

Prácticas recomendadas para la implementación de Catalyst 6500 VSS

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Prácticas recomendadas de implementación de VSS](#)

[Alta disponibilidad de VSS](#)

[Recuperación del link ascendente](#)

[Pérdida y recuperación de link VSL](#)

[Redundancia con módulos de servicio](#)

[Multicast \(multidifusión\)](#)

[Calidad de servicio](#)

[SPAN](#)

[Miscelánea](#)

[Preguntas Frecuentes](#)

[¿Se pueden utilizar supervisores duales en cada chasis con VSS?](#)

[Al eliminar los comandos de preempt en los Catalyst 6500 Series Switches en el Modo VSS,](#)

[¿recargará los switches?](#)

[Información Relacionada](#)

[Introducción](#)

Este documento proporciona las prácticas recomendadas para los escenarios de implementación de Cisco Catalyst 6500 Virtual Switching System (VSS) 1440.

Este documento proporciona guía de configuración modular. Por lo tanto, puede leer cada sección de forma independiente y realizar cambios en un enfoque por fases. Este documento asume una comprensión básica y familiaridad con la interfaz de usuario del software Cisco IOS®. El documento no cubre el diseño general de la red.

[Prerequisites](#)

[Requirements](#)

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte [Convenciones de Consejos Técnicos Cisco para obtener más información sobre las convenciones del documento.](#)

Prácticas recomendadas de implementación de VSS

Las soluciones que ofrece este documento representan años de experiencia de campo de los ingenieros de Cisco que trabajan con redes complejas y muchos de los clientes más grandes. En consecuencia, este documento hace hincapié en las configuraciones que hacen que las redes tengan éxito. Este documento ofrece estas soluciones:

- Soluciones fáciles de gestionar y que los equipos de operaciones de red configuran
- Soluciones que promueven la alta disponibilidad y la alta estabilidad

Alta disponibilidad de VSS

- [Reenvío ininterrumpido](#)
- [Sincronización MAC OOB](#)

Reenvío ininterrumpido

Los switches Catalyst de la serie 6500 admiten resistencia a fallos, porque permite que un motor supervisor redundante tome el control si falla el motor supervisor principal. Cisco Non Stop Forwarding (NSF) funciona con Stateful SwitchOver (SSO) para minimizar la cantidad de tiempo que una red no está disponible para sus usuarios después de un switchover mientras se reenvían los paquetes IP.

Recomendaciones

- El reenvío ininterrumpido es obligatorio para la convergencia del switchover del supervisor en menos de un segundo.
- Utilice los temporizadores Hello y Dead predeterminados para los protocolos EIGRP / OSPF cuando se ejecute en un entorno VSS.
- Si ejecuta el sistema con el software modular Cisco IOS, se recomienda utilizar un temporizador OSPF Dead de mayor valor.

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
```

Consulte [Configuración de NSF con Redundancia de Supervisor Engine SSO](#) para obtener más información sobre NSF.

Sincronización MAC OOB

En el switching distribuido, cada tarjeta de función distribuida (DFC) mantiene su propia tabla CAM. Esto significa que cada DFC aprende la dirección MAC y la envejece, lo que depende del envejecimiento CAM y de la coincidencia de tráfico de esa entrada en particular. Con el switching distribuido, es normal que el motor supervisor no vea tráfico para una dirección MAC determinada durante un tiempo, por lo que la entrada puede caducar. Actualmente hay dos mecanismos disponibles para mantener las tablas CAM consistentes entre los diferentes motores, como DFC, que está presente en los módulos de línea, y Policy Feature Card (PFC), que está presente en los módulos supervisores:

- Inundación a Entramado (FF)
- Notificación MAC (MN)

Cuando una entrada de dirección MAC envejece en el PFC, el comando **show mac-address address <MAC_Address> all muestra el DFC o PFC que mantiene esta dirección MAC**. Para evitar que el envejecimiento de una entrada en DFC o PFC, incluso si no hay tráfico para esa dirección MAC, habilite la sincronización de la dirección MAC . Ejecute el comando **mac-address-table synchronization** global configuration y el comando **clear mac-address-table dynamic** privileged EXEC para habilitar la sincronización. Este comando mac-address-table synchronization está disponible en Cisco IOS Software Releases 12.2(18)SXE4 y posteriores. Después de que lo habilite, es posible siga viendo entradas que no están presentes en el PFC o el DFC. Sin embargo, el módulo tiene una manera de aprender de otros módulos que utilicen Canal Ethernet fuera de banda (EOBC).

Recomendaciones

Habilite la sincronización MAC fuera de banda. Se utiliza para sincronizar las tablas de

direcciones mac a través de los motores de reenvío. Si WS-6708-10G está presente en el sistema VSS, la sincronización MAC se habilita automáticamente. Si no es así, se debe habilitar 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
```

Terminología VSS

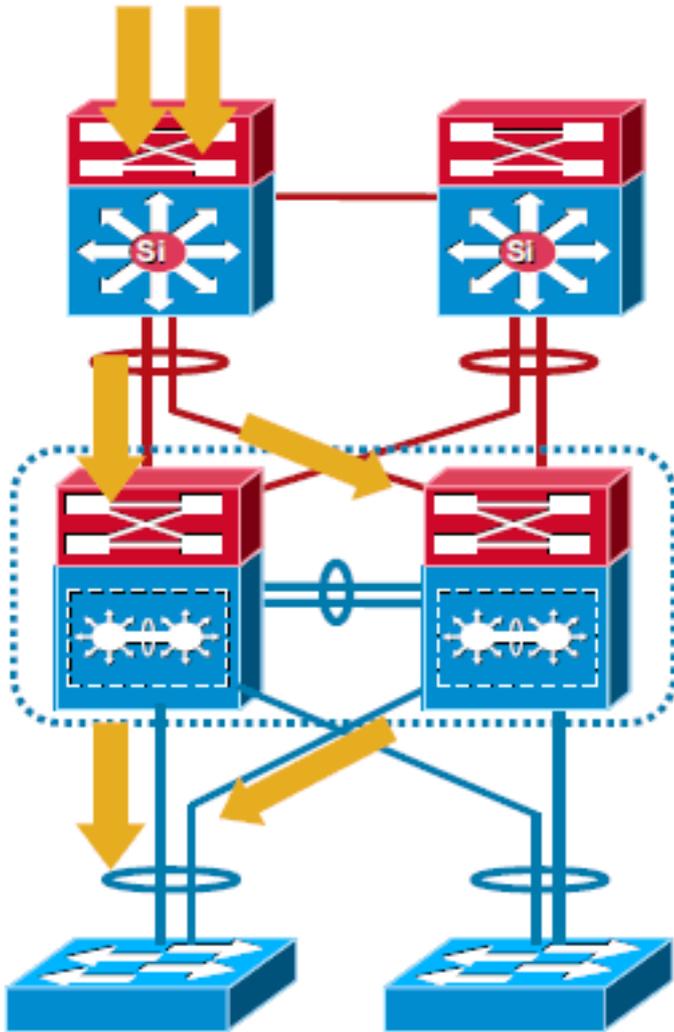
- **Virtual Switch Link (VSL):** canal de puerto especial necesario para agrupar dos switches físicos en un switch virtual.
- **Protocolo VSL (VSLP):** se ejecuta entre el switch activo y en espera a través del VSL y tiene dos componentes: LMP y RRPP
Protocolo de administración de enlaces (LMP): se ejecuta sobre cada enlace individual en VSL
Protocolo de resolución de funciones (RRP): se ejecuta en cada lado (cada par) del canal de puerto VSL

Planificación de capacidad para VSL

Idealmente, en la configuración VSS de doble conexión, no se envía tráfico de datos en el link VSL. Cada switch está programado para elegir sus interfaces locales para el reenvío de tráfico.

Se requiere una planificación de capacidad de enlace VSL adicional para el tráfico transportado por:

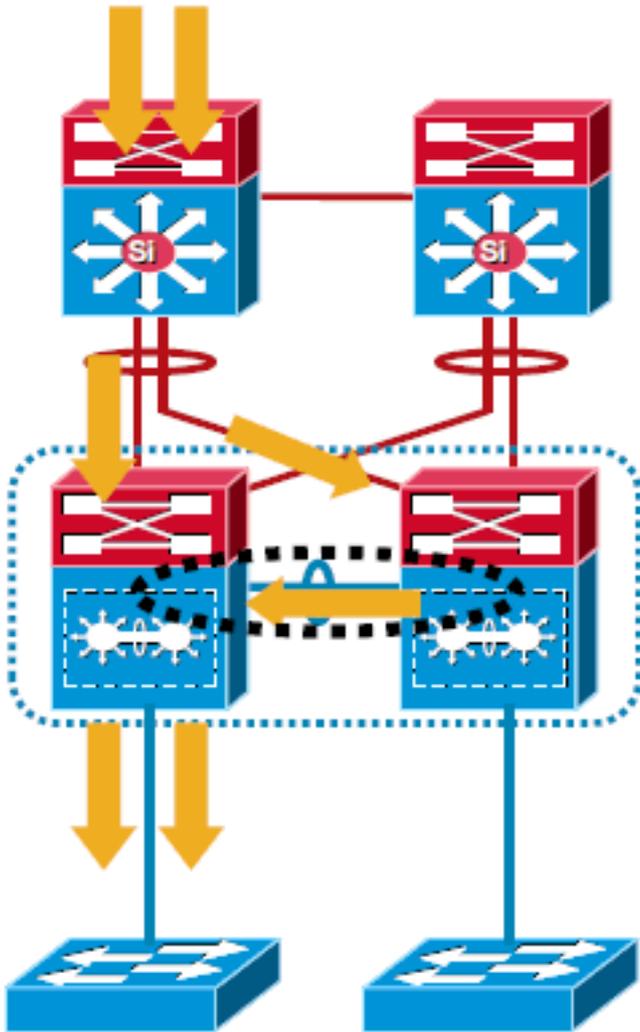
- Dispositivos de un solo enlace
- SPAN remoto de un switch a otro
- Tráfico del módulo de servicio " FWSM, ACE, etc.



Consulte [Tráfico en el VSL](#) para obtener más información.

Recomendaciones

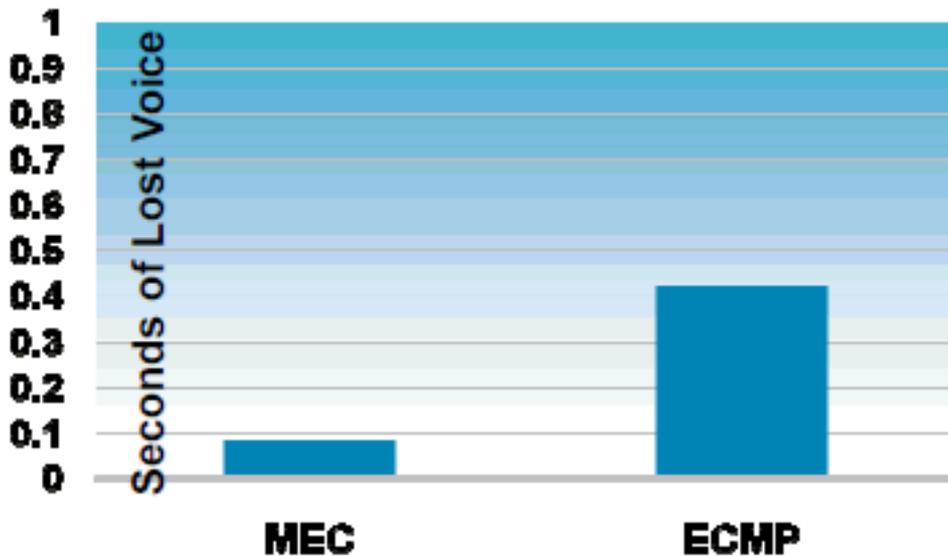
- Siempre se conectan dispositivos de **doble casa** a VSS.
- Siempre agrupe **VSL EtherChannel en la potencia de 2**, porque tiene mejores resultados de hash para optimizar el intercambio de carga del tráfico.
- La redundancia del VSL sigue siendo crítica junto con la resistencia de los enlaces VSL.
- La recomendación es que, al menos, el ancho de banda VSL sea igual a los enlaces ascendentes conectados a un único switch físico.



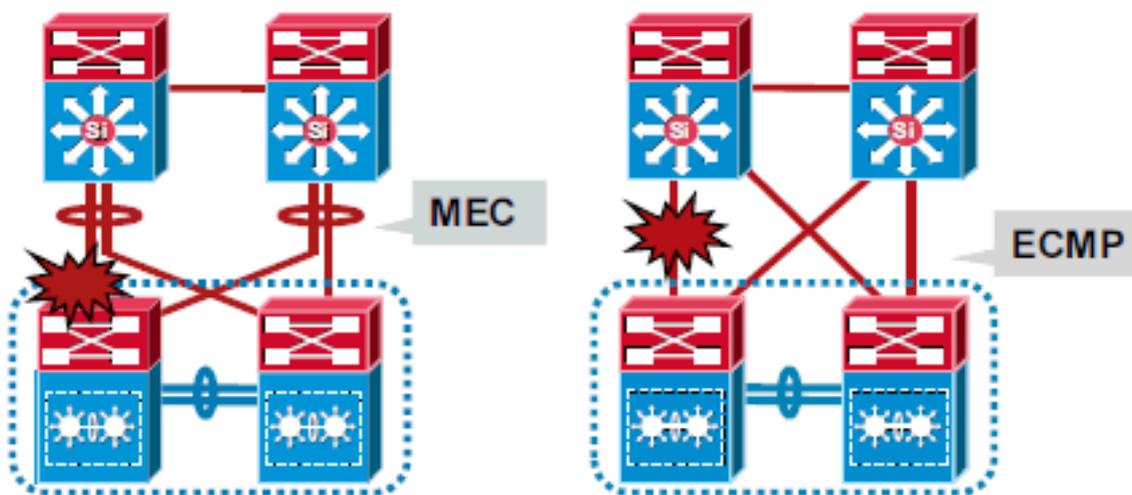
Recuperación del link ascendente

La recuperación de los enlaces ascendentes (enlaces al núcleo) se puede lograr mediante la función MultiChassis EtherChannel (MEC) o la función Equal Cost MultiPath (ECMP).

La convergencia MEC es **coherente e independiente** del número de rutas. Mientras que la convergencia del ECMP **depende** del número de rutas. Este gráfico indica la magnitud de la pérdida en una sesión de voz.



Estas imágenes muestran escenarios de falla de link con MEC y ECMP:



EtherChannel de varios chasis

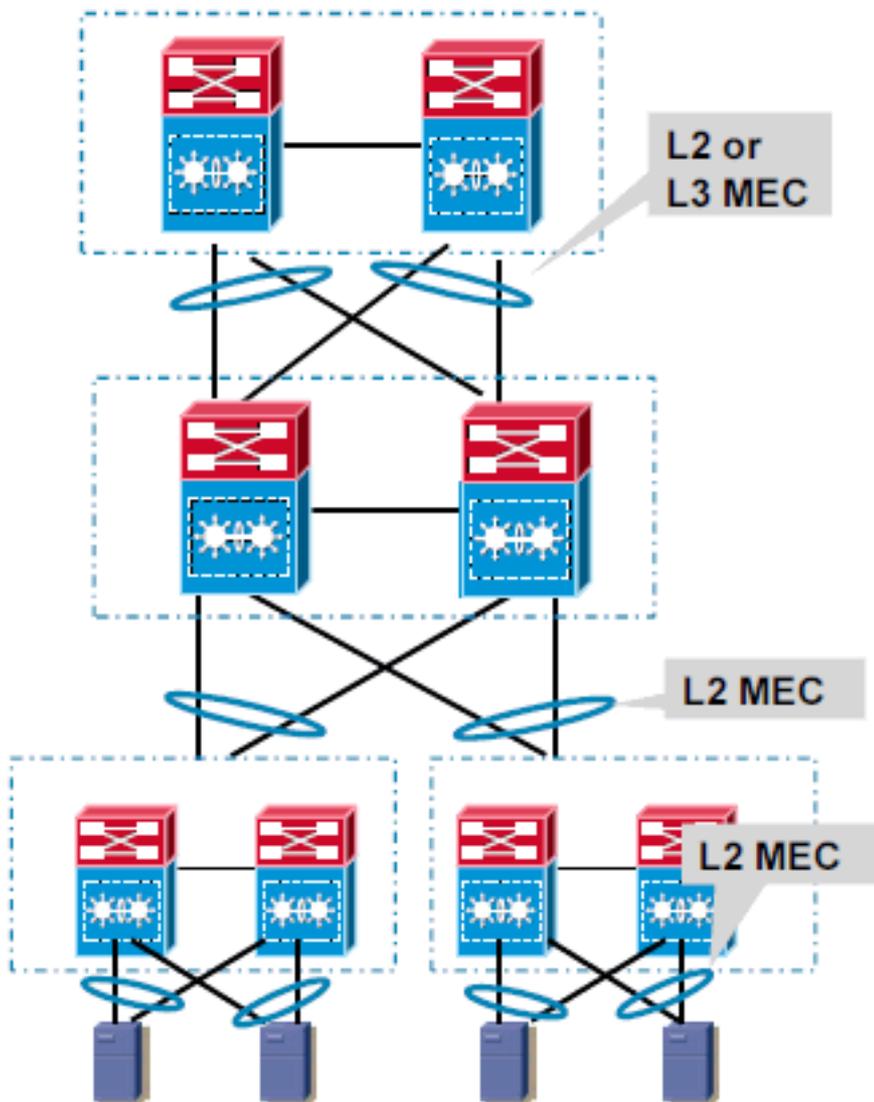
Un EtherChannel de varios chasis es un EtherChannel con puertos que terminan en ambos chasis del VSS. Un MEC VSS puede conectarse a cualquier elemento de red que admita EtherChannel, como un host, servidor, router o switch. En el VSS, un MEC es un EtherChannel con capacidad adicional. El VSS equilibra la carga entre los puertos en cada chasis de forma independiente. Por ejemplo, si el tráfico ingresa al chasis activo, el VSS selecciona un link MEC del chasis activo. Esta capacidad de MEC garantiza que el tráfico de datos no atraviese innecesariamente el VSL.

- El MEC L2 habilita la topología sin loops, duplica el ancho de banda del link ascendente ya que no se bloquean los links y proporciona una convergencia más rápida que el STP.
- La MEC L3 proporciona recuentos de vecinos reducidos, mejor distribución de carga (L2 y L3 para unidifusión y multidifusión), menor utilización de enlaces VSL para flujos de multidifusión y convergencia más rápida que la ECMP.

Refiérase a [Multichassis EtherChannels](#) para obtener más información sobre MEC.

Recomendaciones

- Ejecute siempre **MEC L2 o L3**.
- No utilice opciones **on** y **off** con negociación de protocolo de enlace troncal o PAgP o LACP. PAgP â€" Ejecute **Desirable-Desirable** con enlaces MEC. LACP â€" Ejecute **Active-Active** con enlaces MEC. Trunk â€" Ejecute **Desirable-Desirable** con enlaces MEC.



Pérdida y recuperación de link VSL

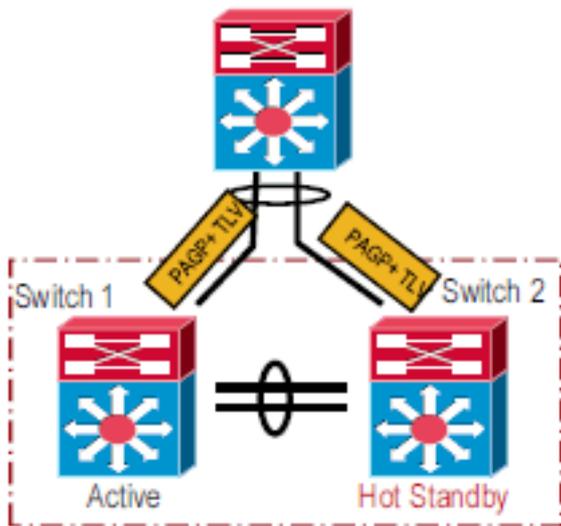
Si el VSL falla, el chasis en espera no puede determinar el estado del chasis activo. Para asegurarse de que el switchover se produzca sin demora, el chasis en espera asume que el chasis activo ha fallado e inicia switchover para asumir el rol activo.

Si el chasis activo original sigue funcionando, ambos chasis ahora están activos. Esta situación se denomina escenario **dual-activo**. Un escenario de doble actividad puede tener efectos adversos en la estabilidad de la red, porque ambos chasis utilizan las mismas direcciones IP, claves SSH e ID de puente STP. El sistema de switching virtual (VSS) debe detectar un escenario de doble actividad y realizar acciones de recuperación.

El sistema de conmutación virtual soporta estos tres métodos para detectar un escenario dual-active:

- PAgP Mejorado â€" Utiliza la mensajería PAgP sobre los links MEC para comunicarse entre los dos chasis a través de un switch vecino. El PAgP mejorado es más rápido que el BFD IP,

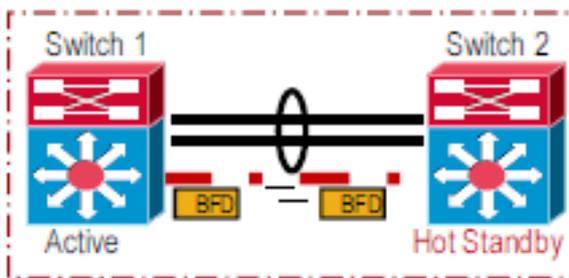
pero requiere un switch vecino que admita las mejoras de



PAgP.

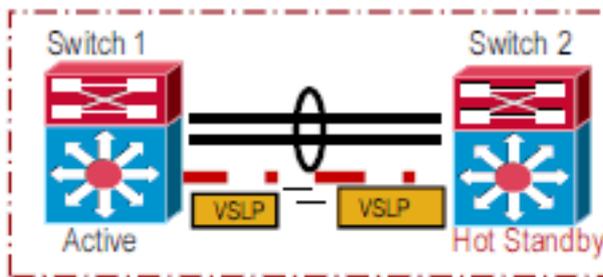
Tabla de soporte de ePAgP:

- IP Bidirectional Forwarding Detection (BFD) " Utiliza la mensajería BFD a través de una conexión Ethernet de respaldo. IP BFD utiliza una conexión directa entre los dos chasis y no requiere soporte de un switch vecino. Este método está disponible en Cisco IOS Software



Release 12.2(33)SXH1 y posteriores.

- VSLP fast-hello dual-active " Utiliza mensajes hello especiales a través de una conexión Ethernet de respaldo. El fast-hello dual-activo es más rápido que el BFD IP y no requiere soporte de un switch vecino. Este método sólo está disponible en Cisco IOS Software

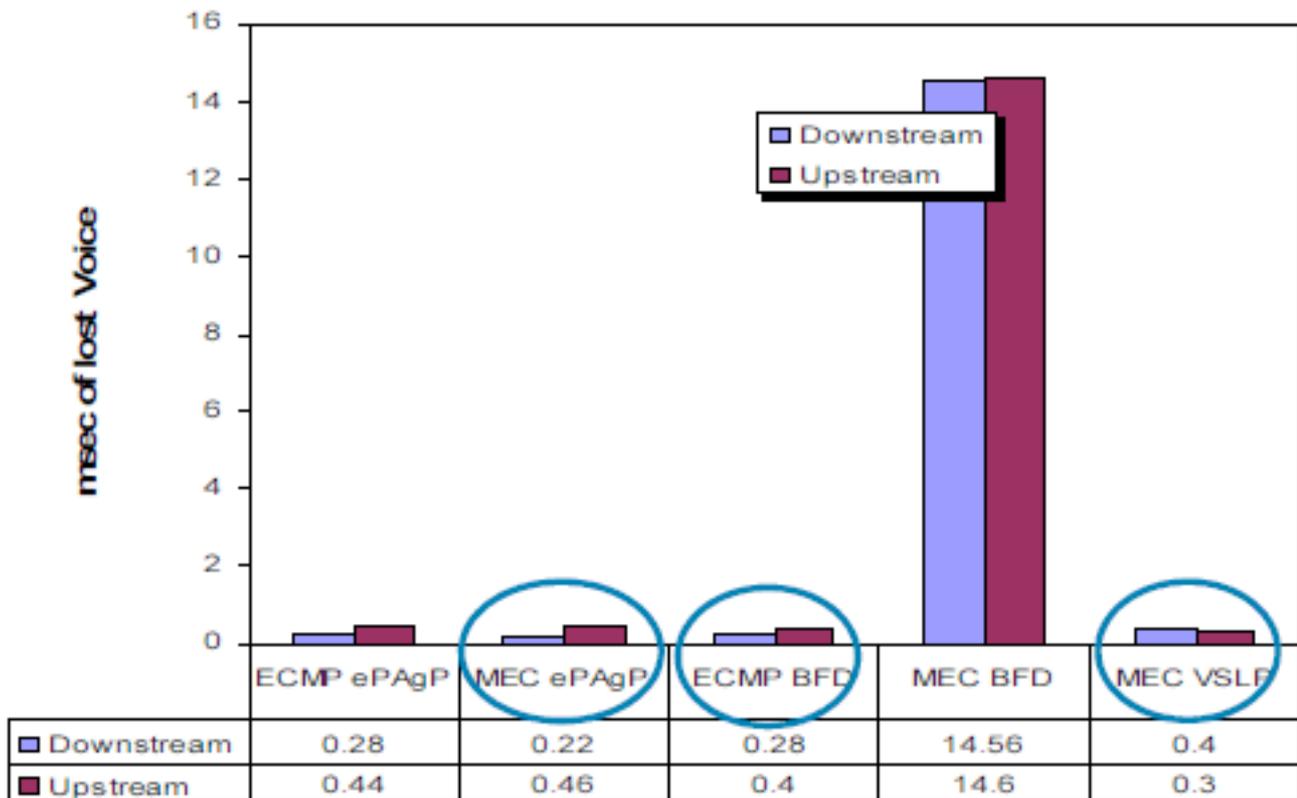


Release 12.2(33)SXI y posteriores.

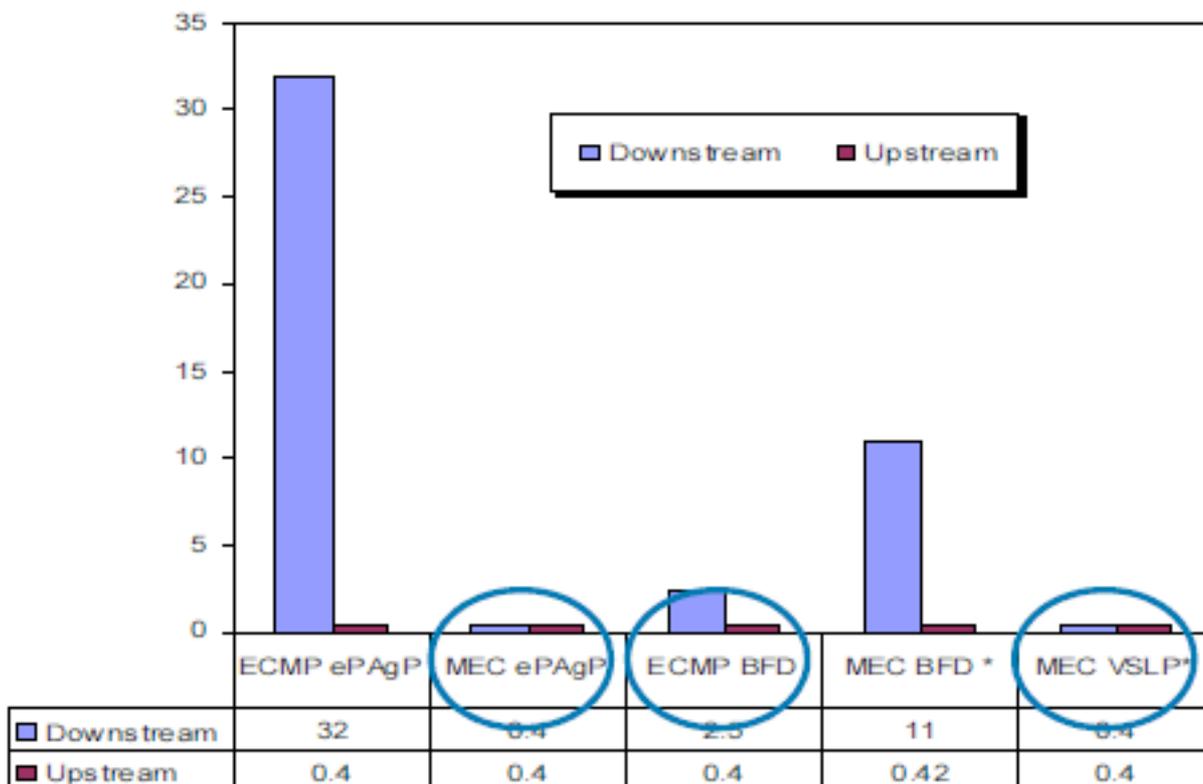
Puede configurar los tres métodos de detección para que estén activos al mismo tiempo.

Estos gráficos proporcionan información sobre la convergencia de algunos protocolos de ruteo IP con respecto a la convergencia activa doble de VSS.

Convergencia EIGRP con temporizadores predeterminados



Convergencia OSPF con temporizadores predeterminados



Recomendaciones

- Active al menos dos enlaces en VSL.
- Utilice **MEC con ePAgP** o **MEC con VSLP Fast Hello** para obtener resultados más rápidos de convergencia de pérdida de link VSL.
- Habilite **ECMP con IP-BFD**.

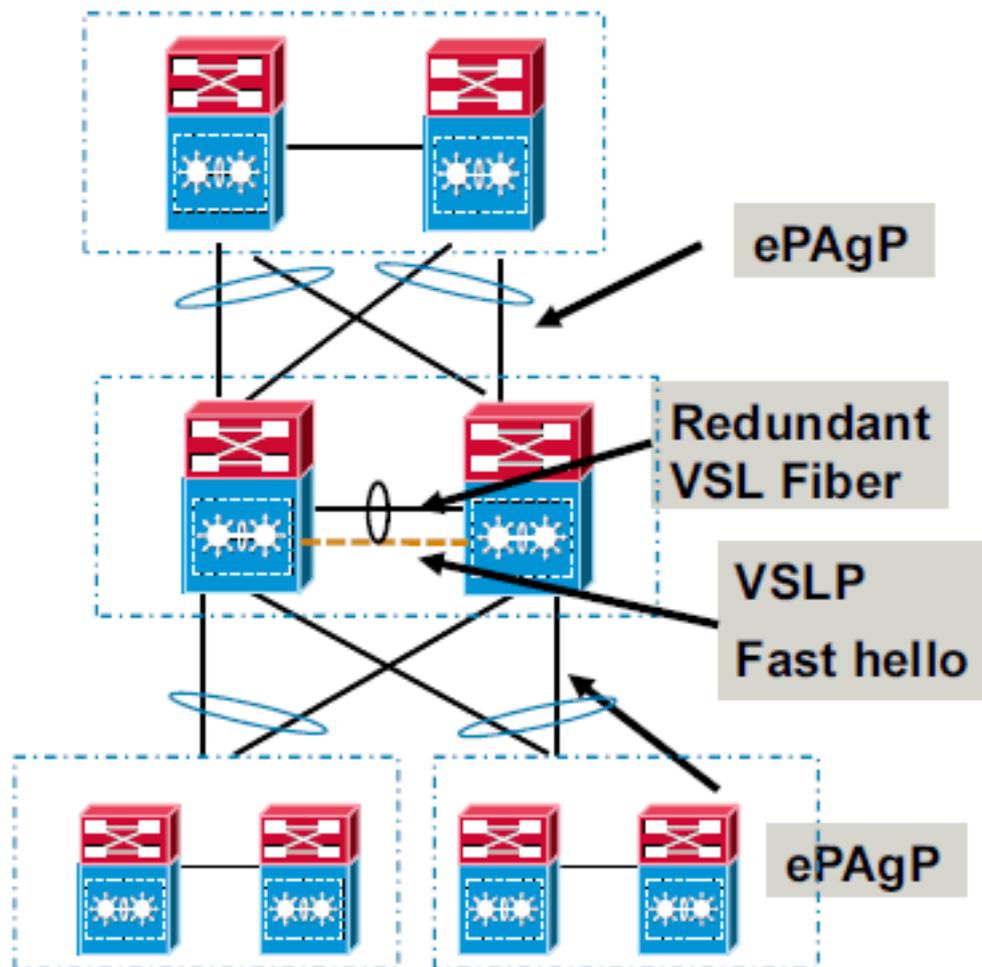
- Habilite ePAgP al núcleo, si la capa de acceso no es compatible con ePAgP.
- Habilite tanto ePAgP como los métodos VSLP Fast Hello basados en el link directo de latidos cardíacos, si es posible.
- Durante el proceso de pérdida y recuperación de VSL no realice cambios de configuración. Después de que se restaura al menos un link de miembro VSL, si la configuración en el chasis ACTIVE antiguo no se **modifica**, ACTIVE antiguo **se reinicia** a arrancar en el estado de redundancia de espera en caliente VSS.

```
*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.
```

Si la **configuración cambia**, marcada *sucia* por el proceso de sincronización de la configuración, el switch no se recarga automáticamente. La recarga manual se debe ejecutar en ACTIVE antigua después de que se corrija y guarde la configuración. Incluso si sólo ingresa al modo de configuración y sale, marca la configuración *sucia* y fuerza una intervención manual.

```
*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



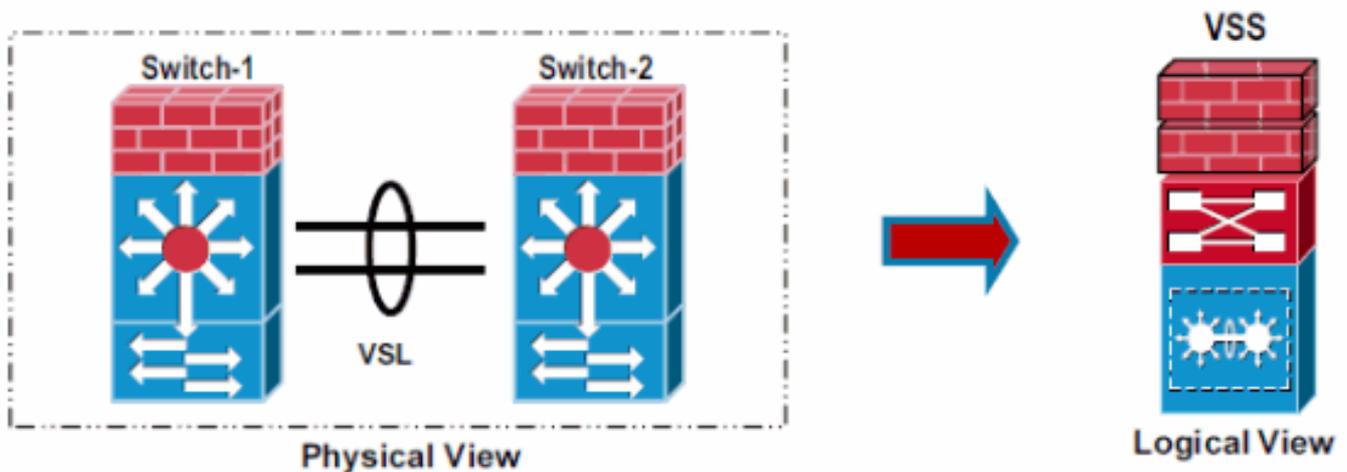
Refiérase a [Detección Dual-Active](#) para obtener más información.

[Redundancia con módulos de servicio](#)

El soporte de módulos de servicio es un requisito clave para posicionar el VSS en el mercado de instalaciones empresariales y Data Centers empresariales. La lista de módulos de servicio admitidos en el Sistema de switch virtual son:

Módulo de servicio	Versión mínima de Cisco IOS	Versión mínima del módulo
Network Analysis Module (NAM-1 y NAM-2) (WS-SVC-NAM-1 y WS-SVC-NAM-2)	12.2(33)S XH1	3.6.1 bis
Application Control Engine (ACE10 y ACE20) (ACE10-6500-K9 y ACE20-MOD-K9)	12.2(33)S XI	A2(1.3)
Módulo de servicios del sistema de detección de intrusiones (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
Módulo de servicios de firewall	12.2(33)S	4.0.4

Los módulos de servicio se pueden colocar en cualquiera de los chasis físicos que componen un VSS.



Recomendaciones

- Para la configuración con más de un módulo de servicio de un tipo dado, configure uno en cada switch físico para una mejor disponibilidad.
- VSL transporta el tráfico en escenarios normales y de conmutación por fallo, el ancho de banda VSL se debe ajustar en consecuencia.

Consulte [Integración de Módulos de Servicio de Cisco con Cisco Catalyst 6500 Virtual Switching System 1440](#) para obtener más información sobre la integración de módulos de servicio.

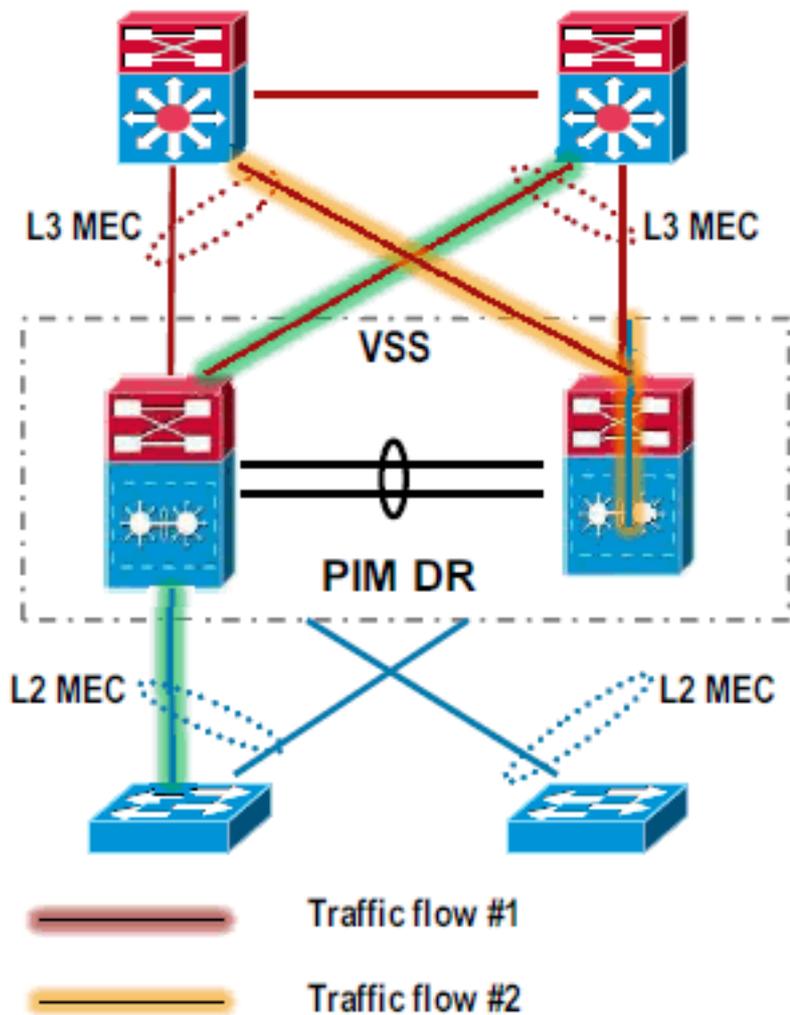
Multicast (multidifusión)

Los protocolos de multidifusión IPv4 se ejecutan en el motor supervisor activo. Los paquetes de protocolo de administración de grupos de Internet (IGMP) y multidifusión independiente de protocolo (PIM) recibidos en el motor supervisor en espera se transmiten a través de VSL al chasis activo. El motor supervisor activo envía paquetes de protocolo IGMP y PIM al motor supervisor en espera para mantener la información de Capa 2 para el stateful switchover (SSO).

Consulte [Multidifusión IPv4](#) para obtener más información.

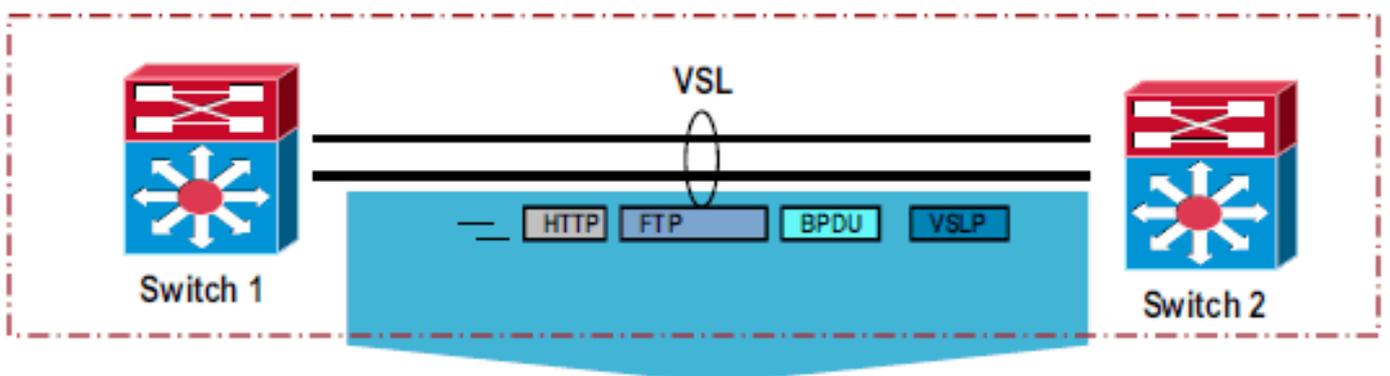
Recomendaciones

- Los dispositivos conectados siempre deben tener **doble conexión** para lograr un rendimiento de replicación óptimo.
- **Se recomienda MEC** en entornos L3 y L2 para proporcionar convergencia determinista.
- MEC elimina el recálculo de Reenvío de Trayectoria Inversa (RPF) durante cualquier falla de link MEC.
- **Replicación de salida** con mejora local para mayor rendimiento de replicación multidifusión.
- La replicación de salida requiere DFC para optimizar el rendimiento de replicación.
- Ajuste el tamaño de VSL para satisfacer los requisitos de tráfico.



Calidad de servicio

Configuración de VSL QoS



- VSL es una ruta crítica de comunicación de datos y control interno, por lo que la configuración de QoS está preconfigurada y no se permiten cambios en la configuración.
- VSL siempre se configura como **Trust CoS** y la colocación en cola de ingreso está habilitada.
- Actualmente sólo se admite la cola y la confianza basada en CoS. Las políticas de servicio no se admiten en VSL.
- Las políticas de QoS se deben aplicar en la interfaz de entrada de los flujos.
- La cola de prioridad está habilitada de forma predeterminada. El tráfico de control VSS y las BPDU reciben una alta prioridad en el link VSL.

Recomendaciones

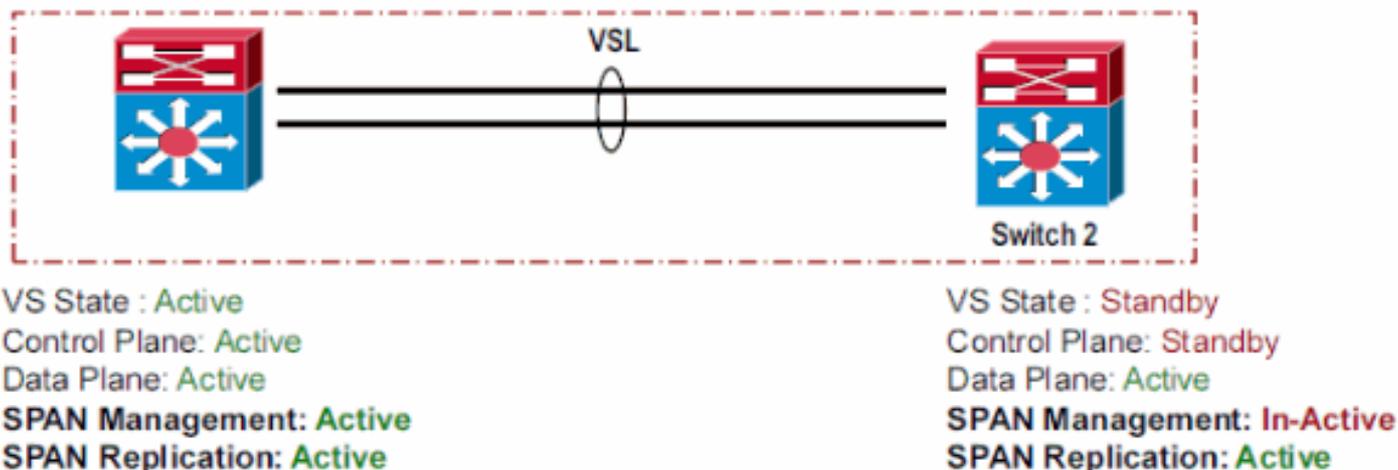
La única diferencia entre las opciones de hardware compatibles con VSL es la configuración de cola. Como la versión actual del software no permite la modificación de la configuración de cola predeterminada, cualquier combinación de puertos compatibles con VSL proporciona los mismos resultados de QoS.

Hardware	Modo de cola	Modo de confianza	Cola de transmisión	Cola de recepción
VSL en enlaces ascendentes " no 10G solamente (predeterminado)	CoS	CoS	1p3q4t (DWRR/SRR)	8q4t
VSL en enlaces ascendentes " 10G solamente	CoS	CoS	1p7q4t (DWRR/SRR)	2q4t
VSL a través de enlaces ascendentes y tarjetas de línea	CoS	CoS	1p3q4t [no 10G] (DWRR/SRR) 1p7q4t [sólo 10G] (DWRR/SRR)	2q4t
VSL en tarjetas de línea	CoS	CoS	1p7q4t (DWRR/SRR)	8q4t

Consulte [Configuración de QoS VSL](#) para obtener más información.

SPAN

En un dominio de switch virtual, el número de sesiones SPAN está limitado por lo que el supervisor activo del switch virtual puede proporcionar.



Virtual Switch System soporta estas capacidades SPAN por dominio de switch virtual.

Atributo	Valor
Sesiones Tx SPAN	14

Rx / Ambas Sesiones SPAN	2
Sesiones SPAN totales	16

Recomendaciones

- Si VSL se configura como origen SPAN local, los puertos de destino SPAN deben estar en el mismo chasis que las interfaces VSL.
- VSL no se puede configurar como destino SPAN.
- VSL no se puede configurar como origen de RSPAN, ERSPAN o Tx sólo SPAN local.
- El puerto de destino de SPAN elimina el encabezado VSL antes de que se transmita el paquete y, por lo tanto, no se puede capturar en los rastros del sniffer.
- Cuando el origen y el destino están ambos en el mismo chasis (activo o en espera), el tráfico SPAN no fluye sobre el link VSL. Para capturar el tráfico de ambos chasis, hay dos opciones que evitan el flujo del tráfico SPAN en el VSL: Para cada interfaz de origen en un chasis, la interfaz de destino debe estar en el mismo chasis. Por ejemplo, PO20 tiene gi1/1/1 y gi2/1/1: necesita tener un destino para cada chasis.

```
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
```

Sin embargo, esto significa que se utilizan ambas sesiones SPAN locales. Por lo tanto, no puede utilizar ninguna otra sesión SPAN local. Puede utilizar la interfaz de destino para SPAN como MEC (recomendado). El puerto de destino puede ser un MEC.

Miscelánea

Recomendaciones

- Utilice un mínimo de un link ascendente de Supervisor para VSL para que VSL se active más rápidamente.
- Configure el comando [switch accept mode virtual](#) después de la conversión VSS. Sin este comando, la conversión no está completa.
- Guarde la copia de seguridad del archivo de configuración tanto en el disco de inicio activo como en el de espera en caliente: Esto es de gran ayuda en situaciones de sustitución de supervisores.
- Use **VSS domain-ID único** dentro de la misma red. El ID de dominio VSS duplicado puede causar inconsistencia de EtherChannel. Este es un ejemplo para cambiar el ID de dominio VSS. Utilice el comando [switch virtual domain domain-id](#) para iniciar el cambio de ID de dominio.

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

Nota: La configuración de ID de dominio 50 surte efecto sólo después de que se ejecute el comando `exec switch Convert mode virtual`. Utilice el comando [switch Convert mode virtual](#) para completar la tarea.

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

Nota: El ID de dominio virtual sólo cambia después de guardar la configuración y recargar el switch.

- Utilice el comando `erase nvram` en lugar del comando `write erase` para restablecer la

configuración de VSS. El comando **write erase** borra las variables startup-config y ROMMon. VSS requiere la variable *switch-id* ROMMon para arrancar en el modo VSS.

- No utilice la precaución. Refiérase a [las recomendaciones de Cisco para que no configure la preferencia del switch](#) para obtener más información.
- No utilice el comando **shutdown** para la simulación de fallas VSL, ya que crea una discordancia de configuración. Si desconecta un cable, proporciona un escenario de falla más realista.
- No cambie el algoritmo de hash VSL mientras el sistema está en producción. El cambio del algoritmo requiere que el canal de puerto se inhabilite y se vuelva a habilitar, con los comandos **shutdown** y **no shutdown**. Si apaga un VSL, provoca una interrupción del tráfico y puede terminar en un escenario de doble actividad.
- Configure el temporizador de envejecimiento MAC a tres veces el valor del temporizador de sincronización MAC. La sincronización MAC predeterminada y los temporizadores de envejecimiento MAC pueden provocar inundaciones de unidifusión desconocidas. VSS puede hacer que el tráfico fluya de forma asimétrica de modo que la dirección MAC de origen sólo se aprenda en un chasis. El temporizador de envejecimiento MAC de 300 segundos y el temporizador de sincronización MAC de 160 segundos permiten hasta 20 segundos de inundación de unidifusión desconocida para cualquier dirección MAC dada en un intervalo de 320 segundos. Para resolver esto, cambie los temporizadores de manera que el temporizador de envejecimiento sea tres veces más largo que el temporizador de sincronización, por ejemplo, **mac-address-table aging-time 480**. El ejemplo de salida de [show mac-address-table aging-time](#) se muestra aquí:

```
switch#sh mac-address-table aging-time
Vlan Aging Time
-----
Global 480
no vlan age other than global age configured
```
- Para que VSS funcione con stateful switchover (SSO), ambos motores supervisores deben ejecutar la misma versión de software.
- Si migra nuevamente a un switch independiente del modo VSS a través del comando [switch Convert mode autónomo](#), completa estas tareas: Convierte el nombre de la interfaz con el nombre del **switch/slot/puerto en slot/puerto**. Quita las interfaces no locales de running-config. Quita la configuración de puertos y canales de puerto VSL. Guarda Running-config en Startup-config. Establece la variable SP rommon SWITCH_NUMBER en 0. Recarga el switch.
- Se requiere el reinicio del switch cuando son estrictamente necesarios; por ejemplo, una actualización del IOS o como un paso de solución de problemas. Un switch activo durante más de dos años significa que es un switch estable y la configuración también es estable.

[Preguntas Frecuentes](#)

[¿Se pueden utilizar supervisores duales en cada chasis con VSS?](#)

Yes. Se admiten supervisores duales en cada chasis VSS configurado para el modo VSS a partir de SX14 y posteriores.

[Al eliminar los comandos de preempt en los Catalyst 6500 Series Switches en el Modo VSS, ¿recargará los switches?](#)

No se recomienda la preferencia del switch. Por lo tanto, quitar los comandos es una buena práctica y no causa una recarga. Para obtener más información sobre la función de preferencia en VSS, refiérase a [Preferencia del Switch](#).

Información Relacionada

- [Prácticas recomendadas para los switches Catalyst serie 6500/6000 y Catalyst serie 4500/4000 que ejecutan el software Cisco IOS](#)
- [Configuración de Virtual Switching Systems](#)
- [Referencia de Comandos del Switch Virtual de Cisco IOS](#)
- [Soporte del producto Cisco Catalyst 6500 Virtual Switching System 1440](#)
- [Soporte Técnico al switch LAN](#)
- [Soporte de Tecnología de LAN Switching](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)