Release Notes for Catalyst 6500 Series Content Switching Module Software Release 2.2(8)

Current Release—May 15, 2003
Previous Releases—2.2(7), 2.2(6), 2.2(5), 2.2(4), 2.2(3), 2.2(2), 2.1(4), 2.1(3), 2.1(2), 2.1(1), 1.2(2), 1.2(1), 1.1

This publication describes the features, modifications, and caveats for the Catalyst 6500 Series Content Switching Module (CSM) software release 2.2(8) running Cisco IOS Release 12.1(13)E3 or Catalyst operating system 7.5 or higher.

Note Except where specifically differentiated, the term “Catalyst 6500 series switches” includes both Catalyst 6500 series and Catalyst 6000 series switches.

Contents

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

System Requirements

This section describes the system requirements for the Catalyst 6500 Series CSM software release 2.2(7).

Memory Requirements

The Catalyst 6500 Series CSM memory is not configurable.

Hardware Supported

Before you can use the Catalyst 6500 Series CSM, you must have a Supervisor Engine 1A or a Supervisor Engine 2 with a Multilayer Switch Feature Card (MSFC1 or MSFC2), a Policy Feature Card (PFC), and any module with ports to connect server and client networks. The PFC is required for the VLAN access control list (VACL) capture functionality.

Caution The WS-X6066-SLB-APC module is not fabric enabled.

Product Number	Product Description	Minimum Software Version	Recommended Software Version	Recommended IOS Release	Recommended Catalyst OS Releases
Content Switching Module					
WS-X6066-SLB-APC with Supervisor Engine 2	Content Switching Module	1.2(1)	1.2(1)	12.1(8a)E	N/A
WS-X6066-SLB-APC with Supervisor Engine 1A or Supervisor Engine 2	Content Switching Module	2.1(1)	2.1(1)	12.1(8a)EX	N/A
WS-X6066-SLB-APC with Supervisor Engine 1A or Supervisor Engine 2	Content Switching Module	2.1(2)	2.1(2)	12.1(8a)EX	N/A
WS-X6066-SLB-APC with Supervisor Engine 1A or Supervisor Engine 2	Content Switching Module	2.1(3)	2.1(3)	12.1(8a)EX	N/A
WS-X6066-SLB-APC with Supervisor Engine 1A or Supervisor Engine 2	Content Switching Module	2.1(4)	2.1(4)	12.1(8a)EX	N/A
WS-X6066-SLB-APC with Supervisor Engine 1A or Supervisor Engine 2	Content Switching Module	2.2(1)	2.2(1)	12.1(11b)E	N/A

Product Number	Product Description	Minimum Software Version	Recommended Software Version	Recommended IOS Release	Recommended Catalyst OS Releases
WS-X6066-SLB-APC with Supervisor Engine 1A or Supervisor Engine 2	Content Switching Module	2.2(2)	2.2(2)	12.1(11b)E	N/A
WS-X6066-SLB-APC with Supervisor Engine 1A or Supervisor Engine 2	Content Switching Module	2.2(3)	2.2(3)	12.1(11b)E	N/A
WS-X6066-SLB-APC with Supervisor Engine 1A or Supervisor Engine 2	Content Switching Module	2.2(4)	2.2(4)	12.1(11b)E	N/A
WS-X6066-SLB-APC with Supervisor Engine 1A or Supervisor Engine 2	Content Switching Module	2.2(5)	2.2(5)	12.1(11b)E	N/A
WS-X6066-SLB-APC with Supervisor Engine 1A or Supervisor Engine 2	Content Switching Module	2.2(6)	2.2(6)	12.1(11b)E	N/A
WS-X6066-SLB-APC with Supervisor Engine 1A or Supervisor Engine 2	Content Switching Module	2.2(7)	2.2(7)	12.1(13)E3	7.5
WS-X6066-SLB-APC with Supervisor Engine 1A or Supervisor Engine 2	Content Switching Module	2.2(8)	2.2(8)	12.1(13)E3	7.5
Console Cable					
72-876-01	Console cable	Not applicable	Not applicable	Not applicable	Not applicable
Accessory Kit					
800-05097-01	Accessory kit (contains the console cable)	Not applicable	Not applicable	Not applicable	Not applicable

Software Compatibility

Software release 1.1(1) requires Cisco IOS Release 12.1(6)E or 12.1(7)E.

Software release 1.2(1) requires Cisco IOS Release 12.1(8a)E.

Software release 2.1(1) requires Cisco IOS Release 12.1(8a)EX or 12.1(11b)E. However, Cisco IOS Release 12.1(11b)E includes some Cisco IOS commands that refer to CSM 2.2 features that are not supported by a CSM 2.1 image.

Software release 2.1(2) and 2.1(2a) requires Cisco IOS Release 12.1(8a)EX.

Software release 2.1(3) and 2.13(a) requires Cisco IOS Release 12.1(8a)EX or 12.1(11b)E. However, Cisco IOS Release 12.1(11b)E includes some Cisco IOS commands that refer to CSM 2.2 features that are not supported by a CSM 2.1 image.

Software release 2.1(4) requires Cisco IOS Release 12.1(8a)EX or 12.1(11b)E. However, Cisco IOS Release 12.1(11b)E includes some Cisco IOS commands that refer to CSM 2.2 features that are not supported by a CSM 2.1 image.

Software release 2.2(1) requires Cisco IOS Release 12.1(8a)EX or higher. However, the features new to CSM Release 2.2(1) are only available with Cisco IOS Release 12.1(11b) E and subsequent releases.

Software release 2.2(2) and 2.2(b) requires Cisco IOS Release 12.1(8a)EX or higher. However, the features new to CSM Release 2.2(2) and 2.2(b) are only available with Cisco IOS Release 12.1(11b) E and subsequent releases

Software release 2.2(3) and 2.2(3a) requires Cisco IOS Release 12.1(8a)EX or higher. However, the features new to CSM Release 2.2(3) are only available with Cisco IOS Release 12.1(11b) E and subsequent releases.

Software release 2.2(4) requires Cisco IOS Release 12.1(8a)EX or higher. However, the features new to CSM Release 2.2(4) are only available with Cisco IOS Release 12.1(11b) E and subsequent releases.

Software release 2.2(5) requires Cisco IOS Release 12.1(8a)EX or higher. However, the features new to CSM Release 2.2(5) are only available with Cisco IOS Release 12.1(11b) E and subsequent releases.

Software release 2.2(6) requires Cisco IOS Release 12.1(8a)EX or higher. However, the features new to CSM Release 2.2(6) are only available with Cisco IOS Release 12.1(11b) E and subsequent releases.

Software release 2.2(7) requires Cisco IOS Release 12.1(8a)EX or higher. However, the features new to CSM Release 2.2(7) are only available with Cisco IOS Release 12.1(13) E3 and Catalyst operating system release 7.5 and subsequent releases.

Software release 2.2(8) requires Cisco IOS Release 12.1(8a)EX or higher. However, the features new to CSM Release 2.2(8) are only available with Cisco IOS Release 12.1(13) E3 and Catalyst operating system release 7.5 and subsequent releases.

Caution Only CSM software release 2.27 and higher can be used in a Catalyst 6500 Series switch with the Catalyst operating system release 7.5.

Software Releases and Orderable Product Number Matrix

Table 1 lists the software releases and applicable ordering information for the Catalyst 6500 series CSM module software.

Table 1 Software Release/Orderable Product Number Matrix

Software Release	Image Filename	Orderable Product Number	Orderable Product Number Spare
12.1(6)E or 12.1(7)E	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM	SC6K-2.1-CSM= SC6K-2.2-CSM=
12.1(8a)EX	c6kslb-apc.2-1-1.bin c6kslb-apc.2-1-2a.bin c6kslb-apc.2-1-3a.bin c6kslb-apc.2-2-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM	SC6K-2.1-CSM= SC6K-2.2-CSM=

Table 1 Software Release/Orderable Product Number Matrix (continued)

Software Release	Image Filename	Orderable Product Number	Orderable Product Number Spare
12.1(11b)E	c6kslb-apc.2-1-1.bin c6kslb-apc.2-1-3a.bin c6kslb-apc.2-1-4.bin c6kslb-apc.2-2-1.bin c6kslb-apc.2-2-2b.bin cc6kslb-apc.2-2-3a.bin c6kslb-apc.2-2-4.bin c6kslb-apc.2-2-5.bin c6kslb-apc.2-2-6.bin	SC6K-2.1-CSM SC6K-2.2-CSM	SC6K-2.1-CSM= SC6K-2.2-CSM=
12.1(13)E3	c6kslb-apc.2-1-1.bin c6kslb-apc.2-1-3a.bin c6kslb-apc.2-1-4.bin c6kslb-apc.2-2-1.bin c6kslb-apc.2-2-2b.bin cc6kslb-apc.2-2-3a.bin c6kslb-apc.2-2-4.bin c6kslb-apc.2-2-5.bin c6kslb-apc.2-2-6.bin c6kslb-apc.2-2-7.bin	SC6K-2.1-CSM SC6K-2.2-CSM	SC6K-2.1-CSM= SC6K-2.2-CSM=

Feature Set

Table 2 describes the CSM features and software descriptions.

Table 2 CSM Feature Set Description

Feature	Image Filename	Orderable Software Product Numbers
Supported Hardware		
Supervisor 1A with MSFC and PFC	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
Supervisor 2	c6slb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
Operating System		
Cisco IOS	All releases	SC6K-2.2-CSM
Catalyst Operating System	c6kslb-apc.2-2-7.bin	SC6K-2.2-CSM
Supported Protocols		
FTP	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
TCP load balancing	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
UDP & all common IP protocol load balancing	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM
Real Time Streaming Protocol (RTSP)	c6slb-apc.2-2-1.bin	SC6K-2.2-CSM
Layer 7 Functionality		
Full regular expression matching	c6slb-apc-1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
URL & cookie switching	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
Generic header parsing	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
Miscellaneous Functionality		
Multiple CSM in a chassis	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
CSM and IOS-SLB functioning simultaneously in a chassis	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
HTTP 1.1 persistence (all GETs balanced to the same server)	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
Full HTTP 1.1 persistence (GETs balanced to multiple servers)	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
Fully configurable NAT	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
Server initiated connections	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM

Table 2 CSM Feature Set Description (continued)

Feature	Image Filename	Orderable Software Product Numbers
Route health injection	c6slb-apc.1-1-1.bin (requires release 12.1(7)E c6slb-apc.1-2-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-2.1-CSM SC6K-2.2-CSM
Round-robin	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
Weighted round-robin (WRR)	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
Least connections	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
Weighted least connections	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
URL hashing	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
Source IP hashing	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
Destination IP hashing	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
Return error code checking	c6slb-apc.2-2-1.bin	SC6K-2.2-CSM
Increased number of VLANs	c6slb-apc.2-2-1.bin	SC6K-2.2-CSM
Reduced time between health probes	c6slb-apc.2-2-1.bin	SC6K-2.2-CSM
In-band health checking	c6slb-apc.2-2-1.bin	SC6K-2.2-CSM
Configurable pending connection timeout	c6slb-apc.2-2-1.bin	SC6K-2.2-CSM
Load Balancing Supported		
Server load balancing	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
Firewall load balancing	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
DNS load balancing	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
Stealth firewall load balancing	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
Transparent cache redirection	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
Reverse proxy cache	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
SSL off-loading	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
VPN-IPSec load balancing	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM

Table 2 CSM Feature Set Description (continued)

Feature	Image Filename	Orderable Software Product Numbers
Stickiness		
Cookie	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
SSL ID	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
Source IP	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
HTTP redirection	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
Redundancy		
Sticky state	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
Full stateful failover (connection redundancy)	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
Health Checking		
HTTP	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
ICMP	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
Telnet	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
TCP	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
SMTP	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
DNS	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM
Management		
SNMP traps	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM

New and Changed Information

- The CSM runs on Cisco IOS Release 12.1.(13)E3 and is supported by the Supervisor Engine 1A or Supervisor Engine 2 with an MSFC1 or MSFC2 and Catalyst operating system release 7.5.
- In the 2.2(7) release, the CSM now supports non-standard HTTP requests from the Wireless Application Protocol (WAP) devices.

- When receiving out-of-order UDP fragments, the CSM will bridge the packets to the appropriate peer VLAN in the bridging-mode.
- There is an enhancement to the predictor IP hash and cookie hash. The CSM will perform a secondary hash if the first hash value resolves in mapping to an out-of-service real server. This allows even distribution of connections. Previously, when a real server became out-of-service, all of its intended connections would go to the next real server in sequence.

Limitations and Restrictions

- The CSM does not support pipelines (multiple HTTP requests sharing the packet boundary) with the persistent rebalance feature.
- When configuring Route Health Injection (RHI), proxy ARP must be disabled on the Catalyst 6500 Series chassis (proxy-ARP is enabled by default). You must disable proxy ARP on a per-interface basis in the interface submode. We recommend that you disable proxy ARP on the VLAN level using the **no ip proxy arp** command.
- The meaning of having no minimum connections (MINCONNS) parameter set in the **real** submode is different between release 2.2(1) and later releases.

  Note Having the no MINCONNS parameter set is the default behavior.

  In all releases, when the MINCONNS value is set, once a real server has reached the maximum connections (MAXCONNS) state, no additional session is balanced to it until the number of open sessions to that real server falls below MINCONNS. With the no MINCONNS value set in release 1.1(1), no additional session would be balanced until the number of open sessions to that real server falls to 0.
- Slot 1 is reserved for the supervisor engine. Slot 2 can contain an additional redundant supervisor engine in case the supervisor engine in slot 1 fails. If a redundant supervisor engine is not required, you can insert the CSM in slots 2 through 6 on a 6-slot chassis, slots 2 through 9 on a 9-slot chassis, or slots 2 through 13 on a 13-slot chassis.
- The connection redundancy feature in 2.1(1) only backs up TCP connections from active to standby CSM. There is no support for connection redundancy of UDP and other non-TCP protocols.
- There is no support for client NAT of IP protocols other than TCP or UDP.
- If neither a real server nor a corresponding virtual server has an explicitly configured TCP/UDP port, then probes requiring such a port are not activated. All CSM health probes other than ICMP periodically create connections to specific TCP or UDP ports on configured real servers. If a health probe is configured on a real server without a configured TCP or UDP port, the CSM chooses the TCP or UDP port to probe from the virtual servers with which the real server is associated. If neither the real server nor the virtual server has a configured port, the CSM simply ignores any configured probes requiring ports to that real server.

- When configuring CSMs for fault tolerance, we recommend that you configure a dedicated link for the fault-tolerant VLAN.

Note Fault tolerance requires CSM release 1.2 or higher.

Note Configuring stateful redundancy with CSMs in separate chassis requires a gigabit link between the CSMs.

Caveats

These sections describe the following release caveats:

Open Caveats in Release 2.2(8)

This section describes known limitations that exist in CSM software release 2.2(8).

- CSCea02255

  The CSM processes the TCP connection, although the MAC address is not intended for that port. Occasionally, the switch floods a SYN (synchronize) packet to all bridge ports. In this case, the CSM incorrectly resets or load balances the unintended connection.

  Workaround: In most cases, the bridge device sends the destination MAC addresses to the correct port.

- CSCdz61644

  These restricted CSM port commands return the “failure” message instead of the “feature not supported” message: **set port cdp**, **set port trap**, **set spantree portpri**, and **set spantree link-type**.

  Workaround: None.

- CSCdz61386

  The last module in the chassis may not be shut down gracefully.

  Workaround: None.

- CSCdz53839

  The standby CSM incorrectly reports that it learned the address resolution protocol (ARP) address for a server or gateway on both sides of the bridging VLANs. The problem is caused by the external device, which overwrites the padding data in the ARP requests inserted by the CSM.

  Workaround: None.

- CSCdz50182

  Token Ring and FDDI VLANs should not be allowed on CSM trunk ports.

  Workaround: None.

- CSCdz12163

  The CSM drops packets because the multilayer switch (MLS) card and the multilayer switch feature card (MSFC) use different MAC addresses. This problem remains in software releases prior to the Catalyst 7.5.1 software release. If any Supervisor Engine 2 in the switch is still running a software release prior to the 7.5.1 software release and the traffic is forwarded by that switch, the CSM drops the packet.

  Workaround: None.

- CSCdy88197

  During a CSM reset, the **show module** command displays the module as faulty when it should be displayed as "Other."

  Workaround: None.

- CSCdy80501

  FTP virtual server IP addresses cannot also be client NAT IP addresses. If there is an overlap between the IP address range for a virtual server on which 'service ftp' is configured and a configured client NAT IP address range, connections through that virtual server are not handled properly.

  Workaround: Configure the FTP virtual server IP address and client NAT addresses to ensure that there is no address overlap.

- CSCdy79826

  When Internet Group Management Protocol (IGMP) snooping is enabled on the Catalyst 6500 series switch, some CSM connection replication frames may be dropped. When you use the CSM connection replication feature, you must disable IGMP snooping on both the active and standby CSM modules.

  Workaround: To disable IGMP snooping, use the **no ip igmp snooping** command in global configuration submode on the Catalyst 6500 series switch.

- CSCdy71303

  TCL script probes are sensitive to network overload, congestion, and delay.

  Workaround: To avoid spurious health monitoring results in which real servers are considered unhealthy due to network delay or congestion, we recommend that you set the "retry" value greater than 1 for all TCL script probes.

- CSCdy64647

  Established FTP connections are not replicated to the standby CSM when the standby becomes operational. To enable an FTP connection for replication from an active CSM to a standby CSM, the standby CSM must be operational at the time the FTP connection is opened. If the FTP connection is opened prior to the standby CSM booting and becoming operational, the FTP connection never replicates to the backup.

  Workaround: None.

- CSCdy32262

  For optimal performance of CSM TCL script probes and TCL standalone scripts, we recommend the following:

  a. Avoid using asynchronous sockets. For example, avoid calling the **socket** command with the **-async** option.

  b. Avoid calling the **gets** command. Use the **read** command instead.

  c. Avoid using the TCL **fileevent** command.

- CSCdy29182

  When multiple CSM users perform a **do copy xx running-config** from a CSM submode in Cisco IOS, the next command entered will fail with the message "% CSM parser state not found." This problem occurs only if the file copied to **running-config** contains at least one CSM command. When the CSM command in the file copied to **running-config** is run, it overwrites the current CSM configuration parser state.

  Workaround: Do not perform a **do copy xx running-config** operation from a CSM configuration submode. You can also exit out to the top level configuration submode and then re-enter the desired CSM configuration submode.

- CSCdy26940

  Beginning with Cisco IOS Release 12.1(13)E, it is possible for multiple users to simultaneously issue configuration commands for the same CSM. When you use this capability, it is possible to corrupt the configuration. In particular, if one user changes the "type" of an object while another user is simultaneously configuring that same object, the configuration will be corrupted. For example, if a user changes probe "FOO" from type "script" to type "http" while another is configuring probe "FOO," the configuration will be corrupted.

  Workaround: Ensure that multiple users do not simultaneously modify the CSM configuration in such an inconsistent way.

- CSCdy00143

  With Multiple Spanning Tree (MST) or Rapid PVST (RPVST) enabled, CSM failover time is excessive. When MST or RPVST is enabled and the spanning tree protocol is configured on a CSM client or server VLAN, it may take up to one minute for traffic flow through a CSM to resume after a CSM failover. The delay is caused by reconvergence of the Spanning Tree Protocol (STP).

  Workaround: Ensure that MST and RPVST are not enabled on the Catalyst 6500 series switch containing the CSM, or ensure that the spanning tree protocol is disabled on the CSM client and server VLANs.

- CSCdx73636

  Some FTP connections may not replicate. An FTP connection through an active CSM is not replicated if no data channel has been setup for the connection. Data channels are typically established when the client uses a **get** or **put** command on a file or performs a directory listing.

  Workaround: None.

- CSCdw84018

  CSM software release 3.1(2) does not support the Real Time Streaming Protocol (RTSP) and User Datagram Protocol (UDP) streaming when a client NAT is enabled. If this configuration is set up, the server attempts to open a UDP connection. Some RTSP clients then fall back to interleaved mode (inline TCP). This mode works in the application software, although the connection is sent to fastpath.

  Workaround: None

- CSCdw49073

  The CSM does not support creating more than 127 virtual servers with the same virtual IP (VIP) address, even though the CLI does allow you to configure more than 127 virtual servers. If you use the CLI to configure more than 127 virtual servers, the 128th and subsequent virtual servers will not function properly.

  Workaround: Do not configure more than 127 virtual servers on the same VIP.

- CSCdv29125

  In firewall configurations using an HTTP 1.1 redirect virtual server, a connection going through the firewalls may remain open after a redirect virtual server connection is established.

  Workaround: None. This connection closes when it times out.

- CSCdv11685

  You cannot configure different fault-tolerant pairs to use the same fault-tolerant VLAN.

  Workaround: Use a different fault-tolerant VLAN for each fault-tolerant CSM pair.

- CSCdv00464

  Issuing the **clear interface gigabit slot/port** command for a CSM gigabit port may not clear the counters.

  Workaround: None.

- CSCdu82478

  In the CSM, it is important that packets transmitted from the CSM toward a client (server) are transmitted on the same VLAN as packets received by the CSM from that same client (server). This constraint may be satisfied as follows:

  – Multiple routes on the CSM to the same destination are supported, but all such routes need to go through gateways on the same VLAN. Ensure that all routes to any particular destination go through the same VLAN. For example, the following configuration is invalid because it is possible for traffic from a remote source to arrive on both VLAN 10 and VLAN 20:

  ```
  Router(config)# module csm 4
  Router(config-module-csm)# vlan 10 client
  Router(config-slb-vlan-client)# gateway 1.1.1.1
  Router(config-module-csm)# vlan 20 client
  Router(config-slb-vlan-client)# gateway 2.2.2.2
  ```

  To make this configuration valid, delete the gateway command from either VLAN 10 or VLAN 20.

  Note NOTE: Do not use the **gateway** command in more than one VLAN.

  – Traffic into the CSM from an IP address must arrive on the same VLAN that the CSM uses to send to that IP address. Ensure that all traffic received by the CSM from a specific destination address arrives on the same VLAN that the CSM uses to reach that destination if the CSM is configured with a route as follows:

  ```
  Router(config)# module csm 4
  Router(config-module-csm)# vlan 10 client
  Router(config-slb-vlan-client)# route 10.0.0.0 255.255.255.0 gateway 1.1.1.1
  ```

  For load balancing to function properly, all traffic arriving from the 10.0.0.0/24 subnet must reach the CSM through VLAN 10.

- CSCdu57891

  The output from the **show interface gigabit slot/port** command may erroneously indicate that one or more of the CSM gigabit ports are down.

  Workaround: Disregard the display.

Resolved Caveats in Release 2.2(8)

This section describes caveats that have been resolved in CSM software release 2.2(8).

-
-
-

Open Caveats in Release 2.2(7)

This section describes known limitations that exist in CSM software release 2.2(7).

- CSCdz61644

  Some restricted CSM port commands return “failure” instead of “feature not supported.”

  Workaround: None

- CSCdz61386

  The last module in the chassis may not be shut down gracefully.

  Workaround: None

- CSCdz53839

  In certain network setups, the standby CSM incorrectly reports that it learned the ARP address for a server or gateway on both sides of the bridging VLANs. The problem is caused by the external device, which overwrites the padding data in the ARP requests inserted by the CSM.

  Workaround: None

- CSCdz50182

  Token Ring and FDDI VLANs should not be allowed on CSM trunk ports.

  Workaround: None

- CSCdz40545

  In a Hybrid Catalyst system, a switch running both Cisco IOS and the Catalyst operating system, the CSM stays as the active system if the MSFC was shut down and the switch processor is still running.

  Workaround: Manually shut down the CSM.

- CSCdz12163

  The CSM drops packets because MLS and the MSFC use different MAC addresses. This problem is still in pre Catalyst 7.5.1 software releases. If any Supervisor engine 2 in the switch is still running pre 7.5.1 software and the traffic is forwarded by that switch, the CSM drops the packet.

  Workaround: None

- CSCdy88197

  During reset of the CSM, **show module** command displays the module as faulty when it should be displayed as “Other.”

  Workaround: None

- CSCdw84018

Release 2.2(x) does not support RTSP UDP streaming when a client NAT is enabled. If this configuration is set up, the server attempts to open a UDP connection. Some RTSP clients then fall back on interleaved mode (inline TCP). This mode will work in the application software, although the connection is sent to fastpath.

Workaround: None

- CSCdw49073

  The CSM does not support creating more than 127 virtual servers with the same virtual IP (VIP) address, even though the CLI does allow you to configure more than 127 virtual servers. If you use the CLI to configure more than 127 virtual servers, the 128th and subsequent virtual servers will not function properly.

  Workaround: Do not configure more than 127 virtual servers on the same VIP.

- CSCdv00464

  Issuing the **clear interface gigabit slot/port** command for a CSM gigabit port may not clear the counters.

  Workaround: None.

- CSCdv11685

  You cannot configure different fault-tolerant pairs to use the same fault-tolerant VLAN.

  Workaround: Use a different fault-tolerant VLAN for each fault-tolerant CSM pair.

- CSCdv29125

  In firewall configurations using an HTTP 1.1 redirect virtual server, a connection going through the firewalls may remain open after a redirect virtual server connection is established.

  Workaround: None. This connection closes when it times out.

- CSCdu57891

  The output from the **show interface gigabit slot/port** command may erroneously indicate that one or more of the CSM gigabit ports are down.

  Workaround: Disregard the display.

- CSCdu82478

  In CSM software release 2.x, it is important that packets transmitted from the CSM toward a client (server) are transmitted on the same VLAN as packets received by the CSM from that same client (server). This constraint may be satisfied as follows:

  – Multiple routes on the CSM to the same destination are supported, but all such routes need to go through gateways on the same VLAN. Ensure that all routes to any particular destination go through the same VLAN. For example, the following configuration is invalid because it is possible for traffic from a remote source to arrive on both VLAN 10 and VLAN 20:

  ```
  Router(config)# module csm 4
  Router(config-module-csm)# vlan 10 client
  Router(config-slb-vlan-client)# gateway 1.1.1.1
  Router(config-module-csm)# vlan 20 client
  Router(config-slb-vlan-client)# gateway 2.2.2.2
  ```

  To make this configuration valid, delete the gateway command from either VLAN 10 or VLAN 20.

Note NOTE: Do not use the **gateway** command in more than one VLAN.

– Traffic into the CSM from an IP address must arrive on the same VLAN that the CSM uses to send to that IP address. Ensure that all traffic received by the CSM from a specific destination address arrives on the same VLAN that the CSM uses to reach that destination if the CSM is configured with a route as follows:

```
Router(config)# module csm 4
Router(config-module-csm)# vlan 10 client
Router(config-slb-vlan-client)# route 10.0.0.0 255.255.255.0 gateway 1.1.1.1
```

For load balancing to function properly, all traffic arriving from the 10.0.0.0/24 subnet must reach the CSM through VLAN 10.

Resolved Caveats in Release 2.2(7)

This section describes caveats that have been resolved in CSM software release 2.2(7).

- CSCdz48294

  When a VLAN interface is removed from the CSM configuration, the learned ARP entries associated with this subnet are still in the ARP table of CSM.

  Workaround: None.

- CSCdz47531

  In the 2.2(7) release, the CSM now supports non-standard HTTP requests from the Wireless Application Protocol (WAP) devices.

  Workaround: None.

- CSCdz38938

  When one of the firewalls fails ARP request, the ICMP health probe to other servers or firewalls will occasionally drop the ICMP reply. If the number of probe attempts is small, other ICMP health probes could incorrectly be marked as failed.

  Workaround: Increase the probe *retries* count, and increase the probe *failed* interval for ICMP.

- CSCdz35004

  The CSM receive engine was limiting the ICMP probe rate to 60 probes per second. With the fix in the 2.2(7) release, the maximum ICMP health probe rate is at 600 probes per second.

  Workaround: None.

- CSCdz34419

  When you configure a virtual server with a wildcard 0.0.0.0 address, and you use the **clear module csm** *id* **conns vserver** *vs-name* command, the command clears all current opened connections in the CSM.

  Workaround: None.

- CSCdz24949

  The **clear module csm** *x* **arp** command does not clear the learned ARP entries.

  Workaround: Any old learned ARP entries are removed in the next ARP probing cycle.

- CSCdy04751

  Sometimes the CSM cannot get the fault tolerance statistics from the hardware. In this case, the **show module csm** *x* **ft** command always returns an error. However, the fault tolerance function is still working.

Workaround: None.

Open Caveats in Release 2.2(6)

This section describes known limitations that exist in CSM software release 2.2(6).

- CSCdw84018

  Release 2.2(x) does not support RTSP UDP streaming when a client NAT is enabled. If this configuration is set up, the server attempts to open a UDP connection. Some RTSP clients then fall back on interleaved mode (inline TCP). This mode will work in the application software, although the connection is sent to fastpath.

  Workaround: None

- CSCdw49073

  The CSM does not support creating more than 127 virtual servers with the same virtual IP (VIP) address, even though the CLI does allow you to configure more than 127 virtual servers. If you use the CLI to configure more than 127 virtual servers, the 128th and subsequent virtual servers will not function properly.

  Workaround: Do not configure more than 127 virtual servers on the same VIP.

- CSCdv00464

  Issuing the **clear interface gigabit slot/port** command for a CSM gigabit port may not clear the counters.

  Workaround: None.

- CSCdv11685

  You cannot configure different fault-tolerant pairs to use the same fault-tolerant VLAN.

  Workaround: Use a different fault-tolerant VLAN for each fault-tolerant CSM pair.

- CSCdv29125

  In firewall configurations using an HTTP 1.1 redirect virtual server, a connection going through the firewalls may remain open after a redirect virtual server connection is established.

  Workaround: None. This connection closes when it times out.

- CSCdu57891

  The output from the **show interface gigabit slot/port** command may erroneously indicate that one or more of the CSM gigabit ports are down.

  Workaround: Disregard the display.

- CSCdu82478

  In CSM software release 2.x, it is important that packets transmitted from the CSM toward a client (server) are transmitted on the same VLAN as packets received by the CSM from that same client (server). This constraint may be satisfied as follows:

  – Multiple routes on the CSM to the same destination are supported, but all such routes need to go through gateways on the same VLAN. Ensure that all routes to any particular destination go through the same VLAN. For example, the following configuration is invalid because it is possible for traffic from a remote source to arrive on both VLAN 10 and VLAN 20:

  ```
  Router(config)# module csm 4
  Router(config-module-csm)# vlan 10 client
  Router(config-slb-vlan-client)# gateway 1.1.1.1
  ```

```
Router(config-module-csm)# vlan 20 client
Router(config-slb-vlan-client)# gateway 2.2.2.2
```

To make this configuration valid, delete the gateway command from either VLAN 10 or VLAN 20.

Note NOTE: Do not use the **gateway** command in more than one VLAN.

– Traffic into the CSM from an IP address must arrive on the same VLAN that the CSM uses to send to that IP address. Ensure that all traffic received by the CSM from a specific destination address arrives on the same VLAN that the CSM uses to reach that destination if the CSM is configured with a route as follows:

```
Router(config)# module csm 4
Router(config-module-csm)# vlan 10 client
Router(config-slb-vlan-client)# route 10.0.0.0 255.255.255.0 gateway 1.1.1.1
```

For load balancing to function properly, all traffic arriving from the 10.0.0.0/24 subnet must reach the CSM through VLAN 10.

Resolved Caveats in Release 2.2(6)

This section describes caveats that have been resolved in CSM software release 2.2(6).

- CSCdz25353

  The CSM drops the HSRP advertising traffic when the CSM should have been repeating them through the peer bridging VLAN.

  Workaround: None

- CSCdz17645

  The CSM drops the ICMP error message “Destination Unreachable with Type=3 and Code=3.”

  Workaround: None

- CSCdz0896

  The CSM does not match lowercase cookies in HTTP headers. Normally the Web browsers use the capital C when sending the Cookie HTTP header field. The CSM now supports the lower-case c for the cookie header because there are private applications using the lower-case form.

  Workaround: None.

- CSCdz03686

  If you configure the alias IP address for a VLAN first, before you configure the IP address for this VLAN, the VLAN IP address configuration fails. You should configure the IP address for the VLAN first.

  Workaround: Remove both the alias and the IP addresses. Then configure the IP address and the alias in the correct order.

- CSCdz02458

  The connections configured for cookie sticky sometimes were not replicated to the standby CSM.

  Workaround: None.

- CSCdy87767

  CSM TCP health probes are using an incorrect Maximum Segment Size (MSS) value of 1480. The correct default MSS option value should be 1460. Most of the servers ignore the high MSS value from the health probe messages.

  Workaround: None.

- CSCdy80475

  Connection replication does not work after removing and adding a fault-tolerant VLAN. After removing the fault-tolerant VLAN between two CSMs, both fault-tolerant modules become active as expected. When you reconfigure the fault-tolerant VLAN, one CSM becomes active and the other becomes the standby module. The active CSM will not replicate the connections to the standby module.

  Workaround: Reboot the standby CSM to resolve the problem.

- CSCdy76100

  Changing the redirect-vserver protocol through the SSL port command in some cases does not take effect. The redirect protocol (HTTP, HTTPS, FTP, etc.) would stay at the previously configured value.

  Workaround: Take the real server out of service, and then return it to in-service to force the CSM to take the new value.

- CSCdy71021

  When configuring the NAT client command for a serverfarm with the FTP service, the CSM stops forwarding the FTP traffic after 8000 connections are made. There is a resource leak in the CSM with the client NAT and FTP service.

  Workaround: None.

- CSCdy76748

  Under packet processing stress (high packet-per-second load), the NAT module on the CSM sends out a corrupted frame, which crashes the CSM resulting in a core dump and reboot.

  Workaround: None.

- CSCdy54047

  The CSM sends multiple GET requests of the same HTTP 1.1 persistent connection to the same server, even though this server has failed in between the GET requests. Thus, the subsequence GET will fail when the server fails.

  Workaround: None

- CSCdy44301

  The CSM is now generating the syslog and SNMP traps when taking the real server out of service. There is no syslog generated when putting the real server in service again.

  Workaround: None.

- CSCdy33708

  The CSM now supports client NAT with the FTP service in the “passive” mode.

  Workaround: Remove the client NAT option from the serverfarm.

Open Caveats in Release 2.2(5)

This section describes known limitations that exist in CSM software release 2.2(5).

- CSCdy33708

  A virtual server configured with the service FTP option does not work if the client NAT option is enabled for the serverfarm and the FTP mode is passive. The passive mode has the client initiating the data connection (port 20). This caveat has been fixed for the port mode.

  Workaround: If FTP passive mode is required, disable the client NAT option, otherwise allow only FTP port mode.

- CSCdw84018

  Release 2.2(x) does not support RTSP UDP streaming when a client NAT is enabled. If this configuration is set up, the server attempts to open a UDP connection. Some RTSP clients then fall back on interleaved mode (inline TCP). This mode will work in the application software, although the connection is sent to fastpath.

  Workaround: None

- CSCdw49073

  The CSM does not support creating more than 127 virtual servers with the same virtual IP (VIP) address, even though the CLI does allow you to configure more than 127 virtual servers. If you use the CLI to configure more than 127 virtual servers, the 128th and subsequent virtual servers will not function properly.

  Workaround: Do not configure more than 127 virtual servers on the same VIP.

- CSCdv00464

  Issuing the **clear interface gigabit slot/port** command for a CSM gigabit port may not clear the counters.

  Workaround: None.

- CSCdv11685

  You cannot configure different fault-tolerant pairs to use the same fault-tolerant VLAN.

  Workaround: Use a different fault-tolerant VLAN for each fault-tolerant CSM pair.

- CSCdv29125

  In firewall configurations using an HTTP 1.1 redirect virtual server, a connection going through the firewalls may remain open after a redirect virtual server connection is established.

  Workaround: None. This connection closes when it times out.

- CSCdu57891

  The output from the **show interface gigabit slot/port** command may erroneously indicate that one or more of the CSM gigabit ports are down.

  Workaround: Disregard the display.

- CSCdu82478

  In CSM software release 2.x, it is important that packets transmitted from the CSM toward a client (server) are transmitted on the same VLAN as packets received by the CSM from that same client (server). This constraint may be satisfied as follows:

– Multiple routes on the CSM to the same destination are supported, but all such routes need to go through gateways on the same VLAN. Ensure that all routes to any particular destination go through the same VLAN. For example, the following configuration is invalid because it is possible for traffic from a remote source to arrive on both VLAN 10 and VLAN 20:

```
Router(config)# module csm 4
Router(config-module-csm)# vlan 10 client
Router(config-slb-vlan-client)# gateway 1.1.1.1
Router(config-module-csm)# vlan 20 client
Router(config-slb-vlan-client)# gateway 2.2.2.2
```

To make this configuration valid, delete the gateway command from either VLAN 10 or VLAN 20.

Note NOTE: Do not use the **gateway** command in more than one VLAN.

– Traffic into the CSM from an IP address must arrive on the same VLAN that the CSM uses to send to that IP address. Ensure that all traffic received by the CSM from a specific destination address arrives on the same VLAN that the CSM uses to reach that destination if the CSM is configured with a route as follows:

```
Router(config)# module csm 4
Router(config-module-csm)# vlan 10 client
Router(config-slb-vlan-client)# route 10.0.0.0 255.255.255.0 gateway 1.1.1.1
```

For load balancing to function properly, all traffic arriving from the 10.0.0.0/24 subnet must reach the CSM through VLAN 10.

Resolved Caveats in Release 2.2(5)

This section describes caveats that have been resolved in CSM software release 2.2(5).

- CSCdy58105

  The web browser will send more data than is specified in the Content Length field of the HTTP request to the email site. If this traffic needs to be load-balanced through the CSM and if the persistent rebalance option is enabled, the CSM will drop these requests.

  Workaround: Disable the persistent rebalance option for virtual server.

- CSCdy57918

  The CSM leaks resources when an SYN and an RST are close to together in certain traffic patterns. This problem only occurs with Layer 4 load-balancing and only if the CSM receives an RST before it makes the load-balancing decision for that connection.

  Workaround: None

- CSCdy54018

  The service RTSP option for load-balancing streaming media traffic has memory leaks, causing the CSM to slowly run out of resources for the new RTSP flows. When resources are not available, the CSM will not load-balance any additional streaming media connections.

  Workaround: Use IP sticky to match the RTSP control and data flows instead of using the service RTSP option.

- CSCdy47910

  In CSM release 2.2(4), when you configure the **route** *subnet netmask* **gateway** *gateway-address* command, the *gateway-address* cannot be in the *specified subnet netmask*. You cannot configure a route which overlaps the VLAN subnet interface.

  Workaround: None

- CSCdy36736

  In previous releases, after the real server failed with the inband health check option, the removal of the inband health option would not enable the server. This problem is resolved so that when you remove the inband health option with the no health option the CSM immediately enables the server without waiting for the failed timer duration.

  Workaround: Configuring the real server with the no in-service option and then enabling it with the **inservice** command.

- CSCdy36605

  In some cases the CSM permanently disables a real server after that server fails the inband health check option. After a server fails, if the CSM sees a successful connection to the server before the failed timer expires, the server is disabled forever.

  Workaround: Configure the real server with the no in-service option, and enable it with the **inservice** command.

Open Caveats in Release 2.2(4)

This section describes known limitations that exist in CSM software release 2.2(4).

- CSCdw84018

  Release 2.2(x) does not support RTSP UDP streaming when a client NAT is enabled. If this configuration is set up, the server attempts to open a UDP connection. Some RTSP clients then fall back on interleaved mode (inline TCP). This mode will work in the application software, although the connection is sent to fastpath.

  Workaround: None

- CSCdw49073

  The CSM does not support creating more than 127 virtual servers with the same virtual IP (VIP) address, even though the CLI does allow you to configure more than 127 virtual servers. If you use the CLI to configure more than 127 virtual servers, the 128th and subsequent virtual servers will not function properly.

  Workaround: Do not configure more than 127 virtual servers on the same VIP.

- CSCdv00464

  Issuing the **clear interface gigabit slot/port** command for a CSM gigabit port may not clear the counters.

  Workaround: None.

- CSCdv11685

  You cannot configure different fault-tolerant pairs to use the same FT VLAN.

  Workaround: Use a different FT VLAN for each fault-tolerant CSM pair.

- CSCdv29125

  In firewall configurations using an HTTP 1.1 redirect virtual server, a connection going through the firewalls may remain open after a redirect virtual server connection is established.

  Workaround: None. This connection closes when it times out.

- CSCdu57891

  The output from the **show interface gigabit slot/port** command may erroneously indicate that one or more of the CSM gigabit ports are down.

  Workaround: Disregard the display.

- CSCdu82478

  In CSM software release 2.x, it is important that packets transmitted from the CSM toward a client (server) are transmitted on the same VLAN as packets received by the CSM from that same client (server). This constraint may be satisfied as follows:

  – Multiple routes on the CSM to the same destination are supported, but all such routes need to go through gateways on the same VLAN. Ensure that all routes to any particular destination go through the same VLAN. For example, the following configuration is invalid because it is possible for traffic from a remote source to arrive on both VLAN 10 and VLAN 20:

  ```
  Router(config)# module csm 4
  Router(config-module-csm)# vlan 10 client
  Router(config-slb-vlan-client)# gateway 1.1.1.1
  Router(config-module-csm)# vlan 20 client
  Router(config-slb-vlan-client)# gateway 2.2.2.2
  ```

  To make this configuration valid, delete the gateway command from either VLAN 10 or VLAN 20.

  

  Note NOTE: Do not use the **gateway** command in more than one VLAN.

  – Traffic into the CSM from an IP address must arrive on the same VLAN that the CSM uses to send to that IP address. Ensure that all traffic received by the CSM from a specific destination address arrives on the same VLAN that the CSM uses to reach that destination if the CSM is configured with a route as follows:

  ```
  Router(config)# module csm 4
  Router(config-module-csm)# vlan 10 client
  Router(config-slb-vlan-client)# route 10.0.0.0 255.255.255.0 gateway 1.1.1.1
  ```

  For load balancing to function properly, all traffic arriving from the 10.0.0.0/24 subnet must reach the CSM through VLAN 10.

Resolved Caveats in Release 2.2(4)

This section describes caveats that have been resolved in CSM software release 2.2(4).

- CSCdy22965

  When Layer 7 features are enabled, it is possible for the CSM to slowly leak Layer 7 session state objects. When the objects have been exhausted, the CSM suspends indefinitely. At that point, the CSM will not pass any traffic but remains responsive to the Cisco IOS configuration and show commands.

This problem occurs only when the CSM is receiving many Layer 7 connections in which the portion of the traffic to be parsed (typically either the HTTP headers or SSL *hello* messages) spans multiple packets, and those connections are terminated before the CSM has received all of the packets that require parsing.

For example, if a GET request spans two packets, and the connection is terminated after the CSM receives the first frame but before it receives the second, a Layer 7 connection object is leaked. Once all those objects are leaked, the CSM suspends indefinitely.

Workaround: None.

- CSCdy22697

  The CSM always drops all ISIS frames it receives. It is desirable that when configured in bridged mode, that the CSM pass ISIS frames from the client-side VLANs to the server-side VLANs and the reverse. This action allows ISIS communication through the CSM.

  Workaround: Prior to software release 2.2(4), the only work around was to not rely upon communication of ISIS frames through a CSM. This issue is resolved in CSM release 2.2(4).

- CSCdy19222

  There is a limit of two configured HSRP routers per CSM. Routes configured with the **route** or **gateway** command in the CSM VLAN submode may point to HSRP routers as the next-hop address. Because the CSM interoperates with HSRP, the set of all IP addresses configured as next-hops in **route** or **gateway** commands cannot contain more than two HSRP IP addresses. That is, a single CSM can interoperate with only two HSRP IP addresses at any given time.

  Workaround: Do not configure routes on the CSM to point to more than two distinct HSRP addresses.

- CSCdy09047

  A real server on which multiple health probes are configured will be considered healthy when one probe recovers, regardless of the state of other health probes on that server. This condition is undesirable, since one or more of these other probes may indicate that the server is still unhealthy. Instead, the real server should be considered healthy only when all probes on that server are successful.

  Workaround: None.

- CSCdy08254

  Configuring an HTTP probe with a Host header field may result in invalid HTTP requests in the keep-alive probe to the real servers. The CSM incorrectly overwrites the Host header field with the IP address of the real server. This condition may result in the CSM erroneously determining the health status of a real server.

  Workaround: Do not configure a Host header for an HTTP probe.

- CSCdy06917

  The replicated call-setup-retry-period-flag for the **show module csm** *x* **connection** command always displays false, even when the connection has been replicated to the peer CSM.

  Workaround: Disregard this display from previous releases.

- CSCdy06651

  It is not possible to configure an inband health probe to permanently disable a real server. When you configure the **health retries** *count* **failed** *seconds* command with a **failed** value of zero, the CSM should permanently disable the real server after it has first detected a failure. Instead, the CSM immediately re-enables the server for load balancing. This caveat occurs in CSM releases 2.2(1), 2.2(2a), and 2.2(3). It is fixed in release 2.2(4) and all other CSM versions.

  Workaround: Set the **failed** value to a very large number, for such as 100, instead of setting it to zero.

- CSCdx91813

  When you enable fail-action purge on a server farm, and a real server in that server farm goes down, it is possible for the CSM to suspend, continue to pass traffic on existing connections, and respond to most CLI commands. However, no new connections can be established through the device.

  When this caveat is triggered by a real server going down, and a pair of CSMs is running in fault tolerant mode, it is possible for the standby CSM to become active for seconds or minutes before it reverts once again to the standby state. At this point, the active CSM is not able to load balance connections. This caveat occurs in CSM releases 2.2(1), 2.2(2), and 2.2(3). It is fixed in release 2.2(4) and all other CSM versions.

  Workaround: Disable fail-action purge on all server farms. If disabling fail-action purge on all server farms is unacceptable for your configuration, you must upgrade to release 2.2.(4) or a subsequent release.

- CSCdx78343

  The connection is closed with a failure message upon receiving an RST from the client. When the client requests an HTTP connection, the CSM establishes the connection between the client and server. Then, if the client sends an RST, the CSM closes the connection and counts it as a failure by increasing the count on the **total conn failurs** counter. This counter shows the number of failed connections to a server. After the CSM makes a load-balancing decision, the number on the counter is increased only if the server resets the connection or the server does not respond to the sync request (SYN).

  Workaround: None

- CSCdx77012

  When you initiate an FTP session and reset the primary CSM with the **hw-module module 4 reset** command, the secondary CSM takes over that session properly. If that FTP session lasts until the primary CSM comes back online, and a *preempt as active* variable for that session still remains in the secondary CSM's connection table, as shown in the **sh ip slb conns** command, any of the following new sessions initiated will not be taken over by the secondary CSM when the primary CSM attempts the next reset. If the initial FTP closes before the primary CSM fault-tolerant state is initiated, this symptom does not occur.

  Workaround: None.

- CSCdx76713

  The alias IP address configuration is not removed when you enter the **no module csm** *x* or the **no vlan** *x* command. As a result, the CSM sends an error when the same alias IP address is configured again. This caveat occurs only in CSM release 2.2(3).

  Workaround: Remove the alias address using the command **no alias** *ip*.

Open Caveats in Release 2.2(3)

This section describes known limitations that exist in CSM software release 2.2(3).

- CSCdw84018

  Release 2.2(x) does not support RTSP UDP streaming when a client NAT is enabled. If this configuration is set up, the server attempts to open a UDP connection. Some RTSP clients then fall back on interleaved mode (inline TCP). This mode will work in the application software, although the connection is sent to fastpath.

  Workaround: None

- CSCdw49073

  The CSM does not support creating more than 127 virtual servers with the same virtual IP (VIP) address, even though the CLI does allow you to configure more than 127 virtual servers. If you use the CLI to configure more than 127 virtual servers, the 128th and subsequent virtual servers will not function properly.

  Workaround: Do not configure more than 127 virtual servers on the same VIP.

- CSCdv00464

  Issuing the **clear interface gigabit slot/port** command for a CSM gigabit port may not clear the counters.

  Workaround: None.

- CSCdv11685

  You cannot configure different fault-tolerant pairs to use the same FT VLAN.

  Workaround: Use a different FT VLAN for each fault-tolerant CSM pair.

- CSCdv29125

  In firewall configurations using an HTTP 1.1 redirect virtual server, a connection going through the firewalls may remain open after a redirect virtual server connection is established.

  Workaround: None. This connection closes when it times out.

- CSCdu57891

  The output from the **show interface gigabit slot/port** command may erroneously indicate that one or more of the CSM gigabit ports are down.

  Workaround: Ignore the display.

- CSCdu82478

  In CSM software release 2.x, it is important that packets transmitted from the CSM toward a client (server) are transmitted on the same VLAN as packets received by the CSM from that same client (server). This constraint may be satisfied as follows:

– Multiple routes on the CSM to the same destination are supported, but all such routes need to go through gateways on the same VLAN. Ensure that all routes to any particular destination go through the same VLAN. For example, the following configuration is invalid because it is possible for traffic from a remote source to arrive on both VLAN 10 and VLAN 20:

```
Router(config)# module csm 4
Router(config-module-csm)# vlan 10 client
Router(config-slb-vlan-client)# gateway 1.1.1.1
Router(config-module-csm)# vlan 20 client
Router(config-slb-vlan-client)# gateway 2.2.2.2
```

To make this configuration valid, delete the gateway command from either VLAN 10 or VLAN 20.

Note NOTE: Do not use the **gateway** command in more than one VLAN.

– Traffic into the CSM from an IP address must arrive on the same VLAN that the CSM uses to send to that IP address. Ensure that all traffic received by the CSM from a specific destination address arrives on the same VLAN that the CSM uses to reach that destination if the CSM is configured with a route as follows:

```
Router(config)# module csm 4
Router(config-module-csm)# vlan 10 client
Router(config-slb-vlan-client)# route 10.0.0.0 255.255.255.0 gateway 1.1.1.1
```

For load balancing to function properly, all traffic arriving from the 10.0.0.0/24 subnet must reach the CSM through VLAN 10.

Resolved Caveats in Release 2.2(3)

This section describes caveats that have been resolved in CSM software release 2.2(3).

- CSCdx78285

  Under heavy load, it is possible for the CSM to reject incoming connections in the mistaken belief that it is low on resources. If this issue occurs, then the line entitled *Pending event: Re-use too soon* in the output of the **show module csm <slot> tech proc 1** command will be increasing rapidly. This issue exists in CSM releases 1.x, 2.1(1), 2.1(2), 2.1(3), 2.2(1), and 2.2(2a).

  Workaround: None.

- CSCdx66816

  Active-active collisions are caused by a serverfarm probe failing. In a complex configuration or under heavy replication traffic, the CSM might exchange its fault tolerance states. This situation causes temporary blocking of the keep-alive fault tolerance messages. The problem is fixed in release 2.2(3).

  Workaround: For previous software releases in which this issue occurs, increase the failover time from 3 (the default) to 10 keep-alive messages using the **failover** command in the **ft** submode.

- CSCdx66674

  When the CSM receives a UDP frame with a 0 checksum on which a NAT operation is to be performed, the CSM will erroneously overwrite the checksum, causing a UDP frame with an incorrect checksum to be transmitted. This issue exists in CSM releases 2.1(1), 2.1(2), 2.1(3), 2.2(1), and 2.2(2a).

  Workaround: None.

Note This issue does not apply to UDP frames that the CSM simply repeats from one bridged VLAN to another with no NAT operation.

- CSCdx66661

  When the active CSM in a redundant pair is reset and the fault tolerance **preempt** option is enabled, it is possible for some traffic to be misdirected toward the standby CSM. This condition will persist until the standby CSM is reset. This issue exists in CSM releases 1.x, 2.1(1), 2.1(2), 2.1(3), 2.2(1), and 2.2(2a).

  Workaround: Reset the standby CSM or do not employ the fault tolerance **preempt** option.

  Note If the standby CSM is reset, application traffic will be handled by the active CSM and not experience disruption.

- CSCdx62207

  With certain patterns of FTP traffic passing through a CSM virtual server on which **service ftp** is enabled, there is some possibility that the CSM will fail. This issue exists in CSM releases 1.x, 2.1(1), 2.1(2), 2.1(3), 2.2(1), and 2.2(2a).

  Workaround: Disable **service ftp** on all virtual servers.

- CSCdx61301

  When a real server fails, the CSM does not purge ICMP flows initiated from that real server even when the **failaction purge** option is enabled. This issue is especially important when a firewall fails when the CSM is load balancing ICMP traffic, as ICMP flows may continue to be sent through the failed firewall for some time.

  Workaround: None. The flows through the failed firewall (or server) eventually time out.

- CSCdx51869

  When an active CSM receives an ARP request on one VLAN in a bridged VLAN pair, it should transmit that ARP frame onto the other VLAN in the pair. If the ARP request is for an IP address outside the subnet for which the CSM is configured, the CSM drops the ARP request. This situation may cause a problem when proxy ARP is employed across the two bridged VLANs. The CSM then may drop any proxy ARP request for an IP address not in its directly connected subnet. This severely limits the IP addresses to which hosts employing proxy ARP are able to communicate.

  This issue exists in CSM releases 2.1(1), 2.1(2), 2.1(3), 2.2(1), and 2.2(2a). It does not exist in any 1.x release.

  Workaround: Avoid using proxy ARP through bridged VLANs on the CSM.

- CSCdx44970

  The CSM is dropping packets generated by intermediate routers directed behind the CSM and generates the following error:

  ```
  ICMP Can't Fragment Error (type 3, code 4)
  ```

  This error is returned by a router that receives a packet too large for it to forward when the DF bit is set.

Note This error is only sent if the DF bit is set; otherwise, packets are just fragmented and passed through.

The packet is dropped and the ICMP error is sent back to the host where the packet originated. This action tells the originating host that it needs to reduce the size of its packets before they can be routed.

Recent system implementations also include the MTU of the next hop in the ICMP message so that the source knows how big its packets can be.

Workaround: Disable the path MTU discovery on the servers behind the CSM.

- CSCdx17864

  When Layer 7 features are enabled on the CSM, the CSM may drop the IP frames it receives if those frames contain multiple IP options. The following features require Layer 7 functionality: URL regular expression matching, cookie regular expression matching, cookie sticky, URL hash sticky, SSL ID sticky, and generic HTTP header parsing. This issue exists in the following CSM releases: 1.x, 2.1(1), 2.1(2), 2.1(3) 2.2(1), 2.2(2).

  Workaround: Multiple IP options are not common in networks, but you can disable the Layer 7 features if this issue causes a problem.

- CSCdx16168

  Due to internal optimizations that improve overall network throughput, the CSM must listen to the HSRP protocol signalling to properly learn the HSRP virtual MAC address that is shared between the active and standby HSRP routers.

  This problem occurs when the HSRP learning code in the CSM assumes that any given HSRP group appears on only one VLAN. If the same HSRP group appears on two different VLANs, the HSRP virtual MAC for the group is learned for only one of these VLANs.

  If the CSM does not properly learn the HSRP virtual MAC address, the following symptoms may occur:

  – Connections are dropped when coming from the HSRP router through the CSM.

  – The CSM sends frames to the physical MAC address on the active HSRP router, not the HSRP virtual MAC address.

  – If connection redundancy is enabled between two CSMs, connections may take an unusually long time to be replicated from the active to the standby CSM.

  Workaround: Change HSRP group numbers to be globally unique.

- CSCdw80718

  Configuring a large number of client VLANs (each configured with its own gateway) can cause the switch console to hang and the configuration performance to be extremely slow.

  Workaround: Limit the number of client-side gateways configured to a small number (less than 10).

Open Caveats in Release 2.2(2)

This section describes known limitations that exist in CSM software release 2.2(2).

- CSCdx17864

  When Layer 7 features are enabled on the CSM, the CSM may drop the IP frames it receives if those frames contain multiple IP options. The following features require Layer 7 functionality: URL regular expression matching, cookie regular expression matching, cookie sticky, URL hash sticky, SSL ID sticky, and generic HTTP header parsing. This issue exists in the following CSM releases: 1.x, 2.1(1), 2.1(2), 2.1(3) 2.2(1), 2.2(2).

  Workaround: Multiple IP options are not common in networks, but you can disable the Layer 7 features if this issue causes a problem.

- CSCdx16168

  Due to internal optimizations that improve overall network throughput, the CSM must listen to the HSRP protocol signalling to properly learn the HSRP virtual MAC address that is shared between the active and standby HSRP routers.

  The caveat is that the HSRP learning code in the CSM assumes that any given HSRP group appears on only one VLAN. If the same HSRP group appears on two different VLANs, the HSRP virtual MAC for the group is learned for only one of these VLANs.

  If the CSM does not properly learn the HSRP virtual MAC address, the following symptoms may occur:

  – Connections are dropped when coming from the HSRP router through the CSM.

  – The CSM sends frames to the physical MAC address on the active HSRP router, not the HSRP virtual MAC address.

  – If connection redundancy is enabled between two CSMs, connections may take an unusually long time to be replicated from the active to the standby CSM.

  Workaround: Change HSRP group numbers to be globally unique.

- CSCdx12809

  The CSM may fail when more than 3000 probes are configured and when there are probes of type ICMP, TCP, and HTTP configured simultaneously.

  Workaround: Reduce the number of probes, reduce the probe rate, or do not configure all three types of probes (TCP, ICMP, and HTTP) simultaneously.

  This issue exists in the following CSM releases: 1.x, 2.1(1), 2.1(2), 2.1(3), 2.2(1), and 2.2(2).

- CSCdw84018

  Release 2.2 does not support RTSP UDP streaming modes when a client NAT is enabled. If this configuration is set up, the server attempts to open a UDP connection, causing the CSM to drop packets. Some RTSP clients then fall back on interleaved mode (inline TCP) which will work in the application software, although the connection is sent to fastpath.

  Workaround: None

- CSCdw80718

  Configuring a large number of client VLANs (each configured with its own gateway) can cause the switch console to hang and the configuration performance to be extremely slow.

  Workaround: Limit the number of client-side gateways configured to a small number (less than 10).

- CSCdw49073

  The CSM does not support creating more than 127 virtual servers with the same virtual IP (VIP) address, even though the CLI does allow you to configure more than 127 virtual servers. If you use the CLI to configure more than 127 virtual servers, the 128th and subsequent virtual servers will not function properly.

  Workaround: Do not configure more than 127 virtual servers on the same VIP.

- CSCdv00464

  Issuing the **clear interface gigabit slot/port** command for a CSM gigabit port may not clear the counters.

  Workaround: None.

- CSCdv11685

  Do not configure different fault-tolerant pairs to use the same FT VLAN.

  Workaround: Use a different FT VLAN for each fault-tolerant CSM pair.

- CSCdv29125

  In firewall configurations using an HTTP 1.1 redirect virtual server, a connection going through the firewalls may remain open after a redirect virtual server connection is established.

  Workaround: None. This connection closes when it times out.

- CSCdu57891

  The output from the **show interface gigabit slot/port** command may erroneously indicate that one or more of the CSM gigabit ports are down.

  Workaround: Ignore the display.

- CSCdu82478

  In CSM software release 2.x, it is important that packets transmitted from the CSM toward a client (server) are transmitted on the same VLAN as packets received by the CSM from that same client (server). This constraint may be satisfied as follows:

  – Multiple routes on the CSM to the same destination are supported, but all such routes need to go through gateways on the same VLAN. Ensure that all routes to any particular destination go through the same VLAN. For example, the following configuration is invalid because it is possible for traffic from a remote source to arrive on both VLAN 10 and VLAN 20:

  ```
  Router(config)# module csm 4
  Router(config-module-csm)# vlan 10 client
  Router(config-slb-vlan-client)# gateway 1.1.1.1
  Router(config-module-csm)# vlan 20 client
  Router(config-slb-vlan-client)# gateway 2.2.2.2
  ```

  To make this configuration valid, delete the gateway command from either VLAN 10 or VLAN 20.

  Note NOTE: Do not use the **gateway** command in more than one VLAN.

  – Traffic into the CSM from an IP address must arrive on the same VLAN that the CSM uses to send to that IP address. Ensure that all traffic received by the CSM from a specific destination address arrives on the same VLAN that the CSM uses to reach that destination if the CSM is configured with a route as follows:

  ```
  Router(config)# module csm 4
  ```

```
Router(config-module-csm)# vlan 10 client
Router(config-slb-vlan-client)# route 10.0.0.0 255.255.255.0 gateway 1.1.1.1
```

For load balancing to function properly, all traffic arriving from the 10.0.0.0/24 subnet must reach the CSM through VLAN 10.

Resolved Caveats in Release 2.2(2)

This section describes caveats that have been resolved in CSM software release 2.2(2).

- CSCdx20633

  DNS probe functionality has changed slightly.

  – If an address has not been configured, then any non-error DNS response is considered healthy.

  – If addresses have been configured, the DNS server must respond definitively with one of the configured addresses to consider the server healthy.

- CSCdx16058

  The system fails when processing certain types of RTSP traffic.

- CSCdx16156

  The CSM does not forward to an HSRP router address without a gateway command. This issue exists in the following CSM releases: 1.x, 2.1(1), 2.1(2), 2.2(1). This caveat is fixed in all other CSM releases, such as 2.1(3) and 2.2(2).

  Due to some internal optimizations to improve overall network throughput, the CSM must listen to HSRP protocol signalling in order to properly learn the HSRP virtual MAC address, for example the HSRP MAC address shared between the active and standby HSRP routers.

  To allow the CSM to learn the HSRP virtual MAC address for an HSRP virtual router IP address, you must explicitly configure the HSRP virtual router IP address as a gateway in the VLAN submode under the **module csm** *mod_num* command. If you configure a route command pointing to the HSRP gateway, the CSM does not properly learn the HSRP information.

  If the CSM does not properly learn the HSRP virtual MAC address, the following symptoms may occur:

  – Connections coming from the HSRP router through the CSM are dropped.

  – The CSM sends frames to the physical MAC address on the active HSRP router, not the HSRP virtual MAC address.

  – Connections may take an unusually long time to be replicated from the active to the standby CSM if connection redundancy is enabled between two CSMs.

  Workaround: Configure the HSRP router using the **gateway** command, not the **route** command.

- CSCdx10302

  The system fails when more than 8K real servers are configured.

  Workaround: Do not configure more than 8K real servers.

- CSCdx08115

  Health probes can run on 32 VLAN interfaces only. The CSM 2.2(1) release supports 255 VLANs. However, when more than 32 VLANs are configured, the CSM VLAN interface IP addresses is not functional for the 33rd and subsequent VLANs. The CSM VLAN interface IP address is the IP address configured in the VLAN submode under **module csm** *slot*. By not being functional, the VLAN addresses will not respond to ICMP requests, nor will health probing functionality work through these interfaces. This problem occurs only in the 2.2(1) release.

  Workaround: Do not run health probes on more than 32 VLAN interfaces.

- CSCdx04521

  The system hangs during IP Option processing. When the CSM receives IP frames with more than ~5 IP options, it is possible that the device will fail.

  This issue exists in CSM releases 1.x, 2.1(1), 2.1(2), and 2.2(1). It is resolved in releases 2.1(3) and 2.2(2).

- CSCdw48046

  When using the destination IP address hash predictor, the CSM reassigns connections from a failed or out-of-service server to the next in-service server. In cases where multiple contiguous servers fail or are taken out-of-service, too many connections may be reassigned to the next in-service server. This condition causes performance problems with the next in-service server. In the worst case scenario, this condition may cause the next in-service server to fail, which in turn may cause the servers in the server farm to fail.

Open Caveats in Release 2.2(1)

This section describes known limitations that exist in CSM software release 2.2(1).

- CSCdw80718

  Configuring a large number of client VLANs (each configured with its own gateway) can cause the switch console to hang and the configuration performance to be extremely slow.

  Workaround: Limit the number of client-side gateways configured to a small number (less than 10).

- CSCdv00464

  Issuing the **clear interface gigabit slot/port** command for a CSM gigabit port may not clear the counters.

  Workaround: None.

- CSCdv11685

  Do not configure different fault-tolerant pairs to use the same FT VLAN.

  Workaround: Use a different FT VLAN for each fault-tolerant CSM pair.

- CSCdv29125

  In firewall configurations using an HTTP 1.1 redirect virtual server, a connection going through the firewalls may remain open after a redirect virtual server connection is established.

  Workaround: None. This connection closes when it times out.

- CSCdu57891

  The output from the **show interface gigabit slot/port** command may erroneously indicate that one or more of the CSM gigabit ports are down.

  Workaround: Ignore the display.

- CSCdu82478

  In CSM software release 2.x, it is important that packets transmitted from the CSM toward a client (server) are transmitted on the same VLAN as packets received by the CSM from that same client (server). This constraint may be satisfied as follows:

  – Multiple routes on the CSM to the same destination are supported, but all such routes need to go through gateways on the same VLAN. Ensure that all routes to any particular destination go through the same VLAN. For example, the following configuration is invalid because it is possible for traffic from a remote source to arrive on both VLAN 10 and VLAN 20:

  ```
  Router(config)# module csm 4
  Router(config-module-csm)# vlan 10 client
  Router(config-slb-vlan-client)# gateway 1.1.1.1
  Router(config-module-csm)# vlan 20 client
  Router(config-slb-vlan-client)# gateway 2.2.2.2
  ```

  To make this configuration valid, delete the gateway command from either VLAN 10 or VLAN 20.

  Note NOTE: Do not use the **gateway** command in more than one VLAN.

  – Traffic into the CSM from an IP address must arrive on the same VLAN the CSM uses to send to that IP address. Ensure that all traffic received by the CSM from a specific destination address arrives on the same VLAN that the CSM uses to reach that destination if the CSM is configured with a route as follows:

  ```
  Router(config)# module csm 4
  Router(config-module-csm)# vlan 10 client
  Router(config-slb-vlan-client)# route 10.0.0.0 255.255.255.0 gateway 1.1.1.1
  ```

  For load balancing to function properly, all traffic arriving from the 10.0.0.0/24 subnet must reach the CSM through VLAN 10.

Resolved Caveats in Release 2.2(1)

This section describes caveats that have been resolved in CSM software release 2.2(1).

- CSCdw84018

  Release 2.2 does not support RTSP UDP streaming modes when a client NAT is enabled. If this configuration is set up, the server attempts to open a UDP connection, causing the CSM to drop packets. Some RTSP clients then fall back on interleaved mode (inline TCP) even though the connection is sent to fastpath.

  Workaround: None

- CSCdw81611

  The CSM drops or corrupts UDP fragments. This issue was originally introduce in Release 2.1.1 and is resolved in Release 2.2.1. Both the drop and the corruption issues are located only in fragments other than the first fragment. In the affected fragments, the CSM is incorrectly interpreting the payload of the frame as UDP port information.

- CSCdw49073

  Configuring more than 128 VIPs with the same IP address can result in unpredictable balancing behavior. The CSM should restrict the user from configuring more than 128 VIPs with the same IP address.

  Workaround: Do not configure more than 127 virtual servers on the same VIP.

- CSCdu04990

  If the CSM parses a cookie to make a connection when the connection is closed, the connection will be listed as being current. If the client makes a connection again after the sticky timer expires, then one more connection goes into a closing state, thereby incrementing the counter by one.

  Workaround: None.

- CSCdu05559

  During heavy traffic conditions in a fault-tolerant configuration, the primary CSM may not be able to send heartbeat messages to the secondary CSM. This condition causes both the primary and secondary CSMs to become active, creating a bridge loop in the network.

  Workaround: Reboot the primary CSM.

- CSCdu33696

  When the CSM is balancing traffic and you configure the CSM with both a DFP agent and a manager, the following may occur:

  – All the counters in the **show ip slb stats** command are reset to 0.

  – The **show** command returns *No ICC Response* intermittently.

  – Unknown real servers with unknown bind IDs and weights appear.

  – Virtual servers send an RST to all connection requests.

  – CSM performance becomes very slow.

  Workaround: Do not configure both a DFP agent and a manager on the CSM when it is balancing traffic.

- CSCdu38154

  Under a heavy FTP connection load you may see warnings about FTP not finding associated sessions. These messages are benign.

  Workaround: None.

- CSCdu46347

  If you change the server farm VLAN IP address when the ICMP probe is configured, the ICMP probe still uses the old IP address instead of the new one. Changing the server farm with ICMP causes probes to fail and eventually brings the virtual server out of service.

  Workaround: Delete the ICMP probe from the server farm configuration, change the VLAN IP address, and then add the ICMP probe back to the server farm configuration.

Note Multiple server farms may be associated with a VLAN IP address. To determine which server farms are associated with a VLAN IP address, issue the **show ip slb real** command, examine the display, identify the real servers that are in the same network as the VLAN IP address, and note the server farm associations of those real servers.

- CSCdu54735

  If the version of software running on the CSM does not correspond to the version of Cisco IOS software running on the Catalyst switch, a spurious memory access message may be displayed when the CSM is inserted into a Catalyst 6500 Series chassis.

  Workaround: If the versions of software do not correspond, either the Cisco IOS or the CSM software must be upgraded for the module to function.

- CSCdv73302

  When serverfarms for the CSM have been configured with health probes and no real servers at the time the module comes online, the probe configuration for the serverfarm is never sent to the module, even when the real servers are later added to the serverfarm.

  Workaround: Configure real servers before configuring probes in ip slb serverfarm submode.

- CSCdv78416

  When using the **no ip slb map** command (or **no map** in the module CSM submode) in Cisco IOS software for the CSM, the memory allocated for match rules is not deallocated. This condition is not usually a problem since the amount of memory required is small.

  Additionally, calling the **no url-map**, **no cookie-map**, or **no header-map** command from SLB policy submode can cause the specified map to be associated with the policy, rather than disassociated, if the policy is not currently associated with a map of that type.

  Workaround: Do not call the command for a policy that is not configured with a map of the given type.

- CSCdw09585

  When two CSMs are configured as a redundant pair and reside in the same chassis, the **advertise active** and **advertise always** commands may fail to advertise routes to the associated VIP after a failover has occurred. When the currently active CSM fails, advertised routes are correctly removed from the route table, but these routes are not reinserted once the standby CSM becomes active. If the active and standby CSMs reside in two different chassis, the **advertise** commands work properly when a failover occurs.

- CSCdw47284

  Client access lists for the CSM are specified in one of two ways:

  – If the list is assigned directly to the virtual server using the **client** command in the vserver submode, the client mask will be changed to 255.255.255.255 during a configuration reload, which occurs when the configuration is first sent to the module on startup.

  – When using the **clear ip slb linecard-config** command.

  You can determine that the mask has been changed by comparing the virtual server output for the **show running** command with the output from the **show ip slb vserver detail** command.

  Workaround: Create a Cisco IOS standard IP access list, assign it to an slb policy, and assign the policy to the virtual server.

Open Caveats in Release 2.1(4)

This section describes known limitations that exist in CSM software release 2.1(4).

- CSCdu82478

  In the CSM software release 2.x, it is important that packets transmitted from the CSM toward a client (server) are transmitted on the same VLAN as packets received by the CSM from that same client (server). This constraint may be satisfied as follows:

  – Multiple routes on the CSM to the same destination are supported, but all such routes need to go through gateways on the same VLAN. Ensure that all routes to any particular destination go through the same VLAN. For example, the following configuration is invalid because it is possible for traffic from a remote source to arrive on both VLAN 10 and VLAN 20:

  ```
  Router(config)# module csm 4
  Router(config-module-csm)# vlan 10 client
  Router(config-slb-vlan-client)# gateway 1.1.1.1
  Router(config-module-csm)# vlan 20 client
  Router(config-slb-vlan-client)# gateway 2.2.2.2
  ```

  To make this configuration valid, delete the gateway command from either VLAN 10 or VLAN 20.

  Note NOTE: Do not use the **gateway** command in more than one VLAN.

  – Traffic into the CSM from an IP address must arrive on the same VLAN that the CSM uses to send traffic to that IP address. Ensure that all traffic received by the CSM from a specific destination address arrives on the same VLAN that the CSM uses to reach that destination if the CSM is configured with a route as follows:

  ```
  Router(config)# module csm 4
  Router(config-module-csm)# vlan 10 client
  Router(config-slb-vlan-client)# route 10.0.0.0 255.255.255.0 gateway 1.1.1.1
  ```

  For load balancing to function properly, all traffic arriving from the 10.0.0.0/24 subnet must reach the CSM through VLAN 10.

- CSCdv00464

  Issuing the **clear interface gigabit slot/port** command for a CSM gigabit port may not clear the counters.

  Workaround: None.

- CSCdv11685

  Do not configure different fault-tolerant pairs to use the same FT VLAN.

  Workaround: Use a different FT VLAN for each fault-tolerant CSM pair.

- CSCdv29125

  In firewall configurations using an HTTP 1.1 redirect virtual server, a connection going through the firewalls may remain open after a redirect virtual server connection is established.

  Workaround: None. This connection closes when it times out.

- CSCdw49073

  The CSM does not support creating more than 127 virtual servers with the same virtual IP (VIP) address, even though the CLI does enable you to configure more than 127 virtual servers. If you use the CLI to configure more than 127 virtual servers, the 128th and subsequent virtual servers will not function properly.

  Workaround: Do not configure more than 127 virtual servers on the same VIP.

- CSCdy09047

  A real server on which multiple health probes are configured will be considered to be healthy when one probe recovers, regardless of the state of other health probes on that server. This is undesirable, since one or more of these other probes may indicate that the server is still unhealthy. Instead, the real server should be considered healthy only when all probes on that server are successful.

  Workaround: None.

- CSCdy19222

  There is a limit of two configured HSRP routers per CSM. Routes configured with the **route** or **gateway** command in the CSM VLAN submode may point to HSRP routers as the next-hop address. Because the CSM interoperates with HSRP, the set of all IP addresses configured as next-hops in **route** or **gateway** commands cannot contain more than two HSRP IP addresses. That is, a single CSM can interoperate with only two HSRP IP addresses at any given time.

  Workaround: Do not configure routes on the CSM to point to more than two distinct HSRP addresses.

Resolved Caveats in Software Release 2.1(4)

This section describes caveats that have been resolved in CSM software release 2.1(4).

- CSCdx16168

  Due to internal optimizations that improve overall network throughput, the CSM must listen to the HSRP protocol signalling to properly learn the HSRP virtual MAC address that is shared between the active and standby HSRP routers.

  The caveat is that the HSRP learning code in the CSM assumes that any given HSRP group appears on only one VLAN. If the same HSRP group appears on two different VLANs, the HSRP virtual MAC for the group is learned for only one of these VLANs.

  If the CSM does not properly learn the HSRP virtual MAC address, the following symptoms may occur:

  – Connections are dropped when coming from the HSRP router through the CSM.

  – The CSM sends frames to the active HSRP router's physical MAC address, not the HSRP virtual MAC address.

  – If connection redundancy is enabled between two CSMs, connections may take an unusually long time to be replicated from the active to the standby CSM.

  Workaround: Change HSRP group numbers to be globally unique.

- CSCdx44970

  The CSM is dropping packets generated by intermediate routers directed behind the CSM and generates the following error:

  ```
  ICMP Can't Fragment Error (type 3, code 4)
  ```

This error is returned by a router that receives a packet too large for it to forward when the DF bit is set.

Note This error is sent only if the DF bit is set; otherwise, packets are just fragmented and passed through.

The packet is dropped and the ICMP error is sent back to the host where the packet originated. This action tells the originating host that it needs to reduce the size of its packets before they can be routed.

Recent system implementations also include the MTU of the next hop in the ICMP message so that the source knows how big its packets can be.

Workaround: Disable the path MTU discovery on the servers behind the CSM.

- CSCdx51869

  When an active CSM receives an ARP request on one VLAN in a bridged VLAN pair, it should transmit that ARP frame onto the other VLAN in the pair. If the ARP request is for an IP address outside the subnet for which the CSM is configured, the CSM drops the ARP request. This situation may cause a problem when proxy ARP is employed across the two bridged VLANs. The CSM then may drop any proxy ARP request for an IP address not in its directly connected subnet. This severely limits the IP addresses to which hosts employing proxy ARP are able to communicate.

  This issue exists in CSM releases 2.1(1), 2.1(2), 2.1(3), 2.2(1), and 2.2(2a). It does not exist in any 1.x release.

  Workaround: Avoid using proxy ARP through bridged VLANs on the CSM.

- CSCdx62207

  With certain patterns of FTP traffic passing through a CSM virtual server on which **service ftp** is enabled, there is some possibility that the CSM will fail. This issue exists in CSM releases 1.x, 2.1(1), 2.1(2), 2.1(3), 2.2(1), and 2.2(2a).

  Workaround: Disable **service ftp** on all virtual servers.

- CSCdx66661

  When the active CSM in a redundant pair is reset and the fault tolerance **preempt** option is enabled, it is possible for some traffic to be misdirected toward the standby CSM. This condition will persist until the standby CSM is reset. This issue exists in CSM releases 1.x, 2.1(1), 2.1(2), 2.1(3), 2.2(1), and 2.2(2a).

  Workaround: Reset the standby CSM or do not employ the fault tolerance **preempt** option.

  Note If the standby CSM is reset, application traffic will be handled by the active CSM and not experience disruption.

- CSCdx66674

  When the CSM receives a UDP frame with a 0 checksum on which a NAT operation is to be performed, the CSM will erroneously overwrite the checksum, causing a UDP frame with an incorrect checksum to be transmitted. This issue exists in CSM releases 2.1(1), 2.1(2), 2.1(3), 2.2(1), and 2.2(2a).

  Workaround: None.

- CSCdx78285

  Under heavy load, it is possible for the CSM to reject incoming connections in the mistaken belief that it is low on resources. If this issue occurs, you will notice a rapid increase in the values displayed in the line entitled *Pending event: Re-use too soon* in the output of the **show module csm <slot> tech proc 1** command. This issue exists in CSM releases 1.x, 2.1(1), 2.1(2), 2.1(3), 2.2(1), and 2.2(2a).

  Workaround: None.

- CSCdx78343

  When receiving a TCP RST (reset from the client side), the CSM incorrectly counts a connection to a real server as having failed. Clients may send RSTs even though no failure of any form has occurred. This count displays in the output of the **show module csm** *slot* **stat** and **show module csm** *slot* **real detail** commands.

  Workaround: When interpreting these statistics in prior releases, be aware that the statistics for connections that are reset by the client are displayed as failed and are counted incorrectly.

- CSCdx17864

  When Layer 7 features are enabled on the CSM, the CSM may drop the IP frames it receives if those frames contain multiple IP options. The following features require Layer 7 functionality: URL regular expression matching, cookie regular expression matching, cookie sticky, URL hash sticky, SSL ID sticky, and generic HTTP header parsing. This issue exists in the following CSM releases: 1.x, 2.1(1), 2.1(2), 2.1(3) 2.2(1), 2.2(2).

  Workaround: Multiple IP options are not common in networks, but you can disable the Layer 7 features if this issue causes a problem.

- CSCdv59690

  Using the **set ip dscp** command in the policy submode, the CSM may be configured to stamp the DSCP value in load balanced frames. The CSM does not correctly stamp such frames when the value configured using this command is greater than 15. As a result, the IP checksum for such packets is incorrect, and these packets are dropped in the network.

  Workaround: Do not configure a policy with a DSCP value of 16 or above.

- CSCdy06917

  The replicated call setup retry period flag for the **show module csm** *x* **connection** command always displays false, even when the connection has actually been replicated to the peer CSM.

  Workaround: Ignore this display from previous releases.

Open Caveats in Release 2.1(3)

This section describes known limitations that exist in CSM software release 2.1(3).

- CSCdu57891

  The output from the **show interface gigabit slot/port** command may erroneously indicate that one or more of the CSM gigabit ports are down.

  Workaround: Ignore the display.

- CSCdu82478

  In the CSM software release 2.x, it is important that packets transmitted from the CSM toward a client (server) are transmitted on the same VLAN as packets received by the CSM from that same client (server). This constraint may be satisfied as follows:

– Multiple routes on the CSM to the same destination are supported, but all such routes need to go through gateways on the same VLAN. Ensure that all routes to any particular destination go through the same VLAN. For example, the following configuration is invalid because it is possible for traffic from a remote source to arrive on both VLAN 10 and VLAN 20:

```
Router(config)# module csm 4
Router(config-module-csm)# vlan 10 client
Router(config-slb-vlan-client)# gateway 1.1.1.1
Router(config-module-csm)# vlan 20 client
Router(config-slb-vlan-client)# gateway 2.2.2.2
```

To make this configuration valid, delete the gateway command from either VLAN 10 or VLAN 20.

Note NOTE: Do not use the **gateway** command in more than one VLAN.

– Traffic into the CSM from an IP address must arrive on the same VLAN the CSM uses to send to that IP address. Ensure that all traffic received by the CSM from a specific destination address arrives on the same VLAN that the CSM uses to reach that destination if the CSM is configured with a route as follows:

```
Router(config)# module csm 4
Router(config-module-csm)# vlan 10 client
Router(config-slb-vlan-client)# route 10.0.0.0 255.255.255.0 gateway 1.1.1.1
```

For load balancing to function properly, all traffic arriving from the 10.0.0.0/24 subnet must reach the CSM through VLAN 10.

- CSCdv00464

  Issuing the **clear interface gigabit slot/port** command for a CSM gigabit port may not clear the counters.

  Workaround: None.

- CSCdv11685

  Do not configure different fault-tolerant pairs to use the same FT VLAN.

  Workaround: Use a different FT VLAN for each fault-tolerant CSM pair.

- CSCdv29125

  In firewall configurations using an HTTP 1.1 redirect virtual server, a connection going through the firewalls may remain open after a redirect virtual server connection is established.

  Workaround: None. This connection closes when it times out.

- CSCdw49073

  The CSM does not support creating more than 127 virtual servers with the same virtual IP (VIP) address, even though the CLI does enable you to configure more than 127 virtual servers. If you use the CLI to configure more than 127 virtual servers, the 128th and subsequent virtual servers will not function properly.

  Workaround: Do not configure more than 127 virtual servers on the same VIP.

- CSCdw80718

  Configuring a large number of client VLANs (each configured with its own gateway) can cause the switch console to hang and the configuration performance to be extremely slow.

  Workaround: Limit the number of client-side gateways configured to a small number (less than 10).

- CSCdx17864

  When Layer 7 features are enabled on the CSM, the CSM may drop the IP frames it receives if those frames contain multiple IP options. The following features require Layer 7 functionality: URL regular expression matching, cookie regular expression matching, cookie sticky, URL hash sticky, SSL ID sticky, and generic HTTP header parsing. This issue exists in the following CSM releases: 1.x, 2.1(1), 2.1(2), 2.1(3) 2.2(1), 2.2(2).

  Workaround: Multiple IP options are not common in networks, but you can disable the Layer 7 features if this issue causes a problem.

- CSCdx16168

  Due to internal optimizations that improve overall network throughput, the CSM must listen to the HSRP protocol signalling to properly learn the HSRP virtual MAC address that is shared between the active and standby HSRP routers.

  The caveat is that the HSRP learning code in the CSM assumes that any given HSRP group appears on only one VLAN. If the same HSRP group appears on two different VLANs, the HSRP virtual MAC for the group is learned for only one of these VLANs.

  If the CSM does not properly learn the HSRP virtual MAC address, the following symptoms may occur:

  – Connections are dropped when coming from the HSRP router through the CSM.

  – The CSM sends frames to the active HSRP router's physical MAC address, not the HSRP virtual MAC address.

  – If connection redundancy is enabled between two CSMs, connections may take an unusually long time to be replicated from the active to the standby CSM.

  Workaround: Change HSRP group numbers to be globally unique.

Resolved Caveats in Software Release 2.1(3)

This section describes caveats that have been resolved in CSM software release 2.1(3).

- CSCdw41620

  The CSM may classify incoming frames incorrectly, causing those frames to be dropped. Such packet loss results in intermittent connectivity to virtual servers configured on the CSM. This problem occurs only if 128 or more virtual servers have been configured on the device since bootup. (This number includes virtual servers that have been configured and subsequently removed from the configuration.) In most production scenarios, virtual servers are configured only when the device boots.

  This defect is present in CSM software releases 1.1(1), 1.2(1), 2.1(1), 2.1(2). This defect is fixed in version 1.2(1).

- CSCdw47545

  DNS probes are always failing, thus taking the servers out of service. The CSM considers the probe reply to be an incorrect reply, even when the returned IP address matches the configured expected IP address.

- CSCdw48046

  When using the destination IP address hash predictor, the CSM reassigns connections from a failed or out-of-service server to the next in-service server. In cases where multiple contiguous servers fail or are taken out-of-service, too many connections may be reassigned to the next in-service server.

This condition causes performance problems with the next in-service server. In the worst case scenario, this condition may cause the next in-service server to fail, which in turn may cause the servers in the server farm to fail.

- CSCdw81611

  The CSM drops or corrupts UDP fragments. This issue was originally introduced in Release 2.1.1 and is resolved in Release 2.2.1. Both the drop and the corruption issues are located only in fragments other than the first fragment. In the affected fragments, the CSM is incorrectly interpreting the payload of the frame as UDP port information.

- CSCdx04521

  The system hangs during IP Option processing. When the CSM receives IP frames with more than ~5 IP options, it is possible that the device will fail.

  This issue exists in CSM releases 1.x, 2.1(1), 2.1(2), and 2.2(1). It is resolved in releases 2.1(3) and 2.2(2).

- CSCdx16156

  The CSM does not forward to an HSRP router address without a gateway command. This issue exists in the following CSM releases: 1.x, 2.1(1), 2.1(2), 2.2(1). This caveat is fixed in all other CSM releases, such as 2.1(3) and 2.2(2).

  Due to some internal optimizations to improve overall network throughput, the CSM must listen to HSRP protocol signalling in order to properly learn the HSRP virtual MAC address, for example the HSRP MAC address shared between the active and standby HSRP routers.

  To allow the CSM to learn the HSRP virtual MAC address for an HSRP virtual router IP address, you must explicitly configure the HSRP virtual router IP address as a gateway in the VLAN submode under the **module csm** *mod_num* command. If you configure a route command pointing to the HSRP gateway, the CSM does not properly learn the HSRP information.

  If the CSM does not properly learn the HSRP virtual MAC address, the following symptoms may occur:

  – Connections coming from the HSRP router through the CSM are dropped.

  – The CSM sends frames to the physical MAC address on the active HSRP router, not the HSRP virtual MAC address.

  – Connections may take an unusually long time to be replicated from the active to the standby CSM if connection redundancy is enabled between two CSMs.

  Workaround: Configure the HSRP router using the **gateway** command, not the **route** command.

- CSCdx20633

  DNS probe functionality has changed slightly.

  – If an address has not been configured, then any non-error DNS response is considered healthy.

  – If addresses have been configured, the DNS server must respond definitively with one of the configured addresses to consider the server healthy.

Open Caveats in Software Release 2.1(2)

This section describes known limitations that exist in CSM software release 2.1(2).

- CSCdu57891

  The output from the **show interface gigabit slot/port** command may erroneously indicate that one or more of the CSM gigabit ports are down.

  Workaround: Ignore the display.

- CSCdu82478

  In the Content Switching Module (CSM) software release 2.1.1, it is important that packets transmitted from the CSM toward a client (server) are transmitted on the same VLAN as packets received by the CSM from that same client (server). This constraint may be satisfied as follows:

  – Ensure that all routes to any particular destination go through the same VLAN. Multiple routes on the CSM to the same destination are supported, but all such routes need to go through gateways on the same VLAN. For example, the following configuration is invalid because it is possible for traffic from a remote source to arrive on both VLAN 10 and VLAN 20:

  ```
  Router(config)# module csm 4
  Router(config-module-csm)# vlan 10 client
  Router(config-slb-vlan-client)# gateway 1.1.1.1
  Router(config-module-csm)# vlan 20 client
  Router(config-slb-vlan-client)# gateway 2.2.2.2
  ```

  To make this a valid configuration, delete the gateway command from either VLAN 10 or VLAN 20.

  Note NOTE: Do not use the **gateway** command in more than one VLAN

  – Ensure that all traffic received by the CSM from a specific destination address arrives on the same VLAN as the route the CSM uses to reach that destination. If the CSM is configured with a route as follows, for load balancing to function properly, all traffic arriving from the 10.0.0.0/24 subnet must reach the CSM through VLAN 10.

  ```
  Router(config)# module csm 4
  Router(config-module-csm)# vlan 10 client
  Router(config-slb-vlan-client)# route 10.0.0.0 255.255.255.0 gateway 1.1.1.1
  ```

- .CSCdv00464

  Issuing the **clear interface gigabit slot/port** command for a CSM gigabit port may not clear the counters.

  Workaround: None.

- CSCdv11685

  Do not configure different fault-tolerant pairs to use the same FT VLAN.

  Workaround: Use a different FT VLAN for each fault-tolerant CSM pair.

- CSCdv29125

  In firewall configurations using an HTTP 1.1 redirect virtual server, a connection going through the firewalls may remain open after a redirect virtual server connection is established.

  Workaround: None. This connection closes when it times out.

Resolved Caveats in Software Release 2.1(2)

This section describes caveats that have been resolved in CSM software release 2.1(2).

- CSCdw05136

  In CSM software release prior to 2.1(1), IP fragments are not supported and are dropped. In software release 2.1(1) of the CSM code, a simple form of support for handling UDP fragments was added. There is a defect in the code handling UDP fragments in 2.1(1). When a CSM running software release 2.1(1) receives UDP fragments, the system may exhibit very substantial performance degradation and instability, possibly resulting in the CSM crashing. This defect is fixed in CSM software release 2.1(2).

  Workaround: When running software release 2.1(1) ensure the CSM does not receive UDP fragments.

- CSCdw09396

  In CSM software release 2.1(1), when the CSM examines HTTP headers that cross multiple packets, it is possible that some connections will hang indefinitely. This defect is fixed in CSM software version 2.1(2).

- CSCdw09585

  When two CSMs are configured as a redundant pair and reside in the same Catalyst 6500 Series chassis, the **advertise active** and **advertise always** commands may fail to advertise routes to the associated VIP after a failover has occurred. When the currently active CSM fails, advertised routes are correctly removed from the route table, but these routes are not re-inserted once the standby CSM becomes active. If the active and standby CSMs reside in two different chassis, the **advertise** commands work properly when a failover occurs. This defect is fixed in version 2.1(2) of the CSM software.

- CSCdw16020

  When POST requests are sent by a client through a Layer 7 virtual server with persistent rebalance enabled, the connection may hang. This is particularly true for large amounts of data in the POST request.

  Workaround: Do the following for this defect:

  – Ensure that no POST requests are sent to virtual servers with resistant rebalance enabled.

  – Ensure that POST requests with small amounts of data (<200 bytes) are sent to virtual servers with persistent rebalance enabled.

  – Turn off persistent rebalance on virtual servers that are enabled for layer 7 analysis and that receive POST requests with large amounts of data.

  This defect is fixed in CSM software release 2.1(2).

- CSCdw24071

  In CSM software version 2.1(1) or earlier, the CSM may crash if it receives a TCP RST frame on a connection at an inappropriate time. In particular, this condition may be triggered if an RST arrives immediately following a valid data frame on the same connection. This condition can occur infrequently and can be prevalent when there are many packet drops or errors in the network due to congested or defective servers or overloaded transmission links. This defect is fixed in CSM software release 2.1(2).

- CSCdw24384

  In a configuration in which connections arrive at a CSM through a redundant router pair running HSRP, it is possible that connections arrive from the standby HSRP peer. When returning traffic back through that redundant router pair, the CSM must send the traffic to the HSRP virtual MAC address shared by the two routers. In CSM software releases 1.2(1) and 2.1(1), the CSM incorrectly forwards such traffic to the real MAC address of the standby router. This defect is fixed in CSM software release 2.1(2).

Open Caveats in Release 2.1(1)

This section describes known limitations that exist in CSM software release 2.1(1).

- CSCdu57891

  The output from the **show interface gigabit slot/port** command may erroneously indicate that one or more of the CSM gigabit ports are down.

  Workaround: Ignore the display.

- CSCdu82478

  In the CSM software release 2.x, it is important that packets transmitted from the CSM toward a client (server) are transmitted on the same VLAN as packets received by the CSM from that same client (server). This constraint may be satisfied as follows:

  – Multiple routes on the CSM to the same destination are supported, but all such routes need to go through gateways on the same VLAN. Ensure that all routes to any particular destination go through the same VLAN.

    For example, the following configuration is invalid because it is possible for traffic from a remote source to arrive on both VLAN 10 and VLAN 20:

    ```
    Router(config)# module csm 4
    Router(config-module-csm)# vlan 10 client
    Router(config-slb-vlan-client)# gateway 1.1.1.1
    Router(config-module-csm)# vlan 20 client
    Router(config-slb-vlan-client)# gateway 2.2.2.2
    ```

    To make this configuration valid, delete the gateway command from either VLAN 10 or VLAN 20.

    Note NOTE: Do not use the **gateway** command in more than one VLAN.

  – Traffic into the CSM from an IP address must arrive on the same VLAN the CSM uses to send to that IP address. Ensure that all traffic received by the CSM from a specific destination address arrives on the same VLAN that the CSM uses to reach that destination if the CSM is configured with a route as follows:

    ```
    Router(config)# module csm 4
    Router(config-module-csm)# vlan 10 client
    Router(config-slb-vlan-client)# route 10.0.0.0 255.255.255.0 gateway 1.1.1.1
    ```

    For load balancing to function properly, all traffic arriving from the 10.0.0.0/24 subnet must reach the CSM through VLAN 10.

- CSCdv00464

  Issuing the **clear interface gigabit slot/port** command for a CSM gigabit port may not clear the counters.

  Workaround: None.

- CSCdv11685

  Do not configure different fault-tolerant pairs to use the same FT VLAN.

  Workaround: Use a different FT VLAN for each fault-tolerant CSM pair.

- CSCdv29125

  In firewall configurations using an HTTP 1.1 redirect virtual server, a connection going through the firewalls may remain open after a redirect virtual server connection is established.

  Workaround: None. This connection closes when it times out.

- CSCdv73302

  When serverfarms for the CSM have been configured with health probes and no real servers at the time the module comes online, the probe configuration for the serverfarm is never sent to the module, even when the real servers are later added to the serverfarm.

  Workaround: Configure real servers before configuring probes in ip slb serverfarm submode.

- CSCdv78416

  When using the **no ip slb map** command (or **no map** in the module CSM submode) in Cisco IOS software for the CSM, the memory allocated for match rules is not deallocated. This condition is not usually a problem since the amount of memory required is small.

  Additionally, calling the **no url-map**, **no cookie-map**, or **no header-map** command from SLB policy submode can cause the specified map to be associated with the policy, rather than disassociated, if the policy is not currently associated with a map of that type.

  Workaround: Do not call the command for a policy that is not configured with a map of the given type.

- CSCdw09585

  When two CSMs are configured as a redundant pair and reside in the same chassis, the **advertise active** and **advertise always** commands may fail to advertise routes to the associated VIP after a failover has occurred. When the currently active CSM fails, advertised routes are correctly removed from the route table, but these routes are not reinserted once the standby CSM becomes active. If the active and standby CSMs reside in two different chassis, the **advertise** commands work properly when a failover occurs.

- CSCdw47284

  Client access lists for the CSM are specified in one of two ways:

  – If the list is assigned directly to the virtual server using the **client** command in the vserver submode, the client mask will be changed to 255.255.255.255 during a configuration reload, which occurs when the configuration is first sent to the module on startup.

  – When using the **clear ip slb linecard-config** command.

  You can determine that the mask has been changed by comparing the virtual server output for the **show running** command with the output from the **show ip slb vserver detail** command.

  Workaround: Create a Cisco IOS standard IP access list, assign it to an slb policy, and assign the policy to the virtual server.

Resolved Caveats in Software Release 2.1(1)

This section describes caveats that have been resolved in CSM software release 2.1(1).

- CSCdu04990

  If the CSM parses a cookie to make a connection when the connection is closed, the connection will be listed as being current. If the client makes a connection again after the sticky timer expires, then one more connection goes into a closing state, thereby incrementing the counter by one.

  Workaround: None.

- CSCdu05559

  During heavy traffic conditions in a fault-tolerant configuration, the primary CSM may not be able to send heartbeat messages to the secondary CSM. This condition causes both the primary and secondary CSMs to become active, creating a bridge loop in the network.

  Workaround: Reboot the primary CSM.

- CSCdu33696

  While the CSM is balancing traffic and you configure the CSM with both a DFP agent and a manager, the following may occur:

  – All the counters in the **show ip slb stats** command are reset to 0.

  – The **show** command returns *No ICC Response* intermittently.

  – Unknown real servers with unknown bind IDs and weights show up.

  – Virtual servers send an RST to all connection requests.

  – CSM performance becomes very slow.

  Workaround: Do not configure both a DFP agent and a manager on the CSM while it is balancing traffic.

- CSCdu38154

  Under a heavy FTP connection load you may see warnings about FTP not finding associated sessions. These messages are benign.

  Workaround: None.

- CSCdu46347

  If you change the server farm VLAN IP address while the ICMP probe is configured, the ICMP probe still uses the old IP address instead of the new one. Changing the server farm with ICMP causes probes to fail and eventually brings the virtual server out of service.

  Workaround: Delete the ICMP probe from the server farm configuration, change the VLAN IP address, and then add the ICMP probe back to the server farm configuration.

Note Multiple server farms may be associated with a VLAN IP address. To determine which server farms are associated with a VLAN IP address, issue the **show ip slb real** command, examine the display, identify the real servers that are in the same network as the VLAN IP address, and note the server farm associations of those real servers.

- CSCdu54735

  If the version of software running on the CSM does not correspond to the version of Cisco IOS software running on the Catalyst switch, a spurious memory access message may be displayed when the CSM is inserted into a Catalyst 6500 Series chassis.

  Workaround: If the versions of software do not correspond, either the Cisco IOS or the CSM software must be upgraded for the module to function.

Open Caveats in Release 1.2(2)

This section describes known limitations that exist in the CSM software release 1.2(2).

- CSCdw47284

  Client access lists for the CSM are specified in one of two ways:

  – If the list is assigned directly to the virtual server using the **client** command in the vserver submode, the client mask will be changed to 255.255.255.255 during a configuration reload, which occurs when the configuration is first sent to the module on startup.

  – When using the **clear ip slb linecard-config** command.

  You can determine that the mask has been changed by comparing the virtual server output for the **show running** command with the output from the **show ip slb vserver detail** command.

  Workaround: Create a Cisco IOS standard IP access list, assign it to an slb policy, and assign the policy to the virtual server.

- CSCdv78416

  When using the **no ip slb map** command (or **no map** in the module CSM submode) in Cisco IOS software for the CSM, the memory allocated for match rules is not deallocated. This condition is not usually a problem since the amount of memory required is small. Additionally, calling the **no url-map**, **no cookie-map**, or **no header-map** command from SLB policy submode can cause the specified map to be associated with the policy, rather than disassociated, if the policy is not currently associated with a map of that type.

  Workaround: Do not call the command for a policy that is not configured with a map of the given type.

- CSCdv73302

  When serverfarms for the CSM have been configured with health probes and no real servers at the time the module comes online, the probe configuration for the serverfarm is never sent to the module, even when the real servers are later added to the serverfarm.

  Workaround: Configure real servers before configuring probes in ip slb serverfarm submode.

- CSCdu04990

  If the CSM parses a cookie to make a connection when the connection is closed, the connection will be listed as being current. If the client makes a connection again after the sticky timer expires, then one more connection goes into a closing state, thereby incrementing the counter by one.

  Workaround: None.

- CSCdu05559

  During heavy traffic conditions in a fault-tolerant configuration, the primary CSM may not be able to send heartbeat messages to the secondary CSM. This condition causes both the primary and secondary CSMs to become active, creating a bridge loop in the network.

  Workaround: Reboot the primary CSM.

- CSCdu33696

  While the CSM is balancing traffic and you configure the CSM with both a DFP agent and a manager, the following may occur:

  – All the counters in the **show ip slb stats** command are reset to 0.

  – The **show** command returns *No ICC Response* intermittently.

  – Unknown real servers with unknown bind IDs and weights show up.

  – Virtual servers send an RST to all connection requests.

  – CSM performance becomes very slow.

  Workaround: Do not configure both a DFP agent and a manager on the CSM while it is balancing traffic.

- CSCdu38154

  Under a heavy FTP connection load you may see warnings about FTP not finding associated sessions. These messages are benign.

  Workaround: None.

- CSCdu46347

  If you change the server farm VLAN IP address while the ICMP probe is configured, the ICMP probe still uses the old IP address instead of the new one. Changing the server farm with ICMP causes probes to fail and eventually brings the virtual server out of service.

  Workaround: Delete the ICMP probe from the server farm configuration, change the VLAN IP address, and then add the ICMP probe back to the server farm configuration.

Note Multiple server farms may be associated with a VLAN IP address. To determine which server farms are associated with a VLAN IP address, issue the **show ip slb real** command, examine the display, identify the real servers that are in the same network as the VLAN IP address, and note the server farm associations of those real servers.

- CSCdu54735

  If the version of software running on the CSM does not correspond to the version of Cisco IOS software running on the Catalyst switch, a spurious memory access message may display when the CSM is inserted into a Catalyst 6500 Series chassis.

  Workaround: If the versions of software do not correspond, either the Cisco IOS or the CSM software must be upgraded for the module to function.

Resolved Caveats in Release 1.2(2)

This section describes caveats that have been resolved in CSM software release 1.2(2).

- CSCdw24071

  In CSM software versions 1.1(1), 1.2(1), and 1.2(1) or earlier, the CSM may fail if it receives a TCP RST frame on a connection at an inappropriate time. This condition may be triggered if an RST frame arrives immediately following a valid data frame on the same connection. This scenario occurs rarely yet is prevalent when many packet drops or errors occur in the network due to congested or defective servers or due to overloaded transmission links. This defect is fixed in versions 2.1(2), and versions later than 2.1(2).

- CSCdw41620

  The CSM may classify incoming frames incorrectly, causing those frames to be dropped. Such packet loss results in intermittent connectivity to virtual servers configured on the CSM. This problem occurs only if 128 or more virtual servers have been configured on the device since bootup. (This number includes virtual servers that have been configured and subsequently removed from the configuration.) In most production scenarios, virtual servers are configured only when the device boots.

  This defect is present in CSM software releases 1.1(1), 1.2(1), 2.1(1), 2.1(2). This defect is fixed in version 1.2(1).

- CSCdw24384

  When connections arrive that are configured to a CSM through a redundant router pair running HSRP, those connections may be from the standby HSRP peer. When returning traffic through that redundant router pair, the CSM must send the traffic to the HSRP virtual MAC address shared by the two routers. In CSM software versions 1.2(1) and 2.1(1), the CSM incorrectly forwards such traffic to the real MAC address of the standby router.

Open Caveats in Release 1.2(1)

This section describes known limitations that exist in the CSM software release 1.2(1).

- CSCdu04990

  If the CSM parses a cookie to make a connection when the connection is closed, the connection will be listed as being current. If the client makes a connection again after the sticky timer expires, then one more connection goes into a closing state, thereby incrementing the counter by one.

  Workaround: None.

- CSCdu05559

  During heavy traffic conditions, in a fault-tolerant configuration, the primary CSM may not be able to send heartbeat messages to the secondary CSM. This condition causes both the primary and secondary CSMs to become active, creating a bridge loop in the network.

  Workaround: Reboot the primary CSM.

- CSCdu33696

  While the CSM is balancing traffic and you configure the CSM with both a DFP agent and a manager, the following may occur:

  – All the counters in the **show ip slb stats** command are reset to 0.

  – The **show** command returns *No ICC Response* intermittently.

  - Unknown real servers with unknown bind IDs and weights show up.
  - Virtual servers send an RST to all connection requests.
  - CSM performance becomes very slow.

  Workaround: Do not configure both a DFP agent and a manager on the CSM while it is balancing traffic.

- CSCdu38154

  Under a heavy FTP connection load you may see warnings about FTP not finding associated sessions. These messages are benign.

  Workaround: None.

- CSCdu46347

  If you change the server farm VLAN IP address while the ICMP probe is configured, the ICMP probe still uses the old IP address instead of the new one. Changing the server farm with ICMP causes probes to fail and eventually brings the virtual server out of service.

  Workaround: Delete the ICMP probe from the server farm configuration, change the VLAN IP address, and then add the ICMP probe back to the server farm configuration.

Note Multiple server farms may be associated with a VLAN IP address. To determine which server farms are associated with a VLAN IP address, issue the **show ip slb real** command, examine the display, identify the real servers that are in the same network as the VLAN IP address, and note the server farm associations of those real servers.

- CSCdu54735

  If the version of software running on the CSM does not correspond to the version of Cisco IOS software running on the Catalyst switch, a spurious memory access message may be displayed when the CSM is inserted into a Catalyst 6500 Series chassis.

  Workaround: If the versions of software do not correspond, either the Cisco IOS or the CSM software must be upgraded for the module to function.

- CSCdv78416

  When using the **no ip slb map** command (or **no map** in the module CSM submode) in Cisco IOS software for the CSM, the memory allocated for match rules is not deallocated. This condition is not usually a problem since the amount of memory required is small. Additionally, calling the **no url-map**, **no cookie-map**, or **no header-map** command from SLB policy submode can cause the specified map to be associated with the policy, rather than disassociated, if the policy is not currently associated with a map of that type.

  Workaround: Do not call the command for a policy that is not configured with a map of the given type.

- CSCdw47284

  Client access lists for the CSM are specified in one of two ways:

  - If the list is assigned directly to the virtual server using the **client** command in the vserver submode, the client mask will be changed to 255.255.255.255 during a configuration reload, which occurs when the configuration is first sent to the module on startup.
  - When using the **clear ip slb linecard-config** command.

You can determine that the mask has been changed by comparing the virtual server output for the **show running** command with the output from the **show ip slb vserver detail** command.

Workaround: Create a Cisco IOS standard IP access list, assign it to an slb policy, and assign the policy to the virtual server.

Resolved Caveats in Release 1.2(1)

This section describes caveats that have been resolved in CSM software release 1.2(1).

- CSCdt30757

  Server-to-server FTP data connections do not work in passive (PASV) mode.

  Workaround: Do not use PASV mode for server-to-server data connections.

- CSCdt42091

  Intensive Telnet/FTP probing may cause a device that is being probed to stop responding. (Generally, intensive probing represents a fault in the device being probed.)

  Workaround: Probe the device at a slower rate and increase the probe interval value.

- CSCdt42937

  If the CSM is forwarding traffic while the CSM is being configured, error messages may appear on the screen.

  Workaround: This message is for information only and may be ignored.

- CSCdt44655

  Booting the CSM with a large number of virtual servers configured (over 2000) causes the CSM to go offline.

  Workaround: Reduce the number of virtual servers and reboot the CSM.

- CSCdt45461

  HTTP GET probes may fail when probing using large HTML pages.

  Workaround: Probe using smaller web pages, or probe using a HEAD request instead of a GET request.

- CSCdt64850, CSCdt75262, CSC77827, CSCdt79110, CSCdt80328

  In configurations approaching the CSM's maximum limits, the CSM may reboot when a maximum load that contains certain traffic mixes and large amounts of invalid traffic is applied.

  Workaround: None.

- CSCdt72948

  IDENT protocol causes slow Telnet connections to the CSM.

  Workaround: Do not use the IDENT protocol to communicate with the CSM.

- CSCdt73069

  When the MAC address corresponding to a real server IP address changes, it may take 5 to 6 minutes before probes to that real server are successful.

  Workaround: None.

- CSCdt73118

  Although it is possible to configure the Catalyst 6500 Series switch remotely using an HTTP server, the CSM does not support this mode of configuration.

  Workaround: None.

- CSCdt76588

  The CSM appears not to see some SYN ACKs when forwarding a heavy flow of traffic.

  Workaround: None.

- CSCdt77071

  When a cookie sticky group or SSL sticky group is created and then associated with a virtual server, the virtual server changes its type to IP sticky.

  Workaround: Create a policy, associate the sticky group with it, and then associate the policy with the virtual server.

- CSCdt78707

  When a VIP is configured and falls outside the address range of existing client VLANs, it will appear as operational when status is displayed using the **show ip slb virtual-server detail** command.

  Workaround: This message is for information only and may be ignored.

- CSCdu24256

  Under heavy traffic stress, ARP requests to virtual servers may fail.

  Workaround: None. Reboot the system to bring the virtual servers back online.

Open Caveats in Release 1.1

This section describes known limitations that exist in the CSM software release 1.1.

- CSCdt10633

  When configuring a fault-tolerant VLAN, a bridge loop may occur if you configure client and server VLANs before configuring the fault-tolerant VLAN.

  Workaround: Configure the fault-tolerant VLAN before configuring the client and server VLANs.

- CSCdt30757

  Server-to-server FTP data connections do not work in PASV (passive) mode.

  Workaround: Do not use PASV mode for server-to-server data connections.

- CSCdt37962

  When a large number of probes (many thousands) or virtual servers (many thousands) are configured, servers may not respond to probes.

  Workaround: In the ip slb probe probe-name ICMP submode, increase the interval seconds value, or decrease the number of probes.

- CSCdt41442

  Using VLAN1 for the client VLAN does not work.

  Workaround: Do not use VLAN1 for the client VLAN.

- CSCdt42091

  Intensive Telnet/FTP probing may cause a device that is being probed to stop responding. (Generally this represents a fault in the device being probed.)

  Workaround: Probe the device at a slower rate and increase the probe interval value.

- CSCdt42937

  If the CSM is forwarding traffic while configuration is occurring, error messages may appear on the screen.

  Workaround: Ignore these error messages.

- CSCdt44655

  Booting the CSM with a large number of virtual servers configured (over 2000) causes the CSM to go offline.

  Workaround: Reduce the number of virtual servers and reboot.

- CSCdt45461

  HTTP GET probes may fail when probing using large HTML pages.

  Workaround: Probe using smaller web pages, or probe using a HEAD request instead of a GET request.

- CSCdt64850, CSCdt75262, CSC77827, CSCdt79110, CSCdt80328

  In configurations approaching the CSM's maximum limits, the CSM may reboot when a maximum load that contains certain traffic mixes and large amounts of invalid traffic is applied.

  Workaround: None.

- CSCdt72948

  IDENT protocol causes slow Telnet connections to CSM.

  Workaround: Do not use the IDENT protocol to communicate with the CSM.

- CSCdt73069

  When the MAC address corresponding to a real server IP address changes, it may take 5 to 6 minutes before probes to that real server are successful.

  Workaround: None.

- CSCdt73118

  Although it is possible to configure the Catalyst 6500 Series switch remotely using HTTP server, the CSM does not support this mode of configuration.

  Workaround: None.

- CSCdt75365

  Trace route to a VIP does not work.

  Workaround: Do not use trace route to a VIP.

- CSCdt76588

  The CSM appears not to see some SYN ACKs when forwarding a heavy flow of traffic.

  Workaround: None.

- CSCdt77071

  When a cookie sticky or SSL sticky group is created and then associated with a virtual server, the virtual server changes its type to IP sticky.

  Workaround: Create a policy, associate the sticky group with it, and then associate the policy with the virtual server.

- CSCdt78663

  When using RHI (Route Health Injection) in a fault-tolerant configuration, traffic from a VIP may go into a routing loop because the standby CSM replies to the VIP ARP request before the active CSM replies. This problem occurs when ip proxy-arp, which is enabled by default, is not disabled.

  Workaround: Disable ip proxy-arp on the MSFC VLAN interfaces that reside on the CSM client VLANs using the **no ip proxy-arp** command.

- CSCdt78707

  When a VIP is configured and falls outside the address range of existing client VLANs, it will appear as operational when status is displayed using the **show ip slb virtual-server detail** command.

  Workaround: Ignore this message.

- CSCdv78416

  When using the **no ip slb map** command (or **no map** in the module CSM submode) in IOS for the CSM, the memory allocated for match rules is not deallocated. This condition is not usually a problem since the amount of memory required is small. Additionally, calling the **no url-map**, **no cookie-map**, or **no header-map** command from SLB policy submode can cause the specified map to be associated with the policy, rather than disassociated, if the policy is not currently associated with a map of that type.

  Workaround: Do not call the command for a policy that is not configured with a map of the given type.

- CSCdv73302

  When serverfarms for the CSM have been configured with health probes and no real servers at the time the module comes online, the probe configuration for the serverfarm is never sent to the module, even when the real servers are later added to the serverfarm.

  Workaround: Configure real servers before configuring probes in ip slb serverfarm submode.

- CSCdw47284

  Client access lists for the CSM are specified in one of two ways:

  – If the list is assigned directly to the virtual server using the **client** command in the vserver submode, the client mask will be changed to 255.255.255.255 during a configuration reload, which occurs when the configuration is first sent to the module on startup.

  – When using the **clear ip slb linecard-config** command.

  You can determine that the mask has been changed by comparing the virtual server output for the **show running** command with the output from the **show ip slb vserver detail** command.

  Workaround: Create a Cisco IOS standard IP access list, assign it to an slb policy, and assign the policy to the virtual server.

Troubleshooting

CSM error messages may be received and reported in the system log (syslog). This section describes these messages.

Message Banners

When syslog messages are received, they are preceded by one of the following banners:

Where # is the slot number of the CSM module.

Error Message `CSM_SLB-4-INVALIDID Module # invalid ID`
`00:00:00: CSM_SLB-4-DUPLICATEID Module # duplicate ID`
`00:00:00: CSM_SLB-3-OUTOFMEM Module # memory error`
`00:00:00: CSM_SLB-4-REGEXMEM Module # regular expression memory error`
`00:00:00: CSM_SLB-4-ERRPARSING Module # configuration warning`
`00:00:00: CSM_SLB-4-PROBECONFIG Module # probe configuration error`
`00:00:00: CSM_SLB-4-ARPCONFIG Module # ARP configuration error`
`00:00:00: CSM_SLB-6-RSERVERSTATE Module # server state changed`
`00:00:00: CSM_SLB-6-GATEWAYSTATE Module # gateway state changed`
`00:00:00: CSM_SLB-3-UNEXPECTED Module # unexpected error`
`00:00:00: CSM_SLB-3-REDUNDANCY Module # FT error`
`00:00:00: CSM_SLB-4-REDUNDANCY_WARN Module # FT warning`
`00:00:00: CSM_SLB-6-REDUNDANCY_INFO Module %d FT info`
`00:00:00: CSM_SLB-3-ERROR Module # error`
`00:00:00: CSM_SLB-4-WARNING Module # warning`
`00:00:00: CSM_SLB-6-INFO Module # info`
`00:00:00: CSM_SLB-4-TOPOLOGY Module # warning`
`00:00:00: CSM_SLB-3-RELOAD Module # configuration reload failed`
`00:00:00: CSM_SLB-3-VERMISMATCH Module # image version mismatch`
`00:00:00: CSM_SLB-4-VERWILDCARD Received CSM-SLB module version wildcard on slot #`
`00:00:00: CSM_SLB-3-PORTCHANNEL Portchannel allocation failed for module #`
`00:00:00: CSM_SLB-3-IDB_ERROR Unknown error occurred while configuring IDB`

Server and Gateway Health Monitoring

Error Message `SLB-LCSC: No ARP response from gateway address A.B.C.D.`

Explanation The configured gateway A.B.C.D. did not respond to ARP requests.

Error Message `SLB-LCSC: No ARP response from real server A.B.C.D.`

Explanation The configured real server A.B.C.D. did not respond to ARP requests.

Error Message `SLB-LCSC: Health probe failed for server A.B.C.D on port P.`

Explanation The configured real server on port P of A.B.C.D. failed health checks.

Error Message `SLB-LCSC: DFP agent <x> disabled server <x>, protocol <x>, port <x>`

Explanation The configured DFP agent has reported a weight of 0 for the specified real server.

Error Message `SLB-LCSC: DFP agent <x> re-enabled server <x>, protocol <x>, port <x>`

Explanation The configured DFP agent has reported a non-zero weight for the specified real server.

Diagnostic Messages

Error Message `SLB-DIAG: WatchDog task not responding.`

Explanation A critical error occurred within the CSM hardware or software.

Error Message `SLB-DIAG: Fatal Diagnostic Error %x, Info %x.`

Explanation A hardware fault was detected. The hardware is unusable and must be repaired or replaced.

Error Message `SLB-DIAG: Diagnostic Warning %x, Info %x.`

Explanation A non-fatal hardware fault was detected.

Fault-Tolerance Messages

Error Message `SLB-FT: No response from peer. Transitioning from Standby to Active.`

Explanation The CSM detected a failure in its fault-tolerant peer and has transitioned to the active state.

Error Message `SLB-FT: Heartbeat intervals are not identical between ft pair.`
`SLB-FT: Standby is not monitoring active now.`

Explanation Proper configuration of the fault-tolerance feature requires that the heartbeat intervals be identical between CSMs within the same fault-tolerance group, and this is currently not the case. The fault-tolerance feature is disabled until the heartbeat intervals have been configured identically.

Error Message `SLB-FT: heartbeat interval is identical again`

Explanation The heartbeat intervals of different CSMs in the same fault-tolerance group have been reconfigured to be identical. The fault-tolerance feature will be re-enabled.

Error Message `SLB-FT: The configurations are not identical between the members of the fault tolerant pair.`

Explanation In order for the fault-tolerance system to preserve the sticky database, the different CSMs in the fault-tolerance group must be identically configured, and this is not currently the case.

Regular Expression Errors

Error Message
```
SLB-LCSC: There was an error downloading the configuration to hardware
SLB-LCSC: due to insufficient memory. Use the 'show ip slb memory'
SLB-LCSC: command to gather information about memory usage.
SLB-LCSC: Error detected while downloading URL configuration for vserver %s.
```

Explanation The hardware does not have sufficient memory to support the desired set of regular expressions. A different set of regular expressions must be configured for the system to function properly.

Error Message
```
SLB-REGEX: Parse error in regular expression <x>.
SLB-REGEX: Syntactic error in regular expression <x>.
```

Explanation The configured regular expression does not conform to the regular expression syntax as described in the user manual.

Error Message
```
SLB-LCSC: Error detected while downloading COOKIE policy map for
vserver <x>.
SLB-LCSC: Error detected while downloading COOKIE <x> for vserver <x>.
```

Explanation An error occurred in configuring the cookie regular expressions for the virtual server. This error is likely due to a syntactic error in the regular expression (see below), or there is insufficient memory to support the desired regular expressions.

Related Documentation

For more detailed installation and configuration information, refer to the following publications:

- *Catalyst 6500 Series Content Switching Module Installation and Configuration Note*
- *Regulatory Compliance and Safety Information for the Catalyst 6500 Series Switches*
- *Catalyst 6500 Series Installation Guide*
- *Catalyst 6500 Series Quick Software Configuration Guide*
- *Catalyst 6500 Series Module Installation Guide*
- *Catalyst 6500 Series Software Configuration Guide*

- *Catalyst 6500 Series Command Reference*
- *Catalyst 6500 Series IOS Software Configuration Guide*
- *Catalyst 6500 Series IOS Command Reference*
- *ATM Software Configuration and Command Reference—Catalyst 5000 Family and Catalyst 6500 Series Switches*
- *System Message Guide—Catalyst 6500 Series, 5000 Family, 4000 Family, 2926G Series, 2948G, and 2980G Switches*
- For information about MIBs, refer to

  http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml
- Release Notes for Catalyst 6500 Series Software Release 5.x

Cisco IOS Software Documentation Set

Cisco IOS Configuration Guides and Command References—Use these publications to help you configure the Cisco IOS software that runs on the MSFC and on the MSM and ATM modules.

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order annual or quarterly subscriptions through the online Subscription Store:

http://www.cisco.com/go/subscription

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can send your comments in e-mail to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.

Cisco TAC Website

The Cisco TAC website (http://www.cisco.com/tac) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

http://tools.cisco.com/RPF/register/register.do

Opening a TAC Case

The online TAC Case Open Tool (http://www.cisco.com/tac/caseopen) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide, and the Internetworking Design Guide. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/go/packet

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.