OSPFv3 の実装

「*OSPFv3 の実装*」のモジュールでは、Open Shortest Path First version 3（OSPFv3）が拡張され、IPv6 ルーティング プレフィクスのサポートが提供されています。

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「OSPFv3 の実装の機能情報」（P.52）を参照してください。

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

目次

OSPFv3 の実装の前提条件

インターフェイスで OSPFv3 をイネーブルにする前に、次の操作を実行する必要があります。

- OSPFv3 ネットワーク戦略と、IPv6 ネットワークのプランニングを完成させる。たとえば、複数のエリアが必要かどうかを決定する必要があります。
- IPv6 ユニキャスト ルーティングをイネーブルにする。
- インターフェイスで IPv6 をイネーブルにする。
- 認証および暗号化をイネーブルにするために、OSPFv3 に対して IP Security（IPsec; IP セキュリティ）セキュア ソケット Application Program Interface（API; アプリケーション プログラム インターフェイス）を設定する。
- OSPFv3 で IPv4 ユニキャスト Address Family（AF; アドレス ファミリ）を使用するには、リンクが IPv6 ユニキャスト AF に参加していない場合でも、リンクで IPv6 をイネーブルにする必要があります。
- OSPFv3 アドレス ファミリ機能を使用すると、ユーザはインターフェイスごとに 2 つのルータ プロセスを持つことはできますが、AF ごとに持てるプロセスは 1 つだけです。AF が IPv4 の場合は、最初に IPv4 アドレスをインターフェイス上で設定する必要がありますが、そのインターフェイスで IPv6 をイネーブルにする必要があります。

OSPFv3 の実装の制約事項

- OSPF バージョン 2 for IPv4 および OSPFv3 を使用してデュアルスタック IP ネットワークを実行している場合、OSPFv3 のイネーブル化に使用するコマンドのデフォルトを変更する際は、注意してください。これらのデフォルトを変更すると、OSPFv3 ネットワークに悪影響を及ぼすことがあります。
- 認証は、Cisco IOS Release 12.3(4)T 以降でサポートされています。
- ESP 認証および暗号化は、Cisco IOS Release 12.4(9)T 以降でサポートされています。
- あるルータ上のインターフェイスで見つかった IPv6 アドレスから発信されたパケットは、そのルータ上では拒否されます。

OSPFv3 の実装について

OSPFv3 の機能

OSPF は、IP 用のルーティング プロトコルです。OSPF は、距離ベクトル型プロトコルではなく、リンクステート型プロトコルです。リンクを、ネットワーキング デバイス上のインターフェイスとして考えます。リンクステート型プロトコルは、送信元マシンと宛先マシンを接続するリンクのステートに基づいて、ルーティングの決定を行います。リンク ステートは、インターフェイスと、その隣接ネットワーキング デバイスとの関係を説明するものです。インターフェイス情報には、インターフェイスの IPv6 プレフィクス、ネットワーク マスク、接続先のネットワークのタイプ、そのネットワークに接続されているルータなどが含まれます。この情報は、さまざまなタイプの Link-State Advertisement（LSA; リンクステート アドバタイズメント）で伝播されます。

ルータの LSA データの集まりは、リンクステート データベースに格納されます。ダイクストラ アルゴリズムが採用されている場合、データベースの内容に基づいて OSPF ルーティング テーブルが作成されます。データベースとルーティング テーブルの違いは、データベースには raw データの完全な集まりが含まれるのに対し、ルーティング テーブルには特定のルータ インターフェイス ポートを経由する既知の宛先への最短パスのリストが含まれることです。

OSPF バージョン 3 は、RFC 5340 に説明されているように、IPv6 および IPv4 ユニキャスト AF をサポートしています。

OSPF バージョン 3 と OSPF バージョン 2 の比較

OSPF バージョン 3 は、OSPF バージョン 2 とほぼ同じです。RFC 5340 に説明されているように、OSPFv3 では、OSPF バージョン 2 が拡張され、IPv6 ルーティング プレフィクスと、より大きなサイズの IPv6 アドレスに対するサポートが提供されています。

OSPFv3 では、ルーティング プロセスを明示的に作成する必要はありません。インターフェイスで OSPFv3 をイネーブルにすると、ルーティング プロセス（およびその関連設定）が作成されます。

OSPFv3 では、各インターフェイスはインターフェイス コンフィギュレーション モードでコマンドを使用してイネーブルにする必要があります。この機能は、ルータ コンフィギュレーション モードを使用してインターフェイスが間接的にイネーブルになる OSPF バージョン 2 とは異なっています。

OSPFv3 で NonBroadcast MultiAccess（NBMA; 非ブロードキャスト マルチアクセス）インターフェイスを使用する場合、ユーザはネイバー リストを使用してルータを手動で設定する必要があります。ネイバー ルータは、それぞれのルータ ID によって識別されます。

IPv6 では、ユーザは 1 つのインターフェイス上に多数のアドレス プレフィクスを設定できます。OSPFv3 には、デフォルトで、1 つのインターフェイス上のすべてのアドレス プレフィクスが組み込まれます。ユーザは一部のアドレス プレフィクスを選択して OSPFv3 にインポートはできません。1 つのインターフェイス上のすべてのアドレス プレフィクスをインポートするか、1 つのインターフェイス上のアドレス プレフィクスを一切インポートしないかのいずれかになります。

OSPF バージョン 2 とは異なり、1 つのリンクで OSPFv3 の複数のインスタンスを実行できます。

OSPF では、自動的にループバック インターフェイスが他よりも優先されます。また、すべてのループバック インターフェイスの中で最も高位の IP アドレスが選択されます。ループバック インターフェイスが存在しない場合、ルータ内で最も高位の IP アドレスが選択されます。特定のインターフェイスを使用するように OSPF に指示することはできません。

OSPFv3 アドレス ファミリ

OSPFv3 アドレス ファミリ機能では、IPv4 および IPv6 ユニキャスト トラフィックの両方がサポートされます。この機能を使用して、ユーザはインターフェイスごとに 2 つのルータ プロセスを持つことはできますが、AF ごとに持てるプロセスは 1 つだけです。IPv4 AF を使用する場合は、最初に IPv4 アドレスをインターフェイス上で設定する必要がありますが、そのインターフェイスで IPv6 をイネーブルにする必要があります。同一のインターフェイス上での、1 つの IPv4 または IPv6 OSPFv3 プロセスによる複数のインスタンスの実行はサポートされていません。

OSPFv3 を使用する IPv6 ネットワークを IGP としているユーザは、同一の IGP を IPv4 ルートの伝送およびインストールに役立てることもできます。このネットワークのすべてのルートには、IPv6 転送スタックがあります。このネットワークの一部（またはすべて）のリンクでは、IPv4 転送の実行および IPv4 アドレスの設定が可能です。IPv4 スタティックまたはダイナミック ルーティング プロトコルを実行しているエッジの周辺には、IPv4 専用ルータのポケットが存在します。このような場合は、ユーザはトンネリング オーバーヘッドを使用せずに、これらのポケット間で IPv4 トラフィックを転送する機能が必要になります。つまり、すべての IPv4 中継ルータが IPv4 および IPv6 両方の転送スタック（たとえばデュアル スタック）を持つことになります。

この機能を使用すると、IPv4 AF 用に別々の（異なる）トポロジを構築できます。この機能により Pv4 ルートが IPv4 RIB にインストールされた後、ネイティブで転送が行われます。OSPFv3 プロセスでは IPv4 AF トポロジがフル サポートされており、ルートをその他のすべての IPv4 ルーティング プロトコルから再配布したり、その他のすべての IPv4 ルーティング プロトコルに再配布したりできます。

OSPFv3 プロセスは、IPv4 または IPv6 のいずれにも設定できます。**address-family** コマンドは、どの AF を OSPFv3 プロセスで実行するかを決定するために使用されます。また、インスタンスごとに設定できるアドレス ファミリは 1 つだけです。AF を選択したら、ユーザはリンク上で複数のインスタンスをイネーブルにして、アドレス ファミリ固有のコマンドをイネーブルにできます。

各 AF には、異なるインスタンス ID 範囲が使用されます。各 AF は異なる隣接関係を確立し、異なるリンク ステート データベースを持ち、異なる最短パス ツリーを計算します。その後、AF は AF 固有の RIB にルートをインストールします。IPv6 ユニキャスト プレフィクスを伝送する LSA は、異なるインスタンス内で変更されることなく、各 AF のプレフィクスを伝送します。

OSPFv3 をイネーブルにしたインターフェイスに設定されている IPv4 サブネットは、IPv6 プレフィクスと同様に、エリア内プレフィクス LSA を介してアドバタイズされます。外部 LSA は、任意の IPv4 ルーティング プロトコル（接続およびスタティックを含む）から再配布された IPv4 ルートのアドバタイズに使用されます。IPv4 OSPFv3 プロセスは SPF 計算を実行して、IPv4 宛先への最短パスを検出します。計算されたこれらのルートは、その後 IPv4 RIB に挿入されます（IPv6 AF の場合、計算されたルートは IPv6 RIB に挿入されます）。

IPv4 OSPFv3 プロセスは一意の pdbindex を IPv4 RIB に割り当てるため、その他すべての IPv4 ルーティング プロトコルからルートを再配布できます。すべてのプロトコルの解析チェーンは同一であるため、IPv4 ルーティング プロトコルに **ospfv3** キーワードを追加すると、どの IPv4 ルーティング プロトコルから使用した場合でも、**redistribute** コマンドに OSPFv3 が表示されます。**ospfv3** キーワードを使用すると、**redistribute ospfv3** コマンドで定義されているように、IPv4 OSPFv3 ルートをその他すべての IPv4 ルーティング プロトコルに再配布できます。

OSPFv3 アドレス ファミリ機能は、Cisco IOS Release 15.1(3)S および Cisco IOS Release 15.2(1)T でサポートされています。これらのリリースよりも古いソフトウェアを実行する Cisco ルータおよびサードパーティ ルータは、AF ビットを設定しないため、IPv4 AF の AF 機能を実行するルータとは隣接できません。そのため、これらのルータは IPv4 AF SPF 計算には参加せず、IPv6 RIB に IPv4 OSPFv3 ルートをインストールすることはありません。

OSPFv3 の LSA タイプ

次に、それぞれ用途の異なる LSA タイプを示します。

- ルータ LSA（タイプ 1）：エリアへのルータのリンクのリンク ステートとコストが説明されます。これらの LSA は、エリア内部でだけフラッディングされます。この LSA は、ルータが Area Border Router（ABR; エリア境界ルータ）か Autonomous System Boundary Router（ASBR; 自律システム境界ルータ）か、およびそのルータが仮想リンクの一端であるかどうかを示します。また、タイプ 1 の LSA は、スタブ ネットワークへのアドバタイズにも使用されます。OSPFv3 では、これらの LSA はアドレス情報を持たず、ネットワークプロトコルに依存しません。OSPFv3 では、ルータ インターフェイス情報は複数のルータ LSA にわたって拡散する場合があります。受信者は、SPF 計算の実行時に、特定のルータから発信されたすべてのルータ LSA を連結する必要があります。
- ネットワーク LSA（タイプ 2）：ネットワークに接続されているすべてのルータのリンクステートおよびコスト情報が説明されます。この LSA は、ネットワーク内のすべてのリンクステートおよびコスト情報を集約したものです。代表ルータだけがこの情報を追跡し、ネットワーク LSA を生成できます。OSPFv3 では、ネットワーク LSA はアドレス情報を持たず、ネットワークプロトコルに依存しません。
- ABR のエリア間プレフィクス LSA（タイプ 3）：他のエリア内のルータ（エリア間ルート）に内部ネットワークがアドバタイズされます。タイプ 3 の LSA は、単一のネットワークを表すことも、1 つのアドバタイズメントとして集約された一連のネットワークを表すこともあります。集約 LSA を生成するのは、ABR だけです。OSPFv3 では、これらの LSA のアドレスは *address*, *mask* ではなく *prefix*, *prefix length* で表されます。デフォルト ルートは、長さが 0 のプレフィクスとして表現されます。
- ASBR のエリア間ルータ LSA（タイプ 4）：ASBR のロケーションがアドバタイズされます。外部ネットワークにアクセスしようとするルータは、これらのアドバタイズメントを使用して、ネクストホップへの最良パスを決定します。タイプ 4 LSA は、ASBR の代わりに ABR により生成されます。
- 自律システム外部 LSA（タイプ 5）：別の AS からルートを再配布します。通常は、別のルーティング プロトコルから OSPFv3 に再配布します。OSPFv3 では、これらの LSA のアドレスは *address*, *mask* ではなく *prefix*, *prefix length* で表されます。デフォルト ルートは、長さが 0 のプレフィクスとして表現されます。
- リンク LSA（タイプ 8）：ローカルリンク フラッディング スコープを持ちます。関連付けられているリンクを越えてフラッディングされることはありません。リンク LSA は、リンクに接続されている他のすべてのルータに対してルータのリンクローカル アドレスを提供し、リンクに接続されている他のルータに、そのリンクに関連付けるプレフィクスのリストを通知します。また、ルータが Options ビットの集まりをアサートして、リンクの起点となるネットワーク LSA と関連付けできるようにします。
- エリア内プレフィクス LSA（タイプ 9）：ルータは、ルータまたは中継ネットワークごとに、それぞれ固有のリンクステート ID を持つ複数のエリア内プレフィクス LSA を発信できます。各エリア内プレフィクス LSA のリンクステート ID は、ルータ LSA またはネットワーク LSA とのアソシエーションを説明するもので、スタブおよび中継ネットワークのプレフィクスを含んでいます。

新しく定義された LSA のほとんどすべてに、アドレス プレフィクスが存在します。プレフィクスは、PrefixLength、PrefixOptions、および Address Prefix の 3 つのフィールドで表現されます。OSPFv3 では、これらの LSA のアドレスは *address*, *mask* ではなく *prefix*, *prefix length* で表されます。デフォルト ルートは、長さが 0 のプレフィクスとして表現されます。タイプ 3 およびタイプ 9 LSA は、すべてのプレフィクス（サブネット）情報を伝送します。これは、OSPFv2 ではルータ LSA およびネットワーク LSA に含まれます。特定の LSA（ルータ LSA、ネットワーク LSA、エリア間ルータ LSA、およびリンク LSA）の Options フィールドは、OSPFv3 をサポートするために 24 ビットに拡張されています。

OSPFv3 では、エリア間プレフィクス LSA、エリア間ルータ LSA、および自律システム外部 LSA のリンクステート ID の機能は、リンクステート データベースの個々の部分を識別することだけです。OSPF バージョン 2 ではリンクステート ID で表されたアドレスまたはルータ ID はすべて、OSPFv3 では LSA の本体で伝送されます。

ネットワーク LSA およびリンク LSA のリンクステート ID は常に、説明されているリンク上の送信元ルータのインターフェイス ID となります。このため、ネットワーク LSA およびリンク LSA は、サイズ制限ができない LSA だけになりました。ネットワーク LSA は、リンクに接続されているすべてのルータをリストする必要があります。リンク LSA は、リンクのルータのアドレス プレフィクスのすべてをリストする必要があります。

OSPFv3 の NBMA

NBMA ネットワークでは、Designated Router（DR; 代表ルータ）または Backup DR（BDR）が LSA フラッディングを実行します。ポイントツーポイントネットワークでは、フラッディングはインターフェイスからネイバーに直接送信されるだけです。

共通セグメントを共有するルータ（2 つのインターフェイス間のレイヤ 2 リンク）は、そのセグメント上でネイバー同士となります。OSPFv3 は、Hello プロトコルを使用して、各インターフェイスから定期的に hello パケットを送信します。ルータがネイバーの Hello パケット内に自身がリストされていることを認識すると、それらのルータはネイバー同士となります。2 つのルータがネイバーになると、データベースの交換や同期化を行うことができるようになります。これにより、隣接が作成されます。すべてのネイバー ルータが隣接を持っているわけではありません。

ポイントツーポイント ネットワークおよびポイントツーマルチポイント ネットワーク上では、ソフトウェアによってルーティング アップデートがすぐ隣のネイバーにフラッディングされます。DR も BDR もないため、すべてのルーティング情報が各ネットワーキング デバイスにフラッディングされます。

ブロードキャストまたは NBMA セグメント上でのみ、OSPFv3 は、1 つのルータを DR に、もう 1 つのルータを BDR に選択することで、セグメント上で交換される情報量を最小化します。このため、セグメント上の各ルータには、情報交換のための中央接続ポイントがあります。各ルータは、セグメント上の他のルータそれぞれとルーティング アップデートを交換するのではなく、DR および BDR と情報を交換します。DR および BDR は、情報を他のルータに中継します。

ソフトウェアによってセグメント上の各ルータのプライオリティが確認され、DR および BDR となるルータが決定されます。最も高いプライオリティのルータが DR として選択されます。プライオリティが同じ場合、より高位のルータ ID を持つルータが優先されます。DR が選択されると、BDR が同様の方法で選択されます。プライオリティが 0 に設定されているルータは、DR または BDR になる資格がありません。

OSPFv3 で NBMA を使用する場合は、自動的にネイバーを検出できません。NBMA インターフェイスで、インターフェイス コンフィギュレーション モードを使用して、手動でネイバーを設定する必要があります。

OSPFv3 Max-Metric ルータ LSA

OSPFv3 Max-Metric ルータ LSA 機能により、OSPFv3 はローカルで生成されたルータ LSA を最大メトリックでアドバタイズできるようになります。この機能を使用すると OSPFv3 プロセスはルータを通過する中継トラフィックをコンバージできるようになりますが、より適切な代替パスが存在する場合は、中継トラフィックを引き込むことはできません。指定したタイムアウトまたは BGP からの通知の後、OSPFv3 は通常のメトリックで LSA をアドバタイズします。

Max-Metric LSA 制御では、LSA アドバタイズメントの使用により OSPFv3 ルータがスタブ ルータ ロールになります。スタブ ルータは、直接接続されたリンクを宛先とするパケットのみを転送します。OSPFv3 ネットワークでは、ルータが接続しているリンクに対して大きなメトリックをアドバタイズすると、このルータを通るパスのコストは代替パスのコストよりも大きくなり、このルータはスタブ ルータになる場合があります。OSPFv3 スタブ ルータ アドバタイズメントを使用すると、ルータは、ルータ LSA 内の接続しているリンクに対して無限メトリック（0xFFFF）をアドバタイズできます。また、リンクがスタブ ネットワークの場合は、通常のインターフェイス コストをアドバタイズします。

OSPFv3 の強制的な SPF

clear ipv6 ospf コマンドとともに **process** キーワードが使用されている場合、OSPFv3 データベースのクリアおよび再入力の後に、SPF アルゴリズムが実行されます。**clear ipv6 ospf** コマンドとともに **force-spf** キーワードが使用されている場合、SPF アルゴリズムの実行前に OSPFv3 データベースはクリアされません。

高速コンバージェンス - LSA および SPF スロットリング

OSPFv3 の LSA および SPF スロットリング機能は、ネットワークが不安定な間、OSPFv3 でのリンク ステート アドバタイズメント アップデートを低速化するためのダイナミック メカニズムを提供します。さらに LSA のレート制限をミリ秒単位で指定することにより、OSPFv3 コンバージェンス時間の短縮が可能になります。

以前は、OSPFv3 はレート制限 SPF 計算および LSA 生成にスタティック タイマーを使用しました。これらのタイマーを設定することもできますが、使用する値は秒単位で指定するため、OSPFv3 コンバージェンスに制限が課せられます。LSA および SPF スロットリングは、すばやく応答できる高度な SPF および LSA レート制限メカニズムを提供することにより、1 秒未満単位でのコンバージェンスを実現し、長引く不安定期間中にも安定性および保護を提供します。

OSPFv3 でのロード バランシング

ルータは、複数のルーティング プロセス（またはルーティング プロトコル）を介して特定のネットワークへの複数のルートを認識すると、最短の管理ディスタンスを持つルートをルーティング テーブルにインストールします。同じ管理ディスタンスを持つ同じルーティング プロセスを介して認識された多数のルートから、1 つのルートを選択する必要があることもあります。この場合、ルータは宛先へのコスト（またはメトリック）が最小のパスを選択します。各ルーティング プロセスにより、そのコストが別々に計算されます。また、ロード バランシングを実現するために、コストを操作する必要がある場合もあります。

OSPFv3 では、次の方法でロード バランシングが自動的に実行されます。OSPFv3 により、複数のインターフェイスを通って宛先に到達できること、および各パスのコストが同じであることが検出された場合は、ルーティング テーブルに各パスがインストールされます。同じ宛先へのパスの数は、**maximum-paths** コマンドを指定しないかぎり制限されません。デフォルトの最大パスは 16 です。有効範囲は 1 ～ 64 です。

OSPFv3 へのアドレスのインポート

OSPFv3 が実行されているインターフェイスで指定されているアドレス セットを OSPFv3 にインポートする場合は、ユーザは特定のアドレスを選択してインポートはできません。すべてのアドレスがインポートされるか、いずれのアドレスもインポートされないかのどちらかです。

OSPFv3 のカスタマイゼーション

ネットワークに合わせて OSPFv3 をカスタマイズできますが、多くの場合、その必要はありません。OSPFv3 のデフォルトは、ほとんどのカスタマーや機能の要件を満たすように設定されています。デフォルトを変更する必要がある場合は、IPv6 コマンド リファレンスを参照して、適切な構文を確認してください。

注意 デフォルトを変更する際は、注意してください。デフォルトを変更すると、OSPFv3 ネットワークに悪影響を及ぼすことがあります。

IPsec を使用した OSPFv3 認証サポート

OSPFv3 パケットが変更されてルータに再送信されることにより、ルータが管理者にとって望ましくない動作をすることにならないように、OSPFv3 パケットを認証する必要があります。OSPFv3 は、IP Security（IPsec; IP セキュリティ）セキュア ソケット Application Program Interface（API; アプリケーション プログラム インターフェイス）を使用して OSPFv3 パケットに認証を追加します。この API は、IPv6 をサポートするように拡張されています。

OSPFv3 では、認証をイネーブルにするために IPsec を使用する必要があります。OSPFv3 で使用するために必要な IPsec API は暗号イメージのみに含まれるため、認証を使用するには暗号イメージが必要です。

OSPFv3 では、認証フィールドが OSPFv3 パケット ヘッダーから削除されています。IPv6 で OSPFv3 を実行する場合、ルーティング変更の整合性、認証、および機密性を確保するために、OSPFv3 には IPv6 Authentication Header（AH; 認証ヘッダー）または IPv6 ESP ヘッダーが必要です。IPv6 AH および ESP 拡張ヘッダーを使用すると、OSPFv3 に認証および機密性を提供できます。

IPsec AH を使用するには、**ipv6 ospf authentication** コマンドをイネーブルにする必要があります。IPsec ESP を使用するには、**ipv6 ospf encryption** コマンドをイネーブルにする必要があります。ESP ヘッダーは、単独で適用することも、AH と組み合せて適用することもできます。ESP を使用した場合、暗号化と認証の両方が提供されます。セキュリティ サービスは、通信する 1 組のホスト、通信する 1 組のセキュリティ ゲートウェイ、またはセキュリティ ゲートウェイとホストの間に提供できます。

IPsec を設定するために、ユーザはセキュリティ ポリシーを設定できます。これは、Security Policy Index（SPI）とキーの組み合せです（このキーはハッシュ値の作成および検証に使用されます）。OSPFv3 の IPsec は、インターフェイスまたは OSPFv3 エリアに対して設定できます。セキュリティを強化するには、ユーザは、IPsec を設定する各インターフェイスで異なるポリシーを設定する必要があります。ユーザが OSPFv3 エリアに対して IPsec を設定した場合、ポリシーはそのエリア内のすべてのインターフェイス（IPsec が直接設定されているインターフェイスを除く）に適用されます。いったん OSPFv3 に対して IPsec を設定すると、IPsec はユーザからは見えなくなります。

トラフィックを保護するために、アプリケーションによりセキュア ソケット API が使用されます。この API によって、アプリケーションによるセキュア ソケットのオープン、リッスン、およびクローズを許可する必要があります。また、アプリケーションと Secure Socket Layer の間のバインディングにより、Secure Socket Layer は、接続のオープンやイベントのクローズなど、ソケットへの変更をアプリケーションに通知できます。セキュア ソケット API は、ソケットを識別できます。つまり、セキュリティを必要とするトラフィックを伝送するローカルおよびリモートのアドレス、マスク、ポート、およびプロトコルを識別できます。

各インターフェイスのセキュア ソケット ステートは、次のいずれかになります。

- NULL：エリアに対して認証が設定されていれば、インターフェイスに対してセキュア ソケットを作成しません。

- DOWN：インターフェイス（またはインターフェイスが含まれるエリア）に対して IPsec は設定されていますが、OSPFv3 がこのインターフェイスに対するセキュア ソケットの作成を IPsec に要求していないか、またはエラー条件が存在します。
- GOING UP：OSPFv3 はセキュア ソケットを IPsec に要求し、IPsec からの CRYPTO_SS_SOCKET_UP メッセージを待っています。
- UP：OSPFv3 は IPsec から CRYPTO_SS_SOCKET_UP メッセージを受信しました。
- CLOSING：インターフェイスのセキュア ソケットはクローズされています。インターフェイスに対して新しいソケットがオープンされることがあります。この場合、現在のセキュア ソケットは DOWN ステートに移行します。オープンされない場合、インターフェイスは UNCONFIGURED となります。
- UNCONFIGURED：インターフェイス上に認証は設定されていません。

DOWN 状態の間は、OSPFv3 はパケットを受け入れたり、送信したりすることはありません。

IPsec の詳細については、「*IPv6 セキュリティへの IPsec の実装*」を参照してください。

OSPFv3 仮想リンク

仮想リンクごとに、マスター セキュリティ情報データブロックが作成されます。各インターフェイスでセキュア ソケットをオープンする必要があるため、トランジット エリア内のインターフェイスごとに、対応するセキュリティ情報データブロックが存在することになります。セキュア ソケット ステートは、インターフェイスのセキュリティ情報データブロック内に保持されます。マスター セキュリティ情報データブロック内のステート フィールドは、仮想リンクに対してオープンされたすべてのセキュア ソケットのステータスを反映しています。すべてのセキュア ソケットが UP の場合、仮想リンクのセキュリティ ステートは UP に設定されます。

IPsec が設定された仮想リンク上を送信されるパケットは、事前に決定された送信元アドレスと宛先アドレスを使用する必要があります。エリアのルータのエリア内プレフィクス LSA で見つかった最初のローカル エリア アドレスが、送信元アドレスとして使用されます。この送信元アドレスはエリア データ構造で保存され、セキュア ソケットがオープンされ、パケットが仮想リンク上を送信されるときに使用されます。送信元アドレスが選択されるまで、仮想リンクはポイントツーポイント ステートに移行しません。また、送信元アドレスまたは宛先アドレスが変更された場合は、以前のセキュア ソケットをクローズして、新しいセキュア ソケットをオープンする必要があります。

（注） IPv4 AF では、仮想リンクはサポートされていません。

OSPFv3 コスト計算

コスト コンポーネントは急速に変更される可能性があるため、変更量を抑えてネットワーク全体の変動を小さくする必要があることがあります。S2、S3、および S4 の推奨値は、ネットワークの変更率を抑えるためのネットワーク シミュレーションに基づいています。S1 の推奨値は 0 です。この変数がルート コスト計算から除外されるようにするためです。

全体のリンク コストは、図 1 に示した式を使用して計算されます。

図 1　　全体のリンク コストの式

$$\text{LinkCost} = \text{OC} + \text{BW}\left(\frac{\text{Throughput\_weight}}{100}\right) + \text{Resources}\left(\frac{\text{Resources\_weight}}{100}\right) + \text{Latency}\left(\frac{\text{Latency\_weight}}{100}\right) + \text{L2\_factor}\left(\frac{\text{L2\_weight}}{100}\right)$$

$$\text{OC} = \left[\frac{(\text{ospf\_reference\_bw})}{(\text{MDR})(1000)}\right] \qquad \boxed{\text{ospf\_reference\_bw} = 10 \wedge 8}$$

$$\text{BW} = \frac{(65535)\left(100 - \frac{\text{CDR}}{\text{MDR}}(100)\right)}{100}$$

$$\text{Resources} = \frac{(100 - \text{resources})^3\,(65535)}{1000000}$$

$$\text{Latency} = \text{latency}$$

$$\text{L2\_factor} = \frac{(100 - \text{RLQ})(65535)}{100}$$

231048

表 1 に、OSPFv3 コスト計算で使用される記号を定義します。

表 1　　OSPFv3 コスト計算の定義

コスト コンポーネント	コンポーネント定義
OC	reference_bw/(MDR*1000) の式（ここで、reference_bw=10^8）を使用して参照帯域幅から計算される「デフォルトの OSPFv3 コスト」。
A ～ D	ラジオ固有のデータベースのさまざまな式。0 ～ 64,000 の範囲の結果が生成されます。
A	CDR 関連および MDR 関連の式： (2^16 * (100 – (CDR * 100 / MDR)))/100
B	リソース関連の式： ((100 – RESOURCES)^3 * 2^16 / 10^6)
C	ラジオにより報告される遅延。報告される時点で、すでに 0 ～ 64K の範囲です（LATENCY）。
D	RLF 関連の式： ((100 – RLF) * 2^16)/100
S1 ～ S4	Command-Line Interface（CLI; コマンドライン インターフェイス）からのスカラ重み付け係数入力。これらのスカラは、A ～ D により計算された値を縮小します。 0 の値は、あるコンポーネントに対して 0 ～ 64,000 の全範囲をディセーブルにし、100 の値はイネーブルにします。

各ネットワークに固有の特性があり、実際のネットワーク パフォーマンスを最適化するために異なる設定が必要となることもあるため、これらの推奨値は、OSPFv3 ネットワークを最適化するための開始点として捉えてください。表 2 に、OSPFv3 コスト メトリックの推奨値設定を示します。

表 2　OSPFv3 コスト メトリックの推奨値設定

設定	メトリックの説明	デフォルト値	推奨値
S1	ipv6 ospf dynamic weight throughout	100	0
S2	ipv6 ospf dynamic weight resources	100	29
S3	ipv6 ospf dynamic weight latency	100	29
S4	ipv6 ospf dynamic weight L2 factor	100	29

次のリストで示すように、この式を使用してデフォルトのパス コストが計算されています。これらの値が使用しているネットワークに適していない場合は、独自のパス コストの計算方法を使用できます。

- 56-kbps シリアル リンク：デフォルトのコストは 1785 です。
- 64-kbps シリアル リンク：デフォルトのコストは 1562 です。
- T1（1.544-Mbps シリアル リンク）：デフォルトのコストは 64 です。
- E1（2.048-Mbps シリアル リンク）：デフォルトのコストは 48 です。
- 4-Mbps トークン リング：デフォルトのコストは 25 です。
- イーサネット：デフォルトのコストは 10 です。
- 16-Mbps トークン リング：デフォルトのコストは 6 です。
- FDDI：デフォルトのコストは 1 です。
- X25：デフォルトのコストは 5208 です。
- 非同期：デフォルトのコストは 10,000 です。
- ATM：デフォルトのコストは 1 です。

これらの設定を示すために、ここでは、VMI インターフェイスに対して OSPFv3 コスト メトリックを定義する例を示します。

```
interface vmi1
 ipv6 ospf cost dynamic weight throughput 0
 ipv6 ospf cost dynamic weight resources 29
 ipv6 ospf cost dynamic weight latency 29
 ipv6 ospf cost dynamic weight L2-factor 29
```

OSPFv3 外部パス プリファレンス オプション

RFC 5340 に従い、ASBR または転送アドレスに複数の AS 内パスを使用できる場合、どのパスが優先されるかは次のルールによって示されます。

- 非バックボーン エリアを使用するエリア内パスは、常に最優先されます。
- その他のパス（エリア内バックボーン パスおよびエリア間パス）の優先度は同等です。

これらのルールは、複数のエリアを通って ASBR に到達可能な場合、または複数存在する AS-external-LSA のいずれを優先するかを決定しようとする場合に適用されます。前者の場合、パスはすべて同じ ASBR で終端しますが、後者の場合は異なる ASBR または転送アドレスで終端します。いずれの場合も、各パスは異なるルーティング テーブルのエントリで表されます。この機能は、**no compatibility rfc1583** コマンドを使用して RFC 1583 との互換性がディセーブルに設定されている場合のみ適用されます（RFC 5340 は RFC 1583 の更新情報を提供します）。

注意 ルーティング ループが発生する可能性を最小にするため、OSPF ルーティング ドメイン内のすべての OSPF ルータで、RFC の互換性を同じ値に設定する必要があります。

OSPFv3 グレースフル リスタート

OSPFv3 でグレースフル リスタート機能を使用すると、OSPFv3 ルーティング プロトコル情報の復元中も、既知のルートを使用してノンストップ データ フォワーディングを実行できます。ルータは、再起動モード（グレースフルリスタート対応ルータなど）か、ヘルパー モード（グレースフル リスタート認識ルータなど）のいずれかで、グレースフル リスタートに参加できます。

グレースフル リスタート機能を実行するには、ルータが High Availability（HA; ハイ アベイラビリティ）Stateful Switchover（SSO; ステートフル スイッチオーバー）モード（つまり、デュアル RP）になっている必要があります。グレースフル リスタート機能を備えたルータは、次の場合に、グレースフル リスタート機能を実行します。

- Route Processor（RP; ルート プロセッサ）障害が発生し、スタンバイ RP へのスイッチオーバーが行われた場合
- スタンバイ RP への計画的な RP スイッチオーバーが行われた場合

グレースフル リスタート機能を使用するには、ネイバー ルータがグレースフルリスタート認識ルータであることが必要です。

SSO および Nonstop Forwarding（NSF; ノンストップ フォワーディング）の詳細については、「*Stateful Switchover*」および「*Cisco Nonstop Forwarding*」を参照してください。

BFD での OSPFv3 のサポート

Bidirectional Forwarding Detection（BFD; 双方向フォワーディング検出）では、OSPFv3 をサポートしています。OSPFv3 に対する BFD の設定方法については、『*Implementing Bidirectional Forwarding Detection for IPv6*』の章を参照してください。

OSPFv3 の実装方法

OSPFv3 ルータ プロセスの設定

ステップ 3 を完了し、OSPFv3 ルータ コンフィギュレーション モードを開始したら、必要に応じてこの作業の以降のステップを任意に実行して、OSPFv3 ルータ コンフィギュレーションを設定します。

この作業は、Cisco IOS Release 15.1(3)S および 15.2(1)T 以降のリリースで実行できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router ospfv3** [*process-id*]
4. **area** *area-ID* [**default-cost** | **nssa** | **stub**]
5. **auto-cost reference-bandwidth** *Mbps*
6. **bfd all-interfaces**
7. **default** {**area** *area-ID* [**range** *ipv6-prefix* | **virtual-link** *router-id*]} [**default-information originate** [**always** | **metric** | **metric-type** | **route-map**] | **distance** | **distribute-list** *prefix-list prefix-list-name* {**in** | **out**} [*interface*] | **maximum-paths** *paths* | **redistribute** *protocol* | **summary-prefix** *ipv6-prefix*]
8. **ignore lsa mospf**
9. **interface-id snmp-if-index**
10. **log-adjacency-changes** [**detail**]
11. **passive-interface** [**default** | *interface-type interface-number*]
12. **queue-depth** {**hello** | **update**} {*queue-size* | **unlimited**}
13. **router-id** {*router-id*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**router ospfv3** [*process-id*] **例：** `Router(config)# router ospfv3 1`	IPv4 または IPv6 アドレス ファミリに対して OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**area** *area-ID* [**default-cost** | **nssa** | **stub**] **例：** `Router(config-router)# area 1`	OSPFv3 エリアを設定します。
ステップ 5	**auto-cost reference-bandwidth** *Mbps* **例：** `Router(config-router)# auto-cost reference-bandwidth 1000`	IPv4 OSPFv3 プロセスで、インターフェイスのメトリックを計算する際に OSPFv3 で使用される基準値を制御します。
ステップ 6	**bfd all-interfaces** **例：** `Router(config-router)# bfd all-interfaces`	OSPFv3 ルーティング プロセスの BFD をイネーブルにします。
ステップ 7	**default** {**area** *area-ID* [**range** *ipv6-prefix* | **virtual-link** *router-id*]} [**default-information originate** [**always** | **metric** | **metric-type** | **route-map**] | **distance** | **distribute-list** *prefix-list prefix-list-name* {**in** | **out**} [*interface*] | **maximum-paths** *paths* | **redistribute** *protocol* | **summary-prefix** *ipv6-prefix*] **例：** `Router(config-router)# default area 1`	OSPFv3 パラメータをデフォルト値に戻します。
ステップ 8	**ignore lsa mospf** **例：** `Router(config-router)# ignore lsa mospf`	ルータが LSA タイプ 6 Multicast OSPFv3 パケットを受信した場合の syslog メッセージの送信を抑制します（LSA タイプ 6 Multicast OSPFv3 はサポートされていません）。
ステップ 9	**interface-id snmp-if-index** **例：** `Router(config-router)# interface-id snmp-if-index`	IPv4 および IPv6 の Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）MIB-II Interface Index（ifIndex; インターフェイス インデックス）ID 番号を使用して OSPFv3 インターフェイスを設定します。
ステップ 10	**log-adjacency-changes** [**detail**] **例：** `Router(config-router)# log-adjacency-changes`	OSPFv3 ネイバーが起動または停止したときに、ルータが syslog メッセージを送信するように設定します。
ステップ 11	**passive-interface** [**default** | *interface-type interface-number*] **例：** `Router(config-router)# passive-interface default`	IPv4 OSPFv3 プロセスを使用しているときに、インターフェイスのルーティング アップデートの送信を抑制します。

	コマンドまたはアクション	目的
ステップ 12	**queue-depth** {**hello** | **update**} {*queue-size* | **unlimited**} **例：** `Router(config-router)# queue-depth update 1500`	IPv4 OSPFv3 プロセスのキューに保持できる着信パケット数を設定します。
ステップ 13	**router-id** {*router-id*} **例：** `Router(config-router)# router-id 10.1.1.1`	固定ルータ ID を使用します。

OSPFv3 への IPv6 アドレス ファミリの設定

OSPFv3 に IPv6 アドレス ファミリを設定するには、次の作業を実行します。ステップ 4 を完了し、IPv6 アドレス ファミリ コンフィギュレーション モードを開始したら、必要に応じてこの作業の以降のステップを任意に実行して、IPv6 AF を設定します。

この作業は、Cisco IOS Release 15.1(3)S および 15.2(1)T 以降のリリースで実行できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router ospfv3** [*process-id*]
4. **address-family ipv6 unicast**
5. **area** *area-ID* **range** *ipv6-prefix*/*prefix-length*
6. **default** {**area** *area-ID* [**range** *ipv6-prefix* | **virtual-link** *router-id*]} [**default-information originate** [**always** | **metric** | **metric-type** | **route-map**] | **distance** | **distribute-list** *prefix-list prefix-list-name* {**in** | **out**} [*interface*] | **maximum-paths** *paths* | **redistribute** *protocol* | **summary-prefix** *ipv6-prefix*]
7. **default-information originate** [**always** | **metric** *metric-value* | **metric-type** *type-value* | **route-map** *map-name*]
8. **default-metric** *metric-value*
9. **distance** *distance*
10. **distribute-list prefix-list** *list-name* {**in** [*interface-type interface-number*] | **out** *routing-process* [*as-number*]}
11. **maximum-paths** *number-paths*
12. **summary-prefix** *prefix* [**not-advertise** | **tag** *tag-value*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router ospfv3** [*process-id*] **例：** `Router(config)# router ospfv3 1`	IPv4 または IPv6 アドレス ファミリに対して OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**address-family ipv6 unicast** または **address-family ipv4 unicast** **例：** `Router(config-router)# address-family ipv6 unicast` または `Router(config-router)# address-family ipv4 unicast`	OSPFv3 の IPv6 アドレス ファミリ コンフィギュレーション モードを開始します。 または OSPFv3 の IPv4 アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**area** *area-ID* **range** *ipv6-prefix*/*prefix-length* **例：** `Router(config-router-af)# area 1 range 2001:DB8:0:0::0/128`	OSPFv3 エリア パラメータを設定します。
ステップ 6	**default** {**area** *area-ID* [**range** *ipv6-prefix* | **virtual-link** *router-id*]} [**default-information originate** [**always** | **metric** | **metric-type** | **route-map**] | **distance** | **distribute-list** *prefix-list prefix-list-name* {**in** | **out**} [*interface*] | **maximum-paths** *paths* | **redistribute** *protocol* | **summary-prefix** *ipv6-prefix*] **例：** `Router(config-router-af)# default area 1`	OSPFv3 パラメータをデフォルト値に戻します。
ステップ 7	**default-information originate** [**always** | **metric** *metric-value* | **metric-type** *type-value* | **route-map** *map-name*] **例：** `Router(config-router-af)# default-information originate always metric 100 metric-type 2`	デフォルトの外部ルートをルーティング ドメインの OSPFv3 に生成します。

	コマンドまたはアクション	目的
ステップ 8	**default-metric** *metric-value* **例：** `Router(config-router-af)# default-metric 10`	OSPFv3 ルーティング プロトコルに再配布される IPv4 および IPv6 ルートのデフォルト メトリック値を設定します。
ステップ 9	**distance** *distance* **例：** `Router(config-router-af)# distance 200`	ルーティング テーブルに挿入された OSPFv3 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。
ステップ 10	**distribute-list prefix-list** *list-name* {**in** [*interface-type interface-number*] | **out** *routing-process* [*as-number*]} **例：** `Router(config-router-af)# distribute-list prefix-list PL1 in Ethernet0/0`	インターフェイス上で受信または送信される OSPFv3 ルーティング アップデートに、プレフィクス リストを適用します。
ステップ 11	**maximum-paths** *number-paths* **例：** `Router(config-router-af)# maximum-paths 4`	OSPFv3 ルーティングのプロセスでサポートできる等価コスト ルートの最大数を制御します。
ステップ 12	**summary-prefix** *prefix* [**not-advertise** | **tag** *tag-value*] **例：** `Router(config-router-af)# summary-prefix FEC0::/24`	OSPFv3 に IPv6 サマリー プレフィクスを設定します。

OSPFv3 への IPv4 アドレス ファミリの設定

OSPFv3 に IPv4 アドレス ファミリを設定するには、次の作業を実行します。ステップ 4 を完了し、IPv4 アドレス ファミリ コンフィギュレーション モードを開始したら、必要に応じてこの作業の以降のステップを任意に実行して、IPv4 AF を設定します。

この作業は、Cisco IOS Release 15.1(3)S および 15.2(1)T 以降のリリースで実行できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router ospfv3** [*process-id*]
4. **address-family ipv4 unicast**
5. **area** ***area-id*** **range** ***ip-address ip-address-mask*** [**advertise** | **not-advertise**] [**cost** ***cost***]
6. **default** {**area** *area-ID* [**range** *ipv6-prefix* | **virtual-link** *router-id*]} [**default-information originate** [**always** | **metric** | **metric-type** | **route-map**] | **distance** | **distribute-list** *prefix-list prefix-list-name* {**in** | **out**} [*interface*] | **maximum-paths** *paths* | **redistribute** *protocol* | **summary-prefix** *ipv6-prefix*]
7. **default-information originate** [**always** | **metric** *metric-value* | **metric-type** *type-value* | **route-map** *map-name*]

8. **default-metric** *metric-value*
9. **distance** *distance*
10. **distribute-list prefix-list** *list-name* {**in** [*interface-type interface-number*] | **out** *routing-process* [*as-number*]}
11. **maximum-paths** *number-paths*
12. **summary-prefix** *prefix* [**not-advertise** | **tag** *tag-value*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router ospfv3** [*process-id*] **例：** `Router(config)# router ospfv3 1`	IPv4 または IPv6 アドレス ファミリに対して OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**address-family ipv4 unicast** **例：** `Router(config-router)# address-family ipv4 unicast`	OSPFv3 の IPv4 アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**area** *area-id* **range** *ip-address ip-address-mask* [**advertise** | **not-advertise**] [**cost** *cost*] **例：** `Router(config-router-af)# area 0 range 192.168.110.0 255.255.0.0`	エリア境界でルートを統合および集約します。
ステップ 6	**default** {**area** *area-ID* [**range** *ipv6-prefix* | **virtual-link** *router-id*]} [**default-information originate** [**always** | **metric** | **metric-type** | **route-map**] | **distance** | **distribute-list** *prefix-list prefix-list-name* {**in** | **out**} [*interface*] | **maximum-paths** *paths* | **redistribute** *protocol* | **summary-prefix** *ipv6-prefix*] **例：** `Router(config-router-af)# default area 1`	OSPFv3 パラメータをデフォルト値に戻します。

	コマンドまたはアクション	目的
ステップ 7	**default-information originate** [**always** | **metric** *metric-value* | **metric-type** *type-value* | **route-map** *map-name*] **例：** `Router(config-router-af)# default-information originate always metric 100 metric-type 2`	デフォルトの外部ルートをルーティング ドメインの OSPFv3 に生成します。
ステップ 8	**default-metric** *metric-value* **例：** `Router(config-router-af)# default-metric 10`	OSPFv3 ルーティング プロトコルに再配布される IPv4 および IPv6 ルートのデフォルト メトリック値を設定します。
ステップ 9	**distance** *distance* **例：** `Router(config-router-af)# distance 200`	ルーティング テーブルに挿入された OSPFv3 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。
ステップ 10	**distribute-list prefix-list** *list-name* {**in** [*interface-type interface-number*] | **out** *routing-process* [*as-number*]} **例：** `Router(config-router-af)# distribute-list prefix-list PL1 in Ethernet0/0`	インターフェイス上で受信または送信される OSPFv3 ルーティング アップデートに、プレフィクス リストを適用します。
ステップ 11	**maximum-paths** *number-paths* **例：** `Router(config-router-af)# maximum-paths 4`	OSPFv3 ルーティングのプロセスでサポートできる等価コスト ルートの最大数を制御します。
ステップ 12	**summary-prefix** *prefix* [**not-advertise** | **tag** *tag-value*] **例：** `Router(config-router-af)# summary-prefix FEC0::/24`	OSPFv3 に IPv6 サマリー プレフィクスを設定します。

OSPFv3 へのルート再配布の設定

この作業は、Cisco IOS Release 15.1(3)S および 15.2(1)T 以降のリリースで実行できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router ospfv3** [*process-id*]
4. **address-family ipv6 unicast**

   または

   address-family ipv4 unicast

5. **redistribute** *source-protocol* [*process-id*] [*options*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router ospfv3** [*process-id*] **例：** `Router(config)# router ospfv3 1`	IPv4 または IPv6 アドレス ファミリに対して OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**address-family ipv6 unicast** または **address-family ipv4 unicast** **例：** `Router(config-router)# address-family ipv6 unicast` または `Router(config-router)# address-family ipv4 unicast`	OSPFv3 の IPv6 アドレス ファミリ コンフィギュレーション モードを開始します。 または OSPFv3 の IPv4 アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**redistribute** *source-protocol* [*process-id*] [*options*] **例：**	あるルーティング ドメインから別のルーティング ドメインへ IPv6 および IPv4 ルートを再配布します。

インターフェイスでの OSPFv3 のイネーブル化

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ospfv3** *process-id* **area** *area-ID* {**ipv4** | **ipv6**} [**instance** *instance-id*]

   または

   ipv6 ospf *process-id* **area** *area-id* [**instance** *instance-id*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface ethernet 0/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ospfv3** *process-id* **area** *area-ID* {**ipv4** | **ipv6**} [**instance** *instance-id*] または **ipv6 ospf** *process-id* **area** *area-id* [**instance** *instance-id*] **例：** `Router(config-if)# ospfv3 1 area 1 ipv4` または `Router(config-if)# ipv6 ospf 1 area 0`	IPv4 または IPv6 AF を設定したインターフェイスで OSPFv3 をイネーブルにします。 または インターフェイスで OSPFv3 をイネーブルにします。

IPv6 または IPv4 アドレス ファミリに対する OSPFv3 エリア範囲の定義

集約されたルートのコストは、集約されるルートの最高コストとなります。たとえば、次のルートが集約されるとします。

```
OI  2001:DB8:0:7::/64 [110/20]
     via FE80::A8BB:CCFF:FE00:6F00, Ethernet0/0
OI  2001:DB8:0:8::/64 [110/100]
     via FE80::A8BB:CCFF:FE00:6F00, Ethernet0/0
OI  2001:DB8:0:9::/64 [110/20]
     via FE80::A8BB:CCFF:FE00:6F00, Ethernet0/0
```

これらは、次のように 1 つの集約されたルートとなります。

```
OI  2001:DB8::/48 [110/100]
     via FE80::A8BB:CCFF:FE00:6F00, Ethernet0/0
```

この作業は、Cisco IOS Release 15.1(3)S および 15.2(1)T 以降のリリースで実行できます。

前提条件

OSPFv3 ルーティングがイネーブルであること。

手順の概要

1. **enable**
2. **configure terminal**
3. **router ospfv3** [*process-id*]
4. **address-family ipv6 unicast**

   または

   address-family ipv4 unicast
5. **area** *area-ID* **range** *ipv6-prefix*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router ospfv3** [*process-id*] **例：** `Router(config)# router ospfv3 1`	IPv4 または IPv6 アドレス ファミリに対して OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**address-family ipv6 unicast** または **address-family ipv4 unicast** **例：** `Router(config-router)# address-family ipv6 unicast` または `Router(config-router)# address-family ipv4 unicast`	OSPFv3 の IPv6 アドレス ファミリ コンフィギュレーション モードを開始します。 または OSPFv3 の IPv4 アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**area** *area-ID* **range** *ipv6-prefix* **例：** `Router(config-router-af)# area 1 range 2001:DB8:0:0::0/128`	OSPFv3 エリア パラメータを設定します。

OSPFv3 エリア範囲の定義

この作業は、Cisco IOS Release 15.1(3)S および 15.2(1)T よりも前のリリースで実行できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **area** *area-id* **range** *ipv6-prefix*/*prefix-length* [**advertise** | **not-advertise**] [**cost** *cost*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 router ospf** *process-id* **例：** `Router(config)# ipv6 router ospf 1`	OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**area** *area-id* **range** *ipv6-prefix*/*prefix-length* [**advertise** | **not-advertise**] [**cost** *cost*] **例：** `Router(config-rtr)# area 1 range 2001:DB8::/48`	エリア境界でルートを統合および集約します。

OSPFv3 への IPsec の設定

OSPFv3 を設定し、認証を決定したら、グループ内の各ルータにセキュリティ ポリシーを定義する必要があります。セキュリティ ポリシーは、キーと SPI の組み合せで構成されます。セキュリティ ポリシーを定義するには、SPI およびキーを定義する必要があります。

認証ポリシーまたは暗号化ポリシーは、インターフェイスまたは OSPFv3 エリアのいずれにも設定できます。セキュリティ ポリシーは、エリアに対して設定した場合、エリア内のすべてのインターフェイスに適用されます。セキュリティを強化する場合は、各インターフェイスで異なるポリシーを使用してください。

認証および暗号化は、仮想リンク上に設定できます。

- 「インターフェイスでの認証の定義」（P.24）
- 「インターフェイスでの暗号化の定義」（P.25）
- 「OSPFv3 エリア内の認証の定義」（P.26）
- 「OSPFv3 エリア内の暗号化の定義」（P.27）
- 「OSPFv3 エリア内の仮想リンクに対する認証および暗号化の定義」（P.28）

インターフェイスでの認証の定義

前提条件

インターフェイスに IPsec を設定する前に、そのインターフェイスに OSPFv3 を設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ospfv3 authentication** {**ipsec** *spi*} {**md5** | **sha1**} {*key-encryption-type key*} | **null**

   または

   ipv6 ospf authentication ipsec spi *spi* **md5** [*key-encryption-type* {*key* | **null**}]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface ethernet 0/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ospfv3 authentication** {**ipsec** *spi*} {**md5** | **sha1**} {*key-encryption-type key*} | **null** または **ipv6 ospf authentication ipsec spi** *spi* **md5** [*key-encryption-type* {*key* | **null**}] **例：** `Router(config-if)# ospfv3 authentication md5 0 275761340947681324733020312097 27` または `Router(config-if)# ipv6 ospf authentication ipsec spi 500 md5 1234567890abcdef1234567890abcdef`	インターフェイスに認証タイプを指定します。

インターフェイスでの暗号化の定義

前提条件

インターフェイスに IPsec を設定する前に、そのインターフェイスに OSPFv3 を設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ospfv3 encryption** {**ipsec spi** ***spi*** **esp** *encryption-algorithm* {***key-encryption-type key***} ***authentication-algorithm*** {***key-encryption-type key***} | **null**}

   または

   ipv6 ospf encryption {**ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key* | **null**}

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* **例：** `Router(config)# interface ethernet 0/0`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ospfv3 encryption** {**ipsec spi** *spi* **esp** *encryption-algorithm* {*key-encryption-type key*} *authentication-algorithm* {*key-encryption-type key*} | **null**} または **ipv6 ospf encryption** {**ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key* | **null**} **例：** `Router(config-if)# ospfv3 encryption ipsec spi 1001 esp null md5 0 275761340947681324733020312097 27` または `Router(config-if) ipv6 ospf encryption ipsec spi 1001 esp null sha1 123456789A123456789B123456789C123456789D`	インターフェイスに暗号化タイプを指定します。

OSPFv3 エリア内の認証の定義

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **area** *area-id* **authentication ipsec spi** *spi* **md5** [*key-encryption-type*] *key*

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**ipv6 router ospf** *process-id* **例：** `Router(config)# ipv6 router ospf 1`	OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**area** *area-id* **authentication ipsec spi** *spi* **md5** [*key-encryption-type*] *key* **例：** `Router(config-rtr)# area 1 authentication ipsec spi 678 md5 1234567890ABCDEF1234567890ABCDEF`	OSPFv3 エリア内の認証をイネーブルにします。

OSPFv3 エリア内の暗号化の定義

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **area** *area-id* **encryption ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 router ospf** *process-id* **例：** `Router(config)# ipv6 router ospf 1`	OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**area** *area-id* **encryption ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key* **例：** `Router(config-rtr)# area 1 encryption ipsec spi 500 esp null md5 1aaa2bbb3ccc4ddd5eee6fff7aaa8bbb`	OSPFv3 エリア内の暗号化をイネーブルにします。

OSPFv3 エリア内の仮想リンクに対する認証および暗号化の定義

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **area** *area-id* **virtual-link** *router-id* **authentication ipsec spi** *spi authentication-algorithm* [*key-encryption-type*] *key*
5. **area** *area-id* **virtual-link** *router-id* **encryption ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 router ospf** *process-id* **例：** `Router(config)# ipv6 router ospf 1`	OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**area** *area-id* **virtual-link** *router-id* **authentication ipsec spi** *spi authentication-algorithm* [*key-encryption-type*] *key* **例：** `Router(config-rtr)# area 1 virtual-link 10.0.0.1 authentication ipsec spi 940 md5 1234567890ABCDEF1234567890ABCDEF`	OSPFv3 エリア内の仮想リンクに対して認証をイネーブルにします。
ステップ 5	**area** *area-id* **virtual-link** *router-id* **encryption ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key* **例：** `Router(config-rtr)# area 1 virtual-link 10.1.0.1 hello-interval 2 dead-interval 10 encryption ipsec spi 3944 esp null sha1 123456789A123456789B123456789C123456789D`	OSPFv3 エリア内の仮想リンクに対して暗号化をイネーブルにします。

OSPFv3 への NBMA インターフェイスの設定

NBMA インターフェイスを使用するように、ネットワークの OSPFv3 をカスタマイズできます。OSPFv3 では、NBMA インターフェイス上でネイバーを自動的に検出できません。NBMA インターフェイスで、インターフェイス コンフィギュレーション モードを使用して、手動でネイバーを設定する必要があります。

前提条件

NBMA インターフェイスを設定する前に、次の作業を実行する必要があります。

- ネットワークを NBMA ネットワークとして設定する。
- 各ネイバーを識別する。

制約事項

- NBMA インターフェイスの使用時に、ネイバーを自動的に検出することはできません。NBMA インターフェイスの使用時には、ネイバーを検出するようにルータを手動で設定する必要があります。
- **ipv6 ospf neighbor** コマンドを設定するときに使用する IPv6 アドレスは、ネイバーのリンクローカル アドレスにする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **frame-relay map ipv6** *ipv6-address dlci* [**broadcast**] [**cisco**] [**ietf**] [**payload-compression** {**packet-by-packet** | **frf9 stac** [*hardware-options*] | **data-stream stac** [*hardware-options*]}]
5. **ipv6 ospf neighbor** *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**]

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 4	**frame-relay map ipv6** *ipv6-address dlci* [**broadcast**] [**cisco**] [**ietf**] [**payload-compression** {**packet-by-packet** | **frf9 stac** [*hardware-options*] | **data-stream stac** [*hardware-options*]}] **例：** `Router(config-if)# frame-relay map ipv6 FE80::A8BB:CCFF:FE00:C01 120`	宛先アドレスへの接続に使用する宛先 IPv6 アドレスと Data-Link Connection Identifier（DLCI; データリンク接続識別子）との間のマッピングを定義します。 • この例では、NBMA リンクはフレーム リレーです。他の種類の NBMA リンクに対しては、別のマッピング コマンドを使用します。
ステップ 5	**ipv6 ospf neighbor** *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**] **例：** `Router(config-if) ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01`	OSPFv3 ネイバー ルータを設定します。

OSPFv3 Max-Metric ルータ LSA の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **max-metric router-lsa** [**external-lsa** [*max-metric-value*]] [**include-stub**] [**inter-area-lsas** [*max-metric-value*]] [**on-startup** {*seconds* | **wait-for-bgp**}] [**prefix-lsa**] [**stub-prefix-lsa** [*max-metric-value*]] [**summary-lsa** [*max-metric-value*]]
5. **exit**
6. **show ospfv3** [*process-id*] [*address-family*] **max-metric**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 router ospf** *process-id* **例：** `Router(config)# ipv6 router ospf 1`	OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**max-metric router-lsa** [**external-lsa** [*max-metric-value*]] [**include-stub**] [**inter-area-lsas** [*max-metric-value*]] [**on-startup** {*seconds* | **wait-for-bgp**}] [**prefix-lsa**] [**stub-prefix-lsa** [*max-metric-value*]] [**summary-lsa** [*max-metric-value*]] **例：** `Router(config-router)# max-metric router-lsa on-startup wait-for-bgp`	OSPFv3 プロトコルを実行するルータが最大メトリックをアドバタイズするように設定して、他のルータがそのルータを SPF 計算で中継ホップとして優先しないようにします。
ステップ 5	**exit** **例：** `Router(config-router)# exit`	現在のコンフィギュレーション モードを終了します。 • このステップでは、Exit コマンドを 2 回イネーブルにして特権 EXEC モードに到達します。
ステップ 6	**show ospfv3** [*process-id*] **max-metric** **例：** `Router# show ospfv3 max-metric`	OSPFv3 最大メトリックの起点情報を表示します。

OSPFv3 高速コンバージェンスに対する LSA および SPF タイマーの調整

この作業は、Cisco IOS Release 15.1(3)S および 15.2(1)T 以降のリリースで実行できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router ospfv3** [*process-id*]
4. **timers lsa arrival** *milliseconds*
5. **timers pacing flood** *milliseconds*
6. **timers pacing lsa-group** *seconds*
7. **timers pacing retransmission** *milliseconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**router ospfv3** [*process-id*] **例：** `Router(config)# router ospfv3 1`	IPv4 または IPv6 アドレス ファミリに対して OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**timers lsa arrival** *milliseconds* **例：** `Router(config-rtr)# timers lsa arrival 300`	ソフトウェアが OSPFv3 ネイバーから同じ LSA を受け入れる最小間隔を設定します。
ステップ 5	**timers pacing flood** *milliseconds* **例：** `Router(config-rtr)# timers pacing flood 30`	LSA フラッド パケット ペーシングを設定します。
ステップ 6	**timers pacing lsa-group** *seconds* **例：** `Router(config-router)# timers pacing lsa-group 300`	OSPFv3 LSA を収集してグループ化し、リフレッシュ、チェックサム、またはエージングを行う間隔を変更します。
ステップ 7	**timers pacing retransmission** *milliseconds* **例：** `Router(config-router)# timers pacing retransmission 100`	IPv4 OSPFv3 での LSA 再送信パケット ペーシングを設定します。

OSPFv3 高速コンバージェンスに対する LSA および SPF スロットリングの設定

この作業は、Cisco IOS Release 15.1(3)S および 15.2(1)T よりも前のリリースで実行できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **timers throttle spf** *spf-start spf-hold spf-max-wait*
5. **timers throttle lsa** *start-interval hold-interval max-interval*
6. **timers lsa arrival** *milliseconds*
7. **timers pacing flood** *milliseconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 router ospf** *process-id* **例：** `Router(config)# ipv6 router ospf 1`	OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**timers throttle spf** *spf-start spf-hold spf-max-wait* **例：** `Router(config-rtr)# timers throttle spf 200 200 200`	SPF スロットリングをオンにします。
ステップ 5	**timers throttle lsa** *start-interval hold-interval max-interval* **例：** `Router(config-rtr)# timers throttle lsa 300 300 300`	OSPFv3 LSA 生成に対するレート制限値を設定します。
ステップ 6	**timers lsa arrival** *milliseconds* **例：** `Router(config-rtr)# timers lsa arrival 300`	ソフトウェアが OSPFv3 ネイバーから同じ LSA を受け入れる最小間隔を設定します。
ステップ 7	**timers pacing flood** *milliseconds* **例：** `Router(config-rtr)# timers pacing flood 30`	LSA フラッド パケット ペーシングを設定します。

イベント ロギングのイネーブル化

この作業は、Cisco IOS Release 15.1(3)S および 15.2(1)T 以降のリリースで実行できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router ospfv3** [*process-id*]
4. **address-family ipv6 unicast**

または

address-family ipv4 unicast

5. **event-log** [**one-shot** | **pause** | **size** *number-of-events*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router ospfv3** [*process-id*] **例：** `Router(config)# router ospfv3 1`	IPv4 または IPv6 アドレス ファミリに対して OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**address-family ipv6 unicast** または **address-family ipv4 unicast** **例：** `Router(config-router)# address-family ipv6 unicast` または `Router(config-router)# address-family ipv4 unicast`	OSPFv3 の IPv6 アドレス ファミリ コンフィギュレーション モードを開始します。 または OSPFv3 の IPv4 アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 5	**event-log** [**one-shot** | **pause** | **size** *number-of-events*] **例：** `Router(config-router)# event-log`	IPv4 OSPFv3 プロセスで OSPFv3 イベント ロギングをイネーブルにします。

Cisco IOS Release 15.1(3)S および 15.2(1)T よりも前のリリースでのイベント ロギングのイネーブル化

この作業は、Cisco IOS Release 15.1(3)S および 15.2(1)T よりも前のリリースで実行できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*

4. **event-log** [**size** [*number of events*]] [**one-shot**] [**pause**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 router ospf** *process-id* **例：** `Router(config)# ipv6 router ospf 1`	OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**event-log** [**size** [*number of events*]] [**one-shot**] [**pause**] **例：** `Router(config-router)# event-log size 10000 one-shot`	イベント ロギングをイネーブルにします。

イベント ログの内容のクリア

手順の概要

1. **enable**
2. **clear ipv6 ospf** [*process-id*] **events**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 必要に応じてパスワードを入力します。
ステップ 2	**clear ipv6 ospf** [*process-id*] **events** **例：** `Router# clear ipv6 ospf 1 events`	OSPFv3 ルーティング プロセス ID に基づいて OSPFv3 イベント ログ コンテンツをクリアします。

RFC 5340 に従った OSPFv3 外部パス プリファレンス

手順の概要

1. **enable**
2. **configure terminal**
3. **router ospfv3** [*process-id*]
4. **no compatible rfc1583**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router ospfv3** [*process-id*] **例：** `Router(config)# router ospfv3 1`	IPv4 または IPv6 アドレス ファミリに対して OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**no compatible rfc1583** **例：** `Router(config-router)# no compatible rfc1583`	RFC 5340 に従った外部パス プリファレンス計算に使用する方法を変更します。

OSPFv3 グレースフル リスタートのイネーブル化

- 「グレースフルリスタート対応ルータでの OSPFv3 グレースフル リスタートのイネーブル化」（P.37）
- 「グレースフルリスタート認識ルータでの OSPFv3 グレースフル リスタートのイネーブル化」（P.38）

グレースフル リスタート対応ルータでの OSPFv3 グレースフル リスタートのイネーブル化

この作業は、Cisco IOS Release 15.1(3)S および 15.2(1)T 以降のリリースで実行できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router ospfv3** [*process-id*]

4. **graceful-restart** [**restart-interval** *interval*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router ospfv3** [*process-id*] **例：** `Router(config)# router ospfv3 1`	IPv4 または IPv6 アドレス ファミリに対して OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**graceful-restart** [**restart-interval** *interval*] **例：** `Router(config-rtr)# graceful-restart`	グレースフル リスタート対応ルータで OSPFv3 グレースフル リスタート機能をイネーブルにします。

グレースフルリスタート対応ルータでの OSPFv3 グレースフル リスタートのイネーブル化

この作業は、Cisco IOS Release 15.1(3)S および 15.2(1)T よりも前のリリースで実行できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **graceful-restart** [**restart-interval** *interval*]

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**ipv6 router ospf** *process-id* **例：** `Router(config)# ipv6 router ospf 1`	OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**graceful-restart** [**restart-interval** *interval*] **例：** `Router(config-rtr)# graceful-restart`	グレースフルリスタート対応ルータで OSPFv3 グレースフル リスタート機能をイネーブルにします。

グレースフル リスタート認識ルータでの OSPFv3 グレースフル リスタートのイネーブル化

この作業は、Cisco IOS Release 15.1(3)S および 15.2(1)T 以降のリリースで実行できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **router ospfv3** [*process-id*]
4. **graceful-restart helper** {**disable** | **strict-lsa-checking**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**router ospfv3** [*process-id*] **例：** `Router(config)# router ospfv3 1`	IPv4 または IPv6 アドレス ファミリに対して OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**graceful-restart helper** {**disable** | **strict-lsa-checking**} **例：** `Router(config-rtr)# graceful-restart helper strict-lsa-checking`	グレースフル リスタート認識ルータで OSPFv3 グレースフル リスタート機能をイネーブルにします。

グレースフルリスタート認識ルータでの OSPFv3 グレースフル リスタートのイネーブル化

この作業は、Cisco IOS Release 15.1(3)S および 15.2(1)T よりも前のリリースで実行できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **graceful-restart helper** {**disable** | **strict-lsa-checking**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 router ospf** *process-id* **例：** `Router(config)# ipv6 router ospf 1`	OSPFv3 ルータ コンフィギュレーション モードをイネーブルにします。
ステップ 4	**graceful-restart helper** {**disable** | **strict-lsa-checking**} **例：** `Router(config-rtr)# graceful-restart helper strict-lsa-checking`	グレースフルリスタート認識ルータで OSPFv3 グレースフル リスタート機能をイネーブルにします。

SPF 計算の強制実行

手順の概要

1. **enable**
2. **clear ospfv3** [*process-id*] **force-spf**
3. **clear ospfv3** [*process-id*] **process**
4. **clear ospfv3** [*process-id*] **redistribution**
5. **clear ipv6 ospf** [*process-id*] {**process** | **force-spf** | **redistribution**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**clear ospfv3** [*process-id*] **force-spf** **例：** `Router# clear ospfv3 1 force-spf`	OSPFv3 プロセスに対して SPF 計算を実行します。 • **clear ospfv3 force-spf** コマンドが設定されている場合、**clear ipv6 ospf** の設定が上書きされます。 • いったん **clear ospfv3 force-spf** コマンドを使用すると、**clear ipv6 ospf** コマンドは使用できなくなります。
ステップ 3	**clear ospfv3** [*process-id*] **process** **例：** `Router# clear ospfv3 2 process`	OSPFv3 プロセスをリセットします。 • **clear ospfv3 force-spf** コマンドが設定されている場合、**clear ipv6 ospf** の設定が上書きされます。 • いったん **clear ospfv3 force-spf** コマンドを使用すると、**clear ipv6 ospf** コマンドは使用できなくなります。
ステップ 4	**clear ospfv3** [*process-id*] **redistribution** **例：** `Router# clear ospfv3 redistribution`	OSPFv3 ルート再配布をクリアします。 • **clear ospfv3 force-spf** コマンドが設定されている場合、**clear ipv6 ospf** の設定が上書きされます。 • いったん **clear ospfv3 force-spf** コマンドを使用すると、**clear ipv6 ospf** コマンドは使用できなくなります。
ステップ 5	**clear ipv6 ospf** [*process-id*] {**process** | **force-spf** | **redistribution**} **例：** `Router# clear ipv6 ospf force-spf`	OSPFv3 ルーティング プロセス ID に基づいて OSPFv3 状態をクリアし、SPF アルゴリズムを強制的に開始します。 • **clear ospfv3 force-spf** コマンドが設定されている場合、**clear ipv6 ospf** の設定が上書きされます。 • いったん **clear ospfv3 force-spf** コマンドを使用すると、**clear ipv6 ospf** コマンドは使用できなくなります。

OSPFv3 の設定と動作の確認

このタスクはオプションです。この作業のコマンドは、Cisco IOS Release 15.1(3)S および 15.2(1)T 以降のリリースで使用できます。

手順の概要

1. **enable**
2. **show ospfv3** [*process-id*] [*address-family*] **border-routers**
3. **show ospfv3** [*process-id* [*area-id*]] [*address-family*] **database** [**database-summary** | **internal** | **external** [*ipv6-prefix*] [*link-state-id*] | **grace** | **inter-area prefix** [*ipv6-prefix* | *link-state-id*] | **inter-area router** [*destination-router-id* | *link-state-id*] | **link** [**interface** *interface-name* | *link-state-id*] | **network** [*link-state-id*] | **nssa-external** [*ipv6-prefix*] [*link-state-id*] | **prefix** [**ref-lsa** {**router** | **network**} | *link-state-id*] | **promiscuous** | **router** [*link-state-id*] | **unknown** [{**area** | **as** | **link**} [*link-state-id*]] [**adv-router** *router-id*] [**self-originate**]

4. **show ospfv3** [*process-id*] [*address-family*] **events** [**generic** | **interface** | **lsa** | **neighbor** | **reverse** | **rib** | **spf**]
5. **show ospfv3** [*process-id*] [*area-id*] [*address-family*] **flood-list** *interface-type interface-number*
6. **show ospfv3** [*process-id*] [*address-family*] **graceful-restart**
7. **show ospfv3** [*process-id*] [*area-id*] [*address-family*] **interface** [*type number*] [**brief**]
8. **show ospfv3** [*process-id*] [*area-id*] [*address-family*] **neighbor** [*interface-type interface-number*] [*neighbor-id*] [**detail**]
9. **show ospfv3** [*process-id*] [*area-id*] [*address-family*] **request-list** [*neighbor*] [*interface*] [*interface-neighbor*]
10. **show ospfv3** [*process-id*] [*area-id*] [*address-family*] **retransmission-list** [*neighbor*] [*interface*] [*interface-neighbor*]
11. **show ospfv3** [*process-id*] [*address-family*] **statistic** [**detail**]
12. **show ospfv3** [*process-id*] [*address-family*] **summary-prefix**
13. **show ospfv3** [*process-id*] [*address-family*] **timers rate-limit**
14. **show ospfv3** [*process-id*] [*address-family*] **traffic** [*interface-type interface-number*]
15. **show ospfv3** [*process-id*] [*address-family*] **virtual-links**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**show ospfv3** [*process-id*] [*address-family*] **border-routers** **例：** `Router# show ospfv3 border-routers`	ABR および ASBR への内部 OSPFv3 ルーティング テーブル エントリを表示します。
ステップ 3	**show ospfv3** [*process-id* [*area-id*]] [*address-family*] **database** [**database-summary** | **internal** | **external** [*ipv6-prefix*] [*link-state-id*] | **grace** | **inter-area prefix** [*ipv6-prefix* | *link-state-id*] | **inter-area router** [*destination-router-id* | *link-state-id*] | **link** [**interface** *interface-name* | *link-state-id*] | **network** [*link-state-id*] | **nssa-external** [*ipv6-prefix*] [*link-state-id*] | **prefix** [**ref-lsa** {**router** | **network**} | *link-state-id*] | **promiscuous** | **router** [*link-state-id*] | **unknown** [{**area** | **as** | **link**} [*link-state-id*]] [**adv-router** *router-id*] [**self-originate**] **例：** `Router# show 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。

	コマンドまたはアクション	目的
ステップ 4	**show ospfv3** [*process-id*] [*address-family*] **events** [**generic** | **interface** | **lsa** | **neighbor** | **reverse** | **rib** | **spf**] **例：** `Router# show ospfv3 events`	OSPFv3 イベントについての詳細情報を表示します。
ステップ 5	**show ospfv3** [*process-id*] [*area-id*] [*address-family*] **flood-list** *interface-type interface-number* **例：** `Router# show ospfv3 flood-list`	インターフェイス上でのフラッディングを待機している OSPFv3 LSA のリストを表示します。
ステップ 6	**show ospfv3** [*process-idS*[*address-family*] **graceful-restart** **例：** `Router# show ospfv3 graceful-restart`	OSPFv3 グレースフル リスタートの情報を表示します。
ステップ 7	**show ospfv3** [*process-id*] [*area-id*] [*address-family*] **interface** [*type number*] [**brief**] **例：** `Router# show ospfv3 interface`	OSPFv3 関連のインターフェイス情報を表示します。
ステップ 8	**show ospfv3** [*process-id*] [*area-id*] [*address-family*] **neighbor** [*interface-type interface-number*] [*neighbor-id*] [**detail**] **例：** `Router# show ospfv3 neighbor`	OSPFv3 ネイバー情報をインターフェイスごとに表示します。
ステップ 9	**show ospfv3** [*process-id*] [*area-id*] [*address-family*] **request-list** [*neighbor*] [*interface*] [*interface-neighbor*] **例：** `Router# show ospfv3 request-list`	ルータから要求されたすべての LSA のリストを表示します。
ステップ 10	**show ospfv3** [*process-id*] [*area-id*] [*address-family*] **retransmission-list** [*neighbor*] [*interface*] [*interface-neighbor*] **例：** `Router# show ospfv3 retransmission-list`	再送信を待機しているすべての LSA のリストを表示します。
ステップ 11	**show ospfv3** [*process-id*] [*address-family*] **statistic** [**detail**] **例：** `Router# show ospfv3 statistics`	OSPFv3 SPF 計算の統計情報を表示します。

	コマンドまたはアクション	目的
ステップ 12	**show ospfv3** [*process-id*] [*address-family*] **summary-prefix** **例：** `Router# show ospfv3 summary-prefix`	OSPFv3 プロセスで設定されているサマリー アドレスの、すべての再配布情報のリストを表示します。
ステップ 13	**show ospfv3** [*process-id*] [*address-family*] **timers rate-limit** **例：** `Router# show ospfv3 timers rate-limit`	レート リミット キュー内のすべての LSA を表示します。
ステップ 14	**show ospfv3** [*process-id*] [*address-family*] **traffic** [*interface-type interface-number*] **例：** `Router# show ospfv3 traffic`	OSPFv3 トラフィック統計情報を表示します。
ステップ 15	**show ospfv3** [*process-id*] [*address-family*] **virtual-links** **例：** `Router# show ospfv3 virtual-links`	OSPFv3 仮想リンクのパラメータと現在の状態を表示します。

OSPFv3 の設定と動作の確認

手順の概要

1. **enable**
2. **show ipv6 ospf** [*process-id*] [*area-id*] **interface** [*interface-type interface-number*]
3. **show ipv6 ospf** [*process-id*] [*area-id*]
4. **show crypto ipsec policy** [**name** *policy-name*]
5. **show crypto ipsec sa** [**map** *map-name* | **address** | **identity** | **interface** *type number* | **peer** [**vrf** *fvrf-name*] **address** | **vrf** *ivrf-name* | **ipv6** [*interface-type interface-number*]] [**detail**]
6. **show ipv6 ospf** [*process-ID*] **event** [**generic** | **interface** | **lsa** | **neighbor** | **reverse** | **rib** | **spf**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**show ipv6 ospf** [*process-id*] [*area-id*] **interface** [*interface-type interface-number*] **例：** `Router# show ipv6 ospf interface`	OSPFv3 関連のインターフェイス情報を表示します。

	コマンドまたはアクション	目的
ステップ 3	**show ipv6 ospf** [*process-id*] [*area-id*] **例：** Router# show ipv6 ospf	OSPFv3 ルーティング プロセスに関する一般的な情報を表示します。
ステップ 4	**show crypto ipsec policy** [**name** *policy-name*] **例：** Router# show crypto ipsec policy	各 IPsec パラメータのパラメータを表示します。
ステップ 5	**show crypto ipsec sa** [**map** *map-name* | **address** | **identity** | **interface** *type number* | **peer** [**vrf** *fvrf-name*] **address** | **vrf** *ivrf-name* | **ipv6** [*interface-type interface-number*]] [**detail**] **例：** Router# show crypto ipsec sa ipv6	現在の Security Association（SA; セキュリティ アソシエーション）によって使用されている設定を表示します。
ステップ 6	**show ipv6 ospf** [*process-ID*] **event** [**generic** | **interface** | **lsa** | **neighbor** | **reverse** | **rib** | **spf**] **例：** Router# show ipv6 ospf event spf	OSPFv3 イベントについての詳細情報を表示します。

例

show ipv6 ospf interface コマンドの出力例

次に、暗号化および認証によって保護された通常のインターフェイスおよび仮想リンクを使用した、**show ipv6 ospf interface** コマンドの出力例を示します。

```
Router# show ipv6 ospf interface

OSPFv3_VL1 is up, line protocol is up
   Interface ID 69
   Area 0, Process ID 1, Instance ID 0, Router ID 10.0.0.1
   Network Type VIRTUAL_LINK, Cost: 64
   Configured as demand circuit.
   Run as demand circuit.
   DoNotAge LSA allowed.
   NULL encryption SHA-1 auth SPI 3944, secure socket UP (errors: 0)
   Transmit Delay is 1 sec, State POINT_TO_POINT,
   Timer intervals configured, Hello 2, Dead 10, Wait 40, Retransmit 5
     Hello due in 00:00:00
   Index 1/3/5, flood queue length 0
   Next 0x0(0)/0x0(0)/0x0(0)
   Last flood scan length is 1, maximum is 1
   Last flood scan time is 0 msec, maximum is 0 msec
```

```
   Neighbor Count is 1, Adjacent neighbor count is 1
     Adjacent with neighbor 10.2.0.1  (Hello suppressed)
   Suppress hello for 1 neighbor(s)
OSPFv3_VL0 is up, line protocol is up
   Interface ID 67
   Area 0, Process ID 1, Instance ID 0, Router ID 10.0.0.1
   Network Type VIRTUAL_LINK, Cost: 128
   Configured as demand circuit.
   Run as demand circuit.
   DoNotAge LSA allowed.
   MD5 authentication SPI 940, secure socket UP (errors: 0)
   Transmit Delay is 1 sec, State POINT_TO_POINT,
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
     Hello due in 00:00:09
   Index 1/2/4, flood queue length 0
   Next 0x0(0)/0x0(0)/0x0(0)
   Last flood scan length is 1, maximum is 10
   Last flood scan time is 0 msec, maximum is 0 msec
   Neighbor Count is 1, Adjacent neighbor count is 1
     Adjacent with neighbor 10.1.0.1  (Hello suppressed)
   Suppress hello for 1 neighbor(s)
Ethernet1/0 is up, line protocol is up
   Link Local Address FE80::A8BB:CCFF:FE00:6601, Interface ID 6
   Area 0, Process ID 1, Instance ID 0, Router ID 10.0.0.1
   Network Type BROADCAST, Cost: 10
   Transmit Delay is 1 sec, State DR, Priority 1
   Designated Router (ID) 10.0.0.1, local address FE80::A8BB:CCFF:FE00:6601
   No backup designated router on this network
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
     Hello due in 00:00:09
   Index 1/1/1, flood queue length 0
   Next 0x0(0)/0x0(0)/0x0(0)
   Last flood scan length is 0, maximum is 0
   Last flood scan time is 0 msec, maximum is 0 msec
   Neighbor Count is 0, Adjacent neighbor count is 0
   Suppress hello for 0 neighbor(s)
Serial12/0 is up, line protocol is up
   Link Local Address FE80::A8BB:CCFF:FE00:6600, Interface ID 50
   Area 1, Process ID 1, Instance ID 0, Router ID 10.0.0.1
   Network Type POINT_TO_POINT, Cost: 64
   AES-CBC encryption SHA-1 auth SPI 2503, secure socket UP (errors: 0)
   authentication NULL
   Transmit Delay is 1 sec, State POINT_TO_POINT,
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
     Hello due in 00:00:09
   Index 1/2/3, flood queue length 0
   Next 0x0(0)/0x0(0)/0x0(0)
   Last flood scan length is 1, maximum is 5
   Last flood scan time is 0 msec, maximum is 0 msec
   Neighbor Count is 1, Adjacent neighbor count is 1
     Adjacent with neighbor 10.2.0.1
   Suppress hello for 0 neighbor(s)
Serial11/0 is up, line protocol is up
   Link Local Address FE80::A8BB:CCFF:FE00:6600, Interface ID 46
   Area 1, Process ID 1, Instance ID 0, Router ID 10.0.0.1
   Network Type POINT_TO_POINT, Cost: 64
   MD5 authentication (Area) SPI 500, secure socket UP (errors: 0)
   Transmit Delay is 1 sec, State POINT_TO_POINT,
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
     Hello due in 00:00:09
   Index 1/1/2, flood queue length 0
   Next 0x0(0)/0x0(0)/0x0(0)
   Last flood scan length is 1, maximum is 5
   Last flood scan time is 0 msec, maximum is 0 msec
```

```
   Neighbor Count is 1, Adjacent neighbor count is 1
     Adjacent with neighbor 10.0.0.1
   Suppress hello for 0 neighbor(s)
```

show ipv6 ospf コマンドの出力例

次に、**show ipv6 ospf** コマンドの出力例を示します。

```
Router# show ipv6 ospf

Routing Process "ospfv3 1" with ID 172.16.3.3
 It is an autonomous system boundary router
 Redistributing External Routes from,
    static
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 1. Checksum Sum 0x218D
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
    Area 1
        Number of interfaces in this area is 2
        SPF algorithm executed 9 times
        Number of LSA 15. Checksum Sum 0x67581
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

show crypto ipsec policy コマンドの出力例

次に、**show crypto ipsec policy** コマンドの出力例を示します。

```
Router# show crypto ipsec policy

Crypto IPsec client security policy data

Policy name:     OSPFv3-1-1000
Policy refcount: 1
Inbound  AH SPI: 1000 (0x3E8)
Outbound AH SPI: 1000 (0x3E8)
Inbound  AH Key: 1234567890ABCDEF1234567890ABCDEF
Outbound AH Key: 1234567890ABCDEF1234567890ABCDEF
Transform set:   ah-md5-hmac
```

show crypto ipsec sa ipv6 コマンドの出力例

次に、**show crypto ipsec sa ipv6** コマンドの出力例を示します。

```
Router# show crypto ipsec sa ipv6

IPv6 IPsec SA info for interface Ethernet0/0

   protected policy name:OSPFv3-1-1000
   IPsec created ACL name:Ethernet0/0-ipsecv6-ACL

   local  ident (addr/prefixlen/proto/port):(FE80::/10/89/0)
   remote ident (addr/prefixlen/proto/port):(::/0/89/0)
   current_peer:::
     PERMIT, flags={origin_is_acl,}
    #pkts encaps:21, #pkts encrypt:0, #pkts digest:21
    #pkts decaps:20, #pkts decrypt:0, #pkts verify:20
    #pkts compressed:0, #pkts decompressed:0
    #pkts not compressed:0, #pkts compr. failed:0
```

```
    #pkts not decompressed:0, #pkts decompress failed:0
    #send errors 0, #recv errors 0

    local crypto endpt. ::, remote crypto endpt. ::
    path mtu 1500, media mtu 1500
    current outbound spi:0x3E8(1000)

     inbound ESP SAs:

     inbound AH SAs:
      spi:0x3E8(1000)
        transform:ah-md5-hmac ,
        in use settings ={Transport, }
        slot:0, conn_id:2000, flow_id:1, crypto map:N/R
        no sa timing (manual-keyed)
        replay detection support:N

     inbound PCP SAs:

     outbound ESP SAs:

     outbound AH SAs:
      spi:0x3E8(1000)
        transform:ah-md5-hmac ,
        in use settings ={Transport, }
        slot:0, conn_id:2001, flow_id:2, crypto map:N/R
        no sa timing (manual-keyed)
        replay detection support:N

     outbound PCP SAs:
```

show ipv6 ospf graceful-restart コマンドの出力例

次に、**show crypto ipsec sa ipv6** コマンドの出力例を示します。

```
Router# show ipv6 ospf graceful-restart

Routing Process "ospf 1"
 Graceful Restart enabled
    restart-interval limit: 120 sec, last restart 00:00:15 ago (took 36 secs)
  Graceful Restart helper support enabled
  Router status : Active
  Router is running in SSO mode
  OSPF restart state : NO_RESTART
  Router ID 10.1.1.1, checkpoint Router ID 10.0.0.0
```

OSPFv3 の実装の設定例

例：インターフェイス設定での OSPFv3 のイネーブル化

次に、OSPFv3 ルーティング プロセス 109 をインターフェイスで実行し、エリア 1 に配置する例を示します。

```
ipv6 ospf 109 area 1
```

例：OSPFv3 エリア範囲の定義

次に、OSPFv3 エリア範囲を指定する例を示します。

```
interface Ethernet7/0
 ipv6 address 2001:DB8:0:7::/64 eui-64
 ipv6 enable
 ipv6 ospf 1 area 1
!
interface Ethernet8/0
 ipv6 address 2001:DB8:0:8::/64 eui-64
 ipv6 enable
 ipv6 ospf 1 area 1
!
interface Ethernet9/0
 ipv6 address 2001:DB8:0:9::/64 eui-64
 ipv6 enable
 ipv6 ospf 1 area 1
!
ipv6 router ospf 1
 router-id 10.11.11.1
 area 1 range 2001:DB8::/48
```

例：インターフェイスでの認証の定義

次に、イーサネット 0/0 インターフェイスで認証を定義する例を示します。

```
interface Ethernet0/0
 ipv6 enable
 ipv6 ospf 1 area 0
 ipv6 ospf authentication ipsec spi 500 md5 1234567890ABCDEF1234567890ABCDEF

interface Ethernet0/0
 ipv6 enable
 ipv6 ospf authentication null
 ipv6 ospf 1 area 0
```

例：OSPFv3 エリア内の認証の定義

次に、OSPFv3 エリア 0 で認証を定義する例を示します。

```
ipv6 router ospf 1
 router-id 10.11.11.1
 area 0 authentication ipsec spi 1000 md5 1234567890ABCDEF1234567890ABCDEF
```

例：NBMA インターフェイスの設定

次に、IPv6 アドレスが FE80::A8BB:CCFF:FE00:C01 の OSPFv3 ネイバー ルータを設定する例を示します。

```
interface serial 0
 ipv6 enable
 ipv6 ospf 1 area 0
 encapsulation frame-relay
 frame-relay map ipv6 FE80::A8BB:CCFF:FE00:C01 120
 ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C0
```

例：OSPFv3 高速コンバージェンスに対する LSA および SPF スロットリングの設定

次に、SPF および LSA スロットル タイマーの設定値を表示する例を示します。

```
Router# show ipv6 ospf

 Routing Process "ospfv3 1" with ID 10.9.4.1
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 It is an autonomous system boundary router
 Redistributing External Routes from,
    ospf 2
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
```

例：SPF 設定の強制実行

次に、SPF をトリガーして、SPF を再実行し、ルーティング テーブルに値を再入力する例を示します。

```
clear ipv6 ospf force-spf
```

その他の関連資料

関連資料

関連項目	参照先
OSPF でのルータ ID の設定	• 『*Cisco IOS IP Routing Protocols Configuration Guide*』の「Configuring OSPF」 • 『*Cisco IOS IP Routing Protocols Command Reference*』
OSPFv3 コマンド	『*Cisco IOS IPv6 Command Reference*』
IPv6 のサポート機能リスト	『*Cisco IOS IPv6 Configuration Guide*』の「Start Here: Cisco IOS Software Release Specifics for IPv6 Features」
基本的な IPv6 接続の実装	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing IPv6 Addressing and Basic Connectivity」
IPsec for IPv6	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing IPsec for IPv6 Security」
OSPFv3 に対する BFD サポート	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing Bidirectional Forwarding Detection for IPv6」
ステートフル スイッチオーバー	『*Cisco IOS High Availability Configuration Guide*』の「Stateful Switchover」
Cisco ノンストップ フォワーディング	『*Cisco IOS High Availability Configuration Guide*』の「Cisco Nonstop Forwarding」

規格

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

MIB

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

RFC

RFC	タイトル
RFC 1583	『*OSPF version 2*』
RFC 2401	『*Security Architecture for the Internet Protocol*』
RFC 2402	『*IP Authentication Header*』
RFC 2406	『*IP Encapsulating Security Payload (ESP)*』
RFC 3137	『*OSPF Stub Router Advertisement*』
RFC 4552	『*Authentication/Confidentiality for OSPFv3*』
RFC 5187	『*OSPFv3 Graceful Restart*』
RFC 5340	『*OSPF for IPv6*』
RFC 5838	『*Support of Address Families in OSPFv3*』

シスコのテクニカル サポート

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

OSPFv3 の実装の機能情報

表 3 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。

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

（注） 表 3 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 3　OSPFv3 の実装の機能情報

機能名	リリース	機能情報
IPv6 ルーティング：高速コンバージェンス：LSA および SPF スロットリング	12.2(33)SB 12.2(33)SRC 12.2(33)XNE 15.0(1)M	OSPFv3 の LSA および SPF スロットリング機能は、ネットワークが不安定な間、OSPFv3 でのリンクステート アドバタイズメント アップデートを低速化するためのダイナミック メカニズムを提供します。 この機能に関する詳細については、次の各項を参照してください。 • 「高速コンバージェンス - LSA および SPF スロットリング」（P.7） • 「OSPFv3 高速コンバージェンスに対する LSA および SPF スロットリングの設定」（P.32） • 「イベント ロギングのイネーブル化」（P.33） • 「イベント ログの内容のクリア」（P.35） • 「例：OSPFv3 高速コンバージェンスに対する LSA および SPF スロットリングの設定」（P.49）
IPv6 ルーティング：OSPFv3 での強制 SPF	12.0(24)S 12.2(18)S 12.2(28)SB 12.2(15)T 12.3 12.3(2)T 12.4 12.4(2)T	この機能により、OSPFv3 データベースのクリアおよび再入力が可能になります。その後で、SPF アルゴリズムが実行されます。 この機能に関する詳細については、次の各項を参照してください。 • 「OSPFv3 の強制的な SPF」（P.7） • 「OSPFv3 グレースフル リスタートのイネーブル化」（P.36）
IPv6 ルーティング：OSPFv3 でのロード バランシング	12.0(24)S 12.2(18)S 12.2(28)SB 12.2(15)T 12.3 12.3(2)T 12.4 12.4(2)T	OSPFv3 では、自動的にロード バランシングが実行されます。 この機能に関する詳細については、次の項を参照してください。 • 「OSPFv3 でのロード バランシング」（P.7）

表 3　OSPFv3 の実装の機能情報 （続き）

機能名	リリース	機能情報
IPv6 ルーティング：OSPFv3 の LSA タイプ	12.0(24)S 12.2(18)S 12.2(28)SB 12.2(15)T 12.3 12.3(2)T 12.4 12.4(2)T	ルータの LSA データの集まりは、リンクステート データベースに格納されます。ダイクストラ アルゴリズムが採用されている場合、データベースの内容に基づいて OSPFv3 ルーティング テーブルが作成されます。 この機能に関する詳細については、次の各項を参照してください。 • 「OSPFv3 の機能」（P.3） • 「OSPFv3 の LSA タイプ」（P.5）
IPv6 ルーティング：OSPFv3 の NBMA インターフェイス	12.0(24)S 12.2(18)S 12.2(28)SB 12.2(15)T 12.3 12.3(2)T 12.4 12.4(2)T	NBMA ネットワークでは、DR または Backup DR が LSA フラッディングを実行します。 この機能に関する詳細については、次の各項を参照してください。 • 「OSPFv3 の NBMA」（P.6） • 「OSPFv3 への NBMA インターフェイスの設定」（P.29）
IPv6 ルーティング：OSPF for IPv6（OSPFv3）	12.0(24)S 12.2(18)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(15)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)M 15.0(1)S	OSPF バージョン 3 for IPv6 では、OSPF バージョン 2 が拡張され、IPv6 ルーティング プレフィクスと、より大きなサイズの IPv6 アドレスに対するサポートが提供されています。 このマニュアルでは、この機能について説明しています。
IPv6 ルーティング：IPsec を使用した OSPF for IPv6 認証サポート	12.3(4)T 12.4 12.4(2)T	OSPF for IPv6 は、IPsec セキュア ソケット API を使用して OSPFv3 パケットに認証を追加します。 この機能に関する詳細については、次の各項を参照してください。 • 「IPsec を使用した OSPFv3 認証サポート」（P.8） • 「OSPFv3 への IPsec の設定」（P.23） • 「インターフェイスでの認証の定義」（P.24） • 「OSPFv3 エリア内の認証の定義」（P.26）

表 3　OSPFv3 の実装の機能情報 （続き）

機能名	リリース	機能情報
IPv6 ルーティング：OSPF IPv6（OSPFv3）IPsec ESP 暗号化および認証	12.4(9)T	IPv6 ESP 拡張ヘッダーを使用すると、OSPFv3 に認証および機密性を提供できます。 この機能に関する詳細については、次の各項を参照してください。 • 「OSPFv3 の実装の制約事項」（P.2） • 「IPsec を使用した OSPFv3 認証サポート」（P.8） • 「インターフェイスでの暗号化の定義」（P.25） • 「OSPFv3 エリア内の暗号化の定義」（P.27） • 「OSPFv3 エリア内の仮想リンクに対する認証および暗号化の定義」（P.28）
OSPFv3 アドレス ファミリ	15.1(3)S 15.2(1)T	OSPFv3 アドレス ファミリ機能では、IPv4 および IPv6 ユニキャスト トラフィックを 1 つのネットワーク トポロジでサポートできます。 この機能に関する詳細については、次の各項を参照してください。 • 「OSPFv3 アドレス ファミリ」（P.4） • 「OSPFv3 ルータ プロセスの設定」（P.13） • 「OSPFv3 への IPv6 アドレス ファミリの設定」（P.15） • 「OSPFv3 への IPv4 アドレス ファミリの設定」（P.17） • 「OSPFv3 へのルート再配布の設定」（P.19） • 「インターフェイスでの OSPFv3 のイネーブル化」（P.20） • 「IPv6 または IPv4 アドレス ファミリに対する OSPFv3 エリア範囲の定義」（P.21） • 「例：インターフェイス設定での OSPFv3 のイネーブル化」（P.48） • 「例：OSPFv3 エリア範囲の定義」（P.48）
OSPFv3 動的インターフェイス コスト サポート	12.4(15)T	OSPFv3 動的インターフェイス コスト サポートは、モバイル アドホック ネットワーキングをサポートする OSPFv3 コスト メトリックの拡張を提供します。 この機能に関する詳細については、次の項を参照してください。 • 「OSPFv3 コスト計算」（P.9）

表 3　OSPFv3 の実装の機能情報 （続き）

機能名	リリース	機能情報
OSPFv3 外部パス プリファレンス オプション	15.1(3)S 15.2(1)T	この機能により、RFC 5340 に従って外部パス プリファレンスを計算する方法が提供されます。 この機能に関する詳細については、次の各項を参照してください。 • 「OSPFv3 外部パス プリファレンス オプション」（P.11） • 「RFC 5340 に従った OSPFv3 外部パス プリファレンス」（P.36）
OSPFv3 for BFD	12.2(33)SRE 15.0(1)S 15.1(2)T	BFD では、ダイナミック ルーティング プロトコル OSPFv3 がサポートされています。 この機能に関する詳細については、次の項を参照してください。 • 「BFD での OSPFv3 のサポート」（P.12）
OSPFv3 グレースフル リスタート	12.2(33)SRE 12.2(33)XNE 12.2(58)SE 15.0(1)M	OSPFv3 でグレースフル リスタート機能を使用すると、OSPFv3 ルーティング プロトコル情報の復元中も、既知のルートを使用してノンストップ データ フォワーディングを実行できます。 この機能に関する詳細については、次の各項を参照してください。 • 「OSPFv3 グレースフル リスタート」（P.12） • 「OSPFv3 グレースフル リスタートのイネーブル化」（P.36）
OSPFv3 Max-Metric ルータ LSA	15.1(3)S 15.2(1)T	OSPFv3 Max-Metric ルータ LSA 機能により、OSPF はローカルで生成されたルータ LSA を最大メトリックでアドバタイズできるようになります。 この機能に関する詳細については、次の各項を参照してください。 • 「OSPFv3 Max-Metric ルータ LSA」（P.6） • 「OSPFv3 Max-Metric ルータ LSA の設定」（P.30）