Open Shortest Path First（OSPF）

この章では、Open Shortest Path First（OSPF）ルーティング プロトコルを使用してデータをルーティングし、認証を実行し、ルーティング情報を再配布するように ASA を設定する方法について説明します。

OSPF について

OSPF は、パスの選択にディスタンス ベクターではなくリンク ステートを使用する Interior Gateway Routing Protocol です。OSPF は、ルーティング テーブル更新ではなく、リンクステート アドバタイズメントを伝達します。ルーティング テーブル全体ではなく LSA だけが交換されるため、OSPF ネットワークは RIP ネットワークよりも迅速に収束します。

OSPF は、リンクステート アルゴリズムを使用して、すべての既知の宛先までの最短パスを構築および計算します。OSPF エリア内の各ルータには、ルータが使用可能なインターフェイスと到達可能なネイバーそれぞれのリストである同一のリンクステート データベースが置かれています。

RIP と比べ OSPF には次の利点があります。

- OSPF では、リンクステート データベースの更新が RIP ほど頻繁に送信されません。また、ステート情報がタイムアウトすると、リンクステート データベースは徐々にではなく、すぐに更新されます。

- ルーティングはコスト、つまり特定のインターフェイスを介してパケットを送信するために必要なオーバーヘッドに基づいて決定されます。ASA は、インターフェイスのコストをリンク帯域幅に基づいて計算し、接続先までのホップ数は使用しません。コストを設定して優先パスを指定することができます。

最短パスを優先するアルゴリズムの欠点は、CPU サイクルとメモリが大量に必要になることです。

ASA は、OSPF プロトコルのプロセスを 2 つ同時に異なるインターフェイス セット上で実行できます。同じ IP アドレスを使用する複数のインターフェイス（NAT ではこのようなインターフェイスが共存可能ですが、OSPF ではアドレスは重複できません）がある場合に、2 つのプロセスを実行できます。あるいは、一方のプロセスを内部で実行しながら別のプロセスを外部で実行し、ルートのサブセットをこの 2 つのプロセス間で再配布することもできます。同様に、プライベート アドレスをパブリック アドレスから分離する必要がある場合もあります。

OSPF ルーティング プロセスには、別の OSPF ルーティング プロセスや RIP ルーティング プロセスから、または OSPF 対応インターフェイスに設定されているスタティック ルートおよび接続ルートから、ルートを再配布できます。

ASA では、次の OSPF の機能がサポートされています。

- エリア内ルート、エリア間ルート、および外部ルート（タイプ I とタイプ II）。
- 仮想リンク。
- LSA フラッディング。
- OSPF パケットの認証（パスワード認証と MD5 認証の両方）。
- ASA の代表ルータまたはバックアップ代表ルータとしての設定。ASA は、ABR として設定することもできます。
- スタブ エリアと Not-So-Stubby Area。
- エリア境界ルータのタイプ 3 LSA フィルタリング。

OSPF は、MD5 およびクリア テキスト ネイバー認証をサポートします。OSPF と他のプロトコル（RIP など）の間のルート再配布にあたっては、攻撃者によるルーティング情報の悪用の可能性があるため、できる限りすべてのルーティング プロトコルで認証を行う必要があります。

NAT を使用していて、OSPF がパブリック エリアおよびプライベート エリアで動作している場合、またアドレス フィルタリングが必要な場合は、2 つの OSPF プロセス（1 つはパブリック エリア用、1 つはプライベート エリア用）を実行する必要があります。

複数のエリアにインターフェイスを持つルータは、エリア境界ルータ（ABR）と呼ばれます。ゲートウェイとして動作し、OSPF を使用しているルータと他のルーティング プロトコルを使用しているルータの間でトラフィックを再配布するルータは、自律システム境界ルータ（ASBR）と呼ばれます。

ABR は LSA を使用して、使用可能なルートに関する情報を他の OSPF ルータに送信します。ABR タイプ 3 LSA フィルタリングを使用して、ABR として機能する ASA により、プライベート エリアとパブリック エリアを分けることができます。タイプ 3 LSA（エリア間ルート）は、

プライベート ネットワークをアドバタイズしなくても NAT と OSPF を一緒に使用できるように、1 つのエリアから他のエリアにフィルタリングできます。

（注） フィルタリングできるのはタイプ 3 LSA のみです。プライベート ネットワーク内の ASBR として設定されている ASA は、プライベート ネットワークを記述するタイプ 5 LSA を送信しますが、これは AS 全体（パブリック エリアも含む）にフラッディングされます。

NAT が採用されているが、OSPF がパブリック エリアだけで実行されている場合は、パブリック ネットワークへのルートを、デフォルトまたはタイプ 5 AS 外部 LSA としてプライベート ネットワーク内で再配布できます。ただし、ASA により保護されているプライベート ネットワークにはスタティック ルートを設定する必要があります。また、同一の ASA インターフェイス上で、パブリック ネットワークとプライベート ネットワークを混在させることはできません。

ASA では、2 つの OSPF ルーティング プロセス（1 つの RIP ルーティング プロセスと 1 つの EIGRP ルーティング プロセス）を同時に実行できます。

fast hello パケットに対する OSPF のサポート

fast hello パケットに対する OSPF のサポートには、1 秒未満のインターバルで hello パケットの送信を設定する方法が用意されています。このような設定により、Open Shortest Path First（OSPF）ネットワークでのコンバージェンスがより迅速になります。

Fast Hello パケットに対する OSPF サポートの前提条件

OSPF がネットワークですでに設定されているか、Fast Hello パケット機能向けの OSPF のサポートと同時に設定される必要があります。

fast hello パケットに対する OSPF のサポートについて

次に、fast hello パケットに関する OSPF のサポートと、OSPF fast hello パケットの利点について説明します。

OSPF Hello インターバルと dead 間隔

OSPF hello パケットとは、OSPF プロセスがネイバーとの接続を維持するために OSPF ネイバーに送信するパケットです。hello パケットは、設定可能なインターバル（秒単位）で送信されます。デフォルトのインターバルは、イーサネット リンクの場合 10 秒、ブロードキャスト以外のリンクの場合 30 秒です。hello パケットには、dead 間隔中に受信したすべてのネイバーのリストが含まれます。dead 間隔も設定可能なインターバル（秒単位）で送信されます。デフォルトは Hello インターバルの値の 4 倍です。Hello インターバルの値は、ネットワーク内ですべて同一にする必要があります。dead 間隔の値も、ネットワーク内ですべて同一にする必要があります。

この2つのインターバルは、リンクが動作していることを示すことにより、接続を維持するために連携して機能します。ルータが dead 間隔内にネイバーから hello パケットを受信しない場合、ルータはこのネイバーがダウンしていると判定します。

OSPF fast hello パケット

OSPF fast hello パケットとは、1 秒よりも短い間隔で送信される hello パケットのことです。fast hello パケットを理解するには、OSPF hello パケット インターバルと dead 間隔との関係についてあらかじめ理解しておく必要があります。OSPF Hello インターバルと dead 間隔 （3 ページ）を参照してください。

OSPF fast hello パケットは、ospf dead-interval コマンドで設定されます。dead 間隔は 1 秒に設定され、hello-multiplier の値は、その 1 秒間に送信する hello パケット数に設定されるため、1 秒未満の「fast」hello パケットになります。

インターフェイスで fast hello パケットが設定されている場合、このインターフェイスから送出される hello パケットでアドバタイズされる Hello インターバルは 0 に設定されます。このインターフェイス経由で受信した hello パケットの Hello インターバルは無視されます。

dead 間隔は、1 つのセグメント上で一貫している必要があり、1 秒に設定するか（fast hello パケットの場合）、他の任意の値を設定します。dead 間隔内に少なくとも 1 つの hello パケットが送信される限り、hello multiplier がセグメント全体で同じである必要はありません。

OSPF Fast Hello パケットの利点

OSPF Fast Hello パケット機能を利用すると、ネットワークがこの機能を使用しない場合よりも、コンバージェンス時間が短くなります。この機能によって、失われたネイバーを 1 秒以内に検出できるようになります。この機能は、ネイバーの損失がオープン システム相互接続（OSI）物理層またはデータリンク層で検出されないことがあっても、特に LAN セグメントで有効です。

OSPFv2 および OSPFv3 間の実装の差異

OSPFv3 には、OSPFv2 との後方互換性はありません。OSPF を使用して、IPv4 および IPv6 トラフィックの両方をルーティングするには、OSPFv2 および OSPFv3 の両方を同時に実行する必要があります。これらは互いに共存しますが、相互に連携していません。

OSPFv3 では、次の追加機能が提供されます。

- リンクごとのプロトコル処理。
- アドレッシング セマンティックの削除。
- フラッディング スコープの追加。
- リンクごとの複数インスタンスのサポート。
- ネイバー探索およびその他の機能に対する IPv6 リンクローカル アドレスの使用。
- プレフィックスおよびプレフィックス長として表される LSA。
- 2 つの LSA タイプの追加。

- 未知の LSA タイプの処理。
- RFC-4552 で指定されている OSPFv3 ルーティング プロトコル トラフィックの IPsec ESP 標準を使用する認証サポート。

OSPF のガイドライン

コンテキスト モードのガイドライン

OSPFv2 は、シングル コンテキスト モードとマルチ コンテキスト モードをサポートしています。

- デフォルトでは、共有インターフェイス間でのマルチキャスト トラフィックのコンテキスト間交換がサポートされていないため、OSPFv2 インスタンスは共有インターフェイス間で相互に隣接関係を形成できません。ただし、OSPFv2 プロセスの OSPFv2 プロセス設定で静的ネイバー設定を使用すると、共有インターフェイスでの OSPFv2 ネイバーシップを形成できます。
- 個別のインターフェイスでのコンテキスト間 OSPFv2 がサポートされています。

（ポイントツーポイント トポロジの場合） マルチ コンテキスト モードでは、スタティック OSPFv2 ネイバーを設定して、ポイントツーポイントの非ブロードキャスト ネットワークを介して OSPFv2 ルートをアドバタイズできます。OSPF 隣接関係を正常に形成するには、共有インターフェイスの OSPF を削除して再設定するときに、次の順序でコマンドを実行します。

- `no router <ospf name>` を使用して OSPF 設定を削除します。その後、 `no ospf network point-to-point non-broadcast` を使用して、インターフェイスの OSPF ポイントツーポイント 非ブロードキャスト設定を削除します。
- 共有インターフェイスで OSPF を再設定する場合は、 `router <ospf name>` を使用して OSPF ルータを設定します。次に `ospf network point-to-point non-broadcast` でインターフェイスを設定します。

OSPFv3 は、シングル モードのみをサポートしています。

キー チェーン認証のガイドライン

OSPFv2 は、単一モードと複数モードの両方で、物理モードでも、仮想モードでも、キーチェーンの認証をサポートしています。ただし、複数モードでキーチェーンが設定できるのはコンテキスト モードのみです。

- 循環キーは OSPFv2 プロトコルにのみ適用されます。キー チェーンを使用した OSPF エリア認証はサポートされていません。
- OSPFv2 内に時間範囲がない既存の MD5 認証も、新しい循環キーとともにサポートされています。

- プラットフォームは SHA1 と MD5 の暗号化アルゴリズムをサポートしていますが、認証には MD5 暗号化アルゴリズムのみが使用されます。

ファイアウォール モードのガイドライン

OSPF は、ルーテッド ファイアウォール モードのみをサポートしています。OSPF は、トランスペアレント ファイアウォール モードをサポートしません。

フェールオーバー ガイドライン

OSPFv2 および OSPFv3 は、ステートフル フェールオーバー をサポートしています。

IPv6 のガイドライン

- OSPFv2 は IPv6 をサポートしません。
- OSPFv3 は IPv6 をサポートしています。
- OSPFv3 は、IPv6 を使用して認証を行います。
- ASA は、OSPFv3 ルートが最適なルートの場合、IPv6 RIB にこのルートをインストールします。
- OSPFv3 パケットは、**capture** コマンドの IPv6 ACL を使用してフィルタリングで除外できます。

OSPFv3 Hello パケットと GRE

通常、OSPF トラフィックは GRE トンネルを通過しません。IPv6 の OSPFv3 が GRE 内でカプセル化されている場合、マルチキャスト宛先などのセキュリティチェックで IPv6 ヘッダー検証が失敗します。このパケットは、宛先が IPv6 マルチキャストであるため、暗黙的なセキュリティチェックの検証でドロップされます。

GRE トラフィックをバイパスするプレフィルタルールを定義できます。ただし、プレフィルタルールでは、内部パケットはインスペクションエンジンによって問い合わせられません。

クラスタリングのガイドライン

- OSPFv3 暗号化はサポートされていません。クラスタリング環境で OSPFv3 暗号化を設定しようとすると、エラー メッセージが表示されます。
- スパンド インターフェイス モードでは、ダイナミック ルーティングは管理専用インターフェイスではサポートされません。
- 個別インターフェイスモードで、OSPFv2 または OSPFv3 ネイバーとして制御ユニットおよびデータユニットが確立されていることを確認します。
- 個別インターフェイスモードでは、OSPFv2 との隣接関係は、制御ユニットの共有インターフェイスの 2 つのコンテキスト間でのみ確立できます。スタティック ネイバーの設定は、

ポイントツーポイン リンクでのみサポートされます。したがって、インターフェイスで許可されるのは 1 つのネイバー ステートメントだけです。

- クラスタで制御ロールの変更が発生した場合、次の挙動が発生します。
  - スパンド インターフェイス モードでは、ルータプロセスは制御ユニットでのみアクティブになり、データユニットでは停止状態になります。コンフィギュレーションが制御ユニットと同期されているため、各クラスタユニットには同じルータ ID があります。その結果、隣接ルータはロール変更時のクラスタのルータ ID の変更を認識しません。
  - 個別インターフェイス モードでは、ルータ プロセスはすべての個別のクラスタ ユニットでアクティブになります。各クラスタ ユニットは設定されたクラスタ プールから独自の個別のルータ ID を選択します。クラスタで制御ロールが変更されても、ルーティングトポロジは変更されません。

マルチプロトコル ラベル スイッチング（MPLS）と OSPF のガイドライン

MPLS 設定ルータから送信されるリンク ステート（LS）アップデート パケットに、Opaque Type-10 リンクステート アドバタイズメント（LSA）が含まれており、この LSA に MPLS ヘッダーが含まれている場合、認証は失敗し、アプライアンスはアップデート パケットを確認せずにサイレントにドロップします。ピア ルータは確認応答を受信していないため、最終的にネイバー関係を終了します。

ネイバー関係の安定を維持するため、ASA の Opaque 機能を無効にします。

```
router ospf process_ID_number
no nsf ietf helper
no capability opaque
```

（注） Firepower 4100/9300 モデルでは、複数の受信キュー間のロードバランシング不足のため、MPLS を使用した際に遅延が大きくなる可能性があります。

双方向フォワーディング検出（BFD）および OSPF に関する注意事項

- OSPFv2 および OSPFv3 インターフェイス（物理インターフェイス、サブインターフェイス、およびポートチャネル）で BFD を有効にできます。
- BFD は、VTI トンネル、DVTI トンネル、ループバック、スイッチポート、VNI、VTEP、および IRB インターフェイスではサポートされません。

ルートの再配布のガイドライン

- IPv4 プレフィックス リストを使用した OSPFv2 でのルートマップの再配布はサポートされています。ただし、IPv6 プレフィックス リストを使用した OSPFv3 でのルートマップの再配布はサポートされていません。再配布には、OSPF のルートマップでアクセス リストを使用します。

- OSPF が、EIGRP ネットワークの一部であるデバイスで設定されている場合、またはその逆の場合は、ルートにタグを付けるように OSPF ルータが設定されていることを確認します（EIGRP はルートタグをまだサポートしていません）。

  OSPF を EIGRP に再配布し、EIGRP を OSPF に再配布する場合は、いずれかのリンクまたはインターフェイスで障害が発生したときや、ルート発信元がダウンしたときにも、ルーティングループが発生します。あるドメインから同じドメインに再度ルートを再配布することを避けるため、ルータは、再配布する際にドメインに属しているルートにタグ付けすることができます。そして、そのタグに基づいて、リモートルータでそれらのルートをフィルタ処理できます。それらのルートはルーティングテーブルにインストールされないため、再度同じドメインに再配布されることはありません。

その他のガイドライン

- OSPFv2 および OSPFv3 は 1 つのインターフェイス上での複数インスタンスをサポートしています。
- OSPFv3 は、非クラスタ環境での ESP ヘッダーを介した暗号化をサポートしています。
- OSPFv3 は非ペイロード暗号化をサポートします。
- OSPFv2 は RFC 4811、4812 および 3623 でそれぞれ定義されている、Cisco NSF グレースフル リスタートおよびIETF NSF グレースフル リスタート メカニズムをサポートします。
- OSPFv3 は RFC 5187 で定義されているグレースフル リスタート メカニズムをサポートします。
- 配布可能なエリア内（タイプ 1）ルートの数は限られています。これらのルートでは、1 つのタイプ 1 LSA にすべてのプレフィックスが含まれています。システムではパケット サイズが 35 KB に制限されているため、3000 ルートの場合、パケットがこの制限を超過します。2900 本のタイプ 1 ルートが、サポートされる最大数であると考えてください。
- ルートアップデートがリンク上の最小 MTU より大きい場合に、ルートアップデートがドロップされることによる隣接フラップを回避するには、リンクの両側のインターフェイスで同じ MTU を設定する必要があります。
- ASA Virtual は、Azure クラウドルーティングの特性により、EIGRP や OSPF などのダイナミックな内部ルーティングプロトコルを使用できません。有効なルーティング テーブルは、仮想クライアントにスタティック/ダイナミック ルートが設定されているかどうかに関係なく、ネクスト ホップを決定します。

  現在、有効なルーティングテーブルまたはシステム ルーティング テーブルはどちらも表示できません。
- パケット サイズが 8190 を超えた場合、OSPFv3 は LS アップデートをドロップします。その結果、隣接関係は終了します。そのため、「ospfv3 mtu-ignore」コマンドを使用してスイッチを設定し、ネイバーシップの終了を回避します。

OSPFv2 の設定

ここでは、ASA で OSPFv2 プロセスを有効化する方法について説明します。

OSPFv2 をイネーブルにした後、ルート マップを定義する必要があります。詳細については、ルート マップの定義を参照してください。その後、デフォルト ルートを生成します。詳細については、スタティック ルートの設定を参照してください。

OSPFv2 プロセスのルート マップを定義した後で、ニーズに合わせてカスタマイズできます。ASA 上で OSPFv2 プロセスをカスタマイズする方法については、OSPFv2 のカスタマイズ （13 ページ）を参照してください。

OSPFv2 をイネーブルにするには、OSPFv2 ルーティング プロセスを作成し、このルーティング プロセスに関連付ける IP アドレスの範囲を指定し、さらにその IP アドレスの範囲にエリア ID を割り当てる必要があります。

最大 2 つの OSPFv2 プロセス インスタンスをイネーブルにできます。各 OSPFv2 プロセスには、独自のエリアとネットワークが関連付けられます。

OSPFv2 をイネーブルにするには、次の手順を実行します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** の順に選択します。

[OSPF Setup] ペインでは、OSPF プロセスのイネーブル化、OSPF エリアおよびネットワークの設定、および OSPF ルート集約の定義を行うことができます。

ステップ 2 ASDM で OSPF をイネーブルにするには、次の 3 つのタブを使用します。

- [Process Instances] タブでは、各コンテキストに対して最大 2 つの OSPF プロセス インスタンスを有効化できます。シングル コンテキスト モードおよびマルチ コンテキスト モードの両方がサポートされます。[Enable Each OSPF Process] チェックボックスをオンにすると、その OSPF プロセスの固有識別子である数値識別子を入力できるようになります。このプロセス ID は内部的に使用されるものであり、他の OSPF デバイスでの OSPF プロセス ID と一致している必要はありません。有効な値の範囲は 1 ～ 65535 です。各 OSPF プロセスには、独自のエリアとネットワークが関連付けられます。

  [Advanced] をクリックすると、[Edit OSPF Process Advanced Properties] ダイアログボックスが表示されます。ここで、各 OSPF プロセスに対して、[Router ID]、スパンド EtherChannel または個別インターフェイス クラスタリングのクラスタ IP アドレス プール、[Adjacency Changes]、[Administrative Route Distances]、[Timers] および [Default Information Originate] を設定することができます。ここで、OSPFv2 をサポートしているすべてのインターフェイスで BFD を有効にするか、特定の OSPFv2 インターフェイスで BFD を有効にすることができます（OSPFv2 インターフェイス パラメータの設定 （18 ページ）を参照）。

- [Area/Networks] タブでは、ASA 上で各 OSPF プロセスに対して指定されているエリアとネットワークが表示されます。このタブからは、エリア ID、エリア タイプ、およびそのエリアに対して設定された認証のタイプを表示できます。OSPFのエリアまたはネットワークを追加または編集する方法については、OSPFv2エリア パラメータの設定 （22ページ）を参照してください。
- [Route Summarization] タブでは、ABR を設定できます。OSPF では、ABR が 1 つのエリアのネットワークを別のエリアにアドバタイズします。1 つのエリア内のネットワーク番号が連続するように割り当てられている場合は、サマリー ルートをアドバタイズするように ABR を設定できます。このサマリー ルートには、そのエリア内の個々のネットワークのうち、指定の範囲に当てはまるものがすべて含まれます。詳細については、OSPFv2 エリア間のルート集約の設定 （17 ページ）を参照してください。

認証用のキー チェーンの設定

デバイスのデータ セキュリティと保護を向上させるため、循環キーを有効にして IGP ピアを認証することができます。循環キーは、悪意のあるユーザーがルーティング プロトコル認証に使用されているキーを推測できないようにし、ネットワークによる誤ったルートのアドバタイズやトラフィックのリダイレクトを防ぎます。頻繁にキーを変更することで、推測されるリスクを最終的に軽減します。キー チェーンを提供するルーティング プロトコルの認証を設定する場合は、キー チェーン内でキーを設定してライフタイムを重複させます。こうすることによって、キーで保護された通信がアクティブなキーがないことよって損失することを防ぐために役立ちます。キーのライフタイムが切れ、アクティブなキーがなくなると、OSPF は最後に有効だったキーを使用してピアとの隣接関係を維持します。

この項では、OSPF ピア認証用のキー チェーンを作成する方法について説明します。また、キー チェーンの属性を追加または編集するステップについても説明します。キー チェーン オブジェクトを設定した後、それを使用して、インターフェイスおよび仮想リンクの OSPFv2 認証を定義することができます。隣接関係を正常に確立するには、ピアに対して同じ認証タイプ（MD5 またはキー チェーン）とキー ID を使用します。インターフェイスの認証を定義する方法についてはOSPFv2 インターフェイス パラメータの設定 （18 ページ）を参照してください。仮想リンクについてはOSPF の仮想リンクの設定 （33 ページ）を参照してください。

キー チェーンを設定するには、次のステップを実行します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Key Chain]** を選択します。

ステップ 2 [Configure Key Chain] セクションで、[Add] をクリックします。

ステップ 3 キー チェーンの名前を [Add Key Chain] ダイアログボックスに入力し、[Ok] をクリックします。

作成されたキー チェーンの名前が [Configure Key Chain] グリッドのリストに表示されます。

ステップ 4 [Configure Key Chain] セクションからキー チェーン名を選択し、[Configure Key] セクションで [Add] をクリックします。既存のキーを編集するには、キー名を選択して [Edit] をクリックします。

選択したアクションに応じて、[Add Key] または [Edit Key] ダイアログボックスが表示されます。

ステップ 5 [キー ID（Key ID）] フィールドにキー識別子を指定します。

キー ID の値には 0 ～ 255 を使用できます。無効なキーを通知する場合にのみ、値 0 を使用します。

（注）
保存されたキー ID は編集できません。

ステップ 6 [Cryptographic Algorithm] ドロップダウンから、[MD5] を選択します。MD5 は、キー チェーンの認証に対してサポートされている唯一のアルゴリズムです。

ステップ 7 [Plain Text] または [Encrypted] オプション ボタンをクリックして暗号化タイプを選択し、[Authentication Key] フィールドにパスワードを入力します。

- パスワードの最大長は 80 文字です。
- パスワードは 10 文字以上必要です。また、数字の後に空白を含む文字列は使用できません。たとえば、「0 pass」や「1」は無効です。

ステップ 8 [Accept Lifetime] フィールドと [Send Lifetime] フィールドにライフタイムの値を入力します。

別のデバイスとのキー交換時にキーを受け入れるか、または送信するための時間間隔をデバイスに指定できます。終了時刻は、期間、受け入れ/送信ライフタイムが終了する絶対時間、または無期限です。

次に、開始と終了の値についての検証ルールを示します。

- 終了ライフタイムを指定した場合、開始ライフタイムを null にできません。
- 受け入れまたは送信のライフタイムの開始ライフタイムは、終了ライフタイムよりも前である必要があります。

ステップ 9 キー チェーンの属性を保存するには、[Ok] をクリックします。[Key Chain] ページで、[Appy] をクリックします。

次のタスク

これで、設定したキーチェーンを適用してインターフェイスおよび仮想リンクのOSPFv2認証を定義できるようになりました。

- OSPFv2 インターフェイス パラメータの設定 （18 ページ）
- OSPF の仮想リンクの設定 （33 ページ）

OSPFv2 ルータ ID の設定

OSPF ルータ ID は、OSPF データベース内の特定のデバイスを識別するために使用されます。OSPF システム内の 2 台のルータが同じルータ ID を持つことはできません。

ルータ ID が OSPF ルーティングプロセスで手動で設定されていない場合、ルータはアクティブインターフェイスの最も高い IP アドレスから決定されたルータ ID を自動的に設定します。ルータ ID を設定すると、ルータに障害が発生するか、または OSPF プロセスがクリアされ、ネイバー関係が再確立されるまで、ネイバーは自動的に更新されません。

OSPF ルータ ID の手動設定

ここでは、ASA の OSPFv2 プロセスで router-id を手動で設定する方法について説明します。

手順

ステップ 1 固定ルータ ID を使用するには、**router-id** コマンドを使用します。

router-id *ip-address*

例：

```
ciscoasa(config-router)# router-id 193.168.3.3
```

ステップ 2 以前の OSPF ルータ ID の動作に戻すには、**no router-id** コマンドを使用します。

no router-id *ip-address*

例：

```
ciscoasa(config-router)# no router-id 193.168.3.3
```

移行中のルータ ID の挙動

ある ASA、たとえば ASA 1 から別の ASA、たとえば ASA 2 に OSPF 設定を移行すると、次のルータ ID 選択動作が見られます。

1. すべてのインターフェイスがシャットダウン モードの場合、ASA 2 は OSPF router-id に IP アドレスを使用しません。すべてのインターフェイスが「admin down」ステートまたはシャットダウン モードの場合に考えられる router-id の設定は次のとおりです。
   - ASA 2 に以前設定された router-id がない場合は、次のメッセージが表示されます。

     ```
     %OSPF: Router process 1 is not running, please configure a router-id
     ```

最初のインターフェイスが起動すると、ASA 2 はこのインターフェイスの IP アドレスをルータ ID として取得します。

- ASA 2 に router-id が以前設定されていて、「no router-id」コマンドが発行されたときにすべてのインターフェイスが「admin down」ステートになっていた場合、ASA 2 は古いルータ ID を使用します。ASA 2 は、「clear ospf process」コマンドが発行されるまで、起動されたインターフェイスの IP アドレスが変更されても、古いルータ ID を使用します。

2. ASA 2 に router-id が以前設定されていて、「no router-id」コマンドが発行されたときに少なくとも 1 つのインターフェイスが「admin down」ステートまたはシャットダウン モードになっていない場合、ASA 2 は新しいルータ ID を使用します。インターフェイスが「down/down」ステートの場合でも、ASA 2 はインターフェイスの IP アドレスから新しいルータ ID を使用します。

OSPFv2 のカスタマイズ

ここでは、OSPFv2 プロセスをカスタマイズする方法について説明します。

OSPFv2 へのルートの再配布

ASA は、OSPFv2 ルーティング プロセス間のルート再配布を制御できます。

（注） 指定されたルーティング プロトコルから、ターゲット ルーティング プロセスに再配布できるルートを定義することでルートを再配布する場合は、デフォルト ルートを最初に生成する必要があります。スタティック ルートの設定を参照し、その後にルート マップの定義に従ってルート マップを定義します。

スタティック ルート、接続されているルート、RIP ルート、または OSPFv2 ルートを OSPFv2 プロセスに再配布するには、次の手順を実行します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Redistribution]** の順に選択します。

[Redistribution] ペインには、1 つのルーティング プロセスから OSPF ルーティング プロセスへのルートを再配布する場合のルールが表示されます。RIP および OSPF で検出されたルートを、EIGRP ルーティング プロセスに再配布することができます。スタティック ルートおよび接続されているルートも、EIGRP ルーティング プロセスに再配布できます。スタティックまたは

接続されているルートが、[Setup] > [Networks] タブで設定されたネットワークの範囲内にある場合は、そのルートを再配布する必要はありません。

ステップ 2 [Add] または [Edit] をクリックします。

または、[Redistribution] ペインでテーブル エントリ（ある場合）をダブルクリックすると、そのエントリの [Add/Edit OSPF Redistribution Entry] ダイアログボックスが開きます。

（注）
以降のステップはすべて、省略可能です。

[Add/Edit OSPF Redistribution Entry] ダイアログボックスでは、[Redistribution] テーブルに新しい再配布ルールを追加することや、既存の再配布ルールを編集することができます。既存の再配布ルールを編集するとき、一部の再配布ルール情報は変更できません。

ステップ 3 ルート再配布エントリに関連付ける OSPF プロセスを選択します。既存の再配布ルールを編集している場合、この設定は変更できません。

ステップ 4 どのソース プロトコルからルートを再配布するかを選択します。次のいずれかのオプションを選択できます。

- [Static]：スタティック ルートを OSPF ルーティング プロセスに再配布します。
- [Connected]：接続されたルート（インターフェイス上で IP アドレスをイネーブルにすることによって自動的に確立されるルート）を OSPF ルーティング プロセスに再配布します。接続済みルートは、AS の外部として再配布されます。
- [OSPF]：別の OSPF ルーティング プロセスからのルートを再配布します。リストから OSPF プロセス ID を選択してください。このプロトコルを選択すると、このダイアログボックスの [Match] のオプションが表示されます。これらのオプションは、スタティック、接続済み、RIP、または EIGRP ルートを再配布するときに選択できます。ステップ 5 に進みます。
- [RIP]：RIP ルーティング プロセスからルートを再配布します。
- [BGP]：BGP ルーティング プロセスからルートを再配布します。
- [EIGRP]：EIGRP ルーティング プロセスからルートを再配布します。リストから EIGRP ルーティング プロセスの自律システム番号を選択してください。

ステップ 5 OSPF をソース プロトコルとして選択した場合は、選択した OSPF ルーティング プロセスに別の OSPF ルーティング プロセスからのルートを再配布するのに使用される条件を選択します。これらのオプションは、スタティック、接続済み、RIP、または EIGRP ルートを再配布するときに選択できます。ルートが再配布されるには、選択した条件と一致している必要があります。次の一致条件から 1 つ以上を選択できます。

- [Internal]：ルートは特定の AS の内部です。
- [External 1]：自律システムの外部だが、OSPF にタイプ 1 外部ルートとしてインポートされるルート。

- [External 2]：自律システムの外部だが、OSPF にタイプ 2 外部ルートとしてインポートされるルート。
- [NSSA External 1]：自律システムの外部だが、OSPF にタイプ 2 NSSA ルートとしてインポートされるルート。
- [NSSA External 2]：自律システムの外部だが、OSPF にタイプ 2 NSSA ルートとしてインポートされるルート。

ステップ 6 [Metric Value] フィールドに、再配布されるルートのメトリック値を入力します。有効値の範囲は 1 ～ 16777214 です。

同じデバイス上で 1 つの OSPF プロセスから別の OSPF プロセスに再配布する場合、メトリック値を指定しないと、メトリックは 1 つのプロセスから他のプロセスへ存続します。他のプロセスを OSPF プロセスに再配布するときに、メトリック値を指定しない場合、デフォルトのメトリックは 20 です。

（注）
メトリックに一致するルートマップを使用したスタティックルートの再配布はサポートされていません。

ステップ 7 [Metric Type] で、次のオプションのいずれかを選択します。

- メトリックがタイプ 1 外部ルートの場合は、[1] を選択します。
- メトリックがタイプ 2 外部ルートの場合は、[2] を選択します。

ステップ 8 タグ値を [Tag Value] フィールドに入力します。

タグ値は 32 ビット 10 進数値です。この値は、OSPF 自身では使用されないが ASBR 間の情報伝達に使用できる外部ルートのそれぞれに関連付けられます。有効値の範囲は、0 ～ 4294967295 です。

ステップ 9 [Use Subnets] チェックボックスをオンにすると、サブネット化ルートの再配布がイネーブルになります。サブネットされていないルートだけを再配布するには、このチェックボックスをオフにします。

ステップ 10 再配布エントリに適用するルート マップの名前を [Route Map] ドロップダウン リストで選択します。

ステップ 11 ルート マップを追加または設定するには、[Manage] をクリックします。

[Configure Route Map] ダイアログボックスが表示されます。

ステップ 12 [Add] または [Edit] をクリックしてから、指定したルーティング プロトコルからのルートのうち、どれをターゲットのルーティング プロセスに再配布するかを定義します。詳細については、ルート マップの定義を参照してください。

ステップ 13 **[OK]** をクリックします。

OSPFv2 にルートを再配布する場合のルート集約の設定

他のプロトコルからのルートを OSPF に再配布する場合、各ルートは外部 LSA で個別にアドバタイズされます。その一方で、指定したネットワーク アドレスとマスクに含まれる再配布ルートすべてに対して 1 つのルートをアドバタイズするように ASA を設定することができます。この設定によって OSPF リンクステート データベースのサイズが小さくなります。

指定した IP アドレス マスク ペアと一致するルートは抑制できます。ルート マップで再配布を制御するために、タグ値を一致値として使用できます。

ルート サマリー アドレスの追加

[Summary Address] ペインには、各 OSPF ルーティング プロセスに設定されたサマリー アドレスに関する情報が表示されます。

他のルーティング プロトコルから学習したルートをサマライズできます。サマリーのアドバタイズに使用されるメトリックは、具体的なルートすべての中で最小のメトリックです。サマリー ルートは、ルーティング テーブルのサイズを削減するのに役立ちます。

OSPF のサマリー ルートを使用すると、OSPF ASBR は、そのアドレスでカバーされるすべての再配布ルートの集約として、1 つの外部ルートをアドバタイズします。OSPF に再配布されている、他のルーティング プロトコルからのルートだけをサマライズできます。

（注） OSPF は summary-address 0.0.0.0 0.0.0.0 をサポートしません。

ネットワーク アドレスとマスクに含まれる再配布ルートすべてに対して 1 つのサマリー ルートをアドバタイズするようにソフトウェアを設定するには、次の手順を実行します。

手順

ステップ 1 メインの ASDM ホーム ページで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Summary Address]** の順に選択します。

ステップ 2 [Add] をクリックします。

[Add OSPF Summary Address Entry] ダイアログボックスが表示されます。[Summary Address] テーブルの既存のエントリに新しいエントリを追加できます。既存のエントリを編集するとき、一部のサマリー アドレス情報は変更できません。

ステップ 3 [OSPF Process] ドロップダウン リストから、サマリー アドレスに関連付けられた指定 OSPF プロセス ID を選択します。既存のエントリを編集する場合、この情報は変更できません。

ステップ 4 [IP Address] フィールドにサマリー アドレスの IP アドレスを入力します。既存のエントリを編集する場合、この情報は変更できません。

ステップ 5 サマリーアドレスのネットワーク マスクを [Netmask] ドロップダウン リストから選択します。既存のエントリを編集する場合、この情報は変更できません。

ステップ 6 [Advertise]チェックボックスをオンにして、サマリールートをアドバタイズします。サマリーアドレスになるルートを抑止するには、このチェックボックスをオフにします。デフォルトでは、このチェック ボックスはオンになっています。

[Tag value] に表示される値は、各外部ルートに付加される 32 ビットの 10 進数値です。この値は OSPF 自身には使用されませんが、ASBR 間の情報伝達に使用できます。

ステップ 7 **[OK]** をクリックします。

OSPF サマリー アドレスの追加または編集

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** の順に選択します。

ステップ 2 [Route Summarization] タブをクリックします。

[Add/Edit Route Summarization Entry] ダイアログボックスが表示されます。

[Add/Edit Route Summarization Entry] ダイアログボックスでは、[Summary Address] テーブルに新しいエントリを追加したり、[Summary Address] テーブルの既存のエントリを変更したりできます。既存のエントリを編集するとき、一部のサマリー アドレス情報は変更できません。

ステップ 3 [OSPF Process] ドロップダウン リストから、サマリー アドレスに関連付けられた指定 OSPF プロセス ID を選択します。既存のエントリを編集する場合、この情報は変更できません。

ステップ 4 [IP Address] フィールドにサマリー アドレスの IP アドレスを入力します。既存のエントリを編集する場合、この情報は変更できません。

ステップ 5 サマリーアドレスのネットワーク マスクを [Netmask] ドロップダウン リストから入力します。既存のエントリを編集する場合、この情報は変更できません。

ステップ 6 [Advertise]チェックボックスをオンにして、サマリールートをアドバタイズします。サマリーアドレスになるルートを抑止するには、このチェックボックスをオフにします。デフォルトでは、このチェック ボックスはオンになっています。

OSPFv2 エリア間のルート集約の設定

ルート集約は、アドバタイズされるアドレスを統合することです。この機能を実行すると、1 つのサマリー ルートがエリア境界ルータを通して他のエリアにアドバタイズされます。OSPF のエリア境界ルータは、ネットワークをある 1 つのエリアから別のエリアへとアドバタイズしていきます。あるエリアにおいて連続する複数のネットワーク番号が割り当てられている場合、指定された範囲に含まれるエリア内の個別のネットワークをすべて含むサマリールートをアドバタイズするようにエリア境界ルータを設定することができます。

ルート集約のアドレス範囲を定義するには、次の手順を実行します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** の順に選択します。

ステップ 2 [Route Summarization] タブをクリックします。

[Add/Edit Route Summarization Entry] ダイアログボックスが表示されます。

[Add/Edit Route Summarization Entry] ダイアログボックスでは、[Summary Address] テーブルに新しいエントリを追加したり、[Summary Address] テーブルの既存のエントリを変更したりできます。既存のエントリを編集するとき、一部のサマリー アドレス情報は変更できません。

ステップ 3 [Area ID] フィールドに OSPF エリア ID を入力します。既存のエントリを編集する場合、この情報は変更できません。

ステップ 4 [IP Address] フィールドにサマリー アドレスの IP アドレスを入力します。既存のエントリを編集する場合、この情報は変更できません。

OSPFv2 インターフェイス パラメータの設定

必要に応じて一部のインターフェイス固有の OSPFv2 パラメータを変更できます。これらのパラメータを必ずしも変更する必要はありませんが、hello インターバル、デッドインターバル、認証キーの各インターフェイスパラメータは、接続されているネットワーク内のすべてのルータで一致している必要があります。これらのパラメータを設定する場合は、ネットワーク上のすべてのルータで、コンフィギュレーションの値が矛盾していないことを確認してください。

ASDM では、[Interface] ペインでインターフェイス固有の OSPF ルーティング プロパティ（たとえば OSPF メッセージ認証やプロパティ）を設定できます。OSPF のインターフェイスを設定するためのタブは次の 2 つです。

- [Authentication] タブには、ASA インターフェイスの OSPF 認証情報が表示されます。
- [Properties] タブには、各インターフェイスに定義された OSPF プロパティがテーブル形式で表示されます。

OSPFv2 インターフェイス パラメータを設定するには、次の手順を実行します。

手順

ステップ 1 [Authentication] タブをクリックすると、ASA のインターフェイスの認証情報が表示されます。このテーブルの行をダブルクリックすると、選択したインターフェイスの [Edit OSPF Authentication Interface] ダイアログボックスが開きます。

ステップ 2 [Edit] をクリックします。

[Edit OSPF Authentication Interface] ダイアログボックスが表示されます。[Edit OSPF Interface Authentication] ダイアログボックスでは、選択したインターフェイスの OSPF 認証タイプおよびパラメータを設定できます。

ステップ 3 関連するオプション ボタンをクリックして、認証タイプを選択します。

- [No authentication]：OSPF 認証が無効になります。
- [Area authentication, if defined]（デフォルト）：そのエリアに指定された認証タイプを使用します。エリア認証の設定については、OSPFv2 エリア パラメータの設定 （22 ページ）を参照してください。エリア認証はデフォルトでディセーブルになっています。したがって、それ以前にエリア認証タイプを指定していない限り、エリア認証を設定するインターフェイスでは、設定するまで認証がディセーブルになっています。
- [Password authentication]：クリア テキストによるパスワード認証が使用されます（セキュリティの懸念がある場合は推奨しません）。
- [MD5 authentication]：MD5 認証を使用します。
- [Key chain authentication]：キー チェーン認証を使用します（推奨）。認証用のキー チェーンの設定については認証用のキー チェーンの設定 （10 ページ）を参照してください。

ステップ 4 パスワード認証を選択した場合は、[Authentication Password] 領域で次のようにパスワードを入力します。

a) [Enter Password] フィールドに、最大 8 文字のテキスト文字列を入力します。
b) [Re-enter Password] フィールドに、パスワードを再入力します。

ステップ 5 キー チェーン認証を選択した場合は、[Enter Key chain name] フィールドにキー チェーン名を入力します。

ステップ 6 MD5 の ID とキーの設定を [ID] 領域で選択します。この領域には、MD5 認証がイネーブルのときの MD5 キーとパラメータの入力に関する設定があります。OSPF 認証を使用するインターフェイス上のすべてのデバイスで、同じ MD5 キーおよび ID を使用する必要があります。

a) [Key ID] フィールドに、数値のキー ID を入力します。有効値の範囲は、1 ～ 255 です。選択したインターフェイスのキー ID が表示されます。
b) [Key] フィールドに、最大 16 バイトの英数字文字列を入力します。選択したインターフェイスのキーが表示されます。
c) [Add] または [Delete] をクリックして、指定された MD5 キーを [MD5 ID and Key] テーブルに追加またはテーブルから削除します。

ステップ 7 [OK] をクリックします。

ステップ 8 [Properties] タブをクリックします。

ステップ 9 編集するインターフェイスを選択します。テーブルの行をダブルクリックすると、選択したインターフェイスの [Properties] タブ ダイアログボックスが開きます。

ステップ 10 [Edit] をクリックします。

[Edit OSPF Interface Properties] ダイアログボックスが表示されます。[Interface] フィールドに、OSPF プロパティ設定の対象であるインターフェイスの名前が表示されます。このフィールドは編集できません。

ステップ 11 このインターフェイスがブロードキャスト インターフェイスかどうかに応じて、[Broadcast] チェックボックスをオンまたはオフにします。

デフォルトでは、イーサネットインターフェイスの場合はこのチェックボックスがオンになっています。このチェックボックスをオフにすると、インターフェイスをポイントツーポイントの非ブロードキャストインターフェイスとして指定したことになります。インターフェイスをポイントツーポイントの非ブロードキャストとして指定すると、OSPF ルートを VPN トンネル経由で送信できます。

インターフェイスをポイントツーポイント、非ブロードキャストとして設定すると、次の制限が適用されます。

- インターフェイスにはネイバーを 1 つだけ定義できます。
- ネイバーは手動で設定する必要があります。詳細については、「スタティック OSPFv2 ネイバーの定義 （28 ページ）」を参照してください。
- クリプト ポイントを指すスタティック ルートを定義する必要があります。詳細については、「スタティック ルートの設定」を参照してください。
- トンネル経由の OSPF がインターフェイスで実行中である場合は、アップストリーム ルータを使用する通常の OSPF を同じインターフェイス上で実行することはできません。
- OSPF ネイバーを指定する前に、クリプト マップをインターフェイスにバインドする必要があります。これは、OSPF アップデートが VPN トンネルを通過できるようにするためです。OSPF ネイバーを指定した後で暗号マップをインターフェイスにバインドした場合は、**clear local-host all** コマンドを使用して OSPF 接続をクリアします。これで、OSPF 隣接関係を VPN トンネル経由で確立できるようになります。

ステップ 12 次のオプションを設定します。

- [Cost] フィールドに、このインターフェイスを通してパケット 1 個を送信するコストを決定する値を入力します。デフォルト値は 10 です。
- [Priority] フィールドに、OSPF ルータ優先順位の値を入力します。

  2 つのルータがネットワークに接続している場合、両方が指定ルータになろうとします。ルータ優先順位の高いデバイスが指定ルータになります。ルータ優先順位が同じ場合は、ルータ ID が高い方が指定ルータになります。

  この設定の有効値の範囲は 0 ～ 255 です。デフォルト値は 1 です。この設定に 0 を入力すると、適切でないルータが指定ルータになったり、指定ルータのバックアップが行われたりします。この設定は、ポイントツーポイントの非ブロードキャストインターフェイスとして設定されているインターフェイスには適用されません。

  マルチコンテキストモードでは、共有インターフェイスに 0 を指定して、デバイスが指定ルータにならないようにします。OSPFv2 インスタンスは、共有インターフェイス間で相互に隣接関係を形成できません。
- [MTU Ignore] チェックボックスをオンまたはオフにします。

OSPF は、ネイバーが共通インターフェイスで同じ MTU を使用しているかどうかをチェックします。このチェックは、ネイバーによる DBD パケットの交換時に行われます。DBD パケットに受信した MTU が着信インターフェイスに設定されている IP MTU より高い場合、OSPF の隣接性は確立されません。

- [Database filter] チェックボックスをオンまたはオフにします。

  この設定は、同期とフラッディングのときに発信 LSA インターフェイスをフィルタリングするのに使用します。デフォルトでは、OSPF は、LSA が到着したインターフェイスを除き、同じエリア内のすべてのインターフェイスで新しい LSA をフラッドします。完全メッシュ化トポロジでは、このフラッディングによって帯域幅が浪費されて、リンクおよび CPU の過剰使用につながることがあります。このチェックボックスをオンにすると、選択されているインターフェイスでは OSPF の LSA フラッディングが行われなくなります。

ステップ 13 このインターフェイスで BFD をイネーブルにするには、[BFD] ドロップダウンリストから [イネーブル（Enable）] を選択します。OSPFv2 をサポートしているすべてのインターフェイスで BFD をイネーブルにするには、OSPFv2 の設定 （9 ページ）を参照してください。

ステップ 14 （任意）[Advanced] をクリックして [Edit OSPF Advanced Interface Properties] ダイアログボックスを開きます。ここでは、OSPF hello 間隔、再送信間隔、送信遅延、およびデッド間隔の値を変更できます。

通常は、ネットワーク上で OSPF の問題が発生した場合にだけ、これらの値をデフォルトから変更する必要があります。

ステップ 15 [Intervals] セクションには、次の値を入力します。

- [Hello Interval] には、インターフェイス上で送信される hello パケットの間隔を秒単位で指定します。hello 間隔を小さくすると、トポロジ変更が検出されるまでの時間が短くなりますが、インターフェイス上で送信されるトラフィックは多くなります。この値は、特定のインターフェイス上のすべてのルータおよびアクセス サーバーで同じである必要があります。有効な値の範囲は、1 ～ 8192 秒です。デフォルト値は 10 秒です。

- [Retransmit Interval] には、このインターフェイスに属する隣接関係の LSA 再送信の間隔を秒単位で指定します。ルータはそのネイバーに LSA を送信すると、確認応答メッセージを受信するまでその LSA を保持します。確認応答を受信しなかった場合、ルータは LSA を再送信します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。有効な値の範囲は、1 ～ 8192 秒です。デフォルト値は 5 秒です。

- [Transmit Delay] には、このインターフェイス上で LSA パケット 1 個を送信するのに必要な時間の推定値を秒単位で指定します。更新パケット内の LSA には、送信前に、このフィールドで指定した値によって増分された経過時間が格納されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。有効な値の範囲は、1 ～ 8192 秒です。デフォルト値は 1 秒です。

ステップ 16 [Detecting Lost Neighbors] セクションで、次のいずれかを実行します。

- [Configure interval within which hello packets are not received before the router declares the neighbor to be down] をクリックします。[Dead Interval] フィールドで、ルータがダウンしていると見なす基準となる時間を秒数で指定します。この時間が経過しても hello パケットが 1 つも受信されない場合は、ネイバーがルータのダウンを宣言します。有効な値の範囲は、1 ～ 8192 秒です。この設定のデフォルト値は、[Hello Interval] フィールドで設定された時間の長さの 4 倍です。
- [Send fast hello packets within 1 seconds dead interval] をクリックします。[Hello multiplier] フィールドで、1 秒ごとに送信される hello パケットの数を指定します。有効な値は、3 ～ 20 です。

OSPFv2 エリア パラメータの設定

複数の OSPF エリア パラメータを設定できます。これらのエリア パラメータ（後述のタスク リストに表示）には、認証の設定、スタブ エリアの定義、デフォルト サマリー ルートへの特定のコストの割り当てがあります。認証では、エリアへの不正アクセスに対してパスワード ベースで保護します。

スタブ エリアは、外部ルートの情報が送信されないエリアです。その代わりに、ABR で生成されるデフォルトの外部ルートがあり、このルートは自律システムの外部の宛先としてスタブ エリアに送信されます。OSPF スタブ エリアのサポートを活用するには、デフォルトのルーティングをスタブ エリアで使用する必要があります。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** の順に選択します。

ステップ 2 [Area/Networks] タブをクリックします。

[Add OSPF Area] ダイアログボックスが表示されます。

ステップ 3 次に示す [Area Type] のオプションのいずれかを選択します。

- [Normal] を選択すると、このエリアは標準の OSPF エリアとなります。エリアを最初に作成するときは、このオプションがデフォルトで選択されています。
- [Stub] を選択すると、このエリアはスタブエリアとなります。スタブエリアには、その向こう側にルータまたはエリアはありません。スタブ エリアは、AS External LSA（タイプ 5 LSA）がスタブエリアにフラッドされないようにします。スタブエリアを作成するときに、サマリー LSA（タイプ 3 および 4）がそのエリアにフラッディングされないように設定するには、[Summary] チェックボックスをオフにします。

- [Summary]チェックボックスは、エリアをスタブエリアとして定義するときに、LSAがこのエリアに送信されないよう設定する場合にオフにします。デフォルトでは、スタブエリアの場合にこのチェックボックスはオンになります。
- [NSSA] を選択すると、このエリアは Not-So-Stubby Area となります。NSSA は、タイプ 7 LSA を受け入れます。NSSA を作成するときに、[Summary] チェックボックスをオフにすることでサマリー LSA がそのエリアにフラッディングされないようにするオプションがあります。また、[Redistribute] チェックボックスをオフにし、[Default Information Originate] チェックボックスをオンにすることで、ルートの再配布をディセーブルにすることもできます。

ステップ 4 [IP Address] フィールドに、エリアに追加するネットワークまたはホストの IP アドレスを入力します。デフォルトエリアを作成するには、**0.0.0.0** およびネットマスク **0.0.0.0** を使用します。**0.0.0.0** を入力できるエリアは 1 つだけです。

ステップ 5 [Network Mask] フィールドに、エリアに追加する IP アドレスまたはホストのネットワーク マスクを入力します。ホストを追加する場合、**255.255.255.255** マスクを選択します。

ステップ 6 [OSPF Authentication type] で、次のオプションから選択します。

- [None] を選択すると、OSPF エリア認証が無効になります。これがデフォルト設定です。
- [Password] を選択すると、クリアテキストパスワードがエリア認証に使用されますが、セキュリティが懸念となっている場合は推奨しません。
- [MD5] を選択すると、MD5 認証ができるようになります。

ステップ 7 [Default Cost] フィールドに値を入力して、[OSPF] エリアのデフォルト コストを指定します。

有効な値の範囲は 0 ～ 65535 です。デフォルト値は 1 です。

ステップ 8 **[OK]** をクリックします。

OSPFv2 フィルタ ルールの設定

OSPF アップデートで受信または送信されるルートまたはネットワークをフィルタリングするには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Filter Rules]** の順に選択します。

ステップ 2 [Add] をクリックします。

ステップ 3 [OSPF AS] で OSPF プロセス ID を選択します。

ステップ 4 [Access List] ドロップダウン リストから標準アクセス リストを選択します。[Manage] をクリックして、新しい ACL を追加します。

ステップ 5 [Direction] ドロップダウン リストから方向を選択します。方向は、フィルタを着信アップデートに適用するか、または発信アップデートに適用するかを指定します。

ステップ 6 着信フィルタには、オプションでインターフェイスを指定して、そのインターフェイスが受信するアップデートにフィルタを制限することができます。

ステップ 7 発信フィルタには、オプションで、配信されるルートのタイプを指定できます。

a) [Protocol] ドロップダウン リストからオプションを選択します。

[BGP]、[EIGRP]、[OSPF]、または [RIP] などのルーティング プロトコルを選択できます。

接続ルートから学習されたピアおよびネットワークをフィルタリングするには、[Connected] を選択します。

スタティック ルートから学習されたピアおよびネットワークをフィルタリングするには、[Static] を選択します。

b) [BGP]、[EIGRP]、または [OSPF] を選択した場合は、そのプロトコルのプロセス ID も [Process ID] で選択します。

ステップ 8 [OK] をクリックします。

ステップ 9 [適用（Apply）] をクリックします。

OSPFv2 NSSA の設定

NSSA の OSPFv2 への実装は、OSPFv2 のスタブ エリアに似ています。NSSA は、タイプ 5 の外部 LSA をコアからエリアにフラッディングすることはありませんが、自律システムの外部ルートをある限られた方法でエリア内にインポートできます。

NSSA は、再配布によって、タイプ 7 の自律システムの外部ルートを NSSA エリア内部にインポートします。これらのタイプ 7 の LSA は、NSSA の ABR によってタイプ 5 の LSA に変換され、ルーティング ドメイン全体にフラッディングされます。変換中は集約とフィルタリングがサポートされます。

OSPFv2 を使用する中央サイトから異なるルーティング プロトコルを使用するリモート サイトに接続しなければならない ISP またはネットワーク管理者は、NSSA を使用することによって管理を簡略化できます。

NSSA が実装される前は、企業サイトの境界ルータとリモート ルータ間の接続では、OSPFv2 スタブ エリアとしては実行されませんでした。これは、リモート サイト向けのルートは、スタブ エリアに再配布することができず、2 種類のルーティング プロトコルを維持する必要があったためです。RIP のようなシンプルなプロトコルを実行して再配布を処理する方法が一般的でした。NSSA が実装されたことで、企業ルータとリモート ルータ間のエリアを NSSA として定義することにより、NSSA で OSPFv2 を拡張してリモート接続をカバーできます。

この機能を使用する前に、次のガイドラインを参考にしてください。

- 外部の宛先に到達するために使用可能なタイプ 7 のデフォルト ルートを設定できます。設定すると、NSSA または NSSA エリア境界ルータまでのタイプ 7 のデフォルトがルータによって生成されます。

- 同じエリア内のすべてのルータは、エリアが NSSA であることを認識する必要があります。そうでない場合、ルータは互いに通信できません。

手順

ステップ 1 メインの ASDM ホーム ページで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** の順に選択します。

ステップ 2 [Area/Networks] タブをクリックします。

ステップ 3 [Add] をクリックします。

[Add OSPF Area] ダイアログボックスが表示されます。

ステップ 4 [Area Type] 領域の [NSSA] オプション ボタンをクリックします。

エリアを Not-So-Stubby Area にするには、このオプションを選択します。NSSA は、タイプ 7 LSA を受け入れます。NSSA を作成するときに、[Summary] チェックボックスをオフにすることでサマリーLSA がそのエリアにフラッディングされないようにするオプションがあります。また、[Redistribute] チェックボックスをオフにし、[Default Information Originate] チェックボックスをオンにすることで、ルートの再配布をディセーブルにすることもできます。

ステップ 5 [IP Address] フィールドに、エリアに追加するネットワークまたはホストの IP アドレスを入力します。デフォルトエリアを作成するには、**0.0.0.0** およびネットマスク **0.0.0.0** を使用します。**0.0.0.0** を入力できるエリアは 1 つだけです。

ステップ 6 [Network Mask] フィールドに、エリアに追加する IP アドレスまたはホストのネットワーク マスクを入力します。ホストを追加する場合、**255.255.255.255** マスクを選択します。

ステップ 7 [Authentication] 領域の [None] オプション ボタンをクリックすると、OSPF エリア認証がディセーブルになります。

ステップ 8 [Default Cost] フィールドに値を入力して、[OSPF] エリアのデフォルト コストを指定します。

有効な値の範囲は 0 ～ 65535 です。デフォルト値は 1 です。

ステップ 9 **[OK]** をクリックします。

クラスタリングの IP アドレス プールの設定（OSPFv2 および OSPFv3）

個別インターフェイス クラスタリングを使用する場合は、ルータ ID のクラスタ プールの IPv4 アドレスの範囲を割り当てることができます。

OSPFv2 の個別インターフェイスのルータ ID のクラスタ プールの IPv4 アドレスの範囲を割り当てるには、次の手順を実行します。

手順

ステップ 1 メインの ASDM ホーム ページで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** の順に選択します。

ステップ 2 [Process Instances] タブをクリックします。

ステップ 3 編集する OSPF プロセスを選択してから [Advanced] をクリックします。

[Edit OSPF Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 4 [Cluster Pool] オプション ボタンをクリックします。クラスタリングを使用している場合は、ルータ ID の IP アドレス プールを指定する必要はありません（つまりフィールドは空）。IP アドレス プールを入力しない場合、ASA は自動的に生成されたルータ ID を使用します。

ステップ 5 IP アドレス プールの名前を入力するか、省略記号をクリックして [Select IP Address Pool] ダイアログボックスを表示します。

ステップ 6 既存の IP アドレス プール名をダブルクリックして、[Assign] フィールドに追加します。[Add] をクリックして、新しい IP アドレス プールを作成することもできます。

[Add IPv4 Pool] ダイアログボックスが表示されます。

ステップ 7 [Name] フィールドに新しい IP アドレス プール名を入力します。

ステップ 8 開始 IP アドレスを入力するか、または省略記号をクリックして、[Browse Starting IP Address] ダイアログボックスを表示します。

ステップ 9 エントリをダブルクリックして、[Starting IP Address] フィールドに追加し、続いて [OK] をクリックします。

ステップ 10 最後の IP アドレスを入力するか、または省略記号をクリックして、[Browse Ending IP Address] ダイアログボックスを表示します。

ステップ 11 エントリをダブルクリックして、[Ending IP Address] フィールドに追加し、続いて [OK] をクリックします。

ステップ 12 ドロップダウン リストからサブネット マスクを選択し、続いて [OK] をクリックします。

[Select IP Address Pool] リストに、新しい IP アドレス プールが表示されます。

ステップ 13 新しい IP アドレス プール名をダブルクリックして、[Assign] フィールドに追加し、続いて [OK] をクリックします。

[Edit OSPF Process Advanced Properties] ダイアログボックスの [Cluster Pool] フィールドに、新しい IP アドレス プール名が表示されます。

ステップ 14 [OK] をクリックします。

ステップ 15 新しく追加された IP アドレス プール設定を変更する場合は、[Edit] をクリックします。

[Edit IPv4 Pool] ダイアログボックスが表示されます。

ステップ 16 ステップ 4 ～ 14 を繰り返します。

（注）

すでに割り当てられ、1 つ以上の接続プロファイルによってすでに使用されている既存の IP アドレス プールを編集または削除することはできません。

ステップ 17 [OK] をクリックします。

ステップ 18 OSPFv3 の個別インターフェイス クラスタリングのルータ ID のクラスタ プールに IPv4 アドレス範囲を割り当てるには、次の手順を実行します。

a) メインの ASDM ホーム ページで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Setup]** の順に選択します。

b) [Process Instances] タブをクリックします。

c) 編集する OSPF プロセスを選択してから [Advanced] をクリックします。

[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。

d) [Router ID] ドロップダウン リストから [Cluster Pool] オプションを選択します。ルータ ID の IP アドレス プールを指定する必要がない場合は、[Automatic] オプションを選択します。IP アドレス プールを設定しない場合、ASA は自動的に生成されたルータ ID を使用します。

e) IP アドレス プール名を入力します。省略記号をクリックして、[IP Address Pool] ダイアログボックスを表示することもできます。

f) 既存の IP アドレス プール名をダブルクリックして、[Assign] フィールドに追加します。[Add] をクリックして、新しい IP アドレス プールを作成することもできます。

[Add IPv4 Pool] ダイアログボックスが表示されます。

g) [Name] フィールドに新しい IP アドレス プール名を入力します。

h) 開始 IP アドレスを入力するか、または省略記号をクリックして、[Browse Starting IP Address] ダイアログボックスを表示します。

i) エントリをダブルクリックして、[Starting IP Address] フィールドに追加し、続いて [OK] をクリックします。

j) 最後の IP アドレスを入力するか、または省略記号をクリックして、[Browse Ending IP Address] ダイアログボックスを表示します。

k) エントリをダブルクリックして、[Ending IP Address] フィールドに追加し、続いて [OK] をクリックします。

l) ドロップダウン リストからサブネット マスクを選択し、続いて [OK] をクリックします。

[Select IP Address Pool] リストに、新しい IP アドレス プールが表示されます。

m) 新しい IP アドレス プール名をダブルクリックして、[Assign] フィールドに追加し、続いて [OK] をクリックします。

[Edit OSPF Process Advanced Properties] ダイアログボックスの [Cluster Pool] フィールドに、新しい IP アドレス プール名が表示されます。

n) [OK] をクリックします。

o) 新しく追加されたクラスタ プールの設定を変更する場合は、[Edit] をクリックします。

[Edit IPv4 Pool] ダイアログボックスが表示されます。

p) ステップ 4 ～ 14 を繰り返します。

（注）
すでに割り当てられ、別の OSPFv3 プロセスによってすでに使用されている既存の IP アドレス プールを編集または削除することはできません。

q) **[OK]** をクリックします。

スタティック OSPFv2 ネイバーの定義

ポイントツーポイントの非ブロードキャスト ネットワークを介して OSPFv2 ルートをアドバタイズするには、スタティック OSPFv2 ネイバーを定義する必要があります。この機能により、OSPFv2 アドバタイズメントを GRE トンネルにカプセル化しなくても、既存の VPN 接続でブロードキャストすることができます。

開始する前に、OSPFv2 ネイバーに対するスタティック ルートを作成する必要があります。スタティック ルートの作成方法の詳細については、スタティック ルートの設定を参照してください。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Static Neighbor]** の順に選択します。

ステップ 2 [Add] または [Edit] をクリックします。

[Add/Edit OSPF Neighbor Entry] ダイアログボックスが表示されます。このダイアログボックスでは、新しいスタティック ネイバーを定義することや、既存のスタティック ネイバーの情報を変更することができます。ポイントツーポイントの非ブロードキャスト インターフェイスごとに、スタティック ネイバーを 1 つ定義する必要があります。次の制約事項に注意してください。

- 異なる 2 つの OSPF プロセスに対して同じスタティック ネイバーを定義できません。
- 各スタティック ネイバーにスタティック ルートを定義する必要があります

ステップ 3 [OSPF Process] ドロップダウン リストで、スタティック ネイバーに関連付ける OSPF プロセスを選択します。既存のスタティック ネイバーを編集している場合、この値は変更できません。

ステップ 4 [Neighbor] フィールドに、スタティック ネイバーの IP アドレスを入力します。

ステップ 5 [Interface] フィールドで、スタティック ネイバーに関連付けるインターフェイスを選択します。既存のスタティック ネイバーを編集している場合、この値は変更できません。

ステップ 6 **[OK]** をクリックします。

ルート計算タイマーの設定

OSPFv2 によるトポロジ変更受信と最短パス優先（SPF）計算開始との間の遅延時間が設定できます。最初に SPF を計算してから次に計算するまでの保持時間も設定できます。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** の順に選択します。

ステップ 2 [Process Instances] タブをクリックします。

ステップ 3 編集する OSPF プロセスを選択してから [Advanced] をクリックします。

[Edit OSPF Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 4 [Timers] 領域では、LSA ペーシングおよび SPF 計算のタイマーの設定に使用される値を変更できます。[Timers] 領域で、次の値を入力します。

- [Initial SPF Delay] は、OSPF がトポロジ変更を受信してから SPF 計算が開始されるまでの時間（ミリ秒）を指定します。有効な値の範囲は、0 ～ 600000 ミリ秒です。
- [Minimum SPF Hold Time] は、連続する SPF 計算間の保持時間をミリ秒で指定します。有効な値の範囲は、0 ～ 600000 ミリ秒です。
- [Maximum SPF Wait Time] は、2 回の連続する SPF 計算間の最大待機時間を指定します。有効な値の範囲は、0 ～ 600000 ミリ秒です。

ステップ 5 **[OK]** をクリックします。

ネイバーの起動と停止のロギング

デフォルトでは、OSPFv2 ネイバーがアップ状態またはダウン状態になったときに、syslog メッセージが生成されます。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** の順に選択します。

ステップ 2 [Process Instances] タブをクリックします。

ステップ 3 [Advanced] をクリックします。

[Edit OSPF Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 4 [Adjacency Changes] 領域には、syslog メッセージ送信を引き起こす隣接関係変更を定義するための設定があります。[Adjacency Changes] 領域で、次の値を入力します。

- [Log Adjacency Changes] チェックボックスをオンにすると、OSPFv2 ネイバーがアップ状態またはダウン状態になるたびに ASA によって syslog メッセージが送信されるようになります。この設定は、デフォルトでオンになっています。
- [Log Adjacency Changes Detail] チェックボックスをオンにすると、ネイバーがアップ状態またはダウン状態になったときだけでなく、状態の変更が発生したときにも ASA によって syslog メッセージが送信されるようになります。デフォルトでは、この設定はオフになっています。

ステップ 5 [OK] をクリックします。

（注）
ネイバーのアップまたはダウンのメッセージが送信されるには、ロギングがイネーブルになっている必要があります。

認証用のキー チェーンの設定

デバイスのデータ セキュリティと保護を向上させるため、循環キーを有効にして IGP ピアを認証することができます。循環キーは、悪意のあるユーザーがルーティング プロトコル認証に使用されているキーを推測できないようにし、ネットワークによる誤ったルートのアドバタイズやトラフィックのリダイレクトを防ぎます。頻繁にキーを変更することで、推測されるリスクを最終的に軽減します。キー チェーンを提供するルーティング プロトコルの認証を設定する場合は、キー チェーン内でキーを設定してライフタイムを重複させます。こうすることによって、キーで保護された通信がアクティブなキーがないことよって損失することを防ぐために役立ちます。キーのライフタイムが切れ、アクティブなキーがなくなると、OSPF は最後に有効だったキーを使用してピアとの隣接関係を維持します。

この項では、OSPF ピア認証用のキー チェーンを作成する方法について説明します。また、キー チェーンの属性を追加または編集するステップについても説明します。キー チェーン オブジェクトを設定した後、それを使用して、インターフェイスおよび仮想リンクの OSPFv2 認証を定義することができます。隣接関係を正常に確立するには、ピアに対して同じ認証タイプ（MD5 またはキー チェーン）とキー ID を使用します。インターフェイスの認証を定義する方法についてはOSPFv2 インターフェイス パラメータの設定 （18 ページ）を参照してください。仮想リンクについてはOSPF の仮想リンクの設定 （33 ページ）を参照してください。

キー チェーンを設定するには、次のステップを実行します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Key Chain]** を選択します。

ステップ 2 [Configure Key Chain] セクションで、[Add] をクリックします。

ステップ 3 キー チェーンの名前を [Add Key Chain] ダイアログボックスに入力し、[Ok] をクリックします。

作成されたキー チェーンの名前が [Configure Key Chain] グリッドのリストに表示されます。

ステップ 4 [Configure Key Chain] セクションからキー チェーン名を選択し、[Configure Key] セクションで [Add] をクリックします。既存のキーを編集するには、キー名を選択して [Edit] をクリックします。

選択したアクションに応じて、[Add Key] または [Edit Key] ダイアログボックスが表示されます。

ステップ 5 [キー ID（Key ID）] フィールドにキー識別子を指定します。

キー ID の値には 0 ～ 255 を使用できます。無効なキーを通知する場合にのみ、値 0 を使用します。

（注）
保存されたキー ID は編集できません。

ステップ 6 [Cryptographic Algorithm] ドロップダウンから、[MD5] を選択します。MD5 は、キー チェーンの認証に対してサポートされている唯一のアルゴリズムです。

ステップ 7 [Plain Text] または [Encrypted] オプション ボタンをクリックして暗号化タイプを選択し、[Authentication Key] フィールドにパスワードを入力します。

- パスワードの最大長は 80 文字です。
- パスワードは 10 文字以上必要です。また、数字の後に空白を含む文字列は使用できません。たとえば、「0 pass」や「1」は無効です。

ステップ 8 [Accept Lifetime] フィールドと [Send Lifetime] フィールドにライフタイムの値を入力します。

別のデバイスとのキー交換時にキーを受け入れるか、または送信するための時間間隔をデバイスに指定できます。終了時刻は、期間、受け入れ/送信ライフタイムが終了する絶対時間、または無期限です。

次に、開始と終了の値についての検証ルールを示します。

- 終了ライフタイムを指定した場合、開始ライフタイムを null にできません。
- 受け入れまたは送信のライフタイムの開始ライフタイムは、終了ライフタイムよりも前である必要があります。

ステップ 9 キー チェーンの属性を保存するには、[Ok] をクリックします。[Key Chain] ページで、[Appy] をクリックします。

次のタスク

これで、設定したキーチェーンを適用してインターフェイスおよび仮想リンクのOSPFv2認証を定義できるようになりました。

• OSPFv2 インターフェイス パラメータの設定 （18 ページ）
• OSPF の仮想リンクの設定 （33 ページ）

OSPF でのフィルタリングの設定

[Filtering] ペインには、各 OSPF プロセスに対して設定済みの ABR タイプ 3 LSA フィルタが表示されます。

ABR タイプ 3 LSA フィルタを設定すると、指定したプレフィックスだけが 1 つのエリアから別のエリアに送信され、その他のプレフィックスはすべて制限されます。このタイプのエリアフィルタリングは、特定の OSPF エリアから、特定の OSPF エリアへ、または同じ OSPF エリアへ同時に適用できます。

OSPF ABR タイプ 3 LSA フィルタリングによって、OSPF エリア間のルート再配布の制御が向上します。

（注） フィルタリングされるのは、ABR から送信されるタイプ 3 LSA だけです。

OSPF でのフィルタリングを設定するには、次の手順を実行します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Filtering]** の順に選択します。

ステップ 2 [Add] または [Edit] をクリックします。

[Add or OSPF Filtering Entry] ダイアログボックスでは、新しいフィルタを [Filter] テーブルに追加することや、既存のフィルタを修正することができます。既存のフィルタを編集するとき、一部のフィルタリング情報は変更できません。

ステップ 3 フィルタ エントリに関連付ける OSPF プロセスを [OSPF Process] ドロップダウン リストで選択します。

ステップ 4 フィルタ エントリに関連付けるエリア ID を [Area ID] ドロップダウン リストで選択します。既存のフィルタ エントリを編集している場合、この設定は変更できません。

ステップ 5 プレフィックス リストを [Prefix List] ドロップダウン リストで選択します。

ステップ 6 フィルタリングするトラフィックの方向を [Traffic Direction] ドロップダウン リストで選択します。

OSPF エリアへの LSA をフィルタリングするには [着信（Inbound）] を選択し、OSPF エリアからの LSA をフィルタリングするには [発信（Outbound）] を選択します。既存のフィルタ エントリを編集している場合、この設定は変更できません。

ステップ 7 [Manage] をクリックすると [Configure Prefix Lists] ダイアログボックスが表示され、ここでプレフィックス リストとプレフィックス ルールを追加、編集、または削除できます。詳細については、プレフィックス リストの設定およびルート アクションのメトリック値の設定を参照してください。

ステップ 8 **[OK]** をクリックします。

OSPF の仮想リンクの設定

OSPF ネットワークにエリアを追加し、そのエリアをバックボーン エリアに直接接続できない場合、仮想リンクを作成する必要があります。仮想リンクは、通過エリアと呼ばれる共通エリアを持つ 2 つの OSPF デバイスを接続します。OSPF デバイスのいずれかは、バックボーン エリアに接続されている必要があります。

新しい仮想リンクを定義する、または既存の仮想リンクのプロパティを変更するには、次の手順を実行します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Virtual Link]** の順に選択します。

ステップ 2 [Add] または [Edit] をクリックします。

[Add OSPF Virtual Link] または [Edit OSPF Virtual Link] ダイアログボックスが表示され、ここで新しい仮想リンクを定義することや、既存の仮想リンクのプロパティを変更することができます。

ステップ 3 仮想リンクに関連付ける OSPF プロセス ID を [OSPF Process] ドロップダウン リストで選択します。既存の仮想リンク エントリを編集している場合、この設定は変更できません。

ステップ 4 仮想リンクに関連付けるエリア ID を [Area ID] ドロップダウン リストで選択します。

ネイバー OSPF デバイスによって共有されるエリアを選択します。[NSSA] エリアまたは [Stub] エリアは選択できません。既存の仮想リンク エントリを編集している場合、この設定は変更できません。

ステップ 5 [Peer Router ID] フィールドに、仮想リンク ネイバーのルータ ID を入力します。

既存の仮想リンク エントリを編集している場合、この設定は変更できません。

ステップ 6 仮想リンクの詳細プロパティを編集するには、[Advanced] をクリックします。

[Advanced OSPF Virtual Link Properties] ダイアログボックスが表示されます。このエリアにある仮想リンクに対して、OSPF プロパティを設定できます。プロパティには、認証およびパケット間隔設定が含まれます。

ステップ 7 [Authentication] 領域で、[Authentication type] を選択します。次のオプション ボタンのいずれかをクリックします。

- [No authentication]：OSPF 認証が無効になります。
- [Password authentication]：クリア テキストによるパスワード認証が使用されます（セキュリティの懸念がある場合は推奨しません）。
- [MD5 authentication]：MD5 認証を使用します。
- [Key chain authentication]：キー チェーン認証を使用します（推奨）。認証用のキー チェーンの設定については認証用のキー チェーンの設定 （10 ページ）を参照してください。

ステップ 8 [Authentication Password] 領域で、パスワードを入力し、もう一度入力します（パスワード認証がイネーブルのとき）。パスワードは、最大 8 文字のテキスト文字列であることが必要です。

ステップ 9 [MD5 IDs and Key] 領域で、MD5 のキーとパラメータを入力します（MD5 認証がイネーブルのとき）。OSPF 認証を使用するインターフェイス上のすべてのデバイスで、同じ MD5 キーおよび ID を使用する必要があります。次の設定を指定します。

a) [Key ID] フィールドに、数値のキー ID を入力します。有効値の範囲は、1 ～ 255 です。選択したインターフェイスのキー ID が表示されます。
b) [Key] フィールドに、最大 16 バイトの英数字文字列を入力します。選択したインターフェイスのキー ID が表示されます。
c) [Add] または [Delete] をクリックして、指定された MD5 キーを [MD5 ID and Key] テーブルに追加またはテーブルから削除します。

ステップ 10 [Interval] 領域で、パケットの間隔を指定します。次のオプションから選択します。

- [Hello Interval] には、インターフェイス上で送信される hello パケットの間隔を秒単位で指定します。hello 間隔を小さくすると、トポロジ変更が検出されるまでの時間が短くなりますが、インターフェイス上で送信されるトラフィックは多くなります。この値は、特定のインターフェイス上のすべてのルータおよびアクセス サーバーで同じである必要があります。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 10 秒です。
- [Retransmit Interval] には、このインターフェイスに属する隣接関係の LSA 再送信の間隔を秒単位で指定します。ルータはそのネイバーに LSA を送信すると、確認応答メッセージを受信するまでその LSA を保持します。確認応答を受信しなかった場合、ルータは LSA を再送信します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 5 秒です。
- [Transmit Delay] には、このインターフェイス上で LSA パケット 1 個を送信するのに必要な時間の推定値を秒単位で指定します。更新パケット内の LSA には、送信前に、このフィールドで指定した値によって増分された経過時間が格納されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。有効値の範囲は、1～65535 秒です。デフォルト値は 1 秒です。
- [Dead Interval] には、ルータがダウンしていると見なす基準となる時間を秒数で指定します。この時間が経過しても hello パケットが 1 つも受信されない場合は、ネイバーがルー

タのダウンを宣言します。有効値の範囲は 1 ～ 65535 です。このフィールドのデフォルト値は、[Hello Interval] フィールドに設定されている時間間隔の 4 倍です。

ステップ 11 **[OK]** をクリックします。

OSPFv3 の設定

ここでは、OSPFv3 ルーティング プロセスの設定に関連するタスクについて説明します。

OSPFv3 の有効化

OSPFv3 をイネーブルにするには、OSPFv3 ルーティング プロセスを作成し、OSPFv3 用のエリアを作成して、OSPFv3 のインターフェイスをイネーブルにする必要があります。その後、ターゲットの OSPFv3 ルーティング プロセスにルートを再配布する必要があります。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Setup]** の順に選択します。

ステップ 2 [Process Instances] タブで、[Enable OSPFv3 Process] チェックボックスをオンにします。最大 2 つの OSPF プロセス インスタンスをイネーブルにできます。シングル コンテキスト モードだけがサポートされます。

ステップ 3 [Process ID] フィールドにプロセス ID を入力します。ID は、任意の正の整数が可能です。

ステップ 4 OSPFv3 をサポートしているすべてのインターフェイスで BFD を有効にするには、[詳細（Advanced）] をクリックします。[OPPFv3プロセスの詳細プロパティの編集（Edit OPPFv3 Process Advanced Properties）] ウィンドウの [すべてのインターフェイスでの BFD の有効化（Enable BFD on all interfaces）] で、[BFDの有効化（Enable BFD）] チェックボックスをオンにします。特定の OSPFv3 インターフェイスで BFD を有効にするには、OSPFv3 インターフェイス パラメータの設定 （35 ページ）を参照してください。

ステップ 5 [Apply] をクリックして変更内容を保存します。

ステップ 6 以降の手順については、OSPFv3エリア パラメータの設定 （37ページ）を参照してください。

OSPFv3 インターフェイス パラメータの設定

必要に応じて特定のインターフェイス固有の OSPFv3 パラメータを変更できます。これらのパラメータを必ずしも変更する必要はありませんが、hello interval と dead interval というインターフェイス パラメータは、接続されているネットワーク内のすべてのルータで一致している必要

があります。これらのパラメータを設定する場合は、ネットワーク上のすべてのルータで、コンフィギュレーションの値が矛盾していないことを確認してください。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Interfaces]** の順に選択します。

ステップ 2 [Authentication] タブをクリックします。

ステップ 3 インターフェイスの認証パラメータを指定するには、インターフェイスを選択し、[Edit] をクリックします。

[OSPFv3インターフェイス認証の編集（Edit OSPFv3 Interface Authentication）] ダイアログボックスが表示されます。

ステップ 4 [認証タイプ（Authentication Type）] ドロップダウンリストから認証タイプを選択します。使用可能なオプションは、[エリア（Area）]、[インターフェイス（Interface）]、[なし（None）] です。[なし（None）] オプションを選択すると、認証が行われません。

ステップ 5 [認証アルゴリズム（Authentication Algorithm）] ドロップダウンリストから認証アルゴリズムを選択します。サポートされる値は、[SHA-1] および [MD5] です。

ステップ 6 [認証キー（Authentication Key）] フィールドに認証キーを入力します。MD5 認証を使用する場合、キーの長さは 32 桁の 16 進数（16 バイト）である必要があります。SHA-1 認証を使用する場合、キーの長さは 40 桁の 16 進数（20 バイト）である必要があります。

ステップ 7 [暗号化アルゴリズム（Encryption Algorithm）] ドロップダウンリストから暗号化アルゴリズムを選択します。サポートされる値は、[AES-CDC]、[3DES]、[DES] です。ヌルのエントリは暗号化されません。

ステップ 8 [暗号キー（Encryption Key）] フィールドに暗号キーを入力します。

ステップ 9 [OK] をクリックします。

ステップ 10 [Properties] タブをクリックします。

ステップ 11 プロパティを変更するインターフェイスを選択し、[Edit] をクリックします。

[Edit OSPFv3 Interface Properties] ダイアログボックスが表示されます。

ステップ 12 [Enable OSPFv3 on this interface] チェックボックスをオンにします。

ステップ 13 ドロップダウン リストからプロセス ID を選択します。

ステップ 14 ドロップダウン リストから領域 ID を選択します。

ステップ 15 （オプション）インターフェイスに割り当てる領域インスタンス ID を指定します。インターフェイスは、OSPFv3 エリアを 1 つだけ保有できます。複数のインターフェイスで同じエリアを使用でき、各インターフェイスは異なるエリア インスタンス ID を使用できます。

ステップ 16 ドロップダウン リストからネットワーク タイプを選択します。サポートされるオプションは、[Default]、[Broadcast]、[Point-to-Point] です。

ステップ 17 [Cost] フィールドにインターフェイスでのパケット送信コストを入力します。

ステップ 18 [Priority] フィールドにルータ プライオリティを入力します。これは、ネットワークにおける指定ルータの特定に役立ちます。有効値の範囲は 0 ～ 255 です。

ステップ 19 このインターフェイスで BFD をイネーブルにするには、[BFDの設定（BFD Configuration）] ドロップダウンリストから [イネーブル（Enable）] を選択します。OSPFv3 をサポートするすべてのインターフェイスで BFD をイネーブルにするには、OSPFv3 の有効化 （35 ページ）を参照してください。

ステップ 20 [Disable MTU mismatch detection] チェックボックスをオンにして、DBD パケットが受信された場合の OSPF MTU 不一致検出をディセーブルにします。OSPF MTU 不一致検出は、デフォルトでイネーブルになっています。

ステップ 21 [Filter outgoing link state advertisements] チェックボックスをオンにして、OSPFv3 インターフェイスに対する出力 LSA をフィルタします。デフォルトでは、すべての発信 LSA がインターフェイスにフラッディングされます。

ステップ 22 インターフェイスへの LSA の不要なフラッディングとリフレッシュを減らすには、[OSPFフラッドリダクション（OSPF Flood Reduction）] チェックボックスをオンにします。

ステップ 23 [タイマー（Timers）] 領域の [Dead間隔（Dead Interval）] フィールドに、hello パケットが確認されない場合にルータがダウンしたとネイバーが判断するまでの待ち時間を秒単位で入力します。この値はネットワーク上のすべてのノードで同じにする必要があります。値の範囲は、1 ～ 65535 です。

ステップ 24 [hello間隔（Hello Interval）] フィールドに、インターフェイスで送信される hello パケットの間隔を秒単位で入力します。この値は特定のネットワーク上のすべてのノードで同じにする必要があります。値の範囲は、1 ～ 65535 です。デフォルトの間隔は、イーサネット インターフェイスで 10 秒、非ブロードキャスト インターフェイスで 30 秒です。

ステップ 25 [再伝送間隔（Retransmit Interval）] フィールドに、インターフェイスに属する隣接関係の LSA 再送信間隔を秒単位で入力します。接続ネットワーク上の任意の 2 台のルータ間で想定される往復遅延より大きな値にする必要があります。有効な値の範囲は、1 ～ 65535 秒です。デフォルトは 5 秒です。

ステップ 26 [伝送遅延（Transmit Delay）] フィールドに、インターフェイスでのリンクステートアップデートパケットの送信に必要な予想時間を秒単位で入力します。有効な値の範囲は、1 ～ 65535 秒です。デフォルト値は 1 秒です。

ステップ 27 [OK] をクリックします。

ステップ 28 [Apply] をクリックして変更内容を保存します。

OSPFv3 エリア パラメータの設定

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Setup]** の順に選択します。

ステップ 2 [Areas] タブをクリックします。

ステップ 3 新しいエリアを追加するには、[Add] をクリックします。既存のエリアを変更するには、[Edit] をクリックします。選択したエリアを削除するには、[Delete] をクリックします。

[Add OSPFv3 Area] ダイアログボックスまたは [Edit OSPFv3 Area] ダイアログボックスが表示されます。

ステップ 4 [OSPFv3 Process ID] ドロップダウン リストから、プロセス ID を選択します。

ステップ 5 ルートが集約されるエリアを指定するエリア ID を [Area ID] フィールドに入力します。

ステップ 6 [Area Type] ドロップダウン リストからエリア タイプを選択します。使用可能なオプションは、[Normal]、[NSSA]、[Stub] です。

ステップ 7 エリアにサマリー LSA の送信を許可する場合は、[Allow sending of summary LSAs into the area] チェックボックスをオンにします。

ステップ 8 標準および not so stubby エリアへのインポート ルートの再配布を許可するには、[Redistribution imports routes to normal and NSSA areas] チェックボックスをオンにします。

ステップ 9 OSPFv3 ルーティング ドメインにデフォルト外部ルートを生成するには、[Default information originate] チェックボックスをチェックします。

ステップ 10 デフォルト ルートの生成に使用するメトリックを [Metric] フィールドに入力します。デフォルト値は 10 です。有効なメトリック値の範囲は、0 ～ 16777214 です。

ステップ 11 [Metric Type] ドロップダウン リストからメトリック タイプを選択します。メトリック タイプは、OSPFv3 ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられた外部リンク タイプです。使用可能なオプションは、タイプ 1 外部ルートの場合は 1、タイプ 2 外部ルートの場合は 2 です。

ステップ 12 [Default Cost] フィールドにコストを入力します。

ステップ 13 [OK] をクリックします。

ステップ 14 [Route Summarization] タブをクリックします。

ステップ 15 ルートを統合および集約するための新しい範囲を指定するには、[Add] をクリックします。ルートを統合および集約する既存の範囲を変更するには、[Edit] をクリックします。

[Add Route Summarization] ダイアログボックスまたは [Edit Route Summarization] ダイアログボックスが表示されます。

ステップ 16 [Process ID] ドロップダウン リストからプロセス ID を選択します。

ステップ 17 [Area ID] ドロップダウン リストからエリア ID を選択します。

ステップ 18 [IPv6 Prefix/Prefix Length] フィールドに IPv6 プレフィックスとプレフィックス長を入力します。

ステップ 19 （オプション）このサマリー ルートのメトリックまたはコストを入力します。宛先への最短パスを決定するための OSPF SPF 計算で使用します。有効値の範囲は 0 ～ 16777215 です。

ステップ 20 [Advertised] チェックボックスをオンにして、アドレス範囲の状態をアドバタイズされた設定し、タイプ 3 サマリー LSA を生成します。

ステップ 21 [OK] をクリックします。

ステップ 22 以降の手順については、仮想リンク ネイバーの設定 （38 ページ）を参照してください。

仮想リンク ネイバーの設定

仮想リンク ネイバーを設定するには、次の手順を実行します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Virtual Link]** の順に選択します。

ステップ 2 新しい仮想リンク ネイバーを追加するには、[Add] をクリックします。既存の仮想リンク ネイバーを変更するには、[Edit] をクリックします。指定された仮想リンク ネイバーを削除するには、[Delete] をクリックします。

[Add Virtual Link] ダイアログボックスまたは [Edit Virtual Link] ダイアログボックスが表示されます。

ステップ 3 [Process ID] ドロップダウン リストからプロセス ID を選択します。

ステップ 4 [Area ID] ドロップダウン リストからエリア ID を選択します。

ステップ 5 [Peer Router ID] フィールドにピア ルータ ID（IP アドレス）を入力します。

ステップ 6 （オプション）[TTL Security] フィールドに仮想リンクの存続可能時間 (TTL) のセキュリティのホップ数を入力します。ホップ数の値は 1 ～ 254 の範囲で指定します。

ステップ 7 [Timers] 領域の [Dead Interval] フィールドに、hello パケットが表示されない場合に、ルータがダウンしたとネイバーが判断するまでの待ち時間を秒単位で入力します。Dead 間隔は符号なし整数です。デフォルトは hello 間隔の 4 倍または 40 秒です。この値は、共通のネットワークに接続されているすべてのルータおよびアクセス サーバーで同じであることが必要です。有効値の範囲は 1 ～ 8192 です。

ステップ 8 [Hello Interval] フィールドに、インターフェイスで送信される hello パケットの間隔を秒単位で入力します。hello 間隔は、hello パケットでアドバタイズされる符号なし整数です。この値は、共通のネットワークに接続されているすべてのルータおよびアクセス サーバーで同じであることが必要です。有効値の範囲は 1 ～ 8192 です。デフォルトは 10 です。

ステップ 9 [Retransmit Interval] フィールドに、インターフェイスに属している隣接ルータの LSA 再送信間隔を秒単位で入力します。再送信間隔は、接続されているネットワーク上の任意の 2 台のルータ間の予想されるラウンドトリップ遅延です。この値は、予想されるラウンドトリップ遅延より大きくなり、1 ～ 8192 の範囲で指定できます。デフォルトは 5 分です。

ステップ 10 [Transmit Delay] フィールドに、インターフェイスのリンク ステート アップデート パケットの送信に必要な予想時間を秒単位で入力します。ゼロよりも大きい整数値を指定します。アップデート パケット内の LSA 自体の経過時間は、転送前にこの値の分だけ増分されます。値の範囲は 1 ～ 8192 です。デフォルトは 1 です。

ステップ 11 [Authentication] 領域の [Enable Authentication] チェックボックスをオンにして、認証をイネーブルにします。

ステップ 12 [Security Policy Index] フィールドに、セキュリティ ポリシー インデックスを入力します。値の範囲は、256～4294967295 の数字です。

ステップ 13 [Authentication Algorithm] ドロップダウン リストから認証アルゴリズムを選択します。サポートされる値は、[SHA-1] および [MD5] です。MD5 認証を使用する場合、キーの長さは 32 桁の 16 進数（16 バイト）である必要があります。SHA-1 認証を使用する場合、キーの長さは 40 桁の 16 進数（20 バイト）である必要があります。

ステップ 14 [Authentication Key] フィールドに認証キーを入力します。キーは 32 文字の 16 進数文字で構成される必要があります。

ステップ 15 [Encryption Algorithm] ドロップダウン リストから暗号化アルゴリズムを選択します。サポートされる値は、[AES-CDC]、[3DES]、[DES] です。ヌルのエントリは暗号化されません。

ステップ 16 [Encryption Key] フィールドに暗号キーを入力します。

ステップ 17 [OK] をクリックします。

ステップ 18 [Apply] をクリックして変更内容を保存します。

OSPFv3 受動インターフェイスの設定

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Setup]** の順に選択します。

ステップ 2 [Process Instances] タブをクリックします。

ステップ 3 編集する OSPFv3 プロセスを選択してから [Advanced] をクリックします。

[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 4 [Passive Interfaces] 領域では、インターフェイスのパッシブ OSPFv3 ルーティングをイネーブルにすることができます。パッシブ ルーティングは、OSPFv3 ルーティング情報のアドバタイズメントの制御に有効であり、インターフェイスでの OSPFv3 ルーティング更新の送受信をディセーブルにします。[Passive Interfaces] 領域で、次の設定を選択します。

- [Global passive] チェックボックスをオンにして、テーブルに表示されているインターフェイスすべてをパッシブにします。個々のインターフェイスをオフにすると、そのインターフェイスは非パッシブになります。
- [Global passive] チェックボックスをオフにすると、すべてのインターフェイスが非パッシブになります。個々のインターフェイスをオンにすると、そのインターフェイスはパッシブになります。

ステップ 5 [OK] をクリックします。

ステップ 6 [Apply] をクリックして変更内容を保存します。

OSPFv3 アドミニストレーティブ ディスタンスの設定

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Setup]** の順に選択します。

ステップ 2 [Process Instances] タブをクリックします。

ステップ 3 編集する OSPF プロセスを選択してから [Advanced] をクリックします。

[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。

[Administrative Route Distances] 領域では、管理ルート間隔の設定に使用された設定を変更することができます。管理ルート間隔は 10～254 の整数です。[Administrative Route Distances] 領域で、次の値を入力します。

- [Inter Area] には、IPv6 ルートの OSPV のエリア間ルートを指定します。
- [Intra Area] には、IPv6 ルートの OSPF のエリア内ルートを指定します。
- [External] には、IPv6 ルートの OSPF の外部タイプ 5 および外部タイプ 7 のルートを指定します。

ステップ 4 [OK] をクリックします。

ステップ 5 [Apply] をクリックして変更内容を保存します。

OSPFv3 タイマーの設定

OSPFv3 の LSA 到着タイマー、LSA ペーシング タイマー、およびスロットリング タイマーを設定できます。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Setup]** の順に選択します。

ステップ 2 [Process Instances] タブをクリックします。

ステップ 3 編集する OSPFv3 プロセスを選択してから [Advanced] をクリックします。

[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 4 [Timers] 領域では、LSA 到着、LSA ペーシング、LSA 再送信、LSA スロットル、SPF スロットル時間の設定に使用された設定を変更することができます。[Timers] 領域で、次の値を入力します。

- [LSA Arrival] には、ネイバーから到着する同一 LSA の最短受信間隔をミリ秒単位で指定します。有効な範囲は 0 ～ 6000,000 ミリ秒です。デフォルトは 1000 ミリ秒です。
- [LSA Flood Pacing] には、フラッディング キュー内の LSA のアップデートのペースをミリ秒単位で指定します。設定できる範囲は 5 ～ 100 ミリ秒です。デフォルト値は、33 ミリ秒です。
- [LSA Group Pacing] には、LSA をグループにまとめてリフレッシュ、チェックサム計算、エージングする間隔を秒単位で指定します。有効な値の範囲は 10 ～ 1800 です。デフォルト値は 240 です。
- [LSA Retransmission Pacing] には、再送信キュー内の LSA がペースされる時間をミリ秒単位で指定します。設定できる範囲は 5 ～ 200 ミリ秒です。デフォルト値は 66 ミリ秒です。
- [LSA Throttle Initial] には、LSA の最初のオカレンスを生成する遅延をミリ秒単位で指定します。デフォルト値は 0 ミリ秒です。
- [LSA Throttle Min Hold] には、同じ LSA を発信する最短遅延時間をミリ秒単位で指定します。デフォルト値は 5000 ミリ秒です。
- [LSA Throttle Max Wait] には、同じ LSA を発信する最長遅延時間をミリ秒単位で指定します。デフォルト値は、5000 ミリ秒です。

（注）
LSA スロットリングでは、最小時間または最大時間が最初のオカレンスの値よりも小さい場合、OSPFv3 が自動的に最初のオカレンス値に修正します。同様に、指定された最遅延が最小遅延よりも小さい場合、OSPFv3 が自動的に最小遅延値に修正します。

- [SPF Throttle Initial] には、SPF 計算の変更を受信する遅延をミリ秒単位で指定します。デフォルト値は 5000 ミリ秒です。
- [SPF Throttle Min Hold] には、1 番目と 2 番目の SPF 計算の間の遅延をミリ秒単位で指定します。デフォルト値は 10000 ミリ秒です。
- [SPF Throttle Max Wait] には、SPF 計算の最長待機時間をミリ秒単位で指定する。デフォルト値は、10000 ミリ秒です。

（注）
SPF スロットリングでは、最小時間または最大時間が最初のオカレンスの値よりも小さい場合、OSPFv3 が自動的に最初のオカレンス値に修正します。同様に、指定された最遅延が最小遅延よりも小さい場合、OSPFv3 が自動的に最小遅延値に修正します。

ステップ 5 [OK] をクリックします。

ステップ 6 [Apply] をクリックして変更内容を保存します。

スタティック OSPFv3 ネイバーの定義

ポイントツーポイントの非ブロードキャストネットワークを介してOSPFv3ルートをアドバタイズするには、スタティック OSPF ネイバーを定義する必要があります。この機能により、OSPFv3 アドバタイズメントを GRE トンネルにカプセル化しなくても、既存の VPN 接続でブロードキャストすることができます。

開始する前に、OSPFv3 ネイバーに対するスタティック ルートを作成する必要があります。スタティック ルートの作成方法の詳細については、スタティック ルートの設定を参照してください。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Static Neighbor]** の順に選択します。

ステップ 2 [Add] または [Edit] をクリックします。

[Add Static Neighbor] または [Edit Static Neighbor] ダイアログボックスが表示されます。このダイアログボックスでは、新しいスタティック ネイバーを定義することや、既存のスタティック ネイバーの情報を変更することができます。ポイントツーポイントの非ブロードキャストインターフェイスごとに、スタティック ネイバーを 1 つ定義する必要があります。次の制約事項に注意してください。

- 異なる 2 つの OSPFv3 プロセスに対して同じスタティック ネイバーを定義できません。
- 各スタティック ネイバーにスタティック ルートを定義する必要があります

ステップ 3 [Interface] ドロップダウン リストから、スタティック ネイバーに関連付けられたインターフェイスを選択します。既存のスタティック ネイバーを編集している場合、この値は変更できません。

ステップ 4 [Link-local address] フィールドに、スタティック ネイバーの IPv6 アドレスを入力します。

ステップ 5 （オプション）[Priority] フィールドに、プライオリティ レベルを入力します。

ステップ 6 （オプション）[Poll Interval] フィールドに、ポーリング間隔を秒単位で入力します。

ステップ 7 **[OK]** をクリックします。

Syslog メッセージの送信

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。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Setup]** の順に選択します。

ステップ 2 [Process Instances] タブをクリックします。

ステップ 3 編集する OSPF プロセスを選択してから [Advanced] をクリックします。

[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。

[Adjacency Changes] 領域では、OSPFv3 ネイバーが起動または停止したときに syslog メッセージを送信するための設定を変更することができます。[Adjacency Changes] 領域で、次の手順を実行します。

- OSPFv3 ネイバーが起動または停止したときに syslog メッセージを送信するには、[Log Adjacency Changes] チェックボックスをオンにします。
- OSPFv3 ネイバーが起動または停止したときだけではなく、各状態の syslog メッセージを送信するには、[Include Details] チェックボックスをオンにします。

ステップ 4 [OK] をクリックします。

ステップ 5 [Apply] をクリックして変更内容を保存します。

Syslog メッセージの抑止

ルータがサポートされていない LSA タイプ 6 Multicast OSPF（MOSPF）パケットを受信した場合の syslog メッセージの送信を抑止するには、次の手順を実行します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Setup]** の順に選択します。

ステップ 2 [Process Instances] タブをクリックします。

ステップ 3 編集する OSPFv3 プロセスを選択してから [Advanced] をクリックします。

[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 4 [Ignore LSA MOSPF] チェックボックスをオンにして、[OK] をクリックします。

集約ルート コストの計算

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Setup]** の順に選択します。

ステップ 2 [Process Instances] タブをクリックします。

ステップ 3 編集する OSPF プロセスを選択してから [Advanced] をクリックします。

[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 4 [RFC1583 Compatible] チェックボックスをオンにして、[OK] をクリックします。

OSPFv3 ルーティング ドメインへのデフォルトの外部ルートの生成

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Setup]** の順に選択します。

ステップ 2 [Process Instances] タブをクリックします。

ステップ 3 編集する OSPFv3 プロセスを選択してから [Advanced] をクリックします。

[Edit OSPFv3 Process Advanced Properties] ダイアログボックスが表示されます。

ステップ 4 [Default Information Originate Area] で、次の手順を実行します。

a) [Enable] チェックボックスをオンにして、OSPFv3 ルーティング プロセスをイネーブルにします。

b) [Always advertise] チェックボックスをオンにして、出口が 1 つであるかどうかにかかわらず、常時デフォルト ルートをアドバタイズします。

c) デフォルト ルートの生成に使用するメトリックを [Metric] フィールドに入力します。有効なメトリック値の範囲は、0 ～ 16777214 です。デフォルト値は 10 です。

d) [Metric Type] ドロップダウン リストは、OSPFv3 ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられた外部リンク タイプです。有効な値は次のとおりです。

- 1：タイプ 1 外部ルート
- 2：タイプ 2 外部ルート

デフォルトはタイプ 2 外部ルートです。

e) [Route Map] ドロップダウン リストから、ルート マップが満たされている場合に、デフォルト ルートを生成するルーティング プロセスを選択します。

ステップ 5 [OK] をクリックします。

ステップ 6 [Apply] をクリックして変更内容を保存します。

IPv6 サマリー プレフィックスの設定

手順

ステップ 1 ASDM のメイン ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Summary Prefix]** の順に選択します。

ステップ 2 新しいサマリープレフィックスを追加するには、[Add] をクリックします。既存のサマリープレフィックスを適用するには、[Edit] をクリックします。サマリー プレフィックスを削除するには、[Delete] をクリックします。

[Add Summary Prefix] ダイアログボックスまたは [Edit Summary Prefix] ダイアログボックスが表示されます。

ステップ 3 [Process ID] ドロップダウン リストからプロセス ID を選択します。

ステップ 4 [IPv6 Prefix/Prefix Length] フィールドに IPv6 プレフィックスとプレフィックス長を入力します。

ステップ 5 [Advertise] チェックボックスをオンにして、指定したプレフィックスとマスクのペアに一致するルートをアドバタイズします。このチェックボックスをオフにすると、指定されたプレフィックスとマスク ペアと一致するルートが抑制されます。

ステップ 6 ルートマップを使用して再配布を制御するように照合値として使用できるタグ値を [Tag] フィールドに入力します。

ステップ 7 [OK] をクリックします。

ステップ 8 [Apply] をクリックして変更内容を保存します。

IPv6 ルートの再配布

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Redistribution]** の順に選択します。

ステップ 2 OSPFv3 プロセスに接続済みルートを再配布するための新しいパラメータを追加するには、[Add] をクリックします。OSPFv3 プロセスに接続済みルートを再配布するための既存のパラメータを変更するには、[Edit] をクリックします。パラメータの選択したセットを削除するには [Delete] をクリックします。

[Add Redistribution] ダイアログボックスまたは [Edit Redistribution] ダイアログボックスが表示されます。

ステップ 3 [Process ID] ドロップダウン リストからプロセス ID を選択します。

ステップ 4 [Source Protocol] ドロップダウン リストから、ルートが再配布されるソース プロトコルを選択します。サポートされるプロトコルは、接続済み、スタティック、OSPF です。

ステップ 5 [Metric] フィールドにメトリック値を入力します。同じルータ上の一方の OSPF プロセスから他方の OSPF プロセスにルートを再配布する場合、メトリック値を指定しないと、メトリックは一方のプロセスから他方のプロセスへ存続します。他のプロセスを OSPF プロセスに再配布するときに、メトリック値を指定しない場合、デフォルトのメトリックは 20 です。

ステップ 6 [Metric Type] ドロップダウン リストからメトリック タイプを選択します。使用可能なオプションは、[None]、[1]、[2] です。

ステップ 7 （オプション）[Tag] フィールドにタグ値を入力します。このパラメータは、ASBR 間で情報の転送に使用される可能性のある各外部ルートに付加される 32 ビットの 10 進数値を指定します。何も指定しない場合、BGP および EGP からのルートにはリモート自律システムの番号が使用されます。その他のプロトコルについては、ゼロが使用されます。有効な値は 0 ～ 4294967295 です。

ステップ 8 [Route Map] ドロップダウン リストからルート マップを選択して、ソース ルーティング プロトコルから現在のルーティング プロトコルへのルートのインポートのフィルタリングをオンにします。このパラメータを指定しない場合、すべてのルートが再配布されます。このパラメータを指定し、ルート マップ タグが表示されていない場合、ルートはインポートされません。

ステップ 9 再配布に接続済みルートを含めるには、[Include Connected] チェックボックスをオンにします。

ステップ 10 [Match] チェックボックスをオンにして他のルーティング ドメインへのルートを再配布し、次のチェックボックスの 1 つをオンにします。

- [Internal] は、特定の自律システムの内部にあるルートです。
- [External 1] は、自律システムの外部ながら、OSPFv3 にタイプ 1 外部ルートとしてインポートされるルートです。
- [External 2] は、自律システムの外部ながら、OSPFv3 にタイプ 2 外部ルートとしてインポートされるルートです。
- [NSSA External 1] は、自律システムの外部ながら、IPv6 用の NSSA の OSPFv3 にタイプ 1 の外部ルートとしてインポートされるルートです。
- [NSSA External 2] は、自律システムの外部ながら、IPv6 用の NSSA の OSPFv3 にタイプ 2 の外部ルートとしてインポートされるルートです。

ステップ 11 [OK] をクリックします。

ステップ 12 [Apply] をクリックして変更内容を保存します。

グレースフル リスタートの設定

ASA では、既知の障害状況が発生することがあります。これにより、スイッチング プラットフォーム全体でパケット転送に影響を与えることがあってはなりません。Non-Stop Forwarding（NSF）機能では、ルーティング プロトコル情報を復元している間に、既知のルートへのデータ転送が続行されます。

ハイアベイラビリティモードでは、アクティブユニットが非アクティブになり、スタンバイユニットが新しいアクティブになると、OSPF プロセスが再起動します。同様に、クラスタモードでは、制御ユニットが非アクティブになり、データユニットが新しい制御ユニットとして選択されると、OSPF プロセスが再起動します。このような OSPF 移行プロセスでは、かなりの遅延が発生します。OSPF プロセスの状態変更時のトラフィック損失を回避するように NSF を設定できます。また NSF 機能は、スケジュール済みヒットレス ソフトウェア アップグレードがあるときに便利です。

グレースフル リスタートは、OSPFv2 と OSPFv3 の両方でサポートされています。NSF Cisco（RFC 4811 および RFC 4812）または NSF IETF（RFC 3623）のいずれかを使用して、OSPFv2 上でグレースフル リスタートを設定できます。graceful-restart（RFC 5187）を使用して、OSPFv3 上でグレースフル リスタートを設定できます。

NSF グレースフル リスタート機能の設定には、機能の設定と NSF 対応または NSF 認識としてのデバイスの設定という 2 つのステップが伴います。NSF 対応デバイスは、ネイバーに対して独自のリスタート アクティビティを示すことができ、NSF 認識デバイスはネイバーのリスタートをサポートすることができます。

デバイスは、いくつかの条件に応じて、NSF 対応または NSF 認識として設定できます。

- デバイスは、現在のデバイスのモードに関係なく、NSF 認識デバイスとして設定できます。
- デバイスを NSF 対応として設定するには、デバイスはフェールオーバーまたはスパンド EtherChannel（L2）クラスタ モードのいずれかである必要があります。
- デバイスを NSF 認識または NSF 対応にするには、必要に応じて opaque リンク ステート アドバタイズメント（LSA）/リンク ローカル シグナリング（LLS）ブロックの機能を使って設定する必要があります。

（注） OSPFv2 用に fast hello が設定されている場合、アクティブ ユニットのリロードが発生し、スタンバイ ユニットがアクティブになっても、グレースフル リスタートは発生しません。これは、ロール変更にかかる時間は、設定されているデッド インターバルよりも大きいためです。

OSPFv2 のグレースフル リスタートの設定

OSPFv2、Cisco NSF および IETF NSF には、2 つのグレースフル リスタート メカニズムがあります。OSPF インスタンスに対しては、これらのグレースフル リスタート メカニズムのうち一

度に設定できるのは 1 つだけです。NSF 認識デバイスは、Cisco NSF ヘルパーと IETF NSF ヘルパーの両方として設定できますが、NSF 対応デバイスはOSPF インスタンスに対して、Cisco NSF または IETF NSF モードのいずれかとして設定できます。

OSPFv2 の Cisco NSF グレースフル リスタートの設定

NSF 対応または NSF 認識デバイスに対して、OSPFv2 の Cisco NSF グレースフル リスタートを設定します。

手順

ステップ 1 メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] > [Advanced] > [Add NSF Properties] の順に選択します。

ステップ 2 [Configuring Cisco NSF] の下で、[Enable Cisco nonstop forwarding (NSF)] チェックボックスをオンにします。

ステップ 3 （オプション）必要に応じて、[Cancels NSF restart when non-NSF-aware neighboring networking devices are detected] チェックボックスをオンにします。

ステップ 4 （オプション）[Configuring Cisco NSF helper] の下で、[Enable Cisco nonstop forwarding (NSF) for helper mode] チェックボックスをオフにします。

（注）
このチェックボックスは、デフォルトではオンになっています。NSF 認識デバイスで Cisco NSF ヘルパー モードをディセーブルにするには、このチェックボックスをオフにします。

ステップ 5 [OK] をクリックします。

ステップ 6 [Apply] をクリックして変更内容を保存します。

OSPFv2 の IETF NSF グレースフル リスタートの設定

NSF 対応または NSF 認識デバイスに対して、OSPFv2 の IETF NSF グレースフル リスタートを設定します。

手順

ステップ 1 メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] > [Advanced] > [Add NSF Properties] の順に選択します。

ステップ 2 [Configuring IETF NSF] で、[Enable IETF nonstop forwarding (NSF)] チェックボックスをオンにします。

ステップ 3 （オプション）[Length of graceful restart interval] フィールドに、リスタート間隔を秒単位で入力します。

（注）

デフォルト値は 120 秒です。30 秒未満の再起動間隔では、グレースフル リスタートが中断します。

ステップ 4 （オプション）[Configuring IETF NSF helper] で、[Enable IETF nonstop forwarding (NSF) for helper mode] チェックボックスをオフにします。

このチェックボックスは、デフォルトではオンになっています。NSF 認識デバイスで IETF NSF ヘルパー モードをディセーブルにするには、このチェックボックスをオフにします。

ステップ 5 [OK] をクリックします。

ステップ 6 [Apply] をクリックして変更内容を保存します。

OSPFv3 のグレースフル リスタートの設定

OSPFv3 の NSF グレースフル リスタート機能を設定するには、2 つのステップを伴います。NSF 対応としてのデバイスの設定と、NSF 認識としてのデバイスの設定です。

手順

ステップ 1 メイン ASDM ウィンドウで、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] > [Advanced] > [Add NSF Properties] の順に選択します。

ステップ 2 [Configuring Graceful Restart] の下で、[Enable Graceful Restart] チェックボックスをオンにします。

ステップ 3 （オプション）[Restart Interval] フィールドにリスタート間隔の値を入力します。

（注）
デフォルト値は 120 秒です。30 秒未満の再起動間隔では、グレースフル リスタートが中断します。

ステップ 4 [Configuring Graceful Restart Helper] の下で、[Enable Graceful Restart Helper] チェックボックスをオンにします。

このチェックボックスは、デフォルトではオンになっています。NSF 認識デバイスでグレースフル リスタート ヘルパー モードをディセーブルにするには、このチェックボックスをオフにします。

ステップ 5 （オプション）[Enable LSA checking] チェックボックスをオンにして、厳密なリンク ステート アドバタイズメント チェックをイネーブルにします。

イネーブルにすると、再起動ルータにフラッディングされる可能性がある LSA への変更があることが検出された場合、またはグレースフル リスタート プロセスが開始されたときに再起動ルータの再送リスト内に変更された LSA があると検出された場合、ヘルパー ルータはルータの再起動プロセスを終了させることを示します。

ステップ 6 [OK] をクリックします。

ステップ 7 [Apply] をクリックして変更内容を保存します。

OSPF のグレースフル リスタート待機タイマーの設定

OSPF ルータでは、すべてのネイバーがパケットに含まれているかが不明な場合は、Hello パケットにアタッチされている EO-TLV に RS ビットを設定することが予期されます。ただし、隣接関係（アジャセンシー）を維持するにはルータの再起動が必要です。ただし、RS ビット値は RouterDeadInterval 秒より長くすることはできません。そのため、Hello パケットの RS ビットを RouterDeadInterval 秒未満に設定するための **timers nsf wait** コマンドが導入されました。NSF 待機タイマーのデフォルト値は 20 秒です。

始める前に

- OSPF の Cisco NSF 待機時間を設定するには、デバイスが NSF 認識または NSF 対応である必要があります。

手順

ステップ 1 OSPF ルータ コンフィギュレーション モードを開始します。

例：

```
ciscoasa(config)# router ospf
```

ステップ 2 タイマーを入力し、NSF を指定します。

例：

```
ciscoasa(config-router)# timers?
router mode commands/options:
  lsa       OSPF LSA timers
  nsf       OSPF NSF timer
  pacing    OSPF pacing timers
  throttle  OSPF throttle timers
ciscoasa(config-router)# timers nsf ?
```

ステップ 3 グレースフルリスタート待機間隔を入力します。この値は、1～65535 の範囲で指定できます。

例：

```
ciscoasa(config-router)# timers nsf wait 200
```

グレースフルリスタート待機間隔を使用することで、待機間隔がルータの dead 間隔よりも長くならないようにできます。

OSPFv2 設定の削除

OSPFv2 設定を削除します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** の順に選択します。

ステップ 2 [Enable this OSPF Process] チェックボックスをオフにします。

ステップ 3 [適用（Apply）] をクリックします。

OSPFv3 設定の削除

OSPFv3 設定を削除します。

手順

ステップ 1 メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Setup]** の順に選択します。

ステップ 2 [Enable OSPFv3 Process] チェックボックスをオフにします。

ステップ 3 [適用（Apply）] をクリックします。

OSPFv2 の例

次の例に、さまざまなオプションのプロセスを使用して OSPFv2 をイネーブルにし、設定する方法を示します。

1. メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** の順に選択します。
2. [Process Instances] タブをクリックし、[OSPF Process 1] フィールドに **2** と入力します。
3. [Area/Networks] タブをクリックし、[Add] をクリックします。
4. [Area ID] フィールドに **0** と入力します。
5. [Area Networks] 領域の [IP Address] フィールドに **10.0.0.0** と入力します。
6. [Netmask] ドロップダウン リストで [255.0.0.0] を選択します。
7. [OK] をクリックします。
8. メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Redistribution]** の順に選択します。

9. [Add] をクリックします。

   [Add/Edit OSPF Redistribution Entry] ダイアログボックスが表示されます。

10. [Protocol] 領域の [OSPF] オプション ボタンをクリックして、ルートが再配布されるソース プロトコルを指定します。[OSPF] を選択すると、別の OSPF ルーティング プロセスからのルートが再配布されるようになります。

11. OSPF プロセス ID を [OSPF Process] ドロップダウン リストで選択します。

12. [Match] 領域の [Internal] チェックボックスをオンにします。

13. [Metric Value] フィールドに、再配布されるルーティングのメトリック値として **5** を入力します。

14. [Metric Type] ドロップダウン リストで、メトリック タイプの値として 1 を選択します。

15. [Route Map] ドロップダウン リストで、1 を選択します。

16. [OK] をクリックします。

17. メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Interface]** の順に選択します。

18. [Properties] タブで、[inside] インターフェイスを選択して [Edit] をクリックします。

    [Edit OSPF Properties] ダイアログボックスが表示されます。

19. [Cost] フィールドに **20** と入力します。

20. [Advanced] をクリックします。

21. [Retransmit Interval] フィールドに **15** と入力します。

22. [Transmit Delay] フィールドに **20** と入力します。

23. [Hello Interval] フィールドに **10** と入力します。

24. [Dead Interval] フィールドに **40** と入力します。

25. [OK] をクリックします。

26. [Edit OSPF Properties] ダイアログボックスで、[Priorities] フィールドに **20** と入力して [OK] をクリックします。

27. [Authentication] タブをクリックします。

    [Edit OSPF Authentication] ダイアログボックスが表示されます。

28. [Authentication] 領域の [MD5] オプション ボタンをクリックします。

29. [MD5 and Key ID] 領域の [MD5 Key] フィールドに **cisco** と入力し、[MD5 Key ID] フィールドに **1** と入力します。

30. [OK] をクリックします。

31. **[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** を選択し、[Area/Networks] タブをクリックします。
32. [OSPF 2] プロセスを選択し、[Edit] を選択します。

    [Edit OSPF Area] ダイアログボックスが表示されます。
33. [Area Type] 領域で、[Stub] を選択します。
34. [Authentication] 領域で、[None] を選択し、[Default Cost] フィールドに **20** と入力します。
35. [OK] をクリックします。
36. メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPF]** > **[Setup]** の順に選択します。
37. [Process Instances] タブをクリックし、[OSPF process 2] チェックボックスをオンにします。
38. [Advanced] をクリックします。

    [Edit OSPF Area] ダイアログボックスが表示されます。
39. [Timers] 領域で、[SPF Delay Time] フィールドに **10** と入力し、[SPF Hold Time] フィールドに **20** と入力します。
40. [Adjacency Changes] 領域の [Log Adjacency Change Details] チェックボックスをオンにします。
41. [OK] をクリックします。
42. [リセット（Reset）] をクリックします。

OSPFv3 の例

次に、ASDM で OSPFv3 ルーティングを設定する例を示します。

1. メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Setup]** の順に選択します。
2. [Process Instances] タブで、次の手順を実行します。
    1. [Enable OSPFv3 Process] チェックボックスをオンにします。
    2. [Process ID] フィールドに **1** を入力します。
3. [Areas] タブをクリックし、続いて [Add] をクリックして、[Add OSPFv3 Area] ダイアログボックスを表示します。
4. [OSPFv3 Process ID] ドロップダウン リストから、**1** を選択します。
5. [Area ID] フィールドに **22** と入力します。

6. [Area Type] ドロップダウン リストから [Normal] を選択します。
7. [Default Cost] フィールドに **10** を入力します。
8. [Redistribution imports routes to normal and NSSA areas] をオンにします。
9. [Metric] フィールドに **20** を入力します。
10. [Metric Type] ドロップダウン リストから **1** を選択します。
11. 使用されているインターフェイスの指定に合わせて、**内部**チェックボックスをオンにします。
12. [Enable Authentication] チェックボックスをオンにします。
13. [Security Policy Index] フィールドに **300** を入力します。
14. [Authentication Algorithm] ドロップダウン リストから [SHA-1] を選択します。
15. [Authentication Key] フィールドに **12345ABCDE** を入力します。
16. [Encryption Algorithm] ドロップダウン リストから [DES] を選択します。
17. [Encryption Key] フィールドに **1122334455aabbccddee** を入力します。
18. [OK] をクリックします。
19. [Route Summarization] タブをクリックし、続いて [Add] をクリックして、[Add Route Summarization] ダイアログボックスを表示します。
20. [Process ID] ドロップダウン リストから **1** を選択します。
21. [Area ID] ドロップダウン リストから **22** を選択します。
22. [IPv6 Prefix/Prefix Length] フィールドに **2000:122::/64** を入力します。
23. （オプション）[Cost] フィールドに **100** を入力します。
24. [Advertised] チェックボックスをオンにします。
25. [OK] をクリックします。
26. メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[OSPFv3]** > **[Interface]** の順に選択します。
27. [Properties] タブをクリックします。
28. **内部**チェックボックスをオンにし、[Edit] をクリックして、[Edit OSPF Properties] ダイアログボックスを表示します。
29. [Cost] フィールドに **20** と入力します。
30. [Priority] フィールドに **1** を入力します。
31. [Point-to-Point] チェックボックスをオンにします。
32. [Dead Interval] フィールドに **40** と入力します。

33. [Hello Interval] フィールドに **10** と入力します。
34. [Retransmit Interval] フィールドに **15** と入力します。
35. [Transmit Delay] フィールドに **20** と入力します。
36. [OK] をクリックします。
37. メイン ASDM ウィンドウで、**[Configuration]** > **[Device Setup]** > **[Routing]** > **[Redistribution]** の順に選択します。
38. [Process ID] ドロップダウン リストから **1** を選択します。
39. [Source Protocol] ドロップダウン リストから [OSPF] を選択します。
40. [Metric] フィールドに **50** を入力します。
41. [Metric Type] ドロップダウン リストから **1** を選択します。
42. [OK] をクリックします。
43. [Apply] をクリックして変更内容を保存します。

OSPF のモニタリング

IP ルーティング テーブルの内容、キャッシュの内容、およびデータベースの内容など、特定の統計情報を表示できます。提供される情報は、リソースの使用状況を判定してネットワークの問題を解決するために使用することもできます。また、ノードの到達可能性情報を表示して、デバイス パケットがネットワークを通過するときにとるルーティング パスを見つけることもできます。

OSPFv2 ルーティングのさまざまな統計情報を ASDM でモニターまたは表示するには、次の手順を実行します。

1. メイン ASDM ウィンドウで、**[Monitoring]** > **[Routing]** > **[OSPF LSAs]** の順に選択します。
2. 選択してモニターできる OSPF LSA は、タイプ 1 ～ 5 と 7 です。各ペインには、次のように 1 つの LSA タイプが表示されます。
   - [Type 1 LSAs] は、特定のエリア内の特定プロセス下にあるすべてのルートを表します。
   - [Type 2 LSAs] には、ルータをアドバタイズする指定ルータの IP アドレスが表示されます。
   - [Type 3 LSAs] には、宛先ネットワークの IP アドレスが表示されます。
   - [Type 4 LSAs] には、AS 境界ルータの IP アドレスが表示されます。
   - [Type 5 LSAs] と [Type 7 LSAs] には、AS 外部ネットワークの IP アドレスが表示されます。

3. [Refresh] をクリックすると、各 LSA タイプのペインが更新されます。
4. メイン ASDM ウィンドウで、**[Monitoring]** > **[Routing]** > **[OSPF Neighbors]** の順に選択します。

   [OSPF Neighbors] ペインの各行は 1 つの OSPF ネイバーを表します。さらに、[OSPF Neighbors] ペインにはそのネイバーが実行されているネットワーク、優先度、状態、デッド時間（秒単位）、ネイバーの IP アドレス、および実行されているインターフェイスも表示されます。OSPF ネイバーが取る可能性のある状態の一覧については、RFC 2328 を参照してください。
5. [Refresh] をクリックすると、[OSPF Neighbors] ペインが更新されます。

OSPFv3 ルーティングのさまざまな統計情報を ASDM でモニターまたは表示するには、次の手順を実行します。

1. メイン ASDM ウィンドウで、**[Monitoring]** > **[Routing]** > **[OSPFv3 LSAs]** の順に選択します。
2. OSPFv3 LSA を選択し、モニターすることができます。[Link State type] ドロップダウン リストでリンク ステート タイプを選択し、指定されたパラメータに従って状態を表示します。サポートされるリンク ステート タイプは、ルータ、ネットワーク、エリア間プレフィックス、エリア間ルータ、AS エクスターナル、NSSA、リンク、エリア内プレフィックスです。
3. [Refresh] をクリックして、各リンク ステート タイプを更新します。
4. メイン ASDM ウィンドウで、**[Monitoring]** > **[Routing]** > **[OSPFv3 Neighbors]** の順に選択します。

   [OSPFv3 Neighbors] ペインの各行は 1 つの OSPFv3 ネイバーを表します。さらに、[OSPFv3 Neighbors] ペインには、ネイバーの IP アドレス、優先度、状態、秒単位のデッド タイム量、動作中のインターフェイスが表示されます。OSPFv3 ネイバーが取る可能性のある状態の一覧については、RFC 5340 を参照してください。
5. [Refresh] をクリックすると、[OSPFv3 Neighbors] ペインが更新されます。

OSPF の履歴

表 *1 : OSPF* の機能履歴

機能名	プラットフォーム リリース	機能情報
OSPF サポート	7.0(1)	Open Shortest Path First（OSPF）ルーティング プロトコルを使用した、データのルーティング、認証、およびルーティング情報の再配布とモニタについて、サポートが追加されました。 次の画面が導入されました。[Configuration] > [Device Setup] > [Routing] > [OSPF]。
マルチ コンテキスト モードのダイナミック ルーティング	9.0(1)	OSPFv2 ルーティングは、マルチ コンテキスト モードでサポートされます。 次の画面が変更されました。[Configuration] > [Device Setup] > [Routing]> [OSPF] > [Setup]
クラスタ	9.0(1)	OSPFv2 および OSPFv3 の場合、バルク同期、ルートの同期およびスパンド EtherChannel ロードバランシングは、クラスタリング環境でサポートされます。
IPv6 の OSPFv3 サポート	9.0(1)	OSPFv3 ルーティングが IPv6 に対してサポートされます。 次の画面が導入されました。[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup]、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Interface]、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Redistribution]、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Summary Prefix]、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Virtual Link]、[Monitoring] > [Routing] > [OSPFv3 LSAs]、[Monitoring] > [Routing] > [OSPFv3 Neighbors]。
Fast Hello に対する OSPF サポート	9.2(1)	OSPF は、Fast Hello パケット機能をサポートしているため、OSPF ネットワークでのコンバージェンスが高速なコンフィギュレーションになります。 次の画面が変更されました。[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Interface] > [Edit OSPF Interface Advanced Properties]
タイマー	9.2(1)	新しい OSPF タイマーを追加し、古いタイマーを廃止しました。 次の画面が変更されました。[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] > [Edit OSPF Process Advanced Properties]
アクセス リストを使用したルート フィルタリング	9.2(1)	ACL を使用したルート フィルタリングがサポートされるようになりました。 次の画面が追加されました。[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Filtering Rules] > [Add Filter Rules]

機能名	プラットフォームリリース	機能情報
OSPF モニタリングの強化	9.2(1)	OSPF モニタリングの詳細情報が追加されました。
OSPF 再配布 BGP	9.2(1)	OSPF 再配布機能が追加されました。 次の画面が追加されました。[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Redistribution]
ノンストップ フォワーディング（NSF）に対する OSPF のサポート	9.3(1)	NSF に対する OSPFv2 および OSPFv3 のサポートが追加されました。 次の画面が追加されました。[Configuration] > [Device Setup] > [Routing] > [OSPF] > [Setup] > [NSF Properties]、[Configuration] > [Device Setup] > [Routing] > [OSPFv3] > [Setup] > [NSF Properties]
ノンストップ フォワーディング（NSF）に対する OSPF のサポート	9.13(1)	NSF 待機タイマーが追加されました。 NSF 再起動間隔のタイマーを設定するための新しいコマンドが追加されました。このコマンドが導入され、待機間隔がルータの dead 間隔よりも長くならないようになりました。 次のコマンドが導入されました。 **timers nsf wait <seconds>**

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。