Cisco Catalyst
Virtual Switching System

BRKCRS-3035

Shawn Wargo
Technical Marketing Engineer
Key Objectives

• Understand the **Key Benefits** of VSS Network Design

• Understand the **VSS Architecture** and how a VSS behaves differently than a Standalone system

• Understand common VSS deployment **Best Practices**
Presentation Legend

- Key Points to Remember
- Reference Materials
- Standalone (Multilayer) Switch
- Virtual Switching System (VSS)
- Layer 2 Link
- Layer 3 Link
Agenda

• Why VSS?
• VSS Conversion and VSS Architecture
• Hardware and Software Requirements
• VSS High Availability and Dual Active
• VSS Redundant Supervisors
• VSL Design Considerations
• VSS Software Upgrades
• Best Practices and Summary
Why VSS?
Catalyst Virtual Switching System

Toplogy Comparisons

Traditional

VSS - Physical

VSS - Logical

Simplify Operations by Eliminating STP, FHRP and Multiple Touch-Points

Double Bandwidth & Reduce Latency with Active-Active Multi-chassis EtherChannel (MEC)

Minimizes Convergence with Sub-second Stateful and Graceful Recovery (SSO/NSF)

Benefits of Virtual Switching
Catalyst Virtual Switching System
Simplified Campus Architecture

**Standalone Challenges**
- Spanning Tree Loops
- First Hop Routing Protocols
- FHRP Tunings
- PIM-DR Priority
- PIM Tunings
- Protocol Dependent Scale
- Unicast Flooding
- Asymmetric Forwarding
- Network/System Redundancy Tradeoff
- Protocol Dependent Recovery
- CAM/ARP Tunings
- OSPF LSA/SPF Tuning
- Control/Mgmt/Forwarding Complexities

**More VSS Benefits**
- Network/System Redundancy
- Scale-independent Recovery
- Hardware Dependent Recovery
- Increase Unicast Capacity
- Increase Multicast Capacity
- Reduced Convergence Times
- Control-plane Simplicity
- Operational Simplicity
- L2-L4 Load Sharing
- Flat L2 Network Topology
Traditional L2 / L3 Campus

Campus Core

Building 1
1000 Ports

Building 2
1000 Ports

Building 3
1000 Ports

Building 4
1000 Ports

Network Design

94 Total Devices of Image & Configuration Management
168 Port-Channels
168 Access Trunks
4032 User Ports

Design Considerations:
STP Loop Prevention
CAM & ARP Tuning
FHRP Tuning / Priority
Routing Protocol Tuning
PIM Tuning / DR priority

94 Separate Configurations of Hostname, VLAN DB, IP/GW, SNMP, NTP, TACACS, VTY, etc.
VSS Campus with Access Stacking

Campus Core

Building 1
1000 Ports

Building 2
1000 Ports

Building 3
1000 Ports

Building 4
1000 Ports

Network Design

25 Total Devices of Image & Configuration Management
24 Port-Channels
24 Access Trunks
4032 User Ports

Design Considerations:
STP Loop Prevention
CAM & ARP Tuning
FHRP Tuning / Priority
Routing Protocol Tuning
PIM Tuning / DR priority

25 Separate Configurations of Hostname, VLAN DB, IP/GW, SNMP, NTP, TACACS, VTY, etc.
# VSS Simplifies Your Configuration

## L2 Spanning Tree Configuration

**Standalone Switch 1**

- Enable 802.1d per VLAN spanning tree enhancements.
- spanning-tree mode rapid-pvst
- spanning-tree loopguard default
- spanning-tree extend system-id
- spanning-tree uplinkfast
- spanning-tree backbonefast

**Standalone Switch 2**

- Enable 802.1d per VLAN spanning tree enhancements.
- spanning-tree mode rapid-pvst
- spanning-tree loopguard default
- spanning-tree extend system-id
- spanning-tree uplinkfast
- spanning-tree backbonefast

**VSS (single configuration)**

- Enable 802.1d per VLAN spanning tree enhancements
- spanning-tree mode rapid-pvst
- spanning-tree extend system-id

## L3 SVI IP Configuration

**Standalone Switch 1**

- Define the Layer 3 SVI for each voice and data VLAN interface Vlan4
- ip address 10.120.4.2 255.255.255.0
- no ip redirects
- no ip unreachables
- Reduce PIM query interval to 250 msec
- ip pim query-interval 250 msec
- ip pim sparse-mode
- load-interval 30
- Define HSRP default gateway with 250/800 msec hello/hold
- standby 1 ip 10.120.4.1
- standby 1 timers msec 250 msec 800
- Set preempt delay large enough to allow network to stabilize
- before HSRP switches back on power on or link recovery
- standby 1 preempt delay minimum 180
- Enable HSRP authentication
- standby 1 authentication cisco123

**Standalone Switch 2**

- Define the Layer 3 SVI for each voice and data VLAN interface Vlan2
- ip address 10.120.2.1 255.255.255.0
- no ip redirects
- no ip unreachables
- ip pim sparse-mode
- load-interval 30

**VSS (single configuration)**

- Define the Layer 3 SVI for each voice and data VLAN interface Vlan4
- ip address 10.120.4.3 255.255.255.0
- no ip redirects
- no ip unreachables
- ip pim sparse-mode
- load-interval 30
- Define HSRP default gateway with 250/800 msec hello/hold
- standby 1 ip 10.120.4.1
- standby 1 timers msec 250 msec 800
- Set preempt delay large enough to allow network to stabilize
- before HSRP switches back on power on or link recovery
- standby 1 preempt delay minimum 180
- Enable HSRP authentication
- standby 1 authentication cisco123
VSS Conversion Process
Migrate from Standalone to VSS
One-time Conversion Process Needed

1. Start with two Standalone systems

2. Apply one-time VSS Conversion commands and reload

3. Both systems are now a Single VSS
Conversion to VSS
Conversion Example

For the purposes of explanation – let’s assume the following setup…

Switch 1

Virtual Switch Link

Switch 2

Port-Channel 1

Port-Channel 2

Virtual Domain 100
Conversion to VSS
Conversion Example

**CONFIGURE THE VSS DOMAIN, SWITCH ID & VSL PORT-CHANNEL**

**Switch 1**

Router(config)#hostname VSS
VSS(config)#switch virtual domain 100

Domain ID 10 config will take effect only after the exec command 'switch convert mode virtual' is issued

VSS(config-vs-domain)#switch 1
VSS(config-vs-domain)#exit

VSS(config)#interface port-channel 1
VSS(config-if)#switch virtual link 1
VSS(config-if)#no shutdown

VSS(config-if)#interface range TenGig 5/4 - 5
VSS(config-if-range)#channel-group 1 mode on
VSS(config-if-range)#no shutdown

**Switch 2**

Router(config)#hostname VSS
VSS(config)#switch virtual domain 100

Domain ID 10 config will take effect only after the exec command 'switch convert mode virtual' is issued

VSS(config-vs-domain)#switch 2
VSS(config-vs-domain)#exit

VSS(config)#interface port-channel 2
VSS(config-if)#switch virtual link 2
VSS(config-if)#no shutdown

VSS(config-if)#interface range TenGig 5/4 - 5
VSS(config-if-range)#channel-group 2 mode on
VSS(config-if-range)#no shutdown
Conversion to VSS
Conversion Example

CONVERT FROM STAND-ALONE TO VIRTUAL SWITCHING

Switch 1

VSS# switch convert mode virtual

This command will convert all interface names to naming convention "interface-type switch-number/slot/port", save the running config to startup-config and reload the switch. Do you want to proceed? [yes/no]: yes
Converting interface names
Building configuration...
[OK]
Saving converted configuration to bootflash: ... Destination filename [startup-config.converted_vs-20141031-150039]?

AT THIS POINT SWITCH 1 WILL REBOOT...

Switch 2

VSS# switch convert mode virtual

This command will convert all interface names to naming convention "interface-type switch-number/slot/port", save the running config to startup-config and reload the switch. Do you want to proceed? [yes/no]: yes
Converting interface names
Building configuration...
[OK]
Saving converted configuration to bootflash: ... Destination filename [startup-config.converted_vs-20141031-150039]?

AT THIS POINT SWITCH 2 WILL REBOOT...
Conversion to VSS
Conversion Example

**BOTH CHASSIS REBOOT AND NEGOTIATE VSS ROLES...**

**Switch 1**

---

System detected Virtual Switch configuration...

Interface TenGigabitEthernet 1/5/4 is member of PortChannel 1
Interface TenGigabitEthernet 1/5/5 is member of PortChannel 1

---

00:00:26: %PFREDUN-6-ACTIVE: Initializing as ACTIVE processor for this switch
Initializing as **Virtual Switch ACTIVE** processor

---

00:01:19: %VSLP-5-RRP_ROLE_RESOLVED: Role resolved as ACTIVE by VSLP

00:01:19: %VSL-5-VSL_CNTRL_LINK: New VSL Control Link 5/4

**Switch 2**

---

System detected Virtual Switch configuration...

Interface TenGigabitEthernet 2/5/4 is member of PortChannel 2
Interface TenGigabitEthernet 2/5/5 is member of PortChannel 2

---

00:00:26: %PFREDUN-6-ACTIVE: Initializing as ACTIVE processor for this switch
Initializing as **Virtual Switch STANDBY** processor

---

00:01:02: %VSLP-5-RRP_ROLE_RESOLVED: Role resolved as STANDBY by VSLP

00:01:02: %VSL-5-VSL_CNTRL_LINK: New VSL Control Link 5/4
Conversion to VSS
Conversion Example – Optional (Occurs Automatically as of 12.2(33)SXI3)

ACCEPT THE VSS CONVERSION...

SWITCH CONSOLE OUTPUT
<VSS>
VSS> switch accept mode virtual
interface Port-channel12
  switch virtual link 2
  no shutdown
interface TenGigabitEthernet2/5/4
  channel-group 2 mode on
  no shutdown
interface TenGigabitEthernet2/5/5
  channel-group 2 mode on
  no shutdown

This command will populate the above VSL configuration from the
standby switch into the running configuration.
The startup configuration will also be updated with the new merged
configuration if merging is successful.
Do you want to proceed? [yes/no]: yes
Merging the standby VSL configuration...

Building configuration...

00:11:33: %PFINIT-5-CONFIG_SYNC: Sync'ing the startup
configuration to the standby Router. [OK]
Conversion to VSS

Conversion Example

**BOTH SWITCHES ARE NOW CONVERTED TO VSS!**

**Switch 1**

```console
VSS# show switch virtual
Switch mode : Virtual Switch
Virtual switch domain number : 100
Local switch number : 1
Local switch operational role: Virtual Switch Active
Peer switch number : 2
Peer switch operational role : Virtual Switch Standby
VSS#
```

**Switch 2**

```console
VSS-sdyb>enable
Standby console disabled
VSS-sdyb>
```

**VSS Domain = 100**

**Switch 1 = VSS Active**

**Switch 2 = VSS Hot Standby**

**NOTE:** The standby console is now disabled for normal CLI input
Conversion to VSS

Controlling the System from a Single CLI

Switch 1

VSS# show module switch 1
Switch Number: 1 Role: Virtual Switch Active

<table>
<thead>
<tr>
<th>Mod Ports</th>
<th>Card Type</th>
<th>Model</th>
<th>Serial No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>20 DCEF74 4 port 40GE / 16 port 10GE</td>
<td>WS-X6804-40G</td>
<td>SAL17470E8G</td>
<td></td>
</tr>
<tr>
<td>5 Supervisor Engine 2T 10GE w/ CTS (Acti)</td>
<td>VS-SUP2T-10G</td>
<td>SAL15338E8G</td>
<td></td>
</tr>
<tr>
<td>5 Supervisor Engine 2T 10GE w/ CTS</td>
<td>VS-SUP2T-10G</td>
<td>SAL16351R99</td>
<td></td>
</tr>
<tr>
<td>10 DCEF74 8 port 40GE / 32 port 10GE</td>
<td>C6800-32P10G-XL</td>
<td>SAL18443C31</td>
<td></td>
</tr>
<tr>
<td>10 DCEF74 8 port 40GE / 8 port 10GE</td>
<td>C6800-8P10G-XL</td>
<td>SAL18342C72</td>
<td></td>
</tr>
<tr>
<td>48 CEFP72 48 port 1000m SFP</td>
<td>WS-X6848-SFP</td>
<td>SAL1815Q8SC</td>
<td></td>
</tr>
</tbody>
</table>

Mod MAC addresses

<table>
<thead>
<tr>
<th>Device</th>
<th>Hw</th>
<th>Fw</th>
<th>Sw</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>2c54.2dc3.e6c5 to 2c54.2dc3.e6cc</td>
<td>1.5 12.2(50r)SYS</td>
<td>15.2(1)SY</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>e02f.6d6a.8374 to e02f.6d6a.8387</td>
<td>1.0 12.2(50r)SYL</td>
<td>15.2(1)SY</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>4c71.fe7c.d7ef to c471.fe7c.d7f6</td>
<td>1.3 12.2(50r)SYS</td>
<td>15.2(1)SY</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>1005.caea.d5ad to 1005.caea.d59a</td>
<td>1.0 15.1(58r)SYS</td>
<td>15.2(1)SY</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>7 b838.61d8.6fb8 to b838.61d8.6fe7</td>
<td>3.0 12.2(18r)S1</td>
<td>15.2(1)SY</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>2c54.2dc3.e6c5 to 2c54.2dc3.e6cc</td>
<td>1.5 12.2(50r)SYS</td>
<td>15.2(1)SY</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>e02f.6d6a.8374 to e02f.6d6a.8387</td>
<td>1.0 12.2(50r)SYL</td>
<td>15.2(1)SY</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>4c71.fe7c.d7ef to c471.fe7c.d7f6</td>
<td>1.3 12.2(50r)SYS</td>
<td>15.2(1)SY</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>1005.caea.d5ad to 1005.caea.d59a</td>
<td>1.0 15.1(58r)SYS</td>
<td>15.2(1)SY</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>7 b838.61d8.6fb8 to b838.61d8.6fe7</td>
<td>3.0 12.2(18r)S1</td>
<td>15.2(1)SY</td>
<td>Ok</td>
<td></td>
</tr>
</tbody>
</table>

Mod Sub-Module

<table>
<thead>
<tr>
<th>Sub-Module</th>
<th>Model</th>
<th>Serial</th>
<th>Hw</th>
<th>Sw</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed Forwarding Card WS-F6K-DFC4-E</td>
<td>WS-F6K-DFC4-E</td>
<td>SAL1803KVP7</td>
<td>1.0</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>Policy Feature Card 4</td>
<td>VS-F6K-PPC4</td>
<td>SAL1535NUL1</td>
<td>1.0</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>Policy Feature Card 4</td>
<td>VS-F6K-PPC4</td>
<td>SAL1535NUL1</td>
<td>1.0</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>CPU Daughterboard</td>
<td>VS-F6K-MSCPS</td>
<td>SAL1534NA61</td>
<td>1.1</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>Policy Feature Card 4</td>
<td>VS-F6K-PPC4</td>
<td>SAL16351R8J</td>
<td>1.2</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>CPU Daughterboard</td>
<td>VS-F6K-MSCPS</td>
<td>SAL1634LAPS</td>
<td>1.4</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>Distributed Forwarding Card C6800-DFC-XL</td>
<td>SAL18443C21</td>
<td>1.0</td>
<td>Ok</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distributed Forwarding Card C6800-DFC-XL</td>
<td>SAL18443C21</td>
<td>1.0</td>
<td>Ok</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distributed Forwarding Card C6800-DFC-XL</td>
<td>SAL18443C21</td>
<td>1.0</td>
<td>Ok</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distributed Forwarding Card C6800-DFC-XL</td>
<td>SAL18443C21</td>
<td>1.0</td>
<td>Ok</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distributed Forwarding Card WS-F6K-DFC4-A</td>
<td>WS-F6K-DFC4-A</td>
<td>SAL1815Q8SC</td>
<td>2.0</td>
<td>Ok</td>
<td></td>
</tr>
</tbody>
</table>

Mod Online Diag Status

<table>
<thead>
<tr>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pass</td>
</tr>
<tr>
<td>Pass</td>
</tr>
<tr>
<td>Pass</td>
</tr>
<tr>
<td>Pass</td>
</tr>
<tr>
<td>Pass</td>
</tr>
<tr>
<td>Pass</td>
</tr>
<tr>
<td>Pass</td>
</tr>
<tr>
<td>VSS#</td>
</tr>
</tbody>
</table>

Switch 2

VSS# show module switch 2
Switch Number: 2 Role: Virtual Switch Standby

<table>
<thead>
<tr>
<th>Mod Ports</th>
<th>Card Type</th>
<th>Model</th>
<th>Serial No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>20 DCEF74 4 port 40GE / 16 port 10GE</td>
<td>WS-X6804-40G</td>
<td>SAL17455F57</td>
<td></td>
</tr>
<tr>
<td>5 Supervisor Engine 2T 10GE w/ CTS (Hot)</td>
<td>VS-SUP2T-10G</td>
<td>SAL17370C8</td>
<td></td>
</tr>
<tr>
<td>5 Supervisor Engine 2T 10GE w/ CTS</td>
<td>VS-SUP2T-10G</td>
<td>SAL16351R99</td>
<td></td>
</tr>
<tr>
<td>40 DCEF74 8 port 40GE / 32 port 10GE</td>
<td>C6800-32P10G-XL</td>
<td>SAL18443C28</td>
<td></td>
</tr>
<tr>
<td>20 DCEF74 8 port 40GE / 16 port 10GE</td>
<td>C6800-16P10G-XL</td>
<td>SAL18442A28</td>
<td></td>
</tr>
<tr>
<td>48 CEFP72 48 port 1000m SFP</td>
<td>WS-X6848-SFP</td>
<td>SAL1811N82E</td>
<td></td>
</tr>
</tbody>
</table>

Mod MAC addresses

<table>
<thead>
<tr>
<th>Device</th>
<th>Hw</th>
<th>Fw</th>
<th>Sw</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>02f.6d6a.8374 to 02f.6d6a.8387</td>
<td>1.0 12.2(50r)SYS</td>
<td>15.2(1)SY</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>02f.6d6a.8374 to 02f.6d6a.8387</td>
<td>1.0 12.2(50r)SYS</td>
<td>15.2(1)SY</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>02f.6d6a.8374 to 02f.6d6a.8387</td>
<td>1.0 12.2(50r)SYS</td>
<td>15.2(1)SY</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>02f.6d6a.8374 to 02f.6d6a.8387</td>
<td>1.0 12.2(50r)SYS</td>
<td>15.2(1)SY</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>02f.6d6a.8374 to 02f.6d6a.8387</td>
<td>1.0 12.2(50r)SYS</td>
<td>15.2(1)SY</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>02f.6d6a.8374 to 02f.6d6a.8387</td>
<td>1.0 12.2(50r)SYS</td>
<td>15.2(1)SY</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>02f.6d6a.8374 to 02f.6d6a.8387</td>
<td>1.0 12.2(50r)SYS</td>
<td>15.2(1)SY</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>02f.6d6a.8374 to 02f.6d6a.8387</td>
<td>1.0 12.2(50r)SYS</td>
<td>15.2(1)SY</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>02f.6d6a.8374 to 02f.6d6a.8387</td>
<td>1.0 12.2(50r)SYS</td>
<td>15.2(1)SY</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>02f.6d6a.8374 to 02f.6d6a.8387</td>
<td>1.0 12.2(50r)SYS</td>
<td>15.2(1)SY</td>
<td>Ok</td>
<td></td>
</tr>
<tr>
<td>02f.6d6a.8374 to 02f.6d6a.8387</td>
<td>1.0 12.2(50r)SYS</td>
<td>15.2(1)SY</td>
<td>Ok</td>
<td></td>
</tr>
</tbody>
</table>

Mod Sub-Module

<table>
<thead>
<tr>
<th>Sub-Module</th>
<th>Model</th>
<th>Serial</th>
<th>Hw</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed Forwarding Card WS-F6K-DFC4-E</td>
<td>WS-F6K-DFC4-E</td>
<td>SAL1800MDW</td>
<td>1.0</td>
<td>Ok</td>
</tr>
<tr>
<td>Policy Feature Card 4</td>
<td>VS-F6K-PPC4</td>
<td>SAL1731CME</td>
<td>2.1</td>
<td>Ok</td>
</tr>
<tr>
<td>Policy Feature Card 4</td>
<td>VS-F6K-PPC4</td>
<td>SAL1731CME</td>
<td>2.1</td>
<td>Ok</td>
</tr>
<tr>
<td>Policy Feature Card 4</td>
<td>VS-F6K-PPC4</td>
<td>SAL1731CME</td>
<td>2.1</td>
<td>Ok</td>
</tr>
<tr>
<td>Policy Feature Card 4</td>
<td>VS-F6K-PPC4</td>
<td>SAL1731CME</td>
<td>2.1</td>
<td>Ok</td>
</tr>
<tr>
<td>Policy Feature Card 4</td>
<td>VS-F6K-PPC4</td>
<td>SAL1731CME</td>
<td>2.1</td>
<td>Ok</td>
</tr>
<tr>
<td>Policy Feature Card 4</td>
<td>VS-F6K-PPC4</td>
<td>SAL1731CME</td>
<td>2.1</td>
<td>Ok</td>
</tr>
<tr>
<td>Policy Feature Card 4</td>
<td>VS-F6K-PPC4</td>
<td>SAL1731CME</td>
<td>2.1</td>
<td>Ok</td>
</tr>
<tr>
<td>Policy Feature Card 4</td>
<td>VS-F6K-PPC4</td>
<td>SAL1731CME</td>
<td>2.1</td>
<td>Ok</td>
</tr>
<tr>
<td>Policy Feature Card 4</td>
<td>VS-F6K-PPC4</td>
<td>SAL1731CME</td>
<td>2.1</td>
<td>Ok</td>
</tr>
</tbody>
</table>

Mod Online Diag Status

<table>
<thead>
<tr>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pass</td>
</tr>
<tr>
<td>Pass</td>
</tr>
<tr>
<td>Pass</td>
</tr>
<tr>
<td>Pass</td>
</tr>
<tr>
<td>Pass</td>
</tr>
<tr>
<td>Pass</td>
</tr>
<tr>
<td>VSS#</td>
</tr>
</tbody>
</table>

Cisco Public
Conversion to VSS
How to configure VSS Ports?

VSS ports use a 3-part notation: Interface <Type> <Switch Number> / <Module Number> / <Port Number>

Layer 2 Configuration

! interface GigabitEthernet1/3/3
  switchport
  switchport mode access
  switchport access vlan 205
  logging event link-status
  load-interval 30
end
!

Layer 3 Configuration

! interface TenGigabitEthernet2/1/1
  ip address 68.7.1.2 255.255.255.0
  logging event link-status
  load-interval 30
  ipv6 address 2015:68:7:1::2/96
  ipv6 ospf 1 area 68
! 

NOTE: The default mode is “routed”. Issue “switchport” to enable L3 CLI
VSS Architecture
VSS Architecture

Key Concepts

Virtual Switch Domain

Virtual Switch 1

- Active Control Plane
- Active Data Plane

Virtual Switch 2

- Hot Standby Control Plane
- Active Data Plane

Virtual Switch Link

Special 10GE Port-Channel joins two Catalyst Switches allowing them to operate as a single logical device

Catalyst Switch that operates as the Active Control Plane for the VSS

Catalyst Switch that operates as the Hot Standby Control Plane for the VSS

Defines 2 Catalyst Switches that are participating together as a Virtual Switching System (VSS)
The **Virtual Switch Link (VSL)** joins two physical chassis together. The VSL provides a control-plane interface to keep both the chassis in sync. The VSS “control-plane” uses the VSL for CPU to CPU communications (programming, statistics, etc.) while the “data-plane” uses the VSL to extend the internal chassis fabric to the remote chassis.

All traffic traversing the VSL is encapsulated into a 32 Byte **Virtual Switch Header (VSH)**. The VSH contains the Source and Destination Port Index, Class of Service (CoS), VLAN ID, other important information from the Layer 2 and Layer 3 headers.
VSS Architecture
Building the Virtual Switch Link

Just as other Port Channels, one link is selected as a “Control Link”, for the purpose of transmitting BPDUs and Port Channel status.

The VSL Port-Channel can consist of up to 8 x 10GE (or 4 x 40GE) member ports.

---

**interface Port-channel1**
no switchport
no ip address
switch virtual link 1
mls qos trust cos
no mls qos channel-consistency

**interface Port-channel2**
no switchport
no ip address
switch virtual link 2
mls qos trust cos
no mls qos channel-consistency
VSS Architecture

VSS Start Up

1. Pre-parse the startup-config file, to bring up VSL modules and interfaces

2. **Link Management Protocol (LMP)** is used to track and reject Unidirectional Links, Exchange Chassis ID, and other information between the 2 switches

3. **Role Resolution Protocol (RRP)** is used to determine compatible Hardware and Software to form the VSL, and to determine which switch becomes Active or Hot Standby
**VSS Architecture**

**show switch virtual link detail**

```plaintext
VSS01#show switch virtual link detail
VSL Status : UP
VSL Uptime : 21 hours, 45 minutes
VSL SCP Ping : Pass
VSL ICC Ping : Pass
VSL Control Link : Te1/2/4
VSL Encryption : Configured Mode - Off, Operational Mode - Off

LMP summary
<table>
<thead>
<tr>
<th>Link info:</th>
<th>Configured: 4</th>
<th>Operational: 4</th>
<th>Timer(s) running</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer Peer</td>
<td>Peer Flag State</td>
<td>Flag MAC</td>
<td>Switch Interface (Time remaining)</td>
</tr>
<tr>
<td>Interface</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Te1/1/4    | vfsp operational | vfsp 0013.5f1c.0680 2 | Te2/1/4 | T4 (152ms)  
|           |                |               |                  |     T5 (59.95s)  |
| Te1/1/5    | vfsp operational | vfsp 0013.5f1c.0680 2 | Te2/2/5 | T4 (152ms)  
|           |                |               |                  |     T5 (59.95s)  |
| Te1/2/4    | vfsp operational | vfsp 0013.5f1c.0680 2 | Te2/2/4 | T4 (152ms)  
|           |                |               |                  |     T5 (59.95s)  |
| Te1/2/5    | vfsp operational | vfsp 0013.5f1c.0680 2 | Te2/1/5 | T4 (152ms)  
|           |                |               |                  |     T5 (59.98s)  |

Flags: v - Valid flag set  
f - Bi-directional flag set  
s - Negotiation flag set  
p - Peer detected flag set

Timers: T4 - Hello Tx Timer  
        T5 - Hello Rx Timer
```
A new VSLP ping mechanism has been implemented in VSS mode to allow the user to objectively verify the health of the VSL itself...

VSLP Ping operates on a per-physical interface basis and parameters such as COUNT, DESTINATION, SIZE, TIMEOUT may also be specified...

VSS# ping vslp output interface tenGigabitEthernet 1/5/4

Type escape sequence to abort.
Sending 5, 100-byte VSLP ping to peer-sup via output port 1/5/4, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 12/12/16 ms
VSS Architecture

VSL Initialization Summary

1. Initialization
   - Rommon & Parse VS Config
   - Bring Up VSL Cards & Ports
   - VSLP – Run LMP
   - VSLP – Run RRP
   - Inter-Chassis SSO Sync
   - Continue IOS Bootup

2. Initialization
   - Rommon & Parse VS Config
   - Bring Up VSL Cards & Ports
   - VSLP – Run LMP
   - VSLP – Run RRP
   - Inter-Chassis SSO Sync
   - Continue IOS Bootup

Switch 1

Virtual Switch Link

Switch 2

Port-Channel 1

Port-Channel 2
After the roles have been resolved through **RRP**, a Configuration Consistency Check is performed across the VSL switches to ensure proper VSL operation. The following items are checked for consistency:

- Switch Virtual Domain ID
- Switch Virtual Switch ID
- Switch Priority
- Switch Preempt
- VSL Port Channel Link ID
- VSL Port state, Interfaces...
- Power Redundancy mode
- Power Enable on VSL cards

If the VSS configurations do NOT match, the Standby Supervisor will revert to RPR mode, disabling all non-VSL interfaces...
VSS forwarding information is exchanged between Supervisors with Stateful Switch-Over (SSO)

One Supervisor is elected **ACTIVE** with the other in **HOT STANDBY** mode

- Active / Standby Supervisors run in SSO Mode – Boot variable, Running-Config, Protocol State, and Line Card Status are fully synchronized

- **Active Supervisor** manages all **Control-Plane** Functions - including Infrastructure Management (Online Insertion Removal, Port Manager, Feature Manager, etc.) and all L2/L3+ Protocols (STP, IP Routing, EtherChannel, SNMP, Telnet, etc.)
C6500 Supervisor VSL In-band Connection

Reduces VSS Boot Time

Allows for the VSL ports to be brought online very early in the boot process

Applicable to both Sup720-10G and Sup2T
VSS Architecture

show switch virtual

```
VSS# show switch virtual ?

dual-active       Virtual switch dual-active information
link              Virtual switch link information
redundancy        vs pseudo-standby status
role              Virtual switch role information
slot-map          virtual slot map table
troubleshooting   vs vsl troubleshooting output
```

**NOTE:** The “troubleshooting” option provides a single command to gather all VSS related troubleshooting data (simplifies gathering data for TAC) 😊
VSS Architecture

show switch virtual role

VSS# show switch virtual role
RRP information for Instance 2

<table>
<thead>
<tr>
<th>Valid</th>
<th>Flags</th>
<th>Peer Count</th>
<th>Preferred Peer</th>
<th>Reserved Peer</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRUE</td>
<td>V</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Switch Number</th>
<th>Switch Status</th>
<th>Preempt Priority</th>
<th>Role</th>
<th>Local SID</th>
<th>Remote SID</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOCAL 2</td>
<td>UP</td>
<td>FALSE(N )</td>
<td>100(100)</td>
<td>ACTIVE 0</td>
<td>0</td>
</tr>
<tr>
<td>REMOTE 1</td>
<td>UP</td>
<td>FALSE(N )</td>
<td>100(100)</td>
<td>STANDBY 928</td>
<td>5923</td>
</tr>
</tbody>
</table>

Peer 0 represents the local switch
Flags : V - Valid
In dual-active recovery mode: No
VSS#
VSS Architecture

show switch virtual role redundancy

VSS# show switch virtual role redundancy
   My Switch Id = 2
   Peer Switch Id = 1
   Last switchover reason = active unit removed
   Configured Redundancy Mode = sso
   Operating Redundancy Mode = sso

Switch 2 Slot 8 Processor Information :
-----------------------------------------------
   Current Software state = ACTIVE
   Uptime in current state = 1 day, 1 hour, 39 minutes
   Image Version = Cisco IOS Software, s2t54 Software (s2t54-ADVENTERPRISEK9_DBG-M), Version 12.2(49)SY131.71, INTERIM SOFTWARE
   Synced to CARSON_BASE_FOR_V122_50_SY_THROTTLE_121610_101313, Weekly Branch: v122_50_sy_throttle
   BOOT = bootdisk:s2t54-adventerprisek9_dbg-mz.SSA.122-49.SY131.71_110421,1;
      CONFIG_FILE =
      BOOTLDR =
   Configuration register = 0x2102
   Fabric State = ACTIVE
   Control Plane State = ACTIVE

Switch 1 Slot 6 Processor Information :
-----------------------------------------------
   Current Software state = STANDBY HOT (switchover target)
   Uptime in current state = 1 day, 1 hour, 35 minutes
   Image Version = Cisco IOS Software, s2t54 Software (s2t54-ADVENTERPRISEK9_DBG-M), Version 12.2(49)SY131.71, INTERIM SOFTWARE
   Synced to CARSON_BASE_FOR_V122_50_SY_THROTTLE_121610_101313, Weekly Branch: v122_50_sy_throttle
   BOOT = bootdisk:s2t54-adventerprisek9_dbg-mz.SSA.122-49.SY131.71_110421,1;
      CONFIG_FILE =
      BOOTLDR =
   Configuration register = 0x2102
   Fabric State = ACTIVE
   Control Plane State = STANDBY
VSS Architecture
Active - Active Data Planes

Both data forwarding planes are **ACTIVE**

Standby Supervisor and all Line Cards with DFC’s are actively forwarding…

```plaintext
VSS# show switch virtual redundancy
My Switch Id = 1
Peer Switch Id = 2

Switch 1 Slot 5 Processor Information :
-----------------------------------------------
Current Software state = ACTIVE

Fabric State = ACTIVE
Control Plane State = ACTIVE

Switch 2 Slot 5 Processor Information :
-----------------------------------------------
Current Software state = STANDBY HOT (switchover target)

Fabric State = ACTIVE
Control Plane State = STANDBY
```
VSS Architecture

Multi-chassis EtherChannel (MEC)

Prior to VSS, an EtherChannel had to reside within the same physical switch: Single Module (EC) or Cross Module (DEC)

In a VSS environment, the two physical chassis form a single logical entity, which allows a new DEC, known as Multi-chassis EtherChannels (MEC)

Stand Alone

Distributed EtherChannel on Single Chassis

Multi-chassis EtherChannel across 2 VSS Chassis

LACP, PAGP and ON EtherChannel modes are supported
Etherchannel Traffic Load Balancing
VSS Architecture
Load-Balancing for MEC & ECMP

The PFC / DFC hash logic for MEC and ECMP load-balancing, which determines which physical port to use, is skewed to always favor LOCAL links!

This avoids overloading the Virtual Switch Link (VSL) with unnecessary traffic loads…

<table>
<thead>
<tr>
<th>Logical Interface</th>
<th>Physical Interface</th>
<th>Result Bundle Hash (RBH) Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PO 10</td>
<td>T 1/1/1</td>
<td>0,1,2,3,4,5,6,7</td>
</tr>
<tr>
<td>PO 10</td>
<td>T 2/1/1</td>
<td>0,1,2,3,4,5,6,7</td>
</tr>
</tbody>
</table>

Blue Traffic destined for the Neighbor will result in **Link 1** of the MEC bundle being chosen.

Orange Traffic destined for the Neighbor will result in **Link 2** of the MEC bundle being chosen.
Etherchannel Concepts
Etherchannel Hash Distribution

The default hashing algorithm will redistribute all the Result Bit Hash values across the available ports when there is a change. This affects all traffic traversing the Etherchannel.

**RBH (for MEC)**

2 Link Bundle Example

<table>
<thead>
<tr>
<th>Link 1</th>
<th>Link 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>7</td>
</tr>
</tbody>
</table>

**RBH (for MEC)**

3 Link Bundle Example

<table>
<thead>
<tr>
<th>Link 1</th>
<th>Link 2</th>
<th>Link 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>
EtherChannel Concepts
EtherChannel Hash Distribution Adaptive

Adaptive Hash Distribution Enhancement allows for the addition or removal of links in a bundle without affecting all of the traffic in an Etherchannel. Note in the below example, only Flow 7 and 8 are affected by the addition of an extra link to the Channel…

<table>
<thead>
<tr>
<th>RBH (for MEC)</th>
<th>Link 1</th>
<th>Link 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link 1</td>
<td>Flow 1</td>
<td>Flow 2</td>
</tr>
<tr>
<td>Link 2</td>
<td>Flow 3</td>
<td>Flow 4</td>
</tr>
<tr>
<td>Link 3</td>
<td>Flow 5</td>
<td>Flow 6</td>
</tr>
<tr>
<td>Link 4</td>
<td>Flow 7</td>
<td>Flow 8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RBH (for MEC)</th>
<th>Link 1</th>
<th>Link 2</th>
<th>Link 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link 1</td>
<td>Flow 1</td>
<td>Flow 2</td>
<td>Flow 7</td>
</tr>
<tr>
<td>Link 2</td>
<td>Flow 3</td>
<td>Flow 4</td>
<td>Flow 8</td>
</tr>
<tr>
<td>Link 3</td>
<td>Flow 5</td>
<td>Flow 6</td>
<td></td>
</tr>
</tbody>
</table>

vss# conf t
Enter configuration commands, one per line. End with CNTL/Z.
vss(config)#port-channel hash-distribution adaptive
vss(config)# ^Z
vss#

Default for Catalyst 6500 VSS beginning in 12.2(33)SXH1
VSS Architecture

How to check an MEC

```
VSS# show etherchannel 1 port-channel
Port-channels in the group:
-----------------------------
Port-channel: Po1
------------
Age of the Port-channel = 2d:21h:10m:59s
Logical slot/port = 46/1 Number of ports = 2
GC = 0x00000000 HotStandBy port = null
Passive port list = Te1/6/4 Te1/6/5
Port state = Port-channel L3-Ag Ag-Inuse
Protocol = -
Fast-switchover = disabled
Load share deferral = disabled

Ports in the Port-channel:

<table>
<thead>
<tr>
<th>Index</th>
<th>Load</th>
<th>Port</th>
<th>EC state</th>
<th>No of bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>95</td>
<td>Te1/6/4</td>
<td>On</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>6A</td>
<td>Te1/6/5</td>
<td>On</td>
<td>4</td>
</tr>
</tbody>
</table>

Time since last port bundled: 2d:21h:08m:34s  Te1/6/5

Last applied Hash Distribution Algorithm: Adaptive

Load values assigned to each port

Hash distribution method
```
VSS Architecture

EtherChannel Hash

An IOS command can be used to determine which physical link in the EtherChannel will be used
It can use various hash inputs to yield an 8(bucket RBH value that will correspond to one of the ports...

VSS# show etherchannel load-balance hash-result interface port-channel 10 switch 1 ip 10.1.1.1 20.1.1.1
Computed RBH: 0x4
Would select Gi2/2/1 of Po10

When using VSS it is best to specify switch <id> with the hash result CLI command, if not the VSS assumes switch <1> when commuting hash results.
VSS Architecture
Catalyst 6500 Sup720 MEC Load-Balance Schemes

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dst-ip</td>
<td>Dst IP Addr</td>
</tr>
<tr>
<td>dst-mac</td>
<td>Dst Mac Addr</td>
</tr>
<tr>
<td>dst-mixed-ip-port</td>
<td>Dst IP Addr and TCP/UDP Port</td>
</tr>
<tr>
<td>dst-port</td>
<td>Dst TCP/UDP Port</td>
</tr>
<tr>
<td>mpls</td>
<td>Load Balancing for MPLS packets</td>
</tr>
<tr>
<td>src-dst-ip</td>
<td>Src XOR Dst IP Addr</td>
</tr>
<tr>
<td>src-dst-mac</td>
<td>Src XOR Dst Mac Addr</td>
</tr>
<tr>
<td>src-dst-mixed-ip-port</td>
<td>Src XOR Dst IP Addr and TCP/UDP Port</td>
</tr>
<tr>
<td>src-dst-port</td>
<td>Src XOR Dst TCP/UDP Port</td>
</tr>
<tr>
<td>src-ip</td>
<td>Src IP Addr</td>
</tr>
<tr>
<td>src-mac</td>
<td>Src Mac Addr</td>
</tr>
<tr>
<td>src-mixed-ip-port</td>
<td>Src IP Addr and TCP/UDP Port</td>
</tr>
<tr>
<td>src-port</td>
<td>Src TCP/UDP Port</td>
</tr>
</tbody>
</table>
## VSS Architecture

Catalyst 6500/6800 Sup2T MEC Load-Balance Schemes

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dst-ip</code></td>
<td>Dst IP Addr</td>
</tr>
<tr>
<td><code>dst-mac</code></td>
<td>Dst Mac Addr</td>
</tr>
<tr>
<td><code>dst-mixed-ip-port</code></td>
<td>Dst IP Addr and TCP/UDP Port</td>
</tr>
<tr>
<td><code>dst-port</code></td>
<td>Dst TCP/UDP Port</td>
</tr>
<tr>
<td><code>mpls</code></td>
<td>Load Balancing for MPLS packets</td>
</tr>
<tr>
<td><code>src-dst-ip</code></td>
<td>Src XOR Dst IP Addr</td>
</tr>
<tr>
<td><code>src-dst-mac</code></td>
<td>Src XOR Dst Mac Addr</td>
</tr>
<tr>
<td><code>src-dst-mixed-ip-port</code></td>
<td>Src XOR Dst IP Addr and TCP/UDP Port</td>
</tr>
<tr>
<td><code>src-dst-port</code></td>
<td>Src XOR Dst TCP/UDP Port</td>
</tr>
<tr>
<td><code>src-ip</code></td>
<td>Src IP Addr</td>
</tr>
<tr>
<td><code>src-mac</code></td>
<td>Src Mac Addr</td>
</tr>
<tr>
<td><code>src-mixed-ip-port</code></td>
<td>Src IP Addr and TCP/UDP Port</td>
</tr>
<tr>
<td><code>src-port</code></td>
<td>Src TCP/UDP Port</td>
</tr>
<tr>
<td><code>vlan-dst-ip</code></td>
<td>Vlan, Dst IP Addr</td>
</tr>
<tr>
<td><code>vlan-dst-mixed-ip-port</code></td>
<td>Vlan, Dst IP Addr and TCP/UDP Port</td>
</tr>
<tr>
<td><code>vlan-src-dst-ip</code></td>
<td>Vlan, Src XOR Dst IP Addr</td>
</tr>
<tr>
<td><code>vlan-src-dst-mixed-ip-port</code></td>
<td>Vlan, Src XOR Dst IP Addr and TCP/UDP Port</td>
</tr>
<tr>
<td><code>vlan-src-ip</code></td>
<td>Vlan, Src IP Addr</td>
</tr>
<tr>
<td><code>vlan-src-mixed-ip-port</code></td>
<td>Vlan, Src IP Addr and TCP/UDP Port</td>
</tr>
</tbody>
</table>
VSS Architecture
Catalyst 4500-E Sup7 and Catalyst 4500-X  MEC Load-Balance Schemes

```plaintext
C4K_VSS(config)#port-channel load-balance ?

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dst-ip</td>
<td>Dst IP Addr</td>
</tr>
<tr>
<td>dst-mac</td>
<td>Dst Mac Addr</td>
</tr>
<tr>
<td>dst-port</td>
<td>Dst TCP/UDP Port</td>
</tr>
<tr>
<td>src-dst-ip</td>
<td>Src XOR Dst IP Addr</td>
</tr>
<tr>
<td>src-dst-mac</td>
<td>Src XOR Dst Mac Addr</td>
</tr>
<tr>
<td>src-dst-port</td>
<td>Src XOR Dst TCP/UDP Port</td>
</tr>
<tr>
<td>src-ip</td>
<td>Src IP Addr</td>
</tr>
<tr>
<td>src-mac</td>
<td>Src Mac Addr</td>
</tr>
<tr>
<td>src-port</td>
<td>Src TCP/UDP Port</td>
</tr>
</tbody>
</table>
```
VSS Enabled Campus Design
Unicast ECMP Traffic Flows

- ECMP forwarding also favors locally attached interfaces
- Hardware FIB first inserts entries for ECMP routes using locally attached links
- If all local links fail, the FIB is programmed to forward across the VSL link

```
cr2-6500-vss# show ip route 10.121.0.0 255.255.128.0 longer-prefixes
D 10.121.0.0/17
 [90/3328] via 10.122.0.33, 2d10h, TenGigabitEthernet2/2/1
 [90/3328] via 10.122.0.27, 2d10h, TenGigabitEthernet1/2/1
 [90/3328] via 10.122.0.22, 2d10h, TenGigabitEthernet2/2/2
 [90/3328] via 10.122.0.20, 2d10h, TenGigabitEthernet1/2/2
```

```
cr2-6500-vss# show mls cef 10.121.0.0 17 switch 1
Codes: decap - Decapsulation, + - Push Label
Index  Prefix             Adjacency
102400 10.121.0.0/17     Tel1/2/2, 0012.da67.7e40 (Hash: 0001)   Tel1/2/1, 0018.b966.e988 (Hash: 0002)
```

Four ECMP Entries
Two FIB Entries
VSS Hardware and Software Requirements
## VSS is supported on Catalyst 6500, 6800, 4500-E and 4500-X

<table>
<thead>
<tr>
<th>Supers</th>
<th>Catalyst 6500 / 6800</th>
<th>Catalyst 4500-E</th>
<th>Catalyst 4500-X</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sup2T, Sup720-10G</td>
<td>Sup7-E, Sup7L-E</td>
<td>Fixed (based on Sup7E)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sup8-E</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mixed / Asymmetric Chassis Support</td>
<td>Yes</td>
<td>Yes *after release 3.5.0E</td>
<td>No, must pair using the same base model, either 16-port or 32-port</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Optional 8-port module is supported</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Trains</td>
<td>Sup2T - 12.2SY, 15.0SY, 15.1SY, 15.2SY</td>
<td>3.6.0E 3.5.0E 3.4.0SG 15.1(2)SG</td>
<td>3.6.0E 3.5.0E, 3.4.0SG</td>
</tr>
<tr>
<td></td>
<td>Sup720-10G - 12.2SXH, 12.2SXI, 12.2SXJ, 15.1SY</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sup SSO</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>No, Future Release</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quad-Sup SSO</td>
<td>Sup2T 15.1SY1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>No, Future Release</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quad-Sup Uplink Forwarding</td>
<td>Sup720-10G 12.2(33)SXI4</td>
<td>No, Future Release</td>
<td>N/A</td>
</tr>
</tbody>
</table>
VSS Requirements

Catalyst 6500 and 6800 Supervisor Modules

- **VSS-capable Supervisors**
  - VS-S720-10G @ 12.2(33)SXH1
  - VS-S2T-10G @ 15.0(1)SY

- **New Forwarding Engine ASICs**
  - Virtual Switch port indexes & maps to allow traffic forwarding across 2 chassis
  - Distributed DFC mode across 2 chassis

- **VSL-capable 10GE uplinks**

- VSS is NOT supported on the Sup720-3B or earlier models
# VSS Requirements

Catalyst 6500 and 6800 VSL Capable Modules

<table>
<thead>
<tr>
<th>Module</th>
<th>Description</th>
<th>VSL (Capable) Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>VS-S720-10G (XL)</td>
<td>720G VSS Capable Supervisor</td>
<td>2</td>
</tr>
<tr>
<td>WS-X6708-10G (XL)</td>
<td>10GE X2 Fiber Line Card</td>
<td>8</td>
</tr>
<tr>
<td>WS-X6716-10G (XL)</td>
<td>10GE X2 Fiber Line Card</td>
<td>4 (Performance mode)</td>
</tr>
<tr>
<td>WS-X6716-10T (XL)</td>
<td>10GE RJ45 Copper Line Card</td>
<td>4 (Performance mode)</td>
</tr>
<tr>
<td>VS-S2T-10G (XL)</td>
<td>720G VSS Capable Supervisor</td>
<td>2</td>
</tr>
<tr>
<td>WS-X6908-10G (XL)</td>
<td>10GE X2 Fiber Line Card</td>
<td>8</td>
</tr>
</tbody>
</table>
# VSS Requirements

Introducing NEW Catalyst 6500 and 6800 VSL capable 10G modules

<table>
<thead>
<tr>
<th>Bandwidth in 6807</th>
<th>32x10G SFP+</th>
<th>16x10G SFP+</th>
<th>8x10G SFP+</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optics:</td>
<td>160G SFP / SFP+</td>
<td>80G SFP / SFP+</td>
<td>80G SFP / SFP+</td>
</tr>
<tr>
<td>Buffers per Port:</td>
<td>250 MB</td>
<td>250 MB</td>
<td>500 MB</td>
</tr>
<tr>
<td>Additional Hardware Features:</td>
<td>VSS &amp; Instant Access, SGT, MACSec, LISP, Dual Priority Queues, Two Level HQoS</td>
<td>VSS &amp; Instant Access, SGT, MACSec, LISP, Dual Priority Queues, Two Level HQoS</td>
<td>VSS &amp; Instant Access, SGT, MACSec, LISP, Dual Priority Queues, Two Level HQoS</td>
</tr>
<tr>
<td>Designed for</td>
<td>Core &amp; Aggregation</td>
<td>Core &amp; Aggregation</td>
<td>Core</td>
</tr>
</tbody>
</table>

Supported With 15.2(1)SY

BRKCRS-3035 © 2015 Cisco and/or its affiliates. All rights reserved. Cisco Public 51
## VSS Requirements

Catalyst 6500 Sup72-10G VSS Supported Ethernet LAN Modules

<table>
<thead>
<tr>
<th>Module</th>
<th>Description</th>
<th>Minimum IOS Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-X6148E-GE-TX</td>
<td>10/100/1000TX Copper Line Card (BUS)</td>
<td>12.2(33)SXJ1</td>
</tr>
<tr>
<td>WS-X6724-SFP</td>
<td>1GE SFP Fiber Line Card (CFC or DFC3C)</td>
<td>12.2(33)SXH1</td>
</tr>
<tr>
<td>WS-X6748-SFP</td>
<td>1GE SFP Fiber Line Card (CFC or DFC3C)</td>
<td>12.2(33)SXH1</td>
</tr>
<tr>
<td>WS-X6748-GE-TX</td>
<td>10/100/1000TX Copper Line Card (CFC or DFC3C)</td>
<td>12.2(33)SXH1</td>
</tr>
<tr>
<td>WS-X6704-10G</td>
<td>10GE Xenpak Fiber Line Card (CFC or DFC3C)</td>
<td>12.2(33)SXH1</td>
</tr>
<tr>
<td>WS-X6708-10G (XL)</td>
<td>10GE X2 Fiber Line Card (DFC3C)</td>
<td>12.2(33)SXH1</td>
</tr>
<tr>
<td>WS-X6716-10G (XL)</td>
<td>10GE X2 Fiber Line Card (DFC3C)</td>
<td>12.2(33)SXH1</td>
</tr>
<tr>
<td>WS-X6716-10T (XL)</td>
<td>10GE RJ45 Copper Line Card (DFC3C)</td>
<td>12.2(33)SXI4</td>
</tr>
</tbody>
</table>
## VSS Requirements
Catalyst 6500 and 6800 Sup2T VSS Supported Ethernet LAN Modules

<table>
<thead>
<tr>
<th>Module</th>
<th>Description</th>
<th>Minimum IOS Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-X6148E-GE-TX</td>
<td>10/100/1000TX Copper Line Card (BUS)</td>
<td>15.1(1)SY</td>
</tr>
<tr>
<td>WS-X6724-SFP</td>
<td>1GE SFP Fiber Line Card (CFC or DFC4)</td>
<td>15.0(1)SY</td>
</tr>
<tr>
<td>WS-X6824-SFP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WS-X6748-SFP</td>
<td>1GE SFP Fiber Line Card (CFC or DFC4)</td>
<td>15.0(1)SY</td>
</tr>
<tr>
<td>WS-X6848-SFP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WS-X6748-GE-TX</td>
<td>10/100/1000TX Copper Line Card (CFC or DFC4)</td>
<td>15.0(1)SY</td>
</tr>
<tr>
<td>WS-X6848-GE-TX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WS-X6704-10G</td>
<td>10GE Xenpak Fiber Line Card (CFC or DFC4)</td>
<td>15.0(1)SY</td>
</tr>
<tr>
<td>WS-X6716-10G (XL)</td>
<td>10GE X2 Fiber Line Card (DFC4)</td>
<td>15.0(1)SY</td>
</tr>
<tr>
<td>WS-X6816-10G (XL)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WS-X6716-10T (XL)</td>
<td>10GE RJ45 Copper Line Card (DFC4)</td>
<td>15.0(1)SY</td>
</tr>
<tr>
<td>WS-X6816-10T (XL)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WS-X6908-10G (XL)</td>
<td>10GE X2 Fiber Line Card (DFC4)</td>
<td>15.0(1)SY</td>
</tr>
<tr>
<td>WS-X6904-40G (XL)</td>
<td>10GE SFP+ / 40GE CFP Fiber Line Card (DFC4)</td>
<td>15.0(1)SY1</td>
</tr>
</tbody>
</table>
# VSS Requirements

Catalyst 6500 and 6800 VSS Service Module Support

<table>
<thead>
<tr>
<th>Module</th>
<th>Description</th>
<th>VSS Minimum Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-SVC-NAM-1, WS-SVC-NAM-2</td>
<td>Network Analysis Module</td>
<td>12.2(33)SXJ1 – Sup720</td>
</tr>
<tr>
<td>WS-SVC-NAM3-G6-K9</td>
<td>Network Analysis Module</td>
<td>15.0(1)Sy – Sup2T</td>
</tr>
<tr>
<td>WS-SVC-WISM-1-K9, WS-SVC-WISM-2-K9</td>
<td>Wireless Services Module (WiSM)</td>
<td>12.2(33) SXJ1 – Sup720</td>
</tr>
<tr>
<td>ACE10-6500-K9, ACE20-6500-K9, ACE30-6500-K9</td>
<td>Application Control Engine</td>
<td>15.0(1)Sy – Sup2T</td>
</tr>
<tr>
<td>WS-SVC-FWSM-1-K9</td>
<td>Firewall Services Module (FWSM)</td>
<td>12.2(33)SXI – Sup720</td>
</tr>
<tr>
<td>WS-SVC-IDSM2-K9</td>
<td>Intrusion Detection System Services Module (IDSM)</td>
<td>15.0(1)Sy – Sup2T</td>
</tr>
<tr>
<td>WS-SVC-ASA-SM1-K9</td>
<td>Adaptive Security Application Services Modules (ASA-SM)</td>
<td>12.2(33)SXJ1 – Sup720</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15.0(1)Sy – Sup2T</td>
</tr>
</tbody>
</table>
# VSS Hardware Requirements

## System PFC Mode Matrix

<table>
<thead>
<tr>
<th>Linecard Type</th>
<th>Sup720-10G (Standalone) System wide PFC Mode</th>
<th>Sup720-10G (VSS) System wide PFC Mode</th>
<th>Sup2T (Standalone) System Wide PFC Mode</th>
<th>Sup2T (VSS) System Wide PFC Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>DFC4</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>PFC4</td>
<td>PFC4</td>
</tr>
<tr>
<td>DFC3C</td>
<td>PFC3C</td>
<td>PFC3C</td>
<td>Not Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td>DFC3B</td>
<td>PFC3B*</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td>DFC3A</td>
<td>PFC3A*</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td>DFC2</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td>CFC</td>
<td>PFC3C</td>
<td>PFC3C</td>
<td>PFC4 (6700-series)</td>
<td>PFC4 (6700-series)</td>
</tr>
<tr>
<td>Classic</td>
<td>PFC3C</td>
<td>Not Supported</td>
<td>6148 Series</td>
<td>WS-X6148E-GE-45AT (only)</td>
</tr>
</tbody>
</table>
VSS Requirements
Catalyst 4500-E and 4500-X VSS Support

- Software support begins with IOS XE 3.4.0SG
- All 10G and 1G ports supported as VSL ports
- EtherChannel rules apply: All ports must be either 10G or 1G
## VSS Requirements

### Catalyst 4500E and 4500X VSS Support Matrix

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Chassis</th>
<th>Supervisor</th>
<th>Modules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalyst 4500E</td>
<td>4503+E</td>
<td>Sup7E</td>
<td>WS-X4748-RJ45-V</td>
</tr>
<tr>
<td></td>
<td>4506+E</td>
<td>Sup7LE</td>
<td>WS-X4712-SFP+E</td>
</tr>
<tr>
<td></td>
<td>4507+E</td>
<td></td>
<td>WS-X4748-UPOE+E</td>
</tr>
<tr>
<td></td>
<td>4510R+E</td>
<td></td>
<td>WS-X4748-RJ45-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>WS-X4606-X2-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>WS-X4648-RJ45V-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>WS-X4648-RJ45V+</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>WS-X4648-RJ45-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>WS-X4640-CSFP-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>WS-X4624-SFP-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>WS-X4612-SFP-E</td>
</tr>
<tr>
<td>Catalyst 4500X</td>
<td>WS-C4500X-32SFP+</td>
<td>-</td>
<td>C4KX-NM-8SFP+</td>
</tr>
<tr>
<td></td>
<td>WS-C4500X-F-32SFP+</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C4500X16SFP+</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C4500X-F-16SFP+</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C4500X-24X-IPB</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C4500X-40X-ES</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-C4500X-24X-ES</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**All supported 4500-E series modules are VSL capable**

**Legacy modules WS-45XX and WS-42XX are not supported**
## VSS Feature Comparison:
### C4500E/X vs C6500/6800

<table>
<thead>
<tr>
<th>Capability</th>
<th>Catalyst 6500</th>
<th>Catalyst 4500E/X Phase I 3.4xSG</th>
<th>Catalyst 4500E/X Phase II 3.5.0E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quad-sup VSS SSO</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Quad Sup Forwarding Uplinks</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Switchport-based Multi-chassis EC</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Routed Port Multi-chassis EC</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Split Brain Detection method</td>
<td>Fast Hello, EPAgP</td>
<td>EPAgP</td>
<td>Fast Hello, EPAgP</td>
</tr>
<tr>
<td>Cross-chassis NSF/SSO</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cross-chassis ISSU</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PoE LC support in VSS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Asymmetric chassis (VSS between different slot E-chassis or base model X-series)</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Smart Install Director w/VSS</td>
<td>Yes</td>
<td>No (Standalone only)</td>
<td>Yes</td>
</tr>
</tbody>
</table>
## Catalyst 4500 Series Feature Differences Between Standalone and VSS mode

<table>
<thead>
<tr>
<th>Features</th>
<th>Standalone</th>
<th>VSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>UniDirectional Ethernet &amp; UniDirectional Link Routing</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Connectivity Fault Management D8.1</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Resilient Ethernet Protocol and associated features</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Flexlinks</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>PVL,L2PT, Fast UDLD</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>WCCP - needs SSO compliance</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Dot1q Tunnel (Legacy dot1q tunnel)</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Vlan Translation (1:1, 1:2-Selective QinQ)</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Mediatrace and Metadata – needs SSO compliance</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>MACsec on VSL ports</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>EnergyWise</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
VSS Requirements
Always Verify Supported Hardware with Software Release Notes

Before every deployment always read the Release Notes for the planned software release and check the Supported Hardware section to verify all components are supported.

• Catalyst 6800/6500/4500 modular platforms are designed for very long product lifecycles
• Investment Protection is a key design criteria
• Overtime older hardware support is not carried forward with the newest software releases in order to minimize complexity, optimize performance, increase feature velocity or all of the above
• New features are sometimes phased in with only the most relevant hardware support in the initial release
High Availability
System Redundancy with SSO/NSF
Single and Dual Chassis Sup Redundancy

- Non-Redundant Systems are Single-Points-Of-Failure
- Single-chassis Redundant Supervisors provide System-level Stateful & Graceful redundancy
- Protects network services, capacity and availability for Wired and WLAN end-points

- Cisco VSS provides inter-chassis redundancy
- Redundant Supervisors between both chassis provides VSS Stateful & Graceful redundancy
- Protects network services and availability at Access layer with redundant paths
Virtual Switching System
Inter Chassis SSO/NSF

1. Virtual Switch incurs a failure of the (SSO) Active Supervisor in Switch 1
The Standby Supervisor detects failure by loss of all VSL ports, or no replies to SSO keep-alive packets

2. The original Standby Supervisor now takes over as the new Virtual Switch Active
Virtual Switch initiates Graceful Restart (NSF)
Non Stop Forwarding of packets continues using hardware entries synched to Switch 2
NSF Aware neighbors exchange protocol updates with the new Virtual Switch Active
High Availability
Redundancy Schemes

The default redundancy mechanism between for VSS is SSO

If a mismatch of occurs between the Active & Standby, the Standby will revert to RPR mode
High Availability
SSO & NSF – L2 & L3 Graceful Restart

Non-Stop Forwarding (NSF), combined with SSO, minimizes traffic loss during Switchover. NSF Aware neighbors continue to forward traffic, using SSO synchronized hardware entries...

VSS#config t
VSS(config)#router ospf 1
VSS(config-router)#nsf

VSS# show ip ospf
Routing Process "ospf 10" with ID 192.168.2.1
Start time: 00:15:29.344, Time elapsed: 23:12:03.484
Supports only single TOS(TOS0) routes
External flood list length 0
Non-Stop Forwarding enabled
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 100 mbps

NSF is supported by BGP, EIGRP, OSPF & IS-IS
High Availability
Failure of MEC member – Upstream Traffic

No Change in Network Topology

Convergence time is determined by Neighbor EtherChannel recalculation

- Neighbor EtherChannel convergence is typically ~100-200ms
- Only the flows on the Failed Link(s) are affected (recalculated)
High Availability
Failure of MEC member – Downstream Traffic

No Change in Network Topology

Convergence time is determined by VSS EtherChannel recalculaton

- VSS EtherChannel convergence is typically ~50-100ms
- Only the flows on the Failed Link(s) are affected (recalculated)
Dual-Active Scenarios
High Availability

Dual-Active Detection

In a VSS Domain, one switch is elected as Active and the other as Standby

All Neighbors view VSS as a single Entity, single MAC, single IP

Since the VSL is always configured as a Port Channel, the chance of the entire VSL going down is remote…

However… IT IS POSSIBLE! 😞

Recommend to deploy the VSL with 2 or more links, distributed across multiple Line Cards to ensure the highest redundancy
High Availability

Dual-Active Detection

If the entire VSL bundle fails, the VSS Domain will enter into a “Dual Active” scenario

Both switches transition to SSO Active state, and share the same network configuration

- IP addresses, MAC address, Router IDs, etc.

This can cause communication problems in the network!

3 Step Process

1. Dual-Active Detection - using any detection method enabled in the system.

2. Previous VSS Active shuts down ALL interfaces, and enters “Recovery Mode”… preventing further network disruption

3. Dual-Active Recovery - when the VSL recovers, the switch in Recovery Mode will reload to boot into a preferred standby state
Dual- Active Scenario

Three Phases to Restoration

1. **Detection**
   - Enhanced PAgP
   - Fast Hello

2. **Recovery**
   - Admin down ports
   - Recover the VSL

3. **Restoration**
   - VSL functional
   - Reload recovery chassis

Recommendation - Configure a minimum of two dual-active detection sessions (same or different)
High Availability
Dual-Active Protocols

Enhanced PAGP

- Requires ePAGP capable neighbor:
  - 3750: 12.2(46)SE
  - 4500: 12.2(44)SE
  - 6500: 12.2(33)SXH1

- Sub-Second Convergence
  - Typically ~200-250ms

VSLP Fast Hello

- Direct L2 Point-to-Point Connection
  - Requires 12.2(33)SXI

- Sub-Second Convergence
  - Typically ~50-100ms

Instant Access (FEX)

- Requires Dual-Home IA Client
  - Only for C6500 / C6800
  - Requires 15.1(2)SY2

- Sub-Second Convergence
  - Typically ~150-200ms
Dual-Active Detection - Option 1

Enhanced PAgP

%DUAL_ACTIVE-SW1_SP-1-DETECTION: Dual-active condition detected: all non-VSL and non-excluded interfaces have been shut down
Enhanced PAgP

How it Works – Normal Operation

Switch 1
Active

Switch 2
Standby

VSS

VSL

TRusted Port-Channel configuration for dual-active detection
Enhanced PAgP
How it Works – Dual-active detection

%DUAL_ACTIVE-SWI_SP-1-DETECTION: Dual-active condition detected: all non-VSL and non-excluded interfaces have been shut down
switch virtual domain 100
dual-active detection pagp
dual-active detection pagp trust channel-group 20
dual-active detection pagp trust channel-group 25

VSS#show switch virtual dual-active pagp
PAgP dual-active detection enabled: Yes
PAgP dual-active version: 1.1

Channel group 20 dual-active detect capability w/nbrs
Dual-Active trusted group: Yes

<table>
<thead>
<tr>
<th>Port</th>
<th>Detect Capable</th>
<th>Name</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Te1/3/5</td>
<td>Yes</td>
<td>SW101</td>
<td>Te1/0/1</td>
</tr>
<tr>
<td>Te2/3/5</td>
<td>Yes</td>
<td>SW101</td>
<td>Te1/0/2</td>
</tr>
</tbody>
</table>

Channel group 25 dual-active detect capability w/nbrs
Dual-Active trusted group: Yes

<table>
<thead>
<tr>
<th>Port</th>
<th>Detect Capable</th>
<th>Name</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Te1/3/4</td>
<td>No</td>
<td>SW103</td>
<td>Te5/1</td>
</tr>
<tr>
<td>Te2/3/4</td>
<td>No</td>
<td>SW103</td>
<td>Te6/1</td>
</tr>
</tbody>
</table>
Dual-Active Detection – Option 2
Detection Method – Fast Hello

VSS Active

VSL

VSLP Fast Hello

Port Channel

VSS Active

%DUAL_ACTIVE-SW1_SP-1-DETECTION: Dual-active condition detected: all non-VSL and non-excluded interfaces have been shut down
Fast Hello

How it Works – Normal Operation

Dedicated Heartbeat Link for Fast Hello session
Fast Hello
How it Works - Dual-active Detection

%DUAL_ACTIVE-SW1_SP-1-DETECTION: Dual-active condition detected: all non-VSL and non-excluded interfaces have been shut down
Dual-Active Scenario
Fast Hello Configuration and Operation

```
switch virtual domain 100
dual-active detection fast-hello

interface GigabitEthernet1/2/3
description "to VSS-SW2 gi2/2/3"
no switchport
no ip address
dual-active fast-hello
!
interface GigabitEthernet2/2/3
description "to VSS-SW1 gi1/2/3"
no switchport
no ip address
dual-active fast-hello

VSS#show switch virtual dual-active fast-hello
Fast-hello dual-active detection enabled: Yes

Fast-hello dual-active interfaces:

<table>
<thead>
<tr>
<th>Port</th>
<th>Local State</th>
<th>Peer Port</th>
<th>Remote State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/2/3</td>
<td>Link up</td>
<td>Gi2/2/3</td>
<td>Link up</td>
</tr>
</tbody>
</table>
```
High Availability

Dual-Active: Recovery Mode

%DUAL_ACTIVE-SW1_SP-1-DETECTION: Dual-active condition detected: all non-VSL and non-excluded interfaces have been shut down

VSS#show switch virtual dual-active summary
Pagp dual-active detection enabled: Yes
Bfd dual-active detection enabled: Yes

No interfaces excluded from shutdown in recovery mode

In dual-active recovery mode: Yes
  Triggered by: Pagp detection
  Triggered on interface: Gi1/2/3
%DUAL_ACTIVE-SW1_SP-1-DETECTION: Dual-active condition detected: all non-VSL and non-excluded interfaces have been shut down

Recovery Mode - Previously Active switch will administratively down all of it’s interfaces and attempt to recover the VSL
High Availability
Dual-Active Detection – Exclude Interfaces

Upon detection of a Dual Active scenario, ALL local interfaces on the Previous-Active are brought down, to avoid disrupting the remainder of the network.

The “exclude interface” command excludes the VSL port members and any pre-configured local interfaces used for management purposes...

VSS#conf t
Enter configuration commands, one per line. End with CNTL/Z.
VSS(config)#switch virtual domain 100
VSS(config-vs-domain)#dual-active exclude interface Gig 1/5/1
VSS(config-vs-domain)#dual-active exclude interface Gig 2/5/1
VSS(config-vs-domain)#^Z
VSS#
High Availability
Dual Active: Recovery Mode

**Important:** DO NOT make any VSS configuration changes while in the Dual Active Recovery mode!

If the running-config is changed, the system will NOT automatically recover, once the VSL is operation again…

You must issue a “write memory” command and manually reload the switch in recovery mode, using the “reload shelf” command.
Dual-Active Restoration
VSS Supervisor Engine Redundancy
VSS Redundant Supervisor Support

Why Are Redundant Supervisors Needed?

1. A Supervisor failure will decrease available VSS bandwidth by 50%

2. Some devices may only single-attach to the VSS (for various reasons)
   - Single NIC Servers, AP’s, Phones, Cameras
   - Service Modules in Local VSS chassis
   - Geographic Separation of VSS chassis

3. Supervisor failure requires manual intervention for recovery
   - Failed Supervisor requires onsite hardware removal
   - Replacement Supervisor requires hardware installation
   - Replacement Supervisor requires software installation
   - Replacement Supervisor requires copy of VSS config
   - Non-Deterministic Outage Time!!!
VSS Single Supervisor
Normal Operation & SSO Redundancy

Control Plane Active
Data Plane Active

Control Plane Standby
Data Plane Active
VSS Single Sup Operation

Supervisor Failure Example
VSS Single Sup Operation
Supervisor Failure Manual Repair Example

- Lose 50% Bandwidth until Repair
- Non-Deterministic Recovery Time
- 100% Impact to Single-Attached Devices
Quad-Sup Uplink Forwarding
RPR-Warm Redundancy Mode

In-Chassis Standby Supervisor
- Downloads & Boots a special Sup720-LC image
- SP CPU runs the Sup720-LC image
- RP CPU is in ROMMON
- Operates as a DFC enabled Line Card
- Some Supervisor Sub-systems are synched between In-Chassis Active and In-Chassis Standby

Subsystems Synched
- Startup-config (@ write memory)
- Vlan.dat (VLAN Database)
- BOOT ROMMON variable
- CONFIG_FILE ROMMON variable
- BOOTLDR ROMMON variable
- DIAG ROMMON variable
- SWITCH_NUMBER ROMMON variable
Quad-Sup Uplink Forwarding
Redundancy Mode

RPR-WARM is a new redundancy mode created for the VSS In-Chassis Standby Supervisor.

RPR-WARM mode primarily allows the ICS Supervisor to operate as a DFC enabled Line Card, but also provides limited synchronization with the ICA Supervisor (Non SSO).

The Supervisor PFC, Fabric and all 1G & 10G uplink ports are Operational and Forwarding.
Quad-Sup Uplink Forwarding

VSS Supervisor Redundancy

Available Bandwidth

100%

Available Bandwidth

50%

Control Plane Active
Data Plane Active

Control Plane RPR-Warm
Data Plane Active

Control Plane RPR-Warm
Data Plane Active

Control Plane Standby
Data Plane Active

Control Plane RPR-Warm
Data Plane Active
## CLI Verification

<table>
<thead>
<tr>
<th>VSS#sho mod</th>
<th>Model</th>
<th>Serial No.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Supervisor</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Engine 720</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10GE (Active)</td>
<td></td>
</tr>
<tr>
<td>5 5</td>
<td>VS-S720-10G</td>
<td>SAD1205069Y</td>
</tr>
<tr>
<td>6 5</td>
<td>VS-S720-10G</td>
<td>SAD1205065B</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mod</th>
<th>MAC addresses</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>001e.4aaa.ee70 to 001e.4aaa.ee77</td>
<td>12.2(2009050 Ok</td>
</tr>
<tr>
<td>6</td>
<td>001e.4aaa.ed58 to 001e.4aaa.ed5f</td>
<td>12.2(2009042 Ok</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mod</th>
<th>Sub-Module</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Policy Feature Card 3</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>MSFC3 Daughterboard</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Policy Feature Card 3</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>MSFC3 Daughterboard</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Online Diag Status</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mod</th>
<th>Online</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Pass</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Pass</td>
<td></td>
</tr>
</tbody>
</table>
CLI Verification

VSS#show switch virtual redundancy
My Switch Id = 1
  Peer Switch Id = 2
  Last switchover reason = user forced
  Configured Redundancy Mode = sso
  Operating Redundancy Mode = sso

Switch 1 Slot 5 Processor Information :
-----------------------------------------------
  Current Software state = ACTIVE
  Image Version = Cisco IOS Software, s72033_rp Software
  Configuration register = 0x2
    Fabric State = ACTIVE
    Control Plane State = ACTIVE

Switch 1 Slot 6 Processor Information :
-----------------------------------------------
  Current Software state = RPR-Warm
  Uptime in current state = 4 days, 17 hours, 36 minutes
  Image Version = << we will show Sup720-LC related image compilation>>
    BOOT = disk0:mz-rbh,12;
    CONFIG_FILE =
    BOOTLDR =
  Configuration register = 0x2
    Fabric State = RPR-Warm
    Control Plane State = RPR-Warm
Quad-Sup Uplink Forwarding
VSS Supervisor Redundancy

- Automated Chassis & Link Recovery
- Deterministic Outage Time (Reload)
- Minimize Outage for Single-Attached Devices

Available Bandwidth
100%
50%

Control Plane Active
Data Plane Active
Control Plane Standby
Control Plane RPR-Warm
Data Plane Active

Reload Time 5 – 15 minutes
Quad Supervisor Uplink Forwarding

Key Points

- **Supported ONLY on Supervisor 720-10G in VSS**
- **Supported provided from 12.2(33)SXI4 onwards**
  - In-Chassis Standby Uplinks are Active & Forwarding (origin of feature name)
  - In-Chassis Standby Supervisor runs in new redundancy mode called RPR-WARM
  - In-Chassis Standby Supervisor runs a special image & operates as a DFC Line Card
  - IOS Image, Boot Variable and Running-Configuration are synchronized
  - Switchover to the In-Chassis Supervisor DOES require a reload of the chassis
  - During boot the In-Chassis Supervisor role negotiation occurs First…
  - Then the In-Chassis Active performs role negotiation between VSS chassis
  - Quad Sup Uplink Forwarding allows deterministic recovery from Supervisor failure events

VS-S720-10G (XL)
VSS Quad-Sup SSO
Standby-HOT Redundancy Mode

- **In-Chassis Standby Supervisor**
  - Boots the same IOS image as ICA
  - Runs a new Inter-Chassis RF/CF Domain
  - ICS becomes Standby-HOT to ICA
  - All Supervisor subsystems & Feature states are synched

- **SSO Synchronization**
  - **Startup-config** (@ write memory)
  - **Vlan.dat** (VLAN Database)
  - **BOOT** ROMMON variable
  - **SWITCH_NUMBER** ROMMON variable
  - **Bulk Synch** (RF / CF)
  - **Periodic Synch** (RF / CF)
**VSS Quad-Sup SSO**

Redundancy Mode

**STANDBY HOT (CHASSIS)** is a new redundancy mode created for the VSS ICS Supervisor

STANDBY HOT (CHASSIS) mode allows the ICS Supervisor to operate in a separate RF/CF (SSO) Domain, while maintaining the Traditional RF/CF (SSO) Domain between VSS chassis.

The ICS PFC, Switch Fabric and all 1G & 10G uplink ports are Operational and Forwarding
VSS Quad-Sup SSO
Ultimate High Availability

- Automated Recovery
- Sub-Second Outage (No Flap) for Single-Attached Devices
- Full SSO Redundancy

Available Bandwidth

50ms – 200ms

100%

50%

Control Plane Active
Data Plane Active

Control Plane Standby
Data Plane Active

Data Plane Active

Control Plane Active
Data Plane Active

Control Plane Standby
(Chassis)
Data Plane Active

Available Bandwidth

Time

100%

50%
VSS Quad-Sup

VSS “Z” Pattern Switchovers

- Switch-Over of the VSS Active Supervisor is ALWAYS across VSS Chassis
- Default Redundancy Domain is responsible for the VSS Active and Standby
VSS Quad-Sup SSO

Redundancy Domains

VSS Domain

Default Redundancy Domain

VS Switch ID 1

VS Switch ID 2

In Chassis Active (ICA)

In Chassis Standby (ICS)

VSS Active

In Chassis Redundancy Domain

VSS Standby

In Chassis Redundancy Domain

SSO

SSO

VS Switch ID 1

VS Switch ID 2

In Chassis Active (ICA)

In Chassis Standby (ICS)

In Chassis Active (ICA)

In Chassis Standby (ICS)
VSS Quad-Sup SSO
Redundancy Domains

VSS Domain
Default Redundancy Domain

VSS Active (Active)
VSS Standby Hot (Switchover Target)

SSO

VS Switch ID 1
VS Switch ID 2

In Chassis Redundancy Domain
In Chassis Redundancy Domain

In Chassis Active (ICA)
In Chassis Standby (ICS) (Standby Hot Chassis)

In Chassis Active (ICA)
In Chassis Standby (ICS) (Standby Hot Chassis)
VSS Quad Sup SSO
Switchovers (First Switchover Example)

In Chassis Redundancy Domain

In Chassis Active (ICA)

VSS Standby Hot (Switchover Target)

In Chassis Active (ICA) (Standby Hot Chassis)

Default Redundancy Domain

VSS Domain

VSS Active (Active)

SSO

VSS Active (Active)

VS Switch ID 1

VS Switch ID 2

In Chassis Active (ICA)

In Chassis Standby (ICS) (Standby Hot Chassis)

SSO
VSS Quad Sup SSO
Switchovers (Second Switchover Example)
Quad-Sup SSO
Supervisor Fail Event – Data-Plane Convergence

Impact on affected Chassis is dependent on:
1. Ingress to Egress module/port relation (Local Switching or Across Fabric)
2. Line Card fabric switchover capabilities
Line Card Data-Plane
Redundancy Dependencies (Local Switching)

- Traffic between ports on the **Same Line Card** (e.g. T2/1/1 & T2/1/2) will **NOT** be affected by Supervisor SSO events...

- **No Card or Port Flaps**
  - ICS SSO Synch of Infrastructure
  - OIR, PM, FM, LTL/FPOE, etc

- **No Packet Loss**
  - Local Switching Hardware (DFC4)
  - ICS SSO Synch of L2/L3
  - FIB/ADJ, MAC, Protocol FSM, etc
Line Card Data-Plane
Redundancy Dependencies (Cross Fabric)

- Traffic between ports that are on Different Line Cards (e.g. T2/1/1 & T2/2/1) WILL be affected by Supervisor SSO events…

- No Card or Port Flaps
  ICS SSO Synch of Infrastructure

- ~50-250ms of Packet Loss
  ICS SSO Synch of L2/L3
  Loss Time = Active ➔ Standby Fabric Switch-Over & Channel Initialization
  New Cards support HW Notification
## Line Card Data-Plane

Hot Sync Fabric and Fast-Hardware Notification

<table>
<thead>
<tr>
<th>Line Card Model</th>
<th>Hot Sync Standby Fabric</th>
<th>Fast-HW Notification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6900-series</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6800-series 10G</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6700-series 10G</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6704-10G</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6800-series 1G</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6700-series 1G</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Classic</td>
<td>N/A</td>
<td>No</td>
</tr>
</tbody>
</table>

*~50ms Convergence*

*~250-300ms Convergence*
### Line Card Data-Plane

**Hot Standby Fabric Support**

<table>
<thead>
<tr>
<th>slot</th>
<th>channel</th>
<th>speed</th>
<th>module</th>
<th>fabric status</th>
<th>hotStandby support</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>40G</td>
<td>OK</td>
<td>OK</td>
<td>Y (hot)</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>40G</td>
<td>OK</td>
<td>OK</td>
<td>Y (hot)</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>20G</td>
<td>OK</td>
<td>OK</td>
<td>Y (hot)</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>20G</td>
<td>OK</td>
<td>OK</td>
<td>Y (hot)</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>20G</td>
<td>OK</td>
<td>OK</td>
<td>Y (hot)</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>20G</td>
<td>OK</td>
<td>OK</td>
<td>Y (hot)</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>20G</td>
<td>OK</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>20G</td>
<td>OK</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>20G</td>
<td>OK</td>
<td>OK</td>
<td>N/A</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>20G</td>
<td>OK</td>
<td>OK</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Line Cards:**
- WS-X6908-10G
- WS-X6748-TX
- WS-X6748-SFP
- VS-S2T-10G
- VS-S2T-10G
Line Card Data Plane Switchover

Backplane Fabric Channels Affect on Cross Module Traffic

Before Switchover

C6506

Slot 5
Active Supervisor

Slot 6
Standby Supervisor (ICS)

Slot 1
Line card

Slot 2
Line card
Line Card Data Plane Switchover

Backplane Fabric Channels Affect on Cross Module Traffic

Before Switchover

C6506

Slot 5
Active Supervisor

Slot 6
Standby Supervisor (ICS)

Slot 1
Line card

Slot 2
Line card

After Switchover

C6506

Slot 6
Active Supervisor

Slot 1
Line card

Slot 2
Line card
Line Card Data Plane Switchover

Backplane Fabric Channels Affect on Local Traffic

Before Switchover

C6506

Slot 5
Active Supervisor

Slot 6
Standby Supervisor (ICS)

Slot 1
Line card

Slot 2
Line card
Line Card Data Plane Switchover

Backplane Fabric Channels Affect on Local Traffic

Before Switchover

C6506

Slot 5
Active Supervisor

Slot 6
Standby Supervisor (ICS)

Slot 1
Line card

Slot 2
Line card

After Switchover

C6506

Slot 6
Active Supervisor

Slot 1
Line card

Slot 2
Line card
VSS Quad-Sup
Viewing Redundancy Status via CLI

VSS_4SUP# show switch virtual redundancy
My Switch Id = 1
Peer Switch Id = 2
Last switchover reason = user forced
Configured Redundancy Mode = sso
Operating Redundancy Mode = sso

Switch 1 Slot 5 Processor Information:
-----------------------------------------------
Current Software state = ACTIVE
Uptime in current state = 2 days, 18 hours, 15 minutes
Image Version = Cisco IOS Software, s2t54 Software (s2t54-ADVIPSERVICESK9-M), Version 15.1(1)WIA111.90, EARLY DEPLOYMENT ENGINEERING WEEKLY BUILD, synced to V122_49_YST273_111_101108
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Tue 02-Oct-12 14:34 by integ
  BOOT = bootdisk:s2t54-advipservicesk9-mz.SSA.150-1.WIA111.90.1;
  CONFIG_FILE =
  BOOTLDR =
  Configuration register = 0x2102
  Fabric State = ACTIVE
  Control Plane State = ACTIVE

Switch 1 Slot 6 Processor Information:
-----------------------------------------------
Current Software state = STANDBY HOT (CHASSIS)
Uptime in current state = 2 days, 18 hours, 29 minutes
Image Version = Cisco IOS Software, s2t54 Software (s2t54-ADVIPSERVICESK9-M), Version 15.1(1)WIA111.90, EARLY DEPLOYMENT ENGINEERING WEEKLY BUILD, synced to V122_49_YST273_111_101108
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Tue 02-Oct-12 14:34 by integ
  BOOT = bootdisk:s2t54-advipservicesk9-mz.SSA.150-1.WIA111.90.1;
  CONFIG_FILE =
  BOOTLDR =
  Configuration register = 0x2102
  Fabric State = ACTIVE
  Control Plane State = STANDBY

Switch 2 Slot 5 Processor Information:
-----------------------------------------------
Current Software state = STANDBY HOT (switchover target)
Uptime in current state = 2 days, 18 hours, 14 minutes
Image Version = Cisco IOS Software, s2t54 Software (s2t54-ADVIPSERVICESK9-M), Version 15.1(1)WIA111.90, EARLY DEPLOYMENT ENGINEERING WEEKLY BUILD, synced to V122_49_YST273_111_101108
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Tue 02-Oct-12 14:34 by integ
  BOOT = bootdisk:s2t54-advipservicesk9-mz.SSA.150-1.WIA111.90.1;
  CONFIG_FILE =
  BOOTLDR =
  Configuration register = 0x2102
  Fabric State = ACTIVE
  Control Plane State = STANDBY

Switch 2 Slot 6 Processor Information:
-----------------------------------------------
Current Software state = STANDBY HOT (CHASSIS)
Uptime in current state = 2 days, 18 hours, 13 minutes
Image Version = Cisco IOS Software, s2t54 Software (s2t54-ADVIPSERVICESK9-M), Version 15.1(1)WIA111.90, EARLY DEPLOYMENT ENGINEERING WEEKLY BUILD, synced to V122_49_YST273_111_101108
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Tue 02-Oct-12 14:34 by integ
  BOOT = bootdisk:s2t54-advipservicesk9-mz.SSA.150-1.WIA111.90.1;
  CONFIG_FILE =
  BOOTLDR =
  Configuration register = 0x2102
  Fabric State = ACTIVE
  Control Plane State = STANDBY
## VSS Quad-Sup File Systems

### Copying Image Before System Upgrade

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show switch virtual</code></td>
<td>Displays the virtual switch configuration.</td>
</tr>
<tr>
<td><code>copy ftp:</code></td>
<td>Initiates the file transfer command.</td>
</tr>
<tr>
<td>Address or name of remote host</td>
<td>Displays the remote host address.</td>
</tr>
<tr>
<td>Source filename</td>
<td>Specifies the source filename for the file transfer.</td>
</tr>
<tr>
<td>Destination filename</td>
<td>Specifies the destination filename for the file transfer.</td>
</tr>
</tbody>
</table>

#### VSS4Sup#show switch virtual

- **Switch mode**: Virtual Switch
- **Virtual switch domain number**: 200
- **Local switch number**: 2
- **Local switch operational role**: Virtual Switch Active
- **Peer switch number**: 1
- **Peer switch operational role**: Virtual Switch Standby

#### VSS4Sup#copy ftp: bootdisk:

1. **Address or name of remote host**: 172.26.210.138
2. **Source filename**: `s2t54-advipservicesk9-mz.SSA.150-1.WIA111.90`
3. **Destination filename**: `sk:s2t54-advipservicesk9-mz.SSA.150-1.WIA111.90`

Loading file...

#### VSS4Sup#$sk:s2t54-advipservicesk9-mz.SSA.150-1.WIA111.90 ics-bootdisk:

- **Destination filename**: `sk:s2t54-advipservicesk9-mz.SSA.150-1.WIA111.90`

Copy in progress...

#### VSS4Sup#$sk:s2t54-advipservicesk9-mz.SSA.150-1.WIA111.90 swl-slot5-bootdisk:

- **Destination filename**: `sk:s2t54-advipservicesk9-mz.SSA.150-1.WIA111.90`

Copy in progress...

#### VSS4Sup#$dvipservicesk9-mz.SSA.150-1.WIA111.90 swl-slot6-slavebootdisk:

- **Destination filename**: `dvipservicesk9-mz.SSA.150-1.WIA111.90`

Copy in progress...
VSS Supervisor Redundancy Comparison

- **Quad-Sup SSO**
  - 1:1 (active/standby) Supervisor Redundancy for single and dual attached devices
  - Automated recovery from Supervisor failure
  - SSO switchover is typically 50ms – 200ms

- **Quad-Sup Uplink Forwarding**
  - 1+1 (active/active) Supervisor Redundancy for dual attached devices
  - Automated recovery from Supervisor failure
  - Deterministic outage duration for single attached devices

- **Single Supervisor (Dual Sup)**
  - 1+1 (active/active) Supervisor Redundancy for dual attached devices
  - Requires manual Supervisor replacement
  - Non-deterministic outage duration for single attached devices
Migrate to VSS Quad Sup SSO

Key Steps in migrating to Quad Sup SSO

• Upgrade the existing Sup2T VSS to version 15.1(1)SY1 or above
• Establish a console connection for each supervisor module in the VSS
• Prepare the ICS supervisor module to boot the same image version as the active VSS
• Insert the redundant supervisor module into the chassis (it does not matter which VSS chassis the redundant supervisor is inserted into first, the VSS active or VSS standby)
• Verify the newly inserted supervisor boots as the ICS
• Configure and connect the ICS supervisor TenGigabit uplink ports into the VSL (optional, but recommended for configuration with an ICS in each chassis)
Migrate from VSS to VS4O
Cross Connect the Sup2T Uplinks
# In-Chassis Supervisor Boot Behavior Scenarios

<table>
<thead>
<tr>
<th>In Chassis Standby</th>
<th>In Chassis Active</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Active Supervisor in VSS Mode - Running Image supporting VS40. (15.1(1)SY1 or newer)</strong></td>
</tr>
<tr>
<td>Standby in VSS mode running VS4O capable image (15.1(1)SY1 or newer)</td>
<td>boots as VS4O In-chassis SSO Standby Hot</td>
</tr>
<tr>
<td>Standby in Standalone mode running VS4O capable image (15.1(1)SY1 or newer)</td>
<td>ICS detects ICA in VSS mode and automatically sets switch number then resets and boots as VS4O In-chassis SSO Standby Hot</td>
</tr>
<tr>
<td>Standby booting with 15.1(1)SY or older image in a standalone default config</td>
<td>ICS will start to boot IOS and recognize it is in an unsupported ICS config and drop to rommon</td>
</tr>
<tr>
<td>Standby booting with 15.1(1)SY or older image in a VSS config</td>
<td>ICS will start to boot IOS and recognize it is in an unsupported ICS config and drop to rommon</td>
</tr>
<tr>
<td>ICS with config-register 0x2102</td>
<td>ICS boots to rommon</td>
</tr>
</tbody>
</table>
VSS Quad-Sup SSO

Best Practices

- Always use at least one uplink from each Supervisor as part of the VSL
- Consider using all the Supervisor uplink ports in the VSL (4 per chassis)
- If using all 4 Supervisor uplinks (per chassis) “swap the 5s” or “swap the 4s” in order to maintain 20Gbps VSL, even during a Supervisor fail event or reload event
- Connect uplink and downlink on local Line Cards (if possible), this will minimize traffic disruption across Supervisor switchover event
- Must explicitly configure NSF (or NSR if supported) for each routing protocol, to provide minimum disruption to L3 routed interfaces
- Use DFC enabled linecards with 512MB of available memory in order to minimize Line Card reload time during EFSU (warm-reload)
- Be sure to copy the system image file to all Supervisor file systems in the same location
VSS Quad-Sup SSO Key Takeaways

• VSS Quad-Sup SSO provides
  – Automated and sub-second recovery from a Sup fail event
  – Sub-second recovery maintains 100% bandwidth for the VSS
  – Maintains network availability for single attached devices

• New Staggered EFSU process reduces the outage time associated with linecard reloads

• Quad-Sup SSO is only supported on Sup2T, available in 15.1(1)SY1

• Quad-Sup Uplink Forwarding is only supported on Sup720-10G
White Paper describes VSS Quad Sup SSO benefits, architecture and migration steps

VSL Design Considerations
VSL Design Considerations

- VSL Path Diversification
- VSL Bandwidth Sizing
- VSL Quality of Service

Borderless Networks: Medium Enterprise Design Profile

VSL Design
Path Diversification (Dual-Sup Design Option #1)

- Minimum of 2 VSL paths provides protection from Port and SFP failures
- Diverse physical paths provides protection from physical layer failures
- No additional VSL-capable Line Cards are required (Minimal Cost)
VSL Design
Path Diversification (Dual-Sup Design Option #2)

- Minimum of 2 VSL paths provides protection from Port and SFP failures
- Separate Line Card provides protection from interface failures on single Supervisor
- Diverse physical paths provides protection from physical layer failures
- Requires a VSL-capable Line Card
VSL Design
Path Diversification (Quad-Sup Design Option #1)

- Maintains 20Gbps VSL bandwidth in event of a Supervisor failure
- Maintains at least 1 local VSL path to the Active Supervisor (no matter which Supervisor becomes Active)
- No additional VSL-capable Line Cards are required (Minimal Cost)
- Supports Staggered Mode upgrade with Sup2T Quad Sup SSO
VSL Design
Path Diversification (Quad-Sup Design Option #2)

- Maintains 30Gbps VSL bandwidth in the event of a Supervisor failure
- Maintains at least 1 local VSL path to the Active Supervisor (no matter which Supervisor becomes Active)
- Provides additional protection against multiple Supervisor failures (compared to option #1)
- Requires a VSL-capable Line Card
Virtual Switch Link

Built In QoS

- **Virtual Switch Link interfaces are restricted from QoS policy changes**
  - Class of Service based queuing is automatically added to the VSL port channel interfaces on Sup720-10G, this is not applicable on systems (trust cos)
  - Default CoS to Queue mapping is enforced
  - Interface Maximum Transmission Unit (MTU) size is automatically set to 9216 bytes

- **Critical control traffic is automatically marked and receives priority queuing**
  - Control traffic is set with CoS=5 BPDU=1
  - Marked in VSL Header (VSH)

```
interface Port-channel11
no switchport
no ip address
switch virtual link 1
mls qos trust cos
no mls qos channel-consistency
```

Sup720-10G Example
Supervisor uplink ports can be configured in either of two modes

- **Normal mode**
  - All 1GE and 10GE ports are available
  - Shared queuing structure
  - TX 1p3q4t / RX 2q4t

- **10G-only mode**
  - Only the 10GE ports are available
  - Additional queues and buffers are allocated to the 10G ports
  - TX 1p7q4t / RX 8q4t

Adjust Etherchannel queuing requirements as needed

- “no mls qos channel-consistency” removes the requirement that all ports in an etherchannel bundle have the same queuing structure

```
interface Port-channel1
no switchport
no ip address
switch virtual link 1
mls qos trust cos
no mls qos channel-consistency
```
VSS In-Service Software Upgrades
VSS Software Upgrades
Using the In Service Software Upgrade (ISSU) Infrastructure

The ISSU Process in VSS is referred to as Enhanced Fast Software Upgrade (EFSU)
**VSS Software Upgrade**

**Full Image Upgrade Bandwidth Availability Graph**

**Fast Software Upgrade (FSU) Bandwidth Availability**

- At step 3 during RPR switchover, bandwidth will be dropped to 0% for 1-2 minutes.

**Enhanced Fast Software Upgrade (EFSU) Bandwidth Availability**

- With EFSU, a minimum of 50% bandwidth is available throughout the software upgrade process.
In Service Software Upgrades
Enhanced Fast Software Upgrade (EFSU)

The Solution
VSS + EFSU

Simplified Upgrade
process with only
Four easy steps

Increased Availability
50% bandwidth always
available neighbors are
dual-attached

Deterministic Recovery
Supports Quad-Sup ISSU / EFSU designs

Switch 1
Version 2
VSS Standby Hot
WS-X6908-10G
Access Switch or Blades

Switch 2
Version 2
VSS Standby Hot
WS-X6908-10G
Access Switch or Blades

Aggregate Bandwidth of both VSS chassis

With EFSU, a minimum of 50% bandwidth is available throughout the software upgrade process

Load 1
Run 2
Accept 3
Commit 4

Version 1
Version 2
Version 1
Version 2

136
Cisco Public
VSS Software Upgrade
EFSU - Full Image Upgrade Process

Switch 1
<table>
<thead>
<tr>
<th>LC</th>
<th>LC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Standby</td>
</tr>
</tbody>
</table>

Switch 2
<table>
<thead>
<tr>
<th>LC</th>
<th>LC</th>
</tr>
</thead>
</table>

ISSU LoadVersion

Switch 1
<table>
<thead>
<tr>
<th>LC</th>
<th>LC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Standby</td>
</tr>
</tbody>
</table>

Switch 2
<table>
<thead>
<tr>
<th>LC</th>
<th>LC</th>
</tr>
</thead>
</table>

ISSU RunVersion

Switch 1
<table>
<thead>
<tr>
<th>LC</th>
<th>LC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standby</td>
<td>Active</td>
</tr>
</tbody>
</table>

Switch 2
<table>
<thead>
<tr>
<th>LC</th>
<th>LC</th>
</tr>
</thead>
</table>

ISSU CommitVersion

Switch 1
<table>
<thead>
<tr>
<th>LC</th>
<th>LC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standby</td>
<td>Active</td>
</tr>
</tbody>
</table>

Switch 2
<table>
<thead>
<tr>
<th>LC</th>
<th>LC</th>
</tr>
</thead>
</table>

= Old Version
= New Version
VSS Software Upgrade

EFSU - Initializing Standby With New Software...

**After the “issu loadversion” command, the Standby Chassis will reload to boot the new image...**

```bash
VSS# issu loadversion sup-bootdisk:New_image
VSS# show issu state

Slot = 22
RP State = Active
**ISSU State = Load Version**
Boot Variable = bootdisk:Old_image,12

Slot = 40
RP State = Standby
**ISSU State = Load Version**
Boot Variable = bootdisk:New_image,12;sup-bootdisk:Old_image,12
```
VSS Software Upgrade

EFSU - Switchover to Standby to Run New Software...

After the “issu runversion” command the Active Supervisor will reload, thus causing the VSS Standby to transition to VSS Active...

```
issu runversion standby-switch-id / slot [standby-image-new]
```

VSS# issu runversion
This command will reload the Active unit. Proceed? [confirm]

VSS# show issu state

```
Slot = 40
RP State = Active
ISSU State = Run Version
Boot Variable = New_image,12;bootdisk:Old_image,12

Slot = 22
RP State = Standby
ISSU State = Run Version
Boot Variable = bootdisk:Old_image,12
```

Rollback timers get activated as soon as "issu runversion" command is issued. It provides a window of time to verify the new software functionality.

Users issue "issu acceptversion" to proceed with the new software image or "issu abortversion" to go back to the previous version.

VSS#  show issu rollback-timer
Rollback Process State = In progress
Configured Rollback Time = 45:00
Automatic Rollback Time = 42:02

VSS(config)# issu set rollback-timer ?
WORD Rollback timer in hh:mm:ss or <seconds> format

Rollback timer can be set between zero seconds and two hours.

Setting the rollback to zero effectively disables the timer.
Enter the "issu acceptversion" command to stop the rollback timer. This allows a trial period where the system can be tested with the new image.

```
issu acceptversion active-switch-id / slot [active-image-new]
```

### VSS# issu acceptversion

% Rollback timer stopped. Please issue the commitversion command.

### VSS# show issu state

```
Slot = 40
  RP State = Active
  ISSU State = Run Version
  Boot Variable = bootdisk:New_image,12;bootdisk:Old_image,12

Slot = 22
  RP State = Standby
  ISSU State = Run Version
  Boot Variable = bootdisk:Old_image,12
```

Only features that are common to both software versions will be enabled during the "ISSU Run Version" stage.
After the “issu commitversion” command, the Standby Supervisor will reload to boot new image...

```
issu commitversion standby-switch-id / slot-number [standby-image-new]
```

```
VSS# issu commitversion  
10:54:37: %PFINIT-SP-5-CONFIG_SYNC: Sync'ing the startup configuration to the standby Router. [OK]

00:32:35: %SYS-SW1_SPSTBY-5-RELOAD: Reload requested - From Active Switch (Reload peer unit).

VSS# show issu state  
     Slot = 40  
      RP State = Active  
   ISSU State = Init  
  Boot Variable = bootdisk:New_image12; Old_image,12

     Slot = 22  
      RP State = Standby  
   ISSU State = Init  
  Boot Variable = bootdisk:New_image,12; Old_image,12
```
EFSU for VSS Quad-Sup SSO

• **New “Staggered” EFSU mode upgrades one Supervisor at a time**
  – Overall effective outage for an individual chassis is greatly minimized
  – Staggered mode reloads the Supervisor modules separately from Line Cards
  – Line Cards must reload (to boot / run the new software), during the process
  – Optional “Tandem” mode will upgrade both Supervisors modules per chassis (same as process with Dual Sup VSS)

• **Staggered EFSU mode is the system default for Sup2T**

• **MUST use at least one VSL port from each Supervisor module!**
  – Needed to maintain VSL (at least 1 connection) during Line Card reloads
  – Recommend using all four Sup uplinks for the VSL, in cross-connection
Staggered Upgrade with Quad-Sup SSO

ISSU Loadversion (Step 1)

A – V1
ICS – V1

Switch ID 1

ISSU State = INIT

#issu loadversion bootdisk:v1.bin

Switch ID 2

S – V1
ICS – V1

ISSU State = LV

A – V1
ICS – V1

Switch ID 1

S – V1
ICS – V2

Switch ID 2
Staggered Upgrade with Quad-Sup SSO
ISSU Loadversion (Step 2)

This step occurs automatically, no CLI input required

VSS Standby ICA (2,1) reloads causing an SSO switchover event, linecards then reload with new version to match the new ICA (2,2)
Staggered Upgrade with Quad-Sup SSO

ISSU Runversion

ISSU State = LV

ISSU State = RV

#issu runversion
Staggered Upgrade with Quad-Sup SSO
ISSU Commitversion (Step 1)

ISSU State = RV

#issu commitversion

ISSU State = CV1
Staggered Upgrade with Quad-Sup SSO
ISSU Commitversion (Step 2)

- Linecards in Switch 1 reload with new version when the new ICA running V2 goes active
- Linecards perform pre-download of image if the Linecard is capable (requires 512MB memory)
VSS Software Upgrade

EFSU Time - Staggered vs Tandem Mode

**Tandem Upgrade**

1. **loadversion**
2. **runversion**
3. **acceptversion**
4. **commitversion**

Each step takes ~10 min chassis reload time.

**Staggered Upgrade**

1. **loadversion**
2. **runversion**
3. **acceptversion**
4. **commitversion**

Each step takes ~1-2 min card reload time.
Quad Sup EFSU Staggered Mode
Requires a VSL Connection Between All Supervisor Modules

VSS#
*Apr 18 05:11:32.897: SW1: Cannot proceed with staggered ISSU upgrade as VSL connection requirement is not met. Please issue Config cli no issu upgrade staggered to disable staggered upgrade
ISSU Show Commands

```
VSS4Sup#show issu state
The system is configured to be upgraded in staggered mode.
4 nodes are found to be online.
Summary: the system will be upgraded in staggered mode.

Slot = 1/5
  RP State = Active
  ISSU State = Init
  Boot Variable = bootdisk:s2t54-advipservicesk9-mz.SSA.150-1.WIA111.90,1;

Slot = 2/5
  RP State = Standby
  ISSU State = Init
  Boot Variable = bootdisk:s2t54-advipservicesk9-mz.SSA.150-1.WIA111.90,1;

Slot = 1/6
  RP State = Active-ICS
  ISSU State = Init
  Boot Variable = bootdisk:s2t54-advipservicesk9-mz.SSA.150-1.WIA111.90,1;

Slot = 2/6
  RP State = Standby-ICS
  ISSU State = Init
  Boot Variable = bootdisk:s2t54-advipservicesk9-mz.SSA.150-1.WIA111.90,1;
```
ISSU Image Version Compatibility

• BOTH software versions MUST support the ISSU infrastructure AND both images must be “compatible” for the process to proceed in SSO redundancy mode

• Check the Cisco Feature Navigator and / or the Software Release Notes, for listing of compatible releases

• In general Cisco will attempt to provide ISSU compatibility for releases within an 18 month time frame of each other
ISSU Image Compatibility Rules

• **18 month window release time frame**
  – exceptions for major releases or other significant changes between releases

• **ISSU requires the same software licenses between images**
  – IP Base to IP Base
  – Advanced IP Services to Advanced IP Services
  – Universal_lite to Universal_lite

• **Not supported from a k9 to a non-k9 image, or vice versa.**
ISSU Compatibility Matrix
Latest Known Compatible Versions – Stored Locally

VSS# `show issu comp-matrix stored`

Number of Matrices in Table = 1

(1) Matrix for s2t54-ADVIPSERVICESK9-M(10) - s2t54-ADVIPSERVICESK9-M(10)

Start Flag (0xDEADBABE)

<table>
<thead>
<tr>
<th>Peer Version</th>
<th>Compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)SY</td>
<td>Incomp(1)</td>
</tr>
<tr>
<td>15.0(1)SY1</td>
<td>Incomp(1)</td>
</tr>
<tr>
<td>15.0(1)SY2</td>
<td>Incomp(1)</td>
</tr>
<tr>
<td>15.0(1)SY3</td>
<td>Incomp(1)</td>
</tr>
<tr>
<td>15.0(1)SY4</td>
<td>Incomp(1)</td>
</tr>
<tr>
<td>15.1(1)SY</td>
<td>Dynamic(0)</td>
</tr>
<tr>
<td><strong>15.1(1)SY1</strong></td>
<td><strong>Comp(3)</strong></td>
</tr>
</tbody>
</table>

VSS#
ISSU Compatibility Matrix @ Cisco.com

VSS & EFSU Important Points

- EFSU supported on Sup720-10G based systems with SXI train and newer
- EFSU supported on Sup2T based systems with 15.0(1)SY and newer
- Dual-homed connectivity is required for minimal traffic disruption with EFSU
  - Single-homed devices will experience an outage when the attached chassis reloads
- **Software images files** must be “ISSU compatible” (not VSS specific)
  - Must be the same image types, meaning “Native to Native” or “Modular to Modular”
  - For Modular images, both images must use the same installation method, therefore “installed mode” or “binary mode”
  - The software feature sets must be the same between the two software image files
- **Always Check the Release Notes** for hardware and software compatibility
The Catalyst 4500-E and 4500-X support ISSU upgrades in VSS mode
- Similar to what is supported on the Catalyst 6500
- Traditional four step ISSU upgrade, described as the “manual method”

Catalyst 4500-E and 4500-X support “ISSU Changeversion” feature, using a single command to execute the upgrade
- single command ISSU upgrade “automatic method”

ISSU Changeversion performs the entire ISSU upgrade process, without user intervention
- supports scheduling option
- skips the intermediate trial phase upgrade, faster overall process
A Virtual Switch Domain ID is allocated during the conversion process and represents the logical grouping the 2 physical chassis within a VSS

It is possible to have multiple VS Domains throughout the network...

Use a UNIQUE VSS Domain-ID for each VSS Domain throughout the network!

Various protocols use Domain-IDs to uniquely identify each pair.
VSS Architecture
Router MAC Address Assignment

In a Virtual Switching System, there is only **one** router MAC address to represent both physical chassis as a single logical device.

By default, the MAC address allocated to the Virtual Switching System is taken from the first Active Switch burnt-in MAC-address, which is negotiated at system initialization.

Regardless of either switch being brought down or up in the future, the same MAC address will be retained so that neighboring network nodes and hosts **do not need to re-learn a new address**.

Recommendation is to use the virtual mac-address option. This eliminates the possibility of a duplicate MAC address in case the original Supervisor is ever reused within the same network.
VSS Architecture
Virtual Router MAC Address Assignment

Instead of using the default (chassis) mac-address assignment, from 12.2(33)SXH2 onwards a “virtual mac-address” can be specified:

VSS(config-vs-domain)# switch virtual domain 10
VSS(config-vs-domain)# mac-address use-virtual
Configured Router mac address is different from operational value. Change will take effect after config is saved and the entire Virtual Switching System (Active and Standby) is reloaded.

VSS# show interface vlan 1
Vlan1 is up, line protocol is up
   Hardware is EtherSVI, address is 0008.e3ff.fc0a (bia 0008.e3ff.fc0a)

Remember: Router MAC is how PFC/DFC knows a packet is destined to L3 Interface

The virtual mac-address is assigned from a reserved pool of MAC addresses with the VSS Domain ID.
The reserved pool is 0008.e3ff.fc00 to 0008.e3ff.ffff
Virtual Switching System
Dual-Attach Whenever Possible

- Dual-Attach connect to neighbor devices whenever possible!
- EtherChannel and CEF load-balancing algorithms have been modified for VSS to always favor locally attached interfaces
- With a Dual-Attached network design
  - Data traffic will not traverse the VSL under normal conditions, only control traffic will traverse the VSL
  - Data traffic will traverse the VSL only if there is a failure event and no local interfaces are available
VSL Bandwidth Sizing
How Many Links are Needed in the VSL?

- **VSL is a 10G or 40G EtherChannel**
  - Supports up to eight links

- **Consider possible failure scenarios**
  - Fiber, SFP, Interface,
  - Line Card, Supervisor,
  - Up/Downstream Switch

- Consider the VSL bandwidth needed for Service Modules

- Consider the VSL bandwidth needed for SPAN sessions
**VSS High Availability**

Non Stop Forwarding in VSS

### EIGRP

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

Router# **show ip protocol**
*** IP Routing is NSF aware ***
Routing Protocol is "eigrp 100 100"

- **EIGRP NSF-aware** route hold timer is 240s
- **EIGRP NSF enabled**

### OSPF

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

Router# **show ip ospf**
Routing Process "ospf 100" with ID 10.120.250.4
Start time: 00:01:37.484, Time elapsed: 3w2d

- **EIGRP NSF-aware** route hold timer is 240s
- **EIGRP NSF enabled**

<snip>

**Remember:** **Non-Stop Forwarding (NSF) is Required** for sub-second Supervisor Switchover convergence, with L3 Routing Protocols
VSS High Availability
Sub-second Protocol Timers and NSF/SSO

- NSF is intended to provide availability through route convergence avoidance
- Fast IGP timers are intended to provide availability through fast route convergence
- In an NSF environment, a dead timer must be greater than:
  SSO recovery + Routing Protocol restart + time to send first hello
- Applicable in VSS and Quad Sup VSS mode
- Recommendation –
  Do NOT configure aggressive timers for Layer 2 protocols, i.e. Fast UDLD
  Do NOT configure aggressive timers for Layer 3 protocols, i.e. OSPF Fast Hello, BFD etc.
  Keep all protocol timers at default settings
VSS High Availability
Dual-Active Detection

Recommendations:

- Enable multiple methods of VSS Dual-Active Detection:
  - FEX MEC with ePAgP MEC
  - VSLP Fast Hello with FEX MEC
- Connect multiple redundant VSL links, to prevent Dual-Active
- Enable ePAgP to Core-layer (if the Access-layer is not ePAgP or FEX capable)
If you need to reload the entire Virtual Switching System (both chassis), the command “reload” can be used to accomplish this task…

VSS# reload
Warning: This command will reload the entire Virtual Switching System (Active and Standby Switch).
Proceed with reload? [confirm]

1d04h: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.

***
*** --- SHUTDOWN NOW ---
***

1d04h: %SYS-5-RELOAD: Reload requested
System Bootstrap, Version 8.5(1)
Copyright (c) 1994-2006 by cisco Systems, Inc.
Cat6k-Sup720/SP processor with 1048576 Kbytes of main memory
NEW command has been introduced to reload a SINGLE VSS member switch.

VSS# redundancy reload ?
peer
shelf <1-2>

vss# redundancy reload shelf 2
Reload the entire remote shelf [confirm]
Preparing to reload remote shelf

VSS# redundancy force-switchover
This will reload the active unit and Force switchover to standby [confirm]

vss#
Revert from VSS to Standalone
Quick way to revert from VSS to Standalone mode

<table>
<thead>
<tr>
<th>VSS# erase nvram:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]</td>
</tr>
<tr>
<td>*Jul 2 10:12:02: %SYS-SW1_SP-7-NV_BLOCK_INIT: Initialized the geometry of nvram</td>
</tr>
<tr>
<td>*Jul 2 10:12:04: %SYS-SW2_SPSTBY-7-NV_BLOCK_INIT: Initialized the geometry of nvram</td>
</tr>
<tr>
<td>VSS#</td>
</tr>
<tr>
<td>VSS#</td>
</tr>
<tr>
<td>*Jul 2 10:12:05: %VS_GENERIC-SW2_SPSTBY-5-VS_SWITCH_NUMBER_CHANGE: Switch_number getting changed from 2 to 0.</td>
</tr>
<tr>
<td>*Jul 2 10:12:05: %VS_GENERIC-SW1_SP-5-VS_SWITCH_NUMBER_CHANGE: Switch_number getting changed from 1 to 0.</td>
</tr>
</tbody>
</table>

• Use the “Erase NVRAM” exec level command
  – Will erase the startup-config and also set the VSS switch number ROMMON variables on both switches to default value of 0

• Reload the chassis after the “Erase NVRAM”, and each Supervisor will boot as a standalone switch, with a default configuration
VSS Deployment Best Practices

<table>
<thead>
<tr>
<th>DO…</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Use a unique Domain ID for multiple VSS in the same network</td>
</tr>
<tr>
<td>✓ Save backup configuration file to all Supervisor file systems in the same location, for example - both Switch 1 &amp; Switch 2 bootdisk:</td>
</tr>
<tr>
<td>✓ Use a minimum of one Supervisor uplink port for the VSL, this provides for faster VSL bring up.</td>
</tr>
<tr>
<td>✓ Dual-home connected devices whenever possible, use L2 or L3 Multi-Chassis Etherchannel or L3 ECMP</td>
</tr>
<tr>
<td>✓ Enable ePAgP and/or VSLP Fast Hello Dual Active Protocol.</td>
</tr>
<tr>
<td>✓ Enable NSF or NSR under all L3 Routing protocols</td>
</tr>
</tbody>
</table>
VSS Deployment Best Practices Con’t

**DO NOT ....**

× **Do NOT Tune VSLP timers!**  
(unless instructed to do so by Cisco)

× **Do NOT Use VSS preemption!**  
(preemption has been removed from SXJ and SY release trains)

× **Do NOT Issue “shutdown” on VSL port-channel interface!**  
This creates a config mismatch. If you want to test dual-active detection mechanisms, simply disconnect the VSL cables. That will create a realistic failure scenario without causing the configurations to get out of sync.

× **Do Not Change VSL hashing algorithm, in production!**  
This requires a shut / no shut on of the VSL port-channel (see above). Shutting down VSL will cause traffic disruption and dual-active scenario.
Summary
Benefit 1: Simple Network Design

- Redundant Topology without First Hop Redundancy Protocols
- No Spanning-Tree Blocking Ports
- Single Control Plane and Management Interface
- Reduces the total number of L3 and L2 protocol peers
Benefit 2: Scales System Capacity

- **Active-Active Fabrics** group resources and activates all available bandwidth

- **Increased Access-layer Uplink Bandwidth**
  (No Spanning-Tree Blocking Ports)

- Enables dual-homed standards-based Link Aggregation for Server and Appliance connectivity
Benefit 3: Increase Network Availability

- Inter-chassis Stateful Switchover enables real-time applications to continue without disruption
- EtherChannel based link resiliency provides sub-second recovery
- Simplified network designs reduces human error in network operations
References

- Borderless Networks: Medium Enterprise Design Profile

- Deployment and Support
  
  Cisco Catalyst 6500 Virtual Switching System Deployment Best Practices

  Migrate Standalone Cisco Catalyst 6500 Switch to Cisco Catalyst 6500 Virtual Switching System

  Troubleshoot Packet Flow in Cisco Catalyst 6500 Series Virtual Switching System 1440

- VSS White Paper

- Catalyst 6500 Series Configuration Guide

- Catalyst 4500 Series Configuration Guide
Call to Action

• Visit the World of Solutions for
  – Cisco Campus
  – Walk in Labs
  – Technical Solution Clinics

• Meet the Engineer

• Lunch time Table Topics

• DevNet zone related labs and sessions

• Recommended Reading: for reading material and further resources for this session, please visit www.pearson-books.com/CLMilan2015
Complete Your **Online Session Evaluation**

- Please complete your online session evaluations after each session. Complete 4 session evaluations & the Overall Conference Evaluation (available from Thursday) to receive your Cisco Live T-shirt.

- All surveys can be completed via the Cisco Live Mobile App or the Communication Stations
TOMORROW starts here.