

# Best Practices für die Bereitstellung des Cisco Catalyst 6500 Virtual Switching System

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Best Practices für die VSS-Bereitstellung](#)

[Hohe VSS-Verfügbarkeit](#)

[Upstream-Link-Wiederherstellung](#)

[VSL-Link-Verlust und -Wiederherstellung](#)

[Redundanz mit Dienstmodulen](#)

[Multicast](#)

[Quality of Service](#)

[SPAN](#)

[Verschiedenes](#)

[Häufig gestellte Fragen](#)

[Können in jedem Chassis mit VSS zwei Supervisoren verwendet werden?](#)

[Werden die Switches beim Entfernen der Freischaltbefehle in Catalyst Switches der Serie 6500 im VSS-Modus neu geladen?](#)

[Zugehörige Informationen](#)

## **[Einführung](#)**

Dieses Dokument enthält Best Practices für Cisco Catalyst 6500 Virtual Switching System (VSS) 1440-Bereitstellungsszenarien.

Dieses Dokument enthält Anleitungen zur modularen Konfiguration. Daher können Sie jeden Abschnitt einzeln lesen und Änderungen in einem stufenweisen Ansatz vornehmen. In diesem Dokument wird davon ausgegangen, dass die Benutzeroberfläche der Cisco IOS® Software allgemein verständlich und bekannt ist. Das Dokument behandelt nicht das allgemeine Netzwerkdesign.

## **[Voraussetzungen](#)**

## **[Anforderungen](#)**

Es gibt keine spezifischen Anforderungen für dieses Dokument.

## Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

## Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions \(Technische Tipps von Cisco zu Konventionen\)](#).

## Best Practices für die VSS-Bereitstellung

Die Lösungen, die dieses Dokument bietet, beinhalten eine jahrelange Erfahrung von Cisco Technikern, die mit komplexen Netzwerken arbeiten, sowie von vielen der größten Kunden. Daher wird in diesem Dokument der Schwerpunkt auf Konfigurationen gelegt, die Netzwerke zum Erfolg verhelfen. Dieses Dokument bietet folgende Lösungen:

- Einfache Verwaltung und Konfiguration durch Netzwerkbetriebsteams
- Lösungen zur Förderung von Hochverfügbarkeit und hoher Stabilität

## Hohe VSS-Verfügbarkeit

- [Weiterleitung ohne Stopp](#)
- [OOB MAC-Synchronisierung](#)

## Weiterleitung ohne Stopp

Catalyst Switches der Serie 6500 unterstützen Fehlerresistenz, da sie eine redundante Supervisor Engine bei Ausfall der primären Supervisor Engine unterstützen. Cisco Non Stopp Forwarding (NSF) arbeitet mit Stateful SwitchOver (SSO) zusammen, um die Zeit zu minimieren, die ein Netzwerk nach einem Switchover für seine Benutzer nicht verfügbar ist, während IP-Pakete weitergeleitet werden.

## **Empfehlungen**

- Die Non-Stopp-Weiterleitung ist für die Konvergenz des Supervisor-Switchover in Sekundenbruchteilen erforderlich.
- Verwenden Sie Hello- und Dead-Standard-Timer für EIGRP-/OSPF-Protokolle, wenn Sie in einer VSS-Umgebung ausführen.
- Wenn Sie das System mit der modularen Cisco IOS-Software ausführen, wird empfohlen, einen OSPF-Dead-Timer mit größerem Wert zu verwenden.

## **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
```

Weitere Informationen zu NSF finden Sie unter [Konfigurieren von NSF mit SSO Supervisor Engine Redundancy \(SSO-Supervisor Engine-Redundanz\)](#).

## OOB MAC-Synchronisierung

Bei verteilten Switches unterhält jede Distributed Feature Card (DFC) eine eigene CAM-Tabelle. Das bedeutet, dass jede DFC die MAC-Adresse erfasst und altert. Dies hängt von der CAM-Alterung und der Datenverkehrsabstimmung für diesen Eintrag ab. Bei verteiltem Switching sieht die Supervisor Engine normalerweise eine Weile keinen Datenverkehr für eine bestimmte MAC-Adresse, sodass der Eintrag ablaufen kann. Derzeit stehen zwei Mechanismen zur Verfügung, um die CAM-Tabellen zwischen den verschiedenen Engines konsistent zu halten, z. B. DFC (in Leitungsmodulen vorhanden) und Policy Feature Card (PFC) in Supervisor-Modulen:

- Flood to Fabric (FF)
- MAC-Benachrichtigung (MN)

Wenn ein MAC-Adresseneintrag im PFC ausgewiesen wird, zeigt der Befehl **show mac-address**

**<MAC\_Address> all** den Befehl DFC oder PFC an, der diese MAC-Adresse enthält. Um zu verhindern, dass ein Eintrag in einer DFC- oder PFC-Adresse veraltet wird, aktivieren Sie die Synchronisierung der MAC-Adresse, selbst wenn kein Datenverkehr für diese MAC-Adresse vorliegt. Geben Sie die **MAC-Adresstabelle zur Synchronisierung des globalen**

Konfigurationsbefehls und des Befehls **clear mac-address-table dynamic** privileged EXEC aus, um die Synchronisierung zu aktivieren. Dieser Befehl zur Synchronisierung der MAC-Adresstabelle ist in den Cisco IOS Software Releases 12.2(18)SXE4 und höher verfügbar. Nach der Aktivierung können Einträge angezeigt werden, die in PFC oder DFC nicht vorhanden sind. Das Modul kann es jedoch auch von anderen Benutzern lernen, die Ethernet Out of Band Channel (EOBC) verwenden.

## Empfehlungen

Aktivieren Sie die Out-of-Band-MAC-Synchronisierung. Sie wird verwendet, um MAC-

Adresstabellen über die Weiterleitungs-Engines hinweg zu synchronisieren. Wenn im VSS-System WS-6708-10G vorhanden ist, wird die MAC-Synchronisierung automatisch aktiviert. Ist dies nicht der Fall, muss die Funktion manuell aktiviert werden.

```
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-Terminologie

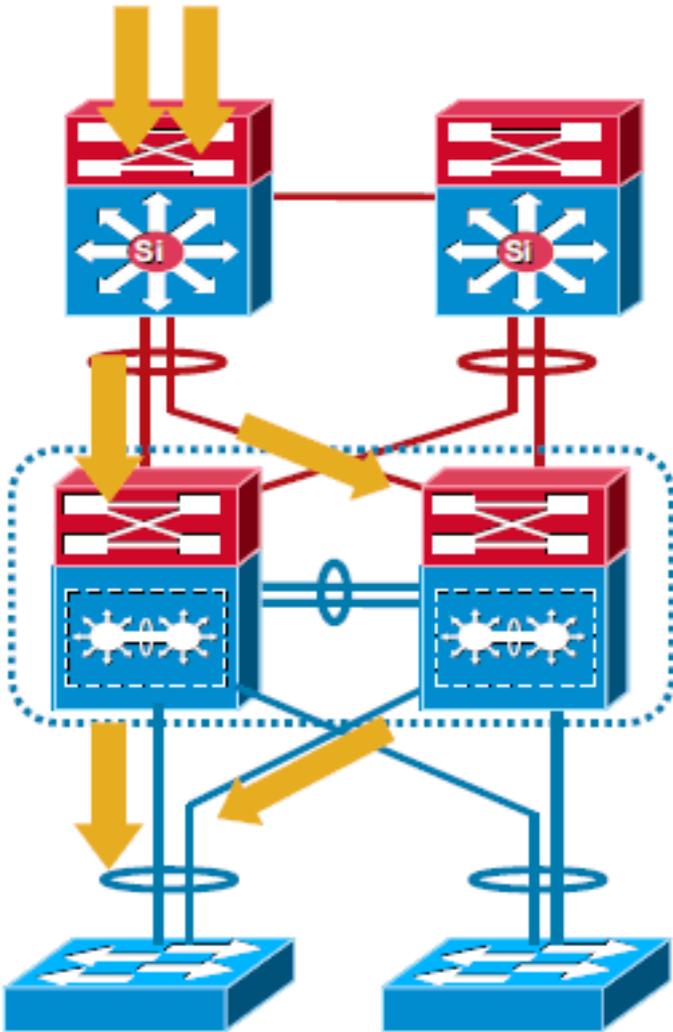
- **Virtual Switch Link (VSL)** - Ein spezieller Port-Channel, der erforderlich ist, um zwei physische Switches in einem virtuellen Switch zu bündeln.
- **VSL Protocol (VSLP)** - Wird zwischen aktivem und Standby-Switch über VSL ausgeführt und besteht aus zwei Komponenten: LMP und RRPLink Management Protocol (**LMP**) - wird über jede einzelne Verbindung in VSL ausgeführtRRP (**Role Resolution Protocol**) - wird auf jeder Seite (pro Peer) des VSL-Port-Channels ausgeführt.

## Kapazitätsplanung für VSL

Im Idealfall wird in der Dual-Homed-VSS-Konfiguration kein Datenverkehr über die VSL-Verbindung gesendet. Jeder Switch ist so programmiert, dass er seine lokalen Schnittstellen für die Weiterleitung des Datenverkehrs auswählt.

Zusätzliche VSL-Kapazitätsplanung ist für Datenverkehr erforderlich, der von:

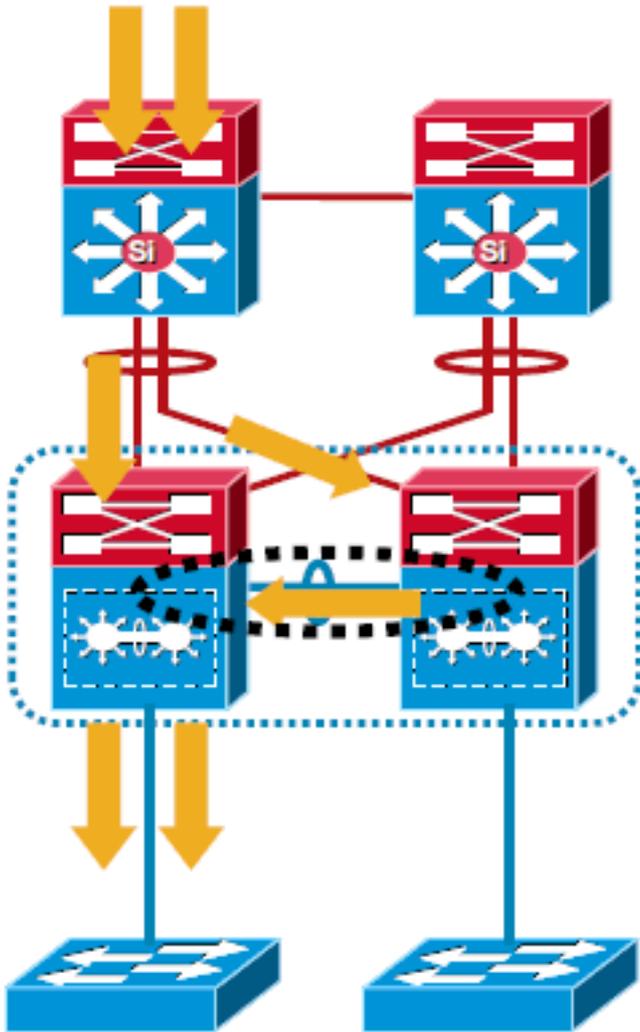
- Single-Homed-Geräte
- Remote-SPAN von einem Switch zu einem anderen
- Dienstmodul-Verkehr " FWSM, ACE, etc.



Weitere Informationen finden Sie unter [Datenverkehr auf dem VSL](#).

## Empfehlungen

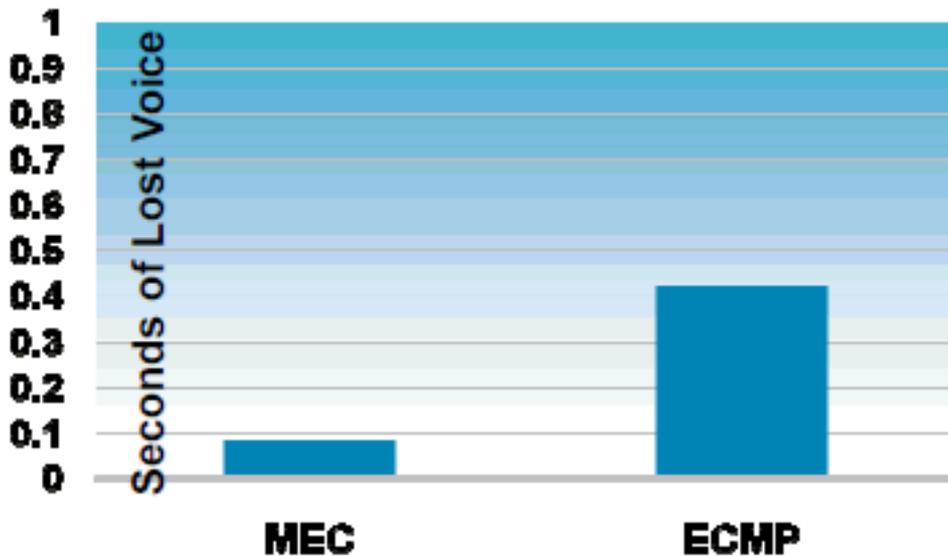
- Immer mit VSS verbundene **Dual-Home-Geräte**
- **VSL-EtherChannel** immer mit einer Leistung von 2 Bündeln, da die Hash-Ergebnisse für eine optimierte Lastverteilung des Datenverkehrs optimiert werden.
- Neben der Ausfallsicherheit von VSL-Verbindungen ist die Redundanz des VSL nach wie vor entscheidend.
- Es wird empfohlen, mindestens über eine VSL-Bandbreite zu verfügen, die den Uplinks entspricht, die mit einem einzigen physischen Switch verbunden sind.



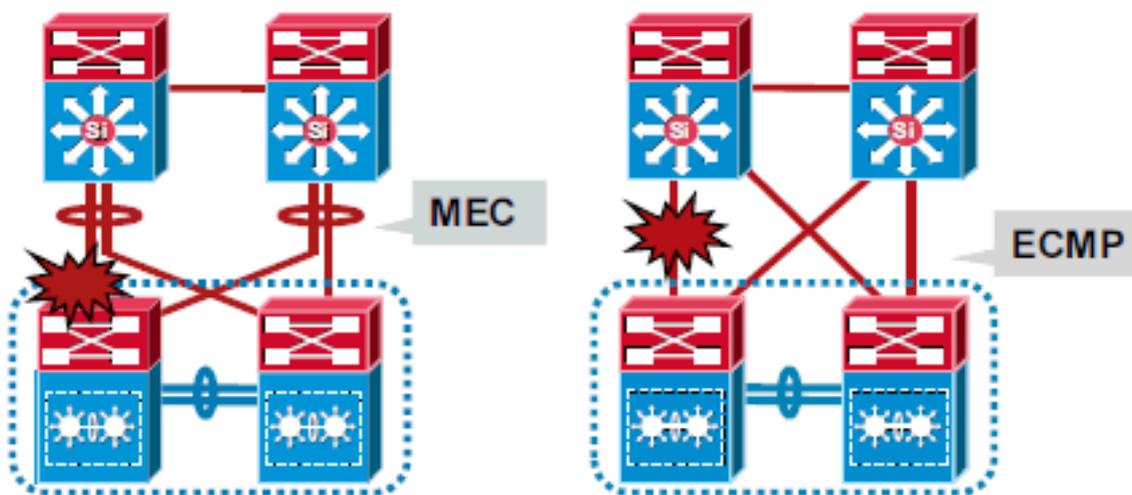
## Upstream-Link-Wiederherstellung

Die Wiederherstellung von Upstream-Verbindungen (Verbindungen zum Core) kann entweder über MultiChassis EtherChannel (MEC) oder die Equal Cost MultiPath (ECMP)-Funktion erreicht werden.

Die MEC-Konvergenz ist **konsistent und unabhängig** von der Anzahl der Routen. Die ECMP-Konvergenz **hängt** von der Anzahl der Routen ab. Dieses Diagramm zeigt das Ausmaß des Verlustes in einer Sprachsituation.



Diese Bilder zeigen Szenarien für Verbindungsausfälle mit MEC und ECMP:



### Multi-Chassis-EtherChannel

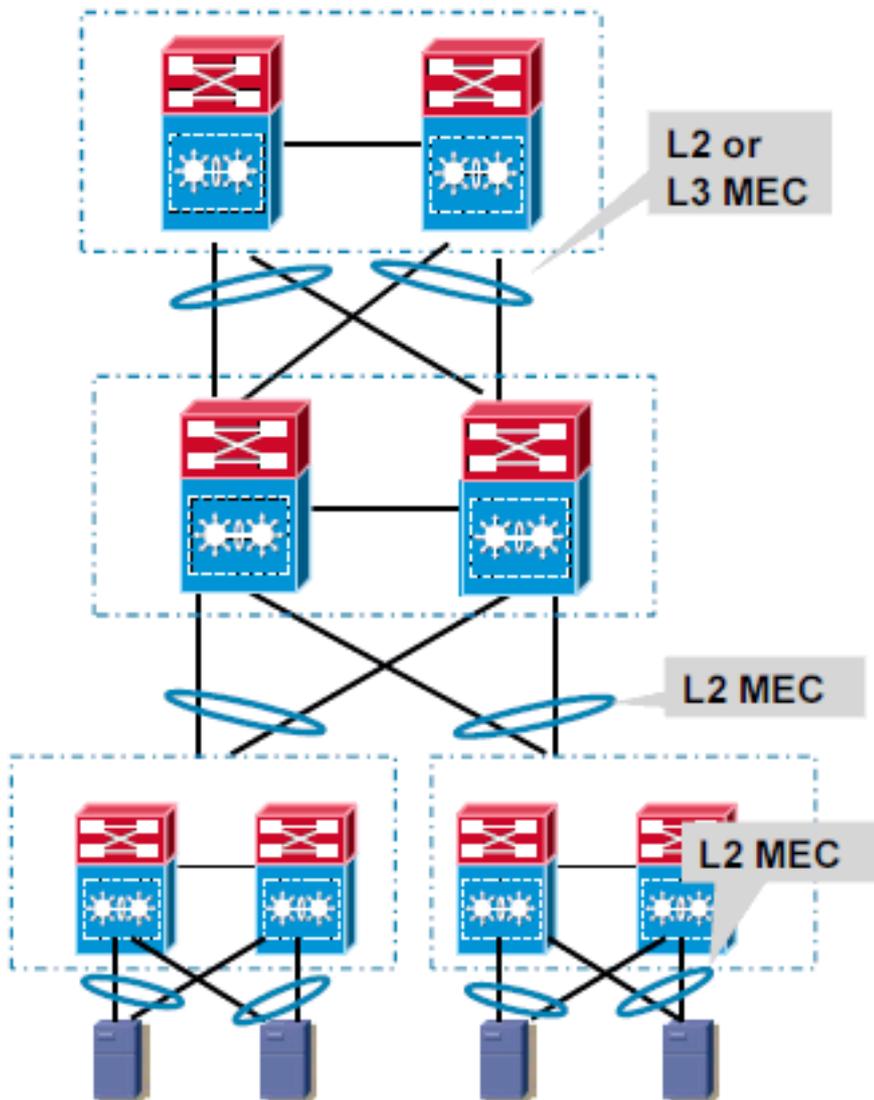
Ein Multi-Chassis-EtherChannel ist ein EtherChannel mit Ports, die auf beiden Chassis des VSS terminieren. Ein VSS MEC kann eine Verbindung zu jedem Netzwerkelement herstellen, das EtherChannel unterstützt, z. B. einen Host, Server, Router oder Switch. Beim VSS ist ein MEC ein EtherChannel mit zusätzlicher Funktionalität. Das VSS verteilt die Last auf die Ports in den einzelnen Chassis unabhängig voneinander. Wenn beispielsweise Datenverkehr in das aktive Chassis gelangt, wählt das VSS eine MEC-Verbindung aus dem aktiven Chassis aus. Diese MEC-Funktion stellt sicher, dass der Datenverkehr nicht unnötig die VSL passiert.

- L2 MEC ermöglicht eine schleifenfreie Topologie, verdoppelt die Uplink-Bandbreite, da keine Verbindungen blockiert werden, und bietet eine schnellere Konvergenz als STP.
- L3 MEC bietet geringere Nachbar-Anzahl, bessere Lastverteilung (L2 und L3 für Unicast und Multicast), geringere VSL-Verbindungsauslastung für Multicast-Datenströme und schnellere Konvergenz als ECMP.

Weitere Informationen zu MEC finden Sie unter [Multichassis EtherChannels](#).

### Empfehlungen

- Führen Sie immer **L2 oder L3 MEC** aus.
- Verwenden Sie keine **Ein-** und **Aus-**Optionen bei der PAgP- oder LACP- oder Trunk-Protokollverhandlung. PAgP â€" Führen Sie **Desirable-Desirable** mit MEC Links aus. LACP â€" Führen Sie **Active-Active** mit MEC-Links aus. Trunk â€" Ausführen **Desirable-Desirable** mit MEC Links.



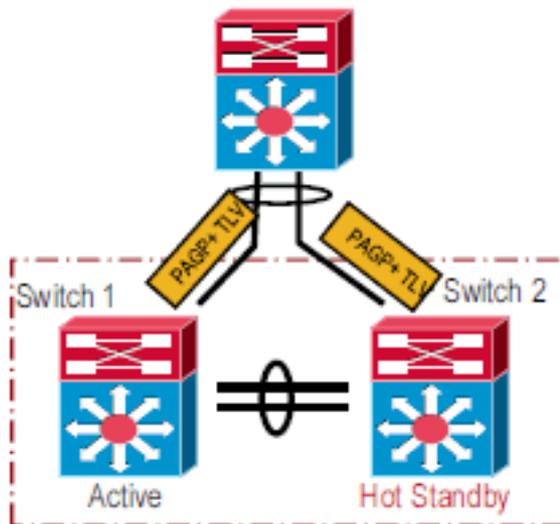
## VSL-Link-Verlust und -Wiederherstellung

Wenn das VSL ausfällt, kann das Standby-Chassis den Zustand des aktiven Chassis nicht bestimmen. Um sicherzustellen, dass der Switchover ohne Verzögerung erfolgt, geht das Standby-Chassis von einem Ausfall des aktiven Chassis aus und initiiert einen Switchover, um die aktive Rolle zu übernehmen.

Wenn das ursprüngliche aktive Chassis noch betriebsbereit ist, sind beide Chassis jetzt aktiv. Diese Situation wird als **Dual-Active**-Szenario bezeichnet. Ein Dual-Active-Szenario kann sich nachteilig auf die Netzwerkstabilität auswirken, da beide Chassis dieselben IP-Adressen, SSH-Schlüssel und STP Bridge-ID verwenden. Das virtuelle Switching-System (VSS) muss ein Dual-Active-Szenario erkennen und Wiederherstellungsmaßnahmen ergreifen.

Das virtuelle Switching-System unterstützt die folgenden drei Methoden, um ein Dual-Active-Szenario zu erkennen:

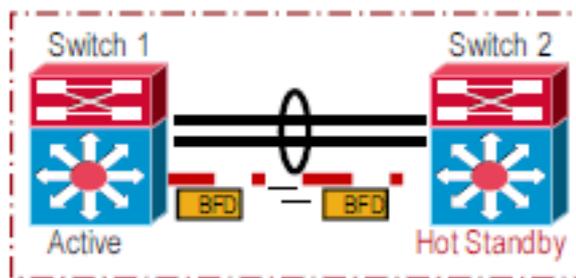
- Enhanced PAgP " verwendet PAgP-Messaging über die MEC-Verbindungen, um zwischen den beiden Chassis über einen Nachbarswitch zu kommunizieren. Enhanced PAgP ist schneller als IP BFD, erfordert jedoch einen Nachbarswitch, der die PAgP-Erweiterungen



unterstützt.

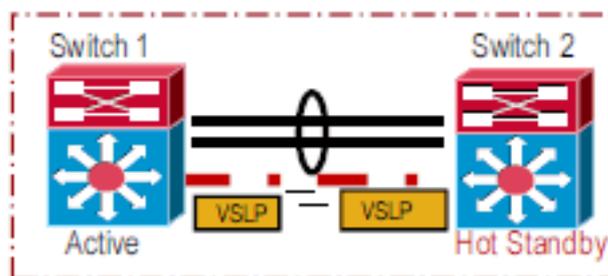
ePAgP-Unterstützungstabelle:

- IP Bidirectional Forwarding Detection (BFD) " verwendet BFD-Messaging über eine Backup-Ethernet-Verbindung. IP BFD verwendet eine direkte Verbindung zwischen den beiden Chassis und benötigt keine Unterstützung von einem Nachbarswitch. Diese Methode ist ab der Cisco IOS-Softwareversion 12.2(33)SXH1



verfügbar.

- VSLP Dual-Active Fast-hello " Verwendet spezielle Hello-Nachrichten über eine Backup-Ethernet-Verbindung. Dual-Active Fast-Hello ist schneller als IP BFD und erfordert keine Unterstützung von einem Nachbarswitch. Diese Methode ist nur in der Cisco IOS Software

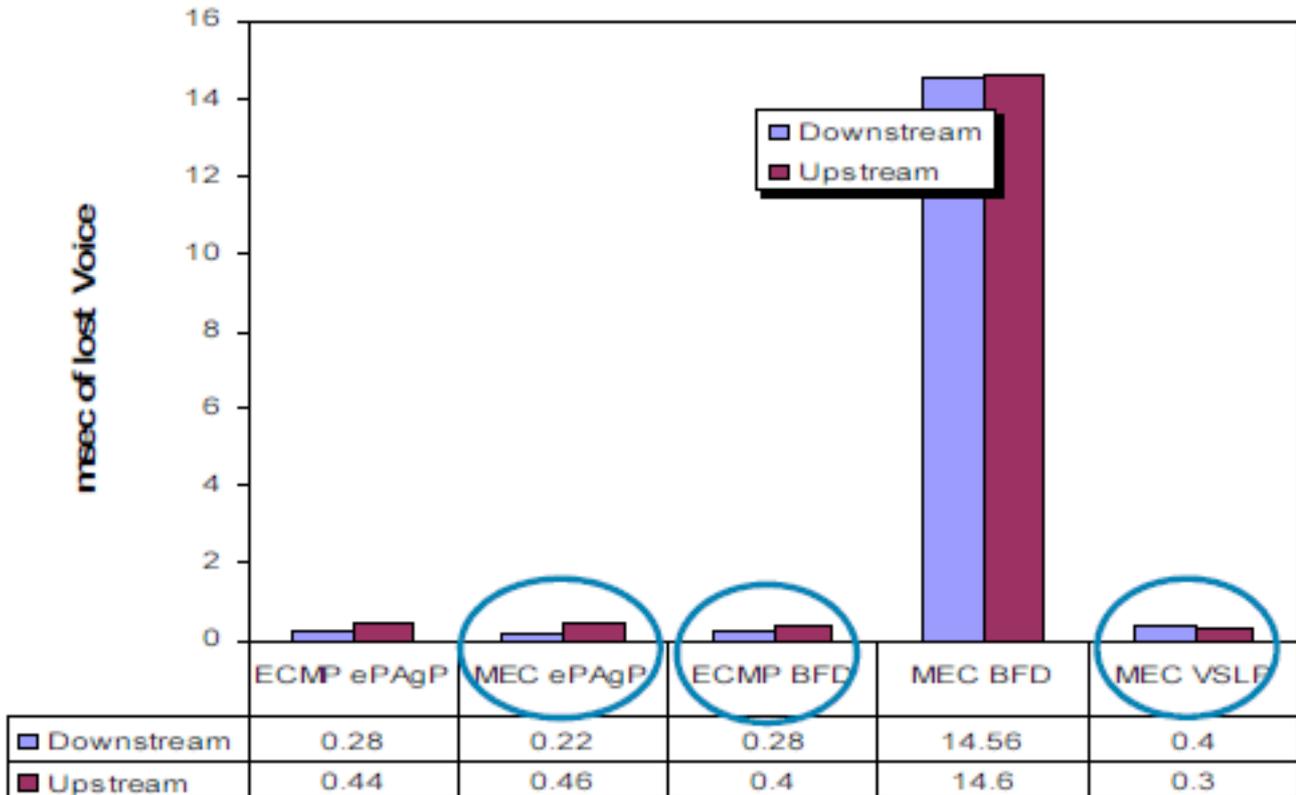


Version 12.2(33)SXI und höher verfügbar.

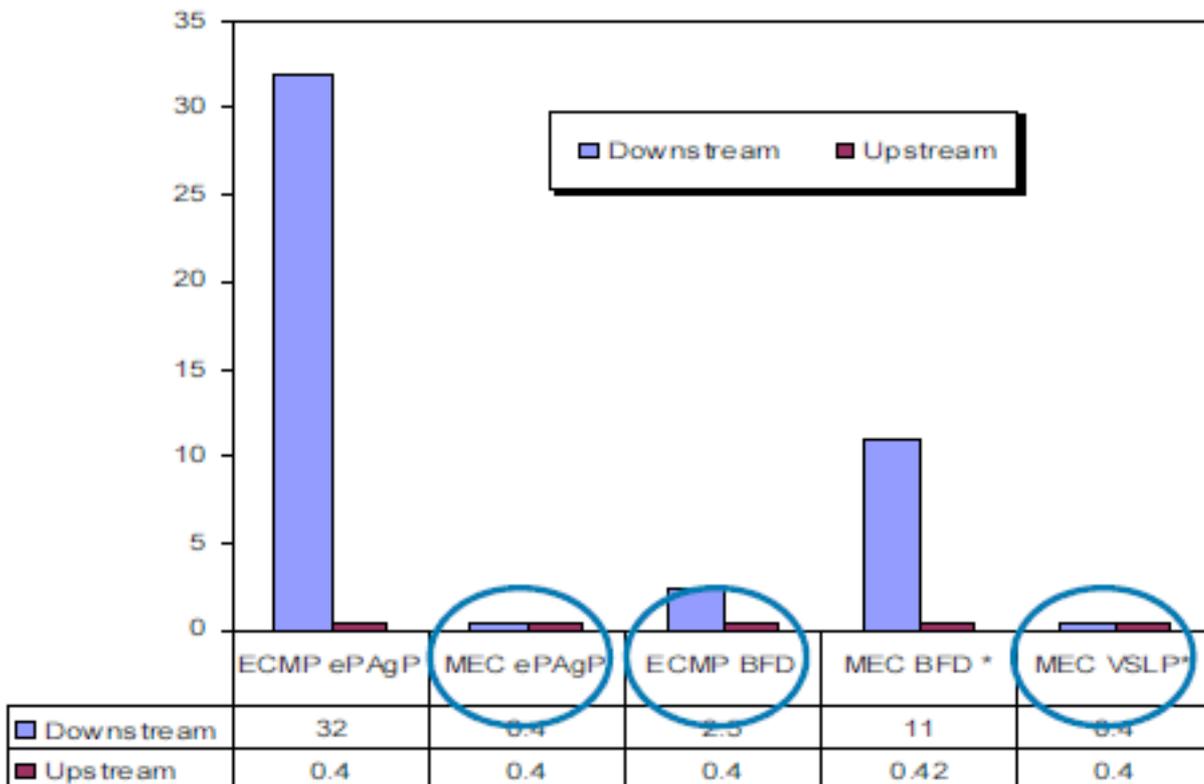
Sie können alle drei Erkennungsmethoden so konfigurieren, dass sie gleichzeitig aktiv sind.

Diese Diagramme enthalten Informationen zur Konvergenz einiger IP-Routing-Protokolle im Hinblick auf die doppelte aktive VSS-Konvergenz.

## EIGRP-Konvergenz mit Standard-Timern



### OSPF-Konvergenz mit Standard-Timern



### Empfehlungen

- Aktivieren Sie mindestens zwei Verbindungen in VSL.
- Verwenden Sie **MEC mit ePAgP** oder **MEC mit VSLP Fast Hello** für schnellere Konvergenz bei VSL-Verbindungsverlusten.
- Aktivieren Sie **ECMP mit IP-BFD**.

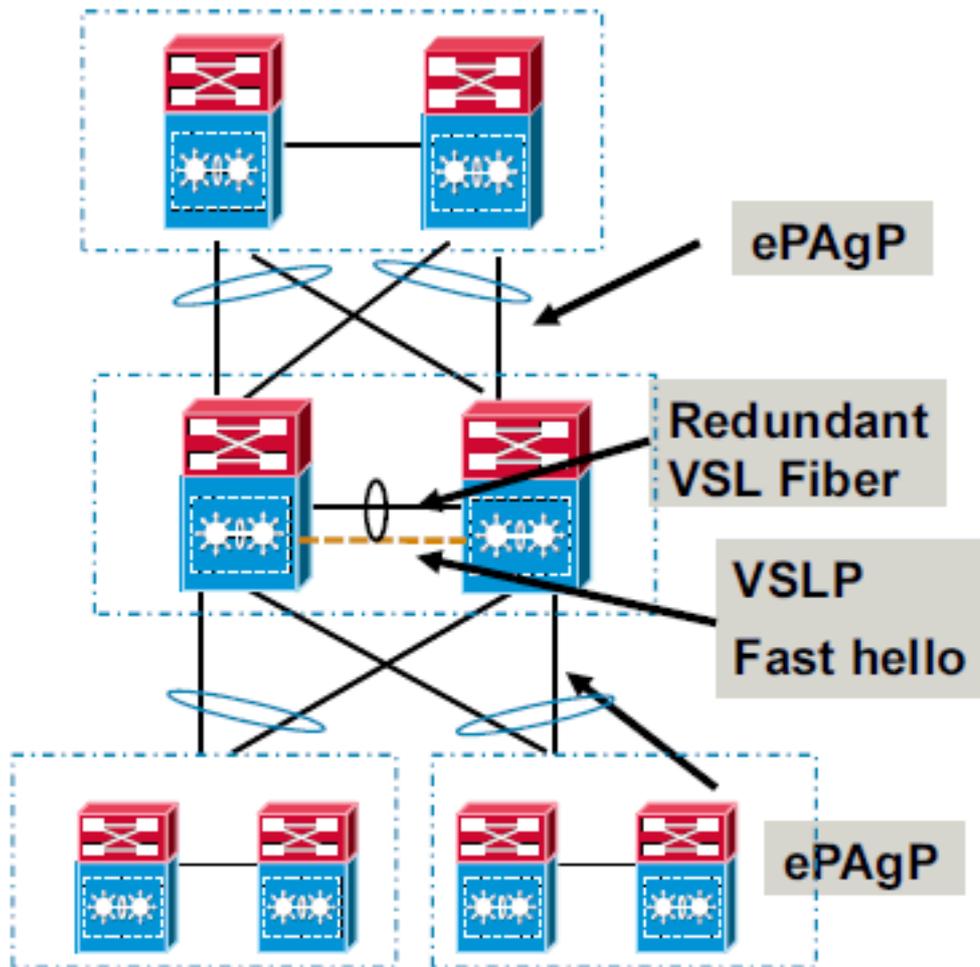
- Aktivieren Sie ePAGP als Core, wenn der Access Layer nicht ePAGP-fähig ist.
- Aktivieren Sie, wenn möglich, sowohl ePAGP als auch Direct Heartbeat-Link-basierte VSLP Fast Hello-Methoden.
- Führen Sie während des VSL-Verlusts und Wiederherstellungsvorgangs keine Konfigurationsänderungen durch. Wenn mindestens eine VSL-Mitgliedsverbindung wiederhergestellt ist und die Konfiguration für das alte ACTIVE-Chassis **unverändert** ist, **startet** die alte ACTIVE **selbst neu**, um im VSS-Hot-Standby-Redundanzstatus zu booten.

```
*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.
```

Wenn die Konfiguration geändert wird, als *verschmutzt* durch den Konfigurationssynchronisierungsprozess markiert, wird der Switch nicht automatisch neu geladen. Nach der Korrektur und Speicherung der Konfiguration muss die alte ACTIVE manuell neu geladen werden. Selbst wenn Sie nur in den Konfigurationsmodus wechseln und den Konfigurationsmodus verlassen, wird die Konfiguration *verschmutzt* und ein manueller Eingriff erzwungen.

```
*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



Weitere Informationen finden Sie unter [Dualaktive Erkennung](#).

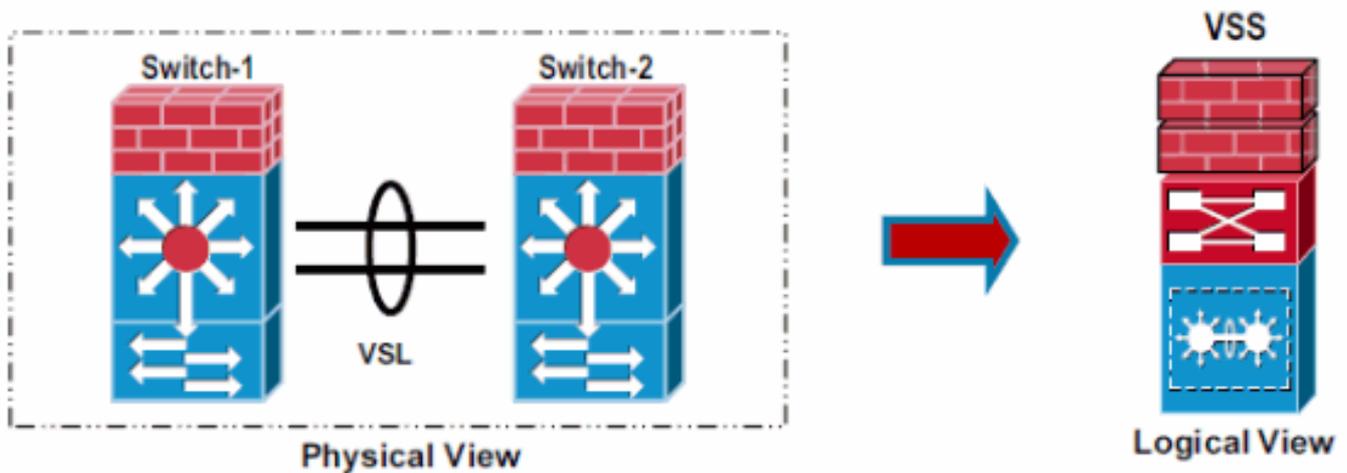
## [Redundanz mit Dienstmodulen](#)

Die Unterstützung von Service-Modulen ist eine der Hauptanforderungen, um das VSS auf dem Markt für Enterprise-Campus und Enterprise-Rechenzentren positionieren zu können. Folgende Dienstmodule werden vom Virtual Switch System unterstützt:

| Servicemodul  | Cisco IOS-Mindestversion | Mindestversion des Moduls |
|---|--------------------------|---------------------------|
| Network Analysis Module (NAM-1 und NAM-2) (WS-SVC-NAM-1 und WS-SVC-NAM-2)     | 12.2(33)SXH 1            | 3,6(1a)                   |
| Application Control Engine (ACE10 und ACE20) (ACE10-6500-K9 und ACE20-MOD-K9) | 12.2(33)SXI              | A2 (1.3)                  |
| Intrusion Detection System Services Module (IDSM-2) (WS-SVC-IDSM2-K9)         | 12.2(33)SXI              | 6,0(2)E1                  |
| Wireless Services Module (WiSM) (WS-SVC-WISM-1-                               | 12.2(33)SXI              | 3.2.171.6                 |

|   |             |       |
|---|-------------|-------|
| K9)   |             |       |
| Firewall Services Module (FWSM) (WS-SVC-FWM-1-K9) | 12.2(33)SXI | 4.0.4 |

Servicemodule können in eines der physischen Chassis eingefügt werden, aus denen ein VSS besteht.



## Empfehlungen

- Für Konfigurationen mit mehr als einem Servicemodul eines bestimmten Typs konfigurieren Sie eines in jedem physischen Switch, um eine optimale Verfügbarkeit zu gewährleisten.
- VSL überträgt den Datenverkehr unter normalen und Failover-Szenarien. Die VSL-Bandbreite muss entsprechend angepasst werden.

Weitere Informationen zur Servicemodul-Integration finden Sie unter [Integrated Cisco Service Modules with Cisco Catalyst 6500 Virtual Switching System 1440](#).

## Multicast

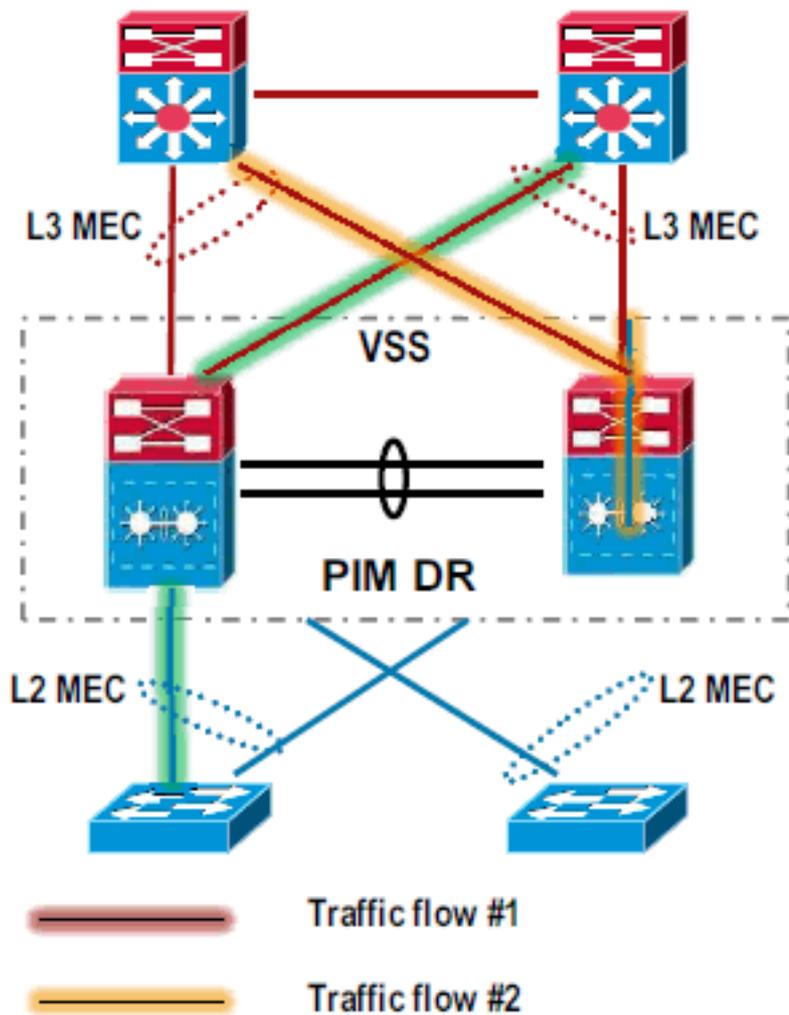
Die IPv4-Multicast-Protokolle werden auf der aktiven Supervisor Engine ausgeführt. Die in der Standby-Supervisor Engine empfangenen Pakete Internet Group Management Protocol (IGMP) und Protocol Independent Multicast (PIM) werden über VSL an das aktive Chassis übertragen. Die aktive Supervisor Engine sendet IGMP- und PIM-Protokollpakete an die Standby-Supervisor Engine, um die Layer-2-Informationen für Stateful Switchover (SSO) aufrechtzuerhalten.

Weitere Informationen finden Sie unter [IPv4-Multicast](#).

## Empfehlungen

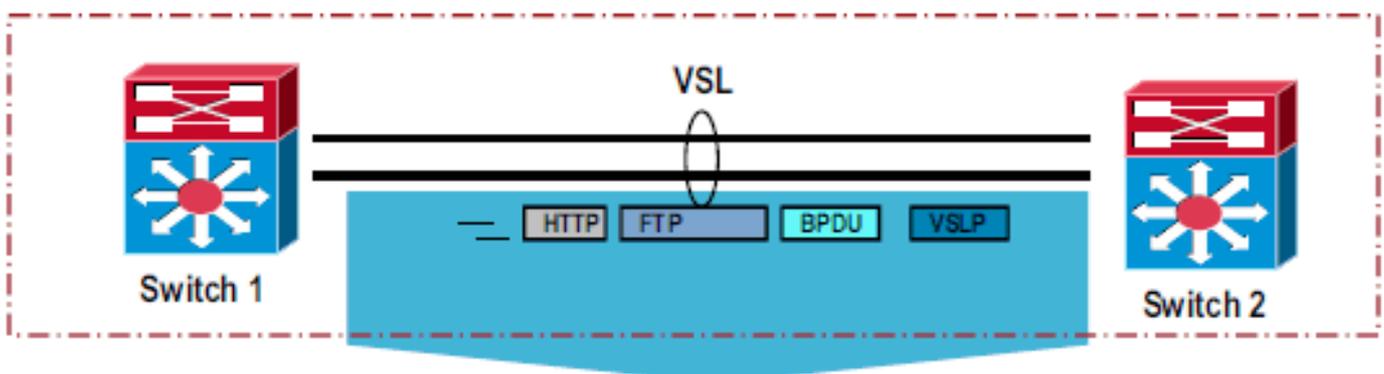
- Verbundene Geräte müssen immer **Dual-Homed** sein, um eine optimale Replikationsleistung zu gewährleisten.
- **MEC wird** in L3- und L2-Umgebungen **empfohlen**, um deterministische Konvergenz bereitzustellen.
- MEC eliminiert Reverse Path Forwarding (RPF)-Neuberechnung während eines MEC-Verbindungsausfalls.
- **Ausgangsreplikation** mit lokaler Erweiterung für einen höheren Multicast-Replikationsdurchsatz.

- Für die Ausgangsreplikation sind DFCs für eine optimierte Replikationsleistung erforderlich.
- Größe des VSL entsprechend der Datenverkehrsanforderungen



## Quality of Service

### VSL-QoS-Einstellungen



- VSL ist ein wichtiger interner Kontroll- und Datenübertragungspfad, und daher sind QoS-Einstellungen vorkonfiguriert, und Konfigurationsänderungen sind nicht zulässig.
- VSL wird immer als **Trust CoS** konfiguriert, und die Eingangswarteschlange ist aktiviert.
- Derzeit werden nur CoS-basierte Vertrauens- und Warteschlangenverwaltung unterstützt. Service-Richtlinien werden von VSL nicht unterstützt.
- QoS-Richtlinien müssen an der Eingabeschnittstelle der Datenflüsse angewendet werden.

- Die Prioritätswarteschlange ist standardmäßig aktiviert. Der VSS-Kontrollverkehr und die BPDUs erhalten auf der VSL-Verbindung eine hohe Priorität.

## Empfehlungen

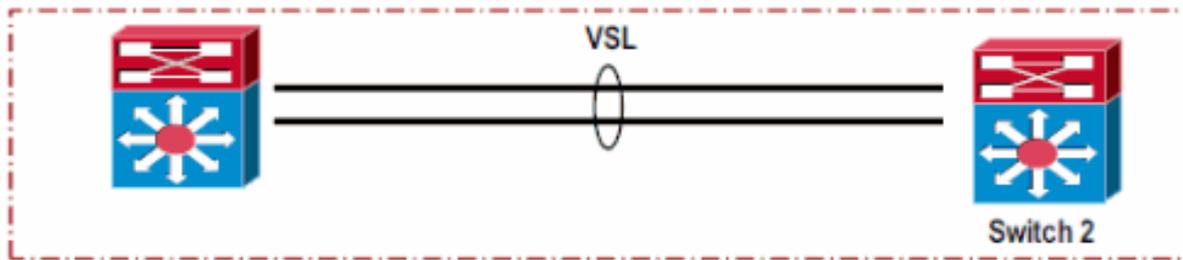
Der einzige Unterschied zwischen den VSL-fähigen Hardware-Optionen ist die Warteschlangenkonfiguration. Da die aktuelle Version der Software keine Änderungen an den Standard-Warteschlangeneinstellungen zulässt, bietet jede Kombination von VSL-fähigen Ports dieselben QoS-Ergebnisse.

| Hardware                                      | Warteschlangenmodus | Trust-Modus | Übertragungswarteschlange                                    | Empfangswarteschlange |
|---|---------------------|-------------|--|-----------------------|
| VSL auf Uplinks<br>"nur Nicht-10G (Standard)" | CoS                 | CoS         | 1p3q4t (DWRR/SRR)  | 8q4t                  |
| VSL nur für Uplinks<br>"10G"                  | CoS                 | CoS         | 1p7q4t (DWRR/SRR)  | 2q4t                  |
| Uplinks und Line Cards mit VSL                | CoS                 | CoS         | 1p3q4t [nicht-10G] (DWRR/SRR)<br>1p7q4t [nur 10G] (DWRR/SRR) | 2q4t                  |
| VSL auf Line Cards                            | CoS                 | CoS         | 1p7q4t (DWRR/SRR)  | 8q4t                  |

Weitere Informationen finden Sie unter [Konfigurieren der VSL-QoS](#).

## SPAN

In einer Virtual Switch-Domäne ist die Anzahl der SPAN-Sitzungen durch die Möglichkeiten des aktiven Virtual Switch Supervisor beschränkt.



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

Virtual Switch System unterstützt diese SPAN-Funktionen pro Virtual Switch Domain.

| Attribut                       | Wert |
|--------------------------------|------|
| Tx SPAN-Sitzungen              | 14   |
| Rx/Beide SPAN-Sitzungen        | 2    |
| Gesamtanzahl an SPAN-Sitzungen | 16   |

## Empfehlungen

- Wenn VSL als lokale SPAN-Quelle konfiguriert ist, müssen sich die SPAN-Zielports im selben Chassis wie die VSL-Schnittstellen befinden.
- VSL kann nicht als SPAN-Ziel konfiguriert werden.
- VSL kann nicht als Quelle für RSPAN, ERSPAN oder nur für Tx-lokale SPAN konfiguriert werden.
- Der VSL-Header wird vom SPAN-Zielport entfernt, bevor das Paket gesendet wird, und kann daher nicht in den Sniffer-Traces erfasst werden.
- Wenn sich Quelle und Ziel beide im selben Chassis (aktiv oder Standby) befinden, fließt der SPAN-Datenverkehr nicht über die VSL-Verbindung. Um Datenverkehr von beiden Chassis zu erfassen, gibt es zwei Optionen, die den SPAN-Datenverkehr im VSL vermeiden: Für jede Quellschnittstelle in einem Chassis muss sich die Zielschnittstelle im gleichen Chassis befinden. Beispielsweise hat PO20 Gi1/1/1 und Gi2/1/1: Sie benötigen ein Ziel für jedes Chassis.

```

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
  
```

Dies bedeutet jedoch, dass Sie beide lokalen SPAN-Sitzungen verwenden. Daher können Sie keine andere lokale SPAN-Sitzung verwenden. Sie können die Zielschnittstelle für SPAN als MEC (empfohlen) verwenden. Beim Zielport kann es sich um einen MEC handeln.

## Verschiedenes

### Empfehlungen

- Verwenden Sie mindestens einen Supervisor-Uplink für VSL, um die VSL-Aktivierung zu beschleunigen.

- Konfigurieren Sie den [virtuellen Befehl für den Akzeptierungsmodus](#) nach der VSS-Konvertierung. Ohne diesen Befehl ist die Konvertierung nicht abgeschlossen.
- Speichern Sie die Sicherung der Konfigurationsdatei auf der aktiven als auch der Hot-Standby-Bootdiskette: Dies ist bei Szenarien für den Ersatz von Supervisoren sehr hilfreich.
- Verwenden Sie **eine eindeutige VSS-Domänen-ID** im selben Netzwerk. Eine doppelte VSS-Domänen-ID kann zu Inkonsistenzen im EtherChannel führen. Im folgenden Beispiel wird die VSS-Domänen-ID geändert. Verwenden Sie den Befehl [virtual domain domain-id](#), um die **Änderung der Domänen-ID zu initiieren**.

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

**Hinweis:** Die Konfiguration der Domänen-ID 50 wird erst wirksam, nachdem der Befehl **virtual exec** für den **Switch-Konvertierungsmodus** ausgegeben wurde. Verwenden Sie den Befehl [Virtueller Switch-Konvertierungsmodus](#), um die Aufgabe abzuschließen.

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

**Hinweis:** Die virtuelle Domänen-ID ändert sich erst, nachdem Sie die Konfiguration gespeichert und den Switch neu geladen haben.

- Verwenden Sie den Befehl **erase nvram** anstelle des Befehls **write erase**, um die VSS-Konfiguration zurückzusetzen. Mit dem Befehl **write erase** werden die Variablen startup-config und ROMMon gelöscht. VSS benötigt eine *Switch-ID-ROMMon-Variable*, um im VSS-Modus zu starten.
- Verwenden Sie keine Freischaltung. Weitere Informationen [finden Sie](#) unter [Cisco Empfehlung, die Switch-Freischaltung nicht zu konfigurieren](#).
- Verwenden Sie den Befehl **shutdown** nicht für die Simulation von VSL-Ausfällen, da dies zu einer Konfigurationsungleichheit führt. Wenn Sie ein Kabel trennen, wird ein realistischeres Fehlerszenario angezeigt.
- Ändern Sie den VSL-Hashing-Algorithmus nicht, während das System in Produktion ist. Bei einer Änderung des Algorithmus muss der Port-Channel deaktiviert und erneut aktiviert werden. Dazu müssen die Befehle **herunterfahren** und **kein Herunterfahren** verwendet werden. Wenn Sie eine VSL herunterfahren, führt dies zu einer Unterbrechung des Datenverkehrs und kann in einem Szenario mit zwei aktiven Verbindungen enden.
- Konfigurieren Sie den MAC-Alterungs-Timer auf das Dreifache des Timer-Werts für die MAC-Synchronisierung. Die Standard-MAC-Synchronisierung und die MAC-Alterungs-Timer können unbekannte Unicast-Flooding verursachen. VSS kann dazu führen, dass der Datenverkehr asymmetrisch fließt, sodass die Quell-MAC-Adresse nur auf einem Chassis erfasst wird. Der MAC-Alterungs-Timer von 300 Sekunden und der MAC-Synchronisierungs-Timer von 160 Sekunden ermöglichen in einem Intervall von 320 Sekunden bis zu 20 Sekunden unbekannte Unicast-Flooding für eine beliebige MAC-Adresse. Um dies zu beheben, ändern Sie die Timer so, dass der Alterungs-Timer dreimal so lang ist wie der Synchronisierungs-Timer, z. B. **MAC-Adresstabelle, Alterungszeit 480**. Die Beispielausgabe der [show mac-address-table aging-time](#) wird hier angezeigt:

```
switch#sh mac-address-table aging-time
Vlan Aging Time
----
Global 480
no vlan age other than global age configured
```

- Damit VSS mit Stateful Switchover (SSO) betrieben werden kann, müssen beide Supervisor Engines dieselbe Softwareversion ausführen.
- Wenn Sie vom VSS-Modus zurück zu einem Standalone-Switch über den [Standalone-Befehl](#)

[konvertieren im Konvertierungsmodus](#) migrieren, werden folgende Aufgaben ausgeführt: Konvertiert den Schnittstellennamen mit dem **Switch-/Steckplatz-/Port**-Namen in **Steckplatz/Port**. Entfernt nicht lokale Schnittstellen aus der running-config-Konfiguration. Entfernt die Konfiguration von VSL-Port-Channels und -Ports. Speichert Running-config in Startup-config. Setzt die SP-ROM-Variable SWITCH\_NUMBER auf 0. Lädt den Switch neu.

- Der Switch muss neu gestartet werden, wenn dies unbedingt erforderlich ist. z. B. ein IOS-Upgrade oder als Fehlerbehebungsschritt. Ein Switch, der mehr als zwei Jahre aktiv ist, ist ein stabiler Switch und die Konfiguration ist ebenfalls stabil.

## Häufig gestellte Fragen

### Können in jedem Chassis mit VSS zwei Supervisoren verwendet werden?

Ja. Zwei Supervisoren werden in jedem für den VSS-Modus konfigurierten VSS-Chassis unterstützt, beginnend mit SXI4 und höher.

### Werden die Switches beim Entfernen der Freischaltbefehle in Catalyst Switches der Serie 6500 im VSS-Modus neu geladen?

Die Switch-Freischaltung wird nicht empfohlen. Aus diesem Grund ist das Entfernen der Befehle eine bewährte Vorgehensweise und führt nicht zum erneuten Laden. Weitere Informationen zur Freischaltungsfunktion von VSS finden Sie unter [Switch-Freischaltung](#).

## Zugehörige Informationen

- [Best Practices für Catalyst Switches der Serien 6500/6000 und 4500/4000 mit Cisco IOS Software](#)
- [Konfigurieren von Virtual Switching-Systemen](#)
- [Cisco IOS Virtual Switch Befehlsreferenz](#)
- [Produktsupport für das Cisco Catalyst 6500 Virtual Switching System 1440](#)
- [Produkt-Support für LAN-Switches](#)
- [Support für LAN-Switching-Technologie](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)