CHAPTER 5

NSF with SSO スーパーバイザ エンジンの冗長構成の設定

この章では、Stateful Switchover（SSO; ステートフル スイッチオーバー）機能を備えた Cisco Nonstop Forwarding（NSF; ノンストップ フォワーディング）を使用してスーパーバイザ エンジンの冗長構成を設定する方法について説明します。

（注）

- この章で使用しているコマンドの構文および使用方法の詳細については、次の URL で『*Catalyst Supervisor Engine 32 PISA Cisco IOS Command Reference*, Release 12.2ZY』を参照してください。

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/command/reference/cmdref.html
- RPR の冗長構成については、第 6 章「RPR スーパーバイザ エンジンの冗長構成の設定」を参照してください。
- NSF with SSO は、IPv6 マルチキャスト トラフィックをサポートしていません。

この章で説明する内容は、次のとおりです。

NSF with SSO スーパーバイザ エンジンの冗長構成の概要

ここでは、NSF with SSO を使用したスーパーバイザ エンジンの冗長構成について説明します。

NSF with SSO スーパーバイザ エンジンの冗長構成の概要

（注）　冗長スーパーバイザ エンジンがスタンバイ モードの場合、冗長スーパーバイザ エンジンの 2 つのギガビット イーサネット インターフェイスは常にアクティブです。

Catalyst 6500 シリーズ スイッチは、プライマリ スーパーバイザ エンジンが故障した場合に冗長スーパーバイザ エンジンがテイクオーバーすることにより、耐障害性をサポートします。Cisco NSF は SSO と連動することによって、スイッチオーバー後にユーザがネットワークを利用できない時間を最小限に抑えるながら、IP パケットの転送を継続します。Catalyst 6500 シリーズ スイッチでは、Route Processor Redundancy（RPR）もサポートします。RPR モードについては、第 6 章「RPR スーパーバイザ エンジンの冗長構成の設定」を参照してください：

次のイベントが発生すると、スイッチオーバーが行われます。

- アクティブ スーパーバイザ エンジンでのハードウェア障害
- スーパーバイザ エンジン間のクロック同期損失
- 手動スイッチオーバー

SSO の動作

SSO は、スーパーバイザ エンジンの 1 つをアクティブに設定してもう 1 つのスーパーバイザ エンジンをスタンバイに指定し、その後これらの間で情報を同期させます。アクティブ スーパーバイザ エンジンが故障したり、スイッチから取り外されたり、またはメンテナンスのため手動でシャットダウンしたりするような場合に、アクティブ スーパーバイザ エンジンから冗長スーパーバイザ エンジンへのスイッチ オーバーが発生します。このタイプのスイッチオーバーでは、レイヤ 2 トラフィックは中断されません。

SSO を実行しているネットワーキング装置では、アクティブ スーパーバイザ エンジンが故障したあとに冗長スーパーバイザ エンジンがいつでも制御を行えるように、両方のスーパーバイザ エンジンが同じ設定で動作していなくてはなりません。また SSO スイッチオーバーでは、Forwarding Information Base（FIB; 転送情報ベース）および隣接エントリを維持していて、スイッチオーバー後にレイヤ 3 トラフィックを転送できます。設定情報とデータ構造は、起動時やアクティブ スーパーバイザ エンジンの設定変更が発生したときに、アクティブ スーパーバイザエンジンから冗長スーパーバイザ エンジンへ同期するようになっています。2 つのスーパーバイザ エンジン間の初期同期後に、SSO は転送情報などの両者間のステート情報を維持しています。

スイッチオーバー時に、システム制御およびルーティング プロトコル実行はアクティブ スーパーバイザから冗長スーパーバイザ エンジンに転送されます。アクティブ スーパーバイザ エンジンから冗長スーパーバイザ エンジンへの切り替えには、0 ～ 3 秒かかります。

NSF の動作

Cisco NSF は、常に SSO とともに稼動し、レイヤ 3 トラフィックの冗長機能を提供します。NSF は、SSO と連動して、スイッチオーバー後にユーザがネットワークを使用できない時間を最小限に抑えます。NSF の主な目的は、スーパーバイザ エンジンのスイッチオーバー後に IP パケットの転送を継続させることです。

Cisco NSF は、ルーティングについては Border Gateway Protocol（BGP）、Open Shortest Path First（OSPF）、Enhanced Interior Gateway Routing Protocol（EIGRP）、および Intermediate System-to-Intermediate System（IS-IS）プロトコルで、転送については Cisco Express Forwarding（CEF）でサポートされています。ルーティング プロトコルは NSF 機能と NSF 認識によって強化されています。つまり、これらのプロトコルを実行しているルータは、スイッチオーバーを検出し、ネットワーク トラフィックの転送を継続して、ピア装置からのルーティング情報を回復するための必要な措置を行います。ピア装置から情報を受信するのではなく、スイッチオーバー後のルーティング情報を回復するためにアクティブ スーパーバイザ エンジンと冗長スーパーバイザ エンジンとの間で同期しているステート情報を使用するように、IS-IS プロトコルを設定できます。

ネットワーキング装置は、NSF 互換ソフトウェアを実行している場合に NSF を認識します。NSF をサポートするように装置を設定した場合に装置は NSF 対応になります。NSF 認識ネイバーまたは NSF 対応ネイバーからルーティング情報を再構築します。

スイッチオーバー中にルーティング プロトコルが Routing Information Base（RIB; ルーティング情報ベース）テーブルを再構築している間、各プロトコルは CEF に依存してパケット転送を継続します。ルーティング プロトコルが収束したあと、CEF が FIB テーブルを更新して失効したルート エントリを削除します。次に、CEF は新しい FIB 情報でライン カードを更新します。

Cisco Express Forwarding

NSF で重要となる要素は、パケット転送です。シスコのネットワーキング装置では、パケット転送は CEF で提供されます。CEF は FIB を維持し、スイッチオーバー時に使用中の FIB 情報を使用してスイッチオーバー中のパケット転送を継続します。この機能により、スイッチオーバー中のトラフィックの中断を低減することができます。

通常の NSF 動作中に、アクティブ スーパーバイザ エンジンの CEF が現行の FIB および隣接データベースを冗長スーパーバイザ エンジンの FIB および隣接データベースと同期させます。アクティブ スーパーバイザ エンジンのスイッチオーバーでは、冗長スーパーバイザ エンジンに最初からアクティブ スーパーバイザ エンジンで使用中のミラー イメージである FIB と隣接データベースがあります。インテリジェント ライン カードを使用したプラットフォームでは、ライン カードはスイッチオーバーの前後で現行の転送情報を維持します。転送エンジンを使用したプラットフォームでは、アクティブ スーパーバイザ エンジンの CEF によって送信される変更を使用して、CEF が冗長スーパーバイザ エンジンの転送エンジンを最新の状態に保ちます。ライン カードや転送エンジンは、インターフェイスやデータ パスが使用可能であるかぎりはスイッチオーバー後も転送を継続できます。

ルーティング プロトコルがプレフィクスごとに RIB を再び読み込み始めるため、CEF に対してプレフィクスごとの更新が行われます。CEF はこれを使用して FIB と隣接データベースを更新します。既存エントリと新規エントリが最新であることを示す新しいバージョン（「エポック」）番号を受信します。ライン カードや転送エンジンでは、コンバージェンス中に転送情報が更新されます。RIB が収束すると、スーパーバイザ エンジンが信号通知を行います。ソフトウェアが、現在のスイッチオーバー エポックよりも古いエポックを持つすべての FIB と隣接エントリを削除します。これで、FIB は最新のルーティング プロトコル転送情報となるのです。

マルチキャスト MLS（MMLS）NSF with SSO

（注）　NSF with SSO は、IPv6 マルチキャスト トラフィックをサポートしていません。IPv6 マルチキャスト トラフィックのサポートを設定する場合、RPR 冗長構成を設定します。

ルータでスイッチングされるレイヤ 3 マルチキャスト トラフィックがスイッチオーバー時に廃棄されないようにするには、Multicast Multilayer Switching（MMLS; マルチキャスト マルチレイヤ スイッチング）NFS with SSO が必要です。マルチキャスト MMLS NSF with SSO がない場合、レイヤ 3 マルチキャスト トラフィックはマルチキャスト プロトコルが収束するまでに廃棄されます。

スイッチオーバー プロセスの間、トラフィックは（前にアクティブであったスーパーバイザ エンジンの）古いデータベースを使用して転送されます。マルチキャスト ルーティング プロトコル コンバージェンスが実行されたあと、新しくアクティブになった Programmable Intelligent Services Accelarator（PISA）によってダウンロードされたショートカットが既存のフローと結合されて新しいショートカットとしてマーキングされます。失効したエントリは、NSF がスイッチオーバー時に機能するように、確実に新しいキャッシュへの円滑な移行を実行する間に、ゆっくりとデータベースから削除されます。

Protocol Independent Multicast（PIM）sparse（疎）モードなどのマルチキャスト ルーティング プロトコルと PIM dense（密）モードがデータ駆動型であるため、マルチキャスト パケットはプロトコルが収束できるようにスイッチオーバー中にルータにリークされます。

トラフィックは双方向 PIM などの制御駆動型プロトコルに対してソフトウェアで転送する必要がないので、スイッチはこれらのプロトコルの古いキャッシュを使用してパケットのリークを継続します。ルータは mroute キャッシュを作成して、ハードウェアにショートカットをインストールします。新しいルートを学習したあと、タイマーがトリガーされ、データベースを捜索して古いフローを消去します。

（注）　マルチキャスト MLS NSF with SSO は、ユニキャスト プロトコルでは NSF のサポートが必要です。

ルーティング プロトコル

ルーティング プロトコルは、アクティブ スーパーバイザ エンジンの PISA 上でだけ動作し、近接ルータからルーティング更新を受信します。ルーティング プロトコルは、冗長スーパーバイザ エンジンの PISA 上では動作しません。スイッチオーバー後に、ルーティング プロトコルは、ルーティング テーブルの再構築に役立てるために、NSF を認識する近接装置が送信するステート情報を要求します。またこの代わりに、近接装置が NSF を認識しないような環境にある NSF 対応装置のルーティング テーブルの再構築に役立つように、アクティブ スーパーバイザ エンジンからのステート情報を冗長スーパーバイザ エンジンと同期させるように、IS-IS プロトコルを設定できます。Cisco NSF は BGP、OSPF、IS-IS、および EIGRP プロトコルをサポートします。

（注）　NSF 動作の場合、ルーティング プロトコルがルーティング情報を再構築している間、ルーティング プロトコルは CEF に依存してパケット転送を継続します。

BGP の動作

NSF 対応ルータが BGP ピアと BGP セッションを開始するときに、OPEN メッセージをピアに送信します。メッセージには、NSF 対応装置に「グレースフル」リスタート機能があることを示すステートメントが含まれています。グレースフル リスタートとは、スイッチオーバー後に BGP ルーティング ピアでルーティング フラップが発生しないようにするための仕組みです。BGP ピアがこの機能を受信すると、メッセージを送信している装置が NSF 対応であることを認識します。NSF 対応ルータと BGP ピアは、セッション確立時に OPEN メッセージでグレースフル リスタート機能を交換する必要があります。両方のピアがグレースフル リスタート機能を交換しない場合、このセッションでグレースフル リスタートは行われません。

スーパーバイザ エンジンのスイッチオーバー中に BGP セッションが切断された場合、NSF 認識 BGP ピアは、NSF 対応ルータに関連したすべてのルートを失効とマーキングします。ただし、所定の時間内は、引き続きこれらのルートを転送の決定に使用します。この機能により、新しくアクティブになったスーパーバイザ エンジンが BGP ピアとのルーティング情報のコンバージェンスを待機している間にパケットが消失することを防げます。

スーパーバイザ エンジンのスイッチオーバーが発生したあと、NSF 対応ルータは BGP ピアとのセッションを再構築します。新しいセッションの再構築中に、再起動したときに NSF 対応ルータを識別する新しいグレースフル リスタート メッセージを送信します。

この時点で、ルーティング情報は 2 つの BGP ピア間で交換されています。この交換が完了すると、NSF 対応装置はルーティング情報を使用して RIB と FIB を新しい転送情報で更新します。NSF 認識装置は、ネットワーク情報を使用して失効したルートを BGP テーブルから削除し、これで BGP プロトコルが完全に収束します。

BGP ピアがグレースフル リスタート機能をサポートしていない場合、OPEN メッセージ内のグレースフル リスタート機能は無視されますが、NSF 対応装置との BGP セッションは確立します。この機能により、NSF 非認識（つまり NSF 機能のない）BGP ピアとのインターオペラビリティが可能になりますが、NSF 非認識 BGP ピアとの BGP セッションではグレースフル リスタート機能は使用できません。

（注） NSF での BGP サポートでは、近接ネットワーキング装置が NSF を認識できなければなりません。つまり、装置はグレースフル リスタート機能に対応している必要があり、セッション確立中に OPEN メッセージでその機能をアドバタイズする必要があります。NSF 対応ルータが特定の BGP ネイバーにグレースフル リスタート機能がないことを検出すると、NSF 対応セッションをそのネイバーと確立しません。グレースフル リスタート機能のある他のすべてのネイバーは、この NSF 対応ネットワーキング装置と NSF 対応セッションを継続します。

OSPF の動作

OSPF NSF 対応ルータがスーパーバイザ エンジンのスイッチオーバーを実行した場合、リンク ステート データベースを OSPF ネイバーと再同期するために、次の作業を実行する必要があります。

- ネイバー関係をリセットせずにネットワーク上の使用可能な OSPF ネイバーを再学習します。
- ネットワークのリンク ステート データベースの内容を再取得します3。

スーパーバイザ エンジンのスイッチオーバー後できるだけ早く、NSF 対応ルータは OSPF NSF 信号を近接 NSF 認識装置に送信します。近接ネットワーキング装置は、この信号をこのルータとの近接関係がリセットされるべきでないことを示すインジケータとして認識します。NSF 対応ルータがネットワーク上の他のルータから信号を受信すると、近接リストを再構築できます。

近接関係が再確立されたあと、NSF 対応ルータはすべての NSF 認識ネイバーとのデータベースの再同期を開始します。この時点で、ルーティング情報は OSPF ネイバー間で交換されています。この交換が完了すると、NSF 対応装置は、ルーティング情報を使用して失効したルートを削除し、RIB を更新し、FIB を新しい転送情報で更新します。ここで OSPF プロトコルが完全に収束されます。

（注）　OSPF NSF では、すべての近接ネットワーキング装置が NSF を認識できなければなりません。NSF 対応ルータが特定のネットワーク セグメントで NSF 非認識ネイバーを検出すると、そのセグメントで NSF 機能をディセーブルにします。NSF 対応または NSF 認識ルータで完全に構成された他のネットワーク セグメントに対しては、継続して NSF 機能を提供します。

IS-IS の動作

IS-IS 対応ルータがスーパーバイザ エンジンのスイッチオーバーを実行した場合、リンク ステート データベースを IS-IS ネイバーと再同期するために、次の作業を実行する必要があります。

- ネイバー関係をリセットせずにネットワーク上の使用可能な IS-IS ネイバーを再学習します。
- ネットワークのリンク ステート データベースの内容を再取得します。

NSF を設定する場合、IS-IS NSF 機能には次の 2 つのオプションがあります。

- Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）IS-IS
- Cisco IS-IS

あるネットワーク セグメントの近接ルータがルータの再起動に関する IETF インターネット ドラフトをサポートするソフトウェア バージョンを実行している場合、再起動する IETF NSF ルータを支援します。IETF を使用すると、近接ルータはスイッチオーバー後のルーティング情報の再構築に役立つ隣接およびリンク ステート情報を提供します。IETF IS-IS 設定のメリットは、標準案に基づくピア装置間の動作にあります。

（注）　ネットワーキング装置で IETF を設定するものの近接ルータが IETF と互換性がない場合、スイッチオーバー後に NSF が打ち切られます。

あるネットワーク セグメントの近接ルータが NSF を認識しない場合、Cisco 設定オプションを使用する必要があります。Cisco IS-IS 設定は、プロトコル隣接およびリンク ステート情報をアクティブ スーパーバイザ エンジンから冗長スーパーバイザ エンジンに転送します。Cisco 設定のメリットは、NSF 認識ネイバーに依存していないことです。

IETF IS-IS 設定

スーパーバイザ エンジンのスイッチオーバー後できるだけ早く、NSF 対応ルータは IETF IS-IS 設定を使用して、IS-IS NSF 再起動要求を隣接 NSF 認識装置に送信します。近接ネットワーキング装置は、この再起動要求をこのルータとの近接関係がリセットされるべきでないが、再起動ルータとの間でデータベースの再同期を開始すべきであることを示すインジケータとして認識します。再起動ルータがネットワーク上のルータから再起動要求応答を受信すると、近接リストを再構築できます。

この交換が完了すると、NSF 対応装置はリンク ステート情報を使用して失効したルートを削除し、RIB を更新し、FIB を新しい転送情報で更新します。ここで IS-IS が完全に収束されます。

あるスーパーバイザ エンジンから別のスーパーバイザ エンジンへのスイッチオーバーは、数秒間以内に発生します。IS-IS は、それに数秒プラスしてルーティング テーブルを再確立し、ネットワークと再同期します。この時点で、IS-IS は 2 回めの NSF 再起動を試行する前に特定の期間待機します。この期間に、新しい冗長スーパーバイザ エンジンが起動してアクティブ スーパーバイザ エンジンとの設定を同期します。IS-IS NSF 動作では、IS-IS NSF がもう一度再起動を試行する前に接続が確実に安定するように特定の期間待機します。この機能により、IS-IS が失効した情報でバックツーバック NSF 再起動を試行しないようにします。

Cisco IS-IS 設定

Cisco 設定オプションを使用することで、冗長スーパーバイザ エンジンに対して、すべての隣接および Label Switched Path（LSP; ラベル スイッチド パス）情報が保存されるか、*チェックポイントに設定*されます。スイッチオーバーのあと、新しくアクティブになったスーパーバイザ エンジンはチェックポイント データを使用して隣接を維持し、ルーティング テーブルを迅速に再構築できます。

（注）　スイッチオーバーのあと、Cisco IS-IS NSF には完全なネイバー隣接および LSP 情報があります。ただし、スイッチオーバーの前に隣接であったすべてのインターフェイスがオンラインになるまで待機します。割り当てられたインターフェイス用の待機時間内にインターフェイスがオンラインにならない場合、近接装置から学習したルートを、ルーティング テーブルの再計算で考慮しないようにします。IS-IS NSF には、何らかの理由で時間内にオンラインにならないインターフェイスに対して、待機時間を延長するコマンドがあります。

あるスーパーバイザ エンジンから別のスーパーバイザ エンジンへのスイッチオーバーは、数秒間以内に発生します。IS-IS は、それに数秒プラスしてルーティング テーブルを再確立し、ネットワークと再同期します。この時点で、IS-IS は 2 回めの NSF 再起動を試行する前に特定の期間待機します。この期間に、新しい冗長スーパーバイザ エンジンが起動してアクティブ スーパーバイザ エンジンとの設定を同期します。この同期が完了したあと、IS-IS 隣接および LSP データに冗長スーパーバイザ エンジンへのチェックポイントが設定されます。ただし、新しい NSF 再起動は、この期間が経過しないと IS-IS で試行されません。この機能により、IS-IS がバックツーバック NSF 再起動を試行しないようにします。

EIGRP の動作

EIGRP NSF 対応ルータが最初に NSF 再起動から復帰したときには、ネイバーはなくトポロジ テーブルは空です。ルータはインターフェイスを立ち上げネイバーを再取得し、トポロジとルーティング テーブルを再構築する必要があるときに、冗長（現在アクティブな）スーパーバイザ エンジンから通知を受けます。ルータとピアの再起動では、再起動したルータへ向かうデータ トラフィックを中断せずにこれらの作業を実行する必要があります。EIGRP ピア ルータは、再起動するルータから学習したルートを維持し、NSF 再起動プロセスを通じてトラフィックを転送し続けます。

ネイバーによって隣接がリセットされないように、再起動ルータは EIGRP パケット ヘッダに再起動を示すための新しい再起動（RS）ビットを使用します。RS ビットは、NSF 再起動中に hello パケットと初期 INIT 更新パケットに設定されます。hello パケットの RS ビットにより、ネイバーに迅速に NSF 再起動を通知できます。RS ビットを検出しない場合、ネイバーは INIT 更新を受信するか hello 保持タイマーの期間が満了することによって、隣接リセットを検出するだけです。RS ビットがないと、ネイバーは NSF を使用して隣接リセットが処理されたか、通常のスタートアップを使用して処理されたかを認識しません。

hello パケットまたは INIT パケットを受信することでネイバーが再起動表示を受信すると、ピア リスト内のピアが再起動したことを認識し、再起動しているルータとの隣接を維持します。次にネイバーは、再起動しているルータに対して、最初の更新パケットに RS ビットを設定してトポロジ テーブルを送信します。この RS ビットは、NSF を認識可能でルータの再起動を支援していることを示します。ネイバーが NSF 再起動ネイバーでない場合は、hello パケットに RS ビットを設定しません。

（注）　ルータが NSF を認識できていても、コールド スタートから立ち上がっているために NSF 再起動ネイバーの支援に参加してない場合もあります。

少なくとも 1 つのピア ルータが NSF を認識している場合、再起動ルータは更新を受信しデータベースを再構築します。次に再起動ルータは、RIB を通知できるように収束されているかどうかを検出する必要があります。各 NSF 認識ルータは、テーブルの内容が終わりであることを示すために、最後の更新パケットに End of Table（EOT; テーブルの終わり）マーカを送信する必要があります。EOT マーカを受信すると、再起動ルータは収束していることがわかります。ここで再起動ルータが更新を送信し始めることができます。

NSF 認識ピアは、再起動ルータから EOT 表示を受信したときにいつ再起動ルータが収束したかを認識します。次にピアは、再起動ネイバーを送信元としてルートを検索するために、トポロジ テーブルをスキャンします。ピアは、ルートのタイムスタンプと再起動イベント タイムスタンプを比較して、ルートがまだ使用可能かどうかを判断します。次に、ピアはアクティブになり、再起動されたルータで使用できなくなったルートの代替パスを検索します。

再起動ルータがすべての EOT 表示をネイバーから受信した場合、または NSF 収束タイマーが満了した場合、EIGRP は RIB にコンバージェンスを通知します。EIGRP は RIB コンバージェンス信号を待機し、待機しているすべての NSF 認識ピアに対してトポロジ テーブルをフラッディングします。

NSF の利点と制約事項

Cisco NSF には次のような利点があります。

- ネットワークのアベイラビリティの向上

  NSF は、ユーザのセッション情報がスイッチオーバー後も維持されるように、ネットワーク トラフィックとアプリケーションのステート情報を転送し続けます。

- 全体的なネットワークの安定

  ネットワークの安定性は、ネットワーク内のルータが故障してルーティング テーブルを消失した時に生成されるルート フラップ数を減らすことで改善できます。

- 近接ルータがリンク フラップを検出しない

  スイッチオーバー全体にわたってインターフェイスはアップのままなので、近接ルータはリンク フラップを検出しません（リンクがダウンせずアップに戻ります）。

- ルーティング フラップの回避

  SSO がスイッチオーバー時にネットワーク トラフィックを転送し続けるので、ルーティング フラップが回避されます。

- ユーザ セッションが失われない

  スイッチオーバー前に確立したユーザ セッションは維持されます。

Cisco NSF with SSO には次のような制約事項があります。

- NSF の動作では、装置に SSO を設定しておく必要があります。
- NSF with SSO は、IP バージョン 4 トラフィックおよびプロトコルだけをサポートします。
- Hot Standby Routing Protocol（HSRP）は SSO を認識しないので、通常の動作中にアクティブ スーパーバイザ エンジンと冗長スーパーバイザ エンジン間でステート情報が維持されません。HSRP と SSO は共存できますが、いずれも別々に機能します。HSRP に依存しているトラフィックは、スーパーバイザ エンジンのスイッチオーバー時に HSRP スタンバイに切り替わる場合があります。
- Gateway Load Balancing Protocol（GLBP）は SSO を認識しないので、通常の動作中にアクティブ スーパーバイザ エンジンと冗長スーパーバイザ エンジン間でステート情報が維持されません。GLBP と SSO は共存できますが、いずれも別々に機能します。GLBP に依存しているトラフィックは、スーパーバイザ エンジンのスイッチオーバー時に GLBP スタンバイに切り替わる場合があります。

- Virtual Redundancy Routing Protocol（VRRP）は SSO を認識しないので、通常の動作中にアクティブ スーパーバイザ エンジンと冗長スーパーバイザ エンジン間でステート情報が維持されません。VRRP と SSO は共存できますが、いずれも別々に機能します。VRRP に依存しているトラフィックは、スーパーバイザ エンジンのスイッチオーバー時に VRRP スタンバイに切り替わる場合があります。
- Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）は、Cisco NSF with SSO ではサポートされていません。ただし、MPLS と NSF with SSO は共存できます。NSF with SSO が MPLS と同じシャーシに構成されている場合、MPLS プロトコルのフェールオーバー パフォーマンスは少なくとも RRP と同等ですが、サポートされている NSF with SSO プロトコルには NSF with SSO の利点が加わります。
- BGP NSF に参加しているすべての近接装置は、NSF 対応で、BGP のグレースフル リスタート用に設定されている必要があります。
- 仮想リンクの OSPF NSF はサポートされていません。
- 同じネットワーク セグメントにあるすべての OSPF ネットワーキング装置は、NSF を認識する必要があります（NSF ソフトウェア イメージを実行している必要があります）。
- IETF IS-IS の場合、すべての近接装置は NSF 認識ソフトウェア イメージを実行している必要があります。
- IPv4 マルチキャスト NSF with SSO がサポートされるのは、PFC3B だけです。
- 元となるユニキャスト プロトコルはマルチキャスト NSF with SSO を使用するために NSF を認識する必要があります。
- Bidirectional Forwarding Detection（BFD; 双方向フォワーディング検出）は SSO を認識せず、NSF with SSO でサポートされません。

スーパーバイザ エンジンの設定の同期化

ここでは、スーパーバイザ エンジンの設定の同期化について説明します。

（注）　SNMP を通じて行われた設定変更は、冗長スーパーバイザ エンジンと同期化されません。SNMP を通じてスイッチを設定したあと、running-config ファイルをアクティブ スーパーバイザ エンジンの startup-config ファイルにコピーして、冗長スーパーバイザ エンジンの startup-config ファイルの同期化を引き起こします。

スーパーバイザ エンジンの冗長構成に関する注意事項および制約事項

ここでは、スーパーバイザ エンジンの冗長構成に関する注意事項および制約事項について説明します。

冗長構成の注意事項および制約事項

次の注意事項と制約事項は、すべての冗長モードに適用されます。

- 冗長スーパーバイザ エンジンがスタンバイ モードの場合、冗長スーパーバイザ エンジンの 2 つのギガビット イーサネット インターフェイスは常にアクティブです。
- スーパーバイザ エンジンを冗長構成にしても、スーパーバイザ エンジンのミラーリングやロードバランスは行われません。スーパーバイザ エンジンのうちの 1 台だけがアクティブになります。
- SNMP を通じて行われた設定変更は、冗長スーパーバイザ エンジンと同期化されません。SNMP を通じてスイッチを設定したあと、running-config ファイルをアクティブ スーパーバイザ エンジンの startup-config ファイルにコピーして、冗長スーパーバイザ エンジンの startup-config ファイルの同期化を引き起こします。
- スーパーバイザ エンジンのスイッチオーバーは、障害のあるスーパーバイザ エンジンがコア ダンプを完了したあとに行われます。コア ダンプには最大で 15 分間かかります。スイッチオーバー時間を短縮するには、スーパーバイザ エンジンでコア ダンプをディセーブルにします。

ハードウェア設定時の注意事項および制約事項

冗長運用を行うには、次の注意事項および制約事項に従う必要があります。

- スーパーバイザ エンジンおよび PISA で実行する Cisco IOS は、スーパーバイザ エンジンおよび PISA ルータが同一である冗長構成をサポートします。スーパーバイザ エンジンおよび PISA ルータが異なる場合、片方が最初に起動されてアクティブになり、もう一方がリセット状態で保留されます。
- 各スーパーバイザ エンジンが単独でスイッチを稼動させるためのリソースを備えているスーパーバイザ エンジンのすべてのリソース（すべてのフラッシュ装置を含む）が重複している必要があります。
- スーパーバイザ エンジンごとに個別のコンソール接続を行ってください。コンソール ポートに Y 字ケーブルを接続しないでください。
- 両方のスーパーバイザ エンジン内のシステム イメージが同じである必要があります（「冗長スーパーバイザ エンジンへのファイルのコピー」（P.5-20）を参照）。

（注） 新たに取り付けられた冗長スーパーバイザ エンジン上で Catalyst オペレーティング システムがインストールされている場合は、アクティブなスーパーバイザ エンジンを取り外して、冗長スーパーバイザ エンジンだけが搭載されている状態でスイッチを起動します。最新のリリース ノートの手順に従って、Catalyst オペレーティング システムから冗長スーパーバイザ エンジンを変換してください。

- startup-config のコンフィギュレーション レジスタが自動起動用に設定されている必要があります。

（注） ネットワークからの起動はサポートされていません。

コンフィギュレーション モードに関する制約事項

スタートアップ同期プロセス中は、設定に関して次の制約事項が適用されます。

- スタートアップ（一括）同期中は、設定を変更できません。このプロセス中に設定を変更しようとすると、次のメッセージが生成されます。

  ```
  Config mode locked out till standby initializes
  ```

- スーパーバイザ エンジンのスイッチオーバー時に設定を変更した場合、その変更内容は失われます。

NSF 設定作業

次に、NFS 機能の設定作業について説明します。

SSO の設定

NSF をサポートしているプロトコルで NSF を使用するには SSO を設定する必要があります。SSO を設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# redundancy`	冗長コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-red)# mode sso`	SSO を設定します。このコマンドを入力すると、冗長スーパーバイザ エンジンがリロードされ、SSO モードでの処理が開始されます。
ステップ 3	`Router# show running-config`	SSO がイネーブルになっていることを確認します。
ステップ 4	`Router# show redundancy states`	動作中の冗長モードを表示します。

次に、システムを SSO 用に設定して、冗長ステートを表示する例を示します。

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# redundancy
Router(config-red)# mode sso
Router(config-red)# end
Router# show redundancy states
my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
           Unit = Primary
        Unit ID = 5

Redundancy Mode (Operational) = sso
Redundancy Mode (Configured)  = sso
     Split Mode = Disabled
   Manual Swact = Enabled
 Communications = Up

   client count = 29
 client_notification_TMR = 30000 milliseconds
          keep_alive TMR = 9000 milliseconds
        keep_alive count = 1
    keep_alive threshold = 18
           RF debug mask = 0x0
Router#
```

マルチキャスト MLS NSF with SSO の設定

（注） このセクションのコマンドはオプションで、設定をカスタマイズするのに使用できます。ほとんどのユーザは、デフォルト設定で十分です。

マルチキャスト MLS NSF with SSO は、SSO が冗長モードとして選択されている場合にデフォルトでオンです。マルチキャスト NSF with SSO パラメータを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# mls ip multicast sso convergence-time` *time*	プロトコルのコンバージェンス用に待機する最大時間を指定します。有効な範囲は、0 ～ 3600 秒です。

	コマンド	目的
ステップ 3	`Router(config)# mls ip multicast sso leak` *interval*	パケット リーク インターバルを指定します。有効な範囲は、0 ～ 3600 秒です。PIM sparse（疎）モードおよび PIM dense（密）モードの場合、これは既存の PIM sparse モードおよび PIM dense モード マルチキャスト転送エントリのパケット リーキングが完了したあとの期間です。
ステップ 4	`Router(config)# mls ip multicast sso leak` *percentage*	マルチキャスト フローの割合を指定します。有効な範囲は、1 ～ 100 % です。この値は、パケット リーキングに対してフラグ付けされている既存の PIM sparse（疎）モードおよび PIM dense（密）モード マルチキャスト フローの合計数の割合を示します。

マルチキャスト NSF with SSO の確認

マルチキャスト NSF with SSO 設定を確認するには、**show mls ip multicast sso** コマンドを入力します。

```
router# show mls ip multicast sso
Multicast SSO is enabled
Multicast HA Parameters
-------------------------------------------------+------+
protocol convergence timeout                      120 secs
flow leak percent                                 10
flow leak interval                                60 secs
```

CEF NSF の設定

ネットワーキング装置が SSO モードで動作している間、CEF NSF 機能はデフォルトで動作します。設定作業は不要です。

CEF NSF の確認

CEF が NSF に対応していることを確認するには、**show cef state** コマンドを入力します。

```
router# show cef state

CEF Status [RP]
CEF enabled/running
dCEF enabled/running
CEF switching enabled/running
CEF default capabilities:
Always FIB switching:      yes
Default CEF switching:     yes
Default dCEF switching:    yes
Update HWIDB counters:     no
Drop multicast packets:    no
.
.
.
CEF NSF capable:           yes
IPC delayed func on SSO:   no
RRP state:
I am standby RRP:          no
My logical slot:           0
RF PeerComm:               no
```

BGP NSF の設定

（注） BGP NSF に参加しているすべてのピア装置に BGP のグレースフル リスタートを設定する必要があります。

NSF の BGP を設定するには、次の作業を行います（各 BGP NSF ピア装置でこの手順を繰り返します）。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# router bgp as-number`	BGP ルーティング プロセスをイネーブルにして、ルータをルータ コンフィギュレーション モードにします。
ステップ 3	`Router(config-router)# bgp graceful-restart`	BGP のグレースフル リスタート機能をイネーブルにして、BGP の NSF を開始します。 BGP セッションが確立されたあとにこのコマンドを入力した場合、BGP ネイバーとグレースフル リスタート機能を交換するためにセッションを再起動する必要があります。 再起動ルータとすべてのピアでこのコマンドを使用します。

BGP NSF の確認

BGP の NSF を確認するには、グレースフル リスタート機能が SSO 対応ネットワーキング装置とその近接装置に設定されているかを確認する必要があります。これを確認するには、次の作業を行います。

ステップ 1　**show running-config** コマンドを入力して、[bgp graceful-restart] が SSO 対応ルータの BGP 設定に表示されることを確認します。

```
Router# show running-config

.
.
.
router bgp 120
.
.
.
bgp graceful-restart
 neighbor 10.2.2.2 remote-as 300
.
.
.
```

ステップ 2　各 BGP ネイバーでステップ 1 を繰り返します。

ステップ 3　SSO 装置と近接装置で、グレースフル リスタート機能がアドバタイズされ受信されたものとして表示されているかを確認し、グレースフル リスタート機能のあるアドレス ファミリーを確認します。アドレス ファミリーがリストされていない場合、BGP NSF も発生しません。

```
router#show ip bgp neighbors x.x.x.x

BGP neighbor is 192.168.2.2,  remote AS YY, external link
  BGP version 4, remote router ID 192.168.2.2
  BGP state = Established, up for 00:01:18
  Last read 00:00:17, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh:advertised and received(new)
    Address family IPv4 Unicast:advertised and received
    Address famiiy IPv4 Multicast:advertised and received
    Graceful Restart Capabilty:advertised and received
      Remote Restart timer is 120 seconds
      Address families preserved by peer:
        IPv4 Unicast, IPv4 Multicast
  Received 1539 messages, 0 notifications, 0 in queue
  Sent 1544 messages, 0 notifications, 0 in queue
  Default minimum time between advertisement runs is 30 seconds
```

OSPF NSF の設定

（注）　OSPF NSF に参加しているすべてのピア装置は OSPF NSF 対応でなければならず、NSF ソフトウェア イメージを装置にインストールすれば自動的に対応するようになります。

OSPF NSF を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# router ospf processID`	OSPF ルーティング プロセスをイネーブルにして、ルータをルータ コンフィギュレーション モードにします。
ステップ 3	`Router(config-router)# nsf`	OSPF の NSF 動作をイネーブルにします。

OSPF NSF の確認

OSPF の NSF を確認するには、NSF 機能が SSO 対応ネットワーキング装置に設定されているかを確認する必要があります。OSPF NSF を確認するには、次の作業を行います。

ステップ 1　**show running-config** コマンドを入力して、[nsf] が SSO 対応装置の OSPF 設定に表示されることを確認します。

```
Router# show running-config

router ospf 120
log-adjacency-changes
nsf
network 192.168.20.0 0.0.0.255 area 0
network 192.168.30.0 0.0.0.255 area 1
network 192.168.40.0 0.0.0.255 area 2
.
.
.
```

ステップ 2　**show ip ospf** コマンドを入力して NSF が装置でイネーブルであることを確認します。

```
router> show ip ospf

Routing Process "ospf 1" with ID 192.168.2.1 and Domain ID 0.0.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
Non-Stop Forwarding enabled, last NSF restart 00:02:06 ago (took 44 secs)
Area BACKBONE(0)
Number of interfaces in this area is 1 (0 loopback)
 Area has no authentication
 SPF algorithm executed 3 times
```

IS-IS NSF の設定

IS-IS NSF を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# router isis` [*tag*]	IS-IS ルーティング プロセスをイネーブルにして、ルータをルータ コンフィギュレーション モードにします。
ステップ 3	`Router(config-router)# nsf` [**cisco** | **ietf**]	IS-IS の NSF 動作をイネーブルにします。 **ietf** キーワードを入力して、ネットワーキング装置の隣接装置が IETF ドラフト ベースの再起動性をサポートしていることを保証している同種ネットワークで IS-IS をイネーブルにします。 **cisco** キーワードを入力して、NSF 認識ネットワーキング装置との隣接装置がない異種ネットワークで IS-IS を実行します。
ステップ 4	`Router(config-router)# nsf interval` [*minutes*]	（任意）NSF 再起動試行間の最小時間を指定します。*連続する* NSF 再起動のデフォルトの時間間隔は、5 分です。
ステップ 5	`Router(config-router)# nsf t3` {**manual** [*seconds*] | **adjacency**}	（任意）IS-IS 自身のリンク ステート情報の生成が過負荷になり、その情報がネイバーにフラッディングする前に、IS-IS が IS-IS データベースの同期を待機する時間を指定します。 IETF 動作を選択した場合だけ、**t3** キーワードが適用されます。**adjacency** を指定した場合、再起動しているルータは近接装置から待機時間を取得します。
ステップ 6	`Router(config-router)# nsf interface wait` *seconds*	（任意）再起動が完了する前に、IS-IS 隣接とのインターフェイスがすべて立ち上がるまで、IS-IS NSF の再起動を待機する長さを指定します。デフォルト値は 10 秒です。

IS-IS NSF の確認

IS-IS の NSF を確認するには、NSF 機能が SSO 対応ネットワーキング装置に設定されているかを確認する必要があります。IS-IS NSF を確認するには、次の作業を行います。

ステップ 1　**show running-config** コマンドを入力して、[nsf] が SSO 対応装置の IS-IS 設定に表示されることを確認します。Cisco IS-IS または IETF IS-IS 設定のいずれかが表示されます。次の表示は、装置で IS-IS NSF のシスコ実装を使用していることを示しています。

```
Router# show running-config
<...Output Truncated...>
router isis
nsf cisco
<...Output Truncated...>
```

ステップ 2　NSF 設定が **cisco** に設定されている場合、**show isis nsf** コマンドを使用して NSF が装置でイネーブルであることを確認します。シスコ設定を使用すると、表示出力はアクティブ RP と冗長 RP で異なります。次の表示は、アクティブ RP 上の Cisco 設定の出力例です。この例で、[NSF restart enabled] が表示されることを確認してください。

```
router# show isis nsf

NSF is ENABLED, mode 'cisco'

RP is ACTIVE, standby ready, bulk sync complete
NSF interval timer expired (NSF restart enabled)
Checkpointing enabled, no errors
Local state:ACTIVE,  Peer state:STANDBY HOT,  Mode:SSO
```

次の表示は、スタンバイ RP 上のシスコ設定の出力例です。この例で、[NSF restart enabled] が表示されることを確認してください。

```
router# show isis nsf

NSF enabled, mode 'cisco'
RP is STANDBY, chkpt msg receive count:ADJ 2, LSP 7
NSF interval timer notification received (NSF restart enabled)
Checkpointing enabled, no errors
Local state:STANDBY HOT,  Peer state:ACTIVE,  Mode:SSO
```

ステップ 3　NSF 設定が **ietf** に設定されている場合、**show isis nsf** コマンドを使用して NSF が装置でイネーブルであることを確認します。次の表示は、ネットワーキング装置上の IETF IS-IS 設定の出力例です。

```
router# show isis nsf

NSF is ENABLED, mode IETF
NSF pdb state:Inactive
NSF L1 active interfaces:0
NSF L1 active LSPs:0
NSF interfaces awaiting L1 CSNP:0
Awaiting L1 LSPs:
NSF L2 active interfaces:0
NSF L2 active LSPs:0
NSF interfaces awaiting L2 CSNP:0
Awaiting L2 LSPs:
Interface:Serial3/0/2
    NSF L1 Restart state:Running
    NSF p2p Restart retransmissions:0
    Maximum L1 NSF Restart retransmissions:3
    L1 NSF ACK requested:FALSE
    L1 NSF CSNP requested:FALSE
    NSF L2 Restart state:Running
    NSF p2p Restart retransmissions:0
    Maximum L2 NSF Restart retransmissions:3
    L2 NSF ACK requested:FALSE
Interface:GigabitEthernet2/0/0
    NSF L1 Restart state:Running
    NSF L1 Restart retransmissions:0
    Maximum L1 NSF Restart retransmissions:3
    L1 NSF ACK requested:FALSE
    L1 NSF CSNP requested:FALSE
    NSF L2 Restart state:Running
    NSF L2 Restart retransmissions:0
    Maximum L2 NSF Restart retransmissions:3
    L2 NSF ACK requested:FALSE
    L2 NSF CSNP requested:FALSE
Interface:Loopback1
    NSF L1 Restart state:Running
    NSF L1 Restart retransmissions:0
```

```
Maximum L1 NSF Restart retransmissions:3
L1 NSF ACK requested:FALSE
L1 NSF CSNP requested:FALSE
NSF L2 Restart state:Running
NSF L2 Restart retransmissions:0
Maximum L2 NSF Restart retransmissions:3
L2 NSF ACK requested:FALSE
L2 NSF CSNP requested:FALSE
```

EIGRP NSF の設定

EIGRP NSF を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# router eigrp` *as-number*	EIGRP ルーティング プロセスをイネーブルにして、ルータをルータ コンフィギュレーション モードにします。
ステップ 3	`Router(config-router)# nsf`	EIGRP NSF をイネーブルにします。 再起動ルータとすべてのピアでこのコマンドを使用します。

EIGRP NSF の確認

EIGRP の NSF を確認するには、NSF 機能が SSO 対応ネットワーキング装置に設定されているかを確認する必要があります。EIGRP NSF を確認するには、次の作業を行います。

ステップ 1　**show running-config** コマンドを入力して、[nsf] が SSO 対応装置の EIGRP 設定に表示されることを確認します。

```
Router# show running-config
.
.
.
router eigrp 100
 auto-summary
 nsf
.
.
.
```

ステップ 2　**show ip protocols** コマンドを入力して NSF が装置でイネーブルであることを確認します。

```
Router# show ip protocols
*** IP Routing is NSF aware ***
Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 100
  EIGRP NSF-aware route hold timer is 240s
  EIGRP NSF enabled
     NSF signal timer is 20s
     NSF converge timer is 120s
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: internal 90 external 170
```

スーパーバイザ エンジンの設定の同期化

通常の動作時には、2 つのスーパーバイザ エンジン間で startup-config および config-register 設定がデフォルトで同期化されます。スイッチオーバー時には、新しいアクティブ スーパーバイザ エンジンが現在の設定を使用します。

冗長スーパーバイザ エンジンへのファイルのコピー

次のコマンドを使用して、冗長スーパーバイザ エンジン上の **disk0:** 装置にファイルをコピーします。

```
Router# copy source_device:source_filename slavedisk0:target_filename
```

次のコマンドを使用して、冗長スーパバイザ エンジン上の **bootdisk:** 装置にファイルをコピーします。

```
Router# copy source_device:source_filename slavesup-bootdisk:target_filename
```

次のコマンドを使用して、冗長 PISA 上の **bootdisk:** 装置にファイルをコピーします。

```
Router# copy source_device:source_filename slavebootdisk:target_filename
```