Release Notes for Catalyst 6500 Series Content Switching Module Software Release 3.2(3)

Current Release: 3.2(3)—July 6, 2004
Previous Releases: 3.2(2, 3.2(1)

This publication describes the features, modifications, and caveats for the Catalyst 6500 series Content Switching Module (CSM) software release 3.2(3) running on a Catalyst 6500 series switch with Cisco IOS software Release 12.1(19)E or Catalyst operating system software release 7.5 or higher.

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

Contents

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

System Requirements

This section describes the system requirements for the Catalyst 6500 series CSM software release 3.2(3).

Memory Requirements

The Catalyst 6500 series CSM memory is not configurable.

Hardware Supported

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

Note To use the CSM with a Supervisor Engine 720, you must use Cisco IOS Release 12.2(14)SX2 software or higher running on the switch.

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

Product Number	Minimum Cisco IOS Release	Recommended Cisco IOS Release	Recommended Catalyst OS Releases
Content Switching Module			
WS-X6066-SLB-APC with Supervisor Engine 1 and MSFC1 or MSFC2	12.1(13)E3	12.1(19)E	7.5
Supervisor Engine 2 with MSFC2	12.1(13)E3	12.1(19)E	7.5
WS-X6066-SLB-APC with Supervisor Engine 720.	12.2(14)SX2	12.2(17a)SX1 or higher	8.1
Console Cable			
72-876-01		Not applicable	
Accessory Kit			
800-05097-01		Not applicable	

Software Compatibility

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

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

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

Table 1 CSM with Cisco IOS Software Requirements

CSM Release	Supervisor Engine 1 MSFC1 or MSFC2		Supervisor Engine 2 with MSFC2		Supervisor 720 with MSFC 3	
	Minimum Software Release	Recommended Software Release	Minimum Software Release	Recommended Software Release	Minimum Software Release	Recommended Software Release
3.2(3)	12.1(13)E3	12.1(19)E	12.1(13)E3	12.1(19)E	12.2(14)SX2	12.2(17a)SX1
3.2(2)	12.1(13)E3	12.1(19)E	12.1(13)E3	12.1(19)E	12.2(14)SX2	12.2(17a)SX1
3.2(1)	12.1(13)E3	12.1(19)E	12.1(13)E3	12.1(19)E	12.2(14)SX2	12.2(17a)SX1

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

CSM Release	Supervisor Engine 1 MSFC1 or MSFC2		Supervisor Engine 2 with MSFC2		Supervisor Engine 720 with MSFC 3	
	Minimum Software Release	Recommended Software Release	Minimum Software Release	Recommended Software Release	Minimum Software Release	Recommended Software Release
3.2(3)	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(19)E with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(14)SX2 with Catalyst operating system 8.1	Cisco IOS 12.2(17a)SX1 with Catalyst operating system 8.1
3.2(2)	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(19)E with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(14)SX2 with Catalyst operating system 8.1	Cisco IOS 12.2(17a)SX1 with Catalyst operating system 8.1
3.2(1)	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(19)E with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.1(13)E3 with Catalyst operating system 7.5	Cisco IOS 12.2(14)SX2 with Catalyst operating system 8.1	Cisco IOS 12.2(17a)SX1 with Catalyst operating system 8.1

Feature Set

Table 3 describes the CSM features and software descriptions.

Table 3 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-3.2-CSM

Table 3 CSM Feature Set Description (continued)

Feature	First Image Release	Supported Release
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-3.2-CSM
Supervisor 720—requires CSM software release 3.1(4) or later.	c6slb-apc.3-2-1.bin	SC6K-3.2-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
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
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
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
UDP & all common IP protocol load balancing Load balancing per packet allowing the CSM to make a load balancing decisions without creating a flow. This feature 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
Real Time Streaming Protocol (RTSP)	c6slb-apc.2-2-1.bin	SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-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
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

Table 3 CSM Feature Set Description (continued)

Feature	First Image Release	Supported Release
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
Miscellaneous Functionality		
TCP fragmentation support, allowing the CSM to handle fragmented TCP packets	c6slb-apc.3-2-1.bin	SC6K-3.2-CSM
Route lookup, allowing 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
Denial of Service (DoS) improvements, allowing TCP termination for all connections to the CSM providing SYN attacks	c6slb-apc.3-2-1.bin	SC6K-3.2-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
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
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
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
HTTP method parsing	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM SC6K-3.2-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
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

Table 3 CSM Feature Set Description (continued)

Feature	First Image Release	Supported Release
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-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-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
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
Least connections	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM
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
URL hashing	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-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
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
Return error code checking	c6slb-apc.2-2-1.bin	SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM
Support for 127VLANs 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
Jumbo Frames allow support of frames of up to 9k bytes for Layer 4 load balancing.	c6slb-apc.3-2-1.bin	SC6K-3.2-CSM

Table 3 CSM Feature Set Description (continued)

Feature	First Image Release	Supported Release
Reduced time between health probes	c6slb-apc.2-2-1.bin	SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM
In-band health checking	c6slb-apc.2-2-1.bin	SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM
Configurable pending connection timeout	c6slb-apc.2-2-1.bin	SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM
IP reassembly for in-order UDP fragments	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM
IP reassembly for out-of-order UDP fragments	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM SC6K-3.2-CSM
VIP connection watermarks	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM SC6K-3.2-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
Real server names	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM SC6K-3.2-CSM
Slowpath performance improvements	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM SC6K-3.2-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
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. This feature 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
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

Table 3 CSM Feature Set Description (continued)

Feature	First Image Release	Supported Release
Stealth firewall load balancing	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
Transparent cache redirection	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-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
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
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
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
Stickiness		
Cookie	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-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
Source IP	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-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
Cisco IOS SLB FWLB interoperation (IP reverse-sticky)	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM SC6K-3.2-CSM
Redundancy		

Table 3 CSM Feature Set Description (continued)

Feature	First Image Release	Supported Release
Sticky state	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
Static sticky entries, allowing prepopulation of the sticky table with entries that force users to connect to specific servers.	c6slb-apc.3-2-1.bin	SC6K-3.2-CSM
Sticky debug tools, including 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. The new **show** command can display sticky entries for Cookie and SSL sticky groups.		
Full stateful failover (connection redundancy)	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM
Failover improvements providing enhancements for preempt option with connection replication, the **forced failover** command	c6slb-apc.3-2-1.bin	SC6K-3.2-CSM
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
Non-TCP connection redundancy	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM SC6K-3.2-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
HTTP	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM
ICMP	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM
Telnet	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM
TCP	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM

Table 3 CSM Feature Set Description (continued)

Feature	First Image Release	Supported Release
SMTP	c6slb-apc.1-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-CSM
DNS	c6kslb-apc.2-1-1.bin	SC6K-2.1-CSM SC6K-2.2-CSM SC6K-3.1-CSM SC6K-3.2-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
TCL (Toolkit Command Language) scripting	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM
Provides User Datagram Protocol (UDP) socket and global variable support. XML configuration from a TCL Script adds the ability to send CSM configuration commands within a TCL script.	c6slb-apc.3-2-1.bin	SC6K-3.2-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
Added management features from release 3.1(1) and 3.2(1). Includes the XML DTD (document definition type), 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
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
SNMP traps on fault-tolerant state changes	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM SC6K-3.2-CSM
Support for CISCO-SLB-MIB	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM SC6K-3.2-CSM
Support for CISCO-SLB-EXT-MIB	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM SC6K-3.2-CSM
XML configuration interface	c6slb-apc.3-1-1.bin	SC6K-3.1-CSM SC6K-3.2-CSM
Resource use display	c6slb-apc.3-1-1.bin c6slb-apc.3-2-1.bin	SC6K-3.1-CSM SC6K-3.2-CSM

New and Changed Information

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

  A new environment variable, REAL_SLOW_START_ENABLE, is included in the 3.1(8) and 3.2(3) software releases to control the rate at which a real server becomes operational when it is put into service. This new variable is only available for a server farm that has been configured with the least connection predictor.

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

  If the configuration value is N, the CSM assigns 2 ^ N (2 raised to the N power) new requests to the newly active server at startup (assuming no connections were terminated at that time). As this server finishes or terminates connections, more connections are assigned. Normal connection assignments resume when the newly activated server has the same number of open connections as the other servers in a serverfarm.
- CSM release 3.2(3) is supported in Catalyst operating system software release 7.6.
- 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

  This file contains the scripts: c6slb-script.3-2-1.tcl.

Limitations and Restrictions

- The CSM does not support pipelines (multiple HTTP requests sharing the packet boundary) with the persistent rebalance feature.
- Internal ports on the CSM (dot1q, trunk, port-channel, and so on.) are automatically configured, with the exception of the VLANs on the trunk, which must be manually added using the **set trunk** *slot* 1 *vlan-list* command in Catalyst operating system.
- When configuring Route Health Injection (RHI), proxy ARP must be disabled on the Catalyst 6500 series switch chassis (proxy-ARP is enabled by default). You must disable proxy ARP on a per-interface basis in the interface submode. We recommend that you disable proxy ARP on the VLAN level using the **no ip proxy arp** command.
- The meaning of having no minimum connections (MINCONNS) parameter set in the **real** submode is different between release 2.2(1) and later releases.

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

In all releases, when the MINCONNS value is set, once a real server has reached the maximum connections (MAXCONNS) state, no additional session is balanced to it until the number of open sessions to that real server falls below MINCONNS. With the no MINCONNS value set in release 1.1(1), no additional session would be balanced until the number of open sessions to that real server falls to 0. With no MINCONNS value set in release 1.2(1), no additional session is balanced until the number of open sessions falls below MAXCONNS.

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

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

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

Caveats

These sections describe the open and resolved caveats in CSM software for all 3.2(x) software releases:

Open Caveats in Software Release 3.2(3)

Note For a description of caveats resolved in CSM software release 3.2(3), see the "Resolved Caveats in Software Release 3.2(3)" section on page 14.

This section describes known limitations that exist in CSM software release 3.2(3).

- CSCef01257

  When you enable the persistent rebalance option for an HTTP connection, the CSM does not send out the reset (RST) response to the previously balanced server if the subsequent HTTP request was rejected by the CSM.

  Workaround: None.

- CSCee22621

  Entering the **no module csm** *slot-number* command removes your existing CSM module configuration with no warning message.

  Workaround: none.

- CSCed24671

  The CSM selects an incorrect route for the predictor forward method if the identity of the route or gateway changes. If the VLAN interface was configured, but the route or gateway was not configured, the CSM learns this device as an external host. If the IP address for this device is then configured as a router or gateway, then its identity changes. This situation only affects the virtual server using the predictor forward to select the destination.

  Workaround: If the VLAN is configured, and the CSM is online, you need to use the **clear module csm** *slot* **arp** command before creating the gateway. Or, reset the CSM after changing the gateway configuration.

- CSCed10730

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

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

- CSCed01651

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

  Workaround: None.

- CSCec84034

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

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

- 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.

- CSCec21915

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

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

- 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-parselength option to reduce the unnecessary wait for invalid HTTP connections.

Resolved Caveats in Software Release 3.2(3)

Note For a description of caveats open in CSM software release 3.2(3), see the "Open Caveats in Software Release 3.2(3)" section on page 12.

- CSCee74402

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

  Workaround: None.

- CSCee71689

  The **failaction purge** command has no effect on UDP traffic when you use Cisco IOS software. The Commands Bad Sequence counter increases for each connection that failed to be purged.

  Workaround: None.

- CSCee70058, CSCee69755

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

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

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

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

Workaround: None.

- CSCee50280

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

  Workaround: None.

- CSCee45978

  When the servers reach the configured “max-conns” state, the CSM sends syslog messages to the Cisco IOS supervisor engine. If there are many servers in a serverfarm in this state, the CSM is slow to respond to connections and user requests. You may not be able to issue commands to the CSM.

  Workaround: Remove the max-conns configuration from the real servers, and apply the max-conns configuration at the virtual server level.

- CSCee45483

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

  Workaround: None.

- CSCee44921

  When configuring a backup real server, the CSM activates the backup server if the primary server failed the health probe. The CSM does not disable the backup server when the primary server becomes healthy again.

  Workaround: Take the primary server out-of-service and then reset it to inservice.

- CSCee42680

  The CSM accepts packets from a multicast destination MAC address, even if the destination IP address (unicast) is not configured on the CSM. As a result, the CSM resets all TCP connections to an IP address associated with a multicast MAC address.

  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 RST or FIN-ACK response. This problem causes the client to retransmit and repeat the FIN response.

  Workaround: None.

- CSCee27428

  After enabling Layer 7 parsing for a virtual server, the CSM sends a SYN-ACK (synchronize-acknowledge) packet for the initial SYN packet from the client. If for some reasons the client resent the SYN packet, the CSM would mistakenly send an ACK (acknowledge) packet without the synchronize (SYN) flag back to the client.

  Workaround: None.

- CSCee26981

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

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

- CSCee15535

  When the virtual server is configured as Layer 7, it shows up as Layer 4 in the **show mod c X vserver detail** command.

  Workaround: None.

- CSCee13546

  The is release has no configuration option for disabling the slow start feature for the leastconns parameter. CSM release 3.2(3) introduces a configurable variable REAL_SLOW_START_ENABLE was introduced to disable or control the rate of ramping up a newly operational server in a serverfarm with predictor leastconns. Refer to the "New and Changed Information" section on page 11 for more information.

  Workaround: None.

- CSCed90292

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

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

- CSCed06861

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

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

Open Caveats in Software Release 3.2(2)

Note For a description of caveats resolved in CSM software release 3.2(2), see the "Resolved Caveats in Software Release 3.2(2)" section on page 18.

This section describes known limitations that exist in CSM software release 3.2(2).

- CSCed24671

  The CSM selects an incorrect route for the predictor forward method if the identity of the route or gateway changes. If the VLAN interface was configured, but the route or gateway was not configured, the CSM learns this device as an external host. If the IP address for this device is then configured as a router or gateway, then its identity changes. This situation only affects the virtual server using the predictor forward to select the destination.

  Workaround: If the VLAN is configured, and the CSM is online, you need to use the **clear module csm** *slot* **arp** command before creating the gateway. Or, reset the CSM after changing the gateway configuration.

- CSCed10730

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

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

- CSCed01651

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

- CSCec84034

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

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

- 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.

- CSCec21915

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

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

- 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-parselength option to reduce the unnecessary wait for invalid HTTP connections.

Resolved Caveats in Software Release 3.2(2)

Note For a description of caveats open in CSM software release 3.2(2), see the "Open Caveats in Software Release 3.2(2)" section on page 16.

- CSCed67747

  In release 3.2(1), the "predictor hash url" option and the HTTP return code checking feature could not be used in a virtual server with a matching URL configured. This problem exists only in this release.

  Workaround: Use the previous release.

- CSCed63583

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

  Workaround: Change the server to also send the Cookie information in the "HTTP 100 Continue" packet.

- CSCed36167

  The CSM receives the UDP fragments in the correct order and then sends the UDP fragments out of order. When another device in the network cannot process the fragments out-of-order, these flows will experience problems.

  Workaround: Make sure that other devices can process the UDP fragments in any order.

- CSCed12746

  The SYN Cookie feature in CSM software release 3.2(1) does not work after the CSM has sent the SYN-ACK packet if the client sends an ACK packet that includes data for the CSM. This condition always exists if the client is another CSM.

  Workaround: Turn off the SYN Cookie feature by setting the SYN_COOKIE_THRESHOLD to a very high value.

- CSCed06861

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

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

- CSCec87250

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

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

- CSCec70074

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

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

- CSCec47603 and CSCec82096

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

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

- CSCec35401

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

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

- CSCec12630

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

  Workaround: None.

- CSCec08598

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

  Workaround: None.

- CSCeb72016

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

  Workaround: None.

- CSCea69875

  An invalid IP checksum packet could bypass the Catalyst 6500 Series switch check and enter the CSM. An invalid IP packet could put the CSM into a non-functional state, causing it to drop all load-balancing traffic. Health probe and bridging traffic would continue to function properly in this case. CSM software release 3.1(4) includes a fix for this problem. However, this fix resolves only some of the load-balancing requests. The fix in CSM software release 3.1(6) should resolve all load-balancing traffic.

  Workaround: None.

Open Caveats in Software Release 3.2(1)

Note For a description of caveats resolved in CSM software release 3.2(1), see the "Resolved Caveats in Software Release 3.2(1)" section on page 20.

This section describes known limitations that exist in CSM software release 3.2(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.

- CSCec21915

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

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

- 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 or not 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 3.2(1)

Note For a description of caveats open in CSM software release 3.2(1), see the "Open Caveats in Software Release 3.2(1)" section on page 20.

CSM software release 3.2(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 CSM software release 3.2(1), 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 CSM software release 3.1(4), the CSM used only the simple round-robin method, with all the real server weights being equal. This feature was broken in 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 appear 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 with fewer than 22 characters.

- CSCeb69592

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

  Workaround: None.

- CSCeb60981

  The CSM might 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 6500 series 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:

- *Catalyst 6500 Series Content Switching Module Installation and Configuration Note*
- *Regulatory Compliance and Safety Information for the Catalyst 6500 Series Switches*
- *Catalyst 6500 Series Installation Guide*
- *Catalyst 6500 Series Quick Software Configuration Guide*
- *Catalyst 6500 Series Module Installation Guide*
- *Catalyst 6500 Series Software Configuration Guide*
- *Catalyst 6500 Series Command Reference*
- *Catalyst 6500 Series IOS Software Configuration Guide*
- *Catalyst 6500 Series IOS Command Reference*
- *ATM Software Configuration and Command Reference—Catalyst 5000 Family and Catalyst 6500 Series Switches*
- *System Message Guide—Catalyst 6500 Series, 5000 Family, 4000 Family, 2926G Series, 2948G, and 2980G Switches*
- For information about MIBs, refer to

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

Cisco IOS Software Documentation Set

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

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

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

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

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

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

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

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco Technical Support Website

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

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

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

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

Submitting a Service Request

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

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

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

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

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

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

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

Definitions of Service Request Severity

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

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

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

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

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

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

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

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

  http://www.ciscopress.com

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

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

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

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

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

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

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

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