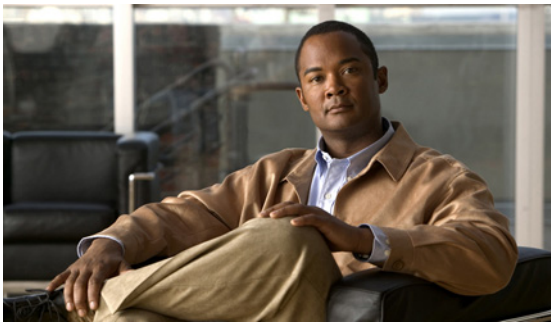

Quick Reference to Best Practices for Cisco IOS on Catalyst 6500 Series Switches

This document is a quick reference to the best practices that have been developed by Cisco for the features in Cisco IOS software on the Catalyst 6500 Series Switches. This document supplements, but does not replace, IOS software documentation.

Note Best Practice recommendations in this document have been tested and verified in Cisco's Data Center Test Lab (DCTL) at RTP, NC.

This document consists of feature-specific sections that follow a consistent pattern, making the type of information in each subsection easily recognizable. Best practices do not need to be implemented simultaneously, but sections are cross referenced to related best practices, making it easier to implement all related best practices at the same time.

To use this document, you should be familiar with the following:

- The Cisco IOS Software user interface—For more information, see the *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.2:

  http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/ffun_c.html
- The Cisco IOS software features in Release 12.2SX—For more information, see the release notes.
  - For Release 12.2(18)SXF and rebuilds:

    http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/release/notes/OL_4164.html
  - For Release 12.2(33)SXH and rebuilds:

    http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/release/notes/ol_14271.html

Note

- When deploying new hardware, enter the **diagnostic start system test all** command (available in Release 12.2(33)SXH and later) to run the Generic Online Diagnostics (GOLD) on-demand tests before putting the hardware into service. With earlier releases, run the test individually.
- Before you RMA hardware, use the Generic Online Diagnostics (GOLD) on-demand tests to confirm that a problem exists.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

This document provides best practices for these features:

1. Best Practices for Layer 2 Features

Cisco Catalyst 6500 best practices are defined for the following layer 2 technologies:

1.1 Best Practices for the Rapid Per-VLAN Spanning Tree Protocol (RPVST)

These sections describe best practices for RPVST:

1.1.1 Description of RPVST

RPVST is a Layer 2 link-management protocol that supports path redundancy and prevents undesirable loops in the network. For a Layer 2 Ethernet network to function properly, only one active Layer 2 path can exist between any two network devices.

RPVST operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

1.1.2 Benefits of the RPVST Best Practices

Without RPVST, or one of the other spanning tree protocols, when there is a physical Layer 2 loop, Layer 2 frames could loop indefinitely and consume all the bandwidth of the network.

1.1.3 Features Incompatible with RPVST

RPVST obsoletes BackboneFast and UplinkFast as it has built in mechanisms that achieve the same.

- UplinkFast
- BackboneFast

1.1.4 Guidelines and Restrictions for RPVST

- Use the default RPVST timer values.
- Create and maintain a Layer 2 topology diagram of your network.
- Observe these limitations on the number of spanning tree and logical interface instances:
  - For Release 12.2(18)SXF and rebuilds and earlier releases:

    http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/release/notes/OL_4164.html#Spanning_Tree_Troubleshooting
  - For Release 12.2(33)SXH and later releases:

    http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/release/notes/ol_14271.html#Spanning_Tree_Troubleshooting

1.1.5 Recommended RPVST Configuration

The following sections describe the recommended RPVST configuration.

1.1.5.1 Recommended Global Configuration

Enable RPVST

Enable Rapid Per-VLAN Spanning Tree protocol (RPVST):

```
Router(config)# spanning-tree mode rapid-pvst
```

Configure Root Bridge Ports

Plan the Layer 2 topology of your network and configure the root bridge port of each VLAN. Use the procedures in the "Configuring the Root Bridge" section of the customer documentation and the "Configuring a Secondary Root Bridge" section.

Note Do not rely on the default spanning tree that RPVST creates. For reliable operation, you must select and configure the root bridge ports.

1.1.5.2 Recommended General Port Configuration

None; use the specific port-type recommendations.

1.1.5.3 Recommended Access Port Configuration

If the port on the far-end device is configured to participate in STP and if the ports are connected by a point-to-point link, enter this command to support the most rapid convergence:

```
Router(config-if)# spanning-tree link-type point-to-point
```

Note If the link is full duplex, there is no need to enter this command as software will detect it.

1.1.5.4 Recommended Layer 2 Trunk Port Configuration

If the port on the far-end device is configured to participate in STP, enter this command to support the most rapid convergence:

```
Router(config-if)# spanning-tree link-type point-to-point
```

1.1.5.5 Recommended Layer 3 Port Configuration

Not applicable.

1.1.5.6 Recommended SVI Configuration

Not applicable.

1.1.6 Documentation for RPVST

See the "Understanding RSTP" section of the customer documentation for more information about RPVST.

1.1.7 Related Features and Best Practices

- 1.2 Best Practices for STP PortFast, page 5
- 1.3 Best Practices for STP BPDU Guard, page 7
- 1.4 Best Practices for STP EtherChannel Guard, page 9
- 1.5 Best Practices for STP Root Guard, page 10
- 1.6 Best Practices for STP Loop Guard, page 12
- 1.8 Best Practices for UniDirectional Link Detection (UDLD), page 15

1.2 Best Practices for STP PortFast

These sections describe best practices for STP PortFast:

- 1.2.1 Description of STP PortFast
- 1.2.2 Benefits of the STP PortFast Best Practices
- 1.2.3 Features Incompatible with STP PortFast
- 1.2.4 Guidelines and Restrictions for STP PortFast
- 1.2.5 Recommended STP PortFast Configuration
- 1.2.6 Documentation for STP PortFast

1.2.1 Description of STP PortFast

STP PortFast causes a Layer 2 LAN port to enter the forwarding state immediately, bypassing the listening and learning states.

1.2.2 Benefits of the STP PortFast Best Practices

STP PortFast skips the normal listening and learning states of STP, which is 30 seconds with the ForwardDelay time set to the default value of 15 seconds.

STP PortFast prevents the generation of STP Topology Change Notifications (TCNs), which are not meaningful from ports that do not receive STP BPDUs. For example, enabling STP PortFast on access ports prevents the TCNs that would otherwise occur when the connected computer is turned on.

1.2.3 Features Incompatible with STP PortFast

Loopguard has no affect on portfast enabled ports.

- STP Loop Guard

1.2.4 Guidelines and Restrictions for STP PortFast

- Configure STP PortFast only on ports that are connected to end host devices that terminate VLANs and from which the port should never receive STP BPDUs, such as:
  - Workstations
  - Servers
  - Ports on routers that are not configured to support bridging
- Configure STP BPDU Guard along with STP PortFast to shut down STP PortFast-enabled ports if they receive a BPDU.

1.2.5 Recommended STP PortFast Configuration

The following sections describe the recommended STP PortFast configuration.

1.2.5.1 Recommended Global Configuration

None.

1.2.5.2 Recommended General Port Configuration

None; use the recommendation for each port type.

1.2.5.3 Recommended Access Port Configuration

Access Ports that Terminate VLANs

On any access port that connects to a device that terminates VLANs (for example, a port that connects to an end station), enable STP PortFast:

```
Router(config-if)# spanning-tree portfast
```

Access Ports that Propagate VLANs

On any access port that connects to a device that propagates VLANs (for example, a port that connects to another switch or a port that connects to a router that is configured to support bridging), disable STP PortFast:

```
Router(config-if)# spanning-tree portfast disable
```

1.2.5.4 Recommended Layer 2 Trunk Port Configuration

Trunk Ports that Terminate VLANs

On any trunk port that connects to a device that terminates VLANs (for example, a port that connects to an end station), enable STP PortFast:

```
Router(config-if)# spanning-tree portfast trunk
```

Trunk Ports that Propagate VLANs

On any trunk port that connects to a device that propagates VLANs (for example, a port that connects to another switch or a port that connects to a router that is configured to support bridging), disable STP PortFast:

```
Router(config-if)# no spanning-tree portfast enable
```

1.2.5.5 Recommended Layer 3 Port Configuration

Not applicable.

1.2.5.6 Recommended SVI Configuration

Not applicable.

1.2.6 Documentation for STP PortFast

See the "Understanding How PortFast Works" section of the customer documentation for more information about STP PortFast.

1.2.7 Related Features and Best Practices

1.1 Best Practices for the Rapid Per-VLAN Spanning Tree Protocol (RPVST), page 3

1.3 Best Practices for STP BPDU Guard, page 7

1.3 Best Practices for STP BPDU Guard

These sections describe best practices for STP BPDU Guard:

1.3.1 Description of STP BPDU Guard

STP BPDU Guard shuts down ports that receive BPDUs.

1.3.2 Benefits of the STP BPDU Guard Best Practices

STP BPDU Guard complements the functionality of STP PortFast. On STP PortFast-enabled ports, STP BPDU Guard provides the protection against Layer 2 loops that STP cannot provide when STP PortFast is enabled.

1.3.3 Features Incompatible with STP BPDU Guard

- STP Loop Guard

1.3.4 Guidelines and Restrictions for STP BPDU Guard

None.

1.3.5 Recommended STP BPDU Guard Configuration

The following sections describe the recommended STP BPDU Guard configuration.

1.3.5.1 Recommended Global Configuration

The following global command enables STP BPDU Guard on all ports where STP PortFast is enabled:

```
Router(config)# spanning-tree portfast bpduguard default
```

1.3.5.2 Recommended General Port Configuration

Not applicable.

1.3.5.3 Recommended Access Port Configuration

Not applicable.

1.3.5.4 Recommended Layer 2 Trunk Port Configuration

Not applicable.

1.3.5.5 Recommended Layer 3 Port Configuration

Not applicable.

1.3.5.6 Recommended SVI Configuration

Not applicable.

1.3.6 Documentation for STP BPDU Guard

See the "Understanding How BPDU Guard Works" section of the customer documentation for more information about STP BPDU Guard.

1.3.7 Related Features and Best Practices

1.1 Best Practices for the Rapid Per-VLAN Spanning Tree Protocol (RPVST), page 3

1.2 Best Practices for STP PortFast, page 5

1.4 Best Practices for STP EtherChannel Guard

These sections describe best practices for STP EtherChannel Guard:

1.4.1 Description of STP EtherChannel Guard

EtherChannel guard detects a misconfigured EtherChannel where interfaces on the Catalyst 6500 series switch are configured as an EtherChannel while interfaces on the other device are not, or not all the interfaces on the other device are in the same EtherChannel.

In response to misconfiguration detected on the other device, EtherChannel guard puts interfaces on the Catalyst 6500 series switch into the errdisabled state.

1.4.2 Benefits of the STP EtherChannel Guard Best Practices

Use the default enabled state of STP EtherChannel Guard to avoid an EtherChannel misconfiguration that could cause a Layer 2 loop and allow Layer 2 frames to loop indefinitely.

1.4.3 Features Incompatible with STP EtherChannel Guard

None.

1.4.4 Guidelines and Restrictions for STP EtherChannel Guard

None.

1.4.5 Recommended STP EtherChannel Guard Configuration

The following sections describe the recommended STP EtherChannel Guard configuration.

1.4.5.1 Recommended Global Configuration

Ensure STP EtherChannel Guard is enabled globally:

```
Router(config)# spanning-tree etherchannel guard misconfig
```

1.4.5.2 Recommended General Port Configuration

None; use the global configuration.

1.4.5.3 Recommended Access Port Configuration

None; use the global configuration.

1.4.5.4 Recommended Layer 2 Trunk Port Configuration

None; use the global configuration.

1.4.5.5 Recommended Layer 3 Port Configuration

None; use the global configuration.

1.4.5.6 Recommended SVI Configuration

None; use the global configuration.

1.4.6 Documentation for STP EtherChannel Guard

See the "Understanding How EtherChannel Guard Works" section of the customer documentation for more information about STP EtherChannel Guard.

1.4.7 Related Features and Best Practices

1.11 Best Practices for EtherChannel, page 20

1.5 Best Practices for STP Root Guard

These sections describe best practices for STP Root Guard:

1.5.1 Description of STP Root Guard

Root guard prevents ports from becoming STP root ports.

1.5.2 Benefits of the STP Root Guard Best Practices

Use STP Root Guard to prevent unsuitable ports from becoming STP root ports. An example of an unsuitable port is a port that link to a device that is outside direct network administrative control.

1.5.3 Features Incompatible with STP Root Guard

Loopguard has no affect on portfast enabled ports.

- STP Loop Guard

1.5.4 Guidelines and Restrictions for STP Root Guard

None.

1.5.5 Recommended STP Root Guard Configuration

The following sections describe the recommended STP Root Guard configuration.

1.5.5.1 Recommended Global Configuration

None.

1.5.5.2 Recommended General Port Configuration

On any port that should never be an STP root port, enable STP root guard:

```
Router(config-if)# spanning-tree guard root
```

1.5.5.3 Recommended Single-VLAN Access Port Configuration

No specific port-type configuration required; use the recommended general port configuration.

1.5.5.4 Recommended Layer 2 Trunk Port Configuration

No specific port-type configuration required; use the recommended general port configuration.

1.5.5.5 Recommended Layer 3 Port Configuration

No specific port-type configuration required; use the recommended general port configuration.

1.5.5.6 Recommended SVI Configuration

Not applicable.

1.5.6 Documentation for STP Root Guard

See the "Understanding How Root Guard Works" section of the customer documentation for more information about STP Root Guard.

1.5.7 Related Features and Best Practices

1.1 Best Practices for the Rapid Per-VLAN Spanning Tree Protocol (RPVST), page 3

1.6 Best Practices for STP Loop Guard

These sections describe best practices for loop guard:

1.6.1 Description of STP Loop Guard

Loop guard is a Cisco proprietary optimization for the spanning tree protocol (STP). Loop guard protects Layer 2 networks from loops that occur when something prevents the normal forwarding of BPDUs on point-to-point links (for example, a network interface malfunction or a busy CPU).

1.6.2 Benefits of the STP Loop Guard Best Practices

Loop guard complements the protection against unidirectional link failures provided by UDLD. Loop guard isolates failures and lets STP converge to a stable topology with the failed component excluded from the STP topology.

1.6.3 Features Incompatible with STP Loop Guard

- STP Root Guard
- STP PortFast

1.6.4 Guidelines and Restrictions for STP Loop Guard

Loop guard operates as a component of STP. There are no compatibility issues between loop guard and the version of STP configured on the network or with the configuration applied to STP timers in the network.

1.6.5 Recommended STP Loop Guard Configuration

The following sections describe the recommended loop guard configuration.

1.6.5.1 Recommended Global Configuration

Enable loop guard globally:

```
Router(config)# spanning-tree loopguard default
```

1.6.5.2 Recommended General Port Configuration

Not applicable; use the recommended global configuration.

1.6.5.3 Recommended Single-VLAN Access Port Configuration

Not applicable; use the recommended global configuration.

1.6.5.4 Recommended Layer 2 Trunk Port Configuration

Not applicable; use the recommended global configuration.

1.6.5.5 Recommended Layer 3 Port Configuration

No specific port-type configuration required; use the recommended global configuration.

1.6.5.6 Recommended SVI Configuration

Not applicable.

1.6.6 Documentation for STP Loop Guard

See the "Understanding How Loop Guard Works" section of the customer documentation for more information about loop guard.

1.6.7 Related Features and Best Practices

1.1 Best Practices for the Rapid Per-VLAN Spanning Tree Protocol (RPVST), page 3

1.7 Best Practices for Extended System ID

These sections describe best practices for Extended System ID:

1.7.1 Description of Extended System ID

A 12-bit extended system ID field is part of the STP bridge ID. Chassis that have only 64 MAC addresses always use the 12-bit extended system ID. On chassis that have 1024 MAC addresses, you can enable use of the extended system ID. STP uses the VLAN ID as the extended system ID.

1.7.2 Benefits of the Extended System ID Best Practices

You must enable the extended system ID to configure extended range VLANs (1006-4094).

You must enable the extended system ID if any switches in the VTP domain have it enabled.

1.7.3 Features Incompatible with Extended System ID

None.

1.7.4 Guidelines and Restrictions for Extended System ID

The extended system ID is enabled permanently on chassis that support 64 MAC addresses.

1.7.5 Recommended Extended System ID Configuration

The following sections describe the recommended Extended System ID configuration.

1.7.5.1 Recommended Global Configuration

Enable the extended system ID:

```
Router(config)# spanning-tree extend system-id
```

1.7.5.2 Recommended General Port Configuration

No port configuration required; use the global configuration.

1.7.5.3 Recommended Access Port Configuration

No port configuration required; use the global configuration.

1.7.5.4 Recommended Layer 2 Trunk Port Configuration

No port configuration required; use the global configuration.

1.7.5.5 Recommended Layer 3 Port Configuration

No specific port-type configuration required; use the recommended global configuration.

1.7.5.6 Recommended SVI Configuration

Not applicable.

1.7.6 Documentation for Extended System ID

See the "Extended System ID" section of the customer documentation for more information.

1.7.7 Related Features and Best Practices

None.

1.8 Best Practices for UniDirectional Link Detection (UDLD)

These sections describe best practices for UniDirectional Link Detection (UDLD):

1.8.1 Description of UDLD

The Cisco-proprietary UDLD protocol monitors the physical configuration of the links between devices and ports that support UDLD. UDLD detects the existence of unidirectional links. When a unidirectional link is detected, UDLD puts the affected port into the errdisabled state and alerts the user. UDLD can operate in either normal or aggressive mode.

Normal-mode UDLD classifies a link as unidirectional if the received UDLD packets do not contain information that is correct for the neighbor device. In addition to the functionality of normal mode UDLD, aggressive-mode UDLD puts ports into the errdisabled state if the relationship between two previously synchronized neighbors cannot be reestablished.

1.8.2 Benefits of the UDLD Best Practices

Configure UDLD to prevent problems from these situations:

- Spanning tree topology loops caused by unidirectional links
- Incorrect cabling of unbundled fiber strands
- Transceiver or link hardware malfunction
- Incorrect or excessive flooding of packets

- Loss of traffic without notice (also know as black holing)

1.8.3 Features Incompatible with UDLD

None.

1.8.4 Guidelines and Restrictions for UDLD

- UDLD can only detect unidirectional links when UDLD is enabled on both ends of a link.
- The UDLD best practices in this document assume that the hello, forward-delay, and maximum aging STP timers are configured with their default values.
- Use UDLD with autonegotiation or link negotiation correctly configured on the link.
- On 802.1Q trunks, UDLD requires that the Native VLAN be correctly configured and that the VLAN be defined and active. There is no requirement for it to carry any traffic.

1.8.5 Recommended UDLD Configuration

The following sections describe the recommended UDLD configuration.

1.8.5.1 Recommended Global Configuration

Enable enable aggressive mode UDLD globally:

```
Router(config)# udld aggressive
```

Note This global command enables UDLD only on fiber-optic LAN ports.

1.8.5.2 Recommended General Port Configuration

In a well designed redundant network, enable aggressive mode UDLD on non-fiber LAN ports that connect to devices that support UDLD:

```
Router(config-if)# udld port aggressive
```

1.8.5.3 Recommended Single-VLAN Access Port Configuration

No specific port-type configuration required; use the general port configuration.

1.8.5.4 Recommended Layer 2 Trunk Port Configuration

No specific port-type configuration required; use the general port configuration.

1.8.5.5 Recommended Layer 3 Port Configuration

No specific port-type configuration required; use the recommended general port configuration.

1.8.5.6 Recommended SVI Configuration

Not applicable.

1.8.6 Documentation for UDLD

See this publication for more information about UDLD:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/udld.html

1.8.7 Related Features and Best Practices

These sections describe features that are recommended for use with UDLD:

- 1.9 Best Practices for Autonegotiation and Link Negotiation, page 17
- 1.6 Best Practices for STP Loop Guard, page 12

1.9 Best Practices for Autonegotiation and Link Negotiation

These sections describe best practices for autonegotiation and link negotiation:

1.9.1 Description of Autonegotiation and Link Negotiation

Autonegotiatation configures the speed and duplex settings on 10/100-Mbps or 10/100/1000-Mbps Ethernet ports. Link negotiation exchanges flow-control parameters and remote fault information on Gigabit and 10-Gigabit Ethernet ports.

1.9.2 Benefits of the Autonegotiation and Link Negotiation Best Practices

Retain the default autonegotiatation configuration (auto) on 10/100-Mbps or 10/100/1000-Mbps Ethernet ports and allow both speed and duplex to be autonegotiated.

Retain the default link negotiation configuration (auto) on Gigabit and 10-Gigabit Ethernet ports and allow link negotiation to exchange flow-control parameters and remote fault information.

Configure a non-default setting only when connecting to ports that do not support autonegotiation or link negotiation.

1.9.3 Features Incompatible with Autonegotiation and Link Negotiation

None.

1.9.4 Guidelines and Restrictions for Autonegotiation and Link Negotiation

- Gigabit and 10-Gigabit Ethernet are full duplex only. You cannot change the duplex mode on Gigabit or 10-Gigabit Ethernet ports or on a 10/100/1000-Mps port configured for Gigabit Ethernet.
- If you set the port speed to auto on a 10/100-Mbps or a 10/100/1000-Mbps Ethernet port, both speed and duplex are autonegotiated. You cannot change the duplex mode of autonegotiation ports.
- Link negotiation is supported on Gigabit and 10-Gigabit Ethernet ports and does not negotiate port speed.

1.9.5 Recommended Autonegotiation and Link Negotiation Configuration

The following sections describe the recommended link negotiation configuration.

1.9.5.1 Recommended Global Configuration

Not applicable.

1.9.5.2 Recommended General Port Configuration

On ports that are connected to devices that also support autonegotiation or link negotiation, retain the default autonegotiation or link negotiation state (enabled), as applicable to each port.

- On 10/100-Mbps and 10/100/1000-Mbps Ethernet ports, autonegotiation is enabled by default. If it has been disabled, revert to the default configuration:

```
Router(config-if)# speed auto
```

- On Gigabit Ethernet and 10 Gigabit Ethernet ports, link negotiation is enabled by default. If it has been disabled, revert to the default configuration:

```
Router(config-if)# no speed nonegotiate
```

On ports that are connected to devices that do not support autonegotiation or link negotiation:

- Enable aggressive mode UDLD.
- See the procedures in the configuration guide to manually configure the port speed and duplex mode as appropriate to support the far-end device.

1.9.5.3 Recommended Single-VLAN Access Port Configuration

No specific port-type configuration required; use the general port configuration.

1.9.5.4 Recommended Layer 2 Trunk Port Configuration

No specific port-type configuration required; use the general port configuration.

1.9.5.5 Recommended Layer 3 Port Configuration

No specific port-type configuration required; use the recommended general port configuration.

1.9.5.6 Recommended SVI Configuration

Not applicable.

1.9.6 Documentation for Autonegotiation and Link Negotiation

See the "Configuring Ethernet Interface Speed and Duplex Mode" section of the customer documentation for more information about autonegotiation and link negotiation.

1.9.7 Related Features and Best Practices

These sections describe features that are recommended for use with autonegotiation and link negotiation:

- 1.8 Best Practices for UniDirectional Link Detection (UDLD), page 15

1.10 Best Practices for Flow Control

These sections describe best practices for flow control:

- 1.10.1 Description of Flow Control
- 1.10.2 Benefits of the Flow Control Best Practices
- 1.10.3 Features Incompatible with Flow Control
- 1.10.4 Guidelines and Restrictions for Flow Control
- 1.10.5 Recommended Flow Control Configuration
- 1.10.6 Documentation for Flow Control
- 1.10.7 Related Features and Best Practices

1.10.1 Description of Flow Control

All Ethernet ports can be configured to respond to IEEE 802.3x pause frames from other devices. Gigabit Ethernet or 10-Gigabit Ethernet ports can be configured to transmit pause frames, but ports on the switch should never need to send pause frames.

1.10.2 Benefits of the Flow Control Best Practices

On ports that connect to a far-end device that might need to send pause frames because of the volume of traffic, you can decide whether it is best to drop traffic at the Catalyst 6500 switch port or to let the far-end device drop the traffic.

To drop the traffic at the Catalyst 6500 switch port, configure the port to respond to pause frames.

To drop the traffic at the far-end device, retain the default flow control configuration (the port will not respond to pause frames).

1.10.3 Features Incompatible with Flow Control

None.

1.10.4 Guidelines and Restrictions for Flow Control

You cannot configure how WS-X6502-10GE 10-Gigabit Ethernet ports respond to pause frames. WS-X6502-10GE 10-Gigabit Ethernet ports are permanently configured to respond to pause frames.

1.10.5 Recommended Flow Control Configuration

The following sections describe the recommended flow control configuration.

1.10.5.1 Recommended Global Configuration

None.

1.10.5.2 Recommended General Port Configuration

If you have decided to drop frames at the Catalyst 6500 switch port instead of on the far-end device, configure the port to respond to pause frames:

- If you know that the device is capable of negotiating flow control, enter this command:

```
Router(config-if)# flowcontrol receive
```

- On a Gigabit Ethernet port, if you do not know that the device is capable of negotiating flow control, enter this command:

```
Router(config-if)# flowcontrol receive desired
```

1.10.5.3 Recommended Single-VLAN Access Port Configuration

None; use the recommended general port configuration.

1.10.5.4 Recommended Layer 2 Trunk Port Configuration

None; use the recommended general port configuration.

1.10.5.5 Recommended Layer 3 Port Configuration

None; use the recommended general port configuration.

1.10.5.6 Recommended SVI Configuration

Not applicable.

1.10.6 Documentation for Flow Control

See the "Configuring IEEE 802.3x Flow Control" section of the customer documentation for more information about flow control.

1.10.7 Related Features and Best Practices

None.

1.11 Best Practices for EtherChannel

These sections describe best practices for EtherChannel:

1.11.1 Description of EtherChannel

An EtherChannel bundles individual Ethernet links into a single logical link that provides the aggregate bandwidth of the member links.

Cisco IOS Software Release 12.2SX supports a maximum of 128 EtherChannels per switch. You can form an EtherChannel with up to eight compatibly configured LAN ports on any switching module. All member ports in each EtherChannel must be the same speed and must all be configured as either Layer 2 or Layer 3 LAN ports.

1.11.2 Benefits of the EtherChannel Best Practices

Using an EtherChannel protocol avoids configuration errors. By default, EtherChannel frame distribution uses IP addresses. For EtherChannels that carry traffic to or from a small number of IP addresses, select one of the other frame distribution options.

1.11.3 Features Incompatible with EtherChannel

None.

1.11.4 Guidelines and Restrictions for EtherChannel

- EtherChannels fall into the following non-exclusive categories, determined by the ports used to form the EtherChannel:
  - Layer 2 EtherChannel—All member ports are configured with the **switchport** command. A Layer 2 EtherChannel can be either an access link or a Layer 2 trunk link.
  - Layer 3 EtherChannel—No member ports are configured with the **switchport** command and the port-channel interface is configured with a Layer 3 address. A Layer 3 EtherChannel can be either a single-VLAN link or a Layer 3 trunk link with subinterfaces configured on the port-channel interface.
  - Single-module EtherChannel—All member ports are on the same switching module.
  - Multi-module EtherChannel—The member ports are on more than one switching module.
  - Non-distributed EtherChannel—All member ports are served by the PFC or by the same DFC.
  - Distributed EtherChannel (DEC)—The member ports are served by the PFC and one or more DFCs or by multiple DFCs. On switching modules with dual switch-fabric connections, a DEC can also be a single-module EtherChannel. Search the release notes for “Dual switch-fabric connections”.
- If you have service modules installed, see this Field Notice:

  http://www.cisco.com/en/US/ts/fn/610/fn61935.html

- The commands in this section can be used on all LAN ports in Catalyst 6500 series switches, including the ports on the supervisor engine and a redundant supervisor engine.
- Release 12.2(17b)SXA and later releases provide support for more than 1 Gbps of traffic per EtherChannel on the WS-X6548-GE-TX and WS-X6548V-GE-TX switching modules.
- With Release 12.2(17a)SX and Release 12.2(17a)SX1, the WS-X6548-GE-TX and WS-X6548V-GE-TX fabric-enabled switching modules do not support more than 1 Gbps of traffic per EtherChannel.
- The WS-X6148-GE-TX and WS-X6148V-GE-TX switching modules do not support more than 1 Gbps of traffic per EtherChannel.
- When you add a member port that does not support ISL trunking to an EtherChannel, Cisco IOS software automatically adds a **switchport trunk encapsulation dot1q** command to the port-channel interface to prevent configuration of the EtherChannel as an ISL trunk. The **switchport trunk encapsulation dot1q** command is inactive when the EtherChannel is not a trunk.
- All Ethernet LAN ports on all modules, including those on a redundant supervisor engine, support EtherChannels (maximum of eight LAN ports) with no requirement that the LAN ports be physically contiguous or on the same module.
- Configure all LAN ports in an EtherChannel to use the same EtherChannel protocol; you cannot run two EtherChannel protocols in one EtherChannel.
- Configure all LAN ports in an EtherChannel to operate at the same speed and in the same duplex mode.
- LACP does not support half-duplex. Half-duplex ports in an LACP EtherChannel are put in the suspended state.
- Enter **no shutdown** commands for all the LAN ports in an EtherChannel. If you shut down a LAN port in an EtherChannel, it is treated as a link failure and its traffic is transferred to one of the remaining ports in the EtherChannel.
- An EtherChannel will not form if one of the LAN ports is a Switched Port Analyzer (SPAN) destination port.
- For Layer 3 EtherChannels, assign Layer 3 addresses to the port channel logical interface, not to the LAN ports in the channel.
- For Layer 2 EtherChannels:
  - Assign all LAN ports in the EtherChannel to the same VLAN or configure them as trunks.
  - If you configure an EtherChannel from trunking LAN ports, verify that the trunking mode is the same on all the trunks. LAN ports in an EtherChannel with different trunk modes can operate unpredictably.
  - An EtherChannel supports the same allowed range of VLANs on all the LAN ports in a trunking Layer 2 EtherChannel. If the allowed range of VLANs is not the same, the LAN ports do not form an EtherChannel.
  - LAN ports with different STP port path costs can form an EtherChannel as long they are compatibly configured with each other. If you set different STP port path costs, the LAN ports are not incompatible for the formation of an EtherChannel.
  - An EtherChannel will not form if protocol filtering is set differently on the LAN ports.

- After you configure an EtherChannel, the configuration that you apply to the port channel interface affects the EtherChannel. The configuration that you apply to the LAN ports affects only the LAN port where you apply the configuration.
- When QoS is enabled, enter the **no mls qos channel-consistency** port-channel interface command to support EtherChannels that have ports with different QoS characteristics.
- Enable QOS after configuring EtherChannel to avoid channels from breaking when QOS gets enabled.

Caution Serious traffic problems can result from mixing manual mode with PAgP or LACP modes, or with a port with no EtherChannel configured. For example, if a port configured in **on** mode is connected to another port configured in **desirable** mode, or to a port not configured for EtherChannel, a bridge loop is created and a broadcast storm can occur. If one end uses the **on** mode, the other end must also.

1.11.5 Recommended EtherChannel Configuration

Layer 3 EtherChannels of all types and single-module non-DEC EtherChannels offer the highest throughput.

CSCti23324 is resolved in Release 12.2(33)SXJ1 and later releases. In releases where CSCti23324 is not resolved, Layer 2 DECs have lower throughput because Layer 2 DEC traffic uses packet recirculation. If possible, configure nondistributed Layer 2 EtherChannels or Layer 3 DECs.

When the switch is in bus mode (also called flow-through mode), Layer 2 multi-module EtherChannels have lower throughput because Layer 2 multi-module EtherChannel traffic uses packet recirculation. If possible, configure single-module EtherChannels or upgrade the installed hardware so that the switch does not operate in bus mode.

Note The sequence of commands to configure a Layer 3 EtherChannel is different than the sequence for a Layer 2 EtherChannel. The following sections describe the recommended EtherChannel configuration, but see the "Configuring EtherChannels" section of the customer documentation for the complete sequence of commands.

1.11.5.1 Recommended Global Configuration

To support DECs on switches equipped with DFCs, ensure that MAC address aging is at least three times as long as the activity time of MAC address synchronization.

- Verify the status of MAC address synchronization:

```
Router# show mac-address-table synchronize statistics | include Status of feature
Status of feature enabled on the switch            :  off
```

- If necessary, enable MAC address synchronization:

```
Router(config)# mac-address-table synchronize
 % Current activity time is [160] seconds
 % Recommended aging time for all vlans is at least three times the activity interval
```

Note With WS-X6716-10GE or WS-X6708-10GE switching modules, MAC address synchronization is enabled by default.

- Verify the activity interval of MAC address synchronization:

```
Router# show mac-address-table synchronize statistics | include activity time
Default activity time                              :  160
Configured current activity time                   :  160
...
```

- Configure MAC address aging to be at least three times as long as the activity time of MAC address synchronization. For example:

```
Router(config)# mac-address-table aging-time 480
```

Note **mac-address-table aging-time 480** is done by default (per CSCsm96610 in SXH2), if synchronization is enabled

Note Switches that handle asymmetric routing traffic have different MAC address aging requirements (see the "1.17 Best Practices for MAC Address Aging" section on page 37).

1.11.5.2 Recommended General Port Configuration

To configure a port as a member in an LACP EtherChannel:

```
Router(config-if)# channel-protocol lacp
Router(config-if)# channel-group group_number mode active
```

To configure a port as a member in an PAgP EtherChannel:

```
Router(config-if)# channel-protocol pagp
Router(config-if)# channel-group group_number mode desirable
```

1.11.5.3 Recommended Single-VLAN Access Port Configuration

No specific port-type configuration required; use the global configuration.

1.11.5.4 Recommended Layer 2 Trunk Port Configuration

No specific port-type configuration required; use the global configuration.

1.11.5.5 Recommended Layer 3 Port Configuration

No specific port-type configuration required; use the recommended global configuration.

1.11.5.6 Recommended SVI Configuration

Not applicable.

1.11.6 Documentation for EtherChannel

See this publication for more information about EtherChannel:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/channel.html

1.11.7 Related Features and Best Practices

1.4 Best Practices for STP EtherChannel Guard, page 9

1.12 Best Practices for VLAN Trunking Protocol (VTP)

These sections describe best practices for VTP:

1.12.1 Description of VTP

A VTP domain, which is also called a VLAN management domain, consists of one or more trunk-connected switches that have the same VTP domain name. VTP allows users to make VLAN configuration changes centrally on one or more switches, which are then communicated to all the other switches in the VTP domain.

VTP has three operating modes:

- Server (default)—Allows configuration of VLANs and propagates those configuration changes. Propagates received configuration changes. Accepts configuration changes from other switches configured as VTP servers.
- Client (must be used with some switches configured as VTP servers)—Does not allow configuration of VLANs. Propagates received configuration changes. Accepts configuration changes from switches configured as VTP servers.
- Transparent—Allows configuration of VLANs but does not propagate those configuration changes. Propagates received configuration changes. Ignores configuration changes from switches configured as VTP servers.
- Off (Release 12.2(33)SXH and later releases)— Allows configuration of VLANs but does not propagate those configuration changes. Does not propagate received configuration changes. Ignores configuration changes from switches configured as VTP servers.

1.12.2 Benefits of the VTP Best Practices

VTP minimizes configuration inconsistencies that can cause problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations. Before you create VLANs, you must decide whether to use VTP in your network. With VTP, you can make configuration changes centrally on one or more switches and have those changes automatically communicated to all the other switches in the network, and put into effect on all switches in the VTP domain.

1.12.3 Features Incompatible with VTP

None, but note that Private VLANs are only be supported in VTP transparent or off modes.

1.12.4 Guidelines and Restrictions for VTP

When implementing VTP in your network, follow these guidelines and restrictions:

- When you configure switches as VTP servers and clients, all the servers and client in a VTP domain accept a propagated VLAN database that has a revision number higher than the current database. This capability provides easy configurability when it is used correctly, but the possibility of serious network problems exists if unintentional changes occur because a VTP client or server switch with a database that has a higher revision number than the current database is introduced into the VTP domain, in which case the VLAN database of the new switch overwrites the current VLAN database.

  Adoption of a new VLAN database might delete VLANs and cause a outage in the network. To ensure that client or server switches always have a configuration revision number that is lower than that of the server, change the client VTP domain name to something other than the standard name, and then revert back to the standard. This action sets the configuration revision on the client to 0.

- Prune VLANs from switches where the VLANs are not used.
  - In VTP server or client mode, you can enter the **vtp pruning** command to automatically prune VLANs where they are not used.
  - In VTP transparent mode, you must manually prune VLANs where they are not used.
- VTPv1 and VTPv2 do not propagate configuration information for extended-range VLANs (VLAN numbers 1006 to 4094). You must configure extended-range VLANs manually on each network device.
- In VTP server or client mode, the VLAN database is saved in the vlan.dat file.
- In VTP transparent mode, the VLAN database is saved in the running-config file and the vlan.dat file.
- Supervisor engine redundancy does not support nondefault VLAN data file names or locations. Do not enter the **vtp file** *file_name* command on a switch that has a redundant supervisor engine.
- Before installing a redundant supervisor engine, enter the **no vtp file** command to return to the default configuration.
- All network devices in a VTP domain must run the same VTP version.
- If you configure a VTP password on one switch, the management domain will not function properly if you do not assign a management domain password to each network device in the domain.
- A VTP version 2-capable network device can operate in the same VTP domain as a network device running VTP version 1 provided VTP version 2 is disabled on the VTP version 2-capable network device (VTP version 2 is disabled by default).
- Do not enable VTP version 2 on a network device unless all of the network devices in the same VTP domain are version 2-capable. When you enable VTP version 2 on a network device, all of the version 2-capable network devices in the domain enable VTP version 2.
- In a Token Ring environment, you must enable VTP version 2 for Token Ring VLAN switching to function properly.
- When you enable or disable VTP pruning on a VTP server, VTP pruning for the entire management domain is enabled or disabled.
- If there is insufficient DRAM available for use by VTP, or if there is an NVRAM error in writing or reading data from vlan.dat file, the VTP mode changes to transparent.

- Network devices in VTP transparent mode do not send VTP Join messages. On Catalyst 6500 series switches with trunk connections to network devices in VTP transparent mode, configure the VLANs that are used by the transparent-mode network devices or that need to be carried across trunks as pruning ineligible. For information about configuring prune eligibility, see the "Configuring the List of Prune-Eligible VLANs" section of the customer documentation.
- Manual pruning is preferable to automatic pruning except in MST environments.

1.12.5 Recommended VTP Configuration

To avoid the possibility of a network outage, configure switches as VTP servers and clients only if you have strict control over the introduction of new hardware and only if all personnel involved in software and hardware maintenance, including network management systems, thoroughly understand the danger of accidentally introducing a new client or server switch that has a VLAN database with a revision number higher than the current database.

Switches operating in VTP transparent mode are safe from propagated accidental VLAN database changes, but all VLAN configuration must be done individually on each switch.

The following sections describe the recommended VTP configuration.

1.12.5.1 Recommended Global Configuration

Configure the VTP password:

```
Router(config)# vtp password your_password
```

Configure a VTP domain name, or ensure that no domain name is entered on any switch:

```
Router(config)# vtp domain domain_name
```

Note The Dynamic Trunking Protocol (DTP) functions only between switches that have the same VTP domain name.

VTP Mode

Decide if your switches are going to operate in VTP transparent mode or in server and client modes.

- To configure VTP transparent mode:

  ```
  Router(config)# vtp mode transparent
  ```

- VTP server mode is the default and does not require any configuration. To configure VTP client mode:

  ```
  Router(config)# vtp mode client
  ```

Additional Global Configuration for VTP Server Mode

- Decide if VTPv2 is required. To configure VTPv2, enter this command on a VTP server:

  ```
  Router(config)# vtp version 2
  ```

- Except on VTP transparent switches, enable pruning:

  ```
  Router(config)# vtp pruning
  ```

1.12.5.2 Recommended General Port Configuration

None.

1.12.5.3 Recommended Access Port Configuration

None.

1.12.5.4 Recommended Layer 2 Trunk Port Configuration

Configure the list of prune-eligible VLANs on a Layer 2 trunk:

```
switchport trunk pruning vlan {none |{{add | except | remove} vlan[,vlan[,vlan[,...]]]}
```

1.12.5.5 Recommended Layer 3 Port Configuration

None.

1.12.5.6 Recommended SVI Configuration

Not applicable.

1.12.6 Documentation for VTP

See this publication for more information about VTP:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vtp.html

1.12.7 Related Features and Best Practices

1.13 Best Practices for Dynamic Trunking Protocol (DTP), page 28

1.13 Best Practices for Dynamic Trunking Protocol (DTP)

These sections describe best practices for DTP:

1.13.1 Description of DTP

The Dynamic Trunking Protocol (DTP) manages trunk autonegotiation on Layer 2 LAN ports. DTP supports ISL and 802.1Q trunks within a VTP domain.

1.13.2 Benefits of the DTP Best Practices

The use of DTP to automatically configure trunks prevents misconfigurations and avoids incorrect traffic flooding that might be caused by a misconfiguration.

1.13.3 Features Incompatible with DTP

None.

1.13.4 Guidelines and Restrictions for DTP

When configuring Layer 2 LAN ports, follow these guidelines and restrictions:

- The following switching modules do not support ISL encapsulation:
  - WS-X6502-10GE
  - WS-X6548-GE-TX, WS-X6548V-GE-TX, WS-X6548-GE-45AF
  - WS-X6148-GE-TX, WS-X6148V-GE-TX, WS-X6148-GE-45AF
- The following configuration guidelines and restrictions apply when using 802.1Q trunks and impose some limitations on the trunking strategy for a network. Note these restrictions when using 802.1Q trunks:
  - When connecting Cisco switches through an 802.1q trunk, make sure the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning tree loops might result.
  - Disabling spanning tree on the native VLAN of an 802.1Q trunk without disabling spanning tree on every VLAN in the network can cause spanning tree loops. We recommend that you leave spanning tree enabled on the native VLAN of an 802.1Q trunk. If this is not possible, disable spanning tree on every VLAN in the network. Make sure your network is free of physical loops before disabling spanning tree.
  - When you connect two Cisco switches through 802.1Q trunks, the switches exchange spanning tree BPDUs on each VLAN allowed on the trunks. The BPDUs on the native VLAN of the trunk are sent untagged to the reserved IEEE 802.1d spanning tree multicast MAC address (01-80-C2-00-00-00). The BPDUs on all other VLANs on the trunk are sent tagged to the reserved Cisco Shared Spanning Tree (SSTP) multicast MAC address (01-00-0c-cc-cc-cd).
  - Non-Cisco 802.1Q switches maintain only a single instance of spanning tree that defines the spanning tree topology for all VLANs. When you connect a Cisco switch to a non-Cisco switch through an 802.1Q trunk, the MST of the non-Cisco switch and the native VLAN spanning tree of the Cisco switch combine to form a single spanning tree topology known as the Common Spanning Tree (CST).
  - Because Cisco switches transmit BPDUs to the SSTP multicast MAC address on VLANs other than the native VLAN of the trunk, non-Cisco switches do not recognize these frames as BPDUs and flood them on all ports in the corresponding VLAN. Other Cisco switches connected to the non-Cisco 802.1q cloud receive these flooded BPDUs. This allows Cisco switches to maintain a per-VLAN spanning tree topology across a cloud of non-Cisco 802.1Q switches. The non-Cisco 802.1Q cloud separating the Cisco switches is treated as a single broadcast segment between all switches connected to the non-Cisco 802.1q cloud through 802.1q trunks.
  - Make certain that the native VLAN is the same on all of the 802.1q trunks connecting the Cisco switches to the non-Cisco 802.1q cloud.
  - If you are connecting multiple Cisco switches to a non-Cisco 802.1q cloud, all of the connections must be through 802.1q trunks. You cannot connect Cisco switches to a non-Cisco 802.1q cloud through ISL trunks or through access ports. Doing so causes the switch to place the ISL trunk port or access port into the spanning tree “port inconsistent” state and no traffic will pass through the port.

1.13.5 Recommended DTP Configuration

The following sections describe the recommended DTP configuration.

1.13.5.1 Recommended Global Configuration

Not applicable.

1.13.5.2 Recommended General Port Configuration

None; use the recommendation for each port type.

1.13.5.3 Recommended Access Port Configuration

Not applicable.

1.13.5.4 Recommended Layer 2 Trunk Port Configuration

- Use the default port configuration, **switchport mode dynamic desirable**, which will negotiate to become a trunk if the far-end port is capable and compatibly configured. Configure trunks to use DTP and 802.1Q encapsulation:

```
Router(config-if)# switchport
Router(config-if)# switchport trunk encapsulation dot1q
```

- Configure the access VLAN, which is the VLAN that is used if the port stops trunking:

```
Router(config-if)# switchport access vlan access_vlan_ID
```

- Configure the native VLAN, which is the VLAN that is used to carry untagged traffic:

```
Router(config-if)# switchport trunk native vlan native_vlan_ID
```

Note On 802.1Q trunks, UDLD requires that the Native VLAN be correctly configured and that the VLAN be defined and active. There is no requirement for it to carry any traffic.

- VLAN 1 is the default VLAN for many features. To avoid the unintentional propagation of VLAN 1 traffic in cases where, incorrectly, another VLAN has not been configured, remove VLAN 1 from any trunk that does not need to carry it:

```
Router(config-if)# switchport trunk allowed vlan remove vlan 1
```

1.13.5.5 Recommended Layer 3 Port Configuration

No specific port-type configuration required; use the recommended global configuration.

1.13.5.6 Recommended SVI Configuration

Not applicable.

1.13.6 Documentation for DTP

See the "Understanding How Layer 2 Switching Works" section of the customer documentation for more information about DTP.

1.13.7 Related Features and Best Practices

None.

1.14 Best Practices for Traffic Storm Control

These sections describe best practices for traffic storm control:

1.14.1 Description of Traffic Storm Control

The traffic storm control feature prevents LAN ports from being disrupted by a broadcast, multicast, or unicast traffic storm. A traffic storm occurs when excessive traffic floods the network, which degrades network performance. Excessive broadcast traffic frequently contains repeated transmissions of the same packets, which makes it acceptable to suppress some of them. With some of the broadcast packets suppressed, enough are transmitted to support normal network operation.

1.14.2 Benefits of the Traffic Storm Control Best Practices

Traffic storm control is implemented in hardware and does not affect the overall performance of the switch. Typically, end-stations such as PCs and servers are the source of broadcast traffic that can be suppressed. To avoid unnecessary processing of excess broadcast traffic, enable traffic storm control for broadcast traffic on access ports that connect to end stations and on ports that connect to key network nodes.

1.14.3 Features Incompatible with Traffic Storm Control

None.

1.14.4 Guidelines and Restrictions for Traffic Storm Control

When configuring traffic storm control, follow these guidelines and restrictions:

- These switching modules do not support traffic storm control:
  - WS-X6148A-GE-45AF
  - WS-X6148A-GE-TX
  - WS-X6148-GE-45AF
  - WS-X6148-GE-TX
  - WS-X6148V-GE-TX

  - WS-X6548-GE-45AF
  - WS-X6548-GE-TX
  - WS-X6548V-GE-TX
- The switch supports multicast and unicast traffic storm control on Gigabit and 10 Gigabit Ethernet LAN ports. Most FastEthernet switching modules do not support multicast and unicast traffic storm control, with the exception of WS-X6148A-RJ-45 and the WS-X6148-SFP.
- The switch supports broadcast traffic storm control on all LAN ports except on those modules previously noted.
- Except for BPDUs, traffic storm control does not differentiate between control traffic and data traffic.
- When multicast suppression is enabled, traffic storm control suppresses BPDUs when the multicast suppression threshold is exceeded on these modules:
  - WS-X6748-SFP
  - WS-X6724-SFP
  - WS-X6748-GE-TX
  - WS-X6748-GE-TX
  - WS-X6704-10GE
  - WS-SUP32-GE-3B
  - WS-SUP32-10GE-3B

  When multicast suppression is enabled on the listed modules, do not configure traffic storm control on STP-protected ports that need to receive BPDUs.

  Except on the listed modules, traffic storm control does not suppress BPDUs.

Note When using WS-6704, be aware of CSCsr52878.

1.14.5 Recommended Traffic Storm Control Configuration

All routers in a VLAN see copies of all broadcast traffic. To avoid high RP CPU utilization caused by a high volume of broadcast traffic, the threshold is typically set to a very low value; for example, less than 1 percent on a Gigabit Ethernet port.

You can use the Top N feature to periodically measure the peak broadcast traffic levels of the selected ports, or if you have a specific required broadcast traffic level (for example, from an application) you could use that requirement as the basis of the threshold.

Base the suppression threshold on your data, plus some additional capacity. For example, if the peak broadcast traffic that is acceptable for a port is 1 percent, a threshold of 1.5 percent might be appropriate. The faster the port speed, the less additional capacity is required.

Use the **show interfaces counters storm-control** command to monitor the effect of the values that you configure, and increase the configured threshold if the TotalSuppDiscards column shows non-zero values.

The following sections describe the recommended traffic storm control configuration.

1.14.5.1 Recommended Global Configuration

Not applicable.

1.14.5.2 Recommended General Port Configuration

On selected ports, configure traffic storm control to suppress broadcast traffic:

```
Router(config-if)# storm-control broadcast level acceptable_broadcast_percentage
```

1.14.5.3 Recommended Access Port Configuration

No specific port-type configuration required; use the general port configuration.

1.14.5.4 Recommended Layer 2 Trunk Port Configuration

No specific port-type configuration required; use the general port configuration.

1.14.5.5 Recommended Layer 3 Port Configuration

No specific port-type configuration required; use the recommended general port configuration.

1.14.5.6 Recommended SVI Configuration

Not applicable.

1.14.6 Documentation for Traffic Storm Control

See this publication for more information about traffic storm control:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/storm.html

1.14.7 Related Features and Best Practices

None.

1.15 Best Practices for Unknown Unicast Flood Blocking (UUFB)

These sections describe best practices for UUFB:

1.15.1 Description of UUFB

Normal Layer 2 switching floods unknown unicast traffic to all Layer 2 ports in a VLAN. You can use UUFB to restrict this behavior on a per-port basis. UUFB permits only egress unicast traffic with known MAC addresses and denies unknown unicast traffic.

1.15.2 Benefits of the UUFB Best Practices

Processing flooded unknown unicast traffic consumes resources on end-stations. To avoid transmitting unnecessary traffic to the end station, enable UUFB on ports to which critical end-stations, like servers, are directly connected.

1.15.3 Features Incompatible with UUFB

None.

1.15.4 Guidelines and Restrictions for UUFB

This recommendation assumes that the end-station's MAC address is always learned on its port. If there is insufficient traffic to ensure that the end-station's MAC address is always learned, configure a static MAC address.

1.15.5 Recommended UUFB Configuration

The following sections describe the recommended UUFB configuration.

1.15.5.1 Recommended Global Configuration

Not applicable.

1.15.5.2 Recommended General Port Configuration

To configure UUFB:

```
Router(config-if)# switchport block unicast
```

1.15.5.3 Recommended Access Port Configuration

No specific port-type configuration required; use the global configuration.

1.15.5.4 Recommended Layer 2 Trunk Port Configuration

No specific port-type configuration required; use the global configuration.

1.15.5.5 Recommended Layer 3 Port Configuration

No specific port-type configuration required; use the recommended global configuration.

1.15.5.6 Recommended SVI Configuration

Not applicable.

1.15.6 Documentation for UUFB

See this publication for more information about UUFB:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/blocking.html

1.15.7 Related Features and Best Practices

None.

1.16 Best Practices for the Port Debounce Timer

These sections describe best practices for the Port Debounce Timer:

1.16.1 Description of the Port Debounce Timer

If the status of a link changes quickly from up to down and then back to up, the port debounce timer suppresses the link status notification. If the link transitions from up to down, but does not come back up, the port debounce timer delays the link status notification.

1.16.2 Benefits of the Port Debounce Timer Best Practices

Suppressing the link status notification allows a quick port status change and recovery to occur without triggering any of the changes that are necessary when a port stays down. The normal operation of DWDM switches sometimes includes quick port status changes and recoveries.

Debounce can also be used to mitigate link flaps because of bad cabling.

1.16.3 Features Incompatible with the Port Debounce Timer

None.

1.16.4 Guidelines and Restrictions for the Port Debounce Timer

Note The **show interfaces debounce** command does not display the default value for 10-GigabitEthernet ports when the port debounce timer is disabled.

Implement the port debounce timer with these default values:

Port Type	Debounce Timer Disabled	Debounce Timer Enabled
Ports operating at 10 Mbps or 100 Mbps	300 milliseconds	3100 milliseconds
Ports operating at 1000 Mbps or 10 Gbps over copper media	300 milliseconds	3100 milliseconds
Ports operating at 1000 Mbps or 10 Gbps over fiber media except WS-X6502-10GE	10 milliseconds	100 milliseconds
WS-X6502-10GE 10-Gigabit ports	1000 milliseconds	3100 milliseconds

1.16.5 Recommended the Port Debounce Timer Configuration

The following sections describe the recommended the Port Debounce Timer configuration.

1.16.5.1 Recommended Global Configuration

Not applicable; use the recommended general port configuration.

1.16.5.2 Recommended General Port Configuration

Enable the port debounce timer on all physical ports that connect to a DWDM switch:

```
Router(config-if)# link debounce
```

1.16.5.3 Recommended Access Port Configuration

No specific port-type configuration required; use the recommended general port configuration.

1.16.5.4 Recommended Layer 2 Trunk Port Configuration

No specific port-type configuration required; use the recommended general port configuration.

1.16.5.5 Recommended Layer 3 Port Configuration

No specific port-type configuration required; use the recommended general port configuration.

1.16.5.6 Recommended SVI Configuration

Not applicable.

1.16.6 Documentation for the Port Debounce Timer

See the "Configuring the Port Debounce Timer" section of the customer documentation for more information.

1.16.7 Related Features and Best Practices

None.

1.17 Best Practices for MAC Address Aging

These sections describe best practices for MAC address aging:

1.17.1 Description of MAC Address Aging

MAC address aging is the process that deletes infrequently-used MAC addresses from the MAC address table.

1.17.2 Benefits of the MAC Address Aging Best Practices

When asymmetric routing occurs, to avoid unicast flooding, increase the MAC address aging time (300 seconds by default) to a value greater than or equal to the ARP timeout (14400 seconds by default).

Note For switches that do not handle asymmetric routing traffic, see the EtherChannel "1.11.5.1 Recommended Global Configuration" section on page 23 for distributed EtherChannel (DEC) MAC address aging recommendations.

1.17.3 Features Incompatible with MAC Address Aging

None.

1.17.4 Guidelines and Restrictions for MAC Address Aging

None.

1.17.5 Recommended MAC Address Aging Configuration

- The ARP timeout is separately configurable on each interface, but is seldom changed from the default value. Verify that no ARP timeout commands have been configured. If the default ARP timeout is configured, this command will have no output:

```
Router# show running-config | include arp timeout
```

- On any interface where a non-default ARP timeout is configured, enter the **no arp timeout** interface command to revert to the default value.
- MAC address aging is globally configurable and also separately configurable on each VLAN. To configure MAC address aging time:

```
Router(config)# mac-address-table aging-time 14400 [vlan vlan_id]
```

1.17.6 Documentation for MAC Address Aging

See the Command References for more information about the MAC address aging commands:

http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html

1.17.7 Related Features and Best Practices

None.

2. Best Practices for Health Monitoring

Cisco Catalyst 6500 best practices are defined for the following health monitoring technologies:

Note

- When you are deploying new hardware, enter the **diagnostic start system test all** command to run the Generic Online Diagnostics (GOLD) on-demand tests before you put the hardware into service.
- Before you RMA hardware, use the Generic Online Diagnostics (GOLD) on-demand tests to confirm that there is a problem.
- Use the **show diagnostic events** command to monitor any intermittent failures.

2.1 Best Practices for GOLD Bootup Online Diagnostics Level

These sections describe best practices for the Generic Online Diagnostics (GOLD) bootup online diagnostics level:

2.1.1 Description of the GOLD Bootup Online Diagnostics Level

There are three bootup diagnostics levels:

- Off—No test are run.
- Minimal—Runs the EARL tests and the loopback tests for all ports.
- Complete—Runs all tests.

2.1.2 Benefits of the GOLD Bootup Online Diagnostics Level Best Practices

If the added boot time is acceptable, configure the complete bootup diagnostics level to provide the most complete verification of the switch. In all cases, boot the switch with the complete bootup diagnostics level configured at least once to verify the hardware; if possible, boot the switch periodically with the complete bootup diagnostics level configured to reverify the hardware.

2.1.3 Features Incompatible with GOLD Bootup Online Diagnostics Level

None.

2.1.4 Guidelines and Restrictions for the GOLD Bootup Online Diagnostics Level

With the complete bootup diagnostics level configured, the bootup time for each module will increase by about 10 seconds compared to the default minimal level. If switch bootup time must be as short as possible, you might not be able to implement this best practice.

2.1.5 Recommended GOLD Bootup Online Diagnostics Level Configuration

The following sections describe the recommended GOLD bootup online diagnostics level configuration.

2.1.5.1 Recommended Global Configuration

Configure the complete bootup diagnostics level:

```
Router(config)# diagnostic bootup level complete
```

2.1.5.2 Recommended General Port Configuration

None; use the global configuration.

2.1.5.3 Recommended Access Port Configuration

None; use the global configuration.

2.1.5.4 Recommended Layer 2 Trunk Port Configuration

None; use the global configuration.

2.1.5.5 Recommended Layer 3 Port or SVI Configuration

None; use the global configuration.

2.1.6 Documentation for the GOLD Bootup Online Diagnostics Level

See the "Setting Bootup Online Diagnostics Level" section of the customer documentation for more information.

2.1.7 Related Features and Best Practices

None.

2.2 Best Practices for GOLD Health-Monitoring Tests

These sections describe best practices for the Generic Online Diagnostics (GOLD) health-monitoring tests:

2.2.1 Description of the GOLD Health-Monitoring Tests

Health-monitoring tests monitor critical system functionality, and they detect and trigger error-recovery in case of test failure.

2.2.2 Benefits of the Health-Monitoring Tests Best Practices

Operating with the health monitoring tests enabled ensures notification of any problem that occurs.

2.2.3 Features Incompatible with the GOLD Health-Monitoring Tests

None.

2.2.4 Guidelines and Restrictions for the GOLD Health-Monitoring Tests

None.

2.2.5 Recommended GOLD Health-Monitoring Tests Configuration

The following sections describe the recommended GOLD health-monitoring tests configuration.

2.2.5.1 Recommended Global Configuration

- Use the default enabled state of the GOLD health-monitoring tests.
- Set the TestSPRPInbandPing test interval to 5 seconds:

```
Router(config)# diagnostic monitor interval module supervisor_engine_slot test
TestSPRPInbandPing 00:00:05 0 0
```

Use the default interval for other tests.

- Enable additional tests as GOLD health-monitoring tests:
  - For each module, enter the **show diagnostic content module** *slot_number* command.
  - In the Attributes column, note the tests that are listed as both "N" (for nondisruptive) and "I" (for inactive); ignore the TestFirmwareDiagStatus test.
  - Check the description of the test as displayed by this command:

    ```
    Router(config)# show diagnostic description module slot_number test test_number
    ```

    For more information, see either the Release 12.2(18)SXF and rebuilds or the Release 12.2(33)SXH and rebuilds Online Diagnostic Tests appendix.
  - If the test is applicable to the traffic on the module, enter the following commands to run the tests as additional health monitoring tests:

```
Router(config)# diagnostic monitor interval module slot_number test test_name 00:00:15 0 0
Router(config)# diagnostic monitor module slot_number test test_name
```

Note With Release 12.2(33)SXH and later releases, you do not need to enter the **00:00:15 0 0** interval values.

2.2.5.2 Recommended General Port Configuration

None; use the global configuration.

2.2.5.3 Recommended Access Port Configuration

None; use the global configuration.

2.2.5.4 Recommended Layer 2 Trunk Port Configuration

None; use the global configuration.

2.2.5.5 Recommended Layer 3 Port or SVI Configuration

None; use the global configuration.

2.2.6 Documentation for the GOLD Health-Monitoring Tests

See the "Configuring Health-Monitoring Diagnostics" section of the customer documentation for more information.

2.2.7 Related Features and Best Practices

None.

2.3 Best Practices for Verifying the System Configuration

These sections describe best practices for verifying the system configuration:

- 2.3.1 Description of Verifying the System Configuration
- 2.3.2 Benefits of the Verifying the System Configuration Best Practices

2.3.1 Description of Verifying the System Configuration

The **show diagnostic sanity** command checks the features configured on the switch against a list of known configuration requirements and displays a list of any conflicts that it finds.

2.3.2 Benefits of the Verifying the System Configuration Best Practices

The **show diagnostic sanity** command identifies problems that exist with the switch configuration. The command output will tell you the following:

- If the switch can ping the gateway of last resort (shown in the command output as the default gateway). The command tests connectivity to either a default gateway or through a routed path.
- UDLD status—Displays:
  - Whether or not UDLD is globally enabled.
  - Per-port UDLD status.
- Trunk port status—Displays information:
  - If a port has the trunking mode set to on
  - If a port is trunking in auto mode
  - If a port has the trunking mode set to desirable but is not trunking
  - If a trunking port negotiates the link as half-duplex
- EtherChannel status—Displays information:
  - If a port has the EtherChannel mode set to “on”.
  - If a port is not a member of an EtherChannel but the mode is set to “desirable”.
- Spanning tree protocol status for VLANs—Displays information:
  - If the root bridge priority is not set.
  - For root bridge ports (shown as “the root”):
    - If the maximum aging time is other than the default.
    - If the forward delay time is other than the default.
    - If the hello time is other than the default.
  - For non-root bridge ports (shown as “the bridge”):
    - If the maximum aging time is other than the default.
    - If the forward delay time is other than the default.
    - If the hello time is other than the default.

- Spanning tree protocol status for ports—Displays information for ports that have:
  - A nondefault STP port priority.
  - A nondefault STP port cost.
  - PortFast enabled.
  - PortFast BPDU Filtering enabled.

  Note PortFast BPDU Filtering is not a recommended feature.

- If the configuration register is set to any value other than 0x2, 0x102, 0x2102.
- If the boot string is empty or if any of the images listed are invalid or absent.
- If IGMP snooping is disabled.
- If IGMP snooping is disabled but RGMP is enabled.
- If multicast is enabled globally but disabled on an interface.
- If SNMP is enabled, if the SNMP access strings [RW,RO] have been left at the default values.

  Note Leaving the SNMP access strings at the default values is a security risk.

- Which ports have flowcontrol receive disabled.
- Which ports have a native VLAN mismatch.
- Which ports have a duplex mismatch.
- Which ports have negotiated half-duplex links.
- Which ports are in the inline power “denied” or “faulty” state.
- Which diagnostic tests failed on bootup.
- If the bootflash is correctly formatted and has enough space to hold a crashinfo file.

2.3.3 Features Incompatible with Verifying the System Configuration

None.

2.3.4 Guidelines and Restrictions for Verifying the System Configuration

None.

2.3.5 Recommended Verifying the System Configuration Procedure

Enter this command:

```
Router# show diagnostic sanity
```

2.3.6 Documentation for Verifying the System Configuration

See the command reference for more information about verifying the system configuration:

http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/show_through_show_fm_summary.html#GUID-B7298D24-081D-409E-946D-8840AF81B49A

2.3.7 Related Features and Best Practices

None.

2.4 Best Practices for GOLD Tcl Script Template

These sections describe best practices for GOLD Tcl Script Template:

Note Release 12.2(33)SXH and later releases support embedded event manager (EEM) Tcl scripting for GOLD.

These sections describe best practices for the GOLD Tcl script template:

2.4.1 Description of GOLD Tcl Script Template

In the following template, *name_of_test* can be one of the following:

- TestAsicSync
- TestFabricHealth
- TestFabricCh0Health
- TestFabricCh1Health
- TestSynchedFabChannel
- TestIntPortLoopback
- TestMacNotification
- TestNonDisruptiveLoopback
- TestPortTxMonitoring
- TestScratchRegister
- TestSPRPInbandPing
- TestUnusedPortLoopback

```
::cisco::eem::event_register_gold card all testing_type monitoring \
test_name name_of_test \
consecutive_failure number_of_failures \
platform_action 0 queue_priority last

namespace import ::cisco::eem::*
namespace import ::cisco::lib::*

# 1. query the information of latest triggered eem event

array set arr_einfo [event_reqinfo]

if {$_cerrno != 0} {
        set result [format "component=%s; subsys err=%s; posix err=%s;\n%s" \
        $_cerr_sub_num $_cerr_sub_err $_cerr_posix_err $_cerr_str]
    error $result
}

set card $arr_einfo(card)

# 2. execute the user-defined config commands

if [catch {cli_open} result] {
    error $result $errorInfo
} else {
    array set cli1 $result
}
if [catch {cli_exec $cli1(fd) "en"} result] {
    error $result $errorInfo
}

if [catch {cli_exec $cli1(fd) \
"diagnostic action mod $card test name_of_test default"} result] {
    error $result $errorInfo
} else {
    set cmd_output $result
}
if [catch {cli_close $cli1(fd) $cli1(tty_id)} result] {
    error $result $errorInfo
}
```

2.4.2 Benefits of the GOLD Tcl Script Template Best Practices

The template shown above has hyperlinks to the relevant sections of the customer documentation.

2.4.3 Features Incompatible with the GOLD Tcl Script Template

None.

2.4.4 Guidelines and Restrictions for the GOLD Tcl Script Template

None.

2.4.5 Recommended GOLD Tcl Script Template Configuration

Follow the procedures in this publication:

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_policy_tcl.html#How_to_Write_Embedded_Event_Manager_Policies_Using_Tcl

2.4.6 Documentation for GOLD Tcl Script Template

See this publication for more information about Tcl scripts:

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_policy_tcl.html

2.4.7 Related Features and Best Practices

None.

2.5 Best Practices for Smart Call Home

These sections describe best practices for Smart Call Home:

Note Release 12.2(33)SXH and later releases support Call Home and Smart Call Home. Smart Call Home requires a Cisco Systems SMARTnet service contract.

These sections describe best practices for Smart Call Home:

2.5.1 Description of Smart Call Home

Call Home provides e-mail-based and web-based notification of critical system events. If you have a service contract directly with Cisco Systems, you can register your devices for the Smart Call Home service.

2.5.2 Benefits of the Smart Call Home Best Practices

- Provides background information and recommendations.
- Provides continuous device health monitoring and real-time diagnostics alerts.
- For known issues, particularly GOLD diagnostics failures, generates Automatic Service Requests with the Cisco TAC.

2.5.3 Features Incompatible with Smart Call Home

None.

2.5.4 Guidelines and Restrictions for Smart Call Home

None.

2.5.5 Recommended Smart Call Home Configuration

See the following publication for procedures:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/callhome.html#Configuring_Call_Home

2.5.6 Documentation for Smart Call Home

See this publication for more information about Smart Call Home:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/callhome.html

2.5.7 Related Features and Best Practices

None.

2.6 Best Practices for Monitoring System Resource Usage

These sections describe best practices for monitoring system resource usage.

Note Release 12.2(18)SXF and later support monitoring system resource usage.

MIB Locator

http://tools.cisco.com/ITDIT/MIBS/servlet/index

2.6.1 Description of Monitoring System Resource Usage

Displays the current utilization of the hardware resources and displays a list of the currently available hardware capacities.

2.6.2 Benefits of the Monitoring System Resource Usage Best Practices

Issue the **show platform hardware capacity** command periodically to monitor system resource usage. Any system resource with usage of 90% or greater should be addressed.

2.6.3 Features Incompatible with Monitoring System Resource Usage

None.

2.6.4 Guidelines and Restrictions for Monitoring System Resource Usage

None.

2.6.5 Recommended Monitoring System Resource Usage Procedure

Enter this command:

```
Router# show platform hardware capacity
```

2.6.6 Documentation for Monitoring System Resource Usage

See the "Determining System Hardware Capacity" section of the customer documentation for more information.

2.6.7 Related Features and Best Practices

None.

2.7 Best Practices for Error Counter Monitoring

These sections describe best practices for error counter monitoring:

Note Release 12.2(33)SXH and later releases support error counter monitoring.

These sections describe best practices for error counter monitoring:

2.7.1 Description of Error Counter Monitoring

This procedure uses the TestErrorCounterMonitor, which monitors the errors and interrupts on each module in the system by periodically polling the module's error counters. If the errors exceed their thresholds, a syslog is displayed with detailed information, which includes the error counter identifier, port number, total failures, consecutive failures, and the severity of the error-counter.

2.7.2 Benefits of the Error Counter Monitoring Best Practices

This procedure allows you to identify errors that need to be submitted to the Cisco TAC for further analysis.

2.7.3 Features Incompatible with Error Counter Monitoring

None.

2.7.4 Guidelines and Restrictions for Error Counter Monitoring

None.

2.7.5 Recommended Error Counter Monitoring Procedure

Step 1 If you suspect that an error has occurred, enter this command:

```
Router# show diagnostic events | include Time|-----|TestErrorCounterMonitor|DV
Time Stamp          ET [Card] Event Message
------------------- -- ------ --------------------------------------------------
10/06 06:26:03.967 E  [5]    TestErrorCounterMonitor: ID:26 IN:0 PO:0 RE:199 R
                             M:255 DV:440 EG:3 CF:1 TF:1
10/06 06:26:03.971 E  [5]    TestErrorCounterMonitor: ID:26 IN:0 PO:1 RE:199 R
                             M:255 DV:440 EG:3 CF:1 TF:1
10/06 06:26:03.971 E  [5]    TestErrorCounterMonitor: ID:26 IN:0 PO:2 RE:199 R
                             M:255 DV:440 EG:3 CF:1 TF:1
10/06 06:26:03.971 E  [5]    TestErrorCounterMonitor: ID:26 IN:0 PO:3 RE:199 R
                             M:255 DV:440 EG:3 CF:1 TF:1
10/06 06:29:03.971 E  [5]    TestErrorCounterMonitor: ID:26 IN:0 PO:0 RE:199 R
                             M:255 DV:1000 EG:3 CF:1 TF:2
```

Step 2 Look for events with timestamps that correspond to the problem and card that you are investigating.

Step 3 Look for incrementing DV and TF values. If DV is incrementing rapidly, for example, going up by 10 or more, and all other values (ID, IN, PO,RE,R, etc.) remain the same, then submit the errors to the Cisco TAC for further analysis.

2.7.6 Documentation for Error Counter Monitoring

See the **show diagnostic events** command for more information.

2.7.7 Related Features and Best Practices

None.

3. Best Practices for Switch Management

Cisco Catalyst 6500 best practices are defined for the following switch management technologies:

3.1 Recommended Switch Management Feature and Command List

Use the following features and commands to configure and manage your switch:

- For initial setup, use the **setup** command—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf002.html#Using_Setup

- Use the **show history** command to display your command entries:
  - `router# show history`
  - `router(config)# do show history`
- For better security:
  - Use SSH instead of TELNET.
  - Use AAA (TACACS or RADIUS) for authentication and authorization.
- Create and maintain a physical and logical network diagram.
- With Release 12.2(33)SXH and later releases, use the Smart Port Macros feature—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/smrtport.html

- With Release 12.2(33)SXH and later releases, use the AutoSecure feature—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/autosec.html

- With Release 12.2(33)SXH and later releases, use the Auto QoS feature—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/auto_qos.html

- With Release 12.2(33)SXH and later releases, the Configuration Replace and Configuration Rollback features are available—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/config-mgmt/configuration/12-2sx/cm-config-rollback.html

- Configure NTP to ensure that time-stamped SYSLOG messages from all devices have consistent timestamps, which makes troubleshooting easier.

  A common use of the NTP-synchronized time is in debug and log time-stamps, configured with these commands:

  ```
  Router(config)# service timestamps debug datetime msec localtime show-timezone
  Router(config)# service timestamps log datetime msec localtime show-timezone
  ```

  See this publication for NTP configuration procedures:

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_basic_sys_manage.html#Configuring_NTP

- Use the default configuration register value: 0x2102. Enter this command to restore the default value:

  ```
  router(config)# config-register 0x2102
  ```

Note The **show diagnostic sanity** command will report a nondefault configuration register value.

- Store a backup software image on another flash device and configure a second boot command for it:

  ```
  Router(config)# boot system flash device_name:image_name
  ```

  Or:

  ```
  Router(config)# boot system flash device_name:image_name
  ```

  If the switch cannot boot the image specified in the first command, it will boot the image specified in the second command.

  See this publication for more information about boot configuration:

  http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_rebooting.html

- Issue the **show platform hardware capacity** command periodically to monitor the flash filesystems:
  - Any system resource with usage of 90% or greater should be addressed.
  - Ensure that there is sufficient space available in the flash filesystems (at least 3MB) for crashinfo collection.

  Note Do not enable creation of core dumps except as instructed by the Cisco TAC.

  See the "Determining System Hardware Capacity" section of the customer documentation for more information.

3.2 Best Practices for Hostname Configuration

These sections describe best practices for hostname configuration:

3.2.1 Description of Hostname Configuration

The host name is used in prompts.

3.2.2 Benefits of the Hostname Configuration Best Practices

Configure a meaningful hostname. Choose a name that means something to the people managing the switch, for example, location or function. A well-thought-out naming convention will prove helpful for administrators when using network management software and when troubleshooting the network.

3.2.3 Features Incompatible with Hostname Configuration

None.

3.2.4 Guidelines and Restrictions for Hostname Configuration

See the **hostname** command Usage Guidelines.

3.2.5 Recommended Hostname Configuration

The following sections describe the recommended hostname configuration.

3.2.5.1 Recommended Global Configuration

Configure the hostname:

```
Router(config)# hostname selected_name
```

For example:

```
Router(config)# hostname 6K-LV2-CL3
6K-LV2-CL3(config)#
```

After the hostname is entered, the CLI prompt changes to reflect the entered name. The hostname is derived from the device type (Catalyst: “6K”), floor location (Level 2), and wiring closet location (Closet 3). Sometimes the name can also incorporate the supervisor type or other relevant information (for example, S720B-LV2-CL3).

3.2.5.2 Recommended General Port Configuration

None; use the global configuration.

3.2.5.3 Recommended Access Port Configuration

None; use the global configuration.

3.2.5.4 Recommended Layer 2 Trunk Port Configuration

None; use the global configuration.

3.2.5.5 Recommended Layer 3 Port or SVI Configuration

None; use the global configuration.

3.2.6 Documentation for Hostname Configuration

See the Configuring the System Name section in this publication for more information about hostname configuration:

http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf012.html#wp1039289

3.2.7 Related Features and Best Practices

None.

3.3 Best Practices for the Login Banner

These sections describe best practices for the login banner:

3.3.1 Description of the Login Banner

The login banner is displayed after the MOTD banner and before the login prompt.

In some legal jurisdictions it can be impossible to prosecute and illegal to monitor malicious users unless they have been notified that they are not permitted to use the switch. The login banner can provide this notice.

Legal notification requirements are complex, vary by jurisdiction and situation, and should be discussed with legal counsel. Even within jurisdictions, legal opinions can differ. In cooperation with counsel, a banner can provide some or all of the this information:

- Notice that the system is to be logged into or used only by specifically authorized personnel and perhaps information about who can authorize use.
- Notice that any unauthorized use of the system is unlawful and can be subject to civil and criminal penalties.
- Notice that any use of the system can be logged or monitored without further notice and that the resulting logs can be used as evidence in court.
- Specific notices required by local laws.

For security purposes, rather than legal, a login banner should not contain any specific information about the switch name, model, software, or ownership. Such information can be abused by malicious users.

3.3.2 Benefits of the Login Banner Best Practices

The configuration of the login banner provides a way to display a message to anyone who accesses the switch. Login banners can be useful to reemphasize the potential law infringement represented by the unauthorized access to the device in question. It can also be used to provide information about the location of the device, the contact details of the administrator, or a message of the month.

For example, the message could be:

```
Access to this device or the attached networks is prohibited without express permission
from the network administrator.
Violators will be prosecuted to the fullest extent of both civil and criminal law.
```

3.3.3 Features Incompatible with the Login Banner

None.

3.3.4 Guidelines and Restrictions for the Login Banner

The login banner cannot be disabled on a per-line basis. To globally disable the login banner, enter the **no banner login** command.

3.3.5 Recommended Login Banner Configuration

The following sections describe the recommended the Login Banner configuration.

3.3.5.1 Recommended Global Configuration

Enter this command:

```
Router(config)# banner login d message_text d
```

Any character that does not appear in *message_text* can be used as the delimiting (*d*) character, including control characters, except ^z (Control-Z).

3.3.5.2 Recommended General Port Configuration

None; use the global configuration.

3.3.5.3 Recommended Access Port Configuration

None; use the global configuration.

3.3.5.4 Recommended Layer 2 Trunk Port Configuration

None; use the global configuration.

3.3.5.5 Recommended Layer 3 Port or SVI Configuration

None; use the global configuration.

3.3.6 Documentation for the Login Banner

See this publication for more information about the login banner:

http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf004.html#wp1001446

3.3.7 Related Features and Best Practices

None.

3.4 Best Practices for System Logging

These sections describe best practices for system messages:

3.4.1 Description of System Logging

System logging (syslog) forwards messages from the syslog sender (the switch) to various destinations, such as the logging buffer, terminal lines, or a UNIX syslog server.

3.4.2 Benefits of the System Logging Best Practices

The recommended configuration increases the usability of administrative connections (console of SSH) and optimizes the syslog configuration.

3.4.3 Features Incompatible with System Logging

None.

3.4.4 Guidelines and Restrictions for System Logging

None.

3.4.5 Recommended System Logging Configuration

The following sections describe the recommended system logging configuration.

3.4.5.1 Recommended Global Configuration

Disable Console Logging

By default, all system messages are sent to the system console. Console logging is a high-priority task in Cisco IOS Software. Disable console logging to avoid a situation in which the switch might hang while waiting for a response from a terminal.

```
Router(config)# no logging console
```

Note You might want to enable console logging during troubleshooting: enter the **logging console** command; you can enter the **logging console** *severity_level* command (*severity_level*: 0 to 7) to obtain a selected level of message logging.

Disable Logging on Other Administrative Connections

This command disables logging for terminal lines other than the system console.

```
Router(config)# no logging monitor
```

Note Enable monitor logging only as specifically required: enter the **logging monitor** command; you can enter the **logging monitor** *severity_level* command (*severity_level*: 0 to 7) to obtain a desired level of message logging.

Enable Message Buffering

Buffered messages can be displayed with the **show logging** command. The logging buffer is circular. Once the logging buffer is filled, older entries are overwritten by newer entries. The size of the logging buffer is user-configurable and is specified in bytes. 16384 provides adequate logging in most cases.

```
Router(config)# logging buffered 16384
```

Filter Noncritical Messages

Filter by severity the messages sent to the syslog servers. The default logging level for all destinations (console, monitor, buffer, and traps) is “debugging” (level 7). If you leave the trap logging level at 7, many noncritical messages are sent to the syslog servers. Set the default logging level for traps to “notifications” (level 5).

```
Router(config)# logging trap notifications
```

Configure the UNIX Logging Server Address

Configure the IP address of the UNIX logging server:

```
Router(config)# logging host ip_address
```

Note Configure the UNIX logging server for “facility local7”.

Configure the Message Source

To make identification of the messages from a particular switch easier, select the interface from which the messages will be sent. The IP address of the interface will be the source address of the messages. This example configures the loopback 0 interface as the source of messages:

```
Router(config)# logging source-interface loopback 0
```

Note Configure the selected interface with the IP address that you want to be used as the source address of the messages.

Enable Timestamped Messages

Enable timestamps on log messages:

```
Router(config)# service timestamps log datetime localtime show-timezone msec
```

Enable timestamps on system debug messages:

```
Router(config)# service timestamps debug datetime localtime show-timezone msec
```

Enable Module Messages

Enable messages from the installed modules:

```
Router(config)# service slave-log
```

3.4.5.2 Recommended General Port Configuration

Enable logging for link status and bundle status on all switch-to-switch links:

```
Router(config-if)# logging event link-status
Router(config-if)# logging event bundle-status
```

Note Ensure that console logging has been disabled before you enter any **logging event** commands.

3.4.5.3 Recommended Access Port Configuration

None; use the global and general port configurations.

3.4.5.4 Recommended Layer 2 Trunk Port Configuration

None; use the global and general port configurations.

3.4.5.5 Recommended Layer 3 Port or SVI Configuration

None; use the global and general port configurations.

3.4.6 Customer Documentation for System Logging

See this publication for more information about system logging:

http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf013.html#Logging_System_Messages

3.4.7 Related Features and Best Practices

None.

3.5 Best Practices for Simple Network Management Protocol (SNMP)

These sections describe best practices for SNMP:

3.5.1 Description of SNMP

The Simple Network Management Protocol (SNMP) is used by network management systems to both get information from the switch and also to make configuration changes.

3.5.2 Benefits of the SNMP Best Practices

With SNMP enabled, configure the SNMP descriptive components to provide a clearer description of the switch and to better identify it as the origin of SNMP alerts.

3.5.3 Features Incompatible with SNMP

None.

3.5.4 Guidelines and Restrictions for SNMP

None.

3.5.5 Recommended SNMP Configuration

The following sections describe the recommended SNMP configuration.

3.5.5.1 Recommended Global Configuration

Enter these commands:

```
Router(config)# snmp-server contact contact_id
Router(config)# snmp-server location switch_location
Router(config)# snmp-server chassis-id id_string
```

Note For the highest level of security, configure SNMPv3 with MD5 authentication and DES encryption.

3.5.5.2 Recommended General Port Configuration

None; use the global configuration.

3.5.5.3 Recommended Access Port Configuration

None; use the global configuration.

3.5.5.4 Recommended Layer 2 Trunk Port Configuration

None; use the global configuration.

3.5.5.5 Recommended Layer 3 Port or SVI Configuration

None; use the global configuration.

3.5.6 Customer Documentation for SNMP

See this publication for more information about SNMP:

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cfg_snmp_sup.html

3.5.7 Related Features and Best Practices

None.

3.6 Best Practices for Software and Configuration Backup

These sections describe best practices for software and configuration backup:

3.6.1 Description of Software and Configuration Backup

Local copies of software images and configuration files provide the quickest replacement for any damaged or deleted files.

3.6.2 Benefits of the Software and Configuration Backup Best Practices

Store copies of the software images and configuration files so that you can quickly replace any damaged or deleted files. Store the copies on other non-removable flash devices, on removal media that is not kept in the switch's slot, or on a TFTP, HTTP, or RCP server. Store a copy of the configuration files on the RP **bootflash:** device.

3.6.3 Features Incompatible with Software and Configuration Backup

None.

3.6.4 Guidelines and Restrictions for Software and Configuration Backup

None.

3.6.5 Recommended Software and Configuration Backup Procedures

Use this command to copy files:

```
Router# copy file_name destination
```

file_name is:

- The software image name
- **const_nvram:startup-config**
- For switches in VTP server mode, **const_nvram:vlan.dat**

destination is:

- **bootflash:**
- **disk0:**
- **disk1:**
- **slot0:**
- **tftp:**

3.6.6 Customer Documentation for Software and Configuration Backup

See this publication for more information about software and configuration backup:

http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_config-files.html

3.6.7 Related Features and Best Practices

None.

3.7 Best Practices for NetFlow Data Export (NDE)

These sections describe best practices for NDE:

3.7.1 Description of NDE

NetFlow collects traffic statistics by monitoring the traffic that flows through the switch and storing the statistics in the NetFlow table. The statistics can be analyzed for management, traffic analysis, and security purposes.

3.7.2 Benefits of the NDE Best Practices

Use NDE for troubleshooting. Except in carefully planned topologies, NDE consumes too many switch and network resources to enable permanently.

3.7.3 Features Incompatible with NDE

None.

3.7.4 Guidelines and Restrictions for NDE

- Only NetFlow version 9 provides NDE support for IP multicast traffic.
- NDE does not support any non-IP protocol, including Internetwork Packet Exchange (IPX).
- When you configure NAT and NDE on an interface, the PFC sends all fragmented packets to the MSFC to be processed in software. (CSCdz51590)

3.7.5 Recommended NDE Configuration

The following sections describe the recommended NDE configuration.

3.7.5.1 Recommended Troubleshooting Procedure

Set the NetFlow Mask

```
Router(config)# mls flow ip interface-full
```

Enable NDE From the PFC

```
Router(config)# mls nde sender
```

Display Statistics

```
Router(config)# show mls netflow ip
```

3.7.6 Customer Documentation for NDE

See these publications for more information about NetFlow and NDE:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/netflow.html

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/nde.html

3.7.7 Related Features and Best Practices

3.10 Best Practices for Switched Port Analyzer (SPAN), page 67

3.8 Best Practices for the Time Domain Reflectometer (TDR)

These sections describe best practices for the TDR:

3.8.1 Description of the TDR

The TDR detects a cable fault by sending a signal through the cable and reading the signal that is reflected back to it.

3.8.2 Benefits of the TDR Best Practices

If you cannot establish a link, use the TDR to conduct in-place testing that determines if the cabling is at fault.

3.8.3 Features Incompatible with the TDR

None.

3.8.4 Guidelines and Restrictions for the TDR

- The TDR can test cables up to a maximum length of 115 meters.
- The TDR is supported on these switching modules:
  - WS-X6748-GE-TX
  - WS-X6548V-GE-TX
  - WS-X6548-GE-TX
  - WS-X6548-GE-45AF
  - WS-X6148V-GE-TX
  - WS-X6148-GE-TX
  - WS-X6148-GE-45AF
  - WS-X6148A-RJ-45
  - WS-X6148A-GE-TX

- WS-X6148A-GE-45AF
- WS-X6148A-45AF

3.8.5 Recommended TDR Procedure

Enter this command to run the TDR:

```
Router# test cable-diagnostics tdr interface interface_type slot/port
```

3.8.6 Customer Documentation for the TDR

See this publication for more information about the TDR:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/intrface.html#Checking_the_Cable_Status_Using_the_TDR

3.8.7 Related Features and Best Practices

None.

3.9 Best Practices for Management Connections

These sections describe best practices for management connections:

3.9.1 Description of Management Connections

Management connections to interfaces on the Catalyst 6500 switch fall into two categories:

- In-band management connection—Uses a network topology where both management and data traffic share the same physical links and network access.
- Out-of-band management connection—Requires a network topology where there are separate physical links and network access for management and data traffic.

The serial link to the console port is inherently an out-of-band management connection, but it is quite common to use a terminal server that provides network access to the serial link, so that the aggregate link (network plus serial) can be either in-band or out-of-band.

Catalyst 6500 switches do not have management-only Ethernet ports, but any port can be configured for for management-only use, and depending on the network topology, it can be either in-band or out-of-band.

3.9.2 Benefits of the Management Connections Best Practices

- Use a loopback interface for in-band management connections, because loopback interfaces are up as long as there is at least one active SVI or active Layer 3 interface.

  Note You must configure routing to support access to loopback interfaces.

- If possible, configure an out-of-band management connection. Physical ports for out-of-band management connections fall into these categories:
  - A console connection through a terminal server that is cabled outside the data network.
  - An Ethernet connection that is cabled outside the data network to a port in a VLAN reserved for management traffic (don't use VLAN 1). Because the connection requires the port to be up, configure the port as a Layer 3 interface with an IP address and use that address for the management connection.
- Configuring both in-band and both out-of-band management connections provides two out-of-band paths in addition to the in-band access.

3.9.3 Features Incompatible with Management Connections

None.

3.9.4 Guidelines and Restrictions for Management Connections

None.

3.9.5 Recommended Management Connections Configuration

Loopback Interface

```
Router(config)# interface loopback loopback_number
Router(config-if)# ip address ip_address subnet_mask
```

Layer 3 Interface

```
Router(config)# interface interface_type slot/port
Router(config-if)# ip address ip_address subnet_mask
```

3.9.6 Customer Documentation for Management Connections

See these publications for more information about management connections:

http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/ffun_c.html

http://www.cisco.com/en/US/docs/ios/12_2/interface/configuration/guide/finter_c.html

3.9.7 Related Features and Best Practices

None.

3.10 Best Practices for Switched Port Analyzer (SPAN)

These sections describe best practices for SPAN:

3.10.1 Description of SPAN

SPAN copies traffic from any of these:

- One or more CPUs (only with Release 12.2(33)SXH and later releases)
- One or more ports
- One or more EtherChannels
- One or more VLANs

SPAN sends the copied traffic to one or more destinations for analysis by a network analyzer.

Note Release 12.2(33)SXH and later releases support these features:

- EtherChannels as SPAN destinations
- Additional local SPAN egress-only sessions
- Distributed egress SPAN
- Input Packets with Don't Learn Option

3.10.2 Benefits of the SPAN Best Practices

Use SPAN for troubleshooting. Except in carefully planned topologies, SPAN consumes too many switch and network resources to enable permanently.

Exercise all possible care when enabling and configuring SPAN. The traffic copied by SPAN can impose a significant load on the switch and the network.

To minimize the load, configure SPAN to copy only the specific traffic that you want to analyze. Select sources that carry as little unwanted traffic as possible. For example, a port as a SPAN source might carry less unwanted traffic than a VLAN.

Note To monitor traffic that can be matched with an ACL, consider using VACL capture.

Before enabling SPAN, carefully evaluate the SPAN source traffic rates, and consider the performance implications and possible oversubscription points, which include these:

- SPAN destination
- Fabric channel
- Rewrite/replication engine
- Forwarding engine (PFC/DFC)

To avoid disrupting traffic, do not oversubscribe any of these points in your SPAN topology. Some oversubscription and performance considerations are:

- SPAN doubles traffic internally
- SPAN adds to the traffic being process by the switch fabric
- SPAN doubles forwarding engine load
- The supervisor engine handles the entire load imposed by egress SPAN (also called transmit SPAN).

Note Egress SPAN should only be enabled for short periods of time during active troubleshooting.

Release 12.2(33)SXH and later releases support distributed egress SPAN, which reduces the load on the supervisor engine.

- The ingress modules handle the load imposed by ingress SPAN sources (also called receive SPAN) on each module. Ingress SPAN adds to rewrite/replication engine load.

3.10.3 Features Incompatible with SPAN

See the "Feature Incompatibilities" section of the customer documentation.

3.10.4 Guidelines and Restrictions for SPAN

See the "Local SPAN, RSPAN, and ERSPAN Configuration Guidelines and Restrictions" section of the customer documentation.

3.10.5 Recommended SPAN Configuration

See the "Configuring Local SPAN, RSPAN, and ERSPAN" section of the customer documentation.

3.10.6 Documentation for SPAN

See this publication for more information about SPAN:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/span.html

3.10.7 Related Features and Best Practices

None.

4. Best Practices for Multicast

These sections describe Cisco Catalyst 6500 best practices for multicast technology:

4.1 Description of Multicast

Multicast is a one-to-many communication method that delivers network traffic from a single source to a group of destinations, with the traffic passing over each link of the connecting network topology only once. Multicast creates copies of the traffic only when the links to the destinations diverge.

4.2 Benefits of the Multicast Best Practices

Multicast is a feature that must be configured compatibly across a network. These best practices focus on the configuration requirements, recommendations, and restrictions that apply to Catalyst 6500 switches in the network.

4.3 Features Incompatible with Multicast

None.

4.4 Guidelines and Restrictions for Multicast

- To avoid processing multicast traffic in software:
  - Ensure that the IIF and OIF MTU sizes match.
  - Ensure that multicast sources are configured not to send multicast data packets with any IP options.
- Do not configure more than 4 bidirectional PIM rendezvous points (RPs) per VPN.
- With multiple multicast routing protocols configured (for example, sparse mode (SM) and Bidirectional PIM), avoid overlapping multicast group ranges.
- When SSM, IGMPv3 and IGMP snooping are configured, use multicast groups that map to unique Layer 2 multicast MAC addresses. Avoid overlapping Layer 2 multicast MAC addresses.
- Ensure that there is at least one IGMP querier-capable device active in each VLAN. In a VLAN where PIM and IGMP are not configured because the multicast traffic does not need to be routed, enable the IGMP snooping querier.

Note The IGMP snooping querier does not support querier elections. Do not enable the IGMP snooping querier on more than one device in a VLAN.

4.5 Recommended Multicast Configuration

These sections describe the recommended multicast configuration:

4.5.1 Platform Independent Configuration

Follow the recommendations in this publication:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6552/prod_presentation0900aecd8031088a.pdf

4.5.2 Replication Mode

Note

- Egress replication mode provides better performance only when there are a significant number of multicast outgoing interfaces (OIFs) served by DFCs. Without a DFC to support local egress replication mode, egress replication mode performance is lower then ingress replication mode because of the load placed on the PFC.
- Ingress marking and egress policing are not compatible with egress replication. (CSCsd41348)
- Egress SPAN is not supported in egress multicast mode. (CSCsa95965)

Use the automatically detected replication mode. If possible, the switch will use egress replication mode.

- If you have configured ingress replication mode, enter this command to return to the automatic detection mode:

```
Router(config)# no mls ip multicast replication-mode ingress
```

- If you have configured egress replication mode, enter this command to return to the automatic detection mode:

```
Router(config)# no mls ip multicast replication-mode egress
```

4.5.3 Local Egress Replication Mode

If the switch is operating in egress replication mode, enable local egress replication mode.

```
Router(config)# mls ip multicast egress local
```

4.5.4 Non-RPF Traffic

The switch uses the NetFlow table to drop non-RPF traffic.

- With a PFC3, configure non-RPF aging:

```
Router(config)# mls ip multicast non-rpf aging fast
Router(config)# mls ip multicast non-rpf aging global
```

- With a PFC2, configure rate limiting of RPF failure traffic:

```
Router(config)# mls rate-limit multicast ipv4 non-rpf pps [packets_in_burst]
```

Note Do not configure ACL-based filtering of RPF failures.

4.5.5 Partially and Completely Switched Flows

For partially switched flows:

- Configure the multicast boundary feature:

```
Router(config-if)# ip multicast boundary access_list [filter-autorp]
```

- Configure these rate limiters:

```
Router(config)# mls rate-limit multicast ipv4 partial 5000 100
Router(config)# mls rate-limit multicast ipv4 fib-miss 5000 100
```

Modify the packets-per-second and burst values based on the convergence requirements of your network and the available CPU capacity.

Note

- For partially switched flows, do not configure the **ip multicast ttl-threshold** command on multicast OIFs.
- To avoid the possibility of ACLs interfering with multicast routing control packets, ensure that multicast sources are configured not to send multicast data packets that use multicast groups that map to 0100.5e00.00xx.

4.5.6 Multicast Consistency Checker

Enable the multicast consistency checker:

```
Router(config)# mls ip multicast consistency-check
Router(config)# mls ip multicast consistency-check type scan-mroute
```

Use the following command as needed for troubleshooting:

```
Router(config)# mls ip multicast consistency-check type rp-sp
```

Note

- The RP-SP multicast consistency checker results are most reliable when multicast traffic levels are stable. When multicast traffic levels vary significantly, the RP-SP multicast consistency checker might indicate a problem when none exists.
- The RP-SP checker is enabled by default in Release 12.2(33)SXH and later releases.

4.5.7 Rate Limit Traffic from Directly Connected Sources

If you have PIM sparse mode configured, enter this command:

```
Router(config)# mls rate-limit multicast ipv4 connected packets_per_second
```

Set a packets-per-second value between 150 and 1000 and modify the packets-per-second and burst values based on the convergence requirements of your network.

4.5.8 Directly Connected Subnets

If the switch is not the first hop router for any multicast sources, disable installation of directly connected subnet entries:

```
Router(config)# no mls ip multicast connected
```

Note If the switch is the first hop router for any multicast source, rate-limit the traffic.

4.5.9 Multicast Redundancy and SSO

- Use the default settings. Enter this command to revert to the defaults:

```
Router(config)# no mls ip multicast sso convergence-time 1
Router(config)# no mls ip multicast sso leak interval 1
Router(config)# no mls ip multicast sso leak percent 1
```

Note When prefaced with the **no** keyword, you can enter any numerical value to revert to the default setting.

- With SSO redundancy configured, use static anycast RP.

Note

- With SSO redundancy configured, do not use auto-RP.
- SSO redundancy is supported only for PIM-DM, PIM-SM, SSM protocols.

4.5.10 PIM snooping

- In VLANs with multicast routers running source-specific multicast (SSM) and directly connected multicast sources, disable PIM snooping in the VLAN:

```
Router(config)# interface vlan vlan_ID
Router(config-if)# no ip pim snooping
```

- In VLANs that have multicast routers running PIM sparse mode (PIM-SM) and directly connected multicast sources, enable PIM snooping on the switch and in the VLAN and ensure that DR flooding is enabled on the switch:

```
Router(config)# ip pim snooping
Router(config)# ip pim snooping dr-flood
Router(config)# interface vlan vlan_ID
Router(config-if)# ip pim snooping
```

Note The presence or absence of any other type of multicast routing, such as SSM or bidirectional PIM, does not affect the need for DR flooding with PIM-SM and directly connected multicast sources.

- DR flooding is not required in these cases:
  - A VLAN with multicast routers running PIM-SM only and with no directly connected multicast sources.
  - A VLAN with multicast routers running SSM only and with no directly connected multicast sources.
  - A VLAN with multicast routers running bidirectional PIM only, whether or not there are any directly connected multicast sources.

  If DR flooding is not required on the switch, disable it to reduce bandwidth usage:

```
Router(config)# no ip pim snooping dr-flood
```

- CSCsh98208—In a VLAN with PIM snooping configured, when the shared tree and shortest path tree (SPT) diverge, PIM snooping might suppress the (S,G) RPT-bit prune message that is sent by a multicast receiver from reaching the upstream router in the shared tree, causing a situation in which more than one upstream router forwards the multicast traffic, each using their own (S,G)-join state, which in turn causes duplicate multicast packets to be delivered to the multicast receivers.

  This situation lasts only briefly because the PIM-ASSERT mechanism stops the extraneous flow, but this cycle repeats again when the next (*,G) join (S,G) RPT bit prune message is sent by one of the receivers.

If the switch is in a topology that has the problem, take one of these actions:

- With Release 12.2(18)SXF9 and later releases, enter this command to disable SGR-prune message suppression:

```
Router(config)# ip pim snooping suppress sgr-prune
```

- With releases earlier than Release 12.2(18)SXF9, disable PIM snooping in the VLAN:

```
Router(config)# interface vlan vlan_ID
Router(config-if)# no ip pim snooping
```

Note

- Bidirectional PIM does not interfere with directly connected sources.
- PIM dense mode (PIM-DM) is not compatible with PIM snooping.

4.5.11 IGMP Snooping

- With Release 12.2(33)SXH and later releases, to prevent depletion of the switch's hardware table capacity, enter the following command:

```
Router(config)# ip igmp snooping source-only-learning limit {1000 | 2000}
```

  - Enter 2000 unless Virtual Switching System (VSS) is configured.
  - Enter 1000 if VSS is configured.

  Modify the value based on the requirements of your network.

- Rate-limit IGMP traffic. Enter the following command:

```
Router(config)# mls rate-limit multicast ipv4 igmp 5000 100
```

  Modify the packets-per-second and burst values based on the requirements of your network and the available CPU capacity.

Note When IGMP/PIM packets are redirected, the forwarding engine cannot apply ACLs or QoS to them.

Note If you see too much source only flooding, you can change the source-only flooding timer with the **ip igmp snooping source-only-learning age-timer** command.

4.6 Documentation for Multicast

See these publications for more information about multicast:

http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_basic_cfg.html

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/mcastv4.html

http://www.cisco.com/en/US/tech/tk828/tech_white_papers_list.html

4.7 Related Features and Best Practices

None.

5. Best Practices for Denial of Service (DoS) Protection and Security

Cisco Catalyst 6500 best practices are defined for the following DoS Protection and Security technologies:

Note

- Disable features that are not being used.
- Disable CDP on ports that connect to partner companies through an extranet, or to nodes in the network that have no need for data provided by CDP. The data provided by CDP could prove useful to a malicious user.
- Use SNMPv3 with MD5 authentication and DES encryption (see the "3.5 Best Practices for Simple Network Management Protocol (SNMP)" section on page 60).
- If you can predict the IP addresses from which administrators make connections, consider using Cisco Lock-and-Key Security, which provides tightly controlled access.
- To decrease the risk of VLAN hopping by specifically crafted malicious traffic, on Layer 2 ports, configure the access VLAN (the VLAN used when the port is not trunking) to be different than the 802.1Q native VLAN (used for untagged traffic when the port is an 802.1Q trunk) or configure 802.1Q trunks to support only tagged traffic.

5.1 Best Practices for Unicast Reverse Path Forwarding (uRPF) Check

These sections describe best practices for uRPF:

For CLI modifications in IOS release SXI, refer to SXI configuration guidelines:

http://www.cisco.com/en/US/products/ps6017/products_installation_and_configuration_guides_list.html

5.1.1 Description of uRPF Check

The uRPF check verifies that the source address of received IP packets is reachable. The uRPF check discards IP packets that lack a verifiable IP source prefix (route), which helps mitigate problems that are caused by traffic with malformed or forged (spoofed) IP source addresses.

5.1.2 Benefits of the uRPF Best Practices

Implement the recommended configuration to take advantage of the PFC3 hardware support for the uRPF check of received IP packets.

5.1.3 Features Incompatible with uRPF

The PFC does not provide hardware-supported uRPF check for policy-based routing (PBR) traffic. (CSCea53554)

5.1.4 Guidelines and Restrictions for uRPF

- uRPF does not provide complete protection against spoofing. Spoofed packets can enter a network through uRPF-enabled interfaces if an appropriate return route to the source IP address exists.
- The switch applies the same uRPF mode to all interfaces where uRPF check is configured. Any change that you make in the uRPF mode on any interfaces is applied to all interfaces where the uRPF check is configured.
- The “allow default” options of the uRPF modes do not offer significant protection against spoofing.
  - Strict uRPF Check with Allow Default:
    Received IP traffic that is sourced from a prefix that exists in the routing table passes the uRPF check if the prefix is reachable through the input interface. If a default route is configured, any IP packet with a source prefix that is not in the routing table passes the uRPF check if the ingress interface is a reverse path for the default route.
  - Loose uRPF Check with Allow Default:
    If a default route is configured, any IP packet passes the uRPF check.
- Avoid configurations that overload the route processor with uRPF checks.
  - Do not configure uRPF to filter with an ACL.
  - Do not configure the global uRPF “punt” check mode.

Note

- Although the software supports up to 8 reverse-path interfaces (16 in Release 12.2(33)SXH and later releases), limit your configuration to the number of reverse-path interfaces described in the “5.1.5 Recommended uRPF Configuration” section on page 78.
- For a list of guidelines and restrictions that applies to other uRPF configurations, see the uRPF Check Guidelines and Restrictions section.

5.1.5 Recommended uRPF Configuration

The following uRPF configuration is recommended.

- PFC2 Configuration Options
- PFC3 Configuration Options
- Maximum Paths
- uRPF Check Strict Mode
- uRPF Check Pass Global Mode
- uRPF Check Group-Interface Global Mode
- uRPF Check Interface Groups

PFC2 Configuration Options

The PFC2 supports the uRPF check for packets that have a single reverse-path interface. If, on any number of interfaces, the switch receives valid IP packets that have one reverse path interface per source prefix, configure uRPF strict mode.

To ensure that no more than one reverse-path interface exists in the routing table for each prefix, enter the **maximum-paths 1** command in config-router mode when configuring OSPF, EIGRP, or BGP.

Note With a PFC2, the hardware FIB supports 256K entries, which includes 16K IP multicast entries. With the uRPF check enabled, there are twice as many IP entries in the FIB, which effectively reduces the table capacity by half. With the uRPF check enabled, the PFC2 cannot support the full internet routing table.

PFC3 Configuration Options

- uRPF Strict Mode—The uRPF strict mode provides the greatest security against spoofed traffic. If, on all uRPF-check enabled interfaces, the switch receives valid IP traffic through interfaces that are reverse paths for the traffic, then strict mode is an option in these circumstances:
  - If, on a maximum of 24 interfaces, divided into four groups of six interfaces each, the switch receives valid IP packets that have up to six reverse-path interfaces per source prefix, configure uRPF strict mode with the interface-group global mode.

    This option requires you to identify the source prefixes and the interfaces that serve as reverse paths for the source prefixes and to configure interface groups for those reverse path interfaces. All of the reverse-path interfaces for each source prefix must be in the same interface group. You can configure four interface groups, with each group containing up to six reverse-path interfaces. There is no limit on the number of source prefixes that an interface group can support.

    To ensure that no more than six reverse-path interfaces exist in the routing table for each prefix, enter the **maximum-paths 6** command in config-router mode when configuring OSPF, EIGRP, or BGP.

    IP traffic with one or two reverse-path interfaces that is received on uPPF-check enabled interfaces outside the interface groups passes the uRPF check if the ingress interface and at most one other interface are reverse paths.

    With maximum paths set to six, IP traffic with more than two reverse-path interfaces that is received on uPPF-check enabled interfaces outside the interface groups always pass the uRPF check.

  - If, on any number of interfaces, the switch receives valid IP packets that have one or two reverse path interfaces per source prefix, configure uRPF strict mode with the pass global mode.

    To ensure that no more than two reverse-path interfaces exist in the routing table for each prefix, enter the **maximum-paths 2** command in config-router mode when configuring OSPF, EIGRP, or BGP.

- uRPF Loose Mode with the Pass Global Mode—The uRPF loose mode provides less protection than strict mode, but it is an option on switches that receive valid IP traffic on interfaces that are not reverse paths for the traffic. The uRPF loose mode verifies that received traffic is sourced from a prefix that exists in the routing table, regardless of the interface on which the traffic arrives.

Maximum Paths

```
Router(config-router)# maximum-paths [1 | 2 | 6]
```

uRPF Check Strict Mode

```
Router(config-if)# ip verify unicast source reachable-via rx
```

uRPF Check Pass Global Mode

```
Router(config)# mls ip cef rpf multipath pass
```

uRPF Check Group-Interface Global Mode

```
Router(config)# mls ip cef rpf multipath interface-group
```

uRPF Check Interface Groups

```
Router(config)# mls ip cef rpf interface-group [0 | 1 | 2 | 3] interface1 [interface2
[interface3 [interface4]]]
```

5.1.6 Documentation for uRPF

See these publications for more information about uRPF:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/secure.html#Configuring_Unicast_Reverse_Path_Forwarding_Check

http://www.cisco.com/web/about/security/intelligence/unicast-rpf.html

5.1.7 Related Features and Best Practices

None.

5.2 Best Practices for Port Security

These sections describe best practices for port security:

5.2.1 Description of Port Security

Port security allows only a configured number of MAC addresses to send traffic into a port.

5.2.2 Benefits of the Port Security Best Practices

- For stable connections (for example, ports that always support the same devices, as in an office environment: devices like an IP phone, a desktop computer, or the same laptop computer), configure port security with sticky MAC addresses. Port security with sticky MAC addresses allows the switch to learn addresses dynamically and then retain the dynamically learned MAC addresses during a link-down condition.
- For flexible connections (for example, connections to conference rooms or connections that support guests), configure port security with activity-based aging.

5.2.3 Features Incompatible with Port Security

- Switch Port Analyzer (SPAN) destination ports.
- EtherChannel port-channel interfaces.
- With releases earlier than Release 12.2(33)SXH, 802.1X port-based authentication.
- With releases earlier than Release 12.2(18)SXE, port security does not support trunks. (With Release 12.2(18)SXE and later releases, port security supports nonnegotiating trunks.)
- With releases earlier than Release 12.2(18)SXE, port security does not support PVLAN ports.
- With releases earlier than Release 12.2(18)SXE, port security does not support IEEE 802.1Q tunnel ports.

5.2.4 Guidelines and Restrictions for Port Security

- With releases earlier than Release 12.2(18)SXE, port security does not support sticky MAC addresses.
- With releases earlier than Release 12.2(18)SXE, port security does not support activity-based aging.
- The PFC2 does not support activity-based aging.
- With the default port security configuration, enter the **errdisable recovery cause psecure-violation** global configuration command to automatically bring secure ports out of the error-disabled state, or manually reenable ports by entering the **shutdown** and **no shut down** interface configuration commands.
- Enter the **clear port-security dynamic** global configuration command to clear all dynamically learned secure addresses. See the Cisco IOS Master Command List, Release 12.2SX, for complete syntax information.
- Port security learns unauthorized MAC addresses with a bit set that causes traffic to them or from them to be dropped. The **show mac-address-table** command displays the unauthorized MAC addresses, but does not display the state of the bit. (CSCeb76844)

- To preserve dynamically learned sticky MAC addresses and configure them on a port following a bootup or a reload and after the dynamically learned sticky MAC addresses have been learned, you must enter a **write memory** or **copy running-config startup-config** command to save them in the startup-config file.

5.2.5 Recommended Port Security Configuration

The following sections describe the recommended port security configuration.

Note The default violation mode (shutdown) provides the greatest security, but does not provide automatic recovery. If the security requirements of your network allow it, you can configure one of the other violation modes or configure automatic recovery with the **errdisable recovery cause psecure-violation** global configuration command.

5.2.5.1 Recommended Global Configuration

Not applicable.

5.2.5.2 Recommended General Port Configuration

None; use the recommendation for each port type.

5.2.5.3 Recommended Access Port Configuration

For All Port Security-Enabled Ports

```
Router(config)# interface type slot/port
Router(config-if)# switchport
Router(config-if)# switchport mode access
Router(config-if)# switchport port-security
Router(config-if)# switchport port-security maximum number_of_addresses
```

Set the *number_of_addresses* value to a number appropriate for the connection.

For Ports with Stable Connections

```
Router(config-if)# switchport port-security mac-address sticky
```

For Ports with Flexible Connections

```
Router(config-if)# switchport port-security aging type inactivity
```

5.2.5.4 Recommended Layer 2 Trunk Port Configuration

Not applicable.

5.2.5.5 Recommended Layer 3 Port or SVI Configuration

Not applicable.

5.2.6 Documentation for Port Security

See this publication for information about port security:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/port_sec.html

5.2.7 Related Features and Best Practices

None.

5.3 Best Practices for Control Plane Policing (CoPP)

These sections describe best practices for CoPP:

5.3.1 Description of CoPP

The control plane policing (CoPP) feature protects the route processor from unnecessary traffic, including DoS traffic.

5.3.2 Benefits of the CoPP Best Practices

CoPP provides increased security.

5.3.3 Features Incompatible with CoPP

None.

5.3.4 Guidelines and Restrictions for CoPP

- Do not include a **class-map class-default** statement in a CoPP policy map. (CSCsi25255, CSCsf25709)
- CoPP is not supported in hardware for broadcast packets. The combination of ACLs, traffic storm control, and CPP software protection provides protection against broadcast DoS attacks.
- CoPP is not supported in hardware for multicast packets. The combination of ACLs, multicast CPU rate limiters, and CoPP software protection provides protection against multicast DoS attacks.
- CoPP does not support ARP policies. ARP policing mechanisms provide protection against ARP storms.
- CoPP does not support non-IP classes except for the default non-IP class. ACLs can be used instead of non-IP classes to drop non-IP traffic, and the default non-IP CoPP class can be used to limit the non-IP traffic that reaches the RP CPU.

- Do not use the **log** keyword in CoPP policy ACLs.
- With a PFC3A, egress QoS and CoPP cannot be configured at the same time. In this situation, CoPP is performed in the software. A warning message is displayed to inform you that egress QoS and CoPP cannot be configured at the same time.
- If you have a large QoS configuration, the system may run out of TCAM space. If this is the case, CoPP may be performed in software.
- When there is a large QoS configuration for other interfaces, you can run out of TCAM space. When this situation occurs, CoPP may be performed entirely in software and result in performance degradation and CPU cycle consumption.
- You must ensure that the CoPP policy does not filter critical traffic such as routing protocols or interactive access to the switches. Filtering this traffic could prevent remote access to the switch, requiring a console connection.
- PFC3 supports built-in special-case rate limiters, which are useful for situations where an ACL cannot be used (for example, TTL, MTU, and IP options). When you enable the special-case rate limiters, you should be aware that the special-case rate limiters will override the CoPP policy for packets matching the rate-limiter criteria.
- CoPP is not enabled in hardware unless QoS is enabled globally with the **mls qos** command. If the **mls qos** command is not entered, CoPP will only work in software.
- Egress CoPP is not supported. Silent mode is not supported. CoPP is only supported on ingress (service-policy output CoPP cannot be applied to the control plane interface).
- ACE hit counters in hardware are only for ACL logic. You can rely on software ACE hit counters and the **show access-list**, **show policy-map control-plane**, and **show mls ip qos** commands to evaluate CPU traffic.
- CoPP is performed on a per-forwarding-engine basis and software CoPP is performed on an aggregate basis.
- CoPP does not support ACEs with the **log** keyword.
- CoPP uses hardware QoS TCAM resources. Enter the **show tcam utilization** command to verify the TCAM utilization.
- Make sure you consider and allow your applications when configuring CoPP.

5.3.5 Recommended CoPP Configuration

Follow these procedures to develop your CoPP configuration:

- Analyze Traffic
- Filter Traffic by Protocol Type
- Filter Traffic by Protocol Type and Source Address Ranges
- Filter Traffic by Protocol Type and Source Address
- Filter Traffic by Protocol Type, Source Address, and Destination Address

Analyze Traffic

Analyze the existing control and management plane access requirements to determine the exact traffic profile for the filtering lists.

Step 1 Make a list of the known protocols that access the Route Processor and divide them into categories. For example, critical, important, normal, undesirable, and default. Your network might require fewer classes, or it might require additional classes.

- ACL 120: critical traffic
- ACL 121: important traffic
- ACL 122: normal traffic
- ACL 123: explicitly denies unwanted traffic (Slammer worm traffic in this example)
- ACL 124: the rest of the traffic

Step 2 Create ACLs that permit all the known protocols. Use different ACL numbers for each type of traffic. Configure an initial ACE in each ACLs with both the source and destination addresses set to **any**. Configure the final entry in the last ACL as **permit ip any any**, which will match traffic not explicitly permitted by other entries in the other ACLs. For example:

```
access-list 120 remark CoPP ACL for critical traffic
! allow BGP from a known peer to this router's BGP TCP port
! Initial ACE
access-list 120 permit any any eq bgp

access-list 121 remark CoPP Important traffic
! permit return traffic from TACACS host
! Initial ACE
access-list 121 permit any any established
! ssh access to the router from a subnet
!Initial ACE
access-list 121 permit any any eq 22
! telnet access to the router from a subnet
!Initial ACE
access-list 121 permit any any eq telnet
! SNMP access from the NMS host to the router
!Initial ACE
access-list 121 permit any any eq snmp
! Allow the router to receive NTP packets from a known clock source
!Initial ACE
access-list 121 permit any any eq ntp

access-list 122 remark CoPP normal traffic
! permit router originated traceroute
access-list 122 permit icmp any any ttl-exceeded
access-list 122 permit icmp any any port-unreachable
! permit receipt of responses to router originated pings
access-list 122 permit icmp any any echo-reply
! allow pings to router
access-list 122 permit icmp any any echo

access-list 123 remark explicitly defined "undesirable" traffic
! permit, for policing, all traffic destined to UDP 1434
access-list 123 permit udp any any eq 1434

!This ACL identifies all other traffic
access-list 124 remark rest of the IP traffic for CoPP
access-list 124 permit ip any any
```

Step 3 Apply the ACLs to a corresponding set of descriptively named class-maps. For example:

```
class-map CoPP-critical
  match access-group 120
class-map CoPP-important
  match access-group 121
```

```
class-map CoPP-normal
  match access-group 122
class-map CoPP-undesirable
  match access-group 123
class-map CoPP-all-other-ip-traffic
  match access-group 124
```

Step 4 Apply the class maps to a policy-map that permits all traffic, regardless of classification. A default policy is not required at this stage of policy development. For example:

```
policy-map CoPP
 class CoPP-critical
  police 31500000 conform-action transmit exceed-action drop
class CoPP-important
   police 125000 3906 3906 conform-action transmit exceed-action drop
 class CoPP-normal
   police 64000 2000 2000 conform-action transmit exceed-action drop
! This policy drops all traffic categorized as undesirable, regardless of rate.
 class CoPP-undesirable
   police 32000 1500 1500 conform-action drop exceed-action drop
```

Step 5 Enter the **show access-lists** command to determine which ACEs in the ACLs are in use (the ACEs each identify a protocol), as well as the number of packets permitted by the final ACL entry (the **permit ip any any** ACE).

Note At this stage, the **show access-lists** command is more useful than the **show tcam interface** command, which shows what is processed in hardware.

Ideally, you will have identified all required traffic destined to the router. Realistically, not all required traffic will be identified prior to deployment. Some extra analysis will be required to determine the unclassified packets. This extra classification step can be accomplished using several techniques: general ACL classification as described in *Characterizing and Tracing Packet Floods Using Cisco Routers* or packet analyzers. Once classified, modify the ACLs as necessary. Use the **show policy-map control-plane** command to collect data (packet count and rate information) about the policies, which will support development of increasingly granular policies.

Filter Traffic by Protocol Type

Step 1 Remove the final **permit ip any any** ACE (**access-list 124 permit ip any any** in the example).

Note You can use this ACL instead of class-default.

Step 2 If necessary, configure additional ACEs for other protocols that you have identified.

Enter the **show access-lists** command to determine which ACEs in the ACLs are in use (the ACEs each identify a protocol). Enter the **show map** command to display the rate data.

Filter Traffic by Protocol Type and Source Address Ranges

Step 1 As appropriate for some protocols, create ACLs that filter traffic by source addresses.

Note The addresses shown in these ACEs are only examples. You must use the addresses that are valid for your network. Configure the ACE with the allocated CIDR block. For example, if your network has been allocated 171.68.0.0/16, then configure that as the source address, rather than a larger subnet. External BGP (eBGP) requires an exception; the permitted source addresses for the session will lie outside the CIDR block.

For example:

```
access-list 120 remark CoPP ACL for critical traffic
! allow BGP from a known peer to this router's BGP TCP port
access-list 120 permit tcp host 47.1.1.1 host 10.9.9.9 eq bgp
! allow BGP from a peer's BGP port to this router
access-list 120 permit tcp host 47.1.1.1 eq bgp host 10.9.9.9
access-list 120 permit tcp host 10.86.183.120 host 10.9.9.9 eq bgp
access-list 120 permit tcp host 10.86.183.120 eq bgp host 10.9.9.9

access-list 121 remark CoPP Important traffic
! permit return traffic from TACACS host
access-list 121 permit tcp host 1.1.1.1 host 10.9.9.9 established
! ssh access to the router from a subnet
access-list 121 permit tcp 10.0.0.0 0.0.0.255 host 10.9.9.9 eq 22
! telnet access to the router from a subnet
access-list 121 permit tcp 10.86.183.0 0.0.0.255 any eq telnet
! SNMP access from the NMS host to the router
access-list 121 permit udp host 1.1.1.2 host 10.9.9.9 eq snmp
! Allow the router to receive NTP packets from a known clock source
access-list 121 permit udp host 1.1.1.3 host 10.9.9.9 eq ntp
```

Step 2 Replace the initial ACLs with the address-filtering ACLs.

This step provides data about traffic from outside the CIDR block.

Filter Traffic by Protocol Type and Source Address

Narrow the ACL permit statements to only allow known authorized source addresses.

Filter Traffic by Protocol Type, Source Address, and Destination Address

Configure destination addresses in the ACEs.

Caution Care must be taken to ensure that the CoPP policy does not filter critical traffic such as routing protocols or interactive access to the routers. Filtering this traffic could prevent remote access to the router, thus requiring a console connection

5.3.6 Documentation for CoPP

See this publication for more information about CoPP, including complete CoPP configuration procedures:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/dos.html#Understanding_How_Control_Plane_Policing_Works

5.3.7 Related Features and Best Practices

None.

5.4 Best Practices for CoPP Support for ISIS

These sections describe best practices for CoPP Support for ISIS:

5.4.1 Description of CoPP Support for ISIS

The control plane policing (CoPP) feature increases security on the switch by protecting the RP from unnecessary or DoS traffic and giving priority to important control plane and management traffic.

Currently the control plane policing (CoPP) feature does not support non-IP classes except for the default non-IP class (class-default). This means that if CoPP is used, since ISIS CLNS packets are non-IP they will end up in the default non-IP class. If the system is subject to a DoS attack and a policy is applied to the default class, ISIS adjacencies could flap or could go down. For this reason it is recommended not to configure a policy under the default class if ISIS is running in the system.

5.4.2 Benefits of CoPP Support for ISIS

ISIS control-plane protection.

5.4.3 Features Incompatible with CoPP Support for ISIS

Not Applicable

5.4.4 Guidelines and Restrictions for CoPP Support for ISIS

For a list of CoPP restrictions, please see the guidelines and restrictions section in “Configuring Control Plane Policing (CoPP)”

5.4.5 Recommended CoPP Support for ISIS Configuration

If the system is under an IP packet DoS attack and ISIS is running, the following configuration could be used.

```
ip access-list extended MATCH-IP-ONLY

class-map MATCH-IP-ONLY
match access-group name MATCH-IP-ONLY

policy-map CoPP
!--- Critical applications
class CRITICAL
    police cir 10000000000 bc 312500000 conform-action transmit exceed-action transmit
!--- To mitigate IP based DoS
class MATCH-IP-ONLY
    police cir 8000 bc 1500 conform-action transmit exceed-action drop
class class-default
```

If the system is under a non-IP packet DoS attack, ACLs can be used to drop the non-IP traffic.

5.4.6 Configuration Guide for CoPP Support for ISIS

See "Configuring Control Plane Policing (CoPP)" for more details on CoPP configuration.

5.4.7 Related Features and Best Practices

Configuring PFC QoS.

5.5 Best Practices for Attack Protection

Protect the switch from TCP SYN flooding attacks and other advanced attacks with one or more of the these:

- 5.5.1 Firewall Services Module (FWSM)
- 5.5.2 Traffic Anomaly Detector Service Module
- 5.5.3 Anomaly Guard Module
- 5.5.4 IOS Access Control Lists (ACLs)
- 5.5.5 VLAN ACLs (VACLs)
- 5.5.6 Port ACLs (PACLs)
- 5.5.7 QoS ACLs
- 5.5.8 Hardware Rate-Limiters
- 5.5.9 Optimized ACL Logging (OAL)
- 5.5.10 AutoSecure
- 5.5.11 DHCP Snooping
- 5.5.12 IP Source Guard
- 5.5.13 Dynamic ARP Inspection (DAI)

5.5.1 Firewall Services Module (FWSM)

See this publication:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/release/notes/OL_4164.html#Firewall_Services_Module

Note Do not configure the Cisco IOS software firewall features, which are supported in some releases and which run in software with very limited hardware support.

5.5.2 Traffic Anomaly Detector Service Module

See this publication:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/release/notes/OL_4164.html#Traffic_Anomaly_Detector_Module

5.5.3 Anomaly Guard Module

See this publication:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/release/notes/OL_4164.html#Anomaly_Guard_Module

5.5.4 IOS Access Control Lists (ACLs)

See these publications:

- Understanding Cisco IOS ACL Support:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/acl.html

- Access Control Lists Overview and Guidelines:

  http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfacls.html

5.5.5 VLAN ACLs (VACLs)

See this publication:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/vacl.html

5.5.6 Port ACLs (PACLs)

Supported in Release 12.2(33)SXH and later releases—See this publication:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vacl.html#Understanding_Port_ACLs

5.5.7 QoS ACLs

See this publication:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/qos.html

5.5.8 Hardware Rate-Limiters

Rate limiting is used to control the rate of traffic sent or received on a network interface. Traffic that is less than or equal to the specified rate is sent, whereas traffic that exceeds the rate is dropped or delayed. It is performed by policing (discarding excess packets), queuing (delaying packets in transit), or congestion control (manipulating the protocol's congestion mechanism). Policing and queuing can be applied to any network protocol.

Note When possible, use CoPP, because CoPP uses ACLs to select the traffic that needs to be dropped, in contrast to the hardware rate-limiters, which cannot distinguish between offending and non-offending traffic.

When CoPP is not an option, you can configure hardware rate limiters to protect the switch control plane and limit CPU utilization:

- mls rate-limit all mtu-failure
- mls rate-limit all ttl-failure
- mls rate-limit layer2 ip-admission
- mls rate-limit layer2 l2pt
- mls rate-limit layer2 pdu
- mls rate-limit layer2 port-security
- mls rate-limit multicast ipv4 connected
- mls rate-limit multicast ipv4 fib-miss
- mls rate-limit multicast ipv4 igmp
- mls rate-limit multicast ipv4 ip-options
- mls rate-limit multicast ipv4 non-rpf
- mls rate-limit multicast ipv4 partial
- mls rate-limit multicast ipv4 pim
- mls rate-limit multicast ipv6 connected
- mls rate-limit multicast ipv6 default-drop
- mls rate-limit multicast ipv6 mld
- mls rate-limit multicast ipv6 route-cntl
- mls rate-limit multicast ipv6 sec
- mls rate-limit multicast ipv6 secondary-drop
- mls rate-limit multicast ipv6 sg
- mls rate-limit multicast ipv6 starg-bridge
- mls rate-limit multicast ipv6 starg-m-bridge
- mls rate-limit unicast acl input
- mls rate-limit unicast acl mac-pbf
- mls rate-limit unicast acl output
- mls rate-limit unicast acl vacl-log
- mls rate-limit unicast cef glean

- mls rate-limit unicast cef receive
- mls rate-limit unicast ip arp-inspection
- mls rate-limit unicast ip dhcp-snooping
- mls rate-limit unicast ip errors
- mls rate-limit unicast ip features
- mls rate-limit unicast ip icmp redirect
- mls rate-limit unicast ip icmp unreachable acl-drop
- mls rate-limit unicast ip icmp unreachable no-route
- mls rate-limit unicast ip options
- mls rate-limit unicast ip rpf-failure

See these publications:

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_white_paper0900aecd805457cc.html#wp9000351

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/dos.html

Note See these sections for information about rate limiting multicast traffic:

- 4.5.4 Non-RPF Traffic, page 71
- 4.5.5 Partially and Completely Switched Flows, page 71
- 4.5.7 Rate Limit Traffic from Directly Connected Sources, page 72
- 4.5.11 IGMP Snooping, page 74

5.5.9 Optimized ACL Logging (OAL)

Optimized ACL Logging (OAL) provides PFC3 hardware support for ACL logging. See this publication:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/acl.html#Optimized_ACL_Logging_with_a_PFC3

5.5.10 AutoSecure

Note Release 12.2(33)SXH and later releases support AutoSecure.

The AutoSecure feature automatically secures the switch. See this publication for information about AutoSecure:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/autosec.html

5.5.11 DHCP Snooping

Note The PFC3 and Release 12.2(18)SXE and later releases support DHCP Snooping.

DHCP snooping acts like a firewall between untrusted hosts and trusted DHCP servers. DHCP snooping provides a valuable security function and is required to support IP Source Guard. See this publication for information about DHCP Snooping:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/snoodhcp.html

5.5.12 IP Source Guard

Note Release 12.2(33)SXH and later releases support IP Source Guard.

IP Source Guard provides source IP address filtering on a Layer 2 port to prevent a malicious host from impersonating a legitimate host by assuming the legitimate host's IP address. IP Source Guard is an effective means of spoofing prevention at Layer 2. See this publication for information about IP Source Guard:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/ipsrcgrd.html

5.5.13 Dynamic ARP Inspection (DAI)

Note The PFC3 and Release 12.2(18)SXE and later releases support DAI.

Dynamic ARP Inspection (DAI) mitigates ARP poisoning attacks. See this publication for information about DAI:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/dynarp.html

5.6 Best Practices for Controlling Management Session Access

These sections describe best practices for controlling management session access:

5.6.1 Description of Controlling Management Session Access

By default, anyone who knows an IP address on the switch can attempt to open a management session. Similarly, if there is a terminal server configured to provide network access to the console connection, anyone who knows an IP address on the terminal server can attempt to make a console connection.

When all the switch or terminal server VTY lines are in use, new management sessions cannot be established, which creates a DoS condition for management session access to the switch.

Controlling management session access can help ensure that all connections are valid.

5.6.2 Benefits of the Controlling Management Session Access Best Practices

5.6.2.1 Use Secure Shell (SSH) and Secure Copy Protocol (SCP)

Secure Shell (SSH) is a network protocol that supports encrypted data exchange between two devices. SSH supports authentication with public-key cryptography.

Instead of Telnet, use SSH to encrypt management session traffic, which prevents access of the data being transmitted by a malicious user. Cisco IOS software supports SSH Version 1.0 (SSHv1) or SSH Version 2.0 (SSHv2).

Cisco IOS software also supports the Secure Copy Protocol (SCP), which supports encrypted connections for copying configuration files or software images. SCP relies on SSH. Use secure file transfer protocols (for example, Secure Copy Protocol (SCP) instead of FTP or TFTP), when you copy configuration data.

5.6.2.2 Configure VTY Lines to Maintain Sessions

Use the **exec-timeout** command to logout idle sessions. Use the **service tcp-keepalive-in** command to enable TCP keepalives, which ensures that the device on the remote end of the connection is still accessible and that half-open or orphaned connections are closed.

5.6.2.3 Limit Access to VTY Lines

If you can predict the networks or IP addresses from which you wish to allow management sessions, use access control lists (ACLs) to deny traffic from unknown sources.

5.6.3 Features Incompatible with Controlling Management Session Access

None.

5.6.4 Guidelines and Restrictions for Controlling Management Session Access

See the customer documentation for the guidelines and restrictions of the features used to control management session access.

5.6.5 Recommended Management Session Access Control Configuration

This example configuration enables management session access control:

```
!
service tcp-keepalives-in
!
hostname selected_name /* For SSH
ip domain name example.com /* For SSH
!
crypto key generate rsa modulus 2048/* For SSH
!
ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 3
ip ssh source-interface type slot/port
!
line vty 0 4
transport input ssh
no transport output
exec-timeout 15 0
login local
access-class 101 in
exit
access-list 101 remark VTY SSH Access ACL
! Configure an appropriate permit statement
access-list 101 permit tcp ... eq 22 log-input
access-list 101 deny ip any any log-input
!
```

This configuration example enables SCP services:

```
!
ip scp server enable
!
```

5.6.6 Documentation for Controlling Management Session Access

See this publication for more information about Secure Shell (SSH):

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_cfg_secure_shell.html

See this publication for more information about Secure Copy:

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_ssh/configuration/12-2sx/sec-secure-copy.html

See this publication for more information about configuring VTY lines:

http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_terminals.html

See this publication for more information about configuring ACLs:

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_acl_ov_guideline.html

5.6.7 Related Features and Best Practices

None.

5.7 Best Practices for NetFlow Data Export (NDE) for Security

Data Export (NDE) is also covered in the "3.7 Best Practices for NetFlow Data Export (NDE)" section on page 62. This section describes the security applications of NDE.

Use NDE to monitor for unusually heavy data-traffic. NDE allows you to see traffic as it traverses the network in real time. NDE allows you to quickly identify and trace network traffic, especially during incident response. NDE can provide visibility into all traffic on the network.

NetFlow data can be viewed and analyzed through the command line interface (CLI) or the data can be exported to a NetFlow collector for aggregation and analysis.

These sections, earlier in this document, describe the best practices for NDE:

- 3.7.1 Description of NDE, page 63
- 3.7.2 Benefits of the NDE Best Practices, page 63
- 3.7.3 Features Incompatible with NDE, page 63
- 3.7.4 Guidelines and Restrictions for NDE, page 63
- 3.7.5 Recommended NDE Configuration, page 63
- 3.7.6 Customer Documentation for NDE, page 63
- 3.7.7 Related Features and Best Practices, page 64

5.8 Best Practices for Private VLANs (PVLANs) for Servers

These sections describe best practices for PVLANs:

- 5.8.1 Description of PVLANs
- 5.8.2 Benefits of the PVLANs Best Practices
- 5.8.3 Features Incompatible with PVLANs
- 5.8.4 Guidelines and Restrictions for PVLANs
- 5.8.5 Recommended PVLANs Configuration
- 5.8.6 Documentation for PVLANs
- 5.8.7 Related Features and Best Practices

5.8.1 Description of PVLANs

Private VLANs (PVLANs) limit connectivity between ports in a VLAN.

5.8.2 Benefits of the PVLANs Best Practices

Networking topologies exist where security can be improved by limiting communication between devices on a single VLAN. For example, PVLANs are often used to prevent communication between servers in a publicly accessible subnet. If one of the servers is compromised, the lack of connectivity to other servers due to the application of PVLANs may help limit the problem to just one server.

5.8.3 Features Incompatible with PVLANs

- VTP client and server modes.

- VLAN database configuration mode.
- VTP does not propagate a private VLAN configuration.

5.8.4 Guidelines and Restrictions for PVLANs

There are extensive guidelines and restrictions for PVLANs. See this publication:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/pvlans.html#Private_VLAN_Configuration_Guidelines_and_Restrictions

5.8.5 Recommended PVLANs Configuration

See the "Configuring Private VLANs" section of the customer documentation.

5.8.6 Documentation for PVLANs

See this publication for more information about PVLANs:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/pvlans.html

5.8.7 Related Features and Best Practices

None.

6. Best Practices for Virtual Switching System (VSS)

Cisco Catalyst 6500 best practices are defined for the following Virtual Switching System (VSS) technologies:

6.1 Best Practices for VSS Standby Console Usage

These sections describe best practices for VSS standby console usage:

6.1.1 Description of VSS Standby Console Usage

VSS converts two physical chassis into one logical device. Hence it is generally recommended to use standby console only during dual-active troubleshooting, if and when the VSL is down. For other information that is needed from the Standby switch, it is recommended to use “remote command” on Active switch.

6.1.2 Benefits of VSS Standby Console Usage

In dual-active scenario, it may be necessary for the administrator to troubleshoot on both chassis consoles. Once the VSL is brought back up, the VSS will be in operation.

6.1.3 Features Incompatible with VSS Standby Console Usage

None.

6.1.4 Guidelines and Restrictions for VSS Standby console usage

Use console line to troubleshoot both chassis if in dual-active scenario.

6.1.5 Recommended VSS Standby Console Usage Configuration

None.

6.1.6 Configuration Guide for VSS Standby Console Usage

None.

6.1.7 Related Features and Best Practices

- Dual-Active Detection
- Configuring Dual-Active Detection

6.2 Best Practices for VSS Image Upgrade

These sections describe best practices for VSS Image Upgrade:

6.2.1 Description of VSS Image Upgrade

Upgrading an image provides most up to date bug fixes, as well as a set of new features. Specific image upgrade steps should be followed to have optimal uptime in VSS.

6.2.2 Benefits of the VSS Image Upgrade Best Practices

Following the steps listed below for VSS image upgrade would provide optimal uptime during upgrade process. The downtime during the image upgrade will be the same as RPR switchover time.

6.2.3 Features Incompatible with VSS Image Upgrade

None.

6.2.4 Guidelines and Restrictions for VSS Image Upgrade

The following steps should be followed while performing image upgrade in VSS:

1. Copy new images to both of the flash devices in the Active and Standby switches.
2. Change the boot variable with the **boot system** *device_name*:*file_name* global configuration command and save the running-config file.
3. Enter the **redundancy reload peer** command.
4. Standby switch will reboot into RPR mode with new image.
5. Enter the **redundancy force switch-over** command.
6. The previous Standby switch will continue to bootup from RPR mode into Active switch. During this time, traffic may be disrupted, until the linecard is completely booted up. Previous Active switch will be rebooted with new image as Standby, and come up in SSO mode.

6.2.5 Recommended VSS Image Upgrade Configuration

None.

6.2.6 Configuration Guide for VSS Image Upgrade

RPR and SSO dependency

Configuring RPR Supervisor Engine Redundancy

6.2.7 Related Features and Best Practices

None.

6.3 Best Practices for VSL Capacity Planning

These sections describe best practices for VSL Capacity Planning:

6.3.1 Description of VSL Capacity Planning

VSL is the most critical link for VSS that carries control traffic, as well as data traffic between two redundant chassis. It is important that enough VSL ports are being connected to reserve enough bandwidth and provide high availability in case of link breakage. It is recommended at minimum that both of the Sup4 uplink ports to be connected between both chassis, and used for VSL. As control and data traffic grows across VSL, additional VSL ports (up to 6 in total, not counting the Sup4 uplinks) can be added on 6708-10GE.

6.3.2 Benefits of VSL Capacity Planning

This will ensure maximum up time and high availability.

6.3.3 Features Incompatible with VSL Capacity Planning

None.

6.3.4 Guidelines and Restrictions for VSL Capacity Planning

None.

6.3.5 Recommended VSL Capacity Planning Configuration

None.

6.3.6 Configuration Guide for VSS Capacity Planning

None.

6.3.7 Related Features and Best Practices

None.

6.4 Best Practices for Migration From Non-VSS to VSS

These sections describe best practices for Migration From Non-VSS to VSS:

6.4.1 Description of Migration From Non-VSS to VSS

In a production network, some migration steps are recommended while converting from non-VSS to VSS. See link in the recommended configuration section for reference to the detailed steps.

6.4.2 Benefits of the Migration From Non-VSS to VSS Best Practices

This achieves the maximum uptime for the production network during the migration.

6.4.3 Features Incompatible with Migration From Non-VSS to VSS

None.

6.4.4 Guidelines and Restrictions for Migration From Non-VSS to VSS

None.

6.4.5 Recommended Migration From Non-VSS to VSS Configuration

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

6.4.6 Configuration Guide for Migration From Non-VSS to VSS

Configuring Virtual Switching Systems

6.4.7 Related Features and Best Practices

None.

6.5 Best Practices for VSS Power Management

These sections describe best practices for VSS Power Management:

6.5.1 Description of VSS Power Management

In VSS, two physical chassis is needed, hence power supplies are needed for each of the chassis. It is recommended to have dual power supply in each of the chassis. Power redundancy mode can be configured separately on each of the chassis. It is recommended that the two chassis are exact replica of each other, to provide full redundancy and achieve minimal downtime in case one of the switch gone down. Also it is recommended that both chassis are configured with the same power redundancy mode, specifically redundant mode

6.5.2 Benefits of the VSS Power Management Best Practices

This achieves the maximum uptime with redundant power supplies in case one of the power supplies has hardware failure.

6.5.3 Features Incompatible with VSS Power Management

None.

6.5.4 Guidelines and Restrictions for VSS Power Management

None.

6.5.5 Recommended VSS Power Management Configuration

The following configuration is needed to configure power redundancy mode as redundant in VSS:

```
Router(config)# power redundancy-mode redundant switch 1
Router(config)# power redundancy-mode redundant switch 2
```

6.5.6 Configuration Guide for VSS Power Management

- VSS Power Management
- Cisco Power Calculator

6.5.7 Related Features and Best Practices

None

6.6 Best Practices for VSS CPU Protection

These sections describe best practices for VSS CPU Protection:

6.6.1 Description of VSS CPU Protection Recommendation

In VSS, Active SP and RP are responsible for many control plane decision and calculations, hence it is important that the Active CPUs are protected with hardware rate-limiters and Control Plane Policing. For a smooth operation, we would like the CPU to be as idle as possible since the bulk of forwarding is handled by hardware. A less busy CPU reacts to events quickly and become more responsive to network operation. There are few features in layer 3 routing might cause busy CPU. We should provide the right implementation to avoid unnecessary CPU hog.

- For IOS features like TCP intercept, PBR, etc., the first packet is always software switched. When the flow established, CPU will program the flow to hardware, the remaining packets are switched by hardware. Therefore, we must avoid sudden large amount of initial packets that overwhelm CPU. Many “mls rate-limit” commands are provided to protect CPU. We should implement them judiciously.
- Some control or resolution packets like ICMP, ARP, etc., must be handled by CPU. Use “mls rate-limit” to limit their frequency hitting CPU.

ACL and QOS classifications are implemented in hardware using TCAM. Although TCAM implementation provides constant lookup rates regardless of size of ACL and QOS entries, optimal use of TCAM resources are still important. Because, when a link flaps, software has to recalculate ACL and QOS entries then reprogram TCAM again, contributing to converging delays.

6.6.2 Benefits of the VSS CPU Protection Recommendation

With CPU being protected, it would help to ensure VSS to be in healthy state.

6.6.3 Features Incompatible with VSS CPU Protection Recommendation

User should be aware of any software switched features that would be software switched by the CPU.

6.6.4 Guidelines and Restrictions for VSS CPU Protection Recommendation

None.

6.6.5 Recommended VSS CPU Protection Configuration

User should configure hardware rate-limiters to protect the CPU, as specified in the reference of the configuration guide section.

6.6.6 Configuration Guide for VSS CPU Protection Recommendation

- **mls rate-limit unicast cef glean 1000**
- Recommended Rate-Limiter Configuration
- Configuring Control Plane Policing

6.6.7 Related Features and Best Practices

None.

6.7 Best Practices for VSS NAM Service Module Integration

These sections describe best practices for VSS NAM Service Module Integration:

6.7.1 Description of VSS Network Analysis Module (NAM) Integration

NAM is a service module that is supported in VSS. It is a tool that helps network administrators to monitor traffic flow, and perform statistical analysis. It is recommended to have NAM in each of the Active and Standby chassis to provide redundancy.

6.7.2 Benefits of the VSS NAM Service Module Integration Best Practices

With NAM installed in redundant fashion, it provides high availability network monitoring.

6.7.3 Features Incompatible with VSS NAM Service Module Integration

None.

6.7.4 Guidelines and Restrictions for VSS NAM Service Module Integration

Same restrictions as SPAN in VSS.

6.7.5 Recommended VSS NAM Service Module Integration Configuration

The following sections describe the recommended NAM configuration.

- Enable NAM management VLAN:

```
Router(config)# analysis switch 1 module 1 management-port access-vlan 100
```

- Configure NAM IP address:

```
Router# session switch 1 slot 1
root@nam# ip address 10.100.1.2
```

6.7.6 Configuration Guide for NAM

Quick Start Guide for Catalyst 6500 Series and Cisco 7600 Series Network Analysis Module, Release 3.6

6.7.7 Related Features and Best Practices

3.10 Best Practices for Switched Port Analyzer (SPAN)

6.8 Best Practices for VSS VSLP Timers

These sections describe best practices for VSS VSLP timers:

6.8.1 Description of VSS VSLP Timers

VSLP Timers control the hello messages that traverse between each end of the VSL links.

6.8.2 Benefits of the VSS VSLP Timers

VSLP timers can be configured to change the transmission interval between hello messages as well as receiving interval timeout across VSL links.

6.8.3 Features Incompatible with VSS VSLP Timers

None.

6.8.4 Guidelines and Restrictions for VSS VSLP Timers

Configuring VSLP Timers

6.8.5 Recommended VSS VSLP Timers Configuration

It is recommended to leave VSLP Timers at default values.

6.8.6 Configuration Guide for VSS VSLP Timers

Configuring the VSLP Timer

6.8.7 Related Features and Best Practices

None.

6.9 Best Practices for Matching PFC and DFC

These sections describe best practices for matching PFC and DFC:

6.9.1 Description of matching PFC and DFC

In VSS, since the switch fabric extends over VSL between two physical chassis, it is recommended that both switches are operating in the same PFC mode. In order to do so, it is recommended to keep all of the PFC and DFC to be the same type. i.e. all 3CXL, or all 3C, but no mix and match.

6.9.2 Benefits of the matching PFC and DFC

This ensures complete redundancy and consistent hardware within VSS.

6.9.3 Features Incompatible with matching PFC and DFC

None.

6.9.4 Guidelines and Restrictions for matching PFC and DFC

None.

6.9.5 Recommended matching PFC and DFC configuration

Default configuration is recommended. In case of PFC/DFC mismatch, it is recommended to force the system into PFC3C mode by issuing the following command:

```
Switch (config)# platform hardware vsl pfc mode pfc3c
```

6.9.6 Configuration Guide for Matching PFC and DFC

SSO dependencies

6.9.7 Related Features and Best Practices

None.

6.10 Best Practices for VSS Domain-ID

These sections describe best practices for VSS domain-ID:

6.10.1 Description VSS Domain-ID

VSS converts two physical chassis into one logical device as known as VSS Domain, each Domain-ID represents a unique node within the network.

6.10.2 Benefits of VSS Domain-ID

A VSS domain share a single point of management, single gateway IP address, and single routing instance and eliminates the dependence on First Hop Redundancy Protocols (FHRP) and Spanning Tree Protocol.

6.10.3 Features Incompatible with VSS Domain-ID

None.

6.10.4 Guidelines and Restrictions for VSS Domain-ID

None.

6.10.5 Recommended VSS Domain-ID Configuration

Use a unique domain-ID ranging from 1 to 255 within the network.

6.10.6 Configuration Guide for VSS Domain-ID

Assigning Virtual Switch Domain and Switch Numbers

6.10.7 Related Features and Best Practices

None.

6.11 Best Practices for VSS Priority/Preemption

These sections describe best practices for VSS Priority/Preemption:

6.11.1 Description of VSS Priority/Preemption

VSS Priority allow switch that has higher priority configured to boot up as Active chassis if both chassis are brought up at the same time or if the other one has not assumed as an active role.

VSS Preemption allow switch with higher priority configured to initiate a switchover to become active if it comes up in standby state after a reload or a switchover.

6.11.2 Benefits of the VSS Priority/Preemption

None.

6.11.3 Features Incompatible with VSS Priority/Preemption

None.

6.11.4 Guidelines and Restrictions for VSS Priority/Preemption

The switch with the higher priority assumes the active role.

The priority range is 1 to 255; the default is 100.

The new priority value only takes effect after you save the configuration and perform a reload of the VSS.

6.11.5 Recommended VSS Priority/Preemption Configuration

It is recommend NOT configuring switch preemption since identical hardware setup between Active/Standby chassis is recommended with virtual router-mac address configured and that all links connected to Neighbor switch through MEC links. Preempt ensures that one particular switch will always be active in the end. However, forcing preemption transitions requires a reload and potential traffic outage.

6.11.6 Configuration Guide for VSS Priority/Preemption

Configuring VSL Switch Priority

6.11.7 Related Features and Best Practices

None.

6.12 Best Practices for VSS Router MAC Address

These sections describe best practices for VSS Router MAC Address:

6.12.1 Description of VSS Router MAC Address

When the VSS is started for the first time, the initial active supervisor engine assigns a router MAC address for the VSS. By default, the supervisor engine assigns a MAC address from its own chassis. After a switchover to the second chassis, the VSS continues to use the MAC address from the previously active chassis as the router MAC address.

6.12.2 Benefits of VSS Router MAC Address

In rare case where both chassis later become inactive and then start up with the second or different supervisor engine becoming the initial active supervisor engine, the VSS will start up with a router MAC address from that respective chassis.

Other Layer 2 hosts that do not respond to GARP (Generic Attribute Registration Protocol) and are not directly connected to the VSS will retain the earlier router MAC address of the VSS, and will not be able to communicate with the VSS.

To avoid this possibility, a virtual router MAC address can be assigned from a reserved pool of addresses with the domain ID encoded in the last octet of the MAC address, or a specific router MAC address can be configured manually.

6.12.3 Features Incompatible with VSS Router MAC Address

None.

6.12.4 Guidelines and Restrictions for VSS Router MAC Address

None.

6.12.5 Recommended VSS Router MAC Address Configuration

Use virtual router MAC address for the VSS:

```
Router(config)# switch virtual domain 1
Router(config-vs-domain)# mac-address use-virtual
```

6.12.6 Configuration Guide for VSS Router MAC Address

Configuring the Router MAC Address Assignment

6.12.7 Related Features and Best Practices

None.

6.13 Best Practices for VSS Standby Port Bringup/Delay

These sections describe best practices for VSS Standby Port Bringup/Delay:

6.13.1 Description of VSS Standby Port Bringup/Delay

When a failed chassis is restarted as the standby chassis, rather than allowing all ports to be activated simultaneously, you can configure the system to defer activation of non-VSL ports and then to activate the ports in groups over a period of time.

6.13.2 Benefits of the VSS Standby Port Bringup/Delay

By delaying standby port bring up, CPU utilization can be lower on the Active chassis.

6.13.3 Features Incompatible with VSS Standby Port Bringup/Delay

None.

6.13.4 Guidelines and Restrictions for VSS Standby Port Bringup/Delay

Only non-VSL ports can be configured

6.13.5 Recommended VSS Standby Port Bringup/Delay Configuration

It is recommended to set the delay time to 300 seconds, and port bring up at 1 port per 1 second.

```
Router(config-vs-domain)# standby port delay 300
Router(config-vs-domain)# standby port bringup 1 1
```

6.13.6 Configuration Guide for VSS Standby port bringup/delay

Configuring Deferred Port Activation During Standby Recovery

6.13.7 Related Features and Best Practices

None.

6.14 Best Practices for VSS IP Connectivity Management

These sections describe best practices for VSS IP Connectivity Management:

6.14.1 Description of VSS IP Connectivity Management

VSS converts two physical chassis into one logical device. Hence from the management perspective (in addition or in lieu of the console port), the management from the IP approach need to be common for both physical switches. It is recommended that L3 MEC be used to provide the IP connectivity for management purpose.

6.14.2 Benefits of VSS IP Connectivity Management

IP connectivity for management will be guarantee whenever the VSS is in operation and the IP address is NOT dependent on which chassis (switch ID 1 or switch ID 2) is the Active switch. Additionally, common IP address for management provide a deterministic origination source IP address and source interface for applications such as (but not limited to) NTP, Radius, SNMP.

6.14.3 Features Incompatible with VSS IP Connectivity Management

None.

6.14.4 Guidelines and Restrictions for VSS IP Connectivity Management

Interfaces used in the MEC for the VSS IP Connectivity Management should NOT be included in the VSS Dual Active Exclusion Interface list.

6.14.5 Recommended VSS IP Connectivity Management Configuration

None.

6.14.6 Configuration Guide for VSS IP Connectivity Management Configuration

```
interface g1/8/1
      channel-group 101 mode active
interface g2/8/2
      channel-group 101 mode active
interface port-channel 101
      description: VSS Network IP Access
      ip address 172.20.1.2 255.255.255.252
```

6.14.7 Related Features and Best Practices

- Dual Active Detection
- Configuring Dual Active Detection

6.15 Best Practices for VSS Dual-Active Detection

These sections describe best practices for VSS Dual-Active Detection:

6.15.1 Description of VSS Dual-Active Detection

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

6.15.2 Benefits of the VSS 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. Additionally, during this scenario, all the interfaces from the original active chassis will be suspended/shut-down. It is recommended if troubleshooting is required is to leverage the console port. If this is not available, it is recommended that non-MEC ports residing on the both switches be configured as L3 port for IP connectivity.

6.15.3 Features Incompatible with VSS Dual-Active Detection

Dual-Active Detection Using PAGP+

Cisco-proprietary protocol for managing EtherChannels. The VSS MEC must have at least one port on each chassis of the VSS and terminates to a Cisco switch.

Dual-Active Detection Using IP BFD

Requires direct connection between the two switches, Regular Layer 3 ping will not function correctly on this connection, the VSS instead uses the Bidirectional Forwarding Detection (BFD) protocol.

6.15.4 Guidelines and Restrictions for VSS Dual-Active Detection

Dual-Active Detection

6.15.5 Recommended VSS Dual-Active Detection Configuration

General Configuration Recommendations

- It is recommended to use PAgP+ for Dual-Active Detection across two different PAgP+ enabled switches. If PAgP+ enabled switches are not available, use BFD Dual-Active Detection instead.
- If troubleshooting is required during the dual-active scenario, it is recommended to leverage the console port for access to the switches. If the IP connectivity for dual-active troubleshooting is the only option, non-MEC ports residing on both switches should be configured as L3 port for IP connectivity.
- Additionally, ensure that those ports are configured in the interface exclusion list and do not participate in the dynamic routing process as network inconsistency may occur during dual-active condition. On VSS, we recommend that the static routes be configured pointing to the VSS next-hop router if the network management is residing on a different subnet.

Configuration for Troubleshooting VSS Dual-Active on IP Connectivity and Interface Exclusion

```
interface GigabitEthernet1/1/24
 no switchport
 ip address 101.1.24.1 255.255.255.0
```

```
interface GigabitEthernet2/3/24
 ip address 102.3.24.1 255.255.255.0

Router(config)# switch virtual domain 1
Router(config-vs-domain)# dual-active exclude interface g1/1/24
WARNING: This interface should only be used for access to the switch when in dual-active
recovery mode and should not be configured for any other purpose

Router(config-vs-domain)# dual-active exclude interface g2/3/24
WARNING: This interface should only be used for access to the switch when in dual-active
recovery mode and should not be configured for any other purpose

Router(config)# ip route 198.2.1.0 255.255.255 101.1.24.2 254

Router(config)# ip route 198.2.1.0 255.255.255 102.3.24.2 254
```

Note 198.2.1.0 is the management network and 102.1.24.2 and 102.3.24.2 are the IP addresses of the next-hop router.

6.15.6 Configuration Guide for VSS Dual-Active Detection Configuration

Configuring Dual-Active Detection

6.15.7 Related Features and Best Practices

None.

6.16 Best Practices for VSS VSLP Timers

These sections describe best practices for VSS VSLP Timers:

- 6.16.1 Description of VSS VSLP Timers
- 6.16.2 Benefits of the VSS VSLP Timers
- 6.16.3 Features Incompatible with VSS VSLP Timers
- 6.16.4 Guidelines and Restrictions for VSS VSLP Timers
- 6.16.5 Recommended VSS VSLP Timers Configuration
- 6.16.6 Configuration Guide for VSS VSLP Timers
- 6.16.7 Related Features and Best Practices

6.16.1 Description of VSS VSLP Timers

VSLP Timers are the hello messages that traverse between each end of the VSL links.

6.16.2 Benefits of the VSS VSLP Timers

VSLP timers can be configured to change the transmission interval between hello messages across VSL links.

6.16.3 Features Incompatible with VSS VSLP Timers

None.

6.16.4 Guidelines and Restrictions for VSS VSLP Timers

Configuring the VSLP Timer

6.16.5 Recommended VSS VSLP Timers Configuration

It is recommended to leave VSLP Timers at default values.

6.16.6 Configuration Guide for VSS VSLP Timers

Configuring the VSLP Timer

6.16.7 Related Features and Best Practices

None.

6.17 Best Practices for VSS STP features

These sections describe best practices for VSS STP features:

6.17.1 Description of STP on VSS

Spanning-Tree Protocol (STP) is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For a Layer 2 Ethernet network to function properly, only one active Layer 2 path can exist between any two network devices.

A Virtual Switching System (VSS) is composed of two independent Catalyst 6500 switches. The two switches are combined using a special port-channel called Virtual Switch Link (VSL).

The STP algorithm is operational only on the active switch. Any BPDU (Bridge Protocol Data Unit) received on the standby port is redirected to the active switch via the VSL.

Although STP is not essential for a VSS to function, it is recommended to enable the protocol in case a loop is introduced in a Layer 2 domain by some other network device.

6.17.2 Benefits of the STP Best Practices for VSS

Since all the BPDUs are redirected to the active switch, there are implications for VSS because the port density is higher for it compared with a non-VSS switch. It is therefore important to follow the best practices for a STP deployment on VSS.

A VSS has the same restriction in terms of the virtual port (VP) instances that can be created per line card and per VSS as does a non-VSS setup. To check the VP instances currently in use please refer to show vlan virtual-port.

It is recommended to have MST (Multiple Spanning Tree) STP protocol for VSS. MST maps multiple VLANs into a spanning tree instance, with each instance having a spanning tree topology independent of other spanning tree instances. This architecture provides multiple forwarding paths for data traffic, enables load balancing, and reduces the number of spanning tree instances required to support a large number of VLANs.

If the number of VLANs are not significant on the VSS then Rapid PVST (Per-VLAN Spanning Tree) can be implemented. The virtual port instances for VSS while running PVST should not exceed 1800 per linecard and 10000 combined.

6.17.3 Features Incompatible with STP on VSS

Flexlink interfaces

6.17.4 Guidelines and Restrictions for STP on VSS

Same as non-VSS

6.17.5 Recommended Configuration for STP on VSS

Same as non-VSS

6.17.6 Configuration Guide for STP on VSS

See the "Configuring MST" section for more information.

See the "Enabling Rapid PVST" section for more information.

6.17.7 Related Features and Best Practices

Configuring Optional STP Features

6.18 Best Practices for VSS in a Layer 2 Campus Environment

These sections describe best practices for VSS in a Layer 2 Campus Environment:

6.18.1 Description of Layer 2 Campus on VSS

VSS is recommended to be positioned as a distribution-layer switch. Multi Chassis Etherchannel (MEC) is one of the primary features now available with the implementation of VSS. It is recommended to use layer 2 MEC from the access-layer switches to the VSS. This will reduce the migration planning required to move from non-VSS infrastructure to one with VSS.

The VSS should be designated the spanning-tree root for the configured STP protocol.

6.18.2 Benefits of VSS in a Layer 2 Campus Environment

Any spanning-tree loop in a non-VSS infrastructure may cause impact to the network infrastructure because non-VSS network relies on STP to determine a loop free environment. A VSS on the other hand only uses STP as a mechanism to prevent loops. A VSS therefore makes it is easier for a network designer to derive a more robust network.

6.18.3 Features Incompatible with Layer 2 Campus on VSS

None.

6.18.4 Guidelines and Restrictions for Layer 2 campus on VSS

Same as non-VSS.

6.18.5 Recommended Configuration for Layer 2 campus on VSS

Please refer to Virtual Switching System Key Concepts section.

6.18.6 Configuration Guide for Layer 2 campus on VSS

See the "Configuring MST" section for more information.

6.18.7 Related Features and Best Practices

Configuring Optional STP Features

6.19 Best practices for SPAN on VSL

These sections describe best practices for SPAN on VSL:

6.19.1 Description of SPAN on VSS

Local SPAN, RSPAN, and ERSPAN sessions allow you to monitor traffic on one or more ports, or one or more VLANs, and send the monitored traffic to one or more destination ports.

In a VSS system, there are restrictions specifically on VSL ports. Since the number of SPAN sessions is same as a non-VSS system, carefully planning will be required to ensure that span traffic does not overwhelm the VSL links. These points will require the user to carefully select the number of ports to use as SPAN source and SPAN destination. Estimate the Minimum and Maximum amount of traffic that would be flowing through the VSL from the sources to the destinations, thus helping to maintain a controlled ratio of SPAN traffic and VSL capacity.

The selection of Centralized and Distributed mode of forwarding plays an important role. As in centralized mode the amount of traffic passing through the VSL depends on the which switch is the active switch. Considering the above points, the user should limit the number of vlan or ports as SPAN source and destination. One single destination port would simplify the design and would have more predictable traffic rate across the VSL. It is also recommended to have the Destination port as PO port, so that the SPAN traffic forwarded to the Destination port would not have to cross the VSL link.

6.19.2 Benefits of VSS best practices for SPAN

If carefully planning is done to monitor the high-bandwidth traffic using SPAN such that the inter-chassis monitoring is minimized, VSL will not be oversubscribed. It is also recommended to use SPAN only while troubleshooting and to be turned off when it is not required.

6.19.3 Features Incompatible

None.

6.19.4 Guidelines and Restrictions for SPAN on VSS

For details refer to the VSS SPAN restrictions.

6.19.5 Recommended Configuration for SPAN on VSS

It is recommended to use the default egress SPAN operating mode for Local SPAN, RSPAN and ERSPAN.

6.19.6 Configuration Guide for VLAN distribution on VSS

See the “Configuring Local SPAN, RSPAN, and ERSPAN” chapter for more information about the commands shown.

6.19.7 Related Features and Best Practices

None.

6.20 Best Practices for MAC Synchronization on VSS

These sections describe best practices for MAC Synchronization on VSS:

6.20.1 Description of MAC Synchronization on VSS

Any new MAC address learnt on any DFC based line card will be propagated to all other DFCs through hardware. This is required to keep MAC tables in sync and to enable L2 forwarding.

6.20.2 Benefits of MAC Synchronization Best Practices for VSS

In virtual switch, frames need to be sent over the VSL to the other core to have MACs learnt in all the DFCs across both cores.

6.20.3 Features Incompatible with MAC Synchronization

None.

6.20.4 Guidelines and Restrictions for MAC Synchronization on VSS

Under high MAC address table utilization in a virtual switch, there are excessive MAC Notification's generated thereby increasing VSL utilization. It is therefore recommended to set the MAC address synchronization timer to 480 seconds.

6.20.5 Recommended Configuration for MAC Synchronization on VSS

```
!
mac-address-table synchronize activity-time 480
!
```

6.20.6 Configuration Guide for MAC Synchronization on VSS

See **mac-address-table synchronize** in the Command Reference for more information.

6.20.7 Related Features and Best Practices

None.

6.21 Best Practices for Multicast on VSS

These sections describe best practices for Multicast on VSS:

6.21.1 Description of Multicast on VSS

The majority of Multicast-related technologies operate the same on VSS, as they already do on non-VSS Catalyst 6500. This section attempts to highlight only the differences and / or additions, which are specific to the VSS architecture.

Because the “Virtual Switch” is comprised of two Catalyst 6500 chassis (VS Active & VS Standby), IPv4 Multicast forwarding support also needs to be extended to the VS Standby.

Both of the VS chassis are connected together by an inter-chassis Virtual Switch Link (VSL), which is shared by both internal control traffic and data traffic, between the two chassis. Multicast routing-protocols and software-switching operate only on the VS Active Route-Processor.

Hence, IGMP & PIM protocol packets received on the VS Standby chassis MUST be redirected to the VS Active chassis, via the VSL. This also applies to VS Standby SP & DFC Statistics, “Partial-Shortcuts” (e.g. Multicast NAT), as well as “Exception-Packets (e.g. non-RPF failures).

In addition, IGMP & PIM protocol packets are redirected to both the VS Active & Standby Switch-Processors, in order to provide IGMP & PIM snooping and L2 SSO capabilities.

6.21.2 Benefits of Multicast on VSS Best Practices

Multicast data forwarding is intended to distribute packets to multiple destinations, without the inefficiencies associated with broadcast and / or multiple (mesh) unicast forwarding designs.

However, the state-driven nature of Multicast coupled with poor network and / or configuration design, can actually lead to inefficient data forwarding, or even loss of data and other system resources.

This is particularly applicable to Catalyst 6500 VSS, because the overall number of modules, interfaces, and the related configuration and routing protocols, are potentially much higher than non-VSS designs.

Thus, utilizing Best Practices will help you to insure a consistent and stable behavior of Multicast data forwarding, when deployed on VSS.

6.21.3 Features Incompatible with Multicast on VSS

- Egress Local Replication
- IPv6 Multicast
- MLD/MLD Snooping

6.21.4 Guidelines and Restrictions for Multicast on VSS

Note All of the existing non-VSS Multicast Guidelines & Restrictions also apply to VSS.

Due to the (possible) large number of available modules and interfaces in VSS mode, the current guidelines & restrictions will apply:

- IPv4 mroute limit is < or = 30K
- IGMP joins (per second) < or = 3K
- PIM query (hello) interval > or = 10 seconds

Other then the general scalability guidelines listed above, Multicast on VSS should operate in the same way as it does on non-VSS Catalyst 6500 systems.

6.21.5 Recommended Multicast on VSS Configuration

Note All of the existing non-VSS Multicast Configurations also apply to VSS.

These sub-sections describe the recommended configuration for Multicast on VSS:

6.21.5.1 Platform Independent Multicast Configuration

All of the existing Platform Independent Multicast Configurations also apply to VSS.

6.21.5.2 Platform Dependent (non-VSS) Multicast Configuration

All of the existing Platform Dependent (non-VSS) Multicast Configurations also apply to VSS.

6.21.5.3 Multicast Replication Mode

Use the default Multicast replication mode.

Note The VSS architecture only supports WS-X6700 linecards, which are all egress-capable. Hence, the default replication mode will be “Egress”.

6.21.5.4 Multicast Redundancy (NSF/SSO)

Use the default Multicast NSF convergence timers.

Note This is especially applicable to Multicast on VSS, due to the potentially large number of modules, ports, and related adjacencies and traffic flows. Using more aggressive timers may result in loss of traffic and/or other system resources, until NSF/SSO is complete.

6.21.5.5 Multicast Timers

Note Millisecond (msec) PIM query-interval is not recommended in VSS mode.

If you have > 50 PIM neighbors, use the default (30 seconds) PIM query-interval.

If your topology has < 50 neighbors, use (non-default) > or = 10 second PIM query-interval.

Use the default IGMP related timers.

Use the default Multicast Flow Statistics Interval (1/4 every 25 seconds).

6.21.5.6 Multicast over MEC

Use the default Etherchannel load-balancing algorithm.

Note Avoid non-MEC (single-chassis attached) Multicast Source & Receiver connections. This design is supported, but will result in loss of traffic when the directly-connected chassis fails.

Wherever possible, you should utilize > or = 2 port Multi-chassis Ether-Channels (MECs) to connect to all of your PIM (or PIM Snooping) neighbors, L2 (IGMP Snooping-capable) switches, and LACP-capable Network Interface Cards (NICs).

This will provide additional bandwidth (via load-balancing), and will insure minimal Multicast traffic loss, during an individual link or module failure, and/or during SSO, without the need for unicast and/or spanning-tree re-convergence.

Refer to the MEC Best Practices documentation for additional information.

6.21.6 Configuration Guide for Multicast on VSS

Note There are no configuration differences for Multicast on VSS.

Refer to the following URLs for additional Multicast configuration information:

- http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti/config_library/12-2sx/imc-12-2sx-library.html
- http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/mcastv4.html
- http://www.cisco.com/en/US/tech/tk828/tech_white_papers_list.html

6.21.7 Related Features and Best Practices

4. Best Practices for Multicast

6.22 Best Practices for VSS QoS

These sections describe best practices for VSS QoS:

6.22.1 Description of Routing Protocol Prioritization traversing VSL

All routing protocol packets need to reach the Active RP to be processed. When the routing protocol packets ingress the Standby switch, they need to traverse the VSL links in order for them to reach the Active RP on the Active Switch.

If PFC QoS is enabled globally, all ports in the VSS will be set to untrusted, except for the VSL links which are always QoS enabled regardless of the global PFC QoS setting. This will cause routing protocol packets ingressing the VSS to lose their precedence marking.

Since the routing protocol packets are not marked, if the VSL links are oversubscribed, the routing protocol packets would not be prioritized while traversing the VSL links and could get dropped, this could cause routing protocol flaps.

This best practice includes recommendations that will keep the routing protocol packets from losing their markings when ingressing the Standby switch so they can be prioritized while traversing the VSL links.

6.22.2 Benefits of Routing Protocol Prioritization traversing VSL

By enabling Routing Protocol Prioritization, the routing protocol packets will be treated with higher priority while traversing the VSL links.

6.22.3 Features Incompatible with Routing Protocol Prioritization traversing VSL

None.

6.22.4 Guidelines and Restrictions for Routing Protocol Prioritization traversing VSL

- For the **mls qos protocol** *protocol_name* command to work, the ports where the routing adjacency is formed has to be untrusted or ignore port trust has to be enabled.
- Do not mark routing protocol packets with a precedence of 5.

6.22.5 Recommended Configuration for Routing Protocol Prioritization traversing VSL

- To mark the routing protocol packets ingressing the switch, issue the following command in global configuration mode:

```
!--- Precedence of 6 is recommended
Router(config)# mls qos protocol protocol_name precedence 6
```

Note For the above command to mark the packets, the port where the adjacency is formed has to be untrusted. If the port is trusted, then ignore port trust has to be enabled

- If the routing protocol packets ingressing the VSS are already marked and PFC QoS is enabled globally, then all that needs to be done is enable trust on the port where the routing adjacency is formed as follows:

```
Router(config-if)# mls qos trust ip-prec
```

Or:

```
Router(config-if)# mls qos trust dscp
```

6.22.6 Configuration Guide for QoS

See the "Configuring PFC QoS" chapter for more information about the commands shown.

6.22.7 Related Features and Best Practices

None.

6.23 Best Practices for Supervisor Engine 720-10G VSS for VSL

These sections describe best practices for Supervisor Engine 720-10G VSS for VSL:

6.23.1 Description of 10G-Only Mode for VSL

The 10 Gigabit Ethernet uplink ports on the Supervisor Engine 720-10G VSS can be used to form a VSL. By default, the queue structure of the three Gigabit Ethernet uplink ports & the two 10 Gigabit Ethernet uplink ports is 2q4t on receive and 1p3q4t on transmit, however, these queue structures can be optimized for the 10 Gigabit Ethernet uplink ports to an 8q4t queue structure on receive and 1p7q4t queue structure on transmit by enabling 10g-only mode.

6.23.2 Benefits of 10G-Only Mode for VSL

By enabling 10G-only mode, the queue structures of the 10 Gigabit Ethernet uplink ports on the Supervisor Engine 720-10G VSS are increased from 2q4t on receive and 1p3q4t on transmit to 8q4t on receive and 1p7q4t on transmit. A higher number queues implies a higher number of traffic classifications that can be treated differently. In other words, more options will exist for classifying important traffic to ensure that it is not dropped if the VSL links are oversubscribed.

The queue structures in 10G-only mode for the Supervisor Engine 720-10G VSS 10 Gigabit Ethernet uplink ports are exactly the same as the ports on the 8-port 10 Gigabit Ethernet line card (WS-X6708-10G-3C/XL).

6.23.3 Features Incompatible with 10G-Only Mode for VSL

IP-BFD dual-active detection cannot be configured on the Supervisor Engine 720-10G VSS Gigabit Ethernet uplink ports in 10G-only mode. IP-BFD dual-active detection is only supported on Gigabit Ethernet ports and the three Gigabit Ethernet uplink ports on the Supervisor Engine 720-10G VSS have to be shutdown to enable 10G-only mode.

6.23.4 Guidelines and Restrictions for 10G-Only Mode for VSL

To enable 10G-only mode, the Gigabit Ethernet uplink ports on the Supervisor Engine 720-10G VSS have to be shutdown.

6.23.5 Recommended 10G-Only Mode for VSL Configuration

- Before 10G-only mode is enabled:

```
Router# show mls qos | include 10g
  QoS 10g-only mode supported: Yes [Current mode: Off]
Router#
```

- This is the queue structure before 10G-only mode is enabled:

```
Router# show queueing interface t1/5/4 | include type
  Transmit queues [type = 1p3q4t]:
  Receive queues [type = 2q4t]:
Router#
```

- The Gigabit Ethernet uplinks need to be shutdown for 10G-only mode to be enabled:

```
Router(config)# mls qos 10g-only
Error: following ports have to be shut to enable 10g-only mode:
Gi1/5/1 Gi1/5/2 Gi1/5/3 Gi2/5/1 Gi2/5/2 Gi2/5/3

Command Rejected!

Router(config)# interface range g1/5/1-3 , g2/5/1-3
```

```
Router(config-if-range)# shutdown
Router(config-if-range)# exit
Router(config)# mls qos 10g-only
HWIF-QOS: Queuing qos cfg (wrr-queue/rcv-queue/priority-queue) will be reset to
default on Supervisor Switch 1 slot 5 interfaces!
HWIF-QOS: Queuing qos cfg (wrr-queue/rcv-queue/priority-queue) will be reset to
default on Supervisor Switch 2 slot 5 interfaces!
Router(config)# end
Router# show mls qos | include 10g
  QoS 10g-only mode supported: Yes [Current mode: On]
Router#
```

- This is the queue structure with 10G-only mode enabled:

```
Router# show queueing interface t1/5/4 | include type
Transmit queues [type = 1p7q4t]:
Receive queues [type = 8q4t]:
Router#
```

6.23.6 Configuration Guide for 10G-only mode for VSL

See the "Configuring PFC QoS" chapter for more information about the commands shown.

6.23.7 Related Features and Best Practices

None.

6.24 Best Practices for Layer 2 QoS on the VSS

These sections describe best practices for Layer 2 QoS on the VSS:

6.24.1 Description of Layer 2 QoS on the VSS

In a Cisco Virtual Switching System, application of QoS service policies (port-based QoS) on physical Layer 2 interfaces (switchport mode access and trunk) is prohibited. This is due to a limitation where only a limited number of interfaces can be indexed uniquely for QoS purposes. QoS service policies can only be applied on Layer 2 Cisco EtherChannel links or multichassis EtherChannel (MEC) and on Layer 3 interfaces (SVIs, physical interfaces, port channels, etc.).

If a policy needs to be set for physical layer 2 interfaces, since Port Based QoS is not supported, VLAN Based QoS can be used instead. All that is required is for ports to be marked indicating they are part of a VLAN QoS policy and to apply the policy on the SVI.

6.24.2 Benefits of VLAN Based QoS on the VSS

To overcome the Port-based QoS limitation on physical interfaces, VLAN Based QoS can be used instead.

6.24.3 Features Incompatible with VLAN Based QoS on the VSS

None.

6.24.4 Guidelines and Restrictions for Layer 2 QoS on the VSS

Port Based QoS is not supported in current software releases.

6.24.5 Recommended VLAN Based QoS Configuration on the VSS

mls qos vlan-based needs to be configured on all physical ports where the policy needs to be applied:

```
Router(config-if)# interface g1/3/1
Router(config-if)# switchport
Router(config-if)# mls qos vlan-based
Router(config-if)# exit
Router(config)# interface vlan 100
Router(config)# service-policy input test
```

Note VLAN Based QoS is enabled by default for all layer 2 physical interfaces in the standby VSS switch.

6.24.6 Configuration Guide for VLAN Based QoS

See the "Configuring PFC QoS" chapter for more information about the commands shown.

6.24.7 Related Features and Best Practices

None.

6.25 Best Practices for VSS Etherchannel Load Distribution

These sections describe best practices for VSS Etherchannel Load Distribution:

6.25.1 Description of VSS Etherchannel Load Distribution

When a member is added or removed from the EtherChannel bundle, the load register has to be reprogrammed for all the member ports, resulting in packet loss in a window of approximately 0.03 seconds. This reprogramming is done using the "fixed" load distribution algorithm.

Although the window of 0.03 seconds may seem small, it translates to a large loss on a high bandwidth 10GE port such as the Virtual Switch Link (VSL).

To alleviate this problem, the "adaptive" load distribution algorithm was formulated. This new algorithm allows this RBH reprogramming to be done exclusively on each port, and will result in lower packet loss during the port addition or removal.

6.25.2 Benefits of Adaptive Load Distribution Algorithm

The main benefit of this feature usage is lower packet loss on high bandwidth bundle interfaces, when the port-channel's member interfaces join or leave the bundle.

6.25.3 Features Incompatible with Adaptive Load Distribution Algorithm

None.

6.25.4 Guidelines and Restrictions for Adaptive Load Distribution Algorithm

None.

6.25.5 Recommended Configuration

- Configure the adaptive hash-distribution algorithm globally:

```
Router(config)# port-channel hash-distribution adaptive
```

- Configure the hash-distribution algorithm on port channel interfaces:

```
Router(config)# interface port-channel channel_number
Router(config-if)# port-channel port hash-distribution adaptive
```

6.25.6 Configuration Guide for VSS Etherchannel Load Distribution

Configuring Virtual Switching Systems

6.25.7 Related Features and Best Practices

None.

6.26 Best Practices for Etherchannel Min-Links in VSS

These sections describe best practices for Etherchannel Min-Links in VSS:

6.26.1 Description for EtherChannel Min-Links in VSS

LACP minlinks (minimum links) feature allows certain number of configurable ports within a port-channel bundle, thereby guaranteeing a fixed bandwidth. When the number of member ports in the EtherChannel fall below the configured value, the port-channel is deemed unusable, allowing traffic to use an alternate route, and hence guaranteeing bandwidth, if configured.

In Virtual Switch, this feature has been enhanced for Multi-chassis EtherChannel, where the “minimum links” requirement is enforced per chassis.

6.26.2 Benefits of Etherchannel Min-Links Best Practices

This feature in Virtual Switch allows traffic to egress a port-channel, in each chassis, with configurable guaranteed bandwidth.

It is recommended to have multiple member interfaces (2+) in each chassis for the selected EtherChannel bundle.

6.26.3 Features Incompatible with Etherchannel Min-Links

None.

6.26.4 Guidelines and Restrictions for Etherchannel Min-Links

This feature is restricted for EtherChannel bundles running LACP (802.1ad). It is not supported for EtherChannel bundles running PAgP.

Minimum configurable value for min-links is 2, hence a minimum of 2 links in each chassis are required for the MEC to remain effective.

Following examples illustrate the min-links feature:

- Interface configuration used:

```
interface Port-channel25
 no switchport
 port-channel min-links 2
end
```

- When the minimum link requirement in a port-channel is not met within a chassis (in the following case, it is chassis 1), the chassis-local ports in that EtherChannel will be put in (m) state, and will allow traffic to traverse the Virtual Switch Link as an alternate path to egress via the member ports of this port-channel on the peer chassis.

```
vip-vs1# show etherchannel 25 summary
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
        d - default port

        w - waiting to be aggregated
Number of channel-groups in use: 125
Number of aggregators:           125

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
25     Po25(RU)        LACP      Gi1/3/1(D)     Gi1/3/2(m)     Gi2/2/25(P)
                                 Gi2/2/26(P)

Last applied Hash Distribution Algorithm: Adaptive
```

- When the minimum link requirement is not met in both chassis, the port-channel will be fallged down and status will be denoted by either (SM) or (RM) as following:

```
vip-vs1# show etherchannel 25 summary
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
        d - default port

        w - waiting to be aggregated
Number of channel-groups in use: 125
Number of aggregators:           125

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
25     Po25(RM)        LACP      Gi1/3/1(D)     Gi1/3/2(D)     Gi2/2/25(D)
                                 Gi2/2/26(w)

Last applied Hash Distribution Algorithm: Adaptive
```

6.26.5 Recommended Etherchannel Min-Links Configuration

```
Router# configure terminal
Router(config)# interface gigabitethernet 1/3/1
Router(config-if)# channel-group 25 mode active
Router(config-if)# exit
Router(config)# interface gigabitethernet 1/3/2
Router(config-if)# channel-group 25 mode active
Router(config-if)# exit
Router(config)# interface gigabitethernet 2/2/25
Router(config-if)# channel-group 25 mode active
Router(config-if)# exit
Router(config)# interface gigabitethernet 2/2/26
Router(config-if)# channel-group 25 mode active
Router(config-if)# exit
Router(config)# interface port-channel 25
```

```
Router(config-if)# port-channel min-links 2
Router(config-if)# end
```

6.26.6 Configuration Guide for Etherchannel Min-Links

Configuring Virtual Switching Systems

6.26.7 Related Features and Best Practices

None.

6.27 Best Practices for LACP Port-Channel Port-Priority in VSS

These sections describe best practices for LACP Port-Channel Port-Priority in VSS:

6.27.1 Description of LACP Port-Channel Port-Priority in VSS

LACP port-priority feature allows LACP system manager switch to prioritize the port aggregation within a port-channel.

For Virtual Switch Systems, LACP port priority plays significant role in Multi-Chassis Etherchannel (MEC) as to which ports are added/removed or put in hot standby within the bundle.

6.27.2 Benefits of LACP Port-Channel Port-Priority in VSS

In VSS system, when multiple (2+) interfaces off Switch-ID 1 and Switch-ID 2 are aggregated in a MEC, it is recommended to configure the port priority in an interleaved fashion across Switch-id chassis.

6.27.3 Features Incompatible with LACP Port-Channel Port-Priority in VSS

None.

6.27.4 Guidelines and Restrictions for LACP Port-Channel Port-Priority in VSS

This feature is restricted for LACP (802.1ad) EtherChannel bundles.

It is recommended to set the LACP system priority on VSS to higher value than the connected peer, to allow the VSS to manage the aggregation of the ports in the EtherChannel bundle.

6.27.5 Recommended LACP Port-Channel Port-Priority in VSS

Following examples illustrate the recommendation for inter-leaving port-priority in MEC member interfaces when used along with LACP max-bundle feature.

- Port-channel configuration used:

```
interface Port-channel25
 no switchport
 lacp max-bundle 2
```

- Port-channel member interfaces configuration used:

```
interface GigabitEthernet1/3/1
 channel-group 25 mode active
 lacp port-priority 1
!
interface GigabitEthernet1/3/2
 channel-group 25 mode active
 lacp port-priority 3
!
interface GigabitEthernet2/2/25
 channel-group 25 mode active
 lacp port-priority 2
!
interface GigabitEthernet2/2/26
 channel-group 25 mode active
 lacp port-priority 4
end
```

- Show command:

```
Router# show etherchannel 25 summary
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
        d - default port

        w - waiting to be aggregated
Number of channel-groups in use: 125
Number of aggregators:           125

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
25     Po25(RU)        LACP      Gi1/3/1(P)     Gi1/3/2(H)     Gi2/2/25(P)
                                                   Gi2/2/26(H)

Last applied Hash Distribution Algorithm: Adaptive
```

Note In the above example, if LACP port-priority was not configured, default priority for the port-channel member interface, would allow only switch 1 member interfaces to be aggregated in the bundle, thus making the EtherChannel a non-MEC.

```
Router# configure terminal
```

```
Router(config)# lacp system-priority 32000
Router(config)# interface gigabitethernet 1/3/1
Router(config-if)# channel-group 25 mode active
Router(config-if)# lacp port-priority 1
Router(config-if)# exit
Router(config)# interface gigabitethernet 1/3/2
Router(config-if)# channel-group 25 mode active
Router(config-if)# lacp port-priority 3
Router(config-if)# exit
Router(config)# interface gigabitethernet 2/2/25
Router(config-if)# channel-group 25 mode active
Router(config-if)# lacp port-priority 2
Router(config-if)# exit
Router(config)# interface gigabitethernet 2/2/26
Router(config-if)# channel-group 25 mode active
Router(config-if)# lacp port-priority 4
Router(config-if)# exit
Router(config)# interface port-channel 25
Router(config-if)# lacp max-bundle 2
Router(config-if)# end
```

6.27.6 Configuration Guide for LACP Port-Channel Port-Priority in VSS

None.

6.27.7 Related Features and Best Practices

None.

6.28 Best Practices for VSS L3

These sections describe best practices for VSS L3:

6.28.1 Preference of MEC over FHRP protocols

The fundamental purpose of FHRP protocols like HSRP and VRRP is to provide first hop redundancy for the hosts. To which GLBP provides additional feature to load balance the traffic between the available redundant first hope links. Both the above features are taken care of by Multi-Ether channel Configuration between the hosts and VSS, as VSS setup provide the necessary Chassis level redundancy. Thus it is recommended instead of FHRP protocols, MEC be implemented wherever possible.

6.28.2 Benefits of MEC over FHRP protocols

The inherit characteristic of MEC provides the necessary redundancy for the hosts to forward the traffic.

FHRP protocols take a heavy toll on the CPU due to the periodic hello messages (Control Plane). Thus getting rid of FHRP protocols will reduce CPU usages.

6.28.3 Features Incompatible

None.

6.28.4 Guidelines and Restrictions

None.

6.28.5 Recommended Configuration

6.28.5.1 Routing Protocol Timers Configuration

Currently, IOS provides aggressive routing protocol timers to help network converged very fast under fault situation. However, it is counter-productive if a router has hardware redundancy built-in. The basic idea is that we do not want layer 3 protocols being too sensitive to hardware fault. We have a better fault handling mechanism in MEC.

Traffic interruption lasts only from the time upstream switch detect link down event until upstream switch select alternate ether-channel member. This interruption is much short than any routing protocol able to perform. Therefore, we recommend not changing routing protocol timers, and we would like to enable NSF on all routing protocols.

6.28.5.2 Benefits of Having Default Timer Configuration

Having a default timer setting would make the system more robust in responding to the changes in the topology.

Features Incompatible

None.

Guidelines and Restrictions

The neighboring devices should be NSF aware.

Recommended Configuration

To enable NSF on the routing protocol like OSPF following configuration is needed:

```
router ospf 6
  nsf
```

Configuration Guide

None.

6.28.5.3 L3 MEC Preference Between Distribution and Core Layer

When placing virtual switch in core layer, or when MEC linking to core switch, these MEC links should be configured as layer-3 port-channels. Although, we can use SVI and layer 2 MEC implementation. A layer-3 port-channel implementation enables routing protocols responding to link down events a lot faster. Here is the logic. If we use SVI and deploy OSPF. There are MEC link and some other links belonged to this SVI, when MEC goes down, however, this SVI being a virtual interface is still up because there is at least one link active. OSPF will re-converge only when dead timer expires. However, if we use layer-3 ether-channels, soon as the link goes down, link down event will trigger OSPF re-convergence.

On the other end, it is recommended when placing virtual switch in distribution layer, MEC linking to access switches are better setup as trunk ports and use SVIs to terminate VLANs. This way, a VLAN domain can spread multiple switches. Enable flexibility to topology changes.

Benefits of Best Practices

Having L3 MEC will have more quick and robust response to the change in the network topology.

Features Incompatible

None.

Guidelines and Restrictions

None.

Recommended Configuration

None.

Configuration Guide

None.

6.28.5.4 Routing Protocols Design on VSS

It is recommended to avoid routing protocol peering on a single routed port. As apart from the routing resiliency issues such a design encourages traffic flow through the VSL links which is not recommended. Also, it is not a good design to have routing protocol peering with both active and standby switch to achieve routing resiliency for the traffic. This is because in case of failure of one of the link, the time taken for the traffic to converge is equal to the convergence time for protocol. (That directly depends on hold-down time of dynamic routing protocol). If L3 MEC is used, the traffic convergence is instant. The other disadvantages are having multiple routing protocol neighbors means increase in control traffic thus increase in CPU utilization.

Benefits of have good Routing Protocol Design on VSS

Proper Routing protocol design have numerous benefits that helps in keeping check on CPU utilization, traffic flowing across the VSL link, convergence and predictable flow of traffic.

Features Incompatible

None.

Guidelines and Restrictions

None.

Recommended Configuration

None.

Configuration Guide

None.