CHAPTER 6

NSF with SSO スーパバイザ エンジンの冗長設定

この章では、Cisco Nonstop Forwarding（NSF）with Stateful Switchover（SSO）を使用して、スーパバイザ エンジン冗長性を設定する方法について説明します。この章の構成は次のとおりです。

（注）

- Release 12.2(18)SXD 以降のリリースでは、Supervisor Engine 720 および Supervisor Engine 2 の NSF with SSO をサポートします。
- Release 12.2(17b)SXA、Release 12.2(17b)SXA の再構築、Release 12.2(17d)SXB、Release 12.2(17d)SXB の再構築では、Supervisor Engine 720 の Single Router Mode（SRM）with SSO がサポートされます（第 7 章「SRM with SSO スーパバイザ エンジンの冗長設定」を参照）。
- Release 12.2(18)SXD 以降のリリースは、SRM with SSO をサポートしません。
- すべてのリリースでは、Route Processor Redundancy（RPR）および Route Processor Redundancy Plus（RPR+）がサポートされます（第 8 章「RPR および RPR+ スーパバイザ エンジンの冗長設定」を参照）。
- 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、『*Cisco 7600 Series Router Cisco IOS Command Reference*』を参照してください。

NSF with SSO スーパバイザ エンジンの冗長構成

ここでは、NSF with SSO を使用したスーパバイザ エンジンの冗長構成を説明します。

NSF with SSO スーパバイザ エンジンの冗長構成の概要

（注）　冗長スーパバイザ エンジンがスタンバイ モードにある場合、冗長スーパバイザ 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必ずアクティブになります。

Cisco 7600 シリーズ ルータは、プライマリ スーパバイザ エンジンが故障した場合に冗長スーパバイザ エンジンが処理を引き継ぐようにすることによって、耐障害性を強化できます。Cisco NSF は SSO と連動して、スイッチオーバーのあとのネットワークを利用できない時間を最小限にし、IP パケットを転送し続けます。Cisco 7600 シリーズ ルータは冗長構成のため、RPR、RPR+、SRM with SSO をサポートします。冗長モードの詳細については、第 8 章「RPR および RPR+ スーパバイザ エンジンの冗長設定」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 スーパバイザ エンジンでのハードウェア障害
- スーパバイザ 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、スーパバイザ エンジンの 1 つがスタンバイとして指定されている場合に、残りのスーパバイザ エンジンをアクティブとして確立します。それから 2 つのスーパバイザ エンジンの間の情報を同期化します。アクティブ スーパバイザ エンジンに障害が発生すると、アクティブ スーパバイザ エンジンから冗長スーパバイザ エンジンへのスイッチオーバーが発生します。またはアクティブ スーパバイザ エンジンがルータから削除、あるいはメンテナンスのため手動でシャットダウンされます。このスイッチオーバーにより、レイヤ 2 トラフィックは中断されません。

SSO を実行するネットワーキング デバイスでは、冗長スーパバイザ エンジンがアクティブ スーパバイザ エンジンに障害が発生したあとのコントロールを常に行えるように、両方のスーパバイザ エンジンは同じ設定で稼働している必要があります。また、SSO スイッチオーバーは Forwarding Information Base（FIB; 転送情報ベース）と隣接エントリを保護し、スイッチオーバーのあとにレイヤ 3 トラフィックを転送できます。設定情報およびデータ構造は、起動時およびアクティブ スーパバイザ エンジン コンフィギュレーションが変更されたときに、アクティブ スーパバイザ エンジンから冗長スーパバイザ エンジンに同期化されます。2 つのスーパバイザ エンジンの間で初期同期化が行われたあと、SSO は両者の間のステート情報（転送情報を含む）を維持します。

スイッチオーバー中、システム コントロールおよびルーティング プロトコルの実行はアクティブ スーパバイザ エンジンから冗長スーパバイザ エンジンに転送されます。ルータがアクティブ スーパバイザ エンジンから冗長スーパバイザ エンジンにスイッチオーバーするのに必要な時間は、プラットフォームによって数秒から 30 秒です。

NSF の動作

Cisco NSF は常に SSO と連動し、レイヤ 3 トラフィックに冗長性を提供します。NSF は SSO と連動して、スイッチオーバーのあとのネットワークを利用できない時間を最小限にします。NSF の主な目的は、スーパバイザ エンジンのスイッチオーバー後、IP パケットを転送し続けることです。

Cisco NSF は、ルーティング用に Border Gateway Protocol（BGP）、Open Shortest Path First（OSPF）、Intermediate System-to-Intermediate System（IS-IS）プロトコルによって、転送用に Cisco Express Forwarding（CEF）によってサポートされます。ルーティング プロトコルでは NSF 機能および認識機能が拡張されました。これは、プロトコルを稼働するルータがスイッチオーバーを検出でき、ネットワーク トラフィックを転送し続け、ピア デバイスからのルート情報を回復するのに必要なアクションを実行できることを意味します。アクティブ スーパバイザ エンジンと冗長スーパバイザ エンジンの間で同期化されたステート情報を使用してピア デバイスから受信した情報ではなく、スイッチオーバー後のルート情報を回復するように、IS-IS プロトコルを設定できます。

ネットワーキング デバイスが NSF 互換ソフトウェアを動作している場合、このデバイスは NSF 認識です。デバイスが NSF をサポートするように設定されている場合、デバイスは NSF 対応で、NSF 認識または NSF 対応ネイバからルーティング情報を再構築します。

各プロトコルは、ルーティング プロトコルが Routing Information Base（RIB）テーブルを再構築する間に、スイッチオーバー中にパケットを転送し続ける CEF に依存します。ルーティング プロトコルがコンバージェンスされたあと、CEF は FIB テーブルを更新し、失効したルート エントリを削除します。それから CEF はライン カードに新しい FIB 情報を更新します。

CEF

NSF の重要な要素は転送用パケットです。Cisco ネットワーキング デバイスでは、パケット転送は CEF によって実行されます。CEF は FIB を維持し、スイッチオーバー時の FIB 情報を使用してスイッチオーバー中にパケットを転送し続けます。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軽減します。

通常の NSF 動作中、アクティブ スーパバイザ エンジンの CEF は現在の FIB および隣接データベースを、冗長スーパバイザ エンジンの FIB および隣接データベースと同期化します。アクティブ スーパバイザ エンジンのスイッチオーバーが発生すると、冗長スーパバイザ エンジンはまず、アクティブ スーパバイザ エンジンに存在するミラーリング イメージである FIB および隣接データベースを持ちます。プラットフォームにインテリジェント ライン カードが装填されている場合、ライン カードはスイッチ上に現在の転送情報を維持します。プラットフォームに転送エンジンが装填されている場合、CEF は冗長スーパバイザ エンジンの転送エンジンに、アクティブ スーパバイザ エンジンの CEF によって送信される変更を維持します。ライン カードまたは転送エンジンは、インターフェイスおよびデータ パスが利用できるようになると、スイッチオーバー後も転送し続けることができます。

ルーティング プロトコルが prefix-by-prefix ベースに RIB を追加すると、アップデートにより CEF に対する prefix-by-prefix アップデートが発生します。これは、FIB および隣接データベースをアップデートするのに使用します。既存または新規エントリは新しいバージョン（[epoch]）番号を受信すると、リフレッシュされたことを示します。転送情報はライン カードまたはコンバージェンス中の転送エンジンで更新されます。RIB がコンバージェンスされると、スーパバイザ エンジンは信号

を出します。ソフトウェアは、現在のスイッチオーバー エポックより前のエポックを持った FIB および隣接エントリをすべて削除します。現在、FIB は最新のルーティング プロトコル転送情報を表示します。

MMLS NSF with SSO

ルータによって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中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）NSF with SSO が必要です。MMLS NSF with SSO を使用しない場合、マルチキャスト プロトコルがコンバージェンスするまで、レイヤ 3 マルチキャスト トラフィックが廃棄されます。

スイッチオーバー プロセス中、古いデータベース（前のアクティブ スーパバイザ エンジンから）を使用してトラフィックが転送されます。マルチキャスト ルーティング プロトコルのコンバージェンスが発生したあと、新規のアクティブな Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）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組み合わされ、新しいショートカットとして表示されます。失効したエントリは徐々にデータベースから削除され、NSF はスイッチオーバー中も機能し、新しいキャッシュへスムーズに移行できます。

Protocol Independent Multicast（PIM）sparse（疎）モードおよび PIM dense（密）モードなどのマルチキャスト ルーティング プロトコルはデータ駆動型なので、プロトコルがコンバージェンスできるように、マルチキャスト パケットは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用にソフトウェアによって転送される必要がないので、ルータ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をリークし続けます。ルータは mroute キャッシュを構築し、ハードウェアにショートカットを導入します。新しいルートが学習されると、データベースを通過し、古いフローを削除するタイマーが起動します。

（注）　MMLS NSF with SSO は、ユニキャスト プロトコルでの NSF サポートを必要とします。

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 スーパバイザ エンジンの MSFC でのみ稼働し、近接ルータからルーティング アップデートを受信します。ルーティング プロトコルは冗長スーパバイザ エンジンの MSFC では稼働しません。スイッチオーバーのあとルーティング プロトコルは、NSF 認識近接デバイスがルーティング テーブルを再構築するステート情報を送信するよう要求します。代わりに、IS-IS プロトコルは、近接デバイスが NSF 認識ではない環境の NSF 対応デバイス上でルーティング テーブルを再構築するため、ステート情報をアクティブ スーパバイザ エンジンから冗長スーパバイザ エンジンに同期化するよう設定できます。Cisco NSF は、BGP、OSPF、IS-IS、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 プロトコルは、ルーティング情報を再構築している間にパケットを転送し続ける CEF に依存します。

BGP の動作

NSF 対応ルータは BGP ピアで BGP セッションを開始し、OPEN メッセージをピアへ送信します。メッセージに含まれるものは、NSF 対応デバイスに [graceful] restart 機能があるステートメントです。グレースフル リスタートは、BGP ルーティング ピアがルーティング フラップがスイッチオーバーのあとに発生するのを防ぐメカニズムです。BGP ピアがこの機能を受信した場合、デバイスが送信するメッセージは NSF 対応であることを認識しています。NSF 対応ルータ ピアおよび BGP ピア両方ともセッションの開始時に、OPEN メッセージ内でグレースフル 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、セッションはグレースフル リスタート対応になりません。

BGP セッションがスーパバイザ エンジン スイッチオーバー中に中断された場合、NSF 認識 BGP ピアが NSF 対応ルータに関連するルートすべてを失効としてマーキングしますが、一定期間の転送先を決定するためにこれらのルートを使用し続けます。この機能は、新しいアクティブ スーパバイザ エンジンが BGP ピアでルーティング情報のコンバージェンスを待っている間に、パケットが失われないようにします。

スーパバイザ エンジン スイッチオーバーが発生したあと、NSF 対応ルータが BGP ピアでセッションを再確立します。新しいセッションの確立時に、再開したときに 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 ピアの間で交換されます。交換が完了すると、NSF 対応デバイスはルーティング情報を使用して新しい転送情報を持った RIB および FIB に更新します。NSF 認識デバイスはネットワーク情報を使用して、失効ルートを BGP テーブルから削除します。それから BGP プロトコルが完全にコンバージェンスされます。

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 対応デバイスに BGP セッションを確立します。この機能により、非 NSF 認識 BGP ピアとのインターオペラビリティ（および NSF 機能なしでのインターオペラビリティ）を可能にしますが、非 NSF 認識 BGP ピアでの BGP セッションはグレースフル リスタート対応になりません。

（注）　NSF の BGP サポートでは、近接ネットワーキング デバイスが NSF 認識である必要があります。つまり、デバイスにはグレースフル リスタート機能があり、セッション確立中に OPEN メッセージ内でこ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 ネイバにグレースフル リスタート機能がないことを検出した場合、そのネイバとの NSF 対応セッションを確立しません。グレースフル リスタート機能のある他のネイバはすべて、NSF 対応ネットワーキング デバイスとの NSF 対応セッションを維持し続けます。

OSPF の動作

OSPF NSF 対応ルータがスーパバイザ エンジン スイッチオーバーを実行する場合、ルータはリンク ステート データベースと OSPF ネイバを再同期化するため、次の作業を行う必要があります。

- 近接関係をリセットしないで、ネットワーク上で利用できる OSPF ネイバを再学習します。
- ネットワークのリンク ステート データベース内容を再取得します。

スーパバイザ エンジン スイッチオーバーのすぐあと、NSF 対応ルータは OSPF NSF 信号を近接 NSF 認識デバイスに送信します。近接ネットワーキング デバイスは、このルータとの近接関係がリセットしてはならないインジケータとしてこの信号を認識します。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、ネイバ リストの再構築を始めます。

近接関係が再構築されると、NSF 対応ルータはデータベースとすべての NSF 認識ネイバの再同期化を始めます。この時点でルーティング情報は OSPF ネイバの間で交換されます。交換が完了すると、NSF 対応デバイスはルーティング情報を使用して、失効ルートを削除し、新しい転送情報を持った RIB および FIB に更新します。それから、OSPF プロトコルは完全にコンバージェンスされます。

（注）　OSPF NSF では、すべての近接ネットワーク デバイスが NSF 認識である必要があります。NSF 対応ルータが特定のネットワーク セグメント上に NSF 認識ネイバがないことを検出した場合、ルータはそのセグメントの NSF 機能をディセーブルにします。NSF 対応または NSF 認識ルータを構成する他のネットワーク セグメントでは、NSF 機能を提供し続けます。

IS-IS の動作

IS-IS NSF 対応ルータがスーパバイザ エンジン スイッチオーバーを実行する場合、ルータはリンク ステート データベースと IS-IS ネイバを再同期化するため、次の作業を行う必要があります。

- 近接関係をリセットしないで、ネットワーク上で利用できる IS-IS ネイバを再学習します。
- ネットワークのリンク ステート データベース内容を再取得します。

NSF を設定する場合、IS-IS NSF 機能は次のオプションを提供します。

- Internet Engineering Task Force（IETF）IS-IS
- Cisco IS-IS

ネットワーク セグメントの近接ルータが、ルータの再起動用に 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 バージョンを稼働している場合、ルータは再起動する IETF NSF ルータを支援します。IETF を使用する場合、近接ルータはスイッチオーバー後のルーティング情報を再構築する隣接情報およびリンク ステート情報を提供します。IETF IS-IS コンフィギュレーションの利点は、提案された標準に基づいたピア デバイスの間の動作であることです。

（注）　ネットワーキング デバイスに IETF を設定する場合で近接ルータが IETF と互換性がないとき、NSF はスイッチオーバー後に中断します。

ネットワーク セグメント上の近接ルータが NSF 認識でない場合、シスコのコンフィギュレーション オプションを使用する必要があります。Cisco IS-IS コンフィギュレーションは、プロトコル隣接情報とリンクステート情報両方をアクティブ スーパバイザ エンジンから冗長スーパバイザ エンジンに送信します。シスコのコンフィギュレーションの利点は、NSF 認識ネイバに依存しないことです。

IETF IS-IS コンフィギュレーション

スーパバイザ エンジン スイッチオーバーの直後、NSF 対応ルータは IETF IS-IS コンフィギュレーションを使用して、IS-IS NSF 再起動要求を近接 NSF 認識デバイスに送信します。近接ネットワーキング デバイスは、このルータとの近接関係をリセットしてはならないインジケータとしてこの再起動要求を認識します。ただし、デバイスはデータベースと再起動するルータとの再同期化を開始します。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を受信すると、ネイバ リストの再構築を始めます。

交換が完了すると、NSF 対応デバイスはリンクステート情報を使用して失効ルートを削除し、新しい転送情報を持った RIB および FIB に更新します。それから IS-IS が完全にコンバージェンスされます。

一方のスーパバイザ エンジンからもう一方のスーパバイザ エンジンへのスイッチオーバーは数秒以内に発生します。IS-IS はルーティング テーブルを再構築し、数秒以内にネットワークと同期化します。この時点で IS-IS は次の NSF 再起動を実行する前に、指定された間隔の間、待機します。この間、新しい冗長スーパバイザ エンジンが起動し、この設定をアクティブ スーパバイザ エンジンと同期化します。IS-IS NSF を再起動しようとする前に接続を安定させるため、IS-IS NSF 動作は指定された間隔の間、待機します。この機能は、IS-IS が失効情報で back-to-back NSF を再起動しないようにします。

Cisco IS-IS コンフィギュレーション

シスコのコンフィギュレーション オプションを使用すると、完全な隣接情報および LSP 情報が保存、または冗長スーパバイザ エンジンまで*チェックポイント*されます。スイッチオーバー後、新しいアクティブ スーパバイザ エンジンがチェックポイントされたデータを使用して、隣接関係を維持し、ルーティング テーブルをただちに再構築できます。

（注）　スイッチオーバー後、Cisco IS-IS NSF には完全なネイバ隣接情報および LSP 情報がありますが、スイッチオーバーの前に、隣接したインターフェイスがすべてオンラインになるまで待機する必要があります。割り当てられたインターフェイス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、近接デバイスから学習されたルートはルーティング テーブルの再計算で考慮されません。IS-IS NSF ではインターフェイスの待機時間を延長するコマンドを提供しますが、どんな理由であれタイミング良くオンラインになることができません。

一方のスーパバイザ エンジンからもう一方のスーパバイザ エンジンへのスイッチオーバーは数秒以内に発生します。IS-IS はルーティング テーブルを再構築し、数秒以内にネットワークと同期化します。この時点で IS-IS は次の NSF 再起動を実行する前に、指定された間隔の間、待機します。この間、新しい冗長スーパバイザ エンジンが起動し、この設定をアクティブ スーパバイザ エンジンと同期化します。同期化が終了すると、IS-IS 隣接および LSP データは冗長スーパバイザ エンジンまでチェックポイントされますが、インターバル時間が満了するまで IS-IS は新しい NSF を再起動しようとしません。この機能は、IS-IS が連続して NSF を再起動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 再起動からバックアップになる場合、ネイバがなく、そのトポロジー テーブルは空です。ルータがインターフェイスを停止し、ネイバを取得、トポロジーおよびルーティング テーブルを再構築する必要がある場合、ルータは冗長スーパバイザ エンジン（現在はアクティブ）によって通知されます。再起動ルータおよびピアは、再起動ルータへのデータ トラフィック転送を中断することなく、次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 再起動プロセスを介してトラフィックを転送し続けます。

ネイバによる隣接のリセットを防ぐには、再起動ルータは EIGRP パケット ヘッダーの新しい Restart（RS）ビットを使用して、再起動を表示します。RS ビットは NSF 再起動中、Hello パケットおよび初期 INIT アップデート パケットに設定されます。Hello パケットの RS ビットを使用すると、ネイバにすばやく NSF 再起動を通知できます。RS ビットを参照しない場合、ネイバは INIT アップデートの受信、または Hello ホールド タイマーの期限切れによってリセットされた隣接関係を検出します。RS ビットを使用しない場合、ネイバは、リセットされた隣接関係を NSF または通常の起動方法を使用して処理する必要があるかどうか認識できません。

ネイバが Hello パケットまたは INIT パケットのいずれかを受信することにより再起動表示を受信すると、ネイバはピア リストの再起動ピアを認識し、再起動ルータとの隣接関係を維持します。ネイバはトポロジー テーブルを、最初のアップデート パケットに設定された RS ビットのある再起動ルータに送信します。このパケットは NSF 認識であり、再起動ルータに役立つことを示しています。ネイバは NSF 再起動ネイバでない場合、Hello パケットに RS ビットを設定しません。

（注）　ルータは NSF 認識ですが、コールド スタートから起動するので NSF 再起動ネイバに参加しません。

最低ピア ルータの 1 つが NSF 認識の場合、再起動ルータはアップデートを受信してからデータベースを再構築します。再起動ルータは Routing Information Base（RIB）に通知できるようにコンバージェンスしたかどうかを認識する必要があります。各 NSF 認識ルータは、End of Table（EOT）内容を表示するために、最新アップデート パケットの EOT マーカーを送信する必要があります。再起動ルータは EOT マーカーを受信すると、コンバージェンスしたことを認識します。再起動ルータは送信アップデートを開始できます。

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再起動ルータがコンバージェンスした時間を認識します。それからピアはトポロジー テーブルをスキャンして、送信元として再起動されたネイバを持ったルートを検索します。ピアはルート 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、ルートがまだ利用できるかどうかを判断します。ピアはアクティブになり、再起動したルータを介して利用できなくなったルート用に代替パスを検索します。

再起動ルータがネイバから EOT 表示すべてを受信したとき、または NSF コンバージェンス タイマーが終了したとき、EIGRP が 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ってから、トポロジー テーブルを NSF 認識待ちピアすべてにフラッディングします。

NSF の利点および制約事項

Cisco NSF には次の利点があります。

- 向上したネットワーク アベイラビリティ

  スイッチオーバー後にユーザ セッション情報を維持するよう、NSF はネットワーク トラフィックおよびアプリケーション ステート情報の転送を続けます。
- ネットワーク全体の安定性

  ネットワークの安定性は、ネットワークのルータに障害が発生し、ルーティング テーブルを失った場合に作成されたルート フラップ数を削除することで向上します。
- 近接するルータはリンク フラップを検出しません。

  インターフェイスはスイッチオーバーの間アップ状態のままなので、近接するルータはリンク フラップを検出しません（リンクは停止せず、バックアップになります）。
- ルーティング フラップの回避

  SSO はスイッチオーバー時にネットワーク トラフィックの転送を続けるので、ルーティング フラップは回避されます。
- ユーザ セッションの損失なし

  スイッチオーバーの前に確立されたユーザ セッションは維持されます。

Cisco NSF with SSO には次の制約事項があります。

- NSF 動作の場合、SSO をデバイス上に設定する必要があります。
- NSF with SSO は IP Version 4 トラフィックとプロトコルのみをサポートします。

- Hot Standby Routing Protocol（HSRP）は SSO 認識ではなく、通常の動作中にステート情報がアクティブ スーパバイザ エンジンと冗長スーパバイザ エンジンの間で維持されないことを示します。HSRP および SSO は共存できますが、それぞれの機能は独立して動作します。HSRP に依存するトラフィックは、スーパバイザ スイッチオーバー時に HSRP スタンバイにスイッチングします。
- Gateway Load Balancing Protocol（GLBP）は SSO 認識ではなく、通常の動作中にステート情報がアクティブ スーパバイザ エンジンと冗長スーパバイザ エンジンの間で維持されないことを示します。GLBP および SSO は共存できますが、それぞれの機能は独立して動作します。GLBP に依存するトラフィックは、スーパバイザ スイッチオーバー時に GLBP スタンバイにスイッチングします。
- Virtual Redundancy Routing Protocols（VRRP）は SSO 認識ではなく、通常の動作中にステート情報がアクティブ スーパバイザ エンジンと冗長スーパバイザ エンジンの間で維持されないことを示します。VRRP および SSO は共存できますが、それぞれの機能は独立して動作します。VRRP に依存するトラフィックは、スーパバイザ スイッチオーバー時に VRRP スタンバイにスイッチングします。
- 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 ではサポートされません。ただし MPLS と NSF with SSO は共存することができます。NSF with SSO が MPLS と同じシャーシに設定された場合、MPLS プロトコルのフェイルオーバパフォーマンスは少なくとも RPR+ と同等になりますが、サポートされる NSF with SSO プロトコルは NSF with SSO に追加された利点をまだ維持しています。
- BGP NSF に参加している近接デバイスはすべて NSF 対応、BGP 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。
- 仮想リンク用 OSPF NSF はサポートされません。
- 同じネットワーク セグメント上のすべての OSPF ネットワーキング デバイスは、NSF 認識（NSF ソフトウェア イメージを稼働）である必要があります。
- IETF IS-IS の場合、近接するデバイスはすべて NSF 認識ソフトウェア イメージを稼働する必要があります。
- マルチキャスト NSF with SSO は Supervisor Engine 720 によってのみ、サポートされます。
- 基礎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 NSF 認識である必要があります。

スーパバイザ エンジンの設定の同期化

ここでは、スーパバイザ 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、冗長スーパバイザ エンジンと同期化されません。SNMP を介してルータを設定すると、running-config ファイルをアクティブ スーパバイザ エンジンの startup-config ファイルにコピーして、冗長スーパバイザ エンジンの startup-config ファイルの同期化を開始します。

スーパバイザ 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。

冗長構成設定時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。

- 冗長スーパバイザ エンジン上の 2 つのギガビット イーサネット インターフェイスは、スーパバイザ エンジンがオンライン上でスタンバイ ステートである限り、常にアクティブです。
- スーパバイザ エンジンを冗長構成にしても、スーパバイザ 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、冗長スーパバイザ エンジンと同期化されません。SNMP を介してルータを設定すると、running-config ファイルをアクティブ スーパバイザ エンジンの startup-config ファイルにコピーして、冗長スーパバイザ エンジンの startup-config ファイルの同期化を開始します。
- スーパバイザ 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。

- スーパバイザ エンジンおよび MSFC で実行する Cisco IOS は、スーパバイザ エンジンおよび MSFC ルータが同一である冗長構成をサポートします。スーパバイザ エンジンおよび MSFC ルータが同一でない場合、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。
- 各スーパバイザ　エンジンが単独でルータを稼働させるためのリソースを備えているスーパバイザ 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（「冗長スーパバイザ エンジンへのファイルのコピー」[p.6-22] を参照）。

（注）　新たに取り付けられた冗長スーパバイザ 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バイザ エンジンを取り外して、冗長スーパバイザ エンジンのみが搭載されている状態でルータを起動します。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 レジスタは自動起動用に設定されていなければなりません。

（注）　ネットワークからの起動はサポートされていません。

Release 12.2(17b)SXA 以降のリリースでこれらの要件が満たされている場合、ルータはデフォルトで SRM with SSO モードで動作します。

Release 12.2(17b)SXA 以降のリリースでこれらの要件が満たされると、ルータで RPR+ モードがデフォルトで機能します。

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 の設定作業

ここでは NSF 機能の設定作業について説明します。

SSO の設定

あらゆるサポート対象プロトコルを持った 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、次の作業を行います。

	コマンド	説明
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。このコマンドが入力されると、冗長スーパバイザ エンジンがリロードされ、SSO モードで動作を開始します。
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。

（注）　**sso** キーワードは、Release 12.2(17b)SXA 以降のリリースでサポートされています。

次に、SSO 対応としてシステムを設定し、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#
```

MMLS NSF with SSO の設定

マルチキャスト NSF with SSO パラメータを設定するには、イネーブル EXEC モードで次のコマンドを使用します（SSO がモードに選択されている場合、MMLS NSF with SSO はデフォルトではオンです）。

（注）　ここで示すコマンドは任意で、設定をカスタマイズするのに使用できます。大半のユーザにとってデフォルト設定が適切です。

	コマンド	説明
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 コンバージェンスの最大待機時間を指定します。有効値は 0 ～ 3600 秒です。
ステップ 3	`Router(config)# mls ip multicast sso leak` *interval*	パケットのリーク間隔を指定します。有効値は 0 ～ 3600 秒です。PIM sparse モードおよび PIM dense モードの場合、既存の PIM sparse モードおよび PIM dense モードのマルチキャスト転送エントリ用のパケット リークが終了したあとの時間を意味します。
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。有効値は 0 ～ 100% です。この値は、パケット リーク用にフラグ付けされる既存の PIM sparse モードおよび PIM dense モード マルチキャスト フローの総数の割合を表示します。

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** コマンドを使用します。

```
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 デバイスが SSO モードで稼働している間、CEF NSF 機能はデフォルトで動作します。したがって設定作業は不要です。

CEF NSF の確認

CEF が NSF 対応であることを確認するには、**show cef state** コマンドを使用します。

```
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 に参加しているピア デバイスすべてに BGP グレースフル リスタートを設定する必要があります。

NSF 用 BGP を設定するには、イネーブル EXEC モードで次のコマンドを使用し、各 BGP NSF ピア デバイスでこの手順を繰り返します。

	コマンド	説明
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、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 グレースフル リスタート機能をイネーブルにし、BGP 用 NSF を開始します。 BGP セッションが確立されたあとでこのコマンドを入力した場合、BGP ネイバと交換する機能のセッションを再開する必要があります。 再起動ルータおよびピアすべてで、このコマンドを使用します。

BGP NSF の確認

BGP 用 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 デバイスおよび近接デバイス上で設定されているか確認する必要があります。確認する手順は、次のとおりです。

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 コンフィギュレーションに表示されているか確認します。

```
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 ネイバでステップ 1 を繰り返します。

ステップ 3　SSO デバイスおよび近接デバイスでは、グレースフル リスタート機能がアドバタイズおよび受信されたことを示していることを確認し、グレースフル リスタート機能を備えたアドレス ファミリーであることを確認します。アドレス ファミリーが表示されていない場合、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 に参加するピア デバイスすべては OSPF NSF 認識である必要があります。これは、デバイス上の NSF ソフトウェア イメージをインストールすると自動的に設定されます。

OSPF 用 NSF を設定するには、イネーブル EXEC モードで次のコマンドを使用します。

	コマンド	説明
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、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 用に NSF 動作をイネーブルにします。

OSPF NSF の確認

OSPF 用 NSF を確認するには、NSF 機能が SSO 対応ネットワーキング デバイス上で設定されているか確認する必要があります。OSPF NSF を確認する手順は、次のとおりです。

ステップ 1　**show running-config** コマンドを入力して、[nsf] が SSO 対応デバイスの OSPF コンフィギュレーションに表示されているか確認します。

```
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　NSF がデバイス上でイネーブルであるか確認するには、**show ip ospf** コマンドを使用します。

```
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 用 NSF を設定するには、イネーブル EXEC モードで次のコマンドを使用します。

	コマンド	説明
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、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 用 NSF をイネーブルにします。 IETF ドラフトベースの再起動をサポートするネットワーキング デバイスを備えた隣接関係が保証される均質なネットワークで IS-IS をイネーブルにするには、**ietf** キーワードを入力します。 NSF認識ネットワーキング デバイスを備えた隣接関係がない均質なネットワークで IS-IS を稼働するには、**cisco** キーワードを入力します。
ステップ 4	`Router(config-router)# nsf interval` [*minutes*]	(任意) NSF 再起動試行までの最小時間を指定します。*連続した* NSF 再起動試行までのデフォルト値は、5 分です。

	コマンド	説明
ステップ 5	`Router(config-router)# nsf t3 {manual [seconds] | adjacency}`	（任意）IS-IS データベースが同期化してから過負荷になったリンクステート情報を生成し、情報をネイバにフラッディングするまで IS-IS が待機する時間を指定します。 **IETF** 動作を選択した場合のみ、**t3** キーワードが適用されます。**adjacency** を指定すると、再起動ルータが近接するデバイスからの待機時間を取得します。
ステップ 6	`Router(config-router)# nsf interface wait seconds`	（任意）IS-IS NSF 再起動は再起動を完了する前に、起動するすべての IS-IS 隣接インターフェイスを待機します。デフォルトは 10 秒です。

IS-IS NSF の確認

IS-IS 用 NSF を確認するには、NSF 機能が SSO 対応ネットワーキング デバイス上で設定されているか確認する必要があります。IS-IS NSF を確認する手順は、次のとおりです。

ステップ 1　**show running-config** コマンドを入力して、[nsf] が SSO 対応デバイスの IS-IS コンフィギュレーションに表示されているか確認します。Cisco IS-IS または IETF IS-IS コンフィギュレーションのいずれかを表示します。次の例は、デバイスがシスコ採用の IS-IS NSF を使用していることを示します。

```
Router# show running-config
.
.
.
router isis
nsf cisco
.
.
.
```

ステップ 2　NSF コンフィギュレーションが **cisco** に設定されている場合、NSF がデバイス上でイネーブルかを確認するには **show isis nsf** コマンドを使用します。シスコのコンフィギュレーションを使用すると、コマンドの出力はアクティブ RP および冗長 RP で異なります。次の表示では、アクティブ RP 上のシスコ コンフィギュレーションの出力例を示します。この例では、[NSF restart enabled] の存在に注意してください。

```
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
```

次に、スタンバイ RP 上のシスコ コンフィギュレーションの出力例を示します。この例では、[NSF restart enabled] の存在に注意してください。

```
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 コンフィギュレーションが **ietf** に設定されている場合、NSF がデバイス上でイネーブルかを確認するには **show isis nsf** コマンドを入力します。次の表示では、ネットワーキング デバイス上の IETF IS-IS コンフィギュレーションの出力例を示します。

```
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 用 NSF を設定するには、イネーブル EXEC モードで次のコマンドを使用します。

	コマンド	説明
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、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 用 NSF をイネーブルにします。 再起動ルータおよびピアすべてで、このコマンドを使用します。

EIGRP NSF の確認

EIGRP 用 NSF を確認するには、NSF 機能が SSO 対応ネットワーキング デバイス上で設定されているか確認する必要があります。EIGRP NSF を確認する手順は、次のとおりです。

ステップ 1　**show running-config** コマンドを入力して、[nsf] が SSO 対応デバイスの EIGRP コンフィギュレーションに表示されているか確認します。

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

ステップ 2　NSF がデバイス上でイネーブルであるか確認するには、**show ip protocols** コマンドを使用します。

```
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 スーパバイザ エンジンが現在の設定を使用します。

2 つのスーパバイザ エンジンが使用する設定を手動で同期化するには、アクティブ スーパバイザ エンジン上で次の作業を行います。

	コマンド	説明
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)# main-cpu`	main-cpu コンフィギュレーション サブモードを開始します。

	コマンド	説明
ステップ 3	`Router(config-r-mc)# auto-sync {startup-config | config-register | bootvar | standard}`	設定要素を同期化します。
ステップ 4	`Router(config-r-mc)# end`	イネーブル EXEC モードに戻ります。
ステップ 5	`Router# copy running-config startup-config`	NVRAM（不揮発性 RAM）上のコンフィギュレーション ファイルを強制的に手動で同期化します。 （注）　DRAM の実行コンフィギュレーション ファイルを同期化する場合、この手順は不要です。

（注）　**auto-sync standard** コマンドを実行しても、ブート変数は同期化されません。

次に、**auto-sync standard** コマンドを使用して、デフォルトの自動同期化機能を再びイネーブルにし、アクティブ スーパバイザ エンジンの startup-config および config-register 設定を冗長スーパバイザ エンジンと同期化させる例を示します。

```
Router(config)# redundancy
Router(config-red)# main-cpu
Router(config-r-mc)# auto-sync standard
Router(config-r-mc)# auto-sync bootvar
Router(config-r-mc)# end
Router# copy running-config startup-config
```

（注）　標準の auto-sync 設定要素を個別に手動で同期化するには、デフォルトの自動同期化機能をディセーブルにします。

次に、デフォルトの自動同期化をディセーブルにして、アクティブ スーパバイザ エンジンから冗長スーパバイザ エンジンへの config-register の自動同期化のみを許可し、スタートアップ コンフィギュレーションの同期化を許可しない例を示します。

```
Router(config)# redundancy
Router(config-red)# main-cpu
Router(config-r-mc)# no auto-sync standard
Router(config-r-mc)# auto-sync config-register
Router(config-r-mc)# end
Router# copy running-config startup-config
```

冗長スーパバイザ 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 MSFC 上の **bootflash:** 装置にファイルをコピーします。

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

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

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