CHAPTER 23

NSF/SSO MSFC 冗長機能の設定

この章では、Catalyst 6500 シリーズ スイッチ上で Cisco Nonstop Forwarding（NSF）/Stateful Switchover（SSO）を使用して Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）冗長機能を設定する手順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完全な構文および使用方法の詳細については、『*Catalyst 6500 Series MSFC Cisco IOS Command Reference*』を参照してください。

（注） *MSFC* という用語は、この章を通じて特に明記されていないかぎり、MSFC2、MSFC2A、および MSFC3 を指します。

（注） 特に明記されていないかぎり、この章で説明する情報および手順は、Policy Feature Card（PFC; ポリシー フィーチャ カード）3B/3BXL を搭載した Supervisor Engine 32、PFC3A/PFC3B/PFC3BXL を搭載した Supervisor Engine 720、および PFC2 を搭載した Supervisor Engine 2 に適用されます。

この章で説明する内容は、次のとおりです。

ハードウェアおよびソフトウェアの要件

ここでは、NSF/SSO を設定する場合のハードウェアおよびソフトウェア要件について説明します。

- サポート対象スーパバイザ エンジン ― Supervisor Engine 2、Supervisor Engine 720、および Supervisor Engine 32（Supervisor Engine 1 では NSF/SSO はサポートされません）。
- サポート対象 MSFC ― MSFC2、MSFC2A、および MSFC3（MSFC はサポートされません）。
- 冗長スーパバイザ エンジンには、同じモデルの PFC と MSFC を搭載した同じタイプのスーパバイザ エンジンを使用する必要があります。
- Rlease 8.5(1) 以降の Catalyst ソフトウェア リリース

（注） SSO が MSFC 上でイネーブルな場合、Release 8.5(1) 以降のスーパバイザ エンジン ソフトウェア リリースにアップグレードする前に、スーパバイザ エンジン上でハイ アベイラビリティをイネーブルにする必要があります。**set system highavailability enable** コマンドを使用して、スーパバイザ エンジン上でハイ アベイラビリティ機能をイネーブルにします。

- Cisco IOS Release 12.2(18)SXF 以降のリリース

NSF/SSO の機能概要

（注）　SSO は、Single Router Mode（SRM）と Dual Router Mode（DRM）に代わる機能です。これらのハイ アベイラビリティ モードは、サポートされません。SRM および DRM の CLI（コマンドライン インターフェイス）処理の詳細については、「設定時の注意事項および制限事項」（p.23-5）を参照してください。

スーパバイザ エンジン上で稼働する Catalyst オペレーティング システムにより、冗長スーパバイザ エンジンのレイヤ 2 ハイ アベイラビリティが提供されます。MSFC 上で稼働する NSF/SSO を備えた Cisco IOS Release 12.2(18)SXF 以降のリリースでは、冗長 MSFC にレイヤ 3 以上のハイ アベイラビリティ機能を提供します。MSFC SSO のハイ アベイラビリティの利点は、次のとおりです。

- ダウンタイムの軽減
- MSFC をシャット ダウンせずにソフトウェアをアップグレード可能
- アクティブ MSFC の障害を検出し、スタンバイ MSFC が既存トラフィック フローの廃棄を最少限にして、システムをテイクオーバー可能

システムが起動し、スーパバイザ エンジンが初期化を完了し動作準備が整ったあと、スーパバイザ エンジンは両方の MSFC に SCP インベントリ メッセージを送信します。インベントリ メッセージには、システム内にどの MSFC が存在するかという情報および他の動作ステート情報が含まれます。ハイ アベイラビリティという観点では、インベントリ メッセージには、アクティブ MSFC となる MSFC およびスタンバイ MSFC となる MSFC を指示する情報が含まれるので、重要です。

スタンバイ MSFC の起動中、イメージ バージョン情報は MSFC 間で交換され、次のいずれかの処理が行われます。

- イメージ バージョン情報が一致し、両方の MSFC が SSO として設定されるか、またはデフォルトに（SSO）設定されると、システムは SSO モードで稼働します。
- イメージ バージョン情報が一致しないか、または MSFC のどちらかで Route Processor Redundancy（RPR）が設定されると、システムは RPR モードで稼働します。

NSF/SSO モードでは、一方の MSFC がアクティブ モードでもう一方の MSFC はホットスタンバイ モードになります。ホットスタンバイ MSFC は、アクティブ MSFC からステート情報を受信することにより、一定の準備ステートを維持します。スーパバイザ エンジンは、スタンバイ MSFC にアクティブ MSFC が行っている処理を引き継ぐように要求する場合があります。スーパバイザ エンジンはアクティブ MSFC をモニタします。MSFC が応答しない場合は、スーパバイザ エンジンは MSFC に切断またはダウンを宣告し、MSFC のリセットを行います。スタンバイ MSFC には、処理を開始するのに必要な最新のステート情報があります（スタンバイ MSFC は完全に初期化されますが、スイッチオーバーが発生するまでは、VLAN［仮想 LAN］は管理上のダウン ステートのままです）。

NSF により、スイッチング モジュールおよびスイッチ ファブリックは、MSFC スイッチオーバーの実行中もパケット転送を継続します。

（注）　検出されたハードウェア障害または CLI コマンドによっても、スイッチオーバーは発生します。

（注）　スーパバイザ エンジン上のハイ アベイラビリティ機能は、MSFC のハイ アベイラビリティ機能とは無関係です。ただし、確実に MSFC SSO 機能を適切に動作させるように、スーパバイザ エンジン上でハイ アベイラビリティをイネーブルにする必要があります。

SSO モードで MSFC を稼働中に、スーパバイザ エンジンのハイ アベイラビリティ機能を実行していない場合、スイッチオーバーは非ステートフル スイッチオーバーとなり、スタンバイ MSFC はスイッチオーバー時にリセットされ、再起動されます。スーパバイザ エンジン上に MSFC の SSO をサポートするのに十分なステート情報がないため、スタンバイ MSFC のリセット / 再起動が発生します。スタンバイ MSFC のリセット / 再起動により、サービスは中断されます。

RPR の概要

（注）　RPR+ モードはサポートされません。

RPR は、*コールド*スタンバイ モードです。スイッチオーバーが発生すると、スタンバイ MSFC は完全に初期化する必要があります。RPR モードは、主として Fast Software Upgrade（FSU）用に使用されます（「高速ソフトウェア アップグレード」[p.23-16] を参照）。RPR モードでは、スタートアップ コンフィギュレーションがスタンバイ MSFC に同期化されますが、スイッチオーバーが発生するまでは一切処理されません。実行コンフィギュレーションは、スタンバイ MSFC に同期化されません。

アクティブ MSFC が完全に起動すると、MSFC 間でのステート情報の交換は行われません。アクティブ MSFC が故障すると、スタンバイ MSFC がスタートアップ コンフィギュレーション ファイルを処理して、初期化を開始します。

イメージの互換性に問題がある場合は、アクティブ MSFC は完全に起動しますが、スタートアップ コンフィギュレーション ファイルを処理する前に、スタンバイ MSFC は起動を中断します。アクティブ MSFC が故障すると、スイッチオーバーがトリガーされ、中断されたスタンバイ MSFC が初期化を開始し、アクティブ MSFC となります。

（注）　MSFC 上で RPR を実行する場合、スーパバイザ エンジン上のハイ アベイラビリティをイネーブルにする必要はありません。

MSFC スイッチオーバーのタイプ

MSFC スイッチオーバーのタイプは、次のとおりです。

- フェールオーバー — アクティブ MSFC が故障するか、または重大なシステム障害が検出され、最終的に ROMMON に入ると、MSFC フェールオーバーが発生します。
- 強制スイッチオーバー — 強制スイッチオーバーは、CLI コマンドを入力するか、またはシャーシからアクティブ MSFC 搭載のスーパバイザ エンジンを取り外すことにより発生します。強制的にスイッチオーバーを実行する MSFC の CLI コマンドは、**redundancy force-switchover** および **reload** コマンドです。強制的にスイッチオーバーを実行するスーパバイザ エンジンの CLI コマンドは、**reset** *mod* コマンドです。この場合 *mod* は、**show module** コマンド表示で示される MSFC のモジュール番号です。

設定時の注意事項および制限事項

ここでは、NSF/SSO を設定する際の設定時の注意事項と制限事項を説明します。

- SSO が MSFC 上でイネーブルな場合、Release 8.5(1) 以降のスーパバイザ エンジン ソフトウェア リリースにアップグレードする前に、スーパバイザ エンジン上でハイ アベイラビリティをイネーブルにする必要があります。**set system highavailability enable** コマンドを使用して、スーパバイザ エンジン上でハイ アベイラビリティ機能をイネーブルにします。
- SSO は、SRM および DRM に代わる機能です。これらのハイ アベイラビリティ モードは、サポートされません。詳細は、次のとおりです。
  - SRM CLI 処理 — Cisco IOS Release 12.2(18)SXF 以降のソフトウェア リリースには、SRM CLI が含まれます。CLI は入力時に受け入れられますが、機能はしません。SRM CLI は、Cisco IOS Release 12.2(18)SXF 以降のソフトウェア リリースで維持され、NSF/SSO への移行を容易にします。ただし、SRM CLI により NVRAM（不揮発性 RAM）のアップデートは行われません。SRM CLI が設定されていて、**write mem** コマンドを入力して SRM 設定を変更しようとする場合、設定内の SRM CLI コマンドは失われます。SRM を持つイメージにダウングレードする場合、元の SRM CLI 設定は失われるため、SRM を再設定する必要があります。このため、SRM から NSF/SSO にアップグレードする前に設定を保存することを推奨します。
  - DRM CLI 処理 — SRM CLI とは異なり、NSF/SSO へのアップグレード後のコンフィギュレーション ファイルには、既存の DRM CLI がシステム起動時のエラーとしてフラグ付けされます。スイッチを再設定して、DRM 設定を削除する必要があります。DRM から NSF/SSO にアップグレードする前に設定を保存することを推奨します。
- スイッチオーバー中は、MSFC によりルーティングされたトラフィックのトラフィック損失が発生します。NSF は、モジュールおよびスイッチ ファブリックによりハードウェア スイッチングされたトラフィックにのみ適用されます。スイッチオーバーが完了するまで、新しいフローは許可されません。
- MSFC に障害があり、スーパバイザ エンジンにこの障害を通知できない場合、スーパバイザ エンジンが MSFC の障害を認識し、スイッチオーバーがトリガーされるまで 30 ～ 40 秒かかる可能性があります。スーパバイザ エンジンが障害通知を受信した場合、スイッチオーバーは直ちにトリガーされます。
- フレーム リレー、Asynchronous Transfer Mode（ATM; 非同期転送モード）、および PPP（ポイントツーポイント プロトコル）の各プロトコルは、SSO モードでサポートされません。
- WAN モジュールは、SSO スイッチオーバーに対して次のように動作します。
  - SSO スイッチオーバーの場合、WAN モジュールは再起動しません。
  - WAN モジュール インターフェイスは、SSO スイッチオーバー中にダウンして、その後アップに戻ります。
  - NSF が WAN インターフェイスで設定されている場合、すべてのルーティング プロトコルは NSF を実行しません。
  - WAN インターフェイスのすべての機能は、SSO スイッチオーバー後に動作を再開します。

- スタンバイ スーパバイザ エンジン /MSFC 挿入 — NSF/SSO 冗長性では、メンテナンスのためのスタンバイ スーパバイザ エンジン /MSFC のホット スワップが可能です。スタンバイ MSFC をホット インサートすると、アクティブ MSFC がスタンバイ MSFC の存在を検出し、スタンバイ MSFC ステートをホットスタンバイに移行させます。スタンバイ MSFC を取り外すと、アクティブ MSFC とスタンバイ MSFC 間の同期化が中断され、スタンバイ MSFC への保留状態のアップデートはすべて廃棄され、シンプレックス モードが開始されます。スタンバイ MSFC ステートは、**show redundancy states** コマンドにより表示されます。
- カウンタおよび統計情報 — MSFC により維持される各種カウンタおよび統計情報は、MSFC 間で同期化されません。
- すべてのサブシステムがハイアベイラビリティ対応であるわけではなく、ハイアベイラビリティ アウェアであるサブシステムでも、それぞれ一連の制限があります。
- 一部のサブシステムでは、それぞれハイ アベイラビリティ固有の設定およびステータス コマンド（ **show isis nsf** など）があります。
- MSFC ソフトウェア イメージは、現在 In-Service Software Upgrade（ISSU）をサポートしません。
- 診断は、ハイ アベイラビリティに統合されません。MSFC 上の診断失敗によるスイッチオーバーは、サポートされません。

CLI を使用した NSF/SSO の設定

ここでは、NSF/SSO を設定する手順について説明します。

SSO の設定

SSO は、デフォルト モードです。デフォルトでは、明示的に SSO として設定されない場合でも、システムは SSO モードでアップします。ただし、明示的に SSO モードを設定することを推奨します。

（注）　次の作業は、RPR モードの設定でも使用できます（**mode sso** の代わりに **mode rpr** を使用）。

SSO モードを設定するには、次の作業を実行します。

	作業	コマンド
ステップ 1	冗長コンフィギュレーション モードを開始します。	`Router(config)# redundancy`
ステップ 2	SSO を設定します。このコマンドにより、冗長 MSFC が再起動され、SSO モードで機能を開始します。	`Router(config-red)# mode sso`
ステップ 3	SSO がイネーブルに設定されたことを確認します。	`Router# show running-config`
ステップ 4	動作冗長モードを表示します。	`Router# show redundancy states`

次に、システムで SSO を設定して、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 = 1  -DISABLED
           Mode = Simplex
           Unit = Primary
        Unit ID = 7
Redundancy Mode (Operational) = Stateful SwitchOver - SSO
Redundancy Mode (Configured)  = Stateful SwitchOver - SSO
Redundancy State              = Non Redundant

     Split Mode = Disabled
   Manual Swact = Disabled  Reason: Simplex mode
 Communications = Down      Reason: Simplex mode

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

CEF NSF の設定

デフォルトでは、Cisco Express Forwarding（CEF) NSF は、ネットワーキング装置が SSO モードで稼働している場合に動作します。設定作業は必要ありません。

CEF NSF の確認

CEF が NSF 対応であることを確認するには、次の作業を実行します。

作業	コマンド
CEF が NSF 対応であることを確認します。	Router# **show cef state**

次に、CEF が NSF 対応であることを確認する例を示します。

```
router# show cef state
CEF Status [RP]
 CEF enabled/running
 dCEF enabled/running
 CEF switching enabled/running
 CEF default capabilities:
  Always CEF switching:               yes
  Always dCEF switching:              yes
  Default CEF switching:              yes
  Default dCEF switching:             yes
  Drop multicast packets:             no
  OK to punt packets:                 yes
  NVGEN CEF state:                    yes
  fastsend() used:                    no
  CEF NSF capable:                    yes
  RPR+/SSO standby capable:           yes
  IPC delayed func on SSO:            no
  FIB auto repair supported:          yes
  LCs not running at init time:       yes
  Hardware forwarding supported:      yes
  Hardware forwarding in use:         yes
  Load-sharing pr. packet supported:  no
 RRP state:
  I am standby RRP:                   no
  RF Peer Presence:                   no
  RF PeerComm reached:                no
  Config Redundancy mode:             Stateful SwitchOver - SSO(7)
  Operating Redundancy mode:          Stateful SwitchOver - SSO(7)
  CEF NSF:                            enabled/not running
 RP state:
  Expanded LC ipc memory:             0 Kbytes
  Linecard reloader type:             aggressive (Default)
  Linecard dFIB structures:           initialized
Router#
```

BGP NSF の設定

（注）　Border Gateway Protocol（BGP）NSF に参加するすべてのピア デバイス上では、BGP の適切な再起動を設定する必要があります。

NSF に BGP を設定するには、次の作業を実行します（この作業を各 BGP NSF ピア デバイス上で繰り返します）。

	目的	コマンド
ステップ 1	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。	`Router# configure terminal`
ステップ 2	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。	`Router(config)# router bgp as-number`
ステップ 3	BGP の適切な再起動機能をイネーブルにして、BGP NSF を開始します。 BGP セッションの確立後にこのコマンドを入力する場合、BGP ネイバと機能を交換できるよう、セッションを再起動する必要があります。 再起動するルータおよびすべてのピアでこのコマンドを使用します。	`Router(config-router)# bgp graceful-restart`

BGP NSF の確認

BGP NSF を確認するには、SSO 対応のネットワーキング装置および近接装置上で、適切な再起動機能が設定されていることを確認する必要があります。確認するには、次の手順を実行します。

ステップ 1　**show running-config** コマンドを入力して、SSO 対応ルータの BGP 設定で [bgp graceful-restart] が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 ネイバ上でステップ 1 を繰り返します。

ステップ 3　SSO 装置および近接装置上で、適切な再起動機能がアドバタイズ済み、受信済みの両方で表示されることを確認して、適切な再起動機能のあるアドレス ファミリーを確認します。

（注）　アドレス ファミリーが表示されない場合、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 に参加するすべてのピア装置では、OSPF NSF 対応にする必要があります。これは、装置に NSF ソフトウェアをインストールすると自動的に実行されます。

OSPF NSF を設定するには、次の作業を実行します。

	目的	コマンド
ステップ 1	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。	`Router# configure terminal`
ステップ 2	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。	`Router(config)# router ospf processID`
ステップ 3	OSPF の NSF 動作をイネーブルにします。	`Router(config-router)# nsf`

OSPF NSF の確認

OSPF NSF を確認するには、NSF 機能が SSO 対応のネットワーキング装置に設定されていることを確認する必要があります。OSPF NSF を確認するには、次の手順を実行します。

ステップ 1　**show running-config** コマンドを入力して、SSO 対応装置の OSPF 設定で [nsf] が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 が装置上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

Intermediate System-to-Intermediate System（IS-IS）NSF を設定するには、次の作業を実行します。

	目的	コマンド
ステップ 1	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。	`Router# configure terminal`
ステップ 2	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。	`Router(config)# router isis [tag]`
ステップ 3	IS-IS の NSF 動作をイネーブルにします。 IETF ドラフトベースの再起動性をサポートするネットワーキング装置との隣接関係が保証されている場合は、**ietf** キーワードを入力して、同種ネットワークで IS-IS をイネーブルにします。 NSF 対応のネットワーキング装置と隣接関係にない場合は、**cisco** キーワードを入力して、異種ネットワークで IS-IS を実行します。	`Router(config-router)# nsf [cisco | ietf]`
ステップ 4	（任意）NSF 再起動試行間の最少時間を指定します。*連続する* NSF 再起動試行間のデフォルト時間は、5 分です。	`Router(config-router)# nsf interval [minutes]`
ステップ 5	（任意）IS-IS 自身のリンクステート情報が一杯になり、その情報がネイバにフラッディングされるまで、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。 **t3** キーワードは、IETF 動作を選択した場合にのみ、適用されます。**adjacency** キーワードを指定すると、再起動中のルータは近接装置から待機時間を取得します。	`Router(config-router)# nsf t3 {manual [seconds] | adjacency}`
ステップ 6	（任意）再起動が完了する前に、IS-IS 隣接関係にあるすべてのインターフェイスがアップするまで IS-IS NSF の再起動を待機する時間を指定します。デフォルトは 10 秒です。	`Router(config-router)# nsf interface wait seconds`

IS-IS NSF の確認

IS-IS NSF を確認するには、NSF 機能が、SSO 対応のネットワーキング装置に設定されていることを確認する必要があります。IS-IS NSF を確認するには、次の作業を実行します。

ステップ 1　**show running-config** コマンドを入力して、SSO 対応装置の IS-IS 設定で [nsf] が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。次に、装置が IS-IS NSF の Cisco 実装 を使用する例を示します。

```
Router# show running-config
(テキスト出力は省略)
router isis
nsf cisco
(テキスト出力は省略)
```

ステップ 2　NSF 設定が **cisco** に設定されている場合、**show isis nsf** コマンドを入力して、NSF が装置上でイネーブルであることを確認します。Cisco 設定を使用すると、表示出力はアクティブ MSFC（Route Processor［RP; ルート プロセッサ］）と冗長 MSFC で異なります。次に、アクティブ MSFC（RP）上の Cisco 設定の出力例を示します。この例で、[NSF restart enabled] があること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 Cisco 設定の出力例を示します。この例で、[NSF restart enabled] があること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 設定が **ietf** に設定されている場合、**show isis nsf** コマンドを入力して、NSF が装置上でイネーブルであることを確認します。次に、ネットワーキング装置上の IETF IS-IS 設定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
```

冗長関連情報の表示

冗長関連情報を表示するには、**show redundancy** [qualifier] コマンドを使用します。サポートされる修飾詞は、次のとおりです。

```
Router# show redundancy ?
  clients          Redundancy Facility (RF) client list
  counters         Redundancy Facility (RF) operational counters
  events           Redundancy Facility (RF) events list
  history          Redundancy Facility (RF) history
  linecard-group   Line card redundancy group information
  states           Redundancy Facility (RF) states
  switchover       Redundancy Facility (RF) switchover
  |                Output modifiers
  <cr>

Router#
```

MSFC スイッチオーバーの実行

スタンバイ MSFC にスイッチオーバーを行うには、**redundancy switch-activity** [**force**] コマンドを使用します。**force** キーワードにより、すべての制限事項が無効になります。

MSFC ソフトウェアのリロードの実行

スタンバイ MSFC（**peer** キーワード）またはシャーシ内のすべてのモジュール（**shelf** キーワード）をリロードするには、**redundancy reload** {**peer** | **shelf**} コマンドを使用します。

冗長関連のデバッグ コマンドの使用

冗長関連のデバッグ情報を表示するには、**debug redundancy** [qualifier] コマンドを使用します。サポートされる修飾詞は、次のとおりです。

```
Router# debug redundancy ?
  config-sync  HA config sync debug option
  ehsa         Redundancy Facility (RF) EHSA
  errors       Redundancy Facility (RF) Errors
  fsm          Redundancy Facility (RF) FSM events
  kpa          Redundancy Facility (RF) keep alive
  msg          Redundancy Facility (RF) Messaging events
  progression  Redundancy Facility (RF) Progression events
  status       Redundancy Facility (RF) Status events
  timer        Redundancy Facility (RF) Timer events

Router#
```

NSF/SSO 固有の冗長情報を表示するには、**debug hybrid-ha** [qualifier] コマンドを使用します。サポートされる修飾詞は、次のとおりです。

```
Router# debug hybrid-ha ?
  all     All Hybrid HA SSO/NSF platform specific debugging messages
  errors  Hybrid HA SSO/NSF platform specific warnings and errors
  events  Hybrid HA SSO/NSF platform specific events
  ipc     Hybrid HA SSO/NSF platform specific IPC related events
  kpa     Hybrid HA SSO/NSF platform specific Keep-Alive related events

Router#
```

ソフトウェアのアップグレード

ここでは、MSFC ソフトウェアをアップグレードする手順について説明します。

（注）　いずれのソフトウェア　アップグレードの手順を実行する場合も、事前に「設定時の注意事項および制限事項」（p.23-5）を参照してください。

高速ソフトウェア アップグレード

（注）　高速ソフトウェア アップグレード中は、システムは RPR モードとなるため、サービスは中断されます。スイッチオーバーは、ステートフルではありません。インターフェイスはダウンしますが、MSFC の初期化で再びアップし、RPR モードでアップになります。さらに、保存されていない設定変更はすべて失われます。

（注）　この手順では、両方の MSFC 上で Cisco IOS リリースが RPR（最低）をサポートする必要があり、両方の MSFC では同じソフトウェア バージョンを稼働する必要があります。アクティブ MSFC は、スタンバイ MSFC がアップすると、スタンバイ イメージ バージョンを確認します。スタンバイ イメージ バージョンがアクティブ イメージ バージョンと異なる場合、冗長モードは RPR に戻ります。

（注）　この手順は、SRM および DRM イメージとは連動しません。

（注）　冗長スーパバイザ エンジンには、同じモデルの PFC と MSFC を搭載した同じタイプのスーパバイザ エンジンを使用する必要があります。

高速ソフトウェア アップグレードにより、ソフトウェアのアップグレードまたはダウングレードに予定されていたダウンタイムが短縮されます。高速ソフトウェア アップグレードの手順には、スタンバイ MSFC およびアクティブ MSFC への新しいイメージのロード、およびスタンバイ MSFC の再起動が含まれます。スタンバイ MSFC 上で稼働する新しいイメージは、アクティブ MSFC 上で現在稼働中のイメージとの互換性がありません。そのため、スタンバイ MSFC は RPR モードでアップします。高速ソフトウェア アップグレードは、アップグレード プロセス中のイメージの非互換性を避けるため、RPR モードで実行されます。

新しいイメージの実行を開始するには、アクティブ MSFC の実行を中断することにより、スタンバイ MSFC に強制的に切り替えます。これで、スタンバイ MSFC はアクティブ MSFC となります。次に、中断していた MSFC の起動が許可されます。これは、スタンバイ MSFC となりますが、新しく

アップグレードされたイメージを実行します。新しいイメージは、両方の MSFC 上で稼働し、スタンバイ MSFC はホットスタンバイ モードでアップします。この時点で、両方の MSFC が同じイメージ バージョンを実行しているため、システムは SSO モードで稼働します。

（注）　スタンバイ MSFC がアクティブ MSFC となるスイッチオーバーをもう一度強制的に行うことにより、MSFC の元の役割（アクティブおよびパッシブ ステータス）に戻すこともできます。

高速ソフトウェア アップグレードを実行するには、次の手順を実行します。

ステップ 1　両方の MSFC に新しいイメージをコピーします。

ステップ 2　起動変数を設定して、**write memory** コマンドにより設定を保存します。

ステップ 3　スタンバイ MSFC をリセットし、オンラインに戻し、新しいイメージを実行します。**show redundancy states** コマンドを入力して、スタンバイ MSFC が完全にオンラインであることを確認します。

ステップ 4　**redundancy force-switchover** コマンドを入力して、手動のスイッチオーバーを実行します。スタンバイ MSFC は、新しいイメージを実行する新しいアクティブ MSFC となります。スイッチオーバー前のシステムは RPR モードであったため、搭載されたモジュールはスイッチオーバー中に新しいソフトウェアによりリセットされ、再度ダウンロードされます。

ステップ 5　新しいスタンバイ MSFC が再起動してオンラインに戻されると、両方の MSFC および搭載されたモジュールは、新しいバージョンのソフトウェアを実行します。

SSO の SRM および DRM からのアップグレード

（注）　このアップグレードにより、サービスは中断されます。実際のダウンタイムはスイッチの設定により変化しますが、システムを起動してオンラインにするのに所要される時間ほど長くはかかりません。

（注）　SSO を SRM および DRM からアップグレードする場合は、アップグレードを実行する前に設定を保存する必要があります。システムが新しいイメージをリロードする際、DRM 設定により解析エラーが生成されます。アップグレード後、SSO を使用するには DRM 設定を再設定する必要があります。

Cisco IOS Release 12.2(18)SXF 以前の Cisco IOS ソフトウェアは、SRM および（または）DRM 対応ですが、SSO へのアップグレードはサポートされていません。これらのソフトウェア イメージは、高速ソフトウェア アップグレード手順ではアップグレードできません。このソフトウェアをアップグレードするには、各 MSFC 上で新しいイメージをロードし、同時に両方の MSFC を起動する必要があります。

MSFC で新しいイメージがロードされたあと、システムを再起動して新しいイメージをロードする必要があります。この起動時間中にスイッチはオフラインになるため、新しいイメージをロードするまでは SSO の利点を確認できません。

混在モードの動作

ソフトウェアのアップグレードで誤りがあると、MSFC 上で SSO ベースのイメージが稼働し、もう一方の MSFC 上で SRM および（または）DRM ベースのイメージが稼働する混在モードの状態となります。この状態は、システムの安定性の問題につながります。

この混在モードでは、アクティブ MSFC 上で SSO ベースのイメージが稼働している場合、アクティブ MSFC は完全に起動し、シンプレックス（非冗長）ステートでアップします。また、SRM および（または）DRM ベースのイメージも起動しますが、スタンバイ ステートのままです。

混在モードのアップグレードとなるもう一つの例は、アクティブ MSFC 上で SRM および（または）DRM イメージが稼働し、スタンバイ MSFC 上で SSO ベースのイメージが稼働する場合です。このモードでは、SRM および（または）DRM イメージが稼働するアクティブ MSFC は完全に起動しますが、スタンバイ MSFC 上で稼働する SSO ベースのイメージは、誤ってその MSFC はアクティブ MSFC で、アクティブ MSFC として起動しようとしていると判断します。スーパイザ エンジンからスタンバイ MSFC であることを示すインベントリ メッセージを受信すると、MSFC の役割不一致エラーを報告して、自身をリロードします。この問題は、アクティブ MSFC 上で SRM、DRM、または boothelper イメージが稼働していて、スタンバイ MSFC 上で SSO 対応のイメージをロードしようとすると発生します。

両方の状況を解決するには、SRM および（または）DRM ソフトウェアを SSO ベースのソフトウェアと同じレベルにアップグレードするか、または SSO ベースのソフトウェアを SRM および（または）DRM イメージのレベルまでダウングレードする必要があります。