

Release Notes for Cisco Content Services Gateway 3.1(3)C6(12) for Cisco IOS Release 12.2(18)SXE

Revised: November 11, 2008
Current Release—3.1(3)C6(12)

This publication describes the requirements, dependencies, and caveats for the Cisco Content Services Gateway (CSG) Release 3.1(3)C6(12).

Contents

- [Introduction, page 2](#)
- [Features, page 2](#)
- [System Requirements, page 7](#)
- [Upgrading to a New CSG Release, page 10](#)
- [Saving and Restoring Configurations, page 10](#)
- [Additional Installation Instructions, page 10](#)
- [Dependencies and Restrictions, page 10](#)
- [Caveats for 3.1\(3\)C6\(12\), page 11](#)
- [Caveats for 3.1\(3\)C6\(11\), page 12](#)
- [Caveats for 3.1\(3\)C6\(10\), page 16](#)
- [Caveats for 3.1\(3\)C6\(9\), page 22](#)
- [Caveats for 3.1\(3\)C6\(8\), page 24](#)
- [Caveats for 3.1\(3\)C6\(7\), page 30](#)
- [Caveats for 3.1\(3\)C6\(6\), page 34](#)
- [Caveats for 3.1\(3\)C6\(5\), page 37](#)
- [Caveats for 3.1\(3\)C6\(4\), page 45](#)



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

© 2008 Cisco Systems, Inc. All rights reserved.

- [Caveats for 3.1\(3\)C6\(3\), page 53](#)
- [Caveats for 3.1\(3\)C6\(2\), page 58](#)
- [Documentation and Technical Assistance, page 64](#)

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)C6(2).

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 8.

- [CSG Features Introduced Prior to CSG R4.1, page 2](#)
- [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 6](#)
- [CSG Features Introduced in CSG R6.9—3.1\(3\)C6\(9\), page 6](#)

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

System Requirements

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

- [Memory Requirements, page 7](#)
- [Hardware Supported, page 7](#)
- [Power Supply, page 7](#)
- [Environmental Requirements, page 8](#)
- [Software Requirements, page 8](#)
- [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 platforms:

- A Supervisor Engine 1A (SUP1A) with a Multilayer Switch Feature Card (MSFC) and a Policy Feature Card (PFC)
- A Supervisor Engine 2 with an MSFC2 (SUP2-MSFC2), and a module with ports to connect server and client networks
- A Supervisor Engine 720 with an MSFC3-BXL (SUP720-MSFC3-BXL), and a module with ports to connect server and client networks

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 ¹	Minimum Cisco IOS Release Required for New Features ²	Minimum CatOS/Hybrid Level Supported	Minimum IOS Level Supported ³
3.1(3)C6(12)	SC-SVC-CSG-B-6.0 SC-SVC-CSG-P-6.0	SUP720-MSFC3-BXL SUP2-MSFC2	12.2(18)SXE	7.6.1	12.2(18)SXD
3.1(3)C6(11)	SC-SVC-CSG-B-6.0 SC-SVC-CSG-P-6.0	SUP720-MSFC3-BXL SUP2-MSFC2	12.2(18)SXE	7.6.1	12.2(18)SXD
3.1(3)C6(10)	SC-SVC-CSG-B-6.0 SC-SVC-CSG-P-6.0	SUP720-MSFC3-BXL SUP2-MSFC2	12.2(18)SXE	7.6.1	12.2(18)SXD
3.1(3)C6(9)	SC-SVC-CSG-B-6.0 SC-SVC-CSG-P-6.0	SUP720-MSFC3-BXL SUP2-MSFC2	12.2(18)SXE	7.6.1	12.2(18)SXD
3.1(3)C6(8)	SC-SVC-CSG-B-6.0 SC-SVC-CSG-P-6.0	SUP720-MSFC3-BXL SUP2-MSFC2	12.2(18)SXE	7.6.1	12.2(18)SXD
3.1(3)C6(7)	SC-SVC-CSG-B-6.0 SC-SVC-CSG-P-6.0	SUP720-MSFC3-BXL SUP2-MSFC2	12.2(18)SXE	7.6.1	12.2(18)SXD
3.1(3)C6(6)	SC-SVC-CSG-B-6.0 SC-SVC-CSG-P-6.0	SUP720-MSFC3-BXL SUP2-MSFC2	12.2(18)SXE	7.6.1	12.2(18)SXD
3.1(3)C6(5)	SC-SVC-CSG-B-6.0 SC-SVC-CSG-P-6.0	SUP720-MSFC3-BXL SUP2-MSFC2	12.2(18)SXE	7.6.1	12.2(18)SXD
3.1(3)C6(4)	SC-SVC-CSG-B-6.0 SC-SVC-CSG-P-6.0	SUP720-MSFC3-BXL SUP2-MSFC2	12.2(18)SXE	7.6.1	12.2(18)SXD
3.1(3)C6(3)	SC-SVC-CSG-B-6.0 SC-SVC-CSG-P-6.0	SUP720-MSFC3-BXL SUP2-MSFC2	12.2(18)SXE	7.6.1	12.2(18)SXD

CSG Release	Software Part Number	Supervisor Hardware Supported ¹	Minimum Cisco IOS Release Required for New Features ²	Minimum CatOS/Hybrid Level Supported	Minimum IOS Level Supported ³
3.1(3)C6(12)	SC-SVC-CSG-B-6.0 SC-SVC-CSG-P-6.0	SUP720-MSFC3-BXL SUP2-MSFC2	12.2(18)SXE	7.6.1	12.2(18)SXD
3.1(3)C6(11)	SC-SVC-CSG-B-6.0 SC-SVC-CSG-P-6.0	SUP720-MSFC3-BXL SUP2-MSFC2	12.2(18)SXE	7.6.1	12.2(18)SXD
3.1(3)C6(10)	SC-SVC-CSG-B-6.0 SC-SVC-CSG-P-6.0	SUP720-MSFC3-BXL SUP2-MSFC2	12.2(18)SXE	7.6.1	12.2(18)SXD
3.1(3)C6(9)	SC-SVC-CSG-B-6.0 SC-SVC-CSG-P-6.0	SUP720-MSFC3-BXL SUP2-MSFC2	12.2(18)SXE	7.6.1	12.2(18)SXD
3.1(3)C6(8)	SC-SVC-CSG-B-6.0 SC-SVC-CSG-P-6.0	SUP720-MSFC3-BXL SUP2-MSFC2	12.2(18)SXE	7.6.1	12.2(18)SXD
3.1(3)C6(7)	SC-SVC-CSG-B-6.0 SC-SVC-CSG-P-6.0	SUP720-MSFC3-BXL SUP2-MSFC2	12.2(18)SXE	7.6.1	12.2(18)SXD
3.1(3)C6(6)	SC-SVC-CSG-B-6.0 SC-SVC-CSG-P-6.0	SUP720-MSFC3-BXL SUP2-MSFC2	12.2(18)SXE	7.6.1	12.2(18)SXD
3.1(3)C6(2)	SC-SVC-CSG-B-6.0 SC-SVC-CSG-P-6.0	SUP720-MSFC3-BXL SUP2-MSFC2	12.2(18)SXE	7.6.1	12.2(18)SXD
3.1(3)C5(6)	SC-SVC-CSG-B-5.0 SC-SVC-CSG-P-5.0	SUP720-MSFC3-BXL SUP2-MSFC2	12.2(18)SXD	7.6.1	SUP720: 12.2(18)SXD1 SUP2: 12.2(17b)SXB

- 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.
- If running Hybrid, make sure the appropriate IOS Hybrid image is available at this level.
- 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
CSG					
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 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
Console Cable					
72-876-01	Console Cable	Not applicable	Not applicable	Not applicable	Not applicable

Product Number	Product Description	Minimum Software Version	Recommended Software Version	Cisco IOS Release	Minimums for CSG/Hybrid
Accessory Kit					
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*.

Dependencies and Restrictions

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

Caveats for 3.1(3)C6(12)

This section lists and describes all caveats, both open and resolved, that affect CSG software release 3.1(3)C6(12).

For information about open or unresolved caveats in the Content Services Gateway 3.1(3)C6(12) 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)C6(12) - Open Caveats

The following list identifies open caveats in CSG Release 3.1(3)C6(12).

- 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 a signed integer greater than 2147483647.

Workaround: Clear the affected user.

- CSCsv23706—CSG: PoD sent too early

When handling prepaid, if the quota server returns a disconnect, the CSG sends a PoD too early.

Workaround: None.

- CSCsv36954—Stack Overflow in BillingStack task

When memory usage reaches 8k, the CSG crashes as a result of a stack overflow.

Workaround: None.

CSG Release 3.1(3)C6(12) - Closed Caveats

The following section lists bugs that are closed in CSG Release 3.1(3)C6(12).

- CSCsi21725—WAP concatenation over IP fragments with reassembled length greater than 1500 bytes is dropped

When WAP 1.x/WSP traffic matches a content and policy with **accounting type wap**, the WAP concatenation packet might be dropped.

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 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 include concatenated PDUs.
- At least one of the concatenated PDUs must be longer than 1472 bytes, such that the complete IP packet formed from that concatenated PDU plus the IP header plus the UDP is longer than 1500 bytes.

- 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.
- CSCsr62399—The **client** command configuration for a content might not work
The CSG might block traffic that should match the default policy under a content, even if the **ip cs** **block** command is not configured. This problem can occur if the **client** command is configured and then unconfigured for a content and traffic is sent that does not match any of the configured policies for the content.
- CSCsv14112—The CSG crashes as a result of “billingTask” stack overflow.
When memory usage reaches 8k, the CSG crashes as a result of a stack overflow.

Caveats for 3.1(3)C6(11)

This section lists and describes all caveats, both open and resolved, that affect CSG software release 3.1(3)C6(11).

For information about open or unresolved caveats in the Content Services Gateway 3.1(3)C6(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)C6(11) - Open Caveats

The following list identifies open caveats in CSG Release 3.1(3)C6(11).

- CSCsi21725—WAP concatenation over IP fragments with reassembled length greater than 1500 bytes is dropped
When WAP 1.x/WSP traffic matches a content and policy with **accounting type wap**, the WAP concatenation packet might be dropped.
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 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 include concatenated PDUs.
 - At least one of the concatenated PDUs must be longer than 1472 bytes, such that the complete IP packet formed from that concatenated PDU plus the IP header plus the UDP is longer than 1500 bytes.**Workaround:** Configure Layer 4 billing for this content.
- 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 a signed integer greater than 2147483647.

Workaround: Clear the affected user.

- CSCsr62399—The **client** command configuration for a content might not work

The CSG might block traffic that should match the default policy under a content, even if the **ip csg block** command is not configured. This problem can occur if the **client** command is configured and then unconfigured for a content and traffic is sent that does not match any of the configured policies for the content.

Workaround: There are several different workarounds:

- Remove the content altogether, then reconfigure the content without the **client** command.

Removing the content removes all of the content policy pairs that use the content from all associated services, so when you reconfigure the content you must also add the content policy pairs to all associated services.

Removing the content also removes it from any associated rulesets, so you must add the reconfigured content to those rulesets, too.

- After unconfiguring the **client** command (using the **no** form of the command), configure a catch-all policy.

For example, for HTTP traffic you can configure a catch-all policy with **accounting type http** for a content, such that all traffic that does not match any of the other configured policies for that content matches the catch-all policy and generates BMA CDRs.

- After unconfiguring the **client** command, force a failover to the standby CSG, wait for the “CSG FT user dump complete” message on the first CSG, then force a failover back to the first CSG.

CSG Release 3.1(3)C6(11) - Closed Caveats

The following section lists bugs that are closed in CSG Release 3.1(3)C6(11).

- 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.
- CSCsi14915—Small buffer leak for SMTP traffic on R6.7.22
A small buffer leak occurs when running SMTP traffic.
- CSCsj68486—The CSG crashes with **PPC exception type 512 on 'core_usage**
A CSG in redundant fault-tolerant mode can crash with the following message:
PPC exception type 512 on 'core_usage
- CSCsk76201—Service Auth/Reauth storm for multiple sessions
The CSG continually resends Quota Service Reauthorization Requests for a specific user and service.
- CSCsk92635—The CSG generates an FPGA1 exception error and resets

The CSG coredumps 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.

- CSCs110958—The **advertise downlink next-hop** command does not route mobile-to-mobile traffic

The **advertise downlink next-hop** command is not sufficient to enable the CSG to route mobile-to-mobile traffic to the correct GGSN processor. This problem can occur for APN subscribers that use pre-allocated static addresses to make them available to traffic from other subscribers.

- CSCs118499—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.

- CSCs134063—Control Retry Timer check with an environment 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.

- CSCs147769—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

- CSCs150131—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.

- 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

- 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.

- 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 on task **IXP3 SA-CORE (Ex 18)(00000000h)**

When an HTTP stream matches a content and policy with **accounting type http**, the CSG might crash with the below signature:

```
!!!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)'
```

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 packet from the server must use “Transfer-Encoding:chunked”.
- 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.

Caveats for 3.1(3)C6(10)

This section lists and describes all caveats, both open and resolved, that affect CSG software release 3.1(3)C6(10).

For information about open or unresolved caveats in the Content Services Gateway 3.1(3)C6(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)C6(10) - Open Caveats

The following list identifies open caveats in CSG Release 3.1(3)C6(10).

- 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 on R6.7.22
 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**.
- CSCsi21725—WAP concatenation over IP fragments with reassembled length greater than 1500 bytes is dropped
 When WAP 1.x/WSP traffic matches a content and policy with **accounting type wap**, the WAP concatenation packet might be dropped.
 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 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 include concatenated PDUs.
 - At least one of the concatenated PDUs must be longer than 1472 bytes, such that the complete IP packet formed from that concatenated PDU plus the IP header plus the UDP is longer than 1500 bytes.**Workaround:** Configure Layer 4 billing for this content.
- CSCsj68486—The CSG crashes with **PPC exception type 512 on 'core_usage**
 A CSG in redundant fault-tolerant mode can crash with the following message:
PPC exception type 512 on 'core_usage
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 a signed integer greater than 2147483647.**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.
- CSCsl10958—The **advertise downlink next-hop** command does not route mobile-to-mobile traffic
The **advertise downlink next-hop** command is not sufficient to enable the CSG to route mobile-to-mobile traffic to the correct GGSN processor. This problem can occur for APN subscribers that use pre-allocated static addresses to make them available to traffic from other subscribers.
Workaround: Add a static route to the configuration, pointing to the subscriber GGSN (if known in advance).

CSG Release 3.1(3)C6(10) - Closed Caveats

The following section lists bugs that are closed in CSG Release 3.1(3)C6(10).

- 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).
- CSCsc32220—The CSG forwards retransmitted SYN/ACKs from the server to the client
The CSG sends a SYN to the server to set up the half-proxy. The server responds with a SYN/ACK. The CSG sends the first request to the server, but the server does not receive the request. The server retransmits the SYN/ACK, which the CSG forwards to the client. (The CSG should drop the retransmitted SYN/ACK.)
For this problem to occur, the following conditions must all be met:
 - The HTTP connection must match a CSG content configured with policies requiring HTTP deep packet inspection (**accounting type http**).
 - The server must retransmit the SYN/ACK.

- CSCsd17624—No ICC response when **noinservice** issued for CSG accounting

The CSG crashes with the following message at the Supervisor Engine console:

```
% No ICC response for TLV type 555 from CSM linecard.
```

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

 - At least one charging gateway (BMA, quota server, or PSD) must be configured on the CSG.
 - The charging gateway must initiate the health check by sending a GTP Node Alive request or GTP Echo Request.
 - The CSG must respond to the probes by sending a GTP Echo response or GTP Node Alive Response.
- 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.
- 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.
- CSCsh44943—No alarm to user while CSG drops packets due to buffer exhaustion

The CSG drops packets due to buffer exhaustion, but no alarm is generated.

For this problem to occur, one of the following counters (in TCP Statistics) must be non-zero:

```
Slowpath(low pri) buffer alloc failures    0          0
Slowpath(high pri) buffer alloc failures  0          0
Block alloc failures                      0          0
Small buffer allocs failures              0          0
Medium buffer allocs failures             0          0
```

Large buffer allocs failures	11553	355
Session table allocs failures	0	0

A non-zero value on of these counters indicates that the CSG might have dropped some packets as a result of buffer exhaustion.

- 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.

- CSCsi07067—RADIUS messages dropped after configuring or unconfiguring accounting
The CSG might drop RADIUS messages after configuring or unconfiguring accounting.
- CSCsi62248—CSG1 crash when operating with maximum CPU and memory usage
The CSG crashes when running under maximum CPU and maximum memory conditions.

- CSCsi83336—Negative Quadrans from QS Creates Large Positive Balance in CSG
A user might end up with a large positive balance when a quota server sends a Service Authorization Response with negative quadrans (-1) for a CSG service. This can occur when the quota server uses negative quadrans in the Service Authorization Response.

- CSCsi85656—The CSG does not forward an HTTP POST that spans multiple packets
The CSG might not forward an HTTP POST that spans multiple packets.

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 POST must not use multipart or chunked processing.
 - The POST must span multiple packets such that end of the HTTP header and the end of the complete HTTP message are in separate packets.
- CSCsi87689—Buffer overrun on tracelog_printf can result in CSG to crash
If CSG is configured for **accounting type rtsp**, the CSG might crash as a result of a buffer overrun when performing a **show tech csg**.
 - 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.
- CSCsj47871—R6.9: The CSG reloads when the **no radius proxy** command is entered

When the **no radius proxy** command is entered, the CSG crashes with the following message on the Supervisor Engine console:

No ICC response for TLV type 660 from CSM linecard

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

- At least one charging gateway (BMA, quota server, or PSD) must be configured on the CSG.
- The charging gateway must initiate the health check by sending a GTP Node Alive request or GTP Echo Request.
- The CSG must respond to the probes by sending a GTP Echo response or GTP Node Alive Response.

- 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.
- 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.

Caveats for 3.1(3)C6(9)

This section lists and describes all caveats, both open and resolved, that affect CSG software release 3.1(3)C6(9).

For information about open or unresolved caveats in the Content Services Gateway 3.1(3)C6(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)C6(9) - Open Caveats

The following list identifies open caveats in CSG Release 3.1(3)C6(9).

- CSCsc32220—The CSG forwards retransmitted SYN/ACKs from the server to the client
The CSG sends a SYN to the server to set up the half-proxy. The server responds with a SYN/ACK. The CSG sends the first request to the server, but the server does not receive the request. The server retransmits the SYN/ACK, which the CSG forwards to the client. (The CSG should drop the retransmitted SYN/ACK.)
For this problem to occur, the following conditions must all be met:
 - The HTTP connection must match a CSG content configured with policies requiring HTTP deep packet inspection (**accounting type http**).
 - The server must retransmit the SYN/ACK.

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.
- 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.
- CSCsi14915—Small buffer leak for SMTP traffic on R6.7.22
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**.
- CSCsi21725—WAP concatenation over IP fragments with reassembled length greater than 1500 bytes is dropped
When WAP 1.x/WSP traffic matches a content and policy with **accounting type wap**, the WAP concatenation packet might be dropped.
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 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 include concatenated PDUs.
 - At least one of the concatenated PDUs must be longer than 1472 bytes, such that the complete IP packet formed from that concatenated PDU plus the IP header plus the UDP is longer than 1500 bytes.**Workaround:** Configure Layer 4 billing for this content.

CSG Release 3.1(3)C6(9) - Closed Caveats

The following section lists bugs that are closed in CSG Release 3.1(3)C6(9).

- 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.
- CSCsi41755—R6.8: Tracebacks caused WAP 1.x user_agent > 64
When WAP 1.x/WSP traffic matches a content and policy with **accounting type wap**, it can trigger a traceback that is not reported in the CDR.

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 wap**.
- The User-Agent header must be present in the packet.
- The User-Agent header value must be greater than 64 bytes.

Caveats for 3.1(3)C6(8)

This section lists and describes all caveats, both open and resolved, that affect CSG software release 3.1(3)C6(8).

For information about open or unresolved caveats in the Content Services Gateway 3.1(3)C6(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)C6(8) - Open Caveats

The following list identifies open caveats in CSG Release 3.1(3)C6(8).

- CSCsc32220—The CSG forwards retransmitted SYN/ACKs from the server to the client
The CSG sends a SYN to the server to set up the half-proxy. The server responds with a SYN/ACK. The CSG sends the first request to the server, but the server does not receive the request. The server retransmits the SYN/ACK, which the CSG forwards to the client. (The CSG should drop the retransmitted SYN/ACK.)

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

- The HTTP connection must match a CSG content configured with policies requiring HTTP deep packet inspection (**accounting type http**).
- The server must retransmit the SYN/ACK.

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.

- 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.

- CSCsi14915—Small buffer leak for SMTP traffic on R6.7.22
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**.
- CSCsi21725—WAP concatenation over IP fragments with reassembled length greater than 1500 bytes is dropped
When WAP 1.x/WSP traffic matches a content and policy with **accounting type wap**, the WAP concatenation packet might be dropped.
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 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 include concatenated PDUs.
 - At least one of the concatenated PDUs must be longer than 1472 bytes, such that the complete IP packet formed from that concatenated PDU plus the IP header plus the UDP is longer than 1500 bytes.**Workaround:** Configure Layer 4 billing for this content.

CSG Release 3.1(3)C6(8) - Closed Caveats

The following section lists bugs that are closed in CSG Release 3.1(3)C6(8).

- 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.
- 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.

- 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.

- CSCek72616—PPC exception type 122 on core_dump(0CC65E70h)

The CSG might receive a partial coredump when detecting an internal error.

- CSCsd50424—The CSG forwards HTTP traffic when no quota is available

The CSG forwards HTTP traffic without requesting quota from the quota server.

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 quota server must send zero quota in the initial service authorization response.
- Immediately thereafter, the client must resend a SYN with the same tuple.
- CSCsd95417—CSG traceback fastblk_free_guts + 0xE8
A CSG user configured for prepaid service can encounter a traceback message and might see high CPU usage as a result.
- CSCse79792—Quota refund for FTP timeout is not working
Quota refund for FTP timeout is not working.
- 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.
- 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.
- 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.
- 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.
- CSCsg84500—The CSG reports high CPU
The CSG CPU load is extremely high (85%) with a low number of subscribers and low traffic.
- 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.

- 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.
- 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.
- 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.
- 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.
- 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.

- 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.

- 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.

- 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”.
- CSCsi11911—CSG R6.7: HTTP traffic causes buffer leak

When an HTTP stream matches a content and policy with **accounting type http**, the CSG might encounter a buffer leak and drop all traffic.

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 CSG must receive an HTTP packet which is the first packet of a transaction with only the PUSH flag set.
- The server must resend the packet with the PUSH/ACK flag set.

Caveats for 3.1(3)C6(7)

This section lists and describes all caveats, both open and resolved, that affect CSG software release 3.1(3)C6(7).

For information about open or unresolved caveats in the Content Services Gateway 3.1(3)C6(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)C6(7) - Open Caveats

The following list identifies open caveats in CSG Release 3.1(3)C6(7).

- CSCsc32220—The CSG forwards retransmitted SYN/ACKs from the server to the client
The CSG sends a SYN to the server to set up the half-proxy. The server responds with a SYN/ACK. The CSG sends the first request to the server, but the server does not receive the request. The server retransmits the SYN/ACK, which the CSG forwards to the client. (The CSG should drop the retransmitted SYN/ACK.)

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

- The HTTP connection must match a CSG content configured with policies requiring HTTP deep packet inspection (**accounting type http**).
- The server must retransmit the SYN/ACK.

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.

CSG Release 3.1(3)C6(7) - Closed Caveats

The following section lists bugs that are closed in CSG Release 3.1(3)C6(7).

- 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.

- 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.
- CSCse31266—R7: The CSG reloads under RTSP traffic load condition
The CSG might reload when handling high RTSP traffic load.
- 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.
- 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.
- 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.
 - 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.
 - 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....
```

- 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.
- 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.
- CSCsg42305—C6.6: The CSG crashes when running HTTPS traffic
The CSG crashes when running HTTPS 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**).
- URL maps or header maps must be configured for the content.
- The browser request must use a CONNECT method.

Caveats for 3.1(3)C6(6)

This section lists and describes all caveats, both open and resolved, that affect CSG software release 3.1(3)C6(6).

For information about open or unresolved caveats in the Content Services Gateway 3.1(3)C6(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)C6(6) - Open Caveats

The following list identifies open caveats in CSG Release 3.1(3)C6(6).

- CSCsc32220—The CSG forwards retransmitted SYN/ACKs from the server to the client
The CSG sends a SYN to the server to set up the half-proxy. The server responds with a SYN/ACK. The CSG sends the first request to the server, but the server does not receive the request. The server retransmits the SYN/ACK, which the CSG forwards to the client. (The CSG should drop the retransmitted SYN/ACK.)
For this problem to occur, the following conditions must all be met:
 - The HTTP connection must match a CSG content configured with policies requiring HTTP deep packet inspection (**accounting type http**).
 - The server must retransmit the SYN/ACK.**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.
- 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.
Workaround: None.

CSG Release 3.1(3)C6(6) - Closed Caveats

The following section lists bugs that are closed in CSG Release 3.1(3)C6(6).

- CSCei57726—Rate limit the CSG GTP reject messages
In response to a GTP reject cause code message from BMA, the CSG sends a log message to the Supervisor. In some cases, the CSG could flood the Supervisor with many log messages and deplete EOBC buffers:

%EOBC-3-NOEOBCBUF: No EOBC buffer available. Dropping the packet.

This might result in degradation of CAT6k performance and might lead to an IOS crash.
- CSCek40246—The CSG: TLV for POP3 and SMTP CDRs has 0 duration
In the CDRs for POP3 and SMTP, the CSG reports 0 duration.
- CSCek41548—The CSG has interoperability issues due to content length 0
The CSG might not forward HTTPS packets for an HTTP stream for an HTTPS port.
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 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 records might not be generated when they should be, based on the configured bytes. Or the records are generated, but with bytes counts larger than the amount configured.
- CSCsc09749—R5.9: CSG/microcode crash when removing user group from accounting
If the CSG is configured for prepaid, and there are ore 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.
- CSCsd27639—Improper passive FTP causes session IXP to crash
When server-initiated FTP or RTSP traffic is received from an unknown MAC address for more than 8 sessions, the CSG hangs, causing a reload.
- CSCsd42458—R7: Connection Timestamps wrong if HTTP session RST by CSG (quota server failed)
If the quota server fails, and a RADIUS Start adds a user to the User Table, and the CSG sends a RST when the client attempts an HTTP connection, then the final eight bytes of the Connection Timestamp TLV are incorrect.
- CSCsd65665—The CSG sends wrong interval usage value for time-based service
For a time-based service, the CSG might send an incorrect interval usage value.
- CSCsd88796—RTSP - The CSG might not parse 5-digit ports correctly
While running RTSP traffic containing UDP as the transport protocol, one set of UDP data traffic maps to CATCHALL policy of type OTHER.
For this problem to occur, all of the following conditions must be met:
 - A combination of traffic types must flow through the CSG.

- The transport header of either the SETUP method or the SETUP REPLY must contain 5-digit port numbers.

- 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. 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.

- CSCse17647—R7: BMA queue stops being processed

When the CSG detects a BMA failure, it might leave the associated CDRs in the to-be-sent queue forever, even after the BMA becomes active.

- CSCse26153—RTSP: Wrong session creation due to referencing of uninitialized storage

An RTSP proxy in the network might send a different set of client ports, which could lead to a different session being created. As a result, RTSP traffic might be blocked, or might map to a catchall policy of **accounting type other** if one is configured.

- 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 longer exists.

- 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.

Caveats for 3.1(3)C6(5)

This section lists and describes all caveats, both open and resolved, that affect CSG software release 3.1(3)C6(5).

For information about open or unresolved caveats in the Content Services Gateway 3.1(3)C6(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)C6(5) - Open Caveats

The following list identifies open caveats in CSG Release 3.1(3)C6(5).

- 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.

Workaround: Take accounting out of service before removing the user group from the accounting configuration.
- CSCsc32220—The CSG forwards retransmitted SYN/ACKs from the server to the client

The CSG sends a SYN to the server to set up the half-proxy. The server responds with a SYN/ACK. The CSG sends the first request to the server, but the server does not receive the request. The server retransmits the SYN/ACK, which the CSG forwards to the client. (The CSG should drop the retransmitted SYN/ACK.)

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

 - The HTTP connection must match a CSG content configured with policies requiring HTTP deep packet inspection (**accounting type http**).
 - The server must retransmit the SYN/ACK.

Workaround: None.
- CSCsd27639—Improper passive FTP causes session IXP to crash

When server-initiated FTP or RTSP traffic is received from an unknown MAC address for more than 8 sessions, the CSG hangs, causing a reload.

Workaround: Make sure proper routing is defined such that the CSG learns source MAC addresses on the return path. You can do this by routing the return traffic through routers that are defined as gateways in the CSG.
- CSCsd42458—R7: Connection Timestamps wrong if HTTP session RST by CSG (quota server failed)

If the quota server fails, and a RADIUS Start adds a user to the User Table, and the CSG sends a RST when the client attempts an HTTP connection, then the final eight bytes of the Connection Timestamp TLV are incorrect.

Workaround: None.
- CSCsd65665—The CSG sends wrong interval usage value for time-based service

The CSG might send an incorrect interval usage value for a time-based service.

Workaround: None.

CSG Release 3.1(3)C6(5) - Closed Caveats

The following section lists bugs that are closed in CSG Release 3.1(3)C6(5).

- CSCeb55530—CSM not forwarding ICMP 3/4 to real server
ICMP type 3/4 messages are not forwarded by the CSG back to the server. This affects the path MTU discovery protocol, and might result in the server sending packets that are too large for the network.
- 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.
- CSCeh45290—CSG switchover to redundant chassis and offline issues during Sup SSO
CSGs installed on different chassis and configured for fault tolerance might failover to the standby CSGs during SSO switchover of the Supervisor Engine 720 with an MSFC3-BXL. The CSGs might also go offline.
- CSCei54668—HTTP requests using LF as end-of-line don't 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.
- CSCej23233—The CSG needs to obscure X-Forwarded-For header

The CSG can obscure the contents of the X-Forwarded-For header, overwriting it with blanks.

- If you want to obscure the contents of the X-Forwarded-For header, use the **variable** command in module CSG configuration mode to set the **CSG_OBSCURE_X_FORWARDED_FOR** environment variable to 1.
- If you do not want to obscure the contents of the X-Forwarded-For header, set the **CSG_OBSCURE_X_FORWARDED_FOR** to 0 (the default setting).

If your configuration is fault-tolerant, keep the following considerations in mind:

- Use the **variable** command in module CSG configuration mode to set the **CSG_FT_CONTENT** environment variable to 1. That is, replicate sessions only if replication is configured in the content.
- Do not configure the **replicate connection tcp** command in CSG content configuration mode.
- CSCej69307—CSG User Table element deleted on interim update
If you enter the **radius start restart session-id** command in CSG user group configuration mode, and a RADIUS Interim-Update is processed, the CSG might end the user's sessions, delete the existing User Table entry, and create a new User Table entry.
- CSCej78221—A CSG refund policy with more than 10 entries causes the Catalyst 6000 family switch to crash

If you enter more than 10 CSG IP or TCP refund flags, the system might become unresponsive and display the following error message:

```
%SYS-3-CPUHOG: Task is running for
(2000)msecs, more than (2000)msecs (49/45),process = Exec.
-Traceback= 41A28B24 402A12B0 4020E488 401E2BEC 401E2D00 401D6EB8
40524DD4 401E6090 402AD22C 402AD218
```

- CSCek33816—CSG can run out of memory when BMA down

When the Billing Mediation Agent (BMA) is down, the CSG continues to forward traffic and generate billing records, and the billing records continue to be buffered into the GTP storage pool. Depending on the user's configuration and traffic load, the resulting combination of a large **records max** value, many User Table entries, and a high session count can deplete the CSG's memory and cause it to reload or failover to the standby CSG.

As part of the CSG's health monitoring process, the CSG monitors itself for low memory conditions.

- If CSG memory usage exceeds a user-specified warning threshold, the CSG issues the following message:

```
% CSM_SLB-3-ERROR: Module 3 error: WARN - CSG memory usage exceeded 85%
(29M/256M)
```

By default, the CSG issues this warning message when memory usage exceeds 85%. To change that threshold, change the setting of the **CSG_MEM_WARN_THRESHOLD** variable (using the **variable** command in module CSG configuration mode). The range for this variable is 1 to 98; the default setting is 85.

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_MEM_WARN_FREQUENCY** variable. The range for the variable is 1 to 99; the default setting is 1.

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

```
% CSM_SLB-3-ERROR: Module 3 error: CRITICAL - CSG max memory reached 98%
(4M/256M)
```

By default, the CSG issues this depletion message when memory usage exceeds 98%. To change that threshold, change the setting of the **CSG_MEM_MAX_THRESHOLD** variable. The range for this variable is 1 to 98; the default setting is 98.

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_MEM_MAX_FREQUENCY** variable. The range for the variable is 1 to 99; the default setting is 1.

- If CSG memory usage exceeds a user-specified failover threshold, the active CSG performs a core dump, fails over to the standby CSG, and issues the following message:

```
% CSM_SLB-3-ERROR: Module 3 error: FAILOVER - CSG memory usage exceeded
98% (1M/256M)
```

By default, the CSG *does not* perform a core dump or failover, nor does it issue this failover message. If you want the CSG to take these actions, you must set a failover threshold by setting the **CSG_MEM_FAILOVER_THRESHOLD** variable. The range for the variable is 0 to 98; the default setting is 0 (no core dump, failover, or message).



Note

Configure this variable on only the active CSG or on the standby CSG, not on both. If you configure this variable on both the active CSG and on the standby CSG, and both CSGs exceed their failover thresholds, then the active CSG fails over to the standby CSG, which fails over to the active CSG, which fails over again to the standby CSG, and so on.

- CSCin97643—CSG crash caused by malformed TCP segment
The active CSG might fail over to the backup CSG when a new HTTP request/response follows the FIN from the client and server.
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 CSG Session must see FINs from both directions.
 - The CSG must receive an HTTP data packet that marks the start of a new request/response.
- CSCin97780—UDP trailer fragments dropped if Header fragments are the first packet of the session
The CSG drops a UDP trailer fragment if a UDP fragment is the first packet of a UDP connection on the CSG.
For this problem to occur, all of the following conditions must be met:
 - The client/server sends a UDP packet that is the first packet of the UDP connection.
 - The UDP packets is fragmented before it reaches the CSG.
 - The fragments reach the CSG in quick succession.
- CSCin97792—On abnormal termination of an HTTP POST, the CSG might charge the entire transaction
When an HTTP stream containing a POST message matches a content and policy with **accounting type http**, and the connection ends before the POST is completed, the CSG charges the entire transaction in upload bytes, even though the actual bytes transferred might be less.
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 browser request must use a POST method.
 - The connection must end before the data in the POST is sent by the client.
- CSCin98124—Malformed packets might cause the CSG to overcharge
The CSG might generate high volume CDRs, overcharging for a Layer 4 inspection, or for Layer 7 inspection downgraded to Layer 4 inspection.
For this problem to occur, all of the following conditions must be met:
 - The CSG must be performing Layer 4 inspection, or Layer 7 inspection that is downgraded to Layer 4 inspection.
 - A TCP segment from the client or server must have a malformed TCP header (that is, the TCP SN must be arbitrary).
 - The CDR generated for the inspection must have a high upload or download byte count.
- CSCin98647—Incorrect download statistics if new session packet is UDP fragments
When a new session is created on a UDP fragment packet, the final or intermediate download statistics might be incorrect.
For this problem to occur, all of the following conditions must be met:
 - The client/server must send a UDP packet which is the first packet of the UDP connection.
 - The UDP packet must be fragmented before it reaches the CSG.

- CSCin98775—SNMP: Unable to do snmpwalk after CSG module is hung
SNMP requests to a Catalyst 6000 family switch chassis might fail when the CSG hangs without rebooting.
- CSCin98918—[CSG] Sanity checks to prevent overcharging on downstream traffic
The CSG might generate high volume CDRs, overcharging for a Layer 4 inspection, or for Layer 7 inspection downgraded to Layer 4 inspection.
For this problem to occur, all of the following conditions must be met:
 - The CSG must be performing Layer 4 inspection, or Layer 7 inspection that is downgraded to Layer 4 inspection.
 - A TCP segment from the client or server must have a malformed TCP header (that is, the TCP SN must be arbitrary).
 - The CDR generated for the inspection must have a high upload or download byte count.
- CSCsc24273—R5.9: When memory is exhausted, the CSG cannot communicate with IOS
If the value configured on the **records max** command in CSG accounting configuration mode is very high, the CSG might crash or be unable to communicate with IOS when its memory is exhausted. The following message might appear on the syslog:
%ICC-4-HEARTBEAT: Card 9 failed to respond to heartbeat
- CSCsc29030—Wrong content length in HTTP POST causes the TCP connection to hang
When the CSG is performing HTTP deep packet inspection (**accounting type http**) for an HTTP session, and the client sends a POST with an invalid content length, the CSG might drop some packets and the session might hang.
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**).
 - A POST with data beyond the content length must be sent (that is, the end of the content must spill over into a subsequent packet). For example, the Content Length might be too short, or another request might be pipelined after the POST beyond the initial packet.
- CSCsc32274—Downgrade during pipeline connection causes CSG failover
The active CSG might fail over to the backup CSG when Layer 7 inspection of an HTTP pipelined connection is downgraded to Layer 4 inspection.
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 flow must have pipelined requests
 - The data flow must trigger a downgrade to Layer 4 inspection (that is, the HTTP request is a HEAD method, or the HTTP headers are malformed and cannot be parsed).
 - Timing must be very fast between requests. The next packet containing a new HTTP request must arrive between the time that the CSG decides to downgrade to Layer 4 inspection and the time that the same packet is forwarded.

- CSCsc32357—Buffer leak running server-side fragments and HTTP

If the CSG is configured for Layer 7 HTTP deep packet inspection, and the server sends an IP fragmented reply, the last packet in the reply is not part of a fragment, then the CSG might drop the packet and might not free buffers.

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**).
- There must be fragmented packets on the server side.
- The server must send an HTTP response that spans multiple fragmented packets.

- CSCsc33554—Layer 7 inspection stops when running low amounts of fragmented HTTP traffic

The active CSG fails over to the standby CSG when processing UDP fragments, or when processing many small HTTP transactions in a burst.

- CSCsc40052—The CSG drops GET on same TCP connection after token-stripping event occurs

If a GET request is sent on the same TCP connection on which a token-stripping event has occurred, the CSG drops the GET request.

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 GET request must be sent on the same TCP connection as the TCP connection on which the token-stripping event took place. If the GET is sent on a different TCP connection, the problem does not occur.
- Token-stripping must be configured for the user group, using the **verify confirmation** command in CSG user group configuration mode.
- Service verification must be configured for the service being used.
- The service verification response must be forward when used with token stripping.

- CSCsc41571—The CSG does not report the URL in the content authorization request

The CSG does not send a content authorization request for the RTSP data stream.

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 requested stream must be interleaved over TCP.
- The **interleaved** parameter must not be the first parameter in the Transport header returned by the server reply to the client SETUP method. For example, the following header triggers the problem because the **unicast;** parameter appears between the **TCP;** parameter and the **interleaved=0-1;** parameter:

RTSP/1.0 200 OK\r\n

Transport: RTP/AVP/TCP;unicast;interleaved=0-1;src=28c07001;mode=PLAY\r\n

- CSCsc43804—The CSG fails to forward packets with IP and TCP option length greater than or equal to 32 bytes

The CSG might not forward a packet that has both the IP and TCP option fields set to 32 bytes or more. The affected session might hang or reset.

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 packet must have both the IP and TCP option fields set to 32 bytes or more.
- 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.
- CSCsc56625—RTSP: UDP sessions maps to the default policy

If the Transport header in the REPLY from the server to a client SETUP request contains only a single server or client port, then while running RTSP traffic using UDP transport, the UDP packets map to a default policy configured with **accounting type other**.

- CSCsc60434—Add CSG remaining capacity metric

All CSG usage information has been consolidated into one number, CSG CPU Utilization, which presents a good overall picture of CSG capacity.

To display CSG CPU Utilization, first enable debugging output for the CPU, using the **debug ip csg cpu** command in privileged EXEC mode, then enter the **show module csg slot tech-support utilization** command.

```
Router# debug ip csg cpu
CSG CPU Utilization debugging is on

Router# show module csg 3 tech-support utilization

Resource Utilization:
Memory
  Available Memory      62%      155M
  Allocated Memory     31%       78M
  OS Static Memory      9%       22M

CSG CPU Utilization: 1m (0.0%), 5m (0.0%)
```

To disable debugging output for the CPU, enter the **no debug ip csg cpu** command in privileged EXEC mode.

- CSCsc67354—RTSP: UDP fragments lead to excess leakage/overcharge

UDP flows for a prepaid customer, with multiple fragment families, allow more bytes than the permitted quota.

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

- The data flow must be a session with a UDP transport layer.
- UDP packets must be fragmented before reaching the CSG.
- The flow must match a prepaid service.

- CSCsc79056—The CSG is unresponsive to commands, does not pass traffic, and does not reset
When the CSG is configured to run WAP or other prepaid traffic, under heavy load with large numbers of quota server responses, the CSG might become unresponsive to commands and might no reload.
- CSCsc81421—RTSP: The CSG does not support a TEARDOWN URL longer than the DESCRIBE URL
If the URL provided by the client in the TEARDOWN message is longer than the “presentation” URL, provided by the client in the DESCRIBE message, then the CSG does not tear down all associated UDP sessions to an RTSP stream. The CDRs are generated for one session (stream-id=0) when the client tears down the stream, but for the other session (stream-id=1) the CDRs are generated when the flow’s idle timeout occurs.
- CSCsc81476—The CSG parses a message sent to a virtual MAC address different from its own
Packets sent to a CSG virtual MAC address might be forwarded to other active CSGs. For example, if the CSGs use the same client and server VLANs, and the switch does not have an entry for the virtual MAC address in the mac-address-table, the packet is sent to all ports in the VLAN. As a result, multiple active CSGs might parse the same message. For instance, a RADIUS Accounting Start message might be processed by two active CSGs, even though it was directed to the virtual MAC address of only one of the CSGs. This creates duplicate subscriber entries in the User Tables of the active CSGs.
- CSCsc95096—The CSG does not forward some chunked POST messages spanning multiple packets
If the first HTTP request is split across packets, such that chunk-length and chunk-body are in separate packets, then the CSG might drop the first HTTP POST request with transfer-encoding:chunked.
- CSCsc97386—Retransmitted packets are not forwarded in some cases
A parsing failure in a pipelined GET request might cause some of the responses to be charged to the last policy. As a result, the CSG might not charge all packets to the correct HTTP deep packet inspection (**accounting type http**) policy.
- CSCsd26182—Pipelined POST causes Layer 4 inspection downgrade
When the CSG parses an HTTP POST request that spans one packet and part of another, the CSG stops parsing HTTP and downgrades the traffic flow to Layer 4 inspection.
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**).
 - A POST with data beyond the content length must be sent (that is, the end of the content must spill over into a subsequent packet). For example, the Content Length might be too short, or another request might be pipelined after the POST beyond the initial packet.
 - After the POST request, additional HTTP requests must be embedded.
- CSCsd41458—R7: Standby crash after 19 hours with 50K prepaid KUT entries
The standby CSG can leak memory when processing FTP sessions. (The active CSG processes the FTP sessions correctly.) If the standby CSG processes enough FTP sessions, it can exhaust memory and crash.
- CSCsd44642—CSG counter for lost records reported incorrectly
The CSG might count lost records incorrectly even though the records are written, processed, and counted correctly by the PSD.

- CSCsd45287—Microcode buffer leak when downgrading

When running HTTP deep packet Layer 7 inspection, the CSG's TCP IXP module might leak buffers if a session is downgraded to Layer 4 inspection, reducing the pool of free buffers. The downgraded session might then fail and reset.

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 session must be an HTTP 1.1 pipelined session.

- CSCsd47115—WAP 1.x incorrect byte count during 3-way handshake

The CSG undercharges the byte count for a WAP transaction.

While awaiting the final ACK for a transaction from the client, the CSG might close out the transaction prematurely and generate a billing record. The CSG allows the final ACK from the client to pass without charge.

- CSCsd59813—R5.11:layer 4 TCP session with OOO IP fragments cause the CSG to crash and failover

When a TCP stream matches a policy with **accounting type other** and there are out-of-order IP fragments, the active CSG might failover to the standby CSG.

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

- The connection must match a CSG content configured with policies configured with **accounting type other**.
- There must be out-of-order IP fragments (that is, an IP trailer fragment must appear before the header IP fragment).

Caveats for 3.1(3)C6(4)

This section lists and describes all caveats, both open and resolved, that affect CSG software release 3.1(3)C6(4).

For information about open or unresolved caveats in the Content Services Gateway 3.1(3)C6(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)C6(4) - Open Caveats

The following list identifies open caveats in CSG Release 3.1(3)C6(4).

- 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.

Workaround: Configure the first character of the header-name in uppercase, regardless of the case in the packet.

- CSCeh45290—CSG switchover to redundant chassis and offline issues during Supervisor SSO
CSGs that are configured for fault-tolerance in different chassis might change state from active to standby when a Supervisor SSO switchover occurs. In some cases, the CSG module might go offline.

Workaround: None. Reset the offline module to bring it back into service.

- CSCin97792—On abnormal term of an HTTP POST, the CSG may charge the entire transaction
When an HTTP stream containing a POST message matches a content and policy with **accounting type http**, and the connection terminates before the POST can complete, the CSG charges the entire transaction in upload bytes, even though the actual bytes transferred might be less.

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

- The HTTP connection must match a CSG content configured with policies requiring HTTP deep packet inspection (**accounting type http**).
- The browser request must use a POST method.
- The connection must terminate before the data in the POST is sent by the client.

HTTP Layer 7 charging is based on the inspection of TCP sequence numbers. The CSG tracks the beginning sequence number of each transaction and scans for the ending sequence number. The Content_Length header tells the CSG how many bytes it can skip before restarting analysis. This allows the CSG to off load forwarding of payload that it does not need to analyze.

Workaround: The FLAG field in the CDRs indicates that the session was abnormally terminated; this might be used by back-end systems to remove the charge.

- CSCsc09749—R5.9: CSG/microcode crash when removing user group from accounting
If the CSG is configured for prepaid, and there are ore 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.

Workaround: Take accounting out of service before removing the user group from the accounting configuration.

- CSCsc29030—Wrong content length in HTTP POST can cause TCP connection to hang
When the CSG is performing Layer 7 inspection of an HTTP session, if the client sends a POST with an invalid content length, the CSG might drop some packets and the session might hang.

Workaround: This is a violation of the protocol. If possible, remove the client from the network. In order for the CSG to pass this type of session correctly, it must be configured for Layer 4 inspection of HTTP traffic.

- CSCsc32220—The CSG forwards retransmitted SYN/ACKs from the server to the client
The CSG sends a SYN to the server to set up the half-proxy. The server responds with a SYN/ACK. The CSG sends the first request to the server, but the server does not receive the request. The server retransmits the SYN/ACK, which the CSG forwards to the client. (The CSG should drop the retransmitted SYN/ACK.)

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

- The HTTP connection must match a CSG content configured with policies requiring HTTP deep packet inspection (**accounting type http**).
- The server must retransmit the SYN/ACK.

Workaround: None.

- CSCsc32357—Buffer leak running server-side fragments and HTTP

If the CSG is configured for Layer 7 HTTP inspection, and the server sends a reply with IP fragments, and the last packet in the reply is not part of a fragment, then the packet might be dropped, and a buffer on the CSG might not be freed.

To view outstanding buffers, enter the **show module csg x tech-support processor 2** command, where *x* is the module number of the CSG. The outstanding buffers are displayed near the bottom of the output. These numbers fluctuate in a live network. Buffer allocate failures could be a sign of a buffer leak.

Workaround: Either run without server-side IP fragmentation, or reconfigure the CSG for Layer 4 inspection.

CSG Release 3.1(3)C6(4) - Closed Caveats

The following section lists bugs that are closed in CSG Release 3.1(3)C6(4).

- CSCei22277—Timerwheel crash observed after RTSP traffic and config changes

The timerwheel crashes during a specific sequence of configuring, testing, unconfiguring, and configuring, as follows:

- Configure a stateless prepaid CSG.
- Run RTSP traffic.
- Unconfigure the prepaid CSG.
- Configure a stateful setup.
- The timerwheel crashes.

- CSCei34455—HTTP pipelining with multipacket GETs might decrease browsing speed

When using a CSG policy with **accounting type http**, and the client uses HTTP pipelining, the client's browsing speed might be reduced.

Sample packet sequence:

- PKT1 HTTP response from the server. forwarded by the server.
- PKT1 is forwarded by the CSG to the client.
- The client sends a GET and also ACKS PKT1.
- The CSG needs more data for this request to analyze this request but does not ACK because of the pipeline condition.
- The server retransmits PKT1, and the CSG forwards PKT1 to the client.

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

- The HTTP connection must match a CSG content configured with policies requiring HTTP deep packet inspection (**accounting type http**).
- The client must pipeline the requests.
- The client must not respond with a naked ACK; instead, it must send a GET packet that ACKs the response.
- The client must send HTTP requests (that is, Method + URL + HTTP headers) that are long enough to span more than one packet.

- CSCei82018—R5.8: Timing issue when handling TCP RST

A heavy load of TCP connection cleanup processing can trigger a timing error in the CSG FIN/RST termination logic, and can cause the CSG to reboot. If the CSG is part of a stateful pair, the primary CSG fails over to the backup CSG.

- CSCei51834—RTSP volume-based prepaid might cause FPGA hang under stress

The CSG encounters an FPGA hang and crashes. The console displays the message: **IXP3 Software exception on task 'IXP3 SA-CORE (Ex 18)(0000000h)'**.

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 RTSP charging must be prepaid with **basis byte**.
- The quota server must be very slow in responding to quota requests. Delays of 25 seconds have been used to cause the problem.
- The CSG must be under heavy load.

Typical RTSP prepaid does not experience the error, as the key is that the quota server responses must be very slow for this error to occur.

- CSCei57256—Machine check or PPC exception and failover when processing bad headers

A CSG PPC exception or machine check can occur, followed by a failover to the backup.

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 HTTP headers must fail parsing.

This defect can also be triggered if the HTTP headers contain carriage-return and line-feed (CRLF) in the **field-name** of the **message-header** (ref: RFC 2616) due to erroneous handling of CRLF.

- CSCei60017—Need to RCP coredump

The CSG needs to be able to copy coredumps using RCP.

- CSCei60055—Unexpected PPC exception caused by packet tag mismatch in FPGA 2

The CSG logs an unexpected PPC exception. The CSG reboots and fails over to its standby. A core dump analysis shows a tag sequence error for FPGA 2.

- CSCei60542—Traceback after FT failover

After a fault-tolerance failover, the console shows the following traceback for the standby-to-active CSG:

```
CSG Quota Manager 10.0.250.153:3386 is active.State Transition Standby -> Active
Standby is Active now (no heartbeat from active unit)
Traceback - 0x001D4D54 0x001F4924 0x001F5900 0x00049BF8 0x001A73F4
```

- CSCei84012—A CSG failover occurs when resending a previously ACKed packet

The CSG might failover to the backup.

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 CSG must resend a packet that it has already ACKed.

For example, the CSG sends an ACK to a client if the CSG has received a packet containing HTTP headers, but the headers continue into a subsequent packet that the client has not yet sent. If the CSG needs to resend this packet because it was lost in transit to the server, a failover might occur.

- CSCei88777—SMTP session fails with postpaid billing plan and AoC

SMTP traffic hangs or does not complete properly when AoC is configured within a postpaid service definition.

- CSCeh89867—0 TCP uploaded bytes reported for HTTP get/response

The CSG might report 0 TCP Uploaded Bytes for an HTTP GET/RESPONSE transaction.

- CSCej03887—The CSG might reload during a spike of session flux due to internal overload

The CSG fails over to the backup CSG during heavy connection setup/cleanup load.

When many TCP connections are open and idle, and all need to be cleaned up simultaneously, the internal CSG TCP cleanup process might become overloaded, causing the primary CSG to fail and restart. The issue has a higher probability of occurring with idle connections matching a policy configured with **accounting type http**, but can occur with other TCP accounting types as well.

This issue might also occur if the CSG is driven with a large burst of TCP connection initiations beyond its performance limits

- CSCej05236—Add CSG **show encap** command

Add a CSG console command to show encap for troubleshooting packets was sent to a wrong station.

Syntax: **show encap** *ip-address netmask*

Examples:

```
CSG> show encap 172.18.45.1 255.255.255.255
```

```
172.18.45.1      /32    00-d0-00-33-a8-0a
```

```
CSG> show encap 20.0.0.0 255.0.0.0
```

```
20.0.0.0        /08    00-80-1c-a8-a8-80
```

```
CSG> show encap 10.10.28.88 255.255.255.255
```

```
Attempted to get info on RESERVED encap.
```

```
10.10.28.88     /32    encap not found!
```

This command does not show the encap for the local defined interfaces. If you try to do so, you receive the “Attempted to get info on RESERVED encap” response.

- CSCej29778—The CSG reports negative byte counts for HTTP

The CSG might report negative byte counts for HTTP.

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 timing of the internal processing must be such that the packet sequence numbers are subtracted incorrectly.

The CSG should detect the miscalculation and zero the byte counts for this transaction, thereby avoiding the negative value. Two statistics counters are added to the **show tech** command output to indicate that this code path is being triggered:

- **up-range= xxxxxxxx** for the upload direction.
- **down-range= yyyyyyyy** for the download direction.

This caveat is similar to CSCej34444, except that CSCej29778 is for **accounting type http** and CSCej34444 is for any other TCP accounting type.

- CSCej34444—The CSG reports negative TCP byte counts

The CSG reports negative TCP byte counts.

For this problem to occur, the flow must match a CSG content configured with a policy with an accounting type configured, and the timing of the internal processing must be such that the packet sequence numbers are subtracted incorrectly.

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

- The data flow must match a CSG content configured with a policy configured with an accounting type.
- The timing of the internal processing must be such that the packet sequence numbers are subtracted incorrectly.

The CSG should detect the miscalculation and zero the byte counts for this transaction, thereby avoiding the negative value. Two statistics counters are added to the **show tech** command output to indicate that this code path is being triggered:

- **up-range= xxxxxxxx** for the upload direction.
- **down-range= yyyyyyyy** for the download direction.

This caveat is similar to CSCej29778, except that CSCej29778 is for **accounting type http** and CSCej34444 is for any other TCP accounting type.

- CSCsa49901—NAT redirect Content Auth issues with URL-based browsing

When a transaction is content-authorized and NAT-redirected to an AoC server, and the second transaction is originated by the client over the same TCP connection, and the CSG does content authorization again, the HTTP transaction gets stuck in the CSG.

- CSCsa88774—CSG: Wrong byte count when server closes pipelined GET

When using HTTP pipelined traffic matching CSG Content Rules with **accounting type http**, if the CSG receives a FIN/ACK from the server side before all the data is received from the server, the CSG might report incorrect download bytes in the billing record.

- CSCsb33581—CSG not forwarding all of server's fragmented reply, then resetting connection

When using a client configured to pipeline HTTP requests, if a server response spans multiple fragmented packets, the CSG might not forward all of the server's fragmented response packets and then sends a RST to both the client and server.

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

- There must be fragmented packets on both client and server side.
- The client must be configured to pipeline HTTP requests.
- The server must send an HTTP response that spans multiple fragmented packets.

- CSCsb42319—RTSP session counts as terminated wrongly
If an RTSP stream is interrupted, and if the session stays idle for 10 seconds, then the CSG times out and closes the session, even if the idle timer for the content is configured with a higher value. this problem occurs on low speed 2G mobile, when there are many interruptions downloading the stream.
- CSCsb43394—RTSP stream does not terminate in duration based billing
During duration-based billing, the RTSP stream continues to play beyond the allocated quota. 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 RTSP service must be configured for duration-based billing.
 - A catchall content must be configured with **accounting type other**.
- CSCsb47507—CSG RSTs connection when multipart POST hits policy with header-maps
When an HTTP stream containing a multipart POST message matches a content and policy with **accounting type http** and a header map, then the CSG does not forward the POST to the server and RSTs the session.
- CSCsb68164—Out-of-order (OOO) FINs are processed, causing negative quota and overcharging
The CSG reports large overcharge and negative quota usage when a TCP FIN is received before the end of data.
For this problem to occur, all of the following conditions must be met:
 - The data flow must match a CSG content rule.
 - The policy must be configured with **accounting type http**.
 - The data flow must terminate with a FIN, but the FIN must be received by the CSG before the last data packet is received.
- CSCsb85008—RTSP - TCP byte counts off by one byte in failure cases
TCP byte counts can be off by one byte in the following situations:
 - When a TCP RST is sent after a TCP FIN. This can occur in both RTSP and FTP connection termination code.
 - When processing an ACK during teardown. This can result in the CSG updating the sequence number, which is not necessary and can result in the TCP byte count being off by one byte. This occurs only in RTSP code.
- CSCsc00967—R5.8: PPC negative TCP bytes for RTSP and FTP control sessions
The CSG might report huge usage for an RTSP or FTP control session, if the control session times out without seeing a packet from the server.
- CSCsc02365—Potential overcharge under certain abnormal server response scenarios
The CSG might overcharge pipelined HTTP transactions under certain connection failure scenarios. 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 must be pipelining the requests.

- The CSG must detect the end of a transaction (n) after receiving and buffering the server response packets for the next transaction ($n+1$). This can occur when there are multiple responses in one packet, and when responses arrive from the server faster than the CSG can analyze them.
- The HTTP connection must terminate abnormally, or it must be downgraded to Layer 4 processing, before all transactions have completed and while the CSG is still processing the previous transaction (n).

The overcharge applies to the next transaction ($n+1$) and is equal to the number of downloaded bytes for the previous transaction (n).

- CSCsc06834—R5.9: UDP fragments may be dropped by CSG

The CSG might drop IP fragments that use UDP as the transport protocol.

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

- IP packets that use UDP as the transport protocol must fragment before reaching the CSG.
- The RTSP flow must match a CSG content rule.
- The policy must be configured with **accounting type rtsp**, **accounting type wap**, and **accounting type other**.

- CSCsc08350—R5.9: CSG crash- with HTTP pipelining of different Methods

An IXP3 software exception occurs on task 'IXP3 SA-CORE (Ex 18)(00000000h).

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 HTTP traffic must be pipelined.
- Either the client must indicate FIN before all responses are received, or a pipelined HEAD or multipart request must occur after the first request in the packet.

- CSCsc10013—R5.9 FPGA3 exception 64 IC_WAITIX - icmd waiting to sync with ePacket

The CSG crashes with the following message:

!!!CORE DUMP <day> <date> <time>

!!!Version: 3.1(3)C<x>(<y>)

FPGA3 exception 64 IC_WAITIX - icmd waiting to sync with ePacket.

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 subscriber must be a prepaid user.
- The flow must be redirected (for example, for account Top-up or Advice of Charge).
- The subscriber's terminal must be actively pipelining at the time of the redirect.

- CSCsc12939—R5.9:RTSP sessions not torn down in the absence of DESCRIBE method

With certain players, the CSG does not correctly report the end of all flows in an RTSP stream when the stream ends. As a result, the following conditions occur:

- The CDR for one or more of the UDP flows is delayed until the idle timer expires. It still contains the correct correlators and byte counts, but it is delayed. Other than the delay, any volume or event charging is still correct.

- If using service duration billing, the duration charging is wrong by the amount of the idle timer.

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 player must fail to send a DESCRIBE message with a **presentation** URL. At the end of the stream, the player must use a TEARDOWN message with the **presentation** URL.

A teardown can be used to terminate all streams or an individual stream. If the teardown is intended for all streams, the URL is the **presentation** URL reported in the DESCRIBE; otherwise, the URL specifically matches the URL of an individual stream. In the latter case, the player is not sending a DESCRIBE message at the beginning of the RTSP session. Therefore, the CSG does not have a **presentation** URL. However, the TEARDOWN message *appears* to be a **presentation** URL. Since the CSG does not have a **presentation** URL to match against, the CSG does not terminate all of the streams. The RTSP RFC is vague in this area.

- CSCsc29237—R5.9a TCP byte count incorrect with missing or retransmitted SYN/SYNACK
When there are retransmitted SYNs and SYN/ACKs for an RTSP control session, the CSG can receive a SYN after receiving a SYN/ACK. This might result in the CSG reporting a zero TCP byte count for the RTSP CDR.

Caveats for 3.1(3)C6(3)

This section lists and describes all caveats, both open and resolved, that affect CSG software release 3.1(3)C6(3).

For information about open or unresolved caveats in the Content Services Gateway 3.1(3)C6(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)C6(3) - Open Caveats

The following list identifies open caveats in CSG Release 3.1(3)C6(3).

- 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.

Workaround: Configure the first character of the header-name in uppercase, regardless of the case in the packet.

- CSCeh45290—CSG switchover to redundant chassis and offline issues during Supervisor SSO

CSGs that are configured for fault-tolerance in different chassis might change state from active to standby when a Supervisor SSO switchover occurs. In some cases, the CSG module might go offline.

Workaround: None. Reset the offline module to bring it back into service.

- CSCeh85135—CSG SUP720 support missing for IPSERVICES images

The CSG support was omitted from 12.2(18)SXE1 images for SUP720-MSFC3-BXL for IP Service.

Workaround: Run `s72033-adventerprisek9_wan-mz.122-18.SXE1`.

- CSCeh89867—0 TCP uploaded bytes reported for HTTP get/response
The CSG might report 0 TCP Uploaded Bytes for an HTTP GET/RESPONSE transaction.
Workaround: None.
- CSCei34455—HTTP pipelining with multipacket GETs might decrease browsing speed.
When using a CSG policy with **accounting type http**, and the client uses HTTP pipelining, the client's browsing speed might be reduced.

Sample packet sequence:

- PKT1 HTTP response from the server. forwarded by the server.
- PKT1 is forwarded by the CSG to the client.
- The client sends a GET and also ACKS PKT1.
- The CSG needs more data for this request to analyze this request but does not ACK because of the pipeline condition.
- The server retransmits PKT1, and the CSG forwards PKT1 to the client.

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

- The HTTP connection must match a CSG content configured with policies requiring HTTP deep packet inspection (**accounting type http**).
- The client must pipeline the requests.
- The client must not respond with a naked ACK; instead, it must send a GET packet that ACKs the response.
- The client must send HTTP requests (that is, Method + URL + HTTP headers) that are long enough to span more than one packet.

Workaround: None.

- CSCei51834—RTSP volume-based prepaid might cause FPGA hang under stress
The CSG encounters an FPGA hang and crashes. The console displays the message: **IXP3 Software exception on task 'IXP3 SA-CORE (Ex 18)(0000000h)'**.

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 RTSP charging must be prepaid with **basis byte**.
- The quota server must be very slow in responding to quota requests. Delays of 25 seconds have been used to cause the problem.
- The CSG must be under heavy load.

Typical RTSP prepaid does not experience the error, as the key is that the quota server responses must be very slow for this error to occur.

Workaround: None, if prepaid volume-based RTSP billing is needed. The issue does not occur for duration-based nor event-based RTSP billing.

- CSCsa49901—NAT redirect Content Auth issues with URL-based browsing
When a transaction is content-authorized and NAT-redirected to an AoC server, and the second transaction is originated by the client over the same TCP connection, and the CSG does content authorization again, the HTTP transaction gets stuck in the CSG.

Workaround: Use URL-redirect instead of NAT-redirect.

- CSCsa88774—CSG: Wrong byte count when server closes pipelined GET
When using HTTP pipelined traffic matching CSG Content Rules with **accounting type http**, if the CSG receives a FIN/ACK from the server side before all the data is received from the server, the CSG might report incorrect download bytes in the billing record.
Workaround: None, if **accounting type http** is required.
- CSCsb33581—CSG not forwarding all of server's fragmented reply, then resetting connection
When using a client configured to pipeline HTTP requests, if a server response spans multiple fragmented packets, the CSG might not forward all of the server's fragmented response packets and then sends a RST to both the client and server.
For this problem to occur, the following conditions must all be met:
 - There must be fragmented packets on both client and server side.
 - The client must be configured to pipeline HTTP requests.
 - The server must send an HTTP response that spans multiple fragmented packets.**Workaround:** None.
- CSCsb42319—RTSP session counts as terminated wrongly
If an RTSP stream is interrupted, and if the session stays idle for 10 seconds, then the CSG times out and closes the session, even if the idle timer for the content is configured with a higher value. this problem occurs on low speed 2G mobile, when there are many interruptions downloading the stream.
Workaround: None.
- CSCsb43394—RTSP stream does not terminate in duration based billing
During duration-based billing, the RTSP stream continues to play beyond the allocated quota.
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 RTSP service must be configured for duration-based billing.
 - A catchall content must be configured with **accounting type other**.**Workaround:** None, if **accounting type rtsp** is required.
- CSCsb47507—CSG RSTs connection when multipart POST hits policy with header-maps
When an HTTP stream containing a multipart POST message matches a content and policy with **accounting type http** and a header map, then the CSG does not forward the POST to the server and RSTs the session.
Workaround: None, if **accounting type http** is required.

CSG Release 3.1(3)C6(3) - Closed Caveats

The following section lists bugs that are closed in CSG Release 3.1(3)C6(3).

- CSCef63149—Slow buffer leak running WAP1 connectionless traffic
WAP1 connectionless buffers might leak with 0 quota and exclude configured MMS options.

- CSCeh75241—The CSG should not grant quota when about to return it
If a CSG prepaid service is configured for **basis fixed**, and one or more new user transactions are processed while the CSG is gathering usage information for ongoing transactions, the CSG might use quota that should be returned to the quota server.
- CSCeh83785—CSG undercharges FTP control connection after quota return
The CSG might undercharge bytes and seconds for FTP control connections. The problem occurs when FTP control connections are mapped to a service that undergoes a quota return or tariff-switch. The CSG stops charging for usage after the time of the quota return or tariff switch for FTP control connections that start before the time of the quota return or tariff switch.
- CSCeh90027—Interleaved RTSP TCP upload byte count off by one
When performing RTSP downloads over TCP or HTTP, the TCP upload byte count for an RTSP interleaved connection is under-reported by one byte.
- CSCei00498—CSGR6.2:Wrong/unexpected frequent quota server reauthorizations for time-based billing
The CSG might immediately request additional quota via a service reauthorization request after the quota server grants quota in a service authorization response. The CSG might repeat this action indefinitely.
- CSCei03388—Initial WAP1 transaction not associated with a service
The username TLV is not located in a WAP CDR, or the first transaction of a WAP session is not associated with a service.
- CSCei03438—R5.7: RTSP RTP sessions might not close after session is complete
When an RTSP control session is created, but no corresponding UDP data sessions are established, the RTSP session block might leak. The RTSP session pool contains a non zero in-use value after all RTSP sessions have terminated and cleaned up.
- CSCei05465—CSG: New RTSP stream not correctly billed
When a second movie is downloaded by the same client before the UDP sessions for the first movie clean up or timeout, and the client and server both reuse the same UDP ports for the second movie, the UDP content for the second movie is either blocked or is not billed as RTSP traffic.
- CSCei09684—R5.7: Server RST and **accounting type http** might cause buffer leak
When running HTTP type traffic through an HTTP type content (filter type HTTP), some buffers might leak. Even under some stress, this appears to be a slow leak. The leak is caused when the CSG receives a server reset immediately following HTTP response data packets which the CSG determines need analysis to detect content length. This problem does not occur on normal FIN-terminated connections.
- CSCei19164—Support unknown packet drop for WAP1
Non-WAP traffic billed as **type wap** is passed through the CSG without charge. Non-WAP traffic is sent to WAP port 9200 or 9201, which is configured to be billed as WAP1 traffic.
To deal with this issue, we have added a new environment variable called `CSG_WAP_DROP_UNKNOWN_PACKETS`. When configured, the CSG drops all traffic that does not contain a valid WTP or WSP PDU type. Valid type values are defined in the WAP WTP/WSP specifications.
- CSCei28962—Uplink volume 0 for method HEAD
When using a CSG policy with **accounting type http**, the CSG does not account uplink traffic for the HTTP Head method.

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 must send an HTTP method HEAD.
 - The server must respond to the request.
- CSCei30534—WAPI.x concatenation breaks when used with next-hop
CSG R5.8 replaces the destination IP in the IP header with the IP Address of the **next-hop** of the policy.
 - CSCei41536—Problem in parsing RTSP return code
When the RTSP flow matches a content and policy configured with **accounting type rtsp**, the RTSP parsing for the return code from the server is incorrect. This results in an RTSP billing record being generated with an invalid RTSP return code.
 - CSCei57726—Rate limit the CSG GTP reject messages
In response to a GTP reject cause code message from BMA, the CSG sends a log message to the Supervisor. In some cases, the CSG could flood the Supervisor with many log messages and deplete EOBC buffers:

%EOBC-3-NOEOBCBUF: No EOBC buffer available. Dropping the packet.

This might result in degradation of CAT6k performance and might lead to an IOS crash.

- CSCsa94400—CSG sometimes does not report RADIUS Attributes in User Profile Request
If there is no User Table entry when data traffic for the user reaches the CSG, a sticky entry is created when a CDR is sent to the BMA. If a RADIUS message is received, the sticky entry is converted to a normal entry. The User Profile Request is sent to the quota server as part of the conversion processing, but the RADIUS attributes are not included.
- CSCsa95287—MIB OID csgQuotaMgrStats missing in the SNMPWALK
If you add a second user-group and accounting service to a configuration in prepaid mode, the CSG cannot retrieve the MIB quota server stats properly by either a manual MIB walk or by SNMP messaging. This is true for all the quota servers that are configured in both of the configured user-groups.
- CSCsa95306—SNMPWALK does not get all CSG user group information
If you add a second user-group and accounting service to a configuration in prepaid mode, the CSG cannot retrieve the MIB quota server stats properly by either a manual MIB walk or by SNMP messaging. This is true for all the quota servers that are configured in both of the configured user-groups.
- CSCsb12505—CSG crash with IXP3 Software exception
The CSG sporadically crashes, reporting an IXP3 crash. The **show tech** command shows **IXP3 Software exception on task 'IXP3 SA-CORE (Ex 18)(00000000h)'**.
- CSCsb12978—CSG: CDR record TCPcountbyte incorrect when getting TCP RST
When a TCP session for HTTP is closed in one direction (server-to-mobile) and that Mobile is sending a TCP RST, the CSG reports incorrect **downloadBytesTCP 1501767**.
- CSCsb18560—CSG is not blocking WAP traffic when billing plan UNKNOWN
The CSG does not block WAP 1.X traffic when the user is known but the billing plan is UNKNOWN.

- CSCsb20432—CSG sporadically sends invalid Content-Provider TLV in CDR
The CSG might sporadically generate a CDR that contains an invalid Content-Provider TLV, or subsequent TLVs following the Content-Provider TLV might be corrupt.
- CSCsb22063—Uploaded byte less if session FIN during processing of HTTP Continuation
When using a CSG policy with **accounting type http**, the CSG might not count all the volume of an HTTP request if the FIN is received before the CSG can forward the entire client request to the server.
- CSCsb22210—CSG not forwarding POST continuation packet if header greater than 1 packet in size
When using a CSG policy with **accounting type http**, HTTP Post requests with “Content-Type: multipart” that have long headers spanning more than one packet are not forwarded. External symptom is that the HTTP transaction does not complete.
- CSCsb30784—RADIUS Access Requests dropped when **no radius ack error** is configured
When **no radius ack error** is configured and data traffic is sent, some RADIUS Access Requests are dropped in the CSG.
- CSCsb33294—An HTTP request might be undercharged if IP Fragmented in Headers
HTTP inspection of IP fragmented traffic might undercharge when the fragments split the HTTP headers in the client request. Buffer counts in CSG Show Tech are incorrect.
- CSCsb33619—The CSG does not forward the request fragment
When HTTP pipelined requests spanning multiple packets are IP-fragmented, the user session might hang and reset.
- CSCsb36179—The CSG does not retransmit the whole fragment family when a server ACK is not received
If the initial transmit of a segment is lost in the CSG-to-server path, the CSG does not retransmit to the server all the fragments of a request which it has ACKed. This causes the session to hang and timeout.
- CSCsb37812—CSG does not forward header fragment to server
If pipelined HTTP requests are fragmented and a request spans multiple TCP segments, the head fragment might not be forwarded by the CSG, and the user session might hang and reset.

Caveats for 3.1(3)C6(2)

This section lists and describes all caveats, both open and resolved, that affect CSG software release 3.1(3)C6(2).

For information about open or unresolved caveats in the Content Services Gateway 3.1(3)C6(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)C6(2) - Open Caveats

The following list identifies open caveats in CSG Release 3.1(3)C6(2).

- 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.

Workaround: Configure the first character of the header-name in uppercase, regardless of the case in the packet.
- CSCeh45290—CSG switchover to redundant chassis and offline issues during Supervisor SSO

CSGs that are configured for fault-tolerance in different chassis might change state from active to standby when a Supervisor SSO switchover occurs. In some cases, the CSG module might go offline.

Workaround: None. Reset the offline module to bring it back into service.
- CSCeh83785—CSG undercharges FTP control connection after quota return

The CSG might undercharge bytes and seconds for FTP control connections.

The problem occurs when FTP control connections are mapped to a service that undergoes a quota return or tariff-switch. The CSG stops charging for usage after the time of the quota return or tariff switch for FTP control connections that start before the time of the quota return or tariff switch.

Workaround: Use a CSG release earlier than CSG R6.
- CSCeh85135—CSG SUP720 support missing for IPSERVICES images

The CSG support was omitted from 12.2(18)SX E1 images for SUP720-MSFC3-BXL for IP Service.

Workaround: Run `s72033-adventerprisek9_wan-mz.122-18.SXE1`.
- CSCsa49901—NAT redirect Content Auth issues with URL-based browsing

When a transaction is content-authorized and NAT-redirectioned to an AoC server, and the second transaction is originated by the client over the same TCP connection, and the CSG does content authorization again, the HTTP transaction gets stuck in the CSG.

Workaround: Use URL-redirect instead of NAT-redirect.
- CSCsa88774—CSG: Wrong byte count when server closes pipelined get

The CSG might report incorrect download bytes in the billing record. When pipelining, if the CSG receives a FIN/ACK from the server side before all the data is received from the server, the CSG creates an incorrect download bytes billing record.

Workaround: None.
- CSCsa94400—CSG sometimes does not report RADIUS Attributes in User Profile Request

The CSG might not include RADIUS attributes in User Profile Request.

If there is no User Table entry when data traffic for the user reaches the CSG, the CSG creates a sticky entry when a CDR is sent to the BMA. If a RADIUS message is received, the sticky entry is converted to a normal entry. The User Profile Request is sent to the Quota Server as part of the conversion processing, but the RADIUS attributes are not included.

The problem can also occur if the user database is used in conjunction with RADIUS inspection and the user database response is received before the RADIUS message arrives.

Workaround: RADIUS Start should be received by the CSG before user traffic.

- CSCsa95287—MIB OID `csgQuotaMgrStats` missing in the `SNMPWALK`
If you add a second user-group and accounting service to a configuration in prepaid mode, the CSG cannot retrieve the MIB quota server stats properly by either a manual MIB walk or by SNMP messaging. This is true for all the quota servers that are configured in both of the configured user-groups.
Workaround: Make sure all configurations for all the user-groups and accounting services are present before booting the switch. If you encounter this issue, resetting the CSGs corrects the problem. Taking both accounting services might also fix the problem.
- CSCsa95306—`SNMPWALK` does not get all CSG user group information
If you add a second user-group and accounting service to a configuration in prepaid mode, the CSG cannot retrieve the MIB quota server stats properly by either a manual MIB walk or by SNMP messaging. This is true for all the quota servers that are configured in both of the configured user-groups.
Workaround: Make sure all configurations for all the user-groups and accounting services are present before booting the switch. If you encounter this issue, resetting the CSGs corrects the problem. Taking both accounting services might also fix the problem.
- CSCeh75241—The CSG should not grant quota when about to return it
If a CSG prepaid service is configured for **basis fixed**, and one or more new user transactions are processed while the CSG is gathering usage information for ongoing transactions, the CSG might use quota that should be returned to the quota server.
Workaround: None.

CSG Release 3.1(3)C6(2) - Closed Caveats

The following section lists bugs that are closed in CSG Release 3.1(3)C6(2).

- CSCef68324—ICMPv6 packet trackback
Cisco Internetwork Operating System (IOS) software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.
Cisco has made free software available to address this vulnerability for all affected customers.
More details can be found in the security advisory that is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml>.
- CSCeg52941—CSG not releasing quota for L7 billing with some FTP servers
When using the CSG for prepaid billing of FTP sessions between the Windows XP FTP Client with a Bison FTP Server, additional quota might be reserved at the end of an FTP data session.
- CSCeg56767—CSG crash when server sending IP packet fragments out of order
If the server sends fragmented IP packets, and those packets arrive at the CSG out of order, the CSG might crash. This issue can occur with a VPN gateway that was not configured to avoid IP fragmentation, and with HTTP or other servers as well.
- CSCeh25758—Service verify token stripping fails with forward and disable set
If the forward action is set and the service verify disable bit is set, the service verify token is not stripped.

- CSCeh28088—Reserved quota not being cleared on backup CSG
The reserved quota field on the backup CSGs KUT might be set to a value even though it should be 0.
- CSCeh30390—CSG next-hop requires gateway to work with HSRP
CSG users who use HSRP must configure a route or default gateway for the HSRP standby/virtual IP address. This enables the CSG to actively monitor the HSRP HELLO message, to track the physical IP and MAC addresses of the HSRP devices. With this HSRP monitoring, the CSG can properly forward the return traffic to the standby/virtual HSRP IP address.
- CSCeh34425—Bytes counts incorrect for ftp control conn cdr if CSG_FTP_PWD=1
If the variable CSG_FTP_PWD is set to 1, the IP and TCP byte counts are incorrect for the CDR generated for the FTP control connection. The byte counts are less than they should be. The CDR for the data connection is correct.
- CSCeh35817—CSG R6: RTP UDP packets not forwarded to client
In a configuration with next-hop addresses in both the client-to-server and server-to-client directions, RTSP data traffic utilizing UDP transport is not forwarded from the server to the client.
- CSCeh37850—Possible for TCP download bytes to be 0 for HTTP1.0 connections
If there is an HTTP 1.0 request, and the response has a body, but no content-length, then the TCP downloaded bytes can be 0 for an HTTP1.0 connection.
- CSCeh42735—RTSP support for TCP payload in multiple IP packets
Traffic on an RTSP data session might be blocked or not associated with the RTSP content definition. RTSP control traffic for specific methods (that is, SETUP/SETUP RSP) must extend into multiple IP packets, and the packet boundaries must split the method between the start of method and the transport header in the case of a SETUP request.
- CSCeh45087—HTTP responses with no content-length TCP bytes not counted for HTTP1.0
If an HTTP1.0 client receives multiple responses from the HTTP server and there is no content-length field specified in those response, only the first response TCP download bytes are counted. The rest are not. None of the responses are counted for TCP download bytes. HTTP1.1 works fine.
- CSCeh46733—RTSP connection without traffic fails to clean up
RTSP content objects that are no longer being used might be displayed in the output of a **show** command. Storage for these objects might not be freed.
- CSCeh47498—The CSG does not forward the FTP PASV command with next-hop
The CSG might not forward FTP control session packets when next-hop routing is specified.
- CSCeh48419—HTTP billing incorrect if Content-Length in HTTP response is wrong
If the server initiates a connection teardown (that is, the server sends the first FIN), and the Content-Length field in the HTTP response is incorrect, the CSG might incorrectly charge for the TCP bytes downloaded in an HTTP Stats record.
- CSCeh49535—HTTP transaction billed incorrectly if Content-Length ends with LFLF
The CSG might bill incorrectly when viewing pages on older Web servers. Some older Web servers end HTTP headers with an LF character, rather than a CRLF character. Under some conditions, this can lead to improper parsing by the CSG. Any further traffic on the same session is billed to the preceding properly parsed policy.

- CSCeh49848—SMTP with AoC exceeds quota when sending attachments
For SMTP traffic that encounters a service configured for content authorization (AoC), user traffic is not stopped when quota is exceeded.
- CSCeh50765—Crash if accounting taken out-of-service during RTSP
The CSG crashes if accounting is taken out-of-service while RTSP traffic is flowing.
- CSCeh54057—I6: Standby CSG reloaded during stress & failover of HTTP L7 sessions
The standby CSG might reload when existing HTTP1.1 sessions are failing over from the primary CSG during a period with a high rate of connection establishment.
- CSCeh56276—Layer 4 content TCP byte counts too low if fragmentation occurs
The CSG might undercharge TCP bytes for fragmented traffic if the flows match a Layer 4 policy/content. The CSG reports low TCP upload byte counts if the fragments are received on the client side, and low TCP download byte counts if the fragments are received on the server side.
- CSCeh56485—CSG: R6 Prevent User Table overwrite when **no radius ack error** is enabled
With **no radius ack error** enabled, existing User Table entries can be stolen when the User Table is full and a new Start is received.
- CSCeh56504—RTSP stream download hangs when configured with AoC
When performing AoC with RTSP data, a timing situation can cause the download to fail. If the AoC request/reply for a stream completes before traffic for the second UDP data session (corresponding to the stream) is seen, the UDP session can hang, preventing traffic from following on that session.
- CSCeh63465—Correlators ID in Content Authorization Request and the related SMTP do not match
Correlators ID in Content Authorization Request and the related SMTP CDR do not match exactly.
- CSCeh66663—Uplink/downlink byte reporting change
Uplink/downlink byte counts in quota server messages and service-level CDRs cannot be mapped to client and server bytes. Traditionally, uplink bytes are bytes from the initiator of the session. The server-init flag in CDRs is used to determine direction and thus client/server bytes can be deduced. However, in quota server messages and service-level CDRs a server-init flag cannot be used, as information from multiple sessions is reported. As a result, client/server bytes cannot be deduced from these messages/CDRs.
- CSCeh68849—The CSG dumps its core due to LaminarStack issue
The CSG crashes. Output indicates:
!!!CORE DUMP FRI APR 01 16:37:50 2005
!!!Version: 3.1(3)C5(6)
PPC exception type 512 on 'LaminarStack(...)'
- CSCeh68856—CSG dumps its core due to TimerWheel issue
The CSG crashes and generates a core dump. The Message shown is “PPC exception type 512 on 'TimerWheel(0D984A78h)'.”
- CSCeh73605—The CSG may reload under stress with small intermediate trigger configured
When the CSG is under stress and intermediate report is configured with a small byte count or time interval, the CSG might generate many stats messages and reloads.
- CSCeh80190—Using WAP with next-hop has issues
If a next-hop IP address is defined in the WAP policy being used, WAP 1.x packets might be dropped.

- CSCeh86704—FTP timeout flag in CDR not always accurate
When the FTP control connection is reset by the client or server, the TCP timeout flag in the IPv4I4Flow TLV might be set in FTP TCP records, when the connection was actually reset and did not time out.
- CSCeh89867—0 TCP uploaded bytes reported for HTTP get/response
The CSG might report 0 TCP Uploaded Bytes for an HTTP GET/RESPONSE transaction.
- CSCsa64249—CSM may core dump while processing ICMP dest-unreachable packet
The CSM might core-dump while processing an ICMP destination-unreachable packet.
 - The syslog message shows, “... unexpected error: PPC exception encountered.”
 - The core-dump shows, “PPC exception type 512 on LaminarStack...”
 - The stack show the function crashed at session_get_entry().
- CSCsa74033—SYN and FIN packets still counted in FTP control session byte count
When using the CSG for FTP connection accounting, the CSG is still counting TCP SYN and FIN packets as one byte each in the FTP control sessions byte-count.
- CSCsa74366—R5.6: OOO packets causes CSG to report negative quota
Out of Order packets can cause the CSG to miscalculate byte counts.
- CSCsa76004—CSG may fail to associate UDP streams with RTSP session
When there is RTSP traffic flowing through a CSG, and client attempts to start 3 or more streams per TCP control session, the CSG might fail to associate the actual UDP RTP traffic with the RTSP control session, and therefore might fail to set the correct correlator values in the UDP CDRs.
- CSCsa78116—The CSG sends ACK with old seqnum, fails to reACK client retransmits
When parsing HTTP headers that span more than one packet, the CSG generates an ACK to request the next packet. If the server has already sent data for a previous request in the persistent connection, the ACK is sent with the wrong (old) TCP sequence number. Most clients accept the ACK anyway, but some ignore it and retransmit their requests. The CSG subsequently drops these retransmits rather than attempting to ACK them.
- CSCsa81477—HTTP page not loaded due to server ACK not processed
HTTP web pages with multiple embedded objects occasionally fail to load with the Sanyo S750 handset.
- CSCsa85282—The CSG does not retransmit HTTP GET if server ACK is not received
If a TCP packet which is sourced by the CSG is not acknowledged by the receiving endpoint, the CSG fails to retransmit the packet. This occurs only for HTTP flows that match an HTTP Layer 7 (**accounting type http**) policy. Packets that the CSG has sourced include SYN/ACK to the client, SYN to the server, and any HTTP packet for which CSG has built and sent its own ACK. An example of the latter case is an HTTP request (GET, POST, and so on) that was ACKed by the CSG to the client to trigger sending of more packets for further header analysis and was later forwarded by the CSG to the server. By building its own ACK, the CSG takes ownership of the packet and must retransmit if delivery to the server fails.
- CSCsa91424—Interval Usage Seconds sometimes appears to be a cumulative value
The CSG might report cumulative values as Interval Usage Seconds.

- CSCsa91620—CSG exception processing fragmented WAP 1.0 traffic
A PPC exception type 666 on BillingStack is seen while performing Layer 7 WAP inspection of non-WAP traffic that contains IP fragments. For example, WAP inspection might be attempted on encrypted WAP traffic, which cannot be done.
- CSCsa94380—The CSG sends invalid Content-Provider TLV in CDR
The CSG sends CDRs to the BMA server that might contain Content-Provider TLVs that contain incorrect data and are not structured correctly.

Documentation and Technical Assistance

This section contains the following information:

- [Related Documentation, page 64](#)
- [Cisco IOS Documentation Set, page 65](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 65](#)

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)C6(2)*

- 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, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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>

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

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, 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. (0809R)

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.