Release Notes for Catalyst 6500 Series Content Switching Module Software Release 4.1(x)

Current Release: 4.1(11)—February 27, 2009
Previous releases: 4.1(1) through 4.1(10)

This publication describes the features, modifications, and caveats for the Catalyst 6500 series Content Switching Module (CSM) software release 4.1(11) operating on a Catalyst 6500 series switch.

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

© 2005—2009 Cisco Systems, Inc. All rights reserved.

System Requirements

This section describes the system requirements for the Catalyst 6500 series CSM software release 4.1(11).

Memory Requirements

The Catalyst 6500 series CSM memory is not configurable.

Hardware Supported

Before you can use the Catalyst 6500 series CSM, you must have a Supervisor Engine 1A or a Supervisor Engine 2 with a Multilayer Switch Feature Card (MSFC) or Multilayer Switch Feature Card 2 (MSFC2), a Policy Feature Card (PFC), 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 Cisco IOS Software	Recommended Cisco IOS Software	Recommended Catalyst Operating System Software
Content Switching Module			
WS-X6066-SLB-APC with Supervisor Engine 1 and MSFC1 or MSFC2	12.1(8a)EX	12.2(18)SXF15	N/A
Supervisor Engine 2 with MSFC2	12.1(8a)EX or 12.2(17d)SXB	12.2(18)SXF15 or higher	N/A
WS-X6066-SLB-APC with Supervisor Engine 720	12.2(14)SX1	12.2(18)SXF15 or higher	N/A
Console Cable			
72-876-01		Not applicable	
Accessory Kit			
800-05097-01		Not applicable	

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.

The recommended release is the base release to support new commands for a given CSM release.

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

Table 1 CSM with Cisco IOS Software Requirements

CSM Release	Supervisor Engine 1 MSFC1 or MSFC2		Supervisor Engine 2 with MSFC2		Supervisor 720 with MSFC 3	
	Minimum Software Release	Recommended Software Release	Minimum Software Release	Recommended Software Release	Minimum Software Release	Recommended Software Release
4.1(11)	12.1(8a)EX	12.2(18)SXF15	12.1(8a)EX or 12.2(17d)SXB	12.2(18)SXF15	12.2(14)SXD 12.2(18)SXD2	12.2(18)SXF15
4.1(10)	12.1(8a)EX	12.2(18)SXF15	12.1(8a)EX or 12.2(17d)SXB	12.2(18)SXF15	12.2(14)SXD 12.2(18)SXD2	12.2(18)SXF15
4.1(9)	12.1(8a)EX	12.2(18)SXF15	12.1(8a)EX or 12.2(17d)SXB	12.2(18)SXF15	12.2(14)SXD 12.2(18)SXD2	12.2(18)SXF15
4.1(8)	12.1(8a)EX	12.2(18)SXF15	12.1(8a)EX or 12.2(17d)SXB	12.2(18)SXF15	12.2(14)SXD 12.2(18)SXD2	12.2(18)SXF15
4.1(7)	12.1(8a)EX	12.2(18)SXF15	12.1(8a)EX or 12.2(17d)SXB	12.2(18)SXF15	12.2(14)SXD 12.2(18)SXD2	12.2(18)SXF15
4.1(6)	12.1(8a)EX	12.2(18)SXF15	12.1(8a)EX or 12.2(17d)SXB	12.2(18)SXF15	12.2(14)SXD 12.2(18)SXD2	12.2(18)SXF15
4.1(5)	12.1(8a)EX	12.2(18)SXF15	12.1(8a)EX or 12.2(17d)SXB	12.2(18)SXF15	12.2(14)SXD 12.2(18)SXD2	12.2(18)SXF15
4.1(4)	12.1(8a)EX	12.2(18)SXF15	12.1(8a)EX or 12.2(17d)SXB	12.2(18)SXF15	12.2(14)SXD 12.2(18)SXD2	12.2(18)SXF15
4.1(3)	12.1(8a)EX	12.2(18)SXF15	12.1(8a)EX or 12.2(17d)SXB	12.2(18)SXF15	12.2(14)SXD 12.2(18)SXD2	12.2(18)SXF15
4.1(2)	12.1(8a)EX	12.2(18)SXF15	12.1(8a)EX or 12.2(17d)SXB	12.2(18)SXF15	12.2(14)SX1	12.2(14)SXF15
4.1(1)[1]	12.1(8a)EX	12.2(18)SXF15	12.1(8a)EX or 12.2(17d)SXB	12.2(18)SXF15	12.2(14)SX1	12.2(14)SXF15

1. Back end encryption requires Cisco IOS software Release 12.2(17d)SXB for the Supervisor Engine 2 or 12.2(17d)SXA for Supervisor Engine 720.

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

CSM Release	Supervisor Engine 1 MSFC1 or MSFC2		Supervisor Engine 2 with MSFC2		Supervisor Engine 720 with MSFC 3	
	Minimum Software Release	Recommended Software Release	Minimum Software Release	Recommended Software Release	Minimum Software Release	Recommended Software Release
4.1(11)	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 7.5	Cisco IOS 12.2(14)SX2 with Catalyst operating system 8.1	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 8.1
4.1(10)	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 7.5	Cisco IOS 12.2(14)SX2 with Catalyst operating system 8.1	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 8.1
4.1(9)	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 7.5	Cisco IOS 12.2(14)SX2 with Catalyst operating system 8.1	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 8.1
4.1(8)	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 7.5	Cisco IOS 12.2(14)SX2 with Catalyst operating system 8.1	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 8.1
4.1(7)	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 7.5	Cisco IOS 12.2(14)SX2 with Catalyst operating system 8.1	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 8.1
4.1(6)	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 7.5	Cisco IOS 12.2(14)SX2 with Catalyst operating system 8.1	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 8.1
4.1(5)	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 7.5	Cisco IOS 12.2(14)SX2 with Catalyst operating system 8.1	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 8.1
4.1(4)	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 7.5	Cisco IOS 12.2(14)SX2 with Catalyst operating system 8.1	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 8.1

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

CSM Release	Supervisor Engine 1 MSFC1 or MSFC2		Supervisor Engine 2 with MSFC2		Supervisor Engine 720 with MSFC 3	
	Minimum Software Release	Recommended Software Release	Minimum Software Release	Recommended Software Release	Minimum Software Release	Recommended Software Release
4.1(3)	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 7.5	Cisco IOS 12.2(14)SX2 with Catalyst operating system 8.1	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 8.1
4.1(2)	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 7.5	Cisco IOS 12.2(14)SX2 with Catalyst operating system 8.1	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 8.1
4.1(1)[1]	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 7.5	Cisco IOS 12.2(14)SX2 with Catalyst operating system 8.1	Cisco IOS 12.2(18)SXF15 with Catalyst operating system 8.1

1. Back end encryption requires Cisco IOS software Release 12.2(17d)SXB for the Supervisor Engine 2 or 12.2(17d)SXA for Supervisor Engine 720.

Software Release 4.1(x) Features

Table 3 lists the features that have been added in CSM software release 4.1(4).

Table 3 New CSM Feature Set Description

Features New in this Release	Description
Server Application State Protocol (SASP)	Allows the CSM to receive traffic weight recommendations from Workload Managers (WMs), to register with WMs, and to enable WMs to suggest to the CSM new load-balancing group members.

Feature Set

Table 4 describes the CSM features and software descriptions.

Table 4 CSM Feature Set Description

Feature	First Image Release	Supported Release
Supported Hardware		
Supervisor 1A with MSFC and PFC	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-4.1-CSM
Supervisor 2 with MSFC2	c6slb-apc.1-2-1.bin	SC6K-1.2-CSM SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-4.1-CSM
Supervisor 720—Requires CSM software release 3.1(4) or later.	c6slb-apc.3-2-1.bin	SC6K-3.2-CSM SC6K-4.1-CSM
Catalyst 6500 Series Supported Operating Systems		
Cisco IOS software	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Catalyst operating system software	c6slb-apc.2-2-7.bin c6slb-apc.3-1-2.bin	SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Supported Protocols		
FTP	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
TCP load balancing	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
UDP and all common IP protocol load balancing 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.	c6kslb-apc.2-1-1.bin c6slb-apc.3-2-1.bin	SC6K-2.1-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM

Table 4 CSM Feature Set Description (continued)

Feature	First Image Release	Supported Release
Real Time Streaming Protocol (RTSP)	c6slb-apc.2-2-1.bin	SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Layer 7 Functionality		
Full regular expression matching	c6slb-apc-1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
URL & cookie switching	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Generic header parsing	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Miscellaneous Functionality		
TCP fragmentation support—Allows the CSM to handle fragmented TCP packets.	c6slb-apc.3-2-1.bin	SC6K-3.2-CSM SC6K-4.1-CSM
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	SC6K-3.2-CSM SC6K-4.1-CSM
Denial of Service (DoS) improvements—Allows TCP termination for all connections to the CSM providing SYN attacks.	c6slb-apc.3-2-1.bin	SC6K-3.2-CSM SC6K-4.1-CSM
Multiple CSMs in a chassis	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
CSM and Cisco IOS-SLB functioning simultaneously in a chassis	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
HTTP 1.1 persistence (all GETs balanced to the same server)	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM

Table 4 CSM Feature Set Description (continued)

Feature	First Image Release	Supported Release
Full HTTP 1.1 persistence (GETs balanced to multiple servers)	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
HTTP method parsing	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Fully configurable NAT	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Server-initiated connections	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Route health injection	c6slb-apc.1-1-1.bin (requires release 12.1(7)E c6slb-apc.1-2-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Round-robin	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Weighted round-robin (WRR)	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Least connections	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM

Table 4 CSM Feature Set Description (continued)

Feature	First Image Release	Supported Release
Weighted least connections	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
URL hashing	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Source IP hashing	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Destination IP hashing	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Return error code checking	c6slb-apc.2-2-1.bin	SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
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	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Jumbo frames—Allows support of frames of up to 9000 bytes for Layer 4 load balancing.	c6slb-apc.3-2-1.bin	SC6K-3.2-CSM SC6K-4.1-CSM
Reduced time between health probes	c6slb-apc.2-2-1.bin	SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
In-band health checking	c6slb-apc.2-2-1.bin	SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Configurable pending connection timeout	c6slb-apc.2-2-1.bin	SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM

Table 4 CSM Feature Set Description (continued)

Feature	First Image Release	Supported Release
IP reassembly for in-order UDP fragments	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
IP reassembly for out-of-order UDP fragments	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
VIP connection watermarks	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
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	SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Real server names	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Slowpath performance improvements	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Load Balancing Supported		
Server load balancing	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
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	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
DNS load balancing	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Stealth firewall load balancing	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-4.1-CSM

Table 4 CSM Feature Set Description (continued)

Feature	First Image Release	Supported Release
Transparent cache redirection	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Reverse proxy cache	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
SSL off-loading	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
VPN-IPsec load balancing	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Enhanced interoperation with the SSL termination engine (STE) for secure socket layer (SSL) load balancing	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Stickiness		
Cookie	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
SSL ID	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Source IP	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
HTTP redirection	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM

Table 4 CSM Feature Set Description (continued)

Feature	First Image Release	Supported Release
Cisco IOS SLB FWLB interoperation (IP reverse-sticky)	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Redundancy		
Sticky state	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
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.3-2-1.bin	
Full stateful failover (connection redundancy)	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Failover improvements—Provide enhancements for preempt option with connection replication, the **forced failover** command.	c6slb-apc.3-2-1.bin	
Backup sorry server (backup serverfarm)	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM
Allows a backup at the real server level	c6slb-apc.3-2-1.bin	SC6K-3.2-CSM SC6K-4.1-CSM
Non-TCP connection redundancy	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
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	SC6K-3.2-CSM SC6K-4.1-CSM
HTTP	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
ICMP	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM

Table 4 CSM Feature Set Description (continued)

Feature	First Image Release	Supported Release
Telnet	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
TCP	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
SMTP	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
DNS	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Optional port for health probes	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM SC6K-3.2-CSM
Support for multiple users simultaneously configuring a CSM	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Toolkit Command Language (TCL) 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	SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
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	SC6K-3.2-CSM SC6K-4.1-CSM
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).	c6slb-apc.3-2-1.bin	SC6K-3.2-CSM SC6K-4.1-CSM
SNMP traps for real server state changes	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM

Table 4 CSM Feature Set Description (continued)

Feature	First Image Release	Supported Release
SNMP traps on fault-tolerant state changes	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Support for CISCO-SLB-MIB	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Support for CISCO-SLB-EXT-MIB	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
XML configuration interface	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM
Resource use display	c6slb-apc.3-1-1.bin c6slb-apc.3-2-1.bin	SC6K-3.1-CSM SC6K-3.2-CSM SC6K-4.1-CSM

New and Changed Information

- New environment variable RHI_ADMIN_DISTANCE.

  When the CSM advertises its route through route health injection (RHI), it reports the administrative distance as 0. The new environment variable RHI_ADMIN_DISTANCE allows you to change this reported distance value. The default is 0; the range is 0—255.

Note The current IOS software on the MSFC does not update its route table with the CSM's reported distance value. To force an update to the route table, bring the virtual server OUTOFSERVICE, then back to OPERATIONAL.

  This change appears in CSM software release 4.1(10).

- New environment variable REBALANCE_SAME_RULE.

  On a persistent rebalance request, the CSM will rebalance only if a new policy is matched. When the environment variable REBALANCE_SAME_RULE is set to 1 (enabled), the CSM will force a rebalance regardless of which policy is matched. The default is 0 (rebalance only on new policy).

  This change appears in CSM software release 4.1(10).

- 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 4.1(9).

- 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 4.1(9).

- 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 that is 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 the 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: Time-Out (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
  ```

- There is an enhancement to the predictor IP hash and cookie hash. The CSM will perform a secondary hash if the first hash value resolves in mapping to an out-of-service real server. This enhancement allows even distribution of connections. Previously, when a real server became out-of-service, all of its intended connections would go to the next real server in sequence.
- For your convenience, sample scripts are available to support the TCL (Toolkit Command Language) feature. Other custom scripts will work, but these sample scripts are supported by Cisco TAC. The file with sample scripts is located at this URL:

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

  The file containing the scripts is: c6slb-script.3-2-1.tcl.
- CSCsg48830

  After sending an FTP 226 response on the control channel, many FTP servers close the data channels. However, some FTP servers allow the data channels to remain open. The FTP RFC allows both behaviors.

  CSCsg48830 adds environment variable FTP_CLOSE_DATA_CONN to configure the CSM behavior after receipt of an FTP 226. If the variable is set to zero, the CSM closes the data channels after it receives an FTP 226 response. If the variable is set to one, the CSM leaves the channels open.

  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: (0 = close) CSM behavior for data channels after receipt of FTP 226 from server.

  This example shows how to configure the environment variable:

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

Limitations and Restrictions

- 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 the Catalyst operating system.
- When configuring Route Health Injection (RHI), proxy ARP must be disabled on the Catalyst 6500 series chassis (proxy ARP is enabled by default). You must disable proxy ARP on a per-interface basis in the interface submode. We recommend that you disable proxy ARP on the VLAN level using the **no ip proxy arp** command.
- The meaning of having no minimum connections (MINCONNS) parameter set in the **real** submode is different between release 2.2(1) and later releases.

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

  In all releases, when the MINCONNS value is set, once a real server has reached the maximum connections (MAXCONNS) state, no additional session is balanced to it until the number of open sessions to that real server falls below MINCONNS. With the no MINCONNS value set in release

1.1(1), no additional session would be balanced until the number of open sessions to that real server falls to 0. With no MINCONNS value set in release 1.2(1), no additional session is balanced until the number of open sessions falls below MAXCONNS.

- Slot 1 is reserved for the supervisor engine. Slot 2 can contain an additional redundant supervisor engine in case the supervisor engine in slot 1 fails. If a redundant supervisor engine is not required, you can insert the CSM in slots 2 through 6 on a 6-slot chassis, slots 2 through 9 on a 9-slot chassis, or slots 2 through 13 on a 13-slot chassis.
- There is no support for client NAT of IP protocols other than TCP or UDP.
- If neither a real server nor a corresponding virtual server has an explicitly configured TCP/UDP port, then probes requiring such a port are not activated. All CSM health probes other than ICMP periodically create connections to specific TCP or UDP ports on configured real servers. If a health probe is configured on a real server without a configured TCP or UDP port, the CSM chooses the TCP or UDP port to probe from the virtual servers with which the real server is associated. If neither the real server nor the virtual server has a configured port, the CSM simply ignores any configured probes requiring ports to that real server.
- When configuring CSMs for fault tolerance, we recommend that you configure a dedicated link for the fault-tolerant VLAN.

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

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

Caveats

These sections describe the open and resolved caveats in CSM software for all 4.1(x) software releases:

Open Caveats in Software Release 4.1(11)

Note For a description of caveats resolved in CSM software release 4.1(11), see the "Resolved Caveats in Software Release 4.1(11)" section on page 18.

This section describes known limitations that exist in CSM software release 4.1(11):

- There are no open caveats in software release 4.1(11).

Resolved Caveats in Software Release 4.1(11)

Note For a description of caveats open in CSM software release 4.1(11), see the "Open Caveats in Software Release 4.1(11)" section on page 18.

- 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.

- 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.

- 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.

- 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.

Workaround: None.

- CSCso00578

  A CSM configured for redundancy may have its Content Switching Replication Protocol (CSRP) replication status stuck in the INIT state.

  Workaround: None.

- CSCsj05855

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

  Workaround: None.

- CSCsx37458

  One or more VIPs on the CSM may not respond to the ping. This condition occurs when the same VIP used in the virtual server is also used in a static NAT entry. The VIP may show up in the CSM ARP table as a NAT entry instead of a virtual server entry. You can display CSM ARP table with the **show mod csm slot arp** command.

  Workaround:

  1. Suspend all virtual servers for the VIP address that does not respond.
  2. Remove the static NAT configuration for that VIP.
  3. Reactivate the virtual servers.
  4. Readd the static NAT.

- CSCsl07382

  Memory leak occurs when Global Server Load Balancing (GSLB) is run on CSM. This condition is observed when CSM is configured for GSLB.

  Workaround: Monitor memory usage on a regular basis through the venus console. You can session to the CSM through session slot *x* processor 0 (with *x* being the slot of the CSM). To perform this session, follow these steps:

  – At the CSM> prompt enter **venus.**

  – At the venus# prompt enter **core_show_usage**.

  If the available memory is less than 20 percent, you must schedule a reboot of the CSM. The memory leak occurs only on the active CSM and when the standby CSM is available for takeover.

Open Caveats in Software Release 4.1(10)

Note For a description of caveats resolved in CSM software release 4.1(10), see the "Resolved Caveats in Software Release 4.1(10)" section on page 20.

This section describes known limitations that exist in CSM software release 4.1(10):

- There are no open caveats in software release 4.1(10).

Resolved Caveats in Software Release 4.1(10)

Note For a description of caveats open in CSM software release 4.1(10), see the "Open Caveats in Software Release 4.1(10)" section on page 19.

This section describes resolved caveats in CSM software release 4.1(10):

- CSCek31065

  A CSM in a redundant configuration with duplicate entries configured with Cisco 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 and server VLAN.

  Workaround: None.

- CSCek37109

  In some situations, the CSM might classify traffic incorrectly, resulting in the CSM attempting to send packets to the SSL daughter card. Because the SSL daughter card is only provisioned on a CSM-S, this action causes a core dump. Also, the CSM increments the statistic "packets shakira" (in "session statistics"), which you can display using the **show mod csm** *x* **tech proc 1** command. This statistic should only increment on a CSM-S.

  Workaround: None.

- CSCek68456

  No error is displayed when an illegal value of SASP_SCALE_WEIGHTS is assigned. Also, the **show run | inc SASP_SCALE_WEIGHTS** command displays the illegal value.

  Workaround: Enter a legal value.

- CSCek71183

  The header insert feature will fail if the header is longer than 127 bytes.

  Workaround: Use a header of 127 bytes or less.

- CSCse21474

  The **show module csm** *number* **conns** command lists the RTSP data channel in the INIT state when it should be displayed in the ESTAB (established) state.

  Workaround: If this is a UDP session, check both odd and even table entries to determine the actual state of the RTSP data channel.

- 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.

- 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.

- CSCsh94471

  When running probe related scripts and clearing the configuration, the CSM may go offline.

  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.

- CSCsi58089

  The CSM may drop a SASP connection if the message sent by the server is greater than 2816 bytes in length.

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

- CSCsj26410

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

  Workaround: None.

- 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 KAL-AP queries slows enough to make the GSS consider the virtual IPs to be down.

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

- 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 header insert is configured, this reset message has an incorrect sequence number.

  Workaround: None.

- CSCsk43903

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

  Workaround: None.

Open Caveats in Software Release 4.1(9)

Note For a description of caveats resolved in CSM software release 4.1(9), see the "Resolved Caveats in Software Release 4.1(9)" section on page 24.

This section describes known limitations that exist in CSM software release 4.1(9):

- CSCek37109

  The CSM can classify traffic incorrectly, resulting in attempts to send packets to the SSL daughter card. This action causes a core dump because the SSL daughter card is only provisioned on a CSM-S. Also, the CSM increments the statistic "packets shakira" (in "session statistics"), which you can display using the command **show mod csm** x **tech proc 1**. This statistic should only increment on a CSM-S.

  Workaround: None.

- CSCeg77526

  After loading a script file into the CSM with a **script file bootflash:myscript.txt** command, the output of the **show module csm** *slot* **script** command lists all of the script functions that were loaded into the CSM.

  When you use the command **no script file bootflash:myscript.txt** 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 perform a reload of the script with the same filename (but newer content) in the current design of the CSM, you must 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. Readd the configuration **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 CSM remain in memory.

- CSCeg15173

  Fragmented Layer 2 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 reassembled fragments that arrived in a reverse order.

- CSCdy67259

  The **TCL ping()** command uses an underlying **ping()** function provided by VxWorks. If the VxWorks ping function receives an ICMP error message (for example host-unreachable), the function does not return with an error, but instead 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 back 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.

- 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 either 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.

- 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.

- 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.

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

Resolved Caveats in Software Release 4.1(9)

Note For a description of caveats open in CSM software release 4.1(9), see the "Open Caveats in Software Release 4.1(10)" section on page 19.

This section describes resolved caveats in CSM software release 4.1(9):

- 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.

- CSCsg99287

  When a probe is configured to an unreachable IP address, the resulting report correctly indicates a failure, but the success counter incorrectly shows a maximum value (4294967293) of successes.

  Workaround: None.

- CSCsg84782

  When a probe is configured to an unreachable IP address, the resulting report displays the status as "???" rather than failed.

  Workaround: None.

- CSCsg82885

  The CSM will not boot after the user configures close to the maximum number of vservers and scripted probes attached to the server farm.

  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.

- 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.

- 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.

- 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.

- 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.

- 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 not operational.

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

- 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.

- 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.

- CSCsf99484

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

  Workaround: None.

- CSCsg16726

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

  Workaround: None.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCse51250

  When two CSMs are deployed in an FT application, the response to a **show module csm x tech-support** command incorrectly displays a very large number for the illegal state transitions counter.

  Workaround: None.

- CSCsd99863

  When performing Layer 7 load balancing, the CSM will generate easily predictable TCP Initial Sequence Numbers (ISN), which weakens security.

  Workaround: Use a firewall in front of the CSM.

- 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.

- 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.

- 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 "Packets with no SMAC, sent to slowpath."

  Workaround: None.

Open Caveats in Software Release 4.1(8)

Note For a description of caveats resolved in CSM software release 4.1(8), see the "Resolved Caveats in Software Release 4.1(8)" section on page 29.

This section describes known limitations that exist in CSM software release 4.1(8):

- CSCek37109

  The CSM can classify traffic incorrectly, resulting in attempts to send packets to the SSL daughter card. This action causes a core dump, because the SSL daughter card is only provisioned on a CSM-S. Also, the CSM increments the statistic "packets shakira" (in "session statistics"), which you can display using the command **show mod csm** x **tech proc 1**. This statistic should only increment on a CSM-S.

  Workaround: None.

- 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 not operational.

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

- CSCeg77526

  After loading a script file into the CSM with a **script file bootflash:myscript.txt** command, the output of the **show module csm** *slot* **script** command lists all of the script functions that were loaded into the CSM.

  When you use the command **no script file bootflash:myscript.txt** 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 perform a reload of the script with the same filename (but newer content) in the current design of the CSM, you must 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, re-add the configuration **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 CSM remain in memory.

- 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.

- CSCdy67259

  The **TCL ping()** command uses an underlying **ping()** function provided by vxworks. The VxWorks ping contains a bug which if the 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 back 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.

- 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 either 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.

- 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.

- 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.

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

Resolved Caveats in Software Release 4.1(8)

Note For a description of caveats open in CSM software release 4.1(8), see the "Open Caveats in Software Release 4.1(8)" section on page 27.

This section describes resolved caveats in CSM software release 4.1(8):

- CSCej70864

  The CSM may produce a core dump when attempting to handle ICMP packets in the Layer 7 part of the code.

  Workaround: None.

  This problem is resolved in CSM software release 4.1(8).

- CSCek39971

The CSM populates the ARP table with MAC addresses for the subnet's network address and broadcast addresses. The ARP table should only contain 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 4.1(8).

- 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 4.1(8).

- 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 4.1(8).

- 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 4.1(8).

- 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.

  This problem is resolved in CSM software release 4.1(8).

- 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 the connection.

  Workaround: If possible, increase the client retransmit time.

  This problem is resolved in CSM software release 4.1(8).

- 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, indicating that the port is not available.

Workaround: None. After receiving the error code, the client reattempt will succeed, as the port number is different. This scenario occurs only during initial creation of the data channel, and does not affect data traffic.

This problem is resolved in CSM software release 4.1(8).

- 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 appears with UDP traffic only. The problem does not occur for TCP connections.

  Workaround: None.

  This problem is resolved in CSM software release 4.1(8).

- 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.

  This problem is resolved in CSM software release 4.1(8).

- 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 4.1(8).

- 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 4.1(8).

- 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 4.1(8).

- CSCsd89567

  When a TCP fails session allocation after buffer allocation, it frees the buffer twice. When this occurs, the CSM can produce a core dump. This happens when Layer 7 policies are configured under load.

  Workaround: Remove all L7 vserver/polices.

  This problem is resolved in CSM software release 4.1(8).

- 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 4.1(8).

- CSCsd97668

  Using a DNS probe with more than one address can cause the probe to fail. The DNS server correctly replies with one of the two addresses every time it is probed, but returns a failure for the other address.

  Workaround: Configure only one **address** command in the DNS probe.

  This problem is resolved in CSM software release 4.1(8).

- CSCse45390

  When a vserver is configured to terminate flows, **show mod csm** *slot* **conns vserver** *nameOfVserver* does not display the connections.

  Workaround: **show mod csm** *slot* **conns detail** displays the connections.

  This problem is resolved in CSM software release 4.1(8).

- CSCse50544

  When the CSM is configured to insert static cookies and the server response comes out of order (the first packet is not the HTTP header), the cookie inserted by the CSM appears in the HTML data (on screen).

  Workaround: None.

  This problem is resolved in CSM software release 4.1(8).

- CSCse78674

  For server-initiated traffic, the CSM corrupts fragmented UDP packets. 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.

  This problem is resolved in CSM software release 4.1(8).

- CSCse98829

  If the GET packet length is 118 bytes or less, the %p command (to attach the uri in the redirect-vserver command) does not append the uri extension. The redirect is sent out without the extension.

  Workaround: Use a larger GET request.

  This problem is resolved in CSM software release 4.1(8).

- CSCsg00909

  The CSM-S may crash when you try to add an additional policy rule, because of an error condition which leaves the regex in a corrupted state.

  Workaround: None.

This problem is resolved in CSM software release 4.1(8).

Open Caveats in Software Release 4.1(7)

For a description of caveats resolved in CSM software release 4.1(7), see the "Resolved Caveats in Software Release 4.1(7)" section on page 35.

This section describes known limitations that exist in CSM software release 4.1(7).

- CSCeg77526

  After loading a script file into the CSM with a **script file bootflash:myscript.txt** command, the output of the **show module csm** *slot* **script** command lists all of the script functions that were loaded into the CSM.

  When you use the command **no script file bootflash:myscript.txt** 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 perform a reload of the script with the same filename (but newer content) in the current design of the CSM, you must 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, re-add the configuration **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 CSM remain in memory.

- 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.

- CSCdy67259

  The **TCL ping()** command uses an underlying **ping()** function provided by vxworks. The VxWorks ping contains a bug which if the 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 back 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.

- 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 either 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.

- 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.

- 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.

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

Resolved Caveats in Software Release 4.1(7)

Note For a description of caveats open in CSM software release 4.1(7), see the "Open Caveats in Software Release 4.1(8)" section on page 27.

- CSCsb46265

  Changing a VLAN IP address can trigger an ARP timeout, which causes the encapsulated ID table to refresh and assigns a new encapsulated ID to each MAC address. Some CSM functions might not update with the newly assigned encapsulated ID. These functions continue to use the older encapsulated ID, which causes traffic to be forwarded to the wrong destination.

  Workaround: Configure static ARP entries for the CSM gateways.

Open Caveats in Software Release 4.1(6)

Note For a description of caveats resolved in CSM software release 4.1(6), see the "Resolved Caveats in Software Release 4.1(6)" section on page 37.

This section describes known limitations that exist in CSM software release 4.1(6).

- CSCsb46265

  Changing a VLAN IP address can trigger an ARP timeout, which causes the encapsulated ID table to refresh and assigns a new encapsulated ID to each MAC address. Some CSM functions might not update with the newly assigned encapsulated ID. These functions continue to use the older encapsulated ID, which causes traffic to be forwarded to the wrong destination.

  Workaround: Configure static ARP entries for the CSM gateways.

- CSCeg77526

  After loading a script file into the CSM with a **script file bootflash:myscript.txt** command, the output of the **show module csm** *slot* **script** command lists all of the script functions that were loaded into the CSM.

  When you use the command **no script file bootflash:myscript.txt** 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 perform a reload of the script with the same filename (but newer content) in the current design of the CSM, you must 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, re-add the configuration **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 CSM remain in memory.

- 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.

- CSCdy67259

  The **TCL ping()** command uses an underlying **ping()** function provided by vxworks. The VxWorks ping contains a bug which if the 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 back 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.

- 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 either 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.

- 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.

- 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.

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

Resolved Caveats in Software Release 4.1(6)

Note For a description of caveats open in CSM software release 4.1(6), see the "Open Caveats in Software Release 4.1(6)" section on page 35.

- CSCsd58615

  Sending a multi-packet 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 than packets from other layers. Also, 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.

- 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, also causing a failure. This situation occurs when a packet larger than the configured MSS is received.

  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.

- CSCsd04062

  The CSM cookie sticky entries remain in the sticky table even when the sticky group configuration is removed from the virtual server and you reconfigure the same sticky group number.

  Workaround: Reset the CSM, or use a different sticky group number.

- CSCsc74507

  A cookie insert gives the same hash result for two different IP addresses, which creates a collision in the sticky table. Only one entry is created.

  The IP addresses involved are 10.96.130.26 <-> 10.96.130.19 and 10.96.130.18 <-> 10.96.130.32 Other IP addresses may also be involved.

  Workaround: Remove the IP addresses from the configuration and then reboot the CSM.

- CSCsc56986

  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, causing delays due to 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.

- CSCsb83818

  You must run a TFTP process on a core dump from the VENUS# prompt in CSM software release 4.1.x and higher.

  Workaround: None.

- CSCsb71260

  When the cookie insert feature is configured with other map policies for a virtual server, the CSM reinserts a new cookie for new TCP connections, even when a previously inserted cookie exists. The CSM reinserts new cookies when the existing map policies do not have a match and when the cookie insert is the default policy.

  Workaround: None.

- CSCsb64954 -

  When the CSM is configured with a virtual server of type “service rtsp,” poor video or audio quality results when MP4 files stream through the module. This situation occurs because the RTSP packets are lost. The “data seq mismatch counter” under the TCP statistics section of the **show tech** command shows the counter increment.

  Workaround: Avoid using the **service rtsp** command.

- 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 lower processor maximum transmission unit PMTU) that is lower than the CSMs MSS 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 CSMs MSS 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).

- 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 c** *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.

- CSCsb40988

  After reaching the configured maximum connections, the sticky timer remains at 0 and may not start for new traffic flows. Also the sticky timer also does not start when you delete connections.

  This symptom is observed on a CSM that is configured using the **NO_TIMEOUT_IP_STICKY_ENTRIES 1** command in CSM mode and the **maxconns** command on the real server.

  Workaround: Remove the maximum connections from the configuration.

- CSCsb40365

  When running scripted probes on the CSM, the command line might stop responding and return a "% No ICC response for TLV *type number"* message from the module after approximately two minutes have passed. The number field changes depending on which command is run in the script.

  Workaround: Rebooting the CSM will fix the problem temporarily.

- CSCsb17046

  Inservice virtual IP addresses do not respond to DNS queries. The CSM does not use a real server if the load is above the threshold of 254. In this situation, the load of a local GSLB real server remains stuck at 255, preventing the CSM from using this real server in the DNS response. The problem occurs when the associated virtual server state changes from out-of-service back to inservice.

  Workaround: None.

- CSCsa88370

  When there is more than one route or gateway configured to reach a real server and the route or gateway chosen by the CSM becomes unavailable, a remote real server might become unreachable due to an ARP failure, even though a valid gateway or route is still available.

  Workaround: Use the **show mod csm slot arp** command to determine which route or gateway is not available, and remove it from the configuration.

- CSCek33744

  The CSM **show tech ft** command may display unrecognizable characters for the fault tolerance high availability state when you enter the **show mod csm ft detailed** command.

  Workaround: Use the **show mod csm ft** command to show the correct FT state.

- CSCei94412

  When the CSM is in bridge mode, HSRP packets are not bridged by the module, which causes packet flooding. This situation occurs when HSRP is configured on the client VLAN and the server's default gateway points to that HSRP address. The flooding occurs when the HSRP virtual MAC times out from the switch CAM tables. The age timer default is 5 minutes of inactivity.

  Workaround: Increase the MAC address table aging timer in the server VLANs, or use the "standby use-bia" parameter.

- CSCei91610

  When an FTP client nictitates a FIN message, the CSM closes the connection and stops transmitting the ACK messages that are sent in response to the server's FIN message to the real server.

  Workaround: None.

- CSCei91452

  FTP data channel breaks 15 minutes into the data transfer.

  Note After the CSM has been up for (0x00ffffff)*(134/166) seconds, or about 156 days, the FTP data channel is timed out after only 15 minutes. Shorter transfers are unaffected. The problem originates from the CSM timestamp calculation process.

  Workaround: Change the value of the "session_clock_max"from 0x00ffffff to 0x0fffffff. This can be done from the VENUS# prompt, with the **session_clock_max = 0x0fffffff** command. A reboot also resets the clock and allows for another 156 days of unaffected service.

- CSCei38917

  Layer 3 fragmented IP flows for the virtual server are dropped by the CSM. This condition occurs in a basic server load balancing design that uses an all zeros virtual server (0.0.0.0/0) and does not have NAT configured on the client and server on the server farm.

  Workaround: Downgrade to CSM software release 4.1(2) or an earlier release, where the problem is not exhibited.

- CSCei37874

  When sending traffic at a slow pace (1cps with the variable REAL_SLOW_START_ENABLE set to 1) and then change the IP address on an ICMP probe configured on only one real server and then activate that probe, it receives all of the new connections until it is again even with the other servers. This situation does not occur in slow start

  Workaround: None.

- CSCei28436

  When mass file transfers are performed, such as several hundred files with the same FTP control connection, the CSM may corrupt a TCP segment on an FTP control session. Subsequent control sessions become unsynchronized between the client and the CSM, causing the FTP session to fail.

  Workaround: None.

- CSCeh61946

  When a CSM that is using software release 3.2.1 is configured with a GSS and sends KAL-AP keepalives to another CSM in the network, it begins to answer commands slowly and eventually becomes unresponsive to **show** commands. The CSM becomes completely unresponsive after approximately 2-4 weeks of uptime.

  Workaround: When the available memory of the CSM falls below 40 percent, do not send GSS KAL-AP keepalives to the CSM, and periodically reload CSMs.

- CSCec75637

  The CSM sends ARP requests for configured routers or real servers only, but not for clients or routers where the client traffic originates. The CSM can only learn about these devices from ARP requests received on the network. If there are no ARP entries for a device, then traffic is dropped to that device, as well as traffic to a virtual source from one of these clients.

  This situation becomes a problem in a redundancy setup with preempt configured. After an initial failover, when the preempt device takes back the master role, clients that are local to the CSM's 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.

- CSCdy30354

  In CMS software releases 3.1(1a) and 3.1(2), the CSM does not record core-dump nor reboot the module when there is an FPGA halt. At this point, the CSM does not perform any function.

  Workaround: Reboot the module.

Open Caveats in Software Release 4.1(5)

Note For a description of caveats resolved in CSM software release 4.1(5), see the "Resolved Caveats in Software Release 4.1(5)" section on page 44.

This section describes known limitations that exist in CSM software release 4.1(5).

- CSCeg77526

  After loading a script file into the CSM with a **script file bootflash:myscript.txt** command, the output of the **show module csm** *slot* **script** command lists all of the script functions that were loaded into the CSM.

  When you use the command **no script file bootflash:myscript.txt** 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 perform a reload of the script with the same filename (but newer content) in the current design of the CSM, you must 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, re-add the configuration **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 CSM remain in memory.

- 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.

- CSCeg04864

  When cookie switching is configured along with multiple cookie values for a particular cookie name, the CSM might incorrectly load-balance a request.

  This problem appears only when the pipe character "|" (which is a regular expression meaning "or") is used between cookie values. The CSM incorrectly searches the second or subsequent regular expression parameters in all cookies in the HTTP header, not just the configured cookie name.

  Also, the problem appears only when the user incorrectly entered the "OR" regular expression for the matching configuration, for example, *ABC | *XYZ.

  The correct syntax should include parentheses around the alternate OR condition, as shown in this example: (*ABC | *XYZ).

  Workaround: Enter the parentheses into the matching string.

- 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_SHOW_START_ENABLE environment variable to 2.

- CSCdy67259

  The **TCL ping()** command uses an underlying **ping()** function provided by vxworks. The VxWorks ping contains a bug which if the 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 back 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.

- 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 either 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.

- 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.

- 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.

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

Resolved Caveats in Software Release 4.1(5)

Note For a description of caveats open in CSM software release 4.1(5), see the "Open Caveats in Software Release 4.1(5)" section on page 41.

- CSCei26434

  In CSM software release 4.1(4), when the least-cons predictor is configured, in some cases the module will load balance to one real server only instead of all real servers that are operational.

  The following conditions cause the CSM to experience this problem:

Step 1 Before the server farm is activated, the real server fails the health probe check. Failure occurs for one of these reasons:

  a. The user has changed the predictor from *other* to *least-conns*.

  b. The CSM was rebooted before the server farm was activated.

  c. The CSM became the fault-tolerant active module for the first time.

Step 2 After traffic travels through the server farm, alternate servers are selected.

Step 3 After the real server passes the health probe check, it is re-enabled, yet all new connection requests are load-balanced to this real server only.

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

  Workaround:

  a) Use another predictor method.

  b) Set this server to out-of-service, and then return it to in service after it passes the health check.

- 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 displays with the **show mod csm** *slot* **sticky** command.

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

  Workaround: Remove the policy, and reconfigure it.

- CSCsa64249

  The CSM may perform a core dump while processing an ICMP destination-unreachable packet. The syslog message shows this message:

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

  The core-dump shows the PPC exception type 512 on the Laminar Stack, and the stack shows the function failed at this location

  ```
  : session_get_entry()
  ```

  The CSM is handling the ICMP destination-unreachable message and needs to receive the matching flow to the VIP to translate it correctly to the real server IP address.

  The session ID that the PowerPC code received was 0x04000000, which is outside the range of valid session IDs. Under rare conditions the session IXP might put a flag in the high order bit of the session ID.

This condition exists on all these CSM releases: 3.1(10), 3.2(3), 4.1(4), and 4.2(1).

Workaround: Disable the CSM from processing all ICMP destination unreachable messages. To disable processing, set the `variable DEST_UNREACHABLE_MASK 0` to zero.

- CSCsa44265

  The GSLB probe counter stops functioning properly if it is configured to probe a local virtual server address. This information causes the probe counter to appear to not be operating or inaccurate. However the state OPERABLE or FAILED may still be correct. This problem may be a cosmetic defect in the counter output.

  Workaround: Because this problem does not seem to affect probes to remote virtual servers (virtual servers not configured locally on the same CSM), move the virtual server off of the local CSM to a remote CSM.

- CSCeh81260

  Sticky is not replicated if the standby CSM comes online after the sticky is created.

  Workaround: Keep the standby CSM powered off, create a flow that results in the creation of the sticky entry on the active CSM. Power on the standby CSM. The sticky entry on the active CSM will not get replicated to the standby CSM.

- 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.

- CSCeh64012

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

  Workaround: Power cycle this CSM.

- 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 appears when 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.

- 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.

- 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.

- CSCeh16627

  CSM in slot 13 goes offline.

  Workaround: None.

- 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.

  Workaround: None. This output indicates a display status problem only.

- CSCef88345

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

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

- CSCed82590

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

  Workaround: Configure the virtual server for the ICMP traffic with an appropriate idle timeout value.

- CSCec87452

  When the CSM is performing a proxy ARP operation, it records a checksum error in the debug log, as shown in this example:

  ```
  Received vlan arp reply for 10.250.13.153, from 10.250.13.250, mac of
  01:50:5a:fa:0d:fa on vlan 113
  proxy arp extension checksum error from ip 0.10.250.13 on vlan 250
  ```

  This message does not indicate a failure in the CSM and appears only when the ARP debugging is enabled. The checksum involved occurs in a proprietary ARP extension where the pad bytes follow the ARP frame. Since many devices reuse buffers without re-initializing these pad bytes, it is possible for the CSM to receive a trailer that appears to be valid but is actually a copy of a trailer that was sent out earlier. The checksum is stored and then checked to detect this case.

  The incorrect IP address occurs because there is a problem with the message formatting, not with the packet or code.

  Workaround:

- CSCdz25122

  The CSM accepted broadcast MAC addresses in response to ARP requests.

  Workaround: None.

Open Caveats in Software Release 4.1(4)

Note For a description of caveats resolved in CSM software release 4.1(4), see the "Resolved Caveats in Software Release 4.1(4)" section on page 49.

This section describes known limitations that exist in CSM software release 4.1(4).

- CSCeg77526

  After loading a script file into the CSM with a **script file bootflash:myscript.txt** command, the output of the **show module csm** *slot* **script** command lists all of the script functions that were loaded into the CSM.

  When you use the command **no script file bootflash:myscript.txt** 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 perform a reload of the script with the same filename (but newer content) in the current design of the CSM, you must 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, re-add the configuration **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 CSM remain in memory.

- 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.

- 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 serverfarm.

  Workaround: Configure the REAL_SHOW_START_ENABLE environment variable to 2.

- CSCdy67259

  The **TCL ping()** command uses an underlying **ping()** function provided by vxworks. The VxWorks ping contains a bug which if the 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 back 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.

- 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 either 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.

- 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.

- 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.

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

Resolved Caveats in Software Release 4.1(4)

Note For a description of caveats open in CSM software release 4.1(4), see the "Open Caveats in Software Release 4.1(4)" section on page 47.

- 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.

- CSCsa57462

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

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

- CSCsa53106

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

- 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.

  Workaround: None.

- CSCsa43697

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

  Workaround: None.

- 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).

- 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.

- 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, configuring a gateway or static route with this device as the next hop may cause the CSM to mark 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

- CSCeg66754

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

  Workaround: None.

- CSCeg61794

  When the CSM is in the process of redirecting more than 16,000 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.

- CSCeg49520

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

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

- CSCeg38929

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

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

- CSCeg35110

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

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

- CSCeg28849

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

  Workaround: Use the round-robin prediction algorithm.

- 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 occurs 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 does not correctly count against these limits on the standby CSM.

  Workaround: None.

- 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.

  Workaround: None.

Open Caveats in Software Release 4.1(3)

Note For a description of caveats resolved in CSM software release 4.1(3), see the "Resolved Caveats in Software Release 4.1(3)" section on page 53.

This section describes known limitations that exist in CSM software release 4.1(3).

- CSCeg35110

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

  This situation is caused by the probe checking the status of one virtual server instead of checking the status of all virtual servers with this IP address.

  Workaround: Remove those virtual servers which are out-of-service.

- CSCee23043

  The cookie offset and length commands cause the CSM to hang and stop responding to CLI commands.

  When you configure a cookie sticky group, the CSM generates a regular expression string so that the hardware can parse the input for the cookie name you specify. The format of this regular expression string is: <cookie-name>=(*)

  When the cookie offset and length values are changed, this regular expression string is changed to those new values. For example, if the cookie-name is FOO, the offset is 2, and the length is 3, then this regular expression string would be: FOO=??(???)*

  The first set of question marks correspond to the offset value. The second set of question marks correspond to the length. The CSM may hang and stop responding to CLI input when this regular expression string is longer than 255 characters.

  For the secondary cookie sticky (for example, cookie in the URL string), the CSM replaces a single question mark with this sequence `[^/?&#+]`.

  For the previous example showing the offset as 2 and length as 3, the secondary cookie string is:

  ```
  FOO=[^/?&#+][^/?&#+]([^/?&#+][^/?&#+][^/?&#+])*
  ```

  As a result, the regular expression string may have more than 255 character if the offset value is 32 and the length is 8.

  Workaround: Reduce the configured values for the offset and length values. You may also, as an alternative work around, reduce the number of characters as the possible delimiters in the URL by configuring the environment variable: `variable HTTP_URL_COOKIE_DELIMITERS "&?"`

- 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.

Resolved Caveats in Software Release 4.1(3)

Note For a description of caveats open in CSM software release 4.1(3), see the "Open Caveats in Software Release 4.1(3)" section on page 52.

CSCeg38830

When you configure the Cookie Insert or Header Insert feature and you enable the sticky database replication option, the CSM may fail and reboot. The core-dump information would show "IXP4 Bad Data exception on task 'IXP4 SA-CORE (Ex 5)(00000000h)." This problem exists in CSM releases 4.1(1) and 4.1(2).

Workaround: Disable the sticky replication option or the Cookie Insert feature.

- CSCeg31247

  The CSM closes the connection when it receives a RST packet that it believed to be the correct sequence number. In some cases, the server would ignore this RST packet because the server had seen data beyond the TCP sequence number in the RST packet. This action causes the situation where the server will still have an opened connection that only can be timed out by the TCP stack on the server. In this 4.1(3) release, there is an additional configurable environment variable "TCP_ACCEPT_RST_EQU_NEXT_GET_SEQ" which forces the CSM to a more strict sequence number check and leaves the connection opened (with a quicker idle timer) on the CSM if the RST packet does not match this condition.

  Workaround: Tune the TCP stack on the server to have a quicker timeout value.

- CSCeg17294

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

  Workaround: None.

- CSCeg07844

  If an RST packet with an invalid sequence number follows the FIN packet immediately, the CSM accepts this RST and closes the connection. This problem occurs for Layer 4 virtual servers only.

  Workaround: None.

- CSCef95806

  When performing Layer 7 load-balancing, sometimes the CSM forwards an RST packet with an invalid TCP checksum value to the server. This condition can cause the server to have unclosed connections.

  Workaround: None.

- CSCef82282

  For a given HTTP request, if the client sends in a valid (not expired) sticky HTTP cookie, the CSM does not learn the new cookie value in the server reply. This action creates a situation in which the real server keeps changing the cookie value that is being used for persistent connections by the CSM. As a result, the subsequence client request with the new cookie value is not sticky.

  Workaround: None.

- CSCef66494

  When enabling the cookie insert sticky feature on the CSM, the module does not insert the configured cookie into the HTTP header of the server response. This action creates a situation in which the CSM incorrectly inserts the cookie into the HTTP body of the server response. These conditions may trigger this problem:

  c. The server response contains multiple packets.

  d. The last packet contains the HTTP body instead of HTTP header.

  e. The last packet contains a blank line (sequence of CR, LF, CR, LF characters).

  f. The server also sent the FIN immediately right after the last packet.

  Workaround: None.

- CSCef27321

  When connections are replicated with destination port translation (the virtual server port is different from the port configured for the real server) to the redundant CSM, the data flows may have been incorrectly set up. If the redundant CSM that is in standby mode becomes active, all traffic that matched these flows would be forward by the CSM with an invalid TCP checksum value.

  Workaround: Remove the destination port configured on the real server.

- CSCee74402

  When configured with a destination port translation for a real server, the CSM is unable to send a RST character to the server when choosing another server for HTTP persistent rebalancing. The connection remains open on the server. This situation prevents the HTTP persistent connection from being re-balanced back to the server.

  Workaround: Remove the destination port configured on the real server.

Open Caveats in Software Release 4.1(2)

Note For a description of caveats resolved in CSM software release 4.1(2), see the "Resolved Caveats in Software Release 4.1(2)" section on page 55.

This section describes known limitations that exist in CSM software release 4.1(2).

- 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.

Resolved Caveats in Software Release 4.1(2)

Note For a description of caveats open in CSM software release 4.1(2), see the "Open Caveats in Software Release 4.1(2)" section on page 55.

CSM software release 4.1(2) is the first release in a new release train. The caveats listed here are those resolved since the last CSM release 3.1(4).

- CSCef38895

  The CSM sometimes drops the first fragment in bridge mode.

  Workaround: None.

- CSCee71689

  The **failaction purge** option does not work in CSM software releases 3.2(1), 3.2(2), and 4.1(1). When the server becomes non-operational, the CSM does not clear the connections associated with this server. The Commands Bad Sequence counter increases for each connection that failed to be purged.

  Workaround: None. Workaround: None.

- CSCec29347

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

  Workaround: None.

- CSCec17979

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

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

- CSCec14873

  The data channel for an FTP connection does not replicate to the standby CSM if the standby module is not online when you run the FTP command.

  Workaround: None.

- CSCec13204

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

  Workaround: None.

- CSCec12711

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

  Workaround: In this release, you can configure the TCP_MSS_OPTION variable to a value used by the CSM for subsequent requests.

- CSCec09135

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

  Workaround: None.

- CSCec09012

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

  Workaround: None.

- CSCec03156

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

  Workaround: You must enter into the CSM debug prompt to access this command.

- CSCeb86683

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

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

  Workaround: None.

- CSCeb80844

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

  Workaround: Use a redirect string smaller than 22 characters.

- CSCeb69592

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

  Workaround: None.

- CSCeb60981

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

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

- CSCeb55530

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

  Workaround: None.

- CSCeb50227

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

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

- CSCea33676

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

  Workaround: None.

- CSCdz18550

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

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

Open Caveats in Software Release 4.1(1)

Note For a description of caveats resolved in CSM software release 4.1(1), see the "Resolved Caveats in Software Release 4.1(1)" section on page 59.

This section describes known limitations that exist in CSM software release 4.1(1).

- 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.

Resolved Caveats in Software Release 4.1(1)

Note For a description of caveats open in CSM software release 33(1), see the "Open Caveats in Software Release 4.1(1)" section on page 58.

CSM software release 4.1(1) is the first release in a new release train. The caveats listed here are those resolved since the last CSM release 3.1(4).

- CSCec29347

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

  Workaround: None.

- CSCec17979

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

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

- CSCec14873

  The data channel for an FTP connection does not replicate to the standby CSM if the standby module is not online when you run the FTP command.

  Workaround: None.

- CSCec13204

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

  Workaround: None.

- CSCec12711

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

  Workaround: In this release, you can configure the TCP_MSS_OPTION variable to a value used by the CSM for subsequent requests.

- CSCec09135

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

  Workaround: None.

- CSCec09012

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

  Workaround: None.

- CSCec03156

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

  Workaround: You must enter into the CSM debug prompt to access this command.

- CSCeb86683

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

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

  Workaround: None.

- CSCeb80844

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

  Workaround: Use a redirect string smaller than 22 characters.

- CSCeb69592

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

  Workaround: None.

- CSCeb60981

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

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

- CSCeb55530

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

  Workaround: None.

- CSCeb50227

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

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

- CSCea33676

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

  Workaround: None.

- CSCdz18550

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

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

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, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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

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

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2005–2009, Cisco Systems, Inc.
All rights reserved.