Open Shortest Path First（OSPF）

Open Shortest Path First（OSPF）は、リンクステート内部ゲートウェイプロトコルです。OSPF ルータは、リンクステート情報を隣接ルータにフラッディングし、OSPF エリア内のすべてのルータがネットワークトポロジを完全に把握できるようにします。

IPv4 ネットワークの場合は OSPFv2、IPv6 ネットワークの場合は OSPFv3 など、IP バージョンに基づいて、個別の OSPF バージョンがあります。これらのバージョンは独立していて、OSPFv3 は OSPFv2 に代わるものではありません。

スマート CLI オブジェクトを使用して OSPFv2 を設定し、デバイスを OSPFv2 ネットワークトポロジに統合することができます。OSPFv3 は設定できません。

OSPFv2 プロセスとエリアの設定

Firepower Threat Defenseで最大 2 つの OSPFv2 プロセスを設定できます。プロセス番号は純粋に内部的なインジケータです。他のデバイスで使用されているプロセス番号と一致させる必要はありませんが、独自のトラッキングを目的として番号を一致させることもできます。

プライベートネットワークの番号（192.168.1.0/24 など）を内部ネットワークに使用する場合は、プライベートアドレスをパブリックアドレスから分離し、これらの内部ネットワークに対して 1 つの OSPFv2 プロセスを使用し、外部の公的にアドレス可能なネットワークに対して 2 番目のプロセスを使用することが必要になる場合があります。プライベート番号を使用しない場合でも、1 つのプロセスを内部で実行し、別のプロセスを外部で実行して、2 つのプロセス間でルートのサブセットを再配布することができます。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。

一方、エリア番号はネットワーク内に存在するため、他の隣接ルータで使用されているものと同じ番号を使用する必要があります。シングルエリアネットワークを設定する場合は、エリア

0（バックボーンエリアとも呼ばれる）を使用します。階層型ネットワーク設計の複数エリアネットワークの場合は、ネットワークで定義されたエリアを理解し、このデバイスをどのエリアに参加させるかを把握する必要があります。

仮想ルータを使用している場合は、仮想ルータごとに 2 つの OSPFv2 プロセスを作成できます。

次の手順で、1 つの OSPFv2 プロセスを作成する方法を説明します。2 番目のプロセスを作成するには、この手順を繰り返します。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータを有効にした場合は、OSPF を設定しているルータの表示アイコン（  ）をクリックします。

ステップ 3 [OSPF] タブをクリックします。

ステップ 4 次のいずれかを実行します。

- 新しいプロセスを作成するには、**[+]** > **[OSPF]** をクリックするか、**[OSPFオブジェクトの作成（Create OSPF Object）]** > **[OSPF]** ボタンをクリックします。
- 編集するオブジェクトの横にある編集アイコン（  ）をクリックします。オブジェクトを編集すると、直接設定していない行が表示される場合があることに注意してください。これらの行は、設定されているデフォルト値を示すために公開されています。

プロセスが不要になった場合は、オブジェクトのごみ箱アイコンをクリックして削除します。

ステップ 5 オブジェクトの名前、さらにオプションで説明を入力します。

ステップ 6 基本的なプロセスのプロパティを設定します。

- **router ospf** *process-id* : *process-id* をクリックし、1 ～ 65535 の番号を入力します。この番号は、このデバイス内のみで意味を持つもので、他のルータで設定されているプロセス番号と一致している必要はありません。この番号は仮想ルータ内で一意である必要があります。
- **log-adj-changes** *log-state* : *log-state* をクリックし、次のいずれかのオプションを選択します。
  - **enable**（推奨）：OSPFv2 ネイバーがアップまたはダウンすると、システムは syslog メッセージを生成します。このオプションを選択すると、追加の **log-adj-changes** *log-type* 行がオブジェクトに追加されます。ネイバーが起動または停止した場合だけでなく、状態が変わるたびに syslog メッセージを送信したい場合、*log-type* をクリックして **detail** を選択します。

    詳細なメッセージが表示されないようにするには、*log-type* をオプションのままにします 。オブジェクトからこの行を削除しないでください。

- **disable**：syslog メッセージは生成されません。**no log-adj-changes** 行がオブジェクトに追加されます。この行は削除しないでください。

ステップ 7 オブジェクト本文の上にある [無効を表示（Show Disabled）] リンクをクリックして、その他のすべての設定行を追加します。

ステップ 8 エリア番号を設定します。

a) **area** *area-id* 行の左にある [+] をクリックして、コマンドを有効にします。コマンドは有効にするまで設定できません。

b) *area-id* をクリックし、エリアの番号を入力します。このエリア番号は、OSPFv2 エリアを定義する他のルータで使用されている番号と同じである必要があります。このエリア ID には、10 進数か IP アドレスを指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。

ステップ 9 エリア内でルーティングする必要があるネットワークとインターフェイスを設定します。

a) **configure area** *area-id options* 行の左にある [+] をクリックします。

b) *area-id* をクリックし、 **area** コマンドと同じエリア番号を入力します。

c) *options* をクリックして、**properties** を選択します。このアクションにより複数の行が追加されます。これには、デフォルトで有効になっている行、**network** コマンドが含まれます。

d) **network** コマンドで *network-object* をクリックし、この領域に含めるネットワークを定義するオブジェクトを選択します。通常、これは直接接続されたネットワークです。たとえば、内部インターフェイスの IP アドレスが 192.168.1.1/24 の場合、このコマンドに関連付けられているネットワークオブジェクトには 192.168.1.0/24 が含まれます。オブジェクトが存在しない場合は、[新しいネットワークの作成（Create New Network）] をクリックして、今すぐ作成します。

e) （オプション）**network** コマンドで *tag-interface* をクリックして、ネットワークにホストまたはルーティングするインターフェイスを選択します。このインターフェイスを選択すると、それがルーティングプロセスで使用されるため、インターフェイス上のアドレスを変更できなくなる場合があります。この場合、インターフェイスアドレッシングへの変更がルーティング設定に影響を与える可能性があることがわかります。

ここでインターフェイスを選択した場合は、インターフェイス上のアドレスを変更する前に、まずルーティングプロセスからインターフェイスを削除する必要があります。次に、IP アドレスを変更した後、必ずここに戻り、新しいネットワークとインターフェイスを選択して、ルーティングプロセスが正しく設定されていることを確認します。

f) その他の新しいエリア行はすべてオプションで、デフォルトでは無効になっています。これらのサービスが必要な場合にのみ設定してください。詳細については、「OSPF プロセスとエリア特性のカスタマイズ （4 ページ）」を参照してください。

ステップ 10 複数エリアネットワークのプロセスを設定する場合は、**area** と **configure area** の行の丸で囲まれた [-] の左側の領域にカーソルを合わせ、**[...]** > **duplicate** をクリックします。次に、前述のように、新しいエリアとそのネットワークを設定します。このルーティングプロセスが参加する必要があるすべてのエリアを定義するまで、このプロセスを繰り返します。

ステップ 11 [OK] をクリックします。

OSPF プロセスとエリア特性のカスタマイズ

OSPF には、デフォルト値を持つ多くのオプションが含まれています。これらの値は、多くのネットワークで適切に機能します。ただし、必要とする動作を正確に得るために、設定を1つ以上調整する必要がある場合があります。以降のトピックでは、OSPFv2 ルーティングプロセスをカスタマイズするためのさまざまな方法について説明します。

OSPF プロセスの詳細設定の構成

OSPFv2 プロセスの全体的な動作を制御する複数の設定を構成できます。これには、ディスタンスメトリック、タイマー、グレースフルリスタート、リンク ステート アドバタイズメントやその他のルーティングアップデートの送信に使用されるルータ ID などがあります。これらの設定の多くには、ほとんどのネットワークに適しているデフォルト設定があります。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータを有効にした場合は、OSPF を設定しているルータの表示アイコン（  ）をクリックします。

ステップ 3 [OSPF] タブをクリックします。

ステップ 4 OSPF プロセスオブジェクトを追加または編集します。

ステップ 5 **setup ospf** 行を見つけます。

オブジェクトを追加する場合は、[無効を表示（Show Disabled）] リンクをクリックして、この行を表示する必要があります。次に、コマンドの [+] をクリックして有効にし、*configuration* をクリックして、**advanced** を選択します。デフォルトで有効になっているコマンドは、デフォルト値を使用してすでに有効になっています。

オブジェクトを編集するときには、その行はすでに有効になっています。

この手順の残りの部分では、[無効を表示（Show Disabled）] をクリックしたことを前提としています。コマンドが表示されない場合は、無効なコマンドが表示されるようになっていることを確認してください。

ステップ 6 （オプション）ルータ ID を設定します。

[+] をクリックして **router-id** コマンドを有効にし、変数をクリックして、このデバイスからルータアップデートを送信するときに使用する IPv4 アドレスを入力します。OSPF システム内の 2 台のルータが同じルータ ID を持つことはできないため、ID がエリア内で一意であることを確認してください。

プロセスに対してルータ ID を明示的に指定しない場合、システムはアクティブインターフェイスに割り当てられている最も大きい IP アドレスを使用します。そのため、選択したインター

フェイスを無効にするか、アドレスを変更すると、ルータ ID が変更される場合があります。ルータ ID を明示的に割り当てることにより、プロセスの一貫性を確保することができます。

ステップ 7 （オプション）サマリールートコストを計算する際に、RFC 1583 互換性を設定します。

[+] をクリックして **configure summary-route-cost** コマンドを有効にし、変数をクリックして、**any**（RFC 1583 互換性をオフにする）、または **rfc1583**（RFC 1583 互換性をオンにする）をクリックします。

OSPF オブジェクトではこのコマンドはデフォルトで有効になっていませんが、実際は RFC 1583 互換性が、サマリールートのコストを計算するときに使用されるデフォルトの方法となっています。定義された設定を CLI で確認すると、無効になっている設定のみが表示されます。

RFC 1583 の互換性が有効な場合、ルーティング ループが発生することがあります。ルーティング ループを防止するには、これを無効にします。RFC 1583 互換性は、OSPF ルーティング ドメイン内のすべての OSPF ルータで同じに設定するようにしてください。

ステップ 8 （オプション）マルチキャスト OSPF（MOSPF）リンク ステート アドバタイズメント（LSA）の syslog メッセージを抑制します。

[+] をクリックして、**ignore lsa mospf** コマンドを有効にします。

システムは、LSA タイプ 6 MOSPF パケットをサポートしていません。このコマンドを有効にすると、システムがこれらのパケットを受信したときに syslog メッセージが送信されないようにできるため、syslog サーバーのノイズを削減できます。

ステップ 9 ディスタンスメトリックを設定します。

次の **distance** コマンドは、デフォルトで有効になっています。ルートのタイプに基づいて、OSPF ルート アドミニストレーティブ ディスタンスを変更できます。距離は 1 ～ 255 で、数値が高いほど信頼度が低下します。これらのメトリックは、異なるプロセスからの類似したルートを比較する際に、学習したルートの相対値を判断するために使用されます。

- **distance ospf inter-area 110**を使用して無効にすることができます。数値をクリックして、あるエリアから別のエリアまでのすべてのルートの距離を設定します。
- **distance ospf intra-area 110**を使用して無効にすることができます。数値をクリックして、エリア内のすべてのルートの距離を設定します。
- **distance ospf external 110**を使用して無効にすることができます。数値をクリックして、再配布によって取得した他のルーティングドメインからのルートの距離を設定します。

ステップ 10 OSPF プロセスのルート計算タイマーを設定します。

次のタイマーコマンドは、これらのデフォルト値で有効になっています。

- **timers lsa arrival 1000**を使用して無効にすることができます。数値をクリックして、システムが OSPF ネイバーから同じリンク ステート アドバタイズメント（LSA）を受け入れる最小間隔を設定します（0 ～ 600000 ミリ秒）。このコマンドを使用して、ネイバーから着信する同じ LSA を受信する間に経過する必要がある最小間隔を指定します。この最小時間より前に着信した LSA は無視されます。

- **timers pacing flood 33**を使用して無効にすることができます。数値をクリックして、フラッディングキュー内の LSA がアップデートの合間にペーシング処理される時間を設定します（5 ～ 100 ミリ秒）。
- **timers pacing lsp-group 240**を使用して無効にすることができます。数値をクリックして、OSPF リンク ステート アドバタイズメント（LSA）を 1 つのグループに収集し、更新、チェックサム、または期限切れにする間隔を設定します（10 ～ 1800 秒）。
- **timers pacing retransmission 66**を使用して無効にすることができます。数値をクリックして、再送信キュー内の LSA がペーシング処理される時間間隔を設定します（5 ～ 200 ミリ秒）。OSPF パケットフラッディングの要件を満たす他のオプションをすべて使用した場合に限り、パケット再送信ペーシングタイマーを変更することが推奨されます。特に、デフォルトのフラッディングタイマーを変更する前に、集約、スタブエリアの使用方法、キューの調整、およびバッファの調整を設定してください。
- **timers throttle lsa 0 5000 5000**を使用して無効にすることができます。数値をクリックして、Open Shortest Path First（OSPF）のリンクステート アドバタイズメント（LSA）生成に対するレート制限値を設定します。LSA および SPF スロットリングは、ネットワークが不安定になっている間に OSPF の LSA 更新頻度を低下させて、より高速な OSPF コンバージェンスを可能にするダイナミックメカニズムを提供します。値は次のとおりです。
  - [インターバル（開始）（Start Interval）]（最初の数値）：LSA の最初のオカレンスを生成する最小遅延（1 ～ 600000 ミリ秒）。LSA の最初のインスタンスは、ローカル OSPF トポロジの変更直後に生成されます。次の LSA は、この開始インターバルの後にのみ生成されます。遅延なしで LSA が生成されるようにするには、0 を指定します。
  - [ホールド時間（Hold Time）]（2 番目の数値）：LSA を再生成する最小遅延（1 ～ 600000 ミリ秒）。この値は、LSA 生成の時間を制限する従属レートを計算するために使用されます。
  - [最大インターバル（Maximum Interval）]（3 番目の数値）：LSA を再生成する最大遅延（1 ～ 600000 ミリ秒）。
- **timers throttle spf 5000 10000 10000**を使用して無効にすることができます。数値をクリックして、最短パス優先（SPF）生成のレート制限値を設定します。値は次のとおりです。
  - [インターバル（開始）（Start Interval）]（最初の数値）：SPF 計算の変更を受信するまでの遅延（1 ～ 600000 ミリ秒）。
  - [ホールド時間（Hold Time）]（2 番目の数値）：1 回目の SPF 計算と 2 回目の SPF 計算の間の遅延（1 ～ 600000 ミリ秒）。
  - [最大インターバル（Maximum Interval）]（3 番目の数値）：SPF 計算の最大待機時間（1 ～ 600000 ミリ秒）。

ステップ 11　（オプション）デフォルトの外部ルートを OSPF ルーティングドメインに生成します。

+ をクリックして、**default-information originate** コマンドを有効にします。次のコマンドを有効にして設定し、機能を微調整することができます（オプション）。

- **default-information originate always**を使用して無効にすることができます。デフォルトルートがない場合でも、常にデフォルトルートをアドバタイズします。
- **default-information originate metric 1 metric-type** *metric-type-value*。デフォルトルートを生成するためのメトリックのタイプと値。
  - **metric** の数値をクリックして、OSPF のデフォルトメトリック値を入力します（0 ～ 16777214）。別の値が必要であることがわかっている場合を除き、「10」と入力します。
  - **metric-type** の数値をクリックして、OSPF 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る外部リンクタイプを選択します（1または2）。デフォルトは 2 です。
- **default-information originate route-map** *route-map*。ルーティングプロセスを指定するルートマップを選択します。このルートマップが一致した場合、このルーティングプロセスによりデフォルトルートが生成されます。

ステップ 12 （オプション）デバイスが高可用性（HA）用に設定されている場合、Non-Stop Forwarding（NSF）グレースフルリスタートを設定します。

システムでは、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。この機能は、コンポーネントに障害が発生した場合（たとえば、HA でアクティブ装置がスタンバイ装置にフェールオーバーした場合や、クラスタのプライマリユニットに障害が発生してセカンダリユニットが新しいプライマリとして選出された場合）、またはスケジュールされたヒットレス ソフトウェア アップグレードがある場合に役立ちます。

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。

デバイスは NSF 対応または NSF 認識として設定できます。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、動作中のモードに関係なく、NSF 認識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、デバイスが高可用性（フェールオーバー）であるかスパンド EtherChannel（L2）クラスタモードである必要があります。

（注）
グレースフルリスタートも設定する場合は、fast hello パケットを使用するように OSPF プロセスを設定しないでください。fast hello パケットを使用するとグレースフルリスタートは発生しません。これは、アクティブユニットとスタンバイユニット間のロール変更にかかる時間が、設定されている dead 間隔を超えるためです。

グレースフルリスタートを設定するには、次の手順を実行します。

a) + をクリックして、**configure nsf graceful-restart** コマンドを有効にします。
b) *mechanism* 変数をクリックして、次のいずれかを選択します。

- **cisco** Cisco RFC 4811 および RFC 4812 に従って NSF 対応デバイスを設定します。
- **ietf** IETF RFC 3623 に従って NSF 対応デバイスを設定します。
- **both** NSF 対応デバイスではなく NSF 認識ヘルパーとしてデバイスを設定します。
- **none** グレースフルリスタートを無効にします（事前に設定している場合）。

c) 前の手順での選択内容により、仕様に従ってグレースフルリスタートを実装するために必要なコマンドが追加されます。これらのコマンドは無効にしないでください。必要に応じて詳細な設定が必要となるコマンドが 1 つだけあります。次に、追加されたコマンドの説明を示します。このコマンドの **no** 形式は、関連する機能をオフにします。

- **nsf cisco helper**を使用して無効にすることができます。Cisco Nonstop Forwarding（NSF）ヘルパーモードを有効にします。NSF 対応 Firewall Threat Defense デバイスがグレースフルリスタートを実行しているときに、ヘルパー Firewall Threat Defense デバイスはそのノンストップ フォワーディングの復帰プロセスを支援します。
- **nsf ietf helper** *mode-option*。IETF ノンストップ フォワーディング（NSF）ヘルパーモードを有効にします。NSF 対応 Firewall Threat Defense デバイスがグレースフルリスタートを実行しているときに、ヘルパー Firewall Threat Defense デバイスはそのノンストップ フォワーディングの復帰プロセスを支援します。オプションで、*mode-option* をクリックして、厳密なリンクステートアドバタイズメント（LSA）チェックを有効にすることができます。厳密な LSA チェックを有効にすると、再起動しているシステムにフラッディングする可能性がある LSA の変更があることをヘルパーシステムが検出した場合、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、再起動しているシステムの再送リスト内に変更された LSA がある場合、ヘルパーシステムは再起動しているシステムのプロセスの支援を終了します。
- **capability lls**を使用して無効にすることができます。シスコ グレースフルリスタートに必要なリンクローカルシグナリング（LLS）を有効にします。
- **capability opaque**を使用して無効にすることができます。IETF グレースフルリスタートに必要な Opaque リンクステート アドバタイズメント（LSA) を有効にします。

ステップ 13 [OK] をクリックします。

OSPF エリアプロパティの設定

複数の OSPF エリアパラメータを設定できます。エリア内でアドバタイズするネットワークに加えて、フィルタリングと仮想リンクを定義できます。さらに、これらのエリアパラメータに

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。

エリアパラメータを設定する場合は、システムがエリア内でどのように機能するかを把握しておく必要があります。

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 はリンクステート アドバタイズメント（LSA）を使用して、使用可能なルータ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すると、ABR として機能するシステムを使用して、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。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータを有効にした場合は、OSPF を設定しているルータの表示アイコン（  ）をクリックします。

ステップ 3 [OSPF] タブをクリックします。

ステップ 4 OSPF プロセスオブジェクトを追加または編集します。

ステップ 5 エリア番号を設定します。

a) **area** *area-id* 行の左にある [+] をクリックして、コマンドを有効にします。コマンドは有効にするまで設定できません。

b) *area-id* をクリックし、エリアの番号を入力します。このエリア番号は、OSPFv2 エリアを定義する他のルータで使用されている番号と同じである必要があります。このエリア ID には、10 進数か IP アドレスを指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。

ステップ 6 エリア内でルーティングする必要があるネットワークとインターフェイスを設定します。

a) **configure area** *area-id options* 行の左にある [+] をクリックします。

b) *area-id* をクリックし、 **area** コマンドと同じエリア番号を入力します。

c) *options* をクリックして、**properties** を選択します。このアクションにより複数の行が追加されます。これには、デフォルトで有効になっている行、**network** コマンドが含まれます。

d) **network** コマンドで *network-object* をクリックし、この領域に含めるネットワークを定義するオブジェクトを選択します。通常、これは直接接続されたネットワークです。たとえば、内部インターフェイスの IP アドレスが 192.168.1.1/24 の場合、このコマンドに関連付けられているネットワークオブジェクトには 192.168.1.0/24 が含まれます。オブジェクト

が存在しない場合は、[新しいネットワークの作成（Create New Network）] をクリックして、今すぐ作成します。

e) （オプション）**network** コマンドで *tag-interface* をクリックして、ネットワークにホストまたはルーティングするインターフェイスを選択します。このインターフェイスを選択すると、それがルーティングプロセスで使用されるため、インターフェイス上のアドレスを変更できなくなる場合があります。この場合、インターフェイスアドレッシングへの変更がルーティング設定に影響を与える可能性があることがわかります。

ここでインターフェイスを選択した場合は、インターフェイス上のアドレスを変更する前に、まずルーティングプロセスからインターフェイスを削除する必要があります。次に、IP アドレスを変更した後、必ずここに戻り、新しいネットワークとインターフェイスを選択して、ルーティングプロセスが正しく設定されていることを確認します。

ステップ 7 （オプション）スタブエリアまたはNot-So-Stubby Area（NSSA）に送信されるデフォルトサマリールートのコストを設定します。

このオプションは、次に説明するように、エリアをスタブまたはNSSAとして設定した場合にのみ有効です。[+] をクリックして、エリアプロパティの次のコマンドを有効にします。

area *area-id* **default-cost 1**

必要に応じて、正しいエリア ID を入力します。次に、番号をクリックして、ルートの相対コストを 0 ～ 16777214 の範囲で入力します。デフォルトは 1 です。数値が大きいほど、宛先に適用される別のルートでルートが使用される可能性が低くなります。

ステップ 8 （オプション）エリアのプレフィックス フィルタリングを設定します。

エリアボーダールータ（ABR）のOSPFv2エリア間のタイプ3リンクステートアドバタイズメント（LSA）でアドバタイズされたプレフィックスをフィルタ処理することができます。プレフィックスの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。プレフィックスのフィルタリングでは、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。

このコマンドを設定する前に、**[デバイス（Device）] > [詳細設定（Advanced Configuration）]** ページで、スマート CLI オブジェクトであるプレフィックスリストを作成する必要があります。インバウンドまたはアウトバウンドアドバタイズメントに対して個別のプレフィックスリストを設定できます。フィルタ方向パラメータの方向を選択します。

area *area-id* **filter-list prefix** *prefix-list filter-direction*

ステップ 9 （オプション）エリアをスタブエリアとして設定します。

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。適切に動作させるには、スタブエリアでデフォルトルーティングを使用する必要があります。スタブエリアに送信される LSA の数をさらに減らすには、ABR で実行する **area stub** コマンドに **no-summary** キーワードを設定して、スタブエリアにサマリー リンク アドバタイズメント（LSA タイプ 3）が送信されないようにします。

エリアをスタブとして設定するには、以下を実行します。

a) setup area-id as type 行の左にある [+] をクリックします。
b) [type] をクリックし、**stub** を選択します。これにより、セットアップ行の後に area stub コマンドが追加されます。
c) オプションで、**area stub** コマンドで [stub-parameters] をクリックし、**no-summary** を選択します。

ステップ 10 （オプション）エリアを Not-So-Stubby Area（NSSA）に設定します。

Not-So-Stubby Area（NSSA）は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 のエリア境界ルータ（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。

OSPF 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、接続エリアに NSSA を利用することによって管理を簡略化できます。スタブエリアにはリモートサイトのルートが再配布されないため、企業サイトの境界ルータとリモートルータ間の接続に OSPFv2 スタブエリアを利用できず、2 つのルーティングプロトコルを維持する必要がありました。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。

エリアを NSSA として設定するには、以下を実行します。

a) **setup** *area-id* **as** *type* 行の左にある [+] をクリックします。
b) [type] をクリックし、**nssa** を選択します。これにより、setup 行の後に、**area nssa** コマンドを含む複数のコマンドが追加されます。このコマンドはイネーブルのままにする必要があります。
c) （オプション）NSSA にタイプ 7 のデフォルトルートを生成するには、[+] をクリックして次のコマンドを有効にします。

   area *area-id* **nssa default-information-originate metric 1 metric-type 2**

   オプションで、次の値を調整できます。

- **metric** の数値をクリックして、OSPF のデフォルトメトリック値を入力します（0 ～ 16777214）。別の値が必要であることがわかっている場合を除き、「10」と入力します。
- **metric-type** の数値をクリックして、OSPF 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る外部リンクタイプを選択します（1 または 2）。デフォルトは 2 です。

d) （オプション）システムが ABR であり、他のルーティングプロトコルから再配布して、NSSA ではなく通常のエリアにのみルートをインポートする場合は、[+] をクリックして次のコマンドを有効にします。

area *area-id* **nssa no-redistribution**

e) （オプション）サマリールートを NSSA に挿入しない場合は、[+] をクリックして次のコマンドを有効にします。

area *area-id* **nssa no-summary**

ステップ 11 （オプション）エリアの仮想リンクを設定します。

OSPF では、すべてのエリアがバックボーン エリアに接続されている必要があります。バックボーンへの接続が失われた場合は、仮想リンクを確立して修復できます。バックボーンエリアに接続されているルータへの仮想リンクを設定できます。

a) **configure area** *area-id* **virtual-link** *ip_address option* 行の左にある [+] をクリックします。
b) [ip_address] をクリックして、仮想リンクを確立するルータのルータ ID を入力します。
c) （オプション）[option] をクリックして **properties** を選択し、次の属性を調整します。これらの属性はすべて、ほとんどのネットワークに適したデフォルト値になっています。これらのコマンドの最初の部分は、同じコマンドのパラメータであるため、省略されています。

- **authentication** *auth-type*。[+] をクリックしてコマンドを有効にし、[auth-type] をクリックして **none**、**password**、または **message-digest** を選択します。[none] 以外の項目を選択した場合は、キーオプションを設定します。このオプションは、OSPFv2 インターフェイスと OSPF 認証の設定 （19 ページ） で説明されているように、OSPF インターフェイスで設定するものと同じです。他のルータが認証を使用している場合にのみ、認証を設定します。
- **hello-interval 10**を使用して無効にすることができます。番号をクリックし、インターフェイスで送信される hello パケットの間隔を 1 ～ 65535 秒の範囲で入力します。
- **retransmit-interval 5**を使用して無効にすることができます。番号をクリックし、仮想リンクの LSA 再送信間の時間を 1 ～ 65535 秒の範囲で入力します。
- **transmit-delay 1**を使用して無効にすることができます。番号をクリックし、OSPF がトポロジ変更を受信してから最短パス優先（SPF）計算を開始するまでの遅延時間を 0 ～ 65535 秒の範囲で入力します。

d) 別の仮想リンクを定義するには、**[...]** > **[重複（Duplicate）]**（**configure area virtual-link** コマンドの横）をクリックします。必要な数だけ定義します。

ステップ 12 （オプション）システムがエリア境界ルータ（ABR）の場合は、エリアのルートを統合または集約するための範囲を設定します。

area range コマンドを設定すると、その結果、1 つの集約ルートが ABR によって他のエリアにアドバタイズされます。ルーティング情報は、エリア境界でまとめられます。エリアの外部では、アドレス範囲ごとに 1 つのルートがアドバタイズされます。この動作は、「経路集約」と呼ばれます。1 つのエリアに複数の **area range** コマンドを設定できます。このように、OSPF は多くの異なるアドレス範囲セットのアドレスを集約できます。

ルート集約を設定するには、以下を実行します。

a) **area** *area-id* **range** *network-object range-parameters* 行の左側にある [+] をクリックします。
b) [network-object] をクリックし、集約するルートのアドレス範囲を定義するネットワークオブジェクトを選択します。
c) （オプション）[range-parameters] をクリックし、次のいずれかの属性を選択します。

- **advertise**を使用して無効にすることができます。アドバタイズするアドレス範囲ステータスを設定し、タイプ 3 サマリー リンクステート アドバタイズメント（LSA）を生成します。これは、[no] オプションを選択した場合のデフォルトです。
- **not-advertise**を使用して無効にすることができます。アドレス範囲ステータスを DoNotAdvertise に設定します。Type 3 サマリー LSA は抑制され、コンポーネント ネットワークは他のネットワークから隠された状態のままです。

d) 別のルート集約を定義するには、**[...]** > **[重複（Duplicate）]**（**area range** コマンドの横）をクリックします。必要な数だけ定義します。

ステップ 13 マルチエリアネットワークのプロセスを設定する場合は、**area** と **configure area** の行の丸で囲まれた [-] の左側の領域にカーソルを合わせ、**[...]** > **[重複（Duplicate）]** をクリックします。次に、前述のように、新しいエリアとそのネットワークを設定します。このルーティングプロセスが参加する必要があるすべてのエリアを定義するまで、このプロセスを繰り返します。

ステップ 14 [OK] をクリックします。

スタティック OSPF ネイバーの設定

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、つまり、VPN トンネルを介して OSPF 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。

通常のブロードキャスト ネットワークのルータは隣接関係を形成できるため、それらのネットワーク上にあるスタティックネイバーを定義する必要はありません。

始める前に

システムがネイバーに到達するために使用するインターフェイスを決定します。ネイバールータを定義する前に、このインターフェイスの OSPF 設定を設定する必要があります。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータを有効にした場合は、OSPF を設定しているルータの表示アイコン（）をクリックします。

ステップ 3 [OSPF] タブをクリックします。

ステップ 4 OSPF インターフェイス オブジェクトを追加または編集し、選択したインターフェイスに対して **ospf network point-to-point non-broadcast** コマンドを有効にします。変更を保存します。

ステップ 5 OSPF プロセスオブジェクトを追加または編集します。

ステップ 6 [無効を表示（Show Disabled）] をクリックしすべてのコマンドを表示し、[+] をクリックして **neighbor** コマンドを有効にします。

ステップ 7 ネイバーアドレスを設定します。

neighbor *ip-address* **interface** *interface*

- [ip-address] をクリックし、ネイバールータの IP アドレスを入力します。
- [interface] をクリックして、システムがルータに到達するために使用するインターフェイスを選択します。

ステップ 8 必要に応じて、ネイバールータのスタティックルートを設定します。

ルータの IP アドレスが、選択したインターフェイスと同じネットワーク上にある場合、スタティックルートは必要ありません。たとえば、IP アドレスが 10.100.10.1/24 であるインターフェイスを選択し、ネイバーアドレスが 10.100.10.2/24 の場合、スタティックルートは必要ありません。

ステップ 9 **[...]** > **[重複（Duplicate）]**（**neighbor** コマンドの横）をクリックして、別のスタティックネイバーを定義できます。必要な数だけ定義します。

ステップ 10 [OK] をクリックします。

OSPF サマリー アドレスの設定

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。ただし、再配布されるルートのうち、指定のネットワークアドレスとマスクに含まれるすべてのものを 1 つのルートで表し、そのルートだけをアドバタイズするようにシステム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廃止できます。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。他のルーティングプロトコルから学習したルートを集約できます。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。集約ルートは、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の集約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。

始める前に

集約するすべてのアドレスのネットワークオブジェクトを作成します。

手順

ステップ1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ2 仮想ルータを有効にした場合は、OSPFを設定しているルータの表示アイコン（）をクリックします。

ステップ3 [OSPF] タブをクリックします。

ステップ4 OSPF プロセスオブジェクトを追加または編集します。

ステップ5 [Show Disabled] をクリックしてすべてのコマンドを公開し、[+] をクリックして **configure** *network-object* **as** *option* **summary-address** コマンドを有効にします。

ステップ6 [network-object] をクリックし、集約するアドレス空間を定義するオブジェクトを選択します。

ステップ7 [options] をクリックし、次のいずれかを選択します。

- **advertising**を使用して無効にすることができます。アドレスに一致するルートをアドバタイズします。
- **non-advertising**を使用して無効にすることができます。アドレスに一致するルートを抑制します。

ステップ8 （オプション）集約されたルートにタグ値を追加するには、[+] をクリックして **summary-address tag** コマンドを有効にし、[tag-number] 変数をクリックして、タグ番号（0～4294967295）を入力します。

この値はOSPF 自体には使用されません。自律システム境界ルータ（ASBR）間で情報を通信するために使用できます。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、その他のプロトコルには 0 が使用されます。

タグ値を使用する主な理由は、タグ番号に基づいて再配布を制御することです。再配布ルートマップでタグ値を使用しない場合は、ここで設定する必要はありません。

ステップ 9 別のルート集約を定義するには、**[...]** > **[重複（Duplicate）]**（**configure summary-address** コマンドの横）をクリックします。必要な数だけ定義します。

ステップ 10 [OK] をクリックします。

OSPF のフィルタ ルールの設定

各フィルタルールに必要なスマート CLI 標準アクセスリストオブジェクトを作成します。拒否アクセス制御エントリ（ACE）を使用してエントリに一致するルートを除外し、更新する必要があるルートの ACE を許可します。

始める前に

エリア境界ルータ（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。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータを有効にした場合は、OSPF を設定しているルータの表示アイコン（）をクリックします。

ステップ 3 [OSPF] タブをクリックします。

ステップ 4 OSPF プロセスオブジェクトを追加または編集します。

ステップ 5 [無効を表示（Show Disabled）] をクリックしてすべてのコマンドを表示し、[+] をクリックして **configure filter-rules** *direction* コマンドを有効にします。

ステップ 6 [direction] をクリックし、**in**（インバウンドアップデートをフィルタ処理する場合）または **out**（アウトバウンドアップデートをフィルタ処理する場合）を選択します。

ステップ 7 インバウンドフィルタの場合は、必要に応じて、アップデートをフィルタ処理するインターフェイスを指定できます。インターフェイスを指定しない場合、フィルタは任意のインターフェイスで受信されるすべてのアップデートに適用されます。

a) [+] をクリックして **distribute-list** *acl-name* **in interface** *interface* コマンドを有効にします。

b) [interface] 変数をクリックし、インターフェイスを選択します。

ステップ 8 アウトバウンドフィルタの場合は、必要に応じて、プロトコルを指定して、そのルーティングプロセスにアドバタイズされたルートにフィルタを制限できます。

distribute-list out コマンドには 2 つの形式があります。一方には [protocol] 変数の後に [identifier] 識別子があり、もう一方には [identifier] 識別子がありません。次のプロトコルを選択できます

が、追加の識別子情報を提供する必要があるかどうかに基づいて、これらのコマンドのバージョン間でプロトコルが分けられます。

- **connected**を使用して無効にすることができます。システムのインターフェイスに直接接続されているネットワークに対して確立されたルート用です。
- **static**を使用して無効にすることができます。手動で作成したスタティックルート用です。
- **rip**を使用して無効にすることができます。RIP にアドバタイズされたルート用です。
- **bgp** *automonous-system*：BGP にアドバタイズされたルート用です。[identifier] をクリックし、システムで定義されている BGP プロセスの自律システム番号を入力します。
- **eigrp** *automonous-system*：EIGRP にアドバタイズされたルート用です。[identifier] をクリックし、システムで定義されている EIGRP プロセスの自律システム番号を入力します。
- **ospf** *process-id*：OSPF にアドバタイズされたルート用です。[identifier] をクリックし、システムで定義されている他の OSPF プロセスのプロセス ID を入力します。

ステップ 9 **[...]** > **[重複（Duplicate）]**（**configure filter-rules** コマンドの横）をクリックして、別のフィルタルールを定義します。必要な数だけ定義します。

ステップ 10 [OK] をクリックします。

OSPF 再配布の設定

他のルーティングプロトコル、接続されたルート、およびスタティックルートからの OSPF プロセスへのルートの再配布を制御できます。

始める前に

OSPF への再配布を設定する前に、ルートを再配布するルーティングプロセスを設定し、変更を展開することがベストプラクティスです。

ルートマップを適用して、再配布されるルートを微調整する場合は、Smart CLI ルートマップオブジェクトを作成します。ルートマップに一致するルートが再配布され、一致しないルートはすべて再配布されません。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータを有効にした場合は、OSPF を設定しているルータの表示アイコン（  ）をクリックします。

ステップ 3 [OSPF] タブをクリックします。

ステップ 4 OSPF プロセスオブジェクトを追加または編集します。

ステップ 5 [無効を表示（Show Disabled）] をクリックしすべてのコマンドを表示し、[+] をクリックして **configure redistribution** コマンドを有効にします。

ステップ 6 [protocol] 変数をクリックし、ルートの再配布元となる送信元プロセスを選択します。**connected** および **static** のルート、あるいは **bgp**、**eigrp**、**isis**、**ospf**、または **rip** のいずれかによって生成されたルートを再配布できます。

ステップ 7 ルーティングプロセスを選択した場合は、[identifier] 変数をクリックして、必要な値を入力します。

- **bgp**、**eigrp**：自律システムの番号を入力します。
- **ospf**を使用して無効にすることができます。プロセス ID 番号を入力します。
- **connected**、**static**、**isis**、**rip**。**none** を入力します。別の値を入力しても、無視されます。

ステップ 8 （任意：IS のみ）**redistribute isis level-2** コマンドで、**level-2** をクリックして、IS-IS エリア（**level-1**）内でのみ学習したルートを再配布するか、IS-IS エリア（**level-2**）間、または両方（**level-1-2**）で再配布するかを選択します。

ステップ 9 （任意：すべてのプロトコル）再配布を制御するためにタグをルートに適用する場合は、[+] をクリックして **redistribute tag** *tag-number* コマンドを有効にし、変数をクリックして、再配布するルートに関連付けられているタグを入力します。タグ番号の範囲は 0 ～ 4294967295 です。

ステップ 10 （任意：すべてのプロトコル）標準クラスに準拠するものだけでなく、すべてのサブネットのルートを再配布する場合は、[+] をクリックして **redistribute subnets** コマンドを有効にします。

たとえば、このコマンドを有効にしない場合、10.100.10.0/24 の特定のルートは再配布されず、代わりに、10.0.0.0/8 のルートのみが再配布されます。

ステップ 11 （任意：すべてのプロトコル）ルートマップに基づいて再配布されるルートを微調整するには、[+] をクリックして **redistribute** *route-map* コマンドを有効にし、変数をクリックして、制限を定義するルートマップを選択します。

ルートマップを適用しない場合は、（再配布用に設定された他のコマンドに適合する）プロセスのすべてのルートが再配布されます。

ステップ 12 （任意：すべてのプロトコル）再配布されたルートのメトリックを微調整するには、[+] をクリックして次のコマンドを有効にし、オプションを設定します。

redistribute *protocol* **metric** *metric-value* **metric-type** *metric-type-value*

変数をクリックして、次のように設定します。

- **metric**を使用して無効にすることができます。配布されているルートのメトリック値（0 ～ 16777214）。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に渡されます。他のプロセスを OSPF プロセスに再配布する場合、デフォルトのメトリックは 20 です。
- **metric-type**を使用して無効にすることができます。メトリックタイプは、OSPF 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。デフォルトは 2 です。

ステップ 13 （任意：OSPF のみ）別の OSPF プロセスからルートを再配布する場合、次のコマンドはデフォルトで有効になっています。[-] をクリックして、不要なコマンドを無効化できます。

これらのコマンドで、OSPF ルートを他のルーティングドメインに再配布する条件を指定します。

- **redistribute ospf match external 1**を使用して無効にすることができます。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。
- **redistribute ospf match external 2**を使用して無効にすることができます。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。
- **redistribute ospf match internal**を使用して無効にすることができます。特定の自律システムの内部ルート。
- **redistribute ospf match nssa-external 1**を使用して無効にすることができます。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、Not-So-Stubby-Area（NSSA）専用としてマークされるルート。
- **redistribute ospf match nssa-external 2**を使用して無効にすることができます。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、Not-So-Stubby-Area（NSSA）専用としてマークされるルート。

ステップ 14 **[...]** > **[重複（Duplicate）]**（**configure redistribution** コマンドの横）をクリックして、別のプロトコルの再配布を設定できます。ネットワークに適したプロトコルごとの再配布を設定します。

ステップ 15 [OK] をクリックします。

OSPFv2 インターフェイスと OSPF 認証の設定

ネイバー OSPF ルータに面しているインターフェイスは、hello パケットなどの方法を用いてルータと通信して、ネイバーの正常性を確認し、ルーティングの更新を共有します。これらの特性の一部にはデフォルト設定がありますが、ベストプラクティスは、OSPF インターフェイス設定オブジェクトを使用してオプションを明示的に設定する方法です。OSPF ネイバールータに隣接する各インターフェイスのオブジェクトを作成します。

（注） ネットワーク上の各ルータは、認証および失われたネイバー検出の hello と dead 間隔について同じ値を持つ必要があります。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータを有効にした場合は、OSPF を設定しているルータの表示アイコン（）をクリックします。

ステップ 3 [OSPF] タブをクリックします。

ステップ 4 次のいずれかを実行します。

- 新しいオブジェクトを作成するには、**[+]** > **[OSPFインターフェイス設定（OSPF Interface Settings）]** をクリックするか、**[OSPFオブジェクトの作成（Create OSPF Object）]** > **[OSPFインターフェイス設定（OSPF Interface Settings）]** ボタンをクリックします。
- 編集するオブジェクトの横にある編集アイコン（）をクリックします。オブジェクトを編集すると、直接設定していない行が表示される場合があることに注意してください。これらの行は、設定されているデフォルト値を示すために公開されています。

インターフェイス設定オブジェクトが不要になった場合は、オブジェクトのごみ箱アイコンをクリックして削除します。

ステップ 5 オブジェクトの名前、さらにオプションで説明を入力します。

ステップ 6 インターフェイスの認証を設定します。

configure authentication *auth-type*

OSPF 認証を設定するには、各 OSPF インターフェイスでパスワードまたは認証キーを設定してから、そのエリア自体で認証を有効にする必要があります。インターフェイスとエリアで同じ認証方式を選択する必要があります。

auth-type をクリックして、次のオプションを選択できます。

- **none**：OSPF 認証を使用しない。リンクで動作するすべての OSPF ルータは、このルータとの隣接関係を確立できます。オブジェクトにコマンド **ospf authentication null** が追加されます。
- **password**：共有パスワードを使用して OSPF 接続を認証する。インターフェイス単位で各ネットワークに個別のパスワードを設定できます。とはいえ、OSPF 情報を交換するには、同じネットワーク上のすべての隣接ルータに同じパスワードを設定する必要があります。

  このオプションを選択すると、2 つのコマンド（**ospf authentication** および **ospf authentication-key** *key*）が追加されます。変数をクリックして、次のように設定します。

  - *key*：パスワードが格納されている秘密鍵オブジェクトを選択します。パスワードは最大 8 文字です。2 文字間にブランクを含めることができます。パスワードの先頭または末尾のブランクは無視されます。オブジェクトがまだ存在しない場合、リストの下部にある [新しい秘密鍵の作成（Create New Secret Key）] をクリックして作成します。

- **message-digest**：メッセージダイジェスト（MD5）を使用して OSPF 接続を認証します。MD5 認証は、通信の整合性を検証し、発信元を認証し、適時性をチェックします。両方のルータで同じ MD5 キーが使用されるように設定する必要があります。

  このオプションを選択すると、2 つのコマンド（**ospf authentication message-digest** および **ospf message-digest-key** *key-id* **md5** *key*）が追加されます。変数をクリックして、次のように設定します。

  - *key-id*：1 ～ 255 の認証キー ID 番号。同じキー ID および関連付けられた MD5 キーを使用して、ネイバールータを設定する必要があります。
  - *key*：MD5 キーが格納されている秘密鍵オブジェクトを選択します。キーは最大 16 文字の英数字のパスワードです。文字間にスペースを含めることができます。キーの先頭または末尾のスペースは無視されます。オブジェクトがまだ存在しない場合、リストの下部にある [新しい秘密鍵の作成（Create New Secret Key）] をクリックして作成します。

ステップ 7 （オプション）リンクステート アドバタイズメント（LSA）タイマーを設定します。

これらのタイマーにはデフォルト値があるため、ネットワークで別の設定が必要な場合にのみ変更する必要があります。次のコマンドを設定します。

- **ospf retransmit interval 5**：OSPF インターフェイスに属する隣接ルータに LSA を再送信する間隔の秒数。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秒数にする必要があります。範囲は 1 ～ 8192 秒です。デフォルト値は 5 秒です。5 をクリックし、新しい数値を入力して値を変更します。
- **ospf transmit-delay 1**：OSPF インターフェイスでリンクステート アップデート パケットを送信するために必要な推定秒数（1 ー 8192 秒）。デフォルト値は 1 秒です。1 をクリックし、新しい数値を入力して値を変更します。

ステップ 8 （オプション）他のすべての設定は、デフォルト値が設定されているか、オプションです。別の動作が必要な場合にのみ、それらを変更するか有効にします。オプションを表示するには、[無効を表示（Show Disabled）] リンクをクリックします。

次に、付加的なインターフェイス設定を示します。設定を有効にするには、コマンドの左側にある [+] をクリックして、コマンドを設定します（必要な場合）。

- **ospf cost** *value*：OSPF インターフェイスでパケットを送信するコスト（リンクステートメトリック）（1 ～ 65535）。値 1 は、インターフェイスに直接接続されているネットワークを表します。変数をクリックし、ネットワークで使用している番号に基づいてインターフェイスの性能を表すコストを入力します。

  値を決定する際、インターフェイスの帯域幅が大きいほど、そのインターフェイスでパケットを送信するための関連コストが低くなります。つまり、コストの値が大きければインターフェイス帯域幅が小さく、コストの値が小さければインターフェイス帯域幅が大きいということになります。選択した特定の数値には固有の意味はありません。この値は、OSPF エリア全体でインターフェイスに設定したその他の値に相対的なものです。これらの値は、接続先への最適ルートの計算に影響します。

Firepower Threat Defense デバイスでの OSPF インターフェイスのデフォルトのコストは 10 です。このデフォルトは、Cisco IOS ソフトウェアとは異なります。Cisco IOS ソフトウェアの場合、デフォルトのコストはファスト イーサネットおよびギガビット イーサネットでは 1、10BaseT では 10 です。ネットワークで ECMP を使用している場合には、このことを考慮に入れることが重要です。

- **ospf database-filter all out**：同期およびフラッディング中の OSPF インターフェイスへのすべての発信 LSA をフィルタで除外します。
- **ospf mtu-ignore**：受信データベースパケットの OSPF 最大伝送ユニット（MTU）不一致検出を無効にします。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、ネイバーがデータベース記述子（DBD）パケットを交換するときに実行されます。DBD パケット内の受信 MTU が着信インターフェイスに設定されている MTU より高い場合、OSPF の隣接性は確立されません。インターフェイス上の MTU 値を同じ値に修正できない場合は、MTU チェックを無効にすることができます。
- **ospf network point-to-point non-broadcast**：OSPF インターフェイスをポイントツーポイントのノンブロードキャスト ネットワークとして設定します。この設定により、VPN トンネルを介して OSPF ルートを送信できるようになります。このオプションを設定すると、ネイバーを動的に検出できなくなります。次の手順の実行も必要です。
  - このインターフェイスに対して 1 つのスタティックネイバーを定義するには、OSPF プロセスオブジェクトを更新します。また、ネイバールータの OSPF プロセスを更新して、このデバイスをスタティックネイバーとして定義します。
  - ネイバールータを指すスタティックルート（各ルータ上）を作成します。
- **ospf priority** *value*：ネットワーク内の他のルータと相対的なルータのプライオリティ（0 ～ 255）。デフォルトのプライオリティは 1 です。ネットワークにアタッチされている 2 つのルータがともに指定ルータになろうとした場合、ルータのプライオリティの高い方が優先されます。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。ルータのプライオリティがゼロに設定されているルータには、指定ルータまたはバックアップ指定ルータになる資格がありません。変数をクリックし、ネットワークで使用する相対的な番号付け方式に基づいてプライオリティを選択します。
- **ospf lost-neighbor-detection** *detection-mechanism*：ネイバールータがダウンしているかどうかをシステムがどのように判断するかを定義します。OSPF は、OSPF ルータがダウンしていると宣言されるたびにルートを再計算する必要があります。失われたネイバー検出の設定の詳細については、OSPFv2 の失われたネイバー検出と fast hello パケットの設定（OSPF インターフェイス設定）（23 ページ）を参照してください。

ステップ 9 [OK] をクリックします。

OSPFv2 の失われたネイバー検出と fast hello パケットの設定（OSPF インターフェイス設定）

OSPF プロセスは定期的に各ネイバールータに hello パケットを送信し、ネイバーが応答できることを確認します。応答の継続的な失敗は、ネイバールータ（全インターフェイスまたは隣接するインターフェイスのみ）がルーティングに使用できないことを示し、OSPF はルートを再計算する必要があり、OSPF システムは更新されたルーティングテーブルへのコンバージェンスが必要となります。

次の値を調整して、ネットワークを微調整できます。理想的には、ネイバーがダウンしていると宣言され、ルートが再計算される頻度を最小限に抑える必要があります。一方、OSPF ルータ（またはインターフェイス）が実際にダウンしたときに、ネットワークが適切なルーティングテーブルに再コンバージェンスするのにかかる時間を最小限に抑える必要もあります。

- [hello間隔（Hello interval）]：hello パケットを送信する時間の間隔です。デフォルトは 10 秒ごとです。必要に応じて、hello が 1 秒未満の間隔で送信される fast hello パケットを設定できます。fast hello パケットを使用すると、ダウンしているネイバーの検出と、ルーティングテーブルの再コンバージェンスが最速になります。
- [dead間隔（Dead interval）]：ネイバーから hello パケットが検出されなかった場合に、ネイバーが dead と宣言されるまでの時間の長さ。デフォルトは 40 秒（デフォルトの hello 間隔の 4 倍）です。ただし、fast hello パケットを使用している場合を除きます（この場合 dead 間隔は常に 1 秒）。小さい dead 間隔を指定すると、ダウンしているネイバーの検出が速くなり、コンバージェンスが向上しますが、ルーティングが不安定になる可能性があります。どのような場合でも、dead 間隔は hello 間隔よりも大きい値に設定する必要があります。ネットワーク内のすべての OSPF ルータで同じ dead 間隔を設定する必要があります。

[OSPFインターフェイス設定（OSPF Interface Settings）] オブジェクトで、失われたネイバー検出を設定します。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーをクリックします。

ステップ 2 仮想ルータを有効にした場合は、OSPF を設定しているルータの表示アイコン（  ）をクリックします。

ステップ 3 [OSPF] タブをクリックします。

ステップ 4 次のいずれかを実行します。

- 新しいオブジェクトを作成するには、**[+] > [OSPFインターフェイス設定（OSPF Interface Settings）]** をクリックするか、**[OSPFオブジェクトの作成（Create OSPF Object）] > [OSPFインターフェイス設定（OSPF Interface Settings）]** ボタンをクリックします。

- 編集するオブジェクトの横にある編集アイコン（  ）をクリックします。オブジェクトを編集すると、直接設定していない行が表示される場合があることに注意してください。これらの行は、設定されているデフォルト値を示すために公開されています。

ステップ 5 **ospf lost-neighbor-detection** *detection-mechanism* コマンドが表示されない場合は、[無効を表示（Show Disabled）] リンクをクリックします。

ステップ 6 コマンドを有効にするには、コマンドの左側にある [+] をクリックします。

ステップ 7 *detection-mechanism* をクリックし、実装するメカニズムを選択します。

- **dead-interval**：標準の hello 間隔を秒単位で設定します。次のコマンドが追加されます。必要に応じて値を調整します。
  - **ospf hello-interval 10**：hello 間隔（1 ～ 8,192 秒）。デフォルトは 10 です。この値は、dead 間隔より小さくする必要があります。値をクリックして、目的の数字を入力します。
  - **ospf dead-interval 40**：dead 間隔（1 ～ 8,192 秒）。推奨値は hello 間隔の 4 倍ですが、コンバージェンスを高速化するために短い時間を設定できます。
- **hello-multiplier**：1 秒未満の fast hello パケットを設定します。次のコマンドが追加されました。値を設定する必要があります。
  - **ospf dead-interval minimal hello-multiplier** *value*：変数をクリックし、1 秒間に送信する hello パケットの数を 3 ～ 20 の間で入力します。dead 間隔は、**minimal** キーワードによって 1 秒に設定されます。

ステップ 8 [OK] をクリックします。

OSPF のモニタリング

OSPF をモニターし、トラブルシューティングを行うには、CLI コンソールを開くか、またはデバイスの CLI にログインして、次のコマンドを使用します。また、[ルーティング（Routing）] ページの [コマンド（Commands）] メニューから、これらのコマンドの一部を選択することもできます。

追加オプションのリストを取得するには、**show ospf ?** を使用します。たとえば、プロセス ID、エリア ID、および仮想ルータを指定して、表示する情報を制限することができます。また、探している情報だけを対象とするその他のオプションも指定できます。次のリストは概要のみです。

- **show ospf**

  OSPFv2 ルーティング プロセスに関する一般情報を表示します。

- **show ospf border-routers**

ABR および ASBR までの内部 OSPFv2 ルーティング テーブル エントリを表示します。

- **show ospf database**

  特定のルータの OSPFv2 データベースに関係する情報のリストを表示します。

- **show ospf events**

  OSPF 内部イベント情報を表示します。

- **show ospf flood-list**

  OSPFv2 パケットペーシングの観察のために、インターフェイスへのフラッディングを待機しているLSAのリストを表示します。OSPFv2アップデートパケットは、自動的にペーシングされるため、各パケットの送信間隔が33ミリ秒未満になることはありません。ペーシングを行わないと、リンクが低速の状態でアップデートパケットの一部が失われたり、ネイバーがアップデートを十分すばやく受信できなくなったり、あるいは、ルータがバッファ スペースを使い切ってしまったりすることがあります。

  ペーシングは、再送信間でも、送信効率を高めて再送信パケットの損失を最小にするために利用されます。インターフェイスからの送信を待機している LSA を表示することもできます。ペーシングの利点は、OSPFv2 アップデートおよび再送信パケットの送信の効率をよくすることです。

- **show ospf interface**

  OSPFv2-related インターフェイスの情報を表示します。

- **show ospf neighbor**

  OSPFv2 ネイバー情報をインターフェイスごとに表示します。

- **show ospf nsf**

  OSPFv2 関連のノンストップ フォワーディング（NSF）情報を表示します。

- **show ospf request-list**

  ルータで要求されるすべての LSA のリストを表示します。

- **show ospf 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。

- **show ospf rib**

  OSPF ルータ情報ベース（RIB）を表示します。

- **show ospf statistics**

  さまざまな OSPF 統計（SPF が実行された回数、理由、期間など）を表示します。

- **show ospf summary-addresses**

  OSPFv2 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。

- **show ospf traffic**

特定の OSPFv2 インスタンスで送信または受信されたパケットのさまざまなタイプのリストを表示します。

- **show ospf virtual-links**

  OSPFv2-related 仮想リンク情報を表示します。

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。

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。