Cisco Catalyst 6500 Virtual Switching System Deployment Best Practices

Document ID: 109547

Contents

Introduction

This document provides best practices for Cisco Catalyst 6500 Virtual Switching System (VSS) 1440 deployment scenarios.

This document provides modular configuration guidance. Therefore, you can read each section independently and make changes in a phased approach. This document assumes a basic comprehension and familiarity with the Cisco IOS® Software user interface. The document does not cover overall network design.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

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.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

VSS Deployment Best Practices

The solutions that this document offers represent years of field experience from Cisco engineers who work with complex networks and many of the largest customers. Consequently, this document emphasizes configurations that make networks successful. This document offers these solutions:

- Solutions that are easy to manage and that network operations teams configure
- Solutions that promote high availability and high stability

VSS High Availability

- Non Stop Forwarding
- OOB MAC Synchronization

Non Stop Forwarding

Catalyst 6500 series switches support fault resistance, because it allows a redundant supervisor engine to take over if the primary supervisor engine fails. Cisco Non Stop Forwarding (NSF) works with Stateful SwitchOver (SSO) in order to minimize the amount of time a network is unavailable to its users after a switchover while IP packets continue to be forwarded.

Recommendations

- Non Stop Forwarding is required for supervisor switchover convergence at sub−second time.
- Use default Hello and Dead timers for EIGRP / OSPF protocols when you run in a VSS environment.
- If you run the system with modular Cisco IOS software, it is recommended to go for larger value OSPF Dead timer.

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
```

Refer to Configuring NSF with SSO Supervisor Engine Redundancy for more information on NSF.

OOB MAC Synchronization

In distributed switching, each Distributed Feature Card (DFC) maintains its own CAM table. This means that each DFC learns the MAC address and ages them, which depends on the CAM aging and traffic matching of that particular entry. With distributed switching, it is normal that the supervisor engine does not see any traffic for a particular MAC address for a while, so the entry can expire. There are currently two mechanisms available to keep the CAM tables consistent between the different engines, such as DFC, which is present in line modules, and Policy Feature Card (PFC), which is present in supervisor modules:

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

When a MAC address entry is aged out on the PFC, the **show mac-address address** <*MAC_Address*> **all** command displays the DFC or PFC that holds this MAC address. In order to prevent the age out of an entry on a DFC or PFC, even if there is not traffic for that MAC address, enable the MAC address synchronization. Issue the **mac-address-table synchronize** global configuration command and **clear mac-address-table dynamic** privileged EXEC command in order to enable the synchronization. This mac-address-table synchronize command is available from Cisco IOS Software Releases 12.2(18)SXE4 and later. After you enable it, it is possible to still see entries that are not present in PFC or DFC. However, the module has a way to learn it from others that use Ethernet Out of Band Channel (EOBC).

Recommendations

Enable Out-of-Band MAC synchronization. It is used in order to synchronize mac-address tables across the forwarding engines. If WS-6708-10G is present in the VSS system, MAC synchronization is automatically enabled. If not, it must be enabled manually.

```
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 Terminology

- **Virtual Switch Link (VSL)** A special port channel required to bundle two physical switches into one virtual switch.
- **VSL Protocol (VSLP)** Runs between active and standby switch over the VSL, and has two components: LMP and RRP

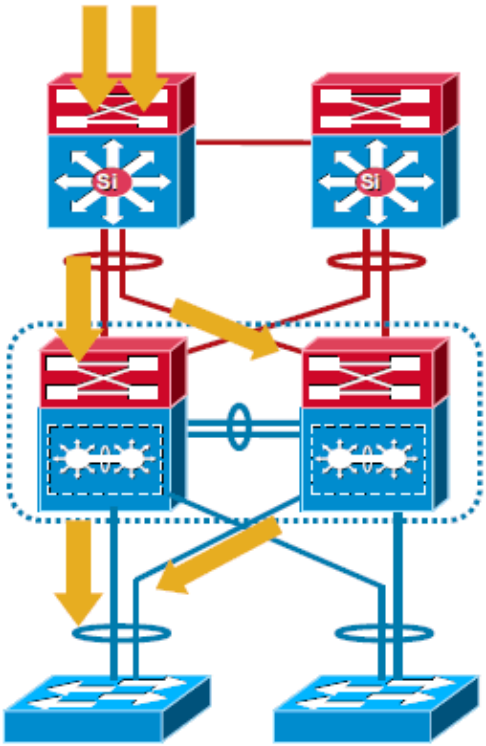
    - **Link Management Protocol (LMP)** Runs over each individual link in VSL
    - **Role Resolution Protocol (RRP)** Runs on each side (each peer) of the VSL port channel

Capacity Planning for VSL

Ideally in dual-homed VSS configuration, no data traffic is sent on the VSL link. Each switch is programmed to choose its local interfaces for traffic forwarding.

Additional VSL link capacity planning is required for traffic carried by:

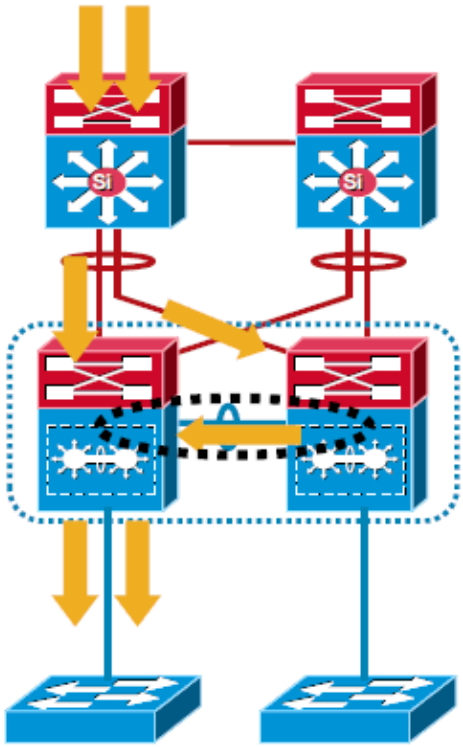
- Single homed devices
- Remote SPAN from one switch to another
- Service module traffic â€ FWSM, ACE, etc.



Refer to Traffic on the VSL for more information.

Recommendations

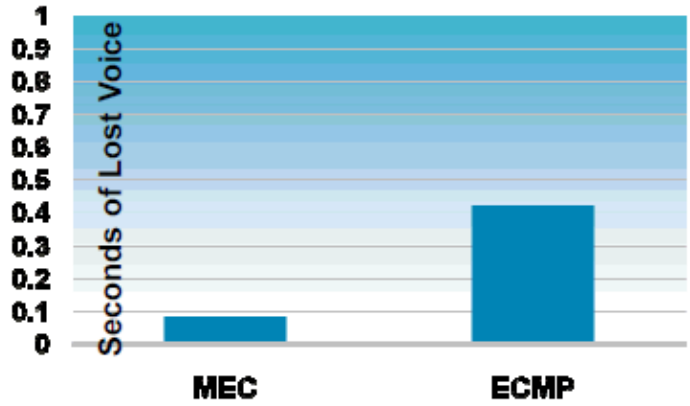
- Always **dual−home** devices connected to VSS.
- Always bundle **VSL EtherChannel in the power of 2**, because it has better hash results for optimized traffic load−sharing.
- Redundancy of the VSL is still critical along with resiliency of VSL links.
- The recommendation is to atleast have VSL bandwidth equal to uplinks connected to a single physical switch.



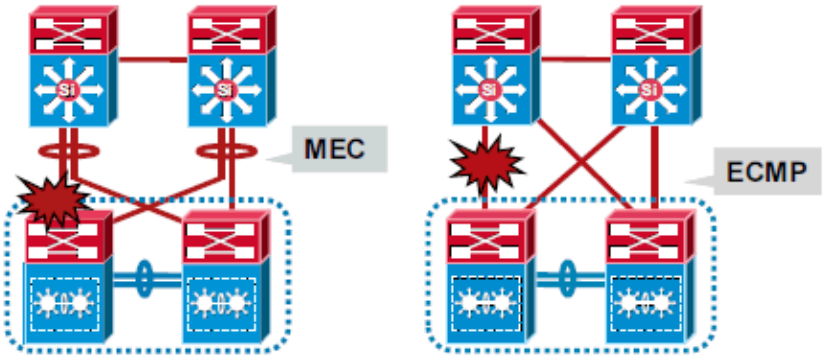
Upstream Link Recovery

The recovery of upstream links (links to the core) can be attained through either MultiChassis EtherChannel (MEC) or the Equal Cost MultiPath (ECMP) feature.

MEC convergence is **consistent and independent** of the number of routes. Whereas, ECMP convergence is **dependent** on the number of routes. This graph indicates the magnitude of loss in a voice session.



These images show link failure scenarios with MEC and ECMP:



MultiChassis EtherChannel

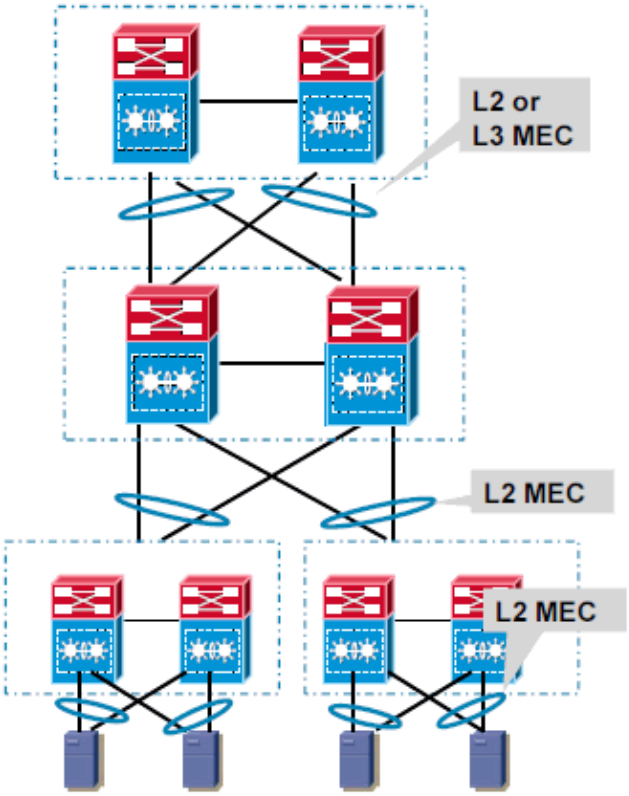
A MultiChassis EtherChannel is an EtherChannel with ports that terminate on both chassis of the VSS. A VSS MEC can connect to any network element that supports EtherChannel, such as a host, server, router, or switch. At the VSS, an MEC is an EtherChannel with additional capability. The VSS balances the load across ports in each chassis independently. For example, if traffic enters the active chassis, the VSS selects an MEC link from the active chassis. This MEC capability ensures that data traffic does not unnecessarily traverse the VSL.

- L2 MEC enables loop free topology, doubles the uplink bandwidth as no links are blocked and provides faster convergence than STP.
- L3 MEC provides reduced neighbor counts, better load−sharing (L2 and L3 for unicast and multicast), reduced VSL link utilization for multicast flows and faster convergence than ECMP.

Refer to Multichassis EtherChannels for more information on MEC.

Recommendations

- Always run **L2 or L3 MEC**.
- Do not use **on** and **off** options with PAgP or LACP or Trunk protocol negotiation.
    - PAgP â€ Run **Desirable−Desirable** with MEC links.
    - LACP â€ Run **Active−Active** with MEC links.
    - Trunk â€ Run **Desirable−Desirable** with MEC links.



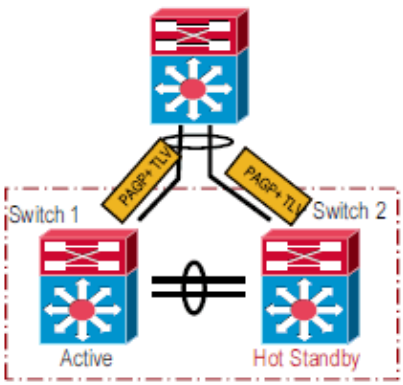
VSL Link Loss and Recovery

If the VSL fails, the standby chassis cannot determine the state of the active chassis. In order to ensure that switchover occurs without delay, the standby chassis assumes the active chassis has failed and initiates switchover to take over the active role.

If the original active chassis is still operational, both chassis are now active. This situation is called a **dual−active** scenario. A dual−active scenario can have adverse affects on network stability, because both chassis use the same IP addresses, SSH keys, and STP bridge ID. The virtual switching system (VSS) must detect a dual−active scenario and take recovery action.

The virtual switching system supports these three methods in order to detect a dual−active scenario:

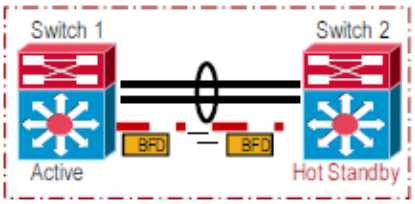
- Enhanced PAgP â€ Uses PAgP messaging over the MEC links in order to communicate between the two chassis through a neighbor switch. Enhanced PAgP is faster than IP BFD, but requires a neighbor switch that supports the PAgP enhancements.



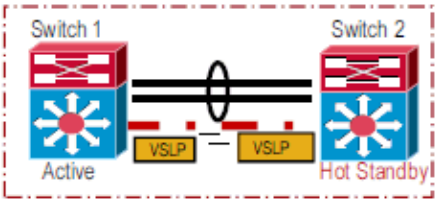
ePAgP Support Table:

Device Series	Minimum Cisco IOS Software
Cisco Catalyst 3750	Cisco IOS 12.2(46)SE
Cisco Catalyst 4500	Cisco IOS 12.2(44)SE
Cisco Catalyst 6500	Cisco IOS 12.2(33)SXH
Cisco Catalyst 6500 VSS	Cisco IOS 12.2(33)SXH1

- IP Bidirectional Forwarding Detection (BFD) â€ Uses BFD messaging over a backup Ethernet connection. IP BFD uses a direct connection between the two chassis and does not require support from a neighbor switch. This method is available in Cisco IOS Software Release 12.2(33)SXH1 and later.



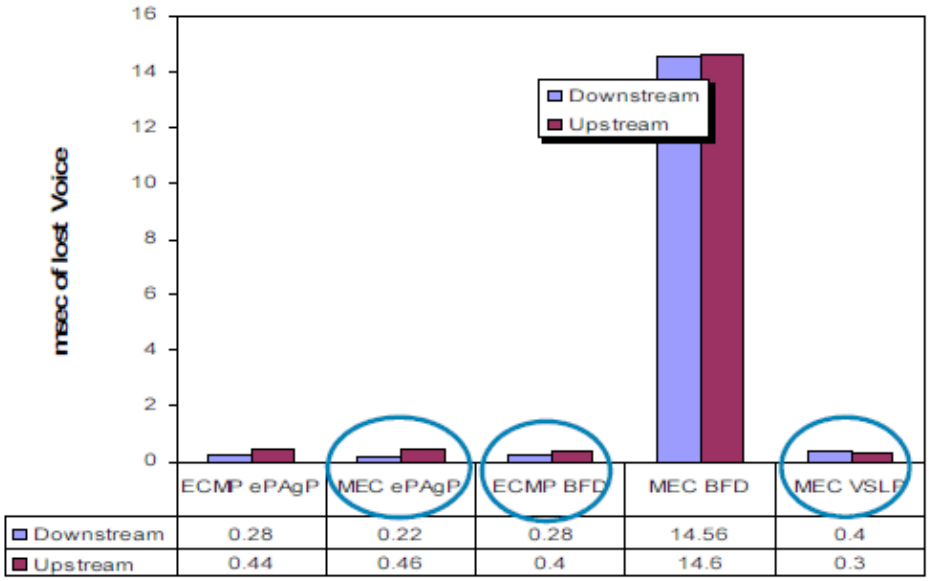
- VSLP dual−active fast−hello â€ Uses special hello messages over a backup Ethernet connection. Dual−active fast−hello is faster than IP BFD and does not require support from a neighbor switch. This method is available only in Cisco IOS Software Release 12.2(33)SXI and later.



You can configure all three detection methods to be active at the same time.

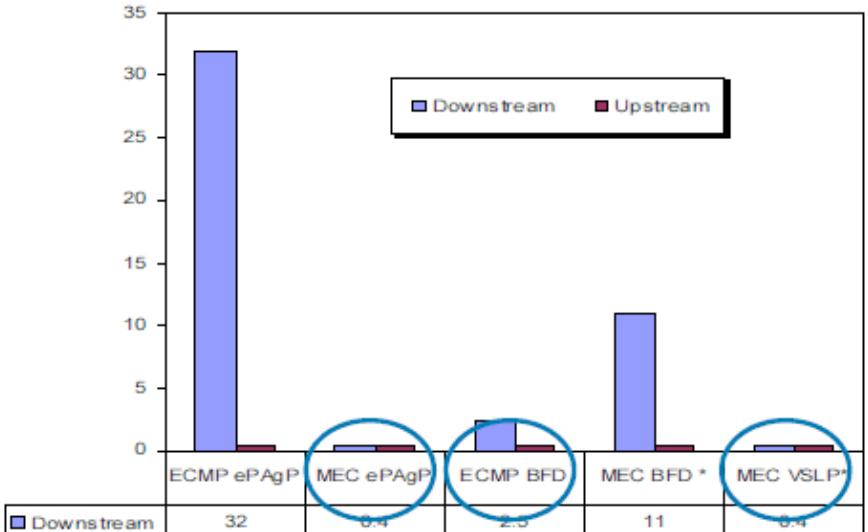
These graphs give information on the convergence of some IP routing protocols with regard to VSS dual active convergence.

EIGRP Convergence with Default timers



	ECMP ePAgP	MEC ePAgP	ECMP BFD	MEC BFD	MEC VSLP
Downstream	0.28	0.22	0.28	14.56	0.4
Upstream	0.44	0.46	0.4	14.6	0.3

OSPF Convergence with Default timers



	ECMP ePAgP	MEC ePAgP	ECMP BFD	MEC BFD *	MEC VSLP*
Downstream	32	0.4	2.5	11	0.4
Upstream	0.4	0.4	0.4	0.42	0.4

Recommendations

- Enable atleast two links in VSL.
- Use **MEC with ePAgP** or **MEC with VSLP Fast Hello** for faster VSL link loss convergence results.
- Enable **ECMP with IP−BFD**.
- Enable ePAgP to core, if the access layer is not ePAgP capable.
- Enable both ePAgP an direct heart beat link based VSLP Fast Hello methods, if possible.
- During VSL loss and recovery process do not perform configuration changes.

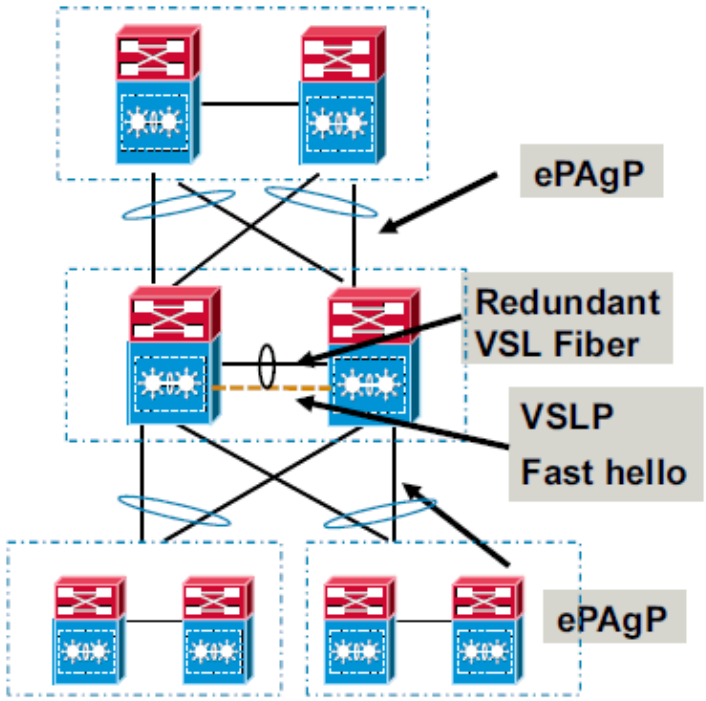
    - ♦ After atleast one VSL member link is restored, if configuration on old ACTIVE chassis is **unchanged**, old ACTIVE **reboots itself** to boot in VSS hot−standby redundancy state.

```
*Apr 6 17:36:33:809: %VSLP−SW1_SP−5−VSL_UP: Ready for Role Resolution with
Switch=2, MAC=0013a.30e1.6800 over Te1/5/5
*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_S
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: VS
change from ACTIVE to HOT_STANDBY.
```

- If the **configuration is changed**, marked *dirty* by the configuration sync process, the switch does not reload automatically.
- Manual reload must be issued on old ACTIVE after configuration is corrected and saved. Even if you just enter configuration mode and exit, it marks the configuration *dirty* and forces a manual intervention.

```
*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 change
Ignored reload request until configuration is

saved
```



Refer to Dual−Active Detection for more information.

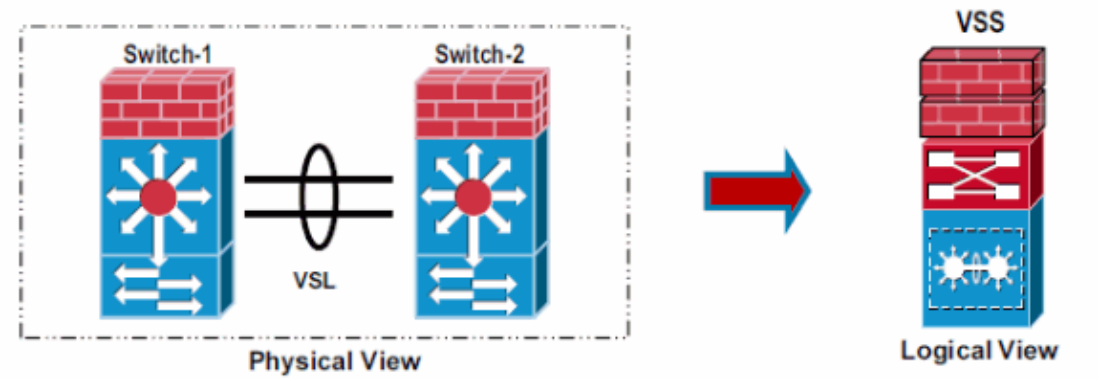
Redundancy with Service Modules

Service module support is a key requirement in order to position the VSS in the enterprise campus and enterprise data center market. The list of service modules that are supported in the Virtual Switch System are:

Service Module	Minimum Cisco IOS Release	Minimum Module Release
Network Analysis Module (NAM−1 and NAM−2)	12.2(33)SXH1	3.6(1a)

(WS−SVC−NAM−1 and WS−SVC−NAM−2)		
Application Control Engine (ACE10 and ACE20) (ACE10−6500−K9 and 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−K9)	12.2(33)SXI	3.2.171.6
Firewall Services Module (FWSM) (WS−SVC−FWM−1−K9)	12.2(33)SXI	4.0.4

Service modules can be placed in either of the physical chassis that comprise a VSS.



Recommendations

- For configuration with more than one service module of a given type, configure one in each physical switch for best availability.
- VSL carries traffic under normal and failover scenarios, VSL bandwidth must be tuned accordingly.

Refer to Integrate Cisco Service Modules with Cisco Catalyst 6500 Virtual Switching System 1440 for more information on service module integration.

Multicast

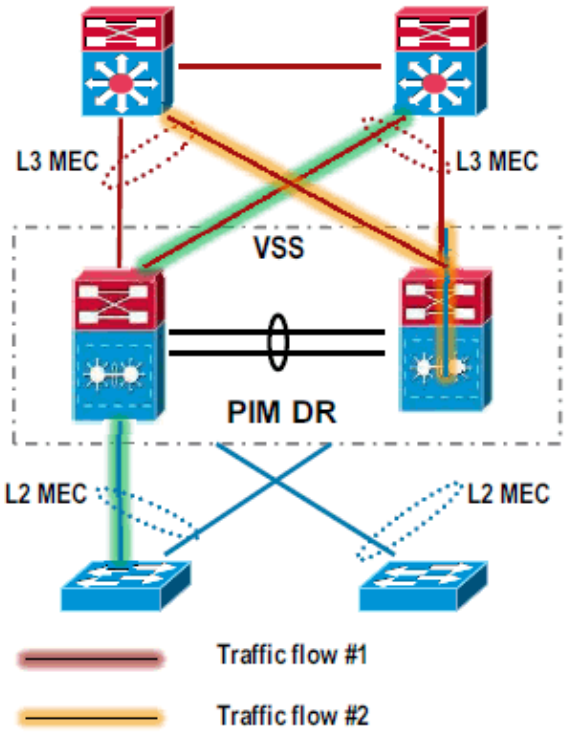
The IPv4 multicast protocols run on the active supervisor engine. Internet Group Management Protocol (IGMP) and Protocol Independent Multicast (PIM) protocol packets received on the standby supervisor engine are transmitted across VSL to the active chassis. The active supervisor engine sends IGMP and PIM protocol packets to the standby supervisor engine in order to maintain Layer 2 information for stateful switchover (SSO).

Refer to IPv4 Multicast for more information.

Recommendations

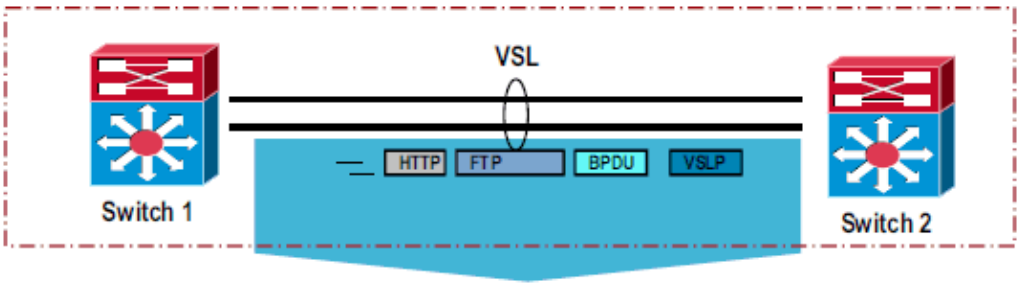
- Connected devices must always be **dual−homed** for optimal replication performance.

- **MEC is recommended** in L3 and L2 environment to provide deterministic convergence.
- MEC eliminates Reverse Path Forwarding (RPF) recalculation during any MEC link failure.
- **Egress replication** with local enhancement for higher multicast replication throughput.
- Egress replication requires DFCs for optimized replication performance.
- Size the VSL to meet traffic requirements.



Qualtiy of Service

VSL QoS Settings



- VSL is a critical internal control and data communication path, and hence QoS settings are pre−configured and configuration changes are not allowed.
- VSL is always configured as **Trust CoS** and ingress queueing is enabled.
- Only CoS based trust and queuing is supported currently. Service policies are not supported on VSL.
- QoS policies must be applied at the input interface of the flows.
- Priority queue is enabled by default. VSS control traffic and BPDUs are given high priority on VSL link.

Recommendations

The only difference between the VSL capable hardware options is the queue configuration. As the current release of software does not allow modification to the default queue settings, any combination of VSL capable

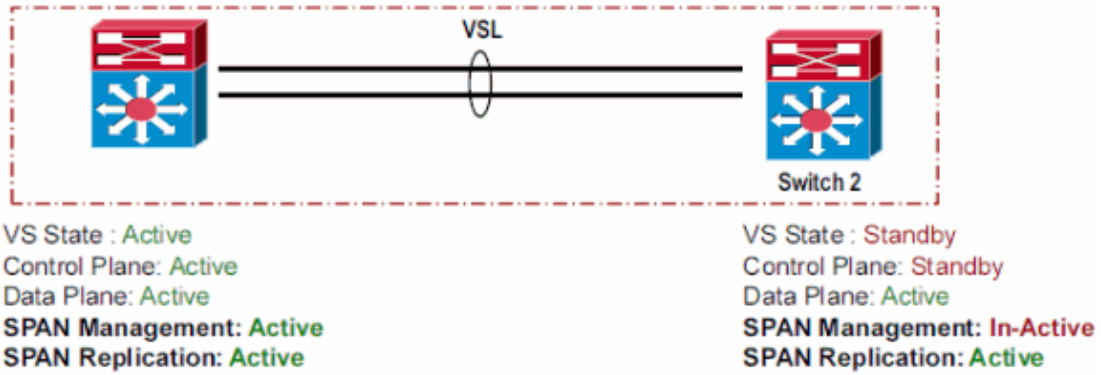
ports provides the same QoS results.

Hardware	Queuing Mode	Trust Mode	Transmit Queue	Receive Queue
VSL on uplinks â€ non−10G only (default)	CoS	CoS	1p3q4t (DWRR/SRR)	8q4t
VSL on uplinks â€ 10G only	CoS	CoS	1p7q4t (DWRR/SRR)	2q4t
VSL across uplinks and line cards	CoS	CoS	1p3q4t [non−10G] (DWRR/SRR) 1p7q4t [10G only] (DWRR/SRR)	2q4t
VSL on line cards	CoS	CoS	1p7q4t (DWRR/SRR)	8q4t

Refer to Configuring VSL QoS for more information.

SPAN

In a Virtual Switch domain, the number of SPAN sessions is limited by what the Virtual Switch active supervisor can provide.



Virtual Switch System supports these SPAN capabilities per Virtual Switch domain.

Attribute	Value
Tx SPAN Sessions	14
Rx / Both SPAN Sessions	2
Total SPAN Sessions	16

Recommendations

- If VSL is configured as local SPAN source, the SPAN destination port(s) must be on the same chassis as the VSL interfaces.

- VSL cannot be configured as SPAN destination.
- VSL cannot be configured as source of RSPAN, ERSPAN, or Tx only local SPAN.
- VSL header is removed by SPAN destination port before packet is transmitted out, and hence cannot be captured in the sniffer traces.
- When the source and destination are both on the same chassis (active or standby), then SPAN traffic does not flow over the VSL link.

  In order to capture traffic from both chassis, there are two options which avoids the flow of SPAN traffic on the VSL:

  - For each source interface on one chassis, the destination interface must be on the same chassis.

    For example, PO20 has gi1/1/1 and gi2/1/1: you need to have one destination for each 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
    ```

    However, this means that you use both the local SPAN sessions. Therefore, you cannot use any other local SPAN session.
  - You can use the destination interface for SPAN as a MEC (recommended).

    The destination port can be a MEC.

Miscellaneous

Recommendations

- Use a minimum of one Supervisor uplink for VSL in order to have faster VSL bring up.
- Configure the **switch accept mode virtual** command after VSS conversion. Without this command, the conversion is not complete.
- Save the backup of the configuration file in both active and hot−standy bootdisk:. This is of much help in supervisor replacement scenarios.
- Use **unique VSS domain−ID** within the same network. Duplicate VSS domain−ID can cause EtherChannel inconsistency.

  Here is an example to change the VSS domain−ID.

  1. Use the **switch virtual domain *domain−id*** command in order to initiate the domain ID change.

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

     Note: Domain ID 50 config takes effect only after the **switch convert mode virtual** exec command is issued.
  2. Use the **switch convert mode virtual** command in order to complete the task.

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

     Note: Virtual Domain ID changes only after you save the config and reload the switch.

- Use the **erase nvram** command instead of the **write erase** command in order to reset the VSS configuration. The **write erase** command erases the startup−config and ROMMon variables. VSS requires *switch−id* ROMMon variable in order to boot in VSS mode.
- Do not use preemption. Refer to Cisco recommends that you do not configure switch preemption for more information.
- Do not use the **shutdown** command for VSL failure simulation, as it creates a configuration mismatch. If you disconnect a cable, it provides more realistic failure scenario.
- Do not change the VSL hashing algorithm while the system is in production. Change of the algorithm requires the port channel to be disabled and re−enabled, with the **shutdown** and **no shutdown** commands. If you shut down a VSL, it causes traffic disruption and can end up in dual−active scenario.
- Configure the MAC aging timer to three times the MAC synchronization timer value.

  The default MAC synchronization and MAC aging timers can cause unknown unicast flooding. VSS can cause traffic to flow asymmetrically such that the source MAC address is only learned on one chassis. The MAC aging timer of 300 seconds and MAC synchronization timer of 160 seconds allows for up to 20 seconds of unknown unicast flooding for any given MAC address in a 320 second interval. In order to resolve this, change the timers such that the aging timer is three times as long as synchronization timer, for example, **mac−address−table aging−time** *480* .

  The sample output of the show mac−address−table aging−time is shown here:

  ```
  switch#sh mac-address-table aging-time
  Vlan Aging Time
  ---- ----------
  Global 480
  no vlan age other than global age configured
  ```
- For VSS to operate with stateful switchover (SSO), both the supervisor engines must run the same software version.
- If you migrate back to a standalone switch from VSS mode through the **switch convert mode stand−alone** command, it completes these tasks:

  - Converts interface name with **switch/slot/port** name to **slot/port**.
  - Removes non−local interfaces from running−config.
  - Removes VSL port channels and ports configuration.
  - Saves Running−config to Startup−config
  - Sets SP rommon variable SWITCH_NUMBER to 0.
  - Reloads the switch.
- Reboot of the switch is required when they are strictly necessary; for example, an IOS upgrade or as a troubleshooting step. A switch being up for more than two years means that it is a stable switch and the configuration is stable as well.

Frequently Asked Questions

Can dual supervisors be used in each chassis with VSS?

Yes. Dual supervisors in each VSS chassis configured for VSS−mode are supported beginning with SXI4 and later.

When removing the preempt commands in Catalyst 6500 Series Switches in VSS Mode, will it reload the switches?

The switch preemption is not recommended. Therefore, removing the commands is a good practice and does not cause a reload. For more information on the Preemption feature on VSS, refer to Switch Preemption.

Related Information

- **Best Practices for Catalyst 6500/6000 Series and Catalyst 4500/4000 Series Switches Running Cisco IOS Software**
- **Configuring Virtual Switching Systems**
- **Cisco IOS Virtual Switch Command Reference**
- **Cisco Catalyst 6500 Virtual Switching System 1440 Product Support**
- **LAN Switches Product Support**
- **LAN Switching Technology Support**
- **Technical Support & Documentation − Cisco Systems**

Contacts & Feedback | Help | Site Map
© 2014 − 2015 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

Updated: Apr 23, 2012 Document ID: 109547
