

# Procedure ottimali per l'installazione di Catalyst 6500 VSS

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Procedure ottimali per l'installazione di VSS](#)

[VSS alta disponibilità](#)

[Ripristino dei collegamenti upstream](#)

[Perdita di collegamenti e ripristino VSL](#)

[Ridondanza con moduli di servizio](#)

[Multicast](#)

[Qualità del servizio](#)

[SPAN](#)

[Varie](#)

[Domande frequenti](#)

[È possibile utilizzare due supervisor in ogni chassis con VSS?](#)

[Quando si rimuovono i comandi di interruzione per diritti di priorità sugli switch Catalyst serie 6500 in modalità VSS, gli switch vengono ricaricati?](#)

[Informazioni correlate](#)

## [Introduzione](#)

Questo documento fornisce le best practice per gli scenari di implementazione di Cisco Catalyst 6500 Virtual Switching System (VSS) 1440.

Questo documento offre linee guida per la configurazione modulare. Pertanto, potete leggere ogni sezione in modo indipendente e apportare modifiche in un approccio a fasi. Per questo documento si presume che l'interfaccia utente del software Cisco IOS® abbia una comprensione e una familiarità di base. Il documento non tratta la progettazione generale della rete.

## [Prerequisiti](#)

### [Requisiti](#)

Nessun requisito specifico previsto per questo documento.

## Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

## Procedure ottimali per l'installazione di VSS

Le soluzioni presentate in questo documento rappresentano anni di esperienza sul campo da parte di tecnici Cisco che lavorano con reti complesse e molti dei più grandi clienti. Di conseguenza, in questo documento vengono enfatizzate le configurazioni che contribuiscono al successo delle reti. Questo documento offre le seguenti soluzioni:

- Soluzioni facili da gestire e configurate dai team operativi di rete
- Soluzioni che promuovono alta disponibilità e alta stabilità

### VSS alta disponibilità

- [Inoltro senza interruzione](#)
- [Sincronizzazione MAC fuori banda](#)

#### Inoltro senza interruzione

Gli switch Catalyst serie 6500 supportano la resistenza agli errori perché consentono a un supervisor engine ridondante di assumere il controllo in caso di guasto del supervisor engine principale. La funzione NSF (Non Stop Forwarding) di Cisco funziona con lo switch SSO (Stateful SwitchOver) per ridurre al minimo il tempo di indisponibilità della rete per gli utenti dopo il passaggio, durante il quale i pacchetti IP continuano a essere inoltrati.

#### **Raccomandazioni**

- L'inoltro senza interruzione è richiesto per la convergenza di switchover del supervisore al secondo.
- Utilizzare i timer Hello e Dead predefiniti per i protocolli EIGRP / OSPF quando si esegue in un ambiente VSS.
- Se si esegue il sistema con il software modulare Cisco IOS, si consiglia di utilizzare un timer OSPF Dead di valore maggiore.

#### **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
```

Per ulteriori informazioni su NSF, fare riferimento a [Configurazione di NSF con la ridondanza del Supervisor Engine](#) SSO.

## Sincronizzazione MAC fuori banda

Nella commutazione distribuita, ogni DFC (Distributed Feature Card) mantiene la propria tabella CAM. Ciò significa che ogni DFC apprende l'indirizzo MAC e lo fa invecchiare, il che dipende dall'invecchiamento della CAM e dalla corrispondenza del traffico di quella particolare voce. Con lo switching distribuito, è normale che il supervisor engine non visualizzi il traffico per un particolare indirizzo MAC per un determinato periodo di tempo, quindi la voce può scadere. Attualmente sono disponibili due meccanismi per mantenere le tabelle CAM coerenti tra i diversi motori, ad esempio DFC, presente nei moduli di linea, e Policy Feature Card (PFC), presente nei moduli supervisor:

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

Quando una voce di indirizzo MAC è obsoleta sul PFC, il comando **show mac-address address <MAC\_Address> all** visualizza il DFC o il PFC che contiene questo indirizzo MAC. Per evitare che una voce di una DFC o di una PFC venga cancellata, anche se non c'è traffico per l'indirizzo MAC, abilitare la sincronizzazione degli indirizzi MAC. Per abilitare la sincronizzazione, usare il comando di configurazione globale **mac-address-table synchronize** e il comando di esecuzione privilegiata **dinamica mac-address-table**. Questo comando **mac-address-table synchronize** è disponibile nel software Cisco IOS versione 12.2(18)SXE4 e successive. Dopo averla attivata, è possibile continuare a visualizzare le voci non presenti in PFC o DFC. Tuttavia, il modulo può essere utilizzato anche da altri utenti che utilizzano EOBC (Ethernet Out of Band Channel).

## Raccomandazioni

Abilita sincronizzazione MAC fuori banda. Viene usato per sincronizzare le tabelle degli indirizzi MAC tra i motori di inoltro. Se nel sistema VSS è presente WS-6708-10G, la sincronizzazione MAC viene attivata automaticamente. In caso contrario, deve essere attivata manualmente.

```
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
```

## [Terminologia VSS](#)

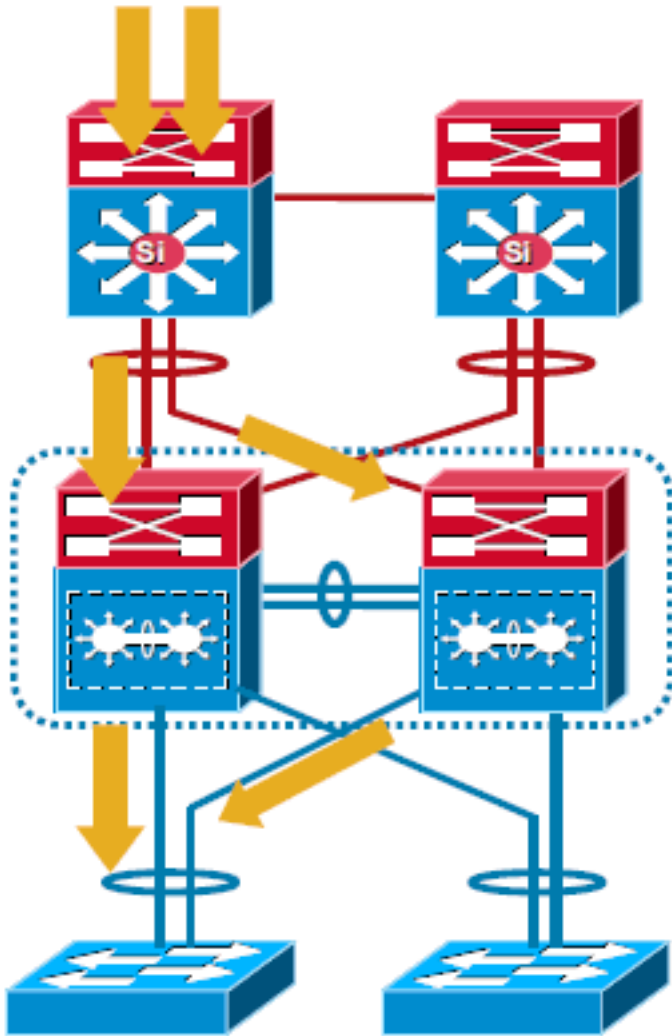
- **Virtual Switch Link (VSL)**: canale di porta speciale richiesto per raggruppare due switch fisici in un unico switch virtuale.
- **VSL Protocol (VSLP)**: viene eseguito tra lo switch attivo e quello in standby sulla VSL e contiene due componenti: **LMP** e **RRPLink Management Protocol (LMP)**: viene eseguito su ogni singolo collegamento in **VSLRRP (Role Resolution Protocol)**: viene eseguito su ciascun lato (ciascun peer) del canale della porta VSL

## [Pianificazione della capacità per VSL](#)

Nella configurazione VSS dual-homed, non è possibile inviare traffico di dati sul collegamento VSL. Ciascuno switch è programmato in modo da scegliere le proprie interfacce locali per l'inoltro del traffico.

È necessaria una pianificazione aggiuntiva della capacità del collegamento VSL per il traffico trasportato da:

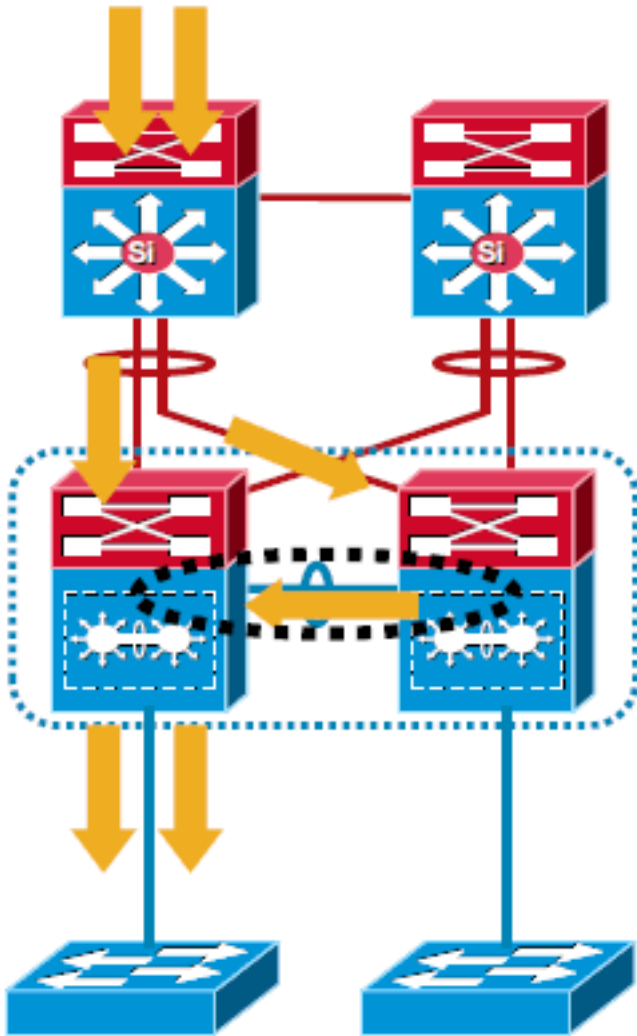
- Singoli dispositivi collegati a casa
- SPAN remoto da uno switch all'altro
- Traffico del modulo di servizio -€" FWSM, ACE, ecc.



Per ulteriori informazioni, fare riferimento al [traffico sul VSL](#).

### Raccomandazioni

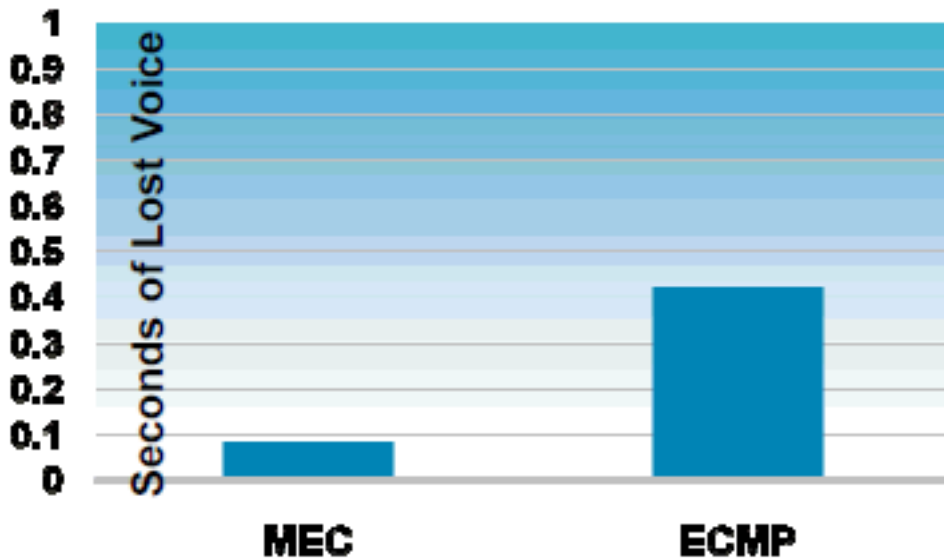
- Sempre dispositivi **dual-home** collegati a VSS.
- Includere sempre **VSL EtherChannel nella potenza di 2**, perché offre risultati hash migliori per la condivisione ottimizzata del carico del traffico.
- La ridondanza della VSL è ancora critica insieme alla resilienza dei collegamenti VSL.
- Si consiglia di avere almeno una larghezza di banda VSL uguale agli uplink connessi a un singolo switch fisico.



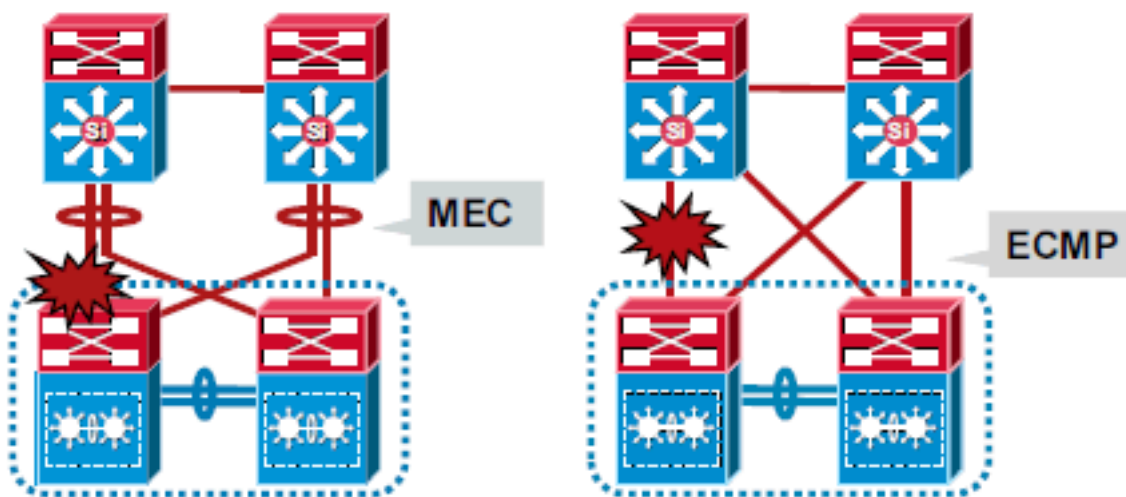
### Ripristino dei collegamenti upstream

Il ripristino dei collegamenti upstream (collegamenti al core) può essere ottenuto tramite la funzionalità MultiChassis EtherChannel (MEC) o la funzionalità Equal Cost MultiPath (ECMP).

La convergenza CEM è **coerente e indipendente** dal numero di percorsi. Mentre, la convergenza ECMP **dipende** dal numero di percorsi. Questo grafico indica l'entità della perdita in una sessione vocale.



Le immagini seguenti mostrano gli scenari di errore dei collegamenti con MEC ed ECMP:



## MultiChassis EtherChannel

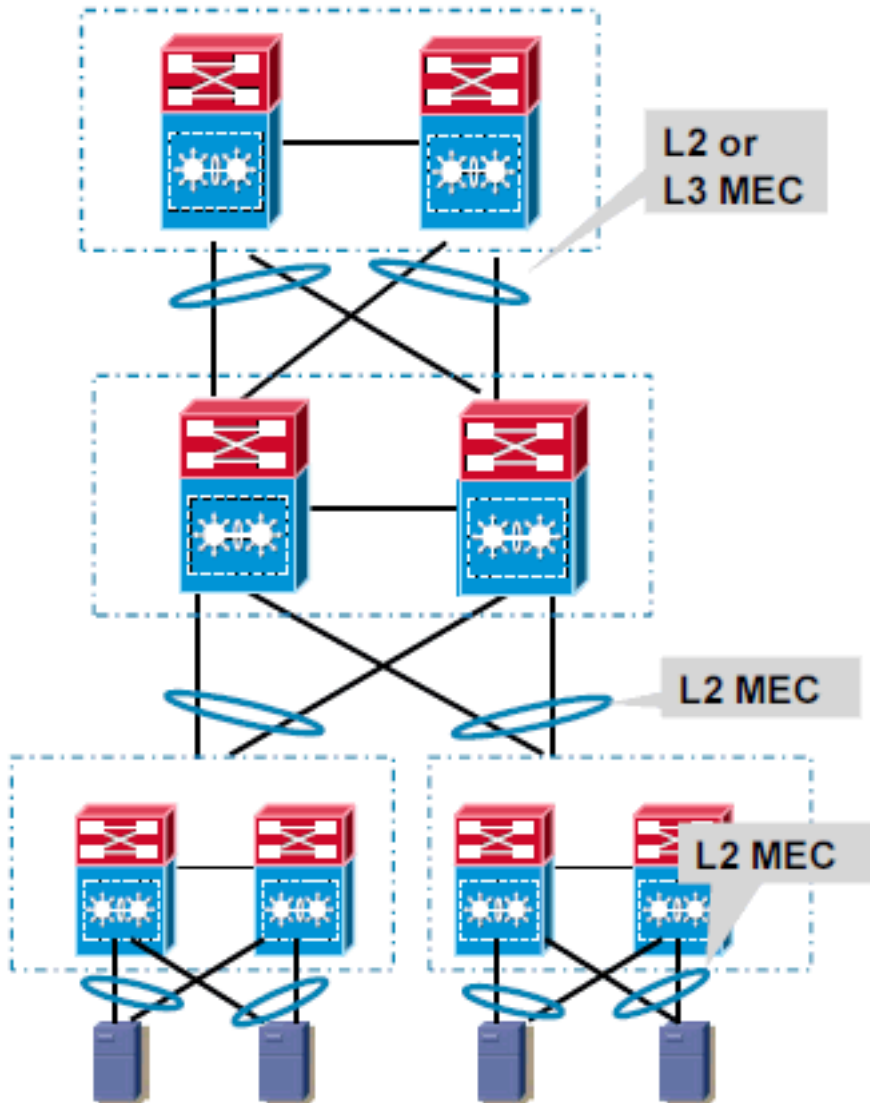
Un MultiChassis EtherChannel è un EtherChannel con porte che terminano su entrambi gli chassis del VSS. Un servizio VSS MEC può connettersi a qualsiasi elemento di rete che supporti EtherChannel, ad esempio un host, un server, un router o uno switch. Nel VSS, un MEC è un EtherChannel con funzionalità aggiuntive. Il servizio VSS bilancia il carico tra le porte di ogni chassis in modo indipendente. Ad esempio, se il traffico entra nello chassis attivo, il servizio VSS seleziona un collegamento MEC dallo chassis attivo. Questa funzionalità MEC assicura che il traffico di dati non attraversi inutilmente la VSL.

- L2 MEC consente una topologia senza loop, raddoppia la larghezza di banda di uplink in quanto nessun collegamento viene bloccato e fornisce una convergenza più rapida rispetto a STP.
- L3 MEC consente di ridurre il numero di router adiacenti, di migliorare la condivisione del carico (L2 e L3 per unicast e multicast), di ridurre l'utilizzo dei collegamenti VSL per i flussi multicast e di velocizzare la convergenza rispetto a ECMP.

Per ulteriori informazioni su MEC, fare riferimento a [MultiChassis EtherChannel](#).

## Raccomandazioni

- Eseguire sempre **MEC L2 o L3**.
- Non utilizzare opzioni di **attivazione e disattivazione** con la negoziazione del protocollo PAgP, LACP o Trunk.PAgP â€" Esegui **desiderabile** con collegamenti MEC.LACP â€" Esegui **Active-Active** con collegamenti MEC.Trunk â€" Esegui **Desirable-Desirable** con collegamenti MEC.



## Perdita di collegamenti e ripristino VSL

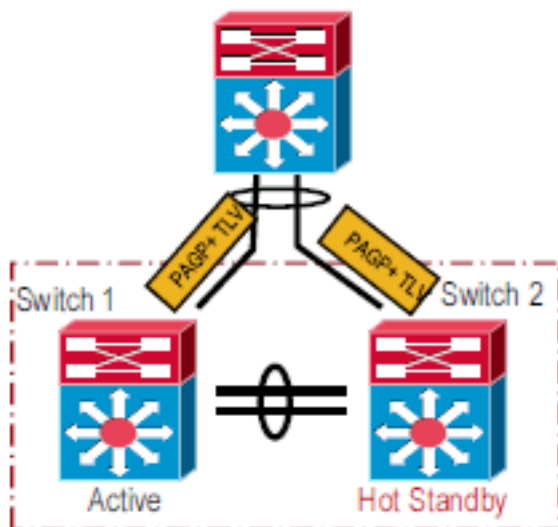
Se la VSL non funziona, lo chassis in standby non è in grado di determinare lo stato dello chassis attivo. Per assicurare che il passaggio avvenga senza indugio, lo chassis in standby presume che lo chassis attivo sia guasto e avvia il passaggio per assumere il ruolo attivo.

Se lo chassis attivo originale è ancora operativo, entrambi gli chassis sono ora attivi. Questa situazione viene definita scenario **dual-active**. Uno scenario a doppia attività può avere effetti negativi sulla stabilità della rete, in quanto entrambi gli chassis utilizzano gli stessi indirizzi IP, chiavi SSH e ID bridge STP. Il sistema di commutazione virtuale (VSS) deve rilevare uno scenario a doppia attività ed eseguire un'azione di ripristino.

Il sistema di commutazione virtuale supporta questi tre metodi per rilevare uno scenario a doppia attività:



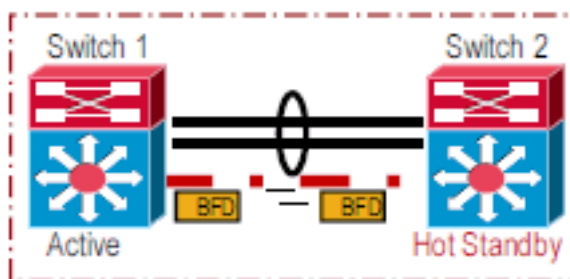
- Enhanced PAgP  $\hat{=}$  utilizza la messaggistica PAgP sui collegamenti MEC per comunicare tra i due chassis tramite uno switch adiacente. Il protocollo PAgP avanzato è piú veloce del protocollo IP BFD, ma richiede uno switch adiacente che supporti i miglioramenti del



protocollo PAgP.

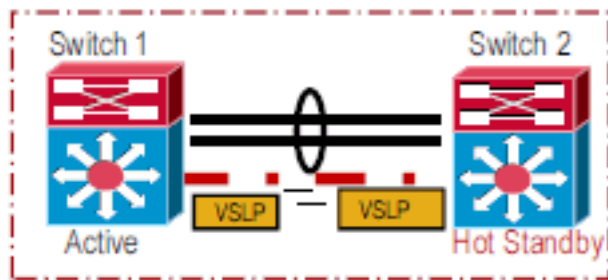
Tabella di supporto ePAgP:

- IP Bidirectional Forwarding Detection (BFD)  $\hat{=}$  Utilizza la messaggistica BFD su una connessione Ethernet di backup. Il protocollo IP BFD utilizza una connessione diretta tra i due chassis e non richiede il supporto di uno switch adiacente. Questo metodo è disponibile a



partire da Cisco IOS versione 12.2(33)SXH1.

- VSLP dual-active fast-hello  $\hat{=}$  Utilizza speciali messaggi di benvenuto su una connessione Ethernet di backup. La funzionalità Dual-Active Fast-Hello è piú veloce dell'IP BFD e non richiede il supporto di uno switch adiacente. Questo metodo è disponibile solo nel software

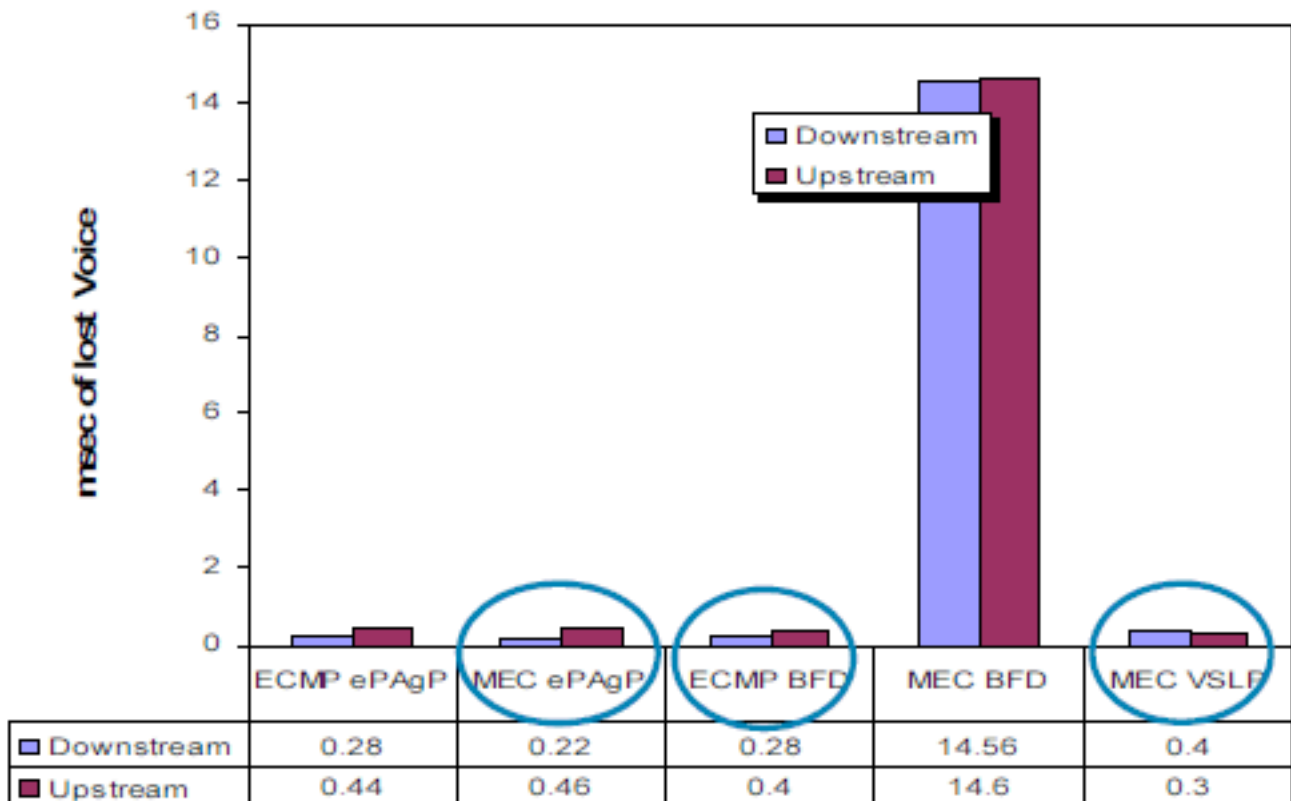


Cisco IOS versione 12.2(33)SXI e successive.

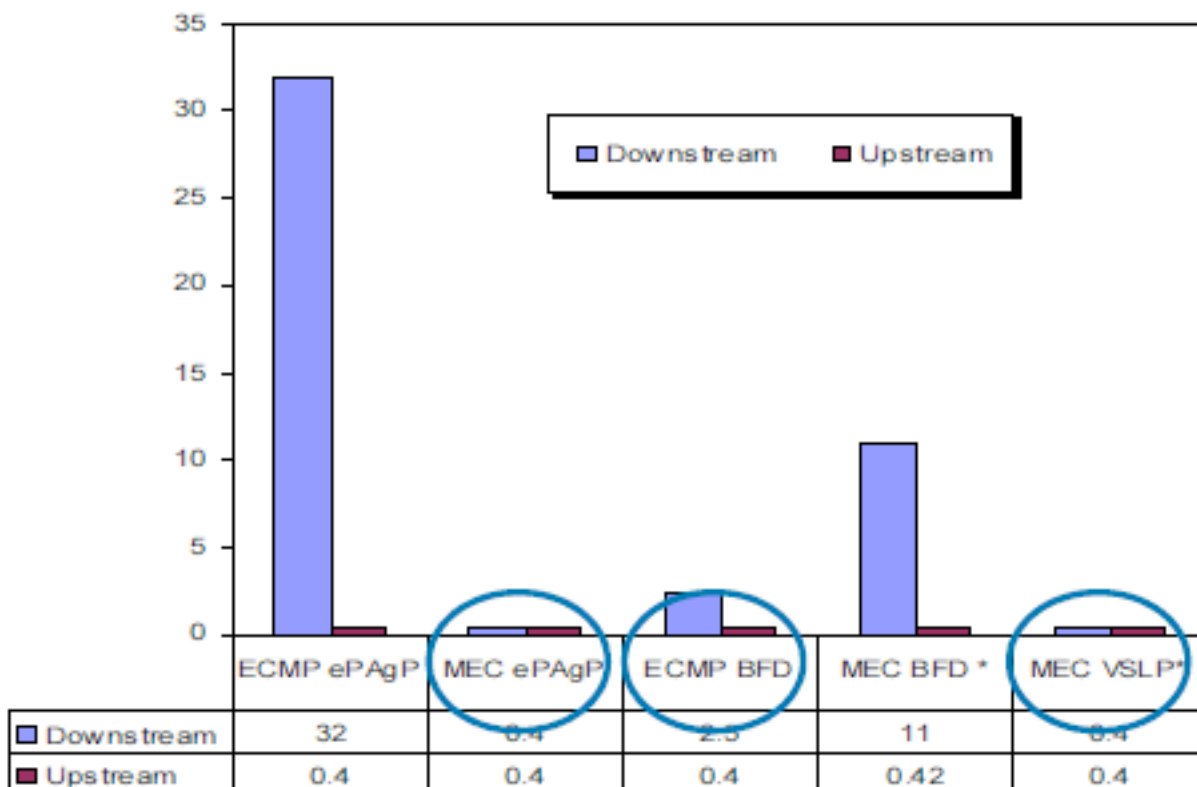
È possibile configurare tutti e tre i metodi di rilevamento in modo che siano attivi contemporaneamente.

Questi grafici forniscono informazioni sulla convergenza di alcuni protocolli di routing IP rispetto alla convergenza attiva doppia VSS.

### Convergenza EIGRP con timer predefiniti



### Convergenza OSPF con timer predefiniti



### Raccomandazioni

- Abilitare almeno due collegamenti in VSL.
- Utilizzare **MEC con ePAgP** o **MEC con VSLP Fast Hello** per risultati più veloci di convergenza della perdita dei collegamenti VSL.
- Abilitare **ECMP con IP-BFD**.

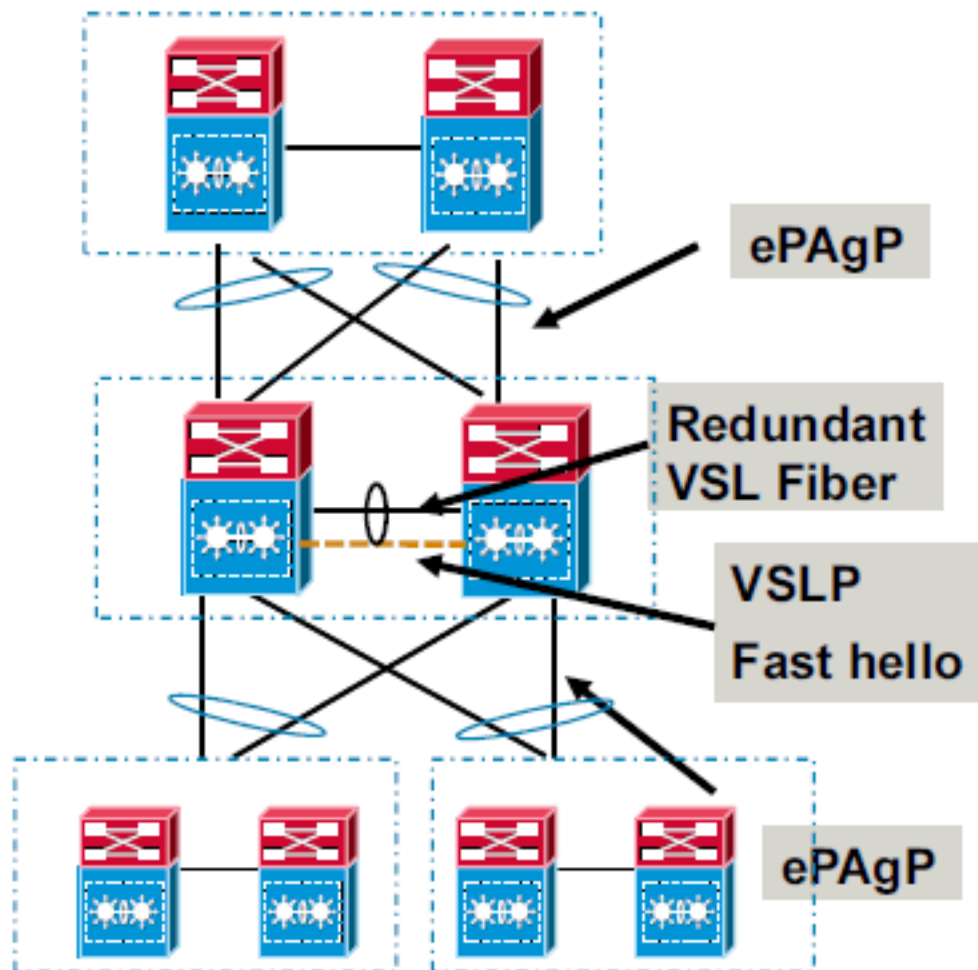
- Abilitare ePAGP per il core, se il livello di accesso non supporta ePAGP.
- Se possibile, abilitare entrambi i metodi VSLP Fast Hello basati su collegamento cardiaco diretto e ePAGP.
- Durante la perdita di VSL e il processo di ripristino non eseguire modifiche alla configurazione. Dopo il ripristino di almeno un collegamento membro VSL, se la configurazione sul vecchio chassis ACTIVE **rimane invariata**, il vecchio **switch ACTIVE si riavvia** per l'avvio in stato di ridondanza VSS hot-standby.

```
*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.
```

Se la configurazione viene modificata, contrassegnata come *dirty* dal processo di sincronizzazione della configurazione, lo switch non si ricarica automaticamente. Il ricaricamento manuale deve essere eseguito sul vecchio ACTIVE dopo la correzione e il salvataggio della configurazione. Anche se si accede semplicemente alla modalità di configurazione e si esce, la configurazione viene *modificata* e viene forzato un intervento manuale.

```
*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



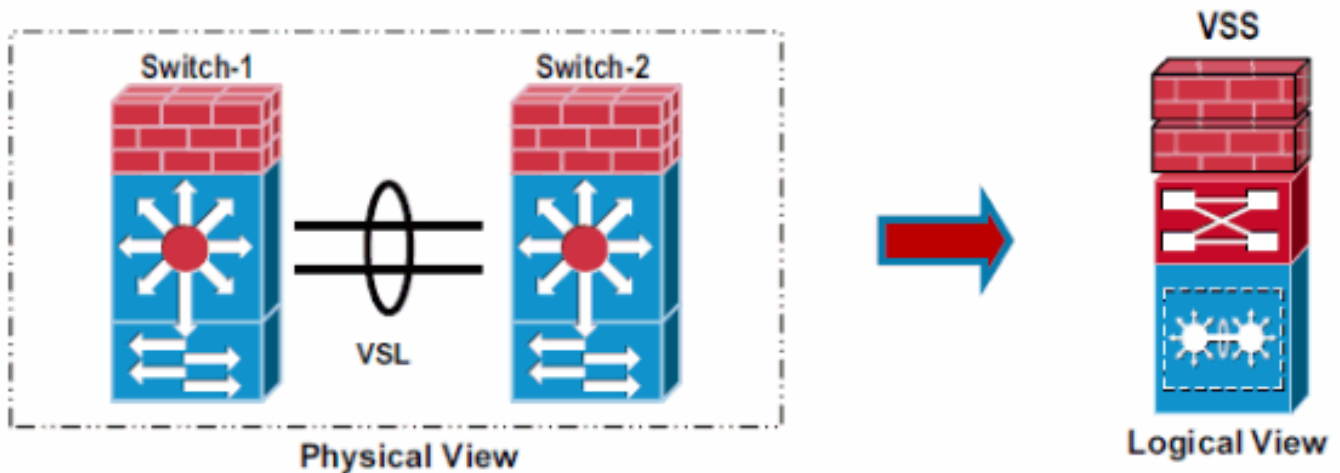
per ulteriori informazioni, fare riferimento a [Rilevamento di attività doppie](#).

### [Ridondanza con moduli di servizio](#)

Il supporto dei moduli di assistenza è un requisito chiave per posizionare il VSS nel mercato dei centri dati aziendali e delle infrastrutture aziendali. Di seguito sono elencati i moduli del servizio supportati nel sistema di commutazione virtuale:

Modulo di servizio	Versione minima di Cisco IOS	Release minima del modulo
Network Analysis Module (NAM-1 e NAM-2) (WS-SVC-NAM-1 e WS-SVC-NAM-2)	12.2(33)S XH1	3.6, paragrafo 1 bis
Application Control Engine (ACE10 e ACE20) (ACE10-6500-K9 e ACE20-MOD-K9)	12.2(33)S XI	A2(1,3)
Modulo dei servizi del sistema di rilevamento intrusioni (IDSM-2) (WS-SVC-IDSM2-K9)	12.2(33)S XI	6.0(2)E1
Wireless Services Module (WiSM) (WS-SVC-WISM-1-K9)	12.2(33)S XI	3.2.171.6
Modulo servizi firewall (FWSM)	12.2(33)S	4.0.4

I moduli di assistenza possono essere collocati in uno dei due chassis fisici che comprendono un VSS.



### Raccomandazioni

- Per la configurazione con più di un modulo di servizio di un determinato tipo, configurarne uno in ciascuno switch fisico per ottenere la massima disponibilità.
- VSL gestisce il traffico in scenari normali e di failover; la larghezza di banda VSL deve essere sintonizzata di conseguenza.

Per ulteriori informazioni sull'integrazione dei moduli di servizio, fare riferimento a [Integrazione dei Cisco Service Module con Cisco Catalyst 6500 Virtual Switching System 1440](#).

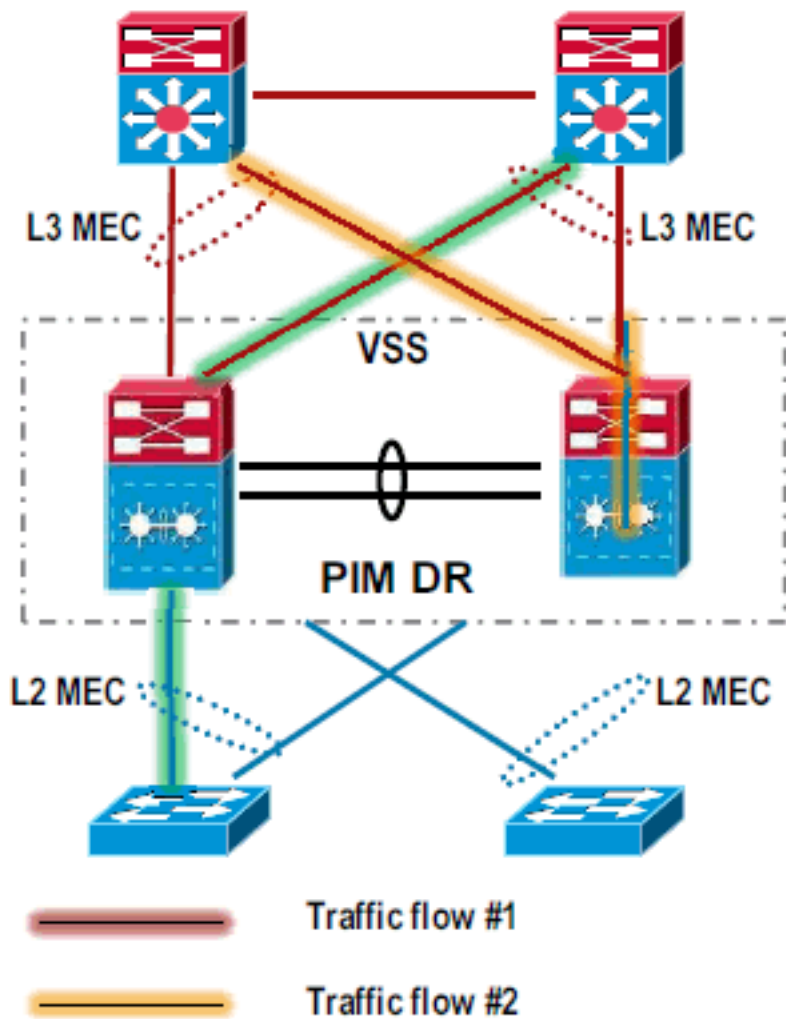
### Multicast

I protocolli multicast IPv4 vengono eseguiti sul supervisor engine attivo. I pacchetti IGMP (Internet Group Management Protocol) e PIM (Protocol Independent Multicast) ricevuti sul supervisor engine di standby vengono trasmessi tramite VSL allo chassis attivo. Il supervisor engine attivo invia i pacchetti dei protocolli IGMP e PIM al supervisor engine di standby per conservare le informazioni di layer 2 per il passaggio con stato (SSO).

Per ulteriori informazioni, fare riferimento a [Multicast IPv4](#).

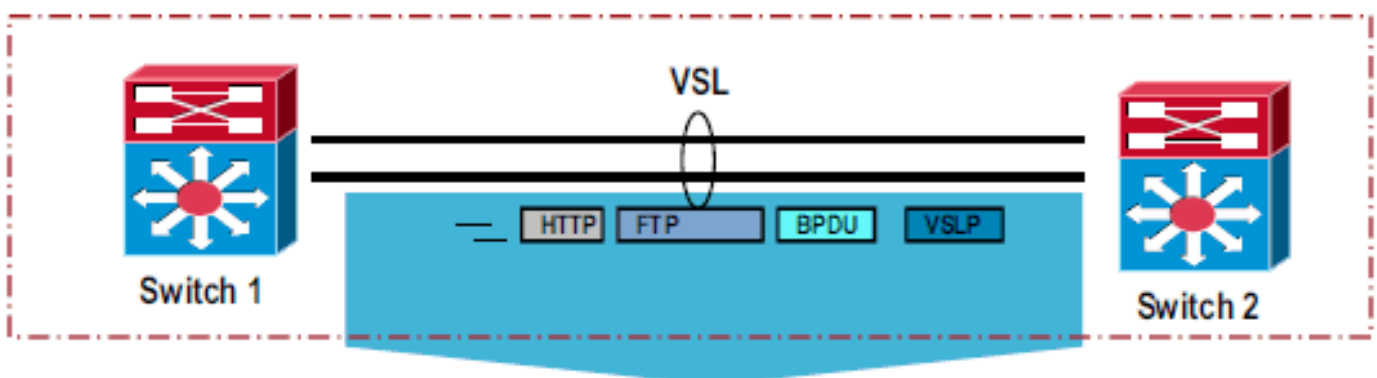
### Raccomandazioni

- I dispositivi collegati devono essere sempre **dotati di doppia abitazione** per ottimizzare le prestazioni di replica.
- **L'MEC è raccomandato** negli ambienti L3 e L2 per fornire una convergenza deterministica.
- La funzione MEC elimina il ricalcolo della funzione di inoltro di percorso inverso (RPF) durante qualsiasi errore di collegamento MEC.
- **Esegue la replica** con miglioramenti locali per una velocità effettiva di replica multicast più elevata.
- La replica in uscita richiede DFC per ottimizzare le prestazioni di replica.
- Ridimensionare la VSL in base ai requisiti del traffico.



## Qualità del servizio

### Impostazioni QoS VSL



- VSL è un percorso di comunicazione dati e di controllo interno critico e pertanto le impostazioni QoS sono preconfigurate e non sono consentite modifiche alla configurazione.
- VSL è sempre configurato come **CoS di attendibilità** e la coda in entrata è abilitata.
- Al momento sono supportati solo l'attendibilità e l'accodamento basati su CoS. I criteri del servizio non sono supportati in VSL.
- I criteri QoS devono essere applicati all'interfaccia di input dei flussi.
- La coda delle priorità è attivata per impostazione predefinita. Al traffico di controllo VSS e alle BPDU viene data alta priorità sul collegamento VSL.

## Raccomandazioni

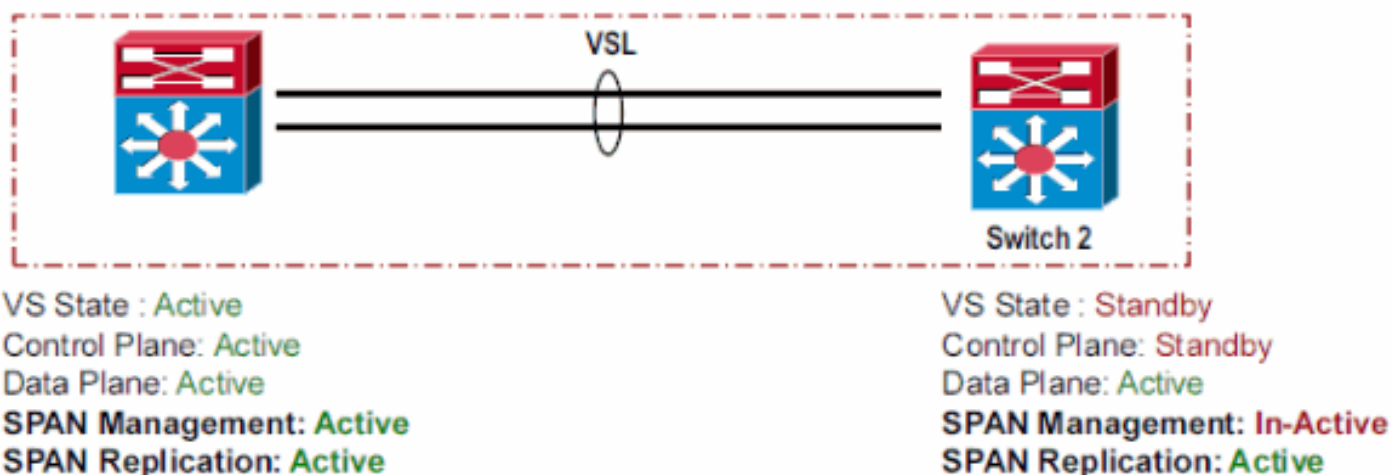
L'unica differenza tra le opzioni hardware compatibili con VSL è la configurazione della coda. Poiché la versione corrente del software non consente la modifica delle impostazioni predefinite della coda, qualsiasi combinazione di porte compatibili con VSL fornisce gli stessi risultati QoS.

Hardware	Modalità di accodamento	Modalità di attendibilità	Coda di trasmissione	Coda di ricezione
VSL su uplink - €" non solo 10G (predefinito)	CoS	CoS	1p3q4t (DWRR/SRR)	8q4t
VSL su uplink - solo €" 10 G	CoS	CoS	1p7q4t (DWRR/SRR)	2q4t
VSL tra uplink e schede di linea	CoS	CoS	1p3q4t [non 10G] (DWRR/SRR) 1p7q4t [solo 10G] (DWRR/SRR)	2q4t
VSL su schede di linea	CoS	CoS	1p7q4t (DWRR/SRR)	8q4t

Per ulteriori informazioni, fare riferimento a [Configurazione di VSL QoS](#).

## SPAN

In un dominio di commutazione virtuale, il numero di sessioni SPAN è limitato da ciò che il supervisore attivo del commutatore virtuale può fornire.



Virtual Switch System supporta queste funzionalità SPAN per ogni dominio di switch virtuale.

Attributo	Valore
Sessioni Tx SPAN	14

Sessioni Rx/Entrambe SPAN	2
Totale sessioni SPAN	16

## Raccomandazioni

- Se VSL è configurato come origine SPAN locale, le porte di destinazione SPAN devono trovarsi sullo stesso chassis delle interfacce VSL.
- Impossibile configurare VSL come destinazione SPAN.
- Impossibile configurare VSL come origine di RSPAN, ERSPAN o Tx solo per SPAN locale.
- L'intestazione VSL viene rimossa dalla porta di destinazione SPAN prima che il pacchetto venga trasmesso in uscita, quindi non può essere acquisita nelle tracce dello sniffer.
- Quando l'origine e la destinazione sono entrambe sullo stesso chassis (attivo o standby), il traffico SPAN non passa sul collegamento VSL. Per acquisire il traffico da entrambi gli chassis, sono disponibili due opzioni che evitano il flusso del traffico SPAN sulla VSL: Per ciascuna interfaccia di origine su uno chassis, l'interfaccia di destinazione deve trovarsi sullo stesso chassis. Ad esempio, PO20 ha gi1/1/1 e gi2/1/1: è necessario disporre di una destinazione per ogni 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
```

Tuttavia, ciò significa che si utilizzano entrambe le sessioni SPAN locali. Pertanto, non è possibile utilizzare altre sessioni SPAN locali. È possibile utilizzare l'interfaccia di destinazione per SPAN come MEC (scelta consigliata). La porta di destinazione può essere un MEC.

## Varie

### Raccomandazioni

- Per velocizzare il VSL, usare almeno un uplink del Supervisor per VSL.
- Configurare il comando [switch accept mode virtual](#) dopo la conversione VSS. Senza questo comando, la conversione non è completa.
- Salvare il backup del file di configurazione sia nel disco di avvio attivo che in quello in standby:. Ciò è di grande aiuto negli scenari di sostituzione del supervisore.
- Utilizzare un ID di dominio VSS univoco nella stessa rete. Un ID di dominio VSS duplicato può causare un'incoerenza di EtherChannel. Di seguito è riportato un esempio per modificare l'ID di dominio VSS. Usare il comando [switch virtual domain domain-id](#) per avviare la modifica dell'ID del dominio.

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

**Nota:** la configurazione del dominio con ID 50 ha effetto solo dopo l'emissione del comando **switch convert mode virtual exec**. Usare il comando [switch convert mode virtual](#) per completare l'attività.

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

**Nota:** l'ID del dominio virtuale viene modificato solo dopo aver salvato la configurazione e ricaricato lo switch.

- Usare il comando **erase nvram** al posto del comando **write erase** per ripristinare la configurazione del Servizio Copia Shadow del volume. Il comando **write erase** cancella le



variabili startup-config e ROMon. Per l'avvio in modalità VSS, il servizio VSS richiede la variabile *ID switch* ROMMon.

- Non utilizzare diritti di priorità. Per ulteriori informazioni, fare riferimento a [Cisco consiglia di non configurare l'interruzione per diritti di priorità](#) dello *switch*.
- Non utilizzare il comando **shutdown** per la simulazione di un errore VSL, in quanto crea una mancata corrispondenza di configurazione. Se si scollega un cavo, lo scenario di errore risulta più realistico.
- Non modificare l'algoritmo di hash VSL mentre il sistema è in produzione. La modifica dell'algoritmo richiede che il canale della porta venga disabilitato e riabilitato, con i comandi **shutdown** e **no shutdown**. Se si arresta una VSL, il traffico viene interrotto e si può verificare uno scenario a doppia attività.
- Configurare il timer di misurazione durata MAC su un valore tre volte superiore al valore del timer di sincronizzazione MAC. La sincronizzazione MAC predefinita e i timer di misurazione durata MAC possono causare un flooding unicast sconosciuto. Il servizio VSS può causare il flusso asimmetrico del traffico in modo che l'indirizzo MAC di origine venga appreso solo su uno chassis. Il timer di aging MAC di 300 secondi e il timer di sincronizzazione MAC di 160 secondi consentono fino a 20 secondi di flooding unicast sconosciuto per ogni indirizzo MAC in un intervallo di 320 secondi. Per risolvere questo problema, modificare i timer in modo che il timer di misurazione durata sia tre volte più lungo del timer di sincronizzazione, ad esempio [mac-address-table aging-time 480](#). Di seguito è riportato l'output di esempio del comando [show mac-address-table-aging-time](#):

```
switch#sh mac-address-table aging-time
Vlan Aging Time
----
Global 480
no vlan age other than global age configured
```
- Affinché VSS funzioni con lo status *eful switchover* (SSO), entrambi i Supervisor Engine devono eseguire la stessa versione del software.
- Se si torna a uno switch standalone dalla modalità VSS con il comando [switch convert mode standalone](#), l'operazione viene completata: Converte il nome dell'interfaccia con il nome **dello switch, dello slot o della porta** in **slot/porta**. Rimuove le interfacce non locali da running-config. Rimuove la configurazione delle porte e dei canali VSL. Salva Running-config in Startup-config. Imposta la variabile SP rommon SWITCH\_NUMBER su 0. Ricarica lo switch.
- Il riavvio dello switch è richiesto quando strettamente necessario; ad esempio, un aggiornamento IOS o come fase di risoluzione dei problemi. Se uno switch viene acceso per più di due anni, si tratta di uno switch stabile e la configurazione è stabile.

## [Domande frequenti](#)

### [È possibile utilizzare due supervisor in ogni chassis con VSS?](#)

Sì. In ogni chassis VSS configurato per la modalità VSS sono supportati due supervisor, a partire da SX14 e versioni successive.

### [Quando si rimuovono i comandi di interruzione per diritti di priorità sugli switch Catalyst serie 6500 in modalità VSS, gli switch vengono ricaricati?](#)

L'interruzione per diritti di priorità è sconsigliata. Pertanto, la rimozione dei comandi è una buona

procedura e non causa un ricaricamento. Per ulteriori informazioni sulla funzionalità di interruzione per diritti di priorità in VSS, vedere [Interruzione per diritti di priorità](#).

## Informazioni correlate

- [Best practice per gli switch Catalyst serie 6500/6000 e Catalyst serie 4500/4000 con software Cisco IOS](#)
- [Configurazione dei sistemi di switching virtuale](#)
- [Guida di riferimento ai comandi di Cisco IOS Virtual Switch](#)
- [Supporto dei prodotti Cisco Catalyst 6500 Virtual Switching System 1440](#)
- [Switch LAN - Supporto dei prodotti](#)
- [Supporto della tecnologia di switching LAN](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)