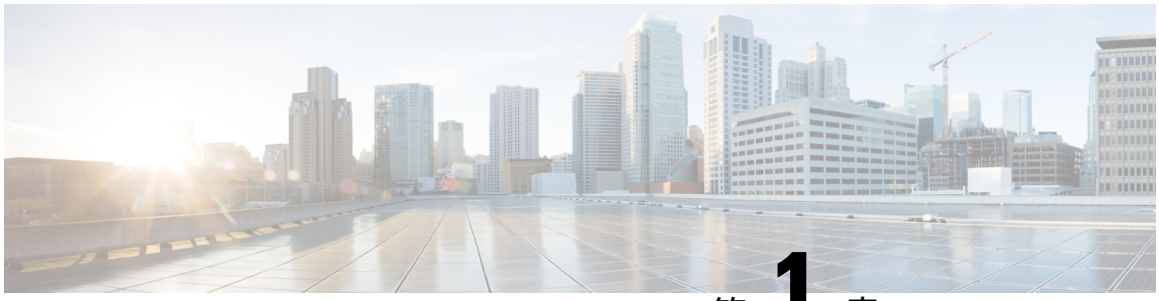
Cisco IOS XE Amsterdam 17.3.x（Catalyst 9400 スイッチ）ハイ アベイラビリティ コンフィギュレーション ガイド

初版：2020 年 7 月 31 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次



第 1 章

ノンストップ フォワーディング/ステートフル スイッチオーバー

Cisco Nonstop Forwarding（NSF）とステートフル スイッチオーバー（SSO）機能を組み合わせることにより、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が最小限に抑えられます。NSF の主な目的は、ルート プロセッサ（RP）のスイッチオーバー後に、引き続き IP パケットを転送することです。

Cisco Nonstop Forwarding とステートフル スイッチオーバーの前提条件

- Cisco Nonstop Forwarding（NSF）は、ステートフル スイッチオーバー（SSO）対応に設定されているネットワークデバイス上で設定する必要があります。
- NSF で Border Gateway Protocol（BGP）に対応するには、ネイバー 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がアドバタイズされる必要があります。NSF 対応デバイスが特定の 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、そのネイバーとは 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すべてのネイバーは、この NSF 対応ネットワーキング デバイスと NSF 対応セッションを継続します。

- NSF で Open Shortest Path First（OSPF）に対応するには、すべてのネイバー 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。NSF 対応デバイス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、そのセグメントについては NSF 機能をディセーブルにします。NSF 対応または NSF 認識デバイスばかりで構成された他のネットワーク セグメントは、継続して NSF 機能を提供します。

Cisco Nonstop Forwarding とステートフル スイッチオーバーの制約事項

NSF with SSO の制約事項を次に示します。

- IP マルチキャスト ルーティングは SSO を認識しないため、NSF はサポートされません。
- NSF が動作するには、SSO をデバイス上に設定する必要があります。
- グレースフル リスタート機能をサポートするためには、すべてのレイヤ 3 のネイバー デバイスが NSF Helper または NSF 対応である必要があります。
- IETF の場合、すべてのネイバー デバイスで NSF 認識ソフトウェア イメージが実行されている必要があります。
- ホット スタンバイ ルーティング プロトコル（HSRP）は、NSF SSO でサポートされていません。
- NSF 認識デバイスは、2 台の NSF 対応ピアが 1 つの NSF の再起動処理を同時に実行することはサポートしません。ただし、NSF 再起動処理が完了した後で、両方のネイバーがピアリング セッションを確立することは可能です。
- SSO の動作では、アクティブデバイスとスタンバイデバイスの両方が同じバージョンの Cisco IOS XE イメージを実行していることを確認します。アクティブデバイスとスタンバイデバイスが異なるイメージで動作している場合、SSO フェールオーバーによって停止が発生することがあります。

Cisco Nonstop Forwarding とステートフル スイッチオーバーに関する情報

Cisco Nonstop Forwarding とステートフル スイッチオーバーの概要

Cisco NSF は、SSO 機能と連動します。デバイスは、アクティブ デバイスが使用できなくなった場合にスタンバイ スイッチが処理を引き継ぐようにすることで障害耐性をサポートします。NSF は SSO と連動して、ネットワークが使用できない時間を最小限に抑えます。

通常、ネットワーキング デバイスが再起動すると、そのデバイスのすべてのルーティング ピアは、デバイスがダウンし、そのあと再びアップになったことを検知します。このような移行によって、いわゆるルーティング フラップが発生します。ルーティング フラップは、複数のルーティング ドメインに広がる場合があります。ルーティングの再起動によって発生したルーティング フラップによって、ルーティングが不安定になります。これはネットワーク全体のパフォーマンスに悪影響を及ぼします。Cisco NSF は、SSO 対応のデバイスにおけるルーティング フラップを抑止することによって、ネットワークの安定性を保ちます。

Cisco NSF と SSO により、スイッチオーバー後にルーティング プロトコル情報が復元される間も、既知のルートでデータ パケットの転送が続行されます。NSF/SSO を使用すると、ピア ネットワーキング デバイスでルーティング フラップが発生しません。データトラフィックはインテリジェント ラインカードまたはデュアル フォワーディング プロセッサ（FP）を介して転送されますが、スタンバイルータプロセッサ（RP）では、スイッチオーバー中に障害が発生したアクティブな RP からの制御と見なされます。SSO の動作を伴う NSF は、スイッチオーバー中にラインカードおよびFP のアクティブ状態が維持され、アクティブ RP の Forwarding Information Base（FIB; 転送情報ベース）が最新状態に維持される機能を提供します。

NSF は、次のような利点を提供します。

- 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。
- ネットワーク全体の安定性：ネットワークの安定性は、ネットワーク内でデバイスに障害が発生し、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。
- ネイバーデバイスがリンクフラップを検出しない：インターフェイスはスイッチオーバーの間アクティブ状態のままなので、ネイバーデバイスはリンクフラップを検出しません（リンクがダウンしてアップに戻ることはありません）。
- 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。
- スイッチオーバーの前に確立したユーザ セッションを維持します。
- スタック メンバーが応答しない場合は、そのメンバーがスタックから削除されます。
- スタンバイ デバイスが応答しない場合は、新しいスタンバイ デバイスが選択されます。
- アクティブ デバイスが応答しない場合は、スタンバイ デバイスがアクティブ デバイスになります。

SSO の動作

スタンバイ デバイスは、SSO モードで稼働する場合、完全に初期化されたステートで起動し、アクティブ デバイスの固定コンフィギュレーションおよび実行コンフィギュレーションと同期されます。その後は、プロトコルのステートを維持し、SSO をサポートする機能に関するハー

ドウェアおよびソフトウェア ステートのすべての変更を同期します。そのため、冗長アクティブ デバイス構成内のレイヤ 2 セッションへの割り込みは最小限になります。

アクティブ デバイスに障害が生じると、スタンバイ デバイスがアクティブ デバイスになります。この新しいアクティブデバイスは既存のレイヤ2スイッチング情報を使用して、トラフィックの転送を続けます。ルーティング テーブルが新しいアクティブ デバイスに再度読み込まれるまで、レイヤ 3 の転送は延期されます。

（注）

- スタンバイデバイスが連邦情報処理標準（FIPS）キーでプログラムされていない場合は、正しい動作モードではないため、警告メッセージが出力されます。
- スイッチは、一方のスーパーバイザモジュールが FIPS モードで、もう一方が非 FIPS モードの場合でも、SSO モードで動作します。

Cisco Nonstop Forwarding の動作

NSF は、常に SSO とともに実行され、レイヤ 3 トラフィックの冗長機能を提供します。NSF は BGP、Enhanced Interior Gateway Routing Protocol（EIGRP）、OSPF ルーティングプロトコルでサポートされ、転送は Cisco Express Forwarding（CEF）でサポートされています。これらルーティング プロトコルは NSF 対応および NSF 認識で機能が強化されており、これらプロトコルを実行するデバイスはスイッチオーバーを検出できるほか、ネットワーク トラフィックの転送を継続するために必要なアクションやピア 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ます。

スイッチオーバー時、ルーティングプロトコルがルーティング情報ベース（RIB）テーブルを再作成している間、それぞれのプロトコルは Cisco Express Forwarding を使用してパケットの転送を継続します。ルーティング プロトコルの収束後、Cisco Express Forwarding は FIB テーブルを更新し、古いルート エントリを削除します。次に、Cisco Express Forwarding は新しい FIB 情報でハードウェアを更新します。

アクティブデバイスのが BGP、OSPF、または EIGRP ルーティングプロトコル用に設定されている場合（**graceful-restart** コマンドを使用）、ルーティングの更新はアクティブデバイスのの選択時に自動的に送信されます。

NSF は 2 つの主要な要素で構成されています。

- NSF 認識：ネットワーキング デバイスが NSF 互換ソフトウェアを実行している場合、このデバイスは NSF 認識です。アクティブデバイスのの選択が行われていても NSF デバイスがまだパケットを転送できることをネイバーデバイスが検出する場合、この機能のことを NSF 認識といいます。レイヤ 3 ルーティング プロトコル（BGP、OSPF、EIGRP）の拡張機能は、Cisco Express Forwarding ルーティング テーブルが時間切れにならないように、または NSF デバイスがルートをドロップしないように、ルート フラッピングを防ぐよう設計されています。NSF 認識デバイスは、ルーティング プロトコル情報をネイバー NSF デバイスに送信します。NSF 認識は、EIGRP スタブ、EIGRP、OSPF プロトコルに対してはデフォルトでイネーブルになります。NSF 認識は BGP に対してデフォルトではディセーブルに設定されています。

- NSF 対応：NSF をサポートするようにデバイスを設定した場合、そのデバイスは 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。NSF は SSO と連動して IP パケットを転送し続けることにより、アクティブ デバイスの選択後にレイヤ 3 ネットワークを利用できない時間を最小限にします。レイヤ 3 ルーティング プロトコル（BGP、OSPFv2、EIGRP）の再コンバージェンスは、ユーザが意識する必要がなく、バックグラウンドで自動的に実行されます。ルーティング プロトコルはネイバー デバイスからルーティング情報を回復し、Cisco Express Forwarding（CEF）テーブルを再構築します。

シスコ エクスプレス フォワーディング

NSF の重要な要素はパケット転送です。シスコのネットワーキング デバイスでは、Cisco Express Forwarding がパケット転送を行います。Cisco Express Forwarding は、転送情報ベース（FIB）を維持し、スイッチオーバー時はその時点で最新の FIB 情報を使用してパケットの転送を継続し、スイッチオーバー時のトラフィックの中断を軽減します。

通常の NSF 操作中、アクティブデバイスの上の Cisco Express Forwarding は、現在の FIB と隣接データベースを、スタンバイデバイスの上の FIB および隣接データベースと同期します。スイッチオーバー時、最初にスタンバイデバイスの上にある FIB および隣接データベースは、アクティブデバイスの上で最新だった FIB と隣接データベースのミラーイメージです。スタンバイデバイスの上の Cisco Express Forwarding は、アクティブデバイスの上の Cisco Express Forwarding によって送信された変更点を反映させて、転送エンジンを最新の状態に保ちます。転送エンジンは、インターフェイスおよびデータ パスが使用可能になりしだい、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 プロトコルはプレフィックス単位で RIB の再読み込みを始めるため、Cisco Express Forwarding にはプレフィックス単位のアップデートが行われ、これが FIB と隣接データベースの更新に使用されます。既存エントリと新規エントリには、最新であることを示す新しいバージョン（「エポック」）番号が付けられます。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、デバイスが信号通知を行います。ソフトウェアは、現在のスイッチオーバー エポックよりも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。これで FIB は最新のルーティング プロトコル転送情報を表示するようになります。

ルーティング プロトコル

ルーティング プロトコルは、アクティブな RP だけで実行され、ネイバー デバイスからルーティングの更新を受信します。ルーティング プロトコルは、スタンバイ RP では実行されません。スイッチオーバー後、ルーティング プロトコルは、ルーティング テーブルを再構築しやすいように NSF 認識ネイバー デバイスにステート情報を送信するよう要求します。また、ネイバーデバイスが NSF 認識ではない環境にある NSF 対応デバイスのルーティングテーブルの再構築では、アクティブ RP からスタンバイ RP にステート情報を同期するように Intermediate System-to-Intermediate System（IS-IS）プロトコルを設定できます。

（注） NSF 動作の場合、ルーティング プロトコルは Cisco Express Forwarding に応じて、ルーティング情報を再構築するとともにパケットの転送を続行します。

BGP の動作

NSF 対応のデバイスは、BGP ピアと BGP セッションを開始すると、OPEN メッセージをピアに送信します。メッセージには、NSF 対応デバイスには「グレースフル」リスタート機能があるという宣言が含まれます。グレースフル リスタートは、BGP ルーティング ピアがスイッチオーバーのあとにルーティング フラップが発生するのを防ぐメカニズムです。BGP ピアはこの機能がある場合、メッセージを送信するデバイスが NSF 対応であることを認識しています。NSF 対応デバイスと BGP ピアの両方が、セッションの確立時に 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、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。

RP 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 対応デバイスに関連付けられ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 RP 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ぐことができます。

RP のスイッチオーバーが発生した後、NSF 対応デバイスは BGP ピアとのセッションを再確立します。新しいセッションの確立中に、NSF 対応デバイスが再起動したことを識別する、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。この交換が完了すると、NSF 対応デバイスはルーティング情報を使用して、RIB と FIB を新しい転送情報で更新します。NSF 認識デバイスは、ネットワーク情報を使用して失効したルートを BGP テーブルから削除します。この後 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 メッセージのグレースフル リスタート機能は無視しますが、NSF 対応デバイスとの BGP セッションは確立します。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 機能が無いインターオペラビリティ）は可能になりますが、非 NSF 認識 BGP ピアとの 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、ネイバー 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 対応デバイスが特定の 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、そのネイバーとは 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ーはすべて、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。

EIGRP の動作

Enhanced Interior Gateway Routing Protocol（EIGRP）NSF 機能は、hello パケットで EIGRP ピアによって交換されます。NSF 対応デバイスは、hello パケットで再起動（RS）ビットを設定したことによって NSF の再起動処理が開始されたことをネイバーに通知します。NSF 認識デバイスが NSF 対応ネイバーから、NSF の再起動処理が進行中であるという通知を受け取ると、NSF 対応デバイスと NSF 認識デバイスは、即座にそれぞれのトポロジテーブルを交換します。トポロジ テーブルの送信が完了すると、NSF 認識デバイスは end-of-table アップデート パケットを送信します。次に NSF 認識デバイスは、NSF 対応デバイスを支援するために次のアクションを実行します。

- EIGRP hello ホールド タイマーの期限を終了し、hello パケットの生成および送信の間隔を短くします。これにより、NSF 認識デバイスは NSF 対応デバイスにより早く応答することで、NSF 対応デバイスがネイバーを再検出し、トポロジ テーブルを再構築するために必要な時間を短縮します。
- ルート ホールド タイマーが開始されます。このタイマーを使用して、NSF 認識デバイスが NSF 対応ネイバーに対する既知のルートを保持している期間を設定します。このタイマーは、**timers nsf route-hold** コマンドで設定されます。デフォルトの期間は 240 秒です。
- ピア リストで、NSF 認識デバイスは NSF 対応ネイバーが再起動していることを示すほか、隣接関係を維持し、NSF 認識デバイスがトポロジ テーブルを送信する準備ができていることを示す信号を NSF 対応ネイバーが送るまで、またはルート ホールド タイマーの期限が切れるまで、NSF 対応ネイバーの既知のルートを保持します。NSF 認識デバイスでルート ホールド タイマーの期限が切れると、NSF 認識デバイスは保持しているルートを破棄し、NSF 対応デバイスをネットワークに参加した新しいデバイスとして扱い、新しいデバイスに対して行うように隣接関係を再度確立します。
- NSF 認識デバイスは、スイッチオーバーの後、コンバージェンス処理中のままの NSF 対応デバイスにクエリーを送信し続けることによって、Stuck In Active（SIA）状態が発生するまでの時間を効果的に延長します。

スイッチオーバー処理が完了すると、NSF 対応デバイスは、サポートしているデバイスに end-of-table（EOT）アップデート パケットを送信することによって、再コンバージェンスされたこと、およびすべてのトポロジテーブルを受信したことをネイバーに通知します。その後、NSF 対応デバイスは通常の処理に戻ります。NSF 認識デバイスは、（再起動中の）NSF 対応デバイスでリフレッシュされないルートに対して、（アクティブな）別のパスを探します。その後、NSF 認識デバイスは通常の処理に戻ります。NSF 対応デバイスによってすべてのパスがリフレッシュされると、NSF 認識デバイスはすぐに通常の処理に戻ります。

（注） NSF 認識デバイスは、EIGRP ネットワーク内で NSF 非認識ネイバーまたは NSF 非対応ネイバーと完全に共存できます。NSF 非認識ネイバーは、NSF 対応を無視し、隣接関係をリセットするか、そうでなければピア セッションを正常に維持します。

OSPF の動作

OSPF NSF 対応デバイスがスーパーバイザ エンジンのスイッチオーバーを実行する場合、ルータは OSPF ネイバーとリンク ステート データベースを再同期化するため、次の作業を行う必要があります。

- ネイバー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 ネイバーを再学習する。
- 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する。

スーパーバイザ エンジン スイッチオーバーのあと、NSF 対応デバイスはできるだけ迅速に OSPF NSF 信号をネイバー NSF 認識デバイスに送信します。ネイバー ネットワーキング デバイスはこの信号により、このデバイスとのネイバー関係をリセットしてはいけないことを認識します。NSF 対応デバイスはネットワーク上の他のデバイスから信号を受信し、ネイバー リストの再構築を開始できます。

ネイバー関係が再構築されると、NSF 対応デバイスはすべての NSF 認識ネイバーとデータベース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 ネイバー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、RIB を更新して、新しい転送情報で FIB を更新します。その後、OSPF プロトコルは完全に収束されます。

（注） OSPF NSF では、すべてのネイバー ネットワーキング デバイスが NSF を認識する必要があります。NSF 対応デバイスは、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、そのセグメントでは NSF 機能をディセーブルにします。NSF 対応または NSF 認識デバイスばかりで構成された他のネットワーク セグメントは、継続して NSF 機能を提供します。

Cisco Nonstop Forwarding とステートフル スイッチオーバーの設定方法

ステートフル スイッチオーバーの設定

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。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**show redundancy states** 例： `Device# show redundancy states`	動作中の冗長モードを表示します。
ステップ 3	**redundancy** 例： `Device(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	**mode sso** 例： `Device(config-red)# mode sso`	ステートフル スイッチオーバーを設定します。 • このコマンドにより、スタンバイスイッチのがリロードされ、SSOモードで機能を開始します。
ステップ 5	**end** 例： `Device(config-red)# end`	冗長コンフィギュレーション モードを終了し、特権EXECモードに戻ります。
ステップ 6	**show redundancy states** 例： `Device# show redundancy states`	動作中の冗長モードを表示します。
ステップ 7	**debug redundancy status** 例： `Device# debug redundancy status`	冗長ステータス イベントのデバッグを有効にします。

Cisco Express Forwarding と Cisco Nonstop Forwarding の確認

手順

show cef state

ネットワーク デバイスでの Cisco Express Forwarding のステートを表示します。

例：

```
Device# show cef state

CEF Status:
RP instance
common CEF enabled
IPv4 CEF Status:
CEF enabled/running
dCEF enabled/running
CEF switching enabled/running
universal per-destination load sharing algorithm, id DEA83012
IPv6 CEF Status:
CEF disabled/not running
dCEF disabled/not running
universal per-destination load sharing algorithm, id DEA83012
RRP state:
I am standby RRP: no
RF Peer Presence: yes
RF PeerComm reached: yes
RF Progression blocked: never
Redundancy mode: rpr(1)
CEF NSF sync: disabled/not running
CEF ISSU Status:
FIBHWIDB broker
No slots are ISSU capable.
FIBIDB broker
No slots are ISSU capable.
FIBHWIDB Subblock broker
No slots are ISSU capable.
FIBIDB Subblock broker
No slots are ISSU capable.
Adjacency update
No slots are ISSU capable.
IPv4 table broker
No slots are ISSU capable.
CEF push
No slots are ISSU capable.
```

Cisco Nonstop Forwarding とステートフル スイッチオーバーの設定例

例：ステートフル スイッチオーバーの設定

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。

```
Device(config)# redundancy
Device(config-red)# mode sso
Device(config-red)# end
Device#
```

次に、**show redundancy** コマンドの出力例を示します。

```
Device# show redundancy states
```

```
       my state = 13 -ACTIVE
     peer state = 1  -DISABLED
           Mode = Simplex
           Unit = Primary
        Unit ID = 3

Redundancy Mode (Operational) = Non-redundant
Redundancy Mode (Configured)  = sso
Redundancy State              = Non Redundant
     Maintenance Mode = Disabled
    Manual Swact = disabled (system is simplex (no peer unit))
 Communications = Down      Reason: Simplex mode

   client count = 103
 client_notification_TMR = 30000 milliseconds
           RF debug mask = 0x0
```

次に、**show redundancy clients** コマンドの出力例を示します。

```
Device# show redundancy clients

 clientID = 29       group_id = 1        clientSeq = 60       Redundancy Mode RF
 clientID = 139      group_id = 1        clientSeq = 62       IfIndex
 clientID = 25       group_id = 1        clientSeq = 71       CHKPT RF
 clientID = 10001    group_id = 1        clientSeq = 85       QEMU Platform RF
 clientID = 77       group_id = 1        clientSeq = 87       Event Manager
 clientID = 1340     group_id = 1        clientSeq = 104      RP Platform RF
 clientID = 1501     group_id = 1        clientSeq = 105      CWAN HA
 clientID = 305     group_id = 1       clientSeq = 110     Multicast ISSU Consolidation
 RF
 clientID = 304      group_id = 1        clientSeq = 111      IP multicast RF Client
 clientID = 22       group_id = 1        clientSeq = 112      Network RF Client
 clientID = 88       group_id = 1        clientSeq = 113      HSRP
 clientID = 114      group_id = 1        clientSeq = 114      GLBP
 clientID = 4700     group_id = 1        clientSeq = 118      COND_DEBUG RF
 clientID = 1341     group_id = 1        clientSeq = 119      IOSXE DPIDX
 clientID = 1505     group_id = 1        clientSeq = 120      IOSXE SPA TSM
 clientID = 75       group_id = 1        clientSeq = 130      Tableid HA
 clientID = 501      group_id = 1        clientSeq = 137      LAN-Switch VTP VLAN
 clientID = 71       group_id = 1        clientSeq = 139      XDR RRP RF Client
 clientID = 24       group_id = 1        clientSeq = 140      CEF RRP RF Client
 clientID = 146      group_id = 1        clientSeq = 142      BFD RF Client
 clientID = 301      group_id = 1        clientSeq = 146      MRIB RP RF Client
 clientID = 306      group_id = 1        clientSeq = 150      MFIB RRP RF Client
 clientID = 402      group_id = 1        clientSeq = 161      TPM RF client
 clientID = 520      group_id = 1        clientSeq = 162      RFS RF
 clientID = 210      group_id = 1        clientSeq = 163      Auth Mgr
 clientID = 10101    group_id = 1        clientSeq = 164      NGMOD HMS RF client
 clientID = 5        group_id = 1        clientSeq = 165      Config Sync RF client
 clientID = 10007    group_id = 1        clientSeq = 170      NGWC FEC Rf client
 clientID = 10009    group_id = 1        clientSeq = 173      NGWC POWERNET Rf client
 clientID = 10100    group_id = 1        clientSeq = 174      NGMOD XCVR RF client
 clientID = 502      group_id = 1        clientSeq = 187      LAN-Switch Port Manager
 clientID = 530      group_id = 1        clientSeq = 189      Access Tunnel
 clientID = 519      group_id = 1        clientSeq = 190      Mac address Table Manager
 clientID = 209      group_id = 1        clientSeq = 209      L2FIB
 clientID = 207      group_id = 1        clientSeq = 215      CFM RF
 clientID = 208      group_id = 1        clientSeq = 218      LLDP
 clientID = 226      group_id = 1        clientSeq = 219      LACP
```

次に、**show redundancy counters** コマンドの出力例を示します。

```
Device# show redundancy counters

Redundancy Facility OMs
               comm link up = 0
             comm link down = 0

          invalid client tx = 0
          null tx by client = 0
                tx failures = 0
      tx msg length invalid = 0

      client not rxing msgs = 0
 rx peer msg routing errors = 0
           null peer msg rx = 0
         errored peer msg rx = 0

                 buffers tx = 7250
     tx buffers unavailable = 0
                 buffers rx = 6786
      buffer release errors = 0

 duplicate client registers = 0
  failed to register client = 0
       Invalid client syncs = 0
```

次に、**show redundancy states** コマンドの出力例を示します。

```
Device# show redundancy states

       my state = 13 -ACTIVE
     peer state = 1  -DISABLED
           Mode = Simplex
           Unit = Primary
        Unit ID = 3

Redundancy Mode (Operational) = Non-redundant
Redundancy Mode (Configured)  = sso
Redundancy State              = Non Redundant
     Maintenance Mode = Disabled
    Manual Swact = disabled (system is simplex (no peer unit))
 Communications = Down      Reason: Simplex mode

   client count = 103
 client_notification_TMR = 30000 milliseconds
           RF debug mask = 0x0
```

Cisco Nonstop Forwarding とステートフル スイッチオーバーに関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*Command Reference (Catalyst 9400 Series Switches)* の「*High Availability*」セクションを参照してください。

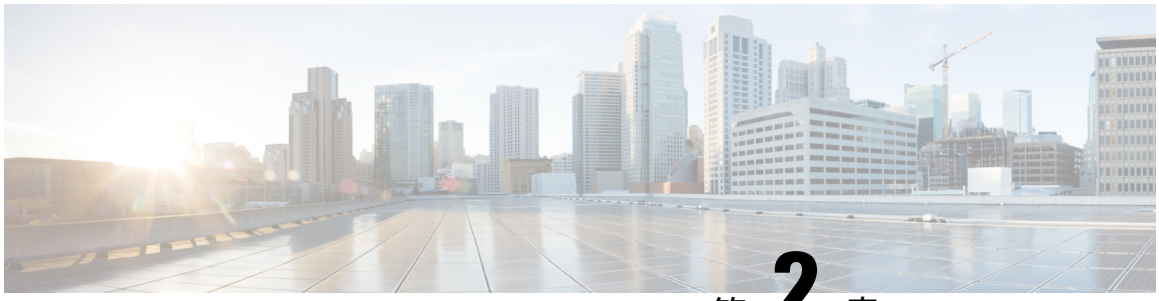
Cisco Nonstop Forwarding とステートフル スイッチオーバーの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.6.2	Cisco Nonstop Forwarding とステートフル スイッチオーバー	Cisco NSF は、SSO 機能と連動します。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、ルート プロセッサ（RP）のスイッチオーバー後に、引き続き IP パケットを転送することです。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com に進みます。



第 2 章

グレースフル挿入と削除の設定

グレースフル挿入と削除（GIR）は、デバイスメンテナンスによるネットワークサービスへの影響を最小限に抑えるための代替方法を提供します。GIR では、ネットワーク内の冗長パスを活用して、メンテナンス中のデバイスのスムーズな取り外しと、アウトオブサービス処理を行い、メンテナンスが完了した時点でサービスに戻します。この章では、GIR の設定方法について説明します。

グレースフル挿入と削除の制約事項

GIR は、レイヤ 2 インターフェイスのシャットダウン、ISIS ルーティングプロトコル、HSRP、VRRPv3、および BGP でサポートされています。これは、カスタマイズされたテンプレートを作成するか、またはテンプレートなしで設定します。

グレースフル挿入と削除について

概要

デバッグやアップグレードを実行するために、グレースフル挿入と削除（GIR）はスイッチをネットワークから分離します。スイッチをメンテナンスモードにするには、**start maintenance** コマンドを使用します。メンテナンスが完了したスイッチは、設定されたメンテナンスタイムアウトに到達した時点で、または **stop maintenance** コマンドにより、通常モードに戻ります。

スイッチをメンテナンス モードに移行する前のメンテナンス モード テンプレートの作成は任意です。デバイスのメンテナンス モードの目的は、ネットワークからの削除時および挿入時のトラフィックの中断を最小限に抑えることです。3 つの主要段階があります。

- ネットワークからのノードのグレースフル削除。
- デバイスでのメンテナンスの実行。
- ネットワークへのグレースフル挿入。

スイッチは、デフォルトのテンプレートまたはカスタムテンプレートを使用してメンテナンス モードに移行させることができます。デフォルトのテンプレートには、ISIS のすべてのインスタンスとともに **shut down l2** が含まれています。カスタムテンプレートでは、必要な ISIS インスタンスと **shutdown l2** オプションを設定できます。メンテナンス モードを開始すると、すべての参加プロトコルが分離され、L2 ポートがシャットダウンされます。通常モードに戻すと、すべてのプロトコルおよび L2 ポートが起動状態に戻ります。

メンテナンス モードへの移行中と終了中にスナップショットが自動的に作成されます。**snapshot create** *snapshot-name snapshot-description* コマンドを使用して、事前に選択した機能のスナップショットをキャプチャし、保存することができます。スナップショットは、メンテナンス モードになる前と通常モードに戻った後に、スイッチの状態を比較するのに便利です。スナップショット プロセスは、次の 3 つの部分で構成されます。

- 事前に選択したスイッチの一部機能の状態のスナップショットを作成し、永続ストレージ メディアに保存する。
- さまざまな時間間隔で取得したスナップショットを一覧にして、管理する。
- スナップショットを比較し、各機能の概要と詳細を表示する。

スイッチに保存できるスナップショットの最大数は 10 です。**snapshot delete** *snapshot-name* コマンドを使用して、特定のスナップショットをデバイスから削除できます。

メンテナンステンプレートまたはスナップショットテンプレートに対して複数のテンプレートを作成できます。ただし、一度に適用できるメンテナンステンプレートとスナップショットテンプレートは 1 つだけです。

スナップショットテンプレートを作成して、特定のスナップショットを生成できます。新しいスナップショットテンプレートは、**snapshot-template***template-name* コマンドを使用して作成できます。**snapshot-template***default-snapshot-template* コマンドを使用すると、メンテナンスモードでデフォルトのスナップショットテンプレートを指定できます。**snapshot create** [**template***template-name*] *snapshot-namesnapshot-description* コマンドを使用すると、スナップショット作成機能に特定のテンプレートを適用できます。

レイヤ 2 インターフェイスのシャットダウン

スイッチ上のポートなどのレイヤ 2 インターフェイスは、システムがメンテナンスモードに移行するときにシャットダウンされます。レイヤ 2 インターフェイスをシャットダウンするに

は、カスタムテンプレートで **shutdown l2**（メンテナンス テンプレート コンフィギュレーション モード）コマンドを使用します。

カスタム テンプレート

ネットワーク管理者として、システムがメンテナンスモードに移行するときに適用するテンプレートを作成できます。これによって、特定のプロトコルを分離できます。分離する必要があるすべてのインスタンスを明示的に指定する必要があります。

異なる設定で複数のテンプレートを作成できます。ただし、メンテナンスモードCLIに適用されるのは、単一のテンプレートのみです。適用すると、そのテンプレートは更新できません。テンプレートを更新する必要がある場合は、そのテンプレートを削除し、変更を加えてから、もう一度適用する必要があります。

テンプレート内の1つのクラスに属するプロトコルは、並行して処理されます。プロトコルの優先順位は、デフォルトのテンプレートの優先順位と同じです。

この機能を設定するには、**system mode maintenance** コマンドを使用してメンテナンスモードを開始し、**template***template-name***calss** コマンドを使用して機能を有効にします。

たとえば、カスタムテンプレートに次のプロトコルがある場合：

```
Maintenance-template foo
  router isis 100
  hsrp Et0/1 1
  hsrp Et0/1 2
  router isis 200

Maintenance-template foo class
  router isis 100
  hsrp Et0/1 1
  hsrp Et0/1 2
  router isis 200
```

上記の例では、isis は CLASS_IGP に属しているため、router isis 100 と router isis 200 は並行して処理されます。IGP クラスに属するこれらのプロトコルの両方に対して確認応答が受信されると、FHRP_CLASS クライアント、hsrp Et0/1 および hsrp Et0/1 2 が並行して処理されます。

テンプレートクラス機能が設定されている場合、プロトコルは、メンテナンスモードを開始するときに、属しているクラスに基づいた順序に従います。通常モードに戻ると、プロトコルは逆の順序に従います。

システム モード メンテナンス カウンタ

GIR には、次のイベントを追跡するカウンタがあります。

- スイッチがメンテナンスに入った回数。
- クライアントごとの Ack 統計情報。
- クライアントごとの Nack 統計情報。
- 特定のクライアントが確認応答しなかった回数。

- GIR 中にスイッチオーバーが発生した回数。GIR インフラは、このカウンタを再同期して複数のスイッチオーバーを追跡する。
- フェールセーフタイマーが期限切れになった回数。
- タイムアウトの期限切れ時にシステムがメンテナンスを終了した回数。

この機能によって追跡されているカウンタを表示するには、特権 EXEC モードで **show system mode maintenance counters** コマンドを入力します。

この機能によってサポートされているカウンタをクリアするには、特権 EXEC モードで**clear system mode maintenance counters**コマンドを入力します。

クライアント応答確認のタイムアウト値は、**failsafe***failsafe-timeout-value* コマンドを使用して設定できます。フェールセーフ時間とは、GIR エンジンがクライアントの移行を許可する時間です。各クライアントは、その移行に関する通知を GIR エンジンに送信します。移行にフェールセーフ時間を超える時間がかかる場合は、移行したと見なされます。フェールセーフタイマーは 5 ー 180 分の範囲で設定でき、デフォルトは 30 分です。

グレースフル挿入と削除の設定方法

メンテナンステンプレートの作成

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**maintenance-template** *template_name* 例： `Device(config)# maintenance-template gir1`	指定した名前でテンプレートを作成します。例については、「例：カスタム プロファイルの作成」を参照してください。
ステップ 4	**router** *routing_protocol instance_id* | **shutdown l2** 例： `Device(config-maintenance-templ)# router isis 1`	このテンプレートに従って分離するインスタンスを作成します。 • **router:** ルーティング プロトコルと関連のインスタンス ID を設定します。

	コマンドまたはアクション	目的
	`Device(config-maintenance-templ)# shutdown l2` `Device(config-maintenance-templ)# router bgp AS-number`	• **shutdown l2:** レイヤ 2 インターフェイスをシャットダウンします。

システム モード メンテナンスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**system mode maintenance** 例： `Device(config)# system mode maintenance`	システム モード メンテナンス設定モードを開始します。 メンテナンス モード パラメータを作成するさまざまなサブコマンドは、このモードで設定します。
ステップ 4	**timeout** *timeout-value* | **template** *template-name* | **failsafe** *failsafe-timeout-value* | **on-reload reset-reason maintenance**	メンテナンス モード パラメータを設定します。 • **timeout:** メンテナンス モードのタイムアウト時間を分単位で設定します。この時間が経過すると、システムは自動的に通常モードに戻ります。デフォルトのタイムアウト値はありません。 • **template:** 指定したテンプレートを使用してメンテナンス モードを設定します。 • **failsafe:**クライアント応答確認のタイムアウト値を設定します。 システムがメンテナンス モードに移行する場合は、そのモードに到達するまで続行されます。メンテナン

	コマンドまたはアクション	目的
		ス モードを終了すると、通常モードになります。 • **on-reload reset-reason maintenance:** システムのリロード時にメンテナンスモードになるようにシステムを設定します。設定されていない場合、システムはリロード時に通常モードになります。

メンテナンス モードの開始と停止

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	**start maintenance** 例： `Device# start maintenance`	システムをメンテナンス モードに移行させます。
ステップ 3	**stop maintenance** 例： `Device# stop maintenance`	システムを通常モードに戻します。

グレースフル挿入と削除のモニタリング

次のコマンドを使用して、GIR機能によって生成された統計情報のステータスを確認したり、統計情報を表示したりします。

表 *1:* 特権 *EXEC* コマンド

コマンド	目的
show system mode [maintenance [clients | template *template-name*]]	システム モードに関する情報を表示します。
show system snapshots [dump *<snapshot-file-name>]*	デバイスに存在するすべてのスナップショットを表示します。

コマンド	目的
show system snapshots [dump *<snapshot-file-name>]***xml**	デバイスに存在するすべてのスナップショットを XML 形式で表示します。
show system snapshots compare *snapshot-name1 snapshot-name2*	メンテナンス モードに移行する前とメンテナンス モードを終了した後に作成したスナップショット間の相違を表示します。

表 *2:* トラブルシューティングするためのグローバル コンフィギュレーション コマンド

コマンド	目的
debug system mode maintenance	GIR 機能をトラブルシューティングに役立つ情報を表示します。

グレースフル削除と挿入の設定例

次に、メンテナンス時に GIR を有効にするために実行した手順の例を示します。

例：メンテナンステンプレートの設定

GIR でサポートされるどのプロトコルも、メンテナンステンプレートで設定できます。この例では、ISIS ルーティング プロトコル インスタンスでメンテナンステンプレート t1 を設定する方法を示します。

```
Device# configure terminal
Device(config)# maintenance-template t1
Device(config-maintenance-templ)# router isis 1
```

次に、shutdown l2 を使用してメンテナンス テンプレート t1 を設定する例を示します。

```
Device# configure terminal
Device(config)# maintenance-template t1
Device(config-maintenance-templ)# shutdown l2
```

次に、BGP ルーティング プロトコル インスタンスを使用してメンテナンステンプレート t1 を設定する例を示します。

```
Device# configure terminal
Device(config)# maintenance-template t1
Device(config-maintenance-templ)# router BGP 1
```

例：システムモードメンテナンスの設定

次に、メンテナンステンプレートを作成し、メンテナンス モード パラメータを設定する例を示します。

```
Device# configure terminal
Device(config)# system mode maintenance
Device(config-maintenance)# timeout 20
Device(config-maintenance)# failsafe 30
Device(config-maintenance)# on-reload reset-reason maintenance
Device(config-maintenance)# template t1
Device(config-maintenance)# exit
```

例：メンテナンスモードの開始と停止

次に、システムをメンテナンス モードに移行する例を示します。

```
Device# start maintenance
```

アクティビティが完了したら、システムをメンテナンス モードから戻すことができます。

次に、システムをメンテナンス モードから戻す例を示します。

```
Device# stop maintenance
```

例：システムモード設定の表示

次に、さまざまなオプションを使用して、システム モード設定を表示する例を示します。

```
Device# show system mode
     System Mode: Normal


Device# show system mode maintenance
     System Mode: Normal
     Current Maintenance Parameters:
     Maintenance Duration: 15(mins)
     Failsafe Timeout: 30(mins)
     Maintenance Template: t1
     Reload in Maintenance: False


Device# show system mode maintenance clients
     System Mode: Normal
     Maintenance Clients:
     CLASS-EGP
     CLASS-IGP
     router isis 1: Transition None
     CLASS-MCAST
     CLASS-L2


Device# show system mode maintenance template default
     System Mode: Normal
     default maintenance-template details:
     router isis 1
     router isis 2


Device# show system mode maintenance template t1
     System Mode: Normal
     Maintenance Template t1 details:
     router isis 1
```

グレースフル挿入と削除に関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*Command Reference (Catalyst 9400 Series Switches)* の「*High Availability*」セクションを参照してください。

グレースフル挿入と削除の機能履歴

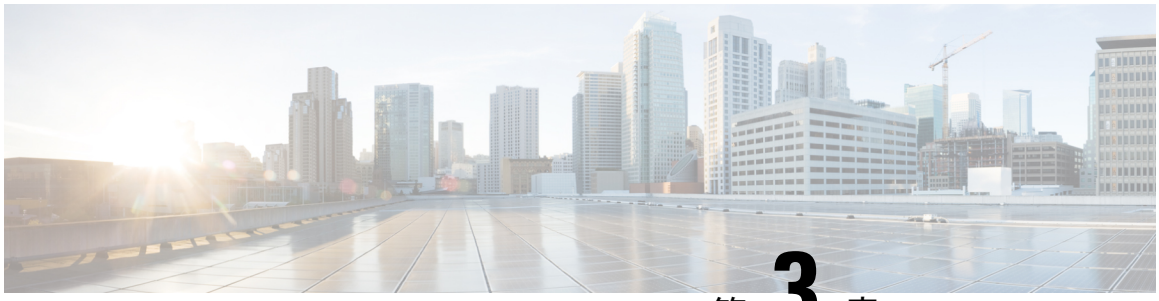
次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.8.1a	グレースフル挿抜	デバイスのメンテナンスによるネットワークサービスへの影響を最小限に抑える代替方法を提供します。GIR では、ネットワーク内の冗長パスを活用して、メンテナンス中のデバイスのスムーズな取り外しと、アウトオブサービス処理を行い、メンテナンスが完了した時点でサービスに戻します。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.9.1	グレースフル挿入と削除（GIR）の機能拡張：スナップショット テンプレート	次の拡張機能が導入されました。 • スナップショット テンプレートを使用して、特定のスナップショットを生成できます。 • 同じカスタムテンプレート内の 1 つのクラスに属するプロトコルは、並行してサービスされます。 • システム モード メンテナンス カウンタが追加されました。スイッチがメンテナンスに入った回数などのイベントの追跡に使用されます。
	GIR Hot Standby Router Protocol（HSRP）向けの GIR レイヤ 2 プロトコルのサポート	GIR は HSRP プロトコルでサポートされるようになりました。
	GIR Virtual Router Redundancy Protocol（VRRP）向けの GIR レイヤ 2 プロトコルのサポート	GIR は VRRPv3 プロトコルでサポートされるようになりました。
Cisco IOS XE Gibraltar 16.10.1	BGP のグレースフル挿入と削除（GIR）サポート	GIR は BGP プロトコルでサポートされるようになりました。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com に進みます。



第 3 章

Cisco StackWise Virtual の設定

Cisco StackWise Virtual の前提条件

- Cisco StackWise Virtual ソリューションのすべてのスイッチは、同じスイッチモデルである必要があります。
- Cisco StackWise Virtual ソリューションのスーパーバイザモジュールは、同じモデルである必要があります。
- 各スイッチのスーパーバイザモジュールは、対称スロットに挿入する必要があります。たとえば、Cisco Catalyst 9407R スイッチでスロット 3 にスーパーバイザモジュールを取り付けた場合は、2 番目のスイッチのスロット 3 にもスーパーバイザモジュールが取り付けられていることを確認します。

  シャーシスロットの制限については、『Cisco Catalyst 9400 Series Supervisor Module Installation Note』を参照してください
- Cisco StackWise Virtual ソリューションのすべてのスイッチは同じレベルのライセンスを実行している必要があります。
- Cisco StackWise Virtual ソリューションのすべてのスイッチは同じソフトウェアバージョンを実行している必要があります。
- Cisco StackWise Virtual ソリューションのすべてのスイッチは同じ SDM テンプレートを実行している必要があります。

- StackWise Virtual リンク（SVL）の設定に使用されるすべてのポートが、同じ速度を共有していること。たとえば、10G または 40G ポートを同時に設定して SVL を形成することはできない。
- ラインカードで SVL およびデュアルアクティブ検出（DAD）リンクを設定する場合は、次の手順を実行することを推奨します。
  - ラインカードで autoLC シャットダウンを有効にします。自動ラインカードシャットダウン機能により、ラインカードの電源優先順位を設定して、電力制限モードで最も優先順位の低いラインカードを自動的にシャットダウンできます。
  - SVL および DAD リンクが設定されているラインカードには、より高い優先順位を設定します。これにより、電力が不十分な状況で、SVL および DAD リンクを備えたラインカードが最後にリロードされます。

グローバルコンフィギュレーションモードで **power supply autoLC** ［ **priority** *physical-slot-number* ］［**shutdown**］コマンドを使用して、autoLC シャットダウンおよびラインカードの電源優先順位を設定できます。

スイッチスタックでは、**power supply switch** *switch-number* **autoLC** ［ **priority** *physical-slot-number* ］［**shutdown**］コマンドを使用します。

Cisco StackWise Virtual の制約事項

- Cisco StackWise Virtual は、Cisco Catalyst 9400 シリーズ スーパーバイザ 1 モジュール（C9400-SUP-1）および Cisco Catalyst 9400 シリーズ スーパーバイザ 1XL モジュール（C9400-SUP-1XL）でサポートされています。この機能には、Cisco Catalyst 9400 シリーズ スーパーバイザ 1 モジュール（C9400-SUP-1）を搭載した特別な追加の C9400-SUP-UPG-LIC= ライセンスが必要です。
- Cisco StackWise Virtual は、シャーシごとに 1 つのスーパーバイザモジュールでのみ設定できます。Cisco StackWise Virtual ソリューションで使用される各シャーシに 2 つのスーパーバイザモジュールを取り付けることができます。ただし、アクティブになるスーパーバイザモジュールは 1 つだけです。他のモジュールの電源はオフになります。
- Cisco StackWise Virtual を展開する場合は、VLAN ID 4094 がネットワーク上のどこでも使用されていないことを確認してください。スタックメンバ間のすべてのシャーシ間システム制御通信は、グローバルな範囲から予約された VLAN ID 4094 で伝送されます。
- 設定変更を有効にするには、デュアルアクティブ検出（DAD）および StackWise Virtual リンク（SVL）の設定を手動で実行し、デバイスを再起動する必要があります。
- Cisco トランシーバモジュールのみがサポートされています。
- デフォルトで割り当てられているインターフェイス VLAN MAC アドレスは、**mac-address** コマンドを使用して上書きできます。このコマンドが、レイヤ 3 のインジェクトされたパケットを必要とする単一の SVI またはルータポートで設定されている場合、デバイス上の他のすべての SVI またはルーテッドポートも、MAC アドレスの最初の 4 つの最上位バイ

ト（4MSB）で設定する必要があります。たとえば、SVI の MAC アドレスを xxxx.yyyy.zzzz に設定する場合、他のすべての SVI の MAC アドレスは xxxx.yyyy で始まるように設定します。レイヤ 3 のインジェクトされたパケットが使用されない場合、この制限は適用されません。

（注） これは、すべてのレイヤ 3 ポート、SVI、およびルーテッドポートに適用されます。これは GigabitEthernet0/0 ポートには適用されません。

- ブロードキャスト、不明なユニキャスト、マルチキャスト（BUM）トラフィックの最適化は、スタンドアロンまたは物理ポートを持つ VLAN には適用されません。

Cisco StackWise Virtual について

Cisco Catalyst 9400 シリーズ スイッチの Cisco StackWise Virtual

このセクションでは、Cisco Catalyst 9400 シリーズ スイッチに固有の Cisco StackWise Virtual の機能について説明します。

- Cisco StackWise Virtual は、Cisco Catalyst 9404R、Cisco Catalyst 9407R、および Catalyst 9410R スイッチでサポートされています。
- Cisco Catalyst 9400 シリーズのスーパーバイザモジュールで SVL および DAD リンクを設定し、イーサネットスイッチングモジュール（ラインカード）を選択できます。SVL 接続は、スーパーバイザモジュールの 10G、40G、または 25G（C9400-SUP-1XL-Y でのみ使用可能）アップリンクポート、およびラインカードの上 10G ダウンリンクポートを介して確立されます。サポートされるスーパーバイザモジュールおよびラインカードの詳細については、次の表を参照してください。

  次の表に、各モジュールの StackWise Virtual 通信メカニズムのマトリックスを示します。

表 *3 :* スーパーバイザモジュールの *StackWise Virtual* の機能マトリックス

製品 ID	StackWise Virtual リンク	デュアルアクティブ検出リンク
スーパーバイザ モジュール		
C9400-SUP-1	サポート対象	サポート対象
C9400-SUP-1XL	サポート対象	サポート対象
C9400-S-BLANK-SUP-1XL-Y	サポート対象	サポート対象

表 *4 :* ラインカードの *StackWise Virtual* の機能マトリックス

製品 ID	StackWise Virtual リンク	デュアルアクティブ検出リンク
ギガビット イーサネット スイッチング モジュール		
C9400-LC-24S	未サポート	サポート対象
C9400-LC-48P	未サポート	サポート対象
C9400-LC-48S	未サポート	サポート対象
C9400-LC-48T	未サポート	サポート対象
C9400-LC-48U	未サポート	サポート対象
10 ギガビット イーサネット スイッチング モジュール		
C9400-LC-24XS	サポート対象	サポート対象
マルチギガビット イーサネット スイッチング モジュール		
C9400-LC-48UX	サポート対象 マルチギガビット（mGig）ポート 25 ー 48	サポート対象

- 25G リンクは、C9400-SUP-1XL-Y のアップリンクポート 1 および 5 を介してのみ確立できます。 25G ポートで SVL または DAD リンクを有効にすると、モジュール上の対応する 10G および 40G ポートは無効になります。たとえば、TwentyFiveGigE1/2/0/1 が SVL ポートとして設定されている場合、TenGigabitEthernet1/2/0/1 から TenGigabitEthernet1/2/0/4 および FortyGigabitEthernet1/2/0/9 は無効になります。同様に 40G ポートの場合、ポート FortyGigabitEthernet1/2/0/9 が SVL ポートとして設定されている場合、ポート TenGigabitEthernet1/2/0/1 から TenGigabitEthernet1/2/0/4 および TwentyFiveGigE1/2/0/1 は無効になります。

  スーパーバイザモジュールでのアップリンクポートの設定の詳細については、『*Interface and Hardware Components Configuration Guide for Catalyst 9400 Switches*』の「Configuring Interface Characteristics」の章の「Uplink Ports」セクションを参照してください。

- Cisco Catalyst 9400 シリーズ スイッチを使用して、Cisco StackWise Virtual ソリューションで最大 8 つの SVL を設定できます。

- SVL は、シャーシあたり最大 80GE（8x10GE または 2x40GE）または 50GE（2x25GE）の組み合わせた帯域幅を持つことができます。

- スタンドアロンシャーシで StackWise Virtual を設定し、スイッチを再起動してスタックを形成すると、インターフェイスの命名規則がデフォルトの 3 タプル（スロット/ベイ/ポート）から 4 タプル（シャーシ/スロット/ベイ/ポート）に変更されます。このタプルには、

インターフェイス名の一部としてのシャーシ識別子が含まれます。たとえば、Gi2/0/1 は Gi1/2/0/1 に変更されます。最初の番号はシャーシ番号を示します。

次に、4 タプルインターフェイスの命名規則の導入による SNMP の変更点について説明します。

- シャーシ 1 および 2 の物理インデックスは、それぞれ 2 および 500 です。
- シャーシ 1 のスロットの物理インデックスは 1000 ー 10000 の範囲であり、シャーシ 2 のスロットは 11000 ー 20000 の範囲です。
- クエリにスロット番号を必要とするすべての MIB オブジェクト識別子（OID）は、フラット番号スペース（1、2、3...20）の物理スロットインデックスを使用します。スロット 1 ー 10 はシャーシ 1、スロット 11 ー 20 はシャーシ 2 を示します。
- **show snmp slot-mapping** コマンドを使用して、シャーシとスロットマッピングを表示します。

スーパーバイザモジュールとラインカード：サポートされる組み合わせ

（注） SVL は、次に示すサポートされる組み合わせの間でのみ形成できます。

- サポートされる組み合わせ 1：同じモデルの任意 2 つの Cisco Catalyst 9400 シリーズ スーパーバイザ モジュール
- サポートされる組み合わせ 2：Cisco Catalyst 9400 シリーズ スーパーバイザ モジュールの 10G アップリンクポート + C9400-LC-24XS
- サポートされる組み合わせ 3：C9400-LC-24XS + C9400-LC-24XS
- サポートされる組み合わせ 4：C9400-LC-48UX + C9400-LC-48UX

（注） サポートされるスーパーバイザモジュールおよびラインカードの詳細については、表 3 : スーパーバイザモジュールの StackWise Virtual の機能マトリックス （27 ページ） を参照してください。

Cisco StackWise Virtual の概要

Cisco StackWise Virtual は、2 台の直接接続されているスイッチを 1 つの仮想スイッチにペアリングするネットワークシステム仮想化技術です。Cisco StackWise Virtual ソリューションのスイッチは、単一のコントロールプレーンと管理プレーンを使用することで業務効率を高めるほか、フォワーディングプレーンの分散によりシステムの帯域幅を拡大し、推奨されるネットワーク設計を使うことで弾力性のあるネットワークの構築を支援します。Cisco StackWise Virtual

により、2 台の直接接続されている物理スイッチはイーサネット接続を使用して、1 台の論理仮想スイッチとして動作できます。

Cisco StackWise Virtual トポロジ

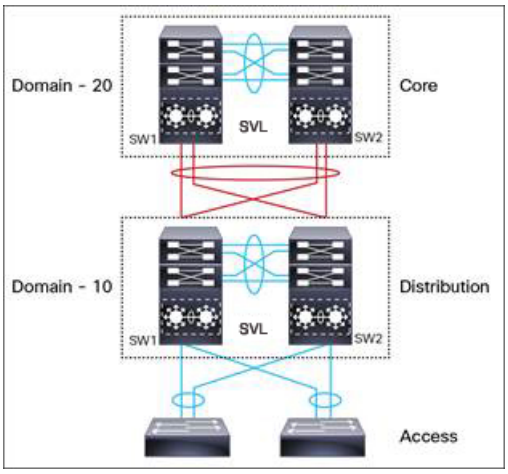
一般的なネットワーク設計は、コア、ディストリビューション、アクセス レイヤで構成されています。スイッチのデフォルト モードはスタンドアロンです。2 台の冗長スイッチをディストリビューション レイヤに展開する場合は、次のネットワークの課題が生じます。

- アクセス レイヤ間で VLAN ID を再使用する場合、ネットワークの全体的なパフォーマンスに影響するスパニング ツリー ループが生じる。
- スパニング ツリー プロトコル ループ、ルートおよびブリッジ プロトコル データ ユニット管理に対してレイヤ 2 ネットワークを保護するには、スパニングツリープロトコルと設定が必要。
- IP ゲートウェイの機能を仮想化するために、First Hop Redundancy Protocol などの追加のプロトコルが必要。これは、各 VLAN の STP ルートのプライオリティに対して整合性を確保する必要がある。
- Protocol Independent Multicast 代表ルータ（PIM DR）設定を最適化し、VLAN 上にマルチキャスト転送トポロジを選択的に構築する必要がある。
- スタンドアロンのディストリビューション レイヤ システムは、プロトコル駆動型のリモート障害検出を提供するため、コンバージェンス時間が遅くなる。FHRP と PIM のタイマーを最適化し、迅速な障害の検出と回復プロセスに対応する必要がある。

アグリゲーションレイヤとコラプスト アグリゲーション レイヤおよびコアレイヤには、Cisco StackWise Virtual モデルが推奨されます。スタックは 25G、40G または 10G リンク上に形成でき、ディストリビューションまたはアグリゲーションスイッチを長距離にわたって展開できます。

STP では、ディストリビューション スイッチに接続されているポートの 1 つをアクセス スイッチ上でブロックし続けます。注意してください。この結果、アクティブ リンクに障害が発生すると STP コンバージェンスを引き起こし、ネットワークにはトラフィックの損失、フラッディング、トランジェント ループの可能性といった問題が生じます。一方、複数のスイッチが論理的に 1 つのスイッチにマージされている場合、ディストリビューション スイッチによりすべてのアクセス スイッチで EtherChannel バンドルを形成できるため、EtherChannel 内にリンク障害が生じても、EtherChannel 内の少なくとも 1 つのメンバーがアクティブであれば影響はありません。

図 *1 : Cisco StackWise Virtual* を使用した一般的なネットワーク設計



StackWise Virtual の EtherChannel は、スタックメンバ間にマルチシャーシ EtherChannel（MEC）を導入できます。アクセス レイヤとアグリゲーション レイヤを 1 つの StackWise Virtual システムに折りたたむと、異なるアクセス レイヤ ドメイン メンバー間およびディストリビューション レイヤとアクセス レイヤのスイッチ間では、MEC がサポートされません。MEC は、ハッシュの結果に関係なく、ローカル リンク上でトラフィックを転送するように設計されています。

コントロール プレーン、管理プレーン、データ プレーンが統合されているため、システムは 1 台のスイッチのように動作します。

複数の物理スイッチの 1 つの論理スイッチへの仮想化は、コントロールと管理プレーンの観点のみに基づきます。コントロール プレーンが共通のため、ピア スイッチに対する 1 つの論理エンティティのように見える場合があります。スイッチのデータプレーンは分散されます。各スイッチは、他のメンバーを使用せずにローカルのインターフェイス上で転送できる能力を備えています。ただし、スイッチに到着するパケットを異なるメンバーのポートから転送する必要がある場合は、入力スイッチで入力処理が実行された後にパケットの転送コンテキストが宛先スイッチに渡されます。出力処理は出力スイッチでのみ実行されます。これにより、宛先ポートがローカル スイッチにあるかリモート スイッチにあるかに関係なく、データ プレーンの動作はスイッチ全体で均一になります。ただし、共通のコントロールプレーンにより、各転送エンティティのデータ プレーン エントリはすべてのスイッチで同等になります。

まら、コントロールプレーン機能の観点から、Cisco StackWise Virtual をアクティブにするスイッチ、Cisco StackWise Virtual をスタンバイにするスイッチを選択する選定メカニズムもあります。アクティブスイッチは、すべての管理、ブリッジングプロトコル、ルーティングプロトコル、およびソフトウェアデータパスを担います。アクティブスイッチがフェールオーバーすると、スタンバイスイッチはアクティブの役割を引き継ぐことができるホットスタンバイ状態になります。

Cisco StackWise Virtual ソリューションのコンポーネントは次の通りです。

- スタック メンバー

- SVL：25G、40G、または10Gイーサネット接続。SVLは、スイッチモデルに応じて25G、40G、または10Gインターフェイスを使用して確立されます。ただし、2つの異なる速度の組み合わせはサポートされていません。

SVLは、イーサネット上でスイッチを接続するリンクです。通常、Cisco StackWise Virtualは複数の25G、40Gまたは10Gの物理リンクで構成されています。スイッチング ユニット間のすべてのコントロール トラフィックとデータ トラフィックの伝送を行います。サポートされるポートでSVLを設定できます。スイッチの電源を入れてハードウェアが初期化されると、コントロールプレーンの初期化の前に、設定されているSVLを探します。

リンク管理プロトコル（LMP）は、リンクが確立されるとすぐにSVLの各リンクでアクティブになります。LMPはリンクの完全性を確保し、リンクの正常性をモニタして維持します。各スイッチの冗長性の役割は、StackWise検出プロトコル（SDP）によって解決されます。ハードウェアとソフトウェアのバージョンにSVLを形成するための互換性があることを確認し、コントロールプレーンの観点からアクティブまたはスタンバイになるスイッチを判別します。

Cisco StackWise Virtual Header（SVH）は64バイトのフレームヘッダーで、Cisco StackWise Virtualドメインの2つのスタックメンバ間で各SVLを通過するコントロール、データ、管理プレーンのすべてのトラフィックに追加されます。SVHカプセル化トラフィックはOSIレイヤ2で動作し、Cisco StackWise Virtualが有効なスイッチでのみ認識および処理できます。SVLインターフェイスはブリッジング不可かつルーティング不可で、L2またはL3ネットワーク上でルーティング不可のトラフィックを許可します。

Cisco StackWise Virtual 冗長性

Cisco StackWise Virtualは、アクティブ スイッチとスタンバイ スイッチ間でステートフル スイッチオーバー（SSO）を行います。以下に示す方法では、Cisco StackWise Virtualの冗長モデルがスタンドアロン モードの冗長モデルと異なります。

- Cisco StackWise Virtualアクティブ スイッチとスタンバイ スイッチは別々のスイッチでホストされ、StackWise Virtualリンクを使用して情報を交換します。
- アクティブ スイッチは、Cisco StackWise Virtualの両方のスイッチを制御します。アクティブ スイッチは、レイヤ2およびレイヤ3の制御プロトコルを実行し、両方のスイッチのスイッチング モジュールを管理します。
- Cisco StackWise Virtualアクティブ スイッチとスタンバイ スイッチは、データ トラフィックの転送を実行します。

（注） Cisco StackWise Virtualアクティブ スイッチに障害が生じた場合、スタンバイ スイッチはスイッチオーバーを開始し、Cisco StackWise Virtualアクティブ スイッチの役割を引き受けます。

SSO 冗長性

StackWise Virtualシステムでは、次の要件を満たしている場合に、SSO冗長性が機能します。

- ソフトウェア アップグレード中である場合を除き、両方のスイッチが同じソフトウェア バージョンを実行していること。
- 2 台のスイッチで、SVL 関連の設定が一致していること。
- ライセンスの種類が、両方のスイッチ モデルで同じであること。
- 両方のスイッチ モデルが同じ StackWise Virtual ドメインにあること。

SSO 冗長性により、StackWise Virtual スタンバイ スイッチは、StackWise Virtual アクティブ スイッチに障害が発生した場合に常に制御を引き受けられるようになっています。設定情報、転送情報、ステート情報は、スタートアップ時や StackWise Virtual アクティブスイッチの設定が変更されたときに、StackWise Virtual アクティブスイッチから冗長スイッチへ同期するようになっています。スイッチオーバー発生時のトラフィックの中断は最小限に抑えられます。

StackWise Virtual が SSO 冗長性の要件を満たしていない場合、ピア スイッチとの関係は確立できません。StackWise Virtual は、StackWise Virtual アクティブ スイッチとスタンバイ スイッチ間でステートフル スイッチオーバー（SSO）を実行します。StackWise Virtual は初期化中に各スイッチの役割を判断します。

StackWise Virtual スタンバイ スイッチの CPU はホット スタンバイ状態で実行されます。StackWise Virtual は、SVL を使用して StackWise Virtual アクティブスイッチから StackWise Virtual スタンバイスイッチに設定データを同期します。また、ハイアベイラビリティをサポートしているプロトコルと機能により、StackWise Virtual スタンバイ スイッチに対してイベントやステート情報が同期されます。

ノンストップ フォワーディング

SSO 冗長モードを使用しているシステムにノンストップ フォワーディング（NSF）技術を導入すると、ネットワークの中断がキャンパスユーザとアプリケーションに対して最小限に抑えられます。高可用性は、コントロール プレーン処理スタックメンバー スイッチがリセットされる場合でも提供されます。下層のレイヤ 3 の障害時には、NSF 対応プロトコルがグレースフル ネットワーク トポロジ再同期を実行します。冗長スタックメンバー スイッチにプリセットされている転送情報はそのまま残るため、このスイッチがネットワーク内でデータ転送を続行します。このサービス可用性により、平均修復時間（MTTR）は大幅に短縮され、平均故障間隔（MTBF）は拡大するため、高いレベルのネットワーク可用性が実現します。

マルチシャーシ EtherChannel

マルチシャーシ EtherChannel（MEC）は、速度やデュプレックスなどの共通の特性を持つ物理ポートがバンドルされた EtherChannel です。それらは、各 Cisco StackWise Virtual システム全体に分散されます。Cisco StackWise Virtual MEC は、EtherChannel をサポートしているネットワーク要素（ホスト、サーバ、ルータ、スイッチなど）に接続できます。Cisco StackWise Virtual は、レイヤ 2 またはレイヤ 3 モードで展開されている最大 128 の MEC をサポートします。EtherChannel 128 は SVL 接続用に予約されています。そのため、使用可能な最大 MEC カウントは 127 です。

Cisco StackWise Virtual システムでは、MEC は追加機能を備えた EtherChannel です。マルチシャーシ EtherChannel リンクは、物理スイッチのローカルポートだけをインデックスポートに追加することで、SVL 経由で伝送を必要とするトラフィックの量を減らします。これにより、スイッチは、マルチシャーシ EtherChannel リンクのローカルポートをリモートスイッチ上のポートよりも優先させることができます。

各 MEC はオプションで、Cisco PAgP、IEEE LACP、または Static ON モードのいずれかをサポートするように設定できます。Cisco PAgP または LACP を使用する EtherChannel と互換性のあるネイバーの実装が推奨されます。Cisco Wireless LAN Controller（WLC）など、リモート接続のネイバーがこのリンクバンドル プロトコルをサポートしていない場合は、Static ON モードを展開できます。これらのプロトコルは、Cisco StackWise Virtual アクティブ スイッチ上でのみ動作します。

MEC は、Cisco StackWise Virtual アクティブ スイッチと Cisco StackWise Virtual スタンバイ スイッチ間に任意の比率で分散させることができる 8 個までの物理リンクをサポートできます。MEC ポートは、両方のスイッチで均等に分散させることをお勧めします。

MEC の最小遅延ロード バランシング

StackWise Virtual 環境は、データ転送が常にスイッチ内で維持されるように設計されています。仮想スタックは常に、ローカルで利用可能なリンク上でトラフィックを転送しようとします。これは、レイヤ 2 とレイヤ 3 の両方のリンクに該当します。ローカル転送の主な目的は、SVL 上で不必要にデータトラフィックが送信されないようにして、遅延（SVL 上の余分なホップ）および輻輳を軽減することです。双方向トラフィックは 2 つの StackWise Virtual メンバ間で負荷分散されます。ただし、各 StackWise Virtual メンバーの入力および出力トラフィックの転送は、MEC の一部であるローカルに接続されているリンクに基づいて使われます。このローカル転送は、StackWise Virtual が有効なキャンパス ネットワークでの収束および障害状態を理解する上で重要な概念です。

アクティブスイッチとスタンバイスイッチは、必要なルックアップを個別に実行し、ローカルリンク上のトラフィックをアップリンクネイバーに転送するローカル転送をサポートしています。接続先が StackWise Virtual ドメイン内のリモートスイッチである場合、入力処理は入力スイッチで実行され、トラフィックは SVL を介して出力処理だけが実行される出力スイッチに転送されます。

MEC 障害シナリオ

次のセクションでは、発生する可能性のある問題と結果の影響について説明します。

単一 MEC リンクの障害

MEC 内のリンクに障害が発生した（そして MEC 内の別のリンクは動作している）場合、通常のポートと同様に、MEC は動作しているリンク間でロード バランシングを再調整します。

Cisco StackWise Virtual アクティブ スイッチへのすべての MEC リンクの障害

Cisco StackWise Virtual アクティブ スイッチへのすべてのリンクに障害が発生した場合、MEC が Cisco StackWise Virtual スタンバイ スイッチへの動作可能なリンクを持つ通常の EtherChannel になります。

Cisco StackWise Virtual アクティブスイッチで終了するデータトラフィックは、Cisco StackWise Virtual スタンバイスイッチまで SVL を通って MEC に到達します。制御プロトコルは、Cisco StackWise Virtual アクティブ スイッチで動作を続行します。プロトコルメッセージは、SVL を通って MEC に到達します。

すべての MEC リンクの障害

MEC 内のすべてのリンクに障害が発生した場合、EtherChannel の論理インターフェイスは Unavailable に設定されます。レイヤ 2 制御プロトコルは、通常の EtherChannel のリンク ダウン イベントと同様の修正措置を実行します。

隣接スイッチでは、ルーティングプロトコルとスパニングツリープロトコル（STP）により、通常の EtherChannel と同様の修正措置が実行されます。

Cisco StackWise Virtual スタンバイ スイッチの障害

Cisco StackWise Virtual スタンバイ スイッチに障害が発生した場合、MEC が、Cisco StackWise Virtual アクティブ スイッチで動作可能なリンクを持つ通常の EtherChannel として機能します。接続されているピアスイッチにより、リンクの障害が検出され、StackWise Virtual アクティブ スイッチへのリンクだけを使用するようにロードバランシングアルゴリズムが調整されます。

Cisco StackWise Virtual アクティブ スイッチの障害

Cisco StackWise Virtual アクティブ スイッチに障害が発生すると、ステートフル スイッチオーバー（SSO）が実行されます。スイッチオーバーの完了後、MEC は新しい Cisco StackWise Virtual アクティブ スイッチで動作可能になります。接続されているピア スイッチにより、（障害となったスイッチへの）リンクの障害が検出され、新しい Cisco StackWise Virtual アクティブ スイッチへのリンクだけを使用するようにロード バランシング アルゴリズムが調整されます。

Cisco StackWise Virtual のパケット処理

Cisco StackWise Virtual では、Cisco StackWise Virtual アクティブ スイッチがレイヤ 2 およびレイヤ 3 のプロトコルと機能を実行し、両方のスイッチ上のポートを管理します。

Cisco StackWise Virtual は、StackWise Virtual リンクを使用してピア スイッチ間でシステムおよびプロトコル情報を通信し、2 台のスイッチ間でデータ トラフィックを伝送します。

ここでは、Cisco StackWise Virtual でのパケット処理について説明します。

StackWise Virtual リンク上のトラフィック

SVL では、2 台のスイッチ間のデータトラフィックとインバンド制御トラフィックが送信されます。SVL を介して転送されるすべてのフレームは、特殊な StackWise Virtual ヘッダー（SVH）でカプセル化されます。SVH は、制御トラフィックとデータ トラフィックで 64 バイトのオーバーヘッドを追加し、これによりピア スイッチでパケットを転送するための情報を Cisco StackWise Virtual に渡します。

SVL は、2 台のスイッチの間で制御メッセージを送信します。メッセージには、Cisco StackWise Virtual アクティブ スイッチが処理し、Cisco StackWise Virtual スタンバイ スイッチのインターフェイスが受信または送信するプロトコルメッセージが含まれます。制御トラフィックには、Cisco StackWise Virtual アクティブ スイッチと Cisco StackWise Virtual スタンバイ スイッチ上のスイッチング モジュール間のモジュール プログラミングも含まれます。

Cisco StackWise Virtual は、以下の状況下で、SVL を介してデータトラフィックを送信します。

- VLAN 上でレイヤ 2 トラフィックのフラッディングが発生しているとき（デュアル ホーム リンクの場合でも）
- Cisco StackWise Virtual アクティブ スイッチ上のソフトウェアでパケットが処理されるが、入力インターフェイスは Cisco StackWise Virtual スタンバイ スイッチ上にあるとき
- 次のように、パケットの宛先がピア スイッチ上にあるとき
  - 既知の宛先インターフェイスがピア スイッチ上にある VLAN 内のトラフィック
  - マルチキャスト グループおよびマルチキャスト レシーバのために複製されたトラフィックがピア スイッチ上にある場合
  - 既知のユニキャスト宛先 MAC アドレスがピア スイッチ上にある場合
  - パケットが、ピア スイッチ上のポートを宛先とする MAC 通知フレームである場合

また、SVL は、NetFlow エクスポートデータや SNMP データなどのシステムデータを Cisco StackWise Virtual スタンバイスイッチから Cisco StackWise Virtual アクティブスイッチに転送します。

SVL のトラフィックは、EtherChannel で利用できるのと同じグローバル ハッシュ アルゴリズム（デフォルトのアルゴリズムは送信元/宛先 IP）に基づいてロードバランシングされます。

Layer 2 Protocols

Cisco StackWise Virtual アクティブ スイッチは、両方のスイッチでレイヤ 2 プロトコル（STP や VTP など）を実行してスイッチング モジュールを管理します。スタンバイスイッチポートで受信されたプロトコルメッセージは、SVL を通過して処理されるアクティブスイッチに到達する必要があります。同様に、スタンバイスイッチポートから送信されるプロトコルメッセージは、アクティブスイッチで発信され、SVL を通過してスタンバイポートに到達します。

Cisco StackWise Virtual のすべてのレイヤ 2 プロトコルは、スタンドアロン モードで同じように動作します。ここでは、Cisco StackWise Virtual の一部のプロトコルについて、動作の違いを説明します。

スパニングツリー プロトコル

Cisco StackWise Virtual アクティブ スイッチでは、STP を実行します。Cisco StackWise Virtual スタンバイスイッチは、SVL 経由で STP BPDU を StackWise Virtual アクティブスイッチにリダイレクトします。

通常、STP ブリッジ ID はスイッチの MAC アドレスから導出されます。スイッチオーバー後もブリッジ ID が変わらないように、Cisco StackWise Virtual は元のスイッチの MAC アドレスを STP ブリッジ ID として使い続けます。

EtherChannel 制御プロトコル

Link Aggregation Control Protocol（LACP）パケットとポート集約プロトコル（PAgP）パケットには、デバイス ID が組み込まれます。Cisco StackWise Virtual は、両方のスイッチに共通のデバイス ID を定義します。3 つのモードがすべてサポートされている場合でも、Multi EtherChannels ではモード ON ではなく PAgP または LACP のいずれかを使用します。

（注） デュアル アクティブ シナリオ検出をサポートするため、新しい PAgP 拡張が定義されています。

スイッチド ポート アナライザ

SVL および fast hello DAD リンクポートでは Switched Port Analyzer（SPAN; スイッチドポートアナライザ）はサポートされていません。これらのポートを SPAN 送信元または SPAN 宛先にすることはできません。Cisco StackWise Virtual は、非 SVL インターフェイスに対してすべての SPAN 機能をサポートします。Cisco StackWise Virtual で利用可能な SPAN セッションの数は、スタンドアロン モードで動作する単一のスイッチのものと同じです。

プライベート VLAN

StackWise Virtual 上のプライベート VLAN は、スタンドアロンモードの場合と同じように動作します。唯一の例外は、独立トランク ポートのネイティブ VLAN を明示的に設定する必要があることです。

STP、EtherChannel 制御プロトコル、SPAN、およびプライベート VLAN 以外に、SVL 接続上で実行される追加のレイヤ 2 コントロール プレーン プロトコルには Dynamic Trunking Protocol（DTP）、Cisco Discovery Protocol（CDP）、VLAN Trunk Protocol（VTP）、Unidirectional Link Detection Protocol（UDLD）があります。

ブロードキャスト、未知のユニキャスト、マルチキャスト

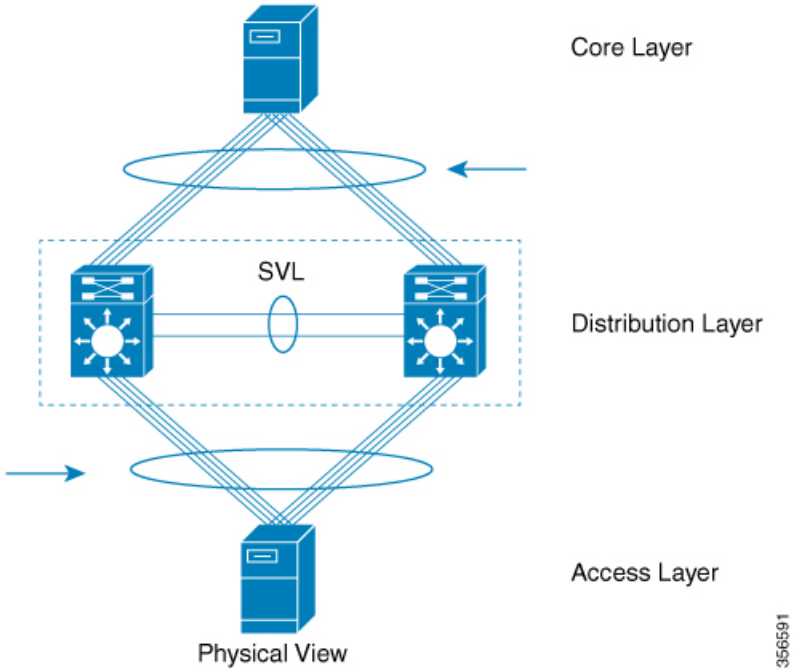
Cisco StackWise Virtual は、ブロードキャスト、未知のユニキャスト、マルチキャスト（BUM）のトラフィックのローカルスイッチングをサポートします。まれな展開シナリオでは、BUM トラフィックは StackWise Virtual リンクを通過します。このセクションでは、Cisco StackWise Virtual のセットアップとローカルスイッチングで BUM トラフィックを処理する方法を説明します。

VLAN が作成されると、StackWise Virtual ポートが VLAN フラッディングリストに追加されます。アクティブスイッチまたはスタンバイスイッチ上の入力 BUM トラフィックは、VLAN 内のポートではなく、他のスイッチへの StackWise Virtual リンクを通過します。このトラフィックは、StackWise Virtual リンクをフラッディングさせ、システムとネットワークのパフォーマンスに影響を与えます。

これに対処するために、StackWise Virtual BUM 最適化機能が導入されました。

Cisco StackWise Virtual の一般的な展開ガイドラインは、図に示すように、アップリンクとダウンリンクで MEC ポートを均等に分散することです。このトポロジでは、BUM トラフィックは、StackWise Virtual リンクではなく、MEC 上のローカルリンクを優先してトラフィックを送信します。スイッチにスタンドアロンポートがある場合、またはアクティブスイッチもしくはスタンバイスイッチの EtherChannel のメンバがダウンしている場合、BUM トラフィックは StackWise Virtual リンクを通過します。VLAN で StackWise Virtual BUM の最適化が有効になっている場合、StackWise Virtual ポートは VLAN フラッディングリストに追加されません。この設計では、MEC ポートチャネルが VLAN の一部である場合にのみ、BUM トラフィックが StackWise Virtual リンクを通過しないようにしています。スタンドアロンポートまたは物理ポートを使用する VLAN の最適化は行われません。

図 *2 : Cisco StackWise Virtual* の推奨トポロジ



Layer 3 Protocols

Cisco StackWise Virtual アクティブスイッチは、StackWise Virtual で使用するレイヤ 3 プロトコルと機能を実行します。すべてのレイヤ 3 プロトコル パケットは、Cisco StackWise Virtual アクティブ スイッチに送信されて処理されます。両方のメンバー スイッチは、それぞれのイン

ターフェイスで入力トラフィックのハードウェア転送を行います。ソフトウェア転送が必要な場合、パケットは Cisco StackWise Virtual アクティブ スイッチに送信されて処理されます。

Cisco StackWise Virtual アクティブ スイッチが割り当てた同じルータ MAC アドレスが、両方の Cisco StackWise Virtual メンバー スイッチのすべてのレイヤ 3 インターフェイスに使用されます。スイッチオーバー後も、元のルータ MAC アドレスが使用されます。ルータの MAC アドレスは、シャーシ MAC に基づいて選択され、スイッチオーバー後にデフォルトで保持されます。

次のセクションでは、Cisco StackWise Virtual のレイヤ 3 プロトコルについて説明します。

IPv4 ユニキャスト

Cisco StackWise Virtual アクティブ スイッチの CPU は、IPv4 ルーティング プロトコルを実行し、必要なソフトウェア転送を行います。Cisco StackWise Virtual スタンバイ スイッチで受信したすべてのルーティング プロトコル パケットは、SVL 経由で Cisco StackWise Virtual アクティブ スイッチにリダイレクトされます。Cisco StackWise Virtual アクティブ スイッチは、いずれかの Cisco StackWise Virtual メンバー スイッチのポートで送信するすべてのルーティング プロトコル パケットを生成します。

ハードウェア転送は、Cisco StackWise Virtual の両方のメンバー間で分配されます。Cisco StackWise Virtual アクティブ スイッチの CPU は、Cisco StackWise Virtual スタンバイ スイッチに転送情報ベース（FIB）のアップデートを送信し、その結果すべてのルートおよび隣接関係がハードウェアにインストールされます。

ローカル隣接（ローカル ポートから到達可能）に送信されるパケットは、入力スイッチでローカルに転送されます。リモート隣接（リモートポートから到達可能）に送信されるパケットは、SVL を通過する必要があります。

Cisco StackWise Virtual アクティブ スイッチの CPU は、すべてのソフトウェア転送と機能の処理を実行します（フラグメンテーションやパケット存続時間超過機能など）。スイッチオーバーが発生すると、新しい Cisco StackWise Virtual アクティブ スイッチが最新の Cisco Express Forwarding 情報やその他の転送情報を取得するまで、ソフトウェア転送は中断します。

仮想スイッチ モードで Non-Stop Forwarding（NSF）をサポートするための要件は、スタンドアロン冗長動作モードと同じです。

ルーティング ピアの観点からは、マルチシャーシ EtherChannel（MEC）はスイッチオーバー中も動作可能です（故障したスイッチへのリンクがダウンしているだけで、ルーティングの隣接部分は有効）。

Cisco StackWise Virtual は、転送情報ベースのエントリにあるすべてのパスについて、それがローカルでもリモートでも、レイヤ 3 でロード バランシングを実行します。

IPv6

Cisco StackWise Virtual は、スタンドアロン システムに存在するため、IPv6 のユニキャストとマルチキャストをサポートします。

IPv4 マルチキャスト

IPv4 マルチキャスト プロトコルは Cisco StackWise Virtual アクティブ スイッチで実行されます。Cisco StackWise Virtual スタンバイ スイッチで受信する Internet Group Management Protocol（IGMP）と Protocol Independent Multicast（PIM）プロトコルパケットは、SVL 経由で StackWise Virtual アクティブスイッチに送信されます。StackWise Virtual アクティブ スイッチは、いずれかの Cisco StackWise Virtual メンバーのポートで送信する IGM および PIM プロトコル パケットを生成します。

Cisco StackWise Virtual アクティブ スイッチは、マルチキャスト転送情報ベース（MFIB）の状態を Cisco StackWise Virtual スタンバイ スイッチに同期します。両方のメンバー スイッチ上で、すべてのマルチキャストルートが、ローカル発信インターフェイス用にのみプログラムされているレプリケーション拡張テーブル（RET）エントリと共にハードウェアにロードされます。両方のメンバー スイッチがハードウェア転送を行うことができます。

（注） スイッチオーバーによってマルチキャストルートが変更されるのを避けるために、マルチキャスト トラフィックを伝送するすべてのリンクは Equal Cost Multipath（ECMP）ではなく MEC として設定することを推奨します。

SVL を通過するパケットのために、すべてのレイヤ 3 マルチキャストの複製が出力スイッチで行われます。出力スイッチに複数のレシーバがある場合、1 パケットだけが複製され、SVL に転送されてから、すべてのローカル出力ポートに複製されます。

ソフトウェア機能

ソフトウェア機能は、Cisco StackWise Virtual アクティブ スイッチでのみ実行されます。ソフトウェア処理が必要な Cisco StackWise Virtual スタンバイスイッチへの着信パケットは、SVL 経由で Cisco StackWise Virtual アクティブスイッチに送信されます。

デュアル アクティブ検出

スタンバイスイッチが SVL の完全な損失を検出すると、アクティブスイッチに障害が発生したと見なし、アクティブスイッチを引き継ぎます。ただし、元の Cisco StackWise Virtual アクティブスイッチが稼動したままの場合、両方のスイッチが Cisco StackWise Virtual アクティブスイッチになります。この状況を、デュアル アクティブ シナリオと呼びます。このシナリオでは、両方のスイッチで同じ IP アドレス、SSH キー、および STP ブリッジ ID が使用されるため、ネットワークの安定性に悪影響を及ぼすことがあります。Cisco StackWise Virtual はデュアルアクティブ シナリオを検出し、リカバリ アクションを実行します。DAD リンクは、これを軽減するために使用される専用リンクです。

使用可能な最後の SVL に障害が生じた場合、Cisco StackWise Virtual スタンバイスイッチは、Cisco StackWise Virtual アクティブスイッチのステートを判断できません。遅延なくネットワークアップタイムを確保するために、Cisco StackWise Virtual スタンバイスイッチは Cisco StackWise Virtual のアクティブロールを引き継ぎます。元の Cisco StackWise Virtual アクティブスイッチ

はリカバリモードを開始し、SVL と管理インターフェイスを除くすべてのインターフェイスがダウンします。

fast hello デュアル アクティブ検出リンク

dual-active fast hello パケット検出方式を使用するには、2 台の Cisco StackWise Virtual スイッチ間に直接イーサネット接続をプロビジョニングする必要があります。最大4つのリンクをこの目的に使用できます。

2 台のスイッチは、スイッチ ステートに関する情報が記述された特殊な dual-active hello メッセージを定期的に交換します。すべての SVL が失敗してデュアルアクティブシナリオが生じると、各スイッチは、ピアのメッセージからデュアルアクティブシナリオが生じていることを認識します。これにより、リカバリ アクション （42 ページ）セクションで説明するようにリカバリ アクションが開始されます。タイマーの期限が満了するまでに、予想していた dual-active fast hello メッセージをピアから受信しなかった場合、スイッチはリンクがデュアル アクティブ検出を実行できる状態にないと見なします。

（注） SVL と DAD リンクに同じポートを使用しないでください。

拡張 PAgP デュアル アクティブ検出

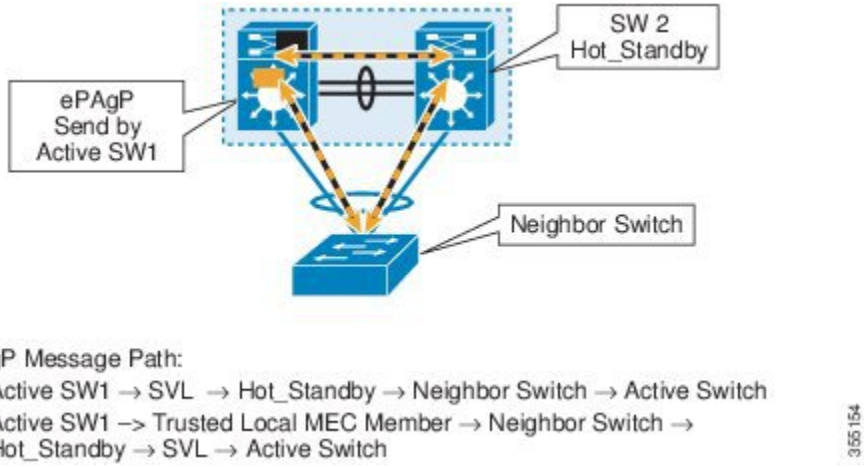
ポート集約プロトコル（PAgP）は、EtherChannel を管理するために使用するシスコ独自のプロトコルです。StackWise Virtual MEC が Cisco スイッチで終端する場合、MEC で PAgP プロトコルを実行できます。PAgP が StackWise Virtual スイッチとアップストリームまたはダウンストリームのスイッチの間の MEC 上で実行されている場合、StackWise Virtual は PAgP を使用してデュアルアクティブシナリオを検出できます。MEC は、StackWise Virtual がセットアップされている各スイッチに少なくとも 1 つのポートを持っている必要があります。

拡張 PAgP は PAgP プロトコルの拡張版です。仮想スイッチ モードでは、ePAgP メッセージに、StackWise Virtual アクティブ スイッチの ID を含む新しい Type Length Value（TLV）が記述されます。新しい TLV を送信するのは、仮想スイッチ モードのスイッチだけです。

StackWise Virtual スタンバイ スイッチは、SVL 障害を検出すると SSO を開始し、StackWise Virtual アクティブ スイッチになります。それ以降、新しくアクティブになった StackWise Virtual スイッチから接続先スイッチに送信される ePAgP メッセージには、新しい StackWise Virtual アクティブ ID が記述されます。接続先スイッチは、新しい StackWise Virtual アクティブ ID が記述された ePAgP メッセージを、両方の StackWise Virtual スイッチに送信します。

前にアクティブだった StackWise Virtual スイッチが動作可能なままの場合は、ePAgP メッセージ内の StackWise Virtual アクティブ ID が変更されているため、デュアル アクティブ シナリオが検出されます。

図 *3 : ePAgP* デュアル アクティブ検出



（注） PAgP フラップを回避し、デュアルアクティブ検出機能が予期どおりに機能するようにするには、コマンドを使用してスタック MAC 永続待機タイマーを無期限に設定する必要があります。 **stack-mac persistent timer 0 .**

リカバリ アクション

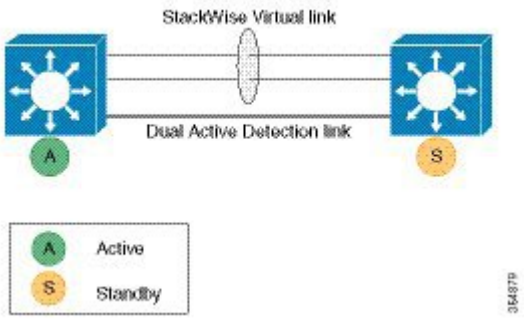
Cisco StackWise Virtual アクティブスイッチは、デュアルアクティブ状態を検出すると、SVL 以外または DAD 以外のすべてのインターフェイスをシャットダウンし、ネットワークから自身を削除します。スイッチは、SVL が回復するまで、リカバリモードで待機します。SVL 障害を物理的に修復する必要があります。スイッチは自動的にリロードされ、スタンバイスイッチとして復元されます。SVL リンクの復元後、スイッチをリカバリモードのままにするには、リカバリによるリロードの無効化 （50 ページ）セクションを参照してください。

Cisco StackWise Virtual の実装

Cisco StackWise Virtual の 2 ノード ソリューションは、通常、アグリゲーション レイヤに展開します。2 つのスイッチを SVL で接続します。

Cisco StackWise Virtual は、2 台のスイッチを多数のポートを備えた 1 つの論理スイッチへと結合し、シングルポイント管理を行えるようにします。メンバスイッチの 1 台がアクティブになりコントロールと管理のプレーンとして動作し、もう一方のスイッチはスタンバイになります。複数の物理スイッチの 1 つの論理スイッチへの仮想化は、コントロールと管理の観点のみに基づきます。コントロール プレーンが共通のため、ピア スイッチに対する 1 つの論理エンティティのように見える場合があります。スイッチのデータ プレーンは集約されており、各スイッチの転送コンテキストは、スイッチ間でトラフィックが転送されるときに、さらに処理するために他のメンバー スイッチに渡されます。ただし、共通のコントロールプレーンにより、各転送エンティティのデータ プレーン エントリはすべてのスイッチで同等になります。

図 *4:2* ノード ソリューション



どのスイッチで Cisco StackWise Virtual をアクティブにし、どのスイッチをコントロールプレーンのスタンバイにするかを決定する選定メカニズムを使用できます。アクティブ スイッチは、管理、ブリッジング プロトコル、ルーティング プロトコル、およびソフトウェア データ パスを担います。これらは、Cisco StackWise Virtual アクティブ スイッチのアクティブなスイッチ スーパーバイザで集中管理されます。

Cisco StackWise Virtual の設定方法

Cisco StackWise Virtual 設定の構成

StackWise Virtual を有効にするには、 次の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device>enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**switch** *switch-number* **renumber** *new switch -number* 例： `Device#switch 1 renumber 2`	（任意）スイッチ番号を再割り当てします。 デフォルトのスイッチ番号は 1 です。新しいスイッチ番号の有効値は 1 および 2 です。
ステップ 3	**switch** *switch-number* **priority** *priority-number* 例：	（任意）優先順位番号を割り当てます。 デフォルトのプ優先順位番号は 1 です。最も高い優先順位番号は 15 です。

	コマンドまたはアクション	目的
	`Device#switch 1 priority 5`	
ステップ 4	**configure terminal** 例： `Device#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 5	**stackwise-virtual** 例： `Device(config)#stackwise-virtual`	Cisco StackWise Virtual を有効にして、StackWise Virtual サブモードを開始します。
ステップ 6	**domain** *id* 例： `Device(config-stackwise-virtual)#domain 2`	（任意）Cisco StackWise Virtual ドメイン ID を指定します。 ドメイン ID の範囲は 1 ～ 255 です。デフォルト値は 1 です。
ステップ 7	**end** 例： `Device(config-stackwise-virtual)#end`	特権 EXEC モードに戻ります。
ステップ 8	**show stackwise-virtual** 例： `Device#show stackwise-virtual`	
ステップ 9	**write memory** 例： `Device#write memory`	システム RAM にある実行コンフィギュレーションを保存し、ROMmon 変数を更新します。変更を保存しないと、スイッチのリロード時に変更がスタートアップ コンフィギュレーションに含まれなくなります。**stackwise-virtual** および **domain** の設定は、リロード後に実行コンフィギュレーションおよびスタートアップ コンフィギュレーションに保存されることに注意してください。
ステップ 10	**reload** 例： `Device#reload`	スイッチを再起動し、スタックを形成します。

Cisco StackWise Virtual リンクの設定

（注） SVL は、サポートされるスイッチモデルのすべての 10G、40G、および 25G インターフェイスでサポートされます。ただし、異なるインターフェイス速度の組み合わせはサポートされていません。

スイッチポートを SVL ポートとして設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device>enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device#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	**interface** { **TenGigabitEthernet** | **FortyGigabitEthernet** | **TwentyFiveGigE** } <*interface*> 例： `Device(config)#interface TenGigabitEthernet1/2/0/4`	イーサネット インターフェイス 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	**stackwise-virtual link** *link value* 例： `Device(config-if)#stackwise-virtual link 1`	インターフェイスを設定された SVL に関連付けます。
ステップ 5	**end** 例： `Device(config-if)#end`	特権 EXEC モードに戻ります。
ステップ 6	**write memory** 例： `Device#write memory`	システム RAM にある実行コンフィギュレーションを保存し、ROMmon 変数を更新します。変更を保存しないと、スイッチのリロード時に変更がスタートアップ コンフィギュレーションに含まれなくなります。**stackwise-virtual link**

	コマンドまたはアクション	目的
		リンク値の設定は、スタートアップ コンフィギュレーションではなく、実行コンフィギュレーションにのみ保存されることに注意してください。
ステップ 7	**reload** 例： `Device#reload`	スイッチを再起動します。

BUM トラフィック最適化の設定

グローバル BUM トラフィック最適化を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device>enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device#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	**svl l2bum optimization** 例： `Device(config)#svl l2bum optimization`	StackWise Virtual セットアップ内の BUM トラフィックの最適化をグローバルに有効にします。この機能は、デフォルトでイネーブルにされています。 この機能を無効化するには、このコマンドの **no** 形式を使用します。
ステップ 4	**end** 例： `Device(config-if)#end`	特権 EXEC モードに戻ります。
ステップ 5	**show platform pm l2bum-status vlan** *vlan-id* 例： `Device# show platform pm l2bum-status vlan 1`	VLAN の転送ポート数（転送ステートの物理ポート数）を表示します。

	コマンドまたはアクション	目的
ステップ 6	**show platform software fed switch ac fss bum-opt summary** 例： `Device# show platform software fed switch ac fss bum-opt summary`	最適化の最終ステートを表示します。

StackWise Virtual Fast Hello デュアルアクティブ検出リンクの設定

StackWise Virtual Fast Hello DAD リンクを設定するには、次の手順を実行します。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device>enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device#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	**interface** { **TenGigabitEthernet** | **FortyGigabitEthernet** | **TwentyFiveGigE** } <*interface*> 例： `Device(config)#interface TenGigabitEthernet1/2/0/5`	イーサネット インターフェイス 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	**stackwise-virtual dual-active-detection** 例： `Device(config-if)#stackwise-virtual dual-active-detection`	インターフェイスを StackWise Virtual デュアル アクティブ検出に関連付けます。 （注） このコマンドは、設定後はデバイス上に表示されませんが、機能し続けます。
ステップ 5	**end** 例： `Device(config-if)#end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**write memory** 例： `Device#write memory`	システム RAM にある実行コンフィギュレーションを保存し、ROMmon 変数を更新します。変更を保存しないと、スイッチのリロード時に変更がスタートアップ コンフィギュレーションに含まれなくなります。**stackwise-virtual dual-active-detection** の設定は、実行コンフィギュレーションにのみ保存され、スタートアップ コンフィギュレーションには保存されないことに注意してください。
ステップ 7	**reload** 例： `Device#reload`	スイッチを再起動し、設定を有効にします。

ePAgP デュアル アクティブ検出の有効化

ePAgP デュアルアクティブ検出をスイッチポートで有効にするには、次の手順を実行します。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device>enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device#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	**interface** { **TenGigabitEthernet** | **FortyGigabitEthernet** | **TwentyFiveGigE** } *interface* 例： `Device(config)#interface TenGigabitEthernet1/2/0/3`	イーサネット インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**channel-group** *group_ID* **mode desirable** 例： `Device(config-if)#channel-group 1 mode desirable`	10 ギガビットイーサネット インターフェイスに対して、1 ～ 128 の範囲のチャネルグループ ID を使用して PAgP MEC を有効にします。
ステップ 5	**exit** 例： `Device(config-if)#exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 6	**interface port-channel** *channel-group-id* 例： `Device(config)#interface port-channel 1`	設定するポートチャネルインターフェイスを選択します。
ステップ 7	**shutdown** 例： `Device(config-if)#shutdown`	インターフェイスをシャットダウンします。
ステップ 8	**exit** 例： `Device(config-if)#exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 9	**stackwise-virtual** 例： `Device(config)#stackwise-virtual`	StackWise Virtual コンフィギュレーション モードを開始します。
ステップ 10	**dual-active detection pagp** 例： `Device(config-stackwise-virtual)#dual-active detection pagp`	pagpデュアルアクティブ検出を有効にします。この設定はデフォルトで有効になっています。
ステップ 11	**dual-active detection pagp trust channel-group** *channel-group id* 例： `Device(config-stackwise-virtual)#dual-active detection pagp trust channel-group 1`	設定した ID のチャネルグループで、デュアルアクティブ検出トラストモードを有効にします。
ステップ 12	**exit** 例： `Device(config-stackwise-virtual)#exit`	StackWise Virtual コンフィギュレーション モードを終了します。
ステップ 13	**interface port-channel** *portchannel* 例：	スイッチにポートチャネルが設定されます。

	コマンドまたはアクション	目的
	`Device(config)#interface port-channel 1`	
ステップ 14	**no shutdown** 例： `Device(config-if)#no shutdown`	スイッチに設定されているポートチャネルを有効にします。
ステップ 15	**end** 例： `Device(config-if)#end`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 16	**write memory** 例： `Device#write memory`	システムRAMにある実行コンフィギュレーションを保存し、ROMmon変数を更新します。変更を保存しないと、スイッチのリロード時に変更がスタートアップコンフィギュレーションに含まれなくなります。**dual-active detection pagp trust channel-group** *channel-group id* の設定は、リロード後に実行コンフィギュレーションとスタートアップコンフィギュレーションに保存されることに注意してください。
ステップ 17	**reload** 例： `Device#reload`	スイッチを再起動し、設定を有効にします。

リカバリによるリロードの無効化

StackWise Virtual リンクの障害から回復した後、リカバリモードのスイッチは、、スイッチを自動的にリロードすることでリカバリアクションを実行します。。これは、リンク障害が発生した場合のデフォルトの動作です。スイッチをリカバリモードに維持し、スイッチが自動的にリロードしないようにするには、次のステップを実行する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device>enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device#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	**stackwise-virtual** 例： `Device(config)#stackwise-virtual`	Cisco StackWise Virtual を有効にして、StackWise Virtual モードを開始します。
ステップ 4	**dual-active recovery-reload-disable** 例： `Device(config-stackwise-virtual)#dual-active recovery-reload-disable`	スイッチの自動リカバリによるリロードを無効にします。 **dual-active recovery-reload-disable** の設定は、実行コンフィギュレーションにのみ保存され、スタートアップ コンフィギュレーションには保存されないことに注意してください。
ステップ 5	**end** 例： `Device(config-stackwise-virtual)#end`	特権 EXEC モードに戻ります。

Cisco StackWise Virtual の無効化

スイッチ上の Cisco StackWise Virtual を無効にするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device>enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device#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。

	コマンドまたはアクション	目的
ステップ 3	**interface** { **TenGigabitEthernet** | **FortyGigabitEthernet** | **TwentyFiveGigE** } *<interface>* 例： `Device(config)#interface TenGigabitEthernet 1/2/0/3`	インターフェイス 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	**no stackwise-virtual dual-active-detection** 例： `Device(config-if)#no stackwise-virtual dual-active-detection`	StackWise Virtual DAD からインターフェイスの関連付けを解除します。
ステップ 5	ステップ ステップ 3 （52 ページ） を繰り返します。 例： `Device(config)#interface TenGigabitEthernet 1/2/0/2`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**no stackwise-virtual link** *link* 例： `Device(config-if)#no stackwise-virtual link 1`	SVL からインターフェイスの関連付けを解除します。
ステップ 7	**exit** 例： `Device(config-if)#exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 8	**no stackwise-virtual** 例： `Device(config)#no stackwise-virtual`	StackWise Virtual の設定を無効にします。
ステップ 9	**exit** 例： `Device(config)#exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 10	**write memory** 例： `Device#write memory`	実行コンフィギュレーションを保存します。
ステップ 11	**reload** 例： `Device#reload`	スイッチを再起動し、設定を有効にします。

StackWise Virtual の設定例

ここでは、次の設定例について説明します。

例：StackWise Virtual リンクの設定

次に、スイッチで SVL を設定するための設定例を示します。

スイッチ 1：

```
Device>enable
Device#configure terminal
Device(config)#interface TenGigabitEthernet1/0/1
Device(config-if)#stackwise-virtual link 1

WARNING: All the extraneous configurations will be removed for TenGigabitEthernet1/0/1
on reboot
INFO: Upon reboot, the config will be part of running config but not part of start up
config.
Device(config-if)#end
Device#write memory
Device#reload
```

スイッチ 2：

```
Device>enable
Device#configure terminal
Device(config)#interface TenGigabitEthernet1/0/1
Device(config-if)#stackwise-virtual link 1

WARNING: All the extraneous configurations will be removed for TenGigabitEthernet1/0/1
on reboot
INFO: Upon reboot, the config will be part of running config but not part of start up
config.
Device(config-if)#end
Device#write memory
Device#reload
```

例：StackWise Virtual Fast Hello デュアルアクティブ検出リンクの設定

次に、スイッチ 1 およびスイッチ 2 での StackWise Virtual Fast Hello デュアルアクティブ検出リンクの設定例を示します。StackWise Virtual リンクポートとしてすでに設定されているポートでは、StackWise Virtual Fast Hello デュアルアクティブ検出リンクを設定できません。

```
On Switch 1:
Device>enable
Device#configure terminal
Device(config)#interface TenGigabitEthernet3/0/1
Device(config-if)#stackwise-virtual dual-active-detection
```

```
WARNING: All the extraneous configurations will be removed for TenGigabitEthernet3/0/1
on reboot
INFO: Upon reboot, the config will be part of running config but not part of start up
config.
Device(config-if)#exit
On Switch 2:
Device(config)#interface TenGigabitEthernet3/0/1
Device(config-if)#stackwise-virtual dual-active-detection
WARNING: All the extraneous configurations will be removed for TenGigabitEthernet3/0/1
on reboot.
INFO: Upon reboot, the config will be part of running config but not part of start up
config.
Device(config-if)#end
On both the switches:
Device#write memory
Device#reload
```

例：StackWise Virtual リンク情報の表示

show stackwise-virtual link コマンドの出力例

```
Device#show stackwise-virtual link
Stackwise Virtual Configuration:
--------------------------------------------
Stackwise Virtual : Enabled
Domain Number :            1

Switch  Stackwise Virtual Link   Ports
------  ----------------------   ------
1       1                        TenGigabitEthernet1/1/0/1
2       1                        TenGigabitEthernet2/1/0/1
```

スタンドアロンモードのデフォルトでは、他のスイッチ番号に明示的に変更されない限り、スイッチはスイッチ 1 として識別されます。StackWise Virtual への変換中に、スイッチ番号は自動的に変更され、StackWise Virtual ドメイン内 2 つのスイッチが反映されます。

例：StackWise Virtual デュアルアクティブ検出リンク情報の表示

show stackwise-virtual dual-active-detection コマンドの出力例

StackWise Virtual DAD リンクの設定：

```
Device#show stackwise-virtual dual-active-detection
Recovery Reload for switch 1: Enabled
Recovery Reload for switch 2: Enabled

Dual-Active-Detection Configuration:
-------------------------------------
Switch   Dad port                        Status
------   ------------                    ---------
1        TenGigabitEthernet1/3/0/1       up
2        TenGigabitEthernet2/3/0/1       up
```

dual-active recovery-reload-disable コマンドを設定した後の StackWise Virtual DAD リンクの設定：

```
Device#show stackwise-virtual dual-active-detection
Recovery Reload for switch 1: Enabled
Recovery Reload for switch 2: Enabled
Dual-Active-Detection Configuration:
-------------------------------------
Switch      Dad port                    Status
------      ------------                ---------
1           TenGigabitEthernet1/3/0/1   up
2           TenGigabitEthernet2/3/0/1   up
```

show stackwise-virtual dual-active-detection epagp コマンドの出力例

StackWise Virtual DAD ePAgP 情報：

```
Device#show stackwise-virtual dual-active-detection pagp
Pagp dual-active detection enabled: Yes
In dual-active recovery mode: No
Recovery Reload for switch 1: Enabled
Recovery Reload for switch 2: Enabled

Channel group 11
                  Dual-Active          Partner              Partner         Partner
Port              Detect Capable       Name                 Port            Version
Fo1/1/0/17        Yes                  SwitchA              Hu2/0/1         1.1
Fo2/2/0/21        Yes                  SwitchA              Hu1/0/4         1.1
```

出力の**Partner Name**フィールドと**Partner Port**フィールドは、MEC を介して PagP ポートチャネルが接続されているピアスイッチの名前とポートを表します。

Cisco StackWise Virtual の設定の確認

StackWise Virtual の設定を確認するには、次の **show** コマンドを使用します。

show stackwise-virtual switch *number <1-2>*	スタック内の特定のスイッチの情報を表示します。
show stackwise-virtual link	StackWise Virtual リンク情報を表示します。
show stackwise-virtual bandwidth	Cisco StackWise Virtual で利用できる帯域幅を表示します。
show stackwise-virtual neighbors	Cisco StackWise Virtual ネイバーを表示します。
show stackwise-virtual dual-active-detection	StackWise Virtual のデュアルアクティブ検出情報を表示します。
show stackwise-virtual dual-active-detection pagp	ePAgP デュアル アクティブ検出情報を表示します。

Switch ½ renumber ½	（任意）新しいスイッチ番号を割り当てます。デフォルトの数は 1 です。

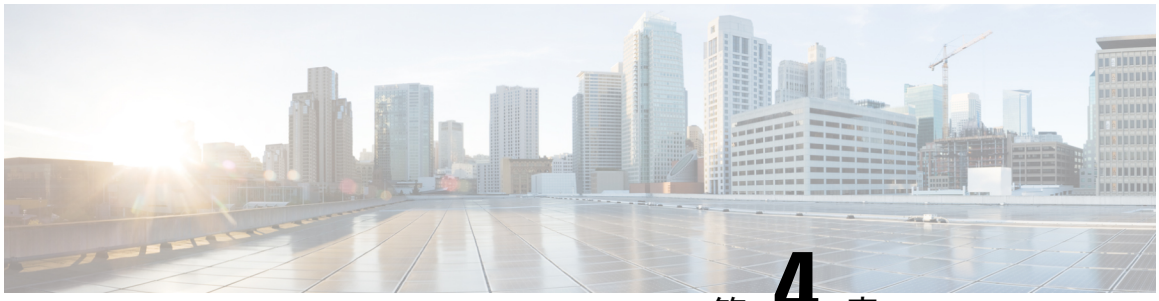
StackWise Virtual に関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	『High Availability Command Reference for Catalyst 9400 Switches』

Cisco StackWise Virtual の機能の履歴と情報

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	この機能が Cisco Catalyst 9404R および Cisco Catalyst 9407R スイッチに導入されました。
Cisco IOS XE Everest 16.11.1	• この機能は、Cisco Catalyst 9410R スイッチに導入されました。 • DAD リカバリのよるリロードを無効にするコマンドが導入されました。
Cisco IOS XE Amsterdam 17.2.x	Cisco StackWise Virtual が設定されたスイッチで BUM トラフィック最適化機能がサポートされるようになりました。



第 4 章

ISSU の設定

ISSU を実行するための前提条件

In-Service Software Upgrade（ISSU）を実行する場合は、次の前提条件が適用されます。

- アクティブのスーパーバイザモジュール が新しい Cisco IOS XE イメージにアクセスできる。または、IOS XE イメージが事前にフラッシュにロードされている。
- デバイスが、インストールモードで実行されている。
- ノンストップ フォワーディング（NSF）を有効にする。

ISSU について

ISSU は、ネットワークがパケットの転送を継続している間に、デバイス上の別のイメージにイメージをアップグレードするプロセスです。ISSU を活用することで、ネットワークを停止させずにソフトウェアをアップグレードすることができます。イメージは、各パッケージが個別にアップグレードされるインストールモードでアップグレードされます。

ISSUは、ソフトウェアのアップグレードとロールバックをサポートします。1つのステップまたは 3 つのステップで実行できます。

Cisco StackWise Virtual ソリューションは ISSU をサポートします。このソリューションは、1つの仮想スイッチを形成するように互いに接続された2つのスイッチで構成されています。詳細については、このマニュアルの「*Cisco StackWise Virtual* の設定」の章を参照してください。

（注）

- ISSU は、スタンドアロンスイッチ上のデュアル スーパーバイザ モジュール設定でサポートされています。
- スイッチに Cisco StackWise Virtual が設定された場合、ISSU は単一のスーパーバイザモジュール設定でのみサポートされます。

ISSU アップグレード

次のステップでは、ISSU を実行する際に従うプロセスについて説明します。

1. スタンバイスイッチとアクティブスイッチのに新しいイメージをコピーします。
2. ファイルを解凍し、アクティブスイッチとスタンバイスイッチの両方のにパッケージをコピーします。
3. スタンバイスイッチのにパッケージをインストールします。
4. スタンバイスイッチのを再起動します。

   これで、スタンバイスイッチのが新しいソフトウェアにアップグレードされます。
5. アクティブスイッチのにパッケージをインストールします。
6. アクティブスイッチのを再起動し、スタンバイを新しいアクティブスイッチのにスイッチオーバーします。スイッチオーバー後、新しいスタンバイスイッチのは新しいソフトウェアで起動します。新しいソフトウェアイメージが新しいアクティブスイッチのにすでにインストールされているため、ISSU が完了します。

ISSU アップグレード：3 ステップのワークフロー

このワークフローには、追加、アクティブ化、コミットの 3 つのステップがあります。アクティブ化後、すべてのスイッチが新しいソフトウェアバージョンにアップグレードされます。ただし、ソフトウェアは自動的にコミットされなるのではなく、**install commit** コマンドを使用して手動で実行する必要があります。このアプローチの利点は、システムを以前のソフトウェアバージョンにロールバックできることです。**install abort-timer-stop** または **install commit** コマンドを使用してロールバックタイマーを停止しない場合、システムは自動的にロールバックします。ロールバックタイマーが停止している場合は、新しいソフトウェアバージョンをデバイス上で任意の期間実行してから、以前のバージョンにロールバックできます。

ISSU アップグレード：1 ステップのワークフロー

このワークフローは1つのステップのみがあり、最適化に役立ちます。アップグレードは自動的にコミットされるため、ロールバックできません。

ISSU リリースのサポートおよび推奨されるリリースの詳細については、「Technical References」→「In-Service Software Upgrade (ISSU)」を参照してください。

ISSU の実行に関する制約事項および注意事項

- ISSU は、Stackwise Virtual の両方のスイッチがインストールモードで起動されている場合にのみサポートされます。（シャーシがバンドルモードで起動されている場合、ISSU はサポートされません）。
- ハードウェアとソフトウェアの同時アップグレードはサポートされていません。一度に実行できるアップグレード操作は 1 つだけです。
- メンテナンスウィンドウ内でアップグレードを実行することを推奨します。
- ISSU プロセスの実行中は、設定を変更しないでください。
- ISSU を使用したダウングレードはサポートされません。
- ISSU は、Cisco IOS XE Fuji 16.9.1 から Cisco IOS XE Fuji 16.9.2 へのアップグレードではサポートされていません。
- ISSU は、Cisco IOS XE Fuji 16.9.x から Cisco IOS XE Gibraltar 16.10.x または Cisco IOS XE Gibraltar 16.11.x へのアップグレードではサポートされていません。これは、シングル スーパーバイザ モジュールとデュアル スーパーバイザ モジュールの両方のセットアップに適用されます。
- Cisco IOS XE Fuji 16.9.x から Cisco IOS XE Gibraltar 16.12.x への ISSU の実行時、OSPFv3 で **interface-id snmp-if-index** コマンドが設定されていないとパケット損失が発生する可能性があります。ISSU を実行する際は、メンテナンス期間中かデバイスをネットワークから分離（メンテナンスモード機能を使用）した後、事前に **interface-id snmp-if-index** コマンドを設定しておいてください。

1 ステップワークフローを使用したソフトウェアのアップグレード

始める前に

- デバイスは、インストールモードで起動する必要があります。
- SVL が起動していることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： `Switch> enable`	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	**install add file** { **ftp:** | **tftp:** | **flash:** | **disk:** ***.bin** } **activate issu commit**	両方のスイッチへのイメージのダウンロードとパッケージへの拡張、手順に従った各スイッチのアップグレードなど、すべてのアップグレード手順のシーケンスを自動化します。 （注） このコマンドは、スイッチがバンドルイメージを使用して起動された場合にエラーをスローします。

3 ステップワークフローを使用したソフトウェアのアップグレード

始める前に

- デバイスは、インストールモードでブートする必要があります。
- SVL が起動していることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： `Switch> enable`	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	**install add file** { **ftp:** | **tftp:** | **flash:** | **disk:** ***.bin** } 例： `Switch# install add file ftp:file.bin`	このコマンドは、イメージをブートフラッシュにダウンロードし、両方のスイッチので展開します。
ステップ 3	**install activate issu** 例：	このコマンドを実行すると、次の一連のイベントが発生します。

	コマンドまたはアクション	目的
	`Switch# install activate issu`	1. ロールバックタイマーが開始されます。ロールバックタイマーが期限切れになると、システムは ISSU の開始前に同じステートにロールバックします。ロールバックタイマーは、**install abort-timer stop** コマンドを使用して停止できます。ISSU は、**install abort issu** コマンドを使用してロールバックできます。 2. スタンバイスイッチのが新しいソフトウェアでプロビジョニングされ、新しいソフトウェアバージョンでリロードされます。次に、アクティブスイッチのに新しいソフトウェアがプロビジョニングされ、リロードされます。新しいイメージを持つスタンバイスイッチのがアクティブスイッチのスになり、古いアクティブスイッチのがスタンバイになります。 3. この手順の最後に、両方のスイッチのが新しいソフトウェアイメージで実行されます。
ステップ 4	**install commit** 例： `Switch# install commit`	**commit** コマンドは、必要なクリーンアップを実行し、新しいソフトウェアを永続的に有効にして（古いバージョンのソフトウェアを削除して）、ロールバックタイマーを停止します。コミット後の再起動は、新しいソフトウェアで起動します。 （注） このコマンドを使用すると、ロールバックは行われません。

ISSU のモニタリング

SatckWise Virtual で ISSU を確認するには、次の **show** コマンドを使用します。

コマンド	説明
show issu clients	現在の ISSU クライアント（つまり、ISSU でサポートされているネットワーク アプリケーションとプロトコル）のリストを表示します。
show issu message types	特定のクライアントでサポートされている ISSU メッセージの形式、バージョン、サイズを表示します。
show issu negotiated	メッセージバージョンまたはクライアント機能に関して発生したネゴシエーションの結果を表示します。
show issu sessions	クライアントステータスが差し迫ったソフトウェアアップグレードと互換性があるかどうかなど、特定の ISSU クライアントに関する詳細情報を表示します。
show issu comp-matrix	ISSU 互換性マトリクスに関する情報を表示します。
show issu entities	1 つ以上の ISSU クライアント内のエンティティに関する情報を表示します。
show issu state [detail]	現在の ISSU ステートを表示します。

ISSU の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

機能名	リリース	機能情報
ISSU	Cicso IOS XE Fuji 16.9.1	この機能が導入されました。
Cisco StackWise Virtual スイッチの ISSU	Cisco IOS XE Fuji 16.9.2	この機能は、Cisco StackWise Virtual スイッチで有効になりました。