

Catalyst 6500 VSS導入のベストプラクティス

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[VSS 配備のベスト プラクティス](#)

[VSS のハイ アベイラビリティ](#)

[アップストリーム リンクの回復](#)

[VSL リンク損失と回復](#)

[サービス モジュールでの冗長性](#)

[マルチキャスト](#)

[Quality of Service \(QoS \)](#)

[SPAN](#)

[その他](#)

[よく寄せられる質問 \(FAQ \)](#)

[VSS ではシャーシごとにデュアル スーパーバイザを使用できますか](#)

[VSS モードの Catalyst 6500 シリーズ スイッチから preempt コマンドを削除すると、スイッチがリロードされますか](#)

[関連情報](#)

概要

このドキュメントでは、Cisco Catalyst 6500 Virtual Switching System (VSS) 1440 の導入シナリオにおけるベスト プラクティスを説明します。

このドキュメントはモジュラ式の設定ガイドになっています。したがって、各セクションを個別に参照して段階的に変更を加えることができます。このドキュメントでは、Cisco IOS® ソフトウェアのユーザ インターフェイスの基本知識があることを前提とします。全体的なネットワーク設計については、このドキュメントでは取り上げません。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、[『シスコテクニカルティップスの表記法』](#)を参照してください。

VSS 配備のベストプラクティス

このドキュメントで説明するソリューションは、複雑なネットワークに取り組み、多くの企業顧客に協力してきたシスコエンジニアの長年にわたる実地経験を反映しています。したがって、このドキュメントで推奨する設定に従うことで、ネットワークを成功に導くことができます。このドキュメントでは、次のソリューションを説明します。

- 管理しやすく、ネットワーク運用チームが設定できるソリューション
- 高可用性と高い安定性を促すソリューション

VSS のハイアベイラビリティ

- [ノンストップフォワーディング](#)
- [OOB MAC 同期](#)

ノンストップフォワーディング

Catalyst 6500 シリーズ スイッチは障害に対する耐性をサポートします。それは、プライマリのスーパーバイザエンジンに障害が発生した場合、冗長スーパーバイザエンジンに切り替えることができるためです。スイッチオーバー後に IP パケットが転送されている間、ユーザがネットワークを使用できない時間を最小限にするために、シスコ ノンストップフォワーディング (NSF) がステートフルスイッチオーバー (SSO) と連動します。

推奨事項

- スーパーバイザスイッチオーバーコンバージェンス時間を 1 秒未満にするには、ノンストップフォワーディングが必要です。
- VSS 環境を動作環境とする場合は、EIGRP または OSPF プロトコルにデフォルトの hello タイマーおよび dead タイマーを使用します。
- モジュラ型 Cisco IOS ソフトウェアを使用してシステムを稼働する場合、OSPF の dead タイマーの値を大きくすることを推奨します。

EIGRP

```
Switch(config)# router eigrp 100
Switch(config-router)# nsf
```

```
Switch# show ip protocols
*** IP Routing is NSF aware ***
```

```
Routing Protocol is "eigrp 100"
```

```
!--- part of the output truncated EIGRP NSF-aware route hold timer is 240s
!--- indicates that EIGRP is configured to be NSF aware !--- part of the output truncated EIGRP
NSF enabled
!--- indicates that EIGRP is configured to be NSF capable !--- rest of the output truncated
OSPF
```

```
Switch(config)# router ospf 100
Switch(config-router)# nsf
```

```
Switch# show ip ospf
```

```
Routing Process "ospf 100" with ID 10.120.250.4
Start time: 00:01:37:484, Time elapsed: 3w2d
!--- part of the output truncated Supports Link-local Signalling (LLS)
!--- indicates that OSPF is configured to be NSF aware !--- part of the output truncated Non-
Stop Forwarding enabled, last NSF restart 3w2d ago (took 31 secs)
!--- indicates that OSPF is configured to be NSF capable !--- rest of the output truncated
NSF についての詳細は、『SSO スーパーバイザ エンジンの冗長性を使用した NSF の設定』を参照してください。
```

OOB MAC 同期

分散型スイッチングでは、分散フィーチャカード (DFC) のそれぞれが独自の CAM テーブルを維持します。つまり、各 DFC が MAC アドレスを学習し、その特定の MAC アドレス エントリの CAM エージングとトラフィック マッチングに応じて MAC アドレス エントリの有効期間を決定します。分散型スイッチングの場合、スーパーバイザ エンジンが特定の MAC アドレスのトラフィックをしばらく観測しないことは珍しくないため、MAC アドレス エントリが期限切れになることがあります。回線モジュール内にある DFC とスーパーバイザ モジュール内にあるポリシー フィーチャカード (PFC) などといった異なるエンジンの中で CAM テーブルの一貫性を維持するには、現在のところ、以下の 2 つのメカニズムを使用できるようになっています。

- ファブリックへのフラッディング (FF)
- MAC 通知 (MN)

PFC 上で MAC アドレス エントリの期限が切れている場合、`show mac-address address <MAC_Address> all` コマンドを使用すると、その MAC アドレスを保有する DFC または PFC が表示されません。MAC アドレスに対するトラフィックがない場合でも、DFC または PFC 上でそのエントリが期限切れにならないようにするには、MAC アドレス同期を有効にします。グローバル コンフィギュレーション コマンド `mac-address-table synchronize` および特権 EXEC コマンド `clear mac-address-table dynamic` を発行すると、同期が有効になります。この `mac-address-table synchronize` コマンドは、Cisco IOS ソフトウェア リリース 12.2(18)SXE4 以降で使用できます。同期を有効にした後も、PFC または DFC に存在しないエントリが表示される場合があります。ただし、モジュールにはエントリの非同期をイーサネット アウトオブバンド チャネル (EOBC) を使用する他のモジュールから学ぶための手段があります。

推奨事項

アウトオブバンド MAC 同期を有効にしてください。これにより、フォワーディング エンジンの中で MAC アドレス テーブルが同期されます。VSS システム内に WS-6708-10G が含まれている場合、MAC 同期は自動的に有効になります。そうでない場合は、手動で有効にする必要があります。

す。

```
Dist-VSS(config)# mac-address-table synchronize
% Current activity time is [160] seconds
% Recommended aging time for all vlans is atleast three times the activity interval
```

```
Dist-VSS# clear mac-address-table dynamic
% MAC entries cleared.
```

```
Dist-VSS# show mac-address-table synchronize statistics
```

```
MAC Entry Out-of-band Synchronization Feature Statistics:
```

```
-----
Switch [1] Module [4]
```

```
-----
Module Status:
```

```
Statistics collected from Switch/Module : 1/4
```

```
Number of L2 asics in this module : 1
```

```
Global Status:
```

```
Status of feature enabled on the switch : on
```

```
Default activity time : 160
```

```
Configured current activity time : 480
```

VSS の用語

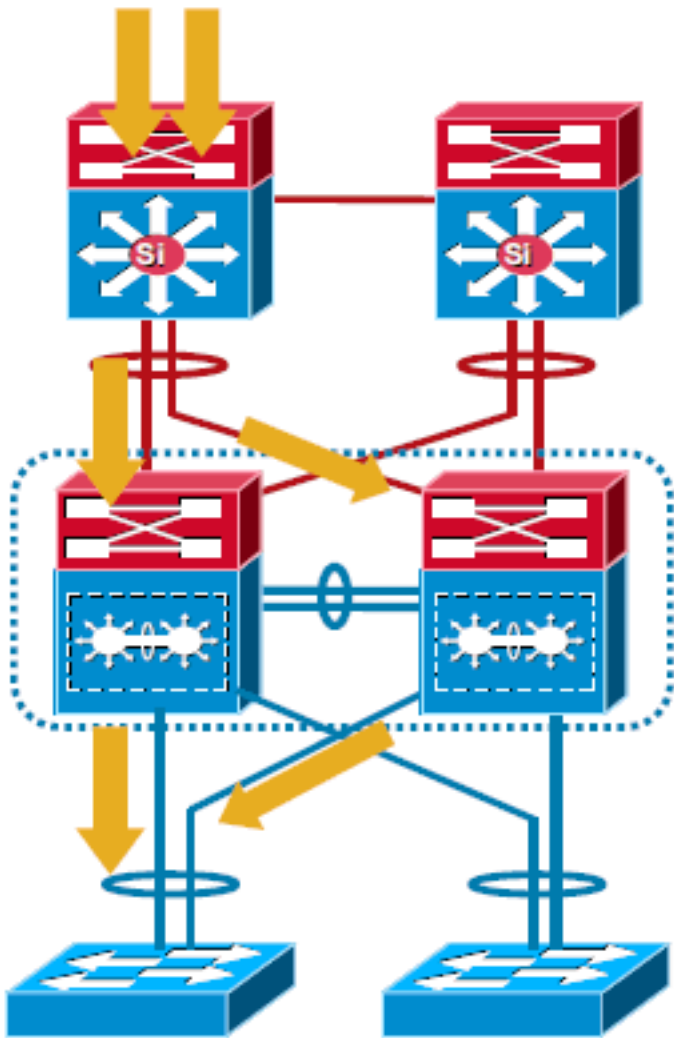
- 仮想スイッチリンク(VSL):2つの物理スイッチを1つの仮想スイッチにバンドルするために必要な特別なポートチャンネル。
- VSL プロトコル (VSLP) : アクティブ スイッチとスタンバイ スイッチの間で VSL に適用されます。このプロトコルにはLMP と RRP という 2 つのコンポーネントがあります。リンク管理プロトコル (LMP) : VSL 内の個別のリンクごとに適用されます。権限解決プロトコル (RRP) : VSL ポート チャンネルの両端 (各ピア) で適用されます。

VSL のキャパシティ プランニング

観念的には、デュアルホーム接続の VSS 設定ではデータ トラフィックは VSL リンクでは送信されません。各スイッチは、トラフィックを転送する際に自身のローカル インターフェイスを選択するようにプログラムされます。

以下のトラフィックには、追加 VSL リンクのキャパシティ プランニングが必要になります。

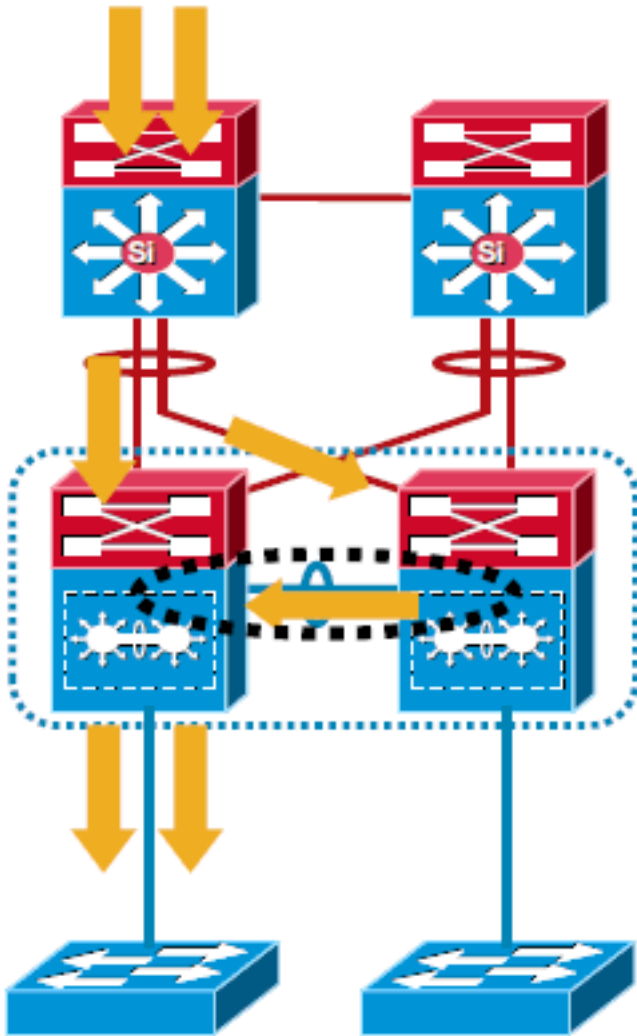
- シングルホーム デバイスで伝送されるトラフィック
- あるスイッチから別のスイッチへのリモート SPAN で伝送されるトラフィック
- サービス モジュール トラフィック (FWSM、ACE など)



詳細は、『[VSL 上のトラフィック](#)』を参照してください。

推奨事項

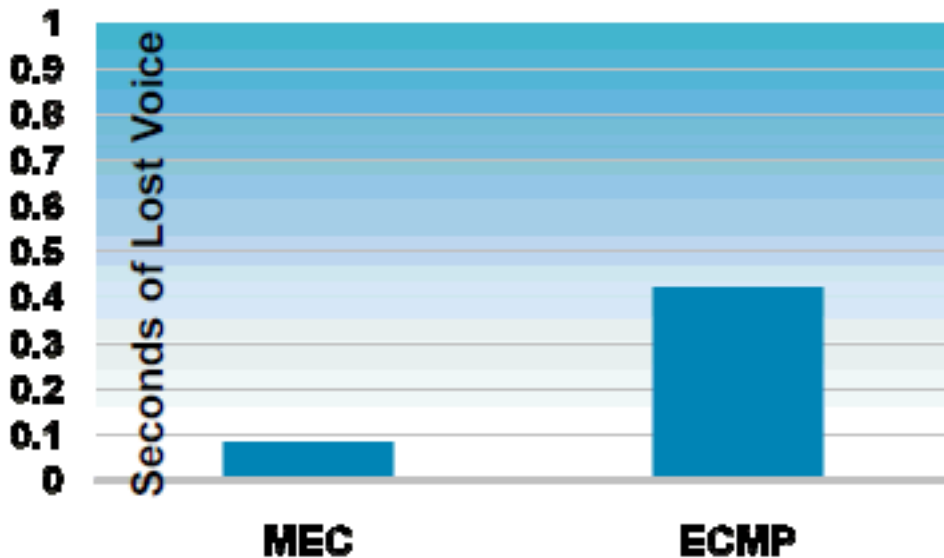
- デュアル ホームのデバイスは常に VSS へ接続されています。
- 最適化されたトラフィックロードシェアリングの優れたハッシュ結果のため、常に 2 の累乗の VSL EtherChannel でバンドルします。
- VSL リンクに復元力があるとしても、VSL の冗長性は極めて重要です。
- VSL 帯域幅を、少なくとも単一の物理スイッチに接続されたアップリンクと同等にすることを推奨します。



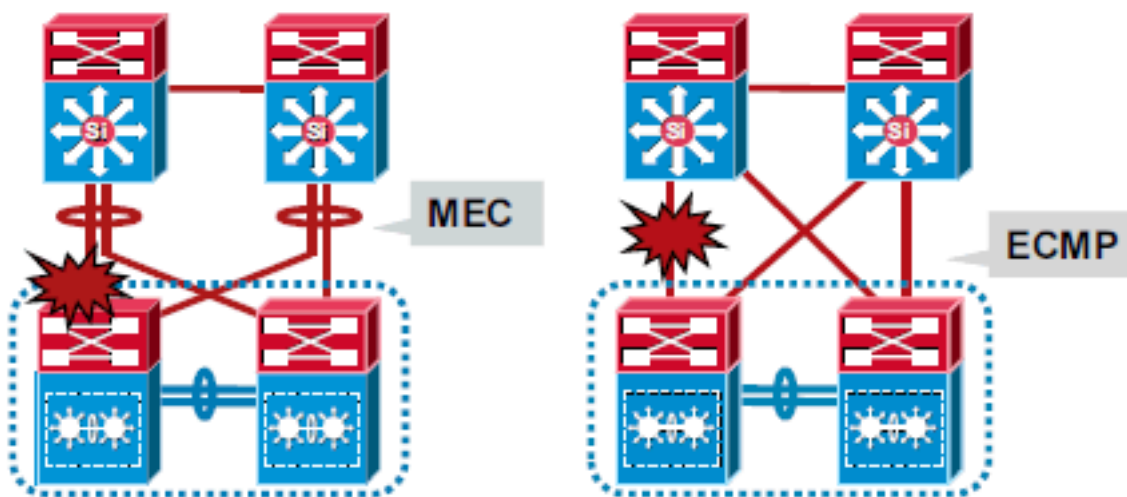
アップストリームリンクの回復

アップストリームリンク（コアへのリンク）のリカバリは、MultiChassis EtherChannel（MEC）または Equal Cost MultiPath（ECMP）機能のいずれかによって達成できます。

MEC コンバージェンスは、ルートの数に依存しておらず、一貫しています。一方、ECMP コンバージェンスは、ルートの数に依存しています。以下の図に、音声セッション損失の大きさを示します。



以下の図は、MEC と ECMP のリンク障害のシナリオを示しています。



MultiChassis EtherChannel

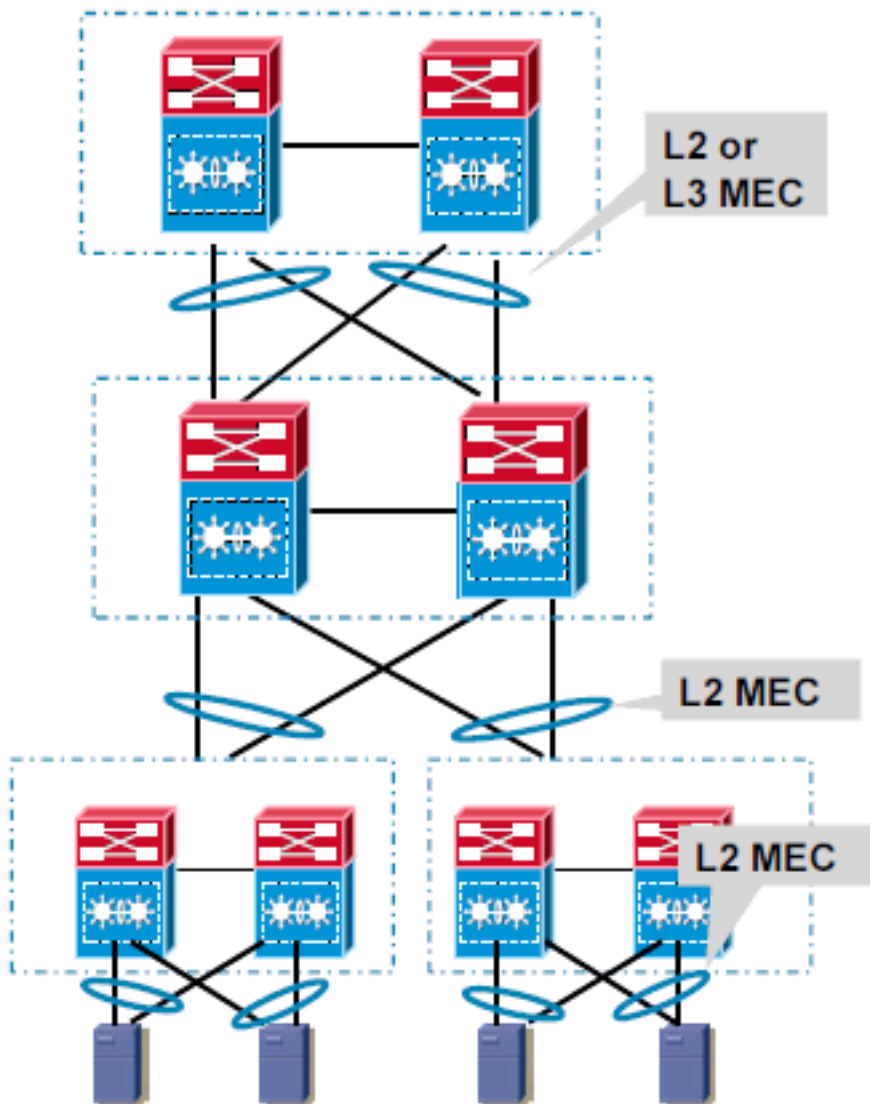
MultiChassis EtherChannel は、VSS の両方のシャーシで終端するポートが搭載された EtherChannel です。VSS MEC は、EtherChannel をサポートしているネットワーク要素 (ホスト、サーバ、ルータ、スイッチなど) に接続できます。VSS での MEC は、追加機能を備えた EtherChannel です。VSS はシャーシごとに独立して、シャーシ内のポートでロード バランシングを行います。たとえば、アクティブ シャーシにトラフィックが到着すると、VSS はアクティブ シャーシの中から MEC リンクを選択します。MEC 機能により、データトラフィックが不必要に VSL を通過しないよう制御できます。

- L2 MEC によりループのないトポロジが実現し、ブロックされるリンクがないことからアップリンク帯域幅が 2 倍になり、コンバージェンス時間が STP よりも短くなります。
- L3 MEC の場合、ネイバー数が削減されて、ロードシェアリングが改善されます (ユニキャストおよびマルチキャストの L2 と L3)。さらに、マルチキャスト フローの VSL リンクの使用率が低下し、コンバージェンス時間が ECMP よりも短くなります。

MEC についての詳細は、『[MultiChassis EtherChannel](#)』を参照してください。

推奨事項

- 常に L2 または L3 MEC を実行します。
- PAgP、LACP、またはトランク プロトコル ネゴシエーションでは、on および off のオプションを使用しないでください。PAgP : MEC リンクで **Desirable-Desirable** を実行します。LACP : MEC リンクで **Active-Active** を実行します。トランク : MEC リンクで **Desirable-Desirable** を実行します。



VSL リンク損失と回復

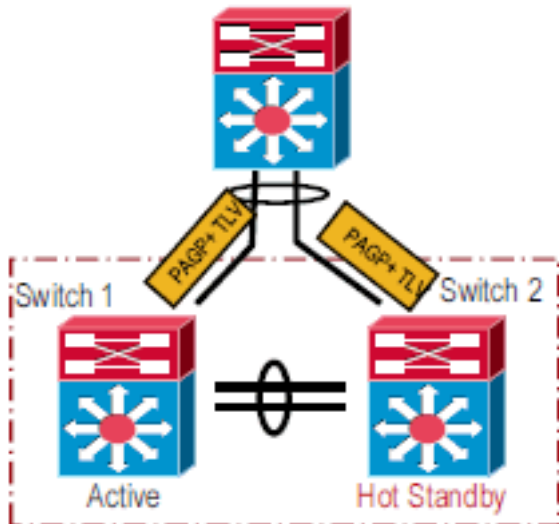
VSL が障害となると、スタンバイ シャーシでは、アクティブ シャーシの状態を検出できません。スイッチオーバーが遅延なく行われるように、スタンバイ シャーシはアクティブ シャーシが障害になったと判断し、スイッチオーバーを開始してアクティブ ロールを代行します。

元のアクティブ シャーシも正常に動作している場合、両方のシャーシがアクティブ状態になります。この状況をデュアル アクティブ シナリオと呼びます。デュアル アクティブ シナリオでは、両方のシャーシで同じ 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。仮想スイッチング システム (VSS) はデュアル アクティブ シナリオを検出して、リカバリ アクションを実行する必要があります。

仮想スイッチング システムはデュアル アクティブ シナリオを検出するために、以下の 3 つの方法をサポートしています。

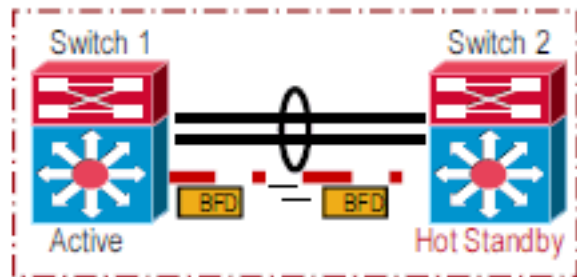
- 拡張 PAgP : MEC リンク上で PAgP メッセージングを使用し、ネイバー スイッチを通して 2

台のシャーシ間の通信を行います。拡張 PAgP は、IP Bidirectional Forwarding Detection (BFD) よりも高速ですが、PAgP 拡張をサポートするネイバー スイッチが必要で



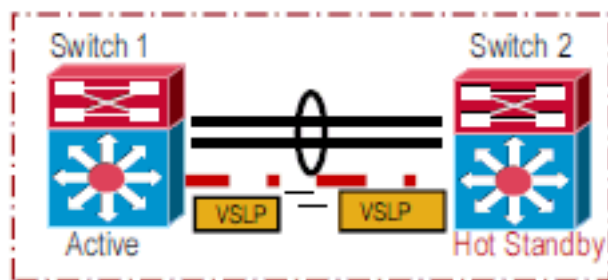
す。 ePAgP サポート表:

- IP 双方向フォワーディング検出 (BFD) : バックアップ イーサネット接続で IP BFD メッセージングを使用します。IP BFD は、2 台のシャーシ間で直接接続を使用するため、ネイバー スイッチからのサポートは不要です。この方法は、Cisco IOS ソフトウェア リリース



12.2(33)SXH1 以降でサポートされています。

- VSLP dual-active fast-hello : バックアップ イーサネット接続で特殊な hello メッセージを使用します。dual-active fast-hello は、IP BFD よりも高速で、ネイバー スイッチからのサポートも不要です。この方法は、Cisco IOS ソフトウェア リリース 12.2(33)SX1 以降でのみサポ

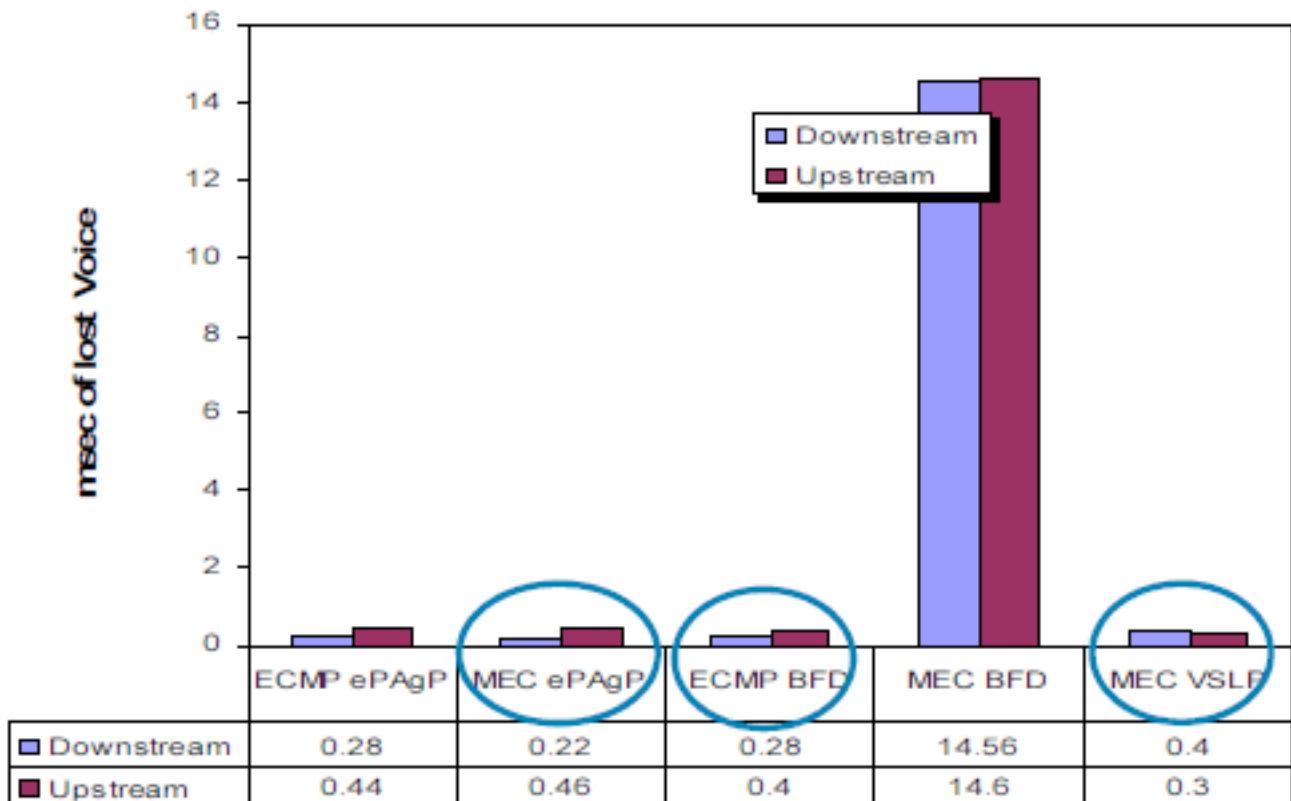


ートされています。

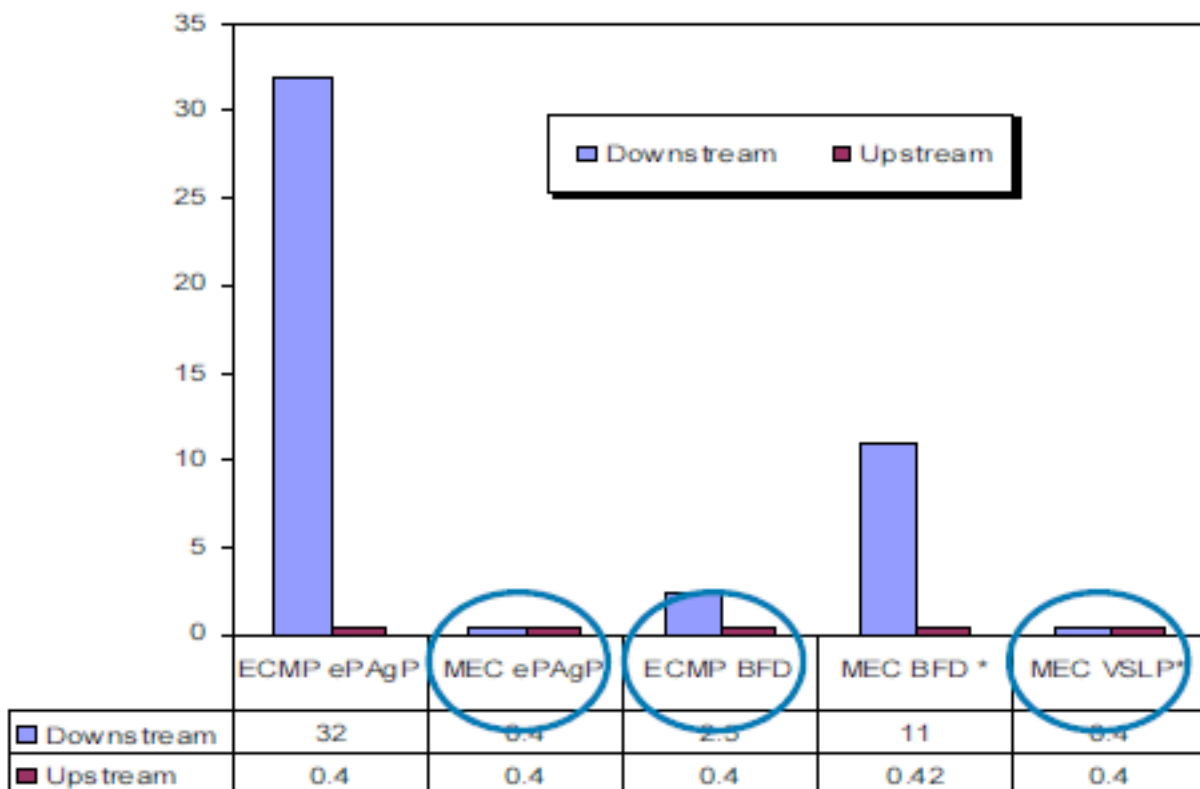
3 つの検出方式を、すべて同時にアクティブに設定できます。

以下のグラフは、VSS デュアル アクティブ コンバージェンスに関する一部の IP ルーティング プロトコルのコンバージェンス情報を示しています。

デフォルト タイマーを使用した EIGRP コンバージェンス



デフォルト タイマーを使用した OSPF コンバージェンス



推奨事項

- VSL では少なくとも 2 つのリンクを有効にします。
- より高速な VSL リンク損失のコンバージェンス結果のためには、ePAgP を使用した MEC または VSLP Fast Hello を使用した MEC を使用します。
- IP-BFD を使用した ECMP をイネーブルにします。

- アクセスレイヤが ePAgP に対応していない場合は、コアに対して ePAgP を有効にします。
- 可能な場合は、ePAgP と直接ハードビート リンクの両方をベースとした VSLP Fast Hello 方法を有効にします。
- VSL 損失およびリカバリ プロセス中は、設定変更を行わないでください。少なくとも 1 つの VSL メンバリンクが回復した後、元の ACTIVE シャーシでの設定が**変更されていない場合**、元の ACTIVE シャーシによって**自身のリブートが行われ**、ホットスタンバイ冗長性の状態で VSS 内でブートされます。

```
*Apr 6 17:36:33:809: %VSLP-SW1_SP-5-VSL_UP: Ready for Role Resolution with Switch=2, MAC=0013a.30e1.6800 over Tel/5/5
```

```
*Apr 6 17:36:36.109: %dualACTIVE-1-VSL_RECOVERED: VSL has recovered during dual ACTIVE situation: Reloading switch 1
```

```
!--- part of output truncated *Apr 6 17:36:36.145: %VSLP-SW1_SP-5-RPR_MSG: Role change from ACTIVE to HOT_STANDBY and hence need to reload *Apr 6 17:36:36.145: %VSLP-SW1_SP-5-RPR_MSG: Reloading the system...
```

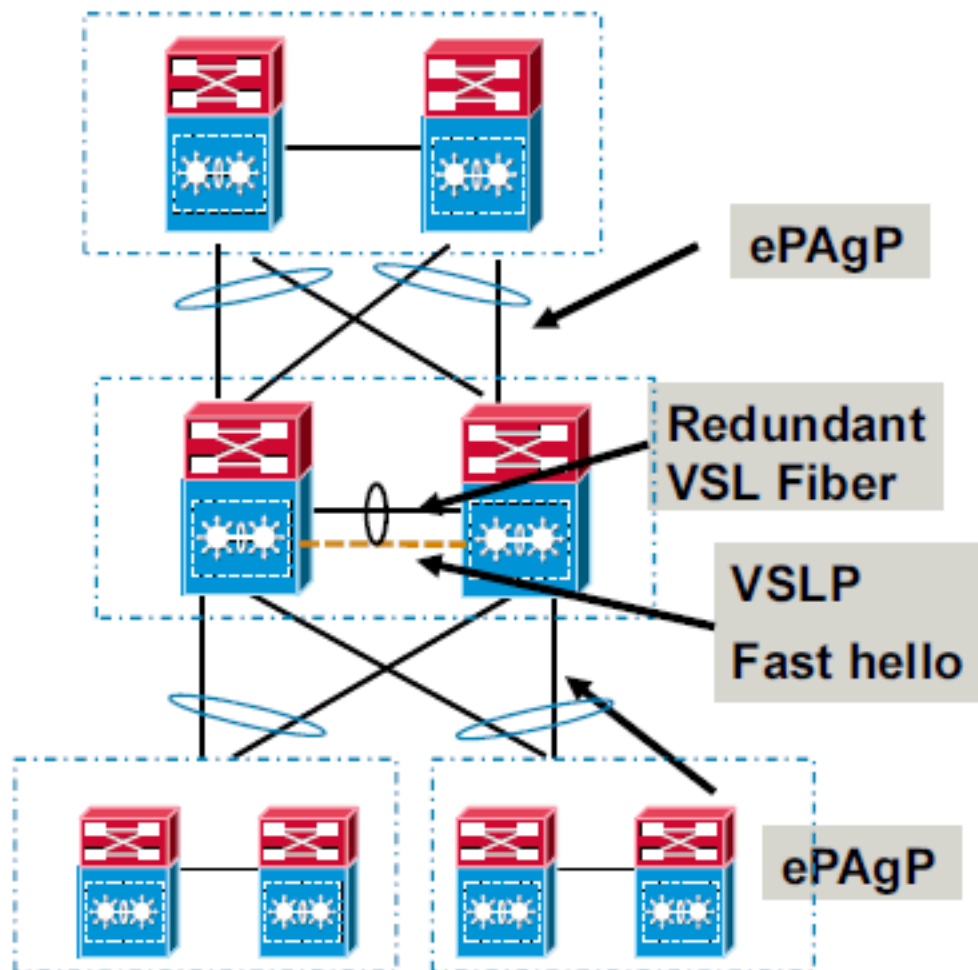
```
*Apr 6 17:36:36.145: %SYS-SW1_SP-5-RELOAD: Reload requested Reload Reason: VSLP HA role change from ACTIVE to HOT_STANDBY.
```

設定が変更されている (設定の同期プロセスによって *dirty* とマークが付けられている) 場合、スイッチでは自動的にリロードが行われません。この場合、設定を修正して保存した後に、古い ACTIVE でリロードを手動で実行する必要があります。コンフィギュレーションモードに切り替えた直後に終了した場合でも、設定には *dirty* とマークが付けられ、手動による介入が強制されます。

```
*Aug 13 04:24:34.716: %dualACTIVE-1-VSL_RECOVERED: VSL has recovered during dual ACTIVE situation: Reloading switch 2
```

```
*Aug 13 04:24:34.716: %VS_GENERIC-5-VS_CONFIG_DIRTY: Configuration has changed. Ignored reload request until configuration is
```

saved



詳細は、『[デュアル アクティブ 検出](#)』を参照してください。

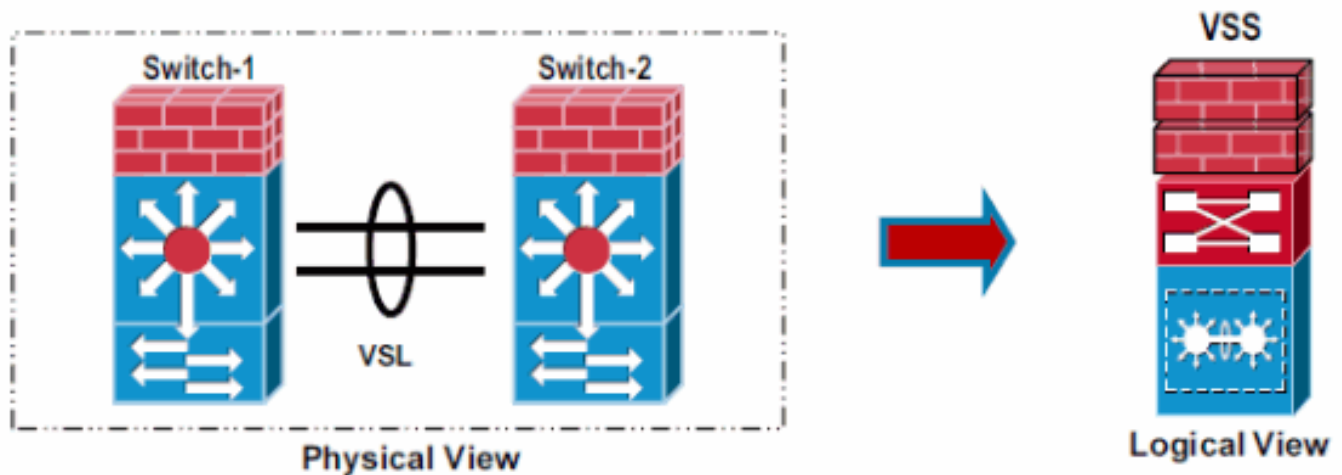
サービス モジュールでの冗長性

サービス モジュールのサポートは、VSS を企業キャンパスおよび企業データセンターの市場に位置付けるための重要な要件です。仮想スイッチ システムでサポートされるサービス モジュールの一覧は次のとおりです。

サービス モジュール	最小 Cisco IOS リリース	最低限のモジュール リリース
Network Analysis Module (NAM) (NAM-1 および NAM-2) (WS-SVC-NAM-1 および WS-SVC-NAM-2)	12.2(33)SXH1	3.6(1a)
アプリケーション コントロール エンジン (ACE10 および ACE20) (ACE10-6500-K9 および ACE20-MOD-K9)	12.2(33)SXI	A2(1.3)
侵入検知システム (IDS) サービス モジュール (IDSM-2) (WS-SVC-IDSM2-K9)	12.2(33)SXI	6.0(2)E1
ワイヤレス サービス モジュール	12.2(33)	3.2.171.6

(WiSM) (WS-SVC-WISM-1-K9))SXI	
ファイアウォール サービス モジュール (FWSM) (WS-SVC-FWM-1-K9)	12.2(33))SXI	4.0.4

サービス モジュールは、VSS を設定している物理シャーシのいずれかに取り付けることができます。



推奨事項

- 特定のタイプのサービス モジュールを 1 つだけ使用する設定の場合、可用性を最大限にするために、物理スイッチごとにその特定のタイプのサービス モジュールを設定します。
- VSL はトラフィックを通常のシナリオとフェースオーバー シナリオで伝送する場合、VSL 帯域幅をそれぞれのシナリオに応じてチューニングする必要があります。

サービス モジュール統合についての詳細は、『[Cisco サービス モジュールの Cisco Catalyst 6500 Virtual Switching System 1440 への統合](#)』を参照してください。

マルチキャスト

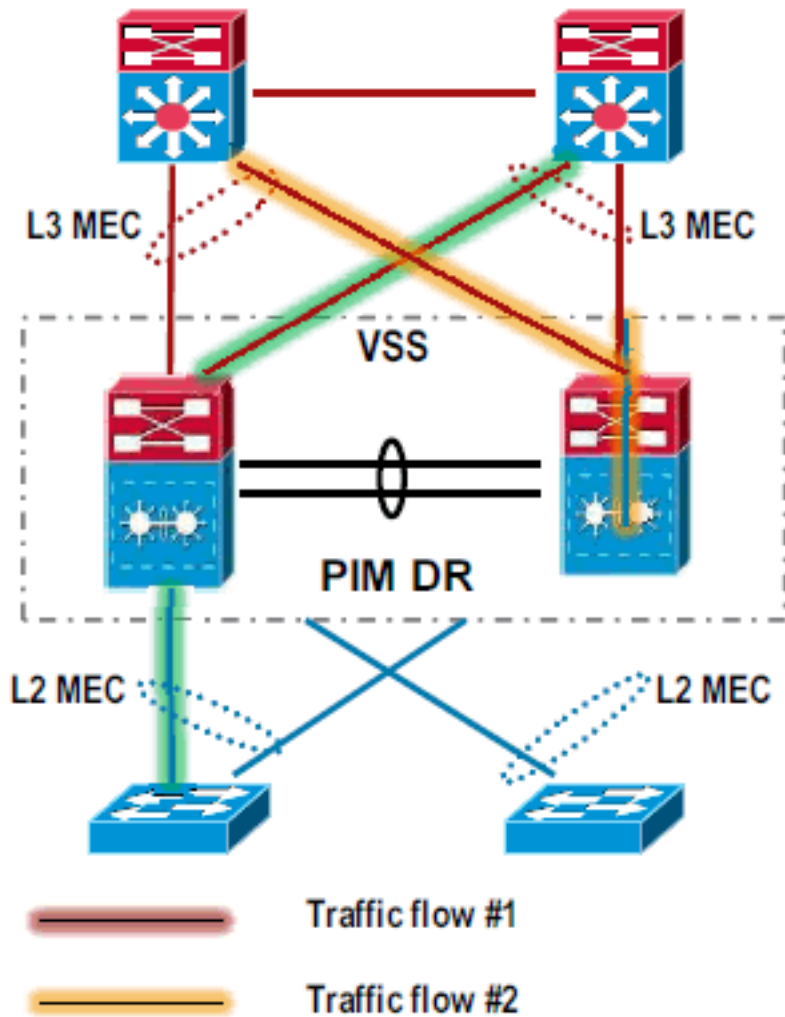
IPv4 マルチキャスト プロトコルは、アクティブ スーパーバイザ エンジン上で実行されます。スタンバイ スーパーバイザ エンジンで受信したインターネット グループ管理プロトコル (IGMP) および Protocol Independent Multicast (PIM) プロトコル パケットは、VSL を通じてアクティブ シャーシに送信されます。アクティブ スーパーバイザ エンジンには、ステートフル スイッチオーバー (SSO) のためのレイヤ 2 情報を維持するために、スタンバイ スーパーバイザ エンジンに IGMP および PIM プロトコル パケットを送信します。

詳細は、『[IPv4 マルチキャスト](#)』を参照してください。

推奨事項

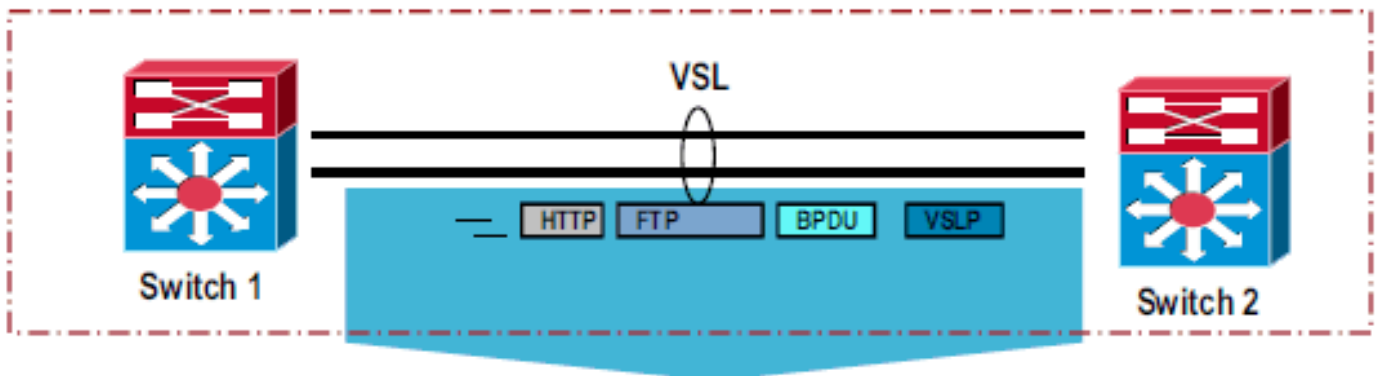
- 接続されたデバイスは、最適な複製パフォーマンスのために常にデュアル ホームである必要があります。
- L3 と L2 の環境では、決定論的なコンバージェンスを提供するために、MEC が推奨されます。
- MEC を使用すると、MEC リンク障害時にリバース パス フォワーディング (RPF) の再計算が行われません。

- より高度なマルチキャスト複製スループットのためのローカルの機能拡張を使用した出力の複製。
- 最適な複製パフォーマンスを達成するためには、出力複製に DFC が必要です。
- トラフィック要件を満たすように VSL のサイズを決定します。



Quality of Service (QoS)

VSL の QoS 設定



- VSL は重要な内部制御およびデータ通信パスであるため、QoS は事前設定されており、設定の変更は許可されません。
- VSL は常に Trust CoS として設定され、入力キューイングがイネーブルになっています。
- 現在、Cos ベースのトラストおよびキューイングがサポートされています。サービス ポリシ

- ーは、VSL ではサポートされません。
- QoS ポリシーはフローの入カインターフェイスで適用する必要があります。
- プライオリティ キューはデフォルトで有効になっています。VSS 制御トラフィックと BPDU には VSL リンクで高プライオリティが割り当てられます。

推奨事項

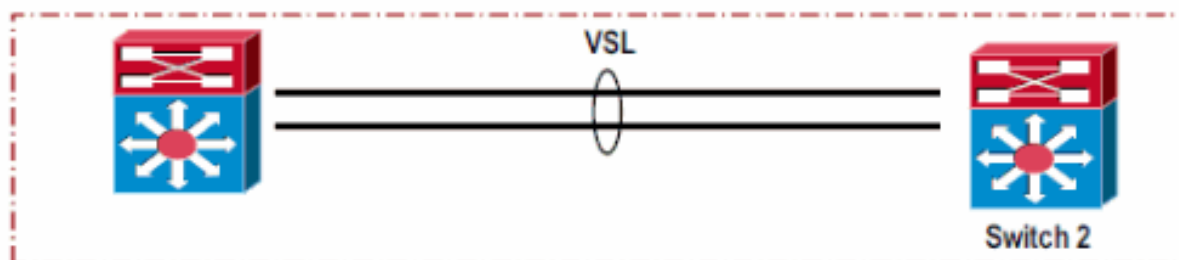
VSL 対応ハードウェアのオプションの間で異なるのは、キュー設定のみです。現在のソフトウェアリリースでは、デフォルト キューの設定を変更することはできません。どの VSL 対応ポートの組み合わせでも、QoS は同じ結果になります。

ハードウェア	キュー イング モード	トラ スト モード	送信キュー	受信 キュー
アップリンク上の VSL : 非 10G のみ (デフォルト)	CoS	CoS	1p3q4t (DWRR /SRR)	8q4t
アップリンク上の VSL : 10G のみ	CoS	CoS	1p7q4t (DWRR /SRR)	2q4t
アップリンクおよびラインカード間の VSL	CoS	CoS	1p3q4t [非 10G] (DWRR/SRR) 1p7q4t [10G のみ] (DWRR/SRR)	2q4t
ラインカード上の VSL	CoS	CoS	1p7q4t (DWRR /SRR)	8q4t

詳細は、『[VSL QoS の設定](#)』を参照してください。

SPAN

仮想スイッチ ドメインでは、SPAN セッションの数が仮想スイッチのアクティブ スーパーバイザの機能によって制限されます。



VS State : Active
 Control Plane: Active
 Data Plane: Active
 SPAN Management: Active
 SPAN Replication: Active

VS State : Standby
 Control Plane: Standby
 Data Plane: Active
 SPAN Management: In-Active
 SPAN Replication: Active

仮想スイッチ システムは、仮想スイッチ ドメインごとに以下の SPAN 機能をサポートします。

属性	値
Tx SPAN セッション数	14
Rx または両 SPAN セッション数	0
SPAN セッションの合計数	16

推奨事項

- VSL がローカル SPAN 送信元として設定されている場合、SPAN 宛先ポートは VSL インターフェイスと同じシャーシ上になければなりません。
- VSL を SPAN 宛先として設定することはできません。
- VSL を RSPAN、ERSPAN、または Tx 専用ローカル SPAN の送信元として設定することはできません。
- VSL ヘッダーはパケットが送信される間に SPAN 宛先ポートで削除されるため、スニファトレースで VSL ヘッダーをキャプチャすることはできません。
- 送信元と宛先が両方とも同じシャーシ (アクティブまたはスタンバイ) にある場合、SPAN トラフィックは VSL リンクで送信されません。両方のシャーシからのトラフィックをキャプチャするために、VSL 上の SPAN トラフィック フローを回避するオプションが 2 つあります。シャーシ上の送信元インターフェイスごとに、同じシャーシ上の宛先インターフェイスを対応させる必要があります。たとえば、PO20 に gi1/1/1 と gi2/1/1 がある場合、シャーシごとに 1 つの宛先が必要です。

```
Monitor session 1 source interface gi1/1/1
Monitor session 1 destination interface gi1/1/2
```

```
Monitor session 2 source interface gi2/1/1
Monitor session 2 destination interface gi2/1/2
```

ただし、これは両方のローカル SPAN セッションを使用することを意味します。したがって、他のローカル SPAN セッションは使用できません。SPAN の宛先インターフェイスを MEC として使用できます (推奨)。宛先ポートは MEC にすることができます。

その他

推奨事項

- VSL の起動時間を短縮するために、VSL には少なくとも 1 つのスーパーバイザ アップリンクを使用してください。
- VSS 変換の後に、**switch accept mode virtual** コマンドを設定します。このコマンドを使用しないと、変換が完了しません。
- 設定ファイルのバックアップをアクティブ ブート ディスクとホットスタンバイ ブート ディスクの両方に保存します。こうしておくと、スーパーバイザの交換シナリオで非常に役立ちます。
- 同じネットワーク内では一意の VSS ドメイン ID を使用します。VSS ドメイン ID が重複すると EtherChannel の不一致が発生する場合があります。以下に、VSS ドメイン ID を変更する例を示します。ドメイン ID の変更を開始するには、[switch virtual domain domain-id コマンドを使用します。](#)

```
switch(config)#switch virtual domain 50
```

注：ドメイン ID 50 の設定は、**switch convert mode virtual exec** コマンドが発行された後の

み有効になります。タスクを完了するには、[switch convert mode virtual コマンドを使用します。](#)

```
switch#switch convert mode virtual
```

注：仮想ドメインIDは、設定を保存してスイッチをリロードした後にのみ変更されます。

- VSS 設定をリセットするには、**write erase** コマンドではなく、**erase nvram** コマンドを使用します。**write erase** コマンドでは、startup-config と ROMMon の変数が消去されてしまいます。VSS モードで起動するためには、VSS に *switch-id* ROMMon 変数が必要です。
 - プリエンプションは使用しないでください。詳細については、[スイッチプリエンプションを設定しないよう推奨する理由を参照してください。](#)
 - 設定のミスマッチの原因となるため、VSL 障害のシミュレーションには、**shutdown** コマンドを使用しないでください。ケーブルを切断すると、より現実的な障害シナリオになります。
 - システムの実稼働中は、VSL ハッシュ アルゴリズムを変更しないでください。アルゴリズムの変更には、**shutdown** コマンドと **no shutdown** コマンドを使用して、ポート チャネルをディセーブルにした後に再びイネーブルにする必要があります。VSL をシャットダウンすると、トラフィックが中断されてデュアル アクティブ シナリオになる可能性があります。
 - MAC エージング タイマーを MAC 同期タイマー値の 3 倍の値に設定します。デフォルトの MAC 同期タイマーおよび MAC エージング タイマーを使用すると、不明ユニキャスト フラッディングが発生する可能性があります。VSS によってトラフィック フローが非同期になり、送信先 MAC アドレスが 1 つのシャーシでのみ学習される場合があります。MAC エージング タイマーを 300 秒に設定し、MAC 同期タイマーを 160 秒に設定すると、所定の MAC アドレスに対して 320 秒間隔で最大 20 秒の不明ユニキャスト フラッディングが許可されます。これを解決するには、エージング タイマー値が同期タイマー値の 3 倍になるように設定を変更します (たとえば、[mac-address-table aging-time 480](#))。以下に、[show mac-address-table aging-time の出力例を示します。](#)
- ```
switch#sh mac-address-table aging-time
Vlan Aging Time

Global 480
no vlan age other than global age configured
```
- VSS をステートフル スイッチオーバー (SSO) と連動させるには、両方のスーパーバイザ エンジンが同じソフトウェア バージョンで稼働している必要があります。
  - 以下のタスクを完了するには、[switch convert mode stand-alone](#) コマンドを使用してスイッチを VSS モードからスタンドアロンに戻します。インターフェイス名を **switch/slot/port** から **slot/port** に変更する実行中の設定から非ローカル インターフェイスを削除する VSL ポート チャネルとポート設定を削除する実行中の設定をスタートアップ設定に保存する SP rommon 変数 SWITCH\_NUMBER を 0 に設定するスイッチをリロードする
  - スイッチのリブートは、どうしても必要な場合に行います。たとえば、IOS をアップグレードする場合や、トラブルシューティングのステップとしてリブートを行う場合です。2 年以上アップ状態を維持しているスイッチは、安定したスイッチであり、設定も同じく安定しています。

## [よく寄せられる質問 \(FAQ\)](#)

### [VSS ではシャーシごとにデュアル スーパーバイザを使用できますか](#)

はい。VSS モード用に設定された各 VSS シャーシ内のデュアル スーパーバイザは、SX14 以降でサポートされます。

## VSS モードの Catalyst 6500 シリーズ スイッチから preempt コマンドを削除すると、スイッチがリロードされますか

スイッチ プリエンプションは推奨されません。したがって、このコマンドを削除することが得策です。このコマンドを削除してもリロードは行われません。VSS でのプリエンプション機能の詳細については、[スイッチプリエンプション](#)を参照してください。

## **関連情報**

- [Cisco IOS が動作している Catalyst 6500/6000 シリーズおよび Catalyst 4500/4000 シリーズ スイッチのベスト プラクティス](#)
- [Virtual Switching System の設定](#)
- [Cisco IOS 仮想スイッチ コマンド リファレンス](#)
- [Cisco Catalyst 6500 Virtual Switching System 1440 製品に関するサポート ページ](#)
- [LAN スイッチ製品のサポート](#)
- [LAN スイッチング テクノロジーに関するサポート ページ](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)