Release Notes for Catalyst 6500 Series Content Switching Module Software Release 4.2(x)

Current Release: 4.2(15) —January 27, 2012
Previous releases: 4.2(14), 4.2(13), 4.2 (12), 4.2(11), 4.2(10), 4.2(9), 4.2(8), 4.2(7), 4.2(6), 4.2(5), 4.2(4), 4.2(3a), 4.2(3)–Deferred, 4.2(2), 4.2(1)

This publication describes the features, modifications, and caveats for the Catalyst 6500 series Content Switching Module (CSM), software release 4.2(x), operating on the following platforms:

- Catalyst 6500 series switch with a Supervisor Engine 2 with MSFC2 and Cisco IOS Release 12.1(8a)EX or higher.
- Supervisor Engine 720 and Cisco IOS Release 12.2(14)SX1 or higher.
- Supervisor Engine 720-10G and Cisco IOS Release 12.2(33)SXI2 or higher.

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

Contents

Americas 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 4.2(x).

Memory Requirements

The Catalyst 6500 series CSM memory is not configurable.

Hardware Supported

Before you can use the Catalyst 6500 series CSM, you must have a Supervisor Engine 1A with a Multilayer Switch Feature Card (MSFC) or MSFC2, a Supervisor Engine 2 with an MSFC2, or a Supervisor Engine 720 with an MSFC3, and a module with ports to connect server and client networks. The PFC is required for the VLAN access control list (VACL) capture functionality.

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

Product Number	Minimum[1] Cisco IOS Software	Recommended[2] Cisco IOS Software	Minimum Catalyst Operating System Software	Recommended Catalyst Operating System Software
Content Switching Module (WS-X6066-SLB-APC)				
Supervisor Engine 1A and MSFC1 or MSFC2	12.1(8a)EX	12.2(18)SXF15	Cisco IOS Release 12.1(13)E3 with Catalyst operating system software 7.5	Cisco IOS Release 12.2(18)SXF16 with Catalyst operating system software 7.5
Supervisor Engine 2 with MSFC2	12.1(8a)EX or 12.2(17d)SXB	12.2(18)SXF15	Cisco IOS Release 12.1(13)E3 with Catalyst operating system software 7.5	Cisco IOS Release 12.2(18)SXF16 with Catalyst operating system software 7.5
Supervisor Engine 720 with MSFC3	12.2(14)SX1	12.2(18)SXF15	Cisco IOS Release 12.2(14)SX2 with Catalyst operating system software 8.2(1)	Cisco IOS Release 12.2(18)SXF16 with Catalyst operating system software 8.2(1)
Supervisor Engine 720-10G	12.2(33)SXI2	12.2(33)SXI2	Not supported	Not supported
Console Cable				
72-876-01		Not applicable		Not applicable

Product Number	Minimum[1] Cisco IOS Software	Recommended[2] Cisco IOS Software	Minimum Catalyst Operating System Software	Recommended Catalyst Operating System Software
Accessory Kit				
800-05097-01		Not applicable		Not applicable

[1] The minimum software release required to support the CSM hardware with a given Supervisor Engine to perform basic CSM configuration.

[2] The base software release required to support new commands for a given CSM release.

Note Back-end encryption requires Cisco IOS Software Release 12.2(17d)SXB for the Supervisor Engine 2 or Cisco IOS Software Release 12.2(17b)SXA for the Supervisor Engine 720.

Software Compatibility

The minimum release that is listed is required to support the CSM hardware with a given supervisor engine to perform basic CSM configuration.

We recommend the base release to support new commands for a given CSM release.

Note Support for the CSM is removed in Cisco IOS Software Release 12.2(33)SXH and later releases up to Release 12.2(33)SXI. The support for the CSM is reenabled in Cisco IOS Software Release 12.2(33)SXI2.

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

Table 1 Cisco IOS Software on the Supervisor Engine and MSFC

CSM Release	Supervisor Engine 1 MSFC1 or MSFC2		Supervisor Engine 2 with MSFC2		Supervisor Engine 720 with MSFC 3	
	Minimum[1] Software Release	Recommended[2] Software Release	Minimum Software Release	Recommended Software Release	Minimum Software Release	Recommended Software Release
4.2(15)	12.1(8a)EX	12.2(18)SXF15	12.1(8a)EX	12.2(18)SXF15	12.2(14)SX1	12.2(18)SXF15
4.2(14)	12.1(8a)EX	12.2(18)SXF15	12.1(8a)EX	12.2(18)SXF15	12.2(14)SX1	12.2(18)SXF15
4.2(13)	12.1(8a)EX	12.2(18)SXF15	12.1(8a)EX	12.2(18)SXF15	12.2(14)SX1	12.2(18)SXF15
4.2(12)	12.1(8a)EX	12.2(18)SXF15	12.1(8a)EX	12.2(18)SXF15	12.2(14)SX1	12.2(18)SXF15
4.2(11)	12.1(8a)EX	12.2(18)SXF15	12.1(8a)EX	12.2(18)SXF15	12.2(14)SX1	12.2(18)SXF15
4.2(10)	12.1(8a)EX	12.2(18)SXF15	12.1(8a)EX	12.2(18)SXF15	12.2(14)SX1	12.2(18)SXF15
4.2(9)	12.1(8a)EX	12.2(18)SXF15	12.1(8a)EX	12.2(18)SXF15	12.2(14)SX1	12.2(18)SXF15
4.2(8)	12.1(8a)EX	12.2(18)SXF15	12.1(8a)EX	12.2(18)SXF15	12.2(14)SX1	12.2(18)SXF15
4.2(7)	12.1(8a)EX	12.2(18)SXF15	12.1(8a)EX	12.2(18)SXF15	12.2(14)SX1	12.2(18)SXF15
4.2(6)	12.1(8a)EX	12.2(18)SXF15	12.1(8a)EX	12.2(18)SXF15	12.2(14)SX1	12.2(18)SXF15
4.2(5)	12.1(8a)EX	12.2(18)SXF15	12.1(8a)EX	12.2(18)SXF15	12.2(14)SX1	12.2(18)SXF15
4.2(4)	12.1(8a)EX	12.2(18)SXF15	12.1(8a)EX	12.2(18)SXF15	12.2(14)SX1	12.2(18)SXF15

Table 1 Cisco IOS Software on the Supervisor Engine and MSFC (continued)

CSM Release	Supervisor Engine 1 MSFC1 or MSFC2		Supervisor Engine 2 with MSFC2		Supervisor Engine 720 with MSFC 3	
4.2(3a)	12.1(8a)EX	12.2(18)SXF15	12.1(8a)EX	12.2(18)SXF15	12.2(14)SX1	12.2(18)SXF15
4.2(3)	12.1(8a)EX	12.2(18)SXF15	12.1(8a)EX	12.2(18)SXF15	12.2(14)SX1	12.2(18)SXF15
4.2(2)	12.1(8a)EX	12.2(18)SXF15	12.1(8a)EX	12.2(18)SXF15	12.2(14)SX1	12.2(18)SXF15
4.2(1)	12.1(8a)EX	12.2(18)SXF15	12.1(8a)EX	12.2(18)SXF15	12.2(14)SX1	12.2(18)SXF15

[1] The minimum software release required to support the CSM hardware with a given Supervisor Engine to perform basic CSM configuration.

[2] The base software release required to support new commands for a given CSM release.

Table 2 Cisco IOS Software on the MSFC and Catalyst Operating System Software on the Supervisor Engine

CSM Release	Supervisor Engine 1 MSFC1 or MSFC2		Supervisor Engine 2 with MSFC2		Supervisor Engine 720 with MSFC 3	
	Minimum[1] Software Release	Recommended[2] Software Release	Minimum Software Release	Recommended Software Release	Minimum Software Release	Recommended Software Release
4.2(15)	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.2(14)SX2 with 8.2(1)	12.2(18)SXE with 8.2(1)
4.2(14)	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.2(14)SX2 with 8.2(1)	12.2(18)SXE with 8.2(1)
4.2(13)	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.2(14)SX2 with 8.2(1)	12.2(18)SXE with 8.2(1)
4.2(12)	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.2(14)SX2 with 8.2(1)	12.2(18)SXE with 8.2(1)
4.2(11)	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.2(14)SX2 with 8.2(1)	12.2(18)SXE with 8.2(1)
4.2(10)	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.2(14)SX2 with 8.2(1)	12.2(18)SXE with 8.2(1)
4.2(9)	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.2(14)SX2 with 8.2(1)	12.2(18)SXE with 8.2(1)
4.2(8)	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.2(14)SX2 with 8.2(1)	12.2(18)SXE with 8.2(1)
4.2(7)	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.2(14)SX2 with 8.2(1)	12.2(18)SXE with 8.2(1)
4.2(6)	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.2(14)SX2 with 8.2(1)	12.2(18)SXE with 8.2(1)
4.2(5)	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.2(14)SX2 with 8.2(1)	12.2(18)SXE with 8.2(1)
4.2(4)	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.2(14)SX2 with 8.2(1)	12.2(18)SXE with 8.2(1)
4.2(3a)	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.2(14)SX2 with 8.2(1)	12.2(18)SXE with 8.2(1)

Table 2 Cisco IOS Software on the MSFC and Catalyst Operating System Software on the Supervisor Engine (continued)

CSM Release	Supervisor Engine 1 MSFC1 or MSFC2		Supervisor Engine 2 with MSFC2		Supervisor Engine 720 with MSFC 3	
4.2(3)	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.2(14)SX2 with 8.2(1)	12.2(18)SXE with 8.2(1)
4.2(2)	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.2(14)SX2 with 8.2(1)	12.2(18)SXE with 8.2(1)
4.2(1)	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.1(13)E3 with 7.5	12.2(18)SXE with 7.5	12.2(14)SX2 with 8.2(1)	12.2(18)SXE with 8.2(1)

[1] The minimum software release required to support the CSM hardware with a given Supervisor Engine to perform basic CSM configuration.

[2] The base software release required to support new commands for a given CSM release.

New Features

Table 3 lists the features that have been added in CSM software release 4.2.

Table 3 New CSM Feature Set Description

New Features in this Release	Description
HTTP header sticky	Allows you to configure the CSM to perform stickiness based on the contents of the HTTP header (for example, the mobile station ISDN number [MSISDN], service key, session ID).
Configuration synchronization	Supports synchronizing the configuration between the active and the standby CSM over the fault-tolerant VLAN.
Failover tracking for interfaces and critical devices	Allows you to track the state of HSRP groups, physical interfaces, and gateways.
Private VLANs	Enables the use of private VLANs (PVLANs) with the CSM.
Partial server farm failover	When you configure a backup server farm, you can define threshold values so that the CSM fails over to the backup server farm if the primary server farm partially fails.
Server probe fail state improvements	Allows you to specify the number of successful retries needed to put a failed server back in service.
Real name option	Allows you to specify details about an entity. This option is applicable for probe, vserver, VLAN, and server farm modes.
NAT configuration enhancements	Provides source NAT (client) configuration rules to the policy level.
Infinite idle timeout	Allows you to keep a connection open for an indefinite time period.

Table 3 New CSM Feature Set Description (continued)

New Features in this Release	Description
VIP dependencies	Allows you to link VIPs together to automatically take a dependant VIP out of service if the specified VIP goes out of service.
Ordering of policies	Provides the ability to assign a priority value to a particular policy.
Maximum parse length reached behavior change	CSM load balances the maximum number of parse length connection requests to the default policies.
Slow start improvements	This feature allow real servers to be in slow-start mode until the slow-start timer value expires or the conn_count is equal to that of the other real servers.
Non-secure router mode	Extends the environment variable to route a SYN packet, in addition to a non-SYN packet, that does not hit a VIP.
Increase virtual server limit	Increases the number of virtual servers configurable with a particular VIP from 128 to 1000.
Remote desktop protocol	Adds an environment variable to configure MSTS-RDP[1].
HTTPS communication	Provides secure, encrypted communication with the HSE[2], SASP[3], and XML APIs.
XML **show** commands	Allows you to retrieve **show** command information for the CSM by using XML commands defined in the DTD[4] through the XML interface.

[1] MSTS-RDP = Microsoft Terminal Services Remote Desktop Protocol

[2] HSE = Hosting Solution Engine

[3] SASP = Server Application State Protocol

[4] DTD = Document Type Definition

Feature Set

Table 4 describes the CSM features and software descriptions.

Table 4 CSM Feature Set Description

Feature	First Image Release
Supported Hardware	
Supervisor 1A with MSFC and PFC	c6slb-apc.1-1-1.bin
Supervisor 2 with MSFC2	c6slb-apc.1-2-1.bin
Supervisor 720 with MSFC3	c6slb-apc.3-1-4.bin
Catalyst 6500 Series Supported Operating Systems	
Cisco IOS software	c6slb-apc.1-1-1.bin
Catalyst operating system software	c6slb-apc.2-2-7.bin c6slb-apc.3-1-2.bin
Supported Protocols	
FTP	c6slb-apc.1-1-1.bin
TCP load balancing	c6slb-apc.1-1-1.bin
UDP and all common IP protocol load balancing	c6kslb-apc.2-1-1.bin
Load balancing per packet—allows the CSC to make load balancing decisions without creating a flow, which is useful when load balancing UDP traffic with flows that exist for a short time period, such as DNS	c6slb-apc.3-2-1.bin
Real Time Streaming Protocol (RTSP)	c6slb-apc.2-2-1.bin
Server Application State Protocol (SASP)	c6slb-apc.4-1-3.bin
Layer 7 Functionality	
Full regular expression matching	c6slb-apc-1-1-1.bin
URL & cookie switching	c6slb-apc.1-1-1.bin
Generic header parsing	c6kslb-apc.2-1-1.bin
Miscellaneous Functionality	
TCP fragmentation support—allows the CSM to handle fragmented TCP packets	c6slb-apc.3-2-1.bin
Route lookup—allows the CSM to work more efficiently with upstream gateways regardless of their redundancy implementation (HSRP, VRRP, proprietary, and so on)	c6slb-apc.3-2-1.bin
Denial of Service (DoS) improvements—allows TCP termination for all connections to the CSM providing SYN attacks	c6slb-apc.3-2-1.bin
Multiple CSMs in a chassis	c6kslb-apc.2-1-1.bin
CSM and Cisco IOS-SLB functioning simultaneously in a chassis	c6kslb-apc.2-1-1.bin
HTTP 1.1 persistence (all GETs balanced to the same server)	c6slb-apc.1-1-1.bin
Full HTTP 1.1 persistence (GETs balanced to multiple servers)	c6kslb-apc.2-1-1.bin
HTTP method parsing	c6slb-apc.3-1-1.bin

Table 4 CSM Feature Set Description (continued)

Feature	First Image Release
Fully configurable NAT NAT configuration enhancements	c6kslb-apc.2-1-1.bin c6slb-apc.4-2-1.bin
Server initiated connections	c6slb-apc.1-1-1.bin
Route health injection	c6slb-apc.1-1-1.bin – requires release 12.1(7)E c6slb-apc.1-2-1.bin
Round-robin	c6slb-apc.1-1-1.bin
Weighted round-robin (WRR)	c6slb-apc.1-1-1.bin
Least connections	c6slb-apc.1-1-1.bin
Weighted least connections	c6slb-apc.1-1-1.bin
URL hashing	c6kslb-apc.2-1-1.bin
Source IP hashing	c6kslb-apc.2-1-1.bin
Destination IP hashing	c6kslb-apc.2-1-1.bin
Return error code checking	c6slb-apc.2-2-1.bin
Support for 127 VLANs Support for 255 VLANs Supports up to 511 server and client VLANs	c6slb-apc.1-1-1.bin c6slb-apc.2-2-1.bin c6slb-apc.3-2-1.bin
Jumbo frames—allows support of frames of up to 9000 bytes for Layer 4 load balancing	c6slb-apc.3-2-1.bin
Reduced time between health probes	c6slb-apc.2-2-1.bin
In-band health checking	c6slb-apc.2-2-1.bin
Configurable pending connection timeout	c6slb-apc.2-2-1.bin
IP reassembly for in-order UDP fragments	c6kslb-apc.2-1-1.bin
IP reassembly for out-of-order UDP fragments	c6slb-apc.3-1-1.bin
VIP connection watermarks	c6slb-apc.3-1-1.bin
Idle timeout for unidirectional flows Allows for the configuration of the idle and pending timeouts for server-initiated connections	c6slb-apc.3-1-1.bin c6slb-apc.3-2-1.bin
Real server names	c6slb-apc.3-1-1.bin
Slowpath performance improvements	c6slb-apc.3-1-1.bin
Real name option	c6slb-apc.4-2-1.bin
Private VLANs	c6slb-apc.4-2-1.bin
Ordering of policies	c6slb-apc.4-2-1.bin
Server probe fail state improvements	c6slb-apc.4-2-1.bin
Infinite idle timeout	c6slb-apc.4-2-1.bin
VIP dependencies	c6slb-apc.4-2-1.bin
Maximum parse length reached behavior change	c6slb-apc.4-2-1.bin

Table 4 CSM Feature Set Description (continued)

Feature	First Image Release
Slow start improvements	c6slb-apc.4-2-1.bin
Non-secure router mode	c6slb-apc.4-2-1.bin
Increase virtual server limit	c6slb-apc.4-2-1.bin
Secure XML communication	c6slb-apc.4-2-1.bin
Load Balancing Supported	
Server load balancing	c6slb-apc.1-1-1.bin
Firewall load balancing Stateful Firewall Load Balancing (FWLB)—allows all connections, both existing and new, to fail over to the secondary firewall in a redundant pair (works only with stateful firewall configurations)	c6kslb-apc.2-1-1.bin c6slb-apc.3-2-1.bin
DNS load balancing	c6kslb-apc.2-1-1.bin
Stealth firewall load balancing	c6kslb-apc.2-1-1.bin
Transparent cache redirection	c6kslb-apc.2-1-1.bin
Reverse proxy cache	c6slb-apc.1-1-1.bin
SSL off-loading	c6slb-apc.1-1-1.bin
VPN-IPSec load balancing	c6kslb-apc.2-1-1.bin
Enhanced interoperation with the SSL termination engine (STE) for Secure Sockets Layer (SSL) load balancing	c6slb-apc.3-1-1.bin
Stickiness	
Cookie	c6slb-apc.1-1-1.bin
SSL ID	c6slb-apc.1-1-1.bin
Source IP	c6slb-apc.1-1-1.bin
HTTP redirection	c6slb-apc.1-1-1.bin
Cisco IOS SLB FWLB interoperation (IP reverse-sticky)	c6slb-apc.3-1-1.bin
HTTP header sticky	c6slb-apc.4-2-1.bin
Redundancy	
Sticky state Static sticky entries—allow prepopulation of the sticky table with entries that force users to connect to specific servers Sticky debug tools—include a show command for the number of sticky table entries and the ability to enter a specific IP address and receive the sticky information for that IP address (new show command can display sticky entries for cookie groups and SSL sticky groups)	c6slb-apc.1-1-1.bin c6slb-apc.3-2-1.bin
Full stateful failover (connection redundancy) Failover improvements—provide enhancements for preempt option with connection replication, the **forced failover** command Partial server farm failover	c6kslb-apc.2-1-1.bin c6slb-apc.3-2-1.bin c6slb-apc.4-2-1.bin

Table 4 CSM Feature Set Description (continued)

Feature	First Image Release
Backup sorry server (backup serverfarm) Allows a backup at the real server level	c6slb-apc.3-1-1.bin c6slb-apc.3-2-1.bin
Non-TCP connection redundancy	c6slb-apc.3-1-1.bin
Configuration synchronization	c6slb-apc.4-2-1.bin
Health Checking	
UDP probe—provides the ability to send UDP probes to specified ports to verify that the CSM does not receive a "port unreachable" message	c6slb-apc.3-2-1.bin
HTTP	c6slb-apc.1-1-1.bin
ICMP	c6slb-apc.1-1-1.bin
Telnet	c6slb-apc.1-1-1.bin
TCP	c6slb-apc.1-1-1.bin
SMTP	c6slb-apc.1-1-1.bin
DNS	c6kslb-apc.2-1-1.bin
Optional port for health probes	c6slb-apc.3-1-1.bin
Support for multiple users simultaneously configuring a CSM	c6slb-apc.3-1-1.bin
TCL (Toolkit Command Language) scripting—provides User Datagram Protocol (UDP) socket and global variable support, and XML configuration from a TCL Script adds the ability to send CSM configuration commands within a TCL script	c6slb-apc.3-1-1.bin c6slb-apc.3-2-1.bin
Failover tracking for interfaces and critical devices	c6slb-apc.4-2-1.bin
Management	
Static Address Resolution Protocol (ARP) entry—provides the ability to manually add entries to the CSM ARP table	c6slb-apc.3-2-1.bin
Added management features from releases 3.1(1) and 3.3(1)—includes the XML document definition type (DTD), the Cisco IOS MIB extensions for the CSM, and the system object identifier (SYSOB ID MIB) XML **show** commands	c6slb-apc.3-2-1.bin c6slb-apc.4-2-1.bin
SNMP traps for real server state changes	c6kslb-apc.2-1-1.bin
SNMP traps on fault-tolerant state changes	c6slb-apc.3-1-1.bin
Support for CISCO-SLB-MIB	c6slb-apc.3-1-1.bin
Support for CISCO-SLB-EXT-MIB	c6slb-apc.3-1-1.bin
XML configuration interface	c6slb-apc.3-1-1.bin
Resource use display	c6slb-apc.3-1-1.bin c6slb-apc.3-2-1.bin

New and Changed Information

- CISCO-SLB-MIB, CISCO-SLB-EXT-MIB, and CISCO-SLB-HEALTH-MON-MIB are supported for the CSM. Some of the tables defined earlier in CISCO-SLB-EXT-MIB have since been moved to the CISCO-SLB-HEALTH-MON-MIB. This change does not affect the behavior of the SNMP walk on those tables.

  The new CISCO-SLB-HEALTH-MON-MIB can be found at this location:

  ftp://ftp-sj.cisco.com/pub/mibs/v2/CISCO-SLB-HEALTH-MON-MIB.my

- CSCeg51185

  To improve the ability of SNMP trap receivers to display meaningful alarm and event messages, additional varbinds have been added in the following traps:

  - ciscoSlbVirtualStateChange - slbVirtualServerFarmName, slbVirtualIpAddress, slbVirtualPort
  - ciscoSlbRealStateChange - slbRealServerFarmName, slbRealIpAddress, slbRealPort

  This change appears in CSM software release 4.2(7).

- CSCsj26953

  A new state, standby(16), has been added to the MIB object slbRealServerState.

  This change appears in CSM software release 4.2(8).

- CSCsg90464

  In a fault tolerant (FT) application, the primary CSM can become unresponsive when the workload of the onboard IXP network processor exceeds 100 percent. Because the CSM software does not check the status of the network processor, this condition may not be detected and CSM failover may not occur. Two environment variables are added to cause the CSM to check the network processor utilization and to set a network processor utilization limit that, if exceeded, will result in a forced reset and a core dump of the CSM.

  The new environment variables have the following syntax:

  Name: IXP1_UTIL_CHECK
  Rights: RW
  Default: 0 (Disabled)
  Valid Values: Integer (0 to 1)
  Description: (Enable = 1) If the CPU utilization of the IXP network processor exceeds the value set in IXP1_OVERLOAD, a CSM reset and a core dump will result.
  Name: IXP1_OVERLOAD
  Rights: RW
  Default: 101
  Valid Values: Integer (101 to 1431655764)
  Description: Sets the CPU utilization percentage of the IXP network processor that will trigger a forced reset of the CSM. We recommend a setting of 101 percent.

  This example shows how to configure the environment variables to trigger a forced reset and core dump of the CSM if the network processor workload exceeds 101 percent:

  ```
  Router(config-module-csm)# variable IXP1_OVERLOAD 101
  Router(config-module-csm)# variable IXP1_UTIL_CHECK 1
  ```

  This change appears in CSM software release 4.2(7).

- CSCsg48830

  The FTP_CLOSE_DATA_CONN environment variable controls how the CSM treats an FTP Transfer Complete (226) response. Some FTP servers will continue to use the same data ports after issuing a Transfer Complete response. Because the CSM closes the connection after the Transfer Complete response, it does not recognize the additional traffic on the old data port. The new environment variable allows the server to reuse the same port after sending the Transfer Complete response. Because this function is only required for specific server or customer configurations, the function is selected through the environment variable.

  The FTP_CLOSE_DATA_CONN variable has the following syntax:

  Name: FTP_CLOSE_DATA_CONN
  Rights: RW
  Value: 0
  Default: 0
  Valid values: Integer (0 to 1)
  Description: Close data channels after a Transfer Complete response (0) or
  allow data port reuse (1).

  This example shows how to configure the environment variable:

  ```
  Router(config-module-csm)# variable FTP_CLOSE_DATA_CONN 1
  ```

  This change appears in CSM software release 4.2(6).

- CSCek56247

  The **count_sticky_entries** command has been added to display the number of active sessions in the sticky table. This command has no arguments, and returns the number of sessions reported by the **show mod csm <> sticky** command.

  This command is added in CSM software release 4.2(6).

- CSCsg29140

  The environment variable MAX_COOKIE_SIZE will now be automatically set to the size of the largest cookie currently configured. The user can change the value of this variable, but if cookies are subsequently added, deleted, or changed, the value may be automatically revised.

  This change appears in CSM software release 4.2(6).

- CSCsa58499

  The sticky entry times out with active flows. The sticky timer resets when new connections encounter a sticky entry. Sticky entries are kept in the sticky table only as long as the client keeps opening new connections at an interval smaller than the sticky timeout. If there is an open connection from a client, that connection is not enough to maintain the sticky entry associated with it in the sticky table. For example, with a sticky timer of 30 minutes and a connection open for one hour, after 30 minutes the sticky entry for that client is removed although that client has an open connection.

  The NO_TIMEOUT_IP_STICKY_ENTRIES environment variable is introduced to configure timeout policy for IP sticky entries with active sessions. The problem is resolved by having the sticky timer for a specific entry reset from the point where the last session ends. When NO_TIMEOUT_IP_STICKY_ENTRIES is set to 1, this timeout policy applies to sessions using IP sticky only. Sessions using other forms of persistence (for example cookie, SSL ID) are not affected by the environment variable.

The NO_TIMEOUT_IP_STICKY_ENTRIES variable has the following syntax:

Name: NO_TIMEOUT_IP_STICKY_ENTRIES
Rights: RW
Value: 0
Default: 0
Valid values: Integer (0 to 1)
Description: Timeout (1 = no timeout) policy for IP sticky entry with active sessions

This example shows how to configure the sticky environment variable:

```
Router(config-module-csm)# variable NO_TIMEOUT_IP_STICKY_ENTRIES 1
```

- CSCek02947

  The SASP_RETRY_COUNT variable is introduced to configure the Server/Application State Protocol (SASP) retry count. Valid values are from 2 to 30; the default value is 8.

- CSCsj26680

  The CHECK_REALS_PERIOD environment variable is introduced to rate-limit the checking of the number of available real servers when a server farm threshold has been configured. If the period since the last counting of servers has not exceeded the configured value (from 1 to 10 seconds), the result from the previous count will be used when making a load-balancing decision. The default value is 0 seconds.

  This change appears in CSM software release 4.2(8).

- CSCsv78324

  A new environmental variable CLIENT_NAT_NO_PAT is introduced to allow the disabling of port address translation (PAT) when client network address translation (NAT) is enabled. A new counter is added in the dump of LB Statistics to indicate that PAT was necessary due to a port collision.

  In normal client NAT operation, a client packet's source IP address is translated (NAT) and the source port number is translated (PAT). When the environmental variable CLIENT_NAT_NO_PAT is set, the CSM retains the original source port number when possible. If the original source port number is already in use by another connection, the CSM must perform PAT to avoid port collision.

  The CLIENT_NAT_NO_PAT variable has the following syntax:

  Name: CLIENT_NAT_NO_PAT
  Rights: RW
  Default: 0
  Valid values: Integer (0 to 1)
  Description: Disables (1 = no PAT) PAT where possible when client NAT is performed.

  This example shows how to configure the environment variable to disable PAT where possible:

  ```
  Router(config-module-csm)# variable CLIENT_NAT_NO_PAT 1
  ```

  To track instances when PAT was necessary to avoid a port collision, a new client NAT source port collision counter ("Cl NAT src port collis.") is introduced in the LB Statistics, which are displayed using the Venus Console. This counter is updated only when CLIENT_NAT_NO_PAT is set.

This example shows how to display the client NAT source port collision counter:

```
VENUS# dump_lb_stats
--------------------------------------------------------------
...
----------------------- LB Statistics ----------------------
--------------------------------------------------------------
...
        LB Rjct: no cl NAT port                       0
        Cl NAT src port collis.                       0

...
```

This change appears in CSM software release 4.2(11).

Limitations and Restrictions

- A CSM running software release 4.2(12), reloads unexpectedly with the following log message:

  ```
  "%CSM_SLB-3-UNEXPECTED: Module 6 unexpected error: IXP3 exception encountered."
  ```

  A core dump is produced with the header

  ```
  "IXP3 Software exception on task 'IXP3 SA-CORE (Ex 18)(00000000h'."
  ```

- A CSM running software release 4.1.2 or later releases (including 4.2.1 and 4.2.2) will not respond to pings to the virtual server when it is configured with service termination. The server is operational and is passing TCP flows to the real servers, which are also operational. This example shows the configuration:

  ```
  vserver test
   virtual a.b.c.d  tcp 0 service termination
   serverfarm servers1
   persistent rebalance
   domain shrun
   inservice
  ```

  If you need to ping the virtual server, do not configure service termination on the virtual server.

- Do not use the **ping** command in a TCL script for a destination that is one or more hops away.

  The **TCL ping()** command uses an underlying ping function provided by VxWorks. The VxWorks ping contains a bug that causes the ping function not to display an error when the ping function receives an ICMP error message (for example, host-unreachable). The function remains in a wait loop until it receives a valid response.

  If the destination host is in the same subnet (Layer 2 adjacent) as the CSM-configured VLAN, then the ICMP request either receives a valid response or is timed out. In this case, the ping() function will not stop responding.

  The problem occurs when the destination IP address is one or more hops away. The router between the CSM and the destination host could respond with a "destination unreachable" message to the CSM if the router determined that the subnet for this IP address is unknown.

- The CSM may block or drop all UDP data channels of an RTSP service if the client NAT is also enabled. This situation can occur when you configure a virtual server, which the CSM uses to parse the RSTP service, and on the same virtual server that you configure a client NAT on the server farm. In this situation, we recommend that you either remove the NAT client configuration from the server farm or remove the service RTSP from the virtual server.

- If your configuration contains a pair of CSMs in a single fault-tolerant group, and these paired CSMs are in an active-standby state, the CSMs might not retain the valid active-standby state if you add another CSM into this same fault-tolerant group. This action causes the fault-tolerant pair of CSMs to enter an invalid active-active state. In this case, remove the third CSM from the network and reboot the paired CSMs to allow them to recover their fault-tolerant state.
- Configure a client NAT pool with the server farm IP address instead of using the **static nat** command. The **static nat** command is normally used for server-initiated connections. In software release 3.2(1), you can configure the NAT client static into a server farm to take advantage of the static NAT feature for traffic matching a virtual server. If you configured the NAT client static into a server farm for FTP or RSTP services, this traffic would not be able to pass through the CSM.
- On systems that use Cisco IOS software and Catalyst operating system software, when you configure the Catalyst 6500 series switch to trust the DSCP priority bits of the incoming traffic, the CSM might reset the DSCP value to zero (0) if these frames are being forwarded by the CSM.
- When you ping to a real server that is reached through a virtual server, which is configured with predictor forward, the ping might fail after the probe to the real server fails. This probe is configured in another server farm with failaction reassign. This example shows the configuration:

  ```
  serverfarm <NAME>
   nat server
   no nat client
   predictor leastconns
   failaction reassign
   real name SERVER-A
     backup real name SERVER-B
     inservice
   real nameSERVER-B
     backup real name SERVER-A
     inservice
   probe <NAME>
  ```

  If failaction reassign is not required (in case the servers do not share connection states and cannot accept connections opened on the other server), remove failaction or use failaction purge.
- Internal ports on the CSM (dot1q, trunk, port-channel, and so on) 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 828 days have elapsed since the CSM was booted, the HTTP probe will fail and will stay in the down state for about 18 minutes. Reboot the CSM before 828 days have elapsed. (CSCso08858)
- When configuring CSMs for fault tolerance, we recommend that you configure a dedicated link for the fault-tolerant VLAN.

  Note Fault tolerance requires CSM release 1.2(1) or higher.

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

  Note CSM configuration synchronization is supported if the system uses Cisco IOS software in the supervisor engine. It is not supported if the system uses Catalyst operating system software in the supervisor engine.

- In an active-standby connection state replication setup, the connection counters on the standby CSM were not the same as the counters on the active CSM. The active CSM correctly shows that the connections were load balanced to various servers within a server farm. On the standby CSM, all replicated connections are assigned to a single real server within a server farm. The number of connections shown in the standby CSM might be different from the number of connections seen in the active CSM. This is a minor issue and does not affect the service. (CSCei73146, CSCee75333)
- The total conns established counter applies only to an active CSM. The standby CSM might display the total established connections when there is a fault-tolerance switchover, but the total conns established counter remains unchanged. (CSCtn16345)

Caveats

These sections describe the open and resolved caveats in CSM software:

- Open and Resolved Caveats in Software Release 4.2(15), page 17
- Open and Resolved Caveats in Software Release 4.2(14), page 18
- Open and Resolved Caveats in Software Release 4.2(13), page 19
- Open and Resolved Caveats in Software Release 4.2(12), page 20

Open and Resolved Caveats in Software Release 4.2(15)

These sections describe the open and resolved caveats in CSM software release 4.2(15):

Open Caveats in Software Release 4.2(15)

Note For a description of caveats resolved in CSM software release 4.2(15), see the "Resolved Caveats in Software Release 4.2(15)" section on page 17.

There are no open caveats in CSM software release 4.2(15).

Resolved Caveats in Software Release 4.2(15)

Note For a description of open caveats in CSM software release 4.2(15), see the "Open Caveats in Software Release 4.2(15)" section on page 17.

This section describes resolved caveats in CSM software release 4.2(15):

- CSCtg41899

  If a new regular expression domain match is added to the GSLB configuration, CSM does not match specific regular expression domains and a wrong A-record response is returned that does not match the correct policy map.

  Workaround: None.
- CSCtn86332

  If a serverfarm going down or up is configured on multiple VIPs, the VIP state change syslog is sent for only one VIP and not for all the VIPs.

Workaround: None.

- CSCtj90108

  With the static NAT configured, server initiated connections may fail on a higher traffic rate.

  Workaround: Disable static NAT.

- CSCtk63031

  The FTP connections do not time out and prevent new connections.

  Workaround: Clear all connections associated with the server. Downgrade your CSM to any CSM release below 4.2(14). Clear all slowpath connections using slowpath_reap_sessions in VENUS.

- CSCts71706

  The sticky replication is not working on CSM 4.2(14).

  Workaround: None.

Open and Resolved Caveats in Software Release 4.2(14)

These sections describe the open and resolved caveats in CSM software release 4.2(14):

- Open Caveats in Software Release 4.2(14), page 18
- Resolved Caveats in Software Release 4.2(14), page 18

Open Caveats in Software Release 4.2(14)

Note For a description of caveats resolved in CSM software release 4.2(14), see the "Resolved Caveats in Software Release 4.2(14)" section on page 18.

There are no open caveats in CSM software release 4.2(14).

Resolved Caveats in Software Release 4.2(14)

Note For a description of open caveats in CSM software release 4.2(14), see the "Open Caveats in Software Release 4.2(14)" section on page 18.

This section describes resolved caveats in CSM software release 4.2(14):

- CSCte28717

  The source-ip sticky may stop working after an extended uptime of approximately 470 days or more. The CSM will not create a new sticky entry.

  Workaround: None.

- CSCte39053

  The default expiration date of the cookies inserted by the CSM is Thursday, 1 Jan 2099, 01:01:50 GMT. After this time, the cookie-insert sticky will not work as expected.

Workaround: The default cookie expiration date can be changed by setting the COOKIE_INSERT_EXPIRATION_DATE environment variable on the CSM. For example, you can move the expiration date to May 25, 2020, by using the following commands:

```
Router# config t
Router(config)# mod csm 8
Router(config-module-csm# variable COOKIE_INSERT_EXPIRATION_DATE "Mon, 25 May 2020
08:00:00 GMT"
```

Make sure to change the slot number. The new expiration date changes in the inserted cookies immediately because this change does not require a reboot of the CSM. This change will not affect the network traffic.

- CSCtg56193

  When the uptime of CSM is more than 828 days, the FTP or RTSP Layer 7 connections are not timing out.

  Workaround: None.

- CSCth52331

  When a standby CSM reaches an uptime of 828 days, the standby CSM can assert mastership for a very short period (around 2 seconds), which creates an active/active situation.

  Workaround: None.

- CSCtg45008

  A new variable, L7_TX_CORE_QUEUE_TIMEOUT, is added to address CSCsh53633, where the CSM that runs release 4.2(6) might reboot due to an IXP 3 and the type of crash is "L7 abort."

  > Variable Name: L7_TX_CORE_QUEUE_TIMEOUT
  >
  > Rights: RW
  >
  > Value: 1
  >
  > Default: 1
  >
  > Valid values: Integer (1 to 10).
  >
  > Description: Time (in seconds) to wait for the Layer 7 TX Core queue to come out of the full state before asserting a core.

  Workaround: None.

Open and Resolved Caveats in Software Release 4.2(13)

These sections describe the open and resolved caveats in CSM software release 4.2(13):

- Open Caveats in Software Release 4.2(13), page 19
- Resolved Caveats in Software Release 4.2(13), page 20

Open Caveats in Software Release 4.2(13)

Note For a description of caveats resolved in CSM software release 4.2(13), see the "Resolved Caveats in Software Release 4.2(13)" section on page 20.

This section describes the open caveats in CSM software release 4.2(13):

- CSCte28717

  The source-ip sticky may stop working after an extended uptime of approximately 470 days or more. The CSM will not create a new sticky entry.

  Workaround: Reboot the CSM.

Resolved Caveats in Software Release 4.2(13)

Note For a description of open caveats in CSM software release 4.2(13), see the "Open Caveats in Software Release 4.2(13)" section on page 19.

This section describes resolved caveats in CSM software release 4.2(13):

- CSCtd31622

  The default expiration date of the cookies inserted by the CSM is Friday, 1 Jan 2010, 01:01:50 GMT. After this time, the cookie-insert sticky will not work as expected.

  Workaround: The default cookie expiration date can be changed by setting the COOKIE_INSERT_EXPIRATION_DATE environment variable on the CSM. For example, you can move the expiration date to May 25, 2020, by using the following commands:

  ```
  Router# config t
  Router(config)# mod csm 8
  Router(config-module-csm# variable COOKIE_INSERT_EXPIRATION_DATE "Mon, 25 May 2020
  08:00:00 GMT"
  ```

  Make sure to change the slot number. The new expiration date changes in the inserted cookies immediately as this change does not require a reboot of the CSM. This change will not affect the production traffic.

- CSCtc25780

  In rare cases, when CSM fault tolerant (FT) synchronization is performed with the **hw-module csm** *mod* **standby config-sync** command and FT VLAN is intermittently down, the standby CSM may send out an ARP packet towards the Layer 2 adjacent nodes using its physical MAC-address, instead of its virtual MAC-address. This causes an outage until the ARP table cache is either cleared or times out.

  Workaround: To prevent rapid failover in the standby CSM2 node, increase the failover timer to 120 seconds on both CSM nodes (active and standby).

Open and Resolved Caveats in Software Release 4.2(12)

These sections describe the open and resolved caveats in CSM software release 4.2(12):

- Open Caveats in Software Release 4.2(12), page 21
- Resolved Caveats in Software Release 4.2(12), page 21

Open Caveats in Software Release 4.2(12)

Note For a description of caveats resolved in CSM software release 4.2(12), see the "Resolved Caveats in Software Release 4.2(11)" section on page 23.

This section describes open caveats in CSM software release 4.2(12):

- CSCsz25520

  In rare cases, CSM may propagate an invalid MAC address table for VLAN 1 with an invalid MAC address back plane, across the CSM port channel Po259 to the back plane on management VLAN 1.

  The following output displays an invalid MAC address across the CSM port channel Po259 to the back plane on management VLAN:

```
Console> enable show mac-address-table | inc 259
*    1  4000.6806.14d9   dynamic  Yes        205   Po259
*    1  4000.6c06.1eb1   dynamic  Yes         90   Po259
*    1  4000.3806.4227   dynamic  Yes         50   Po259
*    1  4000.2e06.47c0   dynamic  Yes        150   Po259
*    1  4000.6c06.916b   dynamic  Yes        255   Po259
*    1  4000.6b06.fe6b   dynamic  Yes        240   Po259
*    1  4000.3406.a2ce   dynamic  Yes        175   Po259
*    1  0000.3206.79e0   dynamic  Yes         15   Po259
*    1  0000.3206.8c3a   dynamic  Yes        135   Po259
*    1  4000.6806.13b8   dynamic  Yes         55   Po259
*    1  0000.3206.69d4   dynamic  Yes         10   Po259
```

  Note Only the last 4 bytes of the MAC address change and point to VLAN 1 on the CSM port channel.

  Workaround: None.

- CSCsx64648

  On a CSM module the configuration synchronization times out with large configuration. For example, the configuration synchronization occurs at 16 K fails at 23 K.

  Workaround: None.

Resolved Caveats in Software Release 4.2(12)

Note For a description of open caveats in CSM software release 4.2(12), see the "Open Caveats in Software Release 4.2(11)" section on page 22.

This section describes resolved caveats in CSM software release 4.2(12):

- CSCsu92969

  Configuring multiple server load balancing (SLB) policies in a particular order causes the connection counter in a real server in the server farm to erroneously report the default maximum connection (MAXCONN) limit of 4294967295 connections. When this condition occurs, the real server refuses new connections.

  Workaround: Remove multiple SLB policies.

- CSCsz81265

When configuring two virtual servers (Layer 3 and Layer 4) with the same virtual IP address, CSM drops ICMP request to the virtual IP address. This condition occurs when both virtual servers are operational, and when there is no connection to the Layer 3 virtual server.

Workaround: Ensure that the Layer 3 virtual server is configured after the Layer 4 virtual server.

- CSCsx37458

  Under certain conditions, one or more VIPs on the CSM will not respond to the ping. This condition occurs, when the same VIP is used in the virtual server and in a static NAT entry. The VIP may be displayed in the CSM ARP table as a SVR NAT entry instead of virtual server entry. You can display the CSM ARP table by using **show mod csm** *slot* **arp** command.

  Workaround:

1. Suspend all vservers for the VIP address which is uncertain.
2. Remove the static NAT configuration for that VIP.
3. Reactivate the virtual servers.
4. Add the static NAT again.

- CSCsz81041

  The CSM does not send a reset upon receiving a synchronize acknowledge (ACK) packet sent to a synchronize start (SYN) packet. This condition occurs in Layer 7 mode when the CSM opens a connection on the backend server, and if the server responds to the SYN with an ACK that has an invalid sequence number.

  Workaround: None.

Open and Resolved Caveats in Software Release 4.2(11)

These sections describe the open and resolved caveats in CSM software release 4.2(11):

- Open Caveats in Software Release 4.2(11), page 22
- Resolved Caveats in Software Release 4.2(11), page 23

Open Caveats in Software Release 4.2(11)

Note For a description of caveats resolved in CSM software release 4.2(11), see the "Resolved Caveats in Software Release 4.2(11)" section on page 23.

This section describes open caveats in CSM software release 4.2(11):

- CSCsu92969

  Configuring multiple server load balancing (SLB) policies in a particular order causes the connection counter in a real server in the server farm to erroneously report the default maximum connection (MAXCONN) limit of 4294967295 connections. When this condition occurs, the real server refuses new connections.

  Workaround: Remove multiple SLB policies.

- CSCsh53633

  In rare cases, a CSM rebooted because of IXP 3. The type of crash was "L7 abort."

  Workaround: None.

Resolved Caveats in Software Release 4.2(11)

Note For a description of open caveats in CSM software release 4.2(11), see the "Open Caveats in Software Release 4.2(11)" section on page 22.

This section describes resolved caveats in CSM software release 4.2(11):

- CSCsr79179

  When the same gateway IP address is configured in both the **gateway** and **route** statements, the **gateway** statement will be ignored, although it will appear in the running configuration. After a failover or a reconfiguration, the active CSM will have no default route, and will drop traffic.

  Workaround: Possible workarounds include the following:

  - Use the **route 0.0.0.0 0.0.0.0 gateway x.x.x.x** command to install the default route.
  - Reload the CSM after the configuration synchronization.
  - Use a configuration that does not specify the same gateway address in the **gateway** and **route** statements.

- CSCsq36042

  When SSL stickiness is configured on a backup server farm, the CSM fails to perform NAT in some cases.

  Workaround: Disable SSL stickiness on the server farm.

- CSCsu39853

  In rare cases, the CSM will stop responding to the CLI but will continue to pass traffic.

  Workaround: None.

Open and Resolved Caveats in Software Release 4.2(10)

These sections describe the open and resolved caveats in CSM software release 4.2(10):

- Open Caveats in Software Release 4.2(10), page 23
- Resolved Caveats in Software Release 4.2(10), page 24

Open Caveats in Software Release 4.2(10)

Note For a description of caveats resolved in CSM software release 4.2(10), see the "Resolved Caveats in Software Release 4.2(10)" section on page 24.

This section describes open caveats in CSM software release 4.2(10):

- CSCsr79179

  When the same gateway IP address is configured in both the **gateway** and **route** statements, the **gateway** statement will be ignored, although it will appear in the running configuration. After a failover or a reconfiguration, the active CSM will have no default route, and will drop traffic.

  Workaround: Possible workarounds include the following:

  - Use the **route 0.0.0.0 0.0.0.0 gateway x.x.x.x** command to install the default route.
  - Reload the CSM after the configuration synchronization.
  - Use a configuration that does not specify the same gateway address in the **gateway** and **route** statements.
- CSCsh53633

  In rare cases, a CSM rebooted because of IXP 3. The type of crash was "L7 abort."

  Workaround: None.

Resolved Caveats in Software Release 4.2(10)

Note For a description of open caveats in CSM software release 4.2(10), see the "Open Caveats in Software Release 4.2(10)" section on page 23.

This section describes resolved caveats in CSM software release 4.2(10):

- CSCsm33035

  When the CSM starts to load balance using the default policy, and then a GET request matches a URL under a subpolicy, the CSM forwards traffic to the real server without modifying the TCP acknowledgement number.

  Workaround: Disable persistent rebalance.
- CSCso00578

  A CSM configured for redundancy may have its CSRP replication status stuck in the INIT state.

  Workaround: None.
- CSCso33427

  When the CSM is configured to load balance IPsec using one Layer 4 virtual server for IKE and another for ESP, the CSM fails to forward to the backend real server any "ICMP can't fragment" messages received at the CSM's virtual IP address and relating to the ESP flow.
- CSCso69828

  When cookie-insert is configured on the CSM and the server sends the FIN/ACK immediately after its HTTP 200 OK response, the CSM may send some subsequent packets out of order and with an incorrect TCP sequence number.
- CSCso81900

  When a NAT pool is modified while configured as part of an SLB policy to a virtual server, traffic is sent to the virtual server with a NAT-supplied source address of 0.0.0.0.

  Workaround: Reboot the CSM.
- CSCsq84207

  Path MTU discovery (PMTUD) performed by a server behind a CSM is not working correctly if the CSM is performing cookie insertion.

  Workaround: Possible workarounds include the following:

  - Reduce the server MSS to a value that allows the cookie insertion without exceeding the MTU of the path to the client.
  - Reduce the CSM default MSS using the environment variable TCP_MSS_OPTION.

- Use a different type of stickiness for the server (for example, application cookies).

Open and Resolved Caveats in Software Release 4.2(9)

These sections describe the open and resolved caveats in CSM software release 4.2(9):

- Open Caveats in Software Release 4.2(9), page 25
- Resolved Caveats in Software Release 4.2(9), page 25

Open Caveats in Software Release 4.2(9)

Note For a description of caveats resolved in CSM software release 4.2(9), see the "Resolved Caveats in Software Release 4.2(9)" section on page 25.

This section describes open caveats in CSM software release 4.2(9):

- CSCso00578

  A CSM configured for redundancy may have its CSRP replication status stuck in the INIT state.

  Workaround: None.

- CSCsh53633

  In rare cases, a CSM rebooted because of IXP 3. The type of crash was "L7 abort."

  Workaround: None.

Resolved Caveats in Software Release 4.2(9)

Note For a description of open caveats in CSM software release 4.2(9), see the "Open Caveats in Software Release 4.2(9)" section on page 25.

This section describes resolved caveats in CSM software release 4.2(9):

- CSCsl40722

  The CSM stops servicing load-balanced connections and probes due to a buffer leak.

  Workaround: Periodically, enter the **show mod csm** *slot* **tech-support all | i outstanding** command. If small buffers reach 24500 or medium buffers reach 20000, the buffers are full and you must reboot the CSM.

- CSCsi58089

  The CSM drops SASP server messages larger than 2816 bytes.

  Workaround: Reduce the number of servers participating in SASP to reduce the length of the SASP messages.

- CSCsk50939

  The CSM stops responding to CAPP-UDP requests from a Global Site Selector (GSS) after changing the CAPP-UDP setting from secure to no secure.

  Workaround: Reload the CSM.

- CSCsl59508

  When a server farm contains many real servers (for example, 100), the CSM may reboot and create a core dump when you add the **predictor leastconns slowstart** *num* command to the server farm.

- CSCsh94471

  In rare cases, the CSM console becomes unresponsive and the **show module csm** *num* command indicates that the CSM is offline.

- CSCsl72371

  When an XML call is contained in a TCL script probe, the CSM probe fails with a memory allocation failure and the CSM console becomes unresponsive.

- CSCsm84686

  When a client sends a SYN packet to a virtual server with the Explicit Congestion Notification (ECN) and Congestion Window Reduced (CWR) flags set, the CSM drops the SYN packet.

  Workaround: Disable ECN on the client.

- CSCsi85407

  In rare cases, when load balancing with a URL spanning multiple packets, the CSM will reboot and create a core dump.

- CSCsi82468

  If persistent rebalance is enabled in a virtual server that contains a redirect server farm, the CSM will send two redirect responses for multipacket GET requests. This condition causes high CPU usage.

  Workaround: Disable persistent rebalance on the virtual server that contains a redirect server farm.

- CSCsj05855

  In rare cases, the CSM may reboot and create a core dump due to memory corruption.

Open and Resolved Caveats in Software Release 4.2(8)

These sections describe the open and resolved caveats in CSM software release 4.2(8):

- Open Caveats in Software Release 4.2(8), page 26
- Resolved Caveats in Software Release 4.2(8), page 27

Open Caveats in Software Release 4.2(8)

Note For a description of caveats resolved in CSM software release 4.2(8), see the "Resolved Caveats in Software Release 4.2(8)" section on page 27.

This section describes open caveats in CSM software release 4.2(8):

- CSCsh53633

  In rare cases, a CSM rebooted because of IXP 3. The type of crash was "L7 abort."

  Workaround: None.

Resolved Caveats in Software Release 4.2(8)

Note For a description of open caveats in CSM software release 4.2(8), see the "Open Caveats in Software Release 4.2(8)" section on page 26.

This section describes resolved caveats in CSM software release 4.2(8):

- CSCse91983

  The **show mod csm** *slot* **tech all** command might display IXP3 utilization above 100 percent when the cookie insert feature and other Layer 7 policies are active, and when CSM traffic suddenly stops and restarts. In response to this traffic fluctuation, the IXP3 clears and then reestablishes its tables. This activity overloads the IXP3, which results in the loss of some redundancy and slow path messages. The IXP3 recovers after the traffic level stabilizes.

  Workaround: None.

- CSCeg15173

  Fragmented Layer 2 Tunneling Protocol (L2TP) tunneled packets are discarded by the CSM, and the Packets Repeat Reverse Fragmentation counter in the CSM increments quickly. This problem occurs when packets arrive out of order (the MF packets arrive last) and are separated in time by about 10 milliseconds.

  Workaround: Design the network so that all fragments follow the same path, forcing them to arrive in order and closer together. You can also configure a static route in the CSM so that the module knows where to send reassembled fragments that arrived in a reverse order.

- CSCsk29021

  When persistent rebalance is configured, the CSM will reexamine a persistent GET and remap it if it matches a different policy. As part of the remapping, the CSM will send a reset to the old connection. If the header insert feature is configured, this reset message has an incorrect sequence number.

  Workaround: None.

- CSCsg37513

  A CSM running software release 3.x restarts with an exception every 81 seconds after upgrading to software release 4.x.

  Workaround: None.

- CSCsg40988

  The CSM halts with the following system log (syslog) error: "%CSM_SLB-3-UNEXPECTED: Module 3 unexpected error: FPGA3 exception encountered."

  Workaround: None.

- CSCsg84530

  The CSM reloads unexpectedly with the following syslog error: "%CSM_SLB-3-UNEXPECTED: Module 3 unexpected error: PPC exception." The console displays the error message "PPC exception type 1792 on FTReplFlow(0C247500h)" followed by a core dump.

  Workaround: None.

- CSCsi29132

  Clients sending persistent connections to a CSM virtual server may see a long delay after an HTTP request. This situation can occur when the virtual server is configured with persistence rebalance and with sticky cookies learned through the server. The CSM may not be forwarding the request to the server if the preceding request had an out-of-order response from the server.

  Workaround: Remove persistence rebalance or remove cookies from the virtual server.

- CSCsj26410

  In earlier CSM releases (for example, Release 3.2(1)), when one of the multiple virtual IP addresses monitored by KeepAlive-Appliance Protocol (KAL-AP) was brought down, the Content and Application Peering Protocol (CAPP) would return a load value of 255. In later CSM releases, CAPP incorrectly returns a load value of 128.

  Workaround: None.

- CSCsj26680

  When you enter the **serverfarm threshold** (vserver submode) command, a CLI lockup can occur. This condition can occur when the primary server farm contains hundreds of real servers that are down and the backup server farm takes over immediately. In this case, the CSM performance drops and the CLI becomes unresponsive.

  Workaround: None.

- CSCsj75481

  The CSM is not passing SYN-ACK in a policy-based routing (PBR) network when the ROUTE_UNKNOWN_FLOW_PKTS environment variable is set to 2. This environment variable specifies whether to route SYN or non-SYN packets that do not match any existing flows.

  Workaround: Downgrade to a CSM version lower than 4.2(4).

- CSCsj82230

  After removing service termination from a virtual server's virtual IP address, the IP address no longer responds to ping requests.

  Workaround: None.

- CSCsj88014

  A large delay in updating LOAD using KAL-AP can occur. When a Global Site Selector (GSS) is configured to probe a large number of virtual IP addresses with KAL-AP, the response to the KAL-AP queries slows down, causing the GSS to consider the virtual IPs to be down.

  Workaround: Consolidate virtual servers to reduce their number, or use TCP keepalives instead.

- CSCsk43903

  A pair of CSMs configured for fault tolerant operation will both enter the active state after 828 days.

  Workaround: None.

- CSCsi96851

  If the CSM is configured to track a nonexistent group, and the group ID is the same as a VLAN ID in which an HSRP group is configured, the CSM will fail over with the syslog message "Forced failover due to HSRPGroup tracking failures."

  Note This resolution is effective only with Cisco IOS Release 12.2SXF10 or later releases, which resolve the associated caveat CSCse54191.

Workaround: None.

- CSCsl23801

  HSRP causes CSM static ARP entries to be overwritten with all zeros (00-00-00-00-00-00). This is an unintended result of a previous caveat resolution.

  Workaround: Downgrade to CSM software release 4.2(1).

- CSCsk98543

  The CSM console might lock up when a backup server farm is configured with a threshold and contains few real servers (for example, less than ten real servers).

  Workaround: Remove the threshold command.

Open and Resolved Caveats in Software Release 4.2(7)

These sections describe the open and resolved caveats in CSM software release 4.2(7):

- Open Caveats in Software Release 4.2(7), page 29
- Resolved Caveats in Software Release 4.2(7), page 30

Open Caveats in Software Release 4.2(7)

Note For a description of caveats resolved in CSM software release 4.2(7), see the "Resolved Caveats in Software Release 4.2(7)" section on page 30.

This section describes open caveats in CSM software release 4.2(7):

- CSCsh53633

  A CSM running 4.2(6) might reboot due to IXP 3. The type of crash is "L7 abort."

  Workaround: None.

- CSCse91983

  The **show mod csm** *slot* **tech all** command might display IXP3 utilization above 100 percent when the cookie insert feature and other Layer 7 policies are active, and when CSM traffic suddenly stops and restarts. In response to this traffic fluctuation, the IXP3 clears and then reestablishes its tables. This activity overloads the IXP3, which results in the loss of some redundancy and slow path messages. The IXP3 recovers after the traffic level stabilizes.

  Workaround: None.

- CSCei73146

  In an active-standby connection state replication setup, the connection counters on the standby CSM were not the same as the counters on the active CSM. The active CSM correctly shows that the connections were load-balanced to various servers within a server farm. On the standby CSM, all replicated connections are assigned to a single real server within a server farm. The number of connections shown in the standby CSM might be different from the number of connections seen in the active CSM. This is a minor issue and does not affect the service.

  Workaround: None.

- CSCsb56078 (duplicate of CSCei73146)

  The wrong real server counter is being incremented. There is an incorrect connection counter on the standby CSM. Traffic reaches the backup server farm, and this server farm is using client NAT.

  Workaround: None.

- CSCeg15173

  Fragmented Layer 2 Tunneling Protocol (L2TP) tunneled packets are discarded by the CSM, and the Packets Repeat Reverse Fragmentation counter in the CSM increments quickly. This problem occurs when packets arrive out of order (the MF packets arrive last) and are separated in time by about 10 milliseconds.

  Workaround: Design the network so that all fragments follow the same path, forcing them to arrive in order and closer together. You can also configure a static route in the CSM so that the module knows where to send reassembled fragments that arrived in a reverse order.

Resolved Caveats in Software Release 4.2(7)

Note For a description of open caveats in CSM software release 4.2(7), see the "Open Caveats in Software Release 4.2(7)" section on page 29.

This section describes resolved caveats in CSM software release 4.2(7):

- CSCsh25401

  After repeated copying of the startup configuration to the running configuration, the active CSM will no longer send its configuration to the standby CSM. The active CSM will display the following log message: "%CSM_SLB-3-REDUNDANCY: Module 3 FT error: Active: Manual bulk sync timed out."

  Workaround: None.

- CSCse93972

  Unless the virtual servers are configured for replication, after a failover from one CSM to another, the formerly active CSM will send idle resets for persistent flows that it hosted before the failover. If the virtual servers are configured for replication, the backup CSM will not send resets.

  Workaround: Configure the virtual servers for replication.

- CSCek31065

  A CSM in a redundant configuration with duplicate entries configured under IOS/SLB can generate the following log message: "9w3d: CSM9: Invalid encaps ID for get info." This message can also occur if the user shuts down or advertises PVLANs, or clears the CSM arp-cache, or configures "secondary" addresses on an MSFC interface VLAN that is associated with the CSM's client/server VLAN.

  Workaround: None.

- CSCek51742

  Under some conditions, the CSM will wait more than nine seconds before sending an ARP request for a locally connected device not in the ARP table. This situation occurs when traffic is sent directly through the CSM in routed mode with ROUTE_UNKNOWN_FLOW_PKTS set to 2.

  Workaround: None.

- CSCek71183

  When using the header insert feature with a header longer than 127 bytes, the rest of the header insert will fail.

  Workaround: Header insert strings within the same map should have the combined length of no more than 127 bytes, including string names and delimiters.

- CSCsd98833

  When a real server is added to a SASP group and the Global Workload Manager (GWM) assigns the new server a weight of 0, the status of the new server should be DFP_THROTTLED. Instead it is shown as OPERATIONAL.

  Workaround: None.

- CSCse93972

  The backup CSM can send resets for flows that correspond to virtual servers that are not configured for replication. This can happen after a failover where a long-lived flow occurred over the CSM when it was the master, but the CSM is now the backup. After the idle timeout, the backup CSM will send a reset. The backup CSM will not send a reset if replication is configured on the virtual server.

  Workaround: Configure replication on the virtual server.

- CSCsg16726

  The CSM ignores an initial SYN packet if the push (PSH) bit is set in the SYN packet.

  Workaround: None.

- CSCsg37513

  The CSM erroneously classifies certain traffic as cookie-insert, and replicates all Layer 7 sessions as insert sessions, causing an exception crash.

  Workaround: None.

- CSCsg82885

  The CSM will not boot after the user configures close to the maximum number of virtual servers and scripted probes attached to the server farm. A warning has been added when the number of TCL scripted probes exceeds 900.

  Workaround: If you need a large number of probes, use CSM native probes rather than TCL scripted probes, because native probes consume less memory space.

- CSCsg91075

  A core dump can occur when the CSM is handling connections using both Server/Application State Protocol (SASP) and Dynamic Feedback Protocol (DFP).

  Workaround: None.

- CSCsg94630

  An expired sticky entry may become active again when the sticky timer wraps around at 497 days.

  Workaround: Before 497 days, either reboot the CSM or clear the sticky table manually.

- CSCsh43381

  When the backup server farm is out of service, the partial serverfarm failover feature ignores failover threshold parameters.

  Workaround: None.

- CSCsh52256

  The CSM does not generate a syslog message if a virtual server dynamically goes out of service because all the real servers failed.

  Workaround: None.

- CSCsh83504

  The CSM may generate conflicting cookie hashes rather than unique values, leading to incorrect load-balancing decisions by the CSM. When a cookie is long enough to cross a packet boundary, a partial hash is created. When the rest of the cookie is received, the rest of the hash is created, possibly taking input from the previous partial hash.

  Workaround: Remove cookie configuration, or use another type of sticky marker such as source IP address, or make sure cookies are short enough to not span packets.

- CSCsh90755

  The CSM may not insert a cookie if the real server sends a return code of 302 with a "Connection: close" header.

  Workaround: None.

- CSCsh96686

  The Server/Application State Protocol (SASP) task can become stuck in a loop. This situation can occur when communications are disrupted between the CSM and a SASP server.

  Workaround: None.

- CSCsh98223

  A CSM core dump can occur with the message, "FPGA4 exception 1 IDLE - idle."

  Workaround: None.

- CSCsi35629

  No SNMP trap is sent when a real server returns to the operational state after a probe failure.

  Workaround: None.

- CSCsi36092

  When a TCP connection to the CSM is being established using a SYN cookie, the CSM can send IP fragments to a Layer 7 virtual server.

  Workaround: None.

- CSCsi36168

  Connections can fail when traffic is sent to a Layer 7 virtual server that has service termination configured.

  Workaround: Don't configure service termination to a Layer 7 virtual server.

Open and Resolved Caveats in Software Release 4.2(6)

These sections describe the open and resolved caveats in CSM software release 4.2(6):

- Open Caveats in Software Release 4.2(6), page 33
- Resolved Caveats in Software Release 4.2(6), page 33

Open Caveats in Software Release 4.2(6)

Note For a description of caveats resolved in CSM software release 4.2(6), see the "Resolved Caveats in Software Release 4.2(6)" section on page 33.

This section describes open caveats in CSM software release 4.2(6):

- CSCse93972

  Unless the virtual servers are configured for replication, after a failover from one CSM to another, the formerly active CSM will send idle resets for persistent flows that it hosted before the failover. If the virtual servers are configured for replication, the backup CSM will not send resets.

  Workaround: Configure the virtual servers for replication.

- CSCse91983

  The **show mod csm** *slot* **tech all** command might display IXP3 utilization above 100 percent when the cookie insert feature and other Layer 7 policies are active, and when CSM traffic suddenly stops and restarts. In response to this traffic fluctuation, the IXP3 clears and then reestablishes its tables. This activity overloads the IXP3, which results in the loss of some redundancy and slow path messages. The IXP3 recovers after the traffic level stabilizes.

  Workaround: None.

- CSCei73146

  In an active-standby connection state replication setup, the connection counters on the standby CSM were not the same as the counters on the active CSM. The active CSM correctly shows that the connections were load-balanced to various servers within a server farm. On the standby CSM, all replicated connections are assigned to a single real server within a server farm. The number of connections shown in the standby CSM might be different from the number of connections seen in the active CSM. This is a minor issue and does not affect the service.

  Workaround: None.

- CSCsb56078 (duplicate of CSCei73146)

  The wrong real server counter is being incremented. There is an incorrect connection counter on the standby CSM. Traffic reaches the backup server farm, and this server farm is using client NAT.

  Workaround: None.

- CSCeg15173

  Fragmented Layer 2 Tunneling Protocol (L2TP) tunneled packets are discarded by the CSM, and the Packets Repeat Reverse Fragmentation counter in the CSM increments quickly. This problem occurs when packets arrive out of order (the MF packets arrive last) and are separated in time by about 10 milliseconds.

  Workaround: Design the network so that all fragments follow the same path, forcing them to arrive in order and closer together. You can also configure a static route in the CSM so that the module knows where to send reassembled fragments that arrived in a reverse order.

Resolved Caveats in Software Release 4.2(6)

Note For a description of open caveats in CSM software release 4.2(6), see the "Open Caveats in Software Release 4.2(6)" section on page 33.

This section describes resolved caveats in CSM software release 4.2(6):

- CSCse97201

  If you configure the CSM with two virtual servers, each with the same virtual IP address but with different subnet masks, the CSM will not redirect traffic to the other server when one of the servers is taken out of service. Changing the subnet masks to be identical will not solve the problem unless you also reboot the CSM.

  Workaround: None.

- CSCsg48830

  Outbound FTP connectivity will hang if the remote FTP server reuses the data port after sending a Transfer Complete response. A new environment variable allows the CSM to accommodate this server behavior. Configuration of the new environment variable is described in "Troubleshooting" section on page 73.

  Workaround: None.

- CSCsg18828

  When you configure session cookies, the CSM includes the attribute **expires=** in the cookie string. This attribute should only appear for persistence cookies, which have a defined expiration date. A new session cookie string format is defined that deletes the attribute.

  Workaround: None.

- CSCej70864

  When a ping request is sent to the virtual server IP address, the CSM will sometimes attempt to reply to the ping rather than forwarding it. In these cases, the CSM will now drop the request rather than reply.

  Workaround: None.

- CSCse50544

  If cookie insertion is configured, the CSM behaves incorrectly when the HTTP server response arrives out of order (data first, then HTTP header in the last packet). In this case, the CSM inserts the cookie in the first packet received (the data packet) rather than in the HTTP header. As a resolution, the CSM will not insert a cookie when the server response is out of order.

  Workaround: Ensure that the HTTP server responses are always received in order.

- CSCsd97668

  When using a DNS probe that expects more than one IP address to be returned, the probe can fail if the DNS server does not return the second address.

  Workaround: Configure the probe to expect only one IP address, and configure the DNS server to return only one IP address.

- CSCsf11010

  When Global Site Selector (GSS) is configured to probe the virtual IP address with KAL-AP, the CSM will answer the probe, even though CAPP UDP is not configured.

  Workaround: Configure CAPP UDP on the CSM.

- CSCsg37187

  The CSM occasionally forgets to send ICMP echo, causing probe failure messages. This situation occurs when the probe parameters for **retries** or **failed** are configured for a value less than their default values.

  Workaround: Use default values for probe **retries** and **failed** parameters.

- CSCsg93384

  Under heavy backpressure from the Catalyst 6500 series switch backplane, the CSM's NAT processor can stop handling traffic until the backpressure subsides. In severe cases, a Layer 7 abort failure can occur in the NAT module.

  Workaround: None.

- CSCsd99863

  When performing Layer7 load balancing, the CSM will generate easily predictable TCP Initial Sequence Numbers (ISN), weakening security.

  Workaround: Use a firewall in front of the CSM.

- CSCek58878

  When using 2- or 3-tiered virtual server tracking, the dependent CSM virtual servers can remain outofservice after the tracked virtual server has recovered to operational status.

  Workaround: None.

- CSCsf99484

  A CSM core dump occurs that is related to the redirect process.

  Workaround: None.

- CSCsd52775

  When IP header insertion is used along with multiple Layer 7 policies in a persistent connection, the CSM sends an incorrect ACK number to finish the TCP handshake.

  Workaround: None.

- CSCsg51792

  A buffer leak can occur when fragmented TCP requests are sent to a virtual server configured for service termination. The resulting loss of buffers can lead to full system failure of load-balancing traffic.

  Workaround: Disable service termination on the virtual server, which will make it a Layer 4 virtual server only.

- CSCse45390

  When the virtual server is configured for service termination, the virtual server may not be listed when you enter the **show mod csm** *$slot* **conns vserver** *$nameOfVserver* command.

  Workaround: Enter the **show mod csm** *$slot* **conns detail** command to display the connections.

- CSCek39783

  If a route entry in the ARP table has the same MAC address as a learned ARP entry, the CSM will reset all connections associated with the route entry whenever the learned entry is updated with a new MAC address.

  Workaround: In the CSM configuration, add a static ARP entry for the learned ARP entry.

- CSCek50448

  During some conditions (for example, rate limiting), the CSM fails to increment the debug counter for packets dropped due to unknown MAC address. As a resolution, a new session statistics counter is added in this version to display the Packets with no SMAC, sent to slowpath message.

  Workaround: None.

- CSCse90720

  When hosting a Layer 7 virtual server, the CSM will answer a client's TCP handshake with an incorrect SYN/ACK sequence number, preventing the connection from establishing. This situation occurs under heavy load when the client resends the initial SYN packet.

  Workaround: None.

- CSCse98829

  In the webhost relocation line of a redirect-vserver configuration, when you use the %p extension to instruct the CSM to append the trailing URI, the URI may not be appended. This situation occurs when the HTTP GET request is smaller than 119 bytes. In response to the small GET request, the redirect is sent out, but the extension is not appended.

  Workaround: Use a larger GET request.

- CSCse93460

  When a server is hosting multiple IP addresses on a single MAC address, the CSM may not remap all flows to the server if the MAC address changes.

  Workaround: For UDP flows, clear the unmapped connections and allow them to reestablish.

- CSCek37109

  A non-SSL CSM can incorrectly classify traffic causing an IXP3 SA-CORE exception failure.

  Workaround: None.

- CSCsg40777

  Inbound traffic on a port of the supervisor engine does not reach the virtual IP address of the CSM if the supervisor engine is performing NAT on the virtual IP address.

  Workaround: Initialize register PI_PN_NONMOD_CRC_CFG_REG to a value of 0x40.

- CSCsg20504

  If the status-tracking feature is enabled, the CSM may stop executing **show** commands and displays the message %No ICC response for TLV. The traffic flow remains normal.

  Workaround: Do not enable the status-tracking feature.

- CSCsf16722

  If you configure the CSM with many virtual servers, the CSM may delay sending responses to KAL-AP queries from the Global Site Selector (GSS). If the response is too slow, the GSS times out and reports that the virtual server is offline.

  Workaround: Reduce the number of virtual servers on the CSM, or use TCP keepalives instead of KAL-AP keepalives.

- CSCsc25061

  When running TCP, if fragmented IP packets are processed on a server farm with the NAT server option enabled, the recalculated TCP checksum may be incorrect.

  Workaround: If possible, turn off the NAT server option on the server farms that receive fragmented TCP packets.

- CSCek22782

  A configuration synchronization check for the active and standby CSMs may fail for configurations that contain the following subcommands: **script**, **ARP**, **variable**, **match**, **failaction**, **NAT client**, **probe**, **domain**, and **url-hash**. When you use these subcommands, and then you change configurations only in the active or the standby CSM, the wrong configuration synchronization state might be displayed. The module might incorrectly display synchronized configurations as "out-of-sync," and configurations that are out of synchronization as synchronized.

Resolved in Cisco IOS Release 12.2(18).

Workaround: None.

Open and Resolved Caveats in Software Release 4.2(5)

These sections describe the open and resolved caveats in CSM software release 4.2(5):

- Open Caveats in Software Release 4.2(5), page 37
- Resolved Caveats in Software Release 4.2(5), page 40

Open Caveats in Software Release 4.2(5)

Note For a description of caveats resolved in CSM software release 4.2(5), see the "Resolved Caveats in Software Release 4.2(5)" section on page 40.

This section describes open caveats in CSM software release 4.2(5):

- CSCsf16722

  If you configure the CSM with a large number of virtual servers, the CSM may delay sending responses to KAL-AP queries from the Global Site Selector (GSS). If the response is too slow, the GSS times out and reports that the virtual server is offline.

  Workaround: Reduce the number of virtual servers on the CSM, or use TCP keepalives instead of KAL-AP keepalives.

- CSCse91983

  The **show mod csm** *slot* **tech all** command might display IXP3 utilization above 100 percent when the cookie insert feature and other Layer 7 policies are active, and when CSM traffic suddenly stops and restarts. In response to this traffic fluctuation, the IXP3 clears and then reestablishes its tables. This activity overloads the IXP3, which results in the loss of some redundancy and slow path messages. The IXP3 recovers after the traffic level stabilizes.

  Workaround: None.

- CSCsc25061

  When running TCP, if fragmented IP packets are processed on a server farm with the NAT server option enabled, the recalculated TCP checksum may be incorrect.

  Workaround: If possible, turn off the NAT server option on the server farms that receive fragmented TCP packets.

- CSCek22782

  A configuration synchronization check for the active and standby CSMs may fail for configurations that contain the following subcommands: **script**, **ARP**, **variable**, **match**, **failaction**, **NAT client**, **probe**, **domain**, and **url-hash**. When you use these subcommands and then you change configurations only in the active or the standby CSM, the wrong configuration synchronization state might be displayed. The module might incorrectly display synchronized configurations as "out-of-sync," and configurations that are out of synchronization as synchronized.

Workaround: None.

- CSCei73146

  In an active-standby connection state replication setup, the connection counters on the standby CSM were not the same as the counters on the active CSM. The active CSM correctly shows that the connections were load-balanced to various servers within a server farm. On the standby CSM, all replicated connections are assigned to a single real server within a server farm. The number of connections shown in the standby CSM might be different from the number of connections seen in the active CSM. This is a minor issue and does not affect the service.

  Workaround: None.

- CSCsc14905

  A CSM running software release 4.1.2 or later (including 4.2.1 and 4.2.2) will not respond to pings to the virtual server when it is configured with service termination. The server is operational and is passing TCP flows to the real servers, which are also operational. This example shows the configuration:

```
vserver test
 virtual a.b.c.d  tcp 0 service termination
 serverfarm servers1
 persistent rebalance
 domain shrun
 inservice
```

  Workaround: Do not configure service termination on the virtual server.

- CSCsb75627

  When you ping to a real server that is reached through a virtual server, which is configured with predictor forward, the ping might fail after the probe to the real server fails. This probe is configured in another server farm with failaction reassign. This example shows the configuration:

```
serverfarm <NAME>
 nat server
 no nat client
 predictor leastconns
 failaction reassign
 real name SERVER-A
   backup real name SERVER-B
   inservice
 real nameSERVER-B
   backup real name SERVER-A
   inservice
 probe <NAME>
```

  Workaround: If failaction reassign is not required (in case the servers do not share connection states and cannot accept connections opened on the other server), remove failaction or use failaction purge.

- CSCsb56078

  The wrong real server counter is being incremented. There is an incorrect connection counter on the standby CSM. Traffic reaches the backup server farm, and this server farm is using client NAT.

  Workaround: None.

- CSCeg15173

Fragmented Layer 2 Tunneling Protocol (L2TP) tunneled packets are discarded by the CSM, and the Packets Repeat Reverse Fragmentation counter in the CSM increments quickly. This problem occurs when packets arrive out of order (the MF packets arrive last) and are separated in time by about 10 milliseconds.

Workaround: Design the network so that all fragments follow the same path, forcing them to arrive in order and closer together. You can also configure a static route in the CSM so that the module knows where to send reassembled fragments that arrived in a reverse order.

- CSCec38106

  On systems that use Cisco IOS software and Catalyst operating system software, when you configure the Catalyst 6500 series switch to trust the DSCP priority bits of the incoming traffic, the CSM might reset the DSCP value to zero (0) if these frames are being forwarded by the CSM.

  Workaround: None.

- CSCec28396

  The **static nat** command is normally used for server-initiated connections. In software release 3.2(1), you can configure the NAT client static into a server farm to take advantage of the static NAT feature for traffic matching a virtual server. If you configured the NAT client static into a sever farm for FTP or RSTP services, this traffic would not be able to pass through the CSM.

  Workaround: Configure a client NAT pool with the server farm IP address instead of using the **static nat** command.

- CSCea43504

  If your configuration contains a pair of CSMs in a single fault-tolerant group and these paired CSMs are in an active-standby state, the CSMs might not retain the valid active-standby state if you add another CSM into this same fault-tolerant group. This action causes the fault-tolerant pair of CSMs to enter an invalid active-active state.

  Workaround: Remove the third CSM from the network and reboot the paired CSMs to allow them to recover their fault-tolerant state.

- CSCdw84018

  The CSM may block or drop all UDP data channels of an RTSP service if the client NAT is also enabled. You must configure a virtual server, which the CSM uses to parse the RSTP service. For this same virtual server, you must also configure a client NAT on the server farm.

  Workaround: Remove the NAT client configuration from the server farm or remove the service RTSP from the virtual server.

- CSCdy67259

  The **TCL ping()** command uses an underlying **ping()** function provided by VxWorks. The VxWorks ping contains a bug that causes the ping function not to display an error when the ping function receives an ICMP error message (for example, host-unreachable). The function remains in a wait loop until it receives a valid response.

  If the destination host is in the same subnet (Layer 2 adjacent) as the CSM-configured VLAN, then the ICMP request either receives a valid response or is timed out. In this case, the ping() function will not stop responding.

  The problem occurs when the destination IP address is one or more hops away. The router between the CSM and the destination host could respond with a "destination unreachable" message to the CSM if the router determined that the subnet for this IP address is unknown.

  Workaround: Do not use the **ping** command in TCL script for a destination that is one hop away.

Resolved Caveats in Software Release 4.2(5)

Note For a description of open caveats in CSM software release 4.2(5), see the "Open Caveats in Software Release 4.2(5)" section on page 37.

This section describes resolved caveats in CSM software release 4.2(5):

- CSCse78674

  The CSM corrupts fragmented UDP packets on server-initiated traffic. The CSM fails to detect that the packet is fragmented and attempts to alter the UPD source port of the packet. This action overwrites the payload data in the fragmented packet and corrupts the packet. Fragmented packets are also corrupted on return flows, because the CSM overwrites the payload data by attempting to modify the UDP destination port.

  Workaround: None.

- CSCse98263

  When you configure multiple header sticky policies across more than one virtual server, some of the real servers ignore the header sticky policies. This problem applies only to header sticky policies (cookie sticky policies function correctly).

  This caveat was introduced in release 4.2(4). Header sticky policies function correctly in earlier releases.

  Workaround: If possible, use cookie sticky policies as an alternative to header sticky policies.

- CSCek49160

  When you use the Server/Application State Protocol (SASP) Global Workload Manager (GWM) test tool, the CSM may not register all of the member servers in the SASP group. This problem occurs when the connection between the CSM and the SASP GWM terminates in the middle of a session and returns to service after the CSM times out.

  This problem will cause the SASP test to fail and may cause the whole SASP test suite to fail.

  Workaround: After a connection failure, remove the SASP agent configuration and add it again to register all the real servers in the server farm.

- CSCek49892

  When a large number of active FTP sessions send messages simultaneously, the CSM may delay responding to PORT commands. If a client retransmits the PORT command, the CSM refuses to connect the client.

  Workaround: If possible, increase the client retransmit time.

- CSCek49909

  When a large number of passive FTP sessions are open, the CSM may delay responding to PASV messages. If a client retransmits the PASV message, the CSM responds with an error code that indicates that the port is not available. This scenario occurs only during initial creation of the data channel and does not affect data traffic.

  Workaround: Ensure that clients initiate a reattempt after receiving the error code. Reattempts connect successfully, because the port number in the reattempt is different from the original request.

- CSCek51235

  When failed probes are added to a server farm used in a dependent vserver, the CSM may fail and produce a core dump. The syslog header indicates a HealthMon exception.

Workaround: None.

- CSCsf21551

  When a server responds to an HTTP probe with an OK message and then sends an RST to close the TCP connection, the CSM places the server in a failed state.

  Workaround: Prevent the real server from sending RSTs after OK messages.

Open and Resolved Caveats in Software Release 4.2(4)

These sections describe the open and resolved caveats in CSM software release 4.2(4):

- Open Caveats in Software Release 4.2(4), page 41
- Resolved Caveats in Software Release 4.2(4), page 44

Open Caveats in Software Release 4.2(4)

Note For a description of caveats resolved in CSM software release 4.2(4), see the "Resolved Caveats in Software Release 4.2(4)" section on page 44.

This section describes open caveats in CSM software release 4.2(4):

- CSCse91983

  The **show mod csm** *slot* **tech all** command might display IXP3 utilization above 100 percent when the cookie insert feature and other Layer 7 policies are active, and when CSM traffic suddenly stops and restarts. In response to this traffic fluctuation, the IXP3 clears and then reestablishes its tables. This activity overloads the IXP3, which results in the loss of some redundancy and slow path messages. The IXP3 recovers after the traffic level stabilizes.

  Workaround: None.

- CSCse78674

  The CSM corrupts fragmented UDP packets on server-initiated traffic. The CSM fails to detect that the packet is fragmented and attempts to alter the UPD source port of the packet. This action overwrites the payload data in the fragmented packet and corrupts the packet. Fragmented packets are also corrupted on return flows, because the CSM overwrites the payload data by attempting to modify the UDP destination port.

  Workaround: None.

- CSCek49160

  When you use the Server/Application State Protocol (SASP) Global Workload Manager (GWM) test tool, the CSM may not register all of the member servers in the SASP group. This problem occurs when the connection between the CSM and the SASP GWM terminates in the middle of a session and returns to service after the CSM times out.

  This problem will cause the SASP test to fail and may cause the whole SASP test suite to fail.

  Workaround: After a connection failure, remove the SASP agent configuration and add it again to register all the real servers in the server farm.

- CSCsc25061

  When running TCP, if fragmented IP packets are processed on a server farm with the NAT server option enabled, the recalculated TCP checksum may be incorrect.

  Workaround: If possible, turn off the NAT server option on the server farms that receive fragmented TCP packets.

- CSCek22782

  A configuration synchronization check for the active and standby CSMs may fail for configurations that contain the following subcommands: **script**, **ARP**, **variable**, **match**, **failaction**, **NAT client**, **probe**, **domain**, and **url-hash**. When you use these subcommands and then you change configurations only in the active or the standby CSM, the wrong configuration synchronization state might be displayed. The module might incorrectly display synchronized configurations as "out-of-sync," and configurations that are out of synchronization as synchronized.

- CSCei73146

  In an active-standby connection state replication setup, the connection counters on the standby CSM were not the same as the counters on the active CSM. The active CSM correctly shows that the connections were load-balanced to various servers within a server farm. On the standby CSM, all replicated connections are assigned to a single real server within a server farm. The number of connections shown in the standby CSM might be different from the number of connections seen in the active CSM. This is a minor issue and does not affect the service.

  Workaround: None.

- CSCsc14905

  A CSM running software release 4.1.2 or later (including 4.2.1 and 4.2.2) will not respond to pings to the virtual server when it is configured with service termination. The server is operational and is passing TCP flows to the real servers, which are also operational. This example shows the configuration:

  ```
  vserver test
   virtual a.b.c.d  tcp 0 service termination
   serverfarm servers1
   persistent rebalance
   domain shrun
   inservice
  ```

  Workaround: Do not configure service termination on the virtual server.

- CSCsb75627

  When you ping to a real server that is reached through a virtual server, which is configured with predictor forward, the ping might fail after the probe to the real server fails. This probe is configured in another server farm with failaction reassign. This example shows the configuration:

  ```
  serverfarm <NAME>
   nat server
   no nat client
   predictor leastconns
   failaction reassign
   real name SERVER-A
     backup real name SERVER-B
     inservice
   real nameSERVER-B
     backup real name SERVER-A
     inservice
   probe <NAME>
  ```

Workaround: If failaction reassign is not required (in case the servers do not share connection states and cannot accept connections opened on the other server), remove failaction or use failaction purge.

- CSCsb56078

  The wrong real server counter is being incremented. There is an incorrect connection counter on the standby CSM. Traffic reaches the backup server farm, and this server farm is using client NAT.

  Workaround: None.

- CSCeg15173

  Fragmented Layer 2 Tunneling Protocol (L2TP) tunneled packets are discarded by the CSM, and the Packets Repeat Reverse Fragmentation counter in the CSM increments quickly. This problem occurs when packets arrive out of order (the MF packets arrive last) and are separated in time by about 10 milliseconds.

  Workaround: Design the network so that all fragments follow the same path, forcing them to arrive in order and closer together. You can also configure a static route in the CSM so that the module knows where to send reassembled fragments that arrived in a reverse order.

- CSCec38106

  On systems that use Cisco IOS software and Catalyst operating system software, when you configure the Catalyst 6500 series switch to trust the DSCP priority bits of the incoming traffic, the CSM might reset the DSCP value to zero (0) if these frames are being forwarded by the CSM.

  Workaround: None.

- CSCec28396

  The **static nat** command is normally used for server-initiated connections. In software release 3.2(1), you can configure the NAT client static into a server farm to take advantage of the static NAT feature for traffic matching a virtual server. If you configured the NAT client static into a sever farm for FTP or RSTP services, this traffic would not be able to pass through the CSM.

  Workaround: Configure a client NAT pool with the server farm IP address instead of using the **static nat** command.

- CSCea43504

  If your configuration contains a pair of CSMs in a single fault-tolerant group and these paired CSMs are in an active-standby state, the CSMs might not retain the valid active-standby state if you add another CSM into this same fault-tolerant group. This action causes the fault-tolerant pair of CSMs to enter an invalid active-active state.

  Workaround: Remove the third CSM from the network and reboot the paired CSMs to allow them to recover their fault-tolerant state.

- CSCdw84018

  The CSM may block or drop all UDP data channels of an RTSP service if the client NAT is also enabled. You must configure a virtual server, which the CSM uses to parse the RSTP service. For this same virtual server, you must also configure a client NAT on the server farm.

  Workaround: Remove the NAT client configuration from the server farm or remove the service RTSP from the virtual server.

- CSCdy67259

  The **TCL ping()** command uses an underlying **ping()** function provided by VxWorks. The VxWorks ping contains a bug that causes the ping function not to display an error when the ping function receives an ICMP error message (for example, host-unreachable). The function remains in a wait loop until it receives a valid response.

If the destination host is in the same subnet (Layer 2 adjacent) as the CSM-configured VLAN, then the ICMP request either receives a valid response or is timed out. In this case, the ping() function will not stop responding.

The problem occurs when the destination IP address is one or more hops away. The router between the CSM and the destination host could respond with a "destination unreachable" message to the CSM if the router determined that the subnet for this IP address is unknown.

Workaround: Do not use the **ping** command in TCL script for a destination that is one hop away.

Resolved Caveats in Software Release 4.2(4)

Note For a description of caveats open in CSM software release 4.2(4), see the "Open Caveats in Software Release 4.2(4)" section on page 41.

This section describes resolved caveats in CSM software release 4.2(4):

- CSCek39783

  The CSM resets the connection that is associated with a route entry in the ARP table, if a learned ARP entry with the same MAC address gets updated with a new MAC address. The underlying problem is that the ARP table in the CSM is getting populated with incorrect entries. This underlying problem is resolved by caveat CSCek39971.

  Workaround: Add a static ARP entry to the CSM configuration for the learned ARP entry (if possible).

  This problem is resolved in CSM software release 4.2(4).

- CSCsc18987

  If two CSMs are running in fault tolerant mode with preempt enabled, and they each have the same priority configured, the modules will continuously oscillate between the active and standby states. This situation occurs when the CSMs both have the same priority and are both running with preempt.

  Workaround: Do not configure the same priority on two CSMs that are running in fault tolerant mode with preempt enabled. If the oscillating state behavior occurs, you must immediately turn off preempt or give one of the CSMs either a higher or lower priority.

  This problem is resolved in CSM software release 4.2(4).

- CSCef10742

  The CSM does not send an SNMP trap when a virtual server is dynamically taken out of service (for example, when all of its real servers have failed).

  Workaround: None.

  This problem is resolved in CSM software release 4.2(4).

- CSCeg52047

  If there is a large amount of data to synchronize between the active and standby CSMs, the **config sync** command may not complete successfully.

  Workaround: Manually replicate the configuration data in the standby CSM.

  This problem is resolved in CSM software release 4.2(4).

- CSCeh66721

  The CSM gradually runs out of memory when more than one HTTP header sticky group is configured for a virtual server.

  Workaround: None.

  This problem is resolved in CSM software release 4.2(4).

- CSCej80361

  When a virtual server is tracking the status of another virtual server (after using the **status-tracking** command), the virtual server status remains out of service, even when the dependent virtual server has returned to service.

  Workaround: None.

  This problem is resolved in CSM software release 4.2(4).

- CSCej80407

  When moderate health-probe traffic is used with the status-tracking feature enabled, the CSM might display a "% No ICC response for TLV type XX from CSM linecard" error message when you enter any command in the CSM CLI. You can session into the system, and traffic continues to flow.

  Workaround: Do not use the status-tracking feature.

  This problem is resolved in CSM software release 4.2(4).

- CSCej83167

  After successfully running the **config sync** command, the CSM status is shown as out-of-sync, even if the configurations are synchronized.

  Workaround: Reboot the standby CSM (with no configuration changes) to correct the synchronization status.

  This problem is resolved in CSM software release 4.2(4).

- CSCek11665

  The CSM does not initiate a failover to the standby CSM when the tracked physical interface is down.

  Workaround: None.

  This problem is resolved in CSM software release 4.2(4).

- CSCek39971

  The ARP table in the CSM is getting populated with entries for the subnet's network address and broadcast addresses. This table should contain only entries for host addresses.

  Workaround: Configure the CSM with static ARP entries for this subnet's network and broadcast addresses.

  This problem is resolved in CSM software release 4.2(4).

- CSCek42608

  When fragmented UDP packets are processed on a server farm with the NAT server option enabled, the recalculated UDP checksum may be incorrect.

  Workaround: If possible, turn off the NAT server option on server farms that receive fragmented UDP packets.

  This problem is resolved in CSM software release 4.2(4).

- CSCek42765

  When configured for fault tolerance, the CSM may oscillate between active state and standby state. This problem occurs when fault tolerance is configured with priorities 253 and 254 and preempt is also configured.

  Workaround: Configure priorities in the range of 0 to 252, and ensure that each CSM has a different priority.

  This problem is resolved in CSM software release 4.2(4).

- CSCek44398

  With FTP service configured on a virtual server, and with client NAT enabled, the CSM is incorrectly setting the TCP sequence numbers on some packets destined to the real server. This problem causes the client session to hang.

  Workaround: None.

  This problem is resolved in CSM software release 4.2(4).

- CSCek45794

  With the variable ROUTE_UNKNOWN_FLOW_PKTS set to 2, the CSM drops all UDP traffic that is directed to virtual servers.

  Workaround: Set the variable ROUTE_UNKNOWN_FLOW_PKTS to zero.

  This problem is resolved in CSM software release 4.2(4).

- CSCek46156

  When loading a large configuration file (18K or more lines long), the CSM cannot ping the local MSFC. If gateway tracking is configured, this problem results in a failover to the standby CSM.

  Workaround: None.

  This problem is resolved in CSM software release 4.2(4).

- CSCsa64249

  While processing an ICMP destination unreachable packet, the CSM may fail and cause a core dump. The syslog message shows the message:

  ```
  ... unexpected error: PPC exception encountered.
  ```

  Workaround: Set the variable DEST_UNREACHABLE_MASK to 0 to disable the CSM from processing ICMP destination unreachable packets.

  This problem is resolved in CSM software release 4.2(4).

- CSCsb74481

  Whenever you have two or more virtual servers using the same real servers, either configure them with the same sever farm or with different server farms pointing to the same real servers. Otherwise, when you clear the connections on one virtual server, the connections on the second virtual server are also cleared.

  This problem has appeared with UDP traffic only. The problem does not occur for TCP connections.

  Workaround: None.

  This problem is resolved in CSM software release 4.2(4).

- CSCsb84180

  The CSM responds to DNS queries from nonexistent domains. After the CSM sends a response to a successful DNS query, queries from nonexistent domains get resolved to the same results used for the configured domains.

  Workaround: None.

  This problem is resolved in CSM software release 4.2(4).

- CSCsb84808

  When two CSMs are configured in a fault tolerant mode, the standby CSM replicates the connection data from the active CSM.

  However, if you reset the active CSM (and the standby CSM takes over), SSL connections are not replicated when the CSM comes back online. If there is a subsequent failover, the CSM may not handle the existing connections correctly.

  Workaround: None.

  This problem is resolved in CSM software release 4.2(4).

- CSCsc74507

  When using the cookie insert feature, two IP addresses may resolve to the same entry in the sticky table, and the second entry will be discarded. These sticky connections will not work correctly (for example, packets will not all be directed to the same real server).

  Workaround: None.

  This problem is resolved in CSM software release 4.2(4).

- CSCsd04062

  When using the cookie insert feature, cookie sticky entries remain in the sticky table even after the sticky group configuration is removed from the virtual server.

  If the same sticky group number is reused for another configuration, the old entries show up in the new sticky group.

  Workaround: Do not reuse the sticky group numbers.

  This problem is resolved in CSM software release 4.2(4).

- CSCsd13447

  After a reload, the CSM incorrectly sets the GSLB real state to unavailable, even though the probes and the virtual server are operational. The CSM subsequently sends DNS responses that reflect the incorrect state. This problem results in client requests being directed away from this CSM, even though it is operational.

  Workaround: None.

  This problem is resolved in CSM software release 4.2(4).

- CSCsd21983

  The probe recovery value for real servers is not processed correctly. A failed real server will become operational again only after one extra positive response.

  For example, if you set the probe recovery value to 3, the real server must generate 4 (instead of 3) positive responses before the CSM sets the server to operational.

  Workaround: Set the probe recovery value to one less than your desired number of positive responses.

  This problem is resolved in CSM software release 4.2(4).

- CSCsd34096

  When you reconfigure a virtual server to use a different server farm, sticky entries are not automatically cleared. These entries cause packets to be directed to the server farm that is no longer active in the virtual server's configuration.

  Workaround: Clear the sticky table when you reconfigure a virtual server to use a different server farm.

  This problem is resolved in CSM software release 4.2(4).

- CSCsd56470

  The CSM may lock up when multiple users try to process XML configuration files at the same time.

  Workaround: None.

  This problem is resolved in CSM software release 4.2(4).

- CSCsd77736

  The following syslog message contains the deprecated **show ip slb memory** command.

  ```
  %CSM_SLB-3-UNEXPECTED: Module # unexpected error:
  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.
  ```

  The message should reference the **show module csm** *slot* **memory** command.

  Workaround: None.

  This problem is resolved in CSM software release 4.2(4).

- CSCsd80681

  During a configuration synchronization between the active CSM and the standby CSM, the supervisor engine might reload either the active or standby CSM due to missing keepalive messages. This action might be related to the number of connections actively getting replicated at the time of the configuration synchronization.

  Workaround: None.

  This problem is resolved in CSM software release 4.2(4).

- CSCsd92029

  With a Layer 7 policy configured on a non-TCP virtual server, the CSM fails to free up the small buffers. Eventually, the CSM will stop processing packets (there are 24,000 small buffers). You can inspect the number of available small buffers by using the following command:

  show mod csm *slot* **tech proc 2**

  Workaround: Do not configure a Layer 7 policy on a non-TCP virtual server.

  This problem is resolved in CSM software release 4.2(4).

- CSCse76730

  If a retransmitted TCP segment has overlapping data with the segment currently being processed, the CSM crashes with a core dump header: FPGA3 IXIC_TAGERR.

  This problem indicates that a Tag error has occurred in FPGA3.

  Workaround: None.

  This problem is resolved in CSM software release 4.2(4).

Open and Resolved Caveats in Software Release 4.2(3a)

These sections describe the open and resolved caveats in CSM software release 4.2(3a):

- Open Caveats in Software Release 4.2(3a), page 49
- Resolved Caveats in Software Release 4.2(3a), page 52

Open Caveats in Software Release 4.2(3a)

Note For a description of caveats resolved in CSM software release 4.2(3a), see the "Resolved Caveats in Software Release 4.2(3a)" section on page 52.

This section describes open caveats in CSM software release 4.2(3a):

- CSCsd80681

  During a configuration synchronization between the active CSM and the standby CSM, the supervisor engine might reload either the active or standby CSM due to missing keepalives. This action might be related to the number of connections actively getting replicated at the time of the configuration synchronization.

  Workaround: None.

- CSCej80407

  When moderate health-probe traffic is used with the status-tracking feature enabled, the CSM might display a "% No ICC response for TLV type XX from CSM linecard" error message when you enter commands. You can session into the system, and traffic continues to pass. This problem occurs with CSM software release 4.2.x

  Workaround: Do not use the status-tracking feature.

- CSCej58455

  A configuration synchronization check for the active and standby CSMs may fail for configurations that contain the following subcommands: **script**, **ARP**, **variable**, **match**, **failaction**, **NAT client**, **probe**, **domain**, and **url-hash**. When you use these subcommands and then you change configurations only in the active or the standby CSM, the wrong configuration synchronization state might be displayed. The module might incorrectly display synchronized configurations as "out-of-sync," and configurations that are out of synchronization as synchronized.

  Workaround: None.

- CSCei73146

  In an active-standby connection state replication setup, the connection counters on the standby CSM were not the same as the counters on the active CSM. The active CSM correctly shows that the connections were load-balanced to various servers within a server farm. On the standby CSM, all replicated connections are assigned to a single real server within a server farm. The number of connections shown in the standby CSM might be different from the number of connections seen in the active CSM. This is a minor issue and does not affect the service.

  Workaround: None.

- CSCsc18987

  If there are two CSMs running in fault tolerant mode with preempt enabled, and they each have the same priority, the modules will continuously change their roles (flip-flop) between active and standby. This situation occurs when the CSMs both have the same priority and are both running with preempt.

  Workaround: Do not configure two CSMs that are running in fault tolerant mode with preempt and that have the same priority configured. If the role changing (flip-flop) behavior occurs, you must immediately turn off preempt or give one of the CSMs either a higher or lower priority.

- CSCsc14905

  A CSM running software release 4.1.2 or later (including 4.2.1 and 4.2.2) will not respond to pings to the virtual server when it is configured with service termination. The server is operational and is passing TCP flows to the real servers, which are also operational. This example shows the configuration:

  ```
  vserver test
   virtual a.b.c.d  tcp 0 service termination
   serverfarm servers1
   persistent rebalance
   domain shrun
   inservice
  ```

  Workaround: Do not configure service termination on the virtual server.

- CSCsb75627

  When you ping to a real server that is reached through a virtual server, which is configured with predictor forward, the ping might fail after the probe to the real server fails. This probe is configured in another server farm with failaction reassign. This example shows the configuration:

  ```
  serverfarm <NAME>
   nat server
   no nat client
   predictor leastconns
   failaction reassign
   real name SERVER-A
     backup real name SERVER-B
     inservice
   real nameSERVER-B
     backup real name SERVER-A
     inservice
   probe <NAME>
  ```

  Workaround: If failaction reassign is not required (in case the servers do not share connection states and cannot accept connections opened on the other server), remove failaction or use failaction purge.

- CSCsb74481

  Whenever you have two or more virtual servers using the same real servers, either configure them with the same sever farm or with different server farms pointing to the same real servers. Otherwise, when you clear the connections on one virtual server, the connections on the second virtual server are also cleared.

  This problem has appeared with UDP traffic only. This problem does not occur for TCP connections. This problem affects all CSM software releases.

  Workaround: None.

- CSCsb56078

The wrong real server counter is being incremented. There is an incorrect connection counter on the standby CSM. Traffic reaches the backup server farm, and this server farm is using client NAT.

Workaround: None.

- CSCeg15173

  Fragmented Layer 2 Tunneling Protocol (L2TP) tunneled packets are discarded by the CSM, and the Packets Repeat Reverse Fragmentation counter in the CSM increments quickly. This problem occurs when packets arrive out of order (the MF packets arrive last) and are separated in time by about 10 milliseconds.

  Workaround: Design the network so that all fragments follow the same path, forcing them to arrive in order and closer together. You can also configure a static route in the CSM so that the module knows where to send reassembled fragments that arrived in a reverse order.

- CSCec38106

  On systems that use Cisco IOS software and Catalyst operating system software, when you configure the Catalyst 6500 series switch to trust the DSCP priority bits of the incoming traffic, the CSM might reset the DSCP value to zero (0) if these frames are being forwarded by the CSM.

  Workaround: None.

- CSCec28396

  The **static nat** command is normally used for server-initiated connections. In software release 3.2(1), you can configure the NAT client static into a server farm to take advantage of the static NAT feature for traffic matching a virtual server. If you configured the NAT client static into a sever farm for FTP or RSTP services, this traffic would not be able to pass through the CSM.

  Workaround: Configure a client NAT pool with the server farm IP address instead of using the **static nat** command.

- CSCea43504

  If your configuration contains a pair of CSMs in a single fault-tolerant group and these paired CSMs are in an active-standby state, the CSMs might not retain the valid active-standby state if you add another CSM into this same fault-tolerant group. This action causes the fault-tolerant pair of CSMs to enter an invalid active-active state.

  Workaround: Remove the third CSM from the network and reboot the paired CSMs to allow them to recover their fault-tolerant state.

- CSCdw84018

  The CSM may block or drop all UDP data channels of an RTSP service if the client NAT is also enabled. You must configure a virtual server, which the CSM uses to parse the RSTP service. For this same virtual server, you must also configure a client NAT on the server farm.

  Workaround: Remove the NAT client configuration from the server farm or remove the service RTSP from the virtual server.

- CSCdy67259

  The **TCL ping()** command uses an underlying **ping()** function provided by VxWorks. The VxWorks ping contains a bug that causes the ping function not to display an error when the ping function receives an ICMP error message (for example, host-unreachable). The function remains in a wait loop until it receives a valid response.

  If the destination host is in the same subnet (Layer 2 adjacent) as the CSM-configured VLAN, then the ICMP request either receives a valid response or is timed out. In this case, the ping() function will not stop responding.

The problem occurs when the destination IP address is one or more hops away. The router between the CSM and the destination host could respond with a "destination unreachable" message to the CSM if the router determined that the subnet for this IP address is unknown.

Workaround: Do not use the **ping** command in TCL script for a destination that is one hop away.

Resolved Caveats in Software Release 4.2(3a)

Note For a description of caveats open in CSM software release 4.2(3a), see the "Open Caveats in Software Release 4.2(3a)" section on page 49.

This section describes resolved caveats in CSM software release 4.2(3a):

- CSCeh61946

  When the CSM receives KAL-AP probes from a GSS, the CSM loses memory, which results in the command operations slowing down and eventual lockup of the CSM.

  Workaround 1: Do not send GSS KAL-AP keepalives to the CSM.

  Workaround 2: When the available memory of the CSM falls below 40 percent, reload the CSM.

- CSCdy30354

  In CSM software releases 4.1.x and 4.2.x, if heavy cookie-insert traffic is used, the core routine might reboot the system before a core is generated. This action results in a supervisor engine reload without a core.

- CSCsd54286

  A cookie insert applied to a jumbo frame causes the module to fail. If the packet is resolved in the Layer 7 module and has four distinct segments to transmit during cookie insert, the Layer 7 module must send two transmit commands. The failure occurs when the second command does not advance the tail pointer in the command queue, causing a repeat of the second partially transmitted command. The invalid transmission may be caught as an illegal header. Sometimes the transmitted command will transmit a faulty packet, which also causes a failure. This situation occurs when a packet larger than the configured MSS is received.

- CSCsd58615

  Sending a multipacket POST to a cookie insert virtual server can cause misclassified packets. When a session becomes invalid, the TCP module attempts to transmit the buffers stored at Layer 7. When those packets are sent from the Layer 7 insert, they must be treated differently from packets from other layers. Some data packets are processed in Layer 4, and then switched to Layer 7 processing. When this layer switching occurs, data packets are counted twice, once as Layer 4 packets and once as Layer 7 packets.

  Workaround: None.

- CSCsd27478

  The CSM might reload with an FPG4 exception in icp.fatPath length error (icpFatErr). This condition occurs when overlapping TCP segments are sent to the CSM out of order.

- CSCsc56986

  A CSM header or cookie insert causes a TCP checksum error when the CSM operates under a heavy load (> 1000 conn/sec).The CSM may incorrectly set the TCP checksum, which causes delays because of retransmission of the packets. This checksum error appears on both the client side and the server side.

This situation occurs only with a virtual server using a cookie insert sticky group or a header insert function.

Workaround: None.

- CSCsd27970

  The CSM drops HTTP GETs to a server on the back end of the Layer 7 connection. CSM release 4.1.x removed the SYNC for TX_CMD messages from TCP to Layer 7. The removed synchronization was replaced for the non-cookie insert case in CSM release 4.1(6).

  Workaround: None.

- CSCek03020

  When sending an incorrect message length from a simulated Server/Application State Protocol (SASP) global workload manager (GWM), the CSM logs the following system messages and reboots:

  ```
  %CSM_SLB-3-UNEXPECTED: Module 9 unexpected error: SASP: connected to GWM ac1f6529:5555
  %C6KPWR-SP-4-DISABLED: power to module in slot 9 set off (Module not responding to
  Keep Alive polling)
  %DIAG-SP-6-RUN_MINIMUM: Module 9: Running Minimum Diagnostics...
  %DIAG-SP-6-DIAG_OK: Module 9: Passed Online Diagnostics
  %OIR-SP-6-INSCARD: Card inserted in slot 9, interfaces are now online
  ```

  Workaround: None.

- CSCsc77672

  Running a load test that sends traffic to a single virtual server with cookie sticky configured causes the IXP1 engine to stop operating after a few minutes of operation. The IXP1 engine shows a CPU utilization that exceeds 100 percent. The ARP table is empty and traffic stops.

  Workaround: None.

- CSCsc53146

  When a virtual server is configured for UDP service per-packet, UDP packets are dropped when performing per-packet load balancing. A CSM module can drop UDP packets and display them in the “packets dropped” column when you enter the **show module csm** *mod_number* **tech-support processor 2** command.

  This symptom occurs in CSM modules running either CSM release 4.1.5 or release 4.2.3, and is present in both the Cisco IOS or the Cisco IOS and Catalyst operating system modes.

  Workaround: Remove the “service per-packet” option from the virtual address configuration in the virtual server.

- CSCsb59273

  The CSM uses its own MSS when using sticky cookie insert. The CSM does not consider the client-sent MSS (from the client SYN signal) but uses its own MSS (the one sent in CSMs SYN-ACK signal) to determine how the server response may increase when inserting a cookie.

  In the client, the CSM paths with an effective MSS (due to a lower processor maximum transmission unit [PMTU]) that is lower than the MSS of the CSM causes the server response to be dropped. When the server response is dropped, the client never receives the first segment of the server response.

  Workaround: Manually lower the MSS of the CSM with the **variable TCP_MSS_OPTION** *new value* command. You may also use a TCP MSS adjustment on a device (such as Cisco PIX Firewall) between the CSM and the lower MTU boundary (such as the start of a tunnel).

Open and Resolved Caveats in Software Release 4.2(3)

These sections describe the open and resolved caveats in CSM software release 4.2(3):

- Open Caveats in Software Release 4.2(3), page 54
- Resolved Caveats in Software Release 4.2(3), page 57

Open Caveats in Software Release 4.2(3)

Note For a description of caveats resolved in CSM software release 4.2(3), see the "Resolved Caveats in Software Release 4.2(3)" section on page 57.

This section describes open caveats in CSM software release 4.2(3):

- CSCej58455

  A configuration synchronization check for the active and standby CSMs may fail for configurations with the following subcommands: script, ARP, variable, match, failaction, NAT client, probe, domain, and url-hash. When using these sub-commands, changing configurations only in the active or the standby CSM may display the wrong configuration synchronization state. The module may show synchronized configurations as out-of-sync, and out of sync configurations as in-sync

  Workaround: For configurations including the subcommands script, ARP variable, match, failaction, NAT client, probe, domain, and url-hash sub-commands you must manually ensure that the configuration commands and sub-commands are synchronized at both the active and standby modules.

- CSCei73146

  In an active-standby connection state replication setup, the connection counters on the standby CSM were not the same as the counters on the active CSM. The active CSM correctly shows that the connections were load-balanced to various servers within a server farm. On the standby CSM, all replicated connections are assigned to a single real server within a server farm. The number of connections shown in the standby CSM might be different from the number of connections seen in the active CSM. This is a minor issue and does not affect the service.

  Workaround: None.

- CSCsc18987

  If there are two CSMs running in fault tolerant mode with preempt enabled and they each have the same priority the modules will continuously change their roles (flip-flop) between active and standby. The CSMs must have the same priority and both must be running with preempt for this situation to occur.

  Workaround: Do not configure two CSMs running in fault tolerant mode with preempt and the same priority configured. If the role changing (flip-flop) behavior occurs then you must immediately turn off preempt or give one of the CSMs either a higher or lower priority.

- CSCsc14905

  A CSM running software release 4.1.2 or later (including 4.2.1 and 4.2.2) will not respond to pings to the virtual server when it is configured with service termination. The server is operational and passing TCP flows to the real servers, which are also operational. This example shows the configuration:

  ```
  vserver test
   virtual a.b.c.d  tcp 0 service termination
  ```

```
 serverfarm servers1
 persistent rebalance
 domain shrun
 inservice
```

Workaround: Do not configure service termination on the virtual server.

- CSCsb75627

  When you ping to a real server reached through a virtual server that is configured with predictor forward the ping might fail after the probe to the real server fails. This probe is configured in another server farm with failaction reassign. This example shows the configuration:

```
serverfarm <NAME>
 nat server
 no nat client
 predictor leastconns
 failaction reassign
 real name SERVER-A
   backup real name SERVER-B
   inservice
 real nameSERVER-B
   backup real name SERVER-A
   inservice
 probe <NAME>
```

  Workaround: If failaction reassign is not required (in case the servers do not share connection states and cannot accept connections opened on the other server), remove failaction or use failaction purge.

- CSCsb74481

  Whenever you have two or more virtual servers using the same real servers, either configure them with the same sever farm or with different server farms pointing to the same real servers. Otherwise, when you clear the connections on one virtual server, the connections on the second virtual server are also cleared.

  This problem has appeared with UDP traffic only. The problem does not occur for TCP connections. It affects all CSM software releases.

  Workaround: None.

- CSCsb59273

  If the total of (real server response segment size) + (size of inserted cookie) exceeds the CSM MSS value of 1460, the CSM splits the result in multiple segments, with a maximum of the CSM MSS value.

  Workaround: Manually lower the CSM MSS with the **variable TCP_MSS_OPTION** *new value* command.

- CSCsb56078

  The wrong real server counter is being incremented. There is an incorrect connection counter on the standby CSM. Traffic reaches the backup server farm and this server farm is using client NAT.

  Workaround: None.

- CSCeg15173

  Fragmented Layer Two Tunneling Protocol (L2TP) tunneled packets are discarded by the CSM, and the Packets Repeat Reverse Fragmentation counter in the CSM increments quickly. This problem occurs when packets arrive out of order (the MF packets arrive last) and are separated in time by about 10 milliseconds.

Workaround: Design the network so that all fragments follow the same path, forcing them to arrive in order and closer together, or you can configure a static route in the CSM so that the module knows where to send re-assembled fragments that arrived in a reverse order.

- CSCec38106

  On systems that use Cisco IOS software and Catalyst operating system software, when you configure the Catalyst 6500 series switch to trust the DSCP priority bits of the incoming traffic, the CSM might reset the DSCP value to zero (0) if these frames are being forwarded by the CSM.

  Workaround: None.

- CSCec28396

  The **static nat** command is normally used for server-initiated connections. In release 3.2(1) you can configure the NAT client static into a server farm to take advantage of the static NAT feature for traffic matching a virtual server. If you configured the NAT client static into a sever farm for FTP or RSTP services, this traffic would not be able to pass through the CSM.

  Workaround: Configure a client NAT pool with the server farm IP address instead of using the **static nat** command.

- CSCea43504

  If your configuration contains a pair of CSMs in a single fault-tolerant group and these paired CSMs are in an active-standby state, the CSMs might not retain the valid active-standby state if you add another CSM into this same fault-tolerant group, causing the fault-tolerant pair of CSMs to enter an invalid active-active state.

  Workaround: Remove the third CSM from the network and reboot the paired CSMs to allow them to recover their fault-tolerant state.

- CSCdw84018

  The CSM may block or drop all UDP data channels of an RTSP service if the client NAT is also enabled. You must configure a virtual server, which the CSM uses to parse the RSTP service. For this same virtual server, you must also configure a client NAT on the server farm.

  Workaround: Remove the NAT client configuration from the server farm or remove the service RTSP from the virtual server.

- CSCdy67259

  The **TCL ping()** command uses an underlying **ping()** function provided by VxWorks. The VxWorks ping contains a bug, which, if the function receives an ICMP error message (for example host-unreachable), the function does not return with an error. The function remains in a wait loop until it receives a valid response.

  If the destination host is in the same subnet (Layer 2 adjacent) as the CSM-configured VLAN, then the ICMP request either receives a valid response or is timed out. In this case, the ping() function will not stop responding.

  The problem occurs when the destination IP address is one or more hops away. The router between the CSM and the destination host could respond with a “destination unreachable” message to the CSM if the router determined that the subnet for this IP address is unknown.

  Workaround: Do not use the **ping** command in TCL script for a destination that is one hop away.

Resolved Caveats in Software Release 4.2(3)

Note For a description of caveats open in CSM software release 4.2(3), see the "Open Caveats in Software Release 4.2(3)" section on page 54.

This section describes resolved caveats in CSM software release 4.2(3):

- CSCsb71260

  When you configure the cookie insert feature with other map policies under a virtual server, the CSM re-inserts a new cookie for each new TCP connection, even if a cookie was inserted previously. The CSM re-inserts new cookies when the existing map policies do not have a match and cookie insert is the default policy.

  Workaround: None

- CSCsb64954

  When configuring the CSM with a virtual server using the **service rtsp** command, the MP4 files streaming through the CSM may have poor video or audio quality. The data sequence mismatch counter under the TCP statistics section of the **show tech** command will also increment.

  Workaround: Do not use the **service rtsp** command.

- CSCsb46265

  When changing a VLAN IP address, an ARP timeout can be triggered. When this situation occurs, the encapsulated identification table is refreshed and each MAC address in the table may be assigned a new encapsulated identification. This problem occurs because the CSM is not updated with the new encapsulated identification. The CSM continues using the previous encapsulated identification, which results in traffic being forwarded to the wrong destination.

  Workaround: Configure static ARP entries for the CSM gateways.

- CSCsb40988

  After reaching the maximum number of connections, the sticky timer may not start for new traffic flows. This situation occurs with the **variable NO_TIMEOUT_IP_STICKY_ENTRIES 1** command configured on a CSM and with the **maxconns** command configured on the real server. The sticky timer also does not start when connections are deleted.

  Workaround: Removing the maximum connections configuration.

- CSCsb17046

  When an associated virtual server goes out of service and then returns to in service, the CSM does not use a real server if the traffic load threshold is configured above 254. This situation occurs because the traffic load of a local GSLB real server becomes stuck at a threshold of 255, preventing the CSM to use this real server when answering a DNS request.

  Workaround: None.

- CSCsb08993

  On a CSM using release 4.2(2) software and configured with the **variable NO_TIMEOUT_IP_STICKY_ENTRIES 1** command, the sticky timeout counter remains 0 regardless of when the idle timer expires. This situation occurs only after changing the configuration with the **sticky group** command when traffic flows are active.

  Workaround: Do not modify the sticky group configuration when there are active traffic flows.

- CSCsb02873

  Two columns display incorrect values for the total pending counter that is received when using the **show module csm X tech probe** command.

  In the display, the left column is supposed to show the total number of probe attempts, and the right column is supposed to show the difference between the current value and the last time you entered the **show** command.

  Workaround: None.

- CSCsa88370

  When more than one route or gateway is configured to connect to a remotely located real server, the remote real server might experience an ARP failure and become unreachable after one of the gateways fails. This situation occurs although a valid gateway or route may still be available.

  Workaround: Use the s**how mod csm** *slot* **arp** command to locate the unavailable gateway, and remove that gateway from the configuration.

- CSCej08044

  Interface device tracking fails when a preempt is configured. The active CSM changes its state to standby when the interface and gateway are shut down. When the interface and gateway are returned to operation, the CSM state does not return to active as it should.

  Workaround: None.

- CSCei94412

  When the CSM is in bridge mode with HSRP configured on the client VALN and the server's default gateway is pointing to that HSRP address, flooding may occur when the HSRP virtual MAC address is aged out from the switches CAM tables (default 5 minutes of inactivity).

  Workaround

  - Increase the mac-address-table aging timer in the server VLANs
  - Use the **standby use-bia** command.

- CSCei91610

  The CSM is not passing ACK or RST requests to real servers.

  Workaround: None.

- CSCei91452

  The FTP data channel crashes 15 minutes into the data transfer as a result of the CSM calculation for timestamps. During non-FTP operation, the data plane monitors flows and times out connections. For FTP however, the PPC must monitor the FTP connections and their timestamps. The session IXP must provide the last time that the flow contained traffic. The PPC will query the session process for the last time (in ticks) that the flow contained traffic and performs a ticks to seconds conversion, multiplying ticks times (134/166) to calculate real seconds.

  The conversion function assumes that the maximum possible for the ticks return value was 0x00ffffff. If the number of ticks returned was greater than 0x00ffffff, the conversion function returns a -1. Because the actual maximum return value from session is 0x0ffffff but the timestamp that was calculated was greater than 0x00ffffff, the session is flagged for a timeout, because the conversion was in error and had returned a -1.

Note This problem occurs after the CSM has been in operation for (0x00ffffff)*(134/166) seconds, or about 156 days. Also, the FTP data channel is timed out only after 15 minutes, so shorter transfers are unaffected.

Workaround: A work around exists that should be performed at the specific direction of TAC or other Cisco Personnel. This caveat manifests itself after the CSM has been up for over 156 days, so please contact TAC if you feel that this bug is affecting you.

- CSCei38917

  The CSM is dropping Layer 3 fragmented IP packets on traffic flows destined for a virtual server. This situation occurs in a basic server load balancing (SLB) design that connects to an all zero's virtual server (0.0.0.0/0) with no NAT client and a non NAT server configured on the server farm. The traffic flows are set up properly and fail when packets in both directions are dropped or incorrectly routed to the gateway.

  Workaround: Downgrade to the CSM software release 4.1(2) or earlier.

- CSCei37874

  A server does not enter slow start mode when sending traffic at a slow pace of 1cps with the variable REAL_SLOW_START_ENABLE set to 1. This situation occurs when an IP address on an ICMP probe is configured on a real server and is then activated. The probe receives all of the new connections until it is again load balanced with the other servers. However, the slow start configured server does not appear to be in the slow start mode.

  Workaround: None.

- CSCei34913

  A CSM drops the out-of-order TCP segments when load balancing at Layer 7 and is waiting for the client to retransmit the segments. TCP segments must be in order, or they are dropped

  Workaround: None.

- CSCei34381, CSCdy00154

  When testing redundancy failovers, the assumed priority value does not change on the active CSM. The priorities are the same between the CSM with no preempt configured. Under these conditions, the higher MAC address takes the active role when there is an active CSM to active CSM situation. Caveat CSCdy00154 provided a fix in CSM software release 3.1(4). The last active CSM remains active which is the correct behavior with CSCdy00154.

  Workaround: None.

- CSCei58018

  When a reset is sent to the CSM and merged out of order packet handling is configured and the sequence number is set to acknowledge the first, but not the last packet sent.

  Workaround: None.

- CSCei35703

  The unsuccessful load-balancing decision message is not displayed in TCP when the process reaches the maximum parse length value that was configured.

  Workaround: None.

- CSCei28436

  A TCP segment may be corrupted on the CSM during an FTP control session, causing the control session to lose synchronization between the client and the CSM. This problem causes the FTP session to fail, usually when file transfers passing several hundreds of files are performed with the same FTP control connection.

  Workaround: None.

- CSCei26434

  The CSM in some cases load-balances to just one real server instead of all operational real servers in a server farm using predictor least-connections. The conditions which lead the CSM into this error condition are:

  a. The real server fails the health probe check prior to this server farm first when activated either by one of these situations:

     •The predictor was changed from other to least-connections

     •The CSM was first rebooted.

     •The CSM became fault-tolerant (FT) active for the first time.

  b. After traffics went through this server farm. Other servers were selected.

  c. When this real server was re-enabled because it passed the health probe check, all the new connection requests are load-balanced only to this real server.

  This problem exists in release 4.1(4) & 4.2(2).

  Workaround: Use another predictor method, and then set this server to out-of-service and then back to inservice after it passes the health check.

- CSCei16475

  If a real server crashes, the sticky timer remains disabled. This symptom is observed when you configure the **variable NO_TIMEOUT_IP_STICKY_ENTRIES 1** command on the CSM.

  Workaround: Disable the variable command.

- CSCeh76411

  When using the CSM NAT pool feature with an FTP virtual server you can allocate ports from the NAT pool and never reclaim those ports. The problem reproduces when a client attempts to re-use an FTP data connection that was used previously in the same session.

  This condition can cause the number of available ports to diminish in this configuration:

  a. Configure service FTP on a virtual server.

  b. Configure client NAT pool for that virtual server.

  The FTP client re-uses the same port when opening the FTP data connections for this same FTP control connection.

  Workaround: Reboot the CSM to recover the allocated ports.

- CSCeh73953

  The CSM can crash during configuration if you remove slb-policies that have a priority option specified. If you do not specify a priority option for slb-policies, the problem does not occur.

  Only the removal of the first policy item in the policy list is allowed when using the **no slb-policy** command. For example, the **no slb-policy P1** command is allowed, but entering the **no slb-policy P2** command causes the CSM to crash.

  Workaround: Remove only the first or top slb-policy item in the policy list.

- CSCeh60960

  When running in router mode with the variable var ROUTE_UNKNOWN_FLOW_PKTS set to either 1 or 2, ICMP or UDP packets do not go directly to the access servers located behind the CSM. Telnet to these servers works fine when this value is set to 2, which is expected.

  Workaround: None.

- CSCeh60704

  The sticky table does not replicate after a configuration synchronization. This situation occurs when traffic is sent to a virtual server that is configured with the **csrp sticky** and **csrp connection**.

  Workaround: Reload the active CSM. Reloading the standby CSM does not correct the problem.

- CSCeh55357

  The CSM incorrectly releases the session entries after performing load-balancing for HTTP redirect-server. This condition causes some of the subsequent requests to the CSM to fail. The following conditions trigger the incorrect releasing of the session or traffic flow entries:

  a. A Layer 7 virtual server was configured with the HTTP persistent rebalance option enabled.

  b. The first two GET requests of a single TCP connection were load-balanced to an HTTP real server.

  c. The third (or subsequent) HTTP GET requests are load-balanced to a configured redirect server.

  After performing an HTTP redirect response for this connection, the CSM does not clean up the session or traffic flow entries for this connection. When a new connection enters the CSM, the CSM re-uses this session entry and fails to perform load balancing for the new request.

  If you enter the **show module csm <slot> tech-support proc 1** command and the value for the attempts to allocate used session counter are shown as incremented in the displayed output, a defect occurred.

  Workaround: Remove the persistent rebalance option for the virtual server.

- CSCeh41862

  When the track gateway feature is used for CSM failover functionality and the host or gateway is more than one hop away from the CSM, the module enters the standby state even if you can ping the host from the CSM. The CSM is attempting to request ARP for the host.

  Workaround: None.

- CSCeg04864

  Configuring cookie switching with multiple cookie values for a specific cookie name, the CSM may incorrectly load balance the request.

  This problem occurs only when the "or" pipe (|) is used between cookie values. Using the pipe character causes the CSM to incorrectly search the second or later regular expression parameter in all of the cookies in the HTTP header and not just the configured cookie name.

  For the expression *ABC | *XYZ the correct syntax must include parentheses around the alternate OR condition as follows: (*ABC | *XYZ).

  Workaround: Enter the parentheses into the matching string.

- CSCed82590

  The CSM forwards ICMP reply packets to the backup CSM instead of forwarding them to the MSFC resulting in a communication failure. This failure occurs when a virtual server designated to load balance the ICMP traffics was configured without a termination process for ICMP request. An appropriate idle or pending timer must be configured to allow the CSM to remember this ICMP request for the specified time.

  Workaround: Configure the virtual server for the ICMP traffics with an appropriate idle timeout value. This configuration allows the CSM to clean up the ICMP flow as soon as the request and reply are complete.

- CSCec75637

  The CSM issues ARP requests only for the configured routers or real servers but not for clients or routers where the client traffic originates. The CSM can learn them only from ARP requests received. If there is no ARP entry for a device, traffic is dropped. The traffic to a virtual source from one of these clients is also dropped.

  This situation becomes a problem in a redundancy setup that is configured with preempt. When an initial failover occurs and the preempt CSM takes becomes active, the clients that are local to the CSM client VLAN (usually a cache or proxy device) are not learned.

  Workaround: Configure a dummy real server to force the CSM to ARP, move the client a router hop away, or reduce the ARP timeout on the client.

Open and Resolved Caveats in Software Release 4.2(2)

These sections describe the open and resolved caveats in CSM software release 4.2(2):

- Open Caveats in Software Release 4.2(2), page 63
- Resolved Caveats in Software Release 4.2(2), page 65

Open Caveats in Software Release 4.2(2)

Note For a description of caveats resolved in CSM software release 4.2(2), see the "Resolved Caveats in Software Release 4.2(2)" section on page 65.

This section describes open caveats in CSM software release 4.2(2):

- CSCeg77526

  After you enter the **script file bootflash:myscript.txt** command to load a script file into the CSM, the output of the **show module csm** *slot* **script** command lists all of the script functions that were loaded into the CSM. When you enter the **no script file bootflash:myscript.txt** command to remove the script file configuration, the **show** command for the script continues to display the same list of script functions.

  This situation occurs because the individual script was loaded into the CSM by using the **script file** command, which loads the script into memory. The CSM does not have a command that allows you to request a reload of the same script file to update the individual script.

  To reload the script with the same filename (but with newer content), perform these steps:

  a. Remove the script with the **no script file bootflash:myscript.txt** command. This command does not destroy nor stop the current probes that are using the existing scripts.

  b. Then, enter the **script file bootflash:myscript.txt** command to reload the new content. The probes will pick up the new script in the next interval of operation.

  Workaround: None. This is the current design for reloading a script. The scripts must remain in memory for the probes to operate. If you want to stop the probes from using those scripts, you must remove the probes. Scripts removed from the CSM remain in memory.

- CSCdy67259

  The **TCL ping**() command uses an underlying **ping**() function provided by VxWorks. The VxWorks ping contains a bug, which, if the function receives an ICMP error message (for example host-unreachable), the function does not return with an error. The function remains in a wait loop until it receives a valid response.

  If the destination host is in the same subnet (Layer 2 adjacent) as the CSM-configured VLAN, then the ICMP request either receives a valid response or is timed out. In this case, the ping() function will not stop responding.

  The problem occurs when the destination IP address is one or more hops away. The router between the CSM and the destination host could respond with a "destination unreachable" message to the CSM if the router determined that the subnet for this IP address is unknown.

  Workaround: Do not use the **ping** command in TCL script for a destination that is one hop away.

- CSCeg15173

  Fragmented Layer Two Tunneling Protocol (L2TP) tunneled packets are discarded by the CSM, and the Packets Repeat Reverse Fragmentation counter in the CSM increases quickly. This problem occurs when packets arrive out of order (the MF packets arrive last) and are separated in time by about 10 milliseconds.

  Workaround: Design the network so that all fragments follow the same path, forcing them to arrive in order and closer together, or you can configure a static route in the CSM so that it knows where to send re-assembled fragments that arrived in a reverse order.

- CSCea43504

  If your configuration contains a pair of CSMs in a single fault-tolerant group and these paired CSMs are in an active-standby state, the CSMs might not retain the valid active-standby state if you add another CSM into this same fault-tolerant group, causing the fault-tolerant pair of CSMs to enter an invalid active-active state.

  Workaround: Remove the third CSM from the network and reboot the paired CSMs to allow them to recover their fault-tolerant state.

- CSCdw84018

  The CSM may block or drop all UDP data channels of an RTSP service if the client NAT is also enabled. You must configure a virtual server, which the CSM uses to parse the RSTP service. For this same virtual server, you must also configure a client NAT on the server farm.

  Workaround: Remove the NAT client configuration from the server farm or remove the service RTSP from the virtual server.

- CSCdv11685

  When more than one pair of redundant CSMs are configured to use the same VLAN ID, the CSM will accept replication messages from all fault-tolerant groups by using the specified VLAN. In this configuration, the session and sticky replication may not work properly.

  Workaround: Configure a unique VLAN trunk for each pair of fault-tolerant groups.

- CSCec28396

  The **static nat** command is normally used for server-initiated connections. In release 3.2(1) you can configure the NAT client static into a server farm to take advantage of the static NAT feature for traffic matching a virtual server. If you configured the NAT client static into a sever farm for FTP or RSTP services, this traffic would not be able to pass through the CSM.

  Workaround: Configure a client NAT pool with the server farm IP address instead of using the **static nat** command.

- CSCeb47499

  The UDP probe configured for a server farm can only detect a failure of a UDP service when the connectivity to the server IP address is opened. The CSM relies on the ICMP port unreachable message from the server so that it can detect whether the UDP service is available. If the interface on the server is down, the UDP probe cannot detect this failure condition.

  Workaround: Configure an ICMP probe to the same server farm where the UDP probe is configured.

- CSCeb52054

  When the Layer 7 virtual servers have many connections that are in the process of load-balancing, the new and existing connections experience slow response from the CSM. The connections, which are still waiting for more data from the client or which are waiting for the response from the server, are considered to be in the process of load-balancing.

  Workaround: Configure the max-conns option on the servers for slow response servers, or lower the number for the max-parselen option to reduce the unnecessary wait for invalid HTTP connections.

- CSCec38106

  On systems that use Cisco IOS software and Catalyst operating system software, when you configure the Catalyst 6500 series switch to trust the DSCP priority bits of the incoming traffic, the CSM might reset the DSCP value to zero (0) if these frames are being forwarded by the CSM.

  Workaround: None.

- CSCef76686

  When you configure a server farm with the least-connections algorithm (**predictor leastconns**) and enable the REAL_SLOW_START_ENABLE environment variable with the default rate (3), the slow-start feature might not take effect for newly activated servers in the server farm.

  Workaround: Configure the REAL_SLOW_START_ENABLE environment variable to 2.

- CSCeh76411

  When you configure **service ftp** on a virtual server and then configure a client NAT pool for that virtual server, the FTP virtual server allocates ports from the NAT pool and does not reclaim them.

  Workaround: Reboot the CSM to recover the allocated ports.

- CSCeh60704

  The sticky table does not replicate after a configuration synchronization. This situation occurs when traffic is sent to a virtual server that is configured with the **csrp sticky** and **csrp connection**.

  Workaround: Reload the active CSM. Reloading the standby CSM does not correct the problem.

- CSCeh78584

  When you configure an alias IP address on a server VLAN on the CSM, you are incorrectly allowed to configure a network address for the alias.

- CSCsa88370

  Due to an ARP failure, a real server that is not directly connected to the CSM may become unreachable after a gateway failure occurs, even though there is still a valid gateway or route available.

  This situation occurs when there is more than one route (gateway) configured to reach the real server and the route chosen by the CSM becomes unavailable.

  Workaround: Remove the failed gateway from the configuration.

- CSCeh41862

  When you configure gateway tracking, if the host or gateway is more than 1 hop away, the CSM goes into standby state, even if the CSM can ping the host.

- CSCeh34176

  The **show module csm** *slot* **stats** command displays the incorrect value for the **Connections Timed-Out** counter.

  Workaround: Enter the **show module csm** *slot* **tech-support proc 1** to display the correct value.

- CSCeh60960

  With the ROUTE_UNKNOWN_FLOW_PKTS environmental variable set to either **1** or **2**, ICMP or UDP packets cannot directly access servers behind the CSM when the CSM is in router mode.

  You can still Telnet to these servers when this environmental variable is set to 2.

  Workaround: None.

Resolved Caveats in Software Release 4.2(2)

Note For a description of caveats open in CSM software release 4.2(2), see the "Open Caveats in Software Release 4.2(2)" section on page 63.

This section describes resolved caveats in CSM software release 4.2(2):

- CSCeh55357

  If you configure a virtual server with the **persistent rebalance** option enabled, the first two GET requests of a single TCP connection are load-balanced to a regular HTTP real server. However, new HTTP GET requests are load-balanced to a configured redirect-server. As a result, the CSM fails to load balance these requests.

  An indication that this condition has occurred is if the output of the **show module csm** *slot* **tech-support proc 1** command shows that the value for the **Attempts to alloc used session** counter has incremented.

  Workaround: Remove the **persistent rebalance** option for this virtual server.

  This problem is resolved in CSM software release 4.2(2).

- CSCeh73953

  If you add several policies to a virtual server and configure the priority option using the **slb-policy** *policy-name* **priority** *priority_value* command, and then remove a policy that is not configured with the highest priority, the CSM might reload.

  This problem does not exist for policies that are not configured with the **priority** option.

  Workaround: Remove only the policy with the highest priority in the list.

  This problem is resolved in CSM software release 4.2(2).

- CSCed82590

  The CSM might forward ICMP reply packets to the backup CSM instead of forwarding the packets to the MSFC. This results in communication failure.

  Workaround: Configuring the virtual server for the ICMP traffics with an appropriate idle timeout value.

  This problem is resolved in CSM software release 4.2(2).

- CSCsa74493

  If you create a server farm and a cookie insert sticky group, and you create a policy to associate both, the CSM generates a static cookie entry that is displayed with the **show mod csm** *slot* **sticky** command.

  If you add a new real server to the server farm, the cookie info is not updated.

  Workaround: Remove the policy and reconfigure it.

  This problem is resolved in CSM software release 4.2(2).

- CSCeg69049

  When you configure a scripted probe with a script name that does not exist, the output of the **show module csm tech-script** command indicates the status of this probe as NOSCRIPT.

  After you load a valid script into the CSM by entering the **script file** command, the output of the **show module csm tech-script** command continues to indicate the status of this probe as NOSCRIPT.

  This is a display status problem only.

  This problem is resolved in CSM software release 4.2(2).

- CSCef88345

A CSM may send the synchronize acknowledge (SYN ACK) packet to the wrong destination in response to a synchronize start (SYN) packet received for a virtual server that requires parsing above Layer 4.

Workaround: Configure the next-hops as real servers in a dummy server farm.

This problem is resolved in CSM software release 4.2(2).

- CSCeh21118

  If you configure **match protocol http cookie** for a virtual server, the CSM might reload after a few million connections have been established to this virtual server. If you have also enabled sticky replication, the CSM might reload sooner.

  The core-dump shows this output:

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

  Workaround: Remove the configuration for cookie map matching.

  This problem is resolved in CSM software release 4.2(2).

- CSCeg49522

  In CSM software release 4.2(1), the ROUTE_UNKNOWN_FLOW_PKTS environment variable accepts a value of 0, 1, or 2. However, when you assign a value of 2 for this variable, the CSM changes it to a value of 3. This problem is a configuration setting problem only. The value of 3 operates as expected (route SYN and non-SYN packets).

  This problem is resolved in CSM software release 4.2(2).

- CSCeh64012

  In rare instances that due to a message timing problem, when the supervisor engine performs an RPR+ switchover from the active to standby supervisor engine, the CSM might go into offline mode, and you cannot enter commands in the CSM CLI.

  Workaround: Power cycle this CSM.

  This problem is resolved in CSM software release 4.2(2).

Open and Resolved Caveats in Software Release 4.2(1)

These sections describe the open and resolved caveats in CSM software release 4.2(1):

- Open Caveats in Software Release 4.2(1), page 67
- Resolved Caveats in Software Release 4.2(1), page 70

Open Caveats in Software Release 4.2(1)

Note For a description of caveats resolved in CSM software release 4.2(1) see the "Resolved Caveats in Software Release 4.2(1)" section on page 70.

This section describes open caveats in CSM software release 4.2(1).

- CSCeg77526

After you enter the **script file bootflash:myscript.txt** command to load a script file into the CSM, the output of the **show module csm** *slot* **script** command lists all of the script functions that were loaded into the CSM. When you enter the **no script file bootflash:myscript.txt** command to remove the script file configuration, the **show** command for the script continues to display the same list of script functions.

This situation occurs because the individual script was loaded into the CSM by using the **script file** command, which loads the script into memory. The CSM does not have a command that allows you to request a reload of the same script file to update the individual script.

In the current design of the CSM, do the following to perform a reload of the script with the same filename (but with newer content):

a. Remove the script with the **no script file bootflash:myscript.txt** command. This command does not destroy nor stop the current probes that are using the existing scripts.

b. Then, enter the **script file bootflash:myscript.txt** command to reload the new content. The probes will pick up the new script in the next interval of operation.

Workaround: None. This is the current design for reloading a script. The scripts must remain in memory for the probes to operate. If you want to stop the probes from using those scripts, you must remove the probes. Scripts removed from the CSM remain in memory.

- CSCdy67259

  The **TCL ping()** command uses an underlying **ping()** function provided by VxWorks. The VxWorks ping contains a bug, which, if the function receives an ICMP error message (for example host-unreachable), the function does not return with an error. The function remains in a wait loop until it receives a valid response.

  If the destination host is in the same subnet (Layer 2 adjacent) as the CSM-configured VLAN, then the ICMP request either receives a valid response or is timed out. In this case, the ping() function will not stop responding.

  The problem occurs when the destination IP address is one or more hops away. The router between the CSM and the destination host could respond with a "destination unreachable" message to the CSM if the router determined that the subnet for this IP address is unknown.

  Workaround: Do not use the **ping** command in TCL script for a destination that is one hop away.

- CSCeg15173

  Fragmented Layer Two Tunneling Protocol (L2TP) tunneled packets are discarded by the CSM, and the Packets Repeat Reverse Fragmentation counter in the CSM increases quickly. This problem occurs when packets arrive out of order (the MF packets arrive last) and are separated in time by about 10 milliseconds.

  Workaround: Design the network so that all fragments follow the same path, forcing them to arrive in order and closer together, or you can configure a static route in the CSM so that it knows where to send re-assembled fragments that arrived in a reverse order.

- CSCea43504

  If your configuration contains a pair of CSMs in a single fault-tolerant group and these paired CSMs are in an active-standby state, the CSMs might not retain the valid active-standby state if you add another CSM into this same fault-tolerant group, causing the fault-tolerant pair of CSMs to enter an invalid active-active state.

  Workaround: Remove the third CSM from the network and reboot the paired CSMs to allow them to recover their fault-tolerant state.

- CSCdw84018

The CSM may block or drop all UDP data channels of an RTSP service if the client NAT is also enabled. You must configure a virtual server, which the CSM uses to parse the RSTP service. For this same virtual server, you must also configure a client NAT on the server farm.

Workaround: Remove the NAT client configuration from the server farm or remove the service RTSP from the virtual server.

- CSCdv11685

  When more than one pair of redundant CSMs are configured to use the same VLAN ID, the CSM will accept replication messages from all fault-tolerant groups by using the specified VLAN. In this configuration, the session and sticky replication may not work properly.

  Workaround: Configure a unique VLAN trunk for each pair of fault-tolerant groups.

- CSCec28396

  The **static nat** command is normally used for server-initiated connections. In release 3.2(1) you can configure the NAT client static into a server farm to take advantage of the static NAT feature for traffic matching a virtual server. If you configured the NAT client static into a sever farm for FTP or RSTP services, this traffic would not be able to pass through the CSM.

  Workaround: Configure a client NAT pool with the server farm IP address instead of using the **static nat** command.

- CSCeb47499

  The UDP probe configured for a server farm can only detect a failure of a UDP service when the connectivity to the server IP address is opened. The CSM relies on the ICMP port unreachable message from the server so that it can detect whether the UDP service is available. If the interface on the server is down, the UDP probe cannot detect this failure condition.

  Workaround: Configure an ICMP probe to the same server farm where the UDP probe is configured.

- CSCeb52054

  When the Layer 7 virtual servers have many connections that are in the process of load-balancing, the new and existing connections experience slow response from the CSM. The connections, which are still waiting for more data from the client or which are waiting for the response from the server, are considered to be in the process of load-balancing.

  Workaround: Configure the max-conns option on the servers for slow response servers, or lower the number for the max-parselen option to reduce the unnecessary wait for invalid HTTP connections.

- CSCec38106

  On systems that use Cisco IOS software and Catalyst operating system software, when you configure the Catalyst 6500 series switch to trust the DSCP priority bits of the incoming traffic, the CSM might reset the DSCP value to zero (0) if these frames are being forwarded by the CSM.

- CSCef76686

  When you configure a server farm with the least-connections algorithm (**predictor leastconns**) and enable the REAL_SLOW_START_ENABLE environment variable with the default rate (3), the slow-start feature might not take effect for newly activated servers in the server farm.

  Workaround: Configure the REAL_SLOW_START_ENABLE environment variable to 2.

Resolved Caveats in Software Release 4.2(1)

Note For a description of caveats open in CSM software release 4.2(1), see the "Open Caveats in Software Release 4.2(1)" section on page 67.

This section describes resolved caveats in CSM software release 4.2(1):

- CSCeg78788

  When the CSM learns an ARP address from a device on the network and that ARP address appears in the CSM ARP table as learned, and you configure a gateway or static route with this device as the next hop, the CSM marks the ARP entry as down and does not learn the ARP address automatically.

  Workaround 1: Instead of using Predictor Forward in the server farm, point to the gateway as a real server.

  Workaround 2: Ping from or to the CSM, or to or from the gateway to populate the gateway in the ARP table.

  This problem is resolved in CSM software release 4.2(1).

- CSCsa43697

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

  This problem is resolved in CSM software release 4.2(1).

- 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 that points to the local virtual server is not operable until you remove the downed (not in service) virtual server from the configuration.

  This problem is resolved in CSM software release 4.2(1).

- CSCeh03583

  In CSM releases 4.1(1), 4.1(2), and 4.1(3), the CSM incorrectly calculates the URL hash value when you configure a specific delimiter to start the hash calculation with these commands:

  ```
  url-hash begin-pattern text
  url-hash end-pattern text
  ```

  As the result, if the two client requests contain two different URL strings (but the data between the hash diameters is the same), the CSM load-balances the requests to two different real servers in a server farm using the predictor hash URL method.

  In CSM release 4.1(1), the module does not accept the configuration for begin and end patterns when using the predictor hash URL. This code change introduced a problem in the CSM 4.1(1), 4.1(2), 4.1(3), 4.1(4) and 4.2(1) releases.

  Workaround: Use a different predictor method when you are not calculating the hash value for the entire URL string. This feature is working on CSM release 3.1(x).

  This problem is resolved in CSM software release 4.2(1).

- 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.

  This problem is resolved in CSM software release 4.2(1).

- 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 server farm. 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.

  This problem is resolved in CSM software release 4.2(1).

- 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.

  This problem is resolved in CSM software release 4.2(1).

- 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.

  This problem is resolved in CSM software release 4.2(1).

- CSCsa57462

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

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

  This problem is resolved in CSM software release 4.2(1).

- CSCsa53106

  When you remove then add back a VLAN with a new gateway, the CSM creates new encaps-mac address entries; however, the session may still select an old encap 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.

This problem is resolved in CSM software release 4.2(1).

- CSCsa51153

  When a server sends a finish (FIN) response for a connection to the CSM, the CSM might send a reset (RST) response and close the connection before the 8-second quick idle timer has expired. In some cases, the client does not have a chance to acknowledge the FIN response from the server.

  This problem is resolved in CSM software release 4.2(1).

- CSCee36210

  When the CSM is configured with Layer 7 parsing on a virtual server, the CSM will acknowledge (ACK) the synchronization (SYN) from the client and wait for the data packets. If the client terminates the connection with a finish (FIN) response without sending any data, the CSM closes the connection without replying with a reset (RST) or FIN-ACK response. This problem causes the client to retransmit and repeat the FIN response.

  This problem is resolved in CSM software release 4.2(1).

- CSCeg61794

  When the CSM is in the process of redirecting more than 16,000 concurrent 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 max-conns limit on the configured redirect vserver objects or on the virtual server object.

  This problem is resolved in CSM software release 4.2(1).

- CSCeg28849

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

  Workaround: Use the round-robin prediction algorithm.

  This problem is resolved in CSM software release 4.2(1).

- 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, then remove the default gateway configuration. You can then reconfigure the route.

  This problem is resolved in CSM software release 4.2(1).

- 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.

  This problem is resolved in CSM software release 4.2(1).

- CSCeg35110

  When you configure more than one virtual server with an IP address that is being used by a DNS server farm (GSLB feature), the health probe for the real server within this server farm might show as failed.

  This situation occurs when the probe checks the status of one virtual server instead of checking the status of all virtual servers with this IP address.

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

  This problem is resolved in CSM software release 4.2(1).

- CSCec21915

  The possible number of VLANs has increased to 511 in CSM software release 3.2(1). This limit represents the total number of IP interfaces and alias IP interfaces that can be configured on the CSM. If you need to configure alias IP addresses, you need to reduce the number of VLAN IP interfaces.

  Workaround: Reduce the number of configured VLANs to accommodate the total number of alias IP addresses.

  This problem is resolved in CSM software release 4.2(1).

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, which 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, which 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 as follows:

```
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:

- *Regulatory Compliance and Safety Information for the Catalyst 6500 Series Switches*
- *Catalyst 6500 Series Content Switching Module Configuration Note*
- *Catalyst 6500 Series Content Switching Module Command Reference*
- *Catalyst 6500 Series Content Switching Module Installation and Verification Note*
- *Catalyst 6500 Series Switch Installation Guide*
- *Catalyst 6500 Series Switch Module Installation Guide*
- *Catalyst 6500 Series Switch Software Configuration Guide*
- *Catalyst 6500 Series Switch Command Reference*
- *Catalyst 6500 Series System Message Guide*
- *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*
- *Catalyst 6500 Series Switch Cisco IOS Command Reference*
- For information about MIBs, refer to this URL:

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

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 and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

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