OSPFv3

この章では、Cisco NX-OS デバイスで IPv6 ネットワーク用の Open Shortest Path First version 3（OSPFv3）を設定する方法について説明します。

この章は、次の項で構成されています。

OSPFv3

OSPFv3 は、IETF リンクステート プロトコル（概要の項を参照）です。OSPFv3 ルータは、hello パケットと呼ばれる特別なメッセージを各 OSPF 対応インターフェイスに送信し、他の OSPFv3 隣接ルータを探索します。ネイバー ルータが発見されると、この 2 台のルータは hello パケットの情報を比較して、両者の設定に互換性のあるかどうかを判定します。これらのネイバー ルータは隣接を確立しようとします。つまり、両者のリンクステート データベースを同期させて、確実に同じ OSPFv3 ルーティング情報を持つようにします。隣接ルータは、各リンクの稼働状態に関する情報、リンクのコスト、およびその他のあらゆるネイバー情報を含むリ

ンクステートアドバタイズメント（LSA）を共有します。これらのルータはその後、受信したLSA をすべての OSPF イネーブル インターフェイスにフラッディングします。これにより、すべてのOSPFv3ルータのリンクステートデータベースが最終的に同じになります。すべてのOSPFv3 ルータのリンクステート データベースが同じになると、ネットワークは収束します（「コンバージェンス」を参照）。その後、各ルータは、ダイクストラの最短パス優先（SPF）アルゴリズムを使用して、自身のルート テーブルを構築します。

OSPFv3 ネットワークは、複数のエリアに分割できます。ルータは、ほとんどの LSA を 1 つのエリア内だけに送信するため、OSPF 対応ルータの CPU とメモリの要件が緩やかになります。

OSPFv3 は IPv6 をサポートしています。IPv4 向けの OSPF の詳細については、OSPFv2を参照してください。

OSPFv3 と OSPFv2 の比較

OSPFv3 プロトコルの大半は OSPFv2 と同じです。OSPFv3 は RFC 2740 に記載されています。

OSPFv3 プロトコルと OSPFv2 プロトコルの重要な相違点は、次のとおりです。

- OSPFv2 を拡張した OSPFv3 では、IPv6 ルーティング プレフィックスとサイズの大きい IPv6 アドレスのサポートを提供しています。
- OSPFv3 の LSA は、アドレスとマスクではなく、プレフィックスとプレフィックス長として表現されます。
- ルータ ID とエリア ID は 32 ビット数で、IPv6 アドレスとは無関係です。
- OSPFv3 では、ネイバー探索およびその他の機能にリンクローカル IPv6 アドレスを使用します。
- OSPFv3 は、IPv6 認証トレーラ（RFC 6506）または IPSec（RFC 4552）を使用できます。ただし、Cisco NX-OS は RFC 6506 をサポートしていません。
- OSPFv3 では、LSA タイプが再定義されています。

Hello パケット

OSPFv3 ルータは、すべての OSPF イネーブル インターフェイスに hello パケットを定期的に送信します。ルータがこの hello パケットを送信する頻度は、インターフェイスごとに設定された hello 間隔により決定されます。OSPFv3 は、hello パケットを使用して、次のタスクを実行します。

- ネイバー探索
- キープアライブ
- 双方向通信
- 指定ルータの選定（「指定ルータ」セクションを参照してください）

helloパケットには、リンクのOSPFv3コスト割り当て、hello間隔、送信元ルータのオプション機能など、送信元のOSPFv3インターフェイスとルータに関する情報が含まれます。これらのhelloパケットを受信するOSPFv3インターフェイスは、設定に受信インターフェイスの設定との互換性があるかどうかを判定します。互換性のあるインターフェイスはネイバーと見なされ、ネイバー テーブルに追加されます（「ネイバー」の項を参照してください）。

helloパケットには、送信元インターフェイスが通信したルータのルータIDのリストも含まれます。受信インターフェイスが、このリストで自身のIDを見つけた場合は、2つのインターフェイス間で双方向通信が確立されます。

OSPFv3は、helloパケットをキープアライブ メッセージとして使用して、ネイバーが通信を継続中であるかどうかを判定します。ルータが設定されたデッド間隔（通常はhello間隔の倍数）でhelloパケットを受信しない場合、そのネイバーはローカル ネイバー テーブルから削除されます。

ネイバー情報

ネイバーであると見なされるようにするには、リモートインターフェイスと互換性があるようにOSPFv3インターフェイスを設定しておく必要があります。この2つのOSPFv3インターフェイスで、次の基準が一致している必要があります。

- hello間隔
- デッド間隔
- エリアID（「エリア」の項を参照）
- オプション機能

一致する場合は、次の情報がネイバー テーブルに入力されます。

- ネイバーID：ネイバー ルータのルータID
- 優先度：ネイバー ルータの優先度。プライオリティは、指定ルータの選定（「指定ルータ」を参照）に使用されます。
- 状態：ネイバーから通信があったか、双方向通信の確立処理中であるか、リンクステート情報を共有しているか、または完全な隣接関係が確立されたかを示します。
- デッド タイム：このネイバーから最後のhelloパケットを受信したあとに経過した時間を示します。
- リンクローカルIPv6アドレス：ネイバーのリンクローカルIPv6アドレス
- 指定ルータ：ネイバーが指定ルータ、またはバックアップ指定ルータとして宣言されたかどうかを示します（「指定ルータ」の項を参照）。
- ローカル インターフェイス：このネイバーのhelloパケットを受信したローカル インターフェイス。

最初の hello パケットが新規ネイバーから受信されると、そのネイバーは、初期化状態のネイバーテーブルに入力されます。いったん双方向通信が確立されると、ネイバー状態は双方向となります。2つのインターフェイスが互いのリンクステートデータベースを交換するため、次に ExStart および交換状態となります。これらがすべて完了すると、ネイバーは完全な状態へと移行し、これが完全な隣接関係となります。ネイバーは、デッド間隔でhelloパケットをまったく送信しない場合は、ダウン状態に移行し、隣接とは見なされなくなります。

隣接関係

すべてのネイバーが隣接関係を確立するわけではありません。ネットワーク タイプと確立された指定ルータに応じて、完全な隣接関係を確立して、すべてのネイバーと LSA を共有するものと、そうでないものがあります。詳細については、「指定されたルータ」の項を参照してください。

隣接関係は、OSPFv3 のデータベース説明（DD）パケット、リンク状態要求（LSR）パケット、およびリンク状態更新（LSU）パケットを使用して確立されます。データベース説明パケットには、ネイバーのリンクステートデータベースからのLSAヘッダーが含まれます（「リンク状態データベース」の項を参照）。ローカル ルータは、これらのヘッダーを自身のリンクステート データベースと比較して、新規の LSA か、更新された LSA かを判定します。ローカル ルータは、新規または更新の情報を必要とする各LSAについて、リンク状態要求（LSR）パケットを送信します。ネイバーは LSU パケットで応答します。このパケット交換は、両方のルータのリンクステート情報が同じになるまで継続します。

指定ルータ

複数のルータを含むネットワークは、OSPFv3 特有の状況です。すべてのルータがネットワークで LSA をフラッディングした場合は、同じリンクステート情報が複数の送信元から送信されます。ネットワークのタイプによっては、OSPFv3 は指定ルータ（DR）という 1 台のルータを使用してLSAのフラッディングを制御し、OSPFv3 の残りの部分に対してネットワークを代表する役割をさせる場合があります（「エリア」の項を参照）。DRがダウンした場合、OSPFv3 はバックアップ指定ルータ（BDR）を選択します。DR がダウンすると、OSPFv3 はこの BDR を使用します。

ネットワーク タイプは次のとおりです。

- ポイントツーポイント：2台のルータ間にのみ存在するネットワーク。ポイントツーポイント ネットワーク上の全ネイバーは隣接関係を確立し、DR は存在しません。
- ブロードキャスト： ブロードキャスト トラフィックが可能なイーサネットなどの共有メディア上で通信できる複数のルータを持つネットワーク。OSPFv3 ルータは DR および BDR を確立し、これらにより、ネットワーク上の LSA フラッディングを制御します。OSPFv3 は、よく知られている IPv6 マルチキャスト アドレス FF02::5 および MAC アドレス 0100.5300.0005 を使用して、ネイバーと通信します。

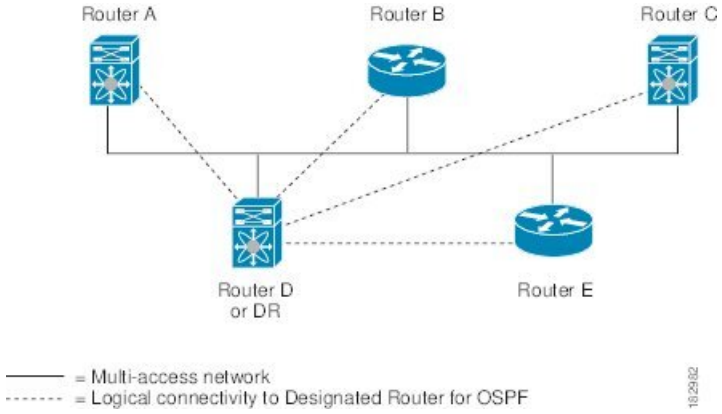
DR と BDR は、hello パケット内の情報に基づいて選択されます。インターフェイスは hello パケットの送信時に、どれが DR および BDR かわかっている場合は、優先フィールドと、DR および BDR フィールドを設定します。ルータは、helloパケットの DR および BDR フィールドで

宣言されたルータと優先フィールドに基づいて、選定手順を実行します。最終的に OSPFv3 は、最も大きいルータ ID を DR および BDR として選択します。

他のルータはすべて DR および BDR と隣接関係を確立し、IPv6 マルチキャスト アドレス FF02::6 を使用して、LSA 更新情報を DR と BDR に送信します。次の図は、すべてのルータと DR との隣接関係を示しています。

DR は、ルータ インターフェイスに基づいています。1 つのネットワークの DR であるルータは、別のインターフェイス上の他のネットワークの DR となることはできません。

図 *1*: マルチアクセス ネットワークの *DR*



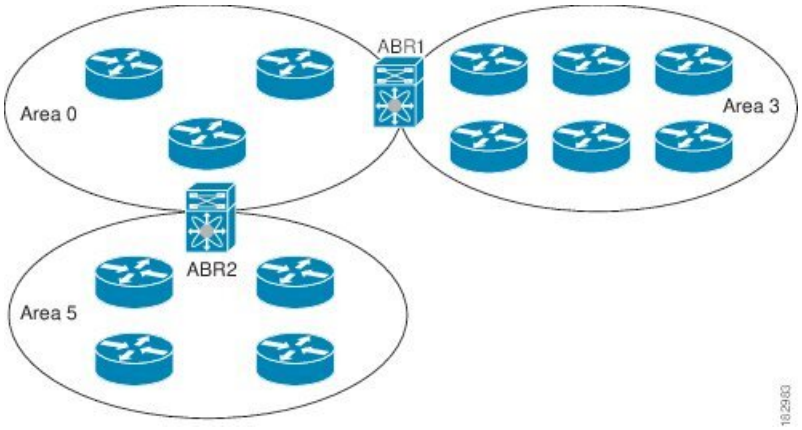
エリア

OSPFv3 ネットワークを複数のエリアに分割すると、ルータに要求される OSPFv3 の CPU とメモリに関する要件を制限できます。エリアとは、ルータの論理的な区分で、OSPFv3 ドメイン内にリンクして別のサブドメインを作成します。LSA フラッディングはエリア内でのみ発生し、リンクステートデータベースはエリア内のリンクにのみ制限されます。定義されたエリア内のインターフェイスには、エリア ID を割り当てることができます。エリア ID は、10.2.3.1 などの、数字またはドット付き 10 進表記で表現される 32 ビット値です。

Cisco NX-OS は常にドット付き 10 進表記でエリアを表示します。

OSPFv3 ネットワーク内に複数のエリアを定義する場合は、0 という予約されたエリア ID を持つバックボーンエリアも定義する必要があります。エリアが複数ある場合は、1 台以上のルータがエリア境界ルータ（ABR）となります。ABR は、バックボーン エリアと他の 1 つ以上の定義済みエリアの両方に接続します。

図 *2 : OSPFv3* エリア



ABR には、接続するエリアごとに個別のリンクステート データベースがあります。ABR は、接続したエリアの 1 つからバックボーン エリアにエリア間プレフィックス（タイプ 3）LSA（「ルート集約」セクションを参照）を送信します。バックボーン エリアは、1 つのエリアに関する集約情報を別のエリアに送信します。図に、エリア 0 が、エリア 5 に関する集約情報をエリア 3 に送信しています。

OSPFv3 では、自律システム境界ルータ（ASBR）という、もう 1 つのルータ タイプも定義されています。このルータは、OSPFv3 エリアを別の自律システム（AS）に接続します。自律システムとは、単一の技術的管理エンティティにより制御されるネットワークです。OSPFv3 は、そのルーティング情報を別の自律システムに再配布したり、再配布されたルートを別の自律システムから受信したりできます。詳細については、「詳細な機能」のセクションを参照してください。

リンクステート アドバタイズメント

OSPFv3 はリンクステート アドバタイズメント（LSA）を使用して、固有のルーティング テーブルを構築します。

リンクステート アドバタイズメント タイプ

OSPFv3 はリンクステート アドバタイズメント（LSA）を使用して、固有のルーティング テーブルを構築します。

次の表に、Cisco NX-OS でサポートされる LSA タイプを示します。

タイプ	名前	説明
1	ルータ LSA	すべてのルータが送信する LSA。この LSA には、すべてのリンクの状態とコストが含まれますが、プレフィックス情報は含まれません。ルータ LSA は SPF 再計算をトリガーします。ルータ LSA はローカル OSPFv3 エリアにフラッディングされます。

タイプ	名前	説明
2	ネットワーク LSA	DR が送信する LSA。この LSA には、マルチアクセス ネットワーク内のすべてのルータの一覧が含まれますが、プレフィックス情報は含まれません。ネットワーク LSA は SPF 再計算をトリガーします。「指定ルータ」のセクションを参照してください。
3	エリア間プレフィックス LSA	ABR が、ローカル エリア内の宛先ごとに外部エリアに送信する LSA。この LSA には、境界ルータからローカルの宛先へのリンク コストが含まれます。「エリア」のセクションを参照してください。
4	エリア間ルータ LSA	エリア境界ルータが外部エリアに送信する LSA。この LSA は、リンク コストを ASBR のみにアドバタイズします。「エリア」の項を参照してください。
5	AS 外部 LSA	ASBR が生成する LSA。この LSA には、外部自律システム宛先へのリンク コストが含まれます。AS 外部 LSA は、自律システム全体にわたってフラッディングされます。「エリア」の項を参照してください。
7	タイプ 7 LSA	ASBR が NSSA 内で生成する LSA。この LSA には、外部自律システム宛先へのリンク コストが含まれます。タイプ 7 LSA は、ローカル NSSA 内のみでフラッディングされます。「エリア」の項を参照してください。
8	リンク LSA	各ルータが、リンクローカル フラッディング スコープを使用して送信する LSA。（「フラッディングと LSA グループ ペーシング」の項を参照）。この LSA には、このリンクのリンクローカル アドレスと IPv6 アドレスが含まれます。
9	エリア内プレフィックス LSA	すべてのルータが送信する LSA。この LSA には、プレフィックスまたはリンク状態へのあらゆる変更が含まれます。エリア内プレフィックス LSA はローカル OSPFv3 エリアにフラッディングされます。この LSA は SPF 再計算をトリガーしません。
11	Grace LSA	再起動されるルータが、リンクローカル フラッディング スコープを使用して送信する LSA。この LSA は、OSPFv3 のグレースフル リスタートに使用されます。「ハイ アベイラビリティおよびグレースフル リスタート」を参照してください。

リンク コスト

各 OSPFv3 インターフェイスは、リンク コストを割り当てられています。このコストは任意の数字です。デフォルトでは、Cisco NX-OS が、設定された参照帯域幅をインターフェイス帯域

幅で割った値をコストとして割り当てます。デフォルトでは、参照帯域幅は 40 Gbps です。リンク コストは各リンクに対して、LSA 更新情報で伝えられます。

フラッディングと LSA グループ ペーシング

OSPFv3 は、LSA のタイプに応じて、ネットワークのさまざまなセクションに LSA の更新をフラッディングします。OSPFv3 は、次のフラッディング スコープを使用します

- リンク ローカル：LSA は、ローカル リンク上でのみフラッディングされます。リンク LSA および猶予 LSA に使用されます。
- エリアローカル：LSA は、単一の OSPF エリア全体にのみフラッディングされます。ルータ LSA、ネットワーク LSA、エリア間プレフィックス LSAs、エリア間ルータ LSA、およびエリア内プレフィックス LSA に使用されます。
- AS スコープ：LSA は、ルーティング ドメイン全体にフラッディングされます。AS スコープは AS 外部 LSA に使用されます。

LSA フラッディングにより、ネットワーク内のすべてのルータが同じルーティング情報を持つことが保証されます。LSA フラッディングは、OSPFv3 エリアの設定により異なります（「エリア」の項を参照）。LSA は、リンクステート リフレッシュ時間に基づいて（デフォルトでは 30 分ごとに）フラッディングされます。各 LSA には、リンクステート リフレッシュ時間が設定されています。

ネットワークの LSA 更新情報のフラッディング レートは、LSA グループ ペーシング機能を使用して制御できます。LSA グループ ペーシングにより、CPU またはバッファの使用率を低下させることができます。この機能により、同様のリンクステート リフレッシュ時間を持つ LSA がグループ化されるため、OSPFv3 で、複数の LSA を 1 つの OSPFv3 更新メッセージにまとめることが可能となります。

デフォルトでは、相互のリンクステート リフレッシュ時間が 10 秒以内の LSA が、同じグループに入れられます。この値は、大規模なリンクステート データベースでは低く、小規模のデータベースでは高くして、ネットワーク上の OSPFv3 負荷を最適化する必要があります。

リンクステート データベース

各ルータは、OSPFv3 ネットワーク用のリンクステート データベースを保持しています。このデータベースには、収集されたすべての LSA が含まれ、ネットワークを通過するすべてのルートに関する情報が格納されます。OSPFv3 は、この情報を使用して、各宛先への最適なパスを計算し、この最適なパスをルーティング テーブルに入力します。

MaxAge と呼ばれる設定済みの時間間隔で受信された LSA 更新情報がまったくない場合は、リンクステート データベースから LSA が削除されます。ルータは、LSA を 30 分ごとに繰り返してフラッディングし、正確なリンクステート情報が期限切れで削除されるのを防ぎます。Cisco NX-OS は、LSA グルーピング機能をサポートし、同時にすべての LSA が更新されないようにします。詳細については、「フラッディングと LSA グループ ペーシング 」のセクションを参照してください。

マルチエリア隣接関係（Multi-Area Adjacency）

OSPFv3 マルチエリア隣接関係により、複数のエリアにあるプライマリ インターフェイス上にリンクを設定できます。このリンクは、それらのエリア内の優先されるエリア内リンクになります。マルチエリア隣接関係では、OSPFv3 エリアにポイントツーポイントの番号なしリンクを確立し、そのエリアにトポロジ パスを提供します。プライマリ隣接関係はリンクを使用して、ネイバー ステートが full の場合に、ルータ LSA で対応するエリアの番号なしポイントツーポイント リンクをアドバタイズします。

マルチエリア インターフェイスは、OSPF の既存のプライマリ インターフェイス上の論理構成体として存在しますが、プライマリ インターフェイス上のネイバー ステートは、マルチエリア インターフェイスと無関係です。マルチエリア インターフェイスはネイバー ルータ上の対応するマルチエリア インターフェイスとの隣接関係を確立します。詳細については、「マルチエリア隣接関係の設定」の項を参照してください。

OSPFv3 と IPv6 ユニキャスト RIB

OSPFv3 は、リンクステート データベースでダイクストラの SPF アルゴリズムを実行します。このアルゴリズムにより、パス上の各リンクのリンク コストの合計に基づいて、各宛先への最適なパスが選択されます。選択された各宛先への最短パスが OSPFv3 ルート テーブルに入力されます。OSPFv3 ネットワークが収束すると、このルート テーブルは IPv6 ユニキャスト ルーティング情報ベース（RIB）にデータを提供します。OSPFv3 は IPv6 ユニキャスト RIB と通信し、次の動作を行います。

- ルートの追加または削除
- 他のプロトコルからのルートの再配布への対応
- 変更されていない OSPFv3 ルートの削除およびスタブ ルータ アドバタイズメントを行うためのコンバージェンス更新情報を提供します（「複数の OSPFv3 インスタンス（Multiple OSPFv3 Instances）」を参照）。

さらに OSPFv3 は、変更済みダイクストラ アルゴリズムを実行して、エリア間プレフィックス、エリア間ルータ、AS 外部、タイプ 7、およびエリア内プレフィックス（タイプ 3、4、5、7、8）の各 LSA の変更の高速再計算を行います。

アドレス ファミリのサポート

Cisco NX-OS は、ユニキャスト IPv6 やマルチキャスト IPv6 などの複数のアドレス ファミリをサポートしています。アドレス ファミリに特有の OSPFv3 機能は、次のとおりです。

- デフォルト ルート
- ルート集約

- ルートの再配布
- 境界ルータのフィルタ リスト
- SPF 最適化

これらの機能の設定時に IPv6 ユニキャスト アドレス ファミリ コンフィギュレーション モードを開始するには、 **address-family ipv6 unicast** コマンドを使用します。

認証および暗号化

OSPFv3 メッセージに認証を設定して、ネットワークでの不正な、または無効なルーティング更新を防止できます。

RFC 4552 は、IPv6 認証ヘッダー (AH) またはカプセル化セキュリティ ペイロード (ESP) 拡張ヘッダーを使用して、OSPFv3 への認証を提供します。Cisco NX-OS 7.0(3)I3(1) 以降、Cisco NX-OS は、IPv6 AH ヘッダーを使用して OSPFv3 パケットを認証することにより、RFC 4552 をサポートします。

Cisco NX-OS は、IP セキュリティ（IPSec）認証方式と、メッセージ ダイジェスト 5（MD5）またはセキュア ハッシュ アルゴリズム 1（SHA1）アルゴリズムをサポートして、OSPFv3 パケットを認証します。OSPFv3 IPSec 認証は、コマンドを使用しする静的キーのみをサポートします。

Cisco NX-OS は、OSPFv3 メッセージの暗号化と認証の両方に IPSec ESP 方式もサポートしています。暗号化は、ESP 暗号化の AES または 3DES アルゴリズムと、ESP 認証の SHA-1 または NULL をサポートします。

Cisco NX-OS リリース 10.4(1)F 以降、Cisco NX-OS は、キーチェーン オプションを使用した暗号化または認証アルゴリズムとキーの構成をサポートしています。

IPSec 暗号化または認証は、OSPFv3 プロセス、エリア、インターフェイス、あるいはその両方に対して構成可能です。認証設定は、プロセスからエリア、インターフェイス レベルに継承されます。認証が 3 つのレベルすべてで構成されている場合、インターフェイス構成がプロセスおよびエリア構成よりも優先され、エリア構成はプロセス レベルよりも優先されます。

高度な機能

Cisco NX-OS は、ネットワークでの OSPFv3 の可用性やスケーラビリティを向上させる高度な OSPFv3 機能をサポートしています。

スタブ エリア

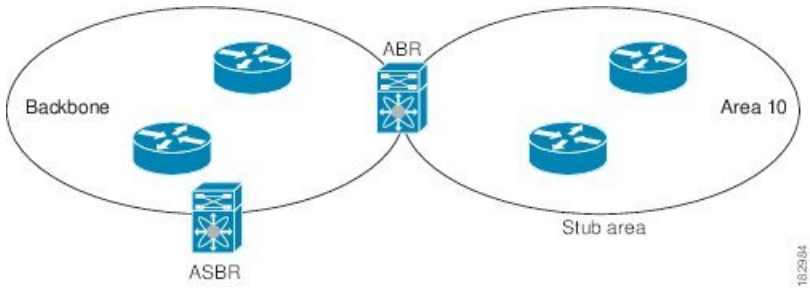
エリアをスタブエリアにすると、エリアでフラッディングされる外部ルーティング情報の量を制限できます。スタブ エリアとは、AS 外部（タイプ 5）LSA（リンクステート アドバタイズメント （6 ページ）の項を参照）が許可されないエリアです。これらの LSA は通常、外部

ルーティング情報を伝播するためにローカル自律システム全体でフラッディングされます。スタブ エリアには、次の要件があります。

- スタブ エリア内のすべてのルータはスタブ ルータです。「スタブ ルーティング」の項を参照してください。
- スタブ エリアには ASBR ルータは存在しません。
- スタブ エリアには仮想リンクを設定できません。

次の図に示す OSPFv3 自律システムでは、エリア 0.0.0.10 内のルータはすべて、外部自律システムに到達するために ABR を通過しなければなりません。エリア 0.0.0.10 は、スタブ エリアとして設定できます。

図 *3:* スタブ エリア



スタブ エリアは、外部自律システムへのバックボーン エリアを通過する必要のあるすべてのトラフィックにデフォルト ルートを使用します。デフォルト ルートは、プレフィックス長が IPv6 向けに 0 に設定されたエリア間プレフィックス LSA です。

Not-So-Stubby Area

Not-So-Stubby Area（NSSA）は、スタブ エリアに似ていますが、NSSA では、再配布を使用して NSSA 内で自律システム外部ルートをインポートできる点が異なります。NSSA ASBR はこれらのルートを再配布し、タイプ 7 LSA を生成して NSSA 全体にフラッディングします。または、このタイプ 7 LSA を AS 外部（タイプ 5）LSA に変換するよう、NSSA を他のエリアに接続する ABR を設定することができます。こうすると、ABR は、これらの AS 外部 LSA を OSPFv3 自律システム全体にフラッディングします。変換中は集約とフィルタリングがサポートされます。タイプ 7 LSA の詳細については、リンクステート アドバタイズメント （6 ページ） の項を参照してください。

たとえば、OSPFv3 を使用する中央サイトを、異なるルーティング プロトコルを使用するリモート サイトに接続するときに NSSA を使用すると、管理作業を簡素化できます。NSSA を使用する前は、企業サイトの境界ルータとリモート ルータの間の接続を OSPFv3 スタブ エリアとして実行できませんでした。これは、リモート サイトへのルートはスタブ エリア内に再配布できないためです。NSSA が実装されたことで、企業ルータとリモートルータ間のエリアを NSSA として定義することにより、OSPFv3 を拡張してリモート接続をカバーできます。（「NSSA の設定」の項を参照）。

バックボーン エリア 0 を NSSA にできません

（注） Cisco NX-OS リリース 9.3(1) 以降、OSPF は RFC 3101 セクション 2.5(3) に準拠するようになりました。Not-so-Stubby Area に接続されたエリア境界ルータが P ビット クリアのデフォルト ルート LSA を受信した場合は、無視されます。OSPF は、これらの条件下で以前にデフォルト ルートを追加していました。

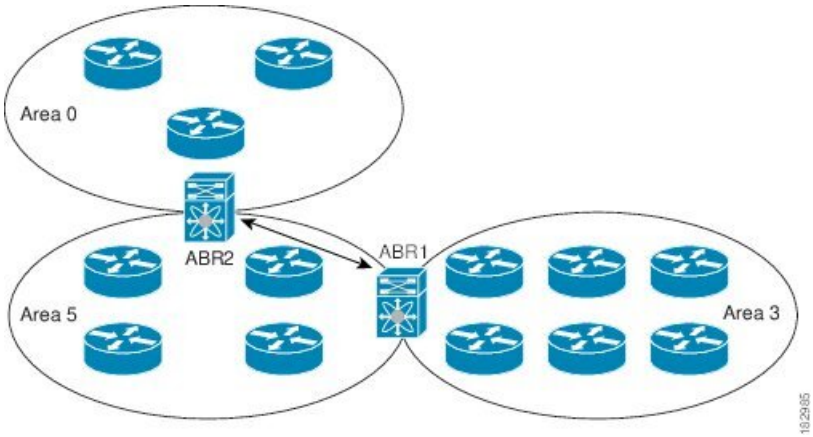
すでに RFC 非準拠の動作を使用するようにネットワークを設計しており、デフォルト ルートが NSSA ABR に追加されると想定している場合は、Cisco NX-OS リリース 9.3(1) 以降にアップグレードするときに動作が変更されます。

古い動作を続行する場合は、**default-route nssa-abr pbit-clear** コマンドで有効にすることができます。このコマンドは、Cisco NX-OS Release 9.3(1) で実装されました。

仮想リンク

仮想リンクを使用すると、物理的に直接接続できない場合に、OSPFv3 エリア ABR をバックボーン エリア ABR に接続できます。図には、エリア 3 をエリア 5 経由でバックボーン エリアに接続する仮想リンクを示します。

図 *4:* 仮想リンク



また、仮想リンクを使用して、分割エリアから一時的に回復できます。分割エリアは、エリア内のリンクがダウンしたために隔離された一部のエリアで、ここからはバックボーンエリアへの代表 ABR に到達できません。

ルートの再配布

OSPFv3 は、ルート再配布を使用して、他のルーティング プロトコルからルートを学習できます。「ルートの再配布の概要」の項を参照してください。リンク コストをこれらの再配布されたルートに割り当てるか、またはデフォルト リンク コストを再配布されたすべてのに割り当てるよう、OSPFv3 を設定します。

ルート再配布では、ルートマップを使用して、再配布する外部ルートを管理します。再配布を指定したルートマップを設定して、どのルートがOSPFv3に渡されるかを制御する必要があります。ルート マップを使用すると、宛先、送信元プロトコル、ルート タイプ、ルート タグなどの属性に基づいて、ルートをフィルタリングできます。ルートマップを使用して、これらの外部ルートがローカル OSPFv3 AS でアドバタイズされる前に AS 外部（タイプ 5）LSA および NSSA 外部（タイプ 7）LSA のパラメータを変更できます。詳細については、「Route Policy Manager の設定」を参照してください。

ルート集約

OSPFv3 は学習したすべてのルートをあらゆる OSPF 対応ルータと共有するので、ルート集約を使用して、それぞれの OSPF 対応ルータにフラッディングされる固有のルートの数を削減した方がよい場合もあります。ルート集約により、より具体的な複数のアドレスが、すべての具体的なアドレスを表す1つのアドレスに置き換えられるため、ルートテーブルが簡素化されます。たとえば、2010:11:22:0:1000::1 と 2010:11:22:0:2000:679:1 を 1 つの集約アドレス 2010:11:22::/32 に置き換えることができます。

一般的には、エリア境界ルータ（ABR）の境界ごとに集約します。集約は2つのエリアの間でも設定できますが、バックボーンの方向に集約する方が適切です。こうすると、バックボーンがすべての集約アドレスを受信し、すでに集約されているそれらのアドレスを他のエリアに投入できるためです。集約には、次の 2 タイプがあります。

- エリア間ルート集約
- 外部ルート集約

エリア間ルート集約は ABR 上で設定し、自律システム内のエリア間のルートを集約します。集約の利点を生かすには、これらのアドレスを1つの範囲内にまとめることができるように、連続するネットワーク番号をエリア内で割り当てます。

外部ルート集約は、ルート再配布を使用して OSPFv3 に投入される外部ルートに特有のルート集約です。集約する外部の範囲が連続していることを確認する必要があります。異なる2台のルータからの重複範囲を集約すると、誤った宛先にパケットが送信される原因となる場合があります。外部ルート集約は、ルートを OSPF に再配布している ASBR で設定してください。

集約アドレスの設定時に Cisco NX-OS は、ルーティング ブラック ホールおよびルート ループを防ぐために、集約アドレスの廃棄ルートを自動的に設定します。

高可用性およびグレースフル リスタート

Cisco NX-OS は、マルチレベルのハイ アベイラビリティ アーキテクチャを提供します。OSPFv3 は、ステートフル リスタートをサポートしています。これは、ノンストップ ルーティング（NSR）とも呼ばれます。OSPFv3 で問題が発生した場合は、以前の実行時状態からの再起動を試みます。この場合、ネイバーはいずれのネイバーイベントも登録しません。最初の再起動が正常ではなく、別の問題が発生した場合、OSPFv3 はグレースフル リスタートを試みます。

グレースフル リスタート、つまり、Nonstop Forwarding（NSF）では、処理の再起動中も OSPFv3 がデータ転送パス上に存在し続けます。OSPFv3 はグレースフル リスタートの実行が必要にな

ると、リンクローカル猶予（タイプ 11）LSA を送信します。この再起動中の OSPFv3 プラットフォームは NSF 対応と呼ばれます。

猶予 LSA には猶予期間が含まれます。猶予期間とは、ネイバー OSPFv3 インターフェイスは再起動中の OSPFv3 インターフェイスからの LSA を待つよう指定された時間です（通常、OSPFv3は隣接関係を切断し、ダウン状態または再起動中のOSPFv3インターフェイスからのすべてのLSAを廃棄します）。参加するネイバーは、NSF ヘルパーと呼ばれ、再起動中の OSPFv3 インターフェイスから発信されたすべての LSA を、インターフェイスがまだ隣接しているかのように保持します。

再起動中の OSPFv3 インターフェイスが稼働を再開すると、ネイバーを再探索して隣接関係を確立し、LSA 更新情報の送信を再開します。この時点で、NSF ヘルパーは、グレースフル リスタートが完了したと認識します。

ステートフル リスタートは次のシナリオで使用されます。

- プロセスでの問題発生後の最初の回復試行
- **system switchover** を使用したユーザー開始スイッチオーバー command

グレースフル リスタートは次のシナリオで使用されます。

- プロセスでの問題発生後の 2 回目の回復試行（4 分以内）
- **restart ospfv3** を使用したプロセスの手動再起動 command
- アクティブ スーパーバイザの削除
- **reload module** *active-sup* を使用したアクティブ スーパーバイザのリロード コマンド

複数の OSPFv3 インスタンス

Cisco NX-OS は、OSPFv3 プロトコルの複数インスタンスをサポートしています。デフォルトでは、すべてのインスタンスが同じシステム ルータ ID を使用します。複数のインスタンスが同じ OSPFv3 自律システムにある場合は、各インスタンスのルータ ID を手動で設定する必要があります。サポートされる OSPFv3 インスタンスの数については、『Cisco Nexus 9000 Series NX-OS Verified Scalability Guide』を参照してください。

OSPFv3 ヘッダーには、特定の OSPFv3 インスタンスの OSPFv3 パケットを識別するためのインスタンス ID フィールドが含まれます。この OSPv3 インスタンスを割り当てることができます。インターフェイスは、パケット ヘッダーの OSPFv3 インスタンス ID が一致しない OSPFv3 パケットをすべてドロップします。

Cisco NX-OS では、インターフェイス上に 1 つの OSPFv3 インスタンスのみが許可されます。

SPF 最適化

Cisco NX-OS は、次の方法で SPF アルゴリズムを最適化します。

- ネットワーク（タイプ 2）LSA、エリア間プレフィックス（タイプ 3）LSA、および AS 外部（タイプ 5）LSA 用部分 SPF：これらの LSA のいずれかが変更されると、Cisco NX-OS は、全体的な SPF 計算ではなく、高速部分計算を実行します。
- SPF タイマー：さまざまなタイマーを設定して、SPF 計算を制御できます。これらのタイマーには、後続の SPF 計算の幾何バックオフが含まれます。幾何バックオフにより、複数の SPF 計算による CPU 負荷が制限されます。

BFD

この機能では、IPv6 用の双方向フォワーディング検出（BFD）をサポートします。BFD は、転送パスの障害を高速で検出することを目的にした検出プロトコルです。BFD は 2 台の隣接デバイス間のサブセカンド障害を検出し、BFD の負荷の一部を、サポートされるモジュール上のデータ プレーンに分散できるため、プロトコル hello メッセージよりも CPU を使いません。詳細については、『Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide』を参照してください。

仮想化のサポート

Cisco NX-OS は、OSPFv3 の複数のプロセス インスタンスをサポートします。各 OSPFv3 インスタンスは、システム制限まで、複数の仮想ルーティングおよび転送（VRF）インスタンスをサポートできます。サポートされる OSPFv3 インスタンスの数については、『Cisco Nexus 9000 Series NX-OS Verified Scalability Guide』を参照してください。

OSPFv3 の前提条件

OSPFv3 の前提条件は次のとおりです。

- OSPFv3 を設定するための、ルーティングの基礎に関する詳しい知識がある。
- スイッチにログオンしている。
- リモート OSPFv3 ネイバーと通信可能な 1 つ以上の IPv6 用インターフェイスが設定されている。
- Enterprise Services ライセンスがインストールされている。
- OSPFv3 ネットワーク戦略と、ネットワークのプランニングが完成している。たとえば、複数のエリアが必要かどうかを決定します。
- OSPF 機能を有効していること（「OSPFv3 の有効化」の項を参照）。
- IPv6 アドレス指定および基本設定に関する詳しい知識がある。IPv6 ルーティングおよびアドレス指定の詳細については、IPv6 アドレスを参照してください。

OSPFv3 の注意事項および制約事項

OSPFv3 設定時の注意事項および制約事項は、次のとおりです。

- リロード時の OSPFv2 の **graceful-restart planned-only** コマンドは、**graceful-restart** コマンドに変換されます。

  これは機能に影響を与えません。**graceful-restart planned-only** が設定にない場合、この問題はそのデバイスには適用されません。

  これは、Cisco NX-OS リリースが 9.3(2) で、CSCvs57583 がリリースに含まれていない場合に発生します。回避策は、**graceful-restart** コマンドを設定解除し、古いコマンドを再設定することです。

- プレフィックス リスト内の名前は、大文字と小文字が区別されません。一意の名前を使用することを推奨します。大文字と小文字を変更して同じ名前を使用しないでください。たとえば、CTCPrimaryNetworks と CtcPrimaryNetworks は 2 つの異なるエントリではありません。

- **no graceful-restart planned only** コマンドを入力すると、グレースフル リスタートは無効になります。

- Cisco NX-OS は、ユーザがエリアを 10 進表記で入力するか、ドット付き 10 進表記で入力するかに関係なく、ドット付き 10 進表記でエリアを表示します。

- 仮想ポート チャネル（vPC）環境で OSPFv3 を設定する場合は、コア スイッチ上のルータ コンフィギュレーション モードで次のタイマー コマンドを使用することにより、vPC ピアリンクがシャットダウンしたときに OSPF の高速コンバージェンスを実現します。

```
switch(config-router)# timers throttle spf 1 50 50
switch(config-router)# timers lsa-arrival 10
```

- スケール シナリオでは、インターフェイスと OSPF プロセスのリンク ステート アドバタイズメントの数が大きい場合、OSPF MIB オブジェクトの SNMP エージェントのタイムアウト値が小さい SNMP ウォークは、タイムアウトになると予想されます。OSPF MIB オブジェクトのポーリング中に問い合わせる SNMP エージェントのタイムアウトを確認する場合は、ポーリングする SNMP エージェントのタイムアウト値を増加してください。

- アドミニストレーティブ ディスタンス機能には、次のガイドラインと制限事項が適用されます。

  - OSPF ルートに複数の等コスト パスがある場合、アドミニストレーティブ ディスタンスを設定しても **match ip route-source** コマンドに対しては決定性を持ちません。 コマンドを使用する必要があります。

  - OSPFv3ルートのルートソースを照合するには、 **match ip route-source** を設定します。次は古い構文です: **match ipv6 route-source** OSPFv3 のルートソースとルータ ID が IPv4 アドレスであるためです。

- アドミニストレーティブ ディスタンスの設定は、**match route-type**、**match ipv6 address prefix-list**、および **match ip route-source prefix-list** コマンドでのみサポートされます。別の match 文は無視されます。
- 廃棄ルートには、アドミニストレーティブ ディスタンス 220 が常に割り当てられます。テーブル マップの設定は OSPF の廃棄ルートには適用されません。
- OSPF ルートのアドミニストレーティブ ディスタンスを設定する場合、**match route-type**、**match ipv6 address**、および **match ip route-source** コマンドの間に優先順位はありません。このように、Cisco NX-OS OSPF アドミニストレーティブ ディスタンスを設定するためのテーブル マップの動作は、Cisco IOS OSPF の場合と異なります。

- vPC コンフィギュレーション モードで **delay restore** *seconds* コマンドを設定する場合や、マルチシャーシ EtherChannel トランク（MCT）上の VLAN がスイッチ仮想インターフェイス（SVI）を使用して OSPFv2 または OSPFv3 によって通知される場合、これらの SVI は設定された時間の間、vPC セカンダリ ノード上で MAX_LINK_COST で通知されます。その結果、すべてのルートまたはホストのプログラミングは、トラフィックを引き込む前に（セカンダリ vPC ノードのピア リロードで）vPC の同期操作後に完了します。この動作により、ノースサウス トラフィックのパケット損失を最小にできます。
- プライマリエリアとマルチエリアに同じエリア *ID* を設定すると、エラーが表示されずに設定が受け入れられます。プライマリエリアとマルチエリアを設定する場合は、同じエリア *ID*を使用しないでください。

（注） Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

- OSPF で **network** *ip address mask* コマンドを使用すると、エラー メッセージが表示され、**area** *area id* コマンドを使用してインターフェイスで OSPF を有効にするように求められます。
- OSPF のデフォルト タイマー（hello-interval:10 および dead-interval:40）を使用することをお勧めします。コンバージェンス時間を短縮するには、OSPF とともに BFD を使用できます。この組み合わせにより、1 秒未満のリンク/隣接フラップ検出と非常に短いコンバージェンス時間が実現します。
- OSPF サポートはアグレッシブタイマーですが、アグレッシブ イマーは調整をすぐにダウンさせ、CPU チャーンを引き起こすため、推奨されません。デフォルトのタイマーを使用し、BFD（双方向転送検出）を使用して 1 秒未満の障害検出を行うことを推奨します。
- ルート ポリシー マネージャ（RPM）は、ルート マップ内のコミュニティ リストを使用して BGP コミュニティ属性に基づいて BGP ルート更新をフィルタリングするための IPv6 再配布をサポートしていません。この機能は、IPv4 再配布でのみ使用できます。

- Cisco NX-OS リリース 10.3(1)F 以降、OSPFv3 は Cisco Nexus 9808 スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、 OSPFv3 は Cisco Nexus 9804 スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、Cisco NX-OS スイッチの OSPFv3 暗号化および認証コマンドに対してキーチェーンのサポートが提供されます。
- Cisco NX-OS リリース 10.4(1)F 以降、OSPFv3 は Cisco Nexus 9808 および 9804 スイッチを搭載した Cisco Nexus X98900CD-A および X9836DM-A ライン カードでサポートされます。
- Cisco NX-OS リリース 10.4(2)F 以降、OSPFv3 は Cisco Nexus 9232E-B1 スイッチでサポートされます。
- Cisco NX-OS リリース 10.6(1)F 以降、OSPFv3 は Cisco Nexus N9336C-SE1 スイッチでサポートされます。

デフォルト設定

次の表に、OSPFv3 パラメータのデフォルト設定値を示します。

表 *1 : OSPFv3* のデフォルト パラメータ

パラメータ	デフォルト
アドミニストレーティブ ディスタンス	110
hello 間隔	10 秒
デッド間隔	40 秒
廃棄ルート	イネーブル
グレースフル リスタートの猶予期間	60 秒
グレースフル リスタートの通知期間	15 秒
OSPFv3 機能	ディセーブル
スタブ ルータ アドバタイズメントの宣言期間	600 秒
リンク コスト計算の参照帯域幅	40 Gbps
LSA 最小到着時間	1000 ミリ秒
LSA グループ ペーシング	10 秒
SPF 計算初期遅延時間	200 ミリ秒

パラメータ	デフォルト
SPF 計算最小ホールド タイム	1000 ミリ秒
SPF 計算の最大待機時間	5000 ミリ秒

基本的な OSPFv3 の設定

OSPFv3 は、OSPFv3 ネットワークを設計したあとに設定します。

OSPFv3 の有効化

手順

ステップ 1 **configure terminal**

例：

```
switch# configure terminal
switch(config)#
```

グローバル コンフィギュレーション モードを開始します。

ステップ 2 [**no**] **feature ospfv3**

例：

```
switch(config)# feature ospfv3
```

OSPFv3 を有効にします。

このコマンドを持つ **no** キーワードを使用すると、OSPFv3 機能を無効にして、関連するすべての設定を削除します。

ステップ 3 （任意） **show feature**

例：

```
switch(config)# show feature
```

有効および無効にされた機能を表示します。

ステップ 4 （任意） **copy running-config startup-config**

例：

```
switch(config)# copy running-config
startup-config
```

この設定変更を保存します。

OSPFv3 インスタンスの作成

OSPFv3 設定の最初のステップは、インスタンスまたは OSPFv3 インスタンスの作成です。作成した OSPFv3 インスタンスには、一意のインスタンス タグを割り当てます。インスタンス タグは任意の文字列です。各 OSPFv3 インスタンスには、省略可能な次のパラメータも設定できます。

- Router ID：この OSPFv3 インスタンスのルータ ID を設定します。このパラメータを使用しない場合は、ルータ ID 選択アルゴリズムが使用されます。「ルータ ID」セクションを参照してください。
- Administrative distance：ルーティング情報の送信元の信頼性をランク付けします。詳細については、「アドミニストレーティブ ディスタンス」のセクションを参照してください。
- Log adjacency changes：OSPFv3 ネイバーの状態が変化するたびにシステム メッセージを作成します。
- 名前のルックアップ：ローカル ホストのデータベースを検索または IPv6 の DNS 名を照会することでホスト名に OSPF ルータ ID を変換します。
- Maximum paths：OSPFv3 が、特定の宛先についてルート テーブルにインストールする同等パスの最大数を設定します。このパラメータは、複数パス間のロードバランシングに使用します。
- Reference bandwidth：ネットワークの算出 OSPFv3 コスト メトリックを制御します。算出コストは、参照帯域幅をインターフェイス帯域幅で割った値です。算出コストは、ネットワークが OSPFv3 インスタンスに追加されるときにリンク コストを割り当てると、無効にすることができます。詳細については、「OSPFv3 でのネットワークの設定」のセクションを参照してください。

OSPFv3 インスタンス パラメータの詳細については、「高度な OSPFv3 の設定」のセクションを参照してください。

始める前に

OSPFv3 機能が有効にされている必要があります（「OSPFv3 の有効化 」のセクションを参照）。

- 使用する予定の OSPFv3 インスタンス タグが、このルータ上では使用されていないことを確認します。
- **show ospfv3** *instance-tag* を使用します。 コマンドを使用して、インスタンス タグが使用されていないことを確認します。
- OSPFv3 がルータ識別子（設定済みのループバック アドレスなど）を入手可能であるか、またはルータ ID オプションを設定する必要があります。

手順

ステップ 1 **configure terminal**

例：

```
switch# configure terminal
switch(config)#
```

グローバル コンフィギュレーション モードを開始します。

ステップ 2 [**no**] **router ospfv3** *instance-tag*

例：

```
switch(config)# router ospfv3 201
 switch(config-router)#
```

新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

（注）
インターフェイス モードでは、**no router ospfv3** *instance tag* コマンドによって OSPF の設定を削除できません。インターフェイス モードで設定された OSPFv3 コマンドはいずれも、手動で削除する必要があります。

ステップ 3 （任意） **router-id** *ip-address*

例：

```
switch(config-router)# router-id
 192.0.2.1
```

OSPFv3 ルータ ID を設定します。このドット付き 10 進表記の ID で、この OSPFv3 インスタンスが識別されます。この ID は、システムの設定済みインターフェイス上に存在する必要があります。

ステップ 4 （任意） **show ipv6 ospfv3** *instance-tag*

例：

```
switch(config-router)# show ipv6 ospfv3
 201
```

OSPFv3 情報を表示します。

ステップ 5 （任意） **log-adjacency-changes** [**detail**]

例：

```
switch(config-router)#
 log-adjacency-changes
```

ネイバーの状態が変化するたびに、システム メッセージを生成します。

ステップ 6 （任意） **passive-interface default**

例：

```
switch(config-router)# passive-interface
 default
```

すべてのインターフェイス上でルーティングが更新されないようにします。このコマンドは、VRF またはインターフェイス コマンド モードの設定によって上書きされます。

ステップ 7 （任意） **distance** *number*

例：

```
switch(config-router-af)# distance 25
```

この OSPFv3 インスタンスのアドミニストレーティブ ディスタンスを設定します。範囲は 1 ～ 255 です。デフォルトは 110 です。

ステップ 8 （任意） **maximum-paths** *paths*

例：

```
switch(config-router-af)# maximum-paths
 4
```

ルート テーブル内の宛先に対する同等 OSPFv3 パスの最大数を設定します。指定できる範囲は 1 ～ 16 です。デフォルト値は 8 です。このコマンドはロード バランシングに使用されます。

ステップ 9 （任意） **copy running-config startup-config**

例：

```
switch(config)# copy running-config startup-config
```

実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします

例

次の例は、OSPFv3 インスタンスを作成する方法を示しています。

```
switch# <userinput>configure terminal</userinput>
switch(config)# <userinput>router ospfv3 201</userinput>
 switch(config-router)# <userinput>copy running-config startup-config</userinput>
```

OSPFv3 でのネットワークの構成

ルータがこのネットワークへの接続に使用するインターフェイスを介して、OSPFv3 へのネットワークを関連付けることで、このネットワークを設定できます（「ネイバー」セクションを参照）。すべてのネットワークをデフォルトバックボーンエリア（エリア 0）に追加したり、任意の 10 進数または IP アドレスを使用して新規エリアを作成したりできます。

すべてのエリアは、バックボーンエリアに直接、または仮想リンク経由で接続する必要があります。

インターフェイスの有効な IPv6 アドレスを設定するまでは、インターフェイス上で OSPFv3 がイネーブルになりません。

始める前に

OSPFv3 機能が有効にされている必要があります（「OSPFv3 の有効化 」のセクションを参照）。

手順

ステップ 1 **configure terminal**

例：

```
switch# configure terminal
switch(config)#
```

グローバル コンフィギュレーション モードを開始します。

ステップ 2 **interface***interface-type slot/port*

例：

```
switch(config)# interface ethernet 1/2
 switch(config-if)#
```

インターフェイス設定モードを開始します。

ステップ 3 **ipv6 address***ipv6-prefix/length*

例：

```
switch(config-if)# ipv6 address
 2001:0DB8::1/48
```

このインターフェイスに IPv6 アドレスを割り当てます。

ステップ 4 **ipv6 router ospfv3***instance-tag***area***area-id* [**secondaries none**]

例：

```
switch(config-if)# ipv6 router ospfv3
 201 area 0
```

OSPFv3 インスタンスおよびエリアにインターフェイスを追加します。

ステップ 5 （任意） **show ipv6 ospfv3***instance-tag***interface***interface-type slot/port*

例：

```
switch(config-if)# show ipv6 ospfv3 201
 interface ethernet 1/2
```

OSPFv3 情報を表示します。

ステップ 6 （任意） **ospfv3 cost***number*

例：

```
switch(config-if)# ospfv3 cost 25
```

このインターフェイスの OSPFv3 コスト メトリックを設定します。デフォルトでは、参照帯域幅とインターフェイス帯域幅に基づいて、コスト メトリックが計算されます。有効な範囲は 1 ～ 65535 です。

ステップ 7 （任意） **ospfv3 dead-interval***seconds*

例：

```
switch(config-if)# ospfv3 dead-interval 50
```

OSPFv3 デッド間隔を秒単位で設定します。有効な範囲は 1 ～ 65535 です。デフォルトでは、hello 間隔の秒数の 4 倍です。

ステップ 8 （任意） **ospfv3 hello-interval***seconds*

例：

```
switch(config-if)# ospfv3 hello-interval
 25
```

OSPFv3 hello 間隔を秒単位で設定します。有効な範囲は 1 ～ 65535 です。デフォルトは 10 秒です。

ステップ 9 （任意） **ospfv3 instance***instance*

例：

```
switch(config-if)# ospfv3 instance 25
```

OSPFv3 インスタンス ID を設定します。有効な範囲は 0 ～ 255 です。デフォルトは 0 です。インスタンス ID のスコープはリンクローカルです。

ステップ 10 （任意） **ospfv3 mtu-ignore**

例：

```
switch(config-if)# ospfv3 mtu-ignore
```

OSPFv3 で、ネイバーとのあらゆる IP 最大伝送単位（MTU）不一致が無視されるよう設定します。デフォルトでは、ネイバー MTU がローカル インターフェイス MTU が不一致の場合には、隣接関係が確立されません。

ステップ 11 （任意） **ospfv3 network** {**broadcast** | **point-point**}

例：

```
switch(config-if)# ospfv3 network
 broadcast
```

OSPFv3 ネットワーク タイプを設定します。

ステップ 12 （任意） [**default** | **no**] **ospfv3 passive-interface**

例：

```
switch(config-if)# ospfv3
 passive-interface
```

インターフェイス上でルーティングが更新されないようにします。このコマンドによって、ルータまたは VRF コマンド モードの設定が上書きされます。**default** オプションは、このインターフェイス モード コマンドを削除して、ルータまたは VRF の設定に戻します（設定がある場合）。

ステップ 13 （任意） **ospfv3 priority***number*

例：

```
switch(config-if)# ospfv3 priority 25
```

エリアの DR の決定に使用される OSPFv3 優先度を設定します。有効な範囲は 0 ～ 255 です。デフォルトは 1 です。「指定ルータ」の項を参照してください。

ステップ 14 （任意） **ospfv3 shutdown**

例：

```
switch(config-if)# ospfv3 shutdown
```

このインターフェイス上の OSPFv3 インスタンスをシャットダウンします。

ステップ 15 （任意） **copy running-config startup-config**

例：

```
switch(config)# copy running-config startup-config
```

実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします

例

次に、OSPFv3 インスタンス 201 にネットワーク エリア 0.0.0.10 を追加する例を示します。

```
switch# configure terminal
 switch(config)# interface ethernet 1/2
 switch(config-if)# ipv6 address 2001:0DB8::1/48
 switch(config-if)# ipv6 router ospfv3 201 area 0.0.0.10
 switch(config-if)# copy running-config startup-config
```

高度な OSPFv3 の構成

OSPFv3 は、OSPFv3 ネットワークを設計したあとに設定します。

境界ルータのフィルタ リストの設定

OSPFv3 ドメインを、関連性のある各ネットワークを含む一連のエリアに分離できます。すべてのエリアは、エリア境界ルータ（ABR）経由でバックボーン エリアに接続している必要があります。OSPFv3 ドメインは、自律システム境界ルータ（ASBR）を介して、外部ドメインにも接続可能です。「エリア」の項を参照してください。

ABR には、省略可能な次の設定パラメータがあります。

- Area range：エリア間のルート集約を設定します。詳細については、「ルート集約の設定」の項を参照してください。
- Filter list：ABR 上で、外部エリアから受信したエリア間プレフィックス（タイプ 3）LSA をフィルタリングします。

ASBR もフィルタ リストをサポートしています。

始める前に

フィルタ リストが、着信または発信エリア間プレフィックス（タイプ 3）LSA の IP プレフィックスのフィルタリングに使用するルート マップを作成します。Route Policy Manager の設定を参照してください。

手順

ステップ 1 **router ospfv3** *instance-tag*

例：

```
switch(config)# router ospfv3 201
 switch(config-router)#
```

インスタンス タグを設定して、新しい OSPFv3 インスタンスを作成します。

ステップ 2 **address-family ipv6 unicast**

例：

```
switch(config-router)# address-family
 ipv6 unicast
 switch(config-router-af)#
```

IPv6 ユニキャスト アドレス ファミリ モードを開始します。

ステップ 3 **area** *area-id* **filter-list route-map** *map-name* {**in | out**}

例：

```
switch(config-router-af)# area 0.0.0.10
 filter-list route-map FilterLSAs in
```

ABR 上で着信または発信エリア間プレフィックス（タイプ 3）LSA をフィルタリングします。

ステップ 4 （任意） **show ipv6 ospfv3 policy statistics area** *id* **filter-list** {**in** | **out**}

例：

```
switch(config-router-af)# show ipv6 ospfv3
 policy statistics area 0.0.0.10
 filter-list in
```

OSPFv3 ポリシー情報を表示します。

ステップ 5 （任意） **copy running-config startup-config**

例：

```
switch(config-router-af)# copy running-config
 startup-config
```

この設定変更を保存します。

例

次に、ルート マップ用にフィルタを設定する例を示します。

```
switch# <userinput>configure terminal</userinput>
 switch(config)# <userinput>router ospfv3 201</userinput>
 switch(config-router)# <userinput>address-family ipv6 unicast</userinput>
 switch(config-router-af)# <userinput>area 0.0.0.10 filter-list route-map FilterLSAs
in</userinput>
 switch(config-router-af)# <userinput>copy running-config startup-config</userinput>
```

スタブ エリアの構成

OSPFv3 ドメインの外部トラフィックが不要な個所にスタブエリアを設定できます。スタブエリアはAS外部（タイプ5）LSAをブロックし、不要な、選択したネットワークへの往復のルーティングを制限します。「スタブエリア」の項を参照してください。また、すべての集約ルートがスタブ エリアを経由しないようブロックすることもできます。

始める前に

- OSPF 機能がイネーブルにされている必要があります（「OSPFv3 のイネーブル化 」の項を参照）。
- 設定されるスタブ エリア内に、仮想リンクと ASBR のいずれも含まれないことを確認します。

手順

ステップ 1 **router ospfv3** *instance-tag*

例：

```
switch(config)# router ospfv3 201
 switch(config-router)#
```

新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

ステップ 2 **area** *area-id* **stub**

例：

```
switch(config-router)# area 0.0.0.10
 stub
```

このエリアをスタブ エリアとして作成します。

ステップ 3 （任意） **address-family ipv6 unicast**

例：

```
switch(config-router)# address-family
 ipv6 unicast
 switch(config-router-af)#
```

IPv6 ユニキャスト アドレス ファミリ モードを開始します。

ステップ 4 （任意） **area** *area-id* **default cost** *cost*

例：

```
switch(config-router-af)# area 0.0.0.10
 default-cost 25
```

このスタブ エリアに送信されるデフォルト サマリ ルートのコスト メトリックを設定します。指定できる範囲は 0 ～ 16777215 です。

ステップ 5 （任意） **copy running-config startup-config**

例：

```
switch(config-router-af)# copy running-config
 startup-config
```

この設定変更を保存します。

例

次に、すべてのサマリ ルート更新をブロックするスタブエリアを作成する例を示します。

```
switch# <userinput>configure terminal</userinput>
 switch(config)# <userinput>router ospfv3 201</userinput>
 switch(config-router)# <userinput>area 0.0.0.10 stub no-summary</userinput>
 switch(config-router)# <userinput>copy running-config startup-config</userinput>
```

Totally Stubby エリアの構成

Totally Stubby エリアを作成して、すべての集約ルート更新がスタブ エリアに入るのを防ぐことができます。

Totally Stubby エリアを作成するには、ルータ コンフィギュレーション モードで次のコマンドを使用します。

手順

---

area *area-id* **stub no-summary**

例：

```
switch(config-router)# area 20 stub
 no-summary
```

このエリアを Totally Stubby エリアとして作成します。

NSSA の設定

OSPFv3 ドメインの一部で一定限度の外部トラフィックが必要な場合は、その部分に NSSA を設定できます。

また、この外部トラフィックを AS 外部（タイプ 5）LSA に変換して、このルーティング情報で OSPFv3 ドメインをフラッディングすることもできます。NSSA は、次のパラメータ（省略可能）で設定できます。

- No redistribution：NSSA をバイパスして OSPFv3 自律システム内の他のエリアに到達するルートを再配布します。このオプションは、NSSA ASBR が ABR も兼ねているときに使用します。
- Default information originate：外部自律システムへのデフォルト ルートのタイプ 7 LSA を生成します。このオプションは、ASBR のルーティング テーブルにデフォルト ルートが含まれる場合に NSSA ASBR 上で使用します。このオプションは、ABR のルーティング テーブルにデフォルト ルートが含まれているかどうかに関係なく、NSSA ABR 上で使用できます。
- Route map：目的のルートのみが NSSA および他のエリア全体でフラッディングされるよう、外部ルートをフィルタリングします。
- No summary：すべての集約ルートが NSSA でフラッディングされないようにします。このオプションは NSSA ABR 上で使用します。
- Translate：NSSA 外のエリア向けに、タイプ 7 LSA を AS 外部 LSA（タイプ 5）に変換します。再配布されたルートを OSPFv3 自律システム全体でフラッディングするには、このコマンドを NSSA ABR 上で使用します。また、これらの AS 外部 LSA の転送アドレスを無効にすることもできます。

（注） 変換オプションでは、個別の **area***area-id***nssa** コマンドが必要ですが、その前に、NSSA を作成し、他のオプションを設定する、**area***area-id***nssa** コマンドが必要です。

始める前に

OSPF 機能が有効にされている必要があります（「OSPFv3 の有効化 」の項を参照）。

- 設定する NSSA 上に仮想リンクがないことと、この NSSA がバックボーン エリアでないことを確認します。

手順

ステップ 1 **router ospfv3***instance-tag*

例：

```
switch(config)# router ospfv3 201
  switch(config-router)#
```

新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

ステップ 2 **area***area-id***nssa** [**no-redistribution**][**default-information-originate**] [**route-map***map-name*] [**no-summary**]

例：

```
switch(config-router)# area 0.0.0.10
  nssa
```

このエリアを NSSA として作成します。

ステップ 3 （任意） **area***area-id***nssa translate type7** {**always | never**} [**suppress-fa**]

例：

```
switch(config-router)# area 0.0.0.10
  nssa translate type7 always
```

AS 外部（タイプ 7）LSA を NSSA 外部（タイプ 5）LSA に変換するように NSSA を設定します。

ステップ 4 （任意） **address-family ipv6 unicast**

例：

```
switch(config-router)# address-family
  ipv6 unicast
  switch(config-router-af)#
```

IPv6 ユニキャスト アドレス ファミリ モードを開始します。

ステップ 5 （任意） **area***area-id***default cost***cost*

例：

```
switch(config-router-af)# area 0.0.0.10
  default-cost 25
```

この NSSA に送信されるデフォルト集約ルートのコスト メトリックを設定します。指定できる範囲は 0 ～ 16777215 です。

ステップ 6 （任意） **copy running-config startup-config**

例：

```
switch(config-router-af)# copy running-config
  startup-config
```

この設定変更を保存します。

例

次に、すべての集約ルート更新をブロックする NSSA を作成する例を示します。

```
switch# <userinput>configure terminal</userinput>
 switch(config)# <userinput>router ospfv3 201</userinput>
```

```
 switch(config-router)# <userinput>area 0.0.0.10 nssa no-summary</userinput>
 switch(config-router)# <userinput>copy running-config startup-config</userinput>
```

次に、デフォルト ルートを生成する NSSA を作成する例を示します。

```
switch# <userinput>configure terminal</userinput>
 switch(config)# <userinput>router ospfv3 201</userinput>
 switch(config-router)# <userinput>area 0.0.0.10 nssa default-info-originate</userinput>

 switch(config-router)# <userinput>copy running-config startup-config</userinput>
```

次に、外部ルートをフィルタリングし、すべての集約ルート更新をブロックするNSSA を作成する例を示します。

```
switch# <userinput>configure terminal</userinput>
 switch(config)# <userinput>router ospfv3 201</userinput>
 switch(config-router)# <userinput>area 0.0.0.10 nssa route-map ExternalFilter
no-summary</userinput>
 switch(config-router)# <userinput>copy running-config startup-config</userinput>
```

<!--CSCvv84492-->次に、NSSA を作成してから、常に AS 外部（タイプ 7）LSA を NSSA 外部（タイプ 5）LSA に変換するように NSSA を設定する例を示します。

```
switch# <userinput>configure terminal</userinput>
 switch(config)# <userinput>router ospfv3 201</userinput>
 switch(config-router)# <userinput>area 0.0.0.10 nssa</userinput>
 switch(config-router)# <userinput>area 0.0.0.10 nssa translate type 7 always</userinput>

 switch(config-router)# <userinput>copy running-config startup-config</userinput>
```

次に、すべての集約ルート更新をブロックする NSSA を作成する例を示します。

```
switch# <userinput>configure terminal</userinput>
 switch(config)# <userinput>router ospfv3 201</userinput>
 switch(config-router)# <userinput>area 0.0.0.10 nssa no-summary</userinput>
 switch(config-router)# <userinput>copy running-config startup-config</userinput>
```

マルチエリアの隣接関係の構成

既存の OSPFv3 インターフェイスには複数のエリアを追加できます。追加の論理インターフェイスはマルチエリア隣接関係をサポートしています。

始める前に

- OSPF 機能がイネーブルにされる必要があります（「OSPFv3 のイネーブル化 」の項を参照）。
- インターフェイスにプライマリ エリアが設定されていることを確認します（「OSPFv3 のネットワークの設定」の項を参照）。

手順

ステップ 1　configure terminal

例：

```
switch# configure terminal
switch(config)#
```

グローバル コンフィギュレーション モードを開始します。

ステップ 2 **interface** *interface-type slot/port*

例：

```
switch(config)# interface ethernet 1/2
  switch(config-if)#
```

インターフェイス設定モードを開始します。

ステップ 3 **ipv6 router ospfv3** *instance-tag* **multi-area** *area-id*

例：

```
switch(config-if)# ipv6 router ospfv3
  201 multi-area 3
```

別のエリアにインターフェイスを追加します。

ステップ 4 （任意） **show ipv6 ospfv3** *instance-tag* **interface** *interface-type slot/port*

例：

```
switch(config-if)# show ipv6 ospfv3 201
  interface ethernet 1/2
```

OSPFv3 情報を表示します。

ステップ 5 （任意） **copy running-config startup-config**

例：

```
switch(config)# copy running-config startup-config
```

実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします

例

次に、OSPFv3 インターフェイスに別のエリアを追加する例を示します。

```
switch# <userinput>configure terminal</userinput>
 switch(config)# <userinput>interface ethernet 1/2</userinput>
 switch(config-if)# <userinput>ipv6 address 2001:0DB8::1/48</userinput>
 switch(config-if)# <userinput>ipv6 ospfv3 201 area 0.0.0.10</userinput>
 switch(config-if)# <userinput>ipv6 ospfv3 201 multi-area 20</userinput>
 switch(config-if)# <userinput>copy running-config startup-config</userinput>
```

仮想リンクの設定

仮想リンクは、隔離されたエリアを中継エリアを介してバックボーン エリアに接続します。[仮想リンク]セクションを展開します。仮想リンクには、省略可能な次のパラメータを設定できます。

- Dead interval：ローカル ルータがデッドであることを宣言し、隣接関係を解消する前に、ネイバーが hello パケットを待つ時間を設定します。
- Hello interval：連続する hello パケット間の時間間隔を設定します。
- Retransmit interval：連続する LSA 間の推定時間間隔を設定します。
- Transmit delay：LSA をネイバーに送信する推定時間を設定します。

（注） リンクがアクティブになる前に、関与する両方のルータで仮想リンクを設定する必要があります。

始める前に

OSPF を有効にする必要があります（「OSPFv3 の有効化」のセクションを参照）。

手順

ステップ 1 **router ospfv3** *instance-tag*

例：

```
switch(config)# router ospfv3 201
  switch(config-router)#
```

新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

ステップ 2 **area** *area-id* **virtual-link** *router-id*

例：

```
switch(config-router)# area 0.0.0.10
  virtual-link 2001:0DB8::1
  switch(config-router-vlink)#
```

リモート ルータへの仮想リンクの端を作成します。仮想リンクをリモート ルータ上に作成して、リンクを完成させる必要があります。

ステップ 3 （任意） **show ipv6 ospfv3 virtual-link** [**brief**]

例：

```
switch(config-router-vlink)# show ipv6 ospfv3
  virtual-link
```

OSPFv3 仮想リンク情報を表示します。

ステップ 4 （任意） **dead-interval** *seconds*

例：

```
switch(config-router-vlink)#
  dead-interval 50
```

OSPFv3 デッド間隔を秒単位で設定します。有効な範囲は 1 ～ 65535 です。デフォルトでは、hello 間隔の秒数の 4 倍です。

ステップ 5 （任意） **hello-interval** *seconds*

例：

```
switch(config-router-vlink)#
  hello-interval 25
```

OSPFv3 hello 間隔を秒単位で設定します。有効な範囲は 1 ～ 65535 です。デフォルトは 10 秒です。

ステップ 6 （任意） **retransmit-interval** *seconds*

例：

```
switch(config-router-vlink)#
  retransmit-interval 50
```

OSPFv3 再送信間隔を秒単位で設定します。有効な範囲は 1 ～ 65535 です。デフォルトは 5 分です。

ステップ 7 （任意） **transmit-delay** *seconds*

例：

```
switch(config-router-vlink)#
  transmit-delay 2
```

OSPFv3 送信遅延を秒単位で設定します。指定できる範囲は 1 ～ 450 です。デフォルトは 1 です。

ステップ 8 （任意） **copy running-config startup-config**

例：

```
switch(config-router-vlink)#
  copy running-config startup-config
```

この設定変更を保存します。

例

次に、2 つの ABR 間に簡単な仮想リンクを作成する例を示します。

ABR 1（ルータ ID 2001:0DB8::1）の設定は、次のとおりです。

```
switch# <userinput>configure terminal</userinput>
 switch(config)# <userinput>router ospfv3 201</userinput>
 switch(config-router)# <userinput>area 0.0.0.10 virtual-link 2001:0DB8::10</userinput>
 switch(config-router-vlink)# <userinput>copy running-config startup-config</userinput>
```

ABR 2（ルータ ID 2001:0DB8::10）の設定は、次のとおりです。

```
switch# <userinput>configure terminal</userinput>
 switch(config)# <userinput>router ospfv3 201</userinput>
 switch(config-router)# <userinput>area 0.0.0.10 virtual-link 2001:0DB8::1</userinput>
 switch(config-router-vlink)# <userinput>copy running-config startup-config</userinput>
```

再配布の構成

他のルーティング プロトコルから学習したルートを、ASBR 経由で OSPFv3 自律システムに再配布できます。

OSPF でのルート再配布には、省略可能な次のパラメータを設定できます。

- Default information originate：外部自律システムへのデフォルト ルートの AS 外部（タイプ 5）LSA を生成します。

（注） Default information originate はオプションのルート マップ内の **match** 文を無視します。

- Default metric：すべての再配布ルートに同じコスト メトリックを設定します。

（注） スタティック ルートを再配布する場合、デフォルトの 7.0(3)I7(6) スタティック ルートを正常に再配布するためには、Cisco NX-OS は **default-information originate** コマンドを必要とします。

始める前に

OSPF 機能が有効にされている必要があります（「OSPFv3 の有効化」の項を参照）。

- 再配布で使用する、必要なルート マップを作成します。

手順

ステップ 1 **configure terminal**

例：

```
switch# configure terminal
switch(config)#
```

グローバル コンフィギュレーション モードを開始します。

ステップ 2 **router ospfv3***instance-tag*

例：

```
switch(config)# router ospfv3 201
  switch(config-router)#
```

新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

ステップ 3 **address-family ipv6 unicast**

例：

```
switch(config-router)# address-family
  ipv6 unicast
  switch(config-router-af)#
```

IPv6 ユニキャスト アドレス ファミリ モードを開始します。

ステップ 4 **redistribute** {**bgp***id* | **direct** | **isis** *id* | **rip** *id* | **static** | **dhcpv6**} **route-map** *map-name*

例：

```
switch(config-router-af)# redistribute
  bgp route-map FilterExternalBGP
```

設定したルート マップ経由で、選択したプロトコルを OSPFv3 に再配布します。

（注）
スタティック ルートを再配布する場合、デフォルトの 7.0(3)I7(6) スタティック ルートを正常に再配布するためには、Cisco NX-OS は **default-information originate** コマンドを必要とします。

ステップ 5 **default-information originate** [**always**] [**route-map** *map-name*]

例：

```
switch(config-router-af)#
  default-information-originate route-map DefaultRouteFilter
```

デフォルトのルートが RIB に存在する場合、この OSPFv3 ドメインにデフォルトのルートを作成します。次の省略可能なキーワードを使用します。

- **always**：ルートが RIB に存在しない場合でも、常にデフォルト ルート 0.0.0. を生成します。
- **route-map**：ルート マップが true を返す場合にデフォルト ルートを生成します。

（注）
このコマンドは、ルート マップの **match** 文を無視します。

ステップ 6 **default-metric** *cost*

例：

```
switch(config-router-af)# default-metric
  25
```

再配布されたルートのコスト メトリックを設定します。指定できる範囲は 1 ～ 16777214 です。このコマンドは、直接接続されたルートには適用されません。ルート マップを使用して、直接接続されたルートのデフォルトのメトリックを設定します。

ステップ 7 （任意） **copy running-config startup-config**

例：

```
switch(config-router-af)# copy running-config
  startup-config
```

この設定変更を保存します。

例

次に、ボーダー ゲートウェイ プロトコル（BGP）を OSPFv3 に再配布する例を示します。

```
switch# <userinput>configure terminal</userinput>
 switch(config)# <userinput>router ospfv3 201</userinput>
 switch(config-router)# <userinput>address-family ipv6 unicast</userinput>
 switch(config-router-af)# <userinput>redistribute bgp route-map
FilterExternalBGP</userinput>
 switch(config-router-af)# <userinput>copy running-config startup-config</userinput>
```

再配布されるルート数の制限

ルート再配布によって、OSPFv3 ルート テーブルに多数のルートを追加できます。外部プロトコルから受け取るルートの数の上限を設定できます。OSPFv3 には、再配布されるルート制限を設定するための次のオプションがあります。

- 上限固定：設定された最大値に OSPFv3 が達すると、メッセージをログに記録します。OSPFv3 はそれ以上の再配布されたルートを受け付けません。任意で、最大値のしきい値パーセンテージを設定して、OSPFv3 がこのしきい値を超えたときに警告を記録するようにすることもできます。
- 警告のみ：OSPFv3 が最大値に達したときのみ、警告のログを記録します。OSPFv3 は、再配布されたルートを受け入れ続けます。
- 取り消し：OSPFv3 が最大値に達したときに設定したタイムアウト期間を開始します。このタイムアウト期間後、現在の再配布されたルート数が最大制限より少なければ、OSPFv3 はすべての再配布されたルートを要求します。再配布されたルートの現在数が最大数に達した場合、OSPFv3 はすべての再配布されたルートを取り消します。OSPFv3 が追加の再配布されたルートを受け付ける前に、この状況を解消する必要があります。任意で、タイムアウト期間を設定できます。

始める前に

OSPF 機能が有効にされている必要があります（「OSPFv3 の有効化 」の項を参照）。

手順

ステップ 1 **configure terminal**

例：

```
switch# configure terminal
switch(config)#
```

グローバル コンフィギュレーション モードを開始します。

ステップ 2 **router ospfv3** *instance-tag*

例：

```
switch(config)# router ospfv3 201
  switch(config-router)#
```

新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

ステップ 3 **address-family ipv6 unicast**

例：

```
switch(config-router)# address-family
  ipv6 unicast
  switch(config-router-af)#
```

IPv6 ユニキャスト アドレス ファミリ モードを開始します。

ステップ 4 **redistribute** {**bgp***id* **| direct | isis** *id* **| rip** *id* **| static**} **route-map** *map-name*

例：

```
switch(config-router-af)# redistribute
  bgp route-map FilterExternalBGP
```

設定したルート マップ経由で、選択したプロトコルを OSPFv3 に再配布します。

ステップ 5 **redistribute maximum-prefix***max* [*threshold*] [**warning-only** | **withdraw** [*num-retries timemout*]]

例：

```
switch(config-router-af)# redistribute
  maximum-prefix 1000 75 warning-only
```

OSPFv2 が配布するプレフィックスの最大数を指定します。指定できる範囲は 0 ～ 65536 です。任意で次のオプションを指定します。

- *threshold*：警告メッセージをトリガーする最大プレフィックスの割合。
- **warning-only**：プレフィックスの最大数を超えた場合に警告メッセージを記録します。
- **withdraw**：再配布されたすべてのルートを取り消し、任意で再配布されたルートを取得しようと試みます。*num-retries* の範囲は 1 ～ 12 です。*timeout* の範囲は 60 ～ 600 秒です。デフォルトは 300 秒です。

ステップ 6 （任意） **show running-config ospfv3**

例：

```
switch(config-router-af)# show
 running-config ospf
```

OSPFv3 設定を表示します。

ステップ 7 （任意） **copy running-config startup-config**

例：

```
switch(config)# copy running-config startup-config
```

実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします

例

次に、OSPF に再配布されるルートの数を制限する例を示します。

```
switch# <userinput>configure terminal</userinput>
 switch(config)# <userinput>router ospfv3 201</userinput>
 switch(config-router)# <userinput>address-family ipv6 unicast</userinput>
 switch(config-router-af)# <userinput>redistribute bgp route-map
FilterExternalBGP</userinput>
 switch(config-router-af)# <userinput>redistribute maximum-prefix 1000 75</userinput>
```

ルート集約の設定

集約したアドレス範囲を設定することにより、エリア間ネットワークのルート集約を設定できます。また、ASBR 上のこれらのルートのサマリ アドレスを設定して、外部の再配布されたルートのルート集約を設定することもできます。詳細については、「ルート集約」を参照してください。

始める前に

OSPF 機能が有効にされている必要があります（「OSPFv3 の有効化 」の項を参照）。

手順

ステップ 1 **configure terminal**

例：

```
switch# configure terminal
switch(config)#
```

グローバル コンフィギュレーション モードを開始します。

ステップ 2 **router ospfv3***instance-tag*

例：

```
switch(config)# router ospfv3 201
switch(config-router)#
```

新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

ステップ 3 **address-family ipv6 unicast**

例：

```
switch(config-router)# address-family
ipv6 unicast
switch(config-router-af)#
```

IPv6 ユニキャスト アドレス ファミリ モードを開始します。

ステップ 4 **area** *area-id* **range** *ipv6-prefix/length* [**no-advertise**] [**cost** *cost*]

例：

```
switch(config-router-af)# area 0.0.0.10
range 2001:0DB8::/48 advertise
```

一定の範囲のアドレスのサマリ アドレスを ABR 上に作成します。このサマリ アドレスをエリア間プレフィックス（タイプ 3）LSA にアドバタイズすることもできます。cost の範囲は 0 ～ 16777215 です。

ステップ 5 **summary-address** *ipv6-prefix/length* [**no-advertise**] [**tag** *tag*]

例：

```
switch(config-router-af)#
summary-address 2001:0DB8::/48 tag 2
```

一定の範囲のアドレスの集約アドレスを ASBR 上に作成します。ルート マップによる再配布で使用できるよう、この集約アドレスにタグを割り当てることもできます。

ステップ 6 （任意） **show ipv6 ospfv3 summary-address**

例：

```
switch(config-router-af)# show ipv6 ospfv3
summary-address
```

OSPFv3 サマリ アドレスに関する情報を表示します。

ステップ 7 （任意） **copy running-config startup-config**

例：

```
switch(config)# copy running-config startup-config
```

実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします

例

次に、ABR 上のエリア間のサマリ アドレスを作成する例を示します。

```
switch# <userinput>configure terminal</userinput>
switch(config)# <userinput>router ospfv3 201</userinput>
switch(config-router)# <userinput>address-family ipv6 unicast</userinput>
switch(config-router-af)# <userinput>area 0.0.0.10 range 2001:0DB8::/48</userinput>
switch(config-router-af)# <userinput>copy running-config startup-config</userinput>
```

次に、ASBR 上のサマリ アドレスを作成する例を示します。

```
switch# <userinput>configure terminal</userinput>
switch(config)# <userinput>router ospfv3 201</userinput>
switch(config-router)# <userinput>address-family ipv6 unicast</userinput>
switch(config-router-af)# <userinput>summary-address 2001:0DB8::/48</userinput>
switch(config-router-af)# <userinput>no discard route internal</userinput>
switch(config-router-af)# <userinput>copy running-config startup-config</userinput>
```

ルートのアドミニストレーティブ ディスタンスの設定

OSPFv3 によって RIB に追加されるルートのアドミニストレーティブ ディスタンスを設定できます。

アドミニストレーティブディスタンスは、ルーティング情報源の信頼性を示す評価基準です。値が高いほど信頼性の評価は低くなります。一般的にルートは、複数のルーティングプロトコルを通じて検出されます。アドミニストレーティブ ディスタンスは、複数のルーティング プロトコルから学習したルートを区別するために使用されます。最もアドミニストレーティブディスタンスが低いルートが IP ルーティング テーブルに組み込まれます。

始める前に

OSPF が有効になっていることを確認します（OSPFv3 （1 ページ） セクションを参照）。

- 「OSPFv3 の注意事項および制約事項 （16 ページ）」のセクションにあるこの機能のガイドラインと制限事項を参照してください。

手順

ステップ 1 **configure terminal**

例：

```
switch# configure terminal
switch(config)#
```

グローバル コンフィギュレーション モードを開始します。

ステップ 2 **router ospfv3** *instance-tag*

例：

```
switch(config)# router ospfv3 201
switch(config-router)#
```

新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

ステップ 3 **address-family ipv6 unicast**

例：

```
switch(config-router)# address-family
ipv6 unicast
switch(config-router-af)#
```

IPv6 ユニキャスト アドレス ファミリ モードを開始します。

ステップ 4 [**no**] **table-map** *map-name*

例：

```
switch(config-router-af)# table-map foo
```

OSPFv3 ルートを RIB に送信する前に、OSPFv3 ルートをフィルタリングまたは変更するポリシーを設定します。マップ名には最大 63 文字の英数字を入力できます。

ステップ 5 **exit**

例：

```
switch(config-router-af)# exit
switch(config-router)#
```

ルータ 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 6 **exit**

例：

```
switch(config-router)# exit
switch(config)#
```

ルータ コンフィギュレーション モードを終了します。

ステップ 7 **route-map** *map-name* [**permit** | **deny**] [*seq*]

例：

```
switch(config)# route-map foo permit 10
switch(config-route-map)#
```

ルートマップを作成するか、または既存のルートマップに対応するルートマップ設定モードを開始します。ルート マップのエントリを順序付けるには、*seq* を使用します。

（注）
permit オプションで、ディスタンスを設定することができます。**deny** オプションを使用すると、デフォルトのディスタンスが適用されます。

ステップ 8 **match route-type** *route-type*

例：

```
switch(config-route-map)# match
route-type external
```

次のルート タイプのいずれかと照合します。

- external：外部ルート（BGP、EIGRP、OSPF タイプ 1 または 2）
- エリア間：OSPF エリア間ルート
- internal：内部ルート（OSPF エリア内またはエリア間ルートを含む）
- エリア内：OSPF のエリア内ルート
- nssa-external：NSSA 外部ルート（OSPF タイプ 1 または 2）
- type-1：OSPF 外部タイプ 1 ルート
- type-2：OSPF 外部タイプ 2 ルート

ステップ 9 **match ip route-source prefix-list** *name*

例：

```
switch(config-route-map)# match ip
route-source prefix-list p1
```

1 つまたは複数の IP プレフィックス リストに対して、ルートの IPv6 ルート送信元アドレスまたはルータ ID と照合します。プレフィックス リストは **ip prefix-list** コマンドを使用して作成します。

（注）
OSPFv3 では、ルータ ID は 4 バイトです。

ステップ 10 **match ipv6 address prefix-list** *name*

例：

```
switch(config-route-map)# match ipv6
address prefix-list p1
```

1 つまたは複数の IPv6 プレフィックス リストと照合。プレフィックス リストは **ip prefix-list** コマンドを使用して作成します。

ステップ 11 **set distance** *value*

例：

```
switch(config-route-map)# set distance
150
```

OSPFv3 のルートのアドミニストレーティブ ディスタンスを設定します。範囲は 1 ～ 255 です。

ステップ 12 （任意） **copy running-config startup-config**

例：

```
switch(config-route-map)# copy
running-config startup-config
```

この設定変更を保存します。

例

次に、OSPFv3 アドミニストレーティブ ディスタンスについて、エリア間ルートを 150、外部ルートを 200、およびプレフィックス リスト p1 内のすべてのプレフィックスを 190 に設定する例を示します。

```
switch# <userinput>configure terminal</userinput>
switch(config)# <userinput>router ospfv3 201</userinput>
switch(config-router)# <userinput>address-family ipv6 unicast</userinput>
switch(config-router-af)# <userinput>table-map foo</userinput>
switch(config-router)# <userinput>exit</userinput>
switch(config)# <userinput>exit</userinput>
switch(config)# <userinput>route-map foo permit 10</userinput>
switch(config-route-map)# <userinput>match route-type inter-area</userinput>
switch(config-route-map)# <userinput>set distance 150</userinput>
switch(config)# <userinput>route-map foo permit 20</userinput>
switch(config-route-map)# <userinput>match route-type external</userinput>
switch(config-route-map)# <userinput>set distance 200</userinput>
switch(config)# <userinput>route-map foo permit 30</userinput>
switch(config-route-map)# <userinput>match ip route-source prefix-list p1</userinput>
switch(config-route-map)# <userinput>match ipv6 address prefix-list p1</userinput>
switch(config-route-map)# <userinput>set distance 190</userinput>
switch(config-route-map)# <userinput>copy running-config startup-config</userinput>
```

デフォルト タイマーの変更

OSPFv3 には、プロトコル メッセージの動作および最短パス優先（SPF）の計算を制御する多数のタイマーが含まれています。OSPFv3 には、省略可能な次のタイマー パラメータが含まれます。

- LSA arrival time：ネイバーから着信する LSA 間で許容される最小間隔を設定します。この時間より短時間で到着する LSA はドロップされます。
- Pacing LSAs：LSA が集められてグループ化され、リフレッシュされて、チェックサムが計算される間隔、つまり期限切れとなる間隔を設定します。このタイマーは、LSA 更新が実行される頻度を制御し、LSA 更新メッセージで送信される LSA 更新の数を制御します（「フラッディングと LSA グループ ペーシング」を参照）。
- Throttle LSAs：LSA 生成のレート制限を設定します。このタイマーは、トポロジが変更された後に LSA が生成される頻度を制御します。
- Throttle SPF calculation：SPF 計算の実行頻度を制御します。

インターフェイス レベルでは、次のタイマーも制御できます。

- Retransmit interval：連続する LSA 間の推定時間間隔を設定します。
- Transmit delay：LSA をネイバーに送信する推定時間を設定します。

hello 間隔とデッド タイマーに関する情報の詳細については、「OSPFv3 のネットワークの設定」の項を参照してください。

手順

ステップ 1 **configure terminal**

例：

```
switch# configure terminal
switch(config)#
```

グローバル コンフィギュレーション モードを開始します。

ステップ 2 **router ospfv3***instance-tag*

例：

```
switch(config)# router ospfv3 201
 switch(config-router)#
```

新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

ステップ 3 **timers lsa-arrival***msec*

例：

```
switch(config-router)# timers
 lsa-arrival 2000
```

LSA 到着時間をミリ秒で設定します。範囲は 10 ～ 600000 です。デフォルトは 1000 ミリ秒です。

ステップ 4 **timers lsa-group-pacing***seconds*

例：

```
switch(config-router)# timers
 lsa-group-pacing 200
```

LSA がグループ化される間隔を秒で設定します。範囲は 1 ～ 1800 です。デフォルトは 10 秒です。

ステップ 5 **timers throttle lsa***start-time hold-interval max-time*

例：

```
switch(config-router)# timers
 throttle lsa network 350 5000 6000
```

LSA 生成のレート制限をミリ秒で設定します。次のタイマーを設定できます。

- *start-time*：指定できる範囲は 0 ～ 5000 ミリ秒です。デフォルト値は 0 ミリ秒です。
- *hold-interval*：指定できる範囲は 50 ～ 30,000 ミリ秒です。デフォルト値は 5000 ミリ秒です。
- *max-time*：指定できる範囲は 50 ～ 30,000 ミリ秒です。デフォルト値は 5000 ミリ秒です。

ステップ 6 **address-family ipv6 unicast**

例：

```
switch(config-router)# address-family
 ipv6 unicast
 switch(config-router-af)#
```

IPv6 ユニキャスト アドレス ファミリ モードを開始します。

ステップ 7 **timers throttle spf***delay-time hold-time max-time*

例：

```
switch(config-router-af)# timers throttle
 spf 3000 2000
```

SPF 最適パス スケジュールを次のタイマを使用して、SPF 最適パス計算間（秒単位）で設定します。

- *delay-time*：範囲は 1 ～ 600000 ミリ秒です。デフォルトは 200 ミリ秒です。
- *hold-time*：範囲は 1 ～ 600000 ミリ秒です。デフォルト値は、1000 ミリ秒です。
- *max-wait* ：範囲は 1 ～ 600000 ミリ秒です。デフォルト値は 5000 ミリ秒です。

ステップ 8 **interface***type slot/port*

例：

```
switch(config)# interface ethernet 1/2
 switch(config-if)#
```

インターフェイス設定モードを開始します。

ステップ 9 **ospfv3 retransmit-interval***seconds*

例：

```
switch(config-if)# ospfv3
 retransmit-interval 30
```

このインターフェイスから送信される各 LSA 間の推定時間間隔を設定します。有効な範囲は 1 ～ 65535 です。デフォルトは 5 分です。

ステップ 10 **ospfv3 transmit-delay***seconds*

例：

```
switch(config-if)# ospfv3
 transmit-delay 600
```

LSA をネイバーに送信する推定時間間隔を秒で設定します。指定できる範囲は 1 ～ 450 です。デフォルトは 1 です。

ステップ 11 （任意） **copy running-config startup-config**

例：

```
switch(config)# copy running-config startup-config
```

実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします

例

次に、lsa-group-pacing オプションで LSA フラッディングを制御する例を示します。

```
switch# <userinput>configure terminal</userinput>
switch(config)# <userinput>router ospfv3 201</userinput>
switch(config-router)# <userinput>timers lsa-group-pacing 300</userinput>
switch(config-router)# <userinput>copy running-config startup-config</userinput>
```

グレースフル リスタートの設定

デフォルトでは、グレースフル リスタートは有効です。OSPFv3 インスタンスのグレースフル リスタートには、省略可能な次のパラメータを設定できます。

- Grace period：グレースフル リスタートの開始後に、ネイバーが隣接関係を解消するまでに待つ時間を設定します。
- Helper mode disabled：ローカル OSPFv3 インスタンスのヘルパー モードをディセーブルにします。OSPFv3 は、ネイバーのグレースフル リスタートには関与しません。
- Planned graceful restart only：予定された再起動の場合にのみグレースフル リスタートがサポートされるよう、OSPFv3 を設定します。

始める前に

OSPFv3 機能が有効にされている必要があります（「OSPFv2 の有効化 」の項を参照）。

- すべてのネイバーで、一致した省略可能なパラメーター式とともにグレースフル リスタートが設定されていることを確認します。

手順

ステップ 1 **configure terminal**

例：

```
switch# configure terminal
switch(config)#
```

グローバル コンフィギュレーション モードを開始します。

ステップ 2 **router ospfv3***instance-tag*

例：

```
switch(config)# router ospfv3 201
switch(config-router)#
```

新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

ステップ 3 **graceful-restart**

例：

```
switch(config-router)# graceful-restart
```

グレースフル リスタートを有効にします。グレースフル リスタートは、デフォルトで有効にされています。

ステップ 4 **graceful-restart grace-period***seconds*

例：

```
switch(config-router)# graceful-restart
grace-period 120
```

猶予期間を秒で設定します。範囲は 5 ～ 1800 秒です。デフォルトは 60 秒です。

ステップ 5 **graceful-restart helper-disable**

例：

```
switch(config-router)# graceful-restart
helper-disable
```

ヘルパー モードを無効にします。デフォルトでは、イネーブルです。

ステップ 6 **graceful-restart planned-only**

例：

```
switch(config-router)# graceful-restart
planned-only
```

予定された再起動時にのみグレースフル リスタートを設定します。

ステップ 7 （任意） **show ipv6 ospfv3***instance-tag*

例：

```
switch(config-router)# show ipv6 ospfv3
201
```

OPSFv3 情報を表示します。

ステップ 8 （任意） **copy running-config startup-config**

例：

```
switch(config)# copy running-config startup-config
```

実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします

例

次に、ディセーブルにされているグレースフル リスタートをイネーブルにし、猶予期間を 120 秒に設定する例を示します。

```
switch# <userinput>configure terminal</userinput>
switch(config)# <userinput>router ospfv3 201</userinput>
switch(config-router)# <userinput>graceful restart</userinput>
switch(config-router)# <userinput>graceful-restart grace-period 120</userinput>
switch(config-router)# <userinput>copy running-config startup-config</userinput>
```

OSPFv3 インスタンスの再起動

OSPv3インスタンスを再起動できます。この処理では、インスタンスのすべてのネイバーが消去されます。

OSPFv3 インスタンスを再起動して、関連付けられたすべてのネイバーを削除するには、次のコマンドを使用します。

手順

restart ospfv3 *instance-tag*

例：

```
switch(config)# restart ospfv3 201
```

OSPFv3 インスタンスを再起動して、すべてのネイバーを削除します。

仮想化による OSPFv3 の設定

複数 OSPFv3 インスタンスを設定できます。各仮想デバイス コンテキスト（VDC）内に複数の VRF を作成して、各 VRF で同じまたは複数の OSPFv3 インスタンスを使用することもできます。VRF には OSPFv3 インターフェイスを割り当てます。

（注） インターフェイスの VRF を設定した後に、インターフェイスの他のすべてのパラメータを設定します。インターフェイスの VRF を設定すると、そのインターフェイスのすべての設定が削除されます。

始める前に

OSPFv3 機能が有効にされている必要があります（「OSPFv3 の有効化」の項を参照）。

手順

ステップ 1 **configure terminal**

例：

```
switch# configure terminal
switch(config)#
```

グローバル コンフィギュレーション モードを開始します。

ステップ 2 **vrf context***vrf-name*

例：

```
switch(config)# vrf context
RemoteOfficeVRF
switch(config-vrf)#
```

新しい VRF を作成し、VRF 設定モードを開始します。

ステップ 3 **router ospfv3***instance-tag*

例：

```
switch(config)# router ospfv3 201
switch(config-router)#
```

新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

ステップ 4 **vrf***vrf-name*

例：

```
switch(config-router)# vrf
RemoteOfficeVRF
switch(config-router-vrf)#
```

ルータ VRF 設定モードを開始します。

ステップ 5 （任意） **maximum-paths***paths*

例：

```
switch(config-router-vrf)# maximum-paths
4
```

この VRF のルート テーブル内の宛先への、同じ OSPFv3 パスの最大数を設定します。このコマンドはロード バランシングに使用します。

ステップ 6 **interface***type slot/port*

例：

```
switch(config)# interface ethernet 1/2
switch(config-if)#
```

インターフェイス設定モードを開始します。

ステップ 7 **vrf member***vrf-name*

例：

```
switch(config-if)# vrf member
RemoteOfficeVRF
```

このインターフェイスを VRF に追加します。

ステップ 8 **ipv6 address***ipv6-prefix/length*

例：

```
switch(config-if)# ipv6 address
2001:0DB8::1/48
```

このインターフェイスの IP アドレスを設定します。このステップは、このインターフェイスを VRF に割り当てたあとに行う必要があります。

ステップ 9 **ipv6 ospfv3***instance-tag***area***area-id*

例：

```
switch(config-if)# ipv6 ospfv3 201
area 0
```

設定した OSPFv3 インスタンスおよびエリアに、このインターフェイスを割り当てます。

ステップ 10 （任意） **copy running-config startup-config**

例：

```
switch(config)# copy running-config startup-config
```

実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします

例

次に、VRF を作成して、その VRF にインターフェイスを追加する例を示します。

```
switch# <userinput>configure terminal</userinput>
switch(config)# <userinput>vrf context NewVRF</userinput>
switch(config-vrf)# <userinput>exit</userinput>
switch(config)# <userinput>router ospfv3 201</userinput>
switch(config-router)# <userinput>exit</userinput>
switch(config)# <userinput>interface ethernet 1/2</userinput>
switch(config-if)# <userinput>vrf member NewVRF</userinput>
switch(config-if)# <userinput>ipv6 address 2001:0DB8::1/48</userinput>
switch(config-if)# <userinput>ipv6 ospfv3 201 area 0</userinput>
switch(config-if)# <userinput>copy running-config startup-config</userinput>
```

暗号化および認証の構成

Cisco Nexus リリース 10.2（1）以降では、ESP カプセル化を使用して OSPFv3 メッセージを暗号化および認証できます。OSPFv3 は、セキュア接続を IPSec に依存しています。IPSec は、2 つのカプセル化タイプをサポートします：認証ヘッダー（AH）およびカプセル化セキュリティペイロード（ESP）です。RFC4552「Authentication/Confidentiality for OSPFv3」は、両方の側面をカバーしています。ESP設定は、OSPFv3 メッセージの暗号化と認証の両方を提供します。

Cisco Nexus リリース 10.4(1)F 以降では、キーチェーン オプションを使用して暗号化および認証アルゴリズムとキーを構成できます。

手順

ステップ 1 制限事項は次のとおりです。

- IPSec トランスポートモードのみがサポートされ、トンネルモードはサポートされません。
- AH と ESP の設定は、インターフェイス上では一緒に使用できません。ただし、2 つの異なるインターフェイスに AH と ESP を設定できます。
- RFC 4552 のセクション 10 で定義されている中断のないキー再生成はサポートされていません。
- 次の暗号化アルゴリズムが ESP でサポートされます。
  - AES-CBC（128 ビット）
  - AES 192 ビットと AES 256 ビットは、このリリースではサポートされません。
  - 3DES-CBC
  - NULL
- ESP では次の認証がサポートされます。
  - SHA-1
  - NULL
- 1 つの ESP CLI で暗号化アルゴリズムと認証アルゴリズムの両方を NULL に設定することはできません。

- 複数のエリアの一部であるインターフェイスは、親と同じ ESP パラメータを使用します。
- 設定中に SPI が競合すると、エラーがユーザにスローされ、設定は保存されません。そのため、ESP 構成を変更する場合は、ユーザーは新しい構成に異なる SPI を使用する必要があります。
- 最大 128 の SA/SPI 値を OSPFv3 プロセスごとに設定できます。

ステップ 2 次のレベルで ESP を設定できます。

- ルータ
- エリア
- インターフェイス
- 仮想リンク

ルータ レベルでの OSPFv3 暗号化の設定

次のコマンドを使用して、ルータ レベルで OSPFv3 パケットを暗号化および認証するように OSPFv3 ESP を設定できます。

始める前に

OSPFv3 機能を有効にします。

認証パッケージを有効にします。

手順

ステップ 1 グローバル設定モードを開始します。

switch# **configure terminal**

ステップ 2 OSPFv3を有効にします。

switch(config)# **feature ospfv3**

ステップ 3 認証パッケージを有効にします。

switch(config)# **feature imp**

ステップ 4 インスタンスタグが設定された新しい OSPFv3 インスタンスを作成します。

switch(config)# **router ospfv3** *instance-tag*

ステップ 5 IPSec ESP 暗号化を有効にします:

switch(config-router)# **encryption ipsec spi** *spi_id* **esp** [*encrypt_algorithm* [**0** | **3** | **7**] *key* | **key-chain** *enc_keychain_name* | **null**] **authentication** [*auth_algorithm* [**0** | **3** | **7**] *key* | **key-chain** *auth_keychain_name* | **null**]

spi_id を使用してセキュリティポリシーインデックスを指定し、*encrypt_algorithm* を使用して暗号化アルゴリズムを定義できます。3DES、AES 128、または null を指定できます。番号 0、3、および 7 は、*key* の形式を指定します。認証アルゴリズムは、*auth_algorithm* （SHA-1 または NULL）で定義できます。

key-chain オプションを使用して、キーとアルゴリズムも構成できます。

ステップ 6 （任意）OSPFv3 情報を表示します。

switch(config)# **show running-config ospfv3**

エリア レベルでの OSPFv3 暗号化の構成

次のコマンドを使用して、エリアレベルでOSPFv3パケットを暗号化および認証するようにOSPFv3 ESPを設定できます。

始める前に

OSPFv3 機能を有効にします。

認証パッケージを有効にします。

手順

ステップ 1 グローバル設定モードを開始します。

switch# **configure terminal**

ステップ 2 OSPFv3を有効にします。

switch(config)# **feature ospfv3**

ステップ 3 認証パッケージを有効にします。

switch(config)# **feature imp**

ステップ 4 インスタンスタグが設定された新しい OSPFv3 インスタンスを作成します。

switch(config)# **router ospfv3** *instance-tag*

ステップ 5 IPSec ESP 暗号化を有効にします:

switch(config-router)#**area** *area-num* **encryption ipsec spi** *spi_val* **esp** *encrypt_algorithm* [**0** | **3** | **7***key* | **key-chain** *enc_keychain_name* | **null**] **authentication** *auth_algorithm* [**0** | **3** | **7**] *key* | **key-chain** *auth_keychain_name* | **null**]

spi_id を使用してセキュリティポリシーインデックスを指定し、*encrypt_algorithm* を使用して暗号化アルゴリズムを定義できます。3DES、AES 128、または null を指定できます。番号 0、3、6 および 7 は、*key* の形式を指定します。認証アルゴリズムは、*auth_algorithm* （SHA-1 または NULL またはキーチェーン）で定義できます。

key-chain オプションを使用して、キーとアルゴリズムも構成できます。

ステップ 6 （任意）OSPFv3 情報を表示します。

switch(config)# **show running-config ospfv3**

インターフェイス レベルでの OSPFv3 暗号化の構成

次のコマンドを使用して、インターフェイス レベルでOSPFv3パケットを暗号化および認証するように OSPFv3 ESP を設定できます。

始める前に

OSPFv3 をイネーブルにする必要があります。

- 認証パッケージを有効にします。

手順

ステップ 1 グローバル設定モードを開始します。

switch# **configure terminal**

ステップ 2 OSPFv3を有効にします。

switch(config)# **feature ospfv3**

ステップ 3 認証モードをイネーブルにします。

switch(config)# **feature imp**

ステップ 4 イーサネット インターフェイス設定モードを開始します:

switch(config)# **interface ethernet** *interface*

ステップ 5 インターフェイスのOSPFv3インスタンスとエリアを指定します。

switch（config-if） **#** instance-tag area-id **ipv6 router ospfv3 area**

ステップ 6 IPSec ESP 暗号化を有効にします:

switch(config-if)# **ospfv3 encryption ipsec spi** *spi_id* **esp** *encrypt_algorithm* [**0** | **3** | **7**] *key* | **key-chain** *enc_keychain_name* | **null**] **authentication** *auth_algorithm* [**0** | **3** | **7**] *key* | **key-chain** *auth_keychain_name* | **null**]

spi_id を使用してセキュリティポリシーインデックスを指定し、*encrypt_algorithm* を使用して暗号化アルゴリズムを定義できます。3DES、AES 128、または null を指定できます。番号 0、3、および 7 は、*key* の形式を指定します。認証アルゴリズムは、*auth_algorithm* （SHA-1 または NULL）で定義できます。

key-chain オプションを使用して、キーとアルゴリズムを構成することもできます。

ステップ 7 （オプション）インターフェイスの実行設定を表示します:

switch(config-if)#**show run interface** *interface*

例

次に、イーサネットインターネット3/2のセキュリティを有効にする例を示します。

```
switch# configure terminal
switch(config)# feature ospfv3
switch(config)# feature imp
switch(config)# interface ethernet 3/2
switch(config-if)# ipv6 router ospfv3 1 area 0.0.0.0
switch(config-if)# ospfv3 encryption ipsec spi 444
esp  Specify encryption parameters
switch(config-if)# ospfv3 encryption ipsec spi 444 esp
3des  Use the triple DES algorithim
aes   Use the AES algorithim
<!--NXOS1-307-->key-chain  Encryption password key-chain
null  Use NULL authentication
switch(config-if)# ospfv3 encryption ipsec spi 444 esp aes
128  Use the 128-bit AES algorithim
switch(config-if)# ospfv3 encryption ipsec spi 444 esp aes 128
0     Specifies an UNENCRYPTED encryption key will follow
3     Specifies an 3DES ENCRYPTED encryption key will follow
7     Specifies a Cisco type 7  ENCRYPTED encryption key will follow
WORD  The UNENCRYPTED (cleartext) encryption key
switch(config-if)# ospfv3 encryption ipsec spi 444 esp aes 128
12345678123456781234567812345678 authentication null
switch(config-if)# sh ospfv3 interface
Ethernet3/2 is up, line protocol is up
IPv6 address 1:1:1:1::2/64
Process ID 1 VRF default, Instance ID 0, area 0.0.0.0
Enabled by interface configuration
State DOWN, Network type BROADCAST, cost 40
ESP Encryption AES, Authentication NULL, SPI 444, ConnId 444
switch(config-if)#
```

仮想リンクの OSPFv3 暗号化の設定

次のコマンドを使用して、仮想リンクの OSPFv3 パケットを暗号化および認証するように OSPFv3 ESP を設定できます。

始める前に

OSPFv3 機能を有効にします。

認証パッケージを有効にします。

手順

ステップ 1 グローバル設定モードを開始します。

switch# **configure terminal**

ステップ 2 OSPFv3を有効にします。

switch(config)# **feature ospfv3**

ステップ 3 認証パッケージを有効にします。

switch(config)# **feature imp**

ステップ 4 インスタンスタグが設定された新しい OSPFv3 インスタンスを作成します。

switch(config)#**router ospfv3** *instance-tag*

ステップ 5 リモートルータへの仮想リンクの端を作成します。仮想リンクをリモートルータ上に作成して、リンクを完成させる必要があります。

switch(config-router)# **area** *area-id* **virtual-link** *router-id*

ステップ 6 IPSec ESP 暗号化を有効にします:

switch(config-router-vlink)# **encryption ipsec spi** *spi_id* **esp** *encrypt_algorithm* [**0** | **3** | **7**] *key* | **key-chain** *enc_keychain_name* | **null**] **authentication** *auth_algorithm* [**0** | **3** | **7**] *key* | **key-chain** *auth_keychain_name* | **null**]

spi_id を使用してセキュリティポリシーインデックスを指定し、*encrypt_algorithm* を使用して暗号化アルゴリズムを定義できます。3DES、AES 128、または null を指定できます。番号 0、3、および 7 は、*key* の形式を指定します。認証アルゴリズムは、*auth_algorithm* （SHA-1 または NULL）で定義できます。

key-chain オプションを使用して、キーとアルゴリズムも構成できます。

ステップ 7 （任意）OSPFv3 情報を表示します。

switch(config)# **show running-config ospfv3**

設定例

次に、仮想リンクを暗号化する例を示します。

```
switch(config)# feature ospfv3
switch(config)# feature imp
switch(config-if)# router ospfv3 1
switch(config-router)# area 0.0.0.1 virtual-link 3.3.3.3
switch(config-router-vlink)# encryption ipsec spi ?
<256-4294967295> SPI Value
switch(config-router-vlink)# encryption ipsec spi 256 esp ?
3des Use the triple DES algorithim
aes Use the AES algorithim
key-chain  Encryption password key-chain
null Use NULL authentication
switch(config-router-vlink)# encryption ipsec spi 256 esp aes 128
123456789A123456789B123456789C12 authentication ?
null Use NULL authentication
sha1 Use the SHA1 algorithim
switch(config-router-vlink)# encryption ipsec spi 256 esp aes 128
123456789A123456789B123456789C12 authentication null
```

（注） 複数の OSPFv3 ネイバーに IPsec ESP を許可するには、次のポリシーマップをコントロール プレーンに適用する必要があります。

```
ipv6 access-list copp-acl-ipsec
10 permit ahp any any
20 permit esp any any

class-map type control-plane match-any copp-class-critical-customized-copp
match access-group name copp-acl-ipsec
policy-map type control-plane customized-copp
class copp-class-critical-customized-copp
police cir 36000 kbps bc 1280000 bytes conform transmit violate drop
control-plane
service-policy input customized-copp
```

ルータ レベルで OSPFv3 認証の構成

次のコマンドを使用して、ルータ レベルで OSPFv3 パケットを認証するように OSPFv3 ESP を構成できます。

始める前に

OSPFv3 が有効になっていることを確認してください。詳細は「OSPFv3 の有効化」を参照してください。

手順

ステップ 1 configure terminal

例：

```
switch# configure terminal
 switch(config)#
```

グローバル コンフィギュレーション モードを開始します。

ステップ 2 **feature ospfv3**

例：

```
switch(config)# feature ospfv3
```

OSPFv3 を有効にします。

ステップ 3 **feature imp**

例：

```
switch(config)# feature imp
```

認証モードを有効にします。

ステップ 4 **router ospfv3 instance-tag**

例：

```
switch(config)# router ospfv3 100
switch(config-router)#
```

新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

ステップ 5 [**no**] **authentication** {**ipsec spi** *spi_id* [*auth_algorithm* [**0** | **3** | **7**] *key* | **key-chain** *auth_keychain_name* | **null**]

例：

認証アルゴリズムおよびキー オプションの場合：

```
switch(config-router)# authentication ipsec spi 475 md5 11111111111111112222222222222222
```

キーチェーンの場合：

```
switch(config-router)# authentication ipsec spi 333 key-chain test1
```

プロセス（または VRF）レベルで OSPFv3 IPSec 認証を設定します。

spi 引数は、セキュリティ パラメータ インデックス（SPI）を指定します。指定できる範囲は 256 ～ 4294967295 です。

auth 引数は、認証のタイプを指定します。サポートされる値は md5 または sha1 です。

0 の場合は、パスワードをクリア テキストで設定します。3 の場合は、パス キーを 3DES 暗号化として設定します。7 パス キーを Cisco タイプ 7 暗号化として設定します。

cleartext オプション（0）を使用する場合、key 引数は md5 では 32 文字、sha1 では 40 文字にする必要があります。

Cisco NX-OS リリース 10.4(1)F 以降では、**key-chain** オプションはキーおよびアルゴリズムを構成するために提供されます。

このコマンドの **no** 形式を使用して、OSPFv3 IPSec 認証を無効にします。

ステップ 6 （任意） **show running-config ospfv3**

例：

```
switch(config)# show running-config ospfv3
```

OSPFv3 認証構成情報を表示します。

ステップ 7 （任意） **copy running-config startup-config**

例：

```
switch(config)# copy running-config
startup-config
```

この設定変更を保存します。

エリア レベルで OSPFv3 認証の構成

次のコマンドを使用して、エリア レベルで OSPFv3 パケットを認証するように OSPFv3 ESP を構成できます。

キーチェーンの構成方法に関する詳細は、『**Cisco Nexus 9000 シリーズ NX-OS セキュリティ構成ガイド**』の「キーチェーン管理の構成」を参照してください。

始める前に

OSPFv3 が有効になっていることを確認してください。詳細は「OSPFv3 を有効にする」を参照してください。

手順

ステップ 1 **configure terminal**

例：

```
switch# configure terminal
                        switch(config)#
```

グローバル コンフィギュレーション モードを開始します。

ステップ 2 **feature ospfv3**

例：

```
switch(config)# feature ospfv3
```

OSPFv3 を有効にします。

ステップ 3 **feature imp**

例：

```
switch(config)# feature imp
```

認証モードを有効にします。

ステップ 4 **router ospfv3 instance-tag**

例：

```
switch(config)# router ospfv3 100
                        switch(config-router)#
```

新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

ステップ 5 [**no**] **area** *area-id-ip* **authentication** {**ipsec spi** *spi_id*[*auth_algorithm* [**0** | **3** | **7**] *key* | **key-chain** *auth_keychain_name* | **null**]

例：

認証アルゴリズムおよびキー オプションの場合：

```
switch(config-router)# area 0 authentication ipsec spi 475 md5 11111111111111112222222222222222
```

キーチェーンの場合：

```
switch(config-router)# area 0 authentication ipsec spi 333 key-chain test1
```

エリア レベルで OSPFv3 IPSec 認証を設定します。

spi 引数は、セキュリティ パラメータ インデックス（SPI）を指定します。指定できる範囲は 256 ～ 4294967295 です。

auth 引数は、認証のタイプを指定します。サポートされる値は MD5 または SHA-1 です。

0 の場合は、パスワードをクリア テキストで設定します。3 の場合は、パス キーを 3DES 暗号化として設定します。7：Cisco タイプ 7 暗号化としてキーを構成します。

cleartext オプション（0）を使用する場合、key 引数は MD5 では 32 文字、SHA-1 では 40 文字にする必要があります。

Cisco NX-OS リリース 10.4(1)F 以降では、**key-chain** オプションはキーおよびアルゴリズムを構成するために提供されます。

このコマンドの **no** 形式を使用して、OSPFv3 IPSec 認証を無効にします。

ステップ 6 **show running-config ospfv3**

例：

```
switch(config)# show running-config ospfv3
```

OSPFv3 認証構成情報を表示します。

ステップ 7 **copy running-config startup-config**

例：

```
switch(config)# copy running-config startup-config
```

この設定変更を保存します。

インターフェイス レベルで OSPFv3 認証の構成

次のコマンドを使用して、間隔レベルで OSPFv3 パケットを認証するように OSPFv3 ESP を構成できます。

キーチェーンの構成方法に関する詳細は、『**Cisco Nexus 9000 シリーズ NX-OS セキュリティ構成ガイド**』の「キーチェーン管理の構成」を参照してください。

始める前に

OSPFv3 が有効になっていることを確認してください。詳細は「OSPFv3 を有効にする」を参照してください。

手順

ステップ 1 configure terminal

例：

```
switch# configure terminal
                        switch(config)#
```

グローバル設定モードを開始します

ステップ 2 **interface***interface-type slot/port*

例：

```
switch(config)# interface ethernet 1/1
                        switch(config-if)#
```

インターフェイス設定モードを開始します。

ステップ 3 [**no**] **ospfv3 authentication** {**disable** | **ipsec spi** *spi_id* {**md5** *akey* | **sha1** *akey* | **key-chain** *keychain_ah*}}

例：

認証アルゴリズムおよびキー オプションの場合：

```
switch(config-if)# ospfv3 authentication ipsec spi 475 md5 11111111111111112222222222222222
```

キーチェーンの場合：

```
switch(config-if)# ospfv3 authentication ipsec spi 333 key-chain test1
```

指定したインターフェイスの OSPFv3 IPSec 認証を設定します。

spi 引数は、セキュリティ パラメータ インデックス（SPI）を指定します。指定できる範囲は 256 ～ 4294967295 です。

auth 引数は、認証のタイプを指定します。サポートされる値は MD5 または SHA-1 です。

0 の場合は、パスワードをクリア テキストで設定します。3 の場合は、パス キーを 3DES 暗号化として設定します。7：Cisco タイプ 7 暗号化としてキーを構成します。

cleartext オプション（0）を使用する場合、key 引数は MD5 では 32 文字、SHA-1 では 40 文字にする必要があります。

Cisco NX-OS リリース 10.4(1)F 以降では、**key-chain** オプションはキーおよびアルゴリズムを構成するために提供されます。

このコマンドの **no** 形式を使用して、OSPFv3 IPSec 認証を無効にします。

ステップ 4 **show running-config ospfv3**

例：

```
switch(config)# show running-config ospfv3
```

OSPFv3 認証構成情報を表示します。

ステップ 5 **copy running-config startup-config**

例：

```
switch(config)# copy running-config startup-config
```

この設定変更を保存します。

仮想リンク レベルで OSPFv3 認証の構成

次のコマンドを使用して、仮想リンク レベルで OSPFv3 パケットを認証するように OSPFv3 ESP を構成できます。

キーチェーンの構成方法に関する詳細は、『**Cisco Nexus 9000 シリーズ NX-OS セキュリティ構成ガイド**』の「キーチェーン管理の構成」を参照してください。

始める前に

OSPFv3 が有効になっていることを確認してください。詳細は「OSPFv3 を有効にする」を参照してください。

手順

ステップ 1 configure terminal

例：

```
switch# configure terminal
switch(config)#
```

グローバル コンフィギュレーション モードを開始します。

ステップ 2 **feature ospfv3**

例：

```
switch(config)# feature ospfv3
```

OSPFv3 を有効にします。

ステップ 3 **feature imp**

例：

```
switch(config)# feature imp
```

認証モードを有効にします。

ステップ 4 **router ospfv3 instance-tag**

例：

```
switch(config)# router ospfv3 100
                        switch(config-router)#
```

新規 OSPFv3 インスタンスを作成して、設定済みのインスタンス タグを割り当てます。

ステップ 5 **area** *area-id* **virtual-link** *router-id*

例：

```
switch(config-router)# area 0.0.0.10 virtual-link 2001:0DB8::1
                        switch(config-router-vlink)#
```

リモート ルータへの仮想リンクの端を作成します。仮想リンクをリモート ルータ上に作成して、リンクを完成させる必要があります。

ステップ 6 [**no**] **authentication** {**ipsec spi** *spi_id* [*auth_algorithm* [**0** | **3** | **7**] *key* | **key-chain** *auth_keychain_name* | **null**]

例：

認証アルゴリズムおよびキー オプションの場合：

```
switch(config-router-vlink)# authentication ipsec spi 475 md5 11111111111111112222222222222222
```

キーチェーンの場合：

```
switch(config-router-vlink)# authentication ipsec spi 333 key-chain test1
```

仮想リンク レベルで OSPFv3 IPSec 認証を構成します。

spi 引数は、セキュリティ パラメータ インデックス（SPI）を指定します。指定できる範囲は 256 ～ 4294967295 です。

auth 引数は、認証のタイプを指定します。サポートされる値は MD5 または SHA-1 です。

0 の場合は、パスワードをクリア テキストで設定します。3 の場合は、パス キーを 3DES 暗号化として設定します。7：Cisco タイプ 7 暗号化としてキーを構成します。

cleartext オプション（0）を使用する場合、key 引数は MD5 では 32 文字、SHA-1 では 40 文字にする必要があります。

Cisco NX-OS リリース 10.4(1)F 以降では、**key-chain** オプションはキーおよびアルゴリズムを構成するために提供されます。

このコマンドの **no** 形式を使用して、OSPFv3 IPSec 認証を無効にします。

ステップ 7 （任意） **show running-config ospfv3**

例：

```
switch(config)# show running-config ospfv3
```

OSPFv3 認証構成情報を表示します。

ステップ 8 （任意） **copy running-config startup-config**

例：

```
switch(config)# copy running-config startup-config
```

この設定変更を保存します。

OSPFv3 設定の確認

OSPFv3 の設定を表示するには、次のいずれかのタスクを実行します。

コマンド	目的
show ipv6 ospfv3 [instance-tag] [vrf vrf-name]	1 つまたは複数の OSPFv3 ルーティング インスタンスに関する情報が表示されます。出力には、次のエリア レベルのカウントが含まれます。 • このエリアのインターフェイス：このエリアに追加されたすべてのインターフェイスの数（設定されたインターフェイス）。 • アクティブ インターフェイス：ルータリンクステートおよび SPF（UP インターフェイス）にあると見なされるすべてのインターフェイスの数。 • パッシブ インターフェイス：OSPF パッシブと見なされるすべてのインターフェイスの数（隣接関係は形成されません）。 • ループバックインターフェイス：すべてのローカルループバックインターフェイスの数。
show ipv6 ospfv3 border-routers	ABR および ASBR への内部 OSPF ルーティング テーブル エントリを表示します。
show ipv6 ospfv3 database	特定のルータの OSPFv3 データベースに関する情報のリストを表示します。
show ipv6 ospfv3 interface *type number* [**vrf** {*vrf-name* | **all** | **default** | **management**}]	OSPFv3 インターフェイス情報を表示します。
show ipv6 ospfv3 neighbors	ネイバー情報を表示します。 **clear ospfv3 neighbors** コマンドを使用すると、すべてのネイバーとの隣接関係を削除できます。
show ipv6 ospfv3 request-list	ルータから要求されている LSA の一覧を表示します。
show ipv6 ospfv3 retransmission-list	再送を待っている LSA の一覧を表示します。
show ipv6 ospfv3 summary-address	OSPFv3 インスタンスで設定されている、すべての集約アドレス再配布情報の一覧を表示します。
show ospfv3 process	プロセス レベルの OSPFv3 認証設定を表示します。

コマンド	目的
show ospfv3 interface *interface-type slot/port*	インターフェイス レベルでの OSPFv3 認証設定を表示します。
show running-configuration ospfv3	現在実行中の OSPFv3 コンフィギュレーションを表示します。

OSPFv3のモニタリング

OSPFv3 統計情報を表示するには、次のコマンドを使用します。

コマンド	目的
show ipv6 ospfv3 memory	OSPFv3 メモリ使用状況の統計情報を表示します。
show ipv6 ospfv3 policy statistics area *area-id* **filter-list** {**in** | **out**} [**vrf** {*vrf-name* | **all** | **default** | **management**}]	エリアの OSPFv3 ルート ポリシー統計情報を表示します。
show ipv6 ospfv3 policy statistics redistribute {**bgp** *id* | **direct** | **isis** *id* | **rip** *id* | **static vrf** {*vrf-name* | **all** | **default** | **management**}]	OSPFv3 ルート ポリシー統計を表示します。
show ipv6 ospfv3 statistics [**vrf** {*vrf-name* | **all** | **default** | **management**}]	OSPFv3 イベント カウンタを表示します。
show ipv6 ospfv3 traffic *interface-type number* [**vrf** {*vrf-name* | **all** | **default** | **management**}]	OSPFv3 パケット カウンタを表示します。

OSPFv3 の設定例

次に、OSPFv3 を設定する例を示します。

```
This example shows how to configure OSPFv3:
        feature ospfv3
        router ospfv3 201
        router-id 290.0.2.1

        interface ethernet 1/2
        ipv6 address 2001:0DB8::1/48
        ipv6 ospfv3 201 area 0.0.0.10
```

key-chain オプションを使用して、OSPFv3 暗号を構成する例を示します。

```
switch(config-if)# ospfv3 encryption ipsec spi 333 esp ?
        3des       Use the triple DES algorithim
        aes        Use the AES algorithim
        key-chain  Encryption password key-chain
        null       Use NULL authentication
        switch(config-if)# ospfv3 encryption ipsec spi 333 esp key-chain ?
        WORD  Encryption key-chain name (Max Size 63)
```

```
        switch(config-if)# ospfv3 encryption ipsec spi 333 esp key-chain test1 ?
        authentication  Specify authentication parameters
        switch(config-if)# ospfv3 encryption ipsec spi 333 esp key-chain test1
authentication ?
        key-chain  Authentication password key-chain
        null       Use NULL authentication
        switch(config-if)# ospfv3 encryption ipsec spi 333 esp key-chain test1
authentication key-chain ?
        WORD Authentication key-chain name (Max Size 63)
        switch(config-if)# ospfv3 encryption ipsec spi 333 esp key-chain test1
authentication key-chain test2 ?
        <CR>
        switch(config-router)# sh ospfv3
        Routing Process 2 with ID 20.20.10.2 VRF default
        Routing Process Instance Number 1
        Install discard route for summarized internal routes.
        ESP Encryption 3DES, Authentication SHA1, SPI 334, ConnId 334
        ESP keychains: Encr test_key_chain_01(ready), Auth test1(ready)
        Number of new LSAs originated : 3
        Number of new LSAs received : 0
```

関連項目

次の項目には、OSPF に関する詳細情報が含まれています。

- OSPFv2
- Route Policy Manager の設定

その他の参考資料

OSPF の実装に関する詳細情報については、次のページを参照してください。

MIB

MIB	MIB のリンク
OSPFv3 に関連する MIB	サポートされている MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/mib/quickreference/cisco-nexus-7000-series-and-9000-series-nx-os-mib-quick-reference.html#con_67262

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