# Release Notes for Catalyst 6500 Series Content Switching Module Software Release 4.3(x)

**Current Release: 4.3(6)—January 27, 2012**
**Previous releases: 4.3(5), 4.3(4), 4.3(3), 4.3(2), 4.3(1)**

This publication describes the features, modifications, and caveats for the Catalyst 6500 series Content Switching Module (CSM), software release 4.3(x), operating on the following platforms:

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

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

## Contents




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

# System Requirements

This section describes the system requirements for the Catalyst 6500 series CSM software release 4.3(x).

## Memory Requirements

The Catalyst 6500 series CSM memory is not configurable.

## Hardware Supported

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

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

| Product Number | Minimum[1] Cisco IOS Software | Recommended[2] Cisco IOS Software | Minimum Catalyst Operating System Software | Recommended Catalyst Operating System Software |
|---|---|---|---|---|
| **Content Switching Module (WS-X6066-SLB-APC)** | | | | |
| Supervisor Engine 1A and MSFC1 or MSFC2 | 12.1(8a)EX | 12.2(18)SXF15 | Cisco IOS Release 12.2(13)E3 with Catalyst operating system software 7.5 | Cisco IOS Release 12.2(18)SXF15 with Catalyst operating system software 7.5 |
| Supervisor Engine 2 with MSFC2 | 12.1(8a)EX or 12.2(17d)SXB | 12.2(18)SXF15 | Cisco IOS Release 12.2(13)E3 with Catalyst operating system software 7.5 | Cisco IOS Release 12.2(18)SXF15 with Catalyst operating system software 7.5 |
| Supervisor Engine 720 with MSFC3 | 12.2(14)SX1 | 12.2(18)SXF15 | Cisco IOS Release 12.2(14)SX2 with Catalyst operating system software 8.2(1) | Cisco IOS Release 12.2(18)SXF15 with Catalyst operating system software 8.2(1) |

| Product Number | Minimum[1] Cisco IOS Software | Recommended[2] Cisco IOS Software | Minimum Catalyst Operating System Software | Recommended Catalyst Operating System Software |
|---|---|---|---|---|
| Supervisor Engine 720-10G | 12.2(33)SXI2 | 12.2(33)SXI2 | Not Supported | Not Supported |
| **Console Cable** | | | | |
| 72-876-01 | | Not applicable | | Not applicable |
| **Accessory Kit** | | | | |
| 800-05097-01 | | Not applicable | | Not applicable |

1. The minimum software release required to support the CSM hardware with a given Supervisor Engine to perform basic CSM configuration.
2. The base software release required to support new commands for a given CSM release.

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

# Software Compatibility

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

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 Cisco IOS Software on the Supervisor Engine and MSFC***

| CSM Release | Supervisor Engine 1 MSFC1 or MSFC2 | | Supervisor Engine 2 with MSFC2 | | Supervisor Engine 720 with MSFC 3 | |
|---|---|---|---|---|---|---|
| | Minimum[1] Software Release | Recommended[2] Software Release | Minimum Software Release | Recommended Software Release | Minimum Software Release | Recommended Software Release |
| 4.3(6) | 12.1(8a)EX | 12.2(18)SXF15 | 12.1(8a)EX | 12.2(18)SXF15 | 12.2(14)SX1 | 12.2(18)SXF15 |
| 4.3(5) | 12.1(8a)EX | 12.2(18)SXF15 | 12.1(8a)EX | 12.2(18)SXF15 | 12.2(14)SX1 | 12.2(18)SXF15 |
| 4.3(4) | 12.1(8a)EX | 12.2(18)SXF15 | 12.1(8a)EX | 12.2(18)SXF15 | 12.2(14)SX1 | 12.2(18)SXF15 |
| 4.3(3) | 12.1(8a)EX | 12.2(18)SXF15 | 12.1(8a)EX | 12.2(18)SXF15 | 12.2(14)SX1 | 12.2(18)SXF15 |
| 4.3(2) | 12.1(8a)EX | 12.2(18)SXF15 | 12.1(8a)EX | 12.2(18)SXF15 | 12.2(14)SX1 | 12.2(18)SXF15 |
| 4.3(2) | 12.1(8a)EX | 12.2(18)SXF15 | 12.1(8a)EX | 12.2(18)SXF15 | 12.2(14)SX1 | 12.2(18)SXF15 |
| 4.3(1) | 12.1(8a)EX | 12.2(18)SXF15 | 12.1(8a)EX | 12.2(18)SXF15 | 12.2(14)SX1 | 12.2(18)SXF15 |

1. The minimum software release required to support the CSM hardware with a given Supervisor Engine to perform basic CSM configuration.
2. The base software release required to support new commands for a given CSM release.

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

| CSM Release | Supervisor Engine 1 MSFC1 or MSFC2 | | Supervisor Engine 2 with MSFC2 | | Supervisor Engine 720 with MSFC 3 | |
|---|---|---|---|---|---|---|
| | Minimum[1] Software Release | Recommended[2] Software Release | Minimum Software Release | Recommended Software Release | Minimum Software Release | Recommended Software Release |
| 4.3(6) | 12.2(13)E3 with 7.5 | 12.2(18)SXF15 with 7.5 | 12.2(13)E3 with 7.5 | 12.2(18)SXF15 with 7.5 | 12.2(33)SX12 with 8.2(1) | 12.2(33)SX12 with 8.2(1) |
| 4.3(5) | 12.2(13)E3 with 7.5 | 12.2(18)SXF15 with 7.5 | 12.2(13)E3 with 7.5 | 12.2(18)SXF15 with 7.5 | 12.2(33)SX12 with 8.2(1) | 12.2(33)SX12 with 8.2(1) |
| 4.3(4) | 12.2(13)E3 with 7.5 | 12.2(18)SXF15 with 7.5 | 12.2(13)E3 with 7.5 | 12.2(18)SXF15 with 7.5 | 12.2(33)SX12 with 8.2(1) | 12.2(33)SX12 with 8.2(1) |
| 4.3(3) | 12.2(13)E3 with 7.5 | 12.2(18)SXF15 with 7.5 | 12.2(13)E3 with 7.5 | 12.2(18)SXF15 with 7.5 | 12.2(33)SX12 with 8.2(1) | 12.2(33)SX12 with 8.2(1) |
| 4.3(2) | 12.2(13)E3 with 7.5 | 12.2(18)SXF15 with 7.5 | 12.2(13)E3 with 7.5 | 12.2(18)SXF15 with 7.5 | 12.2(14)SX2 with 8.2(1) | 12.2(18)SXF15 with 8.2(1) |
| 4.3(1) | 12.2(13)E3 with 7.5 | 12.2(18)SXF15 with 7.5 | 12.2(13)E3 with 7.5 | 12.2(18)SXF15 with 7.5 | 12.2(14)SX2 with 8.2(1) | 12.2(18)SXF15 with 8.2(1) |

1. The minimum software release required to support the CSM hardware with a given Supervisor Engine to perform basic CSM configuration.
2. The base software release required to support new commands for a given CSM release.

# New Features

Table 3 lists the features that have been added in CSM software release 4.3(x). For detailed information about using the new features, see the "New and Changed Information" section on page 9.

*Table 3 New CSM Feature Set Description*

| New Features in this Release | Description |
|---|---|
| New predictor type staticload added | When the configured predictor type is staticload, load balancing across real servers of the server farm will be based on a statically configured load value. Either the CLI or the XML configuration feature can be used to configure the predictor type and the load value of the real servers. |
| Enhanced **show module csm** *slot* **vserver detail** command | Displayed information from the **show module csm** *slot* **vserver detail** command now includes the virtual server's current load value and the number of virtual server transitions. |

# Feature Set

Table 4 describes the CSM features and software descriptions.

*Table 4 CSM Feature Set Description*

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

*Table 4 CSM Feature Set Description (continued)*

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

*Table 4 CSM Feature Set Description (continued)*

| Feature | First Image Release |
|---|---|
| Slow start improvements | c6slb-apc.4-2-1.bin |
| Non-secure router mode | c6slb-apc.4-2-1.bin |
| Increase virtual server limit | c6slb-apc.4-2-1.bin |
| Secure XML communication | c6slb-apc.4-2-1.bin |
| **Load Balancing Supported** | |
| Server load balancing | c6slb-apc.1-1-1.bin |
| Firewall load balancing | c6kslb-apc.2-1-1.bin |
| 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) | c6slb-apc.3-2-1.bin |
| DNS load balancing | c6kslb-apc.2-1-1.bin |
| Stealth firewall load balancing | c6kslb-apc.2-1-1.bin |
| Transparent cache redirection | c6kslb-apc.2-1-1.bin |
| Reverse proxy cache | c6slb-apc.1-1-1.bin |
| SSL off-loading | c6slb-apc.1-1-1.bin |
| VPN-IPSec load balancing | c6kslb-apc.2-1-1.bin |
| Enhanced interoperation with the SSL termination engine (STE) for secure socket layer (SSL) load balancing | c6slb-apc.3-1-1.bin |
| Load balancing based on static load | c6slb-apc.4-3-1.bin |
| **Stickiness** | |
| Cookie | c6slb-apc.1-1-1.bin |
| SSL ID | c6slb-apc.1-1-1.bin |
| Source IP | c6slb-apc.1-1-1.bin |
| HTTP redirection | c6slb-apc.1-1-1.bin |
| Cisco IOS SLB FWLB interoperation (IP reverse-sticky) | c6slb-apc.3-1-1.bin |
| HTTP header sticky | c6slb-apc.4-2-1.bin |
| **Redundancy** | |
| Sticky state | c6slb-apc.1-1-1.bin |
| Static sticky entries—allow prepopulation of the sticky table with entries that force users to connect to specific servers | c6slb-apc.3-2-1.bin |
| 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) | |
| Full stateful failover (connection redundancy) | c6kslb-apc.2-1-1.bin |
| Failover improvements—provide enhancements for preempt option with connection replication, the **forced failover** command | c6slb-apc.3-2-1.bin |
| Partial server farm failover | c6slb-apc.4-2-1.bin |

*Table 4 CSM Feature Set Description (continued)*

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

# New and Changed Information

- CSCsv78324

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

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

  The CLIENT_NAT_NO_PAT variable has the following syntax:

  Name: CLIENT_NAT_NO_PAT

  Rights: RW

  Default: 0

  Valid values: Integer (0 to 1)

  Description: Disables (1 = no PAT) PAT where possible when client NAT is performed.

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

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

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

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

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

  This change appears in CSM software release 4.3(3).

- New predictor type staticload feature.

  Supplementing the existing predictor types for server load balancing (such as round-robin, least connections, or address hashing), a new predictor type staticload has been added. When the configured predictor type is staticload, load balancing across real servers of the server farm will be based on a load value statically configured by the user.

  The selection of the predictor type is made in the server farm configuration submode, as shown in this example:

```
Router(config-slb-sfarm)# predictor staticload
```

  You can specify the static load for each real server in the real server configuration submode as shown in this example:

```
Router(config-slb-real)# staticload real_server_load
```

  The range for the *real_server_load* argument is from 2 to 254. The default value of 2 indicates the least load, while a value of 254 indicates the maximum load.

As an alternative to the CLI, the XML configuration feature can be used to configure the predictor type and the load value of the real servers.

- Enhanced **show module csm** *slot* **vserver detail** command.

  Displayed information from the **show module csm** *slot* **vserver detail** command now includes the virtual server's current load value and the number of virtual server transitions. When the staticload predictor has been selected, the current load is the average of the configured static loads for the server farm. (If the staticload predictor is not selected, the current load shows the dynamic load of the virtual IP address.) The transition count indicates the number of times a load of 255 has been reported to the Global Site Selector (GSS).

  The following is an example of the **show module csm** *slot* **vserver detail** command output:

```
Router# show module csm slot vserver detail

<vserver_name>, type = SLB, state = OPERATIONAL, v_index = 52
  virtual = <vserver_ip/mask>:<port> bidir, TCP, service = NONE, advertise = FALSE
  idle = 3600, replicate csrp = sticky/connection, vlan = ALL, pending = 30, layer 7
  max parse len = 4000, persist rebalance = TRUE
  ssl sticky offset = 0, length = 32
  conns = <current_connections>, total conns = <total_connections>
   current load = <avg.config.load>, transition count = <trans.count>
  Default policy:
    server farm = serverfarm_name, backup = <not assigned>
    sticky: timer = 0, subnet = 0.0.0.0, group id = 0
  Policy          Tot matches  Client pkts  Server pkts
  ------------------------------------------------------
  (default)       0            0            0
```

- 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.

- New environment variable PARSE_REVERSE_RESET.

  When both sticky and persistent rebalance are configured, the CSM enables the PARSE_REVERSE_TRAFFIC flag for the session descriptor so that it will inspect all server replies. In rare cases, the PARSE_REVERSE_TRAFFIC flag is not cleared after parsing, and subsequent packets from the client are dropped as invalid packets. When the environment variable PARSE_REVERSE_RESET is set to 1 (enabled), the PARSE_REVERSE_TRAFFIC flag will be reset on the next received packet. The default is 0.

- 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).

- New environment variable ARP_VALIDATE_SOURCE_SUBNET.

When ARP_VALIDATE_SOURCE_SUBNET is set to 1 (enabled), the CSM will validate the source subnet of received ARP frames. An ARP frame from an incorrect source subnet will not be processed but will be eligible for repeating. The default is 1 (enabled). This variable was introduced in software release 4.2(7).

# Limitations and Restrictions

- A CSM running software release 4.1(2) or later releases will not respond to pings to the virtual server when it is configured with service termination. The server is operational and is passing TCP flows to the real servers, which are also operational. This example shows the configuration:

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

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

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

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

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

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

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

- If your configuration contains a pair of CSMs in a single fault-tolerant group, and these paired CSMs are in an active-standby state, the CSMs might not retain the valid active-standby state if you add another CSM into this same fault-tolerant group. This action causes the fault-tolerant pair of CSMs to enter an invalid active-active state. In this case, remove the third CSM from the network and reboot the paired CSMs to allow them to recover their fault-tolerant state.

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

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

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

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

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

- Internal ports on the CSM (dot1q, trunk, port-channel, and so on) are automatically configured, with the exception of the VLANs on the trunk, which must be manually added using the **set trunk** *slot* 1 *vlan-list* command in 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.

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

- The **show mod csm** *slot* **tech all** command may display IXP3 utilization above 100 percent when the cookie insert feature and other Layer 7 policies are active and CSM traffic suddenly stops and restarts. In response to this traffic fluctuation, the IXP3 clears and then reestablishes its tables. This activity overloads the IXP3, which results in the loss of some redundancy and slow path messages. The IXP3 recovers after the traffic level stabilizes. (CSCse91983)
- In an active-standby connection state replication setup, the connection counters on the standby CSM were not the same as the counters on the active CSM. The active CSM correctly shows that the connections were load balanced to various servers within a server farm. On the standby CSM, all replicated connections are assigned to a single real server within a server farm. The number of connections shown in the standby CSM might be different from the number of connections seen in the active CSM. This is a minor issue and does not affect the service. (CSCei73146, CSCee75333)
- Fragmented Layer 2 Tunneling Protocol (L2TP) tunneled packets are discarded by the CSM, and the Packets Repeat Reverse Fragmentation counter in the CSM increments quickly. This problem occurs when packets arrive out of order (the MF packets arrive last) and are separated in time by about 10 milliseconds. To avoid this issue, design the network so that all fragments follow the same path, forcing them to arrive in order and closer together. You can also configure a static route in the CSM so that the module knows where to send reassembled fragments that arrived in a reverse order. (CSCeg15173)
- The total conns established counter applies only to an active CSM. The standby CSM might display the total established connections when there is a fault-tolerance switchover, but the total conns established counter remains unchanged. (CSCtn16345)

# Open and Resolved Caveats in Software Release 4.3(6)

These sections describe the open and resolved caveats in CSM software release 4.3(6):


- Open Caveats in Software Release 4.3(6), page 13
- Resolved Caveats in Software Release 4.3(6), page 14


## Open Caveats in Software Release 4.3(6)

**Note** For a description of caveats resolved in CSM software release 4.3(6), see the "Resolved Caveats in Software Release 4.3(6)" section on page 14.

There are no open caveats in CSM software release 4.3(6).

## Resolved Caveats in Software Release 4.3(6)

**Note** For a description of open caveats in CSM software release 4.3(6), see the "Open Caveats in Software Release 4.3(6)" section on page 13.

This section describes resolved caveats in CSM software release 4.3(6):

- CSCtg41899

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

  **Workaround**: None.

- CSCtn86332

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

  **Workaround**: None.

- CSCtj90108

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

  **Workaround**: Disable static NAT.

- CSCtk63031

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

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

- CSCts71706

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

  **Workaround**: None.

# Open and Resolved Caveats in Software Release 4.3(5)

These sections describe the open and resolved caveats in CSM software release 4.3(5):



## Open Caveats in Software Release 4.3(5)

**Note** For a description of caveats resolved in CSM software release 4.3(5), see the "Resolved Caveats in Software Release 4.3(5)" section on page 15.

There are no open caveats in CSM software release 4.3(5).

# Resolved Caveats in Software Release 4.3(5)

**Note** For a description of open caveats in CSM software release 4.3(5), see the "Open Caveats in Software Release 4.3(5)" section on page 14.

This section describes resolved caveats in CSM software release 4.3(5):

- CSCsh20330

  An issue can occur with two operational vservers, VS1 and VS2, when vserver VS2 is tracking the primary vserver VS1. If vserver VS1 goes into OUTOFSERVICE mode because of probes or real server failures, vserver VS2 also goes into OUTOFSERVICE mode as expected. However, in a few seconds, vserver VS2 comes back into OPERATIONAL mode, even when the primary vserver VS1 is in OUTOFSERVICE mode.

  **Workaround**: None.

- CSCte28717

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

  **Workaround**: None.

- CSCte39053

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

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

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

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

- CSCtg56193

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

  **Workaround**: None.

- CSCth52331

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

  **Workaround**: None.

- CSCtg45008

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

Variable Name: L7_TX_CORE_QUEUE_TIMEOUT

Rights: RW

Value: 1

Default: 1

Valid values: Integer (1 to 10).

Description: Time (in seconds) to wait for the Layer 7 TX Core queue to come out of the full state before asserting a core.

**Workaround**: None.

# Open and Resolved Caveats in Software Release 4.3(4)

These sections describe the open and resolved caveats in CSM software release 4.3(4):


- Open Caveats in Software Release 4.3(4), page 16
- Resolved Caveats in Software Release 4.3(4), page 16


## Open Caveats in Software Release 4.3(4)

**Note** For a description of caveats resolved in CSM software release 4.3(4), see the "Resolved Caveats in Software Release 4.3(4)" section on page 16.

This section describes the open caveats in CSM software release 4.3(4):

- CSCte28717

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

  **Workaround**: Reboot the CSM.

## Resolved Caveats in Software Release 4.3(4)

**Note** For a description of open caveats in CSM software release 4.3(4), see the "Open Caveats in Software Release 4.3(4)" section on page 16.

This section describes resolved caveats in CSM software release 4.3(4):

- CSCtd31622

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

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

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

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

- CSCtc25780

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

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

# Open and Resolved Caveats in Software Release 4.3(3)

These sections describe the open and resolved caveats in CSM software release 4.3(3):



## Open Caveats in Software Release 4.3(3)

**Note** For a description of caveats resolved in CSM software release 4.3(3), see the "Resolved Caveats in Software Release 4.3(3)" section on page 18.

This section describes open caveats in CSM software release 4.3(3):

- CSCsz25520

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

  The following output displays an invalid MAC address across the CSM port channel Po259 to the back plane on management VLAN 1:

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

```
*    1  4000.6806.13b8   dynamic  Yes          55   Po259
*    1  0000.3206.69d4   dynamic  Yes          10   Po259
```

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

**Workaround**: None.

- CSCsx64648

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

  **Workaround**: None.

# Resolved Caveats in Software Release 4.3(3)

**Note** For a description of open caveats in CSM software release 4.3(3), see the "Open Caveats in Software Release 4.3(3)" section on page 17.

This section describes resolved caveats in CSM software release 4.3(3):

- CSCsm33035

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

  **Workaround**: Disable persistent rebalance.

- CSCsq36042

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

  **Workaround**: Disable SSL stickiness on the server farm.

- CSCsu39853

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

  **Workaround**: None.

- CSCso69828

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

  **Workaround**: None.

- CSCsz81041

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

  **Workaround**: None.

- CSCsu92969

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

  **Workaround**: Remove multiple SLB policies.

- CSCsz81265

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

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

- CSCsx37458

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

  **Workaround**:

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

# Open and Resolved Caveats in Software Release 4.3(2)

These sections describe the open and resolved caveats in CSM software release 4.3(2):


- Open Caveats in Software Release 4.3(2), page 19
- Resolved Caveats in Software Release 4.3(2), page 20


## Open Caveats in Software Release 4.3(2)

**Note** For a description of caveats resolved in CSM software release 4.3(2), see the "Resolved Caveats in Software Release 4.3(2)" section on page 20.

This section describes open caveats in CSM software release 4.3(2):

- CSCsu39853

  In rare cases, the CLI becomes unresponsive while traffic passes normally.

  **Workaround**: None.

- CSCsh53633

  A CSM running 4.2(6) had a reboot due to IXP 3. The type of crash was known as a "L7 abort."

  **Workaround**: None.

# Resolved Caveats in Software Release 4.3(2)

**Note** For a description of open caveats in CSM software release 4.3(2), see the "Open Caveats in Software Release 4.3(2)" section on page 19.

This section describes resolved caveats in CSM software release 4.3(2):

- CSCsj26680

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

  **Workaround**: None.

- CSCsj88014

  A large delay can occur when updating LOAD using KAL-AP. 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.

- CSCsi85407

  Under a high traffic load, the CSM may halt unexpectedly. The console displays the error message: "P:\ixp1200\core\l7\l7_main.c(395) warning: TX Queue overflow. Shutting down CORE_TX_Q" followed by a core dump.

  **Workaround**: None.

- CSCsh94471

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

- CSCsk43903

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

  **Workaround**: None.

- CSCsk29021

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

  **Workaround**: None.

- 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.

- CSCsl23801

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

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

- CSCsj05855

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

  **Workaround**: None.

- CSCsl59508

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

  **Workaround**: Do not use the **slowstart** command option.

- CSCsk98543

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

  **Workaround**: Remove the threshold command.

- CSCsl07382

  When the CSM is configured for Global Server Load Balancing (GSLB), the active CSM can exhibit a slow memory leak.

  **Workaround**: Monitor memory usage regularly by using the venus console. Open a session to the active CSM by entering the **session slot** *x* **processor 0** command. At the CSM> prompt, enter the **venus** command. At the venus# prompt, enter the **core_show_usage** command. If available memory is less than 20 percent, schedule a reboot of the CSM. Because the memory leak occurs only on the active CSM, the standby CSM should be available to take over.

- CSCsi58089

  The CSM drops SASP server messages larger than 2816 bytes.

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

- CSCsl72371

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

  **Workaround**: None.

- 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.

- CSCso00578

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

  **Workaround**: None.

- CSCso33427

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

  **Workaround**: Possible workarounds include the following:

  - Reduce the server MSS to a value that will not exceed the MTU of the path to the client.
  - Reduce the CSM default MSS using the environment variable TCP_MSS_OPTION.

- CSCso81900

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

  **Workaround**: Reboot the CSM.

- CSCsq84207

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

  **Workaround**: Possible workarounds include the following:

  - Reduce the server MSS to a value that allows the cookie insertion without exceeding the MTU of the path to the client.
  - Reduce the CSM default MSS by using the environment variable TCP_MSS_OPTION.
  - Use a different type of stickiness for the server (for example, application cookies).

- CSCsr79179

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

  **Workaround**: Possible workarounds include the following:

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

- 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.

- CSCsl40722

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

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

# Open and Resolved Caveats in Software Release 4.3(1)

These sections describe the open and resolved caveats in CSM software release 4.3(1):


- Open Caveats in Software Release 4.3(1), page 23
- Resolved Caveats in Software Release 4.3(1), page 24

# Open Caveats in Software Release 4.3(1)

**Note** For a description of caveats resolved in CSM software release 4.3(1), see the "Resolved Caveats in Software Release 4.3(1)" section on page 24.

This section describes open caveats in CSM software release 4.3(1):

- CSCsj26680

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

  **Workaround**: None.

- CSCsj88014

  A large delay can occur when updating LOAD using KAL-AP. 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.

- CSCsh53633

  A CSM running 4.2(6) had a reboot due to IXP 3. The type of crash was known as a "L7 abort."

  **Workaround**: None.

- CSCei73146

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

  **Workaround**: None.

- CSCeg15173

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

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

- CSCsi85407

  Under a high traffic load, the CSM may halt unexpectedly. The console displays the error message: "P:\ixp1200\core\l7\l7_main.c(395) warning: TX Queue overflow. Shutting down CORE_TX_Q" followed by a core dump.

  **Workaround**: None.

# Resolved Caveats in Software Release 4.3(1)

**Note** For a description of open caveats in CSM software release 4.3(1), see the "Open Caveats in Software Release 4.3(1)" section on page 23.

This section describes resolved caveats in CSM software release 4.3(1):

- CSCsg37513

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

  **Workaround**: None.

- 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.

- CSCsi29132

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

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

- CSCsj75481

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

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

# Troubleshooting

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

## Message Banners

When syslog messages are received, they are preceded by one of the following banners (where # is the slot number of the CSM module):

**Error Message** `CSM_SLB-4-INVALIDID Module # invalid ID`

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

## Server and Gateway Health Monitoring

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

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

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

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

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

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

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

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

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

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

# Diagnostic Messages

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

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

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

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

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

**Explanation** A non-fatal hardware fault was detected.

# Fault Tolerance Messages

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

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

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

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

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

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

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

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

# Regular Expression Errors

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

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

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

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

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

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

# XML Errors

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

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

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

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

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

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

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

# Related Documentation

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

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

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

## Cisco IOS Software Documentation Set

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

# Obtaining Documentation and Submitting a Service Request

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

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

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

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