Cisco IOS XE Everest 16.6.x（Catalyst 9500 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：2017 年 7 月 31 日

最終更新：2017 年 11 月 3 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/

© 2017 Cisco Systems, Inc. All rights reserved.

目 次

第 1 章

NSF with SSO の設定 1

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 1

機能情報の確認 1

ノンストップ フォワーディング/ステートフル スイッチオーバーの前提条件 1

ノンストップ フォワーディング/ステートフル スイッチオーバーの制約事項 2

NSF with SSO に関する情報 2

ノンストップ フォワーディング/ステートフル スイッチオーバーの概要 2

SSO の動作 3

NSF の動作 5

Cisco Express Forwarding; シスコ エクスプレス フォワーディング 6

ルーティング プロトコル 7

Cisco NSF with SSO の設定方法 9

SSO の設定 9

ノンストップ フォワーディング/ステートフル スイッチオーバーの設定例 10

例：SSO の設定 10

Cisco Express Forwarding NSF の確認 11

ノンストップ フォワーディング/ステートフル スイッチオーバーに関するその他の関連資料 12

ノンストップ フォワーディング/ステートフル スイッチオーバーの機能の履歴と情報 13

第 2 章

Cisco StackWise Virtual の設定 15

機能情報の確認 15

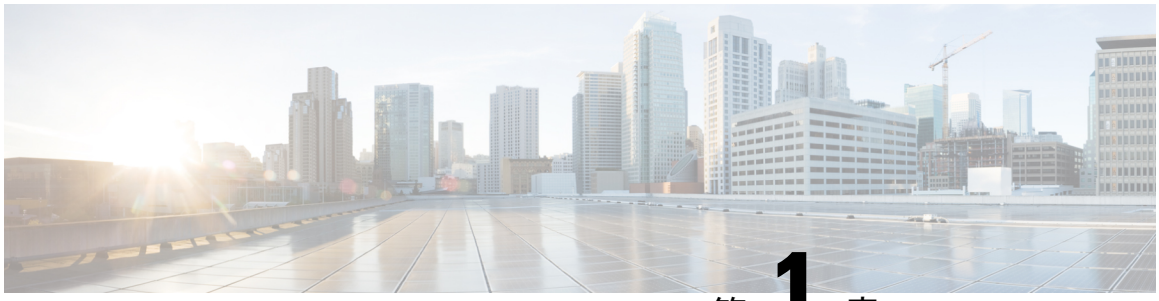
Cisco StackWise Virtual の前提条件 15

Cisco StackWise Virtual の制約事項 16

Cisco StackWise Virtual について 16
StackWise Virtual の概要 16
Cisco StackWise Virtual トポロジ 16
Cisco StackWise Virtual 冗長性 18
SSO 冗長性 19
ノンストップ フォワーディング 19
マルチシャーシ EtherChannel 20
MEC の最小遅延ロード バランシング 20
MEC 障害シナリオ 21
Cisco StackWise Virtual のパケット処理 22
StackWise Virtual リンク上のトラフィック 22
レイヤ 2 プロトコル 23
レイヤ 3 プロトコル 24
デュアル アクティブ検出 26
fast hello デュアル アクティブ検出リンク 26
拡張 PAgP デュアル アクティブ検出 26
リカバリ アクション 27
Cisco StackWise Virtual の実装 28
Cisco StackWise Virtual の設定方法 28
Cisco StackWise Virtual 設定の構成 28
Cisco StackWise Virtual リンクの設定 29
StackWise Virtual デュアル アクティブ検出リンクの設定 30
ePAgP デュアル アクティブ検出の有効化 31
Cisco StackWise Virtual の無効化 33
Cisco StackWise Virtual の設定の確認 34
StackWise Virtual に関するその他の関連資料 35
Cisco StackWise Virtual の機能の履歴と情報 35

第 3 章 グレースフル挿入と削除（GIR）の設定 37
グレースフル挿入と削除の制約事項 37
グレースフル挿入と削除について 37

概要 37
レイヤ 2 インターフェイスのシャットダウン 38
カスタム テンプレート 38
グレースフル挿入と削除の設定方法 39
メンテナンス テンプレートの作成 39
システム モード メンテナンスの設定 39
メンテナンス モードの開始と停止 40
グレースフル削除と挿入の設定例 41
例：メンテナンス テンプレートの設定 41
例：システム モード メンテナンスの設定 41
例：メンテナンス モードの開始と停止 41
例：システム モード設定の表示 42
グレースフル挿入と削除のモニタリング 42
グレースフル挿入と削除に関するその他の関連資料 43



第 1 章

NSF with SSO の設定

• 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 （1 ページ）

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）は、ステートフル スイッチオーバー（SSO）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。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびCisco 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 には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

ノンストップ フォワーディング/ステートフル スイッチオーバーの前提条件

- NSF は、SSO が設定されているネットワーク デバイスに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。

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。HSRP を NSF SSO で使用しないでください。
- 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。

NSF with SSO に関する情報

ノンストップ フォワーディング/ステートフル スイッチオーバーの概要

Cisco Nonstop Forwarding（NSF）は、ステートフル スイッチオーバー（SSO）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 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。スイッチオーバー中にラインカードおよびFPのアップ状態を保ち、アクティブ RP の転送情報ベース（FIB）を最新の状態に維持する機能は、Cisco NSF/SSO の動作で非常に重要です。

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ップ状態のままなので、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 デバイスがスタンバイ用に選択されます。
- 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。
- 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、次の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。

次の機能のステートは、アクティブ デバイスとスタンバイ デバイスの両方に保存されます。

- 802.3
- 802.3u
- 802.3x（フロー制御）
- 802.3ab（GE）
- 802.3z（CWDM を含めたギガビット イーサネット）
- 802.3ad（LACP）
- 802.1p（レイヤ 2 QoS）
- 802.1q
- 802.1X（認証）
- 802.1D（スパニングツリー プロトコル）
- 802.3af（インライン パワー）
- PAgP
- VTP
- ダイナミック ARP インスペクション
- DHCP スヌーピング
- IP ソース ガード
- IGMP スヌーピング（バージョン 1 および 2）
- DTP（802.1Q および ISL）
- MST
- PVST+
- Rapid PVST
- PortFast/UplinkFast/BackboneFast
- BPDU ガードおよびフィルタリング
- ボイス VLAN
- ポート セキュリティ

- ユニキャスト MAC フィルタリング
- ACL（VACL、PACL、RACLS）
- QoS（DBL）
- マルチキャスト ストーム制御/ブロードキャスト ストーム制御

SSO は、次の機能と互換性があります。ただし、次の機能のプロトコル データベースはスタンバイ スイッチとアクティブ スイッチの間で同期されません。

- レイヤ 2 プロトコル トンネリング（L2PT）を備えた 802.1Q トンネリング
- ベビー ジャイアント
- ジャンボ フレーム サポート
- Cisco Discovery Protocol
- フラッディング ブロック
- UDLD
- SPAN/RSPAN
- NetFlow

SSO がイネーブルにされている場合、デバイス上のすべてのレイヤ 3 プロトコルが、スタンバイ デバイスで学習されます。

NSF の動作

ノンストップ フォワーディング（NSF）は常にステートフル スイッチオーバー（SSO）とともに実行され、レイヤ 3 トラフィックの冗長性を確保します。NSF は BGP、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 デバイスが BGP（**graceful-restart** コマンドを使用）、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、ルーティングの更新はアクティブ デバイス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。

Cisco Express Forwarding; シスコ エクスプレス フォワーディング

Cisco IOS ノンストップ 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、アクティブなデバイス上の 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 デバイス上の Cisco Express Forwarding は、アクティブ デバイス上の 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 IS-IS（Intermediate System-to-Intermediate System）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** コマンドで設定します。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 NSF with SSO の設定方法

SSO の設定

あらゆるサポート対象プロトコルを持った NSF を使用するには、SSO を設定する必要があります。

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 モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**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 スイッチが再起動され、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。

ノンストップ フォワーディング/ステートフル スイッチオーバーの設定例

例：SSO 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 states** コマンドの出力例を示します。

```
show redundancy states
 my state = 13 -ACTIVE
 peer state = 8 -STANDBY HOT
 Mode = Duplex
 Unit = Primary
 Unit ID = 5
 Redundancy Mode (Operational) = sso
 Redundancy Mode (Configured) = sso
 Split Mode = Disabled
 Manual Swact = Enabled
 Communications = Up
 client count = 29
 client_notification_TMR = 30000 milliseconds
 keep_alive TMR = 9000 milliseconds
 keep_alive count = 1
 keep_alive threshold = 18
 RF debug mask = 0x0
```

Cisco Express Forwarding NSF 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.
```

ノンストップ フォワーディング/ステートフル スイッチオーバーに関するその他の関連資料

関連資料

関連項目	参照先
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 Commands』

MIB

MIB	MIB リンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Product Alert Tool（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

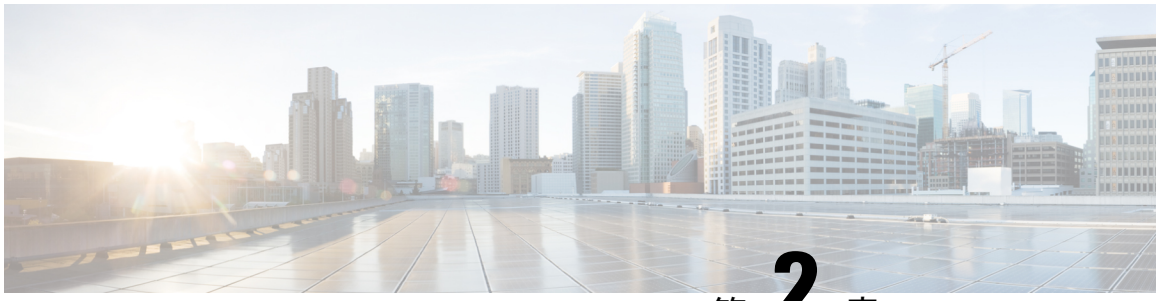
ノンストップ フォワーディング/ステートフル スイッチオーバーの機能の履歴と情報

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 リリースのみを示しています。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Cisco 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。

表 *1:* ノンストップ フォワーディング/ステートフル スイッチオーバーの機能の情報

機能名	リリース	機能情報
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 IOS XE Everest 16.6.1	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。



第 2 章

Cisco StackWise Virtual の設定

- 機能情報の確認 （15 ページ）
- Cisco StackWise Virtual の前提条件 （15 ページ）
- Cisco StackWise Virtual の制約事項 （16 ページ）
- Cisco StackWise Virtual について （16 ページ）
- Cisco StackWise Virtual の設定方法 （28 ページ）
- Cisco StackWise Virtual の設定の確認 （34 ページ）
- StackWise Virtual に関するその他の関連資料 （35 ページ）
- Cisco StackWise Virtual の機能の履歴と情報 （35 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびCisco 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 には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

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 のすべてのスイッチは互換性のあるソフトウェアのバージョンを実行している必要があります。

Cisco StackWise Virtual の制約事項

- Cisco IOS XE Everest 16.6.1 では、サポートされている Cisco StackWise Virtual リンクの最大数は 8 です。
- Cisco IOS XE Everest 16.6.1 で、Cisco StackWise Virtual は C9500-24Q スイッチ モデルでのみサポートされています。
- デュアル アクティブと StackWise Virtual リンクの設定は動的に実行され、デバイスは設定後に再起動されます。

Cisco StackWise Virtual について

StackWise Virtual の概要

Cisco StackWise Virtual は、2 台のスイッチを 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、コントロール プレーンと管理プレーンを 1 つにすることで業務を簡素化して効率性を高めるほか、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台のスイッチは 40-G または10-G イーサーネット接続を使用して 1 台の論理的な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。

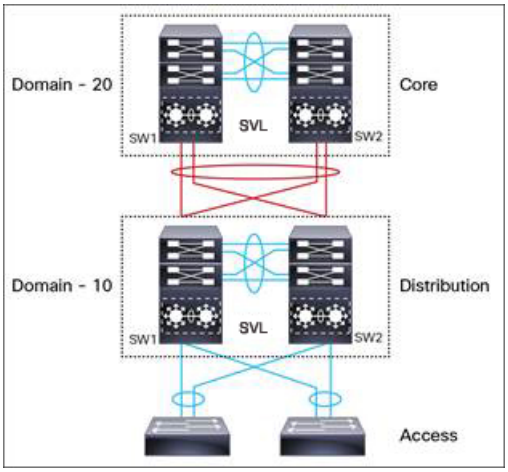
- アクセス レイヤ間で VLAN ID を再使用する場合、ネットワークの全体的なパフォーマンスに影響するスパニング ツリー ループが生じる。
- スパニング ツリー プロトコル ループ、ルートおよびブリッジ プロトコル データ ユニット管理に対してレイヤ 2 ネットワークを保護するには、スパニング ツリー プロトコルと設定が必要。
- IP ゲートウェイの機能を仮想化するために、First Hop Redundancy Protocol などの追加のプロトコルが必要。これは、各 VLAN の STP ルートのプライオリティに対して整合性を確保する必要がある。
- Protocol Independent 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。Cisco StackWise 技術では、イーサネット ネットワーク上に拡張する場合、従来のバック スタック ケーブルの長さが制限にならないため柔軟性が得られます。スタックは冗長 40-G または 10-G ファイバ 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 メンバー間に MEC を実装できます。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。

また、Cisco StackWise Virtual をアクティブにするスイッチ、コントロール プレーンの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。これらは、Cisco StackWise Virtual アクティブ スイッチのアクティブ スーパーバイザで集中管理されます。

Cisco StackWise Virtual メンバー スイッチは、Virtual Communication Manager（VCM）と呼ばれる仮想ソフトウェア モジュールを使用して StackWise Virtual リンク上で互いに通信します。

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
- StackWise Virtual リンク：10-Gb または 40-Gb イーサーネット接続

StackWise Virtual リンクは、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 10-G または 40-G 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。物理ポートは、StackWise Virtual リンクとして設定できます。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 StackWise Virtual リンクを探します。

Cisco StackWise Virtual Header（SVH）は 64 バイトのオーバーヘッドフレームで、Cisco StackWise Virtual ドメインの 2 つのスタック メンバー間で各 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、StackWise Virtual リンク関連の設定が一致していること。
- ノンストップ フォワーディング（NSF）設定が SSO ピアリングの構築に依存していないこと。
- 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、起動時や 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、StackWise Virtual リンクを使用して 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）技術を実装すると、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透過的になります。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。

Cisco StackWise Virtual システムで、MEC は追加機能を備えた EtherChannel です。つまり、Cisco StackWise Virtual は、スイッチのバック スタックのように、各スイッチのポート全体でロードバランシングを行います。たとえば、トラフィックが Cisco StackWise Virtual アクティブ スイッチに入る場合、Cisco StackWise Virtual は Cisco StackWise Virtual アクティブ スイッチのパケットから生成されたハッシュに基づいて MEC リンクを選択します。

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、StackWise Virtual リンク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 メンバー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。

パケットを受信すると必ず、そのフローについて計算されたハッシュ値に基づいて宛先ポートが選択されます。宛先ポートは、MEC のポートがローカル チャネルで利用できる場合でも、リモート スイッチで選択できます。このため、MEC メンバー ポートの 1 つ以上のポートがローカル スイッチにある場合でも、ユニキャスト トラフィックが StackWise Virtual リンク上を移動することがあります。同様に、マルチキャスト トラフィックも、StackWise Virtual リンクを介して送信されます。

（注） 最小遅延ロード バランシングは、Cisco IOS XE Denali 16.3.3 ではサポートされていません。

MEC 障害シナリオ

MECでは、各スイッチへのリンクを少なくとも1つは持つように構成することを推奨します。この構成により、スイッチに障害が発生した場合でも、データ トラフィックの代替パスを常に確保できます。

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 StackWise Virtual リンクを介して 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、StackWise Virtual リンクを介して 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、StackwWise 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

StackWise Virtual リンクでは、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。StackWise Virtual リンク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。

StackWise Virtual リンクは、2 台のスイッチ間で制御メッセージを転送します。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、StackWise Virtual リンクを介してデータ 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、StackWise Virtual リンクは、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。

StackWise Virtual リンク上のトラフィックは、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。

レイヤ 2 プロトコル

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。Cisco StackWise Virtual スタンバイ スイッチのスイッチング モジュールで送受信するプロトコル メッセージは、StackWise Virtual リンクを通過して Cisco StackWise Virtual アクティブ スイッチに到達する必要があります。

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、StackWise Virtual リンクを介して、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

StackWise Virtual リンク ポートではスイッチ ポート アナライザ（SPAN）はサポートされません。SVL 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。

レイヤ 3 プロトコル

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 MAC アドレスは設定可能であり、仮想MAC（ドメインIDから取得）、シャーシMAC（スイッチオーバー後も保持される）、ユーザ設定の MAC アドレスの 3 種類のオプションから選択できます。Cisco StackWise Virtual は、デフォルトで仮想 MAC アドレスを使用します。

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、StackWise Virtual リンク経由で 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、StackWise Virtual 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、StackWise Virtual リンク経由で 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。

StackWise Virtual リンク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、StackWise Virtual 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、StackWise Virtual リンク経由で 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

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。デュアルアクティブ検出リンクは、これを軽減するために使用される専用リンクです。

StackWise Virtual リンク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 スイッチの状態を判断できません。遅延なくスイッチオーバーを確実に実行するために、Cisco StackWise Virtual スタンバイ スイッチは Cisco StackWise Virtual アクティブ スイッチに障害が発生したものと想定し、スイッチオーバーを開始して Cisco StackWise Virtual のアクティブ ロールを引き継ぎます。

fast hello デュアル アクティブ検出リンク

（注） Cisco IOS XE Denali 16.3.3 では、fast hello デュアル アクティブ検出方式のみサポートされています。

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 Stackwise Virtual リンク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 （27 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） StackWise Virtual リンクとデュアル アクティブ検出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

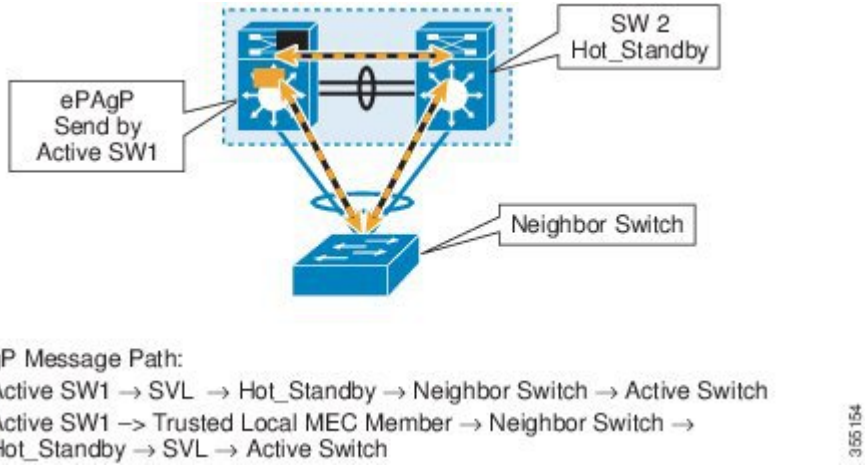
デュアル アクティブ シナリオを検出できます。MEC は、StackWise Virtual が設定されている各スイッチに少なくとも 1 つのポートを持っている必要があります。

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 *2 : 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 stac mac persistency wait timer 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

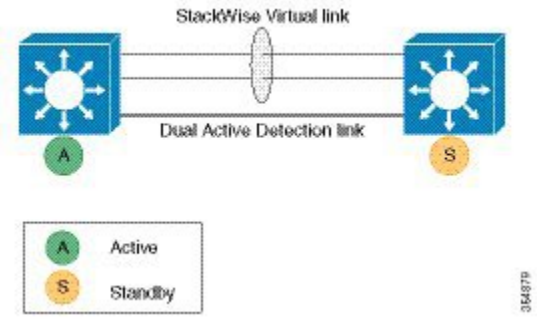
Cisco StackWise Virtual アクティブ スイッチは、デュアル アクティブ状態を検出すると、StackWise Virtual リンク以外のすべてのインターフェイスをシャットダウンし、ネットワークから自身を削除します。スイッチは、StackWise Virtual リンクが回復するまで、リカバリ モードで待機します。StackWise Virtual リンクの障害を物理的に修復し、リカバリ スイッチを手動でリロードしてスタンバイ スイッチにしてください。

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 StackWise Virtual Link（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。メンバー スイッチの 1 台がコントロールと管理のプレーンのマスターになり、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 *3:2* 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 モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 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 サブモードを開始します。
ステップ 4	**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。

次のタスク

Cisco StackWise Virtual を有効にして必要なインターフェイスを Cisco StackWise Virtual リンクに設定してから、**show stackwise-virtual** コマンドを使用して設定情報を確認します。確認後、設定を保存して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） Cisco StackWise Virtual リンクは、すべての 10-G インターフェイスおよび 40-G インターフェイスでサポートされます。ただし、両方のインターフェイスの組み合わせはサポートされていません。

StackWise Virtual リンク ポートとして 10 ギガビット イーサネット ポートを設定するには、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 モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 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** *<interface>* 例： `Device(config)#interface TenGigabitEthernet1/0/2`	10-G 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。 40-G イーサネット インターフェイスには、**interface FortyGigabitEthernet** *<interface>* コマンドを使用できます。
ステップ 4	**stackwise-virtual link** *link value* 例： `Device(config-if)#stackwise-virtual link 1`	インターフェイスと設定した StackWise Virtual リンクを関連付けます。

StackWise Virtual デュアル アクティブ検出リンクの設定

StackWise デュアル アクティブ検出リンクとして 10 ギガビット イーサネット ポートを構成するには、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 モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 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** *<interface>* 例： `Device(config)#interface TenGigabitEthernet1/0/41`	10-G 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。 （注） 1Gインターフェイスは、デュアル アクティブ検出リンクとして設定することもできます。 これは、任意のインターフェイスの 1 と番号付けされているリンクでのみサポートされます。 StackWise Virtual リンクとデュアル アクティブ検出リンクには、異なるポートを使用する必要があります。
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。

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 10 ギガビット イーサネットで有効にするには、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 モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 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** *interface* 例： `Device(config)#interface TenGigabitEthernet1/0/5`	10-G 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	**channel-group** *group_ID* **mode desirable** 例： `Device(config-if)#channel-group 1 mode desirable`	10-G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	**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 7	**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 8	**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 9	**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 10	**interface port-channel** *portchannel* 例： `Device(config)#interface port-channel 1`	スイッチにポートチャネルが設定されます。
ステップ 11	**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 12	**exit** 例：	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。

	コマンドまたはアクション	目的
	`Device(config-if)#exit`	

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 モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 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** *interface* 例： `Device(config)#interface TenGigabitEthernet1/0/41`	10-G 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`	10-Gイーサネットインターフェイスと StackWise Virtual デュアル アクティブ検出の関連付けを解除します。
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 TenGigabitEthernet** *interface* 例： `Device(config)#interface TenGigabitEthernet1/0/5`	10-G 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 7	**no stackwise-virtual link** リンク 例： `Device(config-if)#no stackwise-virtual link 1`	Stackwise Virtual リンクから 10-G イーサネットインターフェイスの関連付けを解除します。

	コマンドまたはアクション	目的
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	**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。 （注） Cisco IOS XE Everest 16.6.1 を開始します。この手順はオプションです。
ステップ 10	**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 11	**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。

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 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。

StackWise Virtual に関するその他の関連資料

関連資料

関連項目	参照先
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, Cisco IOS XE Everest 16.6.1 (Catalyst 9500 Switches)』

MIB

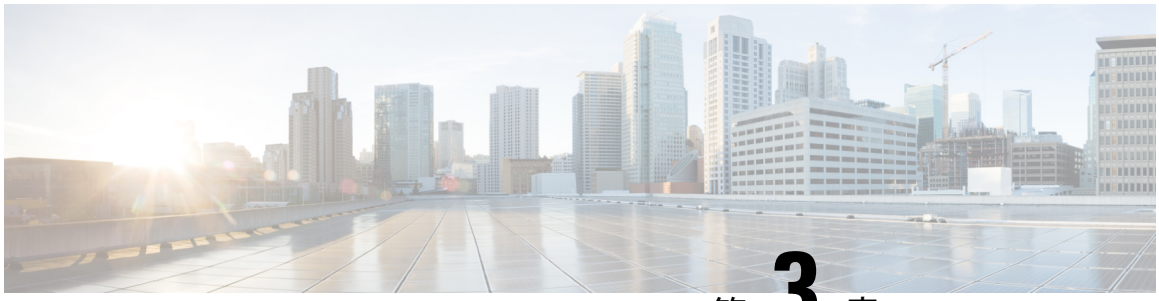
MIB	MIB リンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Product Alert Tool（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

Cisco StackWise Virtual の機能の履歴と情報

リリース	変更箇所
Cisco IOS XE Everest 16.6.1	この機能が導入されました。



第 3 章

グレースフル挿入と削除（GIR）の設定

- グレースフル挿入と削除の制約事項 （37 ページ）
- グレースフル挿入と削除について （37 ページ）
- グレースフル挿入と削除の設定方法 （39 ページ）
- グレースフル削除と挿入の設定例 （41 ページ）
- グレースフル挿入と削除のモニタリング （42 ページ）
- グレースフル挿入と削除に関するその他の関連資料 （43 ページ）

グレースフル挿入と削除の制約事項

Cisco IOS XE Everest 16.6.1 では、レイヤ 2 インターフェイスのシャットダウンと ISIS ルーティング プロトコルで GIR がサポートされます。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。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。

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。

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。

レイヤ2インターフェイスのシャットダウン

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 インターフェイスは、カスタム テンプレートで **shutdown l2** コマンドを使用してシャットダウンします。

カスタム テンプレート

ネットワーク管理者は、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、管理者は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。

管理者は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。

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 モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# config t`	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`
	`Device(config-maintenance-templ)# shutdown l2`
		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。
		• **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 モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例：	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
	`Device# config t`	
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。 • **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:**メンテナンス モードでシステムをリロードします。

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 モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。

	コマンドまたはアクション	目的
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

次に、ISIS 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# config 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# config terminal
Device (config)# maintenance-template t1
Device (config-maintenance-templ)# shutdown l2
```

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# config 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のモニタリング

表 *2:* 特権 *EXEC show* 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。

コマンド	目的
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。キーワードにdumpを使用して、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 *3:* グローバル トラブルシューティング 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するための情報を表示します。

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	参照先
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, Cisco IOS XE Everest 16.6.1.』

MIB

MIB	MIB リンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
シスコのサポートWebサイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Product Alert Tool（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support