



## OSPFv2 の設定

この章では、Cisco NX-OS デバイスで IPv4 ネットワーク用の Open Shortest Path First version 2 (OSPFv2) 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。

- [OSPFv2 について \(1 ページ\)](#)
- [OSPFv2 およびユニキャスト RIB \(8 ページ\)](#)
- [認証 \(9 ページ\)](#)
- [高度な機能 \(10 ページ\)](#)
- [ライセンス要件 \(15 ページ\)](#)
- [OSPFv2 の前提条件 \(15 ページ\)](#)
- [OSPFv2 の注意事項および制約事項 \(15 ページ\)](#)
- [OSPFv2 のデフォルト設定 \(17 ページ\)](#)
- [基本的な OSPFv2 の設定 \(18 ページ\)](#)
- [高度な OSPFv2 の設定 \(29 ページ\)](#)
- [OSPFv2 設定の確認 \(55 ページ\)](#)
- [OSPFv2 のモニタリング \(56 ページ\)](#)
- [OSPFv2 の設定例 \(56 ページ\)](#)
- [その他の参考資料 \(57 ページ\)](#)

## OSPFv2 について

OSPFv2 は、IPv4 ネットワーク用 IETF リンクステートプロトコルです（「[リンクステートプロトコル](#)」の項を参照）。OSPFv2 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て、ほかの OSPFv2 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。これらの隣接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 OSPFv2 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 対応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 OSPFv2 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 OSPFv2 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。

OSPFv2 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。

OSPFv2 は IPv4 をサポートし、OSPFv3 は IPv6 をサポートしています。詳細については、[OSPFv3 の設定](#)を参照してください。



- 
- (注) Cisco NX-OS 上の OSPFv2 は、RFC 2328 をサポートしています。この RFC では、ルートサマリー コストの計算に、RFC1583 で使用する計算と互換性がない別の方法が導入されました。また RFC 2328 では、AS-external パスに対して異なる選択基準が導入されました。すべてのルータが同じ RFC をサポートしていることを確認することが重要です。RFC。RFC1583 にのみ準拠しているルータがネットワークに含まれる場合は、**rfc1583compatibility** コマンドを使用します。デフォルトでサポートされている OSPFv2 用の RFC 標準は、Cisco NX-OS と Cisco IOS とで異なる場合があります。値が同じになるように設定するには、調整が必要です。詳細については、「[OSPF RFC 互換モードの例](#)」の項を参照してください。
- 

## Hello パケット

OSPFv2 ルータは、すべての OSPF 対応インターフェイスに hello パケットを定期的送信します。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。OSPFv2 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 OSPFv2 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 OSPFv2 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 OSPFv2 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（「[ネイバー情報](#)」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。

OSPFv2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

ネイバーであると思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、OSPFv2 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 OSPFv2 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）
- 認証
- 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：ネイバーのルータ ID。
- プライオリティ：ネイバーのプライオリティ。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後に経過した時間を示します。
- IP アドレス：ネイバーの IP 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](#)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。

## 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、「[指定ルータ](#)」セクションを参照してください。

隣接関係は、OSPF 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 (「[リンクステートデータベース](#)」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続きます。

## 指定ルータ

複数のルータを含むネットワークは、OSPF 特有の状況です。すべてのルータがネットワークで LSA をフラッドした場合は、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、OSPFv2 は指定ルータ (DR) という 1 台のルータを使用して LSA のフラッドを制御し、OSPFv2 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、OSPFv2 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、OSPFv2 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。

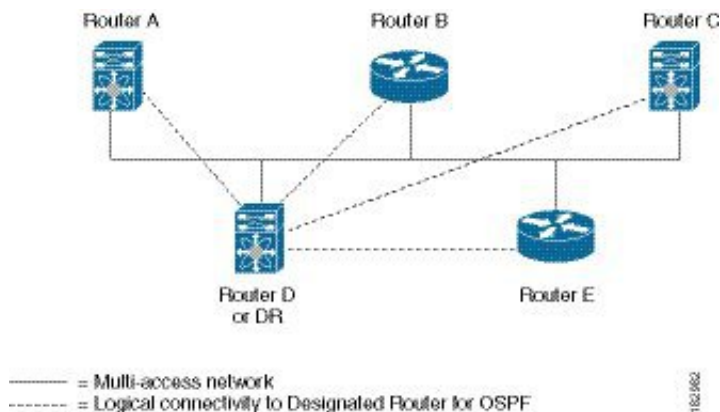
- ポイントツーポイント：2 台のルータ間にのみ存在するネットワーク。ポイントツーポイント ネットワーク上の全ネイバーは隣接関係を確立し、DR は存在しません。
- ブロードキャスト：ブロードキャストトラフィックが可能なイーサネットなどの共有メディア上で通信できる複数のルータを持つネットワーク。OSPFv2 ルータは DR および BDR を確立し、これらにより、ネットワーク上の LSA フラッドを制御します。OSPFv2 は、よく知られている IPv4 マルチキャストアドレス 224.0.0.5 および MAC アドレス 0100.5300.0005 を使用して、ネイバーと通信します。

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 OSPFv2 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、IPv4 マルチキャストアドレス 224.0.0.6 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



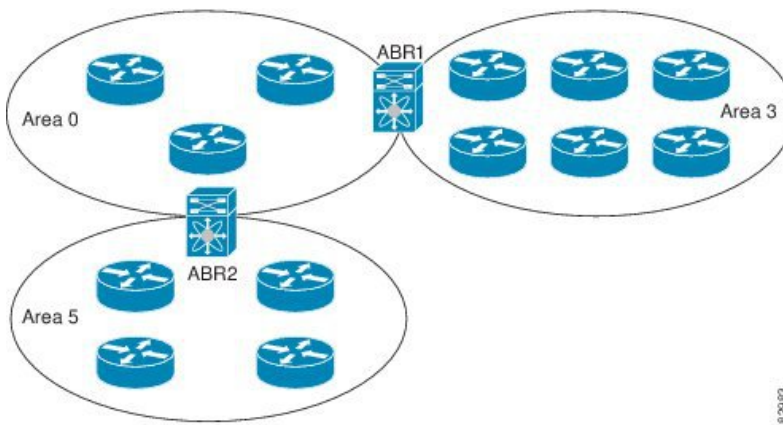
## エリア

OSPFv2 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 OSPFv2 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、OSPFv2 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 進表記で入力できる 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。

OSPFv2 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。図では、ABR が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する方法を示します。

図 2: OSPFv2 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ネットワーク集約 (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。OSPFv2 エリア図に、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。

OSPFv2 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、OSPFv2 エリアを別の自律システムに接続します。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。OSPFv2 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、「[高度な機能](#)」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

OSPFv2 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

OSPFv2 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。

表 1: 表 5-1 LSA タイプ

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、およびリンク上のすべての OSPFv2 ネイバーの一覧が含まれます。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 OSPFv2 エリアにフラッドイングされます。
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。ネットワーク LSA は SPF 再計算をトリガーします。「 <a href="#">指定ルータ</a> 」のセクションを参照してください。
3	ネットワーク集約 LSA	エリア境界ルータが、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、エリア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。「 <a href="#">エリア</a> 」のセクションを参照してください。
4	ASBR 集約 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。「 <a href="#">エリア</a> 」の項を参照してください。

タイプ	名前	説明
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ドイングされます。「 <a href="#">エリア</a> 」の項を参照してください。
7	NSSA 外部 LSA	ASBR が Not-So-Stubby Area (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。NSSA 外部 LSA は、ローカル NSSA 内のみでフラッドイングされます。「 <a href="#">エリア</a> 」のセクションを参照してください。
9-11	不透明 LSA	OSPF の拡張に使用される LSA。「 <a href="#">不透明 LSA</a> 」のセクションを参照してください。

## リンク コスト

各 OSPFv2 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。

## フラッドイングと LSA グループ ペーシング

OSPFv2 ルータは LSA を受信すると、その LSA をすべての OSPF 対応インターフェイスに転送し、この情報を使用して OSPFv2 エリアをフラッドイングします。この LSA フラッドイングにより、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 フラッドイングは、OSPFv2 エリアの設定により異なります（「[エリア](#)」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）フラッドイングされます。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 更新情報のフラッドイングレートは、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 またはバッファの高い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、OSPFv2 で、複数の LSA を 1 つの OSPFv2 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 OSPFv2 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、OSPFv2 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。OSPFv2 は、この情報を使用して、各宛先への最適パスを計算し、この最適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ドイングし、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、「[フラッドイングと 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。

## 不透明 LSA

不透明 LSA により、OSPF 機能の拡張が可能となります。不透明 LSA は、標準 LSA ヘッダーと、それに続くアプリケーション固有の情報で構成されます。この情報は、OSPFv2 または他のアプリケーションにより使用される場合があります。OSPFv2 は、OSPFv2 グレースフル リスタート機能をサポートするために Opaque LSA を使用します（「[高可用性およびグレースフル リスタート](#)」セクションを参照）。次のような 3 種類の不透明 LSA タイプが定義されています。

- LSA タイプ 9：ローカル ネットワークにフラッドイングされます。
- LSA タイプ 10：ローカル エリアにフラッドイングされます。
- LSA タイプ 11：ローカル自律システムにフラッドイングされます。

## OSPFv2 およびユニキャスト RIB

OSPFv2 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。そして、選択された各宛先への最短パスが OSPFv2 ルート テーブルに入力されます。OSPFv2 ネットワークが収束すると、このルート テーブルはユニキャスト RIB にデータを提供します。OSPFv2 はユニキャスト 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 OSPFv2 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の提供（「[OSPFv2 スタブルータ アドバタイズメント](#)」セクションを参照）

さらに OSPFv2 は、変更済みダイクストラ アルゴリズムを実行して、集約および外部（タイプ 3、4、5、7）LSA の変更の高速再計算を行います。



## 認証

OSPFv2 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。Cisco NX-OS は、次の 2 つの認証方式をサポートしています。

- 簡易パスワード認証
- MD5 認証ダイジェスト

OSPFv2 認証は、OSPFv2 エリアに対して、またはインターフェイスごとに設定できます。

### 簡易パスワード認証

簡易パスワード認証では、OSPFv2 メッセージの一部として送信された単純なクリアテキストのパスワードを使用します。受信 OSPFv2 ルータが OSPFv2 メッセージを有効なルート更新情報として受け入れるには、同じクリアテキストパスワードで設定されている必要があります。パスワードがクリアテキストであるため、ネットワーク上のトラフィックをモニタできるあらゆるユーザがパスワードを入手できます。

### 暗号化認証

暗号化認証では、暗号化されたパスワードを OSPFv2 認証に使用します。トランスミッタは、送信するパケットとキー文字列を使用してコードを計算し、そのコードとキー ID をパケットに挿入して、パケットを送信します。受信側は、受信したパケットとローカルに設定されたキースtring (パケット内のキー ID に対応) を使用してコードをローカルに計算することにより、パケット内のコードを検証します。

メッセージダイジェスト 5 (MD5) とハッシュベースのメッセージ認証コードセキュアハッシュアルゴリズム (HMAC-SHA) 暗号化認証の両方がサポートされています。

### MD5 認証

OSPFv2 メッセージを認証するには、MD5 認証を使用する必要があります。そのためには、ローカルルータとすべてのリモート OSPFv2 ネイバーが共有するパスワードを設定します。Cisco NX-OS は各 OSPFv2 メッセージに対して、メッセージと暗号化されたパスワードに基づく MD5 一方向メッセージダイジェストを作成します。インターフェイスはこのダイジェストを OSPFv2 メッセージとともに送信します。受信する OSPFv2 ネイバーは、同じ暗号化パスワードを使用して、このダイジェストを確認します。メッセージが変更されていない場合はダイジェストの計算が同一であるため、OSPFv2 メッセージは有効と見なされます。

MD5 認証には、ネットワークでのメッセージの再送を防ぐための、各 OSPFv2 メッセージのシーケンス番号が含まれます。

## HMAC-SHA 認証

Cisco NX-OS リリース 7.0 (3) I3 (1) 以降、OSPFv2 は RFC 5709 をサポートしており、MD5 よりも高いセキュリティを提供する HMAC-SHA アルゴリズムを使用できます。HMAC-SHA-1、HMAC-SHA-256、HMAC-SHA-384。および HMAC-SHA-512 アルゴリズムは、OSPFv2 認証でサポートされます。

## 高度な機能

Cisco NX-OS は、ネットワークでの OSPFv2 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。

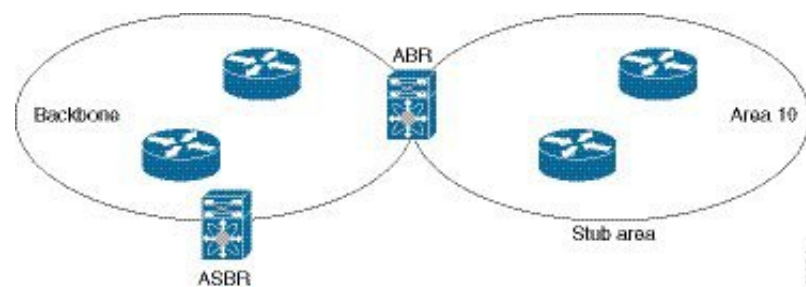
## スタブエリア

エリアをスタブエリアにすると、エリアでフラッド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ドされます。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。

次の図には、外部 AS に到達するためにエリア 0.0.0.10 内のすべてのルータが ABR を通過する必要のある OSPFv2 AS の例を示します。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。IPv4 の場合のデフォルトルートは 0.0.0.0 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、NSSA 外部 (タイプ 7) LSA を生成して NSSA 全体でフラッディングします。または、NSSA を他のエリアに接続する ABR を設定することにより、この NSSA 外部 LSA を AS 外部 (タイプ 5) LSA に変換することもできます。こうすると、ABR は、これらの AS 外部 LSA を OSPFv2 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。NSSA 外部 LSA に関する情報については、[リンクステートアドバタイズメント \(6 ページ\)](#) セクションを参照してください。

たとえば、OSPFv2 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。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、NSSA を使用する前に、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 OSPFv2 スタブエリアとして実行できません。NSSA を使用すると、企業の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 (「[NSSA の設定](#)」を参照) ことで、OSPFv2 を拡張してリモート接続性をサポートできます。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。

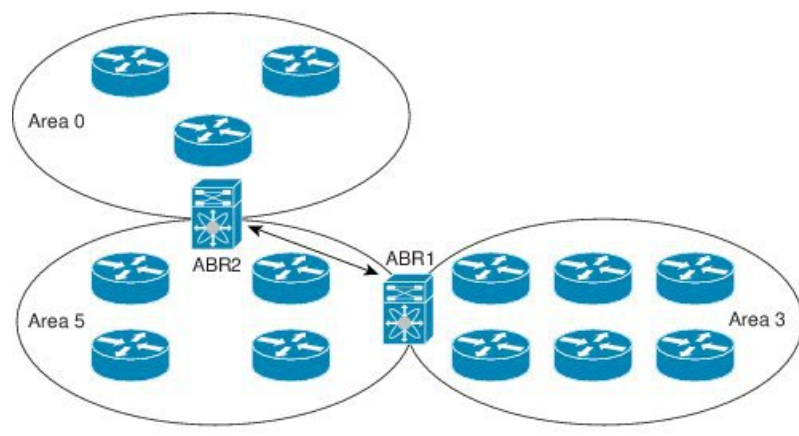
すでに RFC 非準拠の動作を使用するようにネットワークを設計しており、デフォルトルートが NSSA ABR に追加されると想定している場合は、Cisco NX-OS リリース 9.3(1) 以降にアップグレードするときに動作が変更されます。

古い動作を続行する場合は、**default-route nssa-abr pbbit-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、OSPFv2 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

OSPFv2 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ルートに割り当てるように、OSPFv2 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 OSPFv2 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 OSPFv2 自律システム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。ルートマップの設定の詳細については、[Route Policy Manager の設定](#) を参照してください。

## ルート集約

OSPFv2 は、学習したすべてのルートを、すべての OSPF 対応ルータと共有するため、ルート集約を使用して、すべての OSPF 対応ルータにフラッドされる一意のルートの数を削減した方がよい場合があります。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、10.1.1.0/24、10.1.2.0/24、および 10.1.3.0/24 というアドレスを 1 つの集約アドレス 10.1.0.0/16 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る必要があります。

外部ルート集約は、ルート再配布を使用して OSPFv2 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、マルチレベルの高可用性 アーキテクチャを提供します。OSPFv2 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。OSPFv2 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、OSPFv2 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 OSPFv2 がデータ転送パス上に存在し続けます。OSPFv2 はグレースフルリスタートを実行する必要がある場合、猶予 LSA と呼ばれるリンクローカル不透明 (タイプ 9) LSA を送信します。この再起動中の OSPFv2 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 OSPFv2 インターフェイスが再起動中の OSPFv2 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、OSPFv2 は隣接関係を切断し、ダウン状態または再起動中の OSPFv2 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 OSPFv2 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 OSPFv2 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 ospf` 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` コマンド

## OSPFv2 スタブルータ アドバタイズメント

OSPFv2 スタブルータ アドバタイズメント機能を使用して、OSPFv2 インターフェイスをスタブルータとして機能するように設定できます。この機能は、ネットワークに新規ルータを機能制限付きで導入する場合や、過負荷になっているルータの負荷を制限する場合など、このルータ経由の OSPFv2 トラフィックを制限するときに使用します。また、この機能は、さまざまな管理上またはトラフィック エンジニアリング上の理由により使用する場合もあります。

OSPFv2 スタブルータ アドバタイズメントは、OSPFv2 ルータをネットワーク トポロジから削除しませんが、他の OSPFv2 ルータがこのルータを使用して、ネットワークの他の部分にトラフィックをルーティングできないようにします。このルータを宛先とするトラフィック、またはこのルータに直接接続されたトラフィックだけが送信されます。

OSPFv2 スタブルータ アドバタイズメントは、すべてのスタブリンク (ローカルルータに直接接続された) を、ローカル OSPFv2 インターフェイスのコストとしてマークします。すべてのリモートリンクは、最大のコスト (0xFFFF) としてマークされます。

## 複数の OSPFv2 インスタンス

Cisco NX-OS は、同じノード上で動作する、OSPFv2 プロトコルの複数インスタンスをサポートしています。同一インターフェイスには複数のインスタンスを設定できません。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 OSPFv2 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 OSPFv2 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。

## 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、ネットワーク集約 (タイプ 3) LSA、および AS 外部 (タイプ 5) LSA 用の部分的 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、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。

## OSPFv2 の仮想化のサポート

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 OSPF 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 OSPFv2 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。

## ライセンス要件

Cisco NX-OS ライセンス方式の推奨の詳細と、ライセンスの取得および適用の方法については、『[Cisco NX-OS Licensing Guide](#)』を参照してください。

## OSPFv2 の前提条件

OSPFv2 には、次の前提条件があります。

- OSPF 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。
- スイッチにログインしている。
- リモート OSPFv2 ネイバーと通信可能な IPv4 用インターフェイスが 1 つ以上設定されている。
- OSPFv2 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 機能がイネーブルにされている（「[OSPFv2の有効化](#)」の項を参照）。

## OSPFv2 の注意事項および制約事項

OSPFv2 設定時の注意事項および制約事項は、次のとおりです。

- OSPFv2 の **graceful-restart planned-only** コマンド (**reload**) 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、CTCPPrimaryNetworks 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。
- すべての OSPFv2 ルータが、同じ RFC 互換モードで動作する必要があります。Cisco NX-OS の OSPFv2 は RFC 2328 に準拠しています。RFC 1583 にのみ対応しているルータがネットワークに含まれている場合は、ルータ設定モードで **rfc1583compatibility** コマンドを使用します。
- 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。
  - 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 ip 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。
  - 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 ip 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。
  - 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。
- vPC 設定モードで **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。

- N9K-X9636C-R および N9K-X9636Q-R ラインカードおよび N9K-C9508-FM-R ファブリックモジュールの場合、**show run ospf** コマンドの出力には、一部の OSPF コマンドのデフォルト値が表示されることがあります。



(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ります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。

## OSPFv2のデフォルト設定

次の表に、OSPFv2 パラメータのデフォルト設定値を示します。

表 2: OSPFv2 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
OSPFv2 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 の最小ホールドタイム	5000 ミリ秒
SPF 計算初期遅延時間	1000 ミリ秒

## 基本的な OSPFv2 の設定

OSPFv2 は、OSPFv2 ネットワークを設計した後に設定します。

### OSPFv2の有効化

OSPFv2 を設定するには、その前に OSPFv2 機能を有効にする必要があります。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>feature ospf</b> 例： switch(config)# feature ospf 例：	OSPFv2 機能を有効にします。
ステップ 3	(任意) <b>show feature</b> 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) <b>copy running-config startup-config</b> 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

OSPFv2 機能をディセーブルにして、関連付けられている設定をすべて削除するには、グローバル設定モードで `no feature ospf` コマンドを使用します。

コマンド	目的
<b>no feature ospf</b> 例 : switch(config)# no feature ospf	OSPFv2 機能を無効にして、関連付けられた設定をすべて削除します。

## OSPFv2インスタンスの作成

OSPFv2 を設定する最初のステップは、OSPFv2 インスタンスを作成することです。作成した OSPFv2 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。

OSPFv2 インスタンス パラメータの詳細については、[高度なOSPFv2の設定 \(29 ページ\)](#) の項を参照してください。

### 始める前に

OSPF 機能をイネーブルにしてあることを確認します（「[OSPFv2の有効化](#)」の項を参照）。

**show ip ospf instance-tag** 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。

OSPFv2 がルータ ID（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

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>[no]router ospf instance-tag</b> 例 : switch(config)# router ospf 201 switch(config-router)	新規 OSPFv2 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	(任意) <b>router-id ip-address</b> 例 : switch(config-router)# router-id 192.0.2.1	OSPFv2 ルータ ID を設定します。この IP アドレスにより、この OSPFv2 インスタンスが識別されます。このアドレスは、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) <b>show ip ospf instance-tag</b> 例 :	OSPF 情報を表示します。

	コマンドまたはアクション	目的
	<code>switch(config-router)# show ip ospf 201</code>	
ステップ 5	(任意) <b>copy running-config startup-config</b> 例： <code>switch(config)# copy running-config startup-config</code>	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**

OSPFv2 インスタンスと、関連付けられている設定をすべて削除するには、グローバルコンフィギュレーションモードで `no feature ospf` コマンドを使用します。

コマンド	目的
<b>no router ospf instance-tag</b> 例： <code>switch(config)# no router ospf 201</code>	OSPF インスタンスと、関連付けられた設定を削除します。



(注) このコマンドは、インターフェイスモードでは OSPF 設定を削除しません。インターフェイスモードで設定された OSPFv2 コマンドはいずれも、手動で削除する必要があります。

## OSPFv2 インスタンスのオプションパラメータの設定

OSPF のオプションパラメータを設定できます。[高度な OSPFv2 の設定 \(29 ページ\)](#) セクションを参照してください。

ルータ コンフィギュレーション モードで、次の OSPFv2 用オプションパラメータを設定できます。

**始める前に**

OSPF 機能を有効にしてあることを確認します（「[OSPFv2 の有効化](#)」の項を参照）。

OSPFv2 がルータ ID（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

	コマンドまたはアクション	目的
ステップ 1	<b>distance number</b> 例 : switch(config-router)# distance 25	この OSPFv2 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 2	<b>log-adjacency-changes [detail]</b> 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 3	<b>maximum-paths path-number</b> 例 : switch(config-router)# maximum-paths 4	ルート テーブル内の宛先への同じ OSPFv2 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されます。指定できる範囲は 1～16 です。デフォルト値は 8 です。
ステップ 4	<b>distance number</b> 例 : switch(config-router)# distance 25	この OSPFv2 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 5	<b>log-adjacency-changes [detail]</b> 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	<b>maximum-paths path-number</b> 例 : switch(config-router)# maximum-paths 4	ルート テーブル内の宛先への同じ OSPFv2 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されます。指定できる範囲は 1～16 です。デフォルト値は 8 です。
ステップ 7	<b>passive-interface default</b> 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 8	(任意) <b>copy running-config startup-config</b> 例 : switch(config-router)# copy running-config startup-config	この設定変更を保存します。

## 例

次の例は、OSPFv2 インスタンスを作成する方法を示しています。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# copy running-config startup-config
```

## OSPFv2でのネットワークの設定

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、OSPFv2 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。



(注) 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。



(注) インターフェイスに有効な IP アドレスを設定するまでは、OSPF はインターフェイス上でイネーブルにされません。

### 始める前に

OSPF 機能をイネーブルにしてあることを確認します（「OSPFv2の有効化」の項を参照）。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>interface interface-type slot/port</b> 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。

	コマンドまたはアクション	目的
ステップ 3	<b>ip address ip-prefix/length</b> 例： switch(config-if)# ip address 192.0.2.1/16	このインターフェイスにIPアドレスおよびサブネットマスクを割り当てます。
ステップ 4	<b>ip router ospf instance-tag area area-id [secondaries none]</b> 例： switch(config-if)# ip router ospf 201 area 0.0.0.15	OSPFv2 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) <b>show ip ospf instance-tag interface interface-type slot/port</b> 例： switch(config-if)# show ip ospf 201 interface ethernet 1/2	OSPF 情報を表示します。
ステップ 6	<b>copy running-config startup-config</b> 例： switch(config-if)# copy running-config startup-config	この設定変更を保存します。
ステップ 7	(任意) <b>ip ospf cost number</b> 例： switch(config-if)# ip ospf cost 25	このインターフェイスの OSPFv2 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 8	(任意) <b>ip ospf dead-interval seconds</b> 例： switch(config-if)# ip ospf dead-interval 50	OSPFv2 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 9	(任意) <b>ip ospf hello-interval seconds</b> 例： switch(config-if)# ip ospf hello-interval 25	OSPFv2 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 10	(任意) <b>ip ospf mtu-ignore</b> 例： switch(config-if)# ip ospf mtu-ignore	OSPFv2 で、ネイバーとのあらゆる IP MTU 不一致が無視されるように設定します。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

	コマンドまたはアクション	目的
		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) <b>[default   no] ip ospf passive-interface</b> 例： <pre>switch(config-if)# ip ospf passive-interface</pre>	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。 <b>default</b> 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 12	(任意) <b>ip ospf priority number</b> 例： <pre>switch(config-if)# ip ospf priority 25</pre>	エリアの DR の決定に使用される OSPFv2 プライオリティを設定します。有効な範囲は 0 ~ 255 です。デフォルトは 1 です。「 <a href="#">指定ルータ</a> 」の項を参照してください。
ステップ 13	(任意) <b>ip ospf shutdown</b> 例： <pre>switch(config-if)# ip ospf shutdown</pre>	このインターフェイス上の OSPFv2 インスタンスをシャットダウンします。

### 例

次に、OSPFv2 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)# ip address 192.0.2.1/16
switch(config-if)# ip router ospf 201 area 0.0.0.10
switch(config-if)# copy running-config startup-config
```

**show ip ospf interface** コマンドを使用し、すれば、インターフェイスの設定を確認できます。**show ip ospf neighbor** コマンドを使用し、すれば、このインターフェイスのNAVERを確認できます。

## エリアの認証の設定

エリア内のすべてのネットワーク、またはエリア内の個々のインターフェイスの認証を設定できます。インターフェイス認証設定を使用すると、エリア認証は無効になります。



## 始める前に

OSPF機能が有効になっていることを確認するには、「[OSPFv2の有効化](#)」セクションを参照してください。

インターフェイス上のすべてのネイバーが、共有認証キーを含め、同じ認証設定を共有することを確認します。

この認証設定のためのキーチェーンを作成します。『[Cisco Nexus 9000 シリーズ NX-OS セキュリティ設定ガイド](#)』を参照してください。



- (注) OSPFv2 の場合、**key key-id** にキー ID があります コマンドは、2-255 の値のみをサポートします。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>router ospf instance-tag</b> 例： <pre>switch(config)# router ospf 201 switch(config-router)#</pre>	新規 OSPFv2 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	<b>area area-id authentication [message-digest]</b> 例： <pre>switch(config-router)# area 0.0.0.10 authentication</pre>	エリアの認証モードを設定します。
ステップ 4	<b>interface interface-type slot/port</b> 例： <pre>switch(config-router)# interface ethernet 1/2 switch(config-if)#</pre>	インターフェイス設定モードを開始します。
ステップ 5	(任意) <b>ip ospf authentication-key [0   3] key</b> 例： <pre>switch(config-if)# ip ospf authentication-key 0 mypass</pre>	このインターフェイスに簡易パスワード認証を設定します。認証が、キーチェーンにもメッセージダイジェストにも設定されていない場合は、このコマンドを使用します。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

	コマンドまたはアクション	目的
		は、パスワードを 3DES 暗号化として設定します。
ステップ 6	(任意) <b>ip ospf message-digest-key</b> <i>key-id</i> <b>md5</b> [ <b>0</b>   <b>3</b> ] <i>key</i> 例 : <pre>switch(config-if)# ip ospf message-digest-key 21 md5 0 mypass</pre>	このインターフェイスにメッセージダイジェスト認証を設定します。認証がメッセージダイジェストに設定されている場合は、このコマンドを使用しません。 <b>key-id</b> の範囲は 1～255 です。MD5 オプションが <b>0</b> の場合はパスワードがクリアテキストで設定され、 <b>3</b> の場合はパスワードが 3DES 暗号化として設定されます。
ステップ 7	(任意) <b>show ip ospf instance-tag</b> <b>interface</b> <i>interface-type slot/port</i> 例 : <pre>switch(config-if)# show ip ospf 201 interface ethernet 1/2</pre>	OSPF 情報を表示します。
ステップ 8	(任意) <b>copy running-config</b> <b>startup-config</b> 例 : <pre>switch(config)# copy running-config startup-config</pre>	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

## インターフェイスの認証の設定

エリア内のすべてのネットワーク、またはエリア内の個々のインターフェイスの認証を設定できます。インターフェイス認証設定を使用すると、エリア認証は無効になります。

### 始める前に

OSPF 機能をイネーブルにしてあることを確認します（「[OSPFv2の有効化](#)」の項を参照）。

インターフェイス上のすべてのネイバーが、共有認証キーを含め、同じ認証設定を共有することを確認します。

この認証設定のためのキーチェーンを作成します。『[Cisco Nexus 9000 シリーズ NX-OS セキュリティ設定ガイド](#)』を参照してください。



(注) OSPFv2 の場合、**key key-id** にキー ID があります コマンドは、2～255 の値のみをサポートします。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>interface interface-type slot/port</b> 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	<b>ip ospf authentication [message-digest]</b> 例 : switch(config-if)# ip ospf authentication	OSPFv2 のインターフェイス認証モードをクリアテキスト タイプとメッセージダイジェストタイプのどちらかでイネーブルにします。これにより、エリアに基づくこのインターフェイスの認証が無効となります。すべてのネイバーが、この認証タイプを共有する必要があります。
ステップ 4	(任意) <b>ip ospf authentication key-chain key-id</b> 例 : switch(config-if)# ip ospf authentication key-chain Test1	OSPFv2 のキーチェーンを使用するようにインターフェイス認証を設定します。キーチェーンの詳細については、『シスコスタンドアロンCisco NX-OSセキュリティ設定ガイド』を参照してください。
ステップ 5	(任意) <b>ip ospf authentication-key [0   3   7] key</b> 例 : switch(config-if)# ip ospf authentication-key 0 mypass	このインターフェイスに簡易パスワード認証を設定します。認証が、キーチェーンにもメッセージダイジェストにも設定されていない場合は、このコマンドを使用します。 オプションは次のとおりです。 <ul style="list-style-type: none"> <li>• 0 : パスワードをクリアテキストで設定します。</li> <li>• 3 : パス キーを 3DES 暗号化として設定します。</li> <li>• 7 : パス キーを Cisco タイプ 7 暗号化として設定します。</li> </ul>
ステップ 6	(任意) <b>ip ospf message-digest-key key-id md5 [0   3   7] key</b> 例 :	このインターフェイスにメッセージダイジェスト認証を設定します。認証がメッセージダイジェストに設定されて

	コマンドまたはアクション	目的
	<pre>switch(config-if)# ip ospf message-digest-key 21 md5 0 mypass</pre>	<p>いる場合は、このコマンドを使用します。key-idの範囲は1～255です。MD5オプションは次のとおりです。</p> <ul style="list-style-type: none"> <li>• 0 : パスワードをクリアテキストで設定します。</li> <li>• 3 : パス キーを 3DES 暗号化として設定します。</li> <li>• 7 : パス キーを Cisco タイプ 7 暗号化として設定します。</li> </ul>
ステップ 7	<p>(任意) <b>show ip ospf instance-tag interface interface-type slot/port</b></p> <p>例 :</p> <pre>switch(config-if)# show ip ospf 201 interface ethernet 1/2</pre>	OSPF 情報を表示します。
ステップ 8	<p>(任意) <b>copy running-config startup-config</b></p> <p>例 :</p> <pre>switch(config)# copy running-config startup-config</pre>	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、インターフェイスに暗号化されていない簡単なパスワードを設定し、イーサネットインターフェイス 1/2 のパスワードを設定する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# exit
switch(config)# interface ethernet 1/2
switch(config-if)# ip router ospf 201 area 0.0.0.10
switch(config-if)# ip ospf authentication
switch(config-if)# ip ospf authentication-key 0 mypass
switch(config-if)# copy running-config startup-config
```

次に、OSPFv2 HMAC-SHA-1 および MD5 暗号化認証を設定する例を示します。

```
switch# configure terminal
switch(config)# key chain chain1
switch(config-keychain)# key 1
switch(config-keychain-key)# key-string 7 070724404206
switch(config-keychain-key)# accept-lifetime 01:01:01 Jan 01 2015 infinite
switch(config-keychain-key)# send-lifetime 01:01:01 Jan 01 2015 infinite
switch(config-keychain-key)# cryptographic-algorithm HMAC-SHA-1
switch(config-keychain-key)# exit
switch(config-keychain)# key 2
switch(config-keychain-key)# key-string 7 070e234f1f5b4a
```

```
switch(config-keychain-key)# accept-lifetime 10:51:01 Jul 24 2015 infinite
switch(config-keychain-key)# send-lifetime 10:51:01 Jul 24 2015 infinite
switch(config-keychain-key)# cryptographic-algorithm MD5
switch(config-keychain-key)# exit
switch(config-keychain)# exit

switch(config)# interface ethernet 1/1
switch(config-if)# ip router ospf 1 area 0.0.0.0
switch(config-if)# ip ospf authentication message-digest
switch(config-if)# ip ospf authentication key-chain chain1

switch(config-if)# show key chain chain1
Key-Chain chain1
Key 1 -- text 7 "070724404206"
cryptographic-algorithm HMAC-SHA-1
accept lifetime UTC (01:01:01 Jan 01 2015)-(always valid) [active]
send lifetime UTC (01:01:01 Jan 01 2015)-(always valid) [active]
Key 2 -- text 7 "070e234f1f5b4a"
cryptographic-algorithm MD
accept lifetime UTC (10:51:00 Jul 24 2015)-(always valid) [active]
send lifetime UTC (10:51:00 Jul 24 2015)-(always valid) [active]

switch(config-if)# show ip ospf interface ethernet 1/1
Ethernet1/1 is up, line protocol is up
IP address 11.11.11.1/24
Process ID 1 VRF default, area 0.0.0.3
Enabled by interface configuration
State BDR, Network type BROADCAST, cost 40
Index 6, Transmit delay 1 sec, Router Priority 1
Designated Router ID: 33.33.33.33, address: 11.11.11.3
Backup Designated Router ID: 1.1.1.1, address: 11.11.11.1
2 Neighbors, flooding to 2, adjacent with 2
Timer intervals: Hello 10, Dead 40, Wait 40, Retransmit 5
Hello timer due in 00:00:08
Message-digest authentication, using keychain key1 (ready)
Sending SA: Key id 2, Algorithm MD5
Number of opaque link LSAs: 0, checksum sum 0
```

## 高度な OSPFv2 の設定

OSPFv2 は、OSPFv2 ネットワークを設計した後に設定します。

### 境界ルータのフィルタ リストの設定

OSPFv2 ドメインを関連ネットワークを含む一連のエリアに分割できます。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。OSPFv2 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。

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。「[ルート集約の設定](#)」の項を参照してください。
- **Filter list** : 外部エリアから受信したネットワーク集約 (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

OSPF 機能がイネーブルになっていることを確認します。「[OSPFv2の有効化](#)」の項を参照してください。

フィルタ リストが、着信または発信ネットワーク集約（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。「[エリア](#)」の項を参照してください。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>router ospf instance-tag</b> 例： switch(config)# router ospf 201 switch(config-router)#	新規 OSPFv2 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	<b>area area-id filter-list route-map map-name {in   out}</b> 例： switch(config-router)# area 0.0.0.10 filter-list route-map FilterLSAs in	ABR 上で着信または発信ネットワーク集約（タイプ 3）LSA をフィルタリングします。
ステップ 4	（任意） <b>show ip ospf policy statistics area id filter-list {in   out}</b> 例： switch(config-router)# show ip ospf policy statistics area 0.0.0.10 filter-list in	OSPF ポリシー情報を表示します。
ステップ 5	（任意） <b>copy running-config startup-config</b> 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、エリア 0.0.0.10 でフィルタ リストを設定する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# area 0.0.0.10 filter-list route-map FilterLSAs in
switch(config-router)# copy running-config startup-config
```

## スタブエリアの設定

OSPFv2 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、選択したネットワークへの往復の不要な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なっていることを確認します。（「[OSPFv2の有効化](#)」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

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>router ospf instance-tag</b> 例： switch(config)# router ospf 201 switch(config-router)#	新規 OSPFv2 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	<b>area area-id stub</b> 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 4	（任意） <b>area area-id default-cost cost</b> 例： switch(config-router)# 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。デフォルトは 1 です。
ステップ 5	（任意） <b>show ip ospf instance-tag</b> 例： switch(config-router)# show ip ospf 201	OSPF 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	(任意) <b>copy running-config startup-config</b> 例 : <pre>switch(config)# copy running-config startup-config</pre>	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、スタブエリアを作成する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# area 0.0.0.10 stub
switch(config-router)# copy running-config startup-config
```

## Totally Stubby エリアの設定

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

	コマンドまたはアクション	目的
ステップ 1	<b>area area-id stub no-summary</b> 例 : <pre>switch(config-router)# area 20 stub no-summary</pre>	このエリアを Totally Stubby エリアとして作成します。

## NSSA の設定

OSPFv2 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 OSPFv2 ドメインをフラッドすることもできます。NSSA は、省略可能な次のパラメータで設定できます。

- **No redistribution** : 再配布されたルートは、NSSA をバイパスして OSPFv2 自律システム内の他のエリアに再配布されます。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 NSSA 外部 (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



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、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かどうかに関係なく、NSSA ASBR 上で使用できます。

- **Route map** : 目的のルートだけが NSSA および他のエリア全体でフラッドイングされるように、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 でフラッドイ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、NSSA 外部 LSA を AS 外部 LSA に変換します。再配布されたルートを OSPFv2 自律システム全体でフラッドイングするには、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。このオプションを選択した場合は、転送アドレスが 0.0.0.0 に設定されます。



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

### 始める前に

OSPF 機能を有効にしてあることを確認します（「OSPFv2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

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>router ospf instance-tag</b> 例： switch(config)# router ospf 201 switch(config-router)#	新規 OSPFv2 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	<b>area area-id nssa [no-redistribution] [default-information-originate] originate [route-map map-name]] [no-summary]</b> 例： switch(config-router)# area 0.0.0.10 nssa no-redistribution	このエリアを NSSA として作成します。

	コマンドまたはアクション	目的
ステップ 4	(任意) <b>area area-id nssa translate type7 {always   never} [suppress-fa]</b>  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 5	(任意) <b>area area-id default-cost cost</b>  例： switch(config-router)# 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。
ステップ 6	(任意) <b>show ip ospf instance-tag</b>  例： switch(config-router)# show ip ospf 201	OSPF 情報を表示します。
ステップ 7	(任意) <b>copy running-config startup-config</b>  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、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# configure terminal
switch(config)# router ospf 201
switch(config-router)# area 0.0.0.10 nssa no-summary
switch(config-router)# copy running-config startup-config
```

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# configure terminal
switch(config)# router ospf 201
switch(config-router)# area 0.0.0.10 nssa default-info-originate
switch(config-router)# copy running-config startup-config
```

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# configure terminal
switch(config)# router ospf 201
switch(config-router)# area 0.0.0.10 nssa route-map ExternalFilter no-summary
switch(config-router)# copy running-config startup-config
```

次に、常に NSSA 外部 (タイプ 5) LSA を AS 外部 (タイプ 7) LSA に変換する NSSA を作成し NSSA を設定する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
```

```
switch(config-router)# area 0.0.0.10 nssa
switch(config-router)# area 0.0.0.10 nssa translate type 7 always
switch(config-router)# copy running-config startup-config
```

## マルチエリアの隣接関係の設定

既存の OSPFv2 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

OSPFv2 機能が有効にされている必要があります（「[OSPFv2の有効化](#)」のセクションを参照）。

インターフェイスにプライマリアreaが設定されていることを確認します（「[OSPFv2でのネットワークの設定](#)」の項を参照）。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  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	<b>interface interface-type slot/port</b>  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	<b>ip router ospf [instance-tag] multi-area area-id</b>  例： switch(config-if)# ip router ospf 201 multi-area 3	別のエリアにインターフェイスを追加します。  (注) Cisco NX-OS リリース 7.0(3)I5(1) 以降では、 <i>instance-tag</i> 引数はオプションです。インスタンスを指定しない場合、マルチエリア設定は、そのインターフェイスのプライマリアreaに設定されている同じインスタンスに適用されます。
ステップ 4	(任意) <b>show ip ospf instance-tag interface interface-type slot/port</b>  例：	OSPFv2 情報を表示します。

	コマンドまたはアクション	目的
	switch(config-if)# show ip ospf 201 interface ethernet 1/2	
ステップ 5	(任意) <b>copy running-config startup-config</b>  例 : switch(config)# copy running-config startup-config	この設定変更を保存します。

### 例

次に、OSPFv2 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# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# ip address 192.0.2.1/16
switch(config-if)# ip router ospf 201 area 0.0.0.10
switch(config-if)# ip router ospf 201 multi-area 20
switch(config-if)# copy running-config startup-config
```

## 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](#)」の項を参照してください。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。

- **Authentication** : 簡単なパスワード認証または MD5 メッセージダイジェスト認証、および関連付けられたキーを設定します。
- **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。

スタブエリアには仮想リンクを追加できません。

### 始める前に

OSPF 機能をイネーブルにしてあることを確認します（「[OSPFv2の有効化](#)」の項を参照）。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>router ospf instance-tag</b> 例： switch(config)# router ospf 201 switch(config-router)#	新規 OSPFv2 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	<b>area area-id virtual link router-id</b> 例： switch(config-router)# area 0.0.0.10 virtual-link 10.1.2.3 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 4	(任意) <b>show ip ospf virtual-link [brief]</b> 例： switch(config-router-vlink)# show ip ospf virtual-link	OSPF 仮想リンク情報を表示します。
ステップ 5	(任意) <b>copy running-config startup-config</b> 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
ステップ 6	(任意) <b>authentication [key-chain key-id message-digest   null]</b> 例： switch(config-router-vlink)# authentication message-digest	エリアに基づくこの仮想リンクの認証がオーバーライドされます。
ステップ 7	(任意) <b>authentication-key [0   3] key</b> 例： switch(config-router-vlink)# authentication-key 0 mypass	この仮想リンクに簡易パスワードを設定します。認証が、キーチェーンにもメッセージダイジェストにも設定されていない場合は、このコマンドを使用します。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、パスワードを 3DES 暗号化として設定します。

	コマンドまたはアクション	目的
ステップ 8	(任意) <b>dead-interval</b> <i>seconds</i> 例： switch(config-router-vlink)# dead-interval 50	OSPFv2 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 9	(任意) <b>hello-interval</b> <i>seconds</i> 例： switch(config-router-vlink)# hello-interval 25	OSPFv2 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 10	(任意) <b>message-digest-key</b> <i>key-id</i> <b>md5</b> <b>[0   3]</b> <i>key</i> 例： switch(config-router-vlink)# message-digest-key 21 md5 0 mypass	この仮想リンクにメッセージダイジェスト認証を設定します。認証がメッセージダイジェストに設定されている場合は、このコマンドを使用します。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、パスワードを 3DES 暗号化として設定します。
ステップ 11	(任意) <b>retransmit-interval</b> <i>seconds</i> 例： switch(config-router-vlink)# retransmit-interval 50	OSPFv2 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 12	(任意) <b>transmit-delay</b> <i>seconds</i> 例： switch(config-router-vlink)# transmit-delay 2	OSPFv2 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。

## 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 27.0.0.55) の設定は、次のとおりです。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# area 0.0.0.10 virtual-link 10.1.2.3
switch(config-router)# copy running-config startup-config
```

ABR 2 (ルータ ID 10.1.2.3) の設定は、次のとおりです。

```
switch# configure terminal
switch(config)# router ospf 101
switch(config-router)# area 0.0.0.10 virtual-link 27.0.0.55
switch(config-router)# copy running-config startup-config
```

## 再配布の設定

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 OSPFv2 自律システムに再配布できます。

デフォルトルートを再配布するには、次のパラメータを指定する必要があります。

デフォルト以外のルートの場合、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 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 機能をイネーブルにします。「[OSPFv2の有効化](#)」を参照してください。

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

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>router ospf instance-tag</b> 例 : switch(config)# router ospf 201 switch(config-router)#	新規 OSPFv2 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	<b>redistribute {bgp id   direct   eigrp id   isis id   ospf id   rip id   static} route-map map-name</b> 例 : switch(config-router)# 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 OSPF 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 <b>default-information originate</b> コマンドを必要とします。

	コマンドまたはアクション	目的
ステップ 4	<b>default-information originate [always] [route-map map-name]</b>  例 : <pre>switch(config-router)# default-information-originate route-map DefaultRouteFilter</pre>	デフォルト ルートが RIB に存在する場合は、この OSPF ドメインにデフォルト 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。 <ul style="list-style-type: none"> <li>• <b>always</b> : 常に 0.0.0 のデフォルト ルートを生成します。ルートが RIB に存在しない場合でも。</li> <li>• <b>route-map</b> : 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。</li> </ul> (注) このコマンドは、ルートマップの <b>match</b> 文を無視します。
ステップ 5	<b>default-metric [cost]</b>  例 : <pre>switch(config-router)# default-metric 25</pre>	再配布されたルートのコスト メトリックを設定します。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 6	(任意) <b>copy running-config startup-config</b>  例 : <pre>switch(config)# copy running-config startup-config</pre>	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、ボーダー ゲートウェイ プロトコル (BGP) を OSPF に再配布する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# redistribute bgp route-map FilterExternalBGP
switch(config-router)# copy running-config startup-config
```

## 再配布されるルート数の制限

ルートの再配布によって、OSPFv2 ルートテーブルに多くのルートが追加される可能性があります。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。OSPFv2 には、再配布ルートの制限を設定するために次のオプションが用意されています。



- 上限固定：設定された最大値に OSPFv2 が達すると、メッセージをログに記録します。OSPFv2 は以降の再配布ルートを受け取りません。任意で、最大値のしきい値パーセンテージを設定して、OSPFv2 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：OSPFv2 が最大値に達したときのみ、警告のログを記録します。OSPFv2 は、再配布されたルートを受け入れ続けます。
- 取り消し：OSPFv2 が最大値に達したときに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、OSPFv2 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、OSPFv2 はすべての再配布されたルートを取り消します。OSPFv2 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 機能を有効にしてあることを確認します（「[OSPFv2の有効化](#)」の項を参照）。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例： <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>router ospf instance-tag</b>  例： <pre>switch(config)# router ospf 201 switch(config-router)#</pre>	新規 OSPFv2 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	<b>redistribute {bgp id   direct   eigrp id   isis id   ospf id   rip id   static} route-map map-name</b>  例： <pre>switch(config-router)# redistribute bgp route-map FilterExternalBGP</pre>	設定したルート マップ経由で、選択したプロトコルを OSPF に再配布します。
ステップ 4	<b>redistribute maximum-prefix max [threshold] [warning-only   withdraw [num-retries timeout]]</b>  例： <pre>switch(config-router)# redistribute maximum-prefix 1000 75 warning-only</pre>	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。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>threshold</b> : 警告メッセージをトリガーする最大プレフィックス数のパーセンテージ。</li> <li>• <b>warning-only</b> : 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。</li> <li>• <b>withdraw</b> : 再配布されたすべてのルートを取り消します。任意で再配布されたルートを取得しようと試みます。<i>num-retries</i> の範囲は 1 ~ 12 です。<i>timeout</i> の範囲は 60 ~ 600 秒です。デフォルトは 300 秒です。<b>clear ip ospf redistribution</b> コマンドは、すべてのルートが取り消された場合に使用します。</li> </ul>
ステップ 5	(任意) <b>show running-config ospf</b> 例 : <pre>switch(config-router)# show running-config ospf</pre>	OSPFv2 設定を表示します。
ステップ 6	(任意) <b>copy running-config startup-config</b> 例 : <pre>switch(config)# copy running-config startup-config</pre>	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# configure terminal
switch(config)# router ospf 201
switch(config-router)# redistribute bgp route-map FilterExternalBGP
switch(config-router)# redistribute maximum-prefix 1000 75
```

## 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、エリア間ルート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 機能を有効にしてあることを確認します（「[OSPFv2の有効化](#)」の項を参照）。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>router ospf instance-tag</b> 例： switch(config)# router ospf 201 switch(config-router)#	新規 OSPFv2 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	<b>area area-id range ip-prefix/length [no-advertise] [cost cost]</b> 例： switch(config-router)# area 0.0.0.10 range 10.3.0.0/16	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 アドレスをネットワーク集約（タイプ 3）LSA にアドバタイズしないようにすることもできます。cost の範囲は 0 ～ 16777215 です。
ステップ 4	<b>summary-address ip-prefix/length [no-advertise   tag tag]</b> 例： switch(config-router)# summary-address 10.5.0.0/16 tag 2	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。ルートマップによる再配布で使用できるよう、このサマリ アドレスにタグを割り当てることもできます。
ステップ 5	（任意） <b>show ip ospf summary-address</b> 例： switch(config-router)# show ip ospf summary-address	OSPF サマリ アドレスに関する情報を表示します。
ステップ 6	（任意） <b>copy running-config startup-config</b> 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# configure terminal
switch(config)# router ospf 201
```

```
switch(config-router)# area 0.0.0.10 range 10.3.0.0/16
switch(config-router)# copy running-config startup-config
```

次に、ASBR 上のサマリ アドレスを作成する例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# summary-address 10.5.0.0/16
switch(config-router)# copy running-config startup-config
```

## スタブルートアドバタイズメントの設定

短期間だけ、このルータ経由の OSPFv2 トラフィックを制限する場合は、スタブルートアドバタイズメントを使用します。詳細については、「[OSPFv2 スタブルータアドバタイズメント](#)」の項を参照してください。

スタブルートアドバタイズメントは、省略可能な次のパラメータで設定できます。

- On startup : 指定した宣言期間だけ、スタブルートアドバタイズメントを送信します。
- Wait for BGP : BGP がコンバージェンスするまで、スタブルートアドバタイズメントを送信します。



(注) ルータの実行コンフィギュレーションがグレースフルシャットダウンを行うよう設定されている場合は、その実行コンフィギュレーションを保存しないでください。保存すると、ルータが、リロード後に最大メトリックをアドバタイズし続けることとなります。

### 始める前に

OSPF 機能を有効にしてあることを確認します（「[OSPFv2の有効化](#)」の項を参照）。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>router ospf instance-tag</b> 例： switch(config)# router ospf 201 switch(config-router)#	新規 OSPFv2 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。

	コマンドまたはアクション	目的
ステップ 3	<b>max-metric router-lsa</b> [ <b>external-lsa</b> [ <i>max-metric-value</i> ]] [ <b>include-stub</b> ] [ <b>on-startup</b> { <i>seconds</i>   <b>wait-for bgp tag</b> }] [ <b>summary-lsa</b> [ <i>max-metric-value</i> ]]  例 : <pre>switch(config-router)# max-metric router-lsa</pre>	OSPFv2 スタブルート アドバタイズメントを設定します。
ステップ 4	(任意) <b>copy running-config startup-config</b>  例 : <pre>switch(config)# copy running-config startup-config</pre>	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、起動時にスタブルータアドバタイズメントを、デフォルトの 600 秒間イネーブルにする例を示します。

```
switch# configure terminal
switch(config)# router ospf 201
switch(config-router)# max-metric router-lsa on-startup
switch(config-router)# copy running-config startup-config
```

## ルートのアドミニストレーティブ ディスタンスの設定

OSPFv2 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 機能がイネーブルにされていることを確認してください（「[OSPFv2の有効化](#)」の項を参照）。

「[OSPFv2の注意事項および制約事項](#)」の項にあるこの機能の注意事項と制限事項を参照してください。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>router ospf instance-tag</b> 例： switch(config)# router ospf 201 switch(config-router)#	新規 OSPFv2 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	<b>[no] table-map map-name</b> 例： switch(config-router)# table-map foo	OSPFv2 ルートを RIB に送信する前に、OSPFv2 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 4	<b>exit</b> 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 5	<b>route-map map-name [permit   deny] [seq]</b> 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、 <i>seq</i> を使用します。  (注) <b>permit</b> オプションで、ディスタンスを設定することができます。 <b>deny</b> 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 6	<b>match route-type route-type</b> 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。  <ul style="list-style-type: none"> <li>• <b>external</b> : 外部ルート (BGP、EIGRP、OSPF タイプ 1 または 2)</li> <li>• <b>inter-area</b> : OSPF エリア間ルート</li> <li>• <b>internal</b> : 内部ルート (OSPF エリア内またはエリア間ルートを含む)</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• intra-area : OSPF エリア内ルート</li> <li>• nssa-external : NSSA 外部ルート (OSPF タイプ 1 または 2)</li> <li>• type-1 : OSPF 外部タイプ 1 ルート</li> <li>• type-2 : OSPF 外部タイプ 2 ルート</li> </ul>
ステップ 7	<b>match ip route-source prefix-list name</b> 例 : <pre>switch(config-route-map)# match ip route-source prefix-list p1</pre>	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 IPv4 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 <b>ip prefix-list</b> コマンドを使用して作成します。
ステップ 8	<b>match ip address prefix-list name</b> 例 : <pre>switch(config-route-map)# match ip address prefix-list p1</pre>	1 つまたは複数の IPv4 プレフィックスリストと照合。プレフィックスリストは <b>ip prefix-list</b> コマンドを使用して作成します。
ステップ 9	<b>set distance value</b> 例 : <pre>switch(config-route-map)# set distance 150</pre>	OSPFv2 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 10	(任意) <b>copy running-config startup-config</b> 例 : <pre>switch(config-route-map)# copy running-config startup-config</pre>	この設定変更を保存します。

## 例

次に、OSPFv2 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# configure terminal
switch(config)# router ospf 201
switch(config-router)# table-map foo
switch(config-router)# exit
switch(config)# route-map foo permit 10
switch(config-route-map)# match route-type inter-area
switch(config-route-map)# set distance 150
switch(config-route-map)# exit
switch(config)# route-map foo permit 20
```

```

switch(config-route-map)# match route-type external
switch(config-route-map)# set distance 200
switch(config-route-map)# exit
switch(config)# route-map foo permit 30
switch(config-route-map)# match ip route-source prefix-list p1
switch(config-route-map)# match ip address prefix-list p1
switch(config-route-map)# set distance 190

```

## デフォルトタイマーの変更

OSPFv2 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。OSPFv2 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 更新の数を最適化します（[フラッドイングと LSA グループ ペーシング](#) セクションを参照）。
- **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、「[OSPFv2でのネットワークの設定](#)」の項を参照してください。

### 始める前に

OSPF 機能を有効にしてあることを確認します（「[OSPFv2の有効化](#)」の項を参照）。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル 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 2	<b>router ospf instance-tag</b> 例 : <pre>switch(config)# router ospf 201 switch(config-router)#</pre>	新規 OSPFv2 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	<b>timers lsa-arrival msec</b> 例 : <pre>switch(config-router)# timers lsa-arrival 2000</pre>	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	<b>timers lsa-group-pacing seconds</b> 例 : <pre>switch(config-router)# timers lsa-group-pacing 1800</pre>	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 240 秒です。
ステップ 5	<b>timers throttle lsa start-time hold-interval max-time</b> 例 : <pre>switch(config-router)# timers throttle lsa 3000 6000 6000</pre>	次のタイマーを使用して、LSA 生成のレート制限をミリ秒で設定します。 <ul style="list-style-type: none"> <li>• <b>start-time</b> : 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。</li> <li>• <b>hold-interval</b> : 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。</li> <li>• <b>max-time</b> : 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。</li> </ul>
ステップ 6	<b>timers throttle spf delay-time hold-time max-wait</b> 例 : <pre>switch(config-router)# timers throttle spf 3000 2000 4000</pre>	SPF 最適パス スケジュールを次のタイマーを使用して、SPF 最適パス計算間 (秒単位) で設定します。 <ul style="list-style-type: none"> <li>• <b>delay-time</b> : 範囲は 1 ~ 600000 ミリ秒です。デフォルトは 200 ミリ秒です。</li> <li>• <b>hold-time</b> : 範囲は 1 ~ 600000 ミリ秒です。デフォルト値は、1000 ミリ秒です。</li> <li>• <b>max-wait</b> : 範囲は 1 ~ 600000 ミリ秒です。デフォルト値は 5000 ミリ秒です。</li> </ul>

	コマンドまたはアクション	目的
ステップ 7	<b>interface</b> <i>type slot/port</i>  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 8	<b>ip ospf hello-interval</b> <i>seconds</i>  例： switch(config-if)# ip ospf hello-interval 30	このインターフェイスの hello 間隔を設定します。有効な範囲は 1 ~ 65535 です。デフォルトは 10 です。
ステップ 9	<b>ip ospf dead-interval</b> <i>seconds</i>  例： switch(config-if)# ip ospf dead-interval 30	このインターフェイスのデッド間隔を設定します。有効な範囲は 1 ~ 65535 です。
ステップ 10	<b>ip ospf retransmit-interval</b> <i>seconds</i>  例： switch(config-if)# ip ospf 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 11	<b>ip ospf transmit-delay</b> <i>seconds</i>  例： switch(config-if)# ip ospf transmit-delay 450 switch(config-if)#	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 12	(任意) <b>show ip ospf</b>  例： switch(config-if)# show ip ospf	OSPF に関する情報を表示します。
ステップ 13	(任意) <b>copy running-config startup-config</b>  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# configure terminal
switch(config)# router ospf 201
switch(config-router)# timers lsa-group-pacing 300
switch(config-router)# copy running-config startup-config
```

## 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。OSPFv2 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 OSPFv2 インスタンスのヘルパー モードを無効にします。OSPFv2 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だけグレースフル リスタートがサポートされるように OSPFv2 を設定します。

### 始める前に

OSPF 機能が有効にされていることを確認してください（「[OSPFv2の有効化](#)」のセクションを参照）。

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

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>router ospf instance-tag</b> 例： switch(config)# router ospf 201 switch(config-router)#	新規 OSPFv2 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	<b>graceful-restart</b> 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	(任意) <b>graceful-restart grace-period seconds</b> 例： switch(config-router)# graceful-restart grace-period 120	猶予期間を秒で設定します。指定できる範囲は 5 ~ 1800 です。デフォルトは 60 秒です。

	コマンドまたはアクション	目的
ステップ 5	(任意) <b>graceful-restart helper-disable</b> 例： switch(config-router)# graceful-restart helper-disable	ヘルパー モードを無効にします。この機能はデフォルトで有効になっています。
ステップ 6	(任意) <b>graceful-restart planned-only</b> 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) <b>show ip ospf instance-tag</b> 例： switch(config-router)# show ip ospf 201	OSPF 情報を表示します。
ステップ 8	(任意) <b>copy running-config startup-config</b> 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# configure terminal
switch(config)# router ospf 201
switch(config-router)# graceful-restart
switch(config-router)# graceful-restart grace-period 120
switch(config-router)# copy running-config startup-config
```

## OSPFv2 インスタンスの再起動

OSPFv2 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。

OSPFv2 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

	コマンドまたはアクション	目的
ステップ 1	<b>restart ospf instance-tag</b> 例 : <pre>switch(config)# restart ospf 201</pre>	OSPFv2 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 OSPFv2 の設定

複数の OSPFv2 インスタンスを作成することができます。また、複数の VRF を作成し、各 VRF で同じ OSPFv2 インスタンスまたは複数の OSPFv3 インスタンスを使用することもできます。VRF に OSPFv2 インスタンスを割り当てることができます。



- (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

OSPF 機能を有効にしてあることを確認します（「[OSPFv2の有効化](#)」の項を参照）。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>vrf context vrf-name</b> 例 : <pre>switch(config)# vrf context RemoteOfficeVRF switch(config-vrf)#</pre>	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	<b>router ospf instance-tag</b> 例 : <pre>switch(config-vrf)# router ospf 201 switch(config-router)#</pre>	新規 OSPFv2 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	<b>vrf vrf-name</b> 例 :	VRF 設定モードを開始します。

	コマンドまたはアクション	目的
	switch(config-router)# vrf RemoteOfficeVRF switch(config-router-vrf)#	
ステップ 5	(任意) <b>maximum-paths path</b>  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 OSPFv2 パスの最大数を設定します。この機能は、ロードバランシングに使用されます。
ステップ 6	<b>interface interface-type slot/port</b>  例： switch(config-router-vrf)# 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	<b>vrf member vrf-name</b>  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	<b>ip address ip-prefix/length</b>  例： switch(config-if)# ip address 192.0.2.1/16	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	<b>ip router ospf instance-tag area area-id</b>  例： switch(config-if)# ip router ospf 201 area 0	このインターフェイスを OSPFv2 インスタンスおよび設定エリアに割り当てます。
ステップ 10	(任意) <b>copy running-config startup-config</b>  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# configure terminal
switch(config)# vrf context NewVRF
switch(config)# router ospf 201
switch(config)# interface ethernet 1/2
switch(config-if)# vrf member NewVRF
switch(config-if)# ip address 192.0.2.1/16
switch(config-if)# ip router ospf 201 area 0
switch(config-if)# copy running-config startup-config
```

## OSPFv2 設定の確認

OSPFv2 設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
<code>show ip ospf [instance-tag] [vrf vrf-name]</code>	<p>1つ以上の OSPF ルーティング インスタンスに関する情報を表示します。出力には、次のエリアレベルのカウントが含まれます。</p> <ul style="list-style-type: none"> <li>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）。</li> <li>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。</li> <li>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）。</li> <li>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。</li> </ul>
<code>show ip ospf border-routers [ vrf { vrf-name   all   default   management } ]</code>	OSPFv2 境界ルータ設定を表示します。
<code>show ip ospf database [ vrf { vrf-name   all   default   management } ]</code>	OSPFv2 リンクステートデータベースの要約を表示します。
<code>show ip ospf interface number [ vrf { vrf-name   all   default   management } ]</code>	OSPFv2-related インターフェイスの情報を表示します。
<code>show ip ospf lsa-content-changed-list neighbor-id interface - type number [ vrf { vrf-name   all   default   management } ]</code>	変更された OSPFv2 LSA を表示します。
<code>show ip ospf neighbors [ neighbor-id ] [ detail ] [ interface - type number ] [ vrf { vrf-name   all   default   management } ] [ summary ]</code>	OSPFv2 ネイバーの一覧を表示します。
<code>show ip ospf request-list neighbor-id interface - type number [ vrf { vrf-name   all   default   management } ]</code>	OSPFv2 リンクステート要求の一覧を表示します。

コマンド	目的
<code>show ip ospf retransmission-list neighbor-id interface - type number [ vrf { vrf-name   all   default   management }]</code>	OSPFv2 リンクステート再送の一覧を表示します。
<code>show ip ospf route [ ospf-route ] [ summary ] [ vrf { vrf-name   all   default   management }]</code>	内部 OSPFv2 ルートを表示します。
<code>show ip ospf summary-address [ vrf { vrf-name   all   default   management }]</code>	OSPFv2 サマリアドレスに関する情報を表示します。
<code>show ip ospf virtual-links [ brief ] [ vrf { vrf-name   all   default   management }]</code>	OSPFv2 仮想リンクに関する情報を表示します。
<code>show ip ospf vrf { vrf-name   all   default   management }</code>	VRF ベースの OSPFv2 設定に関する情報を表示します。
<code>show running-configuration ospf</code>	現在実行中の OSPFv2 設定を表示します。

## OSPFv2 のモニタリング

OSPFv2 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
<code>show ip ospf policy statistics area area-id filter list {in   out} [vrf {vrf-name   all   default   management}]</code>	エリアの OSPFv2 ルート ポリシー統計情報を表示します。
<code>show ip policy statistics redistribute {bgp id   direct   eigrp id   isis id   ospf id   rip id   static} [vrf {vrf-name   all   default   management}]</code>	OSPFv2 ルート ポリシー統計情報を表示します。
<code>show ip ospf statistics [vrf {vrf-name   all   default   management}]</code>	OSPFv2 イベントカウンタを表示します。
<code>show ip ospf traffic [interface-type number] [vrf {vrf-name   all   default   management}]</code>	OSPFv2 パケットカウンタを表示します。

## OSPFv2 の設定例

次に、OSPFv2 を設定する例を示します。

```
feature ospf
router ospf 201
  router-id 290.0.2.1
interface ethernet 1/2
  ip router ospf 201 area 0.0.0.10
```



```
ip ospf authentication
ip ospf authentication-key 0 mypass
```

## OSPF RFC 互換モードの例

次に、RFC 1583 互換ルータと互換性を持つように OSPF を設定する例を示します。



- (注) RFC1583 互換の OSPF のみを実行するルータに接続するすべての VRF で、RFC 1583 の互換性を設定する必要があります。

```
switch# configure terminal
switch(config)# feature ospf
switch(config)# router ospf Test1
switch(config-router)# rfc1583compatibility
switch(config-router)# vrf A
switch(config-router-vrf)# rfc1583compatibility
```

## 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。

## OSPFv2 の関連資料

関連項目	マニュアル タイトル
キーチェーン	<a href="#">『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』</a>
IPv6 ネットワーク向け OSPFv3	<a href="#">OSPFv3 の設定</a>
ルート マップ	<a href="#">Route Policy Manager の設定</a>

## MIB

MIB	MIB のリンク
OSPFv2 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。 <a href="ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html">ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html</a>



## 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。