドロップ ポリシーを実装します。 この機能に関する詳細については、次の各項を参照してください。 • 「QoS for IPv6 の実装方針」（P.2） • 「IPv6 トラフィックの輻輳回避」（P.4）

1. この機能は、Cisco IOS Release 12.0(28)S が稼動する Cisco 12000 シリーズ インターネット ルータ上でサポートされます。
2. Cisco IOS Release 12.2(18)SXE は、この機能をサポートしています。Cisco IOS Release 12.2(18)SXE は、Cisco Catalyst 6500 および Cisco 7600 シリーズ ルータに固有です。

RIP for IPv6 の実装

この章では、ルーティング情報プロトコル for IPv6 を設定する方法について説明します。RIP は、ルーティング メトリックとしてホップ カウントを使用するディスタンスベクトル ルーティング プロトコルです。また、小規模ネットワークで最も一般的に使用されている Interior Gateway Protocol（IGP; 内部ゲートウェイ プロトコル）です。

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「RIP for IPv6 の実装の機能情報」（P.16）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

RIP for IPv6 の実装の前提条件

- この章では、IPv6 アドレッシングおよび基本設定に精通していることを前提としています。詳細については、「*Implementing IPv6 Addressing and Basic Connectivity*」を参照してください。

- この章では、IPv4 に精通していることを前提としています。IPv4 の設定およびコマンド リファレンス情報については、「関連資料」に記載されている資料を参照してください。

RIP for IPv6 の実装に関する情報

RIP for IPv6

IPv6 RIP は、IPv4 の RIP と同様に機能し、同じ利点を提供します。RFC 2080 で詳述されている IPv6 用の RIP 拡張には、IPv6 アドレスとプレフィクスのサポート、および RIP アップデート メッセージの宛先アドレスとして、すべての RIP ルータのマルチキャスト グループ アドレス FF02::9 を使用することが含まれています。IPv6 の RIP に固有の新しいコマンドも、Cisco IOS Command-Line Interface（CLI; コマンドライン インターフェイス）に追加されています。

IPv6 RIP の Cisco IOS ソフトウェア実装では、IPv6 RIP プロセスごとに Routing Information Database（RIB; ルーティング情報データベース）と呼ばれるローカル ルーティング テーブルが維持されます。IPv6 RIP RIB には、隣接するすべてのネットワーク デバイスから学習した最良コストの IPv6 RIP ルート セットが格納されます。IPv6 RIP が 2 つの異なるネイバーから同じルートを学習し、それぞれのルートのコストが異なる場合、コストの安いルートだけがローカル RIB に格納されます。また、RIB には、RIP プロセスが RIP を実行しているネイバーにアドバタイズしている期限切れのルートも格納されます。IPv6 RIP は、期限の切れていないすべてのルートを、そのローカル RIB からマスター IPv6 RIB に挿入しようと試みます。同じルートが別のルーティング プロトコルから学習されており、そのルートの管理ディスタンスが IPv6 RIP よりも優れている場合、その RIP ルートは IPv6 RIB には追加されませんが、IPv6 RIP RIB にはそのまま残ります。

IPv6 RIP のノンストップ フォワーディング

Cisco Nonstop Forwarding（NSF; ノンストップ フォワーディング）では、ルーティング プロトコルが収束している間もパケット転送が続行され、その結果、スイッチオーバー時のルート フラップが回避されます。RP フェールオーバーが発生すると、Forwarding Information Base（FIB; 転送情報ベース）は、新たな設定によってインストール済みのパスを古いものとしてマークします。続いて、ルーティング プロトコルが再収束し、RIB および FIB に値を格納します。すべての NSF ルーティング プロトコルが収束すると、FIB に保持されている古いルートが削除されます。ルーティング プロトコルで RIB および FIB に値を再格納できなかった場合は、古いルートを検出するためにフェールセーフ タイマーが必要となります。

RIP は IPv6 NSF クライアントとして登録されます。これにより、RIP がスタンバイ上で収束を完了するまで、シスコ エクスプレス フォワーディング テーブルにインストールされている RIP ルートを使用できるという利点が得られます。

RIP for IPv6 の実装方法

サポートされているルーティング プロトコルを IPv6 で設定する場合は、ルーティング プロセスを作成し、そのルーティング プロセスをインターフェイスに対してイネーブルにして、特定のネットワークに合せてルーティング プロトコルをカスタマイズする必要があります。

（注） ここでは、IPv6 RIP ルーティング プロトコルを作成し、ルーティング プロセスをインターフェイス上でイネーブルにするための設定作業について説明します。次の各項では、RIP のカスタマイズについては詳しく説明していません。IPv6 でのプロトコルの機能は、IPv4 の場合と同じであるためです。IPv4 と IPv6 の設定の詳細およびコマンド リファレンス情報については、「関連資料」に記載されている資料を参照してください。

次の各項の作業では、IPv6 RIP を設定する方法を示します。一覧内の各作業は、必須と任意に分けています。

ここでは、次の各手順について説明します。

- 「IPv6 RIP プロセスのイネーブル化」（P.3）（必須）
- 「IPv6 RIP のカスタマイズ」（P.4）（任意）
- 「IPv6 RIP ルーティング プロセスへのルートの再配布」（P.6）（任意）
- 「IPv6 RIP ルートのルート タグの設定」（P.7）（任意）
- 「IPv6 RIP ルーティング アップデートのフィルタリング」（P.8）（任意）
- 「IPv6 RIP の設定および動作の確認」（P.10）（任意）

IPv6 RIP プロセスのイネーブル化

前提条件

IPv6 RIP を実行するようにルータを設定する前に、グローバル コンフィギュレーション モードで **ipv6 unicast-routing** コマンドを使用して IPv6 をグローバルにイネーブルにし、IPv6 RIP をイネーブルにするすべてのインターフェイス上で IPv6 をイネーブルにします。基本的な IPv6 接続作業の詳細については、「*IPv6 アドレッシングと基本接続の実装*」の章を参照してください。

グローバル値を設定または変更する場合は、手順 1 および 2 を実行してから、グローバル コンフィギュレーション モードで任意の **ipv6 router rip** コマンドを使用します（例については、「IPv6 RIP のカスタマイズ」（P.4）を参照してください）。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **interface** *type number*
5. **ipv6 rip** *name* **enable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 unicast-routing** **例：** `Router(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。
ステップ 4	**interface** *type number* **例：** `Router(config)# interface Ethernet 0/0`	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ipv6 rip** *name* **enable** **例：** `Router(config-if)# ipv6 rip process1 enable`	指定した IPv6 RIP ルーティング プロセスをインターフェイス上でイネーブルにします。

IPv6 RIP のカスタマイズ

この任意の作業は、IPv6 RIP でサポートする等価コスト パスの最大数を設定し、IPv6 RIP タイマーを調整して、デフォルトの IPv6 ルートを生成することで IPv6 RIP をカスタマイズする方法を示しています。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router rip** *word*
4. **maximum-paths** *number-paths*
5. **exit**
6. **interface** *type number*
7. **ipv6 rip** *name* **default-information** {**only** | **originate**} [**metric** *metric-value*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 router rip** *word* **例：** `Router(config)# ipv6 router rip process1`	IPv6 RIP ルーティング プロセスを設定し、IPv6 RIP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。 • *word* 引数を使用して、特定の IPv6 RIP ルーティング プロトコルを識別します。
ステップ 4	**maximum-paths** *number-paths* **例：** `Router(config-router)# maximum-paths 1`	（任意）IPv6 RIP でサポートできる等価コスト ルートの最大数を定義します。 • *number-paths* 引数は、1 ～ 64 の整数です。RIP のデフォルトは 4 パスです。
ステップ 5	**exit** **例：** `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**interface** *type number* **例：** `Router(config)# interface Ethernet 0/0`	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ipv6 rip** *name* **default-information** {**only** | **originate**} [**metric** *metric-value*] **例：** `Router(config-if)# ipv6 rip process1 default-information originate`	（任意）IPv6 デフォルト ルート（::/0）を生成し、指定したインターフェイスから送信される指定した RIP ルーティング プロセスのアップデートに含めます。 **（注）** IPv6 デフォルト ルート（::/0）がインターフェイスから発信されたあとのルーティング ループを避けるために、ルーティング プロセスではインターフェイス上で受信したすべてのデフォルト ルートを無視します。 • **only** キーワードを指定すると、デフォルト ルート（::/0）が発信されますが、このインターフェイスで送信されるアップデート内の他のすべてのルートは抑制されます。 • **originate** キーワードを指定すると、このインターフェイスで送信されるアップデート内の他のすべてのルートに加えて、デフォルト ルート（::/0）が発信されます。

IPv6 RIP ルーティング プロセスへのルートの再配布

RIP では、再配布するルートを選択するためのルート マップの使用がサポートされています。ルートは、ルート マップのプレフィクス リストを使用してプレフィクスで指定することも、ルート マップの「タグの照合」機能を使用してタグで指定することもできます。

RIP でアドバタイズできる最大メトリックは 16 であり、メトリック 16 は到達不能なルートを示します。そのため、16 以上のメトリックでルートを再配布すると、RIP はデフォルトでこれらを到達不能としてアドバタイズします。これらのルートは、ネイバー ルータでは使用されません。ユーザはこれらのルートに 15 よりも小さい再配布メトリックを設定する必要があります。

（注） ルートは 15 以下のメトリックでアドバタイズする必要があります。RIP ルータは常にインターフェイス コスト（デフォルトは 1）を受信されたルートのメトリックに追加します。ルートをメトリック 15 でアドバタイズすると、ネイバーがこれに 1 を追加し、メトリックは 16 になります。メトリック 16 は到達不能であるため、ネイバーはルーティング テーブルにそのルートをインストールしません。

メトリックを指定しなかった場合、ルートの現在のメトリックが使用されます。ルートの現在のメトリックを確認するには、**show ipv6 route** コマンドを入力します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 rip** *name* **enable**
5. **redistribute** *protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [**metric** *metric-value*] [**metric-type** {**internal** | **external**}] [**route-map** *map-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface Ethernet 0/0`	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**ipv6 rip** *word* **enable** **例：** `Router(config-if)# ipv6 router one enable`	インターフェイス上で IPv6 Routing Information Protocol（RIP; ルーティング情報プロトコル）のルーティング プロセスをイネーブルにします。
ステップ 5	**redistribute** *protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [**metric** *metric-value*] [**metric-type** {**internal** | **external**}] [**route-map** *map-name*] **例：** `Router(config-router)# redistribute bgp 65001 route-map bgp-to-rip`	指定したルートを IPv6 RIP ルーティング プロセスに再配布します。 • *protocol* 引数は、**bgp**、**connected**、**isis**、**rip**、または **static** キーワードのいずれかにすることができます。 • **rip** キーワードおよび *process-id* 引数では、IPv6 RIP ルーティング プロセスを指定します。 （注） **connected** キーワードは、IPv6 アドレスをインターフェイスに割り当てることによって自動的に確立されるルートを示します。

IPv6 RIP ルートのルート タグの設定

ルート再配布の実行時に、数値タグをルートに関連付けることができます。タグは RIP によってルートとともにアドバタイズされ、隣接するルートのルーティング テーブルにルートとともにインストールされます。

タグ付きルート（たとえば、すでにタグが付いている IPv6 ルーティング テーブル内のルート）を RIP に再配布すると、RIP は自動的にタグとルートをアドバタイズします。再配布ルート マップを使用してタグを指定した場合、RIP はルーティング テーブル タグよりもルート マップ タグを優先して使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
4. **match ipv6 address** {**prefix-list** *prefix-list-name* | *access-list-name*}
5. **set tag** tag-*value*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] **例：** `Router(config)# route-map bgp-to-rip permit 10`	ルート マップを定義し、ルート マップ コンフィギュレーション モードを開始します。 • **match** コマンドを使用して、この手順を実行します。
ステップ 4	**match ipv6 address** {**prefix-list** *prefix-list-name* | *access-list-name*} **例：** `Router(config-route-map)# match ipv6 address prefix-list bgp-to-rip-flt`	照合される IPv6 プレフィクスのリストを指定します。
ステップ 5	**set tag** *tag-value* **例：** `Router(config-route-map)# set tag 4`	再配布されるルートに関連付けるタグ値を設定します。

IPv6 RIP ルーティング アップデートのフィルタリング

配布リストを使用したルート フィルタリングにより、RIP が受信およびアドバタイズするルートを制御できます。この制御は、グローバルに実行することも、インターフェイスごとに実行することもできます。

この作業は、インターフェイス上で受信または送信される IPv6 RIP ルーティング アップデートにプレフィクス リストを適用することで、IPv6 RIP ルーティング アップデートをフィルタリングする方法を示しています。

IPv6 配布リスト

フィルタリングは、配布リストによって制御されます。入力配布リストはルート受信を制御し、入力フィルタリングはネイバーから受信されたアドバタイズメントに適用されます。入力フィルタリングをパスしたルートだけが RIP ローカル ルーティング テーブルに挿入され、IPv6 ルーティング テーブルへの挿入候補となります。

出力配布リストはルート アドバタイズメントを制御します。出力フィルタリングは、ネイバーに送信されるルート アドバタイズメントに適用されます。出力フィルタリングをパスしたルートだけがアドバタイズされます。

グローバル配布リスト（特定のインターフェイスに適用されるのではない配布リスト）は、すべてのインターフェイスに適用されます。配布リストでインターフェイスを指定している場合、その配布リストはそのインターフェイスにしか適用されません。

インターフェイス配布リストが常に優先されます。たとえば、インターフェイス上でルートが受信されると、インターフェイス フィルタが deny に設定され、グローバル フィルタが permit に設定されている場合、ルートはブロックされます。また、インターフェイス フィルタでは渡され、グローバル フィルタではブロックされる場合、ルートは渡されます。

IPv6 プレフィクス リストのオペランド キーワード

IPv6 プレフィクス リストは、permit 文または deny 文を適用する前に照合が必要な特定のプレフィクスまたはプレフィクスの範囲を指定するために使用されます。2 つのオペランド キーワードを使用して、照合するプレフィクス長の範囲を指定できます。ある値以下のプレフィクス長は、**le** キーワードで

設定します。ある値以上のプレフィクス長は、**ge** キーワードを使用して指定します。**ge** および **le** キーワードを使用すると、通常の *ipv6-prefix*/*prefix-length* 引数よりも詳細に、照合するプレフィクス長の範囲を指定できます。プレフィクス リストのエントリと照合される候補プレフィクスに対して、次の 3 つの条件が存在する可能性があります。

- 候補プレフィクスは、指定したプレフィクス リストおよびプレフィクス長エントリと一致している必要があります。
- 省略可能な **le** キーワードの値によって、許可されるプレフィクス長が、*prefix-length* 引数から **le** キーワードの値（この値を含む）までの範囲で指定されます。
- 省略可能な **ge** キーワードの値によって、許可されるプレフィクス長が、**ge** キーワードの値から 128（この値を含む）までの範囲で指定されます。

（注） 最初の条件は、他の条件が有効になる前に一致している必要があることに注意してください。

ge または **le** キーワードを指定しなかった場合は、完全一致であると想定されます。1 つのキーワード オペランドだけを指定した場合、そのキーワードの条件が適用され、もう 1 つの条件は適用されません。*prefix-length* 値は、**ge** 値よりも小さい必要があります。**ge** 値は、**le** 値以下である必要があります。**le** 値は、128 以下である必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 prefix list** *prefix-list-name* [**seq** *seq-number*] {**deny** *ipv6-prefix*/*prefix-length* | **description** *text*} [**ge** *ge-value*] [**le** *le-value*]
4. **ipv6 prefix list** *prefix-list-name* [**seq** *seq-number*] {**permit** *ipv6-prefix*/*prefix-length* | **description** *text*} [**ge** *ge-value*] [**le** *le-value*]
5. プレフィクス リストの構築に必要な数だけ、ステップ 3 および 4 を繰り返します。
6. **ipv6 router rip** *name*
7. **distribute-list prefix-list** *prefix-list-name* {**in** | **out**} [*interface-type interface-number*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 prefix list** *prefix-list-name* [**seq** *seq-number*] {**deny** *ipv6-prefix*/*prefix-length* | **description** *text*} [**ge** *ge-value*] [**le** *le-value*] **例：** `Router(config)# ipv6 prefix-list abc permit 2001:0db8::/16`	IPv6 プレフィクス リストのエントリを作成します。
ステップ 4	**ipv6 prefix list** *prefix-list-name* [**seq** *seq-number*] {**deny** *ipv6-prefix*/*prefix-length* | **description** *text*} [**ge** *ge-value*] [**le** *le-value*] **例：** `Router(config)# ipv6 prefix-list abc deny ::/0`	IPv6 プレフィクス リストのエントリを作成します。
ステップ 5	プレフィクス リストの構築に必要な数だけ、ステップ 3 および 4 を繰り返します。	—
ステップ 6	**ipv6 router rip** *name* **例：** `Router(config)# ipv6 router rip process1`	IPv6 RIP ルーティング プロセスを設定します。
ステップ 7	**distribute-list prefix-list** *prefix-list-name* {**in** | **out**} [*interface-type interface-number*] **例：** `Router(config-rtr-rip)# distribute-list prefix-list process1 in ethernet 0/0`	インターフェイス上で受信または送信される IPv6 RIP ルーティング アップデートに、プレフィクス リストを適用します。

IPv6 RIP の設定および動作の確認

ユーザは IPv6 RIP の設定および動作を確認できます。この作業では、IPv6 RIP の情報を表示して、設定および動作を確認する方法を示します。

手順の概要

1. **show ipv6 rip** [*name*] [**database** | **next-hops**]
2. **show ipv6 route** [*ipv6-address* | *ipv6-prefix*/*prefix-length* | *protocol* | *interface-type interface-number*]
3. **enable**
4. **debug ipv6 rip** [*interface-type interface-number*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show ipv6 rip** [*name*] [**database** | **next-hops**] **例：** `Router> show ipv6 rip process1 database`	（任意）現在の IPv6 RIP プロセスに関する情報を表示します。 • この例の場合、指定した IPv6 RIP プロセスの IPv6 RIP プロセス データベース情報が表示されます。
ステップ 2	**show ipv6 route** [*ipv6-address* | *ipv6-prefix*/*prefix-length* | *protocol* | *interface-type interface-number*] **例：** `Router> show ipv6 route rip`	（任意）IPv6 ルーティング テーブルの現在の内容を表示します。 • この例では、IPv6 RIP ルートだけが表示されます。
ステップ 3	**enable** **例：** `Router> enable`	特権 EXEC モードなど、高位の権限レベルをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 4	**debug ipv6 rip** [*interface-type interface-number*] **例：** `Router# debug ipv6 rip`	（任意）IPv6 RIP ルーティング トランザクションのデバッグ メッセージを表示します。

例

- 「show ipv6 rip コマンドの出力例」（P.11）
- 「show ipv6 route コマンドの出力例」（P.12）
- 「debug ipv6 rip コマンドの出力例」（P.12）

show ipv6 rip コマンドの出力例

次の例では、**show ipv6 rip** コマンドを使用して、現在のすべての IPv6 RIP プロセスに関する出力情報を表示しています。

```
Router> show ipv6 rip

RIP process "process1", port 521, multicast-group FF02::9, pid 62
     Administrative distance is 120. Maximum paths is 1
     Updates every 5 seconds, expire after 15
     Holddown lasts 10 seconds, garbage collect after 30
     Split horizon is on; poison reverse is off
     Default routes are generated
     Periodic updates 223, trigger updates 1
  Interfaces:
    Ethernet0/0
  Redistribution:
    Redistributing protocol bgp 65001 route-map bgp-to-rip
```

次の例では、**show ipv6 rip** コマンドで *name* 引数および **database** キーワードを指定して、指定した IPv6 RIP プロセス データベースに関する出力情報を表示しています。次に示す process1 という名前の IPv6 RIP プロセスの出力には、タイマー情報が表示されており、ルート 2001:0db8::16/64 にはルート タグが設定されています。

```
Router> show ipv6 rip process1 database
```

```
RIP process "process1", local RIB
 2001:0db8::/64, metric 2
     Ethernet0/0/FE80::A8BB:CCFF:FE00:B00, expires in 13 secs
 2001:0db8::/16, metric 2 tag 4, installed
     Ethernet0/0/FE80::A8BB:CCFF:FE00:B00, expires in 13 secs
 2001:0db8:1::/16, metric 2 tag 4, installed
     Ethernet0/0/FE80::A8BB:CCFF:FE00:B00, expires in 13 secs
 2001:0db8:2::/16, metric 2 tag 4, installed
     Ethernet0/0/FE80::A8BB:CCFF:FE00:B00, expires in 13 secs
 ::/0, metric 2, installed
     Ethernet0/0/FE80::A8BB:CCFF:FE00:B00, expires in 13 secs
```

次の例では、**show ipv6 rip** ユーザ EXEC コマンドで *name* 引数および **next-hops** キーワードを指定して、指定した IPv6 RIP プロセスに関する出力情報を表示しています。

```
Router> show ipv6 rip process1 next-hops

RIP process "process1", Next Hops
  FE80::A8BB:CCFF:FE00:A00/Ethernet0/0 [4 paths]
```

show ipv6 route コマンドの出力例

ルートの現在のメトリックは、**show ipv6 route** コマンドを入力することで確認できます。次の例では、**show ipv6 route** コマンドで **rip** プロトコル キーワードを指定して、すべての IPv6 RIP ルートに関する出力情報を表示しています。

```
Router> show ipv6 route rip

IPv6 Routing Table - 17 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
R   2001:0db8:1::/32 [120/2]
     via FE80::A8BB:CCFF:FE00:A00, Ethernet0/0
R   2001:0db8:2::/32 [120/2]
     via FE80::A8BB:CCFF:FE00:A00, Ethernet0/0
R   2001:0db8:3::/32 [120/2]
     via FE80::A8BB:CCFF:FE00:A00, Ethernet0/0
```

debug ipv6 rip コマンドの出力例

次の例では、**debug ipv6 rip** コマンドを使用して、IPv6 RIP ルーティング トランザクションのデバッグ メッセージを表示しています。

（注） デフォルトでは、**debug** コマンドからの出力、およびシステム エラー メッセージがコンソールに送信されます。デバッグ出力を再誘導するには、特権 EXEC モード内で **logging** コマンド オプションを使用します。指定できる宛先として、コンソール、仮想端末、内部バッファ、および syslog サーバを実行している UNIX ホストがあります。

```
Router# debug ipv6 rip

RIPng: Sending multicast update on Ethernet0/0 for process1
       src=FE80::A8BB:CCFF:FE00:B00
       dst=FF02::9 (Ethernet0/0)
       sport=521, dport=521, length=112
       command=2, version=1, mbz=0, #rte=5
       tag=0, metric=1, prefix=2001:0db8::/64
       tag=4, metric=1, prefix=2001:0db8:1::/16
       tag=4, metric=1, prefix=2001:0db8:2;:/16
```

```
        tag=4, metric=1, prefix=2001:0db8:3::/16
        tag=0, metric=1, prefix=::/0
RIPng: Next RIB walk in 10032
RIPng: response received from FE80::A8BB:CCFF:FE00:A00 on Ethernet0/0 for process1
        src=FE80::A8BB:CCFF:FE00:A00 (Ethernet0/0)
        dst=FF02::9
        sport=521, dport=521, length=92
        command=2, version=1, mbz=0, #rte=4
        tag=0, metric=1, prefix=2001:0db8::/64
        tag=0, metric=1, prefix=2001:0db8:1::/32
        tag=0, metric=1, prefix=2001:0db8:2::/32
        tag=0, metric=1, prefix=2001:0db8:3::/32
```

IPv6 RIP の設定例

ここでは、次の設定例について説明します。

- 「例：IPv6 RIP の設定」（P.13）

例：IPv6 RIP の設定

次の例では、process1 という名前の IPv6 RIP プロセスをルータおよびイーサネット インターフェイス 0/0 上でイネーブルにしています。イーサネット インターフェイス 0/0 で送信されるルータ アップデート内の他のすべてのルートに加えて、IPv6 デフォルト ルート（::/0）がアドバタイズされます。また、プレフィクス リストと一致するルートがタグ付けされるルート マップに応じて、BGP ルートが process1 という名前の RIP プロセスに再配布されます。パラレル パスの数は、ルート タギングを実行できるように 1 に設定され、IPv6 RIP タイマーが調整されます。eth0/0-in-flt という名前のプレフィクス リストによって、イーサネット インターフェイス 0/0 のインバウンド ルーティング アップデートがフィルタリングされます。

```
ipv6 router rip process1
 maximum-paths 1
 redistribute bgp 65001 route-map bgp-to-rip
 distribute-list prefix-list eth0/0-in-flt in Ethernet0/0
!
interface Ethernet0/0
 ipv6 address 2001:0db8::/64 eui-64
 ipv6 rip process1 enable
 ipv6 rip process1 default-information originate
!
ipv6 prefix-list bgp-to-rip-flt seq 10 deny 2001:0db8:3::/16 le 128
ipv6 prefix-list bgp-to-rip-flt seq 20 permit 2001:0db8:1::/8 le 128
!
ipv6 prefix-list eth0/0-in-flt seq 10 deny ::/0
ipv6 prefix-list eth0/0-in-flt seq 15 permit ::/0 le 128
!
route-map bgp-to-rip permit 10
 match ipv6 address prefix-list bgp-to-rip-flt
 set tag 4
```

関連情報

他の IPv6 ルーティング プロトコルを実装する場合は、「*Implementing IS-IS for IPv6*」または「*Implementing Multiprotocol BGP for IPv6*」の章を参照してください。

その他の関連資料

関連資料

関連項目	参照先
IPv4 RIP の設定作業	『*Cisco* IOS IP Routing Protocols Configuration Guide』の「Configuring Routing Information Protocol」
RIP コマンド：完全なコマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS IP Routing Protocols Command Reference*』の「RIP Commands」
IPv6 のサポート機能リスト	『*Cisco IOS IPv6 Configuration Guide*』の「Start Here: Cisco IOS Software Release Specifics for IPv6 Features」
IPv6 コマンド：コマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS IPv6 Command Reference*』

規格

規格	タイトル
この機能によってサポートされる新しい規格または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
•	選択したプラットフォーム、Cisco ソフトウェア リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2080	『*RIPng for IPv6*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

RIP for IPv6 の実装の機能情報

表 1 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どのソフトウェア イメージが特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1　RIP for IPv6 の実装の機能情報

機能名	リリース	機能情報
IPv6 ルーティング：RIP for IPv6（RIPng）	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA1 2.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	IPv6 用の RIP 拡張には、IPv6 アドレスとプレフィクスのサポート、および RIP アップデート メッセージの宛先アドレスとして、すべての RIP ルータのマルチキャスト グループ アドレス FF02::9 を使用することが含まれています。 このマニュアルでは、この機能について説明しています。
IPv6 ルーティング：ルート再配布	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA1 2.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T	ルートは、ルート マップのプレフィクス リストを使用してプレフィクスで指定することも、ルート マップの「タグの照合」機能を使用してタグで指定することもできます。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 RIP ルーティング プロセスへのルートの再配布」（P.6） • 「IPv6 RIP ルートのルート タグの設定」（P.7） • 「例：IPv6 RIP の設定」（P.13）
IPv6：RIPng ノンストップ フォワーディング	12.2(33)SRE	IPv6 RIPng ノンストップ フォワーディング機能がサポートされています。 この機能に関する詳細については、次の項を参照してください。 • 「IPv6 RIP のノンストップ フォワーディング」（P.2）

IPv6 での選択的パケット廃棄の実装

このマニュアルでは、IPv6 の Selective Packet Discard（SPD; 選択的パケット廃棄）機能について説明します。IPv6 の SPD 機能は、Route Processor（RP; ルート プロセッサ）上でプロセス レベル入力キューを管理します。SPD では、プロセス レベル キューに輻輳が発生している間、ルーティング プロトコル パケットや、その他の重要なトラフィック制御レイヤ 2 キープアライブが優先されます。

機能情報の確認

お使いのソフトウェア リリースが、このモジュールで説明されている機能の一部をサポートしていないことがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「IPv6 で選択的パケット廃棄を実装するための機能情報」（P.8）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

目次

IPv6 での選択的パケット廃棄の実装に関する情報

IPv6 での SPD の概要

SPD メカニズムは、RP 上でプロセス レベル入力キューを管理します。SPD では、プロセス レベル キューに輻輳が発生している間、ルーティング プロトコル パケットや、その他の重要なトラフィック制御レイヤ 2 キープアライブが優先されます。

SPD ステート チェック

RP 上の IPv6 プロセス入力キューでは、SPD ステート チェックが実行されます。IP precedence が 7 などのプライオリティの高いパケットは、SPD の対象にはならず、決してドロップされることはありません。一方、それ以外のすべてのパケットは、IPv6 パケット入力キューの長さと SPD ステートに従ってドロップされる可能性があります。SPD ステートには次の種類があります。

- normal：キュー サイズが最大値未満です。
- full drop：キュー サイズが最大値以上です。

normal ステートでは、正しい形式と不正な形式のパケットがルータでドロップされることはありません。full drop ステートでは、正しい形式と不正な形式のすべてのパケットがルータでドロップされます。

SPD モード

ユーザは、ルータが特定の SPD ステートになったときに、IPv6 SPD モードをイネーブルにできます。IPv6 SPD が random drop ステートの場合、SPD aggressive drop モードにより、不正な形式のパケットがドロップされます。OSPF モードでは、OSPF パケットを SPD プライオリティで処理できます。

SPD ステートは、プロセス入力キューのサイズに応じて normal（ドロップなし）、random drop、または max になります。プロセス入力キューが SPD 最小しきい値よりも小さい場合、SPD は何も行わず、normal ステートになります。normal ステートでは、パケットはドロップされません。入力キューが最大しきい値に到達すると、SPD は max ステートになります。このステートでは、通常プライオリティのパケットが廃棄されます。入力キューが最小しきい値と最大しきい値の間にある場合、SPD は random drop ステートになります。このステートでは、通常パケットがドロップされることがあります。

SPD ヘッドルーム

SPD では、通常の IPv6 パケットの動作は変更されません。一方、ルーティング プロトコル パケットは、SPD が IPv6 precedence フィールドで認識するため、より高いプライオリティが与えられます。したがって、IPv6 precedence が 7 に設定されていると、そのパケットが優先されます。

SPD では、precedence が 7 の IPv6 パケットを優先させるために、それらを通常の入力キュー制限を超えてプロセス レベル入力キューにキューイングすることを Cisco IOS ソフトウェアに許可します。通常の制限を超えて許可されるパケットの数は、SPD ヘッドルームと呼ばれます。SPD ヘッドルームのデフォルトは 100 です。つまり、precedence の高いパケットは、入力保持キューのサイズが 175（入力キューのデフォルト サイズ + SPD ヘッドルーム サイズ）よりも小さければドロップされません。

Connectionless Network Service Intermediate System-to-Intermediate System（CLNS IS-IS）パケット、PPP パケット、High-Level Data Link Control（HDLC; ハイレベル データリンク コントロール）キープアライブなどの非 IPv6 パケットは、レイヤ 3 ではなくレイヤ 2 であるため、通常のプライオリティとして処理されました。さらに、レイヤ 3 以上で動作する Interior Gateway Protocol（IGP; 内部ゲートウェイ プロトコル）は、通常の IPv6 パケットよりも優先されますが、Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）とは同じプライオリティが与えられます。そのため、BGP コンバージェンス中または BGP アクティビティが非常に活発な間は、IGP の hello および keepalive がドロップされて IGP 隣接関係が失われることがよくありました。

IGP とリンクの安定性は微妙かつ重要な問題であるため、こうしたパケットには最高のプライオリティが与えられ、デフォルトが 10 パケットの拡張 SPD ヘッドルームも与えられます。これらのパケットは、入力保持キューのサイズが 185（入力キューのデフォルト サイズ + SPD ヘッドルーム サイズ + SPD 拡張ヘッドルーム）未満であれば、ドロップされません。

IPv6 での選択的パケット廃棄の実装方法

SPD プロセス入力キューの設定

IPv6 での SPD 機能は、デフォルトでイネーブルになっています。IPv6 SPD プロセス入力キュー内の最大および最小パケット数を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 spd queue max-threshold** *value*
4. **ipv6 spd queue min-threshold** *value*
5. **exit**
6. **show ipv6 spd**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 spd queue max-threshold** *value* **例：** `Router(config)# ipv6 spd queue max-threshold 100`	SPD プロセス入力キュー内の最大パケット数を設定します。
ステップ 4	**ipv6 spd queue min-threshold** *value* **例：** `Router(config)# ipv6 spd queue min-threshold 4094`	IPv6 SPD プロセス入力キュー内の最小パケット数を設定します。 **（注）** この最小しきい値は、最大しきい値の設定よりも小さくする必要があります。

	コマンドまたはアクション	目的
ステップ 5	**exit** **例：** `Router(config)# exit`	ルータを特権 EXEC モードに戻します。
ステップ 6	**show ipv6 spd** **例：** `Router# show ipv6 spd`	IPv6 SPD 設定を表示します。

SPD モードの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 spd mode** {**aggressive** | **tos protocol ospf**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 spd mode** {**aggressive**	**tos protocol ospf**} **例：** `Router(config)# ipv6 spf mode aggressive`	IPv6 SPD モードを設定します。

SPD ヘッドルームの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **spd headroom** *size*
4. **spd extended-headroom** *size*
5. **exit**
6. **show ipv6 spd**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**spd headroom** *size* **例：** `Router(config)# spd headroom 200`	SPD ヘッドルームを設定します。
ステップ 4	**spd extended-headroom** *size* **例：** `Router(config)# spd extended-headroom 11`	拡張 SPD ヘッドルームを設定します。
ステップ 5	**exit** **例：** `Router(config)# exit`	ルータを特権 EXEC モードに戻します。
ステップ 6	**show ipv6 spd** **例：** `Router# show ipv6 spd`	IPv6 SPD 設定を表示します。

IPv6 で選択的パケット廃棄を実装するための設定例

例：SPD プロセス入力キューの設定

次に、SPD プロセス入力キュー設定の例を示します。最大プロセス入力キューしきい値は 1、SPD ステートは normal です。ヘッドルームと拡張ヘッドルームの各値はデフォルトに設定されています。

```
Router# ipv6 spd queue max-threshold 1
Router# show ipv6 spd

Current mode: normal
Queue max threshold: 1, Headroom: 100, Extended Headroom: 10
IPv6 packet queue: 0
```

その他の参考資料

関連資料

関連項目	参照先
IPv6 のサポート機能リスト	『*Cisco IOS IPv6 Configuration Guide*』の「Start Here: Cisco IOS Software Release Specifics for IPv6 Features」
IPv6 コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト、使用に関する注意事項、および例	『*Cisco IOS IPv6 Command Reference*』

規格

規格	タイトル
この機能によってサポートされる新しい規格または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2474	『*Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*』
RFC 4594	『*Configuration Guidelines for DiffServ Service Classes*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 で選択的パケット廃棄を実装するための機能情報

表 1 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どのソフトウェア イメージが特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1　IPv6 で選択的パケット廃棄を実装するための機能情報

機能名	リリース	機能情報
IPv6 選択的パケット廃棄	12.2(33)SRC 12.2(33)SXH 15.0(1)S	SPD メカニズムは、RP 上でプロセス レベル入力キューを管理します。SPD では、プロセス レベル キューに輻輳が発生している間、ルーティング プロトコル パケットや、その他の重要なトラフィック制御レイヤ 2 キープアライブが優先されます。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 での SPD の概要」（P.2） • 「SPD プロセス入力キューの設定」（P.3） • 「SPD ヘッドルームの設定」（P.4） • 「例：SPD プロセス入力キューの設定」（P.5） **ipv6 spd queue max-threshold**、**show ipv6 spd**、**spd extended-headroom**、**spd headroom** の各コマンドが導入または修正されました。
IPv6：完全な選択的パケット廃棄サポート	15.1(3)T	ユーザは、ルータが特定の SPD ステートになったときの IPv6 SPD モードを設定できるようになりました。 この機能に関する詳細については、次の各項を参照してください。 • 「SPD モード」（P.2） • 「SPD プロセス入力キューの設定」（P.3） • 「SPD モードの設定」（P.4） **clear ipv6 spd**、**debug ipv6 spd**、**ipv6 spd mode**、**ipv6 spd queue max-threshold**、**ipv6 spd queue min-threshold**、**monitor event-trace ipv6 spd**、**show ipv6 spd**、**spd extended-headroom**、**spd headroom** の各コマンドが導入または修正されました。

IPv6 向けスタティック ルートの実装

この章では、IPv6 向けのスタティック ルートを設定する方法について説明します。ルーティングでは、ネットワーク内でパケットが通過するパスを定義します。外部ネットワークへのパスが 1 つしかない小規模ネットワークやネットワーク セクションの場合は、ダイナミック ルーティング プロトコルの代わりに、手動で設定したスタティック ルートを使用できます。冗長性がないと、スタティック ルートの利便性が制限されます。また、大規模ネットワークの場合、手動でルートを再設定すると、管理上のオーバーヘッドが大きくなる可能性があります。

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「IPv6 向けスタティック ルートの実装の機能情報」（P.16）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

IPv6 向けスタティック ルートの実装の前提条件

- このマニュアルでは、IPv4 に精通していることを前提としています。IPv4 の設定およびコマンド リファレンス情報については、「関連資料」の関連資料を参照してください。
- スタティック IPv6 ルートを使用するルータを設定する前に、**ipv6 unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 パケットの転送をイネーブルにし、1 つ以上のインターフェイスで IPv6 をイネーブルにし、そのインターフェイスで IPv6 アドレスをイネーブルにする必要があります。基本的な IPv6 接続作業の詳細については、「*Implementing Ipv6 Addressing and Basic Connectivity*」の章を参照してください。

IPv6 向けスタティック ルートの実装に関する情報

スタティック ルート

ネットワーキング デバイスでは、手動で設定したルート情報、またはルーティング プロトコルを使用してダイナミックに学習し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、手動で設定され、2 つのネットワーク デバイス間の明示パスを定義します。ダイナミック ルーティング プロトコルとは異なり、スタティック ルートは動的に更新されず、ネットワーク トポロジが変更された場合は手動で再設定する必要があります。スタティック ルートを使用する利点は、セキュリティとリソースの効率性です。スタティック ルートでは、ダイナミック ルーティング プロトコルよりも少ない帯域幅を使用し、ルートの計算および通信に CPU サイクルが使用されません。スタティック ルートを使用する場合の主なデメリットは、ネットワーク トポロジが変更された場合に自動的に再設定されないことです。

スタティック ルートはダイナミック ルーティング プロトコルに再配布できますが、ダイナミック ルーティング プロトコルによって生成されたルートは、スタティック ルーティング テーブルに再配布できません。スタティック ルートを使用するルーティング ループの設定を回避するアルゴリズムはありません。

スタティック ルートは、外部ネットワークへのパスが 1 つしかない小規模ネットワークでは有用です。また、大規模ネットワークの場合は、より厳格な制御が必要な、他のネットワークへの特定のタイプのトラフィックやリンクにセキュリティを提供します。一般に、大半のネットワークでは、ダイナミック ルーティング プロトコルを使用してネットワーキング デバイス間の通信を行いますが、特殊なケース用として 1 つまたは 2 つのスタティック ルートを設定している場合があります。

直接接続されているスタティック ルート

直接接続されているスタティック ルートでは、出力インターフェイスだけが指定されます。宛先は、出力インターフェイスに直接接続されていると想定されるため、パケットの宛先はネクストホップ アドレスとして使用されます。次に、このような定義の例を示します。

```
ipv6 route 2001:0DB8::/32 ethernet1/0
```

この例では、アドレス プレフィクス 2001:0DB8::/32 を持つすべての宛先が、インターフェイス Ethernet1/0 を介して直接到着可能であることを指定しています。

直接接続されたスタティック ルートは、有効な IPv6 インターフェイス（つまり、アップ状態にあり、かつ IPv6 がイネーブルになっているインターフェイス）を示している場合にかぎり、IPv6 ルーティング テーブルに挿入される候補となります。

再帰スタティック ルート

再帰スタティック ルートでは、ネクストホップだけが指定されます。出力インターフェイスは、ネクストホップから得られます。次に、このような定義の例を示します。

```
ipv6 route 2001:0DB8::/32 2001:0DB8:3000:1
```

この例では、アドレス プレフィクス 2001:0DB8::/32 を持つすべての宛先が、アドレス 2001:0DB8:3000:1 を持つホストを介して到着可能であることを指定しています。

再帰スタティック ルートが有効である（つまり、IPv6 ルーティング テーブルに挿入される候補である）のは、指定したネクストホップが直接的または間接的に有効な IPv6 出力インターフェイスに解決され、ルートが自己再帰型ではなく、再帰深度が IPv6 転送の最大再帰深度を超えていない場合だけです。

ルートは、ルート自身が独自のネクストホップを解決するために使用される場合、自己再帰型となります。たとえば、IPv6 ルーティング テーブルに次のルートがあるとします。

```
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
R   2001:0DB8::/32 [130/0]
     via ::, Serial2/0
B   2001:0DB8:3000:0/16 [200/45]
     Via 2001:0DB8::0104
```

次の例では、再帰 IPv6 スタティック ルートを定義します。

```
ipv6 route
2001:0DB8::/32 2001:0BD8:3000:1
```

このスタティック ルートは、自己再帰型であるため、IPv6 ルーティング テーブルには挿入されません。スタティック ルートのネクストホップ 2001:0DB8:3000:1 は、自身が再帰ルートである（つまり、ネクストホップだけを指定する）BGP ルート 2001:0DB8:3000:0/16 を介して解決されます。BGP ルートのネクストホップ 2001:0DB8::0104 は、スタティック ルートを介して解決されます。したがって、スタティック ルートは、スタティック ルート自身のネクストホップを解決するために使用されることになります。

一般に、自己再帰型スタティック ルートの手動設定は禁止されていませんが、有用ではありません。ただし、IPv6 ルーティング テーブルに挿入された再帰スタティック ルートが、ダイナミック ルーティング プロトコルを介して学習された、ネットワークでの何らかの一時的変更の結果として自己再帰になる場合があります。このような状況が発生すると、スタティック ルートが自己再帰になった事実が検出され、そのスタティック ルートは IPv6 ルーティング テーブルから削除されます（設定からは削除されません）。以降のネットワーク変更によって、スタティック ルートが自己再帰でなくなる場合があります。この場合、そのスタティック ルートは IPv6 ルーティング テーブルに再挿入されます。

（注） Cisco IOS Release 12.2(15)T 以降のリリースでは、IPv6 再帰スタティック ルートが 1 分おきにチェックされます。したがって、再帰スタティック ルートは、そのネクストホップが有効になったあと、ルーティング テーブルに挿入されるまで最大 1 分かかる場合があります。同様に、ルートのネクストホップが無効になったあと、ルーティング テーブルからそのルートが削除されるまでに 1 分ほどかかる場合があります。

完全指定のスタティック ルート

完全指定のスタティック ルートでは、出力インターフェイスとネクストホップの両方が指定されています。この形式のスタティック ルートは、出力インターフェイスがマルチアクセス インターフェイスであり、ネクストホップを明示的に識別する必要がある場合に使用されます。ネクストホップは、指定した出力インターフェイスに直接接続されている必要があります。次の例では、完全指定のスタティック ルートの定義を示します。

```
ipv6 route 2001:DB8:/32 ethernet1/0 2001:0DB8:3000:1
```

完全指定のルートが有効である（つまり、IPv6 ルーティング テーブルに挿入される候補である）のは、指定した IPv6 インターフェイスが IPv6 対応であり、かつアップ状態となっている場合です。

フローティング スタティック ルート

フローティング スタティック ルートは、設定されたルーティング プロトコルを介して学習されたダイナミック ルートのバックアップに使用されるスタティック ルートです。フローティング スタティック ルートは、バックアップしているルーティング プロトコルよりも高い管理ディスタンスを使用して設定されます。このため、ルーティング プロトコルを介して学習されたダイナミック ルートは、フローティング スタティック ルートよりも常に優先して使用されます。ルーティング プロトコルを介して学習されたダイナミック ルートが失われると、フローティング スタティック ルートが代わりに使用されます。次に、フローティング スタティック ルートを定義する例を示します。

```
ipv6 route 2001:DB8:/32 ethernet1/0 2001:0DB8:3000:1 210
```

3 つのタイプの IPv6 スタティック ルートのいずれも、フローティング スタティック ルートとして使用できます。フローティング スタティック ルートは、ダイナミック ルーティング プロトコルよりも大きい管理ディスタンスを使用して設定する必要があります。これは、小さい管理ディスタンスが設定されたルートの方が優先されるためです。

（注） デフォルトで、スタティック ルートはダイナミック ルートよりも小さい管理ディスタンスを持っているため、スタティック ルートは、ダイナミック ルートよりも優先して使用されます。

IPv6 向けスタティック ルートの実装方法

ここでは、スタティック IPv6 ルートの設定方法について説明します。

スタティック IPv6 ルートの設定

ここでは、デフォルトのスタティック IPv6 ルート、ポイントツーポイント インターフェイスを介したスタティック IPv6 ルート、およびマルチアクセス インターフェイスに対するスタティック IPv6 ルートを設定する方法について説明します。

IPv6 でのスタティック ルート

ipv6 route コマンドを使用して、IPv6 スタティック ルートを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 route** *ipv6-prefix/prefix-length* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [**tag** *tag*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 route** *ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [**tag** *tag*] **例：** `Router(config)# ipv6 route ::/0 serial 2/0`	スタティック IPv6 ルートを設定します。 • デフォルトのスタティック IPv6 ルートは、シリアル インターフェイス上で設定されます。 • この表の直後の構文例で、スタティック ルートを設定するための **ipv6 route** コマンドの特別な使用法を参照してください。

例

「手順の詳細」（P.5）に含まれている構文例に加えて、次の構文例では、さまざまなタイプのスタティック ルートを設定するための **ipv6 route** の使用法を示しています。

ポイントツーポイント インターフェイスを介して直接接続されているスタティック ルートの構文例

次に、ポイントツーポイント インターフェイスを介して直接接続されているスタティック ルートを設定する例を示します。

```
Router(config)# ipv6 route 2001:0DB8::/32 serial 0
```

ブロードキャスト インターフェイス上の直接接続されたスタティック ルートの構文例

次に、ブロードキャスト インターフェイス上の直接接続されたスタティック ルートを設定する例を示します。

```
Router(config)# ipv6 route 2001:0DB8::1/32 ethernet1/0
```

ブロードキャスト インターフェイス上の完全指定のスタティック ルートの構文例

次に、ブロードキャスト インターフェイス上の完全指定のスタティック ルートを設定する例を示します。

```
Router(config)# ipv6 route 2001:0DB8::1/32 ethernet1/0 fe80::1
```

再帰スタティック ルート

次の例では、出力インターフェイスの自動的な取得元となる、指定のネクストホップ アドレスにスタティック ルートが設定されています。

```
Router(config)# ipv6 route 2001:0DB8::/32 2001:0DB8:2002:1
```

フローティング スタティック IPv6 ルートの設定：例

ここでは、フローティング スタティック IPv6 ルートを設定する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 route** *ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [**tag** *tag*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 route** *ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [**tag** *tag*] **例：** `Router(config)# ipv6 route 2001:0DB8::/32 serial 2/0 201`	スタティック IPv6 ルートを設定します。 • この例では、フローティング スタティック IPv6 ルートが設定されます。管理ディスタンス 200 が設定されています。 • デフォルトの管理ディスタンスは、次のとおりです。 – 接続されているインターフェイス：0 – スタティック ルート：1 – Enhanced Interior Gateway Routing Protocol（EIGRP）サマリー ルート：5 – external Border Gateway Protocol（eBGP; 外部ボーダー ゲートウェイ プロトコル）：20 – 内部 Enhanced IGRP：90 – IGRP：100 – Open Shortest Path First：110 – Intermediate System-to-Intermediate System（IS-IS）：115 – Routing Information Protocol（RIP; ルーティング情報プロトコル）：120 – Exterior Gateway Protocol（EGP; 外部ゲートウェイ プロトコル）：140 – EIGRP 外部ルート：170 – 内部 BGP：200 – 不明：255

スタティック IPv6 ルートの設定と動作の確認

ここでは、スタティック IPv6 ルートの設定と動作を確認するための情報を表示する方法について説明します。

show ipv6 static コマンドを使用して、一連のスタティック ルート、および各ルートのインストール ステータス、つまり各ルートのエントリが IPv6 ルーティング テーブルに表示されるかどうかを示します。

show ipv6 route コマンドを使用して、インストールされたルートが IPv6 ルーティング テーブルに存在し、各ルート定義が、予想されるコストとメトリックを反映していることを確認します。設定したスタティック ルートが IPv6 ルーティング テーブルに表示されない場合は、テーブル内に別の送信元から

（ルーティング プロトコルからなど）のより小さい管理ディスタンスが存在する可能性があります。ルーティング テーブルに対するこのような変更は、スタティック ルートにデフォルトでない管理ディスタンスを指定した場合にだけ発生します。

より小さい管理ディスタンスが存在する場合、スタティック ルートは「フローティング」となり、ルーティング プロトコルを介して学習されたルートが失われた場合にだけルーティング テーブルに挿入されます。より小さい管理ディスタンスがルーティング テーブルに存在しない場合は、スタティック ルートが使用されます。

detail キーワードを指定した **show ipv6 static** コマンドを使用して、不一致の原因を識別します。たとえば、スタティック ルートが直接スタティック ルートである場合、そのインターフェイスはダウンしているか、または IPv6 がそのインターフェイス上でイネーブルになっていない可能性があります。

手順の概要

1. **enable**
2. **show ipv6 static** [*ipv6-address* | *ipv6-prefix*/*prefix-length*][**interface** *interface-type interface-number*] [**recursive**] [**detail**]

   または

   show ipv6 route [*ipv6-address* | *ipv6-prefix*/*prefix-length* | *protocol* | *interface-type interface-number*]
3. **debug ipv6 routing**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。

ステップ 2	**show ipv6 static** [*ipv6-address* | *ipv6-prefix*/*prefix-length*][**interface** *interface-type interface-number*] [**recursive**] [**detail**]
	
	または
	
	show ipv6 route [*ipv6-address* | *ipv6-prefix*/*prefix-length* | *protocol* | *interface-type interface-number*]
	
	例：
	`Router# show ipv6 static`
	
	または
	
	例：
	`Router# show ipv6 route static`
		IPv6 ルーティング テーブルの現在の内容を表示します。
		• これらの例は、IPv6 スタティック ルートを表示する 2 つの方法を示しています。

ステップ 3	**debug ipv6 routing** **例：** `Router# debug ipv6 routing`	IPv6 ルーティング テーブルの更新およびルート キャッシュの更新に関するデバッグ メッセージを表示します。

例

ここでは、次の出力例について説明します。

コマンド構文でオプションが指定されていない場合の show ipv6 static コマンドの出力例

このコマンドでオプションが指定されていない場合、IPv6 ルーティング テーブルにインストールされているルートは、次の例で示すように、アスタリスクでマーク付けされます。

```
Router# show ipv6 static

IPv6 Static routes
Code: * - installed in RIB
* 2001:0DB8:3000:0/16, interface Ethernet1/0, distance 1
* 2001:0DB8:4000:0/16, via nexthop 2001:0DB8:1:1, distance 1
  2001:0DB8:5000:0/16, interface Ethernet3/0, distance 1
* 2001:0DB8:5555:0/16, via nexthop 2001:0DB8:4000:1, distance 1
  2001:0DB8:5555:0/16, via nexthop 2001:0DB8:9999:1, distance 1
* 2001:0DB8:5555:0/16, interface Ethernet2/0, distance 1
* 2001:0DB8:6000:0/16, via nexthop 2001:0DB8:2007:1, interface Ethernet1/0, distance 1
```

IPv6 アドレスおよびプレフィクス コマンドを含む show ipv6 static コマンドの出力例

ipv6-address または *ipv6-prefix/prefix-length* 引数が指定されている場合、そのアドレスまたはネットワークのスタティック ルートに関する情報だけが表示されます。次に、IPv6 プレフィクス 2001:0DB8:200::/35 を入力した場合の **show ipv6 static** コマンドの出力例を示します。

```
Router# show ipv6 static 2001:0DB8:5555:0/16

IPv6 Static routes
Code: * - installed in RIB
* 2001:0DB8:5555:0/16, via nexthop 2001:0DB8:4000:1, distance 1
  2001:0DB8:5555:0/16, via nexthop 2001:9999:1, distance 2
* 2001:0DB8:5555:0/16, interface Ethernet2/0, distance 1
```

show ipv6 static interface コマンドの出力例

インターフェイスが指定されている場合、指定されたインターフェイスを発信インターフェイスとして使用するスタティック ルートだけが表示されます。**interface** キーワードは、**show ipv6 static** コマンドで指定した IPv6 アドレスおよびプレフィクスを含めて使用することも、含めずに使用することもできます。

```
Router# show ipv6 static interface ethernet3/0

IPv6 Static routes
Code: * - installed in RIB
```

show ipv6 static recursive コマンドの出力例

recursive キーワードが **show ipv6 static** コマンドで指定されている場合、再帰スタティック ルートだけが表示されます。**recursive** キーワードは、**interface** キーワードと相互排他的ですが、コマンド構文に含まれる IPv6 プレフィクス付きでも IPv6 プレフィクスなしでも使用できます。

```
Router# show ipv6 static recursive

IPv6 Static routes
Code: * - installed in RIB
* 2001:0DB8:4000:0/16, via nexthop 2001:0DB8:1:1, distance 1
* 2001:0DB8:5555:0/16, via nexthop 2001:0DB8:4000:1, distance 2
  2001:0DB8:5555:0/16, via nexthop 2001:0DB8:9999:1, distance 3
```

show ipv6 static detail コマンドの出力例

detail キーワードが指定されている場合、次の追加情報も表示されます。

- 有効な再帰ルートの場合は、出力パス セットおよび最大解決深度
- 無効な再帰ルートの場合は、ルートが有効でない理由
- 無効なダイレクト ルートまたは完全指定のルートの場合は、ルートが有効でない理由

```
Router# show ipv6 static detail

IPv6 Static routes
Code: * - installed in RIB
* 2001:0DB8:3000:0/16, interface Ethernet1/0, distance 1
* 2001:0DB8:4000:0/16, via nexthop 2001:0DB8:2001:1, distance 1
     Resolves to 1 paths (max depth 1)
     via Ethernet1/0
  2001:0DB8:5000:0/16, interface Ethernet3/0, distance 1
     Interface is down
* 2001:0DB8:5555:0/16, via nexthop 2001:0DB8:4000:1, distance 1
     Resolves to 1 paths (max depth 2)
     via Ethernet1/0
  2001:0DB8:5555:0/16, via nexthop 2001:0DB8:9999:1, distance 1
     Route does not fully resolve
* 2001:0DB8:5555:0/16, interface Ethernet2/0, distance 1
* 2001:0DB8:6000:0/16, via nexthop 2001:0DB8:2007:1, interface Ethernet1/0, distance 1
```

show ipv6 route コマンドの出力例

次の例では、**show ipv6 route** コマンドを使用して、ポイントツーポイント インターフェイスを介したスタティック ルートの設定を確認しています。

```
Router# show ipv6 route

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
S   2001:0DB8::/32 [1/0]
     via ::, Serial2/0
```

次の例では、**show ipv6 route** コマンドを使用して、マルチアクセス インターフェイス上のスタティック ルートの設定を確認しています。IPv6 リンクローカル アドレス（FE80::1）が、ネクストホップ ルータです。

```
Router# show ipv6 route

IPv6 Routing Table - 11 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
```

```
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
S   2001:0DB8::/32 [1/0]
     via FE80::1, Ethernet0/0
```

IPv6 ルーティング テーブル内のすべてのスタティック ルートを表示するには、次のように、protocol 引数の値として static を指定して **show ipv6 route static** コマンドを使用します。

```
Router# show ipv6 route static

IPv6 Routing Table - 330 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
S   2001:0DB8::/32 [1/0]
     via ::, Tunnel0
S   3FFE:C00:8011::/48 [1/0]
     via ::, Null0
S   ::/0 [254/0]
     via 2001:0DB8:2002:806B, Null
```

debug ipv6 routing コマンドの出力例

次の例では、**debug ipv6 routing** コマンドを使用して、IPv6 RIP ルートが削除された場合の、IPv6 ルーティング テーブルへのフローティング スタティック ルートのインストールを確認します。フローティング スタティック IPv6 ルートは、以前は管理ディスタンス値 130 を使用して設定されていました。RIP ルートはデフォルトで 120 の管理ディスタンスを持つため、バックアップ ルートは、フローティング スタティック ルートとして追加されており、RIP ルートが優先されるルートになります。RIP ルートが削除されると、フローティング スタティック ルートが IPv6 ルーティング テーブルにインストールされます。

```
Router# debug ipv6 routing

*Oct 10 18:28:00.847: IPv6RT0: rip two, Delete 2001:0DB8::/32 from table
*Oct 10 18:28:00.847: IPv6RT0: static, Backup call for 2001:0DB8::/32
*Oct 10 18:28:00.847: IPv6RT0: static, Add 2001:0DB8::/32 to table
*Oct 10 18:28:00.847: IPv6RT0: static, Adding next-hop :: over Serial2/0 for
2001:0DB8::/32, [130/0]
```

IPv6 向けスタティック ルートの実装の設定例

スタティック ルートは、さまざまな目的に使用できます。一般的な使用方法は、次のとおりです。

- 手動集約
- トラフィック廃棄
- デフォルトの固定ルート
- バックアップ ルート

多くの場合、Cisco IOS ソフトウェアには、同一の目的を果たすための代替メカニズムが用意されています。スタティック ルートを使用するか、またはいずれかの代替メカニズムを使用するかは、ローカルの状況によって決まります。

- 「例：手動集約の設定」（P.12）
- 「例：トラフィック廃棄の設定」（P.12）
- 「例：デフォルトの固定ルートの設定」（P.13）
- 「フローティング スタティック IPv6 ルートの設定：例」（P.6）

例：手動集約の設定

次に、RIP にアドバタイズされるローカル インターフェイス プレフィクスを集約するために使用するスタティック ルートの例を示します。スタティック ルートは、廃棄ルートとしても機能し、パケットのうち、ルータで受信され、宛先が 2001:0DB8:1::/48 で、より詳細なインターフェイス プレフィクスではカバーされないパケットを廃棄します。

```
Router> enable
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# interface ethernet0/0
Router(config-if)# ipv6 address 2001:0DB8:2:1234/64
Router(config-if)# exit
Router(config)#
Router(config)# interface ethernet1/0
Router(config-if)# ipv6 address 2001:0DB8:3:1234/64
Router(config-if)# exit
Router(config)#

Router(config)# interface ethernet2/0
Router(config-if)# ipv6 address 2001:0DB8:4:1234/64
Router(config-if)# exit
Router(config)#

Router(config)# interface ethernet3/0
Router(config-if)# ipv6 address 2001:0DB8::1234/64
Router(config-if)# ipv6 rip one enable
Router(config-if)# exit
Router(config)#

Router(config)# ipv6 router rip one
Router(config-rtr)# redistribute static
Router(config-rtr)# exit
Router(config)#

Router(config)# ipv6 route 2001:0DB8:1:1/48 null0
Router(config)# end
Router#

00:01:30: %SYS-5-CONFIG_I: Configured from console by console

Router# show ipv6 route static

IPv6 Routing Table - 3 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S   2001:0DB8:1::/48 [1/0]
     via ::, Null0
```

例：トラフィック廃棄の設定

インターフェイス null0 をポイントするようにスタティック ルートを設定することで、特定のプレフィクスへのトラフィックを廃棄できます。たとえば、プレフィクス 2001:0DB8:42:1/64 へのすべてのトラフィックを廃棄する必要がある場合は、次のスタティック ルートが定義されます。

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# ipv6 route 2001:0DB8:42:1::/64 null0
Router(config)# end
Router#
00:05:44: %SYS-5-CONFIG_I: Configured from console by console
```

例：デフォルトの固定ルートの設定

デフォルトのスタティック ルートは、多くの場合、単純なルータ トポロジで使用されます。次の例では、ルータは、イーサネット 0/0 を介してそのローカル サイトに接続され、Serial2/0 と Serial3/0 を介して主要な企業メッセージに接続されます。非ローカル トラフィックはすべて、2 つのシリアル インターフェイスを介してルーティングされます。

```
Router(config)# interface ethernet0/0
Router(config-if)# ipv6 address 2001:0DB8:17:1234/64
Router(config-if)# exit

Router(config)# interface Serial2/0
Router(config-if)# ipv6 address 2001:0DB8:1:1234/64
Router(config-if)# exit

Router(config)# interface Serial3/0
Router(config-if)# ipv6 address 2001:0DB8:2:124/64
Router(config-if)# exit

Router(config)# ipv6 route ::/0 Serial2/0
Router(config)# ipv6 route ::/0 Serial3/0
Router(config)# end
Router#

00:06:30: %SYS-5-CONFIG_I: Configured from console by console
Router# show ipv6 route static

IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S   ::/0 [1/0]
     via ::, Serial2/0
     via ::, Serial3/0
```

例：フローティング スタティック ルートの設定

多くの場合、フローティング スタティック ルートは、接続の問題が発生した場合にバックアップ パスを提供するために使用されます。次の例では、ルータは、Serial2/0 を介したネットワーク コアへの接続を持ち、IS-IS を介してルート 2001:0DB8:1:1/32 を学習しています。Serial2/0 インターフェイスに障害が発生するか、またはルート 2001:0DB8:1:1/32 が IS-IS を介して学習されなくなった（ネットワークのいずれかの箇所で接続が失われていることを示します）場合、トラフィックはバックアップ ISDN インターフェイスを介してルーティングされます。

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Router(config)# interface ethernet0/0
Router(config-if)# ipv6 address 2001:0DB8:17:1234/64
Router(config-if)# exit

Router(config)# interface Serial2/0
Router(config-if)# ipv6 address 2001:0DB8:1:1234/64
Router(config-if)# ipv6 router isis
Router(config-if)# exit

Router(config)# router isis
Router(config-router)# net 42.0000.0000.0000.0001.00
Router(config-router)# exit

Router(config)# interface BRI1/0
Router(config-if)# encapsulation ppp
Router(config-if)# ipv6 enable
Router(config-if)# isdn switch-type basic-net3
Router(config-if)# ppp authentication chap optional
Router(config-if)# ppp multilink
Router(config-if)# exit

Router(config)# dialer-list 1 protocol ipv6 permit
Router(config)# ipv6 route 2001:0DB8:1::/32 BRI1/0 200
Router(config)# end
Router#
00:03:07: %SYS-5-CONFIG_I: Configured from console by console
2001:0DB8:5000:)/16, interface Ethernet3/0, distance 1
```

関連情報

ルーティング プロトコルを実装する場合は、「*Implementing RIP for IPv6*」、「*Implementing IS-IS for IPv6*」、「*Implementing OSPF for IPv6*」、または「*Implementing Multiprotocol BGP for IPv6*」の章を参照してください。

その他の関連資料

関連資料

関連項目	参照先
IP スタティック ルートの設定	『*Cisco* IOS IP Routing Protocols Configuration Guide』の「*Protocol-Independent Routing*」
IP スタティック ルート コマンド：complete コマンドの構文、コマンド モード、デフォルト、使用上の注意事項、例	『*Cisco IOS IP Routing Protocols Command Reference*』
IPv6 のサポート機能リスト	『*Cisco IOS IPv6 Configuration Guide*』の「Start Here: Cisco IOS Software Release Specifics for IPv6 Features」
IPv6 コマンド：コマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS IPv6 Command Reference*』

規格

規格	タイトル
この機能によってサポートされる新しい規格または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
•	選択したプラットフォーム、Cisco ソフトウェア リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によってサポートされる新しい RFC または変更された RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

IPv6 向けスタティック ルートの実装の機能情報

表 1 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どのソフトウェア イメージが特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1　IPv6 向けスタティック ルートの実装の機能情報

機能名	リリース	機能情報
IPv6 ルーティング：スタティック ルーティング	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(17a)SX1 12.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	スタティック ルートは、手動で設定され、2 つのネットワーク デバイス間の明示パスを定義します。 このマニュアルでは、この機能について説明しています。

IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装

この章では、シスコのネットワーク デバイス用の Cisco IOS IPv6 トラフィック フィルタおよびファイアウォール機能を設定する方法について説明します。これらのセキュリティ機能を使用すると、パフォーマンス低下や障害、さらには悪意のある攻撃や通常のネットワーク ユーザによる悪意はないが破壊的なミスによって引き起こされるデータ損失やセキュリティ侵害からネットワークを守ることができます。

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装の機能情報」（P.36）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装の前提条件

IPv6 アドレッシングおよび基本設定を熟知している必要があります。詳細については、「*Implementing IPv6 Addressing and Basic Connectivity*」の章を参照してください。

IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装の制約事項

Cisco IOS Release 12.2(2)T から Cisco IOS Release 12.2(13)T、および Cisco IOS Release 12.0(22)S 以降のリリースでは、標準の IPv6 Access Control List（ACL; アクセス コントロール リスト）機能だけがサポートされています。Cisco IOS Release 12.0(23)S および 12.2(13)T 以降のリリースでは、標準の IPv6 ACL 機能が拡張されて、IPv6 オプション ヘッダー、および任意でより細かい制御を行うための上位層プロトコル タイプ情報に基づくトラフィック フィルタリングがサポートされています（IPv4 での拡張 ACL に似た機能）。

IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装に関する情報

IPv6 トラフィック フィルタリングのアクセス コントロール リスト

IPv6 での標準の ACL 機能は、IPv4 での標準の ACL に似ています。アクセス リストによって、ルータ インターフェイスでブロックされるトラフィックおよび転送されるトラフィックが決定され、送信元アドレスと宛先アドレスに基づいて、特定のインターフェイスへの着信と発信をフィルタリングできます。各アクセス リストの最後には、暗黙的な deny 文が指定されています。IPv6 ACL を定義し、拒否条件と許可条件を設定するには、グローバル コンフィギュレーション モードで **deny** キーワードと **permit** キーワードを指定して **ipv6 access-list** コマンドを使用します。

Cisco IOS Release 12.0(23)S および 12.2(13)T 以降では、標準 IPv6 ACL 機能が拡張されて、IPv6 オプション ヘッダー、および任意でより細かい制御を行うための上位層プロトコル タイプ情報に基づくトラフィック フィルタリングがサポートされています（IPv4 での拡張 ACL に似た機能）。

IPsec 認証ヘッダーの IPv6 ACL 拡張

この機能によって、Authentication Header（AH; 認証ヘッダー）の有無にかかわらず、TCP、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）、ICMP、SCTP などの Upper Layer Protocol（ULP; 上位層プロトコル）でマッチングを実行できます。

TCP または UDP トラフィックは、AH が存在する場合でも存在しない場合でも、TCP、UDP、ICMP、SCTP などの Upper Layer Protocol（ULP; 上位層プロトコル）に対してマッチングできます。この機能が導入されるまでは、このようなマッチングは AH が存在しない場合にだけ使用できました。

この機能によって、キーワード **auth** が **permit** コマンドと **deny** コマンドに導入されました。**auth** キーワードを指定すると、特定のプロトコル、つまり TCP や UDP とともに認証ヘッダーが存在するかどうかに照らしてトラフィックをマッチングできます。

AH ヘッダーが存在する場合は、IPv6 トラフィックを ULP に対してマッチングできます。このマッチングを実行するには、**permit** コマンドまたは **deny** コマンドを使用するときに、*protocol* 引数に **ahp** オプションを入力します。

IPv6 でのアクセス クラス フィルタリング

IPv6 ACL に基づく、ルータとの間の着信接続と発信接続のフィルタリングは、ライン コンフィギュレーション モードで **ipv6 access-class** コマンドを使用して実行します。**ipv6 access-class** コマンドは、IPv6 ACL が名前で定義される点を除き、**access-class** コマンドに似ています。IPv6 ACL が着信トラフィックに適用される場合、ACL 内の送信元アドレスは、着信接続の送信元アドレスに照らしてマッチングされ、ACL 内の宛先アドレスは、インターフェイス上のローカル ルータ アドレスと照合されます。IPv6 ACL が発信トラフィックに適用される場合、ACL 内の送信元アドレスは、インターフェイス上のローカル ルータ アドレスに照らしてマッチングされ、ACL 内の宛先アドレスは、発信接続の送信元アドレスと照合されます。ユーザが任意の接続を試行できるように、すべての仮想端末回線で同じ制限を設定することを推奨します。

Cisco IOS Firewall for IPv6

Cisco IOS Firewall 機能を使用すると、高度なトラフィック フィルタリング機能をネットワークのファイアウォールの不可欠な部分として組み込むことができます。Cisco IOS Firewall for IPv6 によって、Cisco IOS Firewall を IPv6 ネットワークに実装できます。Cisco IOS Firewall は、IPv4 ネットワーク用の Cisco IOS Firewall と共存し、すべてのデュアル スタック ルータでサポートされています。

Cisco IOS Firewall for IPv6 機能は、次のとおりです。

- フラグメント化されたパケット インスペクション：フラグメント ヘッダーを使用して、フラグメント処理をトリガーします。Cisco IOS Firewall Virtual Fragment Reassembly（VFR）は、シーケンスから外れたフラグメントを調べ、それらのパケットを正しい順序に切り替え、一意の識別子が設定された単一の IP からのフラグメント数を調べ（Denial-of-Service（DoS; サービス拒絶）攻撃）、仮想再アセンブリを実行して、パケットを上位層プロトコルに移動します。
- IPv6 DoS 攻撃の軽減：SYN 半開接続を含む、IPv4 実装と同じ方法で、軽減メカニズムが実装されています。
- トンネル化パケット インスペクション：Cisco IOS Firewall ルータで終端するトンネル化 IPv6 パケットは、Cisco IOS Firewall for IPv6 によって検査できます。
- ステートフル パケット インスペクション：この機能によって、TCP、UDP、Internet Control Message Protocol version 6（ICMPv6; インターネット制御メッセージ プロトコル バージョン 6）、および FTP の各セッションのステートフル パケット インスペクションを実行できます。
- IPv4 ネットワークから発信され、IPv6 環境で終端するパケットのステートフル インスペクション：この機能では、IPv4 から IPv6 への変換サービスを使用します。
- 大半の IPv6 拡張ヘッダー情報の解釈または認識：この機能によって、ルーティング ヘッダー、ホップバイホップ オプション ヘッダー、およびフラグメント ヘッダーを含む、IPv6 拡張ヘッダー情報が解釈または認識されます。
- Port-to-Application Mapping（PAM）：Cisco IOS Firewall for IPv6 には PAM が含まれています。

Cisco IOS Firewall for IPv6 での PAM

PAM を使用して、ネットワーク サービスとアプリケーション用の TCP または UDP ポート番号をカスタマイズできます。PAM ではこの情報を使用して、アプリケーションに関連する登録済み、つまり既知のポートと異なるポートを使用しているサービスを実行するネットワーク環境をサポートします。

PAM では、ポート情報を使用して、ポートからアプリケーションへのデフォルト マッピング情報のテーブルをファイアウォールで確立します。PAM テーブルの情報によって、Context-Based Access Control（CBAC; コンテキストベース アクセス コントロール）がサポートしているサービスを非標準ポートで実行できます。CBAC での調査は、アプリケーションに関連付けられている既知のポート、つまり登録済みのポートだけを使用するトラフィックに限定されますが、PAM を使用すると、ネットワーク管理者は、特定のアプリケーションおよびサービスのネットワーク アクセス コントロールをカスタマイズできます。

PAM では、ホストまたはサブネット固有のポート マッピングもサポートしています。これにより、標準 ACL を使用して単一のホストまたはサブネットに PAM を適用できます。ホストまたはサブネット固有のポート マッピングは、標準の ACL を使用して行われます。

Cisco IOS Firewall アラート、監査証跡、およびシステム ロギング

Cisco IOS Firewall によって、ファイアウォールで追跡されたイベントに基づくリアルタイム アラートおよび監査証跡が生成されます。拡張された監査証跡機能では、システム ロギングを使用して、すべてのネットワーク トランザクションを追跡したり、タイムスタンプ、送信元ホスト、宛先ホスト、および使用されたポートを記録したり、高度なセッションベースのレポート用に送信バイト総数を記録したりします。リアルタイム アラートは、システムで疑わしいアクティビティが検出されると、システム ロギング エラー メッセージを中央管理コンソールに送信します。Cisco IOS Firewall インスペクション ルールを使用して、アプリケーション プロトコル単位でアラートと監査証跡情報を設定できます。たとえば、TCP トラフィック用の監査証跡情報を生成する場合、TCP インスペクションを定義する Cisco IOS Firewall ルールで、この情報の生成を指定できます。

Cisco IOS Firewall によって、検査されたセッションの詳細を記録する監査証跡メッセージが提供されます。監査証跡情報は、CBAC インスペクション ルールを使用してアプリケーション単位で設定できます。検査されたプロトコルを識別するには、応答側に関連付けられているポート番号を使用します。ポート番号は、アドレスの直後に表示されます。

IPv6 パケット インスペクション

ヘッダー フィールド（トラフィック クラス、フロー ラベル、ペイロード長、次ヘッダー、ホップ リミット、および送信元アドレスや宛先アドレス）は、すべて IPv6 インスペクション用に使用されます。IPv6 ヘッダー フィールドの詳細および説明については、RFC 2474 を参照してください。

トンネリング サポート

IPv4 でトンネルされる IPv6 パケットは、検査されません。トンネルがルータで終端され、そのトンネルからの IPv6 出トラフィックが終端されない場合、そのトラフィックは検査されます。

仮想フラグメント再アセンブリ

VFR がイネーブルの場合、VFR 処理は、ACL 入力リストが着信パケットに照らしてチェックされたあとに開始されます。入力パケットには、適切な VFR 情報がタグ付けされます。

Cisco IOS Firewall の制約事項

IPv6 では、Cisco IOS Intrusion Detection System（IDS; 侵入検知システム）がサポートされていません。

Cisco IOS Zone-Based Firewall for IPv6

IPv6 トラフィックをサポートするために、Cisco IOS Zone-Based Firewall for IPv6 は Cisco IOS Zone-Based Firewall for IPv4 と共存します。この機能では、TCP、UDP、ICMPv6、および FTP の各セッションに対して MIB サポートが提供されます。

Zone-Based Firewall の詳細については、『*Cisco IOS Security Configuration Guide: Securing the Data Plane*』の「Zone-Based Policy Firewall」を参照してください。

IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装方法

次の各項の作業では、IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装方法を示します。

- 「IPv6 トラフィック フィルタリングの設定」（P.5）
- 「vty へのアクセスの制御」（P.8）
- 「TCP または UDP マッチングの設定」（P.11）
- 「Cisco IOS Release 12.2(11)T、12.0(22)S、または以前のリリースにおけるトラフィック フィルタリング用 IPv6 ACL の作成」（P.12）
- 「Cisco IOS Firewall for IPv6 の設定」（P.14）
- 「IPv6 でのゾーンベースのファイアウォールの設定」（P.19）
- 「IPv6 セキュリティの設定と動作の確認」（P.23）
- 「IPv6 セキュリティの設定と動作のトラブルシューティング」（P.25）

IPv6 トラフィック フィルタリングの設定

ここでは、IPv6 トラフィック フィルタリングをイネーブルにする方法について説明します。

- 「トラフィック フィルタリング用の IPv6 ACL の作成および設定」（P.6）
- 「インターフェイスへの IPv6 ACL の適用」（P.8）

制約事項

- Cisco IOS Release 12.2(13)T、12.0(23)S、または以降のリリースを実行している場合は、「トラフィック フィルタリング用の IPv6 ACL の作成および設定」の項に進みます。Cisco IOS Release 12.2(11)T、12.0(22)S、または以前のリリースを実行している場合は、「Cisco IOS Release 12.2(11)T、12.0(22)S、または以前のリリースにおけるトラフィック フィルタリング用 IPv6 ACL の作成」の項に進みます。
- IPv6 ACL は、一意な名前で定義されています（IPv6 では番号付き ACL はサポートしていません）。IPv4 ACL および IPv6 ACL は、同じ名前を共有できません。

トラフィック フィルタリング用の IPv6 ACL の作成および設定

ここでは、トラフィックをフィルタリングし、ファイアウォールとして機能し、または潜在的なウイルスを検出するようにネットワーキング デバイスを設定する方法について説明します。次の作業では、IPv6 ACL を作成し、Cisco IOS Release 12.2(13)T および 12.0(23)S または以降のリリースでトラフィックをフィルタリングするようにその IPv6 ACL を設定する方法について説明します。

前提条件

Cisco IOS Release 12.2(13)T および 12.0(23)S または以降のリリースでは、下位互換性のために、グローバル コンフィギュレーション モードでの **deny** キーワードと **permit** キーワードを指定した **ipv6 access-list** コマンドが引き続きサポートされています。ただし、グローバル コンフィギュレーション モードで拒否条件と許可条件を使用して定義された IPv6 ACL は、IPv6 アクセス リスト コンフィギュレーション モードに変換されます。変換された IPv6 ACL 設定の例については、「例：IPv6 ACL の作成および適用」の項を参照してください。

制約事項

- 各 IPv6 ACL には、IPv6 ネイバー探索をイネーブルにするための暗黙的な許可ルールが含まれています。ユーザは、ACL 内に deny ipv6 any any 文を配置することでこれらのルールを上書きできます。IPv6 ネイバー探索プロセスでは、IPv6 ネットワーク層サービスを利用するため、デフォルトで、インターフェイス上での IPv6 ネイバー探索パケットの送受信が IPv6 ACL によって暗黙的に許可されます。IPv4 の場合、IPv6 ネイバー探索プロセスに相当する Address Resolution Protocol（ARP; アドレス解決プロトコル）では、個別のデータ リンク レイヤ プロトコルを利用するため、デフォルトで、インターフェイス上での ARP パケットの送受信が IPv4 ACL によって暗黙的に許可されます。
- 時間ベースの ACL および再帰 ACL は、Cisco 12000 シリーズ プラットフォーム上の IPv4 または IPv6 ではサポートされていません。Cisco 12000 シリーズでは、IPv6 の **permit** コマンドの **reflect** キーワード、**timeout** キーワード、および **time-range** キーワードが除外されています。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *access-list-name*
4. **permit** *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
   または
   deny *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 access-list** *access-list-name* **例：** `Router(config)# ipv6 access-list outbound`	IPv6 ACL を定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。 • *access-list name* 引数には、IPv6 ACL の名前を指定します。IPv6 ACL の名前にスペースまたは引用符を含めることはできません。また、先頭を数字にすることはできません。

ステップ 4	**permit protocol** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
	
	または
	
	deny *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**]
	
	例：
	`Router(config-ipv6-acl)# permit tcp 2001:0DB8:0300:0201::/32 eq telnet any reflect reflectout`
	
	または
	
	例：
	`Router(config-ipv6-acl)# deny tcp host 2001:0db8:1::1 any log-input`
		IPv6 ACL の許可条件または拒否条件を指定します。

インターフェイスへの IPv6 ACL の適用

ここでは、Cisco IOS Release 12.2(13)T および 12.0(23)S または以降のリリースで IPv6 ACL をインターフェイスに適用する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 traffic-filter** *access-list-name* {**in** | **out**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface ethernet 0`	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 traffic-filter** *access-list-name* {**in** | **out**} **例：** `Router(config-if)# ipv6 traffic-filter outbound out`	指定した IPv6 アクセス リストを、前のステップで指定したインターフェイスに適用します。

vty へのアクセスの制御

ここでは、ルータ上の vty へのアクセスを制限する方法について説明します。

- 「IPv6 ACL の作成によるアクセス クラス フィルタリングの提供」（P.8）
- 「仮想端末回線への IPv6 ACL の適用」（P.10）

IPv6 ACL の作成によるアクセス クラス フィルタリングの提供

ここでは、IPv6 ACL を作成してアクセス クラス フィルタリングを提供することで、ルータ上の vty へのアクセスを制限する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *access-list-name*
4. **permit** *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
   または
   deny *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 access-list** *access-list-name* **例：** `Router(config)# ipv6 access-list cisco`	IPv6 ACL を定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。

ステップ 4	**permit protocol** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
	
	または
	
	deny *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**]
	
	例：
	`Router(config-ipv6-acl)# permit ipv6 host 2001:0DB8:0:4::32 any eq telnet`
	または
	
	例：
	`Router(config-ipv6-acl)# deny ipv6 host 2001:0DB8:0:6::6/32 any`
		IPv6 ACL の許可条件または拒否条件を指定します。

仮想端末回線への IPv6 ACL の適用

アクセス クラス フィルタリング用の IPv6 ACL を作成したあとに、指定した仮想端末回線にその ACL を適用する必要があります。次の作業では、仮想端末回線に ACL を適用する方法を示します。

手順の概要

1. **enable**
2. **configure terminal**
3. **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]

4. **ipv6 access-class** *ipv6-access-list-name* {**in** | **out**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*] **例：** `Router(config)# line vty 0 4`	設定する特定の回線を識別し、ライン コンフィギュレーション モードを開始します。 • この例では、**vty** キーワードを使用して、リモート コンソール アクセス用の仮想端末回線を指定します。
ステップ 4	**ipv6 access-class** *ipv6-access-list-name* {**in** | **out**} **例：** `Router(config-line)# ipv6 access-class cisco in`	IPv6 ACL に基づいて、ルータとの間の着信接続と発信接続をフィルタリングします。

TCP または UDP マッチングの設定

AH の有無に関係なく、TCP または UDP トラフィックを ULP（TCP、UDP、ICMP、SCTP など）に対してマッチングできます。この機能が導入されるまでは、このようなマッチングは AH が存在しない場合にだけ使用できました。

AH が存在する場合は、**permit icmp** コマンドおよび **deny icmp** コマンドで **auth** キーワードを使用すると、TCP または UDP トラフィックを ULP に対してマッチングできます。AH が存在しない TCP または UDP トラフィックでは、マッチングは実行されません。

AH ヘッダーが存在する場合は、IPv6 トラフィックを ULP に対してマッチングできます。このマッチングを実行するには、**permit** コマンドまたは **deny** コマンドを使用するときに、*protocol* 引数に **ahp** オプションを入力します。

この作業では、AH が存在する場合に、TCP または UDP トラフィックを ULP に対してマッチングできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *access-list-name*
4. **permit icmp auth**

   または
   deny icmp auth

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router# enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 access-list** *access-list-name* **例：** `Router(config)# ipv6 access-list list1`	IPv6 アクセス リストを定義し、ルータを IPv6 アクセス リスト コンフィギュレーション モードにします。
ステップ 4	**permit icmp auth** または **deny icmp auth** **例：** `Router(config-ipv6-acl)# permit icmp auth`	AH の存在に照らしたマッチングに使用される **auth** キーワードを使用して、IPv6 ACL の許可条件と拒否条件を指定します。

Cisco IOS Release 12.2(11)T、12.0(22)S、または以前のリリースにおけるトラフィック フィルタリング用 IPv6 ACL の作成

ここでは、Cisco IOS Release 12.2(11)T、12.0(22)S、または以前のリリースで ACL を作成および適用する方法について説明します。

- 「Cisco IOS Release 12.2(11)T、12.0(22)S、または以前のリリースにおける IPv6 ACL の作成」（P.12）
- 「Cisco IOS Release 12.2(11)T、12.0(22)S、または以前のリリースのインターフェイスへの IPv6 ACL の適用」（P.13）

Cisco IOS Release 12.2(11)T、12.0(22)S、または以前のリリースにおける IPv6 ACL の作成

ここでは、IPv6 ACL を作成し、Cisco IOS Release 12.2(11)T、12.0(22)S、または以前のリリースのトラフィックを通過またはブロックするようにこの IPv6 ACL を設定する方法について説明します。

制約事項

- *source-ipv6-prefix* 引数によって、トラフィックがパケット送信元アドレス別にフィルタリングされ、*destination-ipv6-prefix* 引数によって、トラフィックがパケット宛先アドレス別にフィルタリングされます。

- Cisco IOS ソフトウェアでは、アクセス リスト内の許可および拒否の条件文に照らして、IPv6 プレフィクスを比較します。すべての IPv6 アクセス リスト（許可および拒否の条件文が含まれていないアクセス リストを含む）には、最後の一致条件として暗黙的な deny any any 文が含まれています。各条件文に適用されるプライオリティ値またはシーケンス値は、文がアクセス リストで適用される順番を示しています。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *access-list-name* {**permit** | **deny**} {*source-ipv6-prefix*/*prefix-length* | **any**} {*destination-ipv6-prefix*/*prefix-length* | **any**} [**priority** *value*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 access-list** *access-list-name* {**permit** | **deny**} {*source-ipv6-prefix*/*prefix-length* | **any**} {*destination-ipv6-prefix*/*prefix-length* | **any**} [**priority** *value*] **例：** `Router(config)# ipv6 access-list list2 deny fec0:0:0:2::/64 any`	IPv6 ACL を作成し、ACL の拒否条件または許可条件を設定します。

Cisco IOS Release 12.2(11)T、12.0(22)S、または以前のリリースのインターフェイスへの IPv6 ACL の適用

ここでは、Cisco IOS Release 12.2(11)T、12.0(22)S、または以前のリリースのインターフェイスに IPv6 ACL を適用する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 traffic-filter** *access-list-name* {**in** | **out**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface ethernet 0`	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 traffic-filter** *access-list-name* {**in** | **out**} **例：** `Router(config-if)# ipv6 traffic-filter list2 out`	指定した IPv6 アクセス リストを、前のステップで指定したインターフェイスに適用します。

Cisco IOS Firewall for IPv6 の設定

ここでは、IPv6 環境用の Cisco IOS Firewall を設定する方法について説明します。この設定シナリオでは、パケット インスペクションと ACL の両方を使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **ipv6 inspect name** *inspection-name protocol* [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**timeout** *seconds*]
5. **interface** *type number*
6. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*}
7. **ipv6 enable**
8. **ipv6 traffic-filter** *access-list-name* {**in** | **out**}
9. **ipv6 inspect** *inspect-name*
10. **ipv6 access-list** *access-list-name*
11. **permit** *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

または
deny *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 unicast-routing** **例：** `Router(config)# ipv6 unicast-routing`	IPv6 ユニキャスト ルーティングをイネーブルにします。
ステップ 4	**ipv6 inspect name** *inspection-name protocol* [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**timeout** *seconds*] **例：** `Router(config)# ipv6 inspect name ipv6_test icmp timeout 60`	ファイアウォール用の一連の IPv6 インスペクション ルールを定義します。
ステップ 5	**interface** *type number* **例：** `Router(config)# interface FastEthernet0/0`	インスペクションが実行されるインターフェイスを指定します。
ステップ 6	**ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*} **例：** `Router(config-if)# ipv6 address 3FFE:C000:0:7::/64 eui-64`	インスペクション インターフェイスのアドレスを指定します。
ステップ 7	**ipv6 enable** **例：** `Router(config-if)# ipv6 enable`	IPv6 ルーティングをイネーブルにします。 **（注）** この手順は、IPv6 アドレスをステップ 6 で指定している場合は省略可能です。
ステップ 8	**ipv6 traffic-filter** *access-list-name* {**in** | **out**} **例：** `Router(config-if)# ipv6 traffic-filter outbound out`	指定した IPv6 アクセス リストを、前のステップで指定したインターフェイスに適用します。

	コマンドまたはアクション	目的
ステップ 9	**ipv6 inspect** *inspection-name* {**in** | **out**} **例：** `Router(config)# ipv6 inspect ipv6_test in`	一連のインスペクション ルールを適用します。
ステップ 10	**ipv6 access-list** *access-list-name* **例：** `Router(config)# ipv6 access-list outbound`	IPv6 ACL を定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。ルータにより、Router(config-ipv6-acl)# に対する変更が要求されます。

ステップ 11	**permit protocol** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
	
	または
	
	deny *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**]
	
	例：
	`Router(config-ipv6-acl)# permit tcp 2001:0DB8:0300:0201::/32 any reflect reflectout`
	または
	
	例：
	`Router(config-ipv6-acl)# deny tcp fec0:0:0:0201::/64 any`
		IPv6 ACL の許可条件または拒否条件を指定します。

PAM for IPv6 の設定

PAM 用の IPv6 アクセス クラス フィルタの作成

ここでは、PAM 環境で使用する IPv6 アクセス クラス フィルタを作成する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *access-list-name*
4. **permit** *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
   または
   deny *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 access-list** *access-list-name* **例：** `Router(config)# ipv6 access-list outbound`	IPv6 ACL を定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。ルータによって、Router(config-ipv6-acl)# への変更が要求されます。

ステップ 4	**permit protocol** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
	
	または
	
	deny *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**]
	
	例：
	`Router(config-ipv6-acl)# permit tcp 2001:0DB8:0300:0201::/32 any reflect reflectout`
	または
	
	例：
	`Router(config-ipv6-acl)# deny tcp fec0:0:0:0201::/64 any`
		IPv6 ACL の許可条件または拒否条件を指定します。

PAM への IPv6 アクセス クラス フィルタの適用

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 port-map** *application-name* **port** *port-num* [**list** *acl-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 port-map** *application-name* **port** *port-num* [**list** *acl-name*] **例：** `Router(config)# ipv6 port-map ftp port 8090 list PAMACL`	システムの PAM を確立します。

IPv6 でのゾーンベースのファイアウォールの設定

次の作業では、IPv6 環境に対して Cisco IOS のゾーンベースのファイアウォールを設定する方法を示します。

- 「検査タイプ パラメータ マップの設定」（P.19）
- 「検査タイプ クラス マップの作成と使用」（P.20）
- 「検査タイプ ポリシー マップの作成と使用」（P.21）
- 「セキュリティ ゾーンとゾーン ペアの作成」（P.22）

検査タイプ パラメータ マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect** {*parameter-map-name* | **global** | **default**}
4. **sessions maximum** *sessions*
5. **ipv6 routing-enforcement-header loose**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type inspect** {*parameter-map-name* | **global** | **default**} **例：** `Router(config)# parameter-map type inspect v6-param-map`	検査アクションに関連した接続しきい値、タイムアウトなどといったパラメータ用の検査タイプ パラメータ マップを設定し、ルータをパラメータ マップ コンフィギュレーション モードにします。
ステップ 4	**sessions maximum** *sessions* **例：** `Router(config-profile)# sessions maximum 10000`	ゾーン ペア上に存在可能な最大許容セッション数を設定します。
ステップ 5	**ipv6 routing-enforcement-header loose** **例：** `Router(config-profile)# ipv6 routing-enforcement-header loose`	レガシー IPv6 検査との下位互換性を提供します。

検査タイプ クラス マップの作成と使用

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect** {**match-any** | **match-all**} *class-map-name*
4. **match protocol tcp**
5. **match protocol udp**
6. **match protocol icmp**
7. **match protocol ftp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect** {**match-any** | **match-all**} *class-map-name* **例：** `Router(config-profile)# class-map type inspect match-any v6-class`	検査タイプ クラス マップを作成し、ルータをクラスマップ コンフィギュレーション モードにします。
ステップ 4	**match protocol tcp** **例：** `Router(config-cmap)# match protocol tcp`	TCP に基づいてクラス マップの一致基準を設定します。
ステップ 5	**match protocol udp** **例：** `Router(config-cmap)# match protocol udp`	UDP に基づいてクラス マップの一致基準を設定します。
ステップ 6	**match protocol icmp** **例：** `Router(config-cmap)# match protocol icmp`	ICMP に基づいてクラス マップの一致基準を設定します。
ステップ 7	**match protocol ftp** **例：** `Router(config-cmap)# match protocol ftp`	FTP に基づいてクラス マップの一致基準を設定します。

検査タイプ ポリシー マップの作成と使用

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type inspect** *policy-map-name*
4. **class type inspect** *class-map-name*
5. **inspect** [*parameter-map-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map type inspect** *policy-map-name* **例：** `Router(config)# policy-map type inspect v6-policy`	検査タイプ ポリシー マップを作成し、ルータをポリシー マップ コンフィギュレーション モードにします。
ステップ 4	**class type inspect** *class-map-name* **例：** `Router(config-pmap)# class type inspect v6-class`	アクションが実行されるトラフィック（クラス）を指定します。
ステップ 5	**inspect** [*parameter-map-name*] **例：** `Router(config-pmap)# inspect`	Cisco IOS ステートフル パケット インスペクションをイネーブルにします。

セキュリティ ゾーンとゾーン ペアの作成

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security 1**
4. **zone security 2**
5. **zone-pair security** *zone-pair-name* **source** {*source-zone-name* | **self** | **default**} **destination** {*destination-zone-name* | **self** | **default**}
6. **service-policy type inspect** *policy-map-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone security** {*zone-name* | **default**} **例：** `Router(global)# zone security 1`	セキュリティ ゾーンを作成します。 • ゾーン ペアを作成できるように、少なくとも 2 つのセキュリティ ゾーンを作成することを推奨します。
ステップ 4	**zone security** {*zone-name* | **default**} **例：** `Router(global)# zone security 2`	セキュリティ ゾーンを作成します。 • ゾーン ペアを作成できるように、少なくとも 2 つのセキュリティ ゾーンを作成することを推奨します。
ステップ 5	**zone-pair security** *zone-pair-name* **source** {*source-zone-name* | **self** | **default**} **destination** {*destination-zone-name* | **self** | **default**} **例：** `Router(global)# zone-pair security zp source z1 destination z2`	ゾーン ペアを作成し、ルータをゾーンペア コンフィギュレーション モードにします。
ステップ 6	**service-policy type inspect** *policy-map-name* **例：** `Router(config-sec-zone-pair)# service-policy type inspect v6-policy`	ファイアウォール ポリシー マップをゾーン ペアに付加します。

IPv6 セキュリティの設定と動作の確認

ここでは、IPv6 セキュリティ オプションの設定と動作を確認するための情報を表示する方法について説明します。必要に応じて次のコマンドを使用して、設定と動作を確認します。

手順の概要

1. **show crypto ipsec sa** [**map** *map-name* | **address** | **identity** | **interface** *interface-type interface-number* | **peer** [**vrf** *fvrf-name*] **address** | **vrf** *ivrf-name* | ipv6 [*interface-type interface-number*]] [**detail**]
2. **show crypto isakmp peer** [**config** | **detail**]
3. **show crypto isakmp profile**
4. **show crypto isakmp sa** [**active** | **standby** | **detail** | **nat**]
5. **show ipv6 access-list** [*access-list-name*]
6. **show ipv6 inspect** {**name** *inspection-name* | **config** | **interfaces** | **session** [**detail**] | **all**}

7. **show ipv6 port-map** [*application* | **port** *port-number*]
8. **show ipv6 prefix-list** [**detail** | **summary**] [*list-name*]
9. **show ipv6 virtual-reassembly interface** *interface-type*
10. **show logging** [**slot** *slot-number* | **summary**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show crypto ipsec sa** [**map** *map-name* | **address** | **identity** | **interface** *interface-type interface-number* | **peer** [**vrf** *fvrf-name*] **address** | **vrf** *ivrf-name* | **ipv6** [*interface-type interface-number*]] [**detail**] **例：** `Router# show crypto ipsec sa ipv6`	現在の SA によって使用されている設定を表示します。
ステップ 2	**show crypto isakmp peer** [**config** | **detail**] **例：** `Router# show crypto isakmp peer`	ピアの説明を表示します。
ステップ 3	**show crypto isakmp profile** **例：** `Router# show crypto isakmp profile`	ルータに定義されている ISAKMP プロファイルをすべてリストします。
ステップ 4	**show crypto isakmp sa** [**active** | **standby** | **detail** | **nat**] **例：** `Router# show crypto isakmp sa`	現在の IKE SA を表示します。
ステップ 5	**show ipv6 access-list** [*access-list-name*] **例：** `Router# show ipv6 access-list`	現在のすべての IPv6 アクセス リストの内容を表示します。
ステップ 6	**show ipv6 inspect** {**name** *inspection-name* | **config** | **interfaces** | **session** [**detail**] | **all**} **例：** `Router# show ipv6 inspect interfaces`	CBAC の設定およびセッション情報を表示します。
ステップ 7	**show ipv6 port-map** [*application* | **port** *port-number*] **例：** `Router# show ipv6 port-map ftp`	PAM の設定を表示します。
ステップ 8	**show ipv6 prefix-list** [**detail** | **summary**] [*list-name*] **例：** `Router# show ipv6 prefix-list`	IPv6 プレフィクス リストまたは IPv6 プレフィクス リストのエントリに関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 9	**show ipv6 virtual-reassembly interface** *interface-type* **例：** `Router# show ipv6 virtual-reassembly interface e1/1`	VFR の設定および統計情報を表示します。
ステップ 10	**show logging** [**slot** *slot-number* | **summary**] **例：** `Router# show logging`	システム ロギング（syslog）の状態および標準のシステム ロギング バッファの内容を表示します。 • **log** キーワードまたは **log-input** キーワードが指定されたアクセス リスト エントリは、パケットがそのアクセス リスト エントリに一致した場合に記録されます。

IPv6 セキュリティの設定と動作のトラブルシューティング

この任意の作業では、IPv6 セキュリティ オプションの設定と動作をトラブルシューティングするための情報を表示する方法について説明します。次のコマンドを必要なときにだけ使用して、設定と動作を確認します。

手順の概要

1. **enable**
2. **clear ipv6 access-list** [*access-list-name*]
3. **clear ipv6 inspect** {**session** *session-number* | **all**}
4. **clear ipv6 prefix-list** [*prefix-list-name*] [*ipv6-prefix*/*prefix-length*]
5. **debug crypto ipsec**
6. **debug crypto engine packet** [**detail**]
7. **debug ipv6 inspect** {**function-trace** | **object-creation** | **object-deletion** | **events** | **timers** | **protocol** | **detailed**}
8. **debug ipv6 packet** [**access-list** *access-list-name*] [**detail**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router# enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**clear ipv6 access-list** [*access-list-name*] **例：** `Router# clear ipv6 access-list tin`	IPv6 アクセス リストの一致カウンタをリセットします。

	コマンドまたはアクション	目的
ステップ 3	**clear ipv6 inspect** {**session** *session-number* | all} **例：** Router# clear ipv6 inspect all	特定の IPv6 セッションまたはすべての IPv6 インスペクション セッションを削除します。
ステップ 4	**clear ipv6 prefix-list** [*prefix-list-name*] [*ipv6-prefix*/*prefix-length*] **例：** Router# clear ipv6 prefix-list	IPv6 プレフィクス リスト エントリのヒット カウントをリセットします。
ステップ 5	**debug crypto ipsec** **例：** Router# debug crypto ipsec	IPsec ネットワーク イベントを表示します。
ステップ 6	**debug crypto engine packet** [**detail**] **例：** Router# debug crypto engine packet	IPv6 パケットの内容を表示します。 **注意** 複数のパケットが暗号化される場合、このコマンドを使用すると、システムのフラッディングが発生し、CPU 使用率が高くなる可能性があります。
ステップ 7	**debug ipv6 inspect** {**function-trace** | **object-creation** | **object-deletion** | **events** | **timers** | **protocol** | **detailed**} **例：** Router# debug ipv6 inspect timers	Cisco IOS Firewall イベントに関するメッセージを表示します。
ステップ 8	**debug ipv6 packet** [**access-list** *access-list-name*] [**detail**] **例：** Router# debug ipv6 packet access-list PAK-ACL	IPv6 パケットのデバッグ メッセージを表示します。

例

ここでは、次の出力例について説明します。

show crypto ipsec sa ipv6 コマンドの出力例

次に、**show crypto ipsec sa ipv6** コマンドの出力例を示します。

```
Router# show crypto ipsec sa ipv6

interface: Tunnel0
     Crypto map tag: Tunnel0-head-0, local addr 3FFE:2002::A8BB:CCFF:FE01:9002

    protected vrf: (none)
    local  ident (addr/mask/prot/port): (::/0/0/0)
    remote ident (addr/mask/prot/port): (::/0/0/0)
    current_peer 3FFE:2002::A8BB:CCFF:FE01:2C02 port 500
      PERMIT, flags={origin_is_acl,}
     #pkts encaps: 133, #pkts encrypt: 133, #pkts digest: 133
     #pkts decaps: 133, #pkts decrypt: 133, #pkts verify: 133
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 60, #recv errors 0

      local crypto endpt.: 3FFE:2002::A8BB:CCFF:FE01:9002,
      remote crypto endpt.: 3FFE:2002::A8BB:CCFF:FE01:2C02
      path mtu 1514, ip mtu 1514
      current outbound spi: 0x28551D9A(676666778)

      inbound esp sas:
       spi: 0x2104850C(553944332)
         transform: esp-des ,
         in use settings ={Tunnel, }
         conn id: 93, flow_id: SW:93, crypto map: Tunnel0-head-0
         sa timing: remaining key lifetime (k/sec): (4397507/148)
         IV size: 8 bytes
         replay detection support: Y
         Status: ACTIVE

      inbound ah sas:
       spi: 0x967698CB(2524354763)
         transform: ah-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 93, flow_id: SW:93, crypto map: Tunnel0-head-0
         sa timing: remaining key lifetime (k/sec): (4397507/147)
         replay detection support: Y
         Status: ACTIVE

      inbound pcp sas:

      outbound esp sas:
       spi: 0x28551D9A(676666778)
         transform: esp-des ,
         in use settings ={Tunnel, }
         conn id: 94, flow_id: SW:94, crypto map: Tunnel0-head-0
         sa timing: remaining key lifetime (k/sec): (4397508/147)
         IV size: 8 bytes
         replay detection support: Y
         Status: ACTIVE

      outbound ah sas:
       spi: 0xA83E05B5(2822636981)
         transform: ah-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 94, flow_id: SW:94, crypto map: Tunnel0-head-0
         sa timing: remaining key lifetime (k/sec): (4397508/147)
         replay detection support: Y
```

```
         Status: ACTIVE

      outbound pcp sas:
```

show crypto isakmp peer コマンドの出力例

次の出力例は、IPv6 ルータ上のピアの説明を示しています。

```
Router# show crypto isakmp peer detail

Peer: 2001:0DB8:0:1::1 Port: 500 Local: 2001:0DB8:0:2::1
Phase1 id: 2001:0DB8:0:1::1
flags:
NAS Port: 0 (Normal)
IKE SAs: 1 IPsec SA bundles: 1
last_locker: 0x141A188, last_last_locker: 0x0
last_unlocker: 0x0, last_last_unlocker: 0x0
```

show crypto isakmp profile コマンドの出力例

次の出力例は、IPv6 ルータで定義されている ISAKMP プロファイルを示しています。

```
Router# show crypto isakmp profile

ISAKMP PROFILE tom
Identities matched are:
ipv6-address 2001:0DB8:0:1::1/32
Certificate maps matched are:
Identity presented is: ipv6-address fqdn
keyring(s): <none>
trustpoint(s): <all>
```

show crypto isakmp sa コマンドの出力例

次の出力例は、アクティブな IPv6 デバイスの SA を示しています。IPv4 デバイスは非アクティブです。

```
Router# show crypto isakmp sa detail

Codes: C - IKE configuration mode, D - Dead Peer Detection
        K - Keepalives, N - NAT-traversal
        X - IKE Extended Authentication
        psk - Preshared key, rsig - RSA signature
        renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local           Remote          I-VRF    Status Encr Hash Auth DH
Lifetime Cap.

IPv6 Crypto ISAKMP SA

  dst: 3FFE:2002::A8BB:CCFF:FE01:2C02
  src: 3FFE:2002::A8BB:CCFF:FE01:9002
  conn-id: 1001  I-VRF:          Status: ACTIVE Encr: des  Hash: sha  Auth:
psk
  DH: 1  Lifetime: 23:45:00 Cap: D    Engine-id:Conn-id = SW:1

  dst: 3FFE:2002::A8BB:CCFF:FE01:2C02
  src: 3FFE:2002::A8BB:CCFF:FE01:9002
  conn-id: 1002  I-VRF:          Status: ACTIVE Encr: des  Hash: sha  Auth:
psk
  DH: 1  Lifetime: 23:45:01 Cap: D    Engine-id:Conn-id = SW:2
```

show ipv6 access-list コマンドの出力例

次の例では、**show ipv6 access-list** コマンドを使用して、IPv6 ACL が正しく設定されていることを確認しています。

```
Router> show ipv6 access-list

IPv6 access list inbound
    permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
    permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
    permit udp any any reflect udptraffic sequence 30

IPv6 access list tcptraffic (reflexive) (per-user)
    permit tcp host 2001:0DB8:1::32 eq bgp host 2001:0DB8:2::32 eq 11000 timeout 300 (time
        left 243) sequence 1
    permit tcp host 2001:0DB8:1::32 eq telnet host 2001:0DB8:2::32 eq 11001 timeout 300
        (time left 296) sequence 2

IPv6 access list outbound
    evaluate udptraffic
    evaluate tcptraffic
```

show ipv6 prefix-list コマンドの出力例

次に、**detail** キーワードを指定した **show ipv6 prefix-list** コマンドの出力例を示します。

```
Router# show ipv6 prefix-list detail

Prefix-list with the last deletion/insertion: bgp-in
ipv6 prefix-list 6to4:
   count: 1, range entries: 0, sequences: 5 - 5, refcount: 2
   seq 5 permit 2001:0db8::/32 (hit count: 313, refcount: 1)
ipv6 prefix-list aggregate:
   count: 2, range entries: 2, sequences: 5 - 10, refcount: 30
   seq 5 deny 3FFE:C00::/24 ge 25 (hit count: 568, refcount: 1)
   seq 10 permit ::/0 le 48 (hit count: 31310, refcount: 1)
ipv6 prefix-list bgp-in:
   count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
   seq 5 deny 5F00::/8 le 128 (hit count: 0, refcount: 1)
   seq 10 deny ::/0 (hit count: 0, refcount: 1)
   seq 15 deny ::/1 (hit count: 0, refcount: 1)
   seq 20 deny ::/2 (hit count: 0, refcount: 1)
   seq 25 deny ::/3 ge 4 (hit count: 0, refcount: 1)
   seq 30 permit ::/0 le 128 (hit count: 240664, refcount: 0)
```

show ipv6 virtual-reassembly コマンドの出力例

次に、**interface** キーワードを指定した **show ipv6 virtual-reassembly** コマンドの出力例を示します。

```
Router# show ipv6 virtual-reassembly interface e1/1

Configuration Information:
---------------------------------
Virtual Fragment Reassembly (VFR) is ENABLED...
Maximum number of datagram that can be reassembled at a time: 64
Maximum number of fragments per datagram: 8
Timeout value of a datagram: 3 seconds

Statistical Information:
---------------------------
Number of datagram being reassembled:12
Number of fragments being processed:48
Total number of datagram reassembled:6950
Total number of datagram failed: 9
```

show logging コマンドの出力例

次の例では、**show logging** コマンドを使用して、list1 という名前のアクセス リストの最初の行（シーケンス 10）に一致するロギング エントリを表示します。

```
Router> show logging

00:00:36: %IPV6-6-ACCESSLOGP: list list1/10 permitted tcp 2001:0db8:1::1(11001)
(Ethernet0/0) -> 2001:0db8:1::2(179), 1 packet
```

clear ipv6 access-list コマンドの出力例

次の例では、**show ipv6 access-list** コマンドを使用して、list1 という名前のアクセス リスト用の一部の一致カウンタを表示します。**clear ipv6 access-list** コマンドを発行して、list1 という名前のアクセス リスト用の一致カウンタをリセットします。**show ipv6 access-list** コマンドを再度使用して、一致カウンタがリセットされたことを示します。

```
Router> show ipv6 access-list list1

IPv6 access list list1
    permit tcp any any log-input (6 matches) sequence 10
    permit icmp any any echo-request log-input sequence 20
    permit icmp any any echo-reply log-input sequence 30

Router# clear ipv6 access-list list1

Router# show ipv6 access-list list1

IPv6 access list list1
    permit tcp any any log-input sequence 10
    permit icmp any any echo-request log-input sequence 20
    permit icmp any any echo-reply log-input sequence 30
```

IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装の設定例

例：IPv6 ACL の作成および適用

例：Release 12.2(13)T または 12.0(23)S 用の IPv6 ACL の作成および適用

次に、Cisco IOS Release 12.2(13)T を実行しているルータの例を示します。

この例では、OUTBOUND および INBOUND という名前の 2 つの IPv6 ACL を設定し、両方の ACL をイーサネット インターフェイス 0 上の発信トラフィックと着信トラフィックに適用します。OUTBOUND リスト内の最初と 2 番めの許可エントリは、ネットワーク 2001:0DB8:0300:0201::/32 から送信されたすべての TCP および User Datagram Protocol（UDP; ユーザ データグラム プロトコル）パケットがイーサネット インターフェイス 0 から出て行くことを許可します。また、エントリは REFLECTOUT という名前の一時的な IPv6 リフレクシブ ACL を設定して、イーサネット インターフェイス 0 上で回帰（着信）TCP および UDP パケットをフィルタリングします。OUTBOUND リストの最初の拒否エントリは、ネットワーク fec0:0:0:0201::/64 から送信されたすべてのパケット（送信元 IPv6 アドレスの最初の 64 ビットとしてサイトローカル プレフィクス fec0:0:0:0201 を持つパケット）がイーサネット インターフェイス 0 から出て行くことを拒否します。

INBOUND リストの **evaluate** コマンドは、REFLECTOUT という名前の一時的な IPv6 リフレクシブ ACL をイーサネット インターフェイス 0 上の着信 TCP および UDP パケットに適用します。OUTBOUND リストによって発信 TCP または UDP パケットがイーサネット インターフェイス 0 上で許可された場合、INBOUND リストは REFLECTOUT リストを使用して、回帰（着信）TCP および UDP パケットを照合（評価）します。

```
ipv6 access-list OUTBOUND
 permit tcp 2001:0DB8:0300:0201::/32 any reflect REFLECTOUT
 permit udp 2001:0DB8:0300:0201::/32 any reflect REFLECTOUT
 deny fec0:0:0:0201::/64 any

ipv6 access-list INBOUND
 evaluate REFLECTOUT

interface ethernet 0
 ipv6 traffic-filter OUTBOUND out
 ipv6 traffic-filter INBOUND in
```

（注） OUTBOUND または INBOUND ACL の最後のエントリとして **permit any any** 文が含まれていないので、イーサネット インターフェイス 0 への出入りが許可されるのは、ACL に設定された許可エントリに一致する TCP と UDP パケット、および ACL 内の暗黙的な許可条件に一致する ICMP パケットだけになります（ACL の末尾にある暗黙的な deny all 条件は、インターフェイス上の他のすべてのパケット タイプを拒否します）。

次の例は、Cisco IOS Release 12.2(13)T または 12.0(23)S を実行するルータ上で実行できます。

次の例は、HTTP アクセスを日中の特定の時間に制限し、許可時間外のアクティビティを記録するように設定します。

```
time-range lunchtime
 periodic weekdays 12:00 to 13:00

ipv6 access-list OUTBOUND
 permit tcp any any eq www time-range lunchtime
 deny tcp any any eq www log-input
 permit tcp 2001:0DB8::/32 any
 permit udp 2001:0DB8::/32 any
```

例：12.2(11)T、12.0(22)S、または以前のリリース用の IPv6 ACL の作成および適用

次に、Cisco IOS Release 12.2(11)T、12.0(22)S、または以前のリリースを実行するルータでの例を示します。

この例では、list2 という名前の IPv6 ACL を設定し、その ACL をイーサネット インターフェイス 0 上の発信トラフィックに適用します。特に、最初の ACL エントリは、ネットワーク fec0:0:0:2::/64（送信元 IPv6 アドレスの最初の 64 ビットとしてサイトローカル プレフィクス fec0:0:0:2 を持つパケット）

がイーサネット インターフェイス 0 から出て行くことを拒否します。2 番めの ACL エントリは、その他のすべてのトラフィックがイーサネット インターフェイス 0 から出て行くことを許可します。2 番めのエントリは、各 IPv6 ACL の末尾に暗黙的な deny all 条件があるため、必要となります。

```
ipv6 access-list list2 deny fec0:0:0:2::/64 any
ipv6 access-list list2 permit any any

interface ethernet 0
 ipv6 traffic-filter list2 out
```

同じ設定が、Cisco IOS Release 12.2(13)T、12.0(23)S、または以降のリリースを実行しているルータで使用されていた場合、その設定は次のように IPv6 アクセス リスト コンフィギュレーション モードに変換されます。

```
ipv6 access-list list2
 deny ipv6 fec0:0:0:2::/64 any
 permit ipv6 any any

interface ethernet 0
 ipv6 traffic-filter list2 out
```

（注） IPv6 は、グローバル コンフィギュレーション モードから IPv6 アクセス リスト コンフィギュレーション モードに変換される **permit any any** 文および **deny any any** 文でプロトコル タイプとして自動的に設定されます。

例：vty へのアクセスの制御

次の例では、仮想端末回線 0 ～ 4 に着信する接続は、acl1 という名前の IPv6 アクセス リストに基づいてフィルタリングされます。

```
ipv6 access-list acl1
 permit ipv6 host 2001:0DB8:0:4::2/32 any
!
line vty 0 4
 ipv6 access-class acl1 in
```

例：TCP または UDP マッチングの設定

次の例では、AH の有無にかかわらず、すべての TCP トラフィックを許可しています。

```
IPv6 access list example1
    permit tcp any any
```

次の例では、AH ヘッダーが存在する場合にだけ TCP または UDP 解析を許可しています。AH が存在しない TCP または UDP トラフィックでは、マッチングは実行されません。

```
IPv6 access list example2
    deny tcp host 2001::1 any log sequence 5
    permit tcp any any auth sequence 10
    permit udp any any auth sequence 20
```

次の例では、認証ヘッダーを持つすべての IPv6 トラフィックを許可しています。

```
IPv6 access list example3
    permit ahp any any
```

例：Cisco IOS Firewall for IPv6 の設定

この Cisco IOS Firewall 設定例では、インバウンド フィルタおよびアウトバウンド フィルタを検査に使用し、アクセス リストを利用してトラフィックを管理しています。この検査メカニズムは、状態が維持される、既存のセッションの間有効なパケットに基づいて、戻されてくるトラフィックを許可する方法です。

```
enable
configure terminal
 ipv6 unicast-routing
  ipv6 inspect name ipv6_test icmp timeout 60
  ipv6 inspect name ipv6_test tcp timeout 60
  ipv6 inspect name ipv6_test udp timeout 60

interface FastEthernet0/0
  ipv6 address 3FFE:C000:0:7::/64 eui-64
  ipv6 enable
  ipv6 traffic-filter INBOUND out
  ipv6 inspect ipv6_test in

interface FastEthernet0/1
  ipv6 address 3FFE:C000:1:7::/64 eui-64
  ipv6 enable
  ipv6 traffic-filter OUTBOUND in

! This is used for 3745b connection to tftpboot server
interface FastEthernet4/0
  ip address 192.168.17.33 255.255.255.0
  duplex auto
  speed 100

ip default-gateway 192.168.17.8
! end of tftpboot server config

! Access-lists to deny everything except for Neighbor Discovery ICMP messages
ipv6 access-list INBOUND
  permit icmp any any nd-na
  permit icmp any any nd-ns
  deny ipv6 any any log

ipv6 access-list OUTBOUND
  permit icmp any any nd-na
  permit icmp any any nd-ns
  deny ipv6 any any log
```

例：Cisco IOS Zone-Based Firewall for IPv6 の設定

次に、ゾーンベースのファイアウォールをイネーブルにし、ルータを通過する IPv6 トラフィックの検査を実現する例を示します。

```
parameter-map type inspect v6-param-map
 sessions maximum 10000
 ipv6 routing-header-enforcement loose
!
!
class-map type inspect match-any v6-class
 match protocol tcp
 match protocol udp
 match protocol icmp
 match protocol ftp
```

```
!
!
policy-map type inspect v6-policy
 class type inspect v6-class
  inspect
!
zone security z1
zone security z2
!
zone-pair security zp source z1 destination z2
 service-policy type inspect v6-policy
```

その他の関連資料

関連資料

関連項目	参照先
IPv6 IPsec	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing IPsec in IPv6 Security」
基本的な IPv6 設定	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing IPv6 Addressing and Basic Connectivity」
ゾーンベースのファイアウォール	『*Cisco IOS Security Configuration Guide: Securing the Data Plane*』の「Zone-Based Policy Firewall」
IPv6 のサポート機能リスト	『*Cisco IOS IPv6 Configuration Guide*』の「Start Here: Cisco IOS Software Release Specifics for IPv6 Features」
IPv6 コマンド：コマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS IPv6 Command Reference*』

規格

規格	タイトル
この機能によってサポートされる新しい規格または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
• CISCO-UNIFIED-FIREWALL-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2401	『*Security Architecture for the Internet Protocol*』
RFC 2402	『*IP Authentication Header*』
RFC 2428	『*FTP Extensions for IPv6 and NATs*』
RFC 2460	『*Internet Protocol, Version 6 (IPv6) Specification*』
RFC 2474	『*Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*』
RFC 3576	『*Change of Authorization*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装の機能情報

表 1 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どのソフトウェア イメージが特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1　IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装の機能情報

機能名	リリース	機能情報
IPv6 サービス：標準アクセス コントロール リスト	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(17a)SX1 12.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	アクセス リストによって、ルータ インターフェイスでブロックされるトラフィックおよび転送されるトラフィックが決定され、送信元アドレスと宛先アドレスに基づいて、特定のインターフェイスへの着信と発信をフィルタリングできます。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装の制約事項」（P.2） • 「IPv6 トラフィック フィルタリングのアクセス コントロール リスト」（P.2） • 「Cisco IOS Firewall for IPv6 での PAM」（P.4） • 「IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装方法」（P.5） • 「IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装の設定例」（P.30）
IPv6 サービス：拡張アクセス コントロール リスト[1]	12.0(23)S 12.2(14)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(17a)SX1 12.2(13)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	標準の IPv6 ACL 機能が拡張されて、IPv6 オプション ヘッダー、および任意でより細かい制御を行うための上位層プロトコル タイプ情報に基づくトラフィック フィルタリングがサポートされています。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装の制約事項」（P.2） • 「IPv6 トラフィック フィルタリングのアクセス コントロール リスト」（P.2） • 「IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装方法」（P.5） • 「IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装の設定例」（P.30）
IPv6 サービス：IPv6 IOS ファイアウォール	12.3(7)T 12.4 12.4(2)T	この機能を使用すると、高度なトラフィック フィルタリング機能をネットワークのファイアウォールの不可欠な部分として組み込むことができます。 この機能に関する詳細については、次の各項を参照してください。 • 「Cisco IOS Firewall for IPv6」（P.3） • 「Cisco IOS Firewall for IPv6 の設定」（P.14）
IPv6 サービス：IPv6 IOS ファイアウォール FTP アプリケーション サポート	12.3(11)T 12.4 12.4(2)T	IPv6 は、この機能をサポートします。 この機能に関する詳細については、次の項を参照してください。 • 「Cisco IOS Firewall for IPv6」（P.3）

表 1　IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装の機能情報 （続き）

機能名	リリース	機能情報
IPsec 認証ヘッダー用の IPv6 ACL 拡張	12.4(20)T	IPsec 認証ヘッダー用の IPv6 ACL 拡張機能を使用すると、IPv6 IPsec 認証ヘッダーが存在する場合には、TCP または UDP 解析を実行できます。 この機能に関する詳細については、次の項を参照してください。 • 「IPsec 認証ヘッダーの IPv6 ACL 拡張」（P.2）
IOS ゾーンベース ファイアウォール	15.1(2)T	IPv6 トラフィックをサポートするために、Cisco IOS Zone-Based Firewall for IPv6 は Cisco IOS Zone-Based Firewall for IPv4 と共存します。 この機能に関する詳細については、次の各項を参照してください。 • 「Cisco IOS Zone-Based Firewall for IPv6」（P.5） • 「IPv6 でのゾーンベースのファイアウォールの設定」（P.19） • 「例：Cisco IOS Zone-Based Firewall for IPv6 の設定」（P.33）

1. IPv6 拡張アクセス コントロール リストおよび Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）を介した IPv6 プロバイダー エッジ ルータは、Cisco IOS Release 12.0(25)S 以降のリリースの Cisco IOS ルータでの Cisco 12000 シリーズ インターネット ルータ IP Service Engineer（ISE）ラインカード上のハードウェア アクセラレータを使用して実装されています。

トンネリング for IPv6 の実装

この章では、IPv4 だけのネットワークから、IPv4 と IPv6 ベースの統合ネットワークへの移行をサポートするために、Cisco IOS ソフトウェアで使用されるオーバーレイ トンネリング技術を設定する方法について説明します。トンネリングでは、IPv4 パケットに IPv6 パケットをカプセル化し、その IPv4 ネットワークをリンク層メカニズムとして使用します。

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「トンネリング for IPv6 の実装の機能情報」（P.25）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

トンネリング for IPv6 の実装の制約事項

- Cisco IOS Release 12.0(21)ST と Cisco IOS Release 12.0(22)S および以前のリリースにおける Cisco 12000 シリーズ Gigabit Switch Router（GSR; ギガビット スイッチ ルータ）では、IPv6 トンネル化パケットの処理に非常に低いプライオリティが設定されています。このため、これらのリリースを使用する GSR では、IPv6 トンネルの使用は、ネットワーク トラフィックが低レベルに維持されており、プロセススイッチング リソースの必要性が最小限に抑えられているトポロジだけに制限することを強く推奨します。
- Cisco IOS Release 12.0(23)S における手動で設定された IPv6 トンネル トラフィックの処理は、GSR の Route Processor（RP; ルート プロセッサ）ではなく、ラインカードの CPU 上のソフトウェアで行われるため、パフォーマンスが向上します。

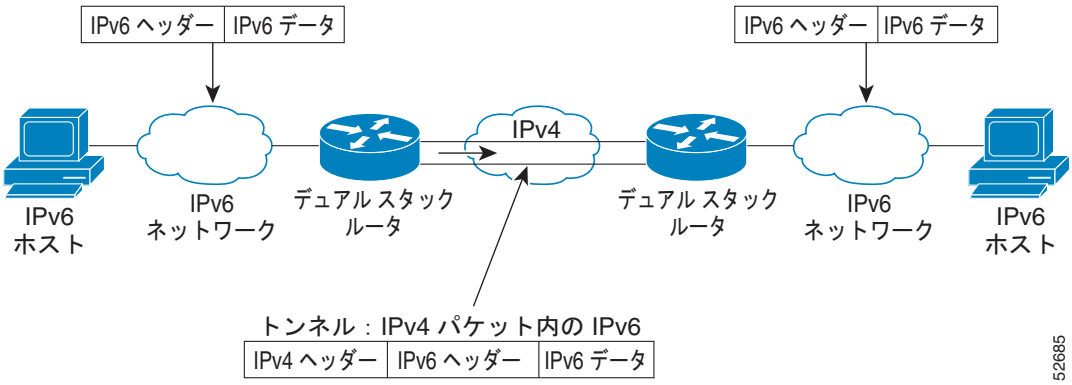
トンネリング for IPv6 の実装に関する情報

オーバーレイ トンネル for IPv6

オーバーレイ トンネリングでは、IPv6 パケットを IPv4 パケットにカプセル化して、IPv4 インフラストラクチャ全体（コア ネットワークまたはインターネット）に配信します（図 1 を参照）。オーバーレイ トンネルを使用することで、孤立した IPv6 ネットワークと通信できます。このとき、孤立した複数の IPv6 ネットワーク間にある IPv4 インフラストラクチャをアップグレードする必要はありません。オーバーレイ トンネルは、境界ルータ間、または境界ルータとホスト間に設定できますが、両方のエンドポイントが IPv4 プロトコル スタックと IPv6 プロトコル スタックの両方をサポートしている必要があります。Cisco IOS IPv6 では、次のタイプのオーバーレイ トンネリング メカニズムをサポートしています。

- 手動
- Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）
- IPv4 互換
- 6to4
- Intra-Site Automatic Tunnel Addressing Protocol（ISATAP）

図 1　オーバーレイ トンネル



（注）　オーバーレイ トンネルによって、インターフェイスの Maximum Transmission Unit（MTU; 最大伝送ユニット）が 20 オクテット少なくなります（IPv4 の基本パケット ヘッダーにオプション フィールドが含まれていないと仮定した場合）。オーバーレイ トンネルを使用するネットワークは、トラブルシューティングが難しくなります。そのため、孤立した IPv6 ネットワークを接続するオーバーレイ トンネルを IPv6 の最終的なネットワーク アーキテクチャとは考えないでください。オーバーレイ トンネルの使用は、IPv4 と IPv6 の両方のプロトコル スタック、または IPv6 プロトコル スタックだけをサポートするネットワークへの移行方法と見なす必要があります。

表 1 は、IPv4 ネットワーク上での IPv6 パケットの伝送にどのトンネル タイプを設定すればよいかを決定する場合に役立ちます。

表 1　IPv4 ネットワーク上で IPv6 パケットを伝送するトンネル タイプの推奨される使用方法

トンネリング タイプ	推奨される使用方法	使用上の注意事項
手動	サイト内、またはサイト間で使用できる単純なポイントツーポイント トンネル	IPv6 パケットだけを伝送できます。
GRE および IPv4 互換	サイト内、またはサイト間で使用できる単純なポイントツーポイント トンネル	IPv6、Connectionless Network Service（CLNS; コネクションレス型ネットワーク サービス）、およびその他の多数のタイプのパケットを伝送できます。
IPv4 互換	ポイントツーマルチポイント トンネル	::/96 プレフィクスを使用します。このトンネル タイプの使用は推奨しません。
6to4	孤立した IPv6 サイトの接続に使用できるポイントツーマルチポイント トンネル	サイトでは、2002::/16 プレフィクスからのアドレスを使用します。
ISATAP	サイト内のシステムの接続に使用できるポイントツーマルチポイント トンネル	サイトでは、任意の IPv6 ユニキャスト アドレスを使用できます。

個々のトンネル タイプについて、このマニュアルで詳しく説明しています。実装する特定のトンネル タイプに関する情報を確認および理解することを推奨します。必要なトンネル タイプに精通している場合は、表 2 で、有用と思われるトンネル設定パラメータの概要を参照してください。

表 2　トンネリング タイプ別のトンネル設定パラメータ

トンネリング タイプ	トンネル設定パラメータ			
	トンネル モード	トンネルの送信元	トンネルの宛先	インターフェイス プレフィクスまたはアドレス
手動	ipv6ip	IPv4 アドレス、または IPv4 が設定されたインターフェイスへの参照。	IPv4 アドレス。	IPv6 アドレス。
GRE/IPv4	gre ip		IPv4 アドレス。	IPv6 アドレス。
IPv4 互換	ipv6ip auto-tunnel		必須ではありません。これらはすべて、ポイントツーマルチポイントのトンネリング タイプです。IPv4 宛先アドレスは、パケット単位で、IPv6 宛先から計算されます。	必須ではありません。インターフェイス アドレスは、::*tunnel-source*/96 として生成されます。
6to4	ipv6ip 6to4			IPv6 アドレス。プレフィクスには、トンネル送信元 IPv4 アドレスが埋め込まれている必要があります。
ISATAP	ipv6ip isatap			変更された eui-64 形式での IPv6 プレフィクス。IPv6 アドレスは、プレフィクスおよびトンネル送信元 IPv4 アドレスから生成されます。

手動で設定された IPv6 トンネル

手動で設定されたトンネルは、IPv4 バックボーンを介した 2 つの IPv6 ドメイン間の固定リンクに相当します。主に、2 つのエッジ ルータ間またはエンド システムとエッジ ルータ間に定期的でセキュアな通信を必要とする安定した接続のために、またはリモート IPv6 ネットワークへの接続のために使用されます。

IPv6 アドレスは、トンネル インターフェイス上で手動で設定され、手動で設定された IPv4 アドレスは、トンネル送信元およびトンネル宛先に割り当てられます。設定されたトンネルの両端にあるホストまたはルータは、IPv4 プロトコル スタックと IPv6 プロトコル スタックの両方をサポートしている必要があります。手動で設定されたトンネルは、境界ルータ間または境界ルータとホスト間で設定できます。シスコ エクスプレス フォワーディング スイッチングは、手動で設定された IPv6 トンネルに使用できます。または、シスコ エクスプレス フォワーディング スイッチングは、プロセス スイッチングが必要な場合はディセーブルにできます。

IPv6 トラフィック用の GRE/IPv4 トンネル サポート

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

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

GRE には、パッセンジャ プロトコルを識別するプロトコル フィールドが含まれています。GRE トンネルを使用すると、Intermediate System-to-Intermediate System（IS-IS）または IPv6 をパッセンジャ プロトコルとして指定できます。これにより、IS-IS トラフィックと IPv6 トラフィックの両方が同じトンネルを通過できます。GRE にプロトコル フィールドが含まれていない場合は、トンネルが IS-IS パケットまたは IPv6 パケットを伝送していたかどうかは識別できません。GRE 内で IS-IS および IPv6 をトンネル化するには、GRE プロトコル フィールドが必要です。

IPv4 パケットと IPv6 パケットの GRE/CLNS トンネル サポート

CLNS ネットワークを介した IPv4 パケットと IPv6 パケットの GRE トンネリングを使用すると、Cisco CLNS Tunnel（CTunnel; CLNS トンネル）を他のベンダーのネットワーク機器と相互運用できます。この機能を使用すると、RFC 3147 に準拠できます。

ヘッダー フィールドで定義されている GRE のオプション サービス（チェックサム、キー、シーケンスなど）は、サポートされていません。これらのサービスの要求を受信したパケットはすべてドロップされます。

この機能に関する詳細については、『*Cisco IOS ISO CLNS Configuration Guide*』を参照してください。

自動 6to4 トンネル

自動 6to4 トンネルを使用すると、孤立した IPv6 ドメインを、IPv4 ネットワークを介してリモート IPv6 ネットワークに接続できます。自動 6to4 トンネルと、手動で設定されたトンネルとの主な違いは、トンネルがポイントツーポイントではなく、ポイントツーマルチポイントである点です。自動 6to4 トンネルでは、ルータは、IPv4 インフラストラクチャを仮想 NonBroadcast MultiAccess（NBMA; 非ブロードキャスト マルチアクセス）リンクとして処理するため、ペアでは設定されません。IPv6 アドレスに埋め込まれた IPv4 アドレスは、自動トンネルのもう一方のエンドを検出するために使用されます。

自動 6to4 トンネルは、孤立した IPv6 ネットワーク内の境界ルータに設定できます。これにより、IPv4 インフラストラクチャを介した別の IPv6 ネットワーク内の境界ルータへのパケット単位のトンネルが作成されます。トンネル宛先は、プレフィクス 2002::/16 で始まる IPv6 アドレス（形式は 2002:*border-router-IPv4-address*::/48）から抽出される、境界ルータの IPv4 アドレスによって決定されます。埋め込まれた IPv4 アドレスのあとには、サイト内のネットワークへの番号付けに使用できる 16 ビットが続きます。6to4 トンネルの両端の境界ルータは、IPv4 プロトコル スタックと IPv6 プロトコル スタックの両方をサポートしている必要があります。6to4 トンネルは、境界ルータ間または境界ルータとホスト間に設定されます。

6to4 トンネルの最も単純な展開シナリオは、複数の IPv6 サイトを相互接続することです。各 IPv6 サイトには、共有 IPv4 ネットワークへの 1 つ以上の接続があります。この IPv4 ネットワークは、グローバル インターネットまたは企業バックボーンである場合があります。主な要件は、各サイトがグローバルに一意な IPv4 アドレスを持っていることです。Cisco IOS ソフトウェアでは、このアドレスを使用して、グローバルに一意な 6to4/48 IPv6 プレフィクスを構成します。他のトンネリング メカニズムと同様に、ホスト名を IPv4 と IPv6 両方の IP アドレスにマッピングする Domain Name System（DNS; ドメイン ネーム システム）によって、アプリケーションは必要なアドレスを選択できます。

自動 IPv4 互換 IPv6 トンネル

自動 IPv4 互換トンネルでは、IPv4 互換 IPv6 アドレスを使用します。IPv4 互換 IPv6 アドレスは、アドレスの上位 96 ビットにゼロを持つ IPv6 ユニキャスト アドレス、および下位 32 ビット内の IPv4 アドレスです。これらのアドレスは 0:0:0:0:0:0:A.B.C.D または ::A.B.C.D として記述できます。ここで、「A.B.C.D」は、埋め込まれた IPv4 アドレスを表します。

トンネル宛先は、IPv4 互換 IPv6 アドレスの下位 32 ビット内の IPv4 アドレスによって自動的に決定されます。IPv4 互換トンネルの両端のホストまたはルータは、IPv4 プロトコル スタックと IPv6 プロトコル スタックの両方をサポートしている必要があります。IPv4 互換トンネルは、境界ルータ間または境界ルータとホスト間に設定できます。IPv4 互換トンネルを使用すると、IPv6 over IPv4 トンネルを簡単に作成できますが、この技術は、大規模ネットワーク用に拡張することはできません。

IPv6 Rapid Deployment トンネル

IPv6 Rapid Deployment（6RD）機能は、6to4 機能を拡張したものです。6RD 機能により、サービス プロバイダーは、IPv4 による IPv6 のカプセル化を使用して、自身の IPv4 ネットワーク上でユニキャスト IPv6 サービスをお客様に提供できます。

6RD と 6to4 トンネリングの主な違いは次のとおりです。

- 6RD では、アドレスのプレフィクスを 2002::/16 にする必要はありません。したがって、SP 自身のアドレス ブロックのプレフィクスを使用できます。この機能により、6RD の動作ドメインを SP ネットワーク内にすることができます。6RD 対応の SP ネットワークに接続されたカスタマー サイトおよび一般 IPv6 インターネットから見れば、提供される IPv6 サービスはネイティブ IPv6 と同等です。
- IPv4 宛先の 32 ビットすべてを IPv6 ペイロード ヘッダーで伝送する必要はありません。IPv4 宛先は、ペイロード ヘッダー内にあるビット データとルータ上の情報を組み合わせて求められます。さらに、IPv4 アドレスは、6to4 の場合とは異なり、IPv6 ヘッダー内での位置が固定ではありません。

ISATAP トンネル

ISATAP は、基礎となる IPv4 ネットワークを IPv6 の NBMA リンク レイヤとして使用する、自動オーバーレイ トンネリング メカニズムです。ISATAP は、ネイティブ IPv6 インフラストラクチャをまだ使用できない（希薄 IPv6 ホストがテスト用に展開されている場合など）サイト内で IPv6 パケットを転送するように設計されています。ISATAP トンネルを使用すると、サイト内の個々の IPv4 または IPv6 デュアル スタック ホストは、基本的には IPv4 インフラストラクチャを使用して IPv6 ネットワークを作成することで、同じ仮想リンク上のこうした他のホストと通信できます。

ISATAP ルータは、標準のルータ アドバタイズメント ネットワーク設定サポートを ISATAP サイトに提供します。この機能によって、クライアントは、イーサネットに接続されている場合と同様に、クライアント自身を自動的に設定できます。また、サイト外の接続を提供するように設定することもできます。ISATAP では、リンク ローカルまたはグローバル（6to4 プレフィクスを含む）な任意のユニキャスト IPv6 プレフィクス（/64）で構成される、適切に定義された IPv6 アドレス形式を使用します。これにより、IPv6 ルーティングをローカルに、またはインターネット上で実行できます。IPv4 アドレスは、IPv6 アドレスの最後の 32 ビットに符号化され、自動 IPv6-in-IPv4 トンネリングを可能にします。

ISATAP トンネリング メカニズムは、IPv6 6to4 トンネリングなどの他の自動トンネリング メカニズムと似ていますが、ISATAP は、サイト間ではなく、サイト内で IPv6 パケットを転送するように設計されています。

ISATAP では、64 ビットの IPv6 プレフィクスおよび 64 ビットのインターフェイス ID が含まれているユニキャスト アドレスを使用します。インターフェイス ID は、アドレスが IPv6 ISATAP アドレスであることを示すために最初の 32 ビットに値 000:5EFE が含まれる、変更された EUI-64 形式で作成されます。表 3 に、ISATAP アドレス形式を示します。

表 3　IPv6 ISATAP のアドレス形式

64 ビット	32 ビット	32 ビット
リンク ローカルまたはグローバル IPv6 ユニキャスト プレフィクス	0000:5EFE	ISATAP リンクの IPv4 アドレス

表 3 に示すように、ISATAP アドレスは、IPv6 プレフィクスと ISATAP インターフェイス ID で構成されています。インターフェイス ID には、基礎となる IPv4 リンクの IPv4 アドレスが含まれています。次の例では、プレフィクスが 2001:0DB8:1234:5678::/64 で、埋め込まれた IPv4 アドレスが 10.173.129.8 である場合、実際の ISATAP アドレスがどのようになるかを示します。ISATAP アドレスでは、この IPv4 アドレスは、16 進形式で 0AAD:8108 として表されます（たとえば、2001:0DB8:1234:5678:0000:5EFE:0AAD:8108）。

仮想トンネル インターフェイスを使用する IPv6 IPsec サイト間保護

IPv6 IPsec 機能では、ネイティブ IPsec IPv6 カプセル化を使用して、すべてのタイプの IPv6 ユニキャストおよびマルチキャスト トラフィックのサイト間 IPv6 暗号保護を提供します。IPsec Virtual Tunnel Interface（VTI; 仮想トンネル インターフェイス）機能では、IKE を管理プロトコルとして使用することでこれを実現します。

IPsec VTI では、ネイティブ IPsec トンネリングがサポートされ、物理インターフェイスの大半のプロパティが含まれています。IPsec VTI によって、複数のインターフェイスにクリプト マップを適用する必要性が軽減され、ルーティング可能なインターフェイスが提供されます。

IPsec VTI を使用すると、IPv6 ルータは、セキュリティ ゲートウェイとして機能し、他のセキュリティ ゲートウェイ ルータとの IPsec トンネルを確立し、パブリック IPv6 インターネット経由で送信される内部ネットワークのトラフィックに IPsec 暗号保護を提供できます。

VTI の詳細については、「*Implementing IPsec in IPv6 Security*」を参照してください。

トンネリング for IPv6 の実装方法

手動 IPv6 トンネルの設定

前提条件

手動で設定された IPv6 トンネルでは、IPv6 アドレスは、トンネル インターフェイス上で設定され、手動で設定された IPv4 アドレスは、トンネル送信元およびトンネル宛先に割り当てられます。設定されたトンネルの両端にあるホストまたはルータは、IPv4 プロトコル スタックと IPv6 プロトコル スタックの両方をサポートしている必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface tunnel** *tunnel-number*
4. **ipv6 address** *ipv6-prefix*/*prefix-length* [**eui-64**]
5. **tunnel source** {*ip-address* | *interface-type interface-number*}
6. **tunnel destination** *ip-address*
7. **tunnel mode ipv6ip**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface tunnel** *tunnel-number* **例：** `Router(config)# interface tunnel 0`	トンネル インターフェイスと番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 address** *ipv6-prefix*/*prefix-length* [**eui-64**] **例：** `Router(config-if)# ipv6 address 3ffe:b00:c18:1::3/127`	インターフェイスに割り当てられている IPv6 ネットワークを指定し、インターフェイスで IPv6 処理をイネーブルにします。
ステップ 5	**tunnel source** {*ip-address* | *interface-type interface-number*} **例：** `Router(config-if)# tunnel source ethernet 0`	トンネル インターフェイスの送信元 IPv4 アドレスまたは送信元インターフェイス タイプと番号を指定します。 • インターフェイスが指定されている場合、そのインターフェイスは IPv4 アドレスを使用して設定されている必要があります。

	コマンドまたはアクション	目的
ステップ 6	**tunnel destination** *ip-address* **例：** `Router(config-if)# tunnel destination 192.168.30.1`	トンネル インターフェイスの宛先 IPv4 アドレスまたはホスト名を指定します。
ステップ 7	**tunnel mode ipv6ip** **例：** `Router(config-if)# tunnel mode ipv6ip`	手動 IPv6 トンネルを指定します。 （注） **tunnel mode ipv6ip** コマンドでは、IPv6 をパッセンジャ プロトコルとして指定し、IPv4 を手動 IPv6 トンネル用のカプセル化プロトコルおよびトランスポート プロトコルの両方として指定します。

GRE IPv6 トンネルの設定

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

前提条件

GRE IPv6 トンネルが設定されている場合、IPv6 アドレスは、トンネル送信元およびトンネル宛先に割り当てられます。トンネル インターフェイスは、割り当て済みの IPv4 アドレスまたは IPv6 アドレスを持つことができます（ここでは説明していません）。設定されたトンネルの両端にあるホストまたはルータは、IPv4 プロトコル スタックと IPv6 プロトコル スタックの両方をサポートしている必要があります。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface tunnel** *tunnel-number* **例：** `Router(config)# interface tunnel 0`	トンネル インターフェイスおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 address** *ipv6-prefix*/*prefix-length* [**eui-64**] **例：** `Router(config-if)# ipv6 address 3ffe:b00:c18:1::3/127`	インターフェイスに割り当てられている IPv6 ネットワークを指定し、インターフェイスでの IPv6 処理をイネーブルにします。
ステップ 5	**tunnel source** {*ip-address* | *ipv6-address* | *interface-type interface-number*} **例：** `Router(config-if)# tunnel source ethernet 0`	トンネル インターフェイスの送信元 IPv4 アドレスまたは送信元インターフェイス タイプと番号を指定します。 • インターフェイスが指定されている場合、そのインターフェイスは IPv4 アドレスを使用して設定されている必要があります。
ステップ 6	**tunnel destination** {*host-name* | *ip-address* | *ipv6-address*} **例：** `Router(config-if)# tunnel destination 2001:0DB8:1111:2222::1/64`	宛先 IPv6 アドレスまたはトンネル インターフェイスのホスト名を指定します。
ステップ 7	**tunnel mode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre** | **gre multipoint** | **gre ipv6** | **ipip** [**decapsulate-any**] | **iptalk** | **ipv6** | **mpls** | **nos**} **例：** `Router(config-if)# tunnel mode gre ipv6`	GRE IPv6 トンネルを指定します。 **（注）** **tunnel mode gre ipv6** コマンドでは、GRE をトンネルのカプセル化プロトコルとして指定します。

自動 6to4 トンネルの設定

前提条件

6to4 トンネルでは、トンネル宛先は、2002: *border-router-IPv4-address*::/48 形式でプレフィクス 2002::/16 に連結される、境界ルータ IPv4 アドレスによって決まります。6to4 トンネルの両端の境界ルータは、IPv4 プロトコル スタックと IPv6 プロトコル スタックの両方をサポートしている必要があります。

制約事項

IPv4 互換トンネル 1 つだけの設定、および 6to4 IPv6 トンネル 1 つだけの設定が、1 台のルータ上でサポートされます。同じルータ上でこれら両方のトンネル タイプを設定する場合は、これらのタイプが同じトンネル送信元を共有しないようにすることを強く推奨します。

6to4 トンネルと IPv4 互換トンネルがインターフェイスを共有できない理由は、両方が NBMA「ポイントツーマルチポイント」アクセス リンクであり、多重化パケット ストリームからのパケットを着信インターフェイスの単一パケット ストリームに整理するにはトンネル送信元だけを使用できる点です。このため、IPv4 プロトコル タイプ 41 を含むパケットがインターフェイスに到着すると、そのパケットは、IPv4 アドレスに基づいて IPv6 トンネル インターフェイスにマッピングされます。ただし、6to4 トンネルと IPv4 互換トンネルの両方が同じ送信元インターフェイスを共有する場合、ルータは、着信パケットの割り当て先となる IPv6 トンネル インターフェイスを特定できません。

手動で設定された IPv6 トンネルの場合、手動トンネルは「ポイントツーポイント」リンクであり、トンネルの IPv4 送信元と IPv4 宛先が両方とも定義されているため、同じ送信元インターフェイスを共有できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface tunnel** *tunnel-number*
4. **ipv6 address** *ipv6-prefix*/*prefix-length* [**eui-64**]
5. **tunnel source** {*ip-address* | *interface-type interface-number*}
6. **tunnel mode ipv6ip 6to4**
7. **exit**
8. **ipv6 route** *ipv6-prefix*/*prefix-length* **tunnel** *tunnel-number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface tunnel** *tunnel-number* **例：** `Router(config)# interface tunnel 0`	トンネル インターフェイスおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**ipv6 address** *ipv6-prefix*/*prefix-length* [**eui-64**] **例：** `Router(config-if)# ipv6 address 2002:c0a8:6301:1::1/64`	インターフェイスに割り当てられた IPv6 アドレスを指定し、インターフェイスでの IPv6 処理をイネーブルにします。 • 最初の 2002::/16 プレフィクスに続く 32 ビットは、トンネル送信元に割り当てられた IPv4 アドレスに対応します。
ステップ 5	**tunnel source** {*ip-address* | *interface-type interface-number*} **例：** `Router(config-if)# tunnel source ethernet 0`	トンネル インターフェイスの送信元インターフェイスのタイプおよび番号を指定します。 （注） **tunnel source** コマンドで指定したインターフェイスのタイプおよび番号は、IPv4 アドレスを使用して設定する必要があります。
ステップ 6	**tunnel mode ipv6ip 6to4** **例：** `Router(config-if)# tunnel mode ipv6ip 6to4`	6to4 アドレスを使用する IPv6 オーバーレイ トンネルを指定します。
ステップ 7	**exit** **例：** `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 8	**ipv6 route** *ipv6-prefix*/*prefix-length* **tunnel** *tunnel-number* **例：** `Router(config)# ipv6 route 2002::/16 tunnel 0`	指定したトンネル インターフェイスに IPv6 6to4 プレフィクス 2002::/16 のスタティック ルートを設定します。 （注） 6to4 オーバーレイ トンネルを設定する場合は、6to4 トンネル インターフェイスに IPv6 6to4 プレフィクス 2002::/16 のスタティック ルートを設定する必要があります。 • **ipv6 route** コマンドで指定したトンネル番号は、**interface tunnel** コマンドで指定したトンネル番号と同じである必要があります。

IPv4 互換 IPv6 トンネルの設定

前提条件

IPv4 互換トンネルでは、トンネル宛先は、IPv4 互換 IPv6 アドレスの下位 32 ビット内の IPv4 アドレスによって自動的に決定されます。IPv4 互換トンネルの両端のホストまたはルータは、IPv4 プロトコル スタックと IPv6 プロトコル スタックの両方をサポートしている必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface tunnel** *tunnel-number*
4. **tunnel source** {*ip-address* | *interface-type interface-number*}
5. **tunnel mode ipv6ip auto-tunnel**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface tunnel** *tunnel-number* **例：** `Router(config)# interface tunnel 0`	トンネル インターフェイスおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**tunnel source** {*ip-address* | *interface-type interface-number*} **例：** `Router(config-if)# tunnel source ethernet 0`	トンネル インターフェイスの送信元インターフェイスのタイプおよび番号を指定します。 **（注）** **tunnel source** コマンドで指定されたインターフェイスのタイプおよび番号は、IPv4 アドレスだけを使用して設定されています。
ステップ 5	**tunnel mode ipv6ip auto-tunnel** **例：** `Router(config-if)# tunnel mode ipv6ip auto-tunnel`	IPv4 互換 IPv6 アドレスを使用して IPv4 互換トンネルを指定します。

6RD トンネルの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface tunnel** *tunnel-number*
4. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*}
5. **tunnel mode ipv6ip** [**6rd** | **6to4** | **auto-tunnel** | **isatap**]
6. **tunnel 6rd prefix** *ipv6-prefix*/*prefix-length*
7. **tunnel 6rd ipv4** {**prefix-length** *length* | **suffix-length** *length*}

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface tunnel** *tunnel-number* **例：** `Router(config)# interface tunnel 1`	トンネル インターフェイスおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**tunnel source** {*ip-address* | *interface-type interface-number*} **例：** `Router(config-if)# tunnel source Ethernet2/0`	トンネル インターフェイスの送信元インターフェイスのタイプおよび番号を指定します。
ステップ 5	**tunnel mode ipv6ip** [**6rd** | **6to4** | **auto-tunnel** | **isatap**] **例：** `Router(config-if)# tunnel mode ipv6ip 6rd`	スタティック IPv6 トンネル インターフェイスを設定します。
ステップ 6	**tunnel 6rd prefix** *ipv6-prefix*/*prefix-length* **例：** `Router(config-if)# tunnel 6rd prefix 2001:B000::/32`	IPv6 rapid 6RD トンネル上で共通の IPv6 プレフィクスを指定します。
ステップ 7	**tunnel 6rd ipv4** {**prefix-length** *length*} {**suffix-length** *length*} **例：** `Router(config-if)# tunnel 6rd ipv4 prefix-length 16 suffix 8`	ドメイン内のすべての 6RD ルータに共通の IPv4 トランスポート アドレスのプレフィクス長およびサフィクス長を指定します。

ISATAP トンネルの設定

前提条件

ISATAP トンネルの設定で使用される **tunnel source** コマンドは、設定済みの IPv4 アドレスを持つインターフェイスをポイントする必要があります。アドバタイズされた ISATAP IPv6 アドレスおよび（1 つまたは複数の）プレフィクスは、ネイティブ IPv6 インターフェイス用として設定されます。IPv6 トンネル インターフェイスは、インターフェイス ID 内の最後の 32 ビットが IPv4 トンネル送信元アドレスを使用して作成されているため、変更された EUI-64 アドレスを使用して設定されている必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface tunnel** *tunnel-number*
4. **ipv6 address** *ipv6-prefix*/*prefix-length* [**eui-64**]

5. **no ipv6 nd ra suppress**
6. **tunnel source** {*ip-address* | *interface-type interface-number*}
7. **tunnel mode ipv6ip isatap**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface tunnel** *tunnel-number* **例：** `Router(config)# interface tunnel 1`	トンネル インターフェイスおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 address** *ipv6-prefix*/*prefix-length* [**eui-64**] **例：** `Router(config-if)# ipv6 address 2001:0DB8:6301::/64 eui-64`	インターフェイスに割り当てられた IPv6 アドレスを指定し、インターフェイスでの IPv6 処理をイネーブルにします。 **（注）** IPv6 アドレスの設定の詳細については、「*Configuring Basic Connectivity for IPv6*」の章を参照してください。
ステップ 5	**no ipv6 nd ra suppress** **例：** `Router(config-if)# no ipv6 nd ra suppress`	IPv6 ルータ アドバタイズメントの送信は、トンネル インターフェイス上ではデフォルトでディセーブルになっています。このコマンドによって、IPv6 ルータ アドバタイズメントの送信が再度イネーブルになり、クライアントの自動設定が可能になります。
ステップ 6	**tunnel source** {*ip-address* | *interface-type interface-number*} **例：** `Router(config-if)# tunnel source ethernet 1/0/1`	トンネル インターフェイスの送信元インターフェイスのタイプおよび番号を指定します。 **（注）** **tunnel source** コマンドで指定したインターフェイスのタイプおよび番号は、IPv4 アドレスを使用して設定する必要があります。
ステップ 7	**tunnel mode ipv6ip isatap** **例：** `Router(config-if)# tunnel mode ipv6ip isatap`	ISATAP アドレスを使用する IPv6 オーバーレイ トンネルを指定します。

IPv6 トンネルの設定と動作の確認

手順の概要

1. **enable**
2. **show interfaces tunnel** *number* [**accounting**]
3. **ping** [*protocol*] *destination*

4. **show ip route** [*address* [*mask*]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**show interfaces tunnel** *number* [**accounting**] **例：** `Router# show interfaces tunnel 0`	（任意）トンネル インターフェイス情報を表示します。 • *number* 引数を使用して、指定したトンネルの情報を表示します。
ステップ 3	**ping** [*protocol*] *destination* **例：** `Router# ping 10.0.0.1`	（任意）基本的なネットワーク接続を診断します。
ステップ 4	**show ip route** [*address* [*mask*]] **例：** `Router# show ip route 10.0.0.2`	（任意）ルーティング テーブルの現在の状態を表示します。 **（注）** この作業に関係のある構文だけを示しています。

例

- 「show interfaces tunnel コマンドの出力例」
- 「ping コマンドの出力例」
- 「show ip route コマンドの出力例」
- 「ping コマンドの出力例」

show interfaces tunnel コマンドの出力例

この例では、手動で設定された IPv6 トンネルと、IPv6 over IPv4 GRE トンネルの両方に適している、汎用的な例を使用します。この例では、2 台のルータがトンネルのエンドポイントとして設定されています。ルータ A は、IPv4 アドレス 10.0.0.1 および IPv6 プレフィクス 2001:0DB8:1111:2222::1/64 を含むトンネル インターフェイス 0 として設定されたイーサネット インターフェイス 0/0 を持ちます。ルータ B は、IPv4 アドレス 10.0.0.2 および IPv6 プレフィクス 2001:0DB8:1111:2222::2/64 を含むトンネル インターフェイス 1 として設定されたイーサネット インターフェイス 0/0 を持ちます。トンネル送信元およびトンネル宛先のアドレスが設定されていることを確認するには、**show interfaces tunnel** コマンドをルータ A で使用します。

```
RouterA# show interfaces tunnel 0

Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.0.0.1 (Ethernet0/0), destination 10.0.0.2, fastswitch TTL 255
  Tunnel protocol/transport GRE/IP, key disabled, sequencing disabled
  Tunnel TTL 255
  Checksumming of packets disabled,  fast tunneling enabled
```

```
  Last input 00:00:14, output 00:00:04, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     4 packets input, 352 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     8 packets output, 704 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

ping コマンドの出力例

ローカル エンドポイントが設定され、機能していることを確認するには、**ping** コマンドをルータ A で使用します。

```
RouterA# ping 2001:0DB8:1111:2222::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:0DB8:1111:2222::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20 ms
```

show ip route コマンドの出力例

リモート エンドポイント アドレスへのルートが存在することを確認するには、**show ip route** コマンドを次のように使用します。

```
RouterA# show ip route 10.0.0.2

Routing entry for 10.0.0.0/24
  Known via "connected", distance 0, metric 0 (connected, via interface)
  Routing Descriptor Blocks:
  * directly connected, via Ethernet0/0
      Route metric is 0, traffic share count is 1
```

ping コマンドの出力例

リモート エンドポイント アドレスに到着できることを確認するには、**ping** コマンドをルータ A で使用します。

（注） フィルタリングが原因で、**ping** コマンドを使用してリモート エンドポイント アドレスに到着できない場合がありますが、トンネル トラフィックは依然としてその宛先に到着している場合があります。

```
RouterA# ping 10.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/21/28 ms
```

リモート IPv6 トンネル エンドポイントが到着可能であることを確認するには、ルータ A で **ping** コマンドを再び使用します。フィルタリングに関する同じ注意事項がこの例にも当てはまります。

```
RouterA# ping 1::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1::2, timeout is 2 seconds:
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20 ms
```

これらの手順は、トンネルのもう一方のエンドポイントで繰り返すことができます。

トンネリング for IPv6 の実装の設定例

例：手動 IPv6 トンネルの設定

次の例では、ルータ A とルータ B 間に手動 IPv6 トンネルを設定します。この例では、ルータ A とルータ B の両方のトンネル インターフェイス 0 が、グローバル IPv6 アドレスを使用して手動で設定されます。トンネル送信元およびトンネル宛先のアドレスについても、手動で設定されます。

ルータ A の設定

```
interface ethernet 0
 ip address 192.168.99.1 255.255.255.0

interface tunnel 0
 ipv6 address 3ffe:b00:c18:1::3/127
 tunnel source ethernet 0
 tunnel destination 192.168.30.1
 tunnel mode ipv6ip
```

ルータ B の設定

```
interface ethernet 0
 ip address 192.168.30.1 255.255.255.0

interface tunnel 0
 ipv6 address 3ffe:b00:c18:1::2/127
 tunnel source ethernet 0
 tunnel destination 192.168.99.1
 tunnel mode ipv6ip
```

例：GRE トンネルの設定

例：IS-IS および IPv6 トラフィックを実行する GRE トンネル

次の例では、ルータ A とルータ B 間で IS-IS と IPv6 の両方のトラフィックを実行する GRE トラフィックを設定します。

ルータ A の設定

```
ipv6 unicast-routing
clns routing
!
interface tunnel 0
 no ip address
 ipv6 address 3ffe:b00:c18:1::3/127
 ipv6 router isis
 tunnel source Ethernet 0/0
 tunnel destination 2001:0DB8:1111:2222::1/64
 tunnel mode gre ipv6
!
interface Ethernet0/0
 ip address 10.0.0.1 255.255.255.0
!
router isis
 net 49.0000.0000.000a.00
```

ルータ B の設定

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

例：IPv6 トンネルのトンネル宛先アドレス

次の例では、IPv6 パケットの GRE トンネリングのトンネル宛先アドレスを設定する方法について説明します。

```
Router(config)# interface Tunnel0
Router(config-if)# no ip address
Router(config-if)# ipv6 router isis
Router(config-if)# tunnel source Ethernet 0/0
Router(config-if)# tunnel destination 2001:0DB8:1111:2222::1/64
Router(config-if)# tunnel mode gre ipv6
Router(config-if)# exit
!
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# exit
```

```
!
Router(config)# ipv6 unicast-routing

Router(config)# router isis
Router(config)# net 49.0000.0000.000a.00
```

例：CLNS で IPv6 パケットを伝送するように GRE モードで CTunnel を設定

次の例では、CLNS ネットワーク内のルータ A とルータ B 間で IS-IS と IPv6 トラフィックの両方を実行する GRE CTunnel を設定します。**ctunnel mode gre** コマンドによって、シスコのネットワーキング デバイスとサードパーティのネットワーキング デバイス間のトンネリングが可能になり、IPv4 と IPv6 の両方のトラフィックを伝送できます。

ctunnel mode gre コマンドによって、RFC 3147 に準拠したトンネリング方法が提供され、シスコの装置とサードパーティのネットワーキング デバイス間のトンネリングが可能になります。

ルータ A

```
ipv6 unicast-routing

clns routing

interface ctunnel 102

 ipv6 address 2001:0DB8:1111:2222::1/64
 ctunnel destination 49.0001.2222.2222.2222.00
 ctunnel mode gre


interface Ethernet0/1
 clns router isis

router isis
 net 49.0001.1111.1111.1111.00
```

ルータ B

```
ipv6 unicast-routing

clns routing

interface ctunnel 201
 ipv6 address 2001:0DB8:1111:2222::2/64
 ctunnel destination 49.0001.1111.1111.1111.00
 ctunnel mode gre

interface Ethernet0/1
 clns router isis

router isis
 net 49.0001.2222.2222.2222.00
```

GRE モードをオフにし、シスコの装置上のエンドポイント間だけのデフォルト シスコ カプセル化ルーティングに CTunnel を戻すには、**no ctunnel mode** コマンドまたは **ctunnel mode cisco** コマンドを使用します。次の例では、IPv4 トラフィックだけを転送するように変更された同じ設定を示します。

例：6to4 トンネルの設定

次の例では、孤立した IPv6 ネットワーク内の境界ルータ上に 6to4 トンネルを設定します。IPv4 アドレスは 192.168.99.1 であり、IPv6 プレフィクス 2002:c0a8:6301::/48 に変換されます。IPv6 プレフィクスは、トンネル インターフェイス用として 2002:c0a8:6301::/64 にサブネット化されます。つまり、最初の IPv6 ネットワークは 2002:c0a8:6301:1::/64、2 番めの IPv6 ネットワークは 2002:c0a8:6301:2::/64 になります。スタティック ルートによって、IPv6 プレフィクス 2002::/16 のその他のすべてのトラフィックは、自動トンネリングのためにトンネル インターフェイス 0 に送信されます。

```
interface Ethernet0
 description IPv4 uplink
 ip address 192.168.99.1 255.255.255.0
!
interface Ethernet1
 description IPv6 local network 1
 ipv6 address 2002:c0a8:6301:1::1/64
!
interface Ethernet2
 description IPv6 local network 2
 ipv6 address 2002:c0a8:6301:2::1/64
!
interface Tunnel0
 description IPv6 uplink
 no ip address
 ipv6 address 2002:c0a8:6301::1/64
 tunnel source Ethernet 0
 tunnel mode ipv6ip 6to4
!
ipv6 route 2002::/16 tunnel 0
```

例：IPv4 互換 IPv6 トンネルの設定

次の例では、手動トンネルのメッシュを設定することなく、複数のルータ間で Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）を実行できるようにする IPv4 互換 IPv6 トンネルを設定します。各ルータには単一の IPv4 互換トンネルがあり、複数の BGP セッションを（各ネイバーへの）各トンネル上で実行できます。イーサネット インターフェイス 0 は、トンネル送信元として使用されます。トンネル宛先は、IPv4 互換 IPv6 アドレスの下位 32 ビット内の IPv4 アドレスによって自動的に決定されます。特に、IPv6 プレフィクス 0:0:0:0:0:0 は、IPv4 アドレス（0:0:0:0:0:0:A.B.C.D または ::A.B.C.D の形式）に連結されて、IPv4 互換 IPv6 アドレスが作成されます。イーサネット インターフェイス 0 は、グローバル IPv6 アドレスおよび IPv4 アドレスを使用して設定されています（このインターフェイスでは、IPv6 プロトコル スタックと IPv4 プロトコル スタックの両方がサポートされています）。

この例ではマルチプロトコル BGP を使用して、IPv6 到着可能情報をピア 10.67.0.2 と交換しています。イーサネット インターフェイス 0 の IPv4 アドレスは、IPv4 互換 IPv6 アドレスの下位 32 ビットで使用されており、ネクストホップ アトリビュートとしても使用されています。BGP ネイバーの IPv4 互換 IPv6 アドレスを使用すると、IPv4 互換トンネルを介して IPv6 BGP セッションを自動的に転送できます。

```
interface tunnel 0
 tunnel source Ethernet 0
 tunnel mode ipv6ip auto-tunnel

interface ethernet 0
 ip address 10.27.0.1 255.255.255.0
 ipv6 address 3000:2222::1/64
```

```
router bgp 65000
 no synchronization
 no bgp default ipv4-unicast
neighbor ::10.67.0.2 remote-as 65002

address-family ipv6
 neighbor ::10.67.0.2 activate
 neighbor ::10.67.0.2 next-hop-self
 network 2001:2222:d00d:b10b::/64
```

例：6RD トンネルの設定

次の例では、6RD トンネルの実行コンフィギュレーションとそれに対応する **show tunnel 6rd** コマンドの出力を示します。

```
interface Tunnel1
 ipv6 address 2001:B000:100::1/32
 tunnel source Ethernet2/1
 tunnel mode ipv6ip 6rd
 tunnel 6rd prefix 2001:B000::/32
 tunnel 6rd ipv4 prefix-len 16 suffix-len 8
end

Router# show tunnel 6rd tunnel 1

Interface Tunnel1:
  Tunnel Source: 10.1.1.1
  6RD: Operational, V6 Prefix: 2001:B000::/32
       V4 Common Prefix Length: 16, Value: 10.1.0.0
       V4 Common Suffix Length: 8, Value: 0.0.0.1
```

例：ISATAP トンネルの設定

次の例では、イーサネット 0 で定義されたトンネル送信元、および ISATAP トンネルの設定に使用する **tunnel mode** コマンドを示します。クライアントの自動設定を可能にするために、ルータ アドバタイズメントがイネーブルになっています。

```
ipv6 unicast-routing
interface tunnel 1
 tunnel source ethernet 0
 tunnel mode ipv6ip isatap
 ipv6 address 2001:0DB8::/64 eui-64
 no ipv6 nd ra suppress
 exit
```

その他の関連資料

関連資料

関連項目	参照先
IPsec VTI	「*Implementing IPsec in IPv6 Security*」
IPv6 のサポート機能リスト	「*Start Here: Cisco IOS Software Release Specifics for IPv6 Features*」

関連項目	参照先
CLNS トンネル	『*Cisco IOS ISO CLNS Configuration Guide*』
IPv6 コマンド：コマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS IPv6 Command Reference*』

規格

規格	タイトル
この機能によってサポートされる新しい規格または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2473	『*Generic Packet Tunneling in IPv6 Specification*』
RFC 2893	『*Transition Mechanisms for IPv6 Hosts and Routers*』
RFC 3056	『*Connection of IPv6 Domains via IPv4 Clouds*』
RFC 4214	『*Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

トンネリング for IPv6 の実装の機能情報

表 4 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どのソフトウェア イメージが特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 4 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 4　トンネリング for IPv6 の実装の機能情報

機能名	リリース	機能情報
IPv6 トンネリング：手動で設定された IPv6 over IPv4 トンネル	12.0(23)S[1] 12.2(14)S 12.2(28)SB 12.2(33)SRA 12.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	手動で設定されたトンネルは、IPv4 バックボーンを介した 2 つの IPv6 ドメイン間の固定リンクに相当します。 この機能に関する詳細については、次の各項を参照してください。 • 「オーバーレイ トンネル for IPv6」（P.2） • 「手動で設定された IPv6 トンネル」（P.4） • 「手動 IPv6 トンネルの設定」（P.8） • 「例：手動 IPv6 トンネルの設定」（P.18）
6to4 トンネルの CEFv6 スイッチング	12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(18)SXE 12.2(12)T 12.4 15.0(1)S	シスコ エクスプレス フォワーディング スイッチングは、手動で設定された IPv6 トンネルに使用できます。 この機能に関する詳細については、次の各項を参照してください。 • 「手動で設定された IPv6 トンネル」（P.4）
IPv6 トンネリング：自動 6to4 トンネル	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(33)SRA1 2.2(18)SXE 12.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	自動 6to4 トンネルを使用すると、孤立した IPv6 ドメインを、IPv4 ネットワークを介してリモート IPv6 ネットワークに接続できます。 この機能に関する詳細については、次の各項を参照してください。 • 「自動 6to4 トンネル」（P.5） • 「自動 6to4 トンネルの設定」（P.10）

表 4　トンネリング for IPv6 の実装の機能情報 （続き）

機能名	リリース	機能情報
IPv6 トンネリング：自動 IPv4 互換トンネル	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(33)SRA 12.2(18)SXE 12.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	自動 IPv4 互換トンネルでは、IPv4 互換 IPv6 アドレスを使用します。 この機能に関する詳細については、次の各項を参照してください。 • 「オーバーレイ トンネル for IPv6」（P.2） • 「自動 IPv4 互換 IPv6 トンネル」（P.5） • 「IPv4 互換 IPv6 トンネルの設定」（P.12） • 「例：IPv4 互換 IPv6 トンネルの設定」（P.21）
IPv6 トンネリング：IPv6 over IPv4 GRE トンネル	12.0(22)S[2] 12.2(14)S 12.2(28)SB 12.2(33)SRA 12.2(17a)SX1 12.2(4)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	GRE トンネルは、2 つのポイント間のリンクであり、リンクごとに個別のトンネルがあります。これらのトンネルは、特定のパッセンジャまたはトランスポート プロトコルに結合されていませんが、この場合、GRE を使用するパッセンジャ プロトコルとして IPv6 を伝送し、トランスポート プロトコルとして IPv4 または IPv6 を伝送します。 この機能に関する詳細については、次の各項を参照してください。 • 「オーバーレイ トンネル for IPv6」（P.2） • 「IPv6 トラフィック用の GRE/IPv4 トンネル サポート」（P.4） • 「GRE IPv6 トンネルの設定」（P.9） • 「例：GRE トンネルの設定」（P.18）
IPv6 トンネリング：トンネル ラインカードを使用する IPv6 over UTI[3]	12.0(23)S[1]	IPv6 は、この機能をサポートします。
IPv6 トンネリング：ISATAP トンネル サポート	12.2(14)S 12.2(28)SB 12.2(33)SRA1 2.2(17a)SX11 2.2(15)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	ISATAP は、基礎となる IPv4 ネットワークを IPv6 の NBMA リンク レイヤとして使用する、自動オーバーレイ トンネリング メカニズムです。 この機能に関する詳細については、次の各項を参照してください。 • 「オーバーレイ トンネル for IPv6」（P.2） • 「ISATAP トンネル」（P.6） • 「ISATAP トンネルの設定」（P.14） • 「例：ISATAP トンネルの設定」（P.22）
IPv6 トンネリング：IPv4 over IPv6 トンネル	12.2(30)S 12.2(33)SRA 12.3(7)T 12.4 12.4(2)T 15.0(1)S	IPv6 では、この機能をサポートします。 この機能に関する詳細については、次の各項を参照してください。 • 「手動で設定された IPv6 トンネル」（P.4） • 「手動 IPv6 トンネルの設定」（P.8）

表 4　トンネリング for IPv6 の実装の機能情報 （続き）

機能名	リリース	機能情報
IPv6 トンネリング：IPv6 over IPv6 トンネル	12.2(30)S 12.3(7)T 12.4 12.4(2)T	IPv6 では、この機能をサポートします。 この機能に関する詳細については、次の各項を参照してください。 • 「手動で設定された IPv6 トンネル」（P.4） • 「手動 IPv6 トンネルの設定」（P.8）
IPv6 トンネリング：IP over IPv6 GRE トンネル	12.2(30)S 12.3(7)T 12.4 12.4(2)T	GRE トンネルは、2 つのポイント間のリンクであり、リンクごとに個別のトンネルがあります。 この機能に関する詳細については、次の各項を参照してください。 • 「オーバーレイ トンネル for IPv6」（P.2） • 「IPv6 トラフィック用の GRE/IPv4 トンネル サポート」（P.4） • 「GRE IPv6 トンネルの設定」（P.9）
IPv6 トンネリング：CLNS ネットワークでの IPv6 GRE トンネル	12.2(25)S 12.2(28)SB 12.2(33)SRA 12.3(7)T 12.4 12.4(2)T	CLNS ネットワークを介した IPv4 パケットと IPv6 パケットの GRE トンネリングを使用すると、Cisco CTunnel を他のベンダーのネットワーク機器と相互運用できます。 この機能に関する詳細については、次の各項を参照してください。 • 「オーバーレイ トンネル for IPv6」（P.2） • 「IPv4 パケットと IPv6 パケットの GRE/CLNS トンネル サポート」（P.5） • 「例：CLNS で IPv6 パケットを伝送するように GRE モードで CTunnel を設定」（P.20）
IPv6 トンネリング：6RD IPv6 Rapid Deployment	15.1(3)T	6RD 機能により、サービス プロバイダーは、IPv4 による IPv6 のカプセル化を使用して、自身の IPv4 ネットワーク上でユニキャスト IPv6 サービスをお客様に提供できます。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 Rapid Deployment トンネル」（P.6） • 「6RD トンネルの設定」（P.13） • 「例：6RD トンネルの設定」（P.22）

1. Cisco IOS Release 12.0(23)S の場合、GSR では、トラフィックをラインカード上で処理することで、手動で設定された IPv6 トンネルのパフォーマンスを強化しています。
2. IPv6 over IPv4 GRE トンネルは、GSR ではサポートされていません。
3. 機能は、GSR だけでサポートされています。