Configuring Virtual Switching Systems

This chapter describes how to configure a virtual switching system (VSS) for the Catalyst 6500 series switch.

Note

For complete syntax and usage information for the commands used in this chapter, see these publications:


This chapter consists of these sections:

- Understanding Virtual Switching Systems, page 4-1
- VSS Configuration Guidelines and Restrictions, page 4-22
- Configuring Virtual Switching Systems, page 4-22

Understanding Virtual Switching Systems

These sections describe virtual switching systems:

- Virtual Switching System Overview, page 4-2
- Virtual Switching System Redundancy, page 4-7
- Multichassis EtherChannels, page 4-10
- Packet Handling, page 4-12
- System Monitoring, page 4-16
- Dual-Active Detection, page 4-18
- Virtual Switching System Initialization, page 4-19
Virtual Switching System Overview

Network operators increase network reliability by configuring switches in redundant pairs and by provisioning links to both switches in the redundant pair. Figure 4-1 shows a typical network configuration. Redundant network elements and redundant links can add complexity to network design and operation. Virtual switching simplifies the network by reducing the number of network elements and hiding the complexity of managing redundant switches and links.

A virtual switching system (VSS) combines a pair of Catalyst 6500 series switches into a single network element. The virtual switching system manages the redundant links, which externally act as a single port channel.

The virtual switching system simplifies network configuration and operation, by reducing the number of Layer 3 routing neighbors and by providing a loop-free Layer 2 topology.

Figure 4-1 Typical Network Design

The following sections present an overview of the VSS. These topics are covered in detail in subsequent chapters:

- **Key Concepts**, page 4-2
- **VSS Functionality**, page 4-4
- **Hardware Requirements**, page 4-6
- **Understanding VSS Topology**, page 4-7

Key Concepts

The virtual switching system incorporates the following key concepts:

- **Virtual Switching System**, page 4-3
- **Active and Standby Chassis**, page 4-3
- **Virtual Switch Link**, page 4-3
- **Multichassis EtherChannel**, page 4-4
Virtual Switching System

A virtual switching system (VSS) combines a pair of switches into a single network element. For example, a VSS in the distribution layer of the network interacts with the access and core networks as if it were a single switch. See Figure 4-2.

An access switch connects to both chassis of the VSS using one logical port channel. The VSS manages redundancy and load balancing on the port channel. This capability enables a loop-free Layer 2 network topology. The virtual switching system also simplifies the Layer 3 network topology, because the VSS reduces the number of routing peers in the network.

Figure 4-2 Virtual Switching System in the Distribution Network

Active and Standby Chassis

When you create or restart a VSS, the peer chassis negotiate their roles. One chassis becomes the active chassis, and the other chassis becomes the standby.

The active chassis controls the VSS. It runs the Layer 2 and Layer 3 control protocols for the switching modules on both chassis. The active chassis also provides management functions for the VSS, such as line card online insertion and removal (OIR) and the console interface.

The active and standby chassis perform packet forwarding for ingress data traffic on their locally hosted interfaces. However, the standby chassis sends all control traffic to the active chassis for processing.

Virtual Switch Link

For the two chassis of the VSS to act as one network element, they need to share control information and data traffic.

The virtual switch link (VSL) is a special link that carries control and data traffic between the two chassis of a virtual switching system, as shown in Figure 4-3. VSL is implemented as an EtherChannel with up to eight links. VSL gives control traffic higher priority than data traffic so that control messages are never discarded. Data traffic is load balanced among the VSL links by the EtherChannel load-balancing algorithm.
Understanding Virtual Switching Systems

**Figure 4-3  Virtual Switch Link**

Multichassis EtherChannel

An EtherChannel (also known as a port channel) is a collection of two or more physical links that combine to form one logical link. Layer 2 protocols operate on the EtherChannel as a single logical entity.

A multichassis EtherChannel (MEC) is a port channel that spans the two chassis of a virtual switching system. The access switch views the MEC as a standard port channel. See Figure 4-4.

The virtual switching system supports a maximum of 128 EtherChannels on one VSS. This limit applies to the combined total of regular EtherChannels and MECs. Because VSL requires two EtherChannel numbers (one for each chassis), there are 126 user-configurable EtherChannels.

**Figure 4-4  Virtual Switching System with MEC**

VSS Functionality

The following sections describe the main functionality of virtual switching systems:

- **Redundancy and High Availability, page 4-5**
- **Packet Handling, page 4-5**
- **System Management, page 4-5**
- **Interface Naming Convention, page 4-5**
- **Software Features, page 4-5**
Redundancy and High Availability

In a VSS, supervisor engine redundancy operates between the active and standby chassis. The peer chassis exchange configuration and state information across the VSL and the standby supervisor engine runs in hot standby mode.

The standby chassis monitors the active chassis using the VSL. If it detects failure, the standby chassis initiates a switchover and takes on the active role. When the failed chassis recovers, it takes on the standby role.

If the VSL fails completely, the standby chassis assumes that the active chassis has failed, and initiates a switchover. After the switchover, if both chassis are active, the dual-active detection feature detects this condition and initiates recovery action. For additional information about dual-active detection, see the “Dual-Active Detection” section on page 4-18.

Packet Handling

The active supervisor engine runs the Layer 2 and Layer 3 protocols and features for the virtual switching system (VSS) and manages the DFC line cards for both chassis.

The VSS uses VSL to communicate protocol and system information between the peer chassis and to carry data traffic between the chassis when required.

Both chassis perform packet forwarding for ingress traffic on their interfaces. If possible, ingress traffic is forwarded to an outgoing interface on the same chassis to minimize data traffic that must traverse the VSL.

Because the standby chassis is actively forwarding traffic, the active supervisor engine distributes updates to the standby supervisor engine PFC and all standby chassis DFCs.

System Management

The active supervisor engine acts as a single point of control for the virtual switching system. For example, the active supervisor engine handles OIR of switching modules on both chassis. The active supervisor engine uses VSL to send messages to and from local ports on the standby chassis.

The command console on the active supervisor engine is used to control both chassis. In virtual switch mode, the command console on the standby supervisor engine blocks attempts to enter configuration mode.

The standby chassis runs a subset of system management tasks. For example, the standby chassis handles its own power management.

Interface Naming Convention

In VSS mode, interfaces are specified using switch number (in addition to slot and port), because the same slot numbers are used on both chassis. For example, command `interface 1/5/4` specifies port 4 of the switching module in slot 5 of switch 1. The command `interface 2/5/4` specifies port 4 on the switching module in slot 5 of switch 2.

Software Features

With some exceptions, the virtual switching system has feature parity with standalone Catalyst 6500 series switch (12.2(33)SXH release). Major exceptions include:

- The virtual switching system does not support MPLS or IPv6.
- The virtual switching system does not support supervisor engine redundancy within the chassis.
Understanding Virtual Switching Systems

Hardware Requirements

The following sections describe the hardware requirements of a virtual switching system:

- Chassis and Modules, page 4-6
- VSL Hardware Requirements, page 4-6
- PFC and DFC Requirements, page 4-6
- Other Modules, page 4-7

Chassis and Modules

Table 4-1 describes the hardware requirements for the VSS chassis and modules.

Table 4-1  Virtual Switching System Hardware Requirements

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Count</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis</td>
<td>2</td>
<td>The virtual switching system is available on chassis that supports VS-S720-10G supervisor engines and WS-X6708-10GE switching modules.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong>  The two chassis do not need to be identical.</td>
</tr>
<tr>
<td>Supervisor Engines</td>
<td>2</td>
<td>The virtual switching system requires Supervisor Engine 720 with 10-Gigabit Ethernet ports. You must use either two VS-S720-10G-3C or two VS-S720-10G-3CXL supervisor engine modules.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The two supervisor engines must match exactly.</td>
</tr>
<tr>
<td>Switching Modules</td>
<td>2+</td>
<td>The virtual switching system requires 67xx series switching modules.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The virtual switching system does not support classic, CEF256 or dCEF256 switching modules. In virtual switch mode, unsupported switching modules remain powered off.</td>
</tr>
</tbody>
</table>

VSL Hardware Requirements

The VSL EtherChannel supports only 10-Gigabit Ethernet ports. The 10-Gigabit Ethernet port can be located on the supervisor engine module or on a WS-X6708-10GE-3C or WS-X6708-10GE-3CXL switching module.

We recommend that you use both of the 10-Gigabit Ethernet ports on the supervisor engines to create the VSL between the two chassis.

You can add additional physical links to the VSL EtherChannel by using the 10-Gigabit Ethernet ports on WS-X6708-10GE switching modules.

PFC and DFC Requirements

The virtual switching system supports DFC3C or DFC3CXL hardware and does not support DFC3A/3B/3BXL hardware.

If any switching module in the VSS is provisioned with DFC3C, the whole VSS must operate in PFC3C mode. If a 67xx series switching module with a DFC3A/3B/3BXL is inserted in the chassis of a VSS, the module will remain unpowered, because VSS supports only DFC3C and DFC3CXL.
If the supervisor engines are provisioned with PFC3C, the VSS will automatically operate in 3C mode, even if some of the line cards are 3CXL. However, if the supervisor engines are provisioned with PFC3CXL, but some of the line cards are 3C, you need to configure the virtual switching system to operate in 3C mode. The `platform hardware vsl pfc mode pfc3c` configuration command sets the system to operate in 3C mode after the next restart. See the “SSO Dependencies” section on page 4-20 for further details about this command.

**Other Modules**

Only the NAM service modules are supported (WS-SVC-NAM-1 and WS-SVC-NAM-2). No WAN modules are currently supported in virtual switch mode.

**Understanding VSS Topology**

A virtual switching system (VSS) contains two chassis that communicate using the virtual switch link (VSL). VSL is a special port group.

We recommend that you configure both of the 10-Gigabit Ethernet ports on the supervisor engines as VSL ports. Optionally, you can also configure the VSL port group to contain switching module 10-Gigabit Ethernet ports. This configuration provides additional VSL capacity. See Figure 4-5 for an example topology.

**Figure 4-5  VSL Topology Example**

---

**Virtual Switching System Redundancy**

The following sections describe how redundancy in a virtual switching system supports network high availability:

- **Overview**, page 4-8
- **RPR and SSO Redundancy**, page 4-8
- **Failed Chassis Recovery**, page 4-9
- **VSL Failure**, page 4-9
- **User Actions**, page 4-10
Overview

A virtual switching system (VSS) operates stateful switchover (SSO) between the active and standby supervisor engines. Compared to standalone mode, a virtual switching system has the following important differences in its redundancy model:

- The active and standby supervisor engines are hosted in separate chassis and use virtual switch link (VSL) to exchange information.
- The active supervisor engine controls both chassis of the VSS. The active supervisor engine runs the Layer 2 and Layer 3 control protocols and manages the line cards on both chassis.
- The active and standby chassis both perform data traffic forwarding.

If the active supervisor engine fails, the standby supervisor engine initiates a switchover and assumes the active role.

RPR and SSO Redundancy

A virtual switching system operates with stateful switchover (SSO) redundancy if it meets the following requirements:

- Both supervisor engines must be running the same software version.
- VSL-related configuration in the two chassis must match.
- PFC mode must match.

See the “SSO Dependencies” section on page 4-20 for additional details about the requirements for SSO redundancy on a virtual switching system.

With SSO redundancy, the standby supervisor engine is always ready to assume control following a fault on the active supervisor engine. Configuration, forwarding, and state information is synchronized from the active supervisor engine to the redundant supervisor engine at startup and whenever changes to the active supervisor engine configuration occur. If a switchover occurs, traffic disruption is minimized.

If a virtual switching system does not meet the requirements for SSO redundancy, the VSS will use route processor redundancy (RPR). With RPR redundancy, the active supervisor engine does not synchronize configuration changes or state information with the standby. The standby supervisor engine is only partially initialized and the switching modules on the standby supervisor are not powered up. If a switchover occurs, the standby supervisor engine completes its initialization and powers up the switching modules. Traffic is disrupted for approximately 2 minutes.

The VSS normally runs stateful switchover (SSO) between the active and standby supervisor engines (see Figure 4-6). The VSS determines the role of each supervisor engine during initialization.

The supervisor engine in the standby chassis runs in hot standby state. The virtual switching system uses the VSL link to synchronize configuration data from the active to the standby supervisor engine. Also, protocols and features that support high availability synchronize their events and state information to the standby supervisor engine.
Failed Chassis Recovery

If the active chassis or supervisor engine fails, the VSS initiates a stateful switchover (SSO) and the former standby supervisor engine assumes the active role. The failed chassis performs recovery action by reloading the supervisor engine.

If the standby chassis or supervisor engine fails, no switchover is required. The failed chassis performs recovery action by reloading the supervisor engine.

The VSL links are unavailable while the failed chassis recovers. After the chassis reloads, it becomes the new standby chassis and the virtual switching system reinitializes the VSL links between the two chassis.

Note

If preemption is enabled and the new standby chassis is higher priority than the active chassis, the VSS performs a second switchover so that the higher priority chassis is active. For information about configuring priority and preemption, see the “Configuring VSL Switch Priority” section on page 4-30.

The switching modules on the failed chassis are unavailable during recovery, so the VSS operates only with the MEC links that terminate on the active chassis. The bandwidth of the VSS is reduced until the failed chassis has completed its recovery and become operational again. Any devices that are connected only to the failed chassis experience an outage.

Note

The VSS may experience a brief data path disruption when the switching modules in the standby chassis become operational after the SSO.

VSL Failure

In virtual switch mode, fast link notification is enabled on all port channel members (including VSL ports) to ensure fast recovery from VSL failures.

Note

Fast link notification is not compatible with link debounce mechanisms. In virtual switch mode, link debounce is disabled on all port channel members.
If a single VSL physical link goes down, the VSS adjusts the port group so that the failed link is not selected.

If the standby chassis detects complete VSL link failure, it initiates a stateful switchover (SSO). If the active chassis has failed (causing the VSL links to go down), the scenario is chassis failure, as described in the previous section.

If only the VSL has failed and the active chassis is still operational, this is a dual-active scenario. The VSS detects that both chassis are operating in active mode and performs recovery action. See the “Dual-Active Detection” section on page 4-18 for additional details about dual-active scenario.

User Actions

From the active chassis command console, users can initiate a VSS switchover or a reload.

If you enter the `reload` command from the command console, the entire virtual switching system performs a reload.

To reload only the standby chassis, use `redundancy reload peer` command.

To force a switchover from the active to the standby supervisor engine, use the `redundancy force-switchover` command.

Multichassis EtherChannels

Multichassis EtherChannel (MEC) is an EtherChannel with ports that terminate on both chassis of the VSS. These sections describe multichassis EtherChannels:

- **Overview, page 4-10**
- **Failure Scenarios, page 4-11**

Overview

Multichassis EtherChannel (MEC) is an EtherChannel with ports that terminate on both chassis of the VSS (see Figure 4-7). A VSS MEC can connect to any network element that supports EtherChannel (such as a host, server, router, or switch).

At the VSS, a MEC is an EtherChannel with additional capability: the VSS balances the load across ports in each chassis independently. For example, if traffic enters the active chassis, the VSS will select a MEC link from the active chassis. This MEC capability ensures that data traffic does not unnecessarily traverse the VSL.

Each MEC can optionally be configured to support either PAgP or LACP. These protocols run only on the active chassis. PAgP or LACP control packets destined for a MEC link on the standby chassis are sent across VSL.
A MEC can support up to eight active physical links, which can be distributed in any way between the active and standby chassis.

**Failure Scenarios**

We recommend that you configure the MEC with at least one link to each chassis. This configuration conserves VSL bandwidth (traffic egress link is on the same chassis as the ingress link), and increases network reliability (if one VSS supervisor engine fails, the MEC is still operational).

The following sections describe possible failures and the resulting impacts:

- **Single MEC Link Failure**, page 4-11
- **All Links to the Active Chassis Fail**, page 4-11
- **All Links to the Standby Chassis Fail**, page 4-12
- **All Links Fail**, page 4-12
- **Standby Chassis Failure**, page 4-12
- **Active Chassis Failure**, page 4-12

**Single MEC Link Failure**

If a link within the MEC fails (and other links in the MEC are still operational), the MEC redistributes the load among the operational links, as in a regular port.

**All Links to the Active Chassis Fail**

If all links to the active chassis fail, the MEC becomes a regular EtherChannel with operational links to the standby chassis.

Data traffic terminating on the active chassis reaches the MEC by crossing the VSL to the standby chassis. Control protocols continue to run in the active chassis. Protocol messages reach the MEC by crossing the VSL.
Understanding Virtual Switching Systems

All Links to the Standby Chassis Fail

If all links fail to the standby chassis, the MEC becomes a regular EtherChannel with operational links to active chassis.

Control protocols continue to run in the active chassis. All control and data path traffic from the standby chassis reaches the MEC by crossing the VSL to the active chassis.

All Links Fail

If all links in a MEC fail, the logical interface for the EtherChannel is set to unavailable. Layer 2 control protocols perform the same corrective action as for a link-down event on a regular EtherChannel.

On adjacent switches, routing protocols and Spanning Tree Protocol (STP) perform the same corrective action as for a regular EtherChannel.

Standby Chassis Failure

If the standby chassis fails, the MEC becomes a regular EtherChannel with operational links on the active chassis.

The connected switches detect the link failures, and adjust their load-balancing algorithms to use only the links to the active chassis.

Active Chassis Failure

Active chassis failure results in a stateful switchover (SSO). See the “Virtual Switching System Redundancy” section on page 4-7 for details about SSO on a virtual switching system. After the switchover, the MEC is operational on the new active chassis. Connected switches detect the link failures (to the failed chassis), and adjust their load-balancing algorithms to use only the links to the new active chassis.

Packet Handling

In a virtual switching system (VSS), the active supervisor engine runs the Layer 2 and Layer 3 protocols and features for the VSS and manages the DFC line cards for both chassis.

The virtual switching system uses VSL to communicate system and protocol information between the peer chassis and to carry data traffic between the two chassis.
Both chassis perform packet forwarding for ingress traffic on their local interfaces. The virtual switching system minimizes the amount of data traffic that must traverse the VSL.

The following sections describe packet handling in a virtual switching system:

- Traffic on VSL, page 4-13
- Layer 2 Protocols, page 4-13
- Layer 3 Protocols, page 4-14
- SPAN, page 4-16

Traffic on VSL

The VSL carries data traffic and in-band control traffic between the two chassis. All frames forwarded over the VSL link are encapsulated with a special 32-byte header, which provides information for the VSS to forward the packet on the peer chassis.

VSL transports control messages between the two chassis. Messages include protocol messages that are processed by the active supervisor engine, but received or transmitted by interfaces on the standby chassis. Control traffic also includes line card programming between the active supervisor engine and line cards on the standby chassis.

The VSS needs to transmit data traffic over VSL under the following circumstances:

- Layer 2 traffic flooded over a VLAN (even for dual-homed links).
- Packets processed by software on the active supervisor engine where the ingress interface is on the standby chassis.
- The packet destination is on the peer chassis, such as the following examples:
  - Traffic within a VLAN where the known destination interface is on the peer chassis.
  - Traffic that is replicated for a multicast group and the multicast receivers are on the peer chassis.
  - The known unicast destination MAC address is on the peer chassis.
  - The packet is a MAC notification frame destined for a port on the peer chassis.

VSL also transports system data, such as NetFlow export data and SNMP data, from the standby chassis to the active supervisor engine.

To preserve the VSL bandwidth for critical functions, the VSS uses strategies to minimize user data traffic that must traverse the VSL. For example, if an access switch is dual-homed (attached with a MEC terminating on both VSS chassis), the VSS transmits packets to the access switch using a link on the same chassis as the ingress link.

Traffic on the VSL is load-balanced with the same global hashing algorithms available for EtherChannels (the default algorithm is source-destination IP).

Layer 2 Protocols

The active supervisor engine runs the Layer 2 protocols (such as STP and VTP) for the line cards on both chassis. Protocol messages that are transmitted and received on the standby chassis line cards must traverse VSL to reach the active supervisor engine.
The following sections describe Layer 2 protocols for a virtual switching system:

- Spanning Tree Protocol, page 4-14
- Virtual Trunk Protocol, page 4-14
- EtherChannel Control Protocols, page 4-14

Spanning Tree Protocol

The active chassis runs Spanning Tree Protocol (STP). The standby chassis redirects STP BPDUs across the VSL to the active chassis.

The STP bridge ID is commonly derived from the chassis MAC address. To ensure that the bridge ID does not change after a switchover, the virtual switching system continues to use the original chassis MAC address for the STP Bridge ID.

Virtual Trunk Protocol

Virtual Trunk Protocol (VTP) uses the IP address of the switch and local current time for version control in advertisements. After a switchover, VTP uses the IP address of the newly active chassis.

EtherChannel Control Protocols

Link Aggregation Control Protocol (LACP) and Port Aggregation Protocol (PAgP) packets contain a device identifier. The virtual switching system defines a common device identifier for both chassis to use.

A new PAgP enhancement has been defined for assisting with dual-active scenario detection. For additional information, see the “Dual-Active Detection” section on page 4-18.

Layer 3 Protocols

The MSFC on the active supervisor engine runs the Layer 3 protocols and features for the VSS. Both chassis perform packet forwarding for ingress traffic on their interfaces. If possible, ingress traffic is forwarded to an outgoing interface on the same chassis, to minimize data traffic that must traverse the VSL.

Because the standby chassis is actively forwarding traffic, the active supervisor engine distributes updates to the standby supervisor engine PFC and all standby chassis DFCs.

The following sections describe Layer 3 protocols for a virtual switching system:

- IPv4, page 4-14
- IPv6 and MPLS, page 4-15
- IPv4 Multicast, page 4-15
- Software Features, page 4-15

IPv4

The supervisor engine on the active chassis runs the IPv4 routing protocols and performs any required software forwarding.

Routing updates received on the standby chassis are redirected to the active chassis across VSL.

Hardware forwarding is distributed across all DFCs on the VSS. The supervisor engine on the active chassis sends FIB updates to all local DFCs, remote DFCs, and the standby supervisor engine PFC.
All hardware routing uses the router MAC address assigned by the active supervisor engine. After a switchover, the original MAC address is still used.

The supervisor engine on the active chassis performs all software forwarding (for protocols such as IPX) and feature processing (such as fragmentation and TTL exceed). If a switchover occurs, software forwarding is disrupted until the new active supervisor engine obtains the latest CEF and other forwarding information.

In virtual switch mode, the requirements to support non-stop forwarding (NSF) are the same as in standalone mode. For additional information about NSF requirements, refer to the Catalyst 6500 Series Switch Cisco IOS Configuration Guide, Release 12.2SX.

From a routing peer perspective, EtherChannels remain operational during a switchover (only the links to the failed chassis are down, so the routing adjacencies remain valid).

The virtual switching system implements path filtering by storing only local paths (paths that do not traverse the VSL) in the FIB entries. Therefore, IP forwarding performs load sharing among the local paths. If no local paths to a given destination are available, the VSS updates the FIB entry to include remote paths (reachable by traversing the VSL).

**IPv6 and MPLS**

The virtual switching system does not support IPv6 or MPLS.

**IPv4 Multicast**

The IPv4 multicast protocols run on the active supervisor engine. Internet Group Management Protocol (IGMP) and Protocol Independent Multicast (PIM) protocol packets received on the standby supervisor engine are transmitted across VSL to the active chassis.

The active supervisor engine sends IGMP and PIM protocol packets to the standby supervisor engine in order to maintain Layer 2 information for stateful switchover (SSO).

The active supervisor engine distributes multicast FIB and adjacency table updates to the standby supervisor and line card DFCs.

The virtual switching system does not support SSO for Layer 3 multicast. Multicast routes are programmed in the hardware in the standby supervisor engine, using nodal NSF updates.

In virtual switch mode, the active chassis does not program the multicast expansion table (MET) on the standby chassis. The standby supervisor engine programs the outgoing interface hardware entries for all local multicast receivers.

If all line cards on the active chassis and standby chassis are egress capable, the multicast replication mode is set to egress mode; otherwise, the mode is set to ingress mode.

In egress mode, replication is distributed to DFCs that have ports in outgoing VLAN for a particular flow. In ingress mode, replication for all outgoing VLANs is done on the ingress DFC.

For packets traversing VSL, all Layer 3 multicast replication occurs on the ingress chassis. If there are multiple receivers on the egress chassis, replicated packets are forwarded over the VSL.

**Software Features**

Software features run only on the active supervisor engine. Incoming packets to the standby chassis that require software processing are sent across the VSL.

For features supported in hardware, the ACL configuration is sent to the TCAM manager on the active supervisor engine, the standby supervisor engine, and all DFCs.
SPAN

The virtual switching system supports all SPAN features for non-VSL interfaces. The virtual switching system supports SPAN features on VSL interfaces with the following limitations:

- If the VSL is configured as a local SPAN source, the SPAN destination interface must be on the same chassis as the source interface.
- VSL cannot be configured as a SPAN destination.
- VSL cannot be configured as a traffic source of RSPAN, ERSPAN, or egress-only SPAN.

The number of SPAN sessions available to a VSS is the same as for a single chassis running in standalone mode.

System Monitoring

The following sections describe system monitoring and system management for a virtual switching system:

- Power Management, page 4-16
- Environmental Monitoring, page 4-16
- File System Access, page 4-16
- Diagnostics, page 4-16
- Service Modules, page 4-17
- Network Management, page 4-17

Power Management

From the active chassis, you can control power-related functions for the standby chassis. For example, use the (no) power enable switch command to control power to the modules and slots on the standby chassis. Use the show power switch command to see the current power settings and status.

Environmental Monitoring

Environmental monitoring runs on both supervisor engines. The standby chassis reports notifications to the active supervisor engine. The active chassis gathers log messages for both chassis. The active chassis synchronizes the calendar and system clock to the standby chassis.

File System Access

You can access file systems of both chassis from the active chassis. Prefix the device name with the switch number and slot number to access directories on the standby chassis. For example, the command dir sw2_slot5disk0 lists the contents of disk0 on the standby chassis (assuming switch 2 is the standby chassis). You can access the standby chassis file system only when VSL is operational.

Diagnostics

You can use the diagnostic schedule and diagnostic start commands on a VSS. In virtual switch mode, these commands require an additional parameter, which specifies the chassis to apply the command.
When you configure a VSL port on a switching module or a supervisor engine module, the diagnostics suite incorporates additional tests for the VSL ports.

Use the `show diagnostic content` command to display the diagnostics test suite for a module.

**VSL Diagnostics**

The following VSL-specific diagnostics tests are available on WS-X6708-10GE switching modules with VSL ports. These tests are disruptive:

- TestVslBridgeLink
- TestVslLocalLoopback

The following VSL-specific diagnostics tests are available on a Supervisor Engine 720-10GE with VSL ports. These tests are disruptive:

- TestVSAciveToStandbyLoopback
- TestVslBridgeLink
- TestVslLocalLoopback

The following VSL-specific diagnostics test is available for VSL ports on the switching module or the supervisor engine. This test is not disruptive:

- TestVslStatus

**Service Modules**

The only service module supported by the virtual switching system is the network analysis module (WS-SVC-NAM-1 and WS-SVC-NAM-2).

The supervisor engine in the same chassis as the NAM controls the powering up of the NAM. After the NAM is online, you initiate a session from the active supervisor engine to configure and maintain the NAM.

The active chassis performs the graceful shutdown of the NAM module, even if the NAM module is in the standby chassis.

Use the `Session` command to connect to the NAM. If NAM is on the standby chassis, the session runs over the VSL.

**Network Management**

The following sections describe network management for a virtual switching system:

- Telnet over SSH Sessions and the Web Browser User Interface, page 4-17
- SNMP, page 4-18
- Command Console, page 4-18

**Telnet over SSH Sessions and the Web Browser User Interface**

A virtual switching system supports remote access using Telnet over SSH sessions and the Cisco web browser user interface.

All remote access is directed to the active supervisor engine, which manages the whole VSS.

If the virtual switching system performs a switchover, Telnet over SSH sessions and web browser sessions are disconnected.
SNMP

The SNMP agent runs on the active supervisor engine.

CISCO-VIRTUAL-SWITCH-MIB is a new MIB for virtual switch mode and contains the following main components:

- **cvsGlobalObjects** - Domain #, Switch #, Switch Mode
- **cvsCoreSwitchConfig** - Switch Priority and Preempt
- **cvsChassisTable** - Chassis Role and Uptime
- **cvsVSLConnectionTable** - VSL Port Count, Operational State
- **cvsVSLStatsTable** - Total Packets, Total Error Packets
- **cvsVSLPortStatsTable** - TX/RX Good, Bad, Bi-dir and Uni-dir Packets

Command Console

You need to cable physical console connections to both supervisor engine console ports. You can only use configuration mode in the console for the active supervisor engine.

The console on the standby chassis will indicate that chassis is operating in standby mode by adding the characters “-stdby” to the command line prompt. You cannot enter configuration mode on the standby chassis console.

The following example shows the prompt on the standby console:

```
Router-stdby> show switch virtual
Switch mode : Virtual Switch
Virtual switch domain number : 100
Local switch number : 1
Local switch operational role: Virtual Switch Standby
Peer switch number : 2
Peer switch operational role : Virtual Switch Active
```

Dual-Active Detection

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

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

The virtual switching system supports two methods for detecting dual-active scenario. One method uses enhanced PAgP messaging over the MEC links to communicate between the two chassis. The other method uses IP BFD messaging over a backup Ethernet connection.

You can configure both detection methods to be active at the same time. The PAgP method takes priority, because it detects dual-active scenario much more quickly than the IP BFD method.

The two methods are described in the following sections:

- **Dual-Active Detection Using Enhanced PAgP**, page 4-19
- **Dual-Active Detection Using IP BFD**, page 4-19
- **Recovery Actions**, page 4-19
Dual-Active Detection Using Enhanced PAgP

Port aggregation protocol (PAgP) is a Cisco-proprietary protocol for managing EtherChannels. If a VSS MEC terminates to a Cisco switch, you can run PAgP protocol on the MEC.

If PAgP is running on the MECs between the VSS and an upstream or downstream switch, the VSS can use PAgP to detect dual-active scenario. The MEC must have at least one port on each chassis of the VSS.

In virtual switch mode, PAgP messages include a new TLV which contains the ID of the active switch. Only switches in virtual switch mode send the new TLV.

For dual-active detection to operate successfully, one or more of the connected switches needs to be able to process the new TLV. Catalyst 6500 series switches with Supervisor Engine 32 and Supervisor Engine 720 have this capability, if they are running Cisco IOS software release 12.2(33)SXH or later. For a list of other Cisco products that support enhanced PAgP, refer to Release Notes for Cisco IOS Release 12.2(33)SXH and Later Releases.

When the standby chassis detects VSL failure, it initiates SSO and becomes active. Subsequent PAgP messages to the connected switch from the newly active chassis contain the new active ID. The connected switch send PAgP messages with the new active ID to both of the VSS chassis.

If the formerly active chassis is still operational, it detects the dual-active scenario because the active ID in the PAgP messages changes. This chassis initiates recovery actions as described in the “Recovery Actions” section on page 4-19.

Dual-Active Detection Using IP BFD

To use the IP BFD detection method, you must provision a direct Ethernet connection between the two switches. Regular Layer 3 ping will not function correctly on this connection, as both chassis have the same IP address. The virtual switching system instead uses the Bidirectional Forwarding Detection (BFD) protocol.

If the VSL goes down, both chassis create BFD neighbors, and try to establish adjacency. If the original active chassis receives an adjacency message, it realizes that this is dual-active scenario, and initiates recovery.

Note

If FlexLinks are configured on the VSS, we recommend using the PAgP detection method. Do not configure FlexLinks and BFD dual-active detection on the same VSS.

Recovery Actions

The chassis shuts down all of its non-VSL interfaces (except interfaces configured to be excluded from shutdown) to remove itself from the network, and waits in recovery mode until the VSL links have recovered. User intervention may be required to fix the VSL failure. When both chassis detect that VSL is operational again, the previously active chassis reloads and comes into service as the standby chassis.

Virtual Switching System Initialization

A virtual switching system (VSS) is formed when the two chassis and the VSL link between them become operational. The peer chassis communicate over the VSL to negotiate the chassis roles.

If only one chassis becomes operational, it assumes the active role. The VSS forms when the second chassis becomes operational and both chassis bring up their VSL interfaces.
Virtual switching system initialization is described in the following sections:

- **Virtual Switch Link Protocol, page 4-20**
- **SSO Dependencies, page 4-20**
- **Initialization Procedure, page 4-21**

**Virtual Switch Link Protocol**

The Virtual Switch Link Protocol (VSLP) consists of several protocols that contribute to virtual switch initialization. The VSLP includes the following protocols:

- **Role Resolution Protocol**
  The peer chassis use Role Resolution Protocol (RRP) to negotiate the role (active or standby) for each chassis.

- **Link Management Protocol**
  The Link Management Protocol (LMP) runs on all VSL links, and exchanges information required to establish communication between the two chassis.

  LMP identifies and rejects any unidirectional links. If LMP flags a unidirectional link, the chassis that detects the condition brings the link down and up to restart the VSLP negotiation. VSL moves the control traffic to another port if necessary.

**SSO Dependencies**

For the VSS to operate with SSO redundancy, the VSS must meet the following conditions:

- **Identical software versions**
  Both supervisor engine modules on the VSS must be running the identical software version.

- **VSL configuration consistency**
  During the startup sequence, the standby chassis sends virtual switch information from the startup-config file to the active chassis.

  The active chassis ensures that the following information matches correctly on both chassis:
  - Switch virtual domain
  - Switch virtual node
  - Switch priority
  - Switch preempt
  - VSL port channel: switch virtual link identifier
  - VSL ports: channel-group number, shutdown, total number of VSL ports
  - Power redundancy-mode
  - Power enable on VSL modules

  If the VSS detects a mismatch, it prints out an error message on the active chassis console and the standby chassis comes up in RPR mode.

  After you correct the configuration file, save the file by entering the `copy running-config startup-config` command on the active chassis, and then restart the standby chassis.
- PFC mode check

If both supervisor engines are provisioned with PFC3C, the VSS will automatically operate in PFC3C mode, even if some of the switching modules are equipped with 3CXL daughter feature cards (DFCs).

However, if the supervisor engines are provisioned with PFC3CXL and there is a mixture of DFC3C and DFC3CXL switching modules, the system PFC mode will depend on how the 3C and 3CXL switching modules are distributed between the two chassis.

Each chassis in the VSS determines its system PFC mode. If the supervisor engine of a given chassis is provisioned with PFC3CXL and all the switching modules in the chassis are provisioned with DFC3CXL, the PFC mode for the chassis is PFC3CXL. However, if any of the switching modules is provisioned with DFC3C, the chassis PFC mode will be set to PFC3C. If there is a mismatch between the PFC modes of two chassis, the VSS will come up in RPR mode instead of SSO mode. You can prevent this situation by using the `platform hardware vsl pfc mode pfc3c` command to force the VSS to operate in PFC3C mode after the next reload.

If these conditions are not met, the VSS operates in RPR redundancy mode. For a description of SSO and RPR, see the “Virtual Switching System Redundancy” section on page 4-7.

### Initialization Procedure

The following sections describe the VSS initialization procedure:

- **VSL Initialization**, page 4-21
- **System Initialization**, page 4-21
- **VSL Down**, page 4-22

#### VSL Initialization

A VSS is formed when the two chassis and the VSL link between them become operational. Because both chassis need to be assigned their role (active or standby) before completing initialization, VSL is brought online before the rest of the system is initialized. The initialization sequence is as follows:

1. The virtual switching system initializes all cards with VSL ports, and then initializes the VSL ports.
2. The two chassis communicate over VSL to negotiate their roles (active or standby).
3. The active chassis completes the boot sequence, including the consistency check described in the “SSO Dependencies” section on page 4-20.
4. If the consistency check completed successfully, the standby chassis comes up in SSO standby mode. If the consistency check failed, the standby chassis comes up in RPR mode.
5. The active chassis synchronizes configuration and application data to the standby chassis.

#### System Initialization

If you boot both chassis simultaneously, the VSL ports become active, and the chassis will come up as active and standby. If priority is configured, the higher priority switch becomes active.

If you boot up only one chassis, the VSL ports remain inactive, and the chassis comes up as active. When you subsequently boot up the other chassis, the VSL links become active, and the new chassis comes up as standby. If you have configured preemption and the new chassis has the higher priority, it will initiate a switchover to become the active switch. The formerly active chassis reloads and comes up as standby.
VSL Down

If the virtual switch link (VSL) is down when both chassis try to boot up, the situation is similar to a dual-active scenario.

One of the chassis becomes active and the other chassis initiates recovery from dual-active scenario. For further information, see the “Configuring Dual-Active Detection” section on page 4-39.

VSS Configuration Guidelines and Restrictions

When configuring the VSS, note the following guidelines and restrictions:

- The virtual switching system configurations in the startup-config file must match on both chassis.
- If you configure new values for switch priority or preemption, the change only takes effect after you save the configuration file and perform a restart.

When configuring MECs, note the following guidelines and restrictions:

- All links in a MEC must terminate locally on the active or standby chassis of the same virtual domain.
- For a MEC using LACP control protocol, minlinks defines the minimum number of physical links in each chassis for the MEC to be operational.
- For a MEC using LACP control protocol, maxbundle defines the maximum number of links in the MEC across the whole VSS.
- MEC supports LACP 1:1 redundancy. For additional information about LACP 1:1 redundancy, refer to the “Configuring LACP 1:1 Redundancy” section on page 4-38.
- A MEC can be connected to another MEC on a different virtual switching system domain.

When configuring dual-active detection, note the following guidelines and restrictions:

- If FlexLinks are configured on the VSS, we recommend using the PAgP detection method. Do not configure FlexLinks and BFD dual-active detection on the same VSS.

Configuring Virtual Switching Systems

These sections describe how to configure virtual switching systems:

- Converting to a Virtual Switching System, page 4-23
- Displaying Virtual Switching System Information, page 4-28
- Converting a Virtual Switching System to Standalone Chassis, page 4-28
- Configuring Virtual Switching System Parameters, page 4-30
- Configuring Multichannel EtherChannels, page 4-37
- Configuring Dual-Active Detection, page 4-39
Chapter 4  Configuring Virtual Switching Systems

Converting to a Virtual Switching System

By default, the Catalyst 6500 series switch is configured to operate in standalone mode (the switch is a single chassis). The virtual switching system combines two standalone switches into one virtual switching system (VSS), operating in virtual switch mode.

To convert two standalone chassis into a VSS, you perform the following major activities:

- Save the standalone configuration files.
- Configure each chassis as a VSS.
- Convert to virtual switching system.
- Configure the peer VSL information.

In virtual switch mode, both chassis use the same configuration file. When you make configuration changes on the active chassis, these changes are automatically propagated to the standby chassis.

The tasks required to convert the standalone chassis to a VSS are detailed in the following sections:

- Backing Up the Standalone Configuration, page 4-23
- Assigning Virtual Switch Domain and Switch Numbers, page 4-24
- Configuring VSL Port Channel and Ports, page 4-24
- Converting the Chassis to Virtual Switch Mode, page 4-25
- Auto-Configuring the Standby VSL Information, page 4-27
- (Optional) Configuring Standby Chassis Modules, page 4-27

In the procedures that follow, the example commands assume the configuration shown in Figure 4-9.

**Figure 4-9  Example VSS**

Two chassis, A and B, are converted into a VSS with virtual switch domain 100. Interface 10-Gigabit Ethernet 5/1 on Switch 1 is connected to interface 10-Gigabit Ethernet 5/2 on Switch 2 to form the VSL.

**Backing Up the Standalone Configuration**

Save the configuration files for both chassis operating in standalone mode. You need these files to revert to standalone mode from virtual switch mode. On Switch 1, perform this task:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Switch-1# copy running-config startup-config</td>
<td>(Optional) Saves the running configuration to startup configuration.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Switch-1# copy startup-config disk0:old-startup-config</td>
<td>Copies the startup configuration to a backup file.</td>
</tr>
</tbody>
</table>
Perform the following task on Switch 2:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch-2# copy running-config startup-config</td>
<td>(Optional) Save the running configuration to the startup configuration file.</td>
</tr>
<tr>
<td>Switch-2# copy startup-config disk0:old-startup-config</td>
<td>Copy the startup configuration to a backup file.</td>
</tr>
</tbody>
</table>

Assigning Virtual Switch Domain and Switch Numbers

You must configure the same virtual switch domain number on both chassis of the VSS. The virtual switch domain is a number between 1 and 255, and must be unique for each VSS in your network (the domain number is incorporated into various identifiers to ensure that these identifiers are unique across the network).

Within the VSS, you must configure a unique switch number for each chassis.

To configure the virtual switch domain and switch number on both chassis, perform this task on Switch 1:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch-1(config)# switch virtual domain 100</td>
<td>Configures the virtual switch domain on Chassis A.</td>
</tr>
<tr>
<td>Switch-1(config-vs-domain)# switch 1</td>
<td>Configures Chassis A as virtual switch number 1.</td>
</tr>
<tr>
<td>Switch-1(config-vs-domain)# exit</td>
<td>Exits config-vs-domain.</td>
</tr>
</tbody>
</table>

Perform the following task on Switch 2:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch-2(config)# switch virtual domain 100</td>
<td>Configures the virtual switch domain on Chassis B.</td>
</tr>
<tr>
<td>Switch-2(config-vs-domain)# switch 2</td>
<td>Configures Chassis B as virtual switch number 2.</td>
</tr>
<tr>
<td>Switch-2(config-vs-domain)# exit</td>
<td>Exits config-vs-domain.</td>
</tr>
</tbody>
</table>

Note: The switch number is not stored in the startup or running configuration, because both chassis use the same configuration file (but must not have the same switch number).

Configuring VSL Port Channel and Ports

The VSL is configured with a unique port channel on each chassis. During the conversion, the VSS configures both port channels on the active chassis. If the standby chassis VSL port channel number has been configured for another use, the VSS comes up in RPR mode. To avoid this situation, check that both port channel numbers are available on both of the chassis.

Check the port channel number by using the `show running-config interface port-channel` command. The command displays an error message if the port channel is available for VSL. For example, the following command shows that port channel 20 is available on Switch 1:

```
Switch-1 # show running-config interface port-channel 20
```
To configure the VSL port channels, perform this task on Switch 1:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Switch-1(config)# interface port-channel 10 Configures port channel 10 on Switch 1.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Switch-1(config-if)# switch virtual link 1 Associates Switch 1 as owner of port channel 10.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Switch-1(config-if)# no shutdown Activates the port channel.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Switch-1(config-if)# exit Exits interface configuration.</td>
</tr>
</tbody>
</table>

Perform the following task on Switch 2:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Switch-2(config)# interface port-channel 20 Configures port channel 20 on Switch 2.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Switch-2(config-if)# switch virtual link 2 Associates Switch 2 as owner of port channel 20.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Switch-2(config-if)# no shutdown Activates the port channel.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Switch-2(config-if)# exit Exits interface configuration mode.</td>
</tr>
</tbody>
</table>

You must add the VSL physical ports to the port channel. In the following example, interface 10-Gigabit Ethernet 3/1 on Switch 1 is connected to interface 10-Gigabit Ethernet 5/2 on Switch 2.

To configure the VSL ports, perform this task on Switch 1:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Switch-1(config)# interface tenGigabitEthernet 5/1 Enters configuration mode for interface t5/1 on Switch 1.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Switch-1(config-if)# channel-group 10 mode on Adds this interface to channel group 10.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Switch-1(config-if)# no shutdown Activates the port.</td>
</tr>
</tbody>
</table>

Perform the following task on Switch 2:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Switch-2(config)# interface tenGigabitEthernet 5/2 Enters configuration mode for interface t5/2 on Switch 2.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Switch-2(config-if)# channel-group 20 mode on Adds this interface to channel group 20.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Switch-2(config-if)# no shutdown Activates the port.</td>
</tr>
</tbody>
</table>

### Converting the Chassis to Virtual Switch Mode

Conversion to virtual switch mode requires a restart for both chassis. After the reboot, commands that specify interfaces with module/port now include the switch number. For example, a port on a switching module is specified by switch/module/port.
Prior to the restart, the VSS converts the startup configuration to use the switch/module/port convention. A backup copy of the startup configuration file is saved on the RP. This file is assigned a default name, but you are also prompted to override the default name if you want to change it.

Prior to the conversion, ensure that the PFC operating mode matches on both chassis. If they do not match, VSS comes up in RPR redundancy mode. Enter the `show platform hardware pfc mode` command on each chassis to display the current PFC mode. If only one of the chassis is in PFC3CXL mode, you can configure it to use PFC3C mode with the `platform hardware vsl pfc mode pfc3c` command.

To verify the PFC operating mode, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>&lt;br&gt;Switch-1# <code>show platform hardware pfc mode</code></td>
<td>Ensures that the PFC operating mode matches on both chassis, to ensure that the VSS comes up in SSO redundancy mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong>&lt;br&gt;Switch-2# <code>show platform hardware pfc mode</code></td>
<td>Ensures that the PFC operating mode matches on both chassis, to ensure that the VSS comes up in SSO redundancy mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong>&lt;br&gt;Switch-1# <code>platform hardware vsl pfc mode pfc3c</code></td>
<td>(Optional) Sets the PFC operating mode to PFC3C on Chassis A.</td>
</tr>
<tr>
<td><strong>Step 4</strong>&lt;br&gt;Switch-2# <code>platform hardware vsl pfc mode pfc3c</code></td>
<td>(Optional) Sets the PFC operating mode to PFC3C on Chassis B.</td>
</tr>
</tbody>
</table>

To convert Chassis 1 to virtual switch mode, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>&lt;br&gt;Switch-1# <code>switch convert mode virtual</code></td>
<td>Converts Switch 1 to virtual switch mode. After you enter the command, you are prompted to confirm the action. Enter <code>yes</code>. The system creates a converted configuration file, and saves the file to the RP bootflash.</td>
</tr>
</tbody>
</table>

To convert Chassis 2 to virtual switch mode, perform this task on Switch 2:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>&lt;br&gt;Switch-2# <code>switch convert mode virtual</code></td>
<td>Converts Switch 2 to virtual switch mode. After you enter the command, you are prompted to confirm the action. Enter <code>yes</code>. The system creates a converted configuration file, and saves the file to the RP bootflash.</td>
</tr>
</tbody>
</table>

*Note* After you confirm the command (by entering `yes` at the prompt), the running configuration is automatically saved as the startup configuration and the chassis reboots. After the reboot, the chassis is in virtual switch mode, so you must specify interfaces with three identifiers (switch/module/port).
Auto-Configuring the Standby VSL Information

The two chassis now form a virtual switching system (VSS). In virtual switch mode, you enter all configuration commands on the active chassis. The startup configuration file is automatically synchronized to the standby chassis.

For the VSS to operate correctly, the active chassis needs the configuration information for the other end of the VSL link (on the standby chassis). Enter the `switch accept mode virtual` command to automatically copy the VSL link configuration from the standby chassis onto the active chassis. The updated configuration is automatically saved to the startup configuration file on the active and standby chassis.

The `switch accept mode virtual` command performs this action only the first time that the chassis come up as a VSS.

To auto-configure the standby chassis VSL link information to the active chassis, perform this task on the active chassis:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Switch-1# switch accept mode virtual</strong></td>
</tr>
<tr>
<td></td>
<td>Copies the VSL link configuration from the standby chassis to the active chassis.</td>
</tr>
<tr>
<td></td>
<td>Prior to performing the action, the VSS displays the configurations that will be copied, and prompts you to proceed or not.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The standby chassis must be in hot standby mode for this command to execute successfully.</td>
</tr>
</tbody>
</table>

(Optional) Configuring Standby Chassis Modules

After the reboot, each chassis contains the module provisioning for its own slots. In addition, the modules from the standby chassis have been automatically provisioned on the active chassis with default configuration.

Configurations for the standby chassis modules are restored to their default settings (for example, no IP addresses).

You can view the module provisioning information in the configuration file, by entering the `show startup-config` command (after you have saved the configuration).

**Note** Do not delete or modify this section of the configuration file.

The following example shows the module provisioning information from a configuration file:

```
module provision switch 1
  slot 1 slot-type 148 port-type 60 number 4  virtual-slot 17
  slot 2 slot-type 148 port-type 60 number 4  virtual-slot 17
  slot 3 slot-type 148 port-type 60 number 4  virtual-slot 17
  slot 4 slot-type 148 port-type 60 number 4  virtual-slot 17
  slot 5 slot-type 148 port-type 60 number 4  virtual-slot 17
module provision switch 2
  slot 1 slot-type 148 port-type 60 number 4  virtual-slot 17
  slot 2 slot-type 148 port-type 60 number 4  virtual-slot 17
  slot 3 slot-type 148 port-type 60 number 4  virtual-slot 17
  slot 4 slot-type 148 port-type 60 number 4  virtual-slot 17
  slot 5 slot-type 148 port-type 60 number 4  virtual-slot 17
```
Cisco IOS Software Configuration Guide, Release 12.2(33)SXH and Later Releases

Chapter 4 Configuring Virtual Switching Systems

Configuring Virtual Switching Systems

The following example shows the information output from these commands:

```
Router# 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

Router# show switch virtual role
Switch  Switch Status  Preempt    Priority  Role     Session ID
Number         Oper(Conf) Oper(Conf)         Local  Remote
------------------------------------------------------------------
LOCAL    1     UP      FALSE(N)   100(100)  ACTIVE   0      0
REMOTE   2     UP      FALSE(N)   100(100)  STANDBY  8158   1991
In dual-active recovery mode: No

Router# show switch virtual link
VSL Status: UP
VSL Uptime: 4 hours, 26 minutes
VSL SCP Ping: Pass OK
VSL ICC (Ping): Pass
VSL Control Link: Te 1/5/1
```

Converting a Virtual Switching System to Standalone Chassis

To convert a VSS into two standalone chassis, you perform the following major steps:

- Copying the VSS Configuration to a Backup File, page 4-29
- Converting the Active Chassis to Standalone, page 4-29
- Converting the Peer Chassis to Standalone, page 4-29
Copying the VSS Configuration to a Backup File

Copy the configuration file from the active chassis. You may need this file if you convert to virtual switch mode again. You only need to save the file from the active chassis, because the configuration file on the standby chassis is identical to the file on the active chassis.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Switch-1# copy running-config startup-config</td>
<td>(Optional) Saves the running configuration to startup configuration. This step is only required if you there are unsaved changes in the running configuration that you want to preserve.</td>
</tr>
<tr>
<td>2</td>
<td>Switch-1# copy startup-config disk0:vs-startup-config</td>
<td>Copies the startup configuration to a backup file.</td>
</tr>
</tbody>
</table>

Converting the Active Chassis to Standalone

When you convert the active chassis to standalone mode, the active chassis removes the provisioning and configuration information related to VSL links and the peer chassis modules, saves the configuration file, and performs a reload. The chassis comes up in standalone mode with only the provisioning and configuration data relevant to the standalone system.

The standby chassis of the VSS becomes active. VSL links on this chassis are down because the peer is no longer available.

To convert the active chassis to standalone mode, perform this task on the active chassis:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch-1# switch convert mode standalone</td>
<td>Converts Switch 1 to standalone mode. After you enter the command, you are prompted to confirm the action. Enter yes.</td>
</tr>
</tbody>
</table>

Converting the Peer Chassis to Standalone

When you convert the new active chassis to standalone mode, the chassis removes the provisioning and configuration information related to VSL links and the peer chassis modules, saves the configuration file and performs a reload. The chassis comes up in standalone mode with only its own provisioning and configuration data.

To convert the peer chassis to standalone, perform this task on the standby chassis:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch-2# switch convert mode standalone</td>
<td>Converts Switch 2 to standalone mode. After you enter the command, you are prompted to confirm the action. Enter yes.</td>
</tr>
</tbody>
</table>
Configuring Virtual Switching System Parameters

These sections describe how to configure virtual switching system parameters:

- Configuring VSL Switch Priority, page 4-30
- Configuring VSLP Timer, page 4-31
- Configuring PFC Mode, page 4-33
- Configuring Virtual Switch Links, page 4-33
- Displaying VSL Information, page 4-34
- Configuring VSL QoS, page 4-35
- Subcommands for VSL Port Channels, page 4-35
- Subcommands for VSL Ports, page 4-36

Configuring VSL Switch Priority

To configure the switch priority, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Step 2</strong></td>
</tr>
<tr>
<td>Router(config)# switch virtual domain 100</td>
<td>Configures the priority for the chassis. The switch with the higher priority assumes the active role. The range is 1 to 255; the default is 100.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If the higher priority switch is currently in standby state, you can make it the active switch by initiating a switchover. Enter the command <strong>redundancy</strong> <strong>force-switchover</strong>.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The new priority value only takes effect after you save the configuration and perform a reload of the VSS.</td>
</tr>
<tr>
<td>Router(config-vs-domain)# no switch [1</td>
<td>2] priority</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Resets the priority value to the default priority value of 100. The new value takes effect after you save the configuration and perform a reload.</td>
</tr>
</tbody>
</table>
Configuring Virtual Switching Systems

If you make configuration changes to the switch priority or preemption, the changes only take effect after you save the running configuration to the startup configuration file and perform a reload. The `show switch virtual role` command shows the operating and configured preemption and priority values. You can manually set the standby switch to active using the `redundancy force-switchover` command.

This example shows how to configure virtual switch priority:

```
Router(config)# switch virtual domain 100
Router(config-vs-domain)# switch 1 priority 200
Router(config-vs-domain)# switch 1 preempt
```

This example shows how to display priority and preemption information for the virtual switching system:

```
Router# show switch virtual role
```

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-vs-domain)# switch [1</td>
<td>2] preempt [delay]</td>
<td>Enables preemption. With preemption enabled, the higher priority switch will initiate a switchover to become active (if it comes up in standby state after a reload or switchover).&lt;br&gt;• delay—(Optional) Number of minutes before the standby chassis takes over as the active chassis. The range is 5 to 20; the default is 5.</td>
</tr>
<tr>
<td>Router(config-vs-domain)# no switch [1</td>
<td>2] preempt</td>
<td>Disables preemption.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-vs-domain)#</td>
<td></td>
<td>Displays the current priority and preemption settings.</td>
</tr>
</tbody>
</table>

This example shows how to configure virtual switch priority:

```
Router(config)# switch virtual domain 100
Router(config-vs-domain)# switch 1 priority 200
Router(config-vs-domain)# switch 1 preempt
Router(config-vs-domain)# exit
```

This example shows how to display priority and preemption information for the virtual switching system:

```
Router# show switch virtual role
```

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-vs-domain)#</td>
<td></td>
<td>Displays the current priority and preemption settings.</td>
</tr>
</tbody>
</table>

**Configuring VSLP Timer**

Each end of the VSL link transmits Hello messages to the other end of the link. You can configure the transmission interval between hello messages. You can also configure the minimum reception interval (if no Hello message is received during this interval, the link is assumed to be down).

The default value for the VSLP timer works well for most configurations. If you set the timer too low, the system may detect false VSL failures, which triggers the recovery actions for dual-active scenario. For more information about dual-active scenario, see the “Dual-Active Detection” section on page 4-18.
Configure the VSLP intervals on the VSL port channel interface. The intervals are applied to each physical link in the VSL.

To configure the VSLP hello packet interval, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Router(config)# interface port-channel num</td>
</tr>
<tr>
<td>Step 2</td>
<td>Router(config-if)# vslp interval 300-5000 min_rx 300-10000 multiplier 3-50</td>
</tr>
<tr>
<td>Step 3</td>
<td>Router(config-if)# no vslp interval int min_rx int multi int</td>
</tr>
<tr>
<td>Step 4</td>
<td>Router# show vslp lmp timer</td>
</tr>
</tbody>
</table>

**Note** We recommend that you configure the same VSLP interval values for both VSL port channels, as shown in the following example. Otherwise, the values change after a switchover.

This example shows how to set the VSLP hello packet interval to 50 seconds on port channel 10 and port channel 25:

Router(config)# interface port-channel 10
Router(config-if)# vslp interval 5000 min_rx 5000 multi 10
Router(config-if)# interface port-channel 25
Router(config-if)# vslp interval 5000 min_rx 5000 multi 10
Configuring PFC Mode

If you have a mixture of DFC3C and DFC3CXL switching modules in the VSS, set the PFC mode by performing this task:

```
Router(config)# platform hardware vsl pfc mode pfc3c
Note: This command requires a system reload before it takes effect.
```

```
Router(config-if)# no platform hardware vsl pfc mode pfc3c
```

Resets the PFC configuration mode to the default setting (PFC3CXL).

```
Router# show platform hardware pfc mode
```

Displays the current settings for the PFC mode.

```
Router(config)# platform hardware vsl pfc mode pfc3c
Router(config)# end
Router# reload
```

This example shows how to set the PFC configuration mode for the VSS to PFC3C. You can wait until the next maintenance window to perform the `reload` command.

```
Router(config)# platform hardware vsl pfc mode pfc3c
PFC Preferred Mode: PFC3CXL. The discrepancy between Operating Mode and Preferred Mode could be due to PFC mode config. Your System has all PFC3XL modules. Remove 'platform hardware vsl pfc mode pfc3c' from global config.
```

```
Router# show platform hardware pfc mode
PFC operating mode : PFC3C
Configured PFC operating mode : PFC3C
```

Configuring Virtual Switch Links

To configure a port channel to be a virtual switch link, perform this task:

```
Router(config)# interface port-channel channel-num
```

Enters configuration mode for the specified port channel.

```
Router(config-if)# switch virtual link switch_num
```

Assigns the port channel to the virtual link for the specified switch.

```
Router(config-if)# no switch virtual link switch_num
```

Removes the VSL configuration.

Note: We recommend that you configure the VSL prior to converting the chassis into a VSS.
This example shows how to configure the virtual switch link:

```
Switch-1(config)# interface port-channel 10
Switch-1(config-if)# switch virtual link 1
Switch-1(config-if)# no shutdown
Switch-1(config)# interface tenGigabitEthernet 5/1
Switch-1(config-if)# channel-group 10 mode on
Switch-1(config-if)# no shutdown

Switch-2(config)# interface port-channel 25
Switch-2(config-if)# switch virtual link 2
Switch-2(config-if)# no shutdown
Switch-2(config)# interface tenGigabitEthernet 5/2
Switch-2(config-if)# channel-group 25 mode on
Switch-2(config-if)# no shutdown
```

### Displaying VSL Information

To display information about virtual switch link, perform one of these tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# show switch virtual link</td>
<td>Displays information about the virtual switch link.</td>
</tr>
<tr>
<td>Router# show switch virtual link port-channel</td>
<td>Displays information about the VSL port channel.</td>
</tr>
<tr>
<td>Router# show switch virtual link port</td>
<td>Displays information about the VSL ports.</td>
</tr>
</tbody>
</table>

This example shows how to display VSL information:

```
Router# show switch virtual link
VSL Status : UP
VSL Uptime : 1 day, 3 hours, 39 minutes
VSL SCP Ping : Pass
VSL ICC Ping : Pass
VSL Control Link : Gi1/4/2

Router# show switch virtual link port-channel
VSL Port Channel Information

Flags:  D - down        P - bundled in port-channel
        I - stand-alone        s - suspended
        H - Hot-standby (LACP only)
        R - Layer3        S - Layer2
        U - in use        N - not in use, no aggregation
        f - failed to allocate aggregator
        M - not in use, no aggregation due to minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated

  Group  Port-channel  Protocol    Ports
  --------------------------
  10   Po10(RU)         -        Te1/5/4(P)  Te1/5/5(P)
  20   Po20(RU)         -        Te2/5/4(P)  Te2/5/5(P)
```
Router# show switch virtual link port
VSL Link Info : Configured: 2 Operational: 1

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>Peer MAC</th>
<th>Peer Switch</th>
<th>Peer Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Te1/5/4</td>
<td>operational</td>
<td>0013.5fcb.1480</td>
<td>2</td>
<td>Te2/5/4</td>
</tr>
<tr>
<td>Te1/5/5</td>
<td>link_down</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>Last operational</th>
<th>Current packet</th>
<th>Last Diag</th>
<th>Time since</th>
</tr>
</thead>
<tbody>
<tr>
<td>Te1/5/4</td>
<td>No failure</td>
<td>Hello bidir</td>
<td>Never ran</td>
<td>7M:51S</td>
</tr>
<tr>
<td>Te1/5/5</td>
<td>No failure</td>
<td>No failure</td>
<td>Never ran</td>
<td>7M:51S</td>
</tr>
</tbody>
</table>

* T5 = min_rx * multiplier

### Configuring VSL QoS

The virtual switching system automatically configures VSL ports for trust CoS, using default CoS mappings (you cannot change the mappings on VSL ports).

For line cards that support per-ASIC configuration, the VSL configuration applies to all ports on the same ASIC (including any non-VSL ports).

The virtual switching system disables the QoS commands on VSL ports (and any non-VSL ports on the same ASIC). For example, you cannot use QoS queuing or map commands on VSL ports.

If your VSS includes WS-X6708-10GE switching modules, enter the `mls qos 10g-only` global configuration command, to ensure that all eight QoS queues are enabled for the 10-Gigabit Ethernet ports.

If you connect a Supervisor Engine 10-Gigabit Ethernet port to a switching module 1-Gigabit Ethernet port, you need to enter the `no mls qos channel-consistency` command on the VSL port channel interface for the EtherChannel to support ports with and without strict-priority queues.

### Subcommands for VSL Port Channels

On a VSL port channel, only a subset of interface subcommands are available in the command console. Table 4-2 describes the available interface subcommands.

**Table 4-2 Interface Subcommands for VSL Port Channels**

<table>
<thead>
<tr>
<th>Subcommand</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Sets a command to its defaults.</td>
</tr>
<tr>
<td>description</td>
<td>Enters a text description for the interface.</td>
</tr>
<tr>
<td>exit</td>
<td>Exits from interface configuration mode.</td>
</tr>
</tbody>
</table>
### Interface Subcommands for VSL Port Channels (continued)

<table>
<thead>
<tr>
<th>Subcommand</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>load-interval</td>
<td>Specifies interval for load calculation for an interface.</td>
</tr>
<tr>
<td>logging</td>
<td>Configures logging for interface.</td>
</tr>
<tr>
<td>mls</td>
<td>Specifies multilayer switching subcommands.</td>
</tr>
<tr>
<td>no</td>
<td>Disables a command, or sets the command defaults.</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shuts down the selected interface.</td>
</tr>
<tr>
<td>switch virtual link</td>
<td>Specifies the switch associated with this port channel.</td>
</tr>
<tr>
<td>vslp</td>
<td>Specifies VSLP interface configuration commands.</td>
</tr>
</tbody>
</table>

### Subcommands for VSL Ports

If a port is included in a VSL port channel, only a subset of interface subcommands are available in the command console. Table 4-3 describes the available interface subcommands.

**Table 4-3 Interface Subcommands for VSL Ports**

<table>
<thead>
<tr>
<th>Subcommand</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>channel-group</td>
<td>Adds the interface to the specified channel group.</td>
</tr>
<tr>
<td>default</td>
<td>Sets a command to its defaults.</td>
</tr>
<tr>
<td>description</td>
<td>Adds a description to the interface.</td>
</tr>
<tr>
<td>exit</td>
<td>Exits from interface configuration mode.</td>
</tr>
<tr>
<td>load-interval</td>
<td>Specifies interval for load calculation for an interface.</td>
</tr>
<tr>
<td>logging</td>
<td>Configures logging for the interface.</td>
</tr>
<tr>
<td>no</td>
<td>Disables a command, or sets the command defaults.</td>
</tr>
<tr>
<td>priority-queue</td>
<td>Configures a COS map or priority queue limit.</td>
</tr>
<tr>
<td>rcv-queue</td>
<td>Configures a COS map or tail-drop threshold.</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shuts down the selected interface.</td>
</tr>
<tr>
<td>vslp</td>
<td>Specifies VSLP interface configuration commands.</td>
</tr>
<tr>
<td>wrr-queue</td>
<td>Configures parameters for WRR queue.</td>
</tr>
</tbody>
</table>
Configuring Multichannel EtherChannels

Configure multichassis EtherChannels (MECs) as you would for a regular EtherChannel. The virtual switching system will recognize that the EtherChannel is a MEC when ports from both chassis are added to the EtherChannel. You can verify the MEC configuration by entering the `show etherchannel` command.

One VSS supports a maximum of 128 port channels.

The following sections provide additional details about MECs:
- Configuring EtherChannel Hash-Distribution Algorithm, page 4-37
- Configuring LACP 1:1 Redundancy, page 4-38

Configuring EtherChannel Hash-Distribution Algorithm

Releases earlier than 12.2(33)SXH support a load-distribution algorithm called the fixed algorithm. When you add a port to the EtherChannel or delete a port from the EtherChannel, the switch updates the Port ASIC for each port in the EtherChannel, which causes a short outage on each port.

Release 12.2(33)SXH and later releases support an additional algorithm called the adaptive algorithm. The adaptive algorithm does not need to update the port ASIC for existing member ports.

The default algorithm for VSS is the adaptive algorithm. You can configure the choice of algorithm globally, or for specific interfaces.

When you change the algorithm, the change is applied at the next member link event. Example events include link down, up, addition, deletion, no shutdown, and shutdown. When you enter the command to change the algorithm, the command console issues a warning that the command does not take effect until the next member link event.

**Note**

Some external devices require the fixed algorithm. For example, the service control engine (SCE) requires incoming and outgoing packets to use the same port.

Configuring the Hash-Distribution Algorithm Globally

To configure the load-sharing algorithm globally, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config)# `port-channel hash-distribution (adaptive</td>
<td>fixed)`</td>
</tr>
<tr>
<td>Router(config)# `(no</td>
<td>default) port-channel hash-distribution`</td>
</tr>
</tbody>
</table>

This example shows how to globally set the hash distribution to adaptive:

```
Router(config)# `port-channel hash-distribution adaptive`
```
Configuring the Hash-Distribution Algorithm for a Port Channel

To configure the hash distribution algorithm for a specific port channel, perform this task:

```
Command                                      Purpose
---                                          ---
Router(config)# interface port-channel channel-num      Enters interface configuration mode for the port channel.
Router(config-if)# port-channel port         Sets the load-sharing algorithm for this interface.
    hash-distribution {adaptive | fixed}       Note: The adaptive hash distribution algorithm is not available on VSL port channels.
Router(config-if)# (no | default) port-channel port
    hash-distribution                        Resets the load-sharing algorithm to its default (adaptive).
```

This example shows how to set the hash distribution algorithm to adaptive on port channel 10:
```
Router (config)# interface port-channel 10
Router (config-if)# port-channel port hash-distribution adaptive
```

Configuring LACP 1:1 Redundancy

The LACP 1:1 redundancy feature provides an EtherChannel configuration with one active link and fast switchover to a hot standby link.

Understanding LACP 1:1 redundancy

To use LACP 1:1 redundancy, you configure a LACP EtherChannel with two ports (one active and one standby). If the active link goes down, the EtherChannel stays up and the system performs fast switchover to the hot standby link. When the failed link becomes operational again, the EtherChannel performs another fast switchover to revert to the original active link.

For the LACP 1:1 redundancy feature to work correctly, especially the fast switchover capability, the feature needs to be enabled at both ends of the link.

Configuring LACP 1:1 Redundancy

For the LACP 1:1 redundancy feature, the LACP EtherChannel must contain exactly two links, of which only one is active.

Link 1 must have a higher port priority than link 2 and the LACP max-bundle must be set to 1. This configuration results in link 1 being active and link 2 being in hot standby state. LACP min-links is set to 1, so that the LACP EtherChannel transitions to the link-up state with one active link.

To configure the LACP 1:1 redundancy feature, perform this task:

```
Command                                      Purpose
---                                          ---
Step 1 Router(config)# interface port-channel number          Selects an LACP port channel interface.
Step 1 Router(config-if)# port-channel lacp
    fast-switchover                             Enables the fast switchover feature for this EtherChannel.
Step 2 Router(config-if)# port-channel max-bundle 1           Sets the maximum number of active member ports to be one.
Step 3 Router(config-if)# port-channel min-links 1             Sets the minimum number of active member ports to be one.
```
Note For the LACP 1:1 redundancy feature to work correctly, especially the fast switchover capability, the feature needs to be enabled at both ends of the EtherChannel.

This example shows how to configure a LACP EtherChannel with 1:1 redundancy. Gigabitethernet 1/3/6 is the active link, as it is configured with a higher port priority:

```
Router# configure terminal
Router# lacp system-priority 33000
Router(config-if)# interface gigabitethernet 1/3/6
Router(config-if)# channel-protocol lacp
Router(config-if)# channel-group 1 mode active
Router(config-if)# lacp port-priority 33000
Router(config-if)# end
Router(config-if)# interface gigabitethernet 2/3/6
Router(config-if)# channel-protocol lacp
Router(config-if)# channel-group 1 mode active
Router(config-if)# end
Router(config-if)# interface port-channel 1
Router(config-if)# port-channel lacp fast-switchover
Router(config-if)# port-channel max-bundle 1
Router(config-if)# port-channel min-links 1
Router(config-if)# end
```

### Configuring Dual-Active Detection

The following sections describe how to configure dual-active detection:

- Configuring Enhanced PAgP Dual-Active Detection, page 4-39
- Configuring BFD Dual-Active Detection, page 4-41
- Configuring the Exclusion List, page 4-42
- Displaying Dual-Active Detection, page 4-42

### Configuring Enhanced PAgP Dual-Active Detection

If enhanced PAgP is running on the MECs between the VSS and its access switches, the VSS can use enhanced PAgP messaging to detect dual-active scenario.

By default, PAgP dual-active detection is enabled. However, the enhanced messages are only sent on port channels with trust mode enabled (see the trust mode description below).
Before changing PAgP dual-active detection configuration, ensure that all port channels with trust mode enabled are in administrative down state. Use the `shutdown` command in interface configuration mode for the port channel. Remember to use the `no shutdown` command to reactivate the port channel when you are finished configuring dual-active detection.

To enable or disable PAgP dual-active detection, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>Router(config)# switch virtual domain domain_id</td>
<td>Enters virtual switch submode.</td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td>Router(config-vs-domain)# dual-active detection pagp trust channel-group group_number</td>
<td>Enables trust mode for the specified port channel.</td>
</tr>
<tr>
<td>Router(config-vs-domain)# no dual-active detection pagp trust channel-group group_number</td>
<td>Disables trust mode for the specified port channel.</td>
</tr>
</tbody>
</table>

You must configure trust mode on the port channels that will detect PAgP dual-active detection. By default, trust mode is disabled.

If PAgP dual-active detection is enabled, you must place the port channel in administrative down state before changing the trust mode. Use the `shutdown` command in interface configuration mode for the port channel. Remember to use the `no shutdown` command to reactivate the port channels when you are finished configuring trust mode on the port channel.

To configure trust mode on a port channel, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>Router(config)# switch virtual domain domain_id</td>
<td>Enters virtual switch submode.</td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td>Router(config-vs-domain)# dual-active detection pagp trust channel-group group_number</td>
<td>Enables trust mode for the specified port channel.</td>
</tr>
<tr>
<td>Router(config-vs-domain)# no dual-active detection pagp trust channel-group group_number</td>
<td>Disables trust mode for the specified port channel.</td>
</tr>
</tbody>
</table>

This example shows how to enable PAgP dual-active detection:

```
Router(config)# interface port-channel 20
Router(config-if)# shutdown
Router(config-if)# exit
Router(config)# switch virtual domain 100
Router(config-vs-domain)# dual-active detection pagp trust channel-group 20
Router(config-vs-domain)# exit
Router(config)# interface port-channel 20
Router(config-if)# no shutdown
Router(config-if)# exit
```

This example shows the error message if you try to enable PAgP dual-active detection when a trusted port channel is not shut down first:

```
Router(config)# switch virtual domain 100
Router(config-vs-domain)# dual-active detection pagp
Trusted port-channel 20 is not administratively down.
To change the pagp dual-active configuration, "shutdown" these port-channels first.
Remember to "no shutdown" these port-channels afterwards.
```
This example shows the error message if you try to configure trust mode for a port channel that is not shut down first:

```
Router(config)# switch virtual domain 100
Router(config-vs-domain)# dual-active detection pagp trust channel-group 20
```

Error message:
```
Trusted port-channel 20 is not administratively down. To change the pagp dual-active trust configuration, "shutdown" the port-channel first. Remember to "no shutdown" the port-channel afterwards.
```

### Configuring BFD Dual-Active Detection

For the BFD dual-active detection, you must configure dual-active interface pairs that will act as BFD messaging links, and enable the BFD dual-active detection mechanism.

To configure BFD dual-active detection, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>Router(config)# switch virtual domain domain_id</td>
<td>Enters virtual switch submode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>Router(config-vs-domain)# dual-active detection bfd</td>
<td>Enables BFD dual-active detection method. By default, BFD detection is enabled.</td>
</tr>
<tr>
<td>Router(config-vs-domain)# no dual-active detection bfd</td>
<td>Disables BFD dual-active detection method.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>Router(config-vs-domain)# dual-active pair interface int_1 interface int_2 bfd</td>
<td>Configures the dual-active pair of interfaces.</td>
</tr>
<tr>
<td>The interfaces must be directly connected (a single Layer 3 hop).</td>
<td></td>
</tr>
<tr>
<td>Router(config-vs-domain)# no dual-active pair interface int_1 interface int_2 bfd</td>
<td>Deletes the dual-active pair of interfaces.</td>
</tr>
</tbody>
</table>

When you configure the dual-active interface pairs, note the following information:

- The individual ports must be configured first with both an IP address and BFD configuration. The configuration is validated when you add the dual-active interface pair.
- The IP addresses assigned to the dual-active pair must be from two different networks or subnetworks.
- The BFD timers must be configured with the same values on the ports at both ends of the link to ensure proper operation of Layer 3 BFD dual-active detection.
- The MAC address cannot be specified on the interface.

**Note**

We recommend that you configure a short BFD interval and small multiplier value (such as 50 to 100 ms for the interval and 3 as the multiplier value). If the interval and multiplier values are large, there is a long delay before the system initiates dual-active mode recovery. A VSS operating in dual-active mode can cause network instability.

This example shows how to configure interfaces for BFD dual-active detection:

```
Router (config)# interface gigabitethernet 1/9/48
Router (config-if)# no switchport
Router (config-if)# ip address 200.230.230.231 255.255.255.0
Router (config-if)# bfd interval 100 min_rx 100 multiplier 50
Router (config-if)# no shutdown
Router (config-if)# interface gigabitethernet 2/1/48
```
Configuring Virtual Switching Systems

Router (config-if)# no switchport
Router (config-if)# ip address 201.230.230.231 255.255.255.0
Router (config-if)# bfd interval 100 min_rx 100 multiplier 50
Router (config-if)# no shutdown
Router (config-if)# exit
Router (config)# switch virtual domain 100
Router (config-vs-domain)# dual-active detection bfd
Router (config-vs-domain)# dual-active pair interface g 1/9/48 interface g 2/1/48 bfd
adding a static route 200.230.230.0 255.255.255.0 Gi2/1/48 for this dual-active pair
adding a static route 201.230.230.0 255.255.255.0 Gi1/9/48 for this dual-active pair
Router (config-vs-domain)# exit
Router (config)# exit
Router# show switch virtual dual-active bfd
Bfd dual-active detection enabled: Yes
Bfd dual-active interface pairs configured:
  interface1 Gi1/9/48 interface2 Gi2/1/48

Configuring the Exclusion List

When dual-active scenario is detected, part of the recovery action is for the chassis to shut down all of its non-VSL interfaces. You can specify one or more interfaces to be excluded from this action (for example, to exclude the interface you use for remote access to the chassis).

To specify interfaces that are not to be shut down by dual-active recovery, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config)# switch virtual domain domain_id</td>
<td>Enters virtual switch submode.</td>
</tr>
<tr>
<td>Router(config-vs-domain)# dual-active exclude interface int</td>
<td>Specifies an interface to exclude from shutting down in dual-active recovery.</td>
</tr>
<tr>
<td>Router(config-vs-domain)# no dual-active exclude interface int</td>
<td>Removes the interface from the exclusion list.</td>
</tr>
</tbody>
</table>

When you configure the exclusion list, note the following information:

- The interface must be a physical port configured with an IP address.
- The interface must not be a VSL port.
- The interface must not be in use for IP BFD dual-active detection.

This example shows how to configure an interface as an exclusion:

Router(config)# switch virtual domain 100
Router (config-vs-domain)# dual-active exclude interface gigabitethernet 1/5/5

Displaying Dual-Active Detection

To display information about dual-active detection, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# show switch virtual dual-active bfd</td>
<td>Displays information about dual-active detection configuration and status.</td>
</tr>
</tbody>
</table>
Chapter 4  Configuring Virtual Switching Systems

This example shows how to display information for BFD dual-active detection:

Router# show switch virtual dual-active bfd
Bfd dual-active detection enabled: Yes

No bfd dual-active interface pairs configured

This example shows how to display the summary status for dual-active detection:

Router# 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: No

This example shows how to display PAgP status and the channel groups with trust mode enabled:

Router# show pagp dual-active
PAgP dual-active detection enabled: Yes
PAgP dual-active version: 1.1

Channel group 3 dual-active detect capability w/nbrs Dual-Active trusted group: No

<table>
<thead>
<tr>
<th>Port</th>
<th>Detect Capable</th>
<th>Partner</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa1/2/33</td>
<td>No</td>
<td>None</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Channel group 4
Dual-Active trusted group: Yes
No interfaces configured in the channel group

Channel group 5
Dual-Active trusted group: Yes
Channel group 5 is not participating in PAGP

Channel group 10 dual-active detect capability w/nbrs Dual-Active trusted group: Yes

<table>
<thead>
<tr>
<th>Port</th>
<th>Detect Capable</th>
<th>Partner</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>G1/6/1</td>
<td>Yes</td>
<td>eden-nbr-</td>
<td>1.1</td>
</tr>
<tr>
<td>G1/5/1</td>
<td>Yes</td>
<td>eden-nbr-</td>
<td>1.1</td>
</tr>
</tbody>
</table>

Channel group 11 dual-active detect capability w/nbrs Dual-Active trusted group: No

<table>
<thead>
<tr>
<th>Port</th>
<th>Detect Capable</th>
<th>Partner</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>G1/6/2</td>
<td>Yes</td>
<td>eden-nbr-</td>
<td>1.1</td>
</tr>
<tr>
<td>G1/5/2</td>
<td>Yes</td>
<td>eden-nbr-</td>
<td>1.1</td>
</tr>
</tbody>
</table>

Channel group 12 dual-active detect capability w/nbrs Dual-Active trusted group: Yes

<table>
<thead>
<tr>
<th>Port</th>
<th>Detect Capable</th>
<th>Partner</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa1/2/13</td>
<td>Yes</td>
<td>eden-nbr-</td>
<td>1.1</td>
</tr>
<tr>
<td>Fa1/2/14</td>
<td>Yes</td>
<td>eden-nbr-</td>
<td>1.1</td>
</tr>
<tr>
<td>G1/2/15</td>
<td>Yes</td>
<td>eden-nbr-</td>
<td>1.1</td>
</tr>
<tr>
<td>G1/2/16</td>
<td>Yes</td>
<td>eden-nbr-</td>
<td>1.1</td>
</tr>
</tbody>
</table>

Note

The `show switch virtual dual-active pagp` command displays the same output as the `show pagp dual-active` command.