ステートフル スイッチオーバー（SSO）

（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、次の資料を参照してください。
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。
- SSO および NSF は IPv6 マルチキャスト トラフィックをサポートしません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

SSO の前提条件

なし。

SSO の制約事項

一般的な制約事項

- 2 つの RP をシャーシに設置し、それぞれが同じバージョンの Cisco IOS ソフトウェアを実行している必要があります。
- 両方の RP は、同じ Cisco IOS イメージを実行する必要があります。2 つの RP が、異なる Cisco IOS イメージを実行している場合、SSO が設定されていても、システムは RPR モードに戻ります。
- SNMP 経由で行った設定変更が、スイッチオーバーの実行後、自動的にスタンバイ RP に設定されないことがあります。
- デュアル プロセッサ間のロード シェアリングはサポートされていません。
- ホット スタンバイ ルーティング プロトコル（HSRP）は、Cisco NSF/SSO でサポートされていません。HSRP を Cisco NSF/SSO で使用しないでください。
- 拡張オブジェクト トラッキング（EOT）は、SSO 認識ではないので、SSO モードで HSRP 仮想ルータ冗長プロトコル（VRRP）、ゲートウェイ ロード バランシング プロトコル（GLBP）とともには使用できません。
- マルチキャストは SSO を認識しないため、スイッチオーバー後に再起動されません。したがって、マルチキャスト テーブルおよびデータ構造は、スイッチオーバー時にクリアされます。

コンフィギュレーション モードに関する制約事項

- 両方の RP のコンフィギュレーション レジスタを同一に設定する必要があります。これにより、いずれか一方の RP がリブートされても、ネットワーキング デバイスの動作が同一に維持されます。
- 起動時の（一括）同期の際、設定の変更はできません。設定を変更する場合は、次のような内容のメッセージが表示するまで待ってください。

```
%HA-5-MODE:Operating mode is sso, configured mode is sso.
```

スイッチオーバー プロセスに関する制約事項

- ファブリックのコンフィギュレーションに対する変更と RP スイッチオーバーが同時に発生した場合、シャーシおよびすべてのラインカードがリセットされます。
- スイッチが SSO モードに設定されていて、スタンバイの準備が完了する前にアクティブ RP に障害が発生した場合、スイッチはフル システム リセットによって回復します。
- アクティブ RP とスタンバイ RP の間での SSO の同期中は、設定されたモードは RPR になります。同期が完了すると、動作モードが SSO になります。同期が完了する前にスイッチオーバーが発生すると、スイッチオーバーが RPR モードになります。
- 一括同期処理が完了する前にスイッチオーバーが発生した場合、新しくアクティブになった RP が不整合な状態になることがあります。この場合、スイッチが再度読み込まれます。

- SSO モードでスイッチオーバーが実行されても、ラインカードはリセットされません。
- RP 自体のインターフェイスはステートフルではなく、スイッチオーバーごとにリセットされます。特に、RP 上の GE インターフェイスは、スイッチ オーバーごとにリセットされ、SSO をサポートしません。
- スイッチオーバーの時点でオンラインでないすべてのラインカードは、リセットされ、スイッチオーバー時にリロードされます。

SSO について

SSO の概要

Catalyst 6500 シリーズ スイッチでは、プライマリのスーパーバイザ エンジンに障害が発生した場合、冗長スーパーバイザ エンジンに切り替えることができることで、障害に対する耐久性が提供されています。シスコ SSO（一般に NSF と使用）は、スイッチオーバー後、IP パケットの転送を継続する一方で、ユーザのネットワーク使用不能時間を最小限に抑えます。Catalyst 6500 シリーズ スイッチは、冗長性のため、Route Processor Redundancy（RPR）をサポートします。詳細については、第 9 章「Route Processor Redundancy（RPR）」を参照してください。

SSO は特にネットワーク エッジで役立ちます。従来から、コア ルータはルータの冗長化とメッシュ接続を使用して、障害ネットワーク要素を迂回したトラフィック伝送を可能にすることにより、ネットワーク障害からシステムを保護します。SSO は、ネットワーク設計内のシングル ポイント障害であり、障害時には顧客に対するサービス提供が中断する可能性があるネットワーク エッジ デバイスを、デュアル ルート プロセッサ（RP）によって保護します。

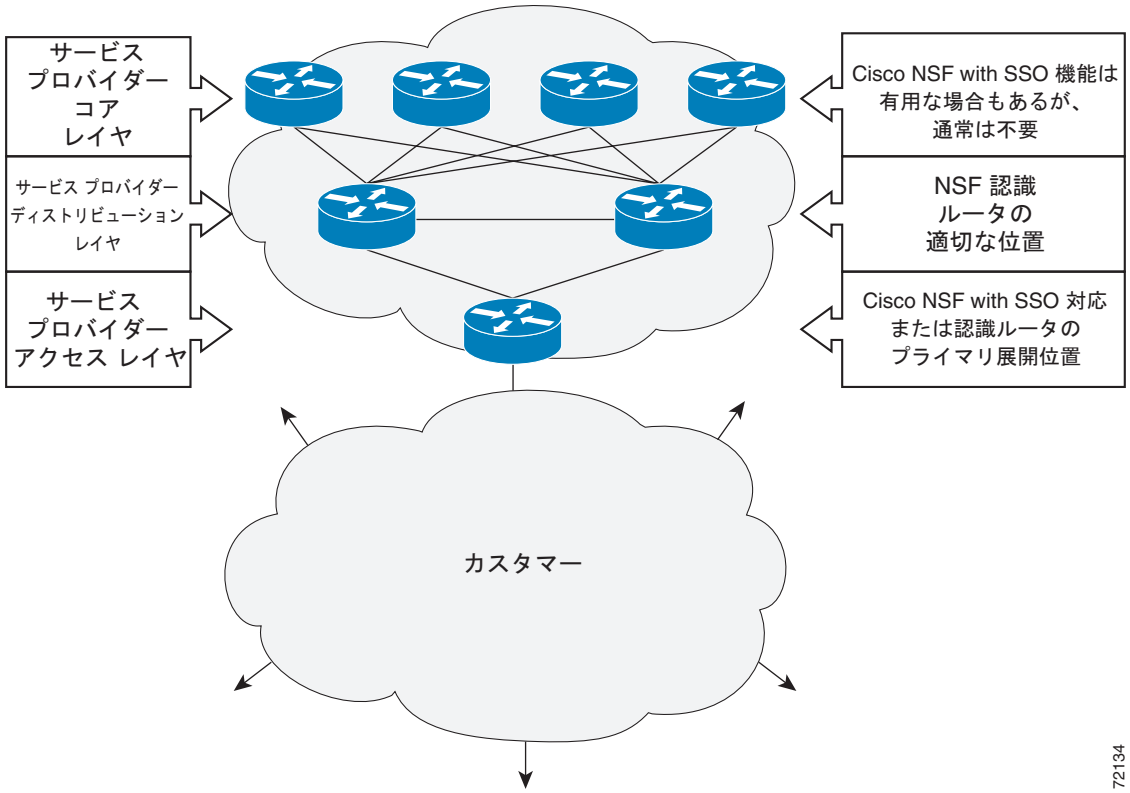
SSO には次のような多くの利点があります。SSO 機能は、ステートフル機能情報を保守するため、ユーザ セッション情報は、スイッチオーバー中に保守され、ラインカードは、引き続き、セッションを損失することなくネットワーク トラフィックを転送します。これにより、ネットワーク アベイラビリティが改善されます。また SSO では、RPR よりもスイッチオーバーが高速で実行されます。これは 1 つにはスタンバイ RP を完全に初期化して完全に設定するからであり、もう 1 つには、ステート情報を同期することによってルーティング プロトコルのコンバージェンスに要する時間を短縮できるからです。ネットワークの安定性は、ネットワーク内でルータに障害が発生し、ルーティング テーブルが失われたときに作成されるルート フラップの数を減らすことで改善できます。

Cisco Nonstop Forwarding（NSF）機能には SSO が必要です（第 8 章「Nonstop Forwarding（NSF）」を参照）。

図 7-1 は、サービス プロバイダー ネットワークに SSO が展開される一般的な方法を示します。この例では、CiscoNSF/SSO が主にサービス プロバイダー ネットワークのアクセス レイヤ（エッジ）に配置されています。このポイントで障害が発生すると、サービス プロバイダー ネットワークへのアクセスが必要なエンタープライズ カスタマーのサービスを損なう可能性があります。

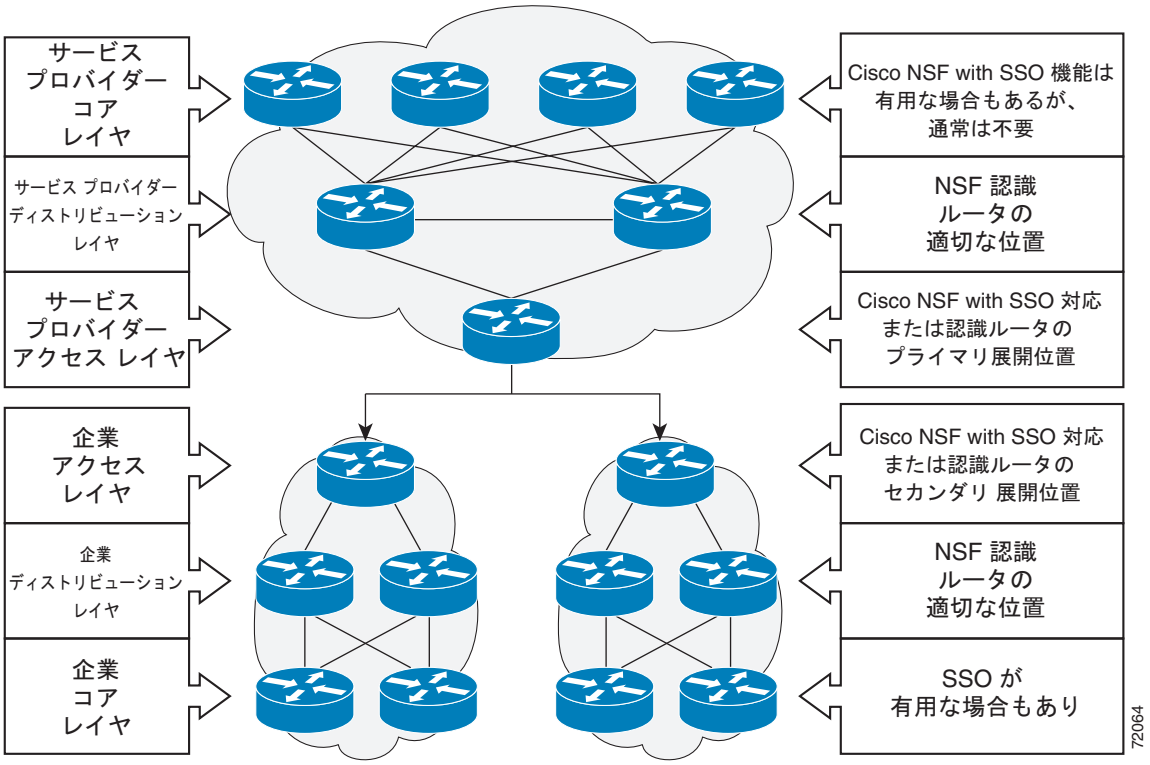
Cisco NSF プロトコルは、ネイバー デバイスが Cisco NSF に参加している必要があるので、それらのネイバー ディストリビューション レイヤ デバイスに Cisco NSF 対応のソフトウェア イメージをインストールする必要があります。その他に、ネットワークのコア レイヤに Cisco NSF と SSO 機能を適用することで、ネットワーク アベイラビリティの利点が得られる可能性もありますが、ネットワーク設計エンジニアと相談して、具体的なサイトの要件を評価してください。

図 7-1　Cisco NSF/SSO ネットワーク構成：サービス プロバイダー ネットワーク



アベイラビリティの向上は、シングル ポイント障害が存在するネットワーク内の他のポイントに Cisco NSF/SSO を展開することによって得られます。図 7-2 は、エンタープライズ ネットワーク アクセス レイヤに Cisco NSF/SSO を適用するもう 1 つの展開方法を示します。この例では、エンタープライズ ネットワーク内の各アクセス ポイントが、ネットワーク設計内の他のシングル ポイント障害を表します。スイッチオーバーまたは計画されたソフトウェア アップグレードが行われても、企業顧客のセッションは中断することなくネットワーク内で稼働し続けます。

図 7-2　Cisco NSF/SSO ネットワーク構成：エンタープライズ ネットワーク



SSO の動作

SSO は RP の 1 つをアクティブ プロセッサ、もう一方の RP をスタンバイ プロセッサとして設定します。SSO は完全にスタンバイ RP を初期化し、アクティブ RP とスタンバイ RP 間で重要なステート情報を同期します。

SSO スイッチオーバー時に、ラインカードではリセットされません。これにより、プロセッサ間のスイッチオーバーが高速化されます。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またはシャットダウン

SSO 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 スイッチオーバーは FIB と隣接エントリを保護し、スイッチオーバーの後にレイヤ 3 トラフィックを転送できます。SSO スイッチオーバー時間は 0 ～ 3 秒です。

ルート プロセッサの同期

同期化の概要

SSO が動作するネットワーキング デバイスでは、アクティブ RP に障害が発生したときに、スタンバイ RP がいつでも制御を引き継げるように、両方の RP で同じコンフィギュレーションを実行する必要があります。起動時およびアクティブ RP のコンフィギュレーションに変更が生じるたびに、SSO はアクティブ RP からスタンバイ RP にコンフィギュレーション情報を同期します。この同期は、次の 2 段階で行われます。

- スタンバイ RP の起動時に、アクティブ RP からスタンバイ RP にコンフィギュレーション情報が同期されます。
- コンフィギュレーションまたはステートに変更が生じたときに、アクティブ RP からスタンバイ RP へのインクリメンタル同期が実行されます。

初期化時の一括同期

SSO を備えたシステムの初期化時に、アクティブ RP はシャーシ探索（システムにあるラインカードの数とタイプ、およびファブリック カードが装着されている場合は、その数とタイプ）を実行し、スタートアップ コンフィギュレーション ファイルを解析します。

アクティブ RP は次に、このデータをスタンバイ RP に同期し、スタンバイ RP に対して初期化を完了するように指示します。この方法により、両方の RP に同じコンフィギュレーション情報が設定されます。

スタンバイ RP は、完全に初期化されていても、アクティブ RP とのみやり取りし、コンフィギュレーション ファイルに変更が生じたときにその増分を受け取ります。スタンバイ RP に対する CLI の実行はサポートされていません。

スタートアップ コンフィギュレーションの同期

システムの起動時に、スタートアップ コンフィギュレーション ファイルがアクティブ RP からスタンバイ RP にコピーされます。スタンバイ RP にある既存のスタートアップ コンフィギュレーション ファイルは上書きされます。

スタートアップ コンフィギュレーションは、RP の NVRAM に保存されたテキスト ファイルです。このファイルは、次の操作を実行するたびに同期されます。

- CLI コマンド **copy system:running-config nvram:startup-config** を使用したとき
- CLI コマンド **copy running-config startup-config** を使用したとき
- CLI コマンド **write memory** を使用したとき
- CLI コマンド **copy** *filename* **nvram:startup-config** を使用したとき
- CISCO_CONFIG_COPY MIB で、MIB 変数 ccCopyEntry の SNMP SET を使用したとき
- **reload** コマンドを使用してシステム コンフィギュレーションを保存したとき
- 強制スイッチオーバー CLI コマンドの入力後に、ステム コンフィギュレーションを保存したとき

インクリメンタル同期

インクリメンタル同期の概要

両方の RP が完全に初期化された後、実行コンフィギュレーションまたはアクティブ RP ステートに対して行われた変更は、発生したときにスタンバイ RP に同期されます。アクティブ RP ステートは、機能情報処理、外部イベント（インターフェイスがアップ状態またはダウン状態になるなど）、またはユーザ コンフィギュレーション コマンド（CLI コマンドや簡易ネットワーク管理プロトコル（SNMP）を使用）やその他の内部イベントの結果として更新されます。

CLI コマンド

CLI による実行コンフィギュレーションの変更は、アクティブ RP からスタンバイ RP に同期されます。実際には、CLI コマンドがアクティブとスタンバイの両方の RP に対して実行されます。

SNMP SET コマンド

SNMP set 操作によるコンフィギュレーション変更は、ケースバイケースで同期されます。現在、次の 2 つの SNMP コンフィギュレーション設定操作のみがサポートされています。

- （インターフェイスの）**shut** および **no-shut**
- **link** *up/down* **trap** *enable/disable*

情報のルーティングおよび転送

情報のルーティングおよび転送は、RP に同期されます。

- SSO 認識機能（SNMP など）のステート変更は、スタンバイ RP へ同期されます。
- シスコ エクスプレス フォワーディングによる転送情報ベース（FIB）の更新は、スタンバイ RP に同期されます。

シャーシのステート

ラインカードの抜き挿しによるシャーシ ステートの変更は、スタンバイ RP に同期されます。

ラインカードのステート

ラインカードのステートの変更は、スタンバイ RP に同期されます。ラインカードのステート情報は、最初、スタンバイ RP の一括同期によって取得されます。一括同期の後、アクティブ プロセッサで受信されたラインカード イベント（インターフェイスのアップ / ダウン状態など）は、スタンバイ RP に同期されます。

カウンタおよび統計情報

アクティブ RP で維持されているさまざまなカウンタおよび統計情報は、頻繁に変更されるうえ、必要とされる同期の程度が大きいため同期されません。統計情報に関連付けられている情報量が非常に大きいため、同期は実際的ではありません。

（注）　RP 間でカウンタと統計情報が同期されないために、この情報をモニタする外部ネットワーク管理システムで問題が生じることがあります。

SSO の動作

SSO 条件

自動または手動スイッチオーバーは、次の条件で実行される可能性があります。

- アクティブ RP のクラッシュまたはリブートを引き起こす原因となる障害状態：自動スイッチオーバー
- アクティブ RP の機能停止が宣言された場合（応答なし）：自動スイッチオーバー
- CLI が呼び出された場合：手動スイッチオーバー

ユーザは CLI コマンドを使用して、アクティブ RP からスタンバイ RP へのスイッチオーバーを強制できます。この手動の手順により、アクティブな RP の「通常の」制御されたシャットダウンが行われ、スタンバイ RP に切り替えられます。この通常シャットダウンにより、不可欠なクリーンアップが行われます。

（注）　この手順を、コア ルータのルーティング プロトコルについてのグレースフル シャットダウン手順と混同しないでください。これらは別個のメカニズムです。

注意　SSO 機能では、手動でスイッチオーバーを実行するコマンドなど、いくつかの新しいコマンドが導入されるとともに、既存のコマンドが変更されています。**reload** コマンドでは、スイッチオーバーは発生しません。**reload** コマンドを実行すると、ボックスが完全にリロードされ、すべてのテーブル エントリが削除され、すべてのラインカードがリセットされて、ノンストップ フォワーディングが中断されます。

スイッチオーバー時間

アクティブ RP からスタンバイ RP に切り替えるためにデバイスに必要な時間は、0 ～ 3 秒です。

新しくアクティブになったプロセッサは、スイッチオーバーの直後に処理を引き継ぎますが、デバイスが完全冗長（SSO）モードで動作を再開するまでには、プラットフォームによっては、数分かかることもあります。スイッチオーバー時間の長さは、複数の要因に左右されます。たとえば、前にアクティブだったプロセッサがクラッシュ情報を取得する時間、コードおよびマイクロコードをロードする時間、およびプロセッサ間のコンフィギュレーションの同期に必要な時間などが要因として挙げられます。

DFC 搭載のスイッチング モジュールでは、転送情報が配信され、同じラインカードから転送されるパケットは、転送遅延がほとんどありません。ただし、ラインカード間でパケットを転送すると、スイッチオーバー時間の間、パケット転送が待機する必要がある可能性があるため、RP との対話が必要です。

アクティブ RP の活性挿抜

アクティブ RP の活性挿抜は、スタンバイ RP へのステートフル スイッチオーバーを自動的に強制します。

高速ソフトウェア アップグレード

Fast Software Upgrade（FSU）を使用して、予定されているダウンタイムを短縮することができます。FSU を使用すると、アップグレードされた Cisco IOS ソフトウェア イメージがあらかじめロードされたスタンバイ RP にシステムをスイッチオーバーできます。FSU は、アップグレードされた Cisco IOS ソフトウェアがあらかじめインストールされているスタンバイ RP に機能を転送することにより、ソフトウェア アップグレード時のダウンタイムを短縮します。また、古いバージョンの Cisco OS にシステムをダウングレードしたり、アップグレードの直後に、前のイメージにダウングレードするためにバックアップ システムをロードしたりするためにも FSU を使用できます。

FSU を実行する前に、ネットワーキング デバイスで SSO を設定する必要があります。

（注） アップグレード プロセスでは、さまざまなイメージが、短時間だけ RP にロードされます。この間、デバイスは RPR モードで動作します。

コア ダンプ処理

SSO をサポートするネットワーキング デバイスでは、スイッチオーバーが行われた後、新しくアクティブになったプライマリ プロセッサが、コア ダンプ処理を実行します。ダンプ処理を待つ必要がないので、プロセッサ間のスイッチオーバー時間が効果的に短縮されます。

スイッチオーバーの後、新しいアクティブ RP は、コア ダンプが完了するまで一定時間待った後、以前のアクティブ RP のリロードを試みます。この待ち時間は設定可能です。たとえば、プラットフォームによっては、以前のアクティブ RP がコア ダンプを実行するのに 1 時間またはそれ以上必要なことがありますが、サイト ポリシーによっては、それほど長い時間待機せずに、以前のアクティブ RP のリセットとリロードを行うことがあります。指定された時間内にコア ダンプが完了しない場合、コア ダンプがまだ実行中であるかどうかとは無関係に、スタンバイがリセットされてリロードされます。

コア ダンプ プロセスは、ファイルの内容を生成したプロセッサを識別するためのスロット番号をコア ダンプ ファイルに追加します。

（注） コア ダンプは、一般的にテクニカルサポート担当者にだけ役立ちます。コア ダンプ ファイルは、非常に大きなバイナリ ファイルであり、TFTP、FTP、またはリモート コピー プロトコル（RCP）サーバを使用して転送した後、ソース コードと詳細なメモリ マップにアクセスできる Cisco Technical Assistance Center（TAC）の担当者に分析してもらう必要があります。

SSO 認識機能

機能が、RP スイッチオーバーを経ても、一部または全体が問題なく動作し続ける場合、その機能やプロトコルは SSO 認識です。SSO 認識機能のステート情報は、これらの機能のステートフル スイッチオーバーを実現するために、アクティブからスタンバイへ同期されます。

SSO 非認識の機能の場合、ステートをダイナミックに作成しても、スイッチオーバー時に失われるため、スイッチオーバーの際に再初期化と再起動が必要になります。

show redundancy clients コマンドの出力には、SSO 認識機能が表示されます（「SSO 機能の確認」（P.7-14）を参照）。

SSO のデフォルト設定

なし。

SSO の設定方法

（注） スイッチにイメージをコピーする方法については、第 6 章「高速ソフトウェア アップグレード」を参照してください。アップグレード プロセスでは、さまざまなイメージが非常に短い期間、RP にロードされます。この間にスイッチオーバーが発生すると、デバイスは RPR モードで回復します。

SSO または RPR 冗長モードが常に設定されます。SSO 冗長モードはデフォルトで設定されます。RPR 冗長モードからデフォルト SSO 冗長モードに戻すには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router> enable`	特権 EXEC モードをイネーブルにします（プロンプトが表示されたらパスワードを入力します）。
ステップ 2	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	`Router(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 4	`Router(config)# mode sso`	アクティブとスタンバイの両方の RP で、冗長コンフィギュレーション モードを SSO に設定します。 **（注）** SSO モードを設定した後、スタンバイ RP が自動的にリセットされます。
ステップ 5	`Router(config-red)# end`	冗長コンフィギュレーション モードを終了して、スイッチを特権 EXEC モードに戻します。
ステップ 6	`Router# copy running-config startup-config`	コンフィギュレーションの変更をスタートアップ コンフィギュレーション ファイルに保存します。

次に、SSO 冗長モードを設定する例を示します。

```
Router> enable
Router# configure terminal
```

```
Router(config)# redundancy
Router(config)# mode sso
Router(config-red)# end
Router# copy running-config startup-config
Router#
```

SSO のトラブルシューティング

考えられる SSO の問題状況

- スタンバイ RP をリセットしたが、生じた問題を説明するメッセージが表示されない：SSO イベントのログなど、スイッチオーバーやその他のイベントが発生した理由を探る鍵となるものを表示するには、新しくアクティブになった RP で **show redundancy history** コマンドを実行します。

  ```
  Router# show redundancy history
  ```

- **show redundancy states** コマンドを実行すると、ネットワーキング デバイスでの設定内容と異なる動作モードが表示される：特定のプラットフォームで **show redundancy states** コマンドを使用すると、プラットフォームごとに設定されたコンフィギュレーション モードではなく、デバイスで実行されている実際の動作冗長モードが出力表示されることがあります。システムの動作モードは、システム イベントに応じて変化する可能性があります。たとえば、SSO を使用するためには、ネットワーキング デバイス上の両方の RP が同じソフトウェア イメージを実行する必要があります。イメージが異なる場合、デバイスはそのコンフィギュレーションに関係なく、SSO モードでは動作しなくなります。

  たとえば、アップグレード プロセス中にごく短時間、さまざまなイメージが RP にロードされます。この間にスイッチオーバーが発生すると、デバイスは RPR モードで回復します。

- デバイスをリロードすると、SSO の動作が中断する：SSO の機能によって新しいコマンドが導入されましたが、その中に、手動でスイッチオーバーを発生させるコマンドがあります。reload コマンドは SSO コマンドではありません。このコマンドを実行すると、ボックスが完全にリロードされ、すべてのテーブル エントリが削除され、すべてのラインカードがリセットされるので、ネットワーク トラフィック転送が中断されます。誤ってボックスをリロードしないようにするには、**redundancy force-switchover** コマンドを使用します。

- ソフトウェア アップグレードの際、ネットワーキング デバイスが SSO ではないモードで表示される：ソフトウェア アップグレード プロセス中は、show redundancy コマンドを使用するとデバイスが SSO ではないモードで動作していることを示します。

  これは正常な動作です。FSU 手順が完了するまで、各 RP では異なるソフトウェア バージョンが実行されています。RP が異なるソフトウェア バージョンを実行している間、モードはいずれかの RPR に変更されます。アップグレードが完了すれば、デバイスは SSO モードに変更されます。

- コア ダンプが完了する前に以前のアクティブ プロセッサのリセットとリロードが実行される：以前のアクティブ プロセッサのリセットとリロードを実行するまでの新しいアクティブ プロセッサの最大待機時間を設定するには、**crashdump-timeout** コマンドを使用します。

- 「send break」コマンドを発行してもシステムのスイッチオーバーが実行されない：これは通常の動作です。「send break」コマンドを使用して、システムをブレークまたは一時停止することは推奨できません。予期しない結果が生じるおそれがあります。手動のスイッチオーバーを開始するには、**redundancy force-switchover** コマンドを使用します。

Cisco IOS ソフトウェアでは、スイッチを再起動し、起動開始から 60 秒以内に Break キーを押すか Telnet セッションから「send break」コマンドを実行すると、ROM モニタ モードを開始できます。send break 機能は、経験豊富なユーザまたは Cisco Technical Assistance Center（TAC）の担当者の指示によって操作しているユーザが、特定のシステム障害の回復やシステム障害の原因の解明を行うのに役立ちます。

SSO のトラブルシューティング

次の各コマンドは、必要に応じて SSO 機能のトラブルシューティングに使用できます。これらのコマンドには、決まった入力順序はありません。

コマンド	目的
Router(config-red)# **crashdump-timeout** [*mm* | *hh*:*mm*]	新しいアクティブ RP が、それまでアクティブだった RP をリロードするまでに待つ最長時間を設定します。
Router# **debug redundancy** {**all** | **ui** | **clk** | **hub**}	ネットワーキング デバイスで、冗長をデバッグします。
Router# **show diag** [*slot-number* | **chassis** | **subslot** *slot*/*subslot*] [**details** | **summary**]	ハードウェア情報を表示します。
Router# **show redundancy** [**clients** | **counters** | **debug-log** | **handover** | **history** | **switchover history** | **states** | **inter-device**]	RP の冗長コンフィギュレーション モードを表示します。スイッチオーバーの回数、システム稼働時間、プロセッサ稼働時間、冗長ステート、およびスイッチオーバーの理由に関する情報もあわせて表示します。
Router# **show version**	各 RP に関するイメージ情報を表示します。

SSO 設定の確認

- SSO が設定されていることを確認する
- デバイス上での SSO の動作の確認
- SSO 機能の確認

SSO が設定されていることを確認する

次の例では、**show redundancy** コマンドを使用して、デバイス上に SSO が設定されていることを確認します。

```
Router> enable
Router# show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 3 days, 4 hours, 35 minutes
Switchovers system experienced = 0
              Standby failures = 1
        Last switchover reason = none

                  Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso
              Maintenance Mode = Disabled
                Communications = Up
```

```
Current Processor Information :
-------------------------------
               Active Location = slot 5
        Current Software state = ACTIVE
       Uptime in current state = 3 days, 4 hours, 35 minutes
                 Image Version = Cisco IOS Software, s2t54 Software ...
Synced to ...
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled ...
                         BOOT = disk0:0726_c4,12
                   CONFIG_FILE =
                       BOOTLDR =
        Configuration register = 0x2102

Peer Processor Information :
-----------------------------
              Standby Location = slot 6
        Current Software state = STANDBY HOT
       Uptime in current state = 3 hours, 55 minutes
                 Image Version = Cisco IOS Software, s2t54 Software ...
Synced to ...
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled ...
                         BOOT = disk0:0726_c4,12
                   CONFIG_FILE =
                       BOOTLDR =
        Configuration register = 0x2102

Router#
```

デバイス上での SSO の動作の確認

次の例では、**show redundancy** コマンドと **states** キーワードを使用して、デバイス上に SSO が設定されていることを確認します。

```
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
Redundancy State              = sso
     Maintenance Mode = Disabled
    Manual Swact = enabled
 Communications = Up

   client count = 135
 client_notification_TMR = 30000 milliseconds
          keep_alive TMR = 9000 milliseconds
        keep_alive count = 1
    keep_alive threshold = 18
           RF debug mask = 0x0

Router#
```

SSO 機能の確認

SSO 機能として登録された機能のリストを表示するには、**show redundancy clients** コマンドを入力します。

```
Router# show redundancy clients
 clientID = 0       clientSeq = 0        RF_INTERNAL_MSG
 clientID = 1319    clientSeq = 1        Cat6k Platform First
 clientID = 29      clientSeq = 60       Redundancy Mode RF
 clientID = 139     clientSeq = 61       IfIndex
 clientID = 3300    clientSeq = 62       Persistent Variable
 clientID = 25      clientSeq = 68       CHKPT RF
 clientID = 1515    clientSeq = 69       HAL RF
 clientID = 3100    clientSeq = 73       MCM
 clientID = 77      clientSeq = 80       Event Manager
 clientID = 1328    clientSeq = 81       Cat6k Asic API RF Cl
 clientID = 1334    clientSeq = 82       Cat6k AUTOSHUT RF Cl
 clientID = 1333    clientSeq = 83       Cat6k OVERSUB RF Cli
 clientID = 1302    clientSeq = 84       Cat6k Fabric Manager
 clientID = 1331    clientSeq = 86       Cat6k Inline Power
 clientID = 1303    clientSeq = 88       Cat6k OIR
 clientID = 518     clientSeq = 89       PM Port Data
 clientID = 1306    clientSeq = 93       Cat6k QoS Manager
 clientID = 1501    clientSeq = 98       Cat6k CWAN HA
 clientID = 1503    clientSeq = 99       CWAN VLAN RF Client
 clientID = 1310    clientSeq = 100      Cat6k Feature Manage
 clientID = 1700    clientSeq = 101      Cat6k L3 Lif
 clientID = 78      clientSeq = 102      TSPTUN HA
 clientID = 305     clientSeq = 103      Multicast ISSU Conso
 clientID = 304     clientSeq = 104      IP multicast RF Clie
 clientID = 22      clientSeq = 105      Network RF Client
 clientID = 88      clientSeq = 106      HSRP
 clientID = 114     clientSeq = 107      GLBP
 clientID = 225     clientSeq = 108      VRRP
 clientID = 1505    clientSeq = 111      Cat6k SPA TSM
 clientID = 1509    clientSeq = 114      Cat6k Online Diag HA
 clientID = 1337    clientSeq = 116      Cat6k MPLS RF Client
 clientID = 75      clientSeq = 120      Tableid HA
 clientID = 1338    clientSeq = 124      Cat6k CTS Manager
 clientID = 512     clientSeq = 126      LAN-Switch BD Manage
 clientID = 501     clientSeq = 127      LAN-Switch VTP VLAN
 clientID = 513     clientSeq = 128      LAN-Switch IDBHAL
 clientID = 71      clientSeq = 129      XDR RRP RF Client
 clientID = 24      clientSeq = 130      CEF RRP RF Client
 clientID = 146     clientSeq = 132      BFD RF Client
 clientID = 301     clientSeq = 135      MRIB RP RF Client
 clientID = 306     clientSeq = 139      MFIB RRP RF Client
 clientID = 1504    clientSeq = 146      Cat6k CWAN Interface
 clientID = 1507    clientSeq = 147      CWAN LTL Mgr HA RF C
 clientID = 520     clientSeq = 151      RFS RF
 clientID = 210     clientSeq = 152      Auth Mgr
 clientID = 5       clientSeq = 153      Config Sync RF clien
 clientID = 138     clientSeq = 155      MDR SM
 clientID = 1308    clientSeq = 156      Cat6k Local Target L
 clientID = 1351    clientSeq = 157      RF VS Client
 clientID = 1358    clientSeq = 158      Cat6k VSlot
 clientID = 502     clientSeq = 162      LAN-Switch Port Mana
 clientID = 514     clientSeq = 163      SWITCH_VLAN_HA
 clientID = 1313    clientSeq = 165      Cat6k Platform
 clientID = 1318    clientSeq = 166      Cat6k Power
 clientID = 23      clientSeq = 171      Frame Relay
 clientID = 49      clientSeq = 172      HDLC
 clientID = 72      clientSeq = 173      LSD HA Proc
```

```
clientID = 113     clientSeq = 174      MFI STATIC HA Proc
clientID = 1335    clientSeq = 180      C6K EFP RF client
clientID = 200     clientSeq = 181      ETHERNET OAM RF
clientID = 207     clientSeq = 183      ECFM RF
clientID = 202     clientSeq = 184      ETHERNET LMI RF
clientID = 208     clientSeq = 186      LLDP
clientID = 20      clientSeq = 193      IPROUTING NSF RF cli
clientID = 21      clientSeq = 197      PPP RF
clientID = 1352    clientSeq = 201      C6K_provision_rf_cli
clientID = 1307    clientSeq = 202      Cat6k IDPROM
clientID = 74      clientSeq = 206      MPLS VPN HA Client
clientID = 34      clientSeq = 208      SNMP RF Client
clientID = 1502    clientSeq = 209      CWAN APS HA RF Clien
clientID = 52      clientSeq = 210      ATM
clientID = 35      clientSeq = 219      History RF Client
clientID = 90      clientSeq = 231      RSVP HA Services
clientID = 250     clientSeq = 243      EEM Server RF CLIENT
clientID = 252     clientSeq = 245      EEM POLICY-DIR RF CL
clientID = 54      clientSeq = 247      SNMP HA RF Client
clientID = 73      clientSeq = 248      LDP HA
clientID = 76      clientSeq = 249      IPRM
clientID = 57      clientSeq = 250      ARP
clientID = 50      clientSeq = 257      FH_RF_Event_Detector
clientID = 1508    clientSeq = 263      CWAN LTL SP RF Clien
clientID = 1304    clientSeq = 267      Cat6k Ehc
clientID = 1305    clientSeq = 271      Cat6k PAgP/LACP
clientID = 503     clientSeq = 272      Spanning-Tree Protoc
clientID = 1309    clientSeq = 273      CMRP RF Client
clientID = 1311    clientSeq = 275      Cat6k L3 Manager
clientID = 1317    clientSeq = 276      Cat6k CAPI
clientID = 1506    clientSeq = 277      CWAN SRP RF Client
clientID = 83      clientSeq = 284      AC RF Client
clientID = 145     clientSeq = 285      VFI Mgr
clientID = 84      clientSeq = 286      AToM manager
clientID = 85      clientSeq = 287      SSM
clientID = 87      clientSeq = 291      SLB RF Client
clientID = 504     clientSeq = 294      Switch SPAN client
clientID = 507     clientSeq = 295      Switch Backup Interf
clientID = 105     clientSeq = 298      DHCP Snooping
clientID = 1510    clientSeq = 304      Call-Home RF
clientID = 203     clientSeq = 307      MVRP RF
clientID = 151     clientSeq = 310      IP Tunnel RF
clientID = 94      clientSeq = 311      Config Verify RF cli
clientID = 516     clientSeq = 314      EnergyWise rf client
clientID = 508     clientSeq = 316      Port Security Client
clientID = 509     clientSeq = 317      LAN-Switch IP Host T
clientID = 515     clientSeq = 318      SISF table
clientID = 135     clientSeq = 322      IKE RF Client
clientID = 136     clientSeq = 323      IPSEC RF Client
clientID = 130     clientSeq = 324      CRYPTO RSA
clientID = 400     clientSeq = 326      IP Admission RF Clie
clientID = 3099    clientSeq = 335      ISSU process
clientID = 4005    clientSeq = 338      ISSU Test Client
clientID = 93      clientSeq = 342      Network RF 2 Client
clientID = 1320    clientSeq = 343      Cat6k PF_ML_RP
clientID = 510     clientSeq = 345      LAN-Switch PAgP/LACP
clientID = 511     clientSeq = 346      LAN-Switch Private V
clientID = 1321    clientSeq = 347      PM SP client
clientID = 1322    clientSeq = 348      VLAN Mapping
clientID = 1315    clientSeq = 350      Cat6k Clear Counter
clientID = 141     clientSeq = 352      DATA DESCRIPTOR RF C
clientID = 1000    clientSeq = 361      CTS HA
clientID = 1001    clientSeq = 362      Keystore
clientID = 3150    clientSeq = 363      SIA SD RF CLIENT
```

```
clientID = 3151    clientSeq = 364      SIA SB RF CLIENT
clientID = 3152    clientSeq = 365      SIA SCL RF CLIENT
clientID = 3153    clientSeq = 366      SIA SVE RF CLIENT
clientID = 3154    clientSeq = 367      SIA TCP RF CLIENT
clientID = 1332    clientSeq = 373      PCLC
clientID = 1367    clientSeq = 375      Cat6k ITASCA_RP
clientID = 4032    clientSeq = 379      ACL handle RF Client
clientID = 4020    clientSeq = 381      IOS Config ARCHIVE
clientID = 4021    clientSeq = 382      IOS Config ROLLBACK
clientID = 1339    clientSeq = 404      Cat6k blue beacon RF
clientID = 1362    clientSeq = 405      VS HA
clientID = 517     clientSeq = 406      LAN-Switch IDBHAL2
clientID = 1336    clientSeq = 415      Cat6k NTI SUP SI swi
clientID = 65000   clientSeq = 416      RF_LAST_CLIENT
```

SSO の設定例

次に、SSO 冗長モードを設定する例を示します。

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# mode sso
Router(config-red)# exit
Router# copy running-config startup-config
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する