Release Notes for Catalyst 6500 Series Content Switching Module Software Release 3.1(10)

March 18, 2005

Previous Releases—3.1(9), 3.1(8), 3.1(7), 3.1(6), 3.1(5), 3,1(4), 3,1(3), 3,1(2), 3.1(1a), 3.1(1)

This publication describes the features, modifications, and caveats for the Catalyst 6500 series Content Switching Module (CSM) software release 3.1(10) operating on a Catalyst 6500 series switch with Cisco IOS software Release 12.1(13)E3 or Catalyst operating system software 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 3.1(10).

Memory Requirements

The minimum recommended memory for a Supervisor Engine in a chassis with a CSM is 256MB of DRAM. Please consult the Cisco Feature Navigator (http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp) for specific requirements.

Hardware Supported

The CSM is now supported with either with a Supervisor Engine 1A (MSFC required), Supervisor Engine 2 (MSFC required), or Supervisor Engine 720 (the MSFC is not optional on the Sup720), and a module with ports to connect server and client networks.

Note To use the CSM with a Supervisor Engine 720, you must use Cisco IOS software release 12.2(14)SX1 or a later release and CSM version 3.1(4) or greater.

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

Product Number	Minimum Cisco IOS Release	Recommended Cisco IOS Release	Recommended Catalyst Operating System Software Releases
Content Switching Module			
WS-X6066-SLB-APC with Supervisor Engine 1 and MSFC1 or MSFC2	12.1(8a)EX	12.1(13)E	N/A
Supervisor Engine 2 with MSFC2	12.1(8a)EX or 12.2(17d)SXB	12.1(13)E or higher	N/A
WS-X6066-SLB-APC with Supervisor Engine 720.	12.2(14)SX1	12.2(14)SX1 or higher	CSM version 3.1(4) or greater
Console Cable			
72-876-01		Not applicable	
Accessory Kit			
800-05097-01		Not applicable	

Software Compatibility

Table 1 and Table 2 list the CSM software release compatibility.

The minimum software release that is listed is required to support the CSM hardware with a given supervisor engine to perform basic CSM configuration. The recommended software release is the base release to support new commands for a given CSM release.

Table 1 CSM with Cisco IOS Software Requirements

CSM Release	Supervisor Engine 1 MSFC1 or MSFC2		Supervisor Engine 2 with MSFC2		Supervisor 720 with MSFC 3	
	Minimum Software Release	Recommended Software Release	Minimum Software Release	Recommended Software Release	Minimum Software Release	Recommended Software Release
3.1(10)	12.1(8a)EX	12.1(13)E	12.1(8a)EX or 12.2(17d)SXB	12.1(13)E	12.2(14)SX1	12.2(14)SX1
3.1(9)	12.1(8a)EX	12.1(13)E	12.1(8a)EX or 12.2(17d)SXB	12.1(13)E	12.2(14)SX1	12.2(14)SX1
3.1(8)	12.1(8a)EX	12.1(13)E	12.1(8a)EX or 12.2(17d)SXB	12.1(13)E	12.2(14)SX1	12.2(14)SX1
3.1(7)	12.1(8a)EX	12.1(13)E	12.1(8a)EX or 12.2(17d)SXB	12.1(13)E	12.2(14)SX1	12.2(14)SX1
3.1(6)	12.1(8a)EX	12.1(13)E	12.1(8a)EX or 12.2(17d)SXB	12.1(13)E	12.2(14)SX1	12.2(14)SX1
3.1(5)	12.1(8a)EX	12.1(13)E	12.1(8a)EX or 12.2(17d)SXB	12.1(13)E	12.2(14)SX1	12.2(14)SX1
3.1(4)	12.1(8a)EX	12.1(13)E	12.1(8a)EX or 12.2(17d)SXB	12.1(13)E	12.2(14)SX1	12.2(14)SX1
3.1(3)	12.1(8a)EX	12.1(13)E	12.1(8a)EX or 12.2(17d)SXB	12.1(13)E	N/A	N/A
3.1(2)	12.1(8a)EX	12.1(13)E	12.1(8a)EX or 12.2(17d)SXB	12.1(13)E	N/A	N/A
3.1(1a)	12.1(8a)EX	12.1(13)E	12.1(8a)EX or 12.2(17d)SXB	12.1(13)E	N/A	N/A

Table 2 CSM with Cisco IOS and Catalyst Operating System Software Requirements

CSM Release	Supervisor Engine 1 MSFC1 or MSFC2		Supervisor Engine 2 with MSFC2		Supervisor Engine 720 with MSFC 3	
	Minimum Software Release	Recommended Software Release	Minimum Software Release	Recommended Software Release	Minimum Software Release	Recommended Software Release
3.1(10)	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(14)SX2 with Catalyst operating system 8.2(1)	Cisco IOS 12.2(14)SX2 with Catalyst operating system 8.2(1)
3.1(9)	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(14)SX2 with Catalyst operating system 8.2(1)	Cisco IOS 12.2(14)SX2 with Catalyst operating system 8.2(1)
3.1(8)	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(14)SX2 with Catalyst operating system 8.2(1)	Cisco IOS 12.2(14)SX2 with Catalyst operating system 8.2(1)
3.1(7)	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(14)SX2 with Catalyst operating system 8.2(1)	Cisco IOS 12.2(14)SX2 with Catalyst operating system 8.2(1)
3.1(6)	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(14)SX2 with Catalyst operating system 8.2(1)	Cisco IOS 12.2(14)SX2 with Catalyst operating system 8.2(1)
3.1(5)	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(14)SX2 with Catalyst operating system 8.2(1)	Cisco IOS 12.2(14)SX2 with Catalyst operating system 8.2(1)
3.1(4)	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(14)SX2 with Catalyst operating system 8.2(1)	Cisco IOS 12.2(14)SX2 with Catalyst operating system 8.2(1)
3.1(3)	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	N/A	N/A

Table 2 CSM with Cisco IOS and Catalyst Operating System Software Requirements (Continued)

CSM Release	Supervisor Engine 1 MSFC1 or MSFC2		Supervisor Engine 2 with MSFC2		Supervisor Engine 720 with MSFC 3	
	Minimum Software Release	Recommended Software Release	Minimum Software Release	Recommended Software Release	Minimum Software Release	Recommended Software Release
3.1(2)	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	N/A	N/A
3.1(1a)	N/A	N/A	N/A	N/A	N/A	N/A

Software Release 3.1 Features

Table 3 lists the features that have been added to the CSM software in release 3.1.

Table 3 Features Added or Changed in CSM Software Release 3.1

Feature	Description
Supervisor 720 is supported in CSM release 3.1(4) and higher.	Provides support for the CSM to operate in a switch running Supervisor 720 hardware.
Catalyst operating system running with the Cisco IOS software. The Catalyst operating system software requires CSM release 3.1(4) and higher.	Provides support for the CSM to operate with the Catalyst operating system software and the Cisco IOS software.
HTTP method parsing	Allows you to configure regular expressions that are matched against the URL in incoming HTTP requests.
IP reassembly for out-of-order UDP fragments	Provides the CSM with the ability to attempt reassembly of UDP fragments, even when the first fragment is not the first fragment received.
VIP connection watermarks	Allows a web-hosting provider to limit the number of connections going through a particular virtual server.
Idle timeout for unidirectional flows	Prevents the idle and pending timeouts from timing out unidirectional connections because no traffic is received in the reverse direction.
Real server names	Allows adding a real server configuration submode outside of the server farm, where the name and address binding occurs. This feature also creates the possibility for adding other features on a per-address basis, in addition to the current structure of per-address or port or server farm configuration. Also provides the ability for real servers with the same IP address to be moved in or out of service simultaneously.

Table 3 Features Added or Changed in CSM Software Release 3.1 (Continued)

Feature	Description
Slowpath performance improvements	Provides slowpath functions for improved performance with health probing, configuration changes, and the ability of the CSM to handle ARP traffic. The XML configuration and TCL scripting features introduced in CSM software release 3.1(1) also benefit from these improvements.
Global server load balancing (GSLB)	Provides for disaster recovery.
Enhanced interoperation with the SSL termination engine (STE) for secure socket layer (SSL) load balancing	Allows you to load balance a virtual server to an STE. Use the **ssl-hash offset** *value* **length** *value* command in the virtual server submode to any SSL virtual server that will be load balanced to STEs.
Cisco IOS SLB FWLB interoperation (IP reverse-sticky) or (IP sticky insert)	Allows you to insert entries into a sticky database as if the connection came from the virtual server instead of the CSM. With sticky insert enabled, pairings between a source IP key and real servers are entered into the specified sticky database containing the inbound real server.
Sorry server (backup serverfarm)	Allows you to specify one or more backup servers to use when all primary servers are disabled or out-of-service.
Non-TCP connection redundancy	Supports stateful failover for all non-TCP protocols and activates failover for TCP or all traffic independently. This feature is configurable in the virtual server submode.
Optional port for health probes	Allows the administrator to override the real server and virtual server port information by explicitly specifying a port to probe in the health probe configuration.
Support for multiple users simultaneously configuring a CSM	Allows more than one user to configure the CSM at the same time.
TCL (Toolkit Command Language) scripting	Provides the capability for the administrator to upload and execute TCL scripts on the CSM.
SNMP traps on fault-tolerant state changes	Enables SNMP traps for real server transitions.
Support for CISCO-SLB-MIB Support for CISCO-SLB-EXT-MIB	Introduces SNMP support for the CSM.
XML configuration interface	Allows for programmatic configuration of the CSM. The [**no**] **xml config** command enables or disables the XML configuration and enters the SLB XML submode.

Table 3 Features Added or Changed in CSM Software Release 3.1 (Continued)

Feature	Description
Resource use display	Run the **show module csm tech-support** command to display CSM resource use.
CiscoView Device Manager for Cisco Content Switching Module 1.0 (CVDM-CSM) is supported in CSM software release 3.1(4) and higher.	CVDM-CSM enables users to easily configure content load-balancing services on their CSMs. It is a task-based tool that enables users to control the versatility of their CSMs by offering configuration based on recommended practices in tasks, such as setting up virtual servers, creating server farms, and applying advanced policies. To access all CiscoView Device Manager documentation, go to this URL: http://www.cisco.com/go/cvdm

Feature Set

Table 4 describes the CSM features and software descriptions.

Table 4 CSM Feature Set Description

Feature	First Image Release	Supported Release
Supported Hardware		
Supervisor 1A with MSFC and PFC	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
Supervisor 2 with MSFC2	c6slb-apc.1-2-1.bin	SC6K-1.2-CSM SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
Supervisor 720	c6slb-apc.3-1-4.bin	SC6K-3.1-CSM
Catalyst 6500 Series Supported Operating Systems		
Cisco IOS software	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
Catalyst operating system software	c6slb-apc.2-2-7.bin c6slb-apc.3-1-2.bin	SC6K-2.2-CSM SC6K-3.1-CSM
Supported Protocols		
FTP	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
TCP load balancing	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM

Table 4 CSM Feature Set Description (Continued)

Feature	First Image Release	Supported Release
UDP & all common IP protocol load balancing	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-3.1-CSM
Real Time Streaming Protocol (RTSP)	c6slb-apc.2-2-1.bin	SC6K-2.2-CSM SC6K-3.1-CSM
Layer 7 Functionality		
Full regular expression matching	c6slb-apc-1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
URL & cookie switching	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
Generic header parsing	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
Miscellaneous Functionality		
Multiple CSMs in a chassis	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
CSM and Cisco IOS-SLB functioning simultaneously in a chassis	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-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 SC6K-3.1-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 SC6K-3.1-CSM
HTTP method parsing	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM
Fully configurable NAT	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
Server initiated connections	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
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-3.1-CSM SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
Round-robin	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM

Table 4 CSM Feature Set Description (Continued)

Feature	First Image Release	Supported Release
Weighted round-robin (WRR)	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
Least connections	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
Weighted least connections	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
URL hashing	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
Source IP hashing	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
Destination IP hashing	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
Return error code checking	c6slb-apc.2-2-1.bin	SC6K-2.2-CSM SC6K-3.1-CSM
Support for 128 VLANs	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
Support for 256 VLANs	c6slb-apc.2-2-1.bin	SC6K-2.2-CSM SC6K-3.1-CSM
Reduced time between health probes	c6slb-apc.2-2-1.bin	SC6K-2.2-CSM SC6K-3.1-CSM
In-band health checking	c6slb-apc.2-2-1.bin	SC6K-2.2-CSM SC6K-3.1-CSM
Configurable pending connection timeout	c6slb-apc.2-2-1.bin	SC6K-2.2-CSM SC6K-3.1-CSM
IP reassembly for in-order UDP fragments	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
IP reassembly for out-of-order UDP fragments	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM
VIP connection watermarks	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM
Idle timeout for unidirectional flows	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM
Real server names	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM
Slowpath performance improvements	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM

Table 4 CSM Feature Set Description (Continued)

Feature	First Image Release	Supported Release
Load Balancing Supported		
Server load balancing	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
Firewall load balancing	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
DNS load balancing	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
Stealth firewall load balancing	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
Transparent cache redirection	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
Reverse proxy cache	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
SSL off-loading	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
VPN-IPSec load balancing	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
Global server load balancing (GSLB)	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM
Enhanced interoperation with the SSL termination engine (STE) for secure socket layer (SSL) load balancing	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM
Stickiness		
Cookie	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
SSL ID	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
Source IP	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
HTTP redirection	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
Cisco IOS SLB FWLB interoperation (IP reverse-sticky)	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM

Table 4 CSM Feature Set Description (Continued)

Feature	First Image Release	Supported Release
Redundancy		
Sticky state	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
Full stateful failover (connection redundancy)	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
Sorry server (backup serverfarm)	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM
Non-TCP connection redundancy	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM
Health Checking		
HTTP	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
ICMP	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
Telnet	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
TCP	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
SMTP	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
DNS	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
Optional port for health probes	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM
Support for multiple users simultaneously configuring a CSM	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM
TCL (Toolkit Command Language) scripting	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM
Management		
SNMP traps for real server state changes	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
SNMP traps on fault-tolerant state changes	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM
Support for CISCO-SLB-MIB	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM
Support for CISCO-SLB-EXT-MIB	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM
XML configuration interface	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM
Resource use display	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM

New and Changed Information

- When you configure the least connection predictor, a slow-start mechanism operates to avoid sending a high rate of new connections to the servers that have just been put in service. The least connections predictor ensures that the server with the fewest number of active connections will receive the next connection request.

  A new environment variable, REAL_SLOW_START_ENABLE, is included in the 3.1(9) software release to control the rate at which a real server becomes operational when it is put into service. This new variable is only available for a server farm that has been configured with the least connection predictor.

  The configurable range for this variable is 0 to 10. The setting of 0 disables the slow start feature. The value from 1 to 10 specifies how fast the newly activated server should become operational. The value of 1 is the slowest rate. The value of 10 specifies that the CSM would assign more requests to the newly activated server. The value of 3 is the default value.

  If the configuration value is N, the CSM assigns 2 ^ N (2 raised to the N power) new requests to the newly active server at startup (assuming no connections were terminated at that time). As this server finishes or terminates connections; more connections are assigned. Normal connection assignments resume when the newly activated server has the same number of open connections as the other servers in a serverfarm.
- CSM release 3.1(4) and later releases are supported with the Supervisor Engine 720 only with Cisco IOS software Release 12.2(14)SX1 software or higher.
- The CSM is supported on the Supervisor Engine 720 with the Catalyst operating system software as of CSM software release 3.14.
- CSM software release 3.1(4) and later releases are supported in a switch running both Cisco IOS software Release 12.1(13)E and higher and the Catalyst operating system software 7.5 or higher for Supervisor Engine 2 and Cisco IOS software release 12.2(14)SX1 or a later release and CSM software release 3.1(4) or greater.
- 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 enhancement 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.
- For your convenience, sample scripts are available to support the TCL (Toolkit Command Language) feature. Other custom scripts will work, but these sample scripts are supported by Cisco TAC. The file with sample scripts is located at this URL:

  http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-intellother

  The following file contains the sample scripts: c6slb-script.3-1-6.tcl.

Limitations and Restrictions

- The CSM does not support pipelines (multiple HTTP requests sharing the packet boundary) with the persistent rebalance feature.
- Internal ports on the CSM (dot1q, trunk, port-channel, etc.) are automatically configured, with the exception of the VLANs on the trunk, which must be manually added using the **set trunk** *slot* 1 *vlan-list* command in Catalyst operating system.

- 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. With no MINCONNS value set in release 1.2(1), no additional session is balanced until the number of open sessions falls below MAXCONNS.
- 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.
- 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 software release 1.2(1) or higher.

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

Caveats

These sections describe the open and resolved caveats in CSM for all 3.1(x) software releases:

Open Caveats in Software Release 3.1(10)

Note For a description of caveats resolved in CSM software release 3.1(10), see the "Resolved Caveats in Software Release 3.1(10)" section on page 18.

This section describes known limitations that exist in CSM software release 3.1(10).

- CSCeh34176

  The value for the Connections Timed-Out counter is not displayed correctly when you use the **show module csm** *slot* **stats** command. This counter is not consistent with the values displayed in the **show module csm** *slot* **tech-support proc 1** command.

  This data shows that the counter is not working properly CSM Code: 3.1.7

```
Switch# show mod csm 1 tech-support proc 1 | inc Time
Timeouts- Sessions examined               447391863   8308996
Timeouts- Sessions timed out               1920012     181
Timeouts- Active sessions timed out        297575      18
Timeouts- Pending sessions timed out       1622437     163
Timeouts- Unidir sessions timed out        0           0
Timeouts- FT sessions timed out            0           0
Switch# show mod csm 1 stats | inc Timed-Out
Connections Timed-Out:      0
Switch# show mod csm 1 tech-support proc 1 | inc Time
Timeouts- Sessions examined               454121112   6729249
Timeouts- Sessions timed out               1920127     115
Timeouts- Active sessions timed out        297594      19
Timeouts- Pending sessions timed out       1622533     96
Timeouts- Unidir sessions timed out        0           0
Timeouts- FT sessions timed out            0           0
Switch#
```

  Workaround: Use the command *show module csm <slot> tech-support proc 1*.

- CSCee27398

  The CSM reserves 141 KB of memory on the PowerPC control processor for each TCL scripted health probe item configured on the CSM. A probe item is an instance of a probe object associated with a single real server.

  This memory usage is much higher than anticipated. The PowerPC "Available Memory" counter from the **show module csm** *slot* **tech-support utilization** command should not be less than 40 MB.

  Workaround: None.

- CSCed10730

  When you configure a CSM in a fault-tolerant configuration and you have a fault-tolerant priority of 254, the CSM may take over the active role from the other CSM at startup. This situation could occur even when the fault-tolerant preempt option is disabled.

  Workaround: Use fault-tolerant priority values lower than 254.

- CSCed01651

  The CSM does not support pipelines (multiple HTTP requests sharing the packet boundary) with the persistent rebalance feature.

  Workaround: None.

- CSCec84034

  The CSM might not replicate the sticky entries for sticky group zero when it is configured under the virtual server. Because of the configuration download order, the active and redundant CSM may be assigned different group numbers when a group was not specified in the configuration.

  Workaround: Configure a sticky group with a specific number, and assign it to the virtual server.

- CSCec55790

  When using Cisco IOS Release 12.1(19)E or later with CSM 3.1(x) software, the sticky timeout is displayed as zero for all sticky entries, and the total entries count (CurrCount) for each sticky is also displayed as zero. These counters are supported only in CSM software release 3.2(1).

  Workaround: Use the corresponding Cisco IOS software Release 12.1(13)E, which displays the configured timeout instead of the current timeout.

- CCSCdz61644

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

  Workaround: None.

- CSCdz50182

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

  Workaround: None.

- CSCdz12163

  The CSM drops packets because the multilayer switch (MLS) module and the multilayer switch feature card (MSFC) use different MAC addresses. This problem remains in software releases earlier than the Catalyst operating system software release 7.5.1. If any Supervisor Engine 2 in the switch is still operating with a software release earlier than the Catalyst operating system software release 7.5.1, 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 that the module is faulty when it should be displayed as "Other."

  Workaround: None.

- CSCdy79826

  When Internet Group Management Protocol (IGMP) snooping is enabled on the Catalyst 6500 series switch, some CSM connection replication frames might be dropped.

  Workaround: Disable IGMP snooping on both the active and standby CSM modules. 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" to a value that is greater than one for all TCL script probes.

- CSCdy64647

  Established FTP connections are not replicated to the redundant CSM when the redundant CSM becomes operational. To enable an FTP connection for replication from an active CSM to a redundant CSM, the redundant CSM must be operational at the time the FTP connection is opened. If the FTP connection is opened prior to the redundant 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 using the **socket** command with the -**async** option.

  b. Avoid using 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 software, 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 entered, 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 reenter the desired CSM configuration submode.

- CSCdy26940

  Beginning with Cisco IOS software 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 user is configuring probe "FOO," the configuration will be corrupted.

Workaround: Ensure that multiple users do not simultaneously modify the CSM configuration with different object types.

- CSCdx73636

  Some FTP connections may not replicate. For example, an FTP connection through an active CSM is not replicated if no data channel has been set up 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

  Entering 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 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 Software Release 3.1(10)

Note For a description of caveats open in CSM software release 3.1(10), see the "Open Caveats in Software Release 3.1(10)" section on page 14.

This section describes the caveats resolved in CSM software release 3.1(10).

- CSCsa64249

  The CSM may generate a core dump while processing an ICMP destination-unreachable packet.

  Workaround: Block all ICMP dest_unreachable packets by setting the DEST_UNREACHABLE_MASK 0 variable to zero.

- CSCsa57462

  If you remove the global real object (by entering the **no real** *global-real-name* command) while the object is configured inside a serverfarm and has a redirect-vserver association, the CSM might stop responding.

  Workaround: Remove the named real mapping configuration from the serverfarm, or remove the association with the redirect-vserver; then remove the global real object.

- CSCsa53106

  When you remove and then add back a VLAN with a new gateway, the CSM creates new encapsulated MAC address entries; however, the session may still select an old encapsulated ID to set up the return flow from the server to the client. The response from the server to the client is not forwarded properly to the client.

  Workaround 1: Reboot the CSM.

  Workaround 2: Add a specific route in the new VLAN for the affected client.

- CSCsa50587

  Under rare conditions, when you configure a CSM module in bridge mode and enable SPAN on the port channel to the CSM or on any of the VLANs that the CSM is bridging, you might notice this behavior: high CPU utilization on the CSM and on the route processor of the Catalyst 6500 series switch, high link utilization on the CSM port channel, and a high rate of MAC address relearning (or MAC address flapping) if MAC move notification is enabled on the switch.

  Workaround 1: Disable SPAN on the CSM port channel and the VLANs associated with bridge mode on the CSM.

  Workaround 2: Use routed mode on the CSM.

- CSCsa43697

  In the output of the **show mod csm probe detail** command, the transitions counter for GSLB statistics do not increment.

  Workaround: None.

- CSCeh21118

  The CSM crashes with this core-dump data:

  IXP4 Bad Data exception on task +IXP4 SA-CORE (Ex 5)...+

  Cookie map matching type for a virtual server was configured. After a few million connections were established to this vserver, a crash could occur. If you have the sticky replication option enabled on this CSM, then the crash might occur sooner.

  This problem exists in all prior CSM releases up to: 3.1(9), 3.2(3), 4.1(4), and 4.2(1).

  Workaround: Remove the configuration for cookie map matching.

- CSCeg88474

  When the active CSM sends a replication sticky message to the standby CSM, the active CSM uses an incorrect source MAC address, which takes the format of a multicast MAC address. A Catalyst 6500 series switch will not drop these packets; however, other Layer 2 switch devices between the Catalyst 6500 switches would drop these packets.

  Workaround: Set up a direct link between the two Catalyst 6500 switches for fault-tolerant VLAN traffic.

- CSCeg66754

  When you enter the **show csm tech-support** command, the GSLB process shows the real server in a down state, yet the output of the **show mod csm** *slot* **real** command shows the real server in an up (operational) state.

  Workaround: None.

- CSCeg61794

  When the CSM is in the process of redirecting more than 16,000 concurrently opened connections, the CSM might reload and produce the following core-dump message:

  ```
  *IXP3 Bad Data exception on task 'IXP3 SA-CORE (Ex 5)(00000000h)*
  ```

  Workaround: Set the number of maximum connections allowed (max-conns limit) on the configured redirect vserver objects or on the virtual server object.

- CSCeg49520

  When you use XML to make configuration modifications to the CSM and configure multiple VLANs and gateways to reach a host, the CSM might not be able to determine which VLAN the host is using to make the XML request.

  Workaround: Configure a specific route for the hosts that allows you to perform XML configuration.

- CSCeg38929

  In systems with a Supervisor Engine 720, if you configure the same IP address for the default gateway and for a specific route (for example, if you enter the **gateway** *ip_addr_x* command and also the **route** *ip_addr* **gateway** *ip_addr_x* command), and then you remove the default gateway, the CSM incorrectly points the servers to another gateway instead of the gateway in the route configuration.

  Workaround: Remove the route configuration, and then remove the default gateway configuration. You can then reconfigure the route.

- CSCeg35110

  If you configure two virtual servers with the same IP address and one of the virtual servers is not in service, a GSLB probe pointing to the local virtual server is not operable until you remove the downed (not in service) virtual server from the configuration.

  Workaround: Remove the virtual servers that are out-of-service.

- CSCeg28849

  When you configure the least-connections (leastconns) prediction algorithm and you define a large number of real servers (20 or more) to a serverfarm, the CSM might experience degraded performance, which could result in dropped connections.

  Workaround: Use the round-robin prediction algorithm.

- CSCeg17294

  In CSM software release 4.1(3), the CSM can support service FTP translation for virtual server ports or real server ports other than port 21. If you have configured the FTP port that is not in the reserved port range, which is 1 through 1023, then an FTP data flow with a particular source port can be mistaken for an RTSP data flow if the FTP data flow was configured on the same CSM.

  Workaround: None.

- CSCef63166

  When connection redundancy is configured, the connection counters on the standby CSM might incorrectly show that all of the replicated connections were assigned only to one server within a serverfarm. This problem is with the counter only; the connection flows will replicate correctly if a switchover occurs. However, if you enter the **maxconns** *max-conns* command to limit the number of active connections to the real server, this problem would not correctly count against these limits on the standby CSM.

  Workaround: None.

Open Caveats in Software Release 3.1(9)

Note For a description of caveats resolved in CSM software release 3.1(9), see the "Resolved Caveats in Software Release 3.1(9)" section on page 24.

This section describes known limitations that exist in CSM software release 3.1(9).

- CSCee27398

  The CSM reserves 141 KB of memory on the PowerPC control processor for each TCL scripted health probe item configured on the CSM. A probe item is an instance of a probe object associated with a single real server.

  This memory usage is much higher than anticipated. The PowerPC "Available Memory" counter from the **show module csm** *slot* **tech-support utilization** command should not be less than 40 MB.

  Workaround: None.

- CSCed10730

  When you configure a CSM in a fault-tolerant configuration and you have a fault-tolerant priority of 254, the CSM may take over the active role from the other CSM at startup. This situation could occur even when the fault-tolerant preempt option is disabled.

  Workaround: Use fault-tolerant priority values lower than 254.

- CSCed01651

  The CSM does not support pipelines (multiple HTTP requests sharing the packet boundary) with the persistent rebalance feature.

  Workaround: None.

- CSCec84034

  The CSM might not replicate the sticky entries for sticky group zero when it is configured under the virtual server. Because of the configuration download order, the active and redundant CSM may be assigned different group numbers when a group was not specified in the configuration.

  Workaround: Configure a sticky group with a specific number, and assign it to the virtual server.

- CSCec55790

  When using Cisco IOS Release 12.1(19)E or later with CSM 3.1(x) software, the sticky timeout is displayed as zero for all sticky entries, and the total entries count (CurrCount) for each sticky is also displayed as zero. These counters are supported only in CSM software release 3.2(1).

  Workaround: Use the corresponding Cisco IOS software Release 12.1(13)E, which displays the configured timeout instead of the current timeout.

- CCSCdz61644

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

  Workaround: None.

- CSCdz50182

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

  Workaround: None.

- CSCdz12163

  The CSM drops packets because the multilayer switch (MLS) module and the multilayer switch feature card (MSFC) use different MAC addresses. This problem remains in software releases earlier than the Catalyst operating system software release 7.5.1. If any Supervisor Engine 2 in the switch is still operating with a software release earlier than the Catalyst operating system software release 7.5.1, 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 that the module is faulty when it should be displayed as "Other."

  Workaround: None.

- CSCdy79826

  When Internet Group Management Protocol (IGMP) snooping is enabled on the Catalyst 6500 series switch, some CSM connection replication frames might be dropped.

  Workaround: Disable IGMP snooping on both the active and standby CSM modules. 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" to a value that is greater than one for all TCL script probes.

- CSCdy64647

  Established FTP connections are not replicated to the redundant CSM when the redundant CSM becomes operational. To enable an FTP connection for replication from an active CSM to a redundant CSM, the redundant CSM must be operational at the time the FTP connection is opened. If the FTP connection is opened prior to the redundant 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 using the **socket** command with the -**async** option.

  b. Avoid using 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 software, 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 entered, 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 reenter the desired CSM configuration submode.

- CSCdy26940

  Beginning with Cisco IOS software 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 user is configuring probe "FOO," the configuration will be corrupted.

  Workaround: Ensure that multiple users do not simultaneously modify the CSM configuration with different object types.

- CSCdx73636

  Some FTP connections may not replicate. For example, an FTP connection through an active CSM is not replicated if no data channel has been set up 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

  Entering 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 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 Software Release 3.1(9)

Note For a description of caveats open in CSM software release 3.1(9), see the "Open Caveats in Software Release 3.1(9)" section on page 21.

This section describes the caveats resolved in CSM software release 3.1(9).

- CSCeg14713

  When you configure the CSM to perform Global Server Load-Balancing (GSLB) for a destination IP that is also a local Virtual IP (VIP) on the module, the CSM does not properly take this local VIP out-of-service. The CSM keeps responding to the DNS request with a VIP address that is out-of-service. The CSM also reports to KAL-AP (keep-alive probe) with the incorrect load value for this local VIP.

  Workaround: None.

- CSCee75746

  When you perform an SNMP MIB request for the packet counter ifHCOutUcastPkts, the CSM Gigabit interfaces may display incorrect 64-bit values.

  Workaround: None.

- CSCee74402

  When the CSM load-balances more than one HTTP request of a persistent connection to the same server with destination port translation, the CSM will send incorrect RST (reset) packets to this server when the CSM rebalances the connection to another server. The incorrect RST packet contains the virtual server port instead of the port configured for the real server.

  Workaround: None.

- CSCee70058, CSCee69755

  The CSM sends an invalid RST packet when it rebalances an HTTP persistent connection from a serverfarm with the predictor forward parameter applied to another serverfarm with real servers. This action creates two problems:

  a. This connection cannot be rebalanced back to the predictor forward designated server farm.

  b. The CSM created invalid learned MAC addresses on the Catalyst series switch bridge table.

  This caveat exists in CSM releases 3.1(5), 3.1(6), 3.1(7), 3.1(8), 3.2(2) and 4.1(1).

  Workaround: None.

- CSCee50280

  The CSM listens on these UDP ports: 5002 used for the CAP protocol and port 53 used for GSLB. The CSM silently discards the packets to port 53 and port 5002 with GSLB features disabled.

  Workaround: None.

- CSCee45483

  With Global Server Load Balancing (GSLB) configured for HTTP probes, the s**how module csm x gslb probe** command output does not show the HTTP counters incrementing.

  Workaround: None.

Open Caveats in Software Release 3.1(8)

Note For a description of caveats resolved in CSM software release 3.1(8), see the "Resolved Caveats in Software Release 3.1(8)" section on page 29.

This section describes known limitations that exist in CSM software release 3.1(8).

- CSCee27398

  The CSM reserves 141 KB of memory on the PowerPC control processor for each TCL scripted health probe item configured on the CSM. A probe item is an instance of a probe object associated with a single real server.

  This memory usage is much higher than anticipated. The PowerPC "Available Memory" counter from the **show module csm** *slot* **tech-support utilization** command should not be less than 40 MB.

  Workaround: None.

- CSCed10730

  When you configure a CSM in a fault-tolerant configuration and you have a fault-tolerant priority of 254, the CSM may take over the active role from the other CSM at startup. This situation could occur even when the fault-tolerant preempt option is disabled.

  Workaround: Use fault-tolerant priority values lower than 254.

- CSCed01651

  The CSM does not support pipelines (multiple HTTP requests sharing the packet boundary) with the persistent rebalance feature.

  Workaround: None.

- CSCec84034

  The CSM might not replicate the sticky entries for sticky group zero when it is configured under the virtual server. Because of the configuration download order, the active and standby CSM may be assigned different group numbers when a group was not specified in the configuration.

  Workaround: Configure a sticky group with a specific number, and assign it to the virtual server.

- CSCec55790

  When using Cisco IOS Release 12.1(19)E or later with CSM 3.1(x) software, the sticky timeout is displayed as zero for all sticky entries, and the total entries count (CurrCount) for each sticky is also displayed as zero. These counters are supported only in the CSM software release 3.2(1).

  Workaround: Use the corresponding Cisco IOS Release 12.1(13)E, which displays the configured timeout instead of the current timeout.

- CCSCdz61644

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

  Workaround: None.

- CSCdz50182

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

  Workaround: None.

- CSCdz12163

  The CSM drops packets because the multilayer switch (MLS) module and the multilayer switch feature card (MSFC) use different MAC addresses. This problem remains in software releases earlier than the Catalyst 7.5.1 software release. If any Supervisor Engine 2 in the switch is still operating with a software release earlier than the Catalyst 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 that the module is faulty when it should be displayed as "Other."

  Workaround: None.

- CSCdy79826

  When Internet Group Management Protocol (IGMP) snooping is enabled on the Catalyst 6500 series switch, some CSM connection replication frames might be dropped.

  Workaround: Disable IGMP snooping on both the active and standby CSM modules. 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" to a value that is greater than one 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 using the **socket** command with the -**async** option.

  b. Avoid using 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 software, 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 entered, 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 reenter 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 user is configuring probe "FOO," the configuration will be corrupted.

Workaround: Ensure that multiple users do not simultaneously modify the CSM configuration with different object types.

- CSCdx73636

  Some FTP connections may not replicate. For example, an FTP connection through an active CSM is not replicated if no data channel has been set up 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 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 Software Release 3.1(8)

Note For a description of caveats open in CSM software release 3.1(8), see the "Resolved Caveats in Software Release 3.1(9)" section on page 24.

This section describes the caveats resolved in CSM software release 3.1(8).

- CSCee45978

  CLI commands sent to the CSM may fail when the servers in a server farm reaches the configured maximum connections (max-conns) value. When the maximum connection value has been met, the servers would not be selected, generating system messages to notify users of the change in the server state. In software release 3.1(8), the configurable global variable INBAND_STATE_CHANGED_MSG_RATE is introduced to control the rate at which these messages are generated and written into the system message log. You must configure a value of zero to suppress the messages from being sent.

  Workaround: Remove the max-conns configuration from the server. The max-conns value can be configured at the virtual server level.

- CSCee44921

  The server configured with “inservice standby” becomes active after it fails and recovers from a health probe check. The server should not start accepting load-balancing traffic after it recovers from health probe failure and should go back to standby mode where it accepts only those connections with the sticky or backup role.

  Workaround: None

- CSCee42680

  When a TCP request with a multicast destination MAC address reaches the CSM, the CSM sends a reset (RST) back to this host. This is a problem even when the TCP request contains the unicast destination IP address that is not owned by the CSM.

  Workaround: None.

- CSCee27428

  The CSM may respond with an acknowledgement (ACK) message instead of synchronization-acknowledgement (SYN-ACK) message for the repeated synchronization (SYN) packet from the client to a Layer 7 virtual server.

  Workaround: None

- CSCee26981

  The CSM may fail to respond if it has to replicate over 256,000 unique sticky entries and replicate over 30,000 new connections per second.

  Workaround: Configure the appropriate subnet mask for IP sticky to reduce the number of sticky entries in the CSM database.

- CSCed90292

  The **clear module csm** *slot* **sticky** command does not clear the sticky entries on the standby CSM.

  Workaround: Enter the **clear module csm** *slot* **sticky** command on the standby CSM.

- CSCed63583

  If the first reply packet from the server is an “HTTP 100 Continue” type reply, then the CSM does not learn the HTTP “Set-Cookie” information from the subsequent “HTTP 200 OK” reply from the server. In this case, the cookie sticky option will not work for the subsequent “HTTP 100 Continue” packet.

  Workaround: Reconfigure the server so that it sends the Cookie information in the “HTTP 100 Continue” packet as well.

- CSCed06861

  The CSM incorrectly replicates the FTP connections to the standby CSM if connection replication is enabled for the FTP server. If the FTP traffic reaches the standby CSM due to bridge flooding, the standby CSM also forwards this traffic. This situation causes the Catalyst switch to recognize that the source MAC address belongs to the standby CSM instead of the active CSM. This situation might cause all other traffic to be incorrectly forwarded to the standby CSM, where the packets will be dropped.

  Workaround: Turn off connection replication for the FTP virtual server.

- CSCec82096

  When you configure the CSM for persistent rebalancing of each HTTP request for the same TCP data stream, the CSM is unable to process requests that contain extra carriage return-line feed (CR-LF) characters that are beyond the "Content Length" specified in the HTTP header.

  Workaround: Change the server to "send HTTP version 1.1" to stop the client from sending these extra characters.

Open Caveats in Software Release 3.1(7)

Note For a description of caveats resolved in CSM software release 3.1(7), see the "Resolved Caveats in Software Release 3.1(7)" section on page 34.

This section describes known limitations that exist in CSM software release 3.1(7).

- CSCed10730

  When configuring a CSM in a fault-tolerant configuration, and you have a fault-tolerant priority of 254, the CSM may take over the active role from the other CSM when it boots up. This situation could occur even when the fault-tolerant preempt option is disabled.

  Workaround: Use fault-tolerant priority values lower than 254.

- CSCed06861

  The CSM incorrectly replicates the FTP connections to the standby CSM if connection replication is enabled for the FTP server. If the FTP traffic is reaching the standby CSM because of bridge flooding, the standby CSM also forwards this traffic. This situation causes the Catalyst switch to recognize that the source MAC address belongs to the standby CSM instead of the active CSM. This situation might cause all other traffic to be incorrectly forwarded to the standby CSM, where the packets will be dropped.

  Workaround: Turn off connection replication for the FTP virtual server.

- CSCed01651

  The CSM does not support pipelines (multiple HTTP requests sharing the packet boundary) with the persistent rebalance feature.

- CSCec84034

  The CSM might not replicate the sticky entries for sticky group zero when it is configured under the virtual server. Because of the configuration download order, the active and standby CSM may be assigned a different group number when the group was not specified in the configuration.

  Workaround: Configure a sticky group with a specific number, and assign it to the virtual server.

- CSCec55790

  When using Cisco IOS Release 12.1(19)E or later with CSM 3.1(x) software, the current sticky timeout is displayed as zero for all sticky entries, and the total entries count (CurrCount) for each sticky is also displayed as zero. These counters are supported only in the CSM software release 3.2(1).

  Workaround: Use the corresponding Cisco IOS Release 12.1(13)E, which displays the configured timeout instead of the current timeout.

- CCSCdz61644

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

  Workaround: None.

- CSCdz50182

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

  Workaround: None.

- CSCdz12163

  The CSM drops packets because the multilayer switch (MLS) module 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 Catalyst 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 that the module is faulty when it should be displayed as "Other."

  Workaround: None.

- CSCdy79826

  When Internet Group Management Protocol (IGMP) snooping is enabled on the Catalyst 6500 series switch, some CSM connection replication frames might be dropped.

  Workaround: Disable IGMP snooping on both the active and standby CSM modules. 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 one 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 using the **socket** command with the -**async** option.

  b. Avoid using 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 software, 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 user is configuring probe "FOO," the configuration will be corrupted.

  Workaround: Ensure that multiple users do not simultaneously modify the CSM configuration with different object types.

- CSCdx73636

  Some FTP connections may not replicate. For example, an FTP connection through an active CSM is not replicated if no data channel has been set up 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 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 Software Release 3.1(7)

Note For a description of caveats open in CSM software release 3.1(7), see the "Open Caveats in Software Release 3.1(7)" section on page 31.

This section describes the caveats resolved in CSM software release 3.1(7).

- CSCed47110

  When the configurations between the active and standby CSMs are out-of-synchronization, and the switch performs an RPR+ switchover to its peer, the standby CSM becomes active. Both CSMs remain in this active-active state and cause load-balancing problems and bridging problems in the network.

  Workaround: Ensure that the configurations are the same on both the active CSM and the standby CSM.

Open Caveats in Software Release 3.1(6)

Note For a description of caveats resolved in CSM software release 3.1(6), see the "Resolved Caveats in Software Release 3.1(6)" section on page 38.

This section describes known limitations that exist in CSM software release 3.1(6).

- CSCed10730

  When configuring a CSM in a fault tolerant (FT) configuration, and you have an fault-tolerant priority of 254, the CSM may take over the active role from the other CSM when it boots up. This situation could occur even when the fault-tolerant preempt option is disabled.

  Workaround: Use fault-tolerant priority values lower than 254.

- CSCed06861

  The CSM incorrectly replicates the FTP connections to the standby CSM if connection replication is enabled for the FTP server. If the FTP traffic is reaching the standby CSM because of bridge flooding, the standby CSM also forwards this traffic. This situation causes the Catalyst switch to recognize that the source MAC address belongs to the standby CSM instead of the active CSM. This situation might cause all other traffic to be incorrectly forwarded to the standby CSM where the packets will be dropped.

  Workaround: Turn off connection replication for the FTP virtual server.

- CSCec84034

  The CSM might not replicate the sticky entries for sticky group zero configured under the virtual server. Because of the configuration download order, the active and standby CSM may be assigned a different group number when the group was not specified in the configuration.

  Workaround: Configure a sticky group with a specific number, and assign it to the virtual server.

- CSCec55790

  When using Cisco IOS Release 12.1(19)E or later with CSM 3.1(x) software, the current sticky timeout is displayed as zero for all sticky entries, and the total entries count (CurrCount) for each sticky is also displayed as zero. These counters are supported only in the CSM software release 3.2(1).

  Workaround: Use the corresponding Cisco IOS Release 12.1(13)E, which displays the configured timeout instead of the current timeout.

- CCSCdz61644

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

  Workaround: None.

- CSCdz50182

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

  Workaround: None.

- CSCdz12163

  The CSM drops packets because the multilayer switch (MLS) module 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 Catalyst 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 that the module is faulty when it should be displayed as "Other."

  Workaround: None.

- CSCdy79826

  When Internet Group Management Protocol (IGMP) snooping is enabled on the Catalyst 6500 series switch, some CSM connection replication frames might be dropped.

  Workaround: Disable IGMP snooping on both the active and standby CSM modules. 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 one 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 using the **socket** command with the -**async** option.

  b. Avoid using 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 user is configuring probe "FOO," the configuration will be corrupted.

  Workaround: Ensure that multiple users do not simultaneously modify the CSM configuration with different object types.

- CSCdx73636

  Some FTP connections may not replicate. For example, an FTP connection through an active CSM is not replicated if no data channel has been set up 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 Software Release 3.1(6)

Note For a description of caveats open in CSM software release 3.1(6), see the "Open Caveats in Software Release 3.1(6)" section on page 35.

This section describes the caveats resolved in CSM software release 3.1(6).

- CSCec87250

  When setting the environment variable HTTP_CASE_SENSITIVE_MATCHING to zero, the CSM converts all configured URL, header, and cookie maps to lowercase when matching them with the incoming requests. The CSM does not convert the cookie sticky name in this case. If you configure the cookie sticky with an uppercase name, it will not match any incoming request, and the cookie sticky will not work.

  Workaround: When setting HTTP_CASE_SENSITIVE_MATCHING to zero, you must configure the HTTP cookie sticky name in lowercase letters.

- CSCec72431

  In Cisco IOS software Release 12.2(17a)SX or later, the downloading order for the fault-tolerant (FT) configurations to the CSM moved to the beginning of the download. In this setup, the prior CSM software releases were not able to calculate configuration parity between the active and standby CSMs. The result was that the fault-tolerant status of the "configuration is out-of-sync" message is unreliable. Disregard this status, and perform a manual comparison of the configurations on the active and standby CSMs.

  Workaround: Use the older releases of Cisco IOS software or update to CSM software release 3.1(6) or later.

- CSCec70074

  If you use the XML interface to configure the CSM, the CSM may reboot if the client XML made a modification request to an unknown server farm name.

  Workaround: Ensure that the client XML can make a configuration change to a configured server farm only.

- CSCec08598

  When the active CSM makes a switchover following the route processor (RP) failover, the route health injection (RHI) static routes in the chassis are not removed until 50 seconds later. This delay prevents the newly active CSM, located in another chassis, from receiving incoming requests. CSM software release 3.1(5) includes the tracking of redundant RP switchover with a configurable variable SWITCHOVER_RP_ACTION.

  Workaround: None.

- CSCea69875

  A bad IP checksum packet could bypass the Catalyst switch check and enter the CSM. A bad IP packet could put the CSM into a non-functional state, causing it to drop all load-balancing traffic. Health probe and bridging traffic would continue to function properly in this case. CSM software release 3.1(4) includes a fix for this problem. However, this fix resolved only some of the load-balancing requests. The fix in CSM software release 3.1(6) should resolve all load-balancing traffic.

  Workaround: None.

Open Caveats in Software Release 3.1(5)

Note For a description of caveats resolved in CSM software release 3.1(5), see the "Resolved Caveats in Software Release 3.1(5)" section on page 43.

This section describes known limitations that exist in CSM software release 3.1(5).

- CSCec55790

  When using Cisco IOS Release 12.1(19)E or later with CSM software release, 3.1(x) the current sticky timeout is displayed as zero for all sticky entries, and the total entries count (CurrCount) for each sticky is also displayed as zero. These counters are supported only in the CSM software release, 3.2(1).

  Workaround: Use the corresponding Cisco IOS Release 12.1(13)E, which displays the configured timeout instead of the current timeout.

- CCSCdz61644

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

  Workaround: None.

- CSCdz50182

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

  Workaround: None.

- CSCdz12163

  The CSM drops packets because the multilayer switch (MLS) module 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 that the module is faulty when it should be displayed as "Other."

  Workaround: None.

- CSCdy79826

  When Internet Group Management Protocol (IGMP) snooping is enabled on the Catalyst 6500 series switch, some CSM connection replication frames might be dropped.

  Workaround: Disable IGMP snooping on both the active and standby CSM modules. 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 one 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 using the **socket** command with the -**async** option.

  b. Avoid using 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 user is configuring probe "FOO," the configuration will be corrupted.

  Workaround: Ensure that multiple users do not simultaneously modify the CSM configuration with different object types.

- CSCdx73636

  Some FTP connections may not replicate. For example, an FTP connection through an active CSM is not replicated if no data channel has been set up 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 Software Release 3.1(5)

Note For a description of caveats open in CSM software release 3.1(5), see the "Open Caveats in Software Release 3.1(5)" section on page 39.

This section describes the caveats resolved in CSM software release 3.1(5).

- CSCec35401

  When forwarding traffic to a destination, the CSM does not preserve the ToS field in the packets. The CSM must respect the TRUST_DSCP configuration on the Catalyst 6500 switch.

  Workaround: Configure the specific differentiated service code point (DSCP) value on each virtual server.

- SCec29347

  When you configure the CSM as the final destination for another Global Server Load Balancing (GSLB) device, the GSLB device can use keepalive application process (KAL-AP) probe to check for the health of a virtual IP address (VIP) in the CSM. This probe is destined to the CSM through the alias IP address. However, the CSM incorrectly responds to the probe using the VLAN IP address, causing the GSLB to ignore the reply from CSM.

  Workaround: None.

- CSCec21143

  When a VLAN interface is removed from the CSM, some of the host entries within the subnet are still in the ARP table of the CSM. The CSM must clean up its ARP table when you remove an IP subnet.

  Workaround: None.

- CSCec17979 and CSCdy80501

  An FTP connection cannot be established if the virtual IP address overlaps with a configured client NAT pool IP address. Even if the FTP virtual server is not using this client NAT, the FTP command cannot pass through the CSM.

  Workaround: Remove any NAT pool containing the IP address that is overlapping with the virtual IP address of an FTP service.

- CSCec13204

  The CSM fails when it is presented with a fragmented UDP packet with no UDP ports, and the IP addresses and IP identification hash to a specific value.

  Workaround: None.

- CSCec12630

  When the CSM rebalances the subsequent request of an HTTP persistent connection, it sends the default maximum session server (MSS) value of 1460 to the new server; however, the CSM should send the MSS value sent by the client in the original SYN packet.

  Workaround: None.

- CSCec09135

  The predictor round-robin feature does recognize all of the different weight values configured for the real server. In CSM software release 3.1(4), the CSM used only the simple round-robin method, with all the real server weights being equal. This feature was broken in CSM software release 3.1(4) only.

  Workaround: None.

- CSCec09012

  When you enter configuration mode to remove a server farm from service, the event is logged in the system log (syslog). When you place a server farm in service using the **inservice** command, this event is not logged into the syslog, causing service monitoring alarms to occur and never become reset.

  Workaround: None.

- CSCec03156

  The **tftp core_dump** *ip-addr* command is added to the CSM prompt when you session into the module. This command allows you to copy the full core-dump file to an external TFTP server.

  Workaround: To access this command you must enter into CSM debug prompt using the **debug module csm** command.

- CSCeb86683 and CSCdz53839

  The standby CSM sometimes sees the ARP responses for a gateway on the opposite VLAN in the bridged mode. This situation causes the standby CSM to repeatedly report that the MAC address of a gateway is changing.

  This problem occurs only if the bridge device was stripping the padding bytes from the ARP response when it flooded the packet from the active CSM port to the standby CSM port. When the bridge device correctly learned the destination MAC address, the ARP response was not flooded.

  Workaround: None.

- CSCeb80844

  If you configure the HTTP redirect string with more than 22 characters, the HTTP redirect traffic might cause the CSM to fail.

  Workaround: Use a redirect string smaller than 22 characters.

- CSCeb72016

  When the CSM receives a finished (FIN) packet from either a client or a server, the CSM places the flow in a quick idle timer of 8 seconds. This action can cause a problem if an external device intended to leave this connection in the half termination state because of its association with another connection. The CSM should provide only a quick idle timer when it receives the FIN packet from both directions. The CSM should provide only a quick idle timer when one FIN packet is received for the configured unidirectional virtual servers.

  Workaround: None.

- CSCeb69592

  The CSM incorrectly terminates an FTP connection if the data transfer command for this connection takes longer than 15 minutes.

  Workaround: None.

- CSCeb60981

  The CSM could fail to respond if you remove a real server from a server farm when a scripted probe is configured and running.

  Workaround: Configure a real server as out-of-service instead of removing it, or remove the scripted probe for that server farm before removing the real server.

- CSCeb55530

  The CSM does not forward the ICMP unreachable messages from the router to the intended server when the Maximum Transmission Unit (MTU) is exceeded. This problem exists in CSM software release 3.1(3) and software release 3.1(4) only.

  Workaround: None.

- CSCeb50227

  The CSM generates few random source MAC addresses into VLAN 1 when there is a high volume of traffic forwarded across the configured bridge VLANs. Over time, this situation could cause an overflow of the MAC address table in the Catalyst switch chassis.

  Workaround: Configure a faster timeout for bridge entries, or configure the virtual server to load-balance this traffic.

- CSCea78134

  In previous releases, the CSM was unable to forward jumbo frames. In CSM software release 3.1(5), a jumbo frame up to 9,216 bytes can be forwarded by the CSM to the peer bridge VLAN. A jumbo frame can also be forwarded to it destination if it matched an existing Layer 4 connection. In a switch running both Cisco IOS software and the Catalyst operating system, you must enable jumbo frame for the CSM internal ports.

  Workaround: None.

- CSCea33676

  The CSM incorrectly stamped the differentiated-services-code-point (DSCP) bits in the least significant bits of the TCP type of service (ToS) byte. The DSCP configuration value of 0 to 63 should be placed in the highest bits.

  Workaround: None.

- CSCdz84503

  In previous releases, the CSM counted all traffic received from a route VLAN that did not match any configured virtual server. This traffic was counted as “server-initiated” connections. In CSM software release 3.1(5), the CSM counts only those connections coming from the configured real servers as server-initiated connections. Other connections are rejected and are counted as “no policy configured” connections.

  Workaround: None.

- CSCdz18550

  When you remove the route for a routed keepalive application process (KAL-AP) probe on a DNS-VIP, the probe always considers the DNS-VIP to be out of service. The probe stays in the failed state even if this route is returned to service.

  Workaround: Take the DNS-VIP (the real server of a DNS-VIP server farm) out of the server farm, and then replace it to the server farm.

- CSCdz01238

  The CSM sends out health checks for the server that was configured to out of service when you configure a keepalive probe into a server farm. This situation causes unnecessary traffic on the network and the CSM.

  Workaround: Remove the real server from the server farm.

Open Caveats in Software Release 3.1(4)

Note For a description of caveats resolved in CSM software release 3.1(4), see the "Resolved Caveats in Software Release 3.1(4)" section on page 49.

This section describes known limitations that exist in CSM software release 3.1(4).

- CSCdz61644

  The following 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.

- 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: In release 3.1(2) or later, you can set the CSM variable "ARP_LEARN_MODE" to zero (0) to prevent the CSM from learning the ARP that is not destined for the CSM.

- CSCdz50182

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

  Workaround: None.

- CSCdz12163

  The CSM drops packets because the multilayer switch (MLS) module 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 that the module is 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 might be dropped.

  Workaround: Disable IGMP snooping on both the active and standby CSM modules. 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 one 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 using the **socket** command with the -**async** option.

  b. Avoid using 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 user is configuring probe "FOO," the configuration will be corrupted.

  Workaround: Ensure that multiple users do not simultaneously modify the CSM configuration with different object types.

- CSCdx73636

  Some FTP connections may not replicate. For example, an FTP connection through an active CSM is not replicated if no data channel has been set up 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 Software Release 3.1(4)

Note For a description of caveats open in CSM software release 3.1(4), see the "Open Caveats in Software Release 3.1(4)" section on page 46.

This section describes the caveats resolved in CSM software release 3.1(4).

- CSCeb55339

  The CSM may crash if it received a bad format ICMP "destination unreachable" type 3/4 message (fragmentation required with the do not fragment bit set) from the router.

  Workaround: None.

- CSCeb42816

  The CSM was incorrectly timing out the FTP connection after 15 minutes without a new FTP command. This behavior is a problem for a file transfer command that lasted more than 15 minutes.

  Workaround: None.

- CSCeb37764

  If you configured the "port" number for an HTTP probe object, the operational state of the "real" server in the Global Server Load Balanced (GSLB) serverfarm does not change, even if the probe has failed. This problem occurs only with GSLB policy.

  Workaround: Do not configure the port number in the HTTP probe for GSLB service.

- CSCeb36142

  The CSM responds to the ARP request for a virtual IP address (VIP) whether or not the virtual server was configured as "inservice." This behavior is changed in release 3.1(4) and later releases. Previously you had to configure "variable ARP_REPLY_FOR_NO_INSERVICE_VIP 1" to maintain this behavior.

  Workaround: None.

- CSCeb32529

  When processing connections to a layer 7 virtual server, by default the CSM replies with a SYN-ACK and Maximum Segment Size (MSS) value of 1460. You can change this setting by configuring the environment variable "TCP_MSS_OPTION" to another value. When the CSM does not have to parse any HTTP or SSL information, the MSS value is correctly passed between the client and the server.

  Workaround: None.

- CSCeb16899

  The **show module csm** *slot* **connection** command always displays the state of an FTP data connection as "CLOSING." This connection is set up by the CSM. The state of these connections should be "ESTAB."

  Workaround: None.

- CSCeb02303

  The CSM marks the HTTP probe as failed if the server does not send the FIN reply after the CSM completes the HTTP keepalive request. The problem occurred because the CSM set the request to HTTP 1.1 and expected a close request from the server.

  Workaround: None.

- CSCea93947

  In hybrid systems (running Cisco IOS and the Catalyst operating system software) in a fault tolerant configuration with a CSM in separate switch chassis, reloading the MSFC in one chassis may cause the active CSM to show that the configuration is out of synchronization with the standby CSM on the other chassis.

  Workaround: None.

- CSCea89687

  The keepalive probes on the standby CSM fail if connections are replicating from the active to the standby module. This problem occurs because the CSM was incorrectly set up with ARP entries for IP addresses in replicated connections that were not directly connected to the CSM VLAN.

  Workaround: None.

- CSCea88822

  In hybrid systems (running Cisco IOS and the Catalyst operating system software) with redundant CSMs, the standby CSM on the same chassis may incorrectly clear the ARP entries when only the MSFC failed or rebooted. This condition prevents the connections destined for certain servers from replicating correctly to the standby CSM.

  Workaround: Reboot the standby CSM if the MSFC in the same chassis was rebooted.

- CSCea87073

  In hybrid systems (running Cisco IOS and the Catalyst operating system software) with redundant CSMs, the MSFC could independently fail with the Catalyst operating system continuing to run. When only the MSFC failed or rebooted, the active CSM on the same chassis incorrectly reset (RST) all the existing connections before entering the standby state. The standby CSM lost all of the replicated connections before it become the active CSM.

  Workaround: None.

- CSCea78185

  When a high volume of RTSP connections pass through the virtual servers with the “service rtsp” option configured, the CSM may fail and reboot.

  Workaround: Remove the “service rtsp” option from the virtual server.

- CSCea69875

  When a packet with an invalid IP header enters the CSM, the module state may change so that the module no longer forwards load-balanced traffic. When the CSM enters such a state, the keepalive traffic and packets that are forwarded to other VLANs are not affected. Only the traffic destined for load balancing fails. The IP checksum value for this type of packet will not be correct. In most cases, the routers drop and do not forward this type of packet to the CSM.

  Workaround: Reboot the CSM module to reset the state.

- CSCdz63514

  The **clear module csm** *slot* **counters** command does not clear the counters for the fault tolerance (FT) statistics.

  Workaround: None.

- CSCdz34419

  The **clear module csm** *slot* **conns vserver** *name* does not work for a virtual server configured as out-of-service.

  Workaround: Configure the virtual server to “inservice” before using the **clear** command.

- CSCdz22187

  By default, the operational state of the backup serverfarm is not used by the virtual server associated with the primary and backup serverfarms. If all the servers in the primary serverfarm are disabled, then the virtual server is recognized as out-of-service.

  You can change this behavior by setting the environment variable “AGGREGATE_BACKUP_SF_STATE_TO_VS” which causes the operational state of a virtual server to depend on both the primary and backup serverfarms.

  Workaround: None.

- CSCdy87727

  Statistics on the standby CSM show the connections counter per real server as zero because the CSM does not count any connection replicated from the active CSM to the real server.

  Workaround: None.

- CSCdy44454

  Software release 3.1(4) supports the "failaction reassign" option for firewall load balancing (FWLB). The CSM reassigns existing connections from a failed firewall to another operating firewall. To be reassigned, the firewalls must have the connection state replication feature. The configuration for this option requires the Cisco IOS Release 12.1(19)E or higher.

  Workaround: None.

- CSCdy00154

  When the fault tolerance (FT) heartbeat traffic between the active and standby CSMs stops, the CSM pair goes into an active-active condition. When the fault-tolerant traffic is restored, the CSM pair cannot determine which CSM was previously active before the interruption.

  The standby module configured previously with a higher fault-tolerant priority takes over as the active CSM which is undesirable. CSM software release 3.1(4) allows the previously active CSM to become active again, regardless of the priority setting.

  Workaround: Set the current active CSM to a higher priority setting.

Open Caveats in Software Release 3.1(3)

Note For a description of caveats resolved in CSM software release 3.1(3), see the "Resolved Caveats in Software Release 3.1(3)" section on page 56.

This section describes known limitations that exist in CSM software release 3.1(3).

- CSCea69875

  When a packet with an invalid IP header enters the CSM, the module state may change so that the module no longer forwards load-balanced traffic. When the CSM enters such a state, the keep-alive traffic and packets that are forwarded to other VLANs are not affected. Only the traffic destined for load balancing stops working. The IP checksum value for this type of packet will not be correct. In most cases, the routers drop and do not forward this type of packet to the CSM.

  Workaround: Reboot the CSM module to reset the state.

- 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.

- 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: In release 3.1(2) or later, you can set the CSM variable "ARP_LEARN_MODE" to zero (0) to prevent the CSM from learning the ARP that is not destined for the CSM.

- 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.

- 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 Software Release 3.1(3)

Note For a description of caveats open in CSM software release 3.1(3), see the "Open Caveats in Software Release 3.1(3)" section on page 52.

This section describes the caveats resolved in CSM software release 3.1(3).

- CSCea55496

  The CSM mishandles an HTTP response from the server, which causes the module to fail and reboot. The following conditions cause this problem to occur:

  a. The CSM received and processed an HTTP header that spanned multiple packets.

  b. The server responded with data but did not acknowledge (ACK) the HTTP request packets sent by the CSM.

  Workaround: None.

- CSCea50526

  The CSM does not set up the real time streaming protocol (RTSP) data channels correctly when the client and server negotiated to have more than one channel open. In this case, the CSM incorrectly swapped the client and server ports. As a result, all RTSP data traffic is either dropped by the CSM or forwarded without the proper NAT information.

  Workaround: Set the RTSP protocol in the server to allow only one data channel port per RTSP connection.

- CSCea49197

  When the traffic from the FTP control channel (port 21) exceeds the limit of 500 packets per second, the CSM may leave additional connections open indefinitely. In this case, the session resources should be recovered. There is a total of one million possible sessions allowed per CSM module.

  Workaround: Reboot the CSM when the number of opened connections is close to one million.

- CSCea48270

  When processing the FTP service, the CSM may fail. This problem occurs when the client or server used a corrupt packet ID in the IP header within the control traffic of an FTP session.

  Workaround: None.

- CSCea42966

  When configured with bridging VLANs and fault tolerance, the CSM might not send gratuitous ARP requests for the real servers after the standby CSM becomes active. As a result, the connection requests from the client to the real server IP and MAC address do not go through immediately. The traffic resumes when the bridge table times out on the client or the ARP table times out on the client or the server side of the transaction.

  Workaround: None.

- CSCea40604

  The CSM might not send out the reset (RST) packets when it closes connections when a server goes down. The CSM clears the connections when a "failaction purge" option is configured into the serverfarm.

  Workaround: Close and reopen the browser to establish a new connection.

- CSCea30762

  The CSM checks the operational status of a virtual IP (VIP) address before it responds to an ICMP request to the VIP. When there are multiple virtual servers with the same VIP address, the CSM does not check the status of all of the virtual servers. If one of the virtual servers is not functioning, the CSM will incorrectly ignore the ICMP request.

  Workaround: Set the global variable in the CSM release 3.1(1a) or later to always respond to the ICMP request.

- CSCea30620

  The CSM might begin inserting and removing route health injection (RHI) routes multiple times for the same VIP when the virtual server first becomes operational, affecting operation on the distance routers for approximately two minutes.

  Workaround: Use software releases with a stable RHI feature: Cisco IOS Release 12.1(13)E and CSM software release 3.1(3).

- CSCea30485

  The CLI for the CSM in Cisco IOS Release 12.1(13)E does not allow you to configure the max-parse-len section of an HTTP request longer than 4000 bytes. In CSM software release 3.1(3), the CSM supports a global variable "MAX_PARSE_LEN_MULTIPLER," which increases the configured max-parse-len value by the value of this variable.

  Workaround: None.

- CSCea24282

  In CSM software release 2.2(x), there were resource leaks when the number of opened FTP connections went above 47,000. This high connection rate caused the CSM to run out of resources to process further FTP traffic. Rebooting the CSM was required to reclaim the resources.

  Workaround: None.

- CSCea22951

  The CSM incorrectly processes the IP sticky configuration option when only the Return Code map is configured for that virtual server. This problem does not occur if other matching rules (ACL, URL, Cookie, etc.) are configured for that virtual server.

  Workaround: Configure the client access list with the value of **catch all "client 0.0.0.0/0"** for the virtual server.

- CSCea21685

  The CSM drops part of an HTTP POST request when the request spans multiple packets. The CSM drops the subsequent packet when it receives the synchronize-acknowledge (SYN-ACK) packet from the server at that same time.

  Workaround: None.

- CSCea02255

  The CSM processes any TCP connection requests on its interfaces, even those with a destination MAC that are not for the CSM. If the switch floods the synchronize (SYN) packet to all bridged ports, this flooding causes the CSM to incorrectly reset or load balance the connections that were not destined for it.

  Workaround: The bridge device should only send the packets to the port where the corresponding destination MAC address exists.

- CSCea19719

  While parsing the HTTP response from the server, the CSM may crash if the response packet from the server is padded with additional bytes at the MAC layer. The problem only occurs when the CSM has to parse the server response for Cookie Sticky or Return Code requests.

  Workaround: None.

- CSCdz34419

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

  Workaround: Enter the **clear** command with a specific real server IP address.

- CSCdz12590

  The CSM might leave the FTP connections in the closed state because the module did not receive the finished (FIN) packet for the FTP connections. The **clear module csm** *slot* **conn** command might be unable to clear these connections.

  Workaround: These FTP connections will be closed by the idle timer in the CSM.

- CSCdy62222

  Under certain conditions, the CSM is unable to process and count the HTTP Return Code from the server as configured. When the server (or client) sends a finished (FIN) packet immediately after the server sends the HTTP response, the CSM does not process the Return Code for this connection.

  Workaround: The timing is much longer in a production network because of heavier traffic, so the above condition is unlikely to occur.

- CSCdy30354

  In CSM releases 3.1(1a) and 3.1(2), the CSM sometimes will not reboot the system when the CSM fails due to a server error.

  Workaround: Manually reset the CSM module.

- 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. This caveat applies only to Cisco IOS releases previous to 12.1(13)E3.

Open Caveats in Software Release 3.1(2)

Note For a description of caveats resolved in CSM software release 3.1(2), see the "Resolved Caveats in Software Release 3.1(2)" section on page 62.

This section describes known limitations that exist in CSM software release 3.1(2).

- 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.

- 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 Software Release 3.1(2)

Note For a description of caveats open in CSM software release 3.1(2), see the "Open Caveats in Software Release 3.1(2)" section on page 58.

- CSCdz87286

  When enabling "persistent rebalancing" for a particular virtual server, the CSM examines every GET of the HTTP 1.1 persistent connection so that it can redirect the request to the correct serverfarm. If the subsequent GET request spans multiple packets and is intended for the same server as the previous GET request, then the CSM is not able to forward the reply back to the client.

  Workaround: Remove the "persistent rebalancing" option from the virtual server.

- CSCdy83794

  The "slot0:" option in the **upgrade** command for the CSM is referencing the MSFC on the active supervisor slot. In CSM release 3.1(2), this option is referencing the active MSFC.

  Workaround: Use the MSFC on the same module as the active supervisor. Use the option "127.0.0.12" (for MSFC on slot 1) or "127.0.0.22" (for MSFC on slot 2) instead of using the "slot0:" option.

- CSCdz81886

  CSM release 3.1(1a) has the problem handling IP fragmented packets. While processing many out-of-order UDP fragments, the CSM can lock up and stop processing all traffic.

  Workaround: None.

- CSCdz60699

  The CSM does not support the non-standard extension in the RTSP message. When the user enables the “service rtsp” for a virtual server, the CSM has to process the RTSP message to set up the peer flows. Any RTSP message with a non-standard extension option sent through this VIP causes the CSM to fail.

  Workaround: Remove the option “service rtsp” for the virtual server.

- CSCdz56924

  In CSM release 3.1(2), the CSM optimizes the use of client NAT pools with multiple IP addresses. The CSM uses the client source port number in determining the corresponding client NAT IP address. This enhancement minimizes the TCP “timewait” port reused condition, causing the server to reject the connection.

  Workaround: None.

- 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 the CSM.

  Workaround: None.

- CSCdz47531

  In CSM release 3.1(2), the CSM supports non-standard HTTP requests from the Wireless Application Protocol (WAP) devices.

  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.

- CSCdz38938

  When one of the firewalls fails the ARP request, the ICMP health probe to other servers or firewalls may drop the ICMP reply. If the number of probe “retries” is small, 60 or less, 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 CSM 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.

- CSCdz25353

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

  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.

- CSCdz17645

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

  Workaround: None

- CSCdy44301

  Using the CSM 3.1(2) release with Cisco IOS Release 12.1(13)E3 causes the CSM to generate SNMP traps when you remove a virtual server from service.

  Workaround: None.

- 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 Software Release 3.1(1a)

Note For a description of caveats resolved in CSM software release 3.1(1a), see the "Resolved Caveats in Software Release 3.1(1a)" section on page 67.

This section describes known limitations that exist in CSM software release 3.1(1a).

- CSCdy80501

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

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

- CSCdy79826

  When 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 CSMs.

  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 to be replicated 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 only occurs 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. This caveat applies only to Cisco IOS releases previous to 12.1(13)E3.

- CSCdx73636

  Some FTP connections may not be replicated. An FTP connection through an active CSM will not be replicated if no data channel has ever 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(1a) 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 to interleaved mode (inline TCP). This mode will work in the application software, although the connection is sent to fastpath.

  Workaround: None

- 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.

- 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 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.

Resolved Caveats in Software Release 3.1(1a)

Note For a description of caveats open in CSM software release 3.1(1a), see the "Open Caveats in Software Release 3.1(1a)" section on page 64.

Because CSM software release 3.1(1a) is the first release in a new release train. There are no resolved caveats in this release.

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.

XML Errors

When an untolerated XML error occurs, the HTTP response contains a 200 code. The portion of the original XML document with the error is returned with an error element that contains the error type and description.

This example shows an error response to a condition where a virtual server name is missing:

```
      <?xml version="1.0"?>
      <config>
       <csm_module slot="4">
        <vserver>
         <error code="0x20">Missing attribute name in element

vserver</error>
        </vserver>
       </csm_module>
      </config>
```

The error codes returned also correspond to the bits of the error tolerance attribute of the configuration element. Returned XML error codes are:

```
XML_ERR_INTERNAL          = 0x0001,
XML_ERR_COMM_FAILURE      = 0x0002,
XML_ERR_WELLFORMEDNESS    = 0x0004,
XML_ERR_ATTR_UNRECOGNIZED = 0x0008,
XML_ERR_ATTR_INVALID      = 0x0010,
XML_ERR_ATTR_MISSING      = 0x0020,
XML_ERR_ELEM_UNRECOGNIZED = 0x0040,
XML_ERR_ELEM_INVALID      = 0x0080,
XML_ERR_ELEM_MISSING      = 0x0100,
XML_ERR_ELEM_CONTEXT      = 0x0200,
XML_ERR_IOS_PARSER        = 0x0400,
XML_ERR_IOS_MODULE_IN_USE = 0x0800,
XML_ERR_IOS_WRONG_MODULE  = 0x1000,
XML_ERR_IOS_CONFIG        = 0x2000
```

The default error_tolerance value is 0x48, which corresponds to ignoring unrecognized attributes and elements.

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 documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain 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 at this URL:

http://www.cisco.com/cisco/web/psa/default.html?mode=prod

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/web/siteassets/locator/index.html

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/web/ordering/root/index.html

Cisco Marketplace:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/web/ordering/root/index.html

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/web/ordering/root/index.html

- 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 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation 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.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

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

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

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

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

http://www.cisco.com/cisco/web/support/index.html

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

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

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request 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 list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/en/US/support/tsd_contact_technical_support.html

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—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.

Severity 2 (S2)—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.

Severity 3 (S3)—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.

Severity 4 (S4)—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.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/web/about/ac123/ac114/about_cisco_packet_magazine.html

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions.

- *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/web/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/web/learning/index.html

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