



# Release Notes for Cisco Content Services Gateway 3.1(3)C7(11) for Cisco IOS Release 12.2(18)SXF or Cisco IOS Release 12.2(18)SRA

---

**Revised: July 2, 2009**  
**Current Release—3.1(3)C7(11)**

This publication describes the requirements, dependencies, and caveats for the Cisco Content Services Gateway (CSG) Release 3.1(3)C7(11).

## Contents

- [Introduction, page 2](#)
- [Features, page 2](#)
- [System Requirements, page 7](#)
- [Upgrading to a New CSG Release, page 11](#)
- [Saving and Restoring Configurations, page 11](#)
- [Additional Installation Instructions, page 11](#)
- [Prerequisites, page 11](#)
- [Restrictions, page 11](#)
- [Caveats for 3.1\(3\)C7\(11\), page 11](#)
- [Caveats for 3.1\(3\)C7\(10\), page 12](#)
- [Caveats for 3.1\(3\)C7\(9\), page 14](#)
- [Caveats for 3.1\(3\)C7\(8\), page 16](#)
- [Caveats for 3.1\(3\)C7\(7\), page 20](#)
- [Caveats for 3.1\(3\)C7\(6\), page 23](#)



---

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

- [Caveats for 3.1\(3\)C7\(5\), page 29](#)
- [Caveats for 3.1\(3\)C7\(4\), page 33](#)
- [Caveats for 3.1\(3\)C7\(3\), page 40](#)
- [Caveats for 3.1\(3\)C7\(2\), page 45](#)
- [Caveats for 3.1\(3\)C7\(1\), page 52](#)
- [Documentation and Technical Assistance, page 54](#)
- [Obtaining Documentation and Submitting a Service Request, page 55](#)

## Introduction

The CSG is a high-speed processing module that brings content billing and user awareness to the Cisco Catalyst® 6500 series switch and Cisco 7600 series router platforms. The CSG is typically located at the edge of a network in an ISP POP, or Regional Data Center.

## Features

This section lists the CSG features, the CSG release in which the feature was introduced, and the minimum CSG release required to support the feature. For full descriptions of all of these features, see the *Cisco Content Services Gateway Installation and Configuration Guide*, Release 3.1(3)C7(1).

To see the software part numbers associated with each CSG release; the Supervisor hardware required by each CSG release; the minimum Cisco IOS release required for new features in each CSG release, the minimum CatOS/Hybrid level supported by each CSG release; and the minimum IOS level supported by each CSG release, see the [“Software Requirements” section on page 9](#).

- [CSG Features Introduced Prior to CSG R4.1, page 3](#)
- [CSG Features Introduced in CSG R4.1—3.1\(3\)C4\(1\), page 3](#)
- [CSG Feature Introduced in CSG R4.8—3.1\(3\)C4\(8\), page 4](#)
- [CSG Feature Introduced in CSG R4.9—3.1\(3\)C4\(9\), page 4](#)
- [CSG Features Introduced in CSG R5.1—3.1\(3\)C5\(1\), page 4](#)
- [CSG Feature Introduced in CSG R5.2—3.1\(3\)C5\(2\), page 5](#)
- [CSG Feature Introduced in CSG R5.3—3.1\(3\)C5\(3\), page 5](#)
- [CSG Feature Introduced in CSG R5.4—3.1\(3\)C5\(4\), page 5](#)
- [CSG Features Introduced in CSG R5.5—3.1\(3\)C5\(5\), page 5](#)
- [CSG Features Introduced in CSG R6.2—3.1\(3\)C6\(2\), page 6](#)
- [CSG Features Introduced in CSG R6.3—3.1\(3\)C6\(3\), page 7](#)
- [CSG Features Introduced in CSG R6.9—3.1\(3\)C6\(9\), page 7](#)
- [CSG Features Introduced in CSG R7.1—3.1\(3\)C7\(1\), page 7](#)

## CSG Features Introduced Prior to CSG R4.1

The following features were introduced Prior to CSG R4.1:

- HTTP 1.0 Content Billing
- HTTP 1.1 Content Billing
- HTTP Records Reporting Flexibility
- HTTP Error Code Reporting
- Billing Mediation Agent (BMA) Load Sharing
- Charging Record Delivery to BMA
- Prepaid Billing Quota Enforcement
- Intermediate Billing Records
- Stateful Redundancy
- Stateful Failover for Replicated TCP Connections
- Browser Identification
- Flow Analysis for Billing and Activity Tracking
- Layer 4 Billing for Non-HTTP
- Filtering Accounting via URL Maps
- Learning User ID via Inspection of RADIUS Accounting Messages
- Learning User ID via XML Query
- TCP Retransmit Volume Exclusion
- Packet Counts
- Postpaid FTP Support
- X-Forwarded-For Support
- CSG MIB Support

## CSG Features Introduced in CSG R4.1—3.1(3)C4(1)

The following features were introduced in CSG R4.1, and require IOS release 12.2(14)ZA1 or later:

- Base WAP Support (see later releases for additional WAP support)
- RADIUS Proxy Support
- Quota Server Loadsharing Support
- RADIUS Accounting Attribute Support

The following features were introduced in CSG R4.1, and require IOS release 12.2(14)ZA2 or later:

- Cisco Persistent Storage Device Support
- Quota Server Load Sharing Support
- Prepaid FTP Billing Support
- Per-Event Filtering and Other Per-Event Actions Support
- SMTP and POP3 Data Mining Support

- Redirect Flexibility Support
- WAP Stateful Failover Support
- WAP URL Mapping Support

**Note**


---

The Cisco IOS 12.2ZA early deployment release has migrated to 12.2SXB and is no longer available.

---

## CSG Feature Introduced in CSG R4.8—3.1(3)C4(8)

The following feature was introduced in CSG R4.8, and requires IOS release 12.2(14)ZA2 or later:

- WAP Advice of Charge

**Note**


---

The Cisco IOS 12.2ZA early deployment release has migrated to 12.2SXB and is no longer available.

---

## CSG Feature Introduced in CSG R4.9—3.1(3)C4(9)

The following feature was introduced in CSG R4.9, and requires IOS release 12.2(14)ZA2 or later:

- RADIUS Stop/Start Support

**Note**


---

The Cisco IOS 12.2ZA early deployment release has migrated to 12.2SXB and is no longer available.

---

## CSG Features Introduced in CSG R5.1—3.1(3)C5(1)

The following features were introduced in CSG R5.1, and require IOS release 12.2(17d)SXB or later:

- WAP 2.0 Limited Support—Requires one or both of the following environment variables:
  - `CSG_HTTP_PERSISTENCE_DISABLE`—Disables HTTP persistent connections. This causes CSG to look at only the first request of a persistent connection, which might conflict with the charging model.
  - `CSG_HTTP_1_0_OPERATION`—Overwrites HTTP version to 1.0. This overwrites the HTTP version, which prevents the server from sending chunked responses.

**Note**


---

WAP2.0 Limited Support is valid only prior to R5.5. Beginning in R5.5, the CSG provides Full Support for WAP 2.0, and the `CSG_HTTP_PERSISTENCE_DISABLE` and `CSG_HTTP_1_0_OPERATION` environment variables are deprecated and no longer required.

---

- Base Real Time Streaming Protocol (RTSP) Billing (see later releases for additional RTSP support)
- Prepaid Error Reimbursement
- WAP Cutoff
- Service Duration Billing
- Report Billing Plan ID to BMA and Quota Server

- Asynchronous Quota Return
- Asynchronous Service Stop
- RADIUS Enhancements
- HTTP URL Redirect
- Base URL Rewriting (see later releases for additional URL rewriting support)
- WAP URL Appending
- Fixed Attribute CDRs
- Port-Number Ranges Support

## CSG Feature Introduced in CSG R5.2—3.1(3)C5(2)

The following feature was introduced in CSG R5.2, and requires IOS release 12.2(17d)SXB or later:

- Same-Port HTTP and HTTPS Proxy (SSL Protocol Switching)

## CSG Feature Introduced in CSG R5.3—3.1(3)C5(3)

The following feature was introduced in CSG R5.3, and requires IOS release 12.2(18)SXD1 or later:

- Service-Level CDR Summarization Limited Support—Supports the following protocols in both fixed and variable format: IP, HTTP, SMTP, POP3 (postpaid only), and IMAP (postpaid only).

## CSG Feature Introduced in CSG R5.4—3.1(3)C5(4)

The following feature was introduced in CSG R5.4, and requires IOS release 12.2(18)SXD1 or later:

- Multiple VSAs for Fixed-Format Records

## CSG Features Introduced in CSG R5.5—3.1(3)C5(5)

The following features were introduced in CSG R5.5, and require IOS release 12.2(18)SXD1 or later:

- HTTP Pipelining and Chunked Transfer Encoding
- TCP Byte Counts for HTTP Billing
- WAP 2.0 Full Support
- WAP URL Rewriting Support
- Service Verification
- RADIUS Handoff Support
- Fixed CDR Support for HTTP
- Fixed CDR Support for RTSP
- Fixed CDR Support for IMAP
- Single CDR Support for WAP Connectionless and HTTP
- SMTP Prepaid/Envelope Support

- SMTP Content Authorization Support
- Base POP3 Support (see later releases for additional POP3 support)
- RADIUS Packet of Disconnect
- RADIUS Endpoint
- RADIUS Proxy Source IP Address
- Service-Level CDR Summarization
- Passthrough Mode and the Default Quota
- IP Fragments Limited Support—Supports IP fragmentation for HTTP, WAP2.0, WAP1.x, and generic Layer 4 flows regardless of the order in which the flows arrive. The CSG does not support IP fragmentation for SMTP, POP3, IMAP4, FTP, and RTSP control connection, nor for RADIUS flows.
- Connection Duration Billing
- URL MAP Support for RTSP
- Postpaid Service Tagging
- Stateful Failover for FTP, HTTP, and IMAP

## CSG Features Introduced in CSG R6.2—3.1(3)C6(2)

The following features were introduced in CSG R6.2, and require IOS release 12.2(18)SXE or later:

- CSG Interface Awareness—requires Supervisor Engine 720 with an MSFC3-BXL (SUP720-MSFC3-BXL)
- Quota Push
- Tariff Switch
- Prepaid Support for POP3
- Prepaid Support for IMAP
- Transaction Support for IMAP
- Enhanced Interoperability with Cisco Service-Aware GGSN
- CSG RADIUS Proxy Enhancements
- Supplemental Usage Reports
- Quota Balance Replacement
- Delayed Quota Reauthorization
- Configurable Reauthorization Threshold

## CSG Features Introduced in CSG R6.3—3.1(3)C6(3)

The following feature was introduced in CSG R6.3, and requires IOS release 12.2(18)SXE or later:

- Unknown Packet Drop

## CSG Features Introduced in CSG R6.9—3.1(3)C6(9)

The following feature was introduced in CSG R6.9, and requires IOS release 12.2(18)SXE or later:

- CSG RADIUS Support for Simultaneous Endpoint and Proxy Modes

## CSG Features Introduced in CSG R7.1—3.1(3)C7(1)

The following features were introduced in CSG R7.1, and require Cisco IOS release 12.2(18)SXF1 or later, or Cisco IOS release 12.2(18)SRA or later:

- RADIUS VSA Subattribute Parsing
- User Table Entry Idle Timeout
- RTSP PAUSE Support
- SMTP CDR Header Removal
- Service-Level CDR Support for FTP, RTSP, and WAP 1.x
- HTTP IP Byte Counting
- Performance Improvements for WAP
- IP Fragment Support for IMAP, POP3, and SMTP
- Support for Out-of-Order Packets for HTTP, IMAP, POP3, and SMTP
- Support for Additional Services, Services Rules, and Content/Policy Pairs
- Support for Multipart HTTP
- Support for WAP Segmentation and Reassembly (SAR)
- Support for Obscuring the IP Address in X-Forwarded-For Headers
- Enhanced Quota Reconciliation
- Enhancements for Layer 2

## System Requirements

This section describes the following memory, hardware, and software requirements for CSG:

- [Memory Requirements, page 8](#)
- [Hardware Supported, page 8](#)
- [Power Supply, page 8](#)
- [Environmental Requirements, page 8](#)
- [Software Requirements, page 9](#)
- [Determining the Software Version, page 10](#)

## Memory Requirements

The CSG memory is not configurable.

## Hardware Supported

Use of the CSG requires one of the following supervisor engines, and a module with ports to connect server and client networks:

- A Supervisor Engine 32 with an MSFC2A and PFC3B (WS-SUP32-GE-3B/MSFC2A/PFC3B or WS-SUP32-10GE-3B/MSFC2A/PFC3B)
- A Supervisor Engine 720 with an MSFC3-BXL (SUP720-MSFC3-BXL)

The WS-SVC-CSG-1 CSG is not fabric-enabled, but the module can operate in a fabric-enabled chassis like any other non-fabric-enabled module.



### Caution

If you use the MSFC, which is internal to the Catalyst 6000 family switch, as the router for both the client and the server side at the same time, you must ensure that packets for billable flows cannot bypass the CSG. Also, if you use static **ip route** statements to switch traffic to the CSGs, packets might loop between the MSFC and CSG in this configuration. To avoid these problems, use other routing techniques to switch packets to the CSG, such as policy-based routing.

## Power Supply

The CSG operates on power supplied by the chassis. Therefore, you can place the CSG in any slot in the Catalyst 6500 series switch or Cisco 7600 series router chassis, except those occupied by the supervisor engine and the standby supervisor engine.

## Environmental Requirements

The following table lists the environmental requirements for the CSG:

Item	Specification
Temperature, ambient operating	0° to 40°C (32° to 104°F)
Temperature, ambient nonoperating	-40° to 70°C (-40° to 158°F)
Humidity (RH), ambient (noncondensing) operating	10% to 90%
Nonoperating relative humidity (noncondensing)	5% to 95%

## Software Requirements

The following table lists the software part numbers for each CSG release; the Supervisor hardware required by each CSG release; the minimum Cisco IOS release required for new features in each CSG release, the minimum CatOS/Hybrid level supported by each CSG release; and the minimum IOS level supported by each CSG release.

CSG Release	Software Part Number	Supervisor Hardware Supported <sup>1</sup>	Minimum Cisco IOS Release Required for New Features <sup>2</sup>	Minimum CatOS/Hybrid Level Supported	Minimum Cisco IOS Level Supported <sup>3</sup>
3.1(3)C7(11))	SC-SVC-CSG-B-7.0 SC-SVC-CSG-P-7.0 SC-SVC-CSG-EP-7.0	SUP720-MSFC3-BXL SUP32-MSFC2A and PFC3B	12.2(18)SXF1 or 12.2(18)SRA	7.6.1	12.2(18)SXF1 or 12.2(18)SRA
3.1(3)C7(10))	SC-SVC-CSG-B-7.0 SC-SVC-CSG-P-7.0 SC-SVC-CSG-EP-7.0	SUP720-MSFC3-BXL SUP32-MSFC2A and PFC3B	12.2(18)SXF1 or 12.2(18)SRA	7.6.1	12.2(18)SXF1 or 12.2(18)SRA
3.1(3)C7(9)	SC-SVC-CSG-B-7.0 SC-SVC-CSG-P-7.0 SC-SVC-CSG-EP-7.0	SUP720-MSFC3-BXL SUP32-MSFC2A and PFC3B	12.2(18)SXF1 or 12.2(18)SRA	7.6.1	12.2(18)SXF1 or 12.2(18)SRA
3.1(3)C7(8)	SC-SVC-CSG-B-7.0 SC-SVC-CSG-P-7.0 SC-SVC-CSG-EP-7.0	SUP720-MSFC3-BXL SUP32-MSFC2A and PFC3B	12.2(18)SXF1 or 12.2(18)SRA	7.6.1	12.2(18)SXF1 or 12.2(18)SRA
3.1(3)C7(7)	SC-SVC-CSG-B-7.0 SC-SVC-CSG-P-7.0 SC-SVC-CSG-EP-7.0	SUP720-MSFC3-BXL SUP32-MSFC2A and PFC3B	12.2(18)SXF1 or 12.2(18)SRA	7.6.1	12.2(18)SXF1 or 12.2(18)SRA
3.1(3)C7(6)	SC-SVC-CSG-B-7.0 SC-SVC-CSG-P-7.0 SC-SVC-CSG-EP-7.0	SUP720-MSFC3-BXL SUP32-MSFC2A and PFC3B	12.2(18)SXF1 or 12.2(18)SRA	7.6.1	12.2(18)SXF1 or 12.2(18)SRA
3.1(3)C7(5)	SC-SVC-CSG-B-7.0 SC-SVC-CSG-P-7.0 SC-SVC-CSG-EP-7.0	SUP720-MSFC3-BXL SUP32-MSFC2A and PFC3B	12.2(18)SXF1 or 12.2(18)SRA	7.6.1	12.2(18)SXF1 or 12.2(18)SRA
3.1(3)C7(4)	SC-SVC-CSG-B-7.0 SC-SVC-CSG-P-7.0 SC-SVC-CSG-EP-7.0	SUP720-MSFC3-BXL SUP32-MSFC2A and PFC3B	12.2(18)SXF1 or 12.2(18)SRA	7.6.1	12.2(18)SXF1 or 12.2(18)SRA
3.1(3)C7(3)	SC-SVC-CSG-B-7.0 SC-SVC-CSG-P-7.0 SC-SVC-CSG-EP-7.0	SUP720-MSFC3-BXL SUP32-MSFC2A and PFC3B	12.2(18)SXF1 or 12.2(18)SRA	7.6.1	12.2(18)SXF1 or 12.2(18)SRA
3.1(3)C7(2)	SC-SVC-CSG-B-7.0 SC-SVC-CSG-P-7.0 SC-SVC-CSG-EP-7.0	SUP720-MSFC3-BXL SUP32-MSFC2A and PFC3B	12.2(18)SXF1 or 12.2(18)SRA	7.6.1	12.2(18)SXF1 or 12.2(18)SRA
3.1(3)C7(1)	SC-SVC-CSG-B-7.0 SC-SVC-CSG-P-7.0 SC-SVC-CSG-EP-7.0	SUP720-MSFC3-BXL SUP32-MSFC2A and PFC3B	12.2(18)SXF1 or 12.2(18)SRA	7.6.1	12.2(18)SXF1 or 12.2(18)SRA

1. Do not use the minimums listed in this table to infer supervisor hardware support. Consult the *Cisco IOS Upgrade Planner* to determine which IOS releases support the desired supervisor hardware.

2. If running Hybrid, make sure the appropriate IOS Hybrid image is available at this level.
3. The feature set is limited to those features that can be configured at this IOS level.

The following table lists the supported hardware and software for the CSG:

Product Number	Product Description	Minimum Software Version	Recommended Software Version	Cisco IOS Release	Minimums for CSG/Hybrid
<b>CSG</b>					
WS-SVC-CSG-1 with SUP1A	CSG	3.1(1)C3(1)	3.1(1)C3(2)	12.1(12c)E4	IOS 12.1(13)E3 CatOS 7.6.1
WS-SVC-CSG-1 with SUP2	CSG	3.1(1)C3(1)	3.1(1)C3(2)	12.1(12c)E4	IOS 12.1(13)E3 CatOS 7.6.1
WS-SVC-CSG-1 with SUP32 with an MSFC2A and PFC3B (WS-SUP32-GE-3B/MSFC2A/PFC3B or WS-SUP32-10GE-3B/MSFC2A/PFC3B)	CSG	3.1(3)C7(1)	3.1(3)C7(11)	12.2(18)SXF1 or 12.2(18)SRA	IOS 12.2(18)SXF1 or IOS 12.2(18)SRA CatOS 7.6.1
WS-SVC-CSG-1 with SUP720 with an MSFC3-BXL (SUP720-MSFC3-BXL)	CSG	3.1(3)C5(5)	3.1(3)C5(5)	12.2(18)SXD	IOS 12.2(18)SXD CatOS 7.6.1
<b>Console Cable</b>					
72-876-01	Console Cable	Not applicable	Not applicable	Not applicable	Not applicable
<b>Accessory Kit</b>					
800-05097-01	Accessory kit (contains the Console Cable)	Not applicable	Not applicable	Not applicable	Not applicable

When using the CSG with some IOS images, you might see the following warning message:

**%PM\_SCP-SP-4-UNK\_OPCODE: Received unknown unsolicited message from module n, opcode 0x330**

You can ignore this message.

## Determining the Software Version

To determine the version of Cisco IOS software that is currently running on your Cisco network device, log in to the device and enter the **show version EXEC** command.

To show CSG versions, use the **show module** command in privileged EXEC mode.

To provide meaningful problem determination information, use the **show tech-support** command in privileged EXEC mode.

## Upgrading to a New CSG Release

For the latest upgrade procedures for the CSG, see the “Configuring the Content Services Gateway” chapter of the *Cisco Content Services Gateway Installation and Configuration Guide*.

## Saving and Restoring Configurations

For information about saving and restoring configurations, see the *Catalyst 6000 Family IOS Software Configuration Guide* or to the *Cisco 7600 Series Cisco IOS Software Configuration Guide*.

## Additional Installation Instructions

For more information about installing the CSG, see the *Cisco Content Services Gateway Installation and Configuration Guide*.

## Prerequisites

For the latest prerequisites for the CSG, see the “Overview” chapter of the *Cisco Content Services Gateway Installation and Configuration Guide*.

## Restrictions

For the latest restrictions for the CSG, see the “Overview” chapter of the *Cisco Content Services Gateway Installation and Configuration Guide*.

## Caveats for 3.1(3)C7(11)

This section lists and describes all caveats, both open and resolved, that affect CSG software release 3.1(3)C7(11).

For information about open or unresolved caveats in the Content Services Gateway 3.1(3)C7(11) release, refer to the Cisco Bug Toolkit at the following URL:

<http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>.

## CSG Release 3.1(3)C7(11) - Open Caveats

There are no open caveats in CSG Release 3.1(3)C7(11).

## CSG Release 3.1(3)C7(11) - Closed Caveats

The following section lists bugs that are closed in CSG Release 3.1(3)C7(11).

- CSCsz96577—Environment variable to disable TCP IXP buffer exhaustion

Under heavy load, the CSG might encounter an IPCP crash as a result of miscommunication between IXP and the PPC:

```
!!!CORE DUMP TUE MAY 05 12:10:39 2009
!!!Version: 3.1(3)C7(7)
PPC exception type 122 on 'core_dump(0CC861A0h)'
```

To help eliminate this problem, the configurable `CSG_TCP_MONITOR_BUFFERS` environment variable is added to the CSG. This variable enables you to set the TCP IXP buffer monitoring interval, in minutes. The range for this variable is 0 to 1440 minutes. The default setting for this variable is 1 minute. Setting this variable to 0 turns off monitoring.

To set this variable, use the `variable` command in module CSG configuration mode.

- CSCta36912—Control the duration of checking billing queue overflow via an environment variable

Under heavy load, the CSG might crash with the following crash signature:

```
!!!CORE DUMP Fri May 22 17:50:08 2009
!!!Version: 3.1(3)C7(10)
PPC exception type 122 on 'core_dump(0CC78178h)'
```

To help eliminate this problem, the configurable `CSG_BILL_Q_OVERFLOW` environment variable is added to the CSG. This variable enables you to set the billing queue overflow monitoring interval, in seconds. The range for this variable is 0 to 3600 seconds. The default setting for this variable is 1 second. Setting this variable to 0 turns off monitoring.

To set this variable, use the `variable` command in module CSG configuration mode.

## Caveats for 3.1(3)C7(10)

This section lists and describes all caveats, both open and resolved, that affect CSG software release 3.1(3)C7(10).

For information about open or unresolved caveats in the Content Services Gateway 3.1(3)C7(10) release, refer to the Cisco Bug Toolkit at the following URL:

<http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>.

## CSG Release 3.1(3)C7(10) - Open Caveats

There are no open caveats in CSG Release 3.1(3)C7(10).

## CSG Release 3.1(3)C7(10) - Closed Caveats

The following section lists bugs that are closed in CSG Release 3.1(3)C7(10).

- CSCsv14112—The CSG crashes after a **billingTask** stack overflow

The CSG might crash with the following crash signature:

```
!!!CORE DUMP WED SEP 03 08:15:11 2008
!!!Version: 3.1(3)C6(11)
PPC exception type 1792 on 'fastblk(0D782310h)'
```

The crash is triggered by memory corruption caused by a stack overflow in the Billing task.

- CSCsv23706—CSG: PoD sent too soon

Even if a user has enough quota, the CSG might send a PoD (Packet of Disconnect).

For this problem to occur, all of the following conditions must be met:

- The user for whom the PoD is being sent must be in prepaid mode.
- The user must have either high number of sessions or long-lived sessions.
- A PoD must be requested by the quota server.

- CSCsv37509—The CSG drops some ICMP packets

The CSG might drop some ICMP packets, resulting in a ping failure.

For this problem to occur, all of the following conditions must be met:

- The CSG must receive an ICMP packet from the client/server.
- The CSG must receive another ICMP packet on the session before it is able to match the contents/policy rule for the session.

- CSCsw17156—The CSG might block HTTP requests

When an HTTP stream matches a content and policy with **accounting type http**, the CSG might block the request and generate a RST back to the subscriber.

For this problem to occur, all of the following conditions must be met:

- The data flow must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
- The configuration include several header maps and URL maps.
- The configuration must consume a large amount of regex memory.
- One of the URL maps that is defined in any of the contents which is inservice and is part of the configured ruleset must be modified.
- The free memory in the rule table must be less than half of the total memory in the rule table.

- CSCsw17512—Too many syslog messages sent to the Supervisor Engine

If the CSG is generating syslog messages at a high rate, the Supervisor Engine might experience high CPU usage.

For this problem to occur, all of the following conditions must be met:

- The CSG must be one of the line cards in the chassis.
- RADIUS must be configured under the user-group configuration.
- The number of RADIUS clients connected to the CSG must exceed the maximum (93).

- CSCsw89769—The CSG might go offline after a Supervisor Engine failover  
The CSG might go offline or crash after a Supervisor Engine switchover.  
For this problem to occur, all of the following conditions must be met:
  - The chassis must have active and standby Supervisor Engines running 12.2(33)SRC images.
  - The Supervisor Engines must be configured for stateful switchover (SSO) redundancy.
  - A Supervisor Engine SSO must occur, with the standby Supervisor Engine taking over as the new active Supervisor Engine.
  - The chassis must have a large number of Gigabit ports (two CEF720 48 Gigabit interfaces).
- CSCsx46442—HTTP session might hang resulting in stale connection  
When an HTTP stream that contains out-of-order packets matches a content and policy with **accounting type http**, the CSG might stop forwarding packets for that session.  
For this problem to occur, all of the following conditions must be met:
  - The data flow must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
  - The client must send a GET.
  - The CSG must forward the GET to the server.
  - The server must send back a response.

## Caveats for 3.1(3)C7(9)

This section lists and describes all caveats, both open and resolved, that affect CSG software release 3.1(3)C7(9).

For information about open or unresolved caveats in the Content Services Gateway 3.1(3)C7(9) release, refer to the Cisco Bug Toolkit at the following URL:

<http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>.

### CSG Release 3.1(3)C7(9) - Open Caveats

There are no open caveats in CSG Release 3.1(3)C7(9).

### CSG Release 3.1(3)C7(9) - Closed Caveats

The following section lists bugs that are closed in CSG Release 3.1(3)C7(9).

- CSCek75928—CSG: Need to be able to mix type HTTP and no billing policies  
The CSG does not allow the user to configure a content that includes a policy with **accounting type http**, and a policy that does not include an accounting statement.

- CSCsc33686—Sessions dropped during RD “wait” when out of quota for **basis seconds** service  
The CSG closes all open sessions during a Reauthorization Delay (RD) “wait” state (that is, action code = wait in Reauthorization Delay TLV in most recent Service Authorization Response, Service Reauthorization Response, Quota Push Request, Quota Return Accept, or Service Verification Response message) for a service that is configured with **basis second** service when the quota for that service expires during the wait period.
- CSCsk51915—Multiprotocol stress: debug messages seen on the standby CSG  
When the multiprotocol (HTTP, FTP, RTSP, TCP and WAP) traffic load is high, the standby CSG might receive the following message:  
**Tack! invalid appl ptr 17ad0/203**  
  
**17ad0/203 src: 40.40.40.2:20 dst: 31.31.11.3:20921 prot: 6**  
**kut index: ip= 31.31.11.3, uid= user22818**  
**flags: NETWORK\_INIT POSTPAID TCP\_ADJ\_NEEDED BACKUP\_NEEDED**  
**prepaid: ip bytes up = 0, ip bytes down = 0**  
**tcp bytes up = 0, tcp bytes down = 0**  
**bytes granted = 0, quads consumed = 0**  
**flags = <none>**
- CSCsk92635—The CSG generates an FPGA1 exception error and resets  
The CSG core dumps and resets after a switchover.  
For this problem to occur, all of the following conditions must be met:
  - The CSG must be under heavy traffic conditions and stress levels.
  - IP addresses for users must be reused from a common pool.
  - The CSG must switch over.
- CSCso99995—The TCP window scaling option might affect CSG throughput  
A TCP session that is using the window scaling option might encounter a reduced download speed.  
For this problem to occur, all of the following conditions must be met:
  - The HTTP connection must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
  - The client or server must use the window scaling option to publish the receiver window size.
- CSCsq00062—Sporadic drops of packets relayed by CSG  
The CSG might not relay some packets in the downlink direction, causing retransmits in the case of TCP (although the problem might not be limited to the downlink direction or to TCP).  
For this problem to occur, all of the following conditions must be met:
  - The CSG must be configured to be fault-tolerant (FT).
  - Replication must be ON for majority of the traffic. (By default, replication is ON for all of the contents, but if **variable CSG\_FT\_CONTENT 1** is configured, replication is ON only for those contents that are configured with the **replication** command.)
- CSCsq55437—CSG crash at **FPGA1 exception 999 IXIC\_ICPAS - iPacket passthrough...**  
When an HTTP stream matches a content and policy with **accounting type http**, the CSG might crash with the following signature:

!!!CORE DUMP SAT MAY 17 19:04:51 2008

!!!Version: 3.1(3)C7(7)

FPGA1 exception 999 IXIC\_ICPAS - iPacket passthrough. ecmd wants to sync.

For this problem to occur, all of the following conditions must be met:

- The HTTP connection must match a CSG content configured with policies requiring HTTP deep packet inspection (**accounting type http**).
  - The TCP handshake must be established between the client and the server.
  - The client must send a malformed packet with the SYN bit set, and the packet length in the IP Header must be less than the combined lengths of the IP plus TCP Header.
- CSCsr13290—The CSG might block traffic that matches **accounting type http**

The CSG might drop sessions that match **accounting type http**, even when the user has enough quota.

For this problem to occur, all of the following conditions must be met:

- The HTTP connection must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
  - Prepaid users must send e-mail.
- CSCsr20149—The CSG might block HTTP POSTs with multipart requests

The CSG might block multipart HTTP POST requests.

For this problem to occur, all of the following conditions must be met:

- The HTTP connection must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
  - The policies must have header maps defined.
  - The transaction must use “Content-Type: multipart...”
- CSCsr62399—The **client** command in CSG content configuration mode might not work

The CSG might block traffic that is expected to match a default policy under a content.

For this problem to occur, all of the following conditions must be met:

- A default policy must be configured.
- The **ip csg block** command in global configuration mode must not be configured.
- The **client** command must be configured in CSG content configuration mode, then unconfigured.
- Traffic that should match a default policy must be sent.

## Caveats for 3.1(3)C7(8)

This section lists and describes all caveats, both open and resolved, that affect CSG software release 3.1(3)C7(8).

For information about open or unresolved caveats in the Content Services Gateway 3.1(3)C7(8) release, refer to the Cisco Bug Toolkit at the following URL:

<http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>.

## CSG Release 3.1(3)C7(8) - Open Caveats

The following list identifies open caveats in CSG Release 3.1(3)C7(8).

- CSCek75928—CSG: Need to be able to mix type HTTP and no billing policies  
 The CSG does not allow the user to configure a content that includes a policy with **accounting type http**, and a policy that does not include an accounting statement.  
**Workaround:** None.
- CSCsc33686—Sessions dropped during RD “wait” when out of quota for **basis seconds** service  
 The CSG closes all open sessions during a Reauthorization Delay (RD) “wait” state (that is, action code = wait in Reauthorization Delay TLV in most recent Service Authorization Response, Service Reauthorization Response, Quota Push Request, Quota Return Accept, or Service Verification Response message) for a service that is configured with **basis second** service when the quota for that service expires during the wait period.  
**Workaround:** None.
- CSCsk51915—Multiprotocol stress: debug messages seen on the standby CSG  
 When the multiprotocol (HTTP, FTP, RTSP, TCP and WAP) traffic load is high, the standby CSG might receive the following message:  

```
Tack! invalid appl ptr 17ad0/203

17ad0/203 src: 40.40.40.2:20 dst: 31.31.11.3:20921 prot: 6
kut index: ip= 31.31.11.3, uid= user22818
flags: NETWORK_INIT POSTPAID TCP_ADJ_NEEDED BACKUP_NEEDED
prepaid: ip bytes up = 0, ip bytes down = 0
tcp bytes up = 0, tcp bytes down = 0
bytes granted = 0, quads consumed = 0
flags = <none>
```

**Workaround:** None.
- CSCsk92635—The CSG generates an FPGA1 exception error and resets  
 The CSG core dumps and resets after a switchover.  
 For this problem to occur, all of the following conditions must be met:
  - The CSG must be under heavy traffic conditions and stress levels.
  - IP addresses for users must be reused from a common pool.
  - The CSG must switch over.**Workaround:** Make sure every user has a unique IP address.
- CSCso99995—The TCP window scaling option might affect CSG throughput  
 A TCP session that is using the window scaling option might encounter a reduced download speed.  
 For this problem to occur, all of the following conditions must be met:
  - The HTTP connection must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
  - The client or server must use the window scaling option to publish the receiver window size.**Workaround:** Use Layer 4 accounting for HTTP, or if Layer 7 accounting is required upgrade to the Cisco Content Services Gateway - 2nd Generation (CSG2).

- CSCsq00062—Sporadic drops of packets relayed by CSG  
When the CSG is used for postpaid service, relaying packets between the subscriber and the application server, some packets are not relayed by the CSG.  
**Workaround:** None.

## CSG Release 3.1(3)C7(8) - Closed Caveats

The following section lists bugs that are closed in CSG Release 3.1(3)C7(8).

- CSCsi14915—Small buffer leak for SMTP traffic  
A small buffer leak occurs when running SMTP traffic.
- CSCsi48584—ARP entries shown as LEARNED, DOWN instead of VSERVER, LOCAL  
The **show module csg arp** command shows some of the ARP entries as LEARNED, DOWN instead of the correct VSERVER, LOCAL. There is no operational impact.
- CSCsk65627—CDRs report negative values for quadrans  
When the usage for a transaction is greater than 2147483647 quadrans, the CSG might report a negative value for quadrans in the BMA CDR.
- CSCsk65641—Total Usage in Service Stop reports a negative value  
The CSG might report a negative value for Total Usage in a Service Stop.  
For this problem to occur, all of the following conditions must be met:
  - Refund must be configured.
  - For a prepaid user, the “Pending Usage” field in the output for the **show ip csg accounting users** command must be greater than 2147483647.
- CSCsk70898—After a CSG upgrade, entPhysicalSoftwareRev still reflects the old CSG version  
MIB entity entPhysicalSoftwareRev does not reflect the current CSG version after a CSG image upgrade.
- CSCsk76201—Service Auth/Reauth storm for multiple sessions  
The CSG might seem to resend Quota Service Reauthorization Requests in an endless loop for a specific user and a specific service.  
The “Reserved” value seen in **show ip csg accounting users** is a signed integer. When this value exceeds 2147483647, this problem can occur.
- CSCsl18499—Tracelog error messages controlled with environment variable  
The configurable **CSG\_EXTRA\_TRACELOG\_ENABLE** environment variable is added to the CSG. This variable enables (1) or disables (0) additional tracelog statistics in the output for the **show tech** command. The default setting for this variable is 0 (disabled).  
To set this variable, use the **variable** command in module CSG configuration mode.
- CSCsl52845—CSG R7.6 Module Reset FPGA5 transmit FIFO Full  
A CSG might reset when running CSG Release 7.6. The following error is observed:
 

```
%CSM_SLB-3-UNEXPECTED: Module 4 unexpected error: Traceback - 0x001F93E0
0x001F8EBC 0x001F865C 0x001FA1F8 0x001AD250
%CSM_SLB-3-UNEXPECTED: Module 4 unexpected error: FPGA1 exception
encountered.
```

**% CSM\_SLB-3-UNEXPECTED: Module 4 unexpected error: Diag - 02000.02000.00001.00001.00001 FPGA5 transmit FIFO full**  
**% CSM\_SLB-3-UNEXPECTED: Module 4 unexpected error: Rebooting...**

- CSCs158710—Traceback on standby CSG

You might see the following traceback on the standby CSG:

```
0x001EB5E4 0x0025FFF4 0x001EA320 0x001EAEEC 0x001DD37C 0x001EA1 5C
0x001F35E8 0x0020694C 0x0002984C 0x000522B0 0x0004ADD8 0x001AD250

0x001EB5E4 0x0025FFF4 0x001EA320 0x001F35F4 0x0020694C 0x000298 4C
0x000522B0 0x0004ADD8 0x001AD250
```

- CSCs179097—HTTP download progresses with insufficient prepaid quota

HTTP download progresses with insufficient prepaid quota

For this problem to occur, all of the following conditions must be met:

- The HTTP connection must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
- The transaction must use “Transfer-Encoding:chunked” or “Content-Type: multipart...”
- The quota must be sufficient to pass the GET but not the response.
- If the transaction uses “Content-Type: multipart...”, the CSG\_MULTIPART\_DISABLE variable must be set to 0.

- CSCs193711—Retry Timer False Alarm by CSG during Stress test

Under heavy load, the CSG might trigger the following false alarm:

**Retry Timer is not running for CSG Billing Agent 4.4.4.15:3386 in ACTIVE state**

- CSCsm45691—CSG R7.5 stops forwarding HTTP traffic for a specific service

Under certain timing conditions, the CSG might leak buffer and drop all HTTP traffic.

For this problem to occur, all of the following conditions must be met:

- The HTTP connection must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
- The response from the server must span at least three packets.

- CSCsm51197—The CSG (active or standby) does not drain PSD data

An active or standby CSG with outstanding CDRs on its associated PSD might stop or fail to drain the CDRs when reset

- CSCsm85751—ServiceStop requests might be reassigned after quota server failover

If **no quota server reassign** is configured and the quota server fails while an unacknowledged ServiceStop request is in the queue for that quota server, the CSG might assign the ServiceStop request to an alternate quota server.

- CSCso18183—Incorrect usage reported when complete quota server outage

When a complete quota server outage occurs, the value reported in the “Service Stop Notification” CDR's Usage TLV is lower than it should be. This problem can occur for prepaid users when **basis second** is configured.

- CSCso39777—Missing RADIUS attributes in first CDR

The CSG might send BMA CDRs with no RADIUS attributes included.

For this problem to occur, all of the following conditions must be met:

- The CSG must be configured to report RADIUS attributes in CDRs.
  - The RADIUS accounting start message must not include billing plan info, but must include RADIUS attributes.
  - The CSG must have sent a user authorization request message to the quota server, and must be awaiting a response from the quota server.
  - User traffic must start before the CSG receives the user authorization response message with the user billing plan information.
- CSCso89281—The CSG crashes at IXP3 Software exception

After upgrading to CSG Release 3.1(3)C7(7), multiple CSGs are crashing at:

```
!!!CORE DUMP MON APR 21 16:17:29 2008
!!!Version: 3.1(3)C7(7)
IXP3 Software exception on task 'IXP3 SA-CORE (Ex 18)(00000000h)'
Registers:
LR =00000000h PC =00000000h SP =00000000h
R00=00000000h R01=00000000h R02=00000000h R03=00000000h
R04=00000000h R05=00000000h R06=00000000h R07=00000000h
R08=00000000h R09=00000000h R10=00000000h R11=00000000h
R12=00000000h R13=00000000h R14=00000000h R15=00000000h
Got tag 1 - tracelog, type 6 size 33284
Block 1(33284) Type 6 - tracelog
End Block 1(33284) - tracelog
```

## Caveats for 3.1(3)C7(7)

This section lists and describes all caveats, both open and resolved, that affect CSG software release 3.1(3)C7(7).

For information about open or unresolved caveats in the Content Services Gateway 3.1(3)C7(7) release, refer to the Cisco Bug Toolkit at the following URL:

<http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>.

## CSG Release 3.1(3)C7(7) - Open Caveats

The following list identifies open caveats in CSG Release 3.1(3)C7(7).

- CSCek75928—CSG: Need to be able to mix type HTTP and no billing policies  
The CSG does not allow the user to configure a content that includes a policy with **accounting type http**, and a policy that does not include an accounting statement.  
**Workaround:** None.
- CSCsc33686—Sessions dropped during RD “wait” when out of quota for **basis seconds** service  
The CSG closes all open sessions during a Reauthorization Delay (RD) “wait” state (that is, action code = wait in Reauthorization Delay TLV in most recent Service Authorization Response, Service Reauthorization Response, Quota Push Request, Quota Return Accept, or Service Verification Response message) for a service that is configured with **basis second** service when the quota for that service expires during the wait period.  
**Workaround:** None.

- CSCsi14915—Small buffer leak for SMTP traffic  
A small buffer leak occurs when running SMTP traffic.  
**Workaround:** Change the policy under the SMTP content from **accounting type smtp** to **accounting type other**.
- CSCsi48584—ARP entries shown as LEARNED, DOWN instead of VSERVER, LOCAL  
The **show module csg arp** command shows some of the ARP entries as LEARNED, DOWN instead of the correct VSERVER, LOCAL. There is no operational impact.  
**Workaround:** None.
- CSCsk51915—Multiprotocol stress: debug messages seen on the standby CSG  
When the multiprotocol (HTTP, FTP, RTSP, TCP and WAP) traffic load is high, the standby CSG might receive the following message:  
**Tack! invalid appl ptr 17ad0/203**  
  
**17ad0/203 src: 40.40.40.2:20 dst: 31.31.11.3:20921 prot: 6  
kut index: ip= 31.31.11.3, uid= user22818  
flags: NETWORK\_INIT POSTPAID TCP\_ADJ\_NEEDED BACKUP\_NEEDED  
prepaid: ip bytes up = 0, ip bytes down = 0  
tcp bytes up = 0, tcp bytes down = 0  
bytes granted = 0, quads consumed = 0  
flags = <none>**  
**Workaround:** None.
- CSCsk65627—CDRs report negative values for quadrans  
When the usage for a transaction is greater than 2147483647 quadrans, the CSG might report a negative value for quadrans in the BMA CDR.  
**Workaround:** Clear the affected user.
- CSCsk65641—Total Usage in Service Stop reports a negative value  
The CSG might report a negative value for Total Usage in a Service Stop.  
For this problem to occur, all of the following conditions must be met:
  - Refund must be configured.
  - For a prepaid user, the “Pending Usage” field in the output for the **show ip csg accounting users** command must be greater than 2147483647.**Workaround:** Clear the affected user.
- CSCsk70898—After a CSG upgrade, entPhysicalSoftwareRev still reflects the old CSG version  
MIB entity entPhysicalSoftwareRev does not reflect the current CSG version after a CSG image upgrade.  
**Workaround:** The MIB is updated after the Supervisor Engine reloads.
- CSCsk76201—Service Auth/Reauth storm for multiple sessions  
The CSG might seem to resend Quota Service Reauthorization Requests in an endless loop for a specific user and a specific service.  
The “Reserved” value seen in **show ip csg accounting users** is a signed integer. When this value exceeds 2147483647, this problem can occur.  
**Workaround:** Clear the affected user.

- CSCsk92635—The CSG generates an FPGA1 exception error and resets. The CSG core dumps and resets after a switchover. For this problem to occur, all of the following conditions must be met:
  - The CSG must be under heavy traffic conditions and stress levels.
  - IP addresses for users must be reused from a common pool.
  - The CSG must switch over.**Workaround:** Make sure every user has a unique IP address.
- CSCsl50131—The CSG resends the same Data Record Transfer Request even within 4 seconds. By default, the CSG sends a retry to a CG for an unacknowledged request every 4 seconds. However, in some cases, the retry interval might be less than the configured interval.
 **Workaround:** None.
- CSCsl52845—CSG R7.6 Module Reset FPGA5 transmit FIFO Full. A CSG might reset when running CSG Release 7.6. The following error is observed:
 

```
% CSM_SLB-3-UNEXPECTED: Module 4 unexpected error: Traceback - 0x001F93E0
0x001F8EBC 0x001F865C 0x001FA1F8 0x001AD250
% CSM_SLB-3-UNEXPECTED: Module 4 unexpected error: FPGA1 exception
encountered.
% CSM_SLB-3-UNEXPECTED: Module 4 unexpected error: Diag -
02000.02000.00001.00001.00001 FPGA5 transmit FIFO full
% CSM_SLB-3-UNEXPECTED: Module 4 unexpected error: Rebooting...
```

**Workaround:** None.
- CSCsl58710—Traceback on standby CSG. You might see the following traceback on the standby CSG:
 

```
0x001EB5E4 0x0025FFF4 0x001EA320 0x001EAECC 0x001DD37C 0x001EA1 5C
0x001F35E8 0x0020694C 0x0002984C 0x000522B0 0x0004ADD8 0x001AD250

0x001EB5E4 0x0025FFF4 0x001EA320 0x001F35F4 0x0020694C 0x000298 4C
0x000522B0 0x0004ADD8 0x001AD250
```

**Workaround:** None.
- CSCsl93711—Retry Timer False Alarm by CSG during Stress test. Under heavy load, the CSG might trigger the following false alarm:
 

```
Retry Timer is not running for CSG Billing Agent 4.4.4.15:3386 in ACTIVE state
```

**Workaround:** Reset the `CSG_CHECK_RETRY_TIMER` environmental variable to 0 (zero).

## CSG Release 3.1(3)C7(7) - Closed Caveats

The following section lists bugs that are closed in CSG Release 3.1(3)C7(7).

- CSCsk49775—The CSG crashes and generates a core dump as a result of a timing issue in the IXPs. The CSG crashes and generates a core dump as a result of a timing issue in the IXPs. The core dump indicates that the network processor was waiting for a memory read operation to complete. The health monitor determined that the IXP was no longer communicating with the PPC, and the PPC forced a reset to prevent a card hang condition.

- CSCsk82190—The standby CSG might become active when adding URLs to a map  
When changes are being made to a URL map in a standby CSG, it might become active, leading to an active/active collision.
- CSCsl50131—The CSG resends the same Data Record Transfer Request even within 4 seconds  
By default, the CSG sends a retry to a CG for an unacknowledged request every 4 seconds. However, in some cases, the retry interval might be less than the configured interval.
- CSCsl20686—CSG: TCP volume reported in CDR usage is wrong with RSTP  
For RTSP, the CSG might report an incorrect TCP volume, far above the reported IP byte volume, in CDR usage corresponding to the TCP session. (The reported IP byte volume is correct.)
- CSCsl34063—Control Retry Timer check with an environmental variable  
The configurable **CSG\_CHECK\_RETRY\_TIMER** environment variable is added to the CSG. This variable enables (1) or disables (0) the retry timer, which the CSG uses to check the status of all of the configured CGs every five minutes. The default setting for this variable is 1 (enabled).  
To set this variable, use the **variable** command in module CSG configuration mode.
- CSCsl47769—The CSG resends GTP messages  
In a CSG with prepaid users, there are many GTP resends. This occurs more often with tariff switching during peak hours.  
For this problem to occur, all of the following conditions must be met:
  - 12,500 concurrent prepaid users
  - 120,000 quota messages per hour
  - 30 to 60 quota messages per second
- CSCsl93623—Retry Timer is not running for BMA  
The Queued Count for a BMA or quota server might increase when under heavy load, and might remain at the higher level. If the **max records** setting is reached, the CSG drops all the new requests to the BMA or quota server.

## Caveats for 3.1(3)C7(6)

This section lists and describes all caveats, both open and resolved, that affect CSG software release 3.1(3)C7(6).

For information about open or unresolved caveats in the Content Services Gateway 3.1(3)C7(6) release, refer to the Cisco Bug Toolkit at the following URL:

<http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>.

## CSG Release 3.1(3)C7(6) - Open Caveats

The following list identifies open caveats in CSG Release 3.1(3)C7(6).

- CSCek75928—CSG: Need to be able to mix type HTTP and no billing policies  
The CSG does not allow the user to configure a content that includes a policy with **accounting type http**, and a policy that does not include an accounting statement.  
**Workaround:** None.

- CSCsc33686—Sessions dropped during RD “wait” when out of quota for **basis seconds** service

The CSG closes all open sessions during a Reauthorization Delay (RD) “wait” state (that is, action code = wait in Reauthorization Delay TLV in most recent Service Authorization Response, Service Reauthorization Response, Quota Push Request, Quota Return Accept, or Service Verification Response message) for a service that is configured with **basis second** service when the quota for that service expires during the wait period.

**Workaround:** None.
- CSCsi14915—Small buffer leak for SMTP traffic

A small buffer leak occurs when running SMTP traffic.

**Workaround:** Change the policy under the SMTP content from **accounting type smtp** to **accounting type other**.
- CSCsi48584—ARP entries shown as LEARNED, DOWN instead of VSERVER, LOCAL

The **show module csg arp** command shows some of the ARP entries as LEARNED, DOWN instead of the correct VSERVER, LOCAL. There is no operational impact.

**Workaround:** None.
- CSCsk49775—The CSG crashes and generates a core dump as a result of a timing issue in the IXPs

The CSG crashes and generates a core dump as a result of a timing issue in the IXPs. The core dump indicates that the network processor was waiting for a memory read operation to complete. The health monitor determined that the IXP was no longer communicating with the PPC, and the PPC forced a reset to prevent a card hang condition.

**Workaround:** None.
- CSCsk51915—Multiprotocol stress: debug messages seen on the standby CSG

When the multiprotocol (HTTP, FTP, RTSP, TCP and WAP) traffic load is high, the standby CSG might receive the following message:

```
Tack! invalid appl ptr 17ad0/203

17ad0/203 src: 40.40.40.2:20 dst: 31.31.11.3:20921 prot: 6
kut index: ip= 31.31.11.3, uid= user22818
flags: NETWORK_INIT POSTPAID TCP_ADJ_NEEDED BACKUP_NEEDED
prepaid: ip bytes up = 0, ip bytes down = 0
tcp bytes up = 0, tcp bytes down = 0
bytes granted = 0, quads consumed = 0
flags = <none>
```

**Workaround:** None.

## CSG Release 3.1(3)C7(6) - Closed Caveats

The following section lists bugs that are closed in CSG Release 3.1(3)C7(6).

- CSCse28514—IOS has mismatch problem with CSG traps - not being sent to NMS agent

CSG-related traps are not being sent to the NMS agent. These are the traps related to changes in states for the BMAs, quota servers, and user database, as well as traps that are generated when records to the BMAs or quota servers are lost.

The CSG cannot generate V1 traps.

- CSCse37975—R7: The CSG resets the client and server for some quota server responses  
Under certain conditions, the CSG might reset both the client and the server.  
For this problem to occur, the following conditions must all be met:
  - The HTTP connection must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
  - The flow must have pipelined GET requests, such that there are at least two complete GETs in the first packet.
  - The Service Authorization Response must arrive within a very narrow time window.
- CSCsh13845—**Tack! invalid appl ptr** debug message on standby CSG

When the FTP traffic load is high, the standby CSG might receive the following message:

**Tack! invalid appl ptr 1fbb12/21e**

```
1fbb12/21e src: 34.0.3.143:28458 dst: 40.40.40.2:21 prot: 6
kut index: <none>
flags: BACKUP_PEND
prepaid: ip bytes up = 0, ip bytes down = 0
tcp bytes up = 0, tcp bytes down = 0
bytes granted = 0, quads consumed = 0
flags = <none>
```

- CSCsh20692—CSG 7x: RTSP tracebacks on backup\_now\_active  
Under heavy load running RTSP traffic, some tracebacks can be seen on the CSG console.
- CSCsh42117—CSG: IPv4 L4 Flow flags field wrong for SMTP transaction  
The persistence flag should be set in the ipv4flow (IPv4 L4 Flow TLV in the CDR) for e-mail protocols for all transactions that end but do not terminate the TCP session. The **NOT CLOSED** flag should also be set in this same condition, as it is for HTTP.
- CSCsh44709—C7.3: PPC exception type 111 on “Refclk Watch(0D710368h)”  
After deleting a VLAN from the configuration, the CSG resets continuously with “error in installing ruleset.” This is working as designed, for contents that are configured in active rulesets.  
When the VLAN is deleted, the CSG takes all contents that reference the VLAN out of service. However, if a content is configured in an active ruleset, the CSG does not remove the content from the ruleset. Then, when the CSG reboots, the ruleset configuration fails and the CSG remains offline.  
To resolve this issue, you must remove the content from the ruleset, then reboot the CSG.
- CSCsh54610—CSG 7.2 prematurely resets FTP sessions  
When running automated FTP tests, 5 to 10% of all tested FTP sessions are prematurely disconnected by the CSG.
- CSCsh64680—HTTP stats CDR generated when billing plan is unknown  
In IPS3.0, when a user has an unknown billing plan due to loss of communication with the CSG, the HTTP statistics CDR might be generated with 0 bytes counted.
- CSCsh69053—Packet log for unparseable packets on the CSG  
The CSG console requires a packet log utility. This utility enables the CSG to log WAP, RTSP, and RADIUS packets (normal and errors).  
The packet log utility can log up to 4096 packets and consumes 6756 KB of memory (allocated as a block, not incrementally).

To select the packets to be logged, use the **pktlog set** console command, with the following options:

- **all**—Log all packets.
- **radius\_err**—Log RADIUS error packets.
- **rtsp\_err**—Log RTSP error packets.
- **rtsp\_pkt**—Log RTSP normal packets.
- **wap\_err**—Log WAP error packets.
- **wap\_pkt**—Log WAP normal packets.

To stop logging selected packets, use the **pktlog clear** console command, with the following options:

- **all**—Stop logging all packets.
- **buffer**—Clears the packet log buffer and deletes all logged packets.
- **radius\_err**—Stop logging RADIUS error packets.
- **rtsp\_err**—Stop logging RTSP error packets.
- **rtsp\_pkt**—Stop logging RTSP normal packets.
- **wap\_err**—Stop logging WAP error packets.
- **wap\_pkt**—Stop logging WAP normal packets.

To display the packet logs, use the **pktlog show** console command, with the following options:

- *captured\_types*—Displays the current packet logging options.
- *ip\_address*—Displays packet logs for the specified IP address.
- *session\_id*—Displays packet logs for the specified session ID.
- **radius\_err**—Displays the RADIUS error packet log.
- **rtsp\_err**—Displays the RTSP error packet log.
- **rtsp\_pkt**—Displays the RTSP normal packet log.
- **wap\_err**—Displays the WAP error packet log.
- **wap\_pkt**—Displays the WAP normal packet log.

By default, the packet log utility is disabled. To enable the packet log utility, the configurable **PKTLOG\_ENABLE** environment variable is added to the CSG. This variable enables (1) or disables (0) the packet log utility. The default setting is 0 (disabled).

The configurable **PKTLOG\_OVERWRITE** environment variable is also added to the CSG. This variable enables the CSG to overwrite packet logs when the buffer is full. To enable the CSG to overwrite packet logs, specify 1 (the default setting). To prevent the CSG from overwriting packet logs, specify 0.

To set these variables, use the **variable** command in module CSG configuration mode.

- CSCsh79224—R7.3 - The CSG might undercharge under certain conditions

The CSG might report a small IP download bytes undercharge for a transaction with **accounting type http**.

For this problem to occur, the following conditions must all be met:

- The HTTP connection must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).

- An HTTP response packet containing an HTTP header must be followed immediately by an HTTP response packet containing data.
- CSCsh80041—TFTP of CSG software under heavy load may result in Active/Active collision  
Under heavy load conditions, while trying to TFTP the CSG software, an Active/Active collision condition might occur. Traffic is disrupted until the duplicate IP address conflict is resolved.
- CSCsh82256— The **undebg all** command is not reflected in the CPU utilization CLI  
If **debug ip csg cpu** has been enabled, entering the **show cpu** command on the CSG console or the **show module csg tech-support utilization** command on the Supervisor displays CPU utilization information even after all debugs have been turned off using the **undebg all** command.
- CSCsi07067—RADIUS messages dropped after configuring or unconfiguring accounting  
The CSG might drop RADIUS messages after configuring or unconfiguring accounting.
- CSCsi08274—CSG unexpected error: Traceback  
The following CSG traceback error might occur on an active CSG:  

```
% CSM_SLB-3-UNEXPECTED: Module 5 unexpected error: Traceback - 0x0025CB8C
0x002029E0 0x00241BE8 0x0020013C 0x00200B0C 0x0004A038 0x001AAE6C
```
- CSCsi49894—Memory leak on standby CSG  
The standby CSG slowly leaks memory, leading to an eventual crash.
- CSCsi54953—CSM\_SLB-3-UNEXPECTED: Module 4 unexpected error: Traceback - 0x0025CB8C  
The following traceback appears in the logs:  

```
% CSM_SLB-3-UNEXPECTED: Module 4 unexpected error:
Traceback - 0x0025CB8C 0x001F6518 0x0025E48C 0x0025E794 0x0025E838
0x001AAE6C
```
- CSCsi62248—The CSG crashes when operating with maximum CPU and memory usage  
The CSG crashes when running under maximum CPU and maximum memory conditions for a period of 2 to 48 hours.
- CSCsi83336—Negative quadrans from the quota server creates a large positive quadrans balance in the CSG  
A user might end up with a large positive quadrans balance when the quota server sends a Service Authorization Response with negative quadrans (-1) for a CSG service.
- CSCsi85656—The CSG does not forward HTTP POSTs that span multiple packets completely  
The CSG does not forward HTTP POSTs that span multiple packets completely.  
For this problem to occur, the following conditions must all be met:
  - The HTTP connection must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
  - The POST must not use “Transfer-Encoding:chunked” or “Content-Type: multipart...”
  - The POST must span multiple packets such that the end of the HTTP header and the end of the complete HTTP message are in separate packets.
- CSCsj01714—**show tech** displays Resource Utilization info twice  
The **show tech** and **show mod csg tech-support** commands might display Resource Utilization twice.

- CSCsj16122—The CSG blocks a GET request under certain timing condition  
The CSG might drop GET requests under certain timing conditions.  
For this problem to occur, the following conditions must all be met:
  - The HTTP connection must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
  - The CSG must receive a FIN from the client while it is waiting for a SYN/ACK from the server.
- CSCsj36402—The CSG allows WAP traffic to pass through despite a service reject from the quota server  
The CSG is allowing WAP 1.x traffic to pass through even if the quota server is denying the service (Quota = 0 quadrans, Cause = 3, Service Denied).  
For this problem to occur, the following conditions must all be met:
  - The WAP 1.x connection must match a CSG content configured with policies that require WAP inspection (**accounting type wap**).
  - The Service Auth/Re-Auth response must have quota = 0 quadrans, Cause = 3.
  - The first packet after the Service Auth/Re-Auth response must not be a REPLY from the server. They are ACKs in the cases where the REPLY is passing through.
- CSCsj39598—Fastblk corruption does not crash the CSG with default value of CSG\_MEM\_ERR\_THRESHOLD  
The active CSG might not fail over to the standby CSG when buffer pools are corrupted with the default value of CSG\_MEM\_ERR\_THRESHOLD.
- CSCsj45257—The CSG shows CDR IP Usage downlink TLV overcharging with HTTP-WAP L7  
The CSG might report an overcharge in the CDR TLV “Service TCP Usage Cumulative Bytes Down”. The overcharge can be up to 20 more than the actual TCP/IP data transferred for a service transaction.  
For this problem to occur, the following conditions must all be met:
  - The HTTP connection must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
  - The packet from the server must use “Transfer-Encoding:chunked”.
  - The chunks must not terminate at packet boundaries.
- CSCsj56218—Add debugs to determine whether the retry timer of a quota server is running  
The queued count of a quota server might increase if the CSG stops retransmitting unacknowledged data requests. This might result in dropped new requests if the queued count reaches the configured maximum records limit.  
For this problem to occur, the following conditions must all be met:
  - The user traffic must be prepaid.
  - The retry count for the quota server must be zero, or it must not be incremented for a long time, even if the CSG has not received an ACK for an already-sent data request to the quota server.
- CSCsj59888—The CSG might overcharge download bytes for the first transaction after an abnormal termination  
The CSG might overcharge download bytes for the first transaction with pipelined GETs after an abnormal termination.  
For this problem to occur, the following conditions must all be met:

- The HTTP connection must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
- The first response from the server must use “Transfer-Encoding:chunked”.
- There must be more than one transaction on the session.
- Before the CSG receives the complete response for the first transaction, the session must terminate.
- CSCsj61839—WAP redirect does not work if the server sends an ACK before a REPLY  
WAP 1.0 redirect does not work if the server sends an ACK before sending a REPLY.  
For this problem to occur, the following conditions must all be met:
  - The WAP 1.x connection must match a CSG content configured with policies that require WAP inspection (**accounting type wap**).
  - Redirect must be configured.
  - An ACK (or some other packet) must precede the packet on which redirect is supposed to occur (GET, POST or REPLY).
- CSCsj89633—The CSG quota usage might become negative, resulting in a reauthorization loop  
The CSG might resend Quota Service Reauthorization Requests in an endless loop for a specific user and a specific service.
- CSCsk34498—The CSG crashes  
The CSG might crash with the following crash signature:

```
!!!CORE DUMP Tue Aug 28 11:31:37 2007
!!!Version: 3.1(3)C7(5)
FPGA1 exception 999 IXIC_ICPAS - iPacket passthrough. ecmd wants to sync.
```

## Caveats for 3.1(3)C7(5)

This section lists and describes all caveats, both open and resolved, that affect CSG software release 3.1(3)C7(5).

For information about open or unresolved caveats in the Content Services Gateway 3.1(3)C7(5) release, refer to the Cisco Bug Toolkit at the following URL:

<http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>.

## CSG Release 3.1(3)C7(5) - Open Caveats

The following list identifies open caveats in CSG Release 3.1(3)C7(5).

- CSCsc33686—Sessions dropped during RD “wait” when out of quota for **basis seconds** service  
The CSG closes all open sessions during a Reauthorization Delay (RD) “wait” state (that is, action code = wait in Reauthorization Delay TLV in most recent Service Authorization Response, Service Reauthorization Response, Quota Push Request, Quota Return Accept, or Service Verification Response message) for a service that is configured with **basis second** service when the quota for that service expires during the wait period.  
**Workaround:** None.

- CSCse28514—IOS has mismatch problem with CSG traps - not being sent to NMS agent  
CSG-related traps are not being sent to the NMS agent. These are the traps related to changes in states for the BMAs, quota servers, and user database, as well as traps that are generated when records to the BMAs or quota servers are lost.

**Workaround:** None.
- CSCse37975—R7: The CSG resets the client and server for some quota server responses  
The CSG might reset both the client and the server. The problem seems to be related to the timing of the second auth\_content\_resp from the quota server.

**Workaround:** None.
- CSCsh20692—CSG 7x: RTSP tracebacks on backup\_now\_active  
Under heavy load running RTSP traffic, some tracebacks can be seen on the CSG console.

**Workaround:** None.
- CSCsh44709—C7.3: PPC exception type 111 on “Refclk Watch(0D710368h)”  
The CSG resets continuously with “error in installing ruleset.” This condition can occur if there are VLAN configurations under contents, but the actual VLANs do not exist.

**Workaround:** Either create the VLANs included under the content, or remove the contents with faulty configurations from the ruleset.
- CSCsh54610—CSG 7.2 prematurely resets FTP sessions  
When running automated FTP tests, 5 to 10% of all tested FTP sessions are prematurely disconnected by the CSG.

**Workaround:** None.
- CSCsh64680—HTTP stats CDR generated when billing plan is unknown  
In IPS3.0, when a user has an unknown billing plan due to loss of communication with the CSG, the HTTP statistics CDR might be generated with 0 bytes counted.

**Workaround:** Configure the BMA to drop the HTTP statistics CDR if this occurs.
- CSCsh79224—R7.3 - The CSG might undercharge under certain conditions  
The CSG might report a small IP download bytes undercharge for a transaction with **accounting type http**.

For this problem to occur, the following conditions must all be met:

  - The HTTP connection must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
  - An HTTP response packet containing an HTTP header must be followed immediately by an HTTP response packet containing data.

**Workaround:** None.
- CSCsh80041—TFTP of CSG software under heavy load may result in Active/Active collision  
Under heavy load conditions, while trying to TFTP the CSG software, an Active/Active collision condition might occur. Traffic is disrupted until the duplicate IP address conflict is resolved.

**Workaround:** Perform CSG software upgrades during off-peak hours.

- CSCsh82256— The **undebug all** command is not reflected in the CPU utilization CLI  
If **debug ip csg cpu** has been enabled, entering the **show cpu** command on the CSG console or the **show module csg tech-support utilization** command on the Supervisor displays CPU utilization information even after all debugs have been turned off using the **undebug all** command.  
**Workaround:** Explicitly turn off the debugs using the **no debug ip csg cpu** command.
- CSCsi07067—RADIUS messages dropped after configuring or unconfiguring accounting  
The CSG might drop RADIUS messages after configuring or unconfiguring accounting.  
**Workaround:** Reload the CSG.
- CSCsi08274—CSG unexpected error: Traceback  
The following CSG traceback error might occur on an active CSG:  

```
% CSM_SLB-3-UNEXPECTED: Module 5 unexpected error: Traceback - 0x0025CB8C
0x002029E0 0x00241BE8 0x0020013C 0x00200B0C 0x0004A038 0x001AAE6C
```

  
**Workaround:** None.
- CSCsi14915—Small buffer leak for SMTP traffic  
A small buffer leak occurs when running SMTP traffic.  
**Workaround:** Change the policy under the SMTP content from **accounting type smtp** to **accounting type other**.
- CSCsi48584—ARP entries shown as LEARNED, DOWN instead of VSERVER, LOCAL  
The **show module csg arp** command shows some of the ARP entries as LEARNED, DOWN instead of the correct VSERVER, LOCAL. There is no operational impact.  
**Workaround:** None.
- CSCsi49894—Memory leak on standby CSG  
The standby CSG slowly leaks memory, leading to an eventual crash.  
**Workaround:** None.
- CSCsi54953—CSM\_SLB-3-UNEXPECTED: Module 4 unexpected error: Traceback - 0x0025CB8C  
The following traceback appears in the logs:  

```
% CSM_SLB-3-UNEXPECTED: Module 4 unexpected error:
Traceback - 0x0025CB8C 0x001F6518 0x0025E48C 0x0025E794 0x0025E838
0x001AAE6C
```

  
**Workaround:** None.

## CSG Release 3.1(3)C7(5) - Closed Caveats

The following section lists bugs that are closed in CSG Release 3.1(3)C7(5).

- CSCek69332—The CSG observed throughput decrease with large CDR backlog to the PSD  
When the CSG has exceeded its CPU capacity, it might drop GTP' ACKs and lose communication with the BMA or the PSD.  
As part of the CSG's health monitoring process, the CSG monitors itself for low CPU conditions.
  - If CSG CPU usage exceeds a user-specified warning threshold, the CSG issues the following message:

**%CSM\_SLB-3-ERROR: Module 3 error: WARN - CSG cpu exceeded 90.0%(91.1%)**

By default, the CSG issues this warning message when CPU usage exceeds 90%. (The second number is the current CSG CPU one-minute average usage.) To change that threshold, change the setting of the **CSG\_CPU\_WARN\_THRESHOLD** variable. The range for this variable is 1 to 95; the default setting is 90.

By default, the CSG issues this warning message once a minute after the threshold has been exceeded. To change the time between warning messages, change the setting of the **CSG\_CPU\_WARN\_FREQUENCY** variable. The range for the variable is 1 to 95; the default setting is 5.

- If CSG CPU usage exceeds a user-specified depletion threshold, the CSG issues the following message:

**%CSM\_SLB-3-ERROR: Module 3 error: CRITICAL - CSG max cpu reached 95.0%(96.1%)**

By default, the CSG issues this depletion message when CPU usage exceeds 95%. (The second number is the current CSG CPU one-minute average usage.) To change that threshold, change the setting of the **CSG\_CPU\_MAX\_THRESHOLD** variable. The range for this variable is 1 to 95; the default setting is 95.

By default, the CSG issues this depletion message once a minute after the threshold has been exceeded. To change the time between depletion messages, change the setting of the **CSG\_CPU\_MAX\_FREQUENCY** variable. The range for the variable is 1 to 95; the default setting is 1.

To set these variables, use the **variable** command in module CSG configuration mode.

- CSCek70725—CSG: RADIUS monitor error counter not correct  
The RADIUS monitor error counters **unable to send to client** and **unable to send to server** might be incremented even when there is no SEND failure.
- CSCek70734—CSG: Enable the capture function  
To enable the CSG to display all messages to the CSG console in the current session, use the **capture** command on the CSG console.
  - Use **capture on** to enable capture.
  - Use **capture off** to disable capture.
- CSCek70871—CSG: Malformed RADIUS message might cause crash  
A malformed RADIUS message might cause the CSG to crash.
- CSCek71453—CSG: Cannot parse unknown VSAs  
The CSG might be unable to parse a RADIUS VSA if the format does not follow RFC 2865. This might result in a user not being added to the User Table.
- CSCek71464—Smooth the GTP process for draining CDRs from the PSD  
As part of the BMA recovery process, the CSG drains CDRs from the PSD and forwards them to the BMA. In a high-traffic environment, this drainage might degrade the throughput of incoming traffic, and could even bring down the CSG.  
To help avoid this problem, the configurable **CSG\_GTP\_DRAIN\_DELAY** environment variable is added to the CSG. This variable enables the user to adjust the GTP PSD drain delay. The range is 0 seconds to 3 seconds. The default setting is 1 second.

The configurable **CSG\_GTP\_DRAIN\_PKT** environment variable is also added to the CSG. This variable enables the user to specify how many packets the CSG is to drain for each delay. The range is 1 packet to 100 packets. The default setting is 2 packets.

To set these variables, use the **variable** command in module CSG configuration mode.

- CSCek71916—CSG: Allow ping request to be sent to RADIUS monitor server  
RADIUS monitor support is enhanced to allow a ping request to be forwarded to the configured server (if there is a configured content to match the flow).
- CSCek72616—PPC exception type 122 on core\_dump(0CC65E70h)  
The CSG might receive a partial coredump when detecting an internal error.
- CSCek74170—High CPU utilization  
Changes to the CSG CPU normalization factor trigger the reporting of higher than expected CPU utilization values.
- CSCsg20166—The billing queue overflows when the CSG is under control and data load  
Under heavy traffic and heavy user activation and deactivation, the CSG generates trace messages and billing queue overflow messages.
- CSCsh43473—The CSG suffers an outage and reloads when some URLs are added  
The CSG resets while adding or modifying policies in a live network.  
For this problem to occur, the following conditions must all be met:
  - There must be HTTP, WAP or RTSP traffic flowing through the CSG.
  - The URL and header maps must be complex.
- CSCsh56109—The CSG drops quota server requests if the source port is not configured  
The CSG does not process requests from the quota server if the source port in the request packet is not the quota server port configured in the CSG.
- CSCsh80143—CSG: Large or incorrect time usage reported for WAP1.x service  
For WAP 1.x traffic that matches a CSG content-policy pair that is configured for **accounting type wap**, the CSG might report a large value, or an incorrect value, for “Interval Usage Seconds” in the Service Stop message.
  - If the **accounting** command in CSG policy configuration mode is configured with **wap connectionless** or **wap connection-oriented**, and **basis bytes** is configured in CSG service configuration mode, the CSG reports a large value for “Interval Usage Seconds”.
  - If the **accounting** command in CSG policy configuration mode is configured with **wap connectionless** or **wap connection-oriented**, and **basis second** is configured in CSG service configuration mode, the CSG requests quota after 2 seconds, and reports incorrect values in the Service Stop message. The CSG does not report a large value for “Interval Usage Seconds”.

## Caveats for 3.1(3)C7(4)

This section lists and describes all caveats, both open and resolved, that affect CSG software release 3.1(3)C7(4).

For information about open or unresolved caveats in the Content Services Gateway 3.1(3)C7(4) release, refer to the Cisco Bug Toolkit at the following URL:

<http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>.

## CSG Release 3.1(3)C7(4) - Open Caveats

The following list identifies open caveats in CSG Release 3.1(3)C7(4).

- CSCsc33686—Sessions dropped during RD “wait” when out of quota for **basis seconds** service

The CSG closes all open sessions during a Reauthorization Delay (RD) “wait” state (that is, action code = wait in Reauthorization Delay TLV in most recent Service Authorization Response, Service Reauthorization Response, Quota Push Request, Quota Return Accept, or Service Verification Response message) for a service that is configured with **basis second** service when the quota for that service expires during the wait period.

**Workaround:** None.
- CSCse28514—IOS has mismatch problem with CSG traps - not being sent to NMS agent

CSG-related traps are not being sent to the NMS agent. These are the traps related to changes in states for the BMAs, quota servers, and user database, as well as traps that are generated when records to the BMAs or quota servers are lost.

**Workaround:** None.
- CSCse37975—R7: The CSG resets the client and server for some quota server responses

The CSG might reset both the client and the server. The problem seems to be related to the timing of the second auth\_content\_resp from the quota server.

**Workaround:** None.
- CSCsg20166—The billing queue overflows when the CSG is under control and data load

Under heavy traffic and heavy user activation and deactivation, the CSG generates trace messages and billing queue overflow messages.

**Workaround:** None.
- CSCsh20692—CSG 7x: RTSP tracebacks on backup\_now\_active

Under heavy load running RTSP traffic, some tracebacks can be seen on the CSG console.

**Workaround:** None.
- CSCsh43473—The CSG suffers an outage and reloads when some URLs are added

The CSG resets while adding or modifying policies in a live network.

For this problem to occur, the following conditions must all be met:

  - There must be HTTP, WAP or RTSP traffic flowing through the CSG.
  - The URL and header maps must be complex.

**Workaround:** Add or modify policies during off-peak hours.
- CSCsh44709—C7.3: PPC exception type 111 on “Refclk Watch(0D710368h)”

The CSG resets continuously with “error in installing ruleset.” This condition can occur if there are VLAN configurations under contents, but the actual VLANs do not exist.

**Workaround:** Either create the VLANs included under the content, or remove the contents with faulty configurations from the ruleset.
- CSCsh54610—CSG 7.2 prematurely resets FTP sessions

When running automated FTP tests, 5 to 10% of all tested FTP sessions are prematurely disconnected by the CSG.

**Workaround:** None.

- CSCsh56109—The CSG drops quota server requests if the source port is not configured  
The CSG does not process requests from the quota server if the source port in the request packet is not the quota server port configured in the CSG.  
**Workaround:** Ensure that the quota server uses the configured port as the source port when sending requests to the CSG.
- CSCsh64680—HTTP stats CDR generated when billing plan is unknown  
In IPS3.0, when a user has an unknown billing plan due to loss of communication with the CSG, the HTTP statistics CDR might be generated with 0 bytes counted.  
**Workaround:** Configure the BMA to drop the HTTP statistics CDR if this occurs.
- CSCsh79224—R7.3 - The CSG might undercharge under certain conditions  
The CSG might report a small IP download bytes undercharge for a transaction with **accounting type http**.  
For this problem to occur, the following conditions must all be met:
  - The HTTP connection must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
  - An HTTP response packet containing an HTTP header must be followed immediately by an HTTP response packet containing data.**Workaround:** None.
- CSCsh80041—TFTP of CSG software under heavy load may result in Active/Active collision  
Under heavy load conditions, while trying to TFTP the CSG software, an Active/Active collision condition might occur. Traffic is disrupted until the duplicate IP address conflict is resolved.  
**Workaround:** Perform CSG software upgrades during off-peak hours.
- CSCsh80143—CSG: Large or incorrect time usage reported for WAP1.x service  
For WAP 1.x traffic that matches a CSG content-policy pair that is configured for **accounting type wap**, the CSG might report a large value, or an incorrect value, for “Interval Usage Seconds” in the Service Stop message.
  - If the **accounting** command in CSG policy configuration mode is configured with **wap connectionless** or **wap connection-oriented**, and **basis bytes** is configured in CSG service configuration mode, the CSG reports a large value for “Interval Usage Seconds”.
  - If the **accounting** command in CSG policy configuration mode is configured with **wap connectionless** or **wap connection-oriented**, and **basis second** is configured in CSG service configuration mode, the CSG requests quota after 2 seconds, and reports incorrect values in the Service Stop message. The CSG does not report a large value for “Interval Usage Seconds”.**Workaround:** Configure **accounting type other** for the WAP policy.

## CSG Release 3.1(3)C7(4) - Closed Caveats

The following section lists bugs that are closed in CSG Release 3.1(3)C7(4).

- CSCeg04168—Need MSS configuration option for servers with MSS below 1460  
When the CSG is operating in half-proxy mode (**accounting type http**), it is necessary to advertise a Maximum Segment Size (MSS) value when establishing a TCP connection with the client. Once the first HTTP transaction is received, the CSG then establishes a TCP connection with the server.

If the server returns an MSS value less than initially advertised by the CSG to the client, datagrams with a size in excess of what the server can handle might be sent by the client. These datagrams are then dropped by the server.

To help avoid this problem, the configurable **CSG\_SET\_MSS** environment variable is added to the CSG. This variable enables the user to set the MSS, in bytes. The range is 1 byte to 1432 bytes. The default setting is 1432 bytes.

To set this variable, use the **variable** command in module CSG configuration mode.

- CSCse35909—CSG Server-initiated FTP and RTSP might not work with next hop configured  
A server- initiated data connection for FTP (active FTP) and RTP stream (RTP sessions initiated from the server) might not work when an FTP or RTSP policy is configured for next hop.  
For this problem to occur, the following conditions must all be met:
  - The client must initiate a control session that matches a policy that is configured with next hop.
  - The control connection must generate a data session.
  - The data session must be initiated by the server.
  - The data session must match the policy that is configured with next hop.
- CSCse61960—The CSG sends service reauthorizations too frequently if the HTTP content-length is incorrect  
The CSG sends Service Reauthorization Request messages too frequently for a prepaid subscriber, even when there is unused quota. Such behavior can overwhelm the quota server and interrupt service. The problem occurs when HTTP 1.1 pipelined traffic with the wrong Content-length is transferred over the user session.
- CSCsf32312—A ping from the CSG is needed to populate the ARP table after removing the **gateway** command  
When you remove the **gateway** command from the CSG's client VLAN, the next hop specified in the command is also removed from the ARP table. Normal traffic does not restore the ARP entry.  
This problem could not be reproduced.
- CSCsg31280—HTTP traffic causes buffer leak  
When an HTTP stream containing a mix of fragmented and non-fragmented IP packets matches a content and policy with **accounting type http**, the CSG might experience a buffer leak and drop all traffic.  
For this problem to occur, the following conditions must all be met:
  - The HTTP connection must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
  - The CSG must receive an HTTP packet which is the first packet of a transaction.
  - The HTTP packet must be followed by another HTTP packet which is fragmented before it reaches the CSG.
- CSCsg88123—The CSG resets the FTP data connection after failover with **csg\_ftp\_pwd=1** configured  
If variable **CSG\_FTP\_PWD = 1** is configured, the CSG resets the FTP data connection after a failover.

- CSCsg93384—Backpressure from the Cisco Catalyst 6500 series switch backplane can cause NAT lockup

If there is a large amount of backpressure from the Cisco Catalyst 6500 series switch backplane, resulting in “TX Window full” and “TX FIFO full” statistics incrementing on the **show mod csm tech proc** command, the NAT processor might stop handling traffic, causing an eventual core dump.

- CSCsh02265—CSG: Add defensive checks to drop malformed TCP packets

The CSG can behave unpredictably when certain types of TCP packets are received.

TCP packets with the following TCP flags can cause problems:

- SYN-FIN
- SYN-RST
- FIN-RST
- SYN-FIN-RST

Also, packets in which the IP packet length is less than sum of the IP header length and the TCP header length can cause problems.

- CSCsh21841—The CSG does not process buffered packets during PWD command transaction

If variable `CSG_FTP_PWD` is set to its default value (0), the CSG does not process buffered packets during PWD command transaction. If the buffered command is PORT from the client, then one of the following conditions might occur:

- If there is no content configured for handling a data-initiated connection, the data connection is not set up.
- If there is a content configured for handling data-initiated connection, the data connection is set up when this content is encountered, while the control connection might be seen for FTP-specific content.

For this problem to occur, the following conditions must all be met:

- Variable `CSG_FTP_PWD` must be set to its default value (0).
- The CSG must buffer a packet from the client and send the PWD command to the server.
- After receiving the response for the PWD command from the server, the CSG must forward the buffered packet to the server without processing it.

- CSCsh26852—CSG: Certain HTTP traffic causes Layer 7 Free Session Objects exhaustion

The CSG might send a TCP reset for an HTTP request that spans more than one packet.

For this problem to occur, the following conditions must all be met:

- The HTTP connection must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
- There must be instances of the policy array filling up.
- The CSG must receive an HTTP request that spans more than one packet.

- CSCsh38000—PPC exception type 512 on “BillingStack(0D784578h)”

When WAP 1.x/WSP traffic matches a content and policy with **accounting type wap**, the CSG might crash, with the system logs showing “PPC exception”.

For this problem to occur, one of the following sets of conditions must be met:

Condition 1:

- The WAP 1.x connection must match a CSG content configured with policies that require WAP inspection (**accounting type wap**).
- The CSG must receive IP fragments, and the combined length of the reassembled IP datagram must be greater than 1500 bytes.
- The reassembled WAP packet must contain concatenated PDUs.
- At least one of the concatenated PDUs must have a length greater than 1472, such that the complete IP packet formed from the that concatenated PDU, plus the IP header, plus the UDP, is greater than 1500 bytes.

## Condition 2.

- The WAP 1.x connection must match a CSG content configured with policies that require WAP inspection (**accounting type wap**).
- The CSG must receive a WAP packet which has a UDP payload of less than 4 bytes; or which has concatenated PDUs, one of which has a payload of less than 4 bytes.
- The WTP header must identify the WAP packet as a segmented INVOKE.
- The WAP packet must not be the first WAP segment.

To help avoid this problem, the configurable **CSG\_MEM\_ERR\_THRESHOLD** environment variable is added to the CSG. This variable enables the user to set the number of memory errors to allow before failing over to the backup CSG. When the threshold is reached, the CSG dumps the memory that is in error to the logs and dumps the buffer pools to the CSG console. The range is 0 errors to 10000 errors. The default setting is 5 errors.

The configurable **DUMP\_BAD\_WAP\_PACKET** environment variable is also added to the CSG. This variable enables the CSG to dump WAP packets that cannot be parsed to the system logs, if debugging is enabled from the VENUS# console. We recommend that you configure this variable only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. The range is 0 (do not dump any WAP packets to the system logs) to 100 (dump the first 100 WAP packets that cannot be parsed). The default setting is 5 (dump the first 5 WAP packets that cannot be parsed).

To set these variables, use the **variable** command in module CSG configuration mode.

- CSCsh51432—CSG 7.3 is overcharging user WAP2/HTTP traffic

In some situations, the CSG is overcharging for WAP2/HTTP traffic.

- CSCsh52926—Limit allocation taken by csg\_string\_table

When WAP 1.x/WSP traffic matches a content and policy with **accounting type wap**, the CSG might lose memory gradually.

For this problem to occur, the following conditions must all be met:

- The WAP 1.x connection must match a CSG content configured with policies that require WAP inspection (**accounting type wap**).
- The WAP packet must have header User-Agent or Content-Type.
- Each different instance of User-Agent or Content-Type must be stored in memory.
- If requests have a different string for these headers, it can cause available memory to decrease gradually.

- CSCsh53004—Cannot send e-mail with an attachment greater than 100 KB with HTTP accounting  
The user cannot send large HTTP POSTs (larger than 1000 KB).

For this problem to occur, the following conditions must all be met:

- The HTTP connection must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
- The HTTP payload must be large, approximately 100 KB or larger.
- The HTTP POST must use multipart or chunked.

To help avoid this problem, the configurable **CSG\_MAX\_POST\_LENGTH** environment variable is added to the CSG. This variable enables the user to set the maximum HTTP POST size, in bytes, to be buffered by the CSG. The range is 0 byte to 10485760 bytes. The default setting is 65536 bytes.

To set this variable, use the **variable** command in module CSG configuration mode.

- CSCsh62718—Block leak in system testbed running HTTP

The CSG cannot forward some traffic or session/connection failures, especially for HTTP and WAP 2.0.

- CSCsh65780—R7.3 - The CSG might not report a constant window under certain conditions

The CSG does not always send an ACK to a client with windows-size set to 8192.

For this problem to occur, the following conditions must all be met:

- The HTTP connection must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
- The CSG release must be Release 3.1(3)C7(3). Prior to CSG Release 3.1(3)C7(3), constant window-size was not implemented.

- CSCsh69444—The CSG is overcharging on downlink WAP2/HTTP traffic

The CSG overcharges slightly for a transaction in IP download bytes reported with **accounting type http**. The overcharge is for the IP downlink bytes; the TCP downlink bytes are charged correctly.

For this problem to occur, the following conditions must all be met:

- The HTTP connection must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
- An HTTP response packet containing HTTP header must be immediately be followed by an HTTP response packet containing data. The CSG counts the HTTP data packet twice.

- CSCsh75948—Fragmented chunked response handling incorrect in tcp\_term

An HTTP server stream with fragmented IP packets might be downgraded to Layer 4 accounting.

For this problem to occur, the following conditions must all be met:

- The HTTP connection must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
- The server-side stream must have IP fragments.
- The IP fragments must be part of an HTTP packet that has an HTTP header.
- The response from the server must be multipart or chunked.

- CSCsh77334—System logs generated on packet drops enabled only from environment variable

In normal operation, the CSG does not print a warning message when it drops packets that cannot be forwarded as a result of parsing errors.

To enable the CSG to print warning messages, the configurable **CSG\_WARN\_PKTDROP\_ERR** environment variable is added to the CSG. If the **CSG\_WARN\_PKTDROP\_ERR** variable is enabled (set to 1), the CSG prints a warning message when it drops packets that cannot be parsed. Otherwise (set to 0, the default setting), the CSG does not print a warning messages.

The configurable `CSG_PKTDROP_WARN_FREQUENCY` environment variable is also added to the CSG. If the `CSG_WARN_PKTDROP_ERR` variable is enabled (set to 1), this variable enables the user to set the frequency of packet drop warning messages, in seconds. The range is 60 seconds (log one message every minute) to 86400 seconds (log one message every 24 hours). The default setting is 300 seconds (log one message every five minutes).

To set these variables, use the **variable** command in module CSG configuration mode.

## Caveats for 3.1(3)C7(3)

This section lists and describes all caveats, both open and resolved, that affect CSG software release 3.1(3)C7(3).

For information about open or unresolved caveats in the Content Services Gateway 3.1(3)C7(3) release, refer to the Cisco Bug Toolkit at the following URL:

<http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>.

## CSG Release 3.1(3)C7(3) - Open Caveats

The following list identifies open caveats in CSG Release 3.1(3)C7(3).

- CSCsc33686**—Sessions dropped during RD “wait” when out of quota for **basis seconds** service

The CSG closes all open sessions during a Reauthorization Delay (RD) “wait” state (that is, action code = wait in Reauthorization Delay TLV in most recent Service Authorization Response, Service Reauthorization Response, Quota Push Request, Quota Return Accept, or Service Verification Response message) for a service that is configured with **basis second** service when the quota for that service expires during the wait period.

**Workaround:** None.
- CSCse35909**—CSG Server-initiated FTP and RTSP might not work with next hop configured

A server- initiated data connection for FTP (active FTP) and RTP stream (RTP sessions initiated from the server) might not work when an FTP or RTSP policy is configured for next hop.

For this problem to occur, the following conditions must all be met:

  - The client must initiate a control session that matches a policy that is configured with next hop.
  - The control connection must generate a data session.
  - The data session must be initiated by the server.
  - The data session must match the policy that is configured with next hop.

**Workaround:** To avoid this problem, take the following steps:

- Define two policies for FTP under the same content, one with next hop (for example, PFTP) and the other without next hop (for example, PFTP\_SI).
- In policy PFTP, define a client-group with an access list (ACL) that points to a group of client-side IP addresses:

```
ip csg policy PFTP
  accounting type ftp customer-string ftp-string
  client-group CI
  next-hop 150.76.50.110
!
ip csg policy PFTP_SI
```

```

accounting type ftp customer-string ftp-string

ip access-list standard CI
 permit 50.76.50.0 0.0.0.255

```

With this configuration, the control session (initiated from the client) matches PFTP, the policy that is configured with next hop, and the data session (initiated from the server) matches PFTP\_SI, the policy that is configured without next hop.

- CSCse37975—R7: The CSG resets the client and server for some quota server responses  
The CSG might reset both the client and the server. The problem seems to be related to the timing of the second auth\_content\_resp from the quota server.  
**Workaround:** None.
- CSCse61960—The CSG sends service reauthorizations too frequently if the HTTP content-length is incorrect  
The CSG sends Service Reauthorization Request messages too frequently for a prepaid subscriber, even when there is unused quota. Such behavior can overwhelm the quota server and interrupt service. The problem occurs when HTTP 1.1 pipelined traffic with the wrong Content-length is transferred over the user session.  
**Workaround:** None.
- CSCsf32312—A ping from the CSG is needed to populate the ARP table after removing the gateway command  
When you remove the **gateway** command from the CSG's client VLAN, the next hop specified in the command is also removed from the ARP table. Normal traffic does not restore the ARP entry.  
**Workaround:** Ping the attached device from the CSG to populate the ARP table with the ARP entry.
- CSCsg20166—The billing queue overflows when the CSG is under control and data load  
Under heavy traffic and heavy user activation and deactivation, the CSG generates trace messages and billing queue overflow messages.  
**Workaround:** None.
- CSCsg88123—The CSG resets the FTP data connection after failover with csg\_ftp\_pwd=1 configured  
If variable CSG\_FTP\_PWD = 1 is configured, the CSG resets the FTP data connection after a failover.  
**Workaround:** Remove variable CSG\_FTP\_PWD = 1 from the configuration.
- CSCsh02265—CSG: Add defensive checks to drop malformed TCP packets  
The CSG can behave unpredictably when certain types of TCP packets are received.  
TCP packets with the following TCP flags can cause problems:
  - SYN-FIN
  - SYN-RST
  - FIN-RST
  - SYN-FIN-RST
 Also, packets in which the IP packet length is less than sum of the IP header length and the TCP header length can cause problems.  
**Workaround:** To avoid the TCP flag problem, install a firewall in front of the CSG to drop malformed packets. There is no workaround for the packet length problem.

- CSCsh20692—CSG 7x: RTSP tracebacks on backup\_now\_active  
Under heavy load running RTSP traffic, some tracebacks can be seen on the CSG console.  
**Workaround:** None.
- CSCsh21841—The CSG does not process buffered packets during PWD command transaction  
If variable CSG\_FTP\_PWD is set to its default value (0), the CSG does not process buffered packets during PWD command transaction.  
If the buffered command is PORT from the client, then one of the following conditions might occur:
  - If there is no content configured for handling a data-initiated connection, the data connection is not set up.
  - If there is a content configured for handling data-initiated connection, the data connection is set up when this content is encountered, while the control connection might be seen for FTP-specific content.
 For this problem to occur, the following conditions must all be met:
  - Variable CSG\_FTP\_PWD must be set to its default value (0).
  - The CSG must buffer a packet from the client and send the PWD command to the server.
  - After receiving the response for the PWD command from the server, the CSG must forward the buffered packet to the server without processing it.**Workaround:** Configure variable CSG\_FTP\_PWD = 1.

## CSG Release 3.1(3)C7(3) - Closed Caveats

The following section lists bugs that are closed in CSG Release 3.1(3)C7(3).

- CSCsd92612—Crash in timerwheel when taking accounting out-of-service while RTSP traffic  
If you are running RTSP traffic (RTP UDP) through the CSG with RTSP filtering configured, and you take accounting out-of-service while there are active RTSP session, the CSG can crash.
- CSCsf17014—R7: Out-of-order HTTP server packets might result in an overcharge  
Out-of-order HTTP packets from the server might result in an overcharge.  
For this problem to occur, all of the following conditions must be met:
  - The HTTP connection must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
  - The policies must be configured with **basis byte ip**.
  - The CSG must receive out-of-order response packets from the server.
  - The CSG must receive the same number of responses as requests.
- CSCsf30387—The CSG crashes with improper RTSP flows  
When the CSG receives RTSP packets that do not end with Ctrl-F Ctrl-F, the CSG might crash while cleaning up these improper RTSP flow connections. This can also occur when all of the RTSP flows use the same session ID.  
If this occurs, the log shows the following messages:
 

```
%CSM_SLB-3-UNEXPECTED: Module 4 unexpected error: PPC exception encountered.
%CSM_SLB-3-UNEXPECTED: Module 4 unexpected error:
Rebooting....
```

- CSCsg23474—The CSG drops WAP 1.x Connect messages for redirect  
Redirect might fail with WAP 1.x connection-oriented sessions when a user is out of balance.  
For this problem to occur, the following conditions must all be met:
  - The user must be out of quota.
  - WAP 1.x connect messages must be redirected.
  - The CSG service must be out-of-balance and must have a catch-all content/policy that matches the WAP 1.x Connect messages.
- CSCsg28997—The CSG stops forwarding traffic when it runs out of buffers  
When handling RADIUS, WAP, and HTTP traffic with IP fragmentation, the CSG might stop forwarding traffic when it runs out of buffers.
- CSCsg35716—The CSG blocks the FTP client ACK when a retransmission of the PASV response is received  
If the FTP data connection is running in passive mode, the CSG might drop FTP data packets when the FTP server retransmits the PASV response during the data connection handshake.
- CSCsg48794—The CSG crashes on FPGA1 exception 999 IXIC\_ICPAS - iPacket passthrough. ecmd  
A CSG running Release 3.1(3)C7(2) and SUP720 Release 12.2(18)SXF6 used in Layer 7 Traffic Authorization mode can crash with the next crash error:
 

```
!!!CORE DUMP WED OCT 25 05:23:27 2006
!!!Version: 3.1(3)C7(2)
FPGA1 exception 999 IXIC_ICPAS - iPacket passthrough. ecmd wants to sync.
```

 Even when running in fault-tolerant mode, both CSGs can crash immediately.
- CSCsg48910—R7: After a POST with a bad boundary, the CSG does not forward subsequent POSTs  
The CSG does not forward some HTTP requests.  
For this problem to occur, the following conditions must all be met:
  - The CSG software used must be at Release 3.1(3)C7(1) or later.
  - There must be some HTTP POSTs that have Content-Type: Multipart.
  - The multipart POSTs must not be RFC-compliant. That is, the boundary strings in header and content must not match, and there must be an epilogue in the POST.
 To help avoid this problem, the configurable `CSG_MULTIPART_DISABLE` environment variable is added to the CSG. In normal operation, the CSG analyzes and buffers a multipart POST completely before forwarding it to the server. When the `CSG_MULTIPART_DISABLE` variable is enabled (set to 1), the CSG downgrades HTTP multipart sessions to Layer 4 accounting, and the CSG stops analyzing the POST when it identifies the the “Content-Type: multipart” header.  
The configurable `CSG_CHUNKED_DISABLE` environment variable is also added to the CSG. In normal operation, the CSG analyzes and buffers a chunked transfer encoding POST completely before forwarding it to the server. When the `CSG_CHUNKED_DISABLE` variable is enabled (set to 1), the CSG downgrades HTTP chunked transfer encoding sessions to Layer 4 accounting, and the CSG stops analyzing the POST when it identifies the “Transfer-Encoding:chunked” header.

The `CSG_MULTIPART_DISABLE` and `CSG_CHUNKED_DISABLE` variables are useful when clients and servers do not conform to the RFC, or when servers are not able to keep up with the complete POST that the CSG sends. We recommend that you keep these variables disabled (set to 0, the default setting) unless multipart or chunked transfer encoding POSTs are not going through. To set these variables, use the **variable** command in module CSG configuration mode.

- CSCsg53479—An HTTP chunked POST gets stuck after the CSG sends an ACK with a zero window  
With accounting-type HTTP configured for the relevant content, the CSG sends an ACK to the client with zero window size.
- CSCsg54466—CSG R7.2-5: Undercharging for HTTP 1.1 pipelined traffic  
When processing HTTP 1.1 pipelining traffic, the CSG can undercharge both upload and download IP byte counts. The CSG might not be able to analyze the server responses to pipelined requests when it encounters the following types of packets:
  - A malformed response packet
  - A response packet with the wrong content length
  - A multipart response packet with an epilogue
- CSCsg54549—R7: Reauthorization requested when sufficient quota is available  
The CSG might send a Service Reauthorization even if there is sufficient quota available. This can occur when a quota server sends a Reauthorization Delay along with non-zero granted quadrans in one of the following messages:
  - Service Authorization Response
  - Service Verification Response
  - Quota Push Request
 In this situation, the CSG cannot handle the delay properly.
- CSCsg74682—IP bytes charged to wrong policy for chunk data  
The CSG might charge IP bytes to a previous policy for HTTP “Transfer-Encoding:chunked” packets. This can occur when the CSG receives HTTP Transfer-Encoding:chunked” packets DATA0, DATA1, DATA2, DATA3 in sequence from the server. DATA0 contains the HTTP header and the chunk length for a chunk of data that spans DATA1, DATA2 and part of DATA3. In this situation, the CSG charges the IP header of DATA0 and DATA3 to the current policy, and charges DATA1 and DATA2 to the previous policy.
- CSCsg84500—The CSG reports high CPU  
The CSG CPU load is extremely high (85%) with a low number of subscribers and low traffic.
- CSCsg90553—CSG7.x: The CSG crashes with an FPGA2 ingress queue full error  
The CSG crashes with WAP/UDP traffic with IP fragmentation. This crash can occur in either of the following scenarios:
  - When the header fragment and the trailer fragment arrive at the CSG almost simultaneously.
  - When there are allocation failures for WAP fragments.
- CSCsg90652—R7: The CSG loops and crashes when receiving a retransmitted packet  
When the CSG handles pipelined HTTP GET requests with more than 16 GET's, and a retransmitted packet arrives that precedes the last 16 GET's, the CSG goes into a loop, stops forwarding traffic, crashes, and resets.

- CSCsh17103—Fix Null pointer access in CSG  
The CSG can crash when it encounters spurious memory accesses. The CSG does not crash when it encounters a NULL pointer access, so when the code does not check the NULL pointer, the CSG can encounter a random memory corruption and crash.
- CSCsh17169—Crash with exception 999 with WAP/UDP fragments  
The CSG can crash when it encounters WAP/UDP traffic with IP fragmentation. The crash can occur when the header fragment and the trailer fragment arrive at the CSG almost simultaneously.

## Caveats for 3.1(3)C7(2)

This section lists and describes all caveats, both open and resolved, that affect CSG software release 3.1(3)C7(2).

For information about open or unresolved caveats in the Content Services Gateway 3.1(3)C7(2) release, refer to the Cisco Bug Toolkit at the following URL:

<http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>.

## CSG Release 3.1(3)C7(2) - Open Caveats

The following list identifies open caveats in CSG Release 3.1(3)C7(2).

- CSCsd92612—Crash in timerwheel when taking accounting out-of-service while RTSP traffic  
If you are running RTSP traffic (RTP UDP) through the CSG with RTSP filtering configured, and you take accounting out-of-service while there are active RTSP session, the CSG can crash.  
**Workaround:** Do not take accounting out-of-service while there are active RTSP sessions.
- CSCse35909—CSG Server-initiated FTP and RTSP might not work with next hop configured  
A server- initiated data connection for FTP (active FTP) and RTP stream (RTP sessions initiated from the server) might not work when an FTP or RTSP policy is configured for next hop.  
For this problem to occur, the following conditions must all be met:
  - The client must initiate a control session that matches a policy that is configured with next hop.
  - The control connection must generate a data session.
  - The data session must be initiated by the server.
  - The data session must match the policy that is configured with next hop.

**Workaround:** To avoid this problem, take the following steps:

- Define two policies for FTP under the same content, one with next hop (for example, PFTP) and the other without next hop (for example, PFTP\_SI).
- In policy PFTP, define a client-group with an access list (ACL) that points to a group of client-side IP addresses:

```
ip csg policy PFTP
  accounting type ftp customer-string ftp-string
  client-group CI
  next-hop 150.76.50.110
!
ip csg policy PFTP_SI
  accounting type ftp customer-string ftp-string
```

```
ip access-list standard CI
 permit 50.76.50.0 0.0.0.255
```

With this configuration, the control session (initiated from the client) matches PFTP, the policy that is configured with next hop, and the data session (initiated from the server) matches PFTP\_SI, the policy that is configured without next hop.

- CSCsf17014—R7: Out-of-order HTTP server packets might result in an overcharge

Out-of-order HTTP packets from the server might result in an overcharge.

For this problem to occur, all of the following conditions must be met:

- The HTTP connection must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
- The policies must be configured with **basis byte ip**.
- The CSG must receive out-of-order response packets from the server.
- The CSG must receive the same number of responses as requests.

**Workaround:** None.

- CSCsf32312—A ping from the CSG is needed to populate the ARP table after removing the **gateway** command

When you remove the **gateway** command from the CSG's client VLAN, the next hop specified in the command is also removed from the ARP table. Normal traffic does not restore the ARP entry.

**Workaround:** Ping the attached device from the CSG to populate the ARP table with the ARP entry.

## CSG Release 3.1(3)C7(2) - Closed Caveats

The following section lists bugs that are closed in CSG Release 3.1(3)C7(2).

- CSCei54668—HTTP requests using LF as end-of-line do not work

Some browsers do not follow RFC2616 and use just a line feed (LF) in HTTP headers rather than carriage return and line feed (CRLF). The CSG does not handle HTTP messages which use LF as end-of-line.

- CSCek28396—CSG R7.2: Add support to correlate Start and Stop for user session

A retransmitted RADIUS Stop might cause the CSG to remove a user entry from the User Table when the entry should not be removed.

To avoid this problem, the CSG must be able to associate a session correlator from the RADIUS Start message with a user entry in the User Table, and compare that correlator with the correlator in the RADIUS Stop message. If the correlators match, the CSG deletes the user entry; otherwise, the CSG retains the entry in the User Table.

The CSG can use the Acct-Session-Id (attribute 44) as the correlator, or it can use the following new vendor-specific attribute (VSA) subattribute (attribute 26, Vendor-Id 9, subattribute 1):

```
csg:user_session_correlator=<string>
```

If both attributes are included in the RADIUS Start or RADIUS Stop message, the CSG uses the VSA subattribute.

To enable this capability, the configurable **CSG\_RADIUS\_CORRELATOR** environment variable is added to the CSG:

- To delete User Table entries without user session correlation, set this variable to 0 (the default setting).
- To enable user session correlation, set this variable to 1.

If there is no correlator saved in the User Table entry, the CSG deletes the entry.

If there is a correlator saved in the User Table entry, the CSG compares it to the correlator in the RADIUS Stop. If the correlators match, the CSG deletes the entry; if they do not match, or if there is no correlator in the RADIUS Stop, the CSG retains the entry in the User Table.

To set this variable, use the **variable** command in module CSG configuration mode.

- CSCek41548—CSG interoperability issue with other vendor due to content length 0

When an HTTP stream containing the CONNECT method, for an HTTPS port, matches a content and policy with **accounting type http** and a policy with header map exists under the content, then CSG does not forward the HTTPS packet.

For this problem to occur, all of the following conditions must be met:

- The data flow must match a CSG Content-Policy pair that is configured for **accounting type http**.
  - The browser request must use a CONNECT method.
  - The content associated with one or more policy statements must have a Header Map defined.
- CSCek44627—Interm records not generated when required

Intermediate billing records are generated with larger byte counts than configured.

- CSCek45331—R7.2: Enhanced Regular Expression Support

The CSG must support the plus sign (+) in match patterns for CSG billing maps, enabling matches to one or more occurrences of the preceding character.

For example, the CSG must allow a match pattern such as:

**/music(/+)sheet.html**

which matches the following character strings:

**/music/sheet.html**

**/music//sheet.html**

**/music////////sheet.html**

To enable this support, the configurable **CSG\_REGEX\_PLUS** environment variable is added to the CSG:

- To treat the plus sign (+) as an ordinary character, set this variable to 0 (the default setting).
- To treat the plus sign (+) as a special character in a regular expression, set this variable to 1.



**Note** To configure the plus sign (+) as an ordinary character in a regular expression, preface the plus sign with a backward slash: \+.

To set this variable for a content, take the content out of service, use the **variable** command in module CSG configuration mode, then return the content to service. You can reset the CSG after setting this variable.



**Note** You must set this variable before configuring the content on the CSG.

The setting of the **CSG\_REGEX\_PLUS** variable affects the following CSG commands:

- The **match** command in CSG header map configuration mode
- The **match** command in CSG URL map configuration mode
- CSCek45371—CSG 7.2: Write coredump to non-boot flash  
Core dumps created by a release prior to CSG 3.1(3)C7(2) are not readable by CSG 3.1(3)C7(2) or later releases, and core dumps created by CSG 3.1(3)C7(2) or later releases are not readable by releases prior to CSG 3.1(3)C7(2). If you need to read a core dump, reload the image that generated the core dump.

- CSCsb83193—SUP32: CSG module offline after SSO switchover with SUP32

The CSG might go offline during Supervisor 32 switchover in stateful switchover (SSO) mode and stop passing traffic.

For this problem to occur, all of the following conditions must be met:

- The Supervisor must be configured for SSO.
- The Supervisor switchover must occur multiple times sequentially.
- CSCsd25751—R7: Remove warning message for HTTP contents on **basis byte ip** services  
The CSG generates the following incorrect warning message if a user attempts to configure an HTTP content on an **basis byte ip** service.

**% Warning, HTTP traffic is metered “basis byte tep” for policy PHTTP in service SERVICE2.**

For this problem to occur, all of the following conditions must be met:

- The HTTP connection must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
- The policies must be configured with **basis byte ip**.
- CSCsd77736—IOS - Syslog messages contain deprecated command **show ip slb memory**  
The following syslog messages contain the deprecated, hidden command **show ip slb memory**  
**% CSM\_SLB-3-UNEXPECTED: Module # unexpected error:  
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.**
- CSCsd88201—The CSG might not send Quota Returns for HTTP pipelined GETs with wrong content

In a Cisco Mobile Exchange (CMX) configuration in which the GGSN acts as a quota server for a postpaid user and the CSG provides content billing (the CSG treats the user as prepaid), the CSG might not send a Quota Return in response to a Quota Return Request.

For this problem to occur, all of the following conditions must be met:

- The data flow must match a CSG Content-Policy pair that is configured for **accounting type http**.
- The HTTP 1.1 flow must have pipelined GET requests.
- In the 200 response, the content-length header field must be set incorrectly.

- CSCsd92669—WAP Disconnect not charged after session timeout
 

A WAP 1.x DISCONNECT transaction is not charged via prepaid. If a WAP DISCONNECT packet is the first packet received for a WAP transaction, the CSG forwards the packet without charge. This is most likely to occur if the client is idle longer than the content idle time configured on the WAP content definition. Thus, the content idle timer expires and the WAP session state information is cleaned up on the CSG. When the user exits the browser, a DISCONNECT flows to the server. The CSG processes and forwards the DISCONNECT but does not charge the user.
- CSCse01713—R7: The CSG resets an active FTP data connection after failover
 

If an active FTP is used between an FTP client and an FTP server, and the CSG classifies the FTP control and data TCP connections as FTP connections (via **accounting type ftp**), and if data traffic is flowing over the FTP data connection when a CSG failover occurs, the newly active CSG sends a TCP RST to the FTP client, resulting in the TCP connection for FTP data being closed.
- CSCse06516—CSG prepaid sessions treated as postpaid after quota server recovery
 

If the **passthrough** command is configured on at least one service, and the CSG receives a RADIUS Start for a prepaid user while the quota server is down, when the quota server recovers, the CSG charges the first session for that user after the quota server recovers as postpaid. Subsequent sessions for that user are charged correctly.
- CSCse07212—R7: IMAP fetch fails when the CSG fails over from active to standby module
 

If an IMAP fetch is in progress between an IMAP client and an IMAP server when a CSG failover occurs, and the CSG classifies the IMAP TCP connection as IMAP (via **accounting type imap**), the newly active CSG does not forward the frames associated with the IMAP fetch.
- CSCse10401—The CSG goes offline during Supervisor switchover, blocking traffic
 

The CSG might go offline during Supervisor switchover in stateful switchover (SSO) mode and stop passing traffic.

For this problem to occur, all of the following conditions must be met:

  - The Supervisor must be configured for SSO.
  - The Supervisor switchover must occur multiple times sequentially.
- CSCse12408—CSG 7.246 traceback pkt\_drv\_bill\_send\_check: invalid session Id (0)
 

A session with session\_id 0 occurs and the following messages are received:

```
pkt_drv_bill_send_check: invalid session Id (0)
pkt_drv_bill_send_check: invalid session Id (0)
pkt_drv_bill_send_check: invalid session Id (0)
pkt_drv_bill_send_check: invalid session Id (0)
pkt_drv_bill_send_check: invalid session Id (0)
```
- CSCse20075—R7: Passthrough mode might fail when **no quota server reassign** is configured
 

If passthrough mode and the **no quota server reassign** command are configured for two or more quota servers, and one of the quota servers fails, passthrough might also fail.
- CSCse24107—A quota server failure with **no quota server reassign** can send requests to the wrong quota server
 

If **no quota server reassign** is configured, and a quota server has failed, but the CSG has not yet marked the quota server as FAILED, the CSG might send GTP transfer requests to an incorrect ACTIVE quota server.

- CSCse30639—Extended UserIndex TLV not included in HTTP header and statistics records  
The CSG might not include the Extended UserIndex TLV in the HTTP header and statistics BMA records. This problem can occur in a Cisco Mobile Exchange (CMX) service-aware configuration when an HTTP transaction is performed for a GPRS user.
- CSCse31266—R7: The CSG reloads under RTSP traffic load condition  
The CSG might reload when handling high RTSP traffic load.
- CSCse40494—RTSP traffic causes hang  
The CSG might hang or become unresponsive while running RTSP traffic in either prepaid or postpaid mode.  
For this problem to occur, all of the following conditions must be met:
  - The RTSP flow must match a CSG content rule.
  - The policy must be configured with **accounting type rtsp**.
  - The CSG must process a TEARDOWN command for an RTSP stream that no long exists.
- CSCse45438—The CSG sends report string attributes that are reserved for future use  
The CSG is sending report string attribute values other than 0x00, 0x01 and 0x02 in RTSP CDRs. The reported attribute values are reserved by Cisco for future use.
- CSCse49567—R7.2: Quota Reauthorization TLV additions  
The CSG supports the following Quota Reauthorization TLV additions:
  - CSG\_PENDING\_QUOTA = 0x55
  - CSG\_RESERVED\_QUOTA = 0x56
- CSCse59953—The CSG crashes on IXP3 software exception  
The active CSG might fail over to the standby CSG when a new HTTP request/response follows the FIN from the client/server.  
For this problem to occur, all of the following conditions must be met:
  - The HTTP connection must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
  - The CSG must receive more requests than responses.
  - The CSG session must receive FINs from both directions.
  - The CSG must receive an ACK for one of the FINs from the server.
  - The CSG must receive an HTTP data packet that marks the start of a new request/response. The SN of the data packet must be greater than the SN of the FIN received from that direction.
- CSCse72201—The CSG cannot parse multiple subattributes in RADIUS VSA  
The CSG might not parse multiple RADIUS subattributes encoded in a single VSA in a RADIUS Access-Accept message.
- CSCse72980—The CSG does not retrieve records from the PSD when the BMA recovers  
If the CSG loses communication with all BMAs, it might not retrieve records from the PSD when one or more BMAs recover.

When communication with the BMAs is lost, the CSG sends records to the PSD. When communication with one or more BMAs is recovered, the CSG fails to retrieve records from the PSD and forward them to the BMA, even though the CSG maintains the PSD in an active state. Echo requests and write requests continue to be processed correctly, and the CSG shows no pending read requests in its record storage statistics.

- CSCse79792—Quota refund for FTP timeout is not working

Quota refund for FTP timeout is not working.

- CSCse86654—Memory pool should stop growing when available memory is less than 2%

When memory usage is greater than 98%, the CSG memory pools might continue to grow, leaving the CSG at less than 2 percent memory.

- CSCse87973—The CSG might crash as a result of a false FPGA hang

When a high rate of traffic flows through the CSG, the PPC might incorrectly mark the FPGA as hung, and the CSG might crash and reload.

- CSCse89087—The CSG does not initiate a server connection for **accounting type http**

When using a CSG policy with **accounting type http**, the CSG might not forward the first HTTP request for a session, and the HTTP transaction might not complete.

For this problem to occur, all of the following conditions must be met:

- The HTTP connection must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
- The CSG must detect downgrade conditions from the server to the client.
- The CSG must block the first GET and fail to initiate the connection to the server.

- CSCse92453—The CSG does not retransmit packets it has ACKed when the client sends FIN/ACK

The CSG might fail to resend HTTP packets from the client after the CSG receives the FIN from the client.

For this problem to occur, all of the following conditions must be met:

- The HTTP connection must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
- The CSG must ACK and own the packets to allow analysis to continue.
- The CSG must send the packets to the server, but the packets must not reach the server.
- The CSG must be responsible for resending the packets.
- The CSG must receive the FIN from the client before the CSG is able to resend the packets.

- CSCsf06831—The CSG might send a gratuitous ARP for content with /32 netmask

The CSG might send a gratuitous ARP request (that is, an ARP request in which the CSG advertises the IP address as its own IP address) for an IP address defined as a match criteria in a CSG content. The CSG sends the gratuitous ARP on exactly one VLAN. The VLAN depends on the configuration.

For this problem to occur, all of the following conditions must be met:

- A CSG content must be configured with a /32 netmask.
- Fault Tolerance must be enabled and alias IP addresses must be configured on one or more VLANs.

- CSCsf11808—The CSG might not forward UDP fragments

The CSG might not forward header or out-of-order trailer IP fragments for a UDP packet.

- CSCsf21476—The **no passthrough** configuration does not work when the quota server does not respond to a User Authorization Request  
If the quota server does not respond to a User Authorization Request, the CSG might forward traffic, even if **no passthrough** is configured on the CSG.
- CSCsf27734—The CSG might crash during under heavy load  
Under heavy traffic conditions and stress levels of user activation and deactivation, the CSG might crash, generate a core dump, and fail over to the standby CSG.
- CSCsf30458—The CSG might report an incorrect value for in-use buffers for CSG NoKUT  
When the **show module csg tech-support** command is entered, the CSG might report an incorrect value for the in-use buffer with NoKUT. The reported value might register 4294967295 continually.
- CSCsg02310—The CSG reset with FPGA 2 iPacket and ePacket tags do not match  
The CSG might failover to the standby CSG when a new HTTP request or response is out of order and has the SYN bit set.  
For this problem to occur, all of the following conditions must be met:
  - The HTTP connection must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
  - The CSG must receive an out-of-order data packet which has the SYN bit set.

## Caveats for 3.1(3)C7(1)

This section lists and describes all caveats, both open and resolved, that affect CSG software release 3.1(3)C7(1).

For information about open or unresolved caveats in the Content Services Gateway 3.1(3)C7(1) release, refer to the Cisco Bug Toolkit at the following URL:

<http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>

## CSG Release 3.1(3)C7(1) - Open Caveats

The following list identifies open caveats in CSG Release 3.1(3)C7(1).

- CSCek44627—R7: Interm records not generated when required  
Intermediate billing records are generated with larger byte counts than configured.  
**Workaround:** None.
- CSCsd92612—Crash in timerwheel when taking accounting out-of-service while RTSP traffic  
If you are running RTSP traffic (RTP UDP) through the CSG with RTSP filtering configured, and you take accounting out-of-service while there are active RTSP session, the CSG can crash.  
**Workaround:** Do not take accounting out-of-service while there are active RTSP sessions.

## CSG Release 3.1(3)C7(1) - Closed Caveats

The following section lists bugs that are closed in CSG Release 3.1(3)C7(1).

- CSCee90050—CSG: general header map matching NOT working

If the first character of a configured HTTP header name is lowercase, the CSG does not match the header fields in the header map.

- CSCsc09749—R5.9: CSG/microcode crash when removing user group from accounting

If the CSG is configured for prepaid, and there are more than 20,000 users in the User Table, and traffic is running, removing the user group configuration from an accounting group might cause the CSG to reload.

This problem could not be reproduced.

- CSCsc49420—HTTP L7 IP fragments with RST do not report terminal stats

For flows that match a CSG policy with **accounting type http**, HTTP packets that are IP fragmented and that have the RESET bit set in the TCP header cause the CSG to fail to report the terminal statistic.

For this problem to occur, all of the following conditions must be met:

- The connection must match a CSG content configured with policies that require HTTP deep packet inspection (**accounting type http**).
- The HTTP packet must be fragmented and must have the RESET bit set in the TCP header of the header fragment.

- CSCsd52400—Deleted ruleset will still be seen under module if it was applied to mod

When the user tries to delete a ruleset which has been applied to modules, the ruleset is deleted but the ruleset name is still visible under **module CSG**.

For this problem to occur, all of the following conditions must be met:

- The **module CSG** must be offline.
- The ruleset must be deleted from the configuration before deleting it from the **module CSG**.

- CSCsd88749—RTSP TCP segment support

If SETUP or SETUP REPLY command methods on the RTSP control channel span more than 2 TCP packets, then RTSP data stream traffic does not map to the RTSP content definition. Instead, it maps to a catchall content definition, if one is configured.

- CSCse14440—The CSG hangs and stops passing traffic

The CSG might hang when its memory is depleted or fragmented, or when it is trying to download a complex URL map. If this occurs, the CSG hangs, stops passing traffic, and stops responding to user commands, and the console stops responding.

To help avoid this problem, the following configurable environment variables are added to the CSG:

- The **CSG\_FAILOVER\_DELAY** environment variable enables you to set the delay time, in seconds, before failover because of a hang associated with IPCP\_READ. The range is 3 to 600; the default setting is 180.
- The **CSG\_IXP\_POLL** environment variable enables you to set the number of times the CSG polls the IXP before deciding there is an IXP hang. The range is 0 to 3600; the default setting is 720.
- The **CSG\_SNMP\_DELAY** environment variable enables you to set the delay time, in seconds, before failing the SNMP query. The range is 3 to 600; the default setting is 10.

To set these variables, use the **variable** command in module CSG configuration mode.

## Documentation and Technical Assistance

This section contains the following information:

- [Related Documentation, page 54](#)
- [Cisco IOS Documentation Set, page 55](#)
- [Obtaining Documentation and Submitting a Service Request, page 55](#)

## Related Documentation

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

- Site Preparation and Safety Guide
- Regulatory Compliance and Safety Information for the Catalyst 6500 Series Switches
- *Catalyst 6500 Series Switch Installation Guide*
- *Catalyst 6500 Series Quick Software Configuration*
- *Catalyst 6500 Series Switch Module Installation Guide*
- *Catalyst 6500 Series Software Configuration Guide*
- *Catalyst 6500 Series Command Reference*
- *Catalyst 6000 Family IOS Software Configuration Guide*
- *Catalyst 6500 Series Cisco IOS Command Reference*
- *Catalyst 6000 Family Flash Card Install Note*
- *ATM Configuration and Command Reference—Cisco Catalyst 6500 Series Switches*
- *System Message Guide - Catalyst Family Switches—Cisco Catalyst 6500 Series Switches*
- Regulatory Compliance and Safety Information for the Cisco 7600 Series Routers
- Cisco 7609 Router Installation Guide
- Cisco 7600 Series Cisco IOS Software Configuration Guide
- Cisco 7600 Series Cisco IOS Command Reference
- For information about MIBs, see:  
<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>
- *Cisco Content Services Gateway Installation and Configuration Guide*, Release 3.1(3)C7(1)
- Cisco IOS Configuration Guides and Command References, Release 12.1—Use these publications to help you configure the Cisco IOS software that runs on the MSFC and on the MSM and ATM modules.

## Cisco IOS Documentation Set

Cisco IOS Configuration Guides and Command References, Release 12.1(12c)E4—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 a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

---

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

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

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

Copyright © 2008, Cisco Systems, Inc. All rights reserved.