



Release Notes for Catalyst 6500 Series Switch Content Switching Module with SSL Software Release 1.1(3)

Current Release—January 28, 2005

This publication describes the features, modifications, and caveats for the Catalyst 6500 series Content Switching Module with SSL (CSM-S) software release 1.1(3) operating on a Catalyst 6500 series switch with a Supervisor Engine 2 with MSFC2 and Cisco IOS Release 12.2(18)SXD or higher or with a Supervisor Engine 720 and Cisco IOS Release 12.2(18)SXE or higher.



Note

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

Contents

- [System Requirements, page 2](#)
- [Limitations and Restrictions, page 8](#)
- [Caveats, page 9](#)
- [Related Documentation, page 23](#)
- [Obtaining Documentation, page 24](#)
- [Documentation Feedback, page 25](#)
- [Obtaining Technical Assistance, page 26](#)
- [Obtaining Additional Publications and Information, page 28](#)



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

Copyright © 2003–2005 Cisco Systems, Inc. All rights reserved.

System Requirements

This section describes the system requirements for the Catalyst 6500 series CSM-S software release 1.1(3).

Memory Requirements

The minimum recommended memory for a Supervisor Engine in a chassis with a CSM-S is 256MB of DRAM. Please consult the Cisco Feature Navigator (<http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>) for specific requirements.

Hardware Supported

Before you can use the Catalyst 6500 series CSM-S, you must have a Supervisor Engine 2 with an MSFC2 or a Supervisor Engine 720 and any module that has ports to connect server and client networks.



Caution

The WS-X6066-SLB-S-K9 CSM-S are not fabric enabled, but the module can operate in a fabric-enabled chassis like any other nonfabric module.

Product Number	Minimum Cisco IOS Software	Recommended Cisco IOS Software	Recommended Catalyst Operating System Software
Content Switching Module			
Supervisor Engine 2 with MSFC2	12.2(18)SXD	12.2(18)SXD and higher.	Not applicable
Supervisor Engine 720.	12.2(18)SXE	12.2(18)SXE and higher.	Not applicable.
Console Cable			
72-876-01		Not applicable	
Accessory Kit			
800-05097-01		Not applicable	

Software Requirements



Caution

The CSM-S release is not supported by the Catalyst operating system software.

Table 1 lists the software releases for the CSM-S:

Table 1 CSM-S Software Requirements

CSM-S Software	Software Part Number	Hardware	Catalyst Operating System Software	Cisco IOS Software
1.1(3)	SC6K-1.1-CSM-S	WS-X6066-SLB-S-K9	Not Applicable	Cisco IOS software Release 12.2(18)SXD and higher on the Supervisor Engine 2 with MSFC2 or Cisco IOS software Release 12.2(18)SXE on the Supervisor Engine 720
1.1(2)	SC6K-1.1-CSM-S	WS-X6066-SLB-S-K9	Not Applicable	Cisco IOS software Release 12.2(18)SXD and higher
1.1(1)	SC6K-1.1-CSM-S	WS-X6066-SLB-S-K9	Not Applicable	Cisco IOS software Release 12.2(18)SXD and higher

Software Compatibility

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

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

Table 2 and Table 3 lists the CSM-S software release compatibility.

Table 2 Cisco IOS Software on the Supervisor Engine and MSFC

CSM-S Software	Cisco IOS Software
1.1(3)	Cisco IOS software Release 12.2(18)SXD and higher on the Supervisor Engine 2 with MSFC2 or Cisco IOS software Release 12.2(18)SXE on the Supervisor Engine 720 for the features new to CSM-S release 1.1(3).
1.1(2)	12.2(18)SXD or higher for the features new to CSM-S release 1.1(2).
1.1(1)	12.2(18)SXD or higher for the features new to CSM-S release 1.1(1).

Table 3 Catalyst Operating System Software on the Supervisor Engine and Cisco IOS Software on the MSFC

CSM-S Software	Catalyst Operating System Software
1.1(3)	The CSM-S is currently not supported by the Catalyst operating system software.
1.1(2)	The CSM-S is currently not supported by the Catalyst operating system software.
1.1(1)	The CSM-S is currently not supported by the Catalyst operating system software.

Software Release 1.1(3) Features

This software release contains feature sets supporting SSL (CSM-S) and functionality from previous CSM releases. The tables in this section list these feature sets.

[Table 4](#) lists the CSM features available in this release and previous releases.

Table 4 CSM Feature Set Description

Features
Supported Hardware
Supervisor 2 with MSFC2 with Cisco IOS software Release 12.2(18)SXD and higher
Supervisor Engine 720 Cisco IOS software Release 12.2(18)SXE and higher
Supported Protocols
TCP load balancing
UDP generic IP protocol load balancing
Special application-layer support for FTP and the Real Time Streaming Protocol (RTSP). The RTSP service on the CSM only supports a maximum of 4 simultaneous child (data) sessions.
Layer 7 Functionality
Full regular expression matching
URL, cookie switching, Generic HTTP header parsing, HTTP method parsing
Miscellaneous Functionality
VIP connection watermarks
Backup (sorry server) and server farm
Optional port for health probes
IP reassembly
TCL (Toolkit Command Language) scripting
XML configuration interface
SNMP
GSLB (Global Server Load Balancing)—requires a license
Resource usage display
Configurable idle and pending connection timeout
Idle timeout for unidirectional flows
SSL Services Module (SSLM) integration for SSL load balancing
Real server names
TCP connection redundancy for all types of flows (TCP, UDP, and IP)
Fault tolerant show command enhancements
Cisco IOS SLB FWLB interoperation (IP reverse-sticky)
Multiple CSMs in a chassis
CSM and Cisco IOS-SLB functioning simultaneously in a chassis

Table 4 CSM Feature Set Description (continued)

Features
Configurable HTTP 1.1 persistence (either all GETs are made to the same server or are balanced to multiple servers)
Fully configurable NAT
Server-initiated connections
Route health injection
Load-balancing Algorithms
Round-robin
Weighted round-robin (WRR)
Least connections
Weighted least connections
URL hashing
Source IP hashing (configurable mask)
Destination IP hashing (configurable mask)
Source and destination IP hashing (configurable mask)
Load Balancing Supported
Server load balancing (TCP, UDP, or generic IP protocols)
Firewall load balancing
DNS load balancing
Stealth firewall load balancing
Transparent cache redirection
Reverse proxy cache
SSL off-loading
VPN-IPSec load balancing
Generic IP devices and protocols
Stickiness
Cookie sticky with configurable offset and length
SSL ID
Source IP (configurable mask)
HTTP redirection
Redundancy
Sticky state
Full stateful failover (connection redundancy)
Health Checking
HTTP
ICMP
Telnet
TCP

Table 4 CSM Feature Set Description (continued)

Features
FTP
SMTP
DNS
Return error-code checking
Inband health checking
User-defined TCL scripts
Management
SNMP traps
Full SNMP and MIB support
XML interface for remote CSM configuration
Back-end encryption support.
Workgroup Manager Support
Server Application State Protocol (SASP)

Table 5 lists the CSM-S features in this release.

Table 5 CSM-S Feature Set Description

Features
Supported Hardware
Supervisor Engine 2 with MSFC2
Supervisor Engine 720
Supported Software
<ul style="list-style-type: none"> • Cisco IOS software Release 12.2(18)SXD with the Supervisor Engine 2 • Cisco IOS software Release 12.2(18)SXE and higher with Supervisor Engine 720
SSL Features
SSL initiation
SSL version 2.0 forwarding
URL rewrite
HTTP header insertion
Wildcard proxy
Handshake Protocol
SSL 3.0
SSL 3.1/TLS 1.0
SSL 2.0 (only ClientHello support)
Session reuse
Session renegotiation
Session timeout

Table 5 CSM-S Feature Set Description (continued)

Features
Symmetric Algorithms
ARC4
DES
3DES
Asymmetric Algorithms
RSA
Hash Algorithms
MD5
SHA1
Cipher Suites
SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_WITH_DES_CBC_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA
Public Key Infrastructure
RSA key pair generation for certificates up to 2048-bit
Secure key storage in CSM-S flash memory device
Certificate enrollment for client and server-type proxy services
Importing and exporting of key and certificate (PKCS12 and PEM)
Duplicating keys and certificates on standby CSM-S using the key and certificate import and export mechanism
Manual key archival, recovery, and backup
Key and certificate renewal using the CLI
Graceful rollover of expiring keys and certificates
Auto-enrollment and auto-renewal of certificates
Importing of certificate authority certificates by cut-and-paste or TFTP
Up to 8 levels of certificate authority in a certificate chain
Generating of self-signed certificate
Manual certificate enrollment using cut-and-paste or TFTP of PKCS10 CSR file
Peer (client and server) certificate authentication
Peer (client and server) certificates
Certificate security attribute-based access control lists
Certificate revocation lists (CRL)
Certificate expiration warning
TCP Termination
RFC 1323
Connection aging

Table 5 CSM-S Feature Set Description (continued)

Features
Connection rate
NAT¹/PAT²
Client and server
Redundancy
When the CSM-S module is in the standby state, you cannot access SSL services.
To have redundancy, you must use either two CSMs or two CSM-S. You cannot mix a CSM and a CSM-S for a supported redundancy configuration.
High Availability
Failure detection (SLB health monitoring schemes)
Module-level redundancy (stateless)
Serviceability
Password recovery
Statistics and Accounting
Total SSL connections attempt per proxy service
Total SSL connections successfully established per proxy service
Total SSL connections failed per proxy service
Total SSL alert errors per proxy service
Total SSL resumed sessions per proxy service
Total encrypted/decrypted packets/bytes per proxy service
Statistics displayed at 1 second, 1 minute, and 5 minutes traffic rate for CPU utilization and SSL-specific counters

1. NAT = Network Address Translation
2. PAT = Port Address Translation

Limitations and Restrictions

- 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.
- 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-S 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-S 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-S 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-S simply ignores any configured probes requiring ports to that real server.

- When configuring CSM-S for fault tolerance, we recommend that you configure a dedicated link for the fault-tolerant VLAN.



Note Configuring stateful redundancy with the CSM-S in separate chassis requires a gigabit link between the CSM-S.

Caveats

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

- [Open Caveats in Software Release 1.1\(3\) for CSM, page 9](#)
- [Resolved Caveats in Software Release 1.1\(3\) for CSM, page 12](#)
- [Open Caveats in Software Release 1.1\(2\) for CSM, page 12](#)
- [Resolved Caveats in Software Release 1.1\(2\) for CSM, page 15](#)
- [Open Caveats in Software Release 1.1\(2\) for SSL, page 17](#)
- [Resolved Caveats in Software Release 1.1\(2\) for SSL, page 20](#)
- [Open Caveats in Software Release 1.1\(1\), page 21](#)
- [Resolved Caveats in Software Release 1.1\(1\), page 23](#)

Open Caveats in Software Release 1.1(3) for CSM



Note

For a description of caveats resolved in CSM-S software release 1.1(3), see the [“Resolved Caveats in Software Release 1.1\(3\) for CSM”](#) section on page 12.

This section describes known limitations that exist in CSM-S software release 1.1(3).

- CSCeg35110

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

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

- CSCef09179

Resetting the CSM-S can cause these messages to appear on the supervisor console:

```
%EARL-SP-STDBY-4-BUS_CONNECTION:Interrupt FM_CRC16_ERR occurring in EARL bus
connection.
%EARL-SP-STDBY-4-BUS_CONNECTION:Interrupt HD_CRC_ERR occurring in EARL bus connection.
%EARL-SP-STDBY-4-BUS_CONNECTION: Interrupt ENCAP_ERR occurring in EARL bus connection.
```

This situation happens only when there is a non-fabric enabled module in the chassis. The CSM-S is a non-fabric enabled module.

Workaround: None.

- CSCef02629

During a supervisor engine switch over, the standby CSM-S fails to initialize and the new standby supervisor engine prints the following message for all CSM-S ports:

```
%PM-STDBY-4-INT_FAILUP:GigabitEthernet7/2 failed to come up.No internal VLAN available
```

Workaround: None.

- CSCee92560

If more than one CSM-S in a chassis is reset through the **hw-reset** command, one of the modules may fail to reboot the first time. This failure may be caused by the supervisor engine timeout value for a module to reset itself. In these cases, the module must be either power-cycled or reset a second time.

Workaround: If the module does not boot after a reset, use the **hw-reset** command to restart the module or power cycle the switch.

- CSCee91798

In a CSM-S fault tolerant configuration, it is possible for a failover to occur between the CSM-S fault-tolerant pair. However, failover may not occur if the SSL daughter card fails. When the SSL daughter card failure is detected, the SSL daughter card is restarted causing all SSL flows to fail, and they will need to be re-established.

Workaround: None.

- CSCee81437

The CSM-S module may stop responding to the supervisor engine keep-alive polling. When this situation occurs, the supervisor power cycles the module to restart it. After restarting, the module operates correctly.

Workaround: None.

- CSCee57427

As of software Release 12.2(18)SXD the CSM-S needed identifiers assigned in the MIBs, for example:

```
CISCO-ENTITY-VENDORTYPE-OID-MIB.my & OLD-CISCO-CHASSIS-MIB.my
```

This situation causes incorrect values to show up through SNMP. New identifier assignments have been made in the MIBs and are available in the 12.2(18)SXD release as follows:

```
CISCO-ENTITY-VENDORTYPE-OID-MIB.my:
csm-ssl(442) -- CSM-S is a content switching module with integrated SSL acceleration

OLD-CISCO-CHASSIS-MIB.my:
cevChassisCSMssl OBJECT IDENTIFIER ::= { cevChassis 479 }
-- CSM-S is a content switching module with integrated SSL acceleration
```

Workaround: None.

- CSCee33514

When the module boots, you may see messages on the CSM-S console, as follows:

```
SCP:Rcvd an Unknown Opcode 0x3e...
SCP:Rcvd an Unknown Opcode 0x3e...
SCP:Subcommand: COMMAND_MODULE_ONLINE
Module has become online.
SCP: SCP_SET_GET_LTL Subcmd 0x9 Unsupported
SCP: SCP_SET_GET_LTL Subcmd 0x9 Unsupported
```

Workaround: None. There is no operational impact to these messages. They can be safely ignored.

- CSCee26687

CSM-S does not allow static ARP for the SSL daughter card interface.

Workaround: None.

- CSCee18203

Thrashing syslog messages may appear under heavy certificate authenticated SSL traffic and the SSL Cisco IOS console may become unresponsive. The heavy traffic is for an SSL proxy-service that has certificate authentication turned on. For example:

```
ssl-proxy(config-ssl-proxy)# authenticate verify { signature-only | all }
```

The more traffic, the more unresponsive the console becomes. At very high traffic loads the following syslog may appear:

```
*Apr 1 22:39:13.071: %SCHED-3-THRASHING: Process thrashing on
watched boolean 'CSM IOS Watch Bool'.
-Process= "CSM IOS I/O Process", ipl= 5, pid= 27
-Traceback= 5233E8 5234CC 5C6044
```

Workaround: None.

- CSCec28396

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

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

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

Resolved Caveats in Software Release 1.1(3) for CSM



Note

For a description of caveats open in CSM-S software release 1.1(3), see the [“Open Caveats in Software Release 1.1\(3\) for CSM”](#) section on page 9.

This section describes the caveats resolved in CSM-S software release 1.1(3).

- CSCsa52051

The **show ssl-proxy version** command incorrectly displays the SSL version number as 2.1(2) as shown in this example:

```
show ssl-proxy version
Cisco Internetwork Operating System Software
IOS (tm) SVCSSL Software (SVCSSL-K9Y9-M), Version 12.2(14.6)SH2(0.19)  INTERIM TEST
SOFTWARE
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 05-Jan-05 10:03 by integ
Image text-base: 0x00400078, data-base: 0x00B06000

ROM: System Bootstrap, Version 12.2(15)YS1 RELEASE SOFTWARE

shakira uptime is 14 hours, 47 minutes
System returned to ROM by power-on
System image file is "tftp://255.255.255.255/unknown"
AP Version 2.1(0.19) 4.2(0.20) 2.1(2)
```

The last value should be "2.1(3)."

Workaround: None.

Open Caveats in Software Release 1.1(2) for CSM



Note

For a description of caveats resolved in CSM-S software release 1.1(2), see the [“Resolved Caveats in Software Release 1.1\(2\) for CSM”](#) section on page 15.

This section describes known limitations that exist in CSM-S software release 1.1(2).

- CSCeg35110

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

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

- CSCef09179

Resetting the CSM-S can cause these messages to appear on the supervisor console:

```
%EARL-SP-STDBY-4-BUS_CONNECTION:Interrupt FM_CRC16_ERR occurring in EARL bus
connection.
%EARL-SP-STDBY-4-BUS_CONNECTION:Interrupt HD_CRC_ERR occurring in EARL bus connection.
%EARL-SP-STDBY-4-BUS_CONNECTION: Interrupt ENCAP_ERR occurring in EARL bus connection.
```

This situation happens only when there is a non-fabric enabled module in the chassis. The CSM-S is a non-fabric enabled module.

Workaround: None.

- CSCef02629

During a supervisor engine switch over, the standby CSM-S fails to initialize and the new standby supervisor engine prints the following message for all CSM-S ports:

```
%PM-STDBY-4-INT_FAILUP:GigabitEthernet7/2 failed to come up.No internal VLAN available
```

Workaround: None.

- CSCee92560

If more than one CSM-S in a chassis is reset through the **hw-reset** command, one of the modules may fail to reboot the first time. This failure may be caused by the supervisor engine timeout value for a module to reset itself. In these cases, the module must be either power-cycled or reset a second time.

Workaround: If the module does not boot after a reset, use the **hw-reset** command to restart the module or power cycle the switch.

- CSCee91798

In a CSM-S fault tolerant configuration, it is possible for a failover to occur between the CSM-S fault-tolerant pair. However, failover may not occur if the SSL daughter card fails. When the SSL daughter card failure is detected, the SSL daughter card is restarted causing all SSL flows to fail, and they will need to be re-established.

Workaround: None.

- CSCee81437

The CSM-S module may stop responding to the supervisor engine keep-alive polling. When this situation occurs, the supervisor power cycles the module to restart it. After restarting, the module operates correctly.

Workaround: None.

- CSCee57427

As of software Release 12.2(18)SXD the CSM-S needed identifiers assigned in the MIBs, for example:

```
CISCO-ENTITY-VENDORTYPE-OID-MIB.my & OLD-CISCO-CHASSIS-MIB.my
```

This situation causes incorrect values to show up through SNMP. New identifier assignments have been made in the MIBs and are available in the 12.2(18)SXD release as follows:

```
CISCO-ENTITY-VENDORTYPE-OID-MIB.my:
csm-ssl(442) -- CSM-S is a content switching module with integrated SSL acceleration
```

```
OLD-CISCO-CHASSIS-MIB.my:
cevChassisCSMssl OBJECT IDENTIFIER ::= { cevChassis 479 }
-- CSM-S is a content switching module with integrated SSL acceleration
```

Workaround: None.

- CSCee33514

When the module boots, you may see messages on the CSM-S console, as follows:

```
SCP:Rcvd an Unknown Opcode 0x3e...
SCP:Rcvd an Unknown Opcode 0x3e...
SCP:Subcommand: COMMAND_MODULE_ONLINE
Module has become online.
SCP: SCP_SET_GET_LTL Subcmd 0x9 Unsupported
SCP: SCP_SET_GET_LTL Subcmd 0x9 Unsupported
```

Workaround: None. There is no operational impact to these messages. They can be safely ignored.

- CSCee26687

CSM-S does not allow static ARP for the SSL daughter card interface.

Workaround: None.

- CSCee18203

Thrashing syslog messages may appear under heavy certificate authenticated SSL traffic and the SSL Cisco IOS console may become unresponsive. The heavy traffic is for an SSL proxy-service that has certificate authentication turned on. For example:

```
ssl-proxy(config-ssl-proxy)# authenticate verify { signature-only | all }
```

The more traffic, the more unresponsive the console becomes. At very high traffic loads the following syslog may appear:

```
*Apr 1 22:39:13.071: %SCHED-3-THRASHING: Process thrashing on
watched boolean 'CSM IOS Watch Bool'.
-Process= "CSM IOS I/O Process", ipl= 5, pid= 27
-Traceback= 5233E8 5234CC 5C6044
```

Workaround: None.

- CSCec28396

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

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

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

Resolved Caveats in Software Release 1.1(2) for CSM



Note

For a description of caveats open in CSM-S software release 1.1(2), see the [“Open Caveats in Software Release 1.1\(2\) for CSM” section on page 12](#).

This section describes the caveats resolved in CSM-S software release 1.1(2).

CSCeg38830

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

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

- CSCeg31247

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

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

- CSCeg17294

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

Workaround: None.
- CSCeg07844

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

Workaround: None.
- CSCef95806

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

Workaround: None.
- CSCef82282

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

Workaround: None.
- CSCef66494

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

 - a. The server response contains multiple packets.
 - b. The last packet contains the HTTP body instead of HTTP header.
 - c. The last packet contains a blank line (sequence of CR, LF, CR, LF characters).
 - d. The server also sent the FIN immediately right after the last packet.

Workaround: None.
- CSCef27321

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

Workaround: Remove the destination port configured on the real server.
- CSCee74402

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

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

Open Caveats in Software Release 1.1(2) for SSL



Note

For a description of caveats resolved in CSM-S software release 1.1(2), see the [“Resolved Caveats in Software Release 1.1\(2\) for SSL” section on page 20](#).

This section describes known limitations that exist in CSM-S software release 1.1(2) for SSL.

- CSCin67360

The SSL Services Module does not support client certificate insertion for SSL client proxy service. If you apply an HTTP header policy to a client proxy service, and configure the HTTP header policy with client certificate insertion and other headers, error messages are displayed and the configuration is not accepted.

Output from the **show running-config** command and the **show ssl-proxy service service_name** command does not show that the HTTP header policy is attached to the client proxy service; however, the SSL Services Module continues to insert the other configured HTTP headers (other than client certificate headers) in the request.

Workaround: Save the configuration and reset the SSL Services Module.

- CSCee69321

When you configure trust points for manual or TFTP enrollment and enter the **crypto ca certificate query** command, the router loses certificates after it is reloaded.

Workaround: Do not enter the **crypto ca certificate query** command if you configure any of the trust points for manual or TFTP enrollment.

- CSCed53976

The SSL Services Module with a virtual TCP policy configured with a low TCP maximum segment size (MSS) value (for example, 256), and with the default SYN timeout on the server side, might experience a software-forced reset due to exhausted resources if the following events occur simultaneously:

- The real server is unreachable.
- There is a burst of approximately 26,000 TCP SYN requests to establish a client connection.
- All connections enter ESTABLISHED state in TCP before the HTTP requests are sent on any of the connections.
- The HTTP requests are more than three times the size of the negotiated MSS value.

Workaround: Do one of the following:

- Stabilize the real server so that it is reachable.
- If the SSL Services Module is used with a Content Switching Module (CSM), enable the health probe for a real server on the CSM.

- CSCed33492

If you add a trailing “/” to the *url* value in the **enrollment url url** command for a trustpoint, the SSL Services Module sends the following GET request during certificate authority authentication:

```
GET //pkiclient.exe?operation=GetCACert&message=t1 HTTP/1.0
```

The pkiclient.exe file is usually located in the /cgi-bin/ directory of the certificate authority server.

Workaround: Do not enter a trailing “/” to the *url* value in the **enrollment url url** command for a trustpoint.

- CSCed14070

When you import a certificate from a PKCS12 or PEM file or when you manually input a certificate authority certificate to the module, and the certificate contains an invalid extension, the SSL peer might reject the certificate.

Workaround: Make sure that the certificate has the correct extension (for example, basic constraint) before importing it to the module.
- CSCec82360

If multiple certificate authority certificates in the database have the same subject name, the certificate chain might contain the wrong certificate authority certificate. If the SSL Services Module is configured as an SSL server, it will send the wrong certificate authority certificate in the chain to the client, which could result in authentication and handshake failures.

Workaround: When a certificate authority has renewed its certificate, make sure that you renew all the SSL certificates issued by this certificate authority. Delete the old certificate authority certificate from the database to avoid this problem.
- CSCec74017

The SSL Services Module does not rewrite the URL if the HTTP header that specifies the relocation string spans more than one TCP segment.

Workaround: None.
- CSCec46997

If you configure a URL rewrite rule, and a server redirects a client to a website that does not have a trailing “/” in the URL, the SSL Services Module does not rewrite the URL.

Workaround: Configure the server to add a trailing “/” to the relocation string.
- CSCec19596

Automatic enrollment might not work correctly if the router does not have a hardware clock (calendar) or if you have not configured a network time protocol (NTP) server.

Workaround 1: Remove the auto-enroll configuration, and then reconfigure auto-enroll to reset the clock manually.

Workaround 2: Reset the enrollment timer by doing the following:

 - a. Copy the “crypto ca trustpoint *trustpoint_label*” and “crypto ca certificate chain *name*” information from the running configuration.
 - b. Delete the trustpoint by entering the **no crypto ca trustpoint *trustpoint_label*** command.
 - c. Paste the trustpoint and certificate chain information to the configuration.
- CSCea57072

The Cisco IOS PKI system does not validate the issuer when using manual enrollment. As a result, a certificate chain may have a root certificate belonging to one certificate authority and a router certificate issued by another certificate authority.

Workaround: None.
- CSCea53069

Windows 2000 certificate authorities occasionally reject certificate enrollment requests issued by the SSL Services Module. The problem originated with the SCEP DLL, and is fixed on the .net version of the certificate authority, but not on the Windows 2000 version.

Workaround: Restart the certificate authority, and issue the enrollment request again.

- CSCea50887
There is no help string for the **test crypto pki self** command, and the generated self-signed certificate is not displayed by the **show crypto ca certificate** command.
Workaround: None.
- CSCea48145
Importing a self-signed certificate with the key pair of the issuer is not supported by the Cisco IOS PKI system.
Workaround: None.
- CSCea32058
For manual certificate enrollment, if the URL string ends with a backslash (/) after the TFTP server name or address (for example, tftp://ipaddress/), the system tries to open a file named “.ca” from the TFTP server.
Workaround: Specify the filename in the URL.
- CSCdz63758
Cutting and pasting the hexadecimal values of a certificate into the configuration from the terminal can cause the data entry to fail.
Workaround: Copy the configuration file to the running-configuration, or import the certificate with the key pair using a PKCS#12 file.
- CSCdz20220
If you import a key pair and a self-signed certificate from a PKCS#12 file to a trustpoint and assign the certificate to a proxy service, installation of the certificate fails after rebooting the system, and the proxy service remains in the “no cert” state.
Workaround: After rebooting, delete the trustpoint and import the PKCS#12 file again. The proxy service automatically reinstalls the self-signed certificate.
- CSCdz03802
When query mode is configured and there are multiple trust points using the same certificate authority URL, only one of these trust points succeeds in obtaining the whole certificate chain after a Cisco IOS reboot.
Workaround: Manually authenticate and enroll these trust points after the failure. Turn off query mode, and save the certificates in the NVRAM.
- CSCdy85233
Exporting a PKCS#12 file using FTP can take up to 20 minutes if a file with the same name exists on the remote host.
Workaround: None.
- CSCdy77843
If you enter the **clear arp** command on the SSL Services Module, all the proxy services go into a “down” state and then go into an “up” state.
Workaround: None.
- CSCdy61618
Syslog messages indicating that proxy services are in the UP state may not be printed for all the services configured in the system while booting.
Workaround: None.

- CSCdy56573
The module might take longer to boot up if there are client NAT pools in the startup-configuration. The delay is proportional to the number of NAT pools in the configuration. With the maximum supported number of NAT pools (64), the delay is up to 4 minutes.
Workaround: None.
- CSCdy46075
When query mode is configured, entering the **no crypto ca certificate query** command on the running configuration does not stop the periodic polling for certificates.
Workaround: None.
- CSCdy43112
When certificate query mode is configured, an “invalid input” message may be displayed on the console following a fingerprint. This message is displayed when a certificate is read from NVRAM on Cisco IOS reboot and does not indicate a real error condition.
Workaround: None.

Resolved Caveats in Software Release 1.1(2) for SSL



Note

For a description of caveats open in CSM-S software release 1.1(2), see the [“Open Caveats in Software Release 1.1\(2\) for SSL” section on page 17](#).

This section describes the caveats resolved in CSM-S software release 1.1(2) for SSL.

- CSCef64660
An HTTP POST request from a client using a Mozilla-based browser does not contain the end-of-header marker (\r\n\r\n) in the first buffer of the request. The SSL Services Module is unable to insert the header.
Workaround: None.
This problem is resolved in SSL software release 2.1(3).
- CSCef45069
The URL rewrite feature rewrites the protocol and the nondefault port (default ports are port 80 for cleartext and port 443 for SSL). However, if a server sends a location URL that specifies the default cleartext port (for example, http://www.cisco.com:80), the SSL Services Module incorrectly rewrites the protocol as https://www.cisco.com:80. Also, if a server sends a location URL that specifies the default SSL port (for example, https://www.cisco.com:443), the SSL Services Module incorrectly rewrites the protocol as http://www.cisco.com:443. Secure HTTP (https://) cannot use port 80, and HTTP (http://) cannot use port 443.
Workaround: Specify a different (nondefault) port on the server (for example, 81 or 444).
This problem is resolved in SSL software release 2.1(3).
- CSCef30438
When you configure an HTTP header policy, the SSL Services Module might truncate or corrupt HTTP POST variables in the decrypted traffic.
Workaround: Remove the HTTP header policy from the SSL proxy service.
This problem is resolved in SSL software release 2.1(3).

- CSCee78711

When you enter the **crypto ca import** command to import a certificate and a private key, and the public key in the certificate does not match the private key, the SSL Services Module allows the import process to succeed. When the public key and private key do not match, the SSL Services Module should report an error and the import process should fail.

Workaround: Locate the matching private key and certificate. Remove the mismatched trustpoint and reimport the matching key and certificate.

This problem is resolved in SSL software release 2.1(3).

- CSCee74850

The certificate revocation list (CRL) lookup fails during certificate authentication when a peer certificate is signed by a subordinate certificate authority and when the SSL Services Module receives only a peer certificate or a partial certificate chain. The following debug message displays if you enter the **debug crypto pki transactions** command:

```
CRYPTO_PKI: status = 1872: failed to verify CRL signature
```

Workaround 1: When declaring the trustpoint, enter the **crl optional** command option for all relevant subordinate certificate authority and root certificate authority.

Workaround 2: Ensure that the peer application sends the full certificate chain.

Workaround 3: Ensure that the peer certificate is signed by the root certificate authority.

This problem is resolved in SSL software release 2.1(3).

- CSCed75777

The output of the **show tech** command does not include system crash information or SSL proxy service information.

Workaround: None.

This problem is resolved in SSL software release 2.1(3).

- CSCea69469

After you successfully export a trustpoint in PEM format, no information is displayed regarding the status of the exported PEM file.

This problem is resolved in SSL software release 2.1(3).

Open Caveats in Software Release 1.1(1)



Note

For a description of caveats resolved in CSM-S software release 1.1(1), see the [“Resolved Caveats in Software Release 1.1\(1\)”](#) section on page 23.

This section describes known limitations that exist in CSM-S software release 1.1(1).

- CSCeg01622

After running a sustained traffic load with the client requesting and receiving pages that are 65535 or more bytes, there is reduced performance over time. Performance over time drops approximately 30 percent. This behavior has not been seen with page sizes less than 63353 bytes.

Workaround: None.

- CSCef02629

During a supervisor engine switch over, the standby CSM-S fails to initialize and the new standby supervisor engine prints the following message for all CSM-S ports:

```
%PM-STDBY-4-INT_FAILUP:GigabitEthernet7/2 failed to come up.No internal VLAN available
```

Workaround: None.

- CSCee92560

If more than one CSM-S in a chassis is reset through the **hw-reset** command, one of the modules may fail to reboot the first time. This failure may be caused by the supervisor engine timeout value for a module to reset itself. In these cases, the module must be either power-cycled or reset a second time.

Workaround: If the module does not boot after a reset, use the **hw-reset** command to restart the module or power cycle the switch.

- CSCee91798

In a CSM-S fault tolerant configuration, it is possible for a failover to occur between the CSM-S fault-tolerant pair. However, failover may not occur if the SSL daughter card fails. When the SSL daughter card failure is detected, the SSL daughter card is restarted causing all SSL flows to fail, and they will need to be re-established.

Workaround: None.

- CSCee81437

The CSM-S module may stop responding to the supervisor engine keep-alive polling. When this situation occurs, the supervisor power cycles the module to restart it. After restarting, the module operates correctly.

Workaround: None.

- CSCee57427

As of software Release 12.2(18)SXD, identifiers were assigned for the CSM-S in the MIBs. For example:

```
CISCO-ENTITY-VENDORTYPE-OID-MIB.my & OLD-CISCO-CHASSIS-MIB.my
```

This situation causes incorrect values to show up through SNMP. New identifier assignments have been made in the MIBs and are available in the 12.2(18)SXD release as follows:

```
CISCO-ENTITY-VENDORTYPE-OID-MIB.my:
csm-ssl(442) -- CSM-S is a content switching module with integrated SSL acceleration
```

```
OLD-CISCO-CHASSIS-MIB.my:
cevChassisCSMssl OBJECT IDENTIFIER ::= { cevChassis 479 }
-- CSM-S is a content switching module with integrated SSL acceleration
```

Workaround: None.

- CSCee33514

When the module boots, you may see messages on the CSM-S console, as follows:

```
SCP:Rcvd an Unknown Opcode 0x3e...
SCP:Rcvd an Unknown Opcode 0x3e...
SCP:Subcommand: COMMAND_MODULE_ONLINE
Module has become online.
SCP: SCP_SET_GET_LTL Subcmd 0x9 Unsupported
SCP: SCP_SET_GET_LTL Subcmd 0x9 Unsupported
```

Workaround: None. There is no operational impact to these messages. They can be safely ignored.

- CSCee26687

CSM-S does not allow static ARP for the SSL daughter card interface.

Workaround: None.

- CSCee18203

Thrashing syslog messages may appear under heavy certificate authenticated SSL traffic and the SSL Cisco IOS console may become unresponsive. The heavy traffic is for an SSL proxy-service that has certificate authentication turned on. For example:

```
ssl-proxy(config-ssl-proxy)# authenticate verify { signature-only | all }
```

The more traffic, the more unresponsive the console becomes. At very high traffic loads the following syslog may appear:

```
*Apr 1 22:39:13.071: %SCHED-3-THRASHING: Process thrashing on
watched boolean 'CSM IOS Watch Bool'.
-Process= "CSM IOS I/O Process", ipl= 5, pid= 27
-Traceback= 5233E8 5234CC 5C6044
```

Workaround: None.

Resolved Caveats in Software Release 1.1(1)



Note

For a description of caveats open in CSM-S software release 1.1(1), see the [“Open Caveats in Software Release 1.1\(1\)”](#) section on page 21.

CSM-S software release 1.1(1) is the first release in a new release train.

Related Documentation

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

- *Catalyst 6500 Series Switch Content Switching Module with SSL Installation Note*
- *Catalyst 6500 Series Switch Content Switching Module with SSL Installation and Configuration Note*
- *Catalyst 6500 Series Switch Content Switching Module with SSL Command Reference*
- *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/univercd/home/home.htm>

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/public/countries_languages.shtml

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

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/en/US/partner/ordering/>
- 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 1 800 553-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.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

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

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

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

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies — security-alert@cisco.com
- Nonemergencies — psirt@cisco.com



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

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/techsupport>

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>

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

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 provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

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/techsupport/contacts>

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/>

- *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/packet>

- *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. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- *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/ipj>

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

<http://www.cisco.com/en/US/learning/index.html>

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.



Copyright © 2005, Cisco Systems, Inc.
All rights reserved.