

Cisco Content Switching Module Software Version 3.1(1) for the Cisco Catalyst 6500 Switch and the Cisco 7600 Internet Router

New Features

New features of the Cisco CSM Software Version 3.1(1) Content Switching Module for the Cisco Catalyst® 6500 Switch and the Cisco 7600 Internet Router include the following:

- *Virtual IP (VIP) connection watermarks*—The VIP connection watermark feature allows the Web-hosting provider to limit the number of connections going through a particular virtual server or set of virtual servers. By using this feature, the network administrator allows a fair distribution of connection resources among all virtual servers. When a virtual server reaches the configured maximum connection limit, no new connections are established to that virtual server until it drops below the connection watermark again. This feature allows Cisco CSM customers to have a shared CSM environment, whether between multiple customers or many departments with an enterprise, without fear that one group will consume all the resources. This feature also can be configured to protect against denial-of-service (DoS) attacks.
- *Backup server farm*—The backup server farm feature allows the administrator to specify one or more backup servers that

will be used when all primary servers in a server farm are unavailable because of health probes or connection thresholds. If configured, when the Cisco CSM receives a connection that matches a policy associated with a server farm in which all the servers are currently down, the CSM load balances this connection to the configured backup server farm. The backup server farm also can be configured to be a Hypertext Transfer Protocol (HTTP) redirect so that clients are redirected to a remote location.

- *Optional port for health probing*—Some of the Cisco CSM supported health probes require that the CSM probe real servers on a specific TCP or User Datagram Protocol (UDP) port. In earlier implementations of Cisco CSM Software, the network administrator cannot explicitly specify a server port when configuring a health probe. Instead, the port is inherited from the virtual servers that are using the server farm with which the probe is associated. This feature allows the administrator to override the real and virtual server port information by explicitly specifying a port to probe in the health probe configuration.



- *IP reassembly*—In Cisco CSM 1.x Software releases, all IP fragments are dropped by the CSM. In Cisco CSM 2.x Software releases, the UDP fragments of a datagram are reassembled as long as the first fragment of the datagram is received by the Cisco CSM before all other fragments. In 3.1(1), the Cisco CSM can handle UDP fragments and assemble them, regardless of the order in which they were received.
- *Toolkit Command Language (TCL) scripting*—To support more flexible health-probing functionality, this feature gives the administrator the ability to upload and execute TCL scripts on the Cisco CSM. The administrator can create a “script probe” that the Cisco CSM periodically executes for each real server in any server farm associated with the probe. Depending upon the exit code of such a script, the real server is considered healthy, suspect, or failed. A wide variety of probing functions are possible using the flexibility of the TCL scripting environment. The Cisco CSM also supports execution of custom TCL scripts that are not directly associated with a particular server health probe. A “standalone script” dynamically executes a task at a specified interval.
- *Extended Markup Language application programming interface (XML API) configuration*—Users can now automate programmatic configuration of the Cisco CSM via a documented XML API. When the network administrator enables this feature, a network management device may connect to the CSM and “push” new configurations to it. The network management device pushes configuration commands to the Cisco CSM using the standard HTTP protocol by sending an XML document in the data portion of an HTTP POST. The full Document Type Definition (DTD) can be found documented in the appendix of the Cisco CSM Installation and Configuration Guide.
- *Simple Network Management Protocol/Management Information Base (SNMP/MIB)*—The Cisco CSM now has full SNMP/MIB support. In this release, the Cisco CSM supports two Read Only MIBs: CISCO-SLB-MIB and CISCO-SLB-EXT-MIB, which are available at <ftp://ftp.cisco.com/pub/mibs/>. Traps can be sent based on real server, virtual server, and fault tolerant state changes.
- *Global server load balancing (GSLB)*—GSLB has increased in popularity as a method for disaster recovery. In this release the Cisco CSM supports GSLB in which the CSM can be configured to act as an authoritative Domain Name System (DNS) server. The Cisco CSM then collects load information from other Cisco CSMs in the network and load balances incoming traffic across these geographically dispersed CSMs.
- *Resource usage display*—A show command has been added to the Cisco CSM that includes multiple parameters for determining how loaded the CSM is at a given moment. The output of this command indicates the CPU usage on each of the processing modules within the Cisco CSM hardware, memory usage, and other related information.
- *HTTP method parsing*—Every HTTP request contains an HTTP method, a URL, and other information such as HTTP headers. This new feature allows the user not only to match HTTP headers, but also to configure policies that match particular HTTP “methods,” such as GET, HEAD, and POST, and to make a load-balancing decision based on this information.
- *Real server names*—The real server configuration on the Cisco CSM now includes assigning an ASCII string name in addition to the current options of IP address and port. This creates a friendlier way to reference real servers, mapping an IP address to a name. It also allows all instances of the real server to be removed from service on a global level with one command, regardless of how many server farms to which a real server belongs.
- *Non-TCP connection state redundancy*—The Cisco CSM currently supports connection state redundancy for TCP protocols. This functionality has been extended to include non-TCP protocols.



- *Reverse sticky*—In a firewall load-balancing environment, this feature allows multiple connections between the same two devices to be stuck to the same firewall based on the IP addresses of the first incoming connection, regardless of the load-balancing algorithm used and regardless of which of the two devices originated the connection. This feature is especially important for firewall load-balancing scenarios where the load balancers on the two sides of the “sandwich” are not both Cisco CSMs. As an example, when using Cisco IOS[®] SLB on one side of the sandwich and the Cisco CSM on the other, the hash algorithms are not the same; therefore, new connections originated by the receiving device might not be load balanced to the same firewall from which the first connection was received. With the Cisco CSM reverse sticky feature configured, the receiving Cisco CSM sets up a sticky entry for connections opened in the opposite direction. This way, after the first connection between two specific devices has been set up on the two Cisco CSMs in the firewall load-balancing sandwich, all subsequent connections are load balanced to the same firewall, regardless of which of the two devices originates them.
- *Unidirectional idle timeout*—This feature allows the user to configure unidirectional timers for specific virtual servers; for flows matching those virtual servers, the Cisco CSM monitors only one direction of the flow. This feature is particularly useful in UDP streaming environments, where unidirectional flows are common and long idle timers are not optimal; unidirectional timers for this kind of flows allow the Cisco CSM to ignore the silent direction of the flow and time out the flow based on only the other direction.
- *SSL service module ID*—The Cisco CSM now has a configurable sticky option that allows the CSM to continue to provide stickiness based on Secure Sockets Layer (SSL) ID, even during SSL ID renegotiation when the Cisco CSM is paired with the SSL Services Module for the Cisco Catalyst 6500. Though the renegotiation process is encrypted, usually making it impossible to use SSL ID effectively for stickiness, the Cisco CSM is able to work in conjunction with the Cisco SSL Services Module, when this feature is configured. This ensures that the stickiness is not broken, even if a SSL ID renegotiation occurs. The result is that the same SSL Service Module is always selected for the same client.



Orderable Product Numbers

Table 1 gives part numbers for ordering Cisco CSM Software.

Table 1 Cisco CSM Part Numbers

Cisco CSM Software Version	Hardware Part Number	Software Part Number	Hardware Requirements	Native Cisco IOS Software Release	Added Features
3.1(1)	WS-X6066-SLB-APC	SC6k-3.1.1-CSM	Supervisor IA with Multilayer Switch Feature Card (MSFC) and Policy Feature Card (PFC) or Supervisor II with MSFC 2	12.1(13)E	<ul style="list-style-type: none"> • VIP connection watermarks • Backup serverfarm • Optional port for probing • IP reassembly • Scriptable health checks • XML API for configuration • SNMP/MIB support • GSLB • Resource usage display • HTTP method parsing • Real server names • Non-TCP connection state redundancy • Reverse IP sticky • SSL services module ID • Unidirectional idle timeout
2.1(4)	WS-X6066-SLB-APC	SC6k-2.1.4-CSM	Supervisor IA with MSFC and PFC or Supervisor II with MSFC 2	12.1(8)EX	<ul style="list-style-type: none"> • Firewall load balancing • Non-TCP load balancing • URL hashing • HTTP 1.1 persistence • Full stateful failover • Generic header parsing • SNMP server health traps • Multiple Cisco CSMs in a chassis • Virtual private network/IP Security (VPN/IPSec) load balancing
2.2(4)	WS-X6066-SLB-APC	SC6k-2.2.4-CSM	Supervisor IA with MSFC and PFC or Supervisor II with MSFC 2	12.1(11)E	<ul style="list-style-type: none"> • Increased VLAN limit • Return code checking • Inband health monitoring • Configuration pending timeout value • Real-Time Streaming Protocol (RTSP) support

Further Information

Download the software release at:

<http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-csm>

Cisco CSM Data Sheet:

http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09186a00800887f3.html

Cisco CSM Installation and Configuration Guide:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html

Software Version 3.1(1) Release Notes:

http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_note09186a00800fe64c.html

Marketing Contacts

Cisco CSM alias, ask-csm-pm@cisco.com

Dyan Gray, Product Manager, dpgray@cisco.com

Stefano Testa, Technical Marketing Engineer, testas@cisco.com



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.
(0402R) 204064_ETMG_WH_05.04