Cisco
Content Services Gateway - 2nd Generation Release 2.0 Installation and Configuration Guide

Cisco IOS Release 12.4(15)MD
December 13, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-15491-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

• Turn the television or radio antenna until the interference stops.

• Move the equipment to one side or the other of the television or radio.

• Move the equipment farther away from the television or radio.

• Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned 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. (1110R)

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.

Cisco Content Services Gateway - 2nd Generation Release 2.0 Installation and Configuration Guide, Cisco IOS Release 12.4(15)MD
Copyright ©2012 Cisco Systems, Inc. All rights reserved.

CONTENTS

Document Revision History xiii

Audience xiii

Organization xiv

Conventions xiv

Related Documentation xv

Obtaining Documentation and Submitting a Service Request xvi

CHAPTER 1 **Overview** 1-1

What's New 1-1

CSG2 Features 1-2

Comparison of CSG1 and CSG2 Hardware Architectures 1-3

MIB Support 1-4

CSG2 Billing Criteria 1-5

CSG2 Interactions with External Entities 1-5

CDR Support 1-6

Fixed CDR Support for HTTP, IMAP, RTSP, and WAP 1-7

Single CDR Support for HTTP and WAP Connectionless 1-7

Service-Level CDR Summarization 1-7

Prepaid and Postpaid Envelope Information Support for SMTP 1-7

Fixed Attribute CDRs for WAP 1-7

Byte Counting 1-8

Byte Counting Overview 1-8

HTTP Byte Counting 1-9

WAP Byte and Packet Counting 1-10

IMAP Byte Counting 1-11

FTP and RTSP Byte Counting 1-12

SIP Byte Counting 1-12

POP3 and SMTP Byte Counting 1-12

Byte and Packet Counting After a Failover 1-12

CSG2 User Table 1-12

CSG2 Interface Awareness 1-13

BMA Features 1-13

Quota Server Features 1-14

Service Features 1-15

IPC Features 1-15
PSD Features 1-16
iSCSI Features 1-16
RADIUS Features 1-16
HTTP Features 1-17
HTTP Pipelining and Chunked Transfer Encoding 1-17
Support for Multipart HTTP 1-18
HTTP 1.0 Content Billing 1-18
HTTP 1.1 Content Billing 1-18
HTTP Records Reporting Flexibility 1-18
HTTP Error Code Reporting 1-18
Learning Client IP Addresses Using Inspection of HTTP X-Forwarded-For Headers 1-18
SIP Features 1-19
WAP Features 1-19
WAP Traffic 1-19
WAP 2.0 1-20
Support for WAP Segmentation and Reassembly (SAR) 1-21
RTSP Features 1-21
RTSP Billing 1-22
Per-Click Authorization 1-22
Correlation 1-22
POP3 Support 1-26
SMTP and POP3 Billing 1-26
SMTP CDR Header Removal 1-27
FTP Billing 1-27
Header, Method, and URL Mapping 1-27
Service Duration Billing 1-27
Charging for Service Duration Billing 1-28
Calculating Usage for Service Duration Billing 1-28
Reporting Quadrans to the Quota Server and to the BMA 1-31
Handling Out-of-Quota Conditions 1-31
Connection Duration Billing 1-32
Postpaid Service Tagging 1-33
Stateful Redundancy and Failover 1-33
“Default” Policy 1-34
Tariff Switch 1-34
Prepaid Error Reimbursement 1-35
Postpaid Billing 1-36
Prepaid Content Billing and Accounting 1-36
Obtaining User IDs 1-38

Filtering Accounting 1-38
Intermediate CDRs 1-38
Packet Forwarding 1-39
URL-Redirect 1-39
Supplemental Usage Reports 1-39
Enhanced Interoperability with Cisco Service-Aware GGSN 1-39
Miscellaneous Features 1-40
IP Fragment Support for All Protocols 1-40
Support for Out-of-Order Packets for All Protocols 1-40
Asynchronous Service Stop 1-40
Support for Port Number Ranges 1-40
Packet Counts 1-40
Negative Quadrans 1-41
Enhancements for Layer 2 1-41
CSG2 Prerequisites 1-41
CSG2 Restrictions 1-41

CHAPTER 2 **Configuring the CSG2** 2-1
Preparing to Install the CSG2 Software 2-1
Installing the CSG2 Software 2-3
Upgrading the CSG2 Software 2-7
Saving and Restoring CSG2 Configurations 2-7
Configuring the CSG2 2-8
Configuring the User Database 2-9
Configuring the CSG2 User Table 2-9
Configuring the Fragment Database 2-11
Configuring the Session Table 2-11
Configuring URL-Redirect 2-11
Configuring Policies and Traffic Types 2-13
Configuring a Content Billing Service 2-13
Configuring Content 2-14
Configuring Single-TP Mode 2-16
Configuring Fixed, Variable, or Combined Format CDR Support 2-17
Fixed CDR Support for HTTP and WAP 2-17
Fixed CDR Support for IMAP 2-18
Fixed CDR Support for RTSP 2-18
Single CDR Support for HTTP and WAP 2-18
Specifying the CDR Format 2-18
Configuring a Refund Policy on the CSG2 2-18

Configuring HTTP Header Reporting 2-19
Configuring SMTP CDR Header Removal 2-19
Configuring Supplemental Usage Reporting 2-20
Configuring Actual PDU Reporting for WAP 2-20
Configuring Maps for Pattern-Matching 2-21
Configuring Connection Redundancy 2-21
Configuring High Availability 2-21
Components That Provide HA 2-22
Enabling HA 2-23
Configuring a Secondary IP Address for HA 2-23
Synchronizing Clocks for HA 2-24
Modifying an HA Configuration 2-24
Distributed Crash Data Collection 2-25
Configuring HA for CSG2s in Different Chassis 2-25
Classifying Data Traffic 2-26
Configuring a CSG2 Subscriber Interface 2-26
Configuring Case Sensitivity 2-26
Configuring WAP and WSP Support 2-27
Counting Bytes and Packets 2-27
Incomplete WAP Transactions 2-27
Multimedia Messaging Service 2-27
Blocking Ports 2-28
Configuring SNMP Timers 2-28
Configuring the SAMI Bit Rate Limit 2-29
Configuring the SNMP Notification Types 2-29
CSG2 Configuration Examples 2-29
Sample Configuration for Subscriber-to-Subscriber Traffic 2-29
Configuring Next-Hop for a Subscriber-to-Subscriber Content 2-30
Configuring Reverse Next-Hop for a Subscriber-to-Subscriber Content 2-30
Configuring Prepaid Subscriber-to-Subscriber Contents for a Service 2-31
Sample Configuration for HTTP X-Forwarded-For 2-31
Sample Configuration for High Availability 2-32
HA Configuration on the Active CSG2 2-32
HA Configuration on the Standby CSG2 2-33
Sample Configuration for HA Peer Connectivity 2-34
Sample Configuration for Supervisor Engine Side 1 2-34
Sample Configuration for CSG2 Side 1 2-35
Sample Configuration for Supervisor Engine Side 2 2-35
Sample Configuration for CSG2 Side 2 2-35
Displaying Port-Channel Information for One Side 2-36

Configuring CSG2 Network/Subscriber Traffic 2-38
Sample Configuration for IPv4-Aware VRF 2-39

CHAPTER 3 **Configuring BMA Support** 3-1
Configuring the BMA Local Port 3-1
Configuring a BMA 3-2
Configuring the BMA Keepalive Time 3-2
Configuring the BMA GTP' Message Buffer 3-3
Configuring the BMA Retransmit Time 3-3
Configuring the BMA Retry Number 3-4
Configuring the BMA Window Size 3-4
Configuring BMA Load Sharing 3-4
Reporting the Billing Plan ID to the BMA 3-5

CHAPTER 4 **Configuring Quota Server Support** 4-1
Configuring the Quota Server Local Port 4-2
Configuring a Quota Server 4-2
Configuring the Quota Server Keepalive Time 4-3
Configuring the Quota Server GTP' Message Buffer 4-3
Configuring the Quota Server Retransmit Time 4-3
Configuring the Quota Server Retry Number 4-4
Configuring the Quota Server Window Size 4-4
Configuring Quota Server Load Sharing 4-5
Reassigning Subscribers to a New Quota Server 4-5
Quota Push 4-5
Replacing Quota Balance 4-6
Delaying Quota Reauthorization 4-6
Asynchronous Quota Return 4-7
Reporting the Billing Plan ID to the Quota Server 4-7
Pricing by Quota Server Configuration Example 4-7
Differentiating Prices Configuration Example 4-8
Reducing the Number of Services Configuration Example 4-9

CHAPTER 5 **Configuring Service Support** 5-1
Configuring a Basic Content Billing Service 5-2
Configuring the Billing Basis for a Service 5-2

Specifying a Service Owner 5-3
Specifying a Service Class 5-3
Configuring a Service Idle Time 5-4
Configuring Advice of Charge 5-4
Enabling AoC URL-Rewriting 5-6
Configuring an AoC Token 5-7
Configuring AoC URL-Appending 5-7
Redirect Flexibility 5-8
Configuring Service Verification 5-8
Enabling Service Verification URL-Rewriting 5-9
Configuring a Service Verification Token 5-9
Enabling Service-Level CDR Summarization 5-10
Configuring Passthrough Mode and the Default Quota 5-11
Flagging of Messages 5-12
User Profile Requests 5-12
Quota Server Recovery 5-12
Configuring Metering 5-12
Configuring an Initial Quota for Metering 5-13
Configuring a Minimum Quota for Metering 5-13
Configuring a Debit Increment for Metering 5-14
Excluding RTSP PAUSE from Metering 5-14
Including IMAP Bytes in Metering 5-15
Excluding MMS from Metering 5-17
Excluding the Final Service Idle from Metering 5-17
Configuring the Quota Reauthorization Threshold 5-18
Configuring the Quota Reauthorization Timeout 5-18
Enabling a Refund Policy for a Service 5-19

CHAPTER 6 **Configuring IPC Support** 6-1
Configuring the IPC Keepalive Time 6-1
Configuring the IPC Retransmit Time 6-1
Configuring the IPC Retry Number 6-2
Changing the IPC Crash Dump Setting 6-2

CHAPTER 7 **Configuring PSD Support** 7-1
Configuring the PSD Local Port 7-2
Configuring the PSD 7-2

Configuring the PSD Packet Drain Settings 7-2
Configuring the PSD Keepalive Time 7-3
Configuring the PSD GTP' Message Buffer 7-3
Configuring the PSD Retransmit Time 7-4
Configuring the PSD Retry Number 7-4
Configuring the PSD Window Size 7-5

CHAPTER 8 **Configuring iSCSI Support** 8-1
iSCSI Overview 8-1
Configuring an iSCSI Target Interface Profile on the CSG2 8-2
Associating an iSCSI Target Interface Profile with the CSG2 8-3
Configuring the iSCSI Packet Drain Settings 8-4
Verifying the iSCSI Session 8-4

CHAPTER 9 **Configuring RADIUS Support** 9-1
Configuring RADIUS Proxy 9-2
Configuring RADIUS Endpoint 9-3
Configuring RADIUS Handoff 9-4
Configuring RADIUS Packet of Disconnect 9-5
Configuring RADIUS Monitor 9-6
RADIUS Attributes and VSA Subattributes 9-7
RADIUS Attributes Required for CSG2 User Table 9-7
Deleting Entries from the CSG2 User Table 9-8
Reporting RADIUS Attributes and VSA Subattributes 9-9
Enabling Roaming Service Control 9-10
Retrieving the Billing Plan ID from RADIUS 9-11
RADIUS Subscriber Cleanup 9-12
RADIUS Error Acknowledgment 9-12
RADIUS Correlation Processing 9-13

CHAPTER 10 **Configuring Prepaid Support** 10-1
Configuring a Prepaid Billing Plan 10-1
Prepaid WAP Support 10-2

APPENDIX A **CSG2 Command Reference** A-1

APPENDIX B **CSG2 Command History—CSG1 R7 to CSG2 R1** B-1

Unchanged Commands B-1
New Commands B-2
Deleted Commands B-3
Changed Commands B-5
Changes to Module CSG Configuration Mode B-10
Changes to Module CSG VLAN Configuration Mode B-10
Changes to Accounting Configuration Mode B-11
Changes to Billing Configuration Mode B-12
Changes to Block Configuration Mode B-12
Changes to Content Configuration Mode B-12
Changes to Map Configuration Mode B-13
Changes to Policy Configuration Mode B-13
Changes to Refund Configuration Mode B-14
Changes to Ruleset Configuration Mode B-14
Changes to Service Configuration Mode B-14
Changes to SNMP Timer Configuration Mode B-15
Changes to Transport-Type Configuration Mode B-15
Changes to User Group Configuration Mode B-16
Changes to Weight Configuration Mode B-17

APPENDIX C **CSG2 Command History—CSG2 R1 to CSG2 R2** C-1

New Commands C-1
Deleted Commands C-2
Changed Commands C-2

APPENDIX D **Protocol Compliance Statements for the CSG2** D-1

Layer 4 Inspection (parse protocol=other) D-1
Layer 7 Inspection (parse protocol=specific protocol) D-1

APPENDIX E **CSG2 System Messages** E-1

CSG2 System Messages E-1
Message: Configuration download error: %s E-1
Message: %s E-2

Message: Startup configuration completed. E-2
Message: Configuration Sync error: %s E-2
Message: %s E-2
Message: %s packet drop: queue size %d reached, record storage %s is currently %s E-3
Message: GTP error: %s E-3
Message: GTP received reject cause code %d from %i:%u E-3
Message: GTP state change: %s E-4
Message: IPC is link failed to processor %u, state = %u, software reloading card now. E-4
Message: %s E-4
Message: iSCSI device %i:%u is full E-5
Message: ISCSI state change: %s E-5
Message: %s transaction discarded due to high load. E-5
Message: Failed to set %s local port. Either there are no IP addresses configured or port %u is in use. E-6
Message: Lock depth %u has crossed threshold. E-6
Message: CSG NTP synchronization is complete E-6
Message: Error: %s E-7
Message: PSD device %i:%u is full E-7
Message: CSG replicate condition: %s E-7
Message: Error: %s E-8
Message: Unexpected condition: %s E-8
SAMI System Messages E-8
Message: Nvram CRC Failure: %d\n E-8
Message: Nvram Erase Failure: handle 0x%x, offset 0x%x, error %s E-9
Message: Nvram Init Failure of flash device at %d:%s E-9
Message: Nvram Init Failure: %s E-9
Message: Nvram Magic Corrupt: Present %d Expected %d\n E-9
Message: Nvram Write Failure: handle 0x%x, offset 0x%x, numbytes 0x%x error %s E-10
Message: Nvram Write Config Failure: \n E-10
Message: Unexpected condition: %s E-10
Message: Unexpected condition: %s E-10
iSCSI System Messages E-11
Message: Error: %s E-11
Message: Error: %s E-11
Message: Warning: %s E-11

APPENDIX F **Monitoring Notifications** F-1
SNMP Overview F-1
MIB Description F-2

SNMP Notifications F-2
SNMP Versions F-3
SNMPv1 and SNMPv2c F-3
SNMPv3 F-4
SNMP Security Models and Levels F-4
Requests for Comments F-4
Object Identifiers F-5
Related Information and Useful Links F-5
TAC Information and FAQs F-5
SNMP Configuration Information F-5
Configuring MIB Support F-6
Determining MIBs Included for Cisco IOS Releases F-6
Downloading and Compiling MIBs F-6
Considerations for Working with MIBs F-7
Downloading MIBs F-8
Compiling MIBs F-8
Enabling SNMP Support F-8
Enabling and Disabling SNMP Notifications F-9
Enabling and Disabling CSG2 Notifications via the CLI F-9
Enabling and Disabling CSG2 SNMP Notifications via SNMP F-10

About This Book

This preface describes who should read the *Cisco Content Services Gateway - 2nd Generation Release 2.0 Installation and Configuration Guide*, Cisco IOS Release 12.4(15)MD, how it is organized, and its document conventions.

This publication does not contain instructions for installing the Cisco 7600 series router. For information on installing the router, see the Installation Guide that came with your router.

Document Revision History

The following table lists the major changes made to this document each release, with the most recent changes listed first.

Revision	Date	Change Summary
OL-13795-01	June 29, 2007	First publication.
OL-13795-01	September 17, 2007	Minor updates.
OL-15491-01	June 1, 2008	Major changes in support of the CSG2 Release 2.
OL-15491-01	October 31, 2008	Minor updates.

Audience

This publication is designed for network administrators and other people who are responsible for setting up, installing, configuring, and operating the CSG2.

Only trained and qualified service personnel (as defined in IEC 60950 and AS/NZS3260) should install, replace, or service the equipment described in this publication.

Organization

This publication is organized as follows:

Chapter	Description
Chapter 1, “Overview”	Presents an overview of the Cisco Content Services Gateway 2 (CSG2).
Chapter 2, “Configuring the CSG2”	Describes how to configure VLANs, virtual servers, billing, and other configuration tasks on the CSG2.
Chapter 3, “Configuring BMA Support”	Describes Billing Mediation Agent (BMA) features and configuration details.
Chapter 4, “Configuring Quota Server Support”	Describes quota server features and configuration details.
Chapter 5, “Configuring Service Support”	Describes content billing service features and configuration details.
Chapter 6, “Configuring IPC Support”	Describes Interprocessor Communication (IPC) features and configuration details.
Chapter 7, “Configuring PSD Support”	Describes Cisco Persistent Storage Device (PSD) features and configuration details.
Chapter 8, “Configuring iSCSI Support”	Describes Internet Small Computer Systems Interface (iSCSI) features and configuration details.
Chapter 9, “Configuring RADIUS Support”	Describes RADIUS features and configuration details.
Chapter 10, “Configuring Prepaid Support”	Describes prepaid features and configuration details.
Appendix A, “CSG2 Command Reference”	Describes the commands that allow you to set up and monitor content billing on the CSG2.
Appendix B, “CSG2 Command History—CSG1 R7 to CSG2 R1”	Describes the changes to commands between the CSG1 and the CSG2 Release 1.
Appendix C, “CSG2 Command History—CSG2 R1 to CSG2 R2”	Describes the changes to commands between the CSG2 Release 1 and the CSG2 Release 2.
Appendix D, “Protocol Compliance Statements for the CSG2”	Provides protocol compliance statements for the CSG2.
Appendix E, “CSG2 System Messages”	Lists and describes Cisco CSG2, SAMI, and iSCSI system messages.
Appendix F, “Monitoring Notifications”	Describes enabling and monitoring CSG2 SNMP notifications in order to manage CSG2-related issues.

Conventions

This publication uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.

Convention	Description
{x | y | z}	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information that the system displays are in `screen` font.
`boldface screen` font	Information that you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Tips use the following conventions:

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information.

Cautions use the following conventions:

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

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

- *Release Notes for Cisco Content Services Gateway - 2nd Generation Release 2.0*, Cisco IOS Release 12.4(15)MD
- *Service and Application Module for IP User Guide*
- *Release Notes for Cisco IOS Release 12.2SR for the Cisco 7600 Series Routers*

- 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 IOS Configuration Guides and Command References, Release 12.2—Use these publications to help you configure the Cisco IOS software that runs on the MSFC and on the MSM and ATM modules.

Obtaining Documentation and Submitting a Service Request

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

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

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

CHAPTER 1

Overview

The Cisco Content Services Gateway - 2nd Generation, more commonly known as the Content Services Gateway 2 or CSG2, is an application that runs on the Service and Application Module for IP (SAMI), a high-speed processing module. The CSG2 provides content-aware billing, service control, traffic analysis, and data mining in a highly scalable, fault-tolerant package. The CSG2 provides the software required by mobile wireless operating companies and other billing, applications, and service customers.

The CSG2 runs on the SAMI, a new-generation high performance service module for the Cisco 7600 series router platforms. The CSG2 is typically located at the edge of a network in an Internet service provider (ISP) point of presence (POP), or Regional Data Center.

In addition to performing standard IP flow accounting, the CSG2 also examines various protocol requests—e-mail, HTTP, FTP, Real Time Streaming Protocol (RTSP), Session Initiation Protocol (SIP), wireless application protocol 1.x and 2.0 (WAP 1.x and WAP 2.0)—to gather URLs and other header information for accounting purposes. Additionally, the CSG2 gathers information on subscriber names and usage statistics, and enables differentiated billing for individual transactions based on hostname, on the directory accessed, or on individual files.

The CSG2 inspects IP traffic at levels deeper than typical routers. When doing so, the CSG2 behaves partly as a proxy server. Therefore, design your network security strategy to protect the CSG2 as you would any proxy or server.

This section includes the following information:

- What's New, page 1-1
- CSG2 Features, page 1-2
- CSG2 Prerequisites, page 1-41
- CSG2 Restrictions, page 1-41

What's New

The CSG2 R2 includes the following new features:

- New RADIUS Features
  - Configuring RADIUS Monitor, page 9-6
  - Enabling Roaming Service Control, page 9-10
- New iSCSI Features
  - iSCSI Features, page 1-16
- New SIP Features

  - SIP Features, page 1-19
- New FTP Features
  - FTP Billing, page 1-27
  - Layer 4 Redundancy—Stateful Redundancy and Failover, page 1-33
- New RTSP Features
  - Layer 4 Redundancy—Stateful Redundancy and Failover, page 1-33
- New CSG2 User Table Features
  - Larger CSG2 User Table—CSG2 User Table, page 1-12
  - Customizable CSG2 User Table deletion rate—Deleting Entries from the CSG2 User Table, page 9-8
- Performance Enhancements
- Secure Shell (SSH) for remote maintenance
- New MIB Support
  - CISCO-PSD-CLIENT-MIB—MIB Support, page 1-4
- New Platform Support
  - –Cisco 7600 Series Supervisor Engine 32, with a Multilayer Switch Feature Card, running Cisco IOS Release 12.2(33)SRC or later and LCP ROMMON Version 12.2[121] or later
  - –Cisco Route Switch Processor 720 with Distributed Forwarding Card DFC3CXL, running Cisco IOS Release 12.2(33)SRC or later

CSG2 Features

The CSG2 Release 12.4(11)MD provides the following basic features and functionality:

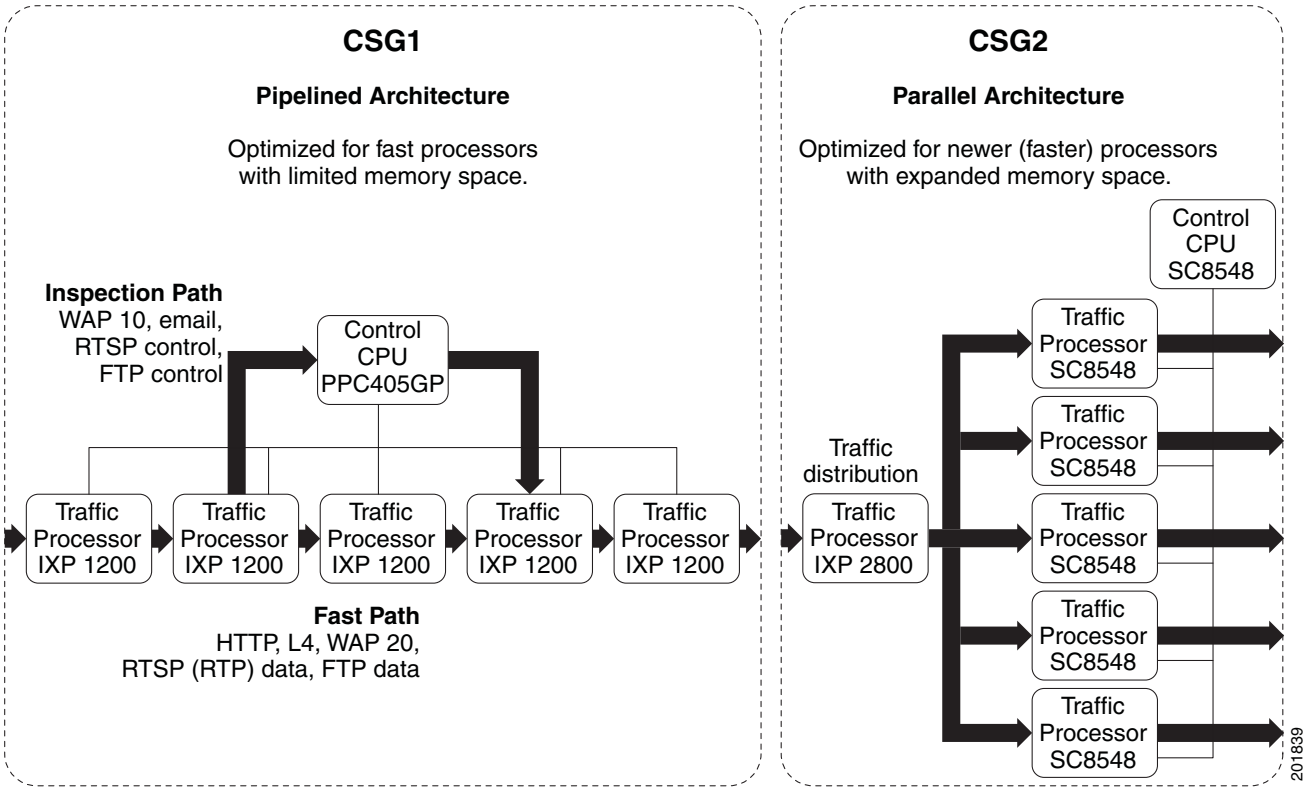
- Comparison of CSG1 and CSG2 Hardware Architectures, page 1-3
- MIB Support, page 1-4
- CSG2 Billing Criteria, page 1-5
- CSG2 Interactions with External Entities, page 1-5
- CDR Support, page 1-6
- Byte Counting, page 1-8
- CSG2 User Table, page 1-12
- CSG2 Interface Awareness, page 1-13
- BMA Features, page 1-13
- Quota Server Features, page 1-14
- Service Features, page 1-15
- IPC Features, page 1-15
- PSD Features, page 1-16
- iSCSI Features, page 1-16
- RADIUS Features, page 1-16

- HTTP Features, page 1-17
- SIP Features, page 1-19
- WAP Features, page 1-19
- RTSP Features, page 1-21
- POP3 Support, page 1-26
- SMTP and POP3 Billing, page 1-26
- SMTP CDR Header Removal, page 1-27
- FTP Billing, page 1-27
- Header, Method, and URL Mapping, page 1-27
- Service Duration Billing, page 1-27
- Connection Duration Billing, page 1-32
- Postpaid Service Tagging, page 1-33
- Stateful Redundancy and Failover, page 1-33
- “Default” Policy, page 1-34
- Tariff Switch, page 1-34
- Prepaid Error Reimbursement, page 1-35
- Postpaid Billing, page 1-36
- Prepaid Content Billing and Accounting, page 1-36
- Obtaining User IDs, page 1-38
- Filtering Accounting, page 1-38
- Intermediate CDRs, page 1-38
- Packet Forwarding, page 1-39
- URL-Redirect, page 1-39
- Supplemental Usage Reports, page 1-39
- Enhanced Interoperability with Cisco Service-Aware GGSN, page 1-39
- Miscellaneous Features, page 1-40

Comparison of CSG1 and CSG2 Hardware Architectures

Figure 1-1 illustrates the key differences between the CSG1 hardware architecture and the CSG2 hardware architecture.

Figure 1-1 Comparison of CSG1 and CSG2 Hardware Architectures



As can be seen, the CSG1 featured a pipelined architecture, with five IXP1200 traffic processors (TPs) running at 166MHz and one Power PC (PPC) 405GP control processor (CP) running at 166MHz.

In contrast, the CSG2 features a parallel architecture, with one IXP2800 flow-distributor TP running at 1.4GHz, five PPC 8548 TPs running at 1.25GHz, and one PPC 8548 CP running at 1.25GHz.

The benefits of the CSG2 approach include:

- Increased processing power
- Reduced inter-CPU data sharing
- Separation of the control and data planes
- Reduced complexity
- Easier debugging

MIB Support

The CSG2 supports the following MIBs:

- CISCO-CONTENT-SERVICES-MIB implemented in the Cisco IOS software.
- CISCO-ENHANCED-MEMPOOL-MIB
- CISCO-ENTITY-VENDORTYPE-OID-MIB
- CISCO-IMAGE-MIB
- CISCO-PING-MIB

- CISCO-PROCESS-MIB
- CISCO-PRODUCTS-MIB
- CISCO-PSD-CLIENT-MIB
- CISCO-SYSLOG-MIB
- CISCO-TCP-MIB
- ENTITY-MIB
- IF-MIB
- MIB II
- RMON2-MIB
- SNMP-FRAMEWORK-MIB
- SNMP-NOTIFICATION-MIB
- SNMP-TARGET-MIB
- SNMPv2-MIB
- SNMPv3-MIB
- TCP-MIB
- UDP-MIB

CSG2 Billing Criteria

The CSG2 can bill different services based on different criteria, as shown in Table 1-1.

Table 1-1 CSG2 Billing Criteria

Service	Subscription	Event	Volume	Duration	Content
Internet and Corporate Access	Yes	No	Yes	No	No
Multimedia Messaging Service (MMS)	Yes	Yes	No	No	Yes
E-mail	Yes	Yes	Yes	No	No
Broadcast Services	No	Yes	No	Yes	Yes
Downloads, Ringtones, Music, etc.	No	Yes	No	No	Yes
Games	Yes	No	No	Yes	Yes

CSG2 Interactions with External Entities

The CSG2 communicates with several different external entities:

- The Billing Mediation Agent (BMA)—The BMA receives the billing records from the CSG2 and formats them as required by the billing engine. At the end of each transaction, a billing record indicating the content accessed and the amount deducted is sent to the BMA, so that it can be logged in the subscriber's bill.

  For more information about the BMA, see the "Configuring BMA Support" section on page 3-1

- The Quota Server—The CSG2 uses quota servers to return billing quota values for subscribers. The quota server interfaces with the billing system balance manager to reserve credit. The quota server then translates the reserved credit for the subscriber into quota based on the business and rating rules for multiple subscriber services on the CSG2.

  For more information about the quota server, see the "Configuring Quota Server Support" section on page 4-1

- An External Extensible Markup Language (XML) User Database—The CSG2 can use an XML database to associate an IP address with a user ID, and can refer to the database when it receives a packet with an unknown IP address. XML-based database queries add additional robustness to the CSG2, allowing continued monitoring across a failover, even in the absence of fresh RADIUS flows.

  For more information about the XML user database, see the "Configuring the User Database" section on page 2-9.

- The Interprocessor Communication (IPC) Module—The CSG2 IPC module provides a communication channel between the CSG2 Control Processor (CP) and Traffic Processors (TPs), and, in a redundant CSG2 deployment, between the TPs on the active CSG2 and their counterparts on the standby CSG2.

  For more information about the IPC module, see the "Configuring IPC Support" section on page 6-1.

- The Cisco Persistent Storage Device (PSD)—The PSD provides backup capabilities as necessary, such as during network outages. The PSD stores the payload from a packet in a queue, and the data can be retrieved exactly as it was sent.

  For more information about the PSD, see the "Configuring PSD Support" section on page 7-1.

- Internet Small Computer Systems Interface (iSCSI)—Instead of using the PSD as backup storage, the CSG2 can use the Storage Area Network (SAN) connected to the iSCSI to store CDRs until the BMAs can be reached.

  For more information about the iSCSI, see the "Configuring iSCSI Support" section on page 8-1.

- The RADIUS Client and Server—RADIUS is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all subscriber authentication and network service access information. The RADIUS client and server retrieve subscriber correlation information (the IP address, the MSISDN, the User-Name, and the Billing Plan) for prepaid subscribers. The CSG2 acts as a RADIUS proxy or RADIUS endpoint to retrieve the subscriber correlation information. In addition, the CSG2 can report RADIUS attributes when it communicates with the BMA and quota servers.

  For more information about RADIUS clients and servers, see the "Configuring RADIUS Support" section on page 9-1.

CDR Support

The CSG2 provides the following call detail record (CDR) support:

- Fixed CDR Support for HTTP, IMAP, RTSP, and WAP, page 1-7
- Single CDR Support for HTTP and WAP Connectionless, page 1-7
- Service-Level CDR Summarization, page 1-7
- Prepaid and Postpaid Envelope Information Support for SMTP, page 1-7
- Fixed Attribute CDRs for WAP, page 1-7

Fixed CDR Support for HTTP, IMAP, RTSP, and WAP

The CSG2 supports the generation of fixed-format CDRs for HTTP, IMAP, RTSP, and WAP.

For more information, see the "Configuring Fixed, Variable, or Combined Format CDR Support" section on page 2-17.

Single CDR Support for HTTP and WAP Connectionless

For HTTP and WAP, the CSG2 reduces the multiple CDRs generated to a single CDR, which is reported at the end of the transaction. This feature is supported for both WAP connectionless and WAP connection-oriented traffic, as well as for HTTP traffic.

For more information, see the "Single CDR Support for HTTP and WAP" section on page 2-18.

Service-Level CDR Summarization

By default, the CSG2 generates billing records for each transaction. This large number of records might overwhelm the charging gateway (CG) or the collector. To prevent this situation, the CSG2 can summarize CDRs at the service level, instead of at the transaction level.

For more information about service-level CDR summarization, see the "Enabling Service-Level CDR Summarization" section on page 5-10.

Prepaid and Postpaid Envelope Information Support for SMTP

The CSG2 provides SMTP with prepaid and postpaid support, including envelope information in the CDR.

SMTP prepaid support includes all existing billing options (including IP bytes, TCP bytes excluding retransmissions, duration, and fixed). SMTP CDRs include e-mail envelope information as well as IP byte counts, TCP byte counts, and e-mail data (X-CSG-SIZE) byte counts for each e-mail message. When multiple e-mails are sent over a single TCP connection, each e-mail message is assigned byte counts until the start of the next e-mail message. The last e-mail is assigned bytes from the start of that e-mail until the end of the TCP connection.

The return code reported in the CDR is the one returned for the DATA portion of the e-mail message. If the CSG2 does not receive that data return code, it reports the last error return code (other than **250**) received for individual recipients (because a bad recipient return code might be the cause of the e-mail not being sent). If the CSG2 receives a QUIT before receiving any return code, it reports a default return code of **554** (Transaction failed). This enables the CSG2 to apply refunding via the SMTP return code value.

If the subscriber runs out of quota in the middle of a transaction, the session is terminated and all known information is reported in a CDR. The application return code indicates whether the e-mail was received, and the authentication failure bit is set in the TCP **flags** field.

There are no commands required to enable this support.

Fixed Attribute CDRs for WAP

To support some legacy billing systems, the CSG2 provides a fixed attribute format for WAP CDRs. The same set of attributes is reported in each CDR regardless of the Wireless Session Protocol (WSP) protocol data unit (PDU) type. CDRs contain zero-length attributes when there is no information to report, but the same set of attributes are always reported in the same sequence.

There are no commands required to enable this support.

Byte Counting

The CSG2 reports the number of IP bytes uploaded and downloaded, the number of TCP bytes uploaded and downloaded by the application, and the packet counts (or PDU counts for WAP records). These counts exclude the IP and TCP headers, as well as retransmissions.

This section includes the following information:

- Byte Counting Overview, page 1-8
- HTTP Byte Counting, page 1-9
- WAP Byte and Packet Counting, page 1-10
- IMAP Byte Counting, page 1-11
- FTP and RTSP Byte Counting, page 1-12
- SIP Byte Counting, page 1-12
- POP3 and SMTP Byte Counting, page 1-12
- Byte and Packet Counting After a Failover, page 1-12

Byte Counting Overview

This section describes how the GGSN and the CSG2 handle traffic, including the types of packets that they might drop. This section includes the following information:

- Byte Counting on the GGSN, page 1-8
- Byte Counting on the CSG2, page 1-8

Byte Counting on the GGSN

Typically, the GGSN forwards all packets to the upstream next-hop. However, the GGSN drops packets that meet one or more of the following conditions:

- The packet is a broadcast or multicast packet.
- The packet contains a destination for which there is no forwarding route.
- The packet is a bad IP packet. For example, there might be a checksum error.
- The packet matches an ACL or filter that is configured to drop the packet.
- The IP option field is set within the IP header of the packet.

The GGSN does not forward the dropped packets to the CSG2, so the CSG2 does not count these packets.

Byte Counting on the CSG2

When the CSG2 receives a packet that matches an allowed content and service, it processes the packet and forwards it to the upstream next-hop. The CSG2 counts all forwarded packets.

There are some conditions that might cause the CSG2 to drop a packet (although these dropped packets account for only a very small percentage of the total network traffic). For example, the CSG2 drops the following types of packets:

- A packet for a TCP connection that is received after the TCP session has been closed or reset. This condition might occur if a handset is out-of-sync with a server.
- A packet for a TCP connection that does not generate a session because the signals are out-of-order. For example, the CSG2 might receive a SYN-ACK without receiving a SYN. This problem might be caused by network congestion, or by an out-of-sync condition.
- An out-of-order TCP packet. This problem might also be caused by network congestion or an out-of-sync condition.
- A packet that matches a content or service that is disallowed.
- A packet that does not match any allowed content.
- A packet that is received after a user has exhausted his quota and before the quota server has responded to a request for more quota.
- A packet that is received while the CSG2 is waiting for a Service Authorization Response.
- A packet that contains a destination for which there is no forwarding route,
- A bad IP packet, such as a packet with a checksum error.
- A packet matches an ACL or filter that is configured to drop the packet.

The CSG2 does not count packets that are dropped.

The CSG2 also does not count some other types of packets, such as:

- A packet that matches a content that belongs to a free service.
- A packet that is generated by the CSG2, such as a reset (RST) for an unexpected TCP signal or AoC signaling.

HTTP Byte Counting

HTTP 1.1 allows a client to send multiple HTTP requests without waiting for the corresponding responses. Therefore, a single IP datagram might contain requests or responses for more than one HTTP transaction. The CSG2 reports the total number of IP bytes of an HTTP transaction transferred between a client and a server.

The CSG2 counts the IP bytes for the TCP session SYN as part of the first transaction. The CSG2 counts the IP bytes for the TCP session FIN, FIN/ACK, or RST as part of the last transaction. The CSG2 counts the IP and TCP header bytes of an IP datagram that contains multiple transactions as part of the first transaction in the datagram.

If the CSG2 receives retransmitted SYN packet before it receives the first SYN/ACK from the server, it includes the IP bytes for the retransmitted SYN packet in the byte counts in the HTTP_Stats CDR.

The CSG2 discards out-of-order FIN packets, even if they contain data, and depends on retransmission of the out-of-order FIN packets to ensure correct billing.

If the final ACK on a TCP 3-way handshake is retransmitted, the CSG2 does not report the IP bytes associated with the retransmitted ACK in the HTTP_Stats CDR.

To enable the CSG2 to count fixed-format HTTP IP bytes more accurately, a new CDR and a new TLV have been added to the existing fixed HTTP intermediate CDRs.

There are no commands required to enable HTTP IP byte counting.

This section includes the following additional information:

- HTTP IP Bytes vs. TCP Bytes, page 1-10
- Counting Uncorrelated HTTP IP Bytes, page 1-10
- Packet Counts for Pipelined HTTP, page 1-10

HTTP IP Bytes vs. TCP Bytes

The CSG2 reports the total number of IP bytes of an HTTP transaction transferred between a client and a server. For a given transaction, there will always be more IP bytes than TCP bytes.

For HTTP quota management, the billing process has always managed IP bytes, not TCP bytes (for **basis byte ip**) and has always provided transaction grants as IP bytes.

From a system behavior point of view, the CSG2 quota management for HTTP may appear different, because the forwarding process takes the granted quota and applies it to IP bytes instead of TCP bytes.

For example, an empty TCP packet for HTTP would have previously consumed 0 bytes of IP quota - now it would take 40 (assuming standard IP and TCP header size).

Note If you want the CSG2 to continue to report TCP byte counts for HTTP transactions, you can configure a service with **basis byte tcp** to count TCP bytes instead of IP bytes as quadrans, and you can configure the CSG2 to inspect BMA records for reported TCP byte counts.

Configuring **basis byte tcp** allows counting of only TCP payload and exclusion of overhead for network retransmission. With this option, the CSG2 excludes IP and TCP headers from volume counts. Retransmitted packets are also not counted.

Counting Uncorrelated HTTP IP Bytes

Sometimes the CSG2 cannot correlate some IP bytes to any transaction at the end of a TCP session. This can include any retransmits or ACKs without payloads that are received after the CSG2 has reported the CDR for a specific transaction. You can configure the CSG2 to include these IP bytes in its reports by setting the **records delay** command inCSG2 content configuration mode to a non-zero value.

Packet Counts for Pipelined HTTP

Packet counts for pipelined HTTP operations are a snapshot of the number of packets detected on the connection since the previous statistics were reported. The packet count might even be zero if two pipelined operations share the same packet.

WAP Byte and Packet Counting

WAP byte counting is always IP-based.

The CSG2 reports WAP datagram sizes (including IP and UDP headers), the number of IP packets per transaction, and PDU counts. (The PDU count is not the same as the packet count. Multiple WAP PDUs can share a single packet.)

Bytes for retransmitted WAP PDUs and segments are not counted against quota, but they are counted and listed separately from non-retransmitted counts in the WAP CDRs.

Byte and PDU counts are further specified by source. Reports include the number of bytes and PDUs uploaded from source to destination and the number of bytes downloaded from destination to source.

The CSG2 splits all concatenated PDUs received from the client into multiple IP packets to be sent to the server. Therefore, packet counts are based on the number of WAP PDUs, not on the number of IP packets.

Byte counting for concatenated PDUs is complicated because multiple transactions are combined into a single IP packet. For example, a concatenated CONNECT/GET shares the same IP/UDP headers, yet they are treated as two separate transactions, they result in two separate CDRs, and they might even be charged differently from each other. In addition to the IP/UDP headers, there are several other bytes in the packet that define it as a concatenated packet. It might not be obvious to which transaction these bytes are assigned. Here is how the CSG2 assigns the IP bytes:

- The size of the IP/UDP headers (usually 28 bytes) is assigned to the first PDU.
- The single byte that identifies the packet as a concatenated packet is also be assigned to the first PDU.
- A one- or two-byte length field is assigned to each PDU.

For example, a CONNECT/GET concatenated PDU that contains one-byte PDU length fields yields the following byte count totals:

- CONNECT transaction = IP/UDP header length + 1 + 1 + PDU size
- GET transaction = 1 + PDU size

IMAP Byte Counting

Service-level fixed-format CDRs for IMAP include the following IMAP-specific counts:

- Number of header retrievals. That is, the number of times that the CSG2 retrieved the header attribute of an e-mail message (for example, **BODY[HEADER]**, **RFC822.HEADER**).
- Header IP bytes sent upstream (client to server)
- Header IP bytes sent downstream (server to client)
- Header TCP bytes sent upstream
- Header TCP bytes sent downstream
- Number of body retrievals. That is, the number of times that the CSG2 retrieved any portion of the body text of an e-mail message (for example, **BODY[]**, **BODY[TEXT]**, **BODY[3]**, **BODY[]<0.4096>**, **RFC822**, **RFC822.TEXT**).
- Body IP bytes sent upstream
- Body IP bytes sent downstream
- Body TCP bytes sent upstream
- Body TCP bytes sent downstream

The CSG2 reports incremental byte counts for the IMAP service-level fixed-format CDRs. For example, if 100 KB of traffic is generated for the first 15 minutes, 50 KB for the next 15 minutes, and the CSG2 generates intermediate CDRs every 15 minutes, then the CSG2 reports the change in the total byte count from the point at which the last CDR was reported to the point at which the current CDR is reported. Thus, the first CDR would report 100 KB, and the second would report 50 KB.

With fixed-format CDRs, the incremental byte counts might be reported at a given time interval or after a volume threshold has been reached (for example, every 15 minutes, or after every 100 KB.)

For IMAP byte counting, keep the following considerations in mind:

- Message tags cannot be longer than 100 bytes. If the CSG2 encounters a message with a tag that is longer than 100 bytes, only the IP and TCP upstream and downstream byte counts are reported.

- The byte counts associated with a continuation response flow are accounted for in the next classified transaction.

FTP and RTSP Byte Counting

For FTP and RTSP, the CSG2 reports the upstream and downstream IP bytes and TCP bytes.

Even though FTP and RTSP data sessions usually appear to be network-initiated, the uploaded bytes for FTP and RTSP (for example, in IP statistics) are counted from the originator of the session, the endpoint from which the first packet for the session is received.

Note For service-level CDRs, the uploaded bytes for FTP and RTSP are counted from the subscriber to the network, and the downloaded bytes are counted from the network to the subscriber.

The CSG2 discards out-of-order FIN packets, even if they contain data, and depends on retransmission of the out-of-order FIN packets to ensure correct billing.

SIP Byte Counting

For SIP, the CSG2 reports the upstream and downstream IP bytes and TCP bytes.

You cannot charge SIP subscriber sessions as a function of the TCP data volume processed. (That is, you cannot configure basis byte tcp in CSG2 service configuration mode for SIP.)

You can charge SIP transactions based on transaction duration time, using the basis seconds transaction command in CSG2 service configuration mode.

POP3 and SMTP Byte Counting

For POP3 and SMTP, the CSG2 reports the upstream and downstream IP bytes and TCP bytes.

Byte and Packet Counting After a Failover

After a failover, the standby CSG2 (now the active CSG2) considers the first 32 KB TCP bytes received to be retransmitted packets and does not count TCP bytes for those packets. However, the IP byte count is counted normally.

CSG2 User Table

The CSG2 User Table identifies all subscribers known to the CSG2. The User Table is populated based on the contents of RADIUS Accounting Start messages, or from the user database, if either feature is enabled in your configuration.

The CSG2 User Table can hold up to 1,250,000 entries with the 2 GB-SAMI option, or up to 500,000 entries with the 1 GB-SAMI option.

For more information about the User Table, see the "Configuring the CSG2 User Table" section on page 2-9.

CSG2 Interface Awareness

Many provider networks offer data access, control over subscriber addressing, and dedicated Virtual Routing and Forwarding (VRF) over the wireless network to enterprises and Mobile Virtual Network Operators (MVNOs). Interface awareness uses VRF tables to enable the CSG2 to distinguish between subscribers and sessions that share the same IP address on different VLANs (that is, subscribers and sessions with overlapping IP addresses). Configurations with overlapping IP address requirements cannot use the CSG2 RADIUS user database to determine the user's identity, because user database queries do not include VRF table information.

Because the quota server can only respond to the CSG2 (that is, there can be no quota server-initiated messages), the Extended User Index TLV is required to in order to identify or trigger action for a subscriber within a CSG2 table.

To support traffic segregation across VLANs, the CSG2 uses next-hop to bind flows to uplink and downlink routing hops. The CSG2 routes uplink packets (from the Network Access Server [NAS]) by applying next-hop policies to the contents on each NAS VLAN. The CSG2 routes downlink packets via the downlink address supplied by the NAS in the RADIUS Accounting start message.

Logically, that means that a dedicated per-VLAN NAS is required for interface awareness. Physically, however, it depends on the capabilities of the NAS. Each RADIUS proxy statement can have a table name. When a User Table entry is created as a result of a Start message sent to that proxy IP address, the specified table name is associated with the subscriber. Depending on your network, you might choose to route this subscriber's traffic different from another subscriber's traffic, even when the source or destination IP addresses are the same. To do so, use the **next-hop** command in CSG2 content configuration mode, or specify the downlink next-hop in the Start message.

To associate a VRF table name with a particular CSG2 component, specify the **vrf** keyword on the appropriate **ip csg** command in global configuration mode. For example, to associate a VRF table name with a particular RADIUS proxy, specify the **vrf** keyword on the **ip csg radius proxy** command in global configuration mode.

When configuring Interface Awareness, keep the following considerations in mind:

- The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters.
- Table IDs and names are not supported or reported in fixed-format TLVs.
- If a content configuration is required on multiple VLANs, you must define the content multiple times, once for each of the VLANs on which it is required. Contents cannot be shared across tables.
- VLAN-specific content configurations must handle all traffic from subscribers arriving on a VLAN marked with a table name. The CSG2 uses the VLAN table name to locate subscriber entries. Therefore, if you want to apply the same contents to multiple tables, you must redefine all of your contents.
- The CSG2 does not support the use of the word **forwarding** as a valid VRF name.

BMA Features

The CSG2 monitors data flows and generates accounting records that can be used to bill customers at a content level. The CSG2 sends the accounting records to a Billing Mediation Agent (BMA), which formats the records as required by the customer's billing system. At the end of each transaction, a billing record indicating the content accessed and the amount deducted is sent to the BMA, so that it can be logged in the subscriber's bill.

The CSG2 provides the following BMA features:

- Configuring the BMA Local Port
- Configuring a BMA
- Configuring the BMA Keepalive Time
- Configuring the BMA GTP' Message Buffer
- Configuring the BMA Retransmit Time
- Configuring the BMA Retry Number
- Configuring the BMA Window Size
- Configuring BMA Load Sharing
- Reporting the Billing Plan ID to the BMA

For descriptions of these features, and instructions for configuring them, see the "Configuring BMA Support" section on page 3-1.

Quota Server Features

The CSG2 uses quota servers to return billing quota values for subscribers. The quota server interfaces with the billing system balance manager to reserve credit. The quota server then translates the reserved credit for the subscriber into quota based on the business and rating rules for multiple subscriber services on the CSG2.

For each CSG2 content billing service, the CSG2 downloads a separate quota, and deducts from that quota. Quotas are specified in units called *quadrans*. A quadran is a generic unit whose "value" is defined by each quota server. A quadran can represent, for example, a click for a per-click service (for example, an HTTP request), or a byte for a per-volume service. The value of a quadran is transparent to the CSG2; the CSG2 simply requests and downloads quadrans as needed from quota servers.

The CSG2 provides the following quota server features:

- Configuring the Quota Server Local Port
- Configuring a Quota Server
- Configuring the Quota Server Keepalive Time
- Configuring the Quota Server GTP' Message Buffer
- Configuring the Quota Server Retransmit Time
- Configuring the Quota Server Retry Number
- Configuring the Quota Server Window Size
- Configuring Quota Server Load Sharing
- Reassigning Subscribers to a New Quota Server
- Quota Push
- Replacing Quota Balance
- Delaying Quota Reauthorization
- Asynchronous Quota Return
- Reporting the Billing Plan ID to the Quota Server
- Pricing by Quota Server Configuration Example

- Differentiating Prices Configuration Example
- Reducing the Number of Services Configuration Example

For descriptions of these features, and instructions for configuring them, see the "Configuring Quota Server Support" section on page 4-1.

Service Features

A CSG2 content billing service is a component of a billing plan to which subscribers subscribe.

You can configure one or more content billing services for the CSG2. Each service represents a group of content that is billed the same way, such as billing per-click (or per-request) or billing per-IP byte, and that shares part of a subscriber's quota. Grouping content into one or more services enables you to separate, for example, a subscriber's prepaid quota for Internet browsing from his quota for e-mails.

The CSG2 provides the following features for content billing services:

- Configuring a Basic Content Billing Service
- Configuring the Billing Basis for a Service
- Specifying a Service Owner
- Specifying a Service Class
- Configuring a Service Idle Time
- Configuring Advice of Charge
- Configuring Service Verification
- Enabling Service-Level CDR Summarization
- Configuring Passthrough Mode and the Default Quota
- Configuring Metering
- Configuring the Quota Reauthorization Threshold
- Configuring the Quota Reauthorization Timeout
- Enabling a Refund Policy for a Service

For descriptions of these features, and instructions for configuring them, see the "Configuring Service Support" section on page 5-1.

IPC Features

The CSG2 Interprocessor Communication (IPC) module provides a communication channel between the CSG2 Control Processor (CP) and Traffic Processors (TPs), and, in a redundant CSG2 deployment, between the TPs on the active CSG2 and their counterparts on the standby CSG2.

The CSG2 provides the following IPC features:

- Configuring the IPC Keepalive Time
- Configuring the IPC Retransmit Time
- Configuring the IPC Retry Number
- Changing the IPC Crash Dump Setting

For descriptions of these features, and instructions for configuring them, see the "Configuring IPC Support" section on page 6-1.

PSD Features

The Cisco Persistent Storage Device (PSD) provides persistent storage capabilities to the CSG2, and allows the CSG2 to store data on the PSD's internal hard drive. The CSG2 provides the following PSD features:

- Configuring the PSD Local Port
- Configuring the PSD
- Configuring the PSD Packet Drain Settings
- Configuring the PSD Keepalive Time
- Configuring the PSD GTP' Message Buffer
- Configuring the PSD Retransmit Time
- Configuring the PSD Retry Number
- Configuring the PSD Window Size

Note The CSG2 supports the Cisco Persistent Storage Device Module Software Release 2.0 or later.

For descriptions of these features, and instructions for configuring them, see the "Configuring PSD Support" section on page 7-1.

iSCSI Features

The CSG2 can use a Storage Area Network (SAN) connected to an Internet Small Computer Systems Interface (iSCSI) to store CDRs when BMAs are unreachable. The CSG2 provides the following iSCSI features:

- iSCSI Overview
- Configuring an iSCSI Target Interface Profile on the CSG2
- Associating an iSCSI Target Interface Profile with the CSG2
- Configuring the iSCSI Packet Drain Settings
- Verifying the iSCSI Session

For descriptions of these features, and instructions for configuring them, see the "Configuring iSCSI Support" section on page 8-1.

RADIUS Features

RADIUS is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all subscriber authentication and network service access information. The RADIUS client and server retrieve subscriber correlation information (the IP address,

the MSISDN, the User-Name, and the Billing Plan) for prepaid subscribers. The CSG2 acts as a RADIUS proxy or RADIUS endpoint to retrieve the subscriber correlation information. In addition, the CSG2 can report RADIUS attributes when it communicates with the BMA and quota servers.

The CSG2 provides the following RADIUS features:

- Configuring RADIUS Proxy
- Configuring RADIUS Endpoint
- Configuring RADIUS Handoff
- Configuring RADIUS Packet of Disconnect
- Configuring RADIUS Monitor
- RADIUS Attributes and VSA Subattributes
- Enabling Roaming Service Control
- Retrieving the Billing Plan ID from RADIUS
- RADIUS Subscriber Cleanup
- RADIUS Error Acknowledgment
- RADIUS Correlation Processing

For descriptions of these features, and instructions for configuring them, see the "Configuring RADIUS Support" section on page 9-1.

HTTP Features

The CSG2 provides the following HTTP features:

- HTTP Pipelining and Chunked Transfer Encoding, page 1-17
- Support for Multipart HTTP, page 1-18
- HTTP 1.0 Content Billing, page 1-18
- HTTP 1.1 Content Billing, page 1-18
- HTTP Records Reporting Flexibility, page 1-18
- HTTP Error Code Reporting, page 1-18
- Learning Client IP Addresses Using Inspection of HTTP X-Forwarded-For Headers, page 1-18

HTTP Pipelining and Chunked Transfer Encoding

The CSG2 supports full HTTP pipelining and chunked transfer encoding. Packet counts for pipelined HTTP operations are a snapshot of the number of packets detected on the connection since the previous statistics were reported. The packet count might even be zero if two pipelined operations share the same packet.

If pipelined connections are replicated to a standby CSG2, and a failover occurs, the CSG2 does not increment the content counters for traffic flowing through these connections. The CSG2 does increment the content counters for new pipelined connections created after the failover.

When performing AoC for a TCP connection carrying pipelined HTTP requests, the CSG2 responds with the redirect to the client as soon as the quota server requests the redirect. This could result in the redirect arriving at the client before responses for previous requests arrive, and the client might associate the redirect with a different request in the pipeline.

There are no commands required to enable this function.

Support for Multipart HTTP

For HTTP sessions, multipart content does not cause the CSG2 to invoke Layer 4 billing for the remainder of the connection. Instead, the CSG2 parses the data for the delimiter specified in the header and continues to use Layer 7 billing.

There are no commands required to enable support for multipart HTTP.

HTTP 1.0 Content Billing

The CSG2 enables you to bill subscribers for individual transactions by discriminating on a per-object basis, and on a per-subscriber basis. Unlike traditional billing models, which bill for broad classes of traffic, this service enables differentiated billing based on the actual object being requested. You can even bill objects at different rates to different customers. For example, you can bill advertisements to the advertiser, rather than to the subscriber.

HTTP 1.1 Content Billing

The CSG2 separately records each request over a persistent HTTP 1.1 session.

HTTP Records Reporting Flexibility

The client's IP address is included in the HTTP Header message. This enables the BMA to identify the client by user ID (and by IP address) immediately, without having to wait for the HTTP Statistics record.

You can configure the CSG2 to send the HTTP Header message as soon as it is generated. This reduces latency and notifies the BMA about the client's transaction as quickly as possible. Although this type of reporting is more efficient, it provides less information; use it only when the BMA needs to react to the client's activity very quickly.

You can configure the CSG2 to not send the HTTP Statistics message. This configuration reduces the load on the BMA and is useful when the billing policy depends only on the event and does not require detailed statistics. Note that the CSG2 still sends the HTTP Statistics message if the session fails (for example, if a Reset [RST] is received without a Finish [FIN], or if the session times out).

HTTP Error Code Reporting

The CSG2 reports HTTP-specific information about the request, such as the URL, as well as HTTP error codes (response codes of 300 or higher).

Learning Client IP Addresses Using Inspection of HTTP X-Forwarded-For Headers

If your network is configured with a gateway or proxy placed between the client and the CSG2, you can configure the CSG2 to determine the client's IP address by inspecting the HTTP X-Forwarded-For header.

The CSG2 can also obscure the contents of X-Forwarded-For headers, overwriting the contents with blanks, thereby preventing the exposure of potentially sensitive IP addresses.

To configure the way the CSG2 is to handle X-Forwarded-For headers, use the **subscriber-ip http-header forwarded-for** command in CSG2 content configuration mode.

SIP Features

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol used for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences.

The CSG2 provides detailed billing information and services for content transported over the network using SIP.

For SIP and Session Description Protocol (SDP), keep the following considerations in mind:

- Individual SIP/SDP headers are not parsed beyond the first 256 characters.
- Domain names used in headers are not resolved to IP addresses. If domain names are used in headers for which IP addresses are required (such as media connect headers), the CSG2 cannot correctly identify and correlate the SIP media traffic.
- The CSG2 cleans up media sessions for SIP calls when a positive response to a BYE request is processed (200 ok). Media packets that flow after the 200 ok are not associated with the media session.

WAP Features

The CSG2 provides the following WAP features:

- WAP Traffic, page 1-19
- WAP 2.0, page 1-20
- Support for WAP Segmentation and Reassembly (SAR), page 1-21

WAP Traffic

The CSG2 can intercept WAP traffic and generate reports that include contextual WAP information and counts of the bytes transferred. WAP functionality provides protocol-level prepaid and postpaid billing, including the following functionality:

- Billing CDRs for Wireless Transaction Protocol (WTP) and WSP in support of WAP 1.2—The ability to generate billing records for each WAP GET, POST, PUSH or CONFIRMED PUSH, ABORT and REPLY PDUs, as well as a summary report at WAP Disconnect. Records include URL, User Agent, source and destination IP, separate IP byte and PDU counts from both the initiator and the responder. (The PDU count is not the same as the packet count. Multiple WAP PDUs can share a single packet.)
- Prepaid billing for WTP and WSP in support of WAP 1.2, including the ability to differentiate WAP browsing from the Multimedia Messaging Service (MMS), and to exclude charging for MMS.
- Top-up capability using URL-redirect.
- URL-map support for WAP.
- Support for multiple services.
- WAP 2.0 support: The CSG2 HTTP support is compatible with WAP 2.0 traffic.
- WAP byte counting is always IP-based.
- Retransmitted bytes are not counted against quota, but they are reported separately in the WAP CDRs.

WAP 2.0

The CSG2 supports billing for the following types of WAP 2.0 network flows:

- Retrieving a message from the network using HTTP.request-method: GET
- Posting a message into the network using HTTP.request-method: POST
- Acknowledging a PUSH indication using HTTP.request-method: POST

WAP 2.0 mobile devices can participate in these flows, implemented as WAP 2.0/TCP across a WAP 2.0 Proxy or Push Proxy Gateway (PPG): WAP 2.0 mobile devices can be configured to use the WAP 2.0 proxy or to ignore it. However, if a WAP 2.0 proxy is not configured, the configuration resembles HTML over HTTP (in that you must choose the appropriate content rules so that HTTP policies can be applied to the WAP 2.0 traffic). The WAP 2.0 proxy enables you to identify WAP 2.0 traffic by configuring a content that examines traffic to and from the WAP 2.0 proxy. Using an account type of **http** enables billing of WAP 2.0, including support for policies based on the HTTP method, URL and HTTP header values. The current limitations of HTTP billing (with respect to Transport Layer Security [TLS]) apply to billing WAP 2.0 and MMS/WAP 2.0.

The CSG2 also supports PPG-Originated TCP (PO-TCP), implemented as WAP 2.0 over SMS OTA-PUSH rather than WAP 2.0 over HTTP. In PO-TCP, the PPG establishes a direct connection to the mobile device using prior knowledge of its IP address. The PPG negotiates an understanding of the mobile device identity and capabilities by using HTTP.request-method: OPTIONS, and then uses HTTP.request-method: POST to deliver the PUSH notification as a WAP 2.0 XML message.

WAP 2.0 mobile devices can implement support for extensive MMS over WAP 2.0. Service providers use MMS to differentiate and promote their products; thus, the billing of MMS over WAP 2.0 needs to be differentiated from other WAP 2.0 billing. The CSG2 can bill MMS over the supported WAP 2.0 flows at a differentiated rate by using HTTP billing capabilities to detect some or all of the following characteristics of MMS/WAP 2.0 traffic:

- The URL of a GET of MMS content points to the MMSC and encodes an MMS message ID.
- The URL of the POST of an MMS message or an MMS message notification acknowledgement points to the MMSC.
- The Content-Type HTTP header of the POST of an MMS message or an MMS message notification acknowledgement is “application/vnd.wap.mms-message”.

MMS over WAP 2.0 allows the following types of notification:

- PO-TCP
- SMS-based notification carrying the Uniform Resource Identifier (URI) for the MMS. The handset then initiates a GET request to that URI to retrieve the information.
- TO-TCP (Terminal-Originated TCP), which starts with SMS, but provides only the IP address of the PPG. The handset must then open a TCP connection and wait for an HTTP request from the PPG. This HTTP request is an OPTIONS method. It must succeed before the handset can retrieve the notification.

The CSG2 Layer 7 billing for MMS relies entirely on the PO-TCP and SMS-based notification types. TO-TCP is not supported.

Note If a terminal reuses a persistent PO-TCP to initiate a new method request, the packets are dropped and the PO-TCP connection appears hung until TCP retry attempts expire.

Support for WAP Segmentation and Reassembly (SAR)

The CSG2 applies the appropriate policy to the WAP transaction if it contains a URL that spans multiple WAP segmented packets.

There are no commands required to enable support for WAP SAR.

RTSP Features

The CSG2 provides the following Real Time Streaming Protocol (RTSP) features:

- RTSP Billing, page 1-22
- Per-Click Authorization, page 1-22
- Correlation, page 1-22

For RTSP, keep the following considerations in mind:

- RTSP offers minimal support for TCP-interleaved and HTTP-tunneled transport. For authorized content, the first stream is sent to the quota server. The action must be identical to that sent for the control connection because the stream is interleaved on the control connection and cannot be ended or charged independent of the control connection.
- RTSP supports multiple transport choices.
  - RTSP clients and servers negotiate the transport choice dynamically before the stream is started.
  - One transport choice is to interleave the stream with the control channel. In this mode, the CSG2 cannot map the transport connection to a different policy, and URL mapping cannot be supported.
  - The other transport choice for RTSP is use of a single HTTP connection. RTSP that is tunneled over HTTP has the same limitation as interleaved RTSP: The stream cannot be mapped to a policy different from the one used by the control connection, as both the stream and the control connection share the same transport.
- The CSG2 does not support multicast RTSP.
- The CSG2 does not support return code-based refunding for RTSP, but it does support flag-based refunding for RTSP.
- The CSG2 does not correlate streams that are described in a container file, such as SMIL.
- The CSG2 parses only the RTSP control session. When multiple RTSP streams are multiplexed over the same transport channel, the CSG2 reports cumulative statistics for all the streams.
- If RTSP URL mapping and filtering are used, and if multiple RTSP streams share the same transport channel, the CSG2 generates a single Content Authorization Request, and the request contains all the URLs carried over that stream. Also, the RTSP stream CDR contains the URLs for all the streams that are multiplexed over the same transport channel.
- If an RTSP proxy is used, place the CSG2 on the client side of the proxy. If the CSG2 is placed on the network side of the proxy, the CSG2 sees packets originating from the proxy, and the CDRs contain the proxy's IP address, instead of the client's.
- The CSG1 created two connections for every session (one for each direction of the flow). The CSG2 creates only the session. Therefore, the RTSP statistics reported by the **show ip csg content name detail** command for the CSG1 differ from those reported for the CSG2.

RTSP Billing

RTSP billing correlates all the streams that are associated with an RTSP session, and reports application-level information (for example, filename) to the billing system.

RTSP billing provides the following functionality:

- Correlation of various streams associated with an RTSP session
- Reporting of application-level information (for example, filename) to the billing system

RTSP uses the following protocols for streaming to the client. The client presents the server with a choice of acceptable protocols and port numbers, and the server responds with its choice of protocol that includes:

- RTSP also requires a UDP server-to-client stream for RTP (audio/video stream delivery), and a bidirectional UDP flow pair for exchanging synchronization information. The ports for the UDP flows are negotiated on the TCP connection during the SETUP exchange.
- RTSP can use RealNetworks Data Transport (RDT) for the stream transport. This establishes a UDP flow in each direction: one for stream delivery from the server, and the other for requesting the resending of lost media packets.
- RTSP can operate completely over the single TCP connection.
- RTSP can be tunneled over HTTP.

RTSP transport modes are negotiated on the control connection using the following methods:

- The client sends a SETUP request that identifies one or more modes it can support.
- The server responds with a mode that it has selected and ports that are to be used.

Per-Click Authorization

Per-click authorization implements functions like AoC redirection and retrieval of price from an external server. For the control session, the CSG2 sends a Content Authorization Request at the beginning of the TCP session. For each transaction involving a data stream, the CSG2 sends a Content Authorization Request before it allows the data stream to flow. This request allows the quota server to inspect the filename before granting authorization.

RTSP allows the multiplexing of multiple data streams over the same transport. For example, audio and video presentations can be multiplexed over the same UDP flows. The quota server must ensure that it does not send contradictory responses to the various Content Authorization Requests. For example, if one request is allowed and the other one is denied, the behavior of the CSG2 is undefined.

Correlation

The CSG2 provides RTSP correlation at the RTSP session level. All TCP/UDP flows associated with an RTSP session share a correlator.

The CSG2 does not correlate RTSP streams that do not share the RTSP session ID.

Correlating Multiple Streams Controlled by a Single RTSP Session

An RTSP session can control multiple streams, such as the audio stream and the video stream for a movie. For instance, a client can perform the following operations over the same RTSP session:

- DESCRIBE rtsp://a.ex.com/movie.sdp

The client requests the description of a movie. The server assigns a session ID to the client, and sends the.sdp file containing information about the movie.

- SETUP rtsp://a.ex.com/movie/audio

  The client requests the setup of a stream.

- SETUP rtsp://a.ex.com/movie/video

  The client requests the setup of a second stream. This results in the setting up of four UDP flows.

- PLAY rtsp://a.ex.com/movie.sdp

In this example, all the streams share the RTSP session and the session ID. There is one RTSP control TCP session, with four associated UDP streams. The CSG2 correlates all four UDP streams with the control session.

Correlating Multiple Streams Controlled by HTTP

HTTP sessions can be used to correlate multiple related RTSP streams. Different RTSP streams could go to different servers. The CSG2 has no easy way to determine which two streams are related. For example, a web server (W) hosts the media description file, movie.sdp; a video server (V) contains the video stream; and an audio server (A) contains the audio stream. Table 1-2 identifies the interactions that occur.

Table 1-2 Multiple Streams Controlled by HTTP

Client	Server	Protocol	Method/URL
C	M	HTTP	GET /movie.sdp
C	V	RTSP	SETUP rtsp://v.eg.com/video
C	A	RTSP	SETUP rtsp://a.eg.com/audio
C	V	RTSP	PLAY rtsp://v.eg.com/video
C	A	RTSP	PLAY rtsp://a.eg.com/audio

In the previous example, there are five concurrent sessions:

- One HTTP 1.1 session
- Two RTSP video sessions
- Two RTSP audio sessions

All of the TCP and UDP sessions associated with an RTSP session can be correlated. In this same example, the sessions associated with the video on server V are correlated. Similarly, the sessions associated with the audio on server A are correlated; however, there is no correlation between the audio and video flows, and neither the audio flow nor the video flow is correlated with the HTTP session.

Implications of Container Files

A container file is a storage entity in which multiple, continuous media types pertaining to the same subscriber presentation are present. A container file represents an RTSP presentation; each of its components is an RTSP stream. While the components are transported as independent streams, it is desirable to maintain a common context for these streams at the server. Synchronized Multimedia Integration Language (SMIL) is an example of a programming language that can be used to describe the contents of a container file.

The CSG2 does not correlate the streams within a container file.

Interleaved RTSP

Interleaved RTSP passes RTSP data in the TCP control session. Because the CSG2 parses the control session, it could cause a large performance bottleneck.

To avoid bottlenecks, the CSG2 performs the following actions for interleaved RTSP sessions:

- Waits for a SETUP request/reply to determine whether this is an interleaved RTSP session.
- Remembers the URL information.
- After determining interleaved RTSP, reports RTSP information to the BMA/quota server, and begins fastpath processing for the connection. Any subsequent transactions on the same RTSP control connection are not visible to the CSG2's billing function.

This method provides some RTSP-level information, but avoids making the RTSP path a target of denial-of-service (DoS) attacks. If most of the RTSP streaming billing applications are protected, customers have some control over the servers to ensure that interleaved RTSP is not used excessively.

CDRs

The CSG2 generates the following CDRs for RTSP:

- TCP control session: TCP, TCPInt, RTSP
- Data streams: RTSP stream
- UDP CDRs for each UDP session

Note If you are using fixed CDR support, the CSG2 does not generate any UDP CDRs.

RTSP billing in the CSG2 is based on inspection of the RTSP SETUP and TEARDOWN messages that are exchanged between the client and server. The CSG2 builds the RTSP CDR immediately after the RTSP TEARDOWN signal if the URL exactly matches the URL from the RTSP SETUP signal. Otherwise, the CSG2 builds the CDR after any condition that causes the flows to be terminated, as when a service_stop is triggered (for example, when the access server sends a RADIUS Accounting Stop for the subscriber).

Session Processing

RTSP control session processing uses an 8-byte correlator is assigned to the RTSP control session. The most significant 6 bytes of the correlator are assigned from the session ID and the session ID sequence. The least significant 2 bytes of the correlator are zeroed (for example, 0x0000).

The CSG2 keeps track of RTSP sessions, and an RTSP session is used to correlate multiple streams that are associated with the session.

Note An RTSP session might comprise more than one TCP session; alternatively, an RTSP session can exist without even one TCP session between client and server.

When the client sends a **setup** command, the CSG2 notes the client ports, and extracts the server port information from the SETUP response. Data connections to these ports are processed as if they hit the *content, policy* definition for the control server.

The following example (from RFC 2326) uses a single RTSP session to control multiple streams. The CSG2 actions are annotated after various steps.

In this example, the client (C) requests a presentation from the media server (M). The movie is stored in a container file. The client has attached an RTSP URL to the container file.

```
C->M: SYN port=RTSP
M->C: SYN-ACK
Assign 8 byte correlator X. Lower two bytes of the correlator are 0.

C->M: DESCRIBE rtsp://foo/twister RTSP/1.0
            CSeq: 1

M->C: RTSP/1.0 200 OK
            CSeq: 1
            Content-Type: application/sdp
            Content-Length: 164

            v=0
            o=- 2890844256 2890842807 IN IP4 172.16.2.93
            s=RTSP Session
            i=An Example of RTSP Session Usage
            a=control:rtsp://foo/twister
            t=0 0
            m=audio 0 RTP/AVP 0
            a=control:rtsp://foo/twister/audio
            m=video 0 RTP/AVP 26
            a=control:rtsp://foo/twister/video

C->M: SETUP rtsp://foo/twister/audio RTSP/1.0
            CSeq: 2
            Transport: RTP/AVP;unicast;client_port=8000-8001

M->C: RTSP/1.0 200 OK
            CSeq: 2
            Transport: RTP/AVP;unicast;client_port=8000-8001;
                       server_port=9000-9001
            Session: 12345678
```

Build RTSP record. Correlator = X + i. The CSG2 makes sure that X + i results in an even number. RTSP usage records for these two UDP flows carry X + i and X + i + 1 as the correlators. The correlators share 63 bits to help bind together the various flows for an RTSP transaction; that also enables you to distinguish the various interim records for one UDP flow from another.

```
C->M: SETUP rtsp://foo/twister/video RTSP/1.0
            CSeq: 3
            Transport: RTP/AVP;unicast;client_port=8002-8003
            Session: 12345678

M->C: RTSP/1.0 200 OK
            CSeq: 3
            Transport: RTP/AVP;unicast;client_port=8002-8003;
                       server_port=9004-9005
            Session: 12345678
```

Build RTSP record. Correlator = X + 3. RTSP usage records generated for these two UDP flows carry the same correlator.

```
C->M: PLAY rtsp://foo/twister RTSP/1.0
            CSeq: 4
            Range: npt=0-
            Session: 12345678


M->C: RTSP/1.0 200 OK
            CSeq: 4
            Session: 12345678
            RTP-Info: url=rtsp://foo/twister/video;
              seq=9810092;rtptime=3450012
```

```
C->M: TEARDOWN rtsp://foo/twister RTSP/1.0
            CSeq: 6
            Session: 12345678
V->C: RTSP/1.0 200 OK
            CSeq: 6
```

This TEARDOWN does not correspond to the SETUP URL; therefore, the CSG2 lets the streams idle out and sends the usage records when the streams idle out.

POP3 Support

The CSG2 generates a single CDR for each POP3 e-mail. The CDR includes all necessary information, such as the IP byte count and the TCP byte count. The CSG2 no longer generates a final TCP Stats record. If a subscriber downloads multiple e-mails during a single TCP session, the CSG2 generates a CDR for the previous e-mail each time it processes a new POP3 RETR (retrieve message) or TOP (retrieve specific lines of the message body) command. The CSG2 generates a CDR for the last e-mail when it processes the POP3 STATS (statistics) command (for TCP termination).

The CSG2 supports POP3 in both prepaid and postpaid mode. For **basis fixed** prepaid billing, the CSG2 treats each e-mail download as a transaction and a prepaid debit subject to weighting.

The CSG2 also supports refunding for POP3. If an e-mail download request (TOP or RETR) flows from the client to the server, and the next server response is not **OK**, or the session ends without seeing **OK**, then the prepaid debit returns the prepaid quota consumed for this transaction. The refund return code used is 554; if you want the CSG2 to provide refunding for POP3, you must specify return code **554** on the **retcode** command in CSG2 refund configuration mode for the POP3 refund definition.

If a subscriber tries to download e-mail and no e-mail exists, the CSG2 generates a POP3 CDR that contains an application return code TLV with a value of 554. This is the only condition in which the CSG2 includes a non-zero return code in a POP3 CDR.

To define the POP3 protocol type for a billing policy, use the **parse protocol pop3** command in CSG2 content configuration mode.

SMTP and POP3 Billing

SMTP is the Internet e-mail transfer protocol that operates over TCP with port 25. Subscribers send messages using SMTP. SMTP is also used to transfer messages between SMTP gateways (or relays). POP3 is a common protocol used to retrieve Internet e-mail from an e-mail server. POP3 also operates over TCP and typically uses port 110.

SMTP and POP3 messages consist of the following parts:

- Envelope—The SMTP and POP3 commands and responses.
- Headers—RFC 2822 headers that appear as contents to the SMTP and POP3 protocols. The RFC 2822 headers are of the form “header field name: header field body.” Some common header field names are “To,” “From,” “Date,” “Subject,” “Cc,” and “Bcc.”
- Body—The part of the message that appears as contents to the SMTP and POP3 protocols, but does not include headers. The headers and body of the message are separated by a blank line (for example, <CR><LF><CR><LF> in RFC 2822).

The CSG2 inspects SMTP and POP3 messages and reports all RFC 2822 header field names and bodies that appear in the header section of the message (before the body of the message). SMTP and POP3 envelope information is not reported, except for the SMTP return code from the DATA command. For

SMTP, the sender and recipients in the SMTP MAIL and RCPT commands are not reported, but the values from the "To," "From," "Date," "Cc," and "Bcc" headers in the contents of the e-mail message are reported to identify senders and recipients.

Because the amount of information in the header section might be greater than an IP packet encapsulated in an Ethernet frame, the information might span multiple records by using the CSG2 Continue Data Record type. Because the amount of information in a single header field might also be greater than an IP packet over Ethernet, the CSG2 Report String Attribute reports also has a continuation option. This means that information for a single header might span multiple CSG2 Report String Attribute reports, which might span multiple CSG2 Data Records.

Note If a TCP connection carries multiple e-mail messages, each e-mail message generates a separate SMTP or POP3 Data Record (plus Continuation Data Records if necessary).

SMTP CDR Header Removal

An SMTP CDR can be very large, as it includes a report attribute for each SMTP header embedded at the beginning of a message. The CSG2 enables you to eliminate these headers from an SMTP CDR, leaving only the SMTP envelope headers and the size attribute in the report. These are reported as X-CSG-MAIL, X-CSG-RCPT and X-CSG-SIZE.

For more information, see the "Configuring SMTP CDR Header Removal" section on page 2-19.

FTP Billing

The CSG supports both postpaid and prepaid FTP protocol-aware billing. The CSG can generate TCP billing records for FTP connections, and records that report FTP-specific information, such as the filename.

Users can define **basis fixed** and **basis byte** prepaid billing services for FTP.

Note There is no regular expression (map) support for differentiating FTP services.

FTP requires a control TCP connection to well-known server port 21.

Header, Method, and URL Mapping

The CSG2 uses maps to match headers, methods, or URLs against a pattern, to determine whether flows will be processed by the CSG2 accounting services.

For more information about maps, see the "Configuring Maps for Pattern-Matching" section on page 2-21.

Service Duration Billing

The Service Duration Billing feature enables the CSG2 to deduct quota based on the time of network usage for prepaid (or "managed") subscribers. With this feature, the subscriber is charged for the time duration of the CSG2 service. The following sections describe how this feature works:

- Charging for Service Duration Billing, page 1-28
- Calculating Usage for Service Duration Billing, page 1-28
- Reporting Quadrans to the Quota Server and to the BMA, page 1-31
- Handling Out-of-Quota Conditions, page 1-31

Charging for Service Duration Billing

Service Duration Billing is charged according to the following rules:

- For TCP sessions, the Last Billable Session Time (LBST) is the timestamp of the end of the session. The end of the session is detected using TCP session termination signaling (RST, FIN/ACK signals) or session idleness.

  Because non-TCP sessions (such as UDP) do not have a Layer 4 session termination mechanism, the LBST for non-TCP sessions is determined based on the time that the last packet was forwarded for the IP session.

- For a service, the First Billable Time (FBT) is the timestamp (in seconds) of the first grant of network access to a session mapped to a duration-based charging prepaid service. Typically, this time is equal to the timestamp of the first Service Authorization Response with a quota other than zero.

- For a service, the Last Billable Time (LBT) is the greatest timestamp (in seconds) of the LBST for all IP sessions mapping to the service for this subscriber. Optionally (and by default), the value for service idle is added to the maximum interval of the LBST when the LBT is calculated. The service idle timeout is added to the duration because the duration calculation already includes the intermediate idle intervals (the ones between IP sessions); this means that the last idle interval is also included.

Calculating Usage for Service Duration Billing

The calculations for Service Duration Billing usage are as follows:

- If the service is ended as a result of service idleness, the calculation for usage is:

  LBT – FBT = Usage

- If the service is ended as a result of an asynchronous event such as subscriber logoff, the calculation for usage is:

  LBT – FBT = Usage

  or

  Asynchronous Event Timestamp – FBT = Usage

  whichever is smaller.

- If the service runs out of quota, the calculation for usage is:

  LBT – FBT = Usage

  or

  Out Of Quota Timestamp – FBT = Usage

  whichever is smaller.

Note If the subscriber runs out of quota, but the subscriber refreshes the quota before the service idles out, the periods (or gaps) of zero quota are not included in the usage calculation.

When a Service Duration Billing service is a member of a billing plan, and an accounting definition is in service and downloaded to a CSG2 module, you cannot modify the billing basis or meter configuration. You are instructed at the console to configure **no inservice** on the downloaded accounting definitions.

The following examples show how Service Billing Duration usage is calculated in different situations. In these examples:

- SIT is the service idle timer, configured by using the **idle** command in CSG2 service configuration mode.
- The service idle time is not included in the billing charge.

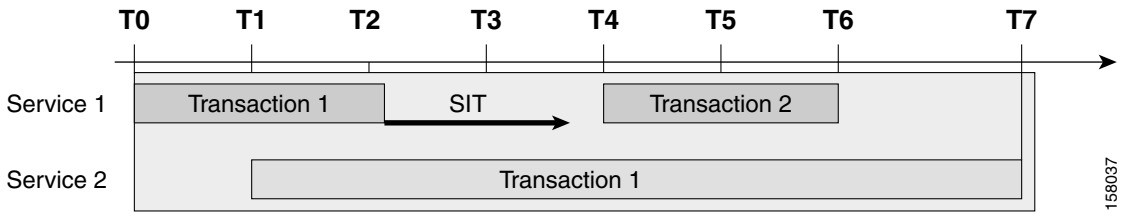
In Figure 1-2, the CSG2 calculates usage for Service 1 as:

(T2 – T0) + (T6 – T4) = Usage

and the usage for Service 2 as:

T7 – T1 = Usage

Figure 1-2 Service Duration Billing—Layer 7 Inspection, Two Services, Overlapping Transactions, Example One



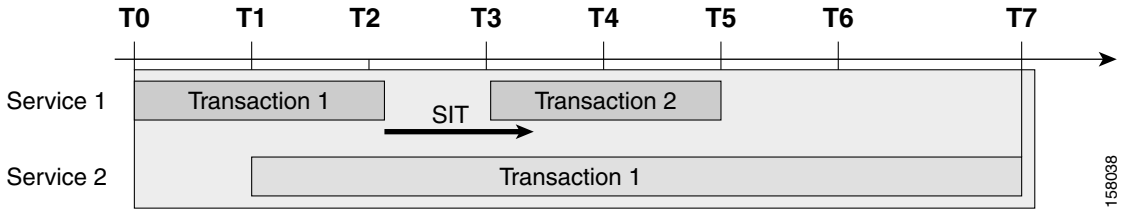
In Figure 1-3, the CSG2 calculates usage for Service 1 as:

T5 – T0 = Usage

and the usage for Service 2 as:

T7 – T1 = Usage

Figure 1-3 Service Duration Billing—Layer 7 Inspection, Two Services, Overlapping Transactions, Example Two



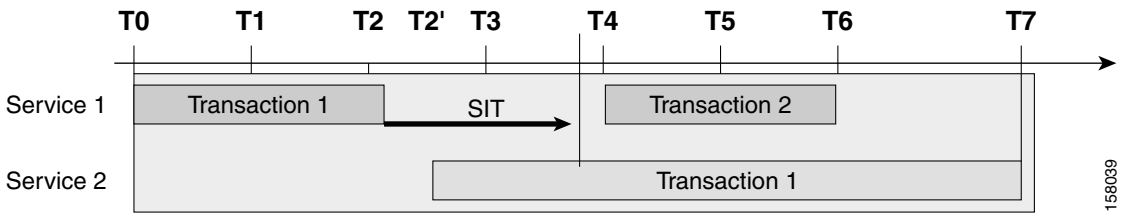
In Figure 1-4, the CSG2 calculates usage for Service 1 as:

(T2 – T0) + (T6 – T4) = Usage

and the usage for Service 2 as:

T7 – T2’ = Usage

Figure 1-4 Service Duration Billing—Layer 7 Inspection, Two Services, Non-Overlapping Transactions, Example One



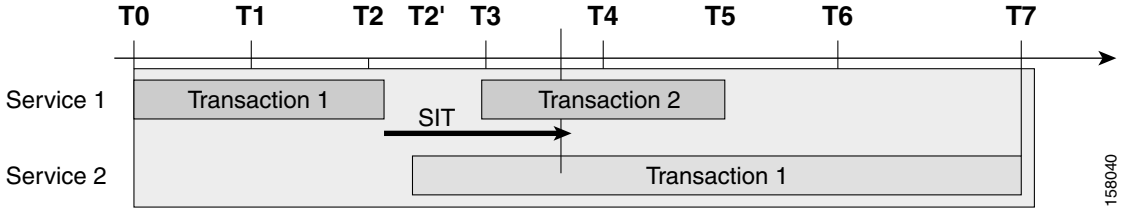
In Figure 1-5, the CSG2 calculates usage for Service 1 as:

T5 – T0 = Usage

and the usage for Service 2 as:

T7 – T2’ = Usage

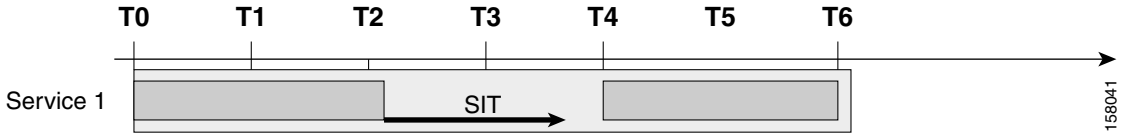
Figure 1-5 Service Duration Billing—Layer 7 Inspection, Two Services, Non-Overlapping Transactions, Example Two



In Figure 1-6, if T4 – T2 > SIT, the CSG2 calculates usage for Service 1 as:

(T2 – T0) + (T6 – T4) = Usage

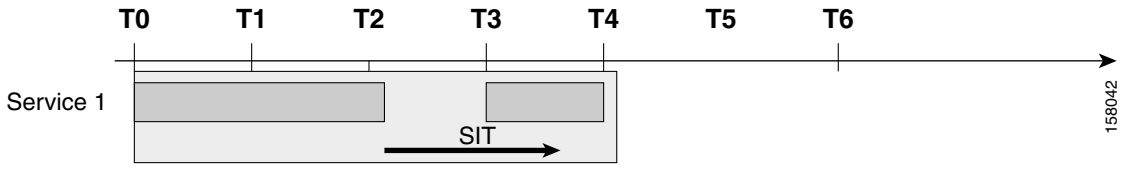
Figure 1-6 Service Duration Billing—Layer 7 Inspection, One Service, Example One



In Figure 1-7, if T3 – T2 < SIT, the CSG2 calculates usage for Service 1 as:

T4 – T0 = Usage

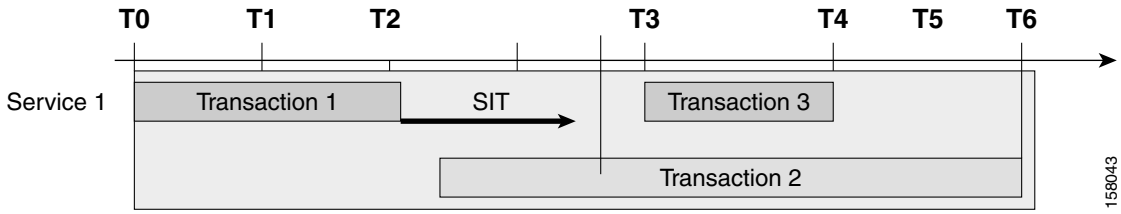
Figure 1-7 Service Duration Billing—Layer 7 Inspection, One Service, Example Two



In Figure 1-8, if the SIT does not time out, the CSG2 calculates usage for Service 1 as:

T6 – T0 = Usage

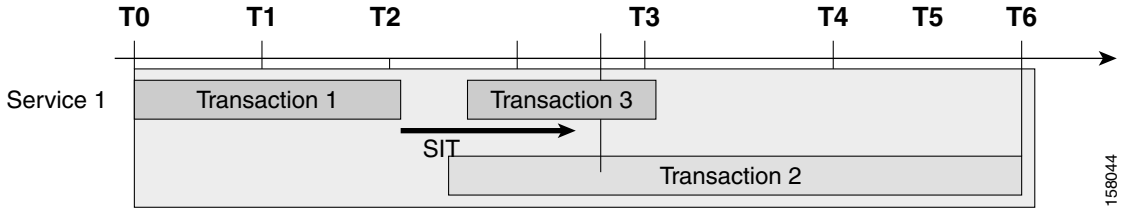
Figure 1-8 Service Duration Billing—Layer 7 Inspection, One Service, Example Three



In Figure 1-9, if the SIT does not time out, the CSG2 calculates usage for Service 1 as:

T6 – T0 = Usage

Figure 1-9 Service Duration Billing—Layer 7 Inspection, One Service, Example Four



Reporting Quadrans to the Quota Server and to the BMA

For Service Duration Billing, quadrans are reported to the quota server and to the BMA in seconds. In messages sent to the BMA on a per–IP-session basis (such as TCP statistics), the prepaid TLVs (Session ID, Service ID, Quadran) are present; the value for quadrans in the Quadran TLV is zero because the duration is based on service, not on individual sessions or on the sum of the durations of the individual sessions.

Handling Out-of-Quota Conditions

When a subscriber runs out of quota, the CSG2 ends the subscriber sessions that are mapped to the service. The sessions are ended using the same asynchronous session mechanism that is used when a subscriber User Table entry is deleted. The CSG2 reauthorizes when the remaining time is low (instead of 0) in order to more quickly determine session processing when zero quota is reached.

Connection Duration Billing

Connection Duration Billing enables the CSG2 to deduct quota based on the time that a subscriber is logged on to the IP network. That differs from Service Duration Billing, which charges on the basis of a service duration. Because the service measures the duration of subscriber access, the service is never idle—it is ended only when the subscriber logs out, or when a Service Stop Request is received from the quota server.

The CSG2 charges on the basis of the following rules:

- The First Billable Time (FBT) is the timestamp, in seconds, of the first non-zero grant of quota in a Service Authorization Response for the Connection Duration service. A Service Authorization Request is generated when the following conditions are met:
  - A User Table entry is created (typically as a result of a RADIUS Accounting Start message).
  - A Connection Duration service is part of the billing profile for the User Table entry (indicated in a RADIUS Access-Accept message, a RADIUS Accounting Start message, or a Quota Server User Profile Response).

  If the subscriber has quota, the FBT is typically the same time as the RADIUS Accounting Start message.
- The Last Billable Time (LBT) is the timestamp, in seconds, when the User Table entry is deleted. During the service lifetime, the CSG2 updates the LBT when either of the following situations occurs:
  - An IP session starts or ends.
  - The CSG2 sends a Service Reauthorization Request. This results in an update to the service balance and usage before the Service Reauthorization Request is sent. The CSG2 uses the following algorithm to calculate the usage:

    LBT – FBT = Usage

    or

    Out Of Quota Timestamp – FBT = Usage

    whichever is smaller.

    Therefore, if the service does not run out of quota, the algorithm is simply as follows:

    LBT – FBT = Usage

    If the subscriber runs out of quota, but refreshes the quota before the service times out, the periods of zero quota are not included in the usage calculation. When the subscriber runs out of quota, existing prepaid and postpaid IP sessions for the subscriber are terminated. If the subscriber does not have quota to proceed, no IP sessions are allowed for the subscriber. The CSG2 provides enforcement only for the policies that have accounting configured.

Connection Duration Billing requires an external quota server. Connection Duration Billing is not supported for internal quota servers, such as a gateway general packet radio service (GPRS) support node (GGSN) for postpaid subscribers. Therefore, you cannot use Connection Duration Billing if your quota servers are GGSNs.

To configure Connection Duration Billing, use the **activation** command and the **basis second** command in CSG2 service configuration mode.

When configuring Service Duration Billing, make sure the content idle timer duration, set using the **idle** command in CSG2 content configuration mode, does not exceed the service idle timer duration, set using the **idle** command in CSG2 service configuration mode.

Postpaid Service Tagging

This feature enables the CSG2 to map postpaid content to a CSG2 service, and to report the service name in a CSG2 Service ID TLV in transaction-level CDRs to the BMA. (The CSG2 Service Session ID TLV is not sent in variable-format records for postpaid service tagging.)

The service must be associated with a billing plan that is configured for postpaid mode. As with prepaid billing plans, the subscriber can be associated with a billing plan via a RADIUS message or a User Profile Response from the quota server. If no quota server is configured, and the billing plan cannot be determined from RADIUS messages, the subscriber is automatically associated with any billing plan configured for postpaid mode. We strongly recommend that you configure only one billing plan for postpaid mode.

Stateful Redundancy and Failover

The CSG2 supports stateful redundancy for HTTP, IMAP, POP3, SMTP, TCP, and WAP connections.

Stateful redundancy is the configuration of the active CSG2 to share information related to billing with its standby CSG2 in the event of a failure. That is, the session continues to be billed even when the active CSG2 fails and the standby CSG2 takes over.

During normal operation, connection and billing state information is sent by the active CSG2 to the standby CSG2, and from the active quota server to the standby quota server. The active CSG2 and the standby CSG2s maintain state information for the configured BMAs. The active CSG2 keeps the standby CSG2 informed about which BMAs and quota servers are being used. If the active CSG2 fails, the standby CSG2 takes over operation and tries to use the same BMAs or quota servers, if it has connectivity. Otherwise, the standby CSG2 selects the BMAs or quota servers that have the highest priority.

The active CSG2 also informs the standby CSG2 when user IDs are added to or removed from the User Table, and sends the correlators to the standby CSG2 to ensure consistency when sending billing records for recovered connections to the BMAs. Quota use is also correlated.

If connections are replicated to a standby CSG2, and a failover occurs, the CSG2 does not increment the content counters for traffic flowing through these connections. The CSG2 does increment the content counters for new connections created after the failover.

The CSG2 provides full stateful failover for IMAP sessions. The CSG2 provides limited stateful failover for FTP, HTTP, POP3, RTSP, SIP, SMTP, and WAP sessions.

- For POP3, SMTP, and WAP sessions, subscriber information and quota information are maintained on the standby CSG2; however, in-process transactions are not. If the active CSG2 fails, the subscriber transaction is completed on the standby, but no quota is charged for the transaction. Normal billing resumes with the subscriber's next transaction.
- For HTTP sessions, subscriber information and quota information are maintained on the standby CSG2; however, the sessions are downgraded to Layer 4. If the active CSG2 fails, the replicated HTTP session continues until it closes and a Layer 4 CDR is generated, but no quota is charged for the transaction. Normal billing resumes with the subscriber's next transaction.
- For FTP, RTSP, and SIP sessions, media traffic is replicated to the standby CSG2 and classified as postpaid type other traffic. A Layer 4 CDR is generated showing only the media traffic that passes on the standby CSG2. Control sessions for FTP, RTSP, and SIP do not have stateful support but are maintained to allow media traffic to pass. This support allows for the best user experience possible at the expense of allowing traffic to pass freely for existing sessions. New sessions starting on the standby CSG2 are handled normally.

The CSG2 also supports stateful redundancy for TCP connections. That is, the session continues to be billed even when the active CSG2 fails and the standby CSG2 takes over.

The CSG2 does not support stateful redundancy for IP or UDP connections.

Note Before manually resetting an active CSG2, make sure the standby CSG2 has the complete subscriber and session fault-tolerant (FT) configuration information. In the logs for the active CSG2, the following message indicates that the exchange with the standby CSG2 was successful: "CSG user and session FT dump complete."

The CSG2 counts and charges packets that complete CSG2 feature processing and are scheduled for forwarding. It is possible for these packets to be dropped in the SAMI module due to incomplete ARP entry, incorrect IP routing, or output queue contention. For example, when an active CSG2 fails over to a standby CSG2 in a redundant configuration, some ARP entries on the standby CSG2 might not yet be populated, and the CSG2 might drop packets. In many cases, you can resolve the problem with incomplete ARP entries by routing subscriber traffic and GTP' control traffic to a common default gateway IP address. Typically, this default gateway IP address is an address on the Supervisor Engine.

The CSG1 and CSG2 cannot act as stateful standbys for each other.

"Default" Policy

The CSG2 matches content on a best-match basis, based on Layer 3 and Layer 4 information. When there is a successful content match, the CSG2 matches against the policies configured within the content, linearly, on a first-match basis. If no policy within the content matches, the CSG2 matches against an implicit "default" policy, which matches all traffic. Matching this "default" policy does not generate a CDR, because no accounting policies can be configured for the "default" policy.

Note Even if you have used the **next-hop** command in CSG2 content configuration mode to define a next-hop IP address, traffic that matches the "default" content might not be routed with next-hop.

Tariff Switch

Tariff switch is a feature in which the CSG2 tracks the total quota usage for a prepaid service at the time of a tariff-time change. The tariff-time change is specified on a per-service basis by the quota server.

The CSG2 supports tariff switch for all prepaid protocols. The CSG2 sends tariff switch TLVs only for transaction-level CDRs, not for service-level CDRs.

The tariff switch usage for the prepaid service is reported to the quota server in the next Service Reauthorization, Quota Return, or Service Stop message sent for this service. The tariff switch usage for a tariff-time change is sent once and is sent in addition to the cumulative usage at the time of the message to the quota server. If the Supplemental Usage Reporting feature is enabled for a service at the tariff switch time, the CSG2 also reports supplemental usage at the tariff switch time in addition to the tariff-time switch usage.

The life of a prepaid service instance might span multiple tariff switch times. For a given service instance associated with a subscriber, the CSG2 can handle only one tariff switch time value.

If a transaction spans multiple tariff switches, the CSG2 reports only the most recent tariff switch information in its record, unless an intermediate record was generated between tariff-switch times.

The CSG2 might not generate a Service Reauthorization Request between tariff switch times. The quota server can force a report of the tariff switch time usage by specifying a quota timeout value in the Service Authorization Response that will force a Quota Return before the next tariff switch time. The quota server must choose the timeout carefully to avoid causing a flood of Quota Return messages at a given time. At any given time, the CSG2 service can track usage for a single tariff switch time; after reporting the usage for a tariff switch, the quota server can specify the time of the next tariff-time change in a Service Authorization Response.

If CSG2 refunding is configured for a prepaid service, the tariff switch usage might not include usage on existing IP sessions at the tariff switch time. This is because the usage cannot be charged until the session ends and the refund conditions are evaluated.

Tariff switch usage for individual transactions is reported to the BMA in the records containing quota usage (typically intermediate and stats records). Note that intermediate records might be sent to the BMA to report tariff switch usage, even without configuration of intermediate records; this is necessary because transactions might span multiple tariff switch times. To avoid flooding the BMA with records, the CSG2 sends intermediate records to the BMA for transactions that span a tariff switch time and do not terminate quickly. If a transaction is configured for BMA reporting using a fixed-format record, the tariff switch usage information is not reported in the record.

The “tariff switch qualified usage” field in the CDR is the cumulative usage since the creation of the service instance.

There are no commands required to enable tariff switch. The output of the **show ip csg users all detail** command displays information about the tariff switch.

Prepaid Error Reimbursement

The Prepaid Error Reimbursement feature (also known as CSG2 quota refund) allows the CSG2 to automatically refund quota for failed transactions, as defined by the CLI.

- To specify IP, TCP, or wireless application protocol (WAP) flag bit masks and values for CSG2 quota refund, use the **flags** command in CSG2 refund configuration mode.
- To specify the range of application return codes for which the CSG2 refunds quota, use the **retcode** command in CSG2 refund configuration mode. The return codes are protocol-specific.

The CSG2 also adds a refund TLV to the statistics records on the BMA interface. The refund TLV is added for transactions that meet a refund condition. The refund amount contains the quota amount to be refunded for the transaction. The refund amount is the same number that is reported in the quadrans TLV. Thus, the full charge for the transaction is always refunded for these protocols.

Note Prepaid Error Reimbursement requires an external quota server. Prepaid Error Reimbursement is not supported for internal quota servers, such as a GGSN for postpaid subscribers. Therefore, you cannot use Prepaid Error Reimbursement if your quota servers are GGSNs.

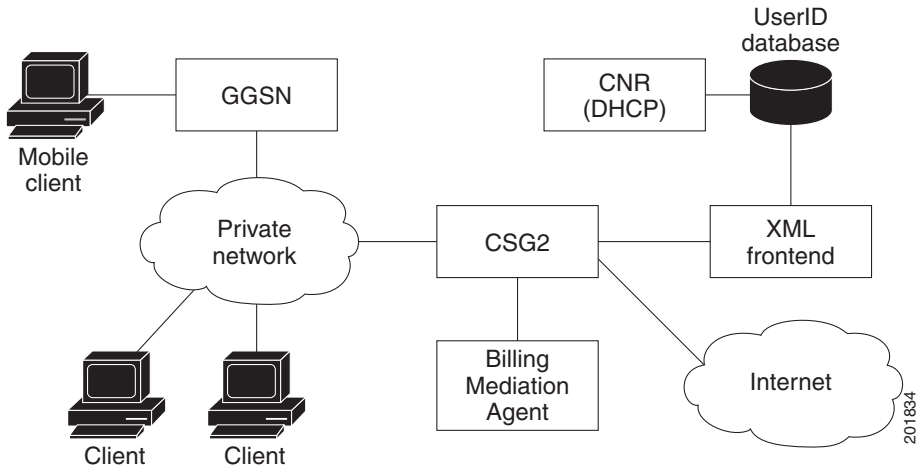
Prepaid Error Reimbursement is not supported for duration-based services.

Service-level CDRs do not contain quota reimbursement information.

Postpaid Billing

Figure 1-10 shows simple traffic flows between the various components in a simple postpaid CSG2 environment.

Figure 1-10 Traffic Flow Between Client and Server



Clients send requests that pass through a private network, or through a GGSN, before they reach the Internet.

The CSG2 monitors data flows and generates accounting records that can be used to bill customers at a content level. The CSG2 sends the accounting records to a Billing Mediation Agent (BMA), which formats the records as required by the customer's billing system.

User IDs are obtained from RADIUS Accounting records, or by querying the user database.

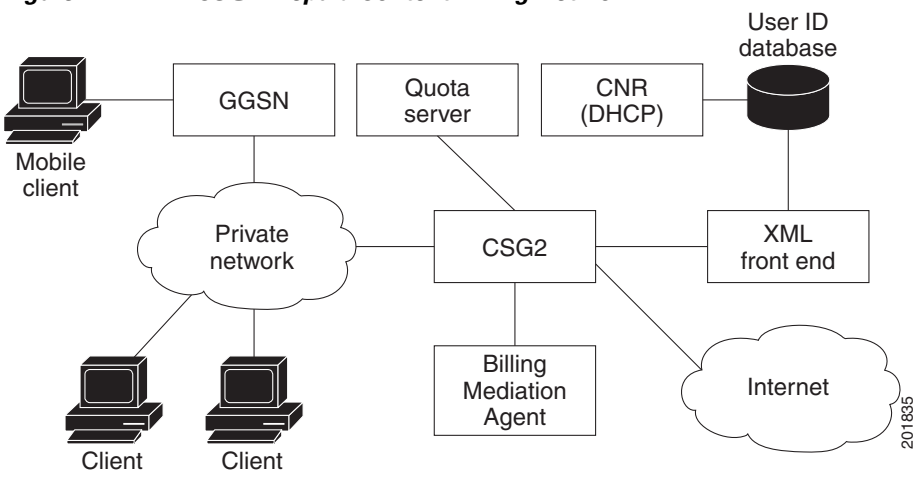
Prepaid Content Billing and Accounting

In addition to postpaid billing, the CSG2 provides prepaid content billing and accounting. You can configure multiple prepaid billing plans, and subscribers can choose the plan that best meets their needs. Each subscriber can use only one billing plan.

The CSG2 uses a BMA to interface with a billing server. At the end of each transaction, the CSG2 sends a billing record to the BMA, indicating the content accessed and the amount deducted. The BMA logs the information in the subscriber's bill.

The CSG2 uses a quota server to keep track of the quota that is left in the subscriber's account. Each CSG2 supports one quota server and multiple idle standby quota servers. The CSG2 allows multiple groups of subscribers on each quota server, with one quota manager for each subscriber. Figure 1-11 illustrates a typical CSG2 prepaid content billing network.

Figure 1-11 CSG2 Prepaid Content Billing Network



Quota is provided by the Quota Manager, on request for quota by the CSG2. This quota is either for an initial service connection, or for reauthorization when the original or last quota grant is depleted. The Quota Manager can provide a value ranging from 0 to 2,147,483,647 (0x00000000 to 0x7FFFFFFF). This value— called "quadrans"— comes in three forms: **basis byte** for volume-based billing, **basis fixed** for event-based billing, and **basis second** for duration-based billing.

When quota is depleted to zero, the subscriber can no longer access the service.

Quota is held on a per-service basis. Therefore, if a subscriber is connected to more than one service, the CSG2 stores quota for each service that is open.

After the subscriber finishes a session by closing the bearer session (a RADIUS Accounting Stop message is sent from a GGSN), the service is stopped, and any unused quota is returned to the Quota Manager.

While this prepaid system is in operation, the normal postpaid system runs by sending CDRs to the BMA.

CSG2 prepaid differs from CSG1 mostly due to the greatly reduced use of reserved quota. HTTP reserves a small amount of quota while processing a single TCP packet; other protocols do not reserve quota at all. This has the following benefits:

- Quota can no longer be "trapped" on a transaction that does not need the quota.
- The TLVs that contain quota balance and usage statistics are more accurate.
- Quota reauthorization thresholds are based on actual usage (except in some refund cases) instead of the sum of usage and reserved quota.
- Service-level CDRs are sent to BMAs at values closer to the volume thresholds.

The following flow example describes a basic prepaid flow between the CSG2 and the Quota Manager:

1. The NAS or GGSN sends a RADIUS Access Request message to the RADIUS Server.
2. On receipt of a RADIUS Access-Accept message from the RADIUS Server, the NAS or GGSN sends a RADIUS Accounting Start message to the RADIUS Server.
3. The CSG2 creates a subscriber entry and links the subscriber IP address to either the username or Calling Station ID (depending upon the configuration of the CSG2).
4. The CSG2 sends a User Authorization Request to the Quota Manager.
5. The Quota Manager replies to the CSG2 with a valid billing plan for the subscriber (User Authorization Response).

6. Subscriber traffic begins to flow from the NAS or GGSN to the requested network.
7. The CSG2 sends a Service Authorization Request to the Quota Manager, requesting quota for this connection.
8. The Quota Manager returns a given quota in the Service Authorization Response (if there is quota to give).
9. The subscriber traffic passes the CSG2 to the service, and the prepaid billing begins.
10. A Service Stop occurs if either the NAS or GGSN sends a RADIUS Accounting Stop message, or if the content and service time out.
11. The Service Stop provides the quota used and returns any remaining quota.

Obtaining User IDs

The CSG2 uses two methods to obtain user IDs:

- The CSG2 can use an external user ID database to map IP addresses to user IDs. When the CSG2 receives a packet with an unknown IP address, and it needs to associate the IP address with a user ID, it queries the database. If the user ID is not available, the CSG2 generates an accounting record without it.
- The CSG2 can act as a RADIUS Accounting Server or as a RADIUS proxy for RADIUS Accounting messages. The CSG2 can examine the accounting messages to determine the user IDs. (The CSG2 does not support full RADIUS Accounting.)

After identifying a subscriber, the CSG2 associates the subscriber's IP address with the user ID. If a quota server has been defined, the CSG2 tries to download the subscriber's profile. The profile indicates whether the subscriber is postpaid or prepaid and indicates the subscriber's billing plan. If the subscriber is prepaid, the CSG2 also downloads the subscriber's quota, and then forwards the subscriber's flows.

Filtering Accounting

Filtering lets you specify the following items:

- Sites to include or exclude for billing information. Specific sites are identified by URL, IP address, protocol, or port parameters.
- A customer string to insert in billing records for the specified site.
- That protocol-specific information is to be generated for billing records to a specified site.

The CSG2 supports Per-Event Filtering, which permits or denies a transaction as directed by the quota server.

To enable Per-Event Filtering, use the **aoc enable** command in CSG2 service configuration mode.

Intermediate CDRs

Typically, the CSG2 sends two billing records for each HTTP session. The CSG2 sends one record for all non-HTTP sessions, when the sessions end. However, for long-lived sessions, you might want to monitor the progress of the session. To monitor long-lived sessions, you can configure the CSG2 to send intermediate CDRs after a specified number of seconds, or after a specified number of bytes, whichever occurs first.

Intermediate counts are also correlated between the active CSG2 and the standby CSG2.

The CSG2 supports intermediate CDRs for FTP, HTTP, IP, RTSP, SIP, TCP, and UDP.

The CSG2 does not support intermediate CDRs for WAP or e-mail protocols (such as IMAP, POP3, and SMTP).

Packet Forwarding

The CSG2 forwards client/server traffic using next-hop, as specified in the content. For example:

```
ip csg content FORWARD-INTERNET-TRAFFIC
 ip any
 next-hop 1.1.1.1
 policy FORWARD_PKT
 inservice
```

In this example, if traffic matches this content and policy, the CSG2 forwards the traffic to the next-hop router that has an IP address of 1.1.1.1.

The CSG2 supports next-hop packet forwarding for all protocols.

Note Even if you have used the **next-hop** command in CSG2 content configuration mode to define a next-hop IP address, traffic that matches the "default" content might not be routed with next-hop.

URL-Redirect

You can configure the CSG2 to respond to an HTTP or WAP subscriber with a response code and a URL to which the subscriber must redirect. For more information about URL-redirect, see the "Configuring URL-Redirect" section on page 2-11.

Supplemental Usage Reports

You can configure the CSG2 to report supplemental usage to the quota server when sending a Service Stop, Quota Return, or Service Reauthorization Request message.

For more information, see the "Configuring Supplemental Usage Reporting" section on page 2-20.

Enhanced Interoperability with Cisco Service-Aware GGSN

The CSG2 can couple with a Cisco GGSN to form a service-aware GGSN. When operating in this mode, the CSG2 gets quota from the GGSN. For more information, see the *Cisco GGSN Release 5.2 Configuration Guide*.

There are no new commands required to enable enhanced interoperability.

Miscellaneous Features

The CSG2 provides the following miscellaneous features:

- IP Fragment Support for All Protocols, page 1-40
- Support for Out-of-Order Packets for All Protocols, page 1-40
- Asynchronous Service Stop, page 1-40
- Support for Port Number Ranges, page 1-40
- Packet Counts, page 1-40
- Negative Quadrans, page 1-41
- Enhancements for Layer 2, page 1-41

IP Fragment Support for All Protocols

The CSG2 supports IP fragmentation for all protocols, including fragments that arrive out of order.

There are no commands required to enable IP fragment support.

Support for Out-of-Order Packets for All Protocols

The CSG2 buffers packets that are received out of order, and processes and forwards them in the proper order.

There are no commands required to enable support for out-of-order packets.

Asynchronous Service Stop

The Asynchronous Service Stop feature allows the quota server to request the CSG2 to stop a prepaid service for a defined subscriber and service, and to send a Service Stop.

Support for Port Number Ranges

When you configure content on the CSG2, you can define a single port number, or a range of port numbers. This eliminates the need to configure a content for each port.

When defining a range of port numbers, choose a range that is applicable to the associated policies. For example, defining a range of port numbers from 80 to 8080 for **parse protocol http** means that the CSG2 must perform intensive HTTP inspection on many intermediate ports, ports that might not be expected to carry HTTP flows. HTTP inspection of such a high volume of non-HTTP flows can result in excessive processing by the CSG2, as well as generating many CDRs that the customer had not planned for.

Packet Counts

The CSG2 reports the number of IP bytes uploaded and downloaded, the number of TCP bytes uploaded and downloaded by the application, and the packet counts (or PDU counts for WAP records). These counts exclude the IP and TCP headers, as well as retransmissions.

Negative Quadrans

The quota balance in a prepaid service can become a negative value when the user's quota is being depleted, and the billing basis is **byte ip** or **byte tcp**. This can occur because the CSG2 forwards the entire received packet as long as the service's available quota is greater than 0. If the forwarded packet has more bytes than the quota balance, the balance becomes negative. Note that the CSG2 might report this negative balance to the quota server as a negative number in the Remaining Quota TLV.

Enhancements for Layer 2

The CSG2 processes “Hello” messages for Hot Standby Router Protocol (HSRP) version 1 and version 2.

If the MAC address of a directly-attached client is unknown, the CSG2 uses the Address Resolution Protocol (ARP) to get the IP address of the client dynamically. A “dummy” route for the client is no longer needed.

There are no commands required to enable these enhancements for Layer 2.

CSG2 Prerequisites

- Under certain conditions, such as low processor memory, a user session to the SAMI might fail. If this occurs, you will need to use the physical front panel consoles to access the SAMI.
- The CSG2 runs with Cisco IOS Release 12.2(33)SRB1 or later.
- If your configuration supports the maximum IP packet length, you must also configure the **buffers huge size 65535** command in global configuration mode.
- When you configure redundant CSG2s, the standby CSG2 must use the same software release as the active CSG2, or a later software release. If your CSG2s act as standbys for each other, they must all use the same software release.
- FTP requires a control TCP connection to well-known server port 21.

CSG2 Restrictions

- The CSG2 supports only Internet Protocol version 4 (IPv4). It does not support Internet Protocol version 6 (IPv6).
- You can install one CSG2 on each SAMI module, and up to nine SAMI modules on each Cisco 7600 series router chassis.
- The CSG2 supports up to 5000 interfaces.
- The CSG2 does not support IP packets larger than 1500 bytes.
- The CSG2 supports up to 10 concurrently active Billing Mediation Agents (BMAs).
- The CSG2 supports up to 10 concurrently active quota servers.
- The CSG2 supports up to 2048 contents, with up to 2033 available for user configuration, and up to 1024 services.
- The CSG2 supports up to 8192 policies.

- The CSG2 supports up to 4096 service rules, where a service rule is defined as a content/policy pair within a service applied to a billing plan.
- The CSG2 supports up to 128 billing plans.
- The CSG2 supports up to 4,000 total VLANs (client and server).
- Do not reuse port numbers on the same IP address.
- The CSG2 does not support dual quota (that is, the ability to deduct quota based on multiple criteria at the same time for the same flow).
- The CSG2 drops packets with Layer 2, Layer 3, or Layer 4 errors, without charging for those packets.
- The CSG2 reports all times in Coordinated Universal Time (UTC), regardless of the setting of the **clock timezone** or **clock summer-time** command in privileged EXEC mode.
- The CSG2 does not support the **clock set** command in privileged EXEC mode.
- The CSG2 does not support the **mset** option on the **standby timers** command in interface configuration mode.
- The CSG2 supports the Cisco Persistent Storage Device Module Software Release 2.0 or later.
- The CSG2 does not support dynamic routing, only static routing.
- For HTTP, the CSG2 imposes the following restrictions:
  - HTTP and HTTPS cannot share the same port. However, SSL can be tunneled over HTTP using the Connect method.
  - When HTTP X-Forwarded-For is enabled, only one CSG2 Traffic Processor (TP) is used for the entire system.
  - With RFC 2818, an HTTP session can become encrypted via the UPGRADE method. If Layer 7 billing is defined for the HTTP port, the session might time out when the UPGRADE occurs, because the CSG2 code cannot parse the encrypted data after TLS negotiation.
  - Some HTTP Layer 7 methods and content types cause the CSG2 to invoke Layer 4 processing for the remainder of the TCP connection. For details, see the HTTP compliance exceptions in the "Layer 7 Inspection (parse protocol=specific protocol)" section on page D-1.
- The CSG2 is transparent to Differentiated Services Code Point (DSCP) tagging. When the CSG2 forwards a packet, it forwards the DSCP value without modification.
- If all quota servers fail, the CSG2 begins storing Service Stop Requests, in order to forward them when a quota server comes back online. In a Cisco mobile Service Exchange Framework (mSEF) GGSN-CSG2 environment, when the GGSN quota server comes back online and the CSG2 forwards the stored Service Stop Requests, if the subscriber's packet data protocol (PDP) context is no longer active or is not known to the Diameter-Closed Loop Charging Interface (D-CLCI) backend, the GGSN quota server might respond to the request with GTP reject code 201.
- If there are no teletypes (TTYs) available, CSG2 configuration commands might fail. Therefore, do not allow the TTYs to become depleted.

CHAPTER 2

Configuring the CSG2

This section describes the steps to take when installing and configuring the Content Services Gateway 2 (CSG2):

- Preparing to Install the CSG2 Software, page 2-1
- Installing the CSG2 Software, page 2-3
- Upgrading the CSG2 Software, page 2-7
- Saving and Restoring CSG2 Configurations, page 2-7
- Configuring the CSG2, page 2-8
- CSG2 Configuration Examples, page 2-29

Note For hardware requirements, such as power supply and environmental requirements, as well as hardware installation instructions, see the *Service and Application Module for IP User Guide*.

Preparing to Install the CSG2 Software

Before you install the CSG2, keep the following considerations in mind:

- When upgrading the CSG2, we do not recommend performing an in-service upgrade from CSG2 Release 4, or any earlier release, to CSG2 Release 5, or any later release.
- The CSG2 requires one of the following Supervisor Engines:
  - Supervisor Engine 720 with an MSFC3-BXL (SUP720-MSFC3-BXL) running Cisco IOS Release 12.2(33)SRB1 or later.
  - Cisco 7600 Series Supervisor Engine 32, with a Multilayer Switch Feature Card, running Cisco IOS Release 12.2(33)SRC or later and LCP ROMMON Version 12.2[121] or later
  - Cisco Route Switch Processor 720 with Distributed Forwarding Card DFC3CXL, running Cisco IOS Release 12.2(33)SRC or later

  The CSG2 does not support any earlier releases of the Cisco IOS. Therefore, you must upgrade to a Supervisor Engine running the specified Cisco IOS release or later, before installing the Service and Application Module for IP (SAMI), and before running or upgrading the CSG2 on the SAMI.

  For details on upgrading the Cisco IOS release running on the Supervisor Engine, refer to the "Upgrading to a New Software Release" section in the *Release Notes for Cisco IOS Release 12.2SR for the Cisco 7600 Series Routers*.

For information about verifying and upgrading the LCP ROMMON image on the Cisco SAMI, see the "Manually Upgrading an LCP ROMMON Image" section in the *Cisco Service and Application Module for IP User Guide*.

- You must configure virtual LANs (VLANs) on the Cisco 7600 series router and assign physical interfaces to the VLANs *before* you configure VLANs for the CSG2. The VLAN IDs for the router and for the CSG2 must be the same. For details, see the *Cisco 7600 Series Cisco IOS Software Configuration Guide*.
- If the Multilayer Switch Function Card (MSFC) is used on the next-hop router on either the subscriber-side VLAN or the network-side VLAN, then you must configure the corresponding Layer 3 VLAN interface.

Caution If you use the MSFC as the router for both the subscriber side and the network side at the same time, you must ensure that packets for billable flows cannot bypass the CSG2. Also, if you use static **ip route** commands to switch traffic to the CSG2s, packets might loop between the MSFC and the CSG2 in this configuration. To avoid these problems, use other routing techniques to switch packets to the CSG2, such as policy-based routing.

The following example shows how to configure the Layer 3 VLAN interface:

```
Sup> enable
Sup# configure terminal
Sup(config)# interface vlan 130
Sup(config-if)# ip address 10.10.1.10 255.255.255.0
Sup(config-if)# no shutdown
Sup(vlan)# exit
```

- The software interface for the CSG2 is the Cisco IOS command-line interface (CLI). For more information about using the CLI and Cisco IOS command modes, see the *Cisco 7600 Series Cisco IOS Software Configuration Guide*.
- During the installation and configuration, enter all commands by either establishing a console connection with the CSG2, or by Telnetting to the CSG2. Enter each configuration command on a separate line.
- In any command mode, you can enter the question mark (?) at the prompt to see a list of available commands. For example:

```
Sup> ?
```

or

```
Sup(config)# ip csg ?
```

The online help shows the default configuration values and the ranges that are available for each command.

Installing the CSG2 Software

You could install the CSG1 software from the Supervisor Engine boot flash memory, from a removable flash PC memory card inserted in the Supervisor Engine, or from an external TFTP server.

However, you install the CSG2 software for the SAMI, independent of the Supervisor Engine. That is, no Supervisor Engine upgrade is needed when you install the CSG2 feature enhancements.

To install the CSG2 software, follow these steps:

Step 1 Assign VLANs to the CSG2 by entering the following commands, beginning in privileged EXEC mode:

```
Sup# enable
Sup# configure terminal
Sup(config)# svclc vlan-group group-number vlan-range
Sup(config)# svclc module slot-number vlan-group group-number
Sup(config)# svclc multiple-vlan-interfaces
```

where:

- *group-number* is the number of the VLAN group that you are assigning to the CSG2.
- *vlan-range* is a list of one or more VLANs in the group, specified as follows:
  - A single number in the range 2 to 1000 or 1025 to 4094
  - A range of numbers separated by a hyphen, such as 2-5
  - Single numbers or ranges of numbers separated by commas, such as 5,7-10,13,45-100
- *slot-number* is the slot in which the CSG2 is installed.

For example, to assign VLAN groups 1 and 6 to the CSG2 in slot 2, enter the following commands, beginning in privileged EXEC mode:

```
Sup# enable
Sup# configure terminal
Sup(config)# svclc vlan-group 1 5,30,43,765
Sup(config)# svclc vlan-group 6 6
Sup(config)# svclc module 2 vlan-group 1,6
Sup(config)# svclc multiple-vlan-interfaces
```

Step 2 Bypass the Domain Name System (DNS) security for the remote copy protocol (rcp) and remote shell (rsh), by entering the following command in global configuration mode:

```
Sup(config)# no ip rcmd domain-lookup
```

Step 3 Enable the CSG2 to copy files to and from the Supervisor Engine, by entering the following command in global configuration mode:

```
Sup(config)# ip rcmd rcp-enable
```

Note Because of the way the CSG2 configuration is stored on the Supervisor Engine, you cannot use the MIB to copy the startup CSG2 configuration directly off of the SAMI. The configuration must be collected via Telnet or Secure Shell (SSH). If you are using CiscoWorks RME to manage your configuration, make sure the option to enable Telnet or Secure Shell (SSH) collection is enabled

Step 4 Enable the CSG2 to execute commands on the Supervisor Engine using rsh or rcp, by entering the following command in global configuration mode:

```
Sup(config)# ip rcmd remote-host local-username {ip-address | host | access-list}
remote-username [enable [level]]
```

where:

- *local-username* is the name of the CSG2 on the local router.
- *ip-address* is the IP address of the remote host from which the local router will accept remotely executed commands.
- *host* is the name of the remote host.
- *access-list* is the number of an access list of remote hosts.
- *remote-username* is the name of the CSG2 on the remote host.
- **enable** enables the CSG2 to execute privileged EXEC commands using rsh, or to copy files to the router using rcp.
- *level* is the privilege level assigned to the CSG2. The privilege level defaults to 15, the highest level.

For example, to enable the CSG2 to copy commands to and from the Supervisor Engine, using remote host HOST1, at the highest privilege level, enter the following command in privileged EXEC mode:

```
Sup(config)# ip rcmd remote-host * HOST1 * enable
```

Step 5 Configure the Supervisor Engine as a Cisco Network Time Protocol (NTP) master clock to which the CSG2 can synchronize itself, by entering the following commands in global configuration mode:

```
Sup(config)# ntp master
Sup(config)# ntp update-calendar
```

Step 6 Download a CSG2 software image from the Supervisor Engine by entering the following command from the Supervisor prompt:

```
Sup# upgrade hw-module slot slot-number software file name
```

where:

- *slot-number* is the slot in which the SAMI is installed.
- *name* is the CSG2 image name.

The following message is displayed while the image is being downloaded:

Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC

When the download is complete, the following prompt is displayed:

```
Sup#
```

Step 7 Power down and reset the CSG2 by entering the following command in privileged EXEC mode:

```
Sup# hw-module module slot-number reset
```

where *slot-number* is the slot in which the CSG2 is installed.

The CSG2 powers down and resets.

Step 8 Establish a console session with the CSG2, by entering the following command in privileged EXEC mode:

```
Sup# session slot slot-number processor 3
```

Or Telnet to the CSG2, by entering the following command in privileged EXEC mode:

```
Sup# telnet 127.0.0.slot-number3
```

where:

- *slot-number* is the slot in which the CSG2 is installed.
- **3** is the control processor (CP) number for the CSG2. Always session into CP 3 when configuring or monitoring the CSG2.

Step 9 Define a GigabitEthernet subinterface for VLAN subscriber and network traffic, and enable 802.1Q encapsulation, by entering the following commands, beginning in privileged EXEC mode:

```
csg2# configure terminal
csg2(config)# interface GigabitEthernet 0/0.3
csg2(config-if)# encapsulation dot1q vlan-id
```

where *vlan-id* is the VLAN identifier.

Step 10 Configure the VLAN as a subscriber interface for the CSG2, by entering the following command in interface configuration mode:

```
csg2(config-if)# ip csg subscriber
```

Step 11 Configure a primary IP address for the interface, by entering the following command in interface configuration mode:

```
csg2(config-if)# ip address ip-address mask
```

where:

- *ip-address* is the primary IP address.
- *mask* is the CSG2 mask for the associated IP subnet.

Step 12 Configure a standby IP address to activate the Hot Standby Router Protocol (HSRP) for the interface, by entering the following command in interface configuration mode:

```
csg2(config-if)# standby ip ip-address
```

where *ip-address* is the standby IP address.

Step 13 If you are not configuring the CSG2 for redundancy (that is, active-only operation), you must define a secondary IP address under the GigabitEthernet interface to be used as the RADIUS endpoint or RADIUS proxy CSG2 IP address. To do so, enter the following command in interface configuration mode:

```
csg2(config-if)# ip address ip-address mask secondary
```

where:

- *ip-address* is the secondary IP address.
- *mask* is the CSG2 mask for the associated IP subnet.

If you are configuring the CSG2 for redundancy (that is, active-standby operation), you must define a standby secondary IP address as the RADIUS endpoint or RADIUS proxy CSG2 IP address.

Step 14 Identify the CSG2 as an endpoint for RADIUS Access and RADIUS Accounting messages, by entering the following command in global configuration mode:

```
csg2(config)# ip csg radius endpoint [vrf csg-vrf-name] csg-address
key [encrypt] secret-string [vrf sub-vrf-name]
```

Or identify the CSG2 as a proxy for RADIUS Access and RADIUS Accounting messages by entering the following command in global configuration mode:

```
csg2(config)# ip csg radius proxy [vrf csg-vrf-name] csg-address [vrf server-vrf-name]
server-address csg-source-address [key [encrypt] secret-string] [vrf sub-vrf-name]
```

where:

- **vrf** *csg-vrf-name*, **vrf** *server-vrf-name*, and **vrf** *sub-vrf-name* are the Virtual Routing and Forwarding (VRF) tables used for RADIUS communication.

Note The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters.

The CSG2 does not support the use of the word **forwarding** as a valid VRF name.

- *csg-address* is the CSG2 IP address.
- *server-address* is the RADIUS proxy server IP address.
- *csg-source-address* is the RADIUS proxy source IP address that the CSG2 is to use when sending packets to the server.
- **key** is the RADIUS key.
- *encrypt* indicates how the *secret-string* is represented when the configuration is displayed (for example, **show run**), or how it is written to nonvolatile memory (for example, **write memory**).
- *secret-string* is the clear password value for MD5 authentication.

Step 15 Enable the CSG2 to synchronize its software clock with the one in the Supervisor Engine, by entering the following command in global configuration mode:

```
csg2(config)# ntp server 127.0.0.xy
```

where:

- *x* is the slot in which the Supervisor Engine is installed.
- *y* identifies the Supervisor Engine—1 for Supervisor Engine 720.

Step 16 Establish a static route for traffic to the CSG2, by entering the following command in global configuration mode:

```
csg2(config)# ip route prefix mask ip-address
```

where:

- *prefix* is the IP route prefix for the destination.
- *mask* is the prefix mask for the destination.
- *ip-address* is the IP address of the next hop that can be used to reach that network.

Step 17 Power down and reset the CSG2 by entering the following command in privileged EXEC mode:

```
Sup# hw-module module slot-number reset
```

where *slot-number* is the slot in which the CSG2 is installed.

The CSG2 powers down and resets.

Upgrading the CSG2 Software

To upgrade the CSG2 software, follow these steps:

Step 1 Download a CSG2 software image from the Supervisor Engine by entering the following command from the Supervisor prompt:

```
Sup# upgrade hw-module slot slot-number software file name
```

where:

- *slot-number* is the slot in which the SAMI is installed.
- *name* is the CSG2 image name.

The following message is displayed while the image is being downloaded:

Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC

When the download is complete, the following prompt is displayed:

```
Sup#
```

Step 2 Establish a console session with the CSG2, by entering the following command in privileged EXEC mode:

```
Sup# session slot slot-number processor 3
```

Or Telnet to the CSG2, by entering the following command in privileged EXEC mode:

```
Sup# telnet 127.0.0.slot-number3
```

where:

- *slot-number* is the slot in which the CSG2 is installed.
- **3** is the control processor (CP) number for the CSG2. Always session into CP 3 when configuring or monitoring the CSG2.

Step 3 At the prompt, enter the following command to reload the CSG2:

```
Router# reload
```

Saving and Restoring CSG2 Configurations

Note In CSG1, the configuration was modified and stored along with the Supervisor Engine configuration.

In CSG2, the configuration is modified and stored by either establishing a session with the control processor (CP), or via a direct console connection with the CSG2.

To save the CSG2 configuration on the Supervisor Engine bootflash and slave bootflash, enter the following command in privileged EXEC mode:

```
csg2(config)# write memory
```

For more information about saving and restoring configurations, see the *Cisco 7600 Series Cisco IOS Software Configuration Guide*.

Configuring the CSG2

Note Unless otherwise specified, all the examples in this guide assume that you have already established a console session with the CSG2, or that you have Telnetted to the CSG2, and that you have entered the appropriate configuration mode for the command that you are configuring.

Perform the following tasks to configure content billing features on the CSG2:

- Configuring the User Database, page 2-9
- Configuring the CSG2 User Table, page 2-9
- Configuring the Fragment Database, page 2-11
- Configuring the Session Table, page 2-11
- Configuring URL-Redirect, page 2-11
- Configuring Policies and Traffic Types, page 2-13
- Configuring a Content Billing Service, page 2-13
- Configuring Content, page 2-14
- Configuring Single-TP Mode, page 2-16
- Configuring Fixed, Variable, or Combined Format CDR Support, page 2-17
- Configuring a Refund Policy on the CSG2, page 2-18
- Configuring HTTP Header Reporting, page 2-19
- Configuring SMTP CDR Header Removal, page 2-19
- Configuring Supplemental Usage Reporting, page 2-20
- Configuring Actual PDU Reporting for WAP, page 2-20
- Configuring Maps for Pattern-Matching, page 2-21
- Configuring Connection Redundancy, page 2-21
- Configuring High Availability, page 2-21
- Classifying Data Traffic, page 2-26
- Configuring a CSG2 Subscriber Interface, page 2-26
- Configuring Case Sensitivity, page 2-26
- Configuring WAP and WSP Support, page 2-27
- Blocking Ports, page 2-28
- Configuring SNMP Timers, page 2-28
- Configuring the SAMI Bit Rate Limit, page 2-29
- Configuring the SNMP Notification Types, page 2-29

Configuring the User Database

The CSG2 can use an XML user database to associate an IP address with a user ID, and can refer to the database when it receives a packet with an unknown IP address. XML-based database queries add additional robustness to the CSG2, allowing continued monitoring across a failover, even in the absence of fresh RADIUS flows.

To configure the user database that you want the CSG2 to query for user IDs, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg database [vrf vrf-name] ip-address port-number local-port`	Identifies the database server that answers CSG2 user ID queries. You can configure one and only one database server to answer CSG2 user ID queries. **Note** The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters. The CSG2 does not support the use of the word **forwarding** as a valid VRF name.

Configuring the CSG2 User Table

The CSG2 User Table identifies all subscribers known to the CSG2. The table is populated on the basis of the contents of RADIUS Accounting Start messages, or from the user database, if either feature is enabled in your configuration.

When the CSG2 processes a data packet, it searches the User Table and queries the user database for source and destination IP addresses that match the data packet:

1. If the User Table contains an entry with a matching source IP address, the CSG2 uses that entry for charging and for CDR generation.
2. If not, then if the User Table contains an entry with a matching destination IP address, the CSG2 uses that entry for charging and for CDR generation.
3. If not, then if the user database is configured and it contains an entry with a matching source IP address or destination IP address, the CSG2 uses the IP address that is returned (and the associated user ID) for charging and for CDR generation.
4. If neither the User Table nor the user database contains a matching source or destination IP address, then the CSG2 uses postpaid charging for the data packet, and the generated CDRs do not contain a user ID.

To configure the User Table, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg entries user profile {quota-server | radius {pass | remove | timeout timeout}}`	Specifies the location from which the CSG2 is to obtain the subscriber profile and billing plan when generating entries for the User Table.

You can set a global idle timer for User Table entries for all billing plans, and you can also set an individual User Table entry idle timer for each individual billing plan.

- If an idle timer is set for a billing plan, the CSG2 uses that idle timer.
- Otherwise, the CSG2 uses the global idle timer.

That is, if there is an entry idle timer value in the billing plan, it is used; otherwise, if there is a global entry idle timer value configured, it is used.

The idle timer for a subscriber entry starts when all billable sessions for that subscriber have ended. Typically, a TCP session ends when the subscriber and the network have sent FIN messages to each other. Other protocols time out based on the configured idle timer value in the content configuration. The timer restarts when a RADIUS Accounting Start or an Interim Accounting message is received. The timer stops when a session starts.

When the idle timer expires, if Packet of Disconnect (PoD) is not configured, the CSG2 deletes the User Table entry. If Packet of Disconnect (PoD) is configured, the CSG2 sends a PoD message and the CSG2 deletes the User Table entry when the PoD message is ACKed, NAKed, or when all retries have been sent; the RADIUS Stop message does not have to be received by the CSG2.

The idle timer also enables the CSG2 to eliminate an idle User Table entry if the NAS fails to deliver a RADIUS Accounting Stop request for an idle subscriber. Eliminating idle entries from the User Table frees up CSG2 resources.

If Connection Duration Billing is enabled, you can use either the global entry idle timer or the billing plan entry idle timer to release a subscriber connection.

The idle timer does not affect sticky user entries.

To set a global User Table idle timer, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg entries user idle` *duration* [**pod**]	(Optional) Specifies how long the CSG2 is to retain entries in the CSG2 User Table.

To set a User Table idle timer for a specific billing plan, enter the following command in CSG2 billing configuration mode:

Command	Purpose
`csg2(config-csg-billing)# entries user idle` *duration* [**pod**]	(Optional) Sets the time after which entries for idle subscribers are deleted from the CSG2 User Table.

The CSG2 User Table can hold up to 1250000 entries with the 2 GB-SAMI option, or up to 500000 entries with the 1 GB-SAMI option. However, the CSG2 also enables you to specify the maximum number of entries allowed in the User Table. To do so, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg entries user max entries`	(Optional) Specifies the maximum number of entries allowed in the CSG2 User Table. The maximum number of entries is not enforced on the buffer pool maximum size, it is enforced during allocation of individual entries to the User Table.

Configuring the Fragment Database

The CSG2 enables you to define the maximum number of entries in the CSG2 fragment database, as well as how long the CSG2 is to retain the entries.

The CSG2 divides the configured maximum number of entries evenly among the traffic processors. For example, if you configure a maximum of 100 entries, the maximum buffer pool size on each traffic processor is 20.

To configure the fragment database, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg entries fragment {idle duration | maximum entries-number}`	(Optional) Defines the maximum number of entries in the CSG2 fragment database, or defines how long the CSG2 is to retain the entries.

Configuring the Session Table

The CSG2 enables you to specify the maximum number of entries allowed in the CSG2 session table. This is the maximum number of sessions that the CSG2 can support. When the number of active sessions reaches the specified maximum, the CSG2 begins dropping incoming new sessions.

The maximum number of entries is not enforced on the buffer pool maximum size, it is enforced during allocation of individual subscriber sessions to the table.

To specify the maximum number of entries allowed in the CSG2 session table, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg entries session user max entries`	(Optional) Specifies the maximum number of entries allowed in the CSG2 session table.

Configuring URL-Redirect

The CSG2 can redirect subscriber flows to an alternate IP address or URL when a subscriber's quota is exhausted. Once configured, the CSG2 redirects subscriber requests to another network that informs the subscriber that the quota has been exceeded and that describes any appropriate actions to take.

In a redirect scenario, the CSG2 responds to the HTTP or WAP subscriber with a response code and a URL to which the subscriber must be redirected.

You can configure the redirect URL using the **ip csg redirect** command in CSG2 user group configuration mode, or the quota server can provide the redirect URL during service authorization (or reauthorization) or content authorization processing.

For service authorization or content authorization, the quota server reply contains the REDIRECT-URL action code and the redirect URL. In some network configurations, you might want the quota server to return the same redirect URL for HTTP and WAP. If you do not want to use a single redirect URL, the service authorization and Content Authorization Requests identify whether the request is for HTTP or WAP.

A redirect URL that is returned from the quota server in a service authorization response, or that is returned in a Content Authorization Response with the REDIRECT_URL action code, takes precedence over a redirect URL that is configured using the **ip csg redirect** command. The CSG2 uses the URL specified by the **ip csg redirect** command when the quota server responds with the FORWARD action code.

- The **ip csg redirect http** command redirects subscriber HTTP flows to the specified alternate URL when the subscriber's quota is exhausted.
- The **ip csg redirect sip** command redirects subscriber SIP flows to the specified alternate URL when the subscriber's quota is exhausted.
- The **ip csg redirect interval** command specifies the length of time, in seconds, during which the CSG2 redirects an out-of-quota subscriber. After this interval, the CSG2 drops the requests until quota can be requested again. The start of the interval is the time of the first redirect after a quota grant of zero. The counter is reset, and the timer is stopped after another quota grant of zero is given.
- The **ip csg redirect maximum** command specifies the maximum number of times a redirect is to be performed for an out-of-quota subscriber during a redirect interval.
- The **ip csg redirect wap** command redirects subscriber WAP flows to the specified alternate URL when the subscriber's quota is exhausted.

For example, if all of the following conditions are met:

- The **ip csg redirect interval** command is set to 8 seconds.
- The **ip csg redirect maximum** command is set to 15.
- The CSG2 receives a Service Authorization Response with zero quadrans.
- The CSG2 has redirect information.

Then redirection occurs when the subscriber runs out of quota (assuming that the subscriber has not received quota in the interim). The 8-second timer starts after the first redirect. Therefore, request 1 is redirected, and up to 14 more requests can be redirected, if they occur within 8 seconds after the first redirect.

URL-redirect requires configuration of a policy and service so that subscribers who have exhausted their quotas can access the network specified in the redirect URL.

To redirect subscriber flows to an alternate IP address when the subscriber's quota is exhausted, or to set the amount of time and the number of redirects that the CSG2 allows, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg redirect {http` *url* `| interval` *seconds* `| maximum` *number* `| sip` *url* `| wap` *url*`}`	(Optional) Redirects subscriber flows to an alternate IP address when the subscriber's quota is exhausted.

Configuring Policies and Traffic Types

Policies are access rules that traffic must match in order to be handled by a specific server farm. Policies allow the CSG2 to apply filters to certain types of traffic subject to the accounting service.

When the CSG2 matches policies, it selects the policy that appears first in the policy list. Policies are located in the policy list in the sequence in which they were configured in the content. You can reorder the policies in the list by removing policies and reentering them in the order that you prefer.

To configure accounting records policies, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`csg2(config)# ip csg policy` *policy-name*	Defines a policy for qualifying flows for CSG2 billing services, and enters CSG2 policy configuration mode. Because of limitations on the number of URL match patterns that the CSG2 can handle, do not define more than 16,000 policies.
Step 2	`csg2(config-csg-policy)# accounting [customer-string` *string*`]`	Specifies accounting and an optional customer string for a CSG2 policy. This command is required if the CSG2 is to generate CDRs for content that matches the CSG2 policy. For FTP and RTSP accounting, the CSG2 matches prepaid services on the basis of the IP address and port number of the control connection to the FTP or RTSP server IP address.
Step 3	`csg2(config-csg-policy)# map` *map-name*	References a header, method, or URL map that is part of a CSG2 billing policy. The conditions specified in the referenced header, method, or URL map must be true in order for the flows to be processed by the CSG2 accounting services. If the conditions are not true, the flows are not processed.

Configuring a Content Billing Service

A CSG2 content billing service is a component of a billing plan to which subscribers subscribe.

For information on configuring one or more content billing services for the CSG2, see the "Configuring Service Support" section on page 5-1.

Configuring Content

The CSG2 uses the Cisco command-line interface (CLI), and requires content configurations or virtual server configurations. This section provides information about configuring content.

A CSG2 content configuration contains the following information:

- Layer 3 information that specifies the IP-level details of the content.
- Layer 4 information that specifies transport layer parameters, such as TCP and User Datagram Protocol (UDP) port numbers.

In order to determine the service for a subscriber, the CSG2 first matches a content with the first packet in a flow, then matches the policy. The CSG2 then uses the content, policy, and the subscriber's billing plan to determine the service.

If the content configuration does not match any service listed under a subscriber's billing plan, the CSG2 considers the service to be either free or postpaid, and the CSG2 forwards the flow and does not try to authorize the subscriber with the quota server. If BMAs are configured, the CSG2 generates a per-transaction CDR.

The CSG2 supports overlapping contents, as when one content is a subset of another. If one content overlaps another, the CSG2 selects the content that best matches the flow. For example, if you configure Content A with **ip any** and Content B with **ip any tcp 80**, the CSG2 matches TCP port 80 flows to Content B, because **ip any tcp 80** is a more precise match than **ip any**.

The CSG2 does not support duplicate contents. That is, you cannot configure two contents with identical configurations.

To configure content for a CSG2 accounting service, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`csg2(config)# ip csg content` *content-name*	Configures content for CSG2 accounting services, and enters CSG2 content configuration mode.
Step 2	`csg2(config-csg-content)# client-group` {*std-access-list-number* | *std-access-list-name*}	References a standard access list that is part of a CSG2 content.
Step 3	`csg2(config-csg-content)# ip` {**any** | *ip-address* [*netmask*]} [**any** | *protocol* [*port-number* [*last-port-number*]]]	Defines the subset of Layer 3 and Layer 4 flows that can be processed by the CSG2 accounting services. *You can define port-number as a single value or as a range of numbers.*
Step 4	`csg2(config-csg-content)# parse protocol` {**ftp** | **http** | **imap** | **other** | **pop3** | **rtsp** | **sip** | **smtp** | **wap** {**connection-oriented** | **connectionless**}}	Defines how the CSG2 is to parse traffic for a content.
Step 5	`csg2(config-csg-content)# policy` *policy-name* [**priority** *priority-number*]	References a CSG2 billing policy.
Step 6	`csg2(config-csg-content)# mode tcp` {**datagram** | **transparent** [**zero**]}	(Optional) Specifies the mode for CSG2 TCP sessions.

	Command	Purpose
Step 7	`csg2(config-csg-content)# next-hop ip-address [reverse] [subscriber media]`	(Optional) Defines a next-hop IP address. **Note** You can configure one forward next-hop, and one reverse next-hop. Even if you have defined a next-hop IP address, traffic that matches the "default" content might not be routed with next-hop. If you specify the **subscriber media** keywords, this command defines the IP address of the next hop for Session Initiation Protocol (SIP) media sessions (used for subscriber-to-subscriber traffic).
Step 8	`csg2(config-csg-content)# block`	(Optional) Forces the CSG2 to drop packets that do not match a configured billing policy.
Step 9	`csg2(config-csg-content)# idle duration`	(Optional) Specifies the minimum amount of time that the CSG2 maintains an idle content connection.
Step 10	`csg2(config-csg-content)# parse length number`	(Optional) Defines the maximum number of Layer 7 bytes that the CSG2 is to parse when attempting to assign a policy. If the parse length is exceeded, the CSG2 blocks or forwards packets on the basis of the **block** command. This command is valid only if **parse protocol http** is also configured.
Step 11	`csg2(config-csg-content)# pending timeout`	(Optional) Sets the pending connection timeout.
Step 12	`csg2(config-csg-content)# records delay seconds`	(Optional) Specifies the delay before the CSG2 is to send the HTTP Statistics CDR. Specifying a records delay enables CSG2 accounting for retransmitted packets and ACKs after the transaction closes, but before the connection closes.
Step 13	`csg2(config-csg-content)# records intermediate {bytes bytes | seconds seconds | bytes bytes seconds seconds}`	(Optional) Enables the generation of intermediate CDRs. If you do not specify the **records intermediate** command, or if you specify the **records intermediate** command for a content for a protocol handler that does not support intermediate statistics, the CSG2 does not generate intermediate CDRs.
Step 14	`csg2(config-csg-content)# replicate [delay seconds]`	(Optional) Replicates the connection state for all TCP connections to the CSG2 content servers on the standby system. Replication is not supported for RTSP or WAP 1.x. For HTTP, the replicated session is treated as Layer 4. No HTTP parsing is performed when the replicated session on the standby CSG2 becomes active.

	Command	Purpose
Step 15	`csg2(config-csg-content)# subscriber-ip http-header x-forwarded-for [obscure]`	(Optional) Specifies that the CSG2 is to obtain the subscriber's IP address from the HTTP X-Forwarded-For header. Single-TP mode is required for HTTP X-Forwarded-For operation. Before configuring the CSG2 for X-Forwarded-For operation, configure the CSG2 for single-TP mode by entering the **ip csg mode single-tp** command, then performing a **write memory**, then restarting the CSG2. If your configuration is fault-tolerant, and you want to obscure the contents of X-Forwarded-For headers, do not configure the **replicate connection tcp** command in CSG2 content configuration mode.
Step 16	`csg2(config-csg-content)# vlan vlan-number`	(Optional) Restricts CSG2 billing content to a single source VLAN. The VLAN number is dependent on the CSG2 card that receives the content. When the content is downloaded to a CSG2 card, the *vlan-number* argument is mapped to a specific VLAN number.
Step 17	`csg2(config-csg-content)# vrf vrf-name`	(Optional) Restricts the CSG2 content to packets within a single Virtual Routing and Forwarding (VRF) table. **Note** The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters. The CSG2 does not support the use of the word **forwarding** as a valid VRF name.
Step 18	`csg2(config-csg-content)# inservice`	Activates the content service on each CSG2. **Note** If there are sessions on a content, and you take the content out of service (with the **no inservice** command), the CSG2 does not allow the content to be placed back in service (with the **inservice** command) until the sessions have been cleaned up. If you try to enter the **inservice** command before the CSG2 has cleaned up the sessions, the command fails.

Configuring Single-TP Mode

In normal multiple-TP mode, the CSG2 distributes subscriber traffic among all of the TPs, based on each subscriber's IP address. In single-TP mode, the CSG2 dispatches traffic for all subscribers to the first TP to be processed.

Single-TP mode is required for HTTP X-Forwarded-For operation. Before configuring the CSG2 for X-Forwarded-For operation, configure the CSG2 for single-TP mode, then perform a **write memory**, then restart the CSG2.

To enable the CSG2 to use a single TP instead of multiple TPs, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg mode single-tp`	Enables the CSG2 to use a single TP instead of multiple TPs. If you intend to operate in single-TP mode, the **ip csg mode single-tp** command must be the first command in your CSG2 configuration.

Configuring Fixed, Variable, or Combined Format CDR Support

The CSG2 supports both fixed and variable format CDR generation. The CSG2 also supports combined (variable-single) format CDR generation for HTTP and WAP traffic.

The same variables are reported in each CDR regardless of Wireless Session Protocol (WSP) Protocol Data Unit (PDU) type. CDRs contain zero-length variables when there is no information to report, but the same set of variables are always reported in the same sequence.

Fixed record format generates CDRs that always contain the same set of Tag-Length-Values (TLVs). Some might have a length of zero. This format is primarily used for integration with legacy billing systems.

This section contains the following information:

- Fixed CDR Support for HTTP and WAP, page 2-17
- Fixed CDR Support for IMAP, page 2-18
- Fixed CDR Support for RTSP, page 2-18
- Single CDR Support for HTTP and WAP, page 2-18
- Specifying the CDR Format, page 2-18

Fixed CDR Support for HTTP and WAP

The CSG2 provides fixed CDR support for HTTP and WAP. This support generates one fixed CDR for every HTTP transaction, instead of two CDRs, which are typically generated at the beginning and end of the transaction.

The single CDR contains all the fields that are included in the HTTP header and HTTP statistics records, in a fixed format. In addition, the same fixed-format service TLVs that were included for WAP are also included for HTTP.

The single CDR also includes RADIUS TLVs, in ascending order, based on the RADIUS TLVs configured using the **ip csg report radius attribute** command in CSG2 global configuration mode. This scheme is very flexible, enabling you to add RADIUS attributes dynamically. This function applies to both WAP and HTTP fixed CDRs. For more information, see the "Reporting RADIUS Attributes and VSA Subattributes" section on page 9-9.

Fixed CDR support does not support RADIUS attribute 26 (the vendor-specific attribute, or VSA), because the list of attributes defined within the VSA is variable. Therefore, a predefined "fixed" list of attributes cannot be determined when RADIUS attribute 26 is configured.

The CSG2 also supports fixed HTTP intermediate records. The fixed intermediate record format is identical to the format of the fixed record created at the end of the transaction, except for the message type, which is necessary to differentiate the two records. The intermediate statistics, such as TCP byte counts, are per intermediate period, and are not cumulative. This differs from the existing HTTP intermediate support for variable format CDRs, in which the TCP byte counts are cumulative.

The Content Delivered TLV contains a value of 0x00 (not delivered) if the HTTP response code is greater than or equal to 400, or if the TCP byte download count is less than 12 bytes.

Fixed CDR Support for IMAP

The CSG2 provides fixed CDR support for the Internet Message Access Protocol (IMAP).

When configuring CSG2 support for IMAP, keep in mind that the CSG2 cannot examine IMAP flows sent over an encrypted tunnel, such as Secure Socket Layer (SSL) or Transport Layer Security (TLS). When an encrypted tunnel is used for IMAP traffic, the CSG2 records only IP and TCP upstream and downstream byte counts. No other counts are provided.

Fixed CDR Support for RTSP

This feature enables the CSG2 to send the existing RTSP stream CDRs in a fixed format. The same fixed-format service TLVs that were included for WAP are also included for RTSP.

Single CDR Support for HTTP and WAP

For HTTP and WAP, the CSG2 reduces the multiple CDRs generated to a single CDR, which is reported at the end of the transaction. This feature is supported for both WAP connectionless and WAP connection-oriented traffic, as well as for HTTP traffic.

The single CDR contains the standard variable format, and it also includes a comprehensive list of TLVs containing all pertinent information for the transaction. For WAP connectionless transactions, it includes everything that is included in a WAP GET and REPLY CDR. For HTTP transactions, it includes everything in the HTTP header and HTTP statistics records.

When you configure single CDR support, the CSG2 suppresses HTTP intermediate record generation.

Specifying the CDR Format

To specify the CDR format to be used by the CSG2, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg records format [fixed | variable [combined {http | wap}]]`	Specifies variable, fixed, or combined (variable-single) CDR format.

Configuring a Refund Policy on the CSG2

The prepaid error reimbursement feature allows the CSG2 to automatically refund quota for failed transactions, as defined by the CLI. The CSG2 checks them in the following order: TCP/WAP flags, Application Return Code. The CSG2 supports flag-based refunding for all protocols. The CSG2 supports return code-based refunding for all protocols except RTSP.

To configure a refund policy on the CSG2, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`csg2(config)# ip csg refund`	(Optional) Specifies a refund policy to apply to the various services, and enters CSG2 refund configuration mode.
Step 2	`csg2(config-csg-refund)# retcode {ftp | http | imap | pop3 | sip | smtp | wap} rc-start [rc-end]`	(Optional) Specifies the range of application return codes for which the CSG2 refunds quota for Prepaid Error Reimbursement. The return codes are protocol-specific.
Step 3	`csg2(config-csg-refund)# flags {ip mask| tcp mask| wap} value`	(Optional) Specifies IP, TCP, or wireless application protocol (WAP) flag bit masks and values for CSG2 Prepaid Error Reimbursement.

For information about enabling a refund policy for a service, see the "Enabling a Refund Policy for a Service" section on page 5-19.

Configuring HTTP Header Reporting

The CSG2 allows you to include multiple HTTP request headers in the CSG2 HTTP_Header CDR.

To define HTTP reporting on the CSG2, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg report http header x-header`	(Optional) Defines the inclusion of multiple HTTP request headers in the CSG2 HTTP_Header CDR.

Configuring SMTP CDR Header Removal

An SMTP CDR can be very large, as it includes a report attribute for each SMTP header embedded at the beginning of a message. The CSG2 enables you to eliminate these headers from an SMTP CDR, leaving only the SMTP envelope headers and the size attribute in the report. These are reported as X-CSG-MAIL, X-CSG-RCPT and X-CSG-SIZE.

You can enable the CSG2 to remove SMTP CDR headers. When SMTP CDR header removal is enabled, the CSG2 reports the following header information to the BMA:

- X-CSG-MAIL
- X-CSG-RCPT
- X-CSG-SIZE

When SMTP CDR header removal is disabled, the CSG2 reports the following header information to the BMA:

- X-CSG-MAIL
- X-CSG-RCPT
- X-CSG-SIZE

- X-Priority[1]
- X-MSMail-Priority[1]
- X-Mailer[1]
- X-MimeOLE[1]

To disable SMTP CDR header removal, including RFC 2822 header TLVs in SMTP CDRs, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg report smtp rfc2822`	(Optional) Specifies that the CSG2 is to include RFC 2822 header TLVs in SMTP CDRs. To enable SMTP CDR header removal, use the **no** form of this command.e

Configuring Supplemental Usage Reporting

You can configure the CSG2 to report supplemental usage to the quota server when sending a Service Stop, Quota Return, or Service Reauthorization Request message. The supplemental usage data reports the uploaded bytes, downloaded bytes, usage time in seconds, and time stamps for the first and last billable sessions. Reports contain statistics since the last report. The supplemental usage is included in the Service Stop Notification (0x0011) and in the Quota Return Notification (0x0009).

If a tariff switch timeout occurs during the interval, the CSG2 sends the tariff switch TLVs along with the supplemental usage TLVs. The supplemental usage TLVs cover the data from the tariff switch time to the end of the interval.

Supplemental usage reporting always reports IP bytes, even if the billing basis is configured for TCP bytes.

To enable supplemental usage reporting on the CSG2, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg report usage {bytes ip | seconds}`	(Optional) Enables CSG2 supplemental usage reporting to the quota server. If you want to report both IP bytes and usage in seconds, you can specify both **ip csg report usage bytes ip** and **ip csg report usage seconds**.

Configuring Actual PDU Reporting for WAP

The CSG2 can report actual protocol data units (PDUs) in wireless application protocol (WAP) CDRs.

To report actual PDUs, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg report wap actual-pdu`	(Optional) Specifies whether actual PDUs are to be reported in CSG2 WAP CDRs.

1. Presence of this header depends on the contents of the SMTP header.

Configuring Maps for Pattern-Matching

The CSG2 maps are used to match URLs or headers against a pattern, to determine whether flows will be processed by the CSG2 accounting services.

To define the CSG2 billing content filters (URL maps and header maps), follow these steps:

	Command	Purpose
Step 1	`csg2(config)# ip csg map map-name`	(Optional) Defines the CSG2 billing content filters (header, method, and URL maps), and enters CSG2 map configuration mode.
Step 2	`csg2(config-csg-map)# match header header-name value`	(Optional) Specifies a header match pattern for a CSG2 billing map.
Step 3	`csg2(config-csg-map)# match method method-name`	(Optional) Specifies a method match pattern for a CSG2 billing map.
Step 4	`csg2(config-csg-map)# match url pattern`	(Optional) Specifies a URL match pattern for a CSG2 billing map.

Note For WAP, the CSG2 supports only URL maps. Header maps and method maps are not supported.

For more information, including how to specify match patterns and how the CSG2 matches those patterns, see the descriptions of the **map**, **match header**, **match method**, and **match url** commands.

Configuring Connection Redundancy

Connection redundancy prevents open connections from becoming unresponsive when the active CSG2 fails and the standby CSG2 becomes active. With connection redundancy, the active CSG2 replicates forwarding information to the standby CSG2 for each connection that is to remain open when the active CSG2 fails over to the standby CSG2.

To enable connection redundancy, enter the **replicate** command in CSG2 content configuration mode.

Configuring High Availability

The CSG1 fault-tolerant feature has been replaced with the CSG2 high availability (HA) feature.

The HA component of the CSG2 provides both stateless and stateful redundancy.

- Stateless HA coordinates traffic delivery to the active system via the redundancy facility (RF) and Hot Standby Routing Protocol (HSRP), through the RF for Interdevice redundancy (RF Interdev).
- Stateful HA provides a state messaging conduit for other CSG2 software components by providing a state encapsulation and delivery service.

For high availability (HA), keep the following consideration in mind:

- When CSG2s are firewall load-balanced, you must configure the **standby use-bia** command in interface configuration mode. Doing so ensures that the MAC address of the active CSG2 device changes (from the firewall load-balancing device's perspective) when a switchover occurs.
- HA does not support the use of the **standby preempt** command in interface configuration mode.

- When an active CSG2 fails over to a standby CSG2, the standby CSG2 sets its initial TCP sequence number based on the first packet it receives on the TCP session. The former standby CSG2—now the active CSG2— counts only the IP bytes for TCP packets, with the sequence number inside the initial sequence number plus 64 KB. This is true for packets from the subscriber and for packets from the network.

This section contains the following information:

- Components That Provide HA, page 2-22
- Enabling HA, page 2-23
- Configuring a Secondary IP Address for HA, page 2-23
- Synchronizing Clocks for HA, page 2-24
- Modifying an HA Configuration, page 2-24
- Distributed Crash Data Collection, page 2-25
- Configuring HA for CSG2s in Different Chassis, page 2-25

Components That Provide HA

Table 2-1 lists the components that interact to provide CSG2 HA.

Table 2-1 Components That Provide HA

Component	Description
Redundancy Facility (RF)	IOS redundancy facility used to coordinate active and standby HA systems and their state progressions.
RF for Interdevice redundancy (RF Interdev)	Software layer that listens for HSRP updates regarding the status of a named HSRP group, and drives the RF state machines with updates when HSRP moves through key state transitions.
Hot Standby Routing Protocol (HSRP)	Layer 3 virtualization protocol that presents adjacent devices with a virtual IP and a virtual MAC address, with the active role coordinated between the devices via priorities and elections.
Stream Control Transmission Protocol (SCTP)	Reliable communications protocol used by RF Interdev for messaging between systems.
CSG2 Internet Exchange Point (IXP)	Classifies ingress packets for delivery to the correct SAMI processor, and directs CSG2 HA stateful messages to the six TPs based on the destination port of the inbound messages.
CSG2 Demultiplexor	Classifies incoming packets, invokes a protocol handler based on classification, and delivers CSG2 HA UDP packets, arriving for local replication of the IP address and port, to the HA packet handler routine for processing.
CSG2 HA—RF Interface	RF client that listens for state transition signals and instructions to bulk_sync (dump the CSG2 state table to the remote system).
CSG2 HA—Messaging	Handles the dump process on the CSG2 and maps incoming messages to the correct receiver routine in other CSG2 HA-aware components.
CSG2 HA—HA-Aware Components	CSG2 software that sends or receives HA messages through the CSG2 HA component.

Enabling HA

The CSG2 uses two separate commands to enable replication. Using separate commands allows for the synchronization of subscriber and quota states independent of per-flow synchronization.

To enable replication of session and flows, use the **replicate** command in CSG2 content configuration mode. For more information, see the "Configuring Content" section on page 2-14

To enable HA state replication between redundant CSG2 systems, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg replicate [vrf vrf-name] local-ip remote-ip base-port`	(Optional) Enables HA state replication between redundant CSG2 systems. **Note** The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters. The CSG2 does not support the use of the word **forwarding** as a valid VRF name.

Configuring a Secondary IP Address for HA

In some configurations, you might want the CSG2 to answer ARPs for CSG2 RADIUS endpoint and proxy IP addresses. To achieve this behavior, you must configure a secondary IP address on the appropriate interface, to facilitate the Layer 2 presence of the IP address on connected VLAN segments.

- In redundant configurations, you must configure the secondary IP address as a standby secondary IP address in interface configuration mode.

  For example, any configuration that uses RADIUS load balancing to distribute traffic across multiple CSG2s, with the CSG2s acting as redundant devices, must use this approach. Note that the RADIUS load balancing real servers must be Layer 2-adjacent to the RADIUS load-balancing device.

```
interface GigabitEthernet0/0.107
 encapsulation dot1Q 107
 ip address 10.10.107.22 255.255.255.0
 standby 0 ip 10.10.107.111
 standby 0 ip 10.10.107.112 secondary
!
ip csg radius endpoint 10.10.107.112 key cisco
```

- In non-redundant configurations, you must configure the secondary IP address as a secondary IP address in interface configuration mode.

```
interface GigabitEthernet0/0.107
 encapsulation dot1Q 107
 ip address 10.10.107.22 255.255.255.0
 ip address 10.10.107.22 255.255.255.0 secondary
!
ip csg radius endpoint 10.10.107.112 key cisco
```

Synchronizing Clocks for HA

HA requires the clocks in your active and standby CSG2s to be synchronized with the clocks in any associated Supervisor Engines, to ensure correct billing. If your active and standby CSG2s are not installed in the same Cisco 7600 series router chassis, you must also synchronize the clocks in the associated Supervisor Engines with each other.

- To synchronize the CSG2 clocks, configure the Cisco Network Time Protocol (NTP) on each SAMI, as described in the "Configuring NTP" procedure in the *Service and Application Module for IP User Guide*.
- To determine whether the clocks are synchronized, enter the **show clock** command on each active Supervisor Engine and on each SAMI, and ensure that the timestamps are identical.
- To display the clock timestamps for all of the SAMIs in a given chassis, enter the **execute-on all-samis** command in privileged EXEC mode.

Note The CSG2 reports all times in Coordinated Universal Time (UTC), regardless of the setting of the **clock timezone** or **clock summer-time** command in privileged EXEC mode.

Modifying an HA Configuration

To ensure stability, RF Interdev forces a system reload if an active system transitions to a standby state, or if communication between an active system and a standby system is interrupted. Both of these conditions can occur when you modify the **ipc zone default** or **standby** configurations for a CSG2 HA configuration.

To avoid forced reloads, use the following procedure when modifying any aspect of a CSG2 HA configuration (such as **ipc**, **standby**, or **replicate**).

Step 1 Remove the standby scheme configured in inter-device configuration mode:

```
csg2(config)# redundancy inter-device
csg2(config-red-interdevice)# no scheme standby SB
```

Step 2 Save the configuration changes to memory:

```
csg2(config)# write memory
```

Step 3 Reload the CSG2:

```
Router# reload
```

Step 4 Modify the CSG2 configuration.

Step 5 Reconfigure the standby scheme configured in inter-device configuration mode, if necessary.

Step 6 Save the configuration changes to memory again:

```
csg2(config)# write memory
```

Step 7 Reload the CSG2 again:

```
Router# reload
```

Distributed Crash Data Collection

The CSG2 uses a control processor (CP) and multiple traffic processors (TPs), operating in parallel. If one of the processors fails, it can be useful to have crash data from all of the processors, not just the failed one. To that end, distributed crash data collection enables the CP and each TP to generate the following crash data:

- Crash information from the failed processor
- Debugging information from all of the non-failed processors

The processors use the following format when creating the crash and debugging information files:

designator_processornumber_timestamp

where:

- *designator* indicates whether the file contains crash information (**crashinfo**) or debugging information (**debuginfo**)
- *processornumber* is the CP or TP number
- *timestamp* is the date and time when the file was created

For example, **crashinfo_proc4_20080603-171440** is a crash information file for TP 4 that was created on June 3, 2008, at 5:14:40PM.

The CSG2's Line Card Processor (LCP) collects each TP's crash and debugging information files and combines the files into a single .tar file, stored on the LCP in the **core:** file system:

lcp# **dir core:**

1048576 Jul 11 16:18:40 2008 crashinfo
1075200 May 3 00:19:05 2008
crashinfo_collection-20080503-001844.tar

You can read the .tar file from the Supervisor Engine. For example, for slot 2:

cat# **dir sami#2-fs:core/**

Directory of sami#2-fs:core/
12 ---- 1048576 Jul 11 2008 16:18:40 +00:00 crashinfo
22 ---- 1075200 May 3 2008 00:19:05 +00:00 crashinfo_collection-20080503-001844.tar

There are no commands required to enable distributed crash data collection.

Note Do not configure the **exception crashinfo file** command in global configuration mode. Doing so can break the file-naming convention and corrupt the crash and debugging information files.

Configuring HA for CSG2s in Different Chassis

If the CSG2s are in different chassis, we recommend that you configure the Supervisor Engines as peers of each other, in addition to configuring them as clients of the same NTP servers. This peer configuration ensures that, if one of the Supervisor Engines loses connectivity to its servers, it can obtain time synchronization information for the peer Supervisor Engine.

Classifying Data Traffic

The CSG2 enables you to classify data traffic on the basis of its access path, using the Network Access Server (NAS) IP address reported in the RADIUS Accounting Start message. Transport-type information is reported in fixed record format CDRs.

To classify data traffic on the basis of its access path, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg transport-type assign` *ip-address value*	(Optional) Classifies data traffic on the basis of its access path.

Configuring a CSG2 Subscriber Interface

To configure a subscriber interface as a CSG2 subscriber interface, enter the following command in interface configuration mode:

Command	Purpose
`Router# ip csg subscriber`	Defines a subscriber interface as a CSG2 subscriber interface. **Note** All traffic routed through the CSG2, including peer-to-peer traffic, must flow from a subscriber interface to a network interface, or from a network interface to a subscriber interface. Therefore, configure the **ip csg subscriber** command on only the subscriber interface, never on the network interface.

Configuring Case Sensitivity

By default, CSG2 header, method, and URL match patterns are case-sensitive.

To explicitly configure the CSG2 to treat match patterns as case-sensitive, enter the following command in global configuration mode:

Command	Purpose
`Router# ip csg case-sensitive`	(Optional) Specifies whether the CSG2 is to treat header, method, and URL match patterns as case-sensitive.

To disable case-sensitivity for CSG2 match patterns, enter the following command in global configuration mode:

Command	Purpose
`Router# no ip csg case-sensitive`	(Optional) Specifies that the CSG2 is to treat header, method, and URL match patterns as not case-sensitive.

Configuring WAP and WSP Support

The CSG2 can intercept wireless application protocol (WAP) traffic and generate reports that include contextual WAP information and counts of the bytes transferred. This feature supports both prepaid and postpaid billing. This section provides the following information:

- Counting Bytes and Packets, page 2-27
- Incomplete WAP Transactions, page 2-27
- Multimedia Messaging Service, page 2-27

Counting Bytes and Packets

The CSG2 reports WAP datagram sizes (including IP and UDP headers), the number of IP packets per transaction, and PDU counts. (The PDU count is not the same as the packet count. Multiple WAP PDUs can share a single packet.) Bytes for retransmitted WAP PDUs and segments are counted and listed separately from non-retransmitted counts in the billing reports. Byte and PDU counts are further specified by source. Reports include the number of bytes and PDUs uploaded from source to destination and the number of bytes downloaded from destination to source.

Incomplete WAP Transactions

When the internal session representing a WAP flow for the CSG2 expires (because of inactivity or receipt of a WAP DISCONNECT packet), any outstanding elements in the WAP transaction queue are reported. These outstanding elements are transactions that were not completed. Examples include a GET request for which a full REPLY was not received, and a segmented POST or PUSH that was incomplete (missing a segment). In such cases, the incomplete flag is set on the Wireless Transaction Protocol (WTP) Info Tag-Length-Value (TLV) in the WAP statistics record. The record reports the Wireless Session Protocol (WSP) PDU type, WTP transaction class, WTP transaction ID, and the number of IP bytes transferred during the attempted transaction.

Multimedia Messaging Service

The CSG2 differentiates Multimedia Messaging Service (MMS) traffic running over WAP from other WAP traffic by inspecting the Wireless Session Protocol (WSP) Content Type. If MMS prepaid charging is disabled, all MMS traffic flows even when non-MMS, WAP traffic is blocked because of insufficient quota. Postpaid reports for MMS are generated as for all WAP traffic.

Typically, several WAP packets are exchanged during a transaction before the WSP Content Type can be identified. When prepaid WAP with free MMS is configured, some packets still flow (even if a subscriber has insufficient quota) in order to identify the WSP Content Type. But the transaction does not complete, and the subscriber does not receive content if he or she has insufficient quota for a non-MMS, WAP request.

It is not always possible to determine the WSP Content Type for incomplete transactions. In these instances, no quota is deducted for prepaid subscribers.

Blocking Ports

RTSP RealPlayer subscribers ignore the explicit definition of port 554 in the URL, and attempt to connect to ports 554, 7070, 80, and 8080. Many other streaming media servers also listen on ports 7070, 80, and 8080. For HTTP transport, if the media streams from any port other than port 554 (such as port 7070, 80, or 8080), the CSG2 does not bill the stream as RTSP. Therefore, for RTSP billing, you must block TCP and HTTP connections to the server network on ports 7070, 80, and 8080.

To block a port, you must configure a content that matches the connection to the server network and sends transactions to a false next-hop IP address, as shown in the following example:

```
ip csg content BLOCK7070
 ip 1.1.1.0 255.255.255.0 tcp 7070
 next-hop 10.10.10.1
 policy RTSP-BLOCK
 inservice
!
ip csg content BLOCK80
 ip 1.1.1.0 255.255.255.0 tcp 80
 next-hop 10.10.10.1
 policy RTSP-BLOCK
 inservice
!
ip csg content BLOCK8080
 ip 1.1.1.0 255.255.255.0 tcp 8080
 next-hop 10.10.10.1
 policy RTSP-BLOCK
 inservice
!
ip csg content RTSPCONTSERVER
 ip 1.1.1.0 255.255.255.0 tcp 554
 idle 50
 replicate
 policy RTSP
 inservice
```

Configuring SNMP Timers

The CSG2 enables you to configure SNMP timers for lost CSG2 records.

To configure an SNMP timer and to enter CSG2 SNMP timer configuration mode, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg snmp timer {bma | psd | quota-server} [interval]`	(Optional) Defines Simple Network Management Protocol (SNMP) timers for lost CSG2 records.

Configuring the SAMI Bit Rate Limit

To specify the bit rate limit to be used by the Service and Application Module for IP (SAMI) for each PowerPC's (PPC's) traffic, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# sami rate bits-per-second all`	(Optional) Specifies the bit rate limit to be used by the SAMI for each PPC's traffic.

Configuring the SNMP Notification Types

To enable Simple Network Management Protocol (SNMP) notification types that are available on the CSG2, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# snmp-server enable traps csg [bma [records | state] | database | quota-server [records | state]]`	(Optional) Enables SNMP notification types that are available on the CSG2.

CSG2 Configuration Examples

This section provides the following sample configurations for CSG2:

- Sample Configuration for Subscriber-to-Subscriber Traffic, page 2-29
- Sample Configuration for HTTP X-Forwarded-For, page 2-31
- Sample Configuration for High Availability, page 2-32
- Sample Configuration for HA Peer Connectivity, page 2-34
- Sample Configuration for IPv4-Aware VRF, page 2-39

Sample Configuration for Subscriber-to-Subscriber Traffic

The CSG2 handles the following scenarios for subscriber-to-subscriber traffic:

- Subscriber-A and Subscriber-B are owned by the same CSG2, which is not a member of a CSG2 cluster.
- Subscriber-A and Subscriber-B are owned by the same CSG2, which is a member of a CSG2 cluster.
- Subscriber-A and Subscriber-B are owned by different CSG2s, both of which are members of a CSG2 cluster.
- Subscriber-A and Subscriber-B are owned by different CSG2s, which are not members of the same CSG2 cluster.

where:

- Subscriber-A is the initiator of the session.
- Subscriber-B refers to the receiver of the session.

- A CSG2 cluster is a group of CSG2s in the same load-balancing group.
- A subscriber is "owned" by a CSG2 if the CSG2 creates a User Table entry that corresponds to the subscriber's IP address.

  If RADIUS endpoint or RADIUS proxy is configured, the CSG2 that "owns" the subscriber is the one that processes RADIUS Accounting Requests for the subscriber.

In each scenario, the CSG2 generates consistent CDRs for both prepaid and postpaid charging:

- The CSG2 charges each subscriber for the transaction, based on the billing plan and service associated with each subscriber. If the subscribers are prepaid, the CSG2 creates a separate service for each subscriber, and the quota server grants quota separately for each service.
- The CSG2 generates two sets of CDRs, one set for each subscriber, in accordance with the billing plan and service associated with each subscriber.

When configuring the CSG2 for subscriber-to-subscriber traffic, keep the following considerations in mind:

- The CSG2 always performs a session lookup for each arriving data packet before matching content.
- Each subscriber-to-subscriber session is flagged with the subscriber IP address and network IP address.
  - For traffic arriving on the subscriber interface, the subscriber IP address is the source IP address and the network IP address is the destination IP address.
  - For traffic arriving on the network interface, the subscriber IP address is the destination IP address and the network IP address is the source IP address.

Configuring Next-Hop for a Subscriber-to-Subscriber Content

On each CSG2 that handles subscriber-to-subscriber traffic, you must configure subscriber-to-subscriber content using the **next-hop** command:

```
ip csg content SUB-TO-SUB
 ip 11.0.0.0 255.0.0.0 any
 next-hop 10.5.1.100
 policy ANY-MS
 vlan 301
 inservice
```

When configuring the **next-hop** configuration, keep the following considerations in mind:

- The **next-hop** configuration applies to traffic that flows in the same direction as the packet that initiates the session.
- In this example, VLAN 301 is a subscriber-side VLAN.
- Configure the IP address of the Supervisor Engine in which the CSG2 is installed as the next-hop IP address for the CSG2, for subscriber-to-subscriber traffic.
- If you are using firewall load balancing, configure an IP address on the Supervisor Engine that is Layer 2-adjacent to the CSG2 as the next-hop IP address.

Configuring Reverse Next-Hop for a Subscriber-to-Subscriber Content

On each CSG2 that handles subscriber-to-subscriber traffic, you must configure reverse subscriber-to-subscriber content using the **next-hop reverse** command:

```
ip csg content REV-SUB-TO-SUB
 ip 11.0.0.0 255.0.0.0 any
```

```
 next-hop 10.5.1.100 reverse
 policy ANY-MS
 vlan 501
 inservice
```

When configuring the **next-hop** configuration, keep the following considerations in mind:

- The **next-hop reverse** configuration applies to traffic that flows in the opposite direction of the packet that initiates the session. For example, if the session is initiated by a packet arriving in the network-to-subscriber direction, the **next-hop reverse** configuration applies to packets received on a subscriber interface.
- In this example, VLAN 501 is a network-side VLAN.
- Configure the IP address of the Supervisor Engine in which the CSG2 is installed as the next-hop reverse IP address for the CSG2, for subscriber-to-subscriber traffic.
- If you are using firewall load balancing, configure an IP address on the Supervisor Engine that is Layer 2-adjacent to the CSG2 as the next-hop reverse IP address.
- We recommend that you configure the **next-hop reverse** command for any contents that handle sessions that are initiated in the server-to-client direction, including subscriber-to-subscriber sessions, peer-to-peer sessions, and network-to-mobile or application-to-mobile sessions.

Configuring Prepaid Subscriber-to-Subscriber Contents for a Service

On each CSG2 that handles prepaid subscriber-to-subscriber traffic, you must configure a service that includes subscriber-to-subscriber contents:

```
ip csg service SUB-TO-SUB
 content REV-SUB-TO-SUB policy ANY-MS
 content SUB-TO-SUB policy ANY-MS
```

Sample Configuration for HTTP X-Forwarded-For

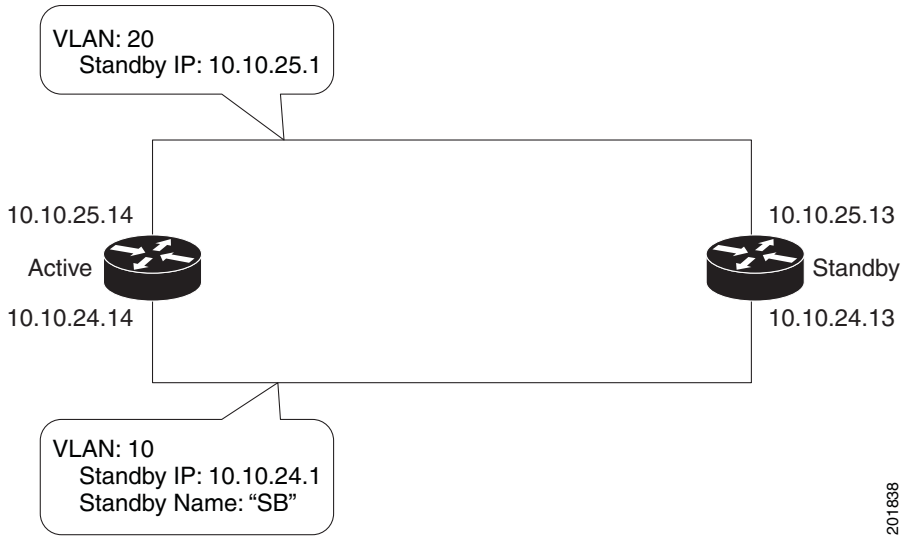
The following example shows how to configure the CSG2 to obtain the subscriber's IP address from the HTTP X-Forwarded-For header, including the configuration of single-TP mode:

```
ip csg mode single-tp

ip csg map WEB
 match url *.(htm|asp|php)

ip csg policy CATCHALL
 accounting

ip csg policy WEB
 accounting
 map WEB

ip csg content XF4
 ip any tcp 80
 subscriber-ip http x-forwarded-for
 policy WEB
 inservice
```

Sample Configuration for High Availability

The following example shows how to configure the CSG2 for High Availability (HA).

Figure 2-1 Configuring the CSG2 for High Availability



HA Configuration on the Active CSG2

```
redundancy inter-device
 scheme standby SB
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 30001
    local-ip 10.10.24.14
   remote-port 30001
    remote-ip 10.10.24.13
!
interface gig 0/0
!
interface gig 0/0.10
 ip csg subscriber
 encaps dot1q 10   vlan 10
 ip address 10.10.24.14 255.255.255.0
 standby use-bia
 standby 5 ip 10.10.24.1
 standby 5 ip 10.10.24.100 secondary
 standby 5 name SB
!
interface gig 0/0.20
 encaps dot1q 20 vlan 20
 ip address 10.10.25.14 255.255.255.0
 standby use-bia
 standby 5 ip 10.10.25.1
 standby 5 follow SB
!
ip csg replicate 10.10.24.14 10.10.14.13 2000
ip csg radius endpoint 10.10.24.100 key cisco
```

HA Configuration on the Standby CSG2

```
redundancy inter-device
 scheme standby SB
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 30001
    local-ip 10.10.24.13
   remote-port 30001
    remote-ip 10.10.24.14
!
interface gig 0/0
!
interface gig 0/0.10
 ip csg subscriber
 encaps dot1q 10
 ip address 10.10.24.13 255.255.255.0
 standby use-bia
 standby 5 ip 10.10.24.1
 standby 5 ip 10.10.24.100 secondary
 standby 5 priority 95
 standby 5 name SB
!

interface gig 0/0.20
 encaps dot1q 20
 ip address 10.10.25.13 255.255.255.0
 standby use-bia
 standby 5 ip 10.10.25.1
 standby 5 priority 95
 standby 5 follow SB
!
ip csg replicate 10.10.24.13 10.10.24.14 2000
ip csg radius endpoint 10.10.24.100 key Cisco
```

Sample Configuration for HA Peer Connectivity

When configuring the CSG2 for HA peer connectivity, keep the following considerations in mind:

- The VLAN used by the CSG2 for HA must be used only for CSG2 HA, and nothing else.
- Each CSG2 in the chassis requires at least a Gigabit of bandwidth for HA operations; we strongly recommend two Gigabits of bandwidth for redundancy. If both the active CSG2 and the standby CSG2 are in the same chassis, then the chassis itself provides the redundancy. However, your CSG2s are then susceptible to the Supervisor Engine or the chassis itself becoming a single point of failure.
- The HA VLAN must be physically redundant, such as a port-channel using at least two different physical ports on at least two different line cards. The port-channel must be able to experience the complete loss of any physical component (card, port, or cable) and still provide sufficient bandwidth for HA. This bandwidth must be reserved for HA via a physical separation or via QoS separation from any other traffic (including CSG2 bearer traffic).

This section includes the following information”

- Sample Configuration for Supervisor Engine Side 1, page 2-34
- Sample Configuration for CSG2 Side 1, page 2-35
- Sample Configuration for Supervisor Engine Side 2, page 2-35
- Sample Configuration for CSG2 Side 2, page 2-35
- Displaying Port-Channel Information for One Side, page 2-36
- Configuring CSG2 Network/Subscriber Traffic, page 2-38

Sample Configuration for Supervisor Engine Side 1

The pertinent configuration for Supervisor Engine side 1 is as follows:

```
svclc multiple-vlan-interfaces
svclc module 4 vlan-group 4,5
svclc vlan-group 4 10,100,200
svclc vlan-group 5 500
!
interface GigabitEthernet1/47
  description inter-chassis port channel
  switchport
  switchport access vlan 500
  channel-group 1 mode on
!
interface GigabitEthernet1/48
  description inter-chassis port channel
  switchport
  switchport access vlan 500
  channel-group 1 mode on
```

The port-channel interface is created as a result of joining channel-group 1 and can be verified using the following command:

```
csg_sup# show running interfaces port-channel 1
Current configuration : 109 bytes
!
interface Port-channel1
  switchport
  switchport access vlan 500
  switchport trunk encapsulation dot1q
end
```

Sample Configuration for CSG2 Side 1

The pertinent configuration for CSG2 side 1 is as follows:

```
redundancy inter-device
  scheme standby SB
!
ipc zone default
  association 1
  no shutdown
  protocol sctp
    local-port 30001
    local-ip 192.168.5.6
    remote-port 30001
    remote-ip 192.168.5.5
!
interface GigabitEthernet0/0.500
  encapsulation dot1Q 500
  ip address 192.168.5.6 255.255.255.0
  standby 0 ip 192.168.5.1
  standby 0 name SB
!
ip csg replicate 192.168.5.6 192.168.5.5 2000
```

Sample Configuration for Supervisor Engine Side 2

The pertinent configuration for Supervisor Engine side 2 is as follows:

```
svclc multiple-vlan-interfaces
svclc module 4 vlan-group 4,5
svclc vlan-group 4 10,100,200
svclc vlan-group 5 500
!
interface GigabitEthernet1/47
  description inter-chassis port channel
  switchport
  switchport access vlan 500
  channel-group 2 mode on
!
interface GigabitEthernet1/48
  description inter-chassis port channel
  switchport
  switchport access vlan 500
  channel-group 2 mode on
```

The port-channel interface is created as a result of joining channel-group 2 and can be verified using the following command:

```
csg_sup# show running interfaces port-channel 2
Current configuration : 109 bytes
!
interface Port-channel2
  switchport
  switchport access vlan 500
  switchport trunk encapsulation dot1q
end
```

Sample Configuration for CSG2 Side 2

The pertinent configuration for CSG2 side 2 is as follows:

```
redundancy inter-device
```

```
  scheme standby SB
!
ipc zone default
  association 1
  no shutdown
  protocol sctp
    local-port 30001
    local-ip 192.168.5.5
    remote-port 30001
    remote-ip 192.168.5.6
!
interface GigabitEthernet0/0.500
  encapsulation dot1Q 500
  ip address 192.168.5.5 255.255.255.0
  standby 0 ip 192.168.5.1
  standby 0 name SB
!
ip csg replicate 192.168.5.5 192.168.5.5 2000
```

Displaying Port-Channel Information for One Side

Use the following commands to display the port-channel information for one side of the configuration:

```
csg_sup# show running interfaces port-channel 2
Building configuration...

Current configuration : 109 bytes
!
interface Port-channel2
  switchport
  switchport access vlan 500
  switchport trunk encapsulation dot1q
end

csg_sup# show interfaces port-channel 2
Port-channel2 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 001f.9ecb.2af6 (bia 001f.9ecb.2af6)
  MTU 1500 bytes, BW 2000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s
  input flow-control is off, output flow-control is off
  Members in this channel: Gi1/47 Gi1/48
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 02:31:37
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 2000 bits/sec, 4 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    2448 packets input, 178170 bytes, 0 no buffer
    Received 2425 broadcasts (2376 multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
    0 input packets with dribble condition detected
    117 packets output, 18805 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 pause output
    0 output buffer failures, 0 output buffers swapped out
```

```
csg_sup# show interfaces gigabitEthernet 1/47
GigabitEthernet1/47 is up, line protocol is up (connected)
  Hardware is c7600 1Gb 802.3, address is 001f.9ecb.2af6 (bia 001f.9ecb.2af6)
  Description: inter-chassis port channel
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s
  input flow-control is off, output flow-control is off
  Clock mode is auto
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:43, output hang never
  Last clearing of "show interface" counters 02:32:31
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 2000 bits/sec, 4 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    7878 packets input, 594299 bytes, 0 no buffer
    Received 7798 broadcasts (7701 multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 8 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
    0 input packets with dribble condition detected
    8395 packets output, 640596 bytes, 0 underruns
    0 output errors, 0 collisions, 4 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 pause output
    0 output buffer failures, 0 output buffers swapped out

csg_sup# show interfaces gigabitEthernet 1/48
GigabitEthernet1/48 is up, line protocol is up (connected)
  Hardware is c7600 1Gb 802.3, address is 001f.9ecb.2af7 (bia 001f.9ecb.2af7)
  Description: inter-chassis port channel
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s
  input flow-control is off, output flow-control is off
  Clock mode is auto
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:49, output 00:00:44, output hang never
  Last clearing of "show interface" counters 02:32:54
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    10771 packets input, 832887 bytes, 0 no buffer
    Received 10556 broadcasts (10438 multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 16 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
    0 input packets with dribble condition detected
    12970 packets output, 990962 bytes, 0 underruns
    0 output errors, 0 collisions, 4 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 pause output
    0 output buffer failures, 0 output buffers swapped out
```

Configuring CSG2 Network/Subscriber Traffic

Inter-chassis network and subscriber traffic must have a similar setup, contained within a redundant inter-chassis connection (that is, a port-channel interface as shown above). This traffic, however, can share the bandwidth in the inter-chassis connection with other VLANS using trunks, as it does not need to be isolated as the CSG2 HA VLAN must be. However, you must ensure you have enough inter-chassis bandwidth to accommodate your anticipated maximum load for the shared port-channel.

Sample Configuration for IPv4-Aware VRF

The following configuration provides VRF support in an IPv4/IPv6 environment:

```
vrf definition MS-30
 address-family ipv4
 exit-address-family
!
ip csg radius proxy vrf MS-30 10.20.1.171 10.0.220.112 10.0.220.174 key test vrf MS-30
ip csg radius endpoint vrf MS-30 10.29.2.175 key test vrf MS-30
ip csg radius pod nas vrf MS-30 1700 key test
!
ip csg policy POL-ANY-MS
 accounting
!
ip csg content ANY-MS
 ip any
 vrf MS-30
 policy POL-ANY-MS
 inservice
```

CHAPTER 3

Configuring BMA Support

The CSG2 monitors data flows and generates accounting records that can be used to bill customers at a content level. The CSG2 sends the accounting records to a Billing Mediation Agent (BMA), which formats the records as required by the customer's billing system. At the end of each transaction, a billing record indicating the content accessed and the amount deducted is sent to the BMA, so that it can be logged in the subscriber's bill.

The CSG2 provides the following features for the BMA:

- Configuring the BMA Local Port, page 3-1
- Configuring a BMA, page 3-2
- Configuring the BMA Keepalive Time, page 3-2
- Configuring the BMA GTP' Message Buffer, page 3-3
- Configuring the BMA Retransmit Time, page 3-3
- Configuring the BMA Retry Number, page 3-4
- Configuring the BMA Window Size, page 3-4
- Configuring BMA Load Sharing, page 3-4
- Reporting the Billing Plan ID to the BMA, page 3-5

Configuring the BMA Local Port

The first step when configuring CSG2 support for the BMA is to configure the local port on which the CSG2 is to communicate with the BMA.

To activate one or more BMAs, you must configure a local port, the local port on which the CSG2 is to communicate with the BMA. The local port must be unique with respect to all other configured local ports, such as the quota server local port.

The CSG2 allows you to configure a port number that is not the general packet radio service (GPRS) tunneling protocol (GTP) prime (GTP') default port (3386).

To configure a local port for the BMA, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg bma local-port port-number`	Configures the local port on which the CSG2 communicates with the BMA. The BMA local port number must be different from the PSD local port number and from the quota server local port number (configured with the **ip csg psd local-port** command and the **ip csg quota-server local-port** command, respectively).

Configuring a BMA

You must configure the BMA to which you want the CSG2 to send accounting records. You can configure only one BMA.

Accounting records are sent only to the configured BMA. This provides a measure of security to ensure that records are not sent to unauthorized systems.

When you configure a BMA, make sure that its IP address and port number match on both the active CSG2 and the standby CSG2.

The CSG2 differentiates BMAs on the basis of their IP addresses and port numbers. You can configure multiple BMAs with the same IP address, but the CSG2 does not support nodealive or redirect for multiple BMAs with the same IP address.

If you have enabled interface awareness, you can also associate a VLAN's Virtual Routing and Forwarding (VRF) table name with the BMA.

To configure a BMA, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg bma [vrf vrf-name] ip-address port-number priority`	Configures the BMA to which the CSG2 is to send billing records. **Note** The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters. The CSG2 does not support the use of the word **forwarding** as a valid VRF name.

Configuring the BMA Keepalive Time

By default, the CSG2 sends keepalive messages to the BMA once every 60 seconds. That setting is sufficient in most environments, but the CSG2 also allows you to change the time between keepalive messages, if necessary.

Note We recommend that you change the keepalive time interval only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

To change the keepalive timer for the BMA, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg bma keepalive` *number-of-seconds*	(Optional) Defines the BMA keepalive time interval for the CSG2.

Configuring the BMA GTP' Message Buffer

By default, the CSG2 can buffer up to 10,000 general packet radio service (GPRS) tunneling protocol prime (GTP') messages for all BMAs. That setting is sufficient in most environments, but the CSG2 also allows you to change the BMA GTP' message buffer, if necessary.

Note We recommend that you change the number of GTP' messages that can be buffered only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

To change the maximum number of GTP' messages, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg bma messages` *number*	(Optional) Specifies the maximum number of GTP' messages that the CSG2 can buffer for the BMA.

Configuring the BMA Retransmit Time

By default, the CSG2 retransmits packets to a BMA once every four seconds. That setting is sufficient in most environments, but the CSG2 also allows you to change the time between retransmits, if necessary.

Note We recommend that you change the retransmit time interval only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

To change the BMA retransmit time interval for the CSG2, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg bma retransmit` *number-of-seconds*	(Optional) Defines the BMA retransmit time interval for the CSG2.

Configuring the BMA Retry Number

By default, the CSG2 retries communication with a BMA three times before determining that the link has failed. That setting is sufficient in most environments, but the CSG2 also allows you to change the number of retries, if necessary.

Note We recommend that you change the number of retries allowed only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

To change the maximum number of BMA retries allowed before the CSG2 determines that the link has failed, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg bma retries` *number-of-retries*	(Optional) Defines the maximum number of BMA retries allowed before the CSG2 determines that the link has failed.

Configuring the BMA Window Size

By default, the CSG2 sets the maximum BMA transmit window size to 128 packets, and sets the minimum BMA transmit window size automatically. Those settings are sufficient in most environments, but the CSG2 also allows you to change the maximum and minimum BMA transmit window sizes, if necessary.

Note We recommend that you change the transmit window size only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

To define the BMA transmit window size for the CSG2, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg bma window {max` *window-size* `| min` *window-size* `| min auto}`	(Optional) Defines the BMA transmit window size for the CSG2.

Configuring BMA Load Sharing

The CSG2 allows load sharing among BMAs. This support is useful in environments in which the number of billing records sent by the CSG2 could overwhelm a single BMA. Multiple BMAs can be simultaneously active, and the CSG2 assigns a BMA to each subscriber. All billing records for the subscriber are sent to the same BMA.

If a BMA fails, all subscribers associated with that BMA are distributed among the other active other BMAs.

The CSG2 maintains GTP' sequence numbers for each BMA.

Note Multiple BMAs cannot have the same IP address.

The CSG2 creates a sticky object to ensure that all the billing records for a subscriber are sent to the same BMA. If the user ID is not available (for example, if the internal table is too small to hold all user ID entries, or if the CSG2 cannot access the user ID database), the CSG2 creates a sticky object for the subscriber IP address. In addition to activating multiple BMAs, the CSG2 allows you to specify the time to wait before it deletes inactive sticky objects.

To configure BMA load sharing, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg bma activate [number [sticky seconds]]`	Activates one or more BMAs.

Reporting the Billing Plan ID to the BMA

The CSG2 reports the billing plan identifier in BMA records. The CSG2 also reports the billing plan ID in messages to the quota server.

There are no commands required to enable billing plan ID reporting.

CHAPTER 4

Configuring Quota Server Support

The CSG2 uses quota servers to return billing quota values for subscribers. The quota server interfaces with the billing system balance manager to reserve credit. The quota server then translates the reserved credit for the subscriber into quota based on the business and rating rules for multiple subscriber services on the CSG2.

For each CSG2 content billing service, the CSG2 downloads a separate quota, and deducts from that quota. Quotas are specified in units called *quadrans*. A quadran is a generic unit whose "value" is defined by each quota server. A quadran can represent, for example, a click for a per-click service (for example, an HTTP request), or a byte for a per-volume service. The value of a quadran is transparent to the CSG2; the CSG2 simply requests and downloads quadrans as needed from quota servers.

The CSG2 provides the following features for the quota server:

- Configuring the Quota Server Local Port, page 4-2
- Configuring a Quota Server, page 4-2
- Configuring the Quota Server Keepalive Time, page 4-3
- Configuring the Quota Server GTP' Message Buffer, page 4-3
- Configuring the Quota Server Retransmit Time, page 4-3
- Configuring the Quota Server Retry Number, page 4-4
- Configuring the Quota Server Window Size, page 4-4
- Configuring Quota Server Load Sharing, page 4-5
- Reassigning Subscribers to a New Quota Server, page 4-5
- Quota Push, page 4-5
- Replacing Quota Balance, page 4-6
- Delaying Quota Reauthorization, page 4-6
- Asynchronous Quota Return, page 4-7
- Reporting the Billing Plan ID to the Quota Server, page 4-7
- Pricing by Quota Server Configuration Example, page 4-7
- Differentiating Prices Configuration Example, page 4-8
- Reducing the Number of Services Configuration Example, page 4-9

Configuring the Quota Server Local Port

The first step when configuring CSG2 support for the quota server is to configure the local port on which the CSG2 is to communicate with the quota server.

For prepaid billing, you must configure at least one quota server local port, the local port on which the CSG2 is to communicate with quota servers.

To configure a local port for quota servers, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg quota-server local-port` *port-number*	Configures the local port on which the CSG2 communicates with quota servers. The quota server local port number must be different from the BMA local port number and from the PSD local port number (configured with the **ip csg bma local-port** command and the **ip csg psd local-port** command, respectively).

Configuring a Quota Server

For prepaid billing, you must configure at least one quota server.

You can configure up to 10 quota servers. Each quota server must have a unique priority and a unique IP address (or a unique IP address-VRF name combination, if VRF is configured).

When you configure a quota server, make sure that its IP address and port number match on both the active CSG2 and the standby CSG2.

The CSG2 differentiates quota servers on the basis of their IP addresses and port numbers. You can configure multiple quota servers with the same IP address, but the CSG2 does not support nodealive or redirect for multiple quota servers with the same IP address.

If you have enabled interface awareness, you can also associate a VLAN's Virtual Routing and Forwarding (VRF) table name with the quota server.

To configure a quota server, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg quota-server` [**vrf** *vrf-name*] *ip-address port-number priority*	Configures the CSG2 quota servers that return billing quota values for subscribers. **Note** The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters. The CSG2 does not support the use of the word **forwarding** as a valid VRF name.

Configuring the Quota Server Keepalive Time

By default, the CSG2 sends keepalive messages to the quota servers once every 60 seconds. That setting is sufficient in most environments, but the CSG2 also allows you to change the time between keepalive messages, if necessary.

Note We recommend that you change the keepalive time interval only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

To change the keepalive timer for the quota servers, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg quota-server keepalive` *number-of-seconds*	(Optional) Defines the quota server keepalive time interval for the CSG2.

Configuring the Quota Server GTP' Message Buffer

By default, the CSG2 can buffer up to 10,000 general packet radio service (GPRS) tunneling protocol prime (GTP') messages for the quota servers. That setting is sufficient in most environments, but the CSG2 also allows you to change the quota server GTP' message buffer, if necessary.

Note We recommend that you change the number of GTP' messages that can be buffered only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

To change the maximum number of GTP' messages, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg quota-server messages` *number*	(Optional) Specifies the maximum number of GTP' messages that the CSG2 can buffer for all quota servers.

Configuring the Quota Server Retransmit Time

By default, the CSG2 retransmits packets to a quota server once every four seconds. That setting is sufficient in most environments, but the CSG2 also allows you to change the time between retransmits, if necessary.

Note We recommend that you change the retransmit time interval only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

To change the quota server retransmit time interval for the CSG2, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg quota-server retransmit` *number-of-seconds*	(Optional) Defines the quota server retransmit time interval for the CSG2.

Configuring the Quota Server Retry Number

By default, the CSG2 retries communication with a quota server three times before determining that the link has failed. That setting is sufficient in most environments, but the CSG2 also allows you to change the number of retries, if necessary.

Note We recommend that you change the number of retries allowed only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

To change the maximum number of quota server retries allowed before the CSG2 determines that the link has failed, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg quota-server retries` *number-of-retries*	(Optional) Defines the maximum number of quota server retries allowed before the CSG2 determines that the link has failed.

Configuring the Quota Server Window Size

By default, the CSG2 sets the maximum quota server transmit window size to 128 packets, and sets the minimum quota server transmit window size automatically. Those settings are sufficient in most environments, but the CSG2 also allows you to change the maximum and minimum quota server transmit window sizes, if necessary.

Note We recommend that you change the transmit window size only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

To define the quota server transmit window size for the CSG2, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg quota-server window` {**max** *window-size* | **min** *window-size* | **min auto**}	(Optional) Defines the quota server transmit window size for the CSG2.

Configuring Quota Server Load Sharing

The CSG2 allows load sharing among quota servers. This support is useful in environments in which the number of quota transactions sent by the CSG2 could overwhelm a single quota server. Multiple quota servers can be simultaneously active, and the CSG2 assigns a quota server to each subscriber. All quota transactions for the subscriber are handled by the same quota server.

If a quota server fails, all subscribers associated with that quota server are distributed among the other active other quota servers.

Note Multiple quota servers cannot have the same IP address.

The CSG2 creates a sticky object to ensure that all the quota transactions for a subscriber are sent to the same quota server. If the user ID is not available (for example, if the internal table is too small to hold all user ID entries, or if the CSG2 cannot access the user ID database), the CSG2 creates a sticky object for the subscriber IP address. In addition to activating multiple quota servers, the CSG2 allows you to specify the time to wait before it deletes inactive sticky objects.

To configure quota server load sharing, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg quota-server activate number`	Activates one or more quota servers.

Reassigning Subscribers to a New Quota Server

If a quota server fails, you can reassign the subscribers to a different quota server.

To reassign subscribers to a different quota server, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg quota-server reassign`	(Optional) Reassigns subscribers to a different CSG2 quota server after a failure.

Quota Push

This feature enables operators to “push” quota for a service instance associated with an individual subscriber. This enables quota servers to provide quota for a subscriber or service before traffic from that subscriber or service reaches the CSG2. This eliminates the delay that can occur when quota is obtained through a service authorization request and response. A sophisticated quota server could also use quota push for better control of quota levels during active sessions.

The CSG2 accepts a quota push for a subscriber at any point after the subscriber and billing plan are known to the CSG2 (that is, when a CSG2 User Table element exists for the subscriber). For example, the CSG2 accepts a quota push after receiving an accounting start but does not require an existing service for the subscriber (one is created). The CSG2 does not begin charging against quota until traffic begins

to arrive and a session is created. Zero-quota might be granted so that cause code and authorization actions can be set (for example, for a free service). A quota download message is sent to the BMA in response to receiving a quota push.

The service idle timer starts whenever quota is pushed, in case the expected traffic never arrives.

The CSG2 rejects the Quota Push message if the "Replace current balance" flag is not set in the Granted Quadrans TLV.

There are no commands required to enable quota push.

Replacing Quota Balance

By default, when the CSG2 receives a quota grant from the quota server, the CSG2 adds the granted quota to the current balance for a subscriber's service. Quota balance replacement enables the quota server to instruct the CSG2 to replace the current quota balance with the amount of granted quota for a subscriber's service. If the replacement grant is provided in a Service Authorization Response, the CSG2 subtracts the amount of quota used since the Service Reauthorization Requests from the granted quota before replacing the balance.

There are no commands required to enable quota balance replacement.

Delaying Quota Reauthorization

The CSG2 accepts the Reauthorization Delay TLV, which specifies the number of seconds the CSG2 delays its next reauthorization request to the quota server for the service specified in the message. This TLV also specifies the action the CSG2 is to take for the service between the time the message is received and the next reauthorization:

- Wait—The CSG2 keeps transactions in a pending state during the delay period. In pending state, the CSG2 maintains the transaction state but drops packets.
- Deny—The CSG2 drops new transactions during the delay period. Existing transactions are dropped if quota expires during the delay period. The CSG2 does not maintain the session state; the subscriber must open a new connection after the delay period.

Note For HTTP pipelining, dropping new transactions can also affect existing transactions if they share the same TCP connection.

Quota servers can use delayed quota reauthorization to deny subscribers access to CSG2 categories without having to continually deny authorization requests (that is, for blacklisting services). To do so, the quota server sends a grant of 0 quadrans in a Service Authorization Response, Quota Push Request, or Service Verification Response message, with a long reauthorization delay timer (0xFFFFFFFF), a Deny action, and a cause code of 0x03.

There are no commands required to enable delayed quota reauthorization.

Asynchronous Quota Return

The Asynchronous Quota Return feature allows the quota server to request the CSG2 to return quota for a defined subscriber and service, and to send a Quota Return. The quota reserved for ongoing transactions is recalled from the transactions and included in the quota returned in the Quota Return message.

The Quota Return message can include the following fields: “remaining quota”, “qualified quadrans”, “qualified usage”, “qualified quota remaining”, “reserved quota”, and “pending quota”. For fixed-cost billing, the “reserved quota” field is not included. For time-based billing, neither the “reserved quota” field nor the “pending quota” field is included. The “qualified usage” field identifies quota that is known to have been consumed, and is the only value that is safe to commit to a back-end system.

Because all of the quota is returned, there is no longer any reserved quota to process ongoing pending transactions. Packets received for pending transactions are dropped. However, time-based billing holds back 5 seconds of quota, so transactions can proceed while returning quota for time-based billing.

There are no commands required to enable delayed quota reauthorization.

Reporting the Billing Plan ID to the Quota Server

The CSG2 reports the billing plan identifier in messages to the quota server. The CSG2 also reports the billing plan ID in billing records.

There are no commands required to enable billing plan ID reporting.

Pricing by Quota Server Configuration Example

The following example shows a CSG2 configuration in which the quota server performs all pricing. In this example:

- Assume that Subscriber X has $10.00 in his account.
- There are two types of content:
  - C1—This content is billed per object (for example, URL GET); each object costs $0.01.
  - C2—This content is billed per byte; each kilobyte costs $0.01.
- The quota server controls each object transaction for content C1.
- The quota server controls all the pricing.

```
ip csg content C1
 policy P1
 inservice
!
ip csg content C2
 policy P2
 inservice
!
ip csg service PERCLICK
 basis fixed
 content C1 policy P1
!
ip csg service PERBYTE
 basis byte ip exclude mms
 content C2 policy P2
```

```
!
ip csg billing REGULAR
 service PERCLICK
 service PERBYTE
```

When Subscriber X, with a subscription to billing plan REGULAR, tries to access content that matches C1, the CSG2 tries to download quota for Subscriber X for service PERCLICK.

The quota server borrows money from Subscriber X's $10.00, and returns some quadrans to the CSG2. Each quadran is good for one object download, or one click. If the quota server is configured for the CSG2 to query for each click, it can choose to send just one quadran at a time, so that the CSG2 queries the quota server each time. However, if the quota server is configured to grant $2.00 worth of quadrans to the CSG2 in one shot, it can send 200 quadrans to the CSG2, which the CSG2 keeps using for Subscriber X's access to C1.

When Subscriber X tries to access content that matches C2, the CSG2 makes another request to the quota server to get Subscriber X's quota for C2. C2 is billed per IP byte. The quota server borrows another $5.00 from Subscriber X's account, and sends 500000 quadrans to the CSG2. As Subscriber X continues to access C2, his traffic is metered for volume. For each byte, the CSG2 deducts one quadran.

Differentiating Prices Configuration Example

The following example extends the previous example by adding a content type that is priced differently. In this example:

- Assume that Subscriber X has $10.00 in his account.
- There are three types of content:
  - C1—This content is billed per *.jpg file, where each JPG file costs $0.01.
  - C2—This content is billed per byte, where each kilobyte costs $0.01.
  - C3—This content is billed per *.mp3 file, where each MP3 file costs $0.05.
- The quota server controls each object transaction for content C1.
- The quota server controls all the pricing.

This configuration requires an additional service type, MP3, which allows the quota server to price object downloads (clicks) differently for MP3 files.

```
ip csg content C1
 policy P1
 inservice
!
ip csg content C2
 policy P2
 inservice
!
ip csg content MP3
 policy P1
 inservice
!
ip csg service PERCLICK
 basis fixed
 content C1 policy P1
!
ip csg service PERBYTE
 basis byte ip
 content C2 policy P2
!
```

```
ip csg service MP3
 basis fixed
 content C1 policy P1
!
ip csg billing REGULAR
 service PERCLICK
 service PERBYTE
 service MP3
```

When Subscriber X tries to download an MP3 file (that is, a file that matches content type MP3), the CSG2 requests the MP3 quota for Subscriber X. Each download of an MP3 file costs $0.05, so the quota server borrows $1.00 from Subscriber X's account, and returns 20 quadrans to the CSG2 for service MP3. The CSG2 can use the quadrans for 20 downloads of MP3 files.

Alternatively, the quota server could send just one quadran, which is enough for only one transaction. This would force the CSG2 to ask for quota before each download of an MP3 file.

Reducing the Number of Services Configuration Example

The "Differentiating Prices Configuration Example" section on page 4-8 shows that you can create a new service for one type of content and differentiate its billing from other types of content.

However, with each new service, the subscriber's quota fragments further, and traffic between the CSG2 and the quota server increases.

You can reduce traffic by specifying a symbolic weight on the CSG2. In the following example, each MP3 download ($0.05) costs five times as much as each JPG download ($0.01). By assigning a weight of 5 to MP3 downloads, you can keep both content C1 and content MP3 under service PERCLICK, thereby reducing the overall number of services and reducing the traffic between the CSG2 and the quota server.

```
ip csg content C1
 policy P1
 inservice
!
ip csg content C2
 policy P2
 inservice
!
ip csg content MP3
 policy P1
 inservice
!
ip csg service PERBYTE
 basis byte ip
 content C2 policy P2
!
ip csg service PERCLICK
 basis fixed
 content C1 policy P1
 content MP3 policy P1 weight 5
!
ip csg billing REGULAR
 service PERCLICK
 service PERBYTE
```

When the quota server borrows $1.00 from Subscriber X's account and sends 100 quadrans for service PERCLICK, the CSG2 can use the quadrans for 100 JPG files, or for 20 MP3 files, or for a mix of the two content types.

CHAPTER 5

Configuring Service Support

A CSG2 content billing service is a component of a billing plan to which subscribers subscribe.

You can configure one or more content billing services for the CSG2. Each service represents a group of content that is billed the same way, such as billing per-click (or per-request) or billing per-IP byte, and that shares part of a subscriber's quota. Grouping content into one or more services enables you to separate, for example, a subscriber's prepaid quota for Internet browsing from his quota for e-mails.

For each service, the CSG2 downloads a separate quota, and deducts from that quota. Quotas are specified in units called *quadrans*. A quadran is a generic unit whose "value" is defined by each quota server. A quadran can represent, for example, a click for a per-click service (for example, an HTTP request), or a byte for a per-volume service. The value of a quadran is transparent to the CSG2; the CSG2 simply requests and downloads quadrans as needed from quota servers.

The CSG2 requests an additional quota grant when a subscriber's per-click quota falls below a specified percentage of the last quota grant, or when a subscriber's per-volume quota falls below a specified percentage of the last quota grant or 32 KB, whichever is greater.

For each service that a subscriber tries to access, the CSG2 maintains a separate logical accounting session. When a subscriber's quota is divided among multiple services, the CSG2 requests an additional quota grant for each service individually, based on its usage.

If a subscriber fails authorization for a service, but continues to send new requests for that service, the CSG2 waits a specified time before sending the quota server a reauthorization request for that subscriber. This ensures that the quota server is not inundated with reauthorization requests from unauthorized subscribers.

The CSG2 allows you to define a pool of up to 1024 services. You can authorize each subscriber for any number of services from that pool, but we recommend that the billing system not authorize each subscriber for more than 10 active services. Exceeding this guideline could lead to the following problems:

- The increase in the number of quota authorizations per subscriber can overload both the quota server and the CSG2.
- As the number of services for which a subscriber is actively authorized increases, the subscriber's quota becomes fragmented. Although the CSG2 allows the billing system to recall and redistribute the quota, so that the subscriber is not denied service because of quota fragmentation, the process increases overhead in both the quota server and the CSG2.

The CSG2 supports multiple protocols under a single service definition.

The CSG2 provides the following features for content billing services:

- Configuring a Basic Content Billing Service, page 5-2
- Configuring the Billing Basis for a Service, page 5-2

- Specifying a Service Owner, page 5-3
- Specifying a Service Class, page 5-3
- Configuring a Service Idle Time, page 5-4
- Configuring Advice of Charge, page 5-4
- Configuring Service Verification, page 5-8
- Enabling Service-Level CDR Summarization, page 5-10
- Configuring Passthrough Mode and the Default Quota, page 5-11
- Configuring Metering, page 5-12
- Configuring the Quota Reauthorization Threshold, page 5-18
- Configuring the Quota Reauthorization Timeout, page 5-18
- Enabling a Refund Policy for a Service, page 5-19

Configuring a Basic Content Billing Service

Each content billing service is associated with one or more contents and policies.

Multiple services can include the same content/policy pair, as long as the services are not associated with the same billing plan. They cannot be associated with the same billing plan because then the match of content/policy pair to service would not be unique.

To configure a content billing service, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`csg2(config)# ip csg service service-name`	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.
Step 2	`csg2(config-csg-service)# content content-name policy policy-name [weight weight-name]`	Configures a content and policy as a member of a CSG2 billing service, and optionally assigns a weight to the content.

Configuring the Billing Basis for a Service

The billing basis specifies how billing is to be charged:

- Per-click (fixed-cost) billing is charged at a fixed cost, which is deducted each time the first packet for a transaction hits a content-policy pair (that is, deducted for each request).
- Volume-based billing can be based on either the number of IP bytes or the number of TCP bytes.
- Duration-based billing can be based on either service duration time or connection duration time.

To configure the billing basis for a service, enter the following command in CSG2 service configuration mode:

Command	Purpose
`csg2(config-csg-service)# basis [byte {ip | tcp} | {fixed | second [connect | transaction]}]`	Specifies the billing basis for a CSG2 content billing service. **Note** The **basis** command applies to prepaid and virtual prepaid billing only. It has no impact on postpaid billing. When changing the basis for a service, the content must be taken out of service.

To specify the activation mode for a CSG2 Connection Duration service, enter the following command in CSG2 service configuration mode:

Command	Purpose
`csg2(config-csg-service)# activation [automatic | user-profile]`	Specifies the activation mode for a CSG2 Connection Duration service (that is, a service configured with **basis second connect**). • **automatic**—Activates the Connection Duration service, unless the billing profile indicates that no service is to be activated. • **user-profile**—Activates the Connection Duration service only if the billing profile specifies this service as the connect service. This is the default setting.

Specifying a Service Owner

The CSG2 enables you to specify an identifier or name for a CSG2 service owner to be used with fixed-record format. The owner is responsible for the content associated with the service.

The administrator who configures owner identification is responsible for its accuracy. Correct configuration requires that contents for this service, their policies, and any associated URL or header maps, identify all data transfers with this owner, and only data transfers with this owner.

To do so, enter the following command in CSG2 service configuration mode:

Command	Purpose
`csg2(config-csg-service)# owner {id` *id* `| name` *name*`}`	Specifies an identifier or name for a CSG2 service owner.

Specifying a Service Class

The CSG2 enables you to specify a service class value to be used with fixed-record format. The class is opaque to the CSG2 and has meaning only for the administrator. It is reported as tariff-class in fixed-record format call detail records (CDRs).

To specify a service class, enter the following command in CSG2 service configuration mode:

Command	Purpose
`csg2(config-csg-service)# class value`	Specifies a service class value.

Configuring a Service Idle Time

The CSG2 enables you to configure an idle timer for a service. The timer begins when there are no sessions. If the timer expires and the subscriber's quota for the service has not been used, the CSG2 assumes that the service is idle and sends a Service Stop to free up the resources.

For services configured with **basis second**, make sure the idle timeout value for the content configurations, set using the **idle** command in CSG2 content configuration mode, does not exceed the service idle timeout value, set using the **idle** command in CSG2 service configuration mode.

To configure a service idle timer, enter the following command in CSG2 service configuration mode:

Command	Purpose
`csg2(config-csg-service)# idle duration`	(Optional) Specifies the minimum amount of time that the CSG2 maintains a service with no subscriber sessions.

Configuring Advice of Charge

Advice of Charge (AoC) is a function that enables a service provider to provide messaging and authorization prompts to its subscribers. The CSG2's support for AoC uses a quota server and a customer-provided notification server to host the actual messaging:

- The quota server is responsible for telling the CSG2 to block subscriber requests and redirect them to the notification server when the subscriber must make a decision to pay for the service. It is also responsible for telling the CSG2 to allow the subscriber request to flow when the subscriber has agreed to pay.
- The notification server is responsible for communicating fees to the subscriber and providing the option to pay. The subscriber's payment decision must be communicated from the notification server to the quota server.

The CSG2's role in the AoC process is to redirect subscriber data requests to the notification server. The CSG2 provides URL-redirect support for HTTP and wireless application protocol 1.x (WAP 1.x), for redirecting to the notification server. With URL-redirect, the notification server can be a standard web server, because the CSG2 does the redirection at the protocol level.

The CSG2 allows the redirection for AoC to be triggered once per service (when the first access to the service is made by the subscriber), or at the start of any new data transaction. The former is accomplished using the CSG2's service verification function, the latter using the CSG2's content authorization function. The URL can be pre-configured, or it can be provided dynamically by the quota server (the more flexible option). You can configure content authorization to request a pass/fail authorization for any transaction (for example, for individual SMTP e-mails), but the CSG2 does not honor redirect requests from the quota server in the middle of a TCP connection.

In general, the method by which the notification server communicates success or failure of the AoC to the quota server is outside the scope of the CSG2's role in the process. However, the CSG2 does provide some additional assists for URL-redirects that greatly ease the burden on the backend systems. For example, the CSG2 provides the ability to strip trailing tokens from a URL. Therefore, an HTTP-based notification server can be deployed such that it will append the results of the AoC to the subscriber's HTTP request when redirecting the subscriber to the final requested content. The CSG2 reports this URL, token and all, to the quota server on the next Content Authorization Request. If configured to do so, upon successfully receiving permission from the quota server to forward the flow, the CSG2 strips the token from the request so that the content server is not confused by the extra data.

You can instruct the CSG2 to obtain authorization from the quota server for each subscriber request for content.

The CSG2's support for AoC has the following restrictions:

- AoC is supported for all protocols except IMAP and POP3. However, AoC via content authorization and URL-redirect is supported for only HTTP, SIP, WAP 1.x, and WAP 2.0.
- AoC token-stripping is not supported for requests in which the URL is fragmented over more than one IP packet.
- AoC is not supported for Connection Duration services (that is, services configured with **basis second connect**).
- When performing AoC for a TCP connection carrying pipelined HTTP requests, the CSG2 responds with the redirect to the subscriber as soon as the quota server requests the redirect. This could result in the redirect arriving at the subscriber before responses for previous requests arrive, and the subscriber might associate the redirect with a different request in the pipeline.
- When a CSG2 prepaid service is configured for AoC, the weighting value for charging the content is not determined until the CSG2 processes the Content Authorization Response. For SMTP billing (**parse protocol smtp**), the CSG2 does not send the Content Authorization Request until it processes the SMTP DATA command. If the CSG2 does not process the SMTP DATA command for a session, then the CSG2 does not charge the session for volume and event billing.
- If a Content Authorization Request is queued to a quota server, and the quota server fails, the CSG2 reassigns the request to the standby quota server or to some other active quota server. If there is no standby quota server or other active quota server, the CSG2 completes the AoC request with action code 0 (Drop).

Note If the quota server queue is very long and very slow, the Interprocessor Communication (IPC) request for the AoC message might timeout on the Traffic Processor (TP). If this occurs, and if the timeout handler on the TP has already triggered, then the CSG2 might treat the response from the quota server as a failed message, dropping the packet.

This section contains the following information:

- Enabling AoC URL-Rewriting, page 5-6
- Configuring an AoC Token, page 5-7
- Configuring AoC URL-Appending, page 5-7
- Redirect Flexibility, page 5-8

Enabling AoC URL-Rewriting

When AoC URL-rewriting is enabled, the CSG2 alerts the quota server of a new transaction, and allows it to direct the CSG2 to perform any of the following mutually exclusive actions:

- **DROP**: Drop all packets for this flow.
- **FORWARD**: Forward the flow without altering the destination (a weight might be specified).
- **REDIRECT-URL**: Redirect subscriber requests to the URL provided by the quota server. The CSG2 sends a Layer 7 redirect to the subscriber (for example, HTTP 302 response) that contains the redirect URL.

To enable AoC URL-rewriting, enter the following command in CSG2 service configuration mode:

Command	Purpose
`csg2(config-csg-service)# aoc enable`	(Optional) Enables Advice of Charge (AoC) URL-rewriting for the CSG2.

Configuring an AoC Token

When direct communication is not possible between the quota server and the notification server, payment decision information can be shared indirectly by modifying the URL in the subscriber request. The notification server appends a string beginning with a token to the originally requested URL and sends it to the subscriber as part of a redirect reply after the subscriber agrees to pay. The CSG2 receives the subsequent GET request containing the rewritten URL and sends it to the quota server in a Content Authorization Request. The quota server recognizes the token string and understands that the subscriber has agreed to pay for the request. It responds to the CSG2 with a FORWARD action code in the Content Authorization Response. The CSG2 detects the token, creates a new GET request that contains the original URL (without the appended token and any characters following it), and sends the GET on behalf of the subscriber. The token must be known by the CSG2, the quota server, and the notification server. The token is administratively defined on the CSG2 by using the CLI. The token must be chosen carefully to ensure that it is present only in URLs that are rewritten by the notification server and not in other subscriber requests.

URL-rewriting allows a top-off server to append parameters to a URL in order to convey state information to the quota server during a Content Authorization Request. Whenever a Content Authorization Response contains the forward action code, and the URL contains the AoC confirmation token, the token and all trailing characters are removed from the URL before the request is forwarded to the server.

If the token uses the URL-escape format, the redirect URL to which the token is being matched must also use the URL-escape format.

The CSG2 supports AoC URL-rewriting for only HTTP and WAP 1.x.

If you have enabled AoC URL-rewriting, you can define a URL-rewriting token for AoC. To do so, enter the following command in CSG2 service configuration mode:

Command	Purpose
`csg2(config-csg-service)# aoc confirm` *token*	(Optional) Configures a token for use in AoC URL-rewriting.

Configuring AoC URL-Appending

Whenever a Content Authorization Response contains a REDIRECT_URL action code for a WAP Content Authorization Request, the CSG2 can optionally append the originally requested URL to the one returned by the quota server.

For example, if the subscriber requests the following URL:

http://www.redirect_url.com/home.wml

and the quota server returns the following URL in a REDIRECT_URL Content Authorization Response:

http://www.redirect_url. .com/charges.wml

then the CSG2 sends the following URL as part of a redirect message to the subscriber:

http://www.redirect_url. .com/charges.wml?www.redirect_url. .com/home.wml

The default behavior is to pass the redirect URL to the subscriber as specified by the quota server without modification.

The CSG2 supports AoC URL-appending for WAP 1.x and WAP 2.0 only.

If you have enabled AoC URL-rewriting, you can enable AoC URL-appending for AoC. To do so, enter the following command in CSG2 service configuration mode:

Command	Purpose
`csg2(config-csg-service)# aoc append url`	(Optional) Specifies that the CSG2 is to append the original URL to the redirect URL sent by the quota server on a Content Authorization REDIRECT_URL response for use in AoC URL-rewriting.

Redirect Flexibility

A quota server can request a redirect for multiple reasons (top-up, "sorry" indication, login request). The CSG2 allows the quota server to return the IP address and port number for each redirect. Thus, a different port number, or even a different network, can be used for every reason that the quota server might request the redirect. The CSG2 stores the most recent redirect address and port number for each service under each subscriber profile, and uses that address and port instead of the globally defined default.

Configuring Service Verification

Service verification is a capability similar to Advice of Charge (AoC), which is provided the first time a subscriber accesses a service using HTTP or WAP 1.x. A Service Verify Request quota management message supplies the quota server with content from the subscriber request (the URL, header information, subscriber agent, and so on). The quota server responds with a Service Verification Response that includes a decision to redirect the request to a notification server, to forward it, or to drop it.

Service verification provides the same URL-rewriting capabilities that are provided by AoC. An administrator uses the command-line interface (CLI) to define the service confirmation token that is used in URL-rewriting.

As long as service verification is enabled, sessions of any type for this subscriber do not trigger service reauthorization requests. Service reauthorization resumes for the subscriber when service verification is disabled.

Service verification supports forward, redirect-URL, and drop authorization action codes sent in a Service Verification Response. Service verification also supports optional downloading of quota for a subscriber in a Service Verification Response. The CSG2 sends service verification requests even when no quota is supplied in the Service Verification Response, if the Service Authorization Response contains the cause TLV with value 0x04 (subscriber low on quota, but service access is permitted). Quota Download call detail records (CDRs) are sent to the BMA, as appropriate, whenever the quota server supplies quota in a Service Verification Response.

Service verification can be used in conjunction with existing AoC functionality.

Service verification is supported only for HTTP and WAP 1.x.

This section contains the following information:

- Enabling Service Verification URL-Rewriting, page 5-9
- Configuring a Service Verification Token, page 5-9

Enabling Service Verification URL-Rewriting

When service verification URL-rewriting is enabled, the CSG2 alerts the quota server of a new transaction, and allows it to direct the CSG2 to perform any of the following mutually exclusive actions:

- **DROP**: Drop all packets for this flow.
- **FORWARD**: Forward the flow without altering the destination (a weight might be specified).
- **REDIRECT-URL**: Redirect subscriber requests to the URL provided by the quota server. The CSG2 sends a Layer 7 redirect to the subscriber (for example, HTTP 302 response) that contains the redirect URL.

To enable service verification, enter the following command in CSG2 service configuration mode:

Command	Purpose
`csg2(config-csg-service)# verify enable`	(Optional) Enables service verification for the CSG2. Service verification is disabled when you enter the **no** form of this command, or when the quota server sends a Service Verify Tag-Length-Value (TLV) in a Service Authorization Response or Service Verification Response.

Configuring a Service Verification Token

URL-rewriting allows a top-off server to append parameters to a URL in order to convey state information to the quota server during a Service Verification Request. Whenever a Service Verification Response contains the forward action code, and the URL contains the verify confirmation token, the token and all trailing characters are removed from the URL before the request is forwarded to the server.

If the token uses the URL-escape format, the redirect URL to which the token is being matched must also use the URL-escape format.

The CSG2 supports URL-rewriting for HTTP, WAP 1.x, and WAP 2.0.

If you have enabled service verification URL-rewriting, you can define a URL-rewriting token for service verification. To do so, enter the following command in CSG2 service configuration mode:

Command	Purpose
`csg2(config-csg-service)# verify confirm` *token*	(Optional) Configures a token for use in CSG2 service verification URL-rewriting.

Enabling Service-Level CDR Summarization

By default, the CSG2 generates billing records for each transaction. This large number of records might overwhelm the charging gateway (CG) or the collector. To prevent this situation, the CSG2 can summarize CDRs at the service level, instead of at the transaction level.

For example, if a subscriber accesses the open Internet service, and the data is billed solely on the basis of volume, it is of little use to generate records for each HTTP transaction. With service-level CDR summarization enabled, the CSG2 generates only consolidated records on service-level usage. Information from individual events is not reported (for example, no URLs).

The CSG2 uses the Service Usage - variable format (0x0040) CDR for service-level CDR summarization.

Service-level CDRs differ from Service Stop CDRs as follows:

- The CSG2 sends a Service Stop message to the quota server when a prepaid service instance ends. At the same time, the CSG2 sends a companion CDR, the Service Stop Notification CDR (0x11), to the BMA.
- The CSG2 sends a service-level CDR to the BMA when a service instance ends, or, if configured, when a volume- or time-based threshold is met. The CSG2 sends service-level CDRs only to the BMA, and only if the service is configured for service-level CDRs.

The CSG2 can generate intermediate service-level CDRs for volume-based billing or for time-based billing. Cause codes 0x0A and 0x0B are used for service-level CDRs generated for volume- or time-based billing.

The CSG2 supports the following protocols in both fixed and variable format: FTP, IP, HTTP, IMAP, POP3, RTSP, SMTP, and WAP 1.x. (POP3 and IMAP are supported in postpaid mode only.)

To configure service-level CDR summarization, enter the following command in CSG2 service configuration mode:

Command	Purpose
`csg2(config-csg-service)#` **`records granularity service`** {**`bytes`** *`bytes`* | **`seconds`** *`seconds`* | **`bytes`** *`bytes`* **`seconds`** *`seconds`*}	(Optional) Specifies that the CSG2 is to generate summarized, service-level CDRs.

Note To enable service-level CDR summarization in postpaid mode, you must also specify that the associated billing plan is postpaid by using the **mode postpaid** command in CSG2 billing configuration mode.

Service-level CDRs are generated only for subscribers with entries in the CSG2 User Table entry. If a subscriber does not have an entry in the User Table, the CSG2 generates transaction-level CDRs.

If there are no quota servers configured on the CSG2, and you want to use service-level CDRs in a postpaid environment (that is, all users are postpaid), you can configure a single postpaid billing plan and assign all users to that billing plan. In the following example, all postpaid users are automatically assigned to billing plan EVERYBODY:

```
ip csg map SPORTS
  match url http://www.nhl.com/*
!
ip csg map MOVIES
  match url http://www.hollywood.com/*
!
```

```
ip csg policy SPORTS
  map SPORTS
!
ip csg policy MOVIES
  map MOVIES
!
ip csg content HTTP
  ip any tcp 80
  policy SPORTS
  policy MOVIES
  inservice
!
ip csg service SPORTS
  content HTTP policy SPORTS
  records granularity service byte 128000
!
ip csg service MOVIES
  content HTTP policy MOVIES
  records granularity service bytes 128000
!
ip csg billing EVERYBODY
  mode postpaid
  service SPORTS
  service MOVIES
```

Configuring Passthrough Mode and the Default Quota

For prepaid subscribers, sessions are blocked when a quota server is not available for authorization grant of quota. In passthrough mode, the CSG2 grants quota for services and their sessions when a quota server is not available. The CSG2 allows all traffic to pass, and CDRs are flagged for special consideration by the BMA.

For each service for which you want to use passthrough mode, you must enable it by entering the following command in CSG2 service configuration mode:

Command	Purpose
`csg2(config-csg-service)# passthrough` *quota-grant*	(Optional) Enables passthrough mode for a CSG2 service.

You also use this command to specify the size of each quota grant (the default quota) to assign to a service. When passthrough mode is enabled for a service, and a session for a service needs quota, and no quota server is active, the CSG2 grants the service the amount of quadrans specified on the **passthrough** command. (There are three types of quadrans: **basis byte** for volume-based billing, **basis fixed** for event-based billing, and **basis second** for duration-based billing.) The CSG2 continues to grant quota as long as a quota server is inactive.

When the service becomes idle, the CSG2 generates and stores a Service Stop Request message, containing the total usage for this instance of the service. When a quota server becomes active, the CSG2 forwards all stored Service Stop Request messages to the quota server.

This section contains the following information about passthrough mode:

- Flagging of Messages, page 5-12
- User Profile Requests, page 5-12
- Quota Server Recovery, page 5-12

Flagging of Messages

To facilitate billing recovery, some messages to the quota server and the BMA include a QuotaServerFlags TLV. The CSG2 adds this TLV whenever it grants a passthrough mode quota to a service.

User Profile Requests

When the CSG2 learns of new subscribers, it typically sends a User Profile Request to an active quota server. This enables the CSG2 to learn the billing plan to use for each subscriber. If the quota server returns a NULL billing plan, this indicates that a subscriber is postpaid.

When passthrough mode is in use for any service, the CSG2 changes the way it processes User Profile Requests. When there is no active quota server, the CSG2 assigns all new subscribers to postpaid processing. The CSG2 reports all sessions for these subscribers as postpaid, and does not flag generated CDRs with a QuotaServerFlags TLV.

If a subscriber is still on the network when the quota server becomes active, the CSG2 sends a normal User Profile Request to the quota server for the subscriber. When the CSG2 receives a response, it updates the subscriber's billing plan. If the updated billing plan is now a prepaid billing plan, the CSG2 blocks new IP sessions started by the subscriber until the quota server grants a quota. IP sessions that were active before the billing plan was updated to prepaid are kept as postpaid, and generate postpaid CDRs until they end.

Quota Server Recovery

When a quota server becomes active, the CSG2 forwards stored Service Stop Requests to it. Additional actions taken by the CSG2 depend on subscriber traffic.

When a subscriber who was forced to postpaid status while the quota server was absent creates a new IP session, the CSG2 issues a User Profile Request followed by a Service Authorization Request, and blocks new traffic until quota has been granted.

Prepaid subscribers might have some services that were granted quota in passthrough mode. For those services, when quota runs low, the CSG2 sends a Service Reauthorization Request to the quota server, flagging the request with the QuotaServerFlags TLV. The usage TLV and remaining TLV contain the sum total of quota granted to the service since it began. This total might be a combination of quota granted by the quota server before the failure and quota granted by the CSG2 in passthrough mode. The requested quadrans TLV contains a request for an additional quota amount.

When the quota server responds to a Service Stop or a Service Reauthorization Request, the CSG2 moves the service out of passthrough mode. If the quota server denies quota when it sends a Service Authorization Response message, the CSG2 blocks the traffic. The CSG2 also flags CDRs generated by traffic for these services, which received passthrough mode quota grants, with QuotaServerFlags TLVs, until a Service Stop Request is sent. That is, once a service is granted a passthrough mode quota, the CSG2 flags all CDRs for that serviced, up to and including the Service Stop. This applies only to prepaid subscribers. Postpaid subscribers CDRs are never flagged.

Configuring Metering

The CSG2 enables you to control some aspects of metering.

This section contains the following information:

- Configuring an Initial Quota for Metering, page 5-13
- Configuring a Minimum Quota for Metering, page 5-13
- Configuring a Debit Increment for Metering, page 5-14
- Excluding RTSP PAUSE from Metering, page 5-14
- Including IMAP Bytes in Metering, page 5-15
- Excluding MMS from Metering, page 5-17
- Excluding the Final Service Idle from Metering, page 5-17

Configuring an Initial Quota for Metering

TheCSG2 enables you to specify the initial quota, in quadrans, debited from the balance at the beginning of a service when the service is configured for Service Duration Billing. The debit occurs when the CSG2 grants the first network access for a session that has been mapped to the service. The initial value is not rounded up to the nearest increment value.

Specifying the initial quota allows you to apply “connection setup charges” to a service.

To specify the initial quota, enter the following command in CSG2 service configuration mode:

Command	Purpose
`csg2(config-csg-service)# meter initial value`	(Optional) Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing.

Configuring a Minimum Quota for Metering

The CSG2enables you to specify the minimum number of quadrans debited for a service or session, excluding the value in **meter initial**.

For example, to force the CSG2 to debit 90 quadrans when less than 90 quadrans of network usage were used for the service, specify **meter minimum 90**. If the initial value is 20 quadrans and the minimum is 90 quadrans, then the minimum total charge is 110 quadrans. The minimum value is applied only if at least 1 session is granted network access for the service.

If **basis second** is configured for the service, the usage is rounded up to the minimum value when the Service Stop is sent. For a minimum value of 90, 150 seconds of network usage is not rounded up for the purpose of calculating usage in the Service Stop, but, for example, 63 seconds of network usage is rounded up to 90 quadrans.

Note The rounding-up of network usage is not reflected in calculations for the Usage Tag-Length-Value (TLV) in Service Reauthorization Requests.

To specify the minimum number of quadrans debited by the CSG2 for a service or session, enter the following command in CSG2 service configuration mode:

Command	Purpose
`csg2(config-csg-service)# meter minimum value`	(Optional) Specifies the minimum number of quadrans debited for a service or session.

Configuring a Debit Increment for Metering

The CSG2enables you to specify the increment, in seconds, for debiting quota upon completion of a service configured for Service Duration Billing. For example, to enable the CSG2 to charge quota per minute instead of per second, specify **meter increment 60**.

If **basis second** is configured for the service, the network usage (usage excluding the initial charge) is rounded up to the nearest integer multiple of the increment value when the Service Stop is sent. For an increment value of 60, the CSG2 does not round up 120 seconds of network usage; however, the CSG2 does round up, say, 163 seconds of network usage to 180 quadrans before it calculates total usage for reporting in the Service Stop.

Note The rounding-up of network usage is not reflected in calculations for the Usage Tag-Length-Value (TLV) in Service Reauthorization Requests.

The increment value is considered when determining whether sufficient quota exists for granting network access for a session. For instance, if the increment is 60, the network usage is 50, and the balance is 10, network access is permitted. However, if the increment is 60, the network usage is 70, and the balance is 10, network access is not permitted because the balance is not sufficient to satisfy the entire increment (that is, a minimum of 1 minute of quota would be required to allow access for a portion of the minute).

To specify the debiting increment, enter the following command in CSG2 service configuration mode:

Command	Purpose
`csg2(config-csg-service)# meter increment value`	(Optional) Specifies the increments for debiting quota by the CSG2 upon completion of a service configured for Service Duration Billing.

Excluding RTSP PAUSE from Metering

The CSG2 monitors the RTSP control session between the RTSP subscriber and network and scans for PAUSE and PLAY methods. When a PAUSE method is detected, the CSG2 initiates an event to inform the prepaid service to stop charging for duration-based billing. Then, when a PLAY method is detected, the CSG2 initiates an event to inform the prepaid service to resume the charging for duration-based billing. The event corresponding to the PLAY is only necessary when the CSG2 is in the PAUSE state.

When configuring RTSP PAUSE support, keep the following considerations in mind:

- RTSP pause is supported only for duration-based billing (**basis second**).

- Duration-based billing applies only to a billing service, and RTSP might not be the only application that is operating over a given billing service. Therefore, the suspension of billing for the PAUSE period applies only if there are no other applications operating over the same billing service.
- Both last billable and intermediate idles for RTSP are excluded from duration-based billing if RTSP PAUSE support is configured.
- RTSP PAUSE support applies only to classical RTSP transport, in which the stream data is transmitted over a separate User Datagram Protocol (UDP) connection. RTSP PAUSE support does not apply to the TCP or HTTP interleaved transport modes.
- RTSP pause support is independent of the UDP content idle timer value and of the RTSP service idle timer. RTSP pause support does not stop the UDP content idle timer.
- RTSP PAUSE support applies only to charges for prepaid quota usage (quadrans TLV).
- The RTSP PAUSE time is not reflected in any CDRs.

To exclude the RTSP PAUSE time from the duration-based billing calculation, enter the following command in CSG2 service configuration mode:

Command	Purpose
`csg2(config-csg-service)# meter exclude pause rtsp`	(Optional) Excludes the RTSP PAUSE time from the CSG2 usage calculation duration billing.

Including IMAP Bytes in Metering

The CSG2 provides transaction support for IMAP. The CSG2 defines an IMAP transaction as a tagged response from an IMAP server that contains TEXT. TEXT is the part of the e-mail that follows the envelope; the presence of TEXT results in a classification of BODY. The CSG2 includes IMAP transaction counts in the Completed Transactions TLV. The CSG2 does not include any envelope information in the IMAP transaction CDRs.

For requests and responses that are not transactions (they do not contain TEXT), the CSG2 accumulates the bytes and includes them in the next transaction. When the IMAP session ends, the CSG2 reports any remaining bytes.

Consider the following simple example of an IMAP transaction with BODY:

Subscriber request: 1 FETCH 5 BODY[]
Network response: * 5 FETCH (BODY[]{55}cr-lf-55-bytes-of-e-mail-followed-by-cr-lf)cr-lf
1 OK FETCH COMPLETE

The CSG2 handles this request and response as follows:

Step 1 The subscriber request is tagged **1**. The CSG2 parses the request and increments the body up byte counts, because the request was for a **BODY[]**.

Step 2 The CSG2 parses the untagged response from the network and notes that it contains TEXT (**BODY[]**).

Step 3 The CSG2 parses the tagged response **1 OK FETCH COMPLETE**, which means this is an IMAP transaction (a tagged response that contains TEXT).

Here is a more complicated example:

Subscriber request: 8 FETCH 1:100 BODY[]<0.5>
Network response: * 1 FETCH (BODY[]<0> “. . . . .”)cr-lf
*** 2 FETCH (BODY[]<0> “. . . . .”)cr-lf**
*** 3 FETCH (BODY[]<0> “. . . . .”)cr-lf**
*** 4 FETCH (BODY[]<0> “. . . . .”)cr-lf**
...
*** 100 FETCH (BODY[]<0> “. . . . .”)cr-lf**
8 OK FETCH COMPLETE

The CSG2 handles this request and response as follows:

Step 1 The subscriber request is tagged **8**. The CSG2 parses the request and increments the body up byte counts, because the request was for a **BODY[]**.

Step 2 The network sends 100 untagged responses which the CSG2 parses, noting that the response contains TEXT (**BODY[]**).

Step 3 The CSG2 parses the tagged response **8 OK FETCH COMPLETE**, which means this is an IMAP transaction (a tagged response that contains TEXT). The CDR reports 100 **BODY** fetches, the request bytes are allocated to body up, and the response bytes are allocated to body down.

The CSG2 categorizes bytes as BODY, HEADER, and OTHER, determined as follows:

- BODY—The bytes are classified as BODY if a fetch request or response is encountered for one of the following specifications (including any appended “<>” subset variants):
  - BODY[]
  - BODY[#]
  - BODY[TEXT]
  - BODY[#.TEXT]
  - BODY.PEEK[]
  - BODY.PEEK[#]
  - BODY.PEEK[TEXT]
  - BODY.PEEK[#.TEXT]
  - RFC822
  - RFC822.TEXT
- HEADER—If the bytes cannot be classified as BODY, then they are classified as HEADER if a fetch request or response is encountered for one of the following specifications (including any appended “<>” subset variants):
  - BODY[HEADER]
  - BODY[#.HEADER]
  - BODY.PEEK[HEADER]
  - BODY.PEEK[#.HEADER]
  - RFC822.HEADER

- OTHER—If request or response cannot be classified as BODY or HEADER, then it is classified as OTHER. OTHER examples include:
  - SYN/FIN/ACK/RST packets that do not contain a payload
  - Non-HEADER or BODY IMAP commands such as **3 select inbox**
  - Retransmitted packets
  - Anything else that is not considered BODY or HEADER
  - If the session becomes encrypted or enters PASSTHRU mode, subsequent packets for the session cannot be parsed and are treated as OTHER.

Note Any IMAP transaction that is not an OK tagged response (such as **1 OK FETCH COMPLETE**) is subject to a prepaid refund.

To specify which IMAP bytes are billed for when doing prepaid debits (BODY only, BODY and HEADER only, or BODY and OTHER only), enter the following command in CSG2 service configuration mode:

Command	Purpose
`csg2(config-csg-service)# meter include imap body {header | only | other}`	(Optional) Specifies which IMAP bytes are billed for by the CSG2 when doing prepaid debits. Because IMAP metering is byte-based, you cannot configure both **meter include imap** and **basis fixed** or **basis second** in the same service. Only **basis byte** is meaningful with **meter include imap**.

Excluding MMS from Metering

By default, the CSG2 treats Multimedia Messaging Service (MMS) traffic like any other WAP 1.x traffic and generates prepaid and postpaid WAP statistics reports for it. The content type distinguishes it as MMS traffic. You can disable MMS prepaid billing by performing the following task:

To disable MMS prepaid billing, excluding MMS bytes from the CSG2 usage calculation, enter the following command in CSG2 service configuration mode:

Command	Purpose
`csg2(config-csg-service)# meter exclude mms wap`	(Optional) Excludes bytes for a WAP 1.x Multimedia Messaging Service (MMS) session from the CSG2 usage calculation.

Excluding the Final Service Idle from Metering

The CSG2 enables you to exclude the final service idle from the CSG2 usage calculation duration billing.

Excluding the final service idle might result in reduced charging because the next service access occurs after the service idles, rather than occurring before the service idles.

You cannot configure both **meter exclude svc-idle** and **basis byte** or **basis fixed** in the same service. Only **basis second** is meaningful with **meter exclude svc-idle**.

To exclude the final service idle, enter the following command in CSG2 service configuration mode:

Command	Purpose
`csg2(config-csg-service)# meter exclude svc-idle`	(Optional) Excludes the final service idle from the CSG2 usage calculation duration billing.

Configuring the Quota Reauthorization Threshold

You can configure the threshold of available quota that triggers CSG2 service reauthorization.

To configure the reauthorization threshold, enter the following command in CSG2 service configuration mode:

Command	Purpose
`csg2(config-csg-service)# reauthorization threshold` *threshold*	(Optional) Configures the CSG2 reauthorization threshold.

For services configured for fixed-cost billing (**basis fixed**), the reauthorization trigger is the smaller of the following values:

- The threshold configured using the **reauthorization threshold** command
- 25% of the last quota grant returned from the quota server

For services configured for volume-based billing (**basis byte**), the reauthorization trigger is the smaller of the following values:

- The threshold configured using the **reauthorization threshold** command
- 32 KB or 25% of the last quota grant returned from the quota server, whichever is larger

For services configured for duration-based billing (**basis second**), the reauthorization trigger is the threshold configured using the **reauthorization threshold** command.

Note The CSG2 can also accept a threshold specified by the quota server in a quota grant to the CSG2. The threshold must appear in each and every quota server response. The quota server threshold, if present, overrides the threshold specified using the **reauthorization threshold** command.

Configuring the Quota Reauthorization Timeout

After the CSG2 receives a grant of zero quadrans in a Service Authorization Response, the CSG2 waits before it requests quota in a Service Reauthorization Request. You can configure a timer to trigger the service reauthorization.

To specify the CSG2 reauthorization timeout, enter the following command in CSG2 service configuration mode:

Command	Purpose
`csg2(config-csg-service)# reauthorization timeout [initial initial-timeout] [maximum maximum-timeout]`	(Optional) Configures the CSG2 reauthorization timeout.

For every quota grant of zero, the reauthorization time doubles, until the maximum timeout is reached. For example, if the initial timeout is set to 30 seconds, and the maximum timeout is set to 250 seconds, the reauthorization times (assuming quota grants of zero) would be:

- 30 seconds
- 60 seconds
- 120 seconds
- 240 seconds
- 250 seconds
- 250 seconds

And so on.

Note The CSG2 can also accept a timeout specified by the quota server in a quota grant to the CSG2. The timeout must appear in each and every quota server response. The quota server timeout, if present, overrides the timeout specified using the **reauthorization timeout** command.

Enabling a Refund Policy for a Service

The prepaid error reimbursement feature allows the CSG2 to automatically refund quota for failed transactions. If you have configured a refund policy for the CSG2, you can enable that refund policy for use by a prepaid service.

For more information about refunding in CSG2, see the "Configuring a Refund Policy on the CSG2" section on page 2-18.

To enable a refund policy, enter the following command in CSG2 service configuration mode:

Command	Purpose
`csg2(config-csg-service)# refund policy-name`	(Optional) Specifies the refund policy for a CSG2 prepaid service.

CHAPTER 6

Configuring IPC Support

The CSG2 Interprocessor Communication (IPC) module provides a communication channel between the CSG2 Control Processor (CP) and Traffic Processors (TPs), and, in a redundant CSG2 deployment, between the TPs on the active CSG2 and their counterparts on the standby CSG2.

The CSG2 provides the following features for the IPC module:

- Configuring the IPC Keepalive Time, page 6-1
- Configuring the IPC Retransmit Time, page 6-1
- Configuring the IPC Retry Number, page 6-2
- Changing the IPC Crash Dump Setting, page 6-2

Configuring the IPC Keepalive Time

By default, the CSG2 sends keepalive messages to the IPC module once every 60 seconds. That setting is sufficient in most environments, but the CSG2 also allows you to change the time between keepalive messages, if necessary.

Note We recommend that you change the keepalive time interval only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

To change the keepalive timer for the IPC module, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg ipc keepalive` *number-of-seconds*	(Optional) Defines the IPC keepalive time interval for the CSG2.

Configuring the IPC Retransmit Time

By default, the CSG2 retransmits packets to an IPC module once every four seconds. That setting is sufficient in most environments, but the CSG2 also allows you to change the time between retransmits, if necessary.

Note We recommend that you change the retransmit time interval only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

To change the IPC retransmit time interval for the CSG2, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg ipc retransmit` *number-of-seconds*	(Optional) Defines the IPC retransmit time interval for the CSG2.

Configuring the IPC Retry Number

By default, the CSG2 retries communication with an IPC module three times before determining that the link has failed. That setting is sufficient in most environments, but the CSG2 also allows you to change the number of retries, if necessary.

Note We recommend that you change the number of retries allowed only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

To change the maximum number of IPC retries allowed before the CSG2 determines that the link has failed, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg ipc retries` *number-of-retries*	(Optional) Defines the maximum number of IPC retries allowed before the CSG2 determines that the link has failed.

Changing the IPC Crash Dump Setting

The CSG2 enables you to define the action to be taken by the CSG2 if an IPC link fails:

- Never generate a crash dump. This is the default setting.
- Wait a specified length of time, then generate a crash dump.

The default setting, to never generate a crash dump, is sufficient in most environments, but the CSG2 also allows you to change the crash dump setting, if necessary.

Note We recommend that you change the crash dump setting only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

To define the action to be taken by the CSG2 if an IPC link fails, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg ipc crashdump [never | tolerance [number of seconds]]`	(Optional) Defines the action to be taken by the CSG2 if an IPC link fails,.

CHAPTER 7

Configuring PSD Support

The CSG2 supports the Cisco Persistent Storage Device (PSD) Module Software Release 2.0 or later. The PSD provides persistent storage capabilities to the CSG2, and allows the CSG2 to store data on the PSD's internal hard drive.

Under normal conditions, the CSG2 sends call detail records (CDRs) to the Billing Mediation Agents (BMAs). If for any reason those BMAs cannot be reached, CDRs are sent to the PSD for safekeeping until contact is reestablished with the BMAs. When contact is reestablished, the CSG2 retrieves the CDRs from the PSD and forwards them to the BMAs.

Note Instead of using the PSD as backup storage, the CSG2 can use the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI). For more information, see the "Configuring iSCSI Support" section on page 8-1.

The CSG2 supports only one type of backup device, either a PSD or an iSCSI device. The PSD and iSCSI features can coexist, but only one can be enabled at a time.

Storage

Under normal conditions, the PSD provides standby capabilities when necessary—for example, during network outages. The PSD stores the payload from the packet in a queue, and is unaware of the content or format of that data, so that the data can be retrieved exactly as it was sent.

Retrieval

Once the CSG2 determines that the regular data server is again reachable (in this case, the BMA), it retrieves the stored data from the PSD. The data is returned to the CSG2 in the same order and form as it was deposited. The CSG2 is responsible for maintaining order, if necessary, or of mixing retrieved data with incoming "live" records. Once the CSG2 acknowledges to the PSD that it has successfully sent the data to the data server (the BMA), the PSD deletes that data. The PSD stores the data until it receives this acknowledgement.

The CSG2 provides the following features for the Cisco Persistent Storage Device (PSD):

- Configuring the PSD Local Port, page 7-2
- Configuring the PSD, page 7-2
- Configuring the PSD Packet Drain Settings, page 7-2
- Configuring the PSD Keepalive Time, page 7-3
- Configuring the PSD GTP' Message Buffer, page 7-3
- Configuring the PSD Retransmit Time, page 7-4

- Configuring the PSD Retry Number, page 7-4
- Configuring the PSD Window Size, page 7-5

Configuring the PSD Local Port

The first step when configuring CSG2 support for the PSD is to configure the local port on which the CSG2 is to communicate with the PSD.

To configure a local port for the PSD, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg psd local-port port-number`	Configures the local port on which the CSG2 communicates with the PSD. The PSD local port number must be different from the BMA local port number and from the quota server local port number (configured with the **ip csg bma local-port** command and the **ip csg quota-server local-port** command, respectively).

Configuring the PSD

You can configure one and only one PSD for each CSG2.

If you have enabled interface awareness, you can also associate a VLAN's Virtual Routing and Forwarding (VRF) table name with the PSD.

To configure a PSD, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg psd [vrf vrf-name] ip-address port-number`	Configures the PSD. **Note** The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters. The CSG2 does not support the use of the word **forwarding** as a valid VRF name.

Configuring the PSD Packet Drain Settings

When the BMA becomes active, the CSG2 begins draining packets from the PSD.

By default, the CSG2 limits the rate at which GTP' messages are read from the PSD to 500 packets/second. However, you can change that rate. For example, you can specify an interval of 2 seconds to yield a rate of 250 packets/second (500 packets/2 seconds).

To configure a delay before the CSG2 begins draining packets, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg psd drain delay number-of-seconds`	(Optional) Defines the delay interval, in seconds, before draining packets from the PSD when the BMA becomes active.

You can also change the rate at which GTP' messages are read from the PSD by changing the number of packets to be drained per interval. For example, specifying that 1000 packets are to be drained per interval yields a rate of 1000 packets/second (1000 packets/1 second).

To configure the number of packets to be drained from the PSD, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg psd drain packet number-of-packets`	(Optional) Defines the number of packets to be drained from the PSD per drain delay interval when the BMA becomes active.

Configuring the PSD Keepalive Time

By default, the CSG2 sends keepalive messages to the PSD once every 60 seconds. That setting is sufficient in most environments, but the CSG2 also allows you to change the time between keepalive messages, if necessary.

Note We recommend that you change the keepalive time interval only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

To change the keepalive timer for the PSD, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg psd keepalive number-of-seconds`	(Optional) Defines the PSD keepalive time interval for the CSG2.

Configuring the PSD GTP' Message Buffer

The CSG2 can buffer general packet radio service (GPRS) tunneling protocol prime (GTP') messages for the BMA. For the PSD, the CSG2 can buffer additional GTP' messages, beyond the size of the BMA GTP' message queue. The default settings are sufficient in most environments, but the CSG2 also allows you to change the PSD GTP' message buffer, if necessary.

Note We recommend that you change the number of GTP' messages that can be buffered only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

To change the maximum number of GTP' messages, beyond the size of the BMA GTP' message queue, that the CSG2 can buffer for the PSD, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg psd margin` *number*	(Optional) Specifies the maximum number of GTP' messages, beyond the size of the BMA message queue, that the CSG2 can buffer for the PSD.

Configuring the PSD Retransmit Time

By default, the CSG2 retransmits packets to the PSD once every four seconds. That setting is sufficient in most environments, but the CSG2 also allows you to change the time between retransmits, if necessary.

Note We recommend that you change the retransmit time interval only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

To change the PSD retransmit time interval for the CSG2, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg psd retransmit` *number-of-seconds*	(Optional) Defines the PSD retransmit time interval for the CSG2.

Configuring the PSD Retry Number

By default, the CSG2 retries communication with the PSD three times before determining that the link has failed. That setting is sufficient in most environments, but the CSG2 also allows you to change the number of retries, if necessary.

Note We recommend that you change the number of retries allowed only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

To change the maximum number of PSD retries allowed before the CSG2 determines that the link has failed, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg psd retries` *number-of-retries*	(Optional) Defines the maximum number of PSD retries allowed before the CSG2 determines that the link has failed.

Configuring the PSD Window Size

By default, the CSG2 sets the maximum PSD transmit window size to 128 packets, and sets the minimum PSD transmit window size automatically. Those settings are sufficient in most environments, but the CSG2 also allows you to change the maximum and minimum PSD transmit window sizes, if necessary.

Note We recommend that you change the transmit window size only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

To define the PSD transmit window size for the CSG2, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg psd window {max` *window-size* `| min` *window-size* `| min auto}`	(Optional) Defines the PSD transmit window size for the CSG2.

CHAPTER 8

Configuring iSCSI Support

Under normal conditions, the CSG2 sends call detail records (CDRs) to the Billing Mediation Agent (BMA). If for any reason those BMAs cannot be reached, CDRs are sent to the Cisco Persistent Storage Device (PSD) for safekeeping until contact is reestablished with the BMAs. When contact is reestablished, the CSG2 retrieves the CDRs from the PSD and forwards them to the BMAs. For more information, see the "Configuring PSD Support" section on page 7-1.

Instead of using the PSD as backup storage, the CSG2 can use the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) to store CDRs until the BMAs can be reached. This chapter describes that function.

Note The CSG2 supports only one type of backup device, either a PSD or an iSCSI device. The PSD and iSCSI features can coexist, but only one can be enabled at a time.

The CSG2 provides the following features for the SAN connected to the iSCSI:

- iSCSI Overview, page 8-1
- Configuring an iSCSI Target Interface Profile on the CSG2, page 8-2
- Associating an iSCSI Target Interface Profile with the CSG2, page 8-3
- Configuring the iSCSI Packet Drain Settings, page 8-4
- Verifying the iSCSI Session, page 8-4

iSCSI Overview

The iSCSI transport protocol operates over TCP/IP, enabling mobile operators and service providers to use their SAN connected to an iSCSI to save CDRs.

SAN technology, which enables customers to build scalable storage solutions, is comprised of the following primary elements:

- **SCSI**—An interface standard which enables multiple devices to be installed on a system, attached to cable to form a chain of devices. Each device is assigned a unique ID, which is expressed as a number, that identifies that device on the bus. SCSI IDs can be broken into Logical Unit Numbers (LUNs), enabling a number of devices to share a single SCSI ID. Devices from which I/O requests originate are called initiators, and devices from which responses originate are called targets.

- **SAN**—Technology that involves moving network storage to a separate network of its own. Disk, tape, and optical storage can then be attached to the storage network that is based on a fabric of switches and hubs that connects storage devices to a heterogeneous set of servers.

  A SAN system provides block-level access to data residing on shared storage arrays through dedicated storage networks.

  Under normal conditions, the SAN connected to the iSCSI provides standby capabilities when necessary—for example, during network outages. The SAN stores the payload from the packet in a queue, and is unaware of the content or format of that data, so that the data can be retrieved exactly as it was sent.

  Once the CSG2 determines that the regular data server is again reachable (in this case, the BMA), it retrieves the stored data from the SAN. The data is returned to the CSG2 in the same order and form as it was deposited. The CSG2 is responsible for maintaining order, if necessary, or of mixing retrieved data with incoming "live" records. Once the CSG2 acknowledges to the SAN that it has successfully sent the data to the data server (the BMA), the SAN deletes that data. The SAN stores the data until it receives this acknowledgement.

- **iSCSI**—Transport protocol that maps SCSI requests and responses over TCP and provides block-level data transfer between the SCSI initiator (such as the CSG2), and the target (the storage device on the SAN). The initiator sends I/O requests and the target sends I/O responses.

A SAN topology is distinguished by the following features:

- Storage is not directly connected to network clients.
- Storage is not directly connected to servers.
- Storage devices are interconnected.
- Multiple servers can share multiple storage devices.

When configuring iSCSI CDR backup and storage on the CSG2, keep the following considerations in mind:

- Currently, iSCSI targets cannot be dynamically discovered.
- The number of TCP connections per iSCSI session is limited to one.
- The iSCSI target device should be preformatted. Each LUN must have only one FAT32 partition.
- Maximum of size of a LUN must not be more than 2TB, which is the maximum disk size supported by a FAT32 file system.

Configuring an iSCSI Target Interface Profile on the CSG2

In the SCSI environment, the CSG2 functions as an iSCSI initiator. To enable the CSG2 to use the SAN for CDR backup storage, you must first configure an iSCSI target interface profile on the CSG2 that includes the name and IP address of the target, and the TCP port on which to "listen" for iSCSI traffic.

To configure the iSCSI target interface profile on the CSG2, complete the following tasks, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# ip iscsi target-profile target-profile-name`	Creates an iSCSI profile for an iSCSI target on the CSG2, and enters iSCSI configuration mode **Note** You can configure one and only one iSCSI profile on a given CSG2.
Step 2	`Router(config-iscsi)# name target-name`	Specifies the name of an iSCSI target in the target profile on the CSG2
Step 3	`Router(config-iscsi)# ip ip-address`	Specifies the IP address of an iSCSI target in the target interface profile on the CSG2.
Step 4	`Router(config-iscsi)# port port-number`	Specifies the number of the port on which to listen for iSCSI traffic in the iSCSI target interface profile on the CSG2.
Step 5	`Router(config-iscsi)# session-timeout`	Specifies the session timeout for an iSCSI target in the target interface profile on the CSG2.
Step 6	`Router(config-iscsi)# target-portal`	Specifies the portal group tag for an iSCSI target in the target interface profile on the CSG2.

Associating an iSCSI Target Interface Profile with the CSG2

After you have configured the iSCSI target interface profile on the CSG2, you must configure the CSG2 to use the iSCSI for CDR storage when no BMA is available. To do so, you must associate the iSCSI target interface profile with the CSG2. This enables the CSG2 to read from and write to the remote SAN, using the iSCSI.

To associate an iSCSI target interface profile with the CSG2, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg iscsi profile target-profile-name`	Specifies the iSCSI target interface profile to be used as backup storage for the CSG2. **Note** You can associate one and only one iSCSI target interface profile at a time with a given CSG2. The profile name specified must be the same as the one configured using the **ip iscsi target-profile** command.

Configuring the iSCSI Packet Drain Settings

When the BMA becomes active, the CSG2 begins draining CDRs from the SAN.

By default, the CSG2 limits the rate at which GTP' messages are read from the SAN to 167 packets/second. However, you can change that rate. For example, you can specify an interval of 2 seconds to yield a rate of 250 packets/second (500 packets/2 seconds).

To configure a delay before the CSG2 begins draining packets, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg iscsi drain delay` *number-of-seconds*	(Optional) Defines the delay interval, in seconds, before draining packets from the iSCSI when the BMA becomes active.

You can also change the rate at which GTP' messages are read from the SAN by changing the number of packets to be drained per interval. For example, specifying that 600 packets are to be drained per interval yields a rate of 200 packets/second (600 packets/3 seconds).

To configure the number of packets to be drained from the iSCSI, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg iscsi drain packet` *number-of-packets*	(Optional) Defines the number of packets to be drained from the iSCSI per drain delay interval when the BMA becomes active.

Verifying the iSCSI Session

To verify that the iSCSI session is up, use the following command in privileged EXEC mode:

Command	Purpose
`Router# show ip iscsi session`	Displays the status of iSCSI session.

CHAPTER 9

Configuring RADIUS Support

RADIUS is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all subscriber authentication and network service access information. The RADIUS client and server retrieve subscriber correlation information (the IP address, the MSISDN, the User-Name, and the Billing Plan) for prepaid subscribers. The CSG2 acts as a RADIUS proxy or RADIUS endpoint to retrieve the subscriber correlation information. In addition, the CSG2 can report RADIUS attributes when it communicates with the BMA and quota servers.

Figure 9-1 illustrates the placement of the Content Services Gateway 2 (CSG2) as a RADIUS Accounting proxy or monitor in the RADIUS Accounting and data flows.

Figure 9-1 RADIUS Accounting and Data Flows—RADIUS Accounting Proxy or Monitor

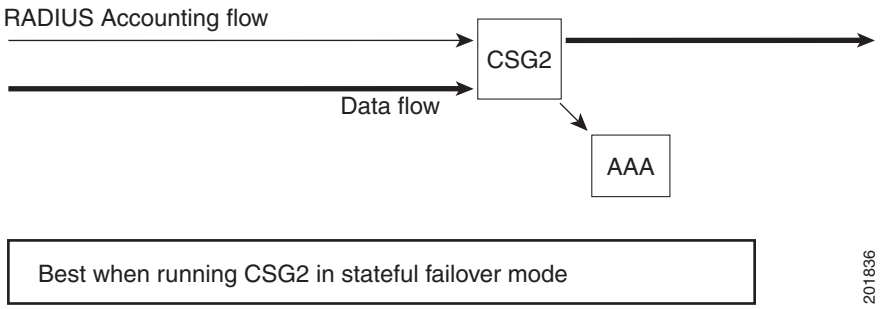
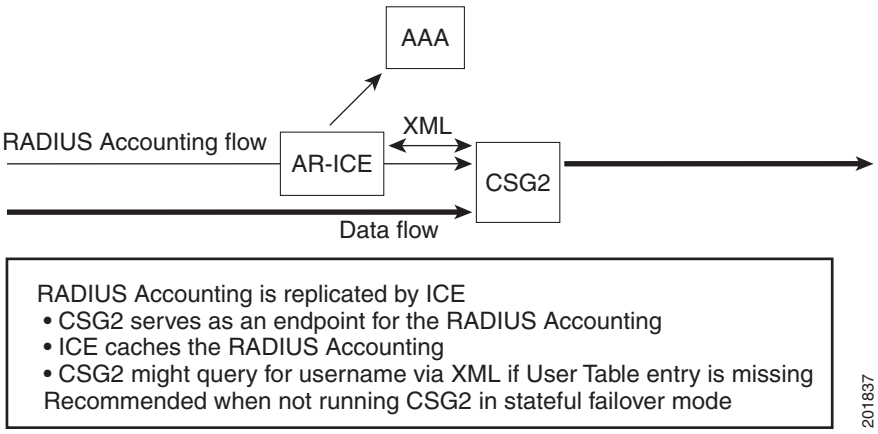


Figure 9-2 illustrates the placement of the CSG2 as a RADIUS Accounting endpoint plus Access Registrar-Identity Cache Engine (AR-ICE) in the RADIUS Accounting and data flows.

Figure 9-2 RADIUS Accounting and Data Flows—RADIUS Accounting Endpoint Plus AR-ICE



The CSG2 provides the following RADIUS features:

- Configuring RADIUS Proxy, page 9-2
- Configuring RADIUS Endpoint, page 9-3
- Configuring RADIUS Handoff, page 9-4
- Configuring RADIUS Packet of Disconnect, page 9-5
- Configuring RADIUS Monitor, page 9-6
- RADIUS Attributes and VSA Subattributes, page 9-7
- Enabling Roaming Service Control, page 9-10
- Retrieving the Billing Plan ID from RADIUS, page 9-11
- RADIUS Subscriber Cleanup, page 9-12
- RADIUS Error Acknowledgment, page 9-12
- RADIUS Correlation Processing, page 9-13

Configuring RADIUS Proxy

The CSG2 can act as a RADIUS proxy, forwarding all of the RADIUS Accounting messages it receives to a configured RADIUS server. When the RADIUS server acknowledges a message with an ACK, the CSG2 forwards the ACK to the client. RADIUS proxy supports both RADIUS Access and RADIUS Accounting.

The CSG2 RADIUS proxy function allows operation with clients that use many port numbers. The RADIUS client sends messages to the configured CSG2 (virtual) IP address. The CSG2 accepts messages for all ports on the configured IP address.

You must configure a RADIUS proxy IP address for the CSG2 to use when it forwards a RADIUS message to the server.

You can also configure an optional RADIUS key.

- If you configure a RADIUS key, the CSG2 parses and acts on a message only if the RADIUS Authenticator is correct.
- If you do not configure a RADIUS key, the CSG2 always parses and forwards every message.

If you have enabled interface awareness, you can also associate a VLAN's Virtual Routing and Forwarding (VRF) table name with a particular RADIUS proxy.

To specify that the CSG2 is a proxy for RADIUS messages, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg radius proxy [vrf csg-vrf-name] csg-address [vrf server-vrf-name] server-address csg-source-address [key [encrypt] secret-string] [vrf sub-vrf-name]`	Specifies that the CSG2 is a proxy for RADIUS messages. **Note** The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters. The CSG2 does not support the use of the word **forwarding** as a valid VRF name.

You can specify up to 64 RADIUS proxies.

Note A RADIUS proxy that is configured with different values for the *csg-address* and *csg-source-address* virtual server IP addresses consumes two RADIUS proxy resources, not just one. As a result, the maximum number of RADIUS proxies is reduced by one for each RADIUS proxy configured with different values for the virtual server IP addresses. In order to configure 64 RADIUS proxies, each RADIUS proxy must be configured with the same IP address for *csg-address* and *csg-source-address*. The virtual server IP address must still be different for each RADIUS proxy command.

Note If you specify the **ip csg entries user profile radius remove** command, you might also need to configure a key.

For Enhanced RADIUS Proxy, in order for the CSG2 to act on the optional Quota Server TLV in a RADIUS Accounting Start message, the referenced quota server must be manually configured prior to receiving the RADIUS Accounting Start message that contains the TLV.

Configuring RADIUS Endpoint

The CSG2 RADIUS features require that you configure the Network Access Server (NAS) to direct RADIUS messages to the CSG2 IP address (or to the alias address if this is a redundant configuration). You must also configure the NAS to the specific port number for the CSG2.

You can also configure an optional RADIUS key.

- If you configure a RADIUS key, the CSG2 parses and acts on a message only if the RADIUS Authenticator is correct.
- If you do not configure a RADIUS key, the CSG2 always parses every message.

If you have enabled interface awareness, you can also associate a VLAN's Virtual Routing and Forwarding (VRF) table name with a particular RADIUS endpoint.

To configure the CSG2 as a RADIUS Accounting endpoint, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg radius endpoint [vrf csg-vrf-name] csg-address key [encrypt] secret-string [vrf sub-vrf-name]`	(Optional) Identifies the CSG2 as an endpoint for RADIUS Accounting messages. **Note** The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters. The CSG2 does not support the use of the word **forwarding** as a valid VRF name.

You can specify up to 64 RADIUS endpoints.

Note When the CSG2 is configured as a RADIUS endpoint, the CSG2 drops all RADIUS packets other than RADIUS Accounting-Request messages.

A RADIUS endpoint that is configured with different values for the *csg-address* and *csg-source-address* virtual server IP addresses consumes two RADIUS endpoint resources, not just one. As a result, the maximum number of RADIUS endpoints is reduced by one for each RADIUS endpoint configured with different values for the virtual server IP addresses. In order to configure 64 RADIUS endpoints, each RADIUS endpoint must be configured with the same IP address for *csg-address* and *csg-source-address*. The virtual server IP address must still be different for each RADIUS endpoint command.

Configuring RADIUS Handoff

In networks that do not use Cisco Home Agents (HAs), the CSG2's RADIUS handoff feature can manage handoffs for roaming subscribers.

When RADIUS handoff is configured, and a RADIUS Accounting Stop is received, the CSG2 starts a handoff timer instead of immediately deleting the CSG2 User Table entry for the roaming subscriber.

- When a handoff occurs, the CSG2 detects a RADIUS Accounting Start message for the same subscriber with a different network address server (NAS) IP address. The CSG2 then uses the existing User Table entry for the subscriber, to preserve the subscriber information, and turns off the timer.
- If the handoff timer expires before the CSG2 detects a RADIUS Accounting Start message for the subscriber, the CSG2 assumes a handoff did not occur and deletes the User Table entry for the subscriber.
- In the event of a failover, all handoff timers are restarted.

To configure RADIUS handoff support, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg radius handoff duration`	(Optional) Configures the CSG2 RADIUS handoff timer.

Configuring RADIUS Packet of Disconnect

The quota server can use the RADIUS Packet of Disconnect (PoD) feature to instruct the CSG2 to disconnect a subscriber. The CSG2 sends a Disconnect-Request to the NAS, identifying the subscriber, and the NAS responds with a Disconnect_ACK (positive acknowledgement) or Disconnect_NAK (negative acknowledgement).

By using one of the following methods, the quota server instructs the CSG2 to disconnect a subscriber:

- The quota server can send the UserDisconnectRequest message to the CSG2. This message uses the UserIndex TLV to identify the subscriber to be disconnected.
- The quota server can use Action Code 4 in the Action TLV in one of the following requests and responses:
  - The Service Authorization Response (indicating that the CSG2 will send the PoD message when the quota runs out)
  - The Service Stop Request (indicating that the CSG2 will send the PoD message immediately)
  - The User Profile Response (indicating that the CSG2 will send the PoD message immediately)

The CSG2 sends the PoD message to the NAS that is specified by the NAS-IP-Address attribute (4) in the RADIUS Accounting Start.

You can also configure an optional RADIUS key.

To configure support for RADIUS PoD, enter the following commands in global configuration mode:

	Command	Purpose
Step 1	`csg2(config)# ip csg radius pod attribute {radius-attribute-number | vsa {vendor-id | 3gpp} radius-subattribute-number}`	(Optional) Specifies the RADIUS attributes and vendor-specific attribute (VSA) subattributes to be copied from the RADIUS Start message and sent to the Network Access Server (NAS) in the PoD message.
Step 2	`csg2(config)# ip csg radius pod nas [vrf vrf-name] [start-ip end-ip] port key [encrypt] secret-string`	(Optional) Specifies the NAS port to which the CSG2 is to send the PoD message, and the key to use in calculating the Authenticator. **Note** The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters. The CSG2 does not support the use of the word **forwarding** as a valid VRF name.
Step 3	`csg2(config)# ip csg radius pod timeout timeout retransmit retransmit`	(Optional) Specifies the number of times to retry the RADIUS PoD message if it is not acknowledged by means of an ACK message, and the interval between retransmissions.

The following sample configuration specifies the following Packet of Disconnect (PoD) characteristics:

- The RADIUS attributes to be copied from the RADIUS Start message and sent to the NAS in the PoD message
- The NAS port to which the CSG2 is to send the PoD message, and the key to use in calculating the Authenticator
- The number of times to retry the RADIUS PoD message if it is not acknowledged, and the interval between retries

Here is a sample configuration for RADIUS PoD:

```
ip csg radius userid User-Name
ip csg radius pod attribute 44
ip csg radius pod nas 1.1.1.0 1.1.1.255 1700 key secret
ip csg radius pod nas 1701 key password
ip csg radius pod timeout 30 retransmits 5
ip csg radius proxy 1.2.3.4 5.6.7.8 key secret
```

Configuring RADIUS Monitor

RADIUS monitor provides a way to insert the CSG2 into the RADIUS flow without changing the authentication, authorization, and accounting (AAA) or Network Access Server (NAS) addresses in the network. The CSG2 monitors the traffic between the RADIUS client and the RADIUS server, and watches for RADIUS messages that match the configured rule.

You must configure the IP address of the RADIUS server. You can also configure an optional RADIUS key.

To configure RADIUS monitor support, enter the following command in global configuration mode:

Command	Purpose
`Router(config)#` **`ip csg radius monitor`** [**`vrf`** *`csg-vrf-name`*] *`server-address server-port`* [**`key`** [*`encrypt`*] *`secret-string`*] [**`vrf`** *`sub-vrf-name`*]	Specifies that the CSG2 is to monitor the RADIUS flows to the specified server. **Note** The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters. The CSG2 does not support the use of the word **forwarding** as a valid VRF name.

To specify that the CSG2 is to monitor the RADIUS flows to the specified Network Access Server (NAS), enter the following command in global configuration mode:

Command	Purpose
`Router(config)# ip csg radius monitor nas` *nas-ip-address* [**vrf** *csg-vrf-name*]	Specifies that the CSG2 is to monitor the RADIUS flows to the specified Network Access Server (NAS). **Note** The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters. The CSG2 does not support the use of the word **forwarding** as a valid VRF name.

Here is a sample configuration for RADIUS monitor:

```
ip csg radius monitor 1.2.3.4 1813 key NAS_TABLE
```

RADIUS Attributes and VSA Subattributes

This section contains the following information:

- RADIUS Attributes Required for CSG2 User Table, page 9-7
- Deleting Entries from the CSG2 User Table, page 9-8
- Reporting RADIUS Attributes and VSA Subattributes, page 9-9

RADIUS Attributes Required for CSG2 User Table

The User Table identifies all subscribers known to the CSG2. The table is populated from the contents of RADIUS Accounting Start messages, or from the user database, if either feature is enabled in your configuration.

The following RADIUS attributes must be in the RADIUS Accounting Start in order for the CSG2 to build an entry for a subscriber in the User Table:

- 8 (Framed-IP-Address)
- Either 4 (NAS-IP-Address) or 32 (NAS-Identifier)
- Either 1 (User-Name) or 31 (Calling-Station-Id), as configured

The CSG RADIUS interface recognizes the following Cisco-specific VSAs:

- Subattribute value **csg:quota_server=<ip>:<port>** includes the quota server IP address and port in a RADIUS Start Accounting Message. You must manually configure the quota server referenced by this subattribute in order for the CSG2 to act on this VSA. If the quota server is not configured, the CSG2 creates a null entry in the User Table for the quota server. The user specified by the RADIUS message uses the quota server in the VSA.

- Subattribute value **csg:downlink_nexthop=<ip>** includes the downlink next-hop IP address in a RADIUS Start Accounting Message. The downlink next-hop IP address is the address to which all downlink traffic is sent for a given user IP address, plus table pairing. If this VSA is not present, traffic is routed based on the routing tables of the CSG2.

When the CSG2 receives the RADIUS Access-Accept with Billing Plan ID included, it caches the information. The cached information is identified by user ID (either RADIUS Attribute 1 or RADIUS Attribute 31, as configured). When the CSG2 receives the RADIUS Accounting Start message with the user ID, the CSG2 builds a User Table entry by using the cached information.

Note Cached information is not displayed in the output of the **show ip csg users** command.

Deleting Entries from the CSG2 User Table

For enhanced network connectivity options, such as secondary packet data protocol (PDP) contexts, the NAS sends multiple RADIUS Accounting Stop messages. In the case of secondary PDP contexts, for example, the NAS sends a RADIUS Accounting Stop as each context is terminated.

The CSG2 removes the subscriber from the User Table when it receives the final stop, which contains an attribute indicating it is final. The CSG2 support for this functionality allows the specific attribute to be configured. If this function is configured, the CSG2 processes only the RADIUS Accounting Stop that contains the configured attribute. The contents of the specified attribute are not examined.

Note Retransmitted RADIUS Accounting Stop messages might cause problems when associating traffic with a subscriber. To avoid any problems, do not configure your RADIUS server to reuse an IP address immediately after it is released by a subscriber.

You can specify the attribute that must be included in the RADIUS Accounting Stop request in order for the CSG2 User Table entry to be deleted. To do so, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg radius stop purge {radius-attribute-number | vsa} {vendor-id | 3gpp} radius-subattribute-number}`	(Optional) Specifies the attribute that must be included in the RADIUS Accounting Stop request in order for the CSG2 User Table entry to be deleted.

By default, the CSG2 deletes 1000 User Table entries per second in response to a RADIUS Accounting On or RADIUS Accounting Off message, or in response to the **clear ip csg user all** command. To specify a different deletion rate, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg radius on-off purge deletions-per-second`	(Optional) Specifies the rate at which the CSG2 is to delete CSG2 User Table entries in response to a RADIUS Accounting On or RADIUS Accounting Off message, or in response to the **clear ip csg user all** command. The actual rate at which the CSG2 deletes User Table entries might be slightly higher or lower than the specified rate.

Reporting RADIUS Attributes and VSA Subattributes

You can specify a set of attributes and VSA subattributes to be extracted from the RADIUS Accounting Start messages for each subscriber. The CSG2 then reports those attributes and subattributes to the Billing Mediation Agent (BMA) and quota server in every call detail record (CDR). The CSG2 can also include the attributes and subattributes in RADIUS PoD messages, if configured to do so.

You can use RADIUS attributes and subattributes to determine where a subscriber is connecting to the network, and for correlation purposes. For example, in a gateway general packet radio service (GPRS) environment you can use attributes and subattributes as follows:

- NAS-IP-Address (4) identifies the gateway that provides accounting control for the subscriber. Examples of such devices include the gateway general packet radio service (GPRS) support node (GGSN), the Packet Data Serving Node (PDSN), the Home Agent, and the Cisco AS5300 Universal Access Server.
- SGSN IP (26/10415/6) identifies the Service GPRS Support Node (SGSN) that the subscriber is accessing.CSG2
- Acct-session-ID (44) uniquely identifies the session on the NAS and can be used correlate GGSN accounting records.

The CSG2 reports attributes and subattributes in the order in which they appear in the RADIUS message. If there are multiple instances of an attribute, the CSG2 reports all of them.

The CSG2 saves and reports attribute and subattribute information for each subscriber.

When the CSG2 receives a new RADIUS Accounting Start or RADIUS Interim Accounting Request, it saves the attribute and subattribute information parsed from the new request.

The CSG2 saves only those attributes or subattributes which meet both of the following criteria:

- They are present in the new RADIUS Accounting Start or RADIUS Interim Accounting Request.
- They are configured for reporting at the time the new request arrives at the CSG2.

All previously stored attribute and subattribute information from previous requests is destroyed, even if the new RADIUS Accounting Start or RADIUS Interim Accounting Request does not contain all of the attributes and subattributes that were present in the previous request. Only the currently stored attributes are reported in CDRs.

Note The impact of RADIUS VSA subattribute parsing on CSG2 performance has not been measured. Storage is consumed based on the attributes selected.

To configure the list of attributes and subattributes to be copied from the RADIUS Start message and sent to the BMA and quota server, enter the following command in global configuration mode:

Command	Purpose
csg2(config)# **ip csg report radius attribute** {*radius-attribute-number* | **vsa**} {*vendor-id* | **3gpp**} *radius-subattribute-number*}	(Optional) Specifies the RADIUS attributes and VSA subattributes to be copied from the RADIUS Start message and sent to the BMA in CSG2 CDRs.

The attributes are configured by their standard number, as shown in the following example:

```
ip csg report radius attribute 3
ip csg report radius attribute 5
ip csg report radius attribute 7
ip csg report radius attribute 44
```

You can specify as many attributes as you want. If you specify so many attributes that the total message size is greater than a single UDP packet, the CSG2 supports continuation messages. A continuation message includes a correlator, a continuation number (so that messages that are received out of order can be reordered), and an indication of the final message.

To specify the list of attributes and subattributes to be copied from the RADIUS Start message and sent to the NAS in the PoD message, see the description of the **ip csg radius pod attribute** command in the "Configuring RADIUS Packet of Disconnect" section on page 9-5.

If both the reporting of RADIUS attributes and Roaming Service Control are enabled, the CSG2 sends the combined list of attributes in every CDR to the BMA and quota server (but only changes in the Roaming Service Control attributes trigger reauthorization). For example, if the CSG2 is configured to report attributes 1, 3, and 5, and configured to monitor attributes 2, 4, and 6 for Roaming Service Control, then the CSG2 reports attributes 1, 2, 3, 4, 5, and 6 in all CDRs to the BMA and quota server. For more information about Roaming Service Control, see the "Enabling Roaming Service Control" section on page 9-10.

Enabling Roaming Service Control

Roaming Service Control, also known as seamless roaming or RADIUS reauthorization, enables the CSG2 to reauthorize prepaid users, instead of ending the users' sessions, when a configured list of attributes changes.

1. When you enable Roaming Service Control, you also configure a list of RADIUS attributes and VSA subattributes to be monitored and saved by the CSG2.
2. When the CSG2 receives a RADIUS Start message, it saves the subset of attributes that are in both the configured list and the message.
3. When the CSG2 receives a subsequent RADIUS Start or RADIUS Interim Accounting message, it compares the saved subset of attributes to the list of attributes in the new message. (The CSG2 compares only the list of attributes, not the actual contents of those attributes.)
4. If any attribute in the saved subset is missing from the list of attributes in the new message, or if there are any new attributes in the message that are not in the saved subset, the CSG2 reauthorizes prepaid users without ending their sessions.
5. If service-level CDR summarization is enabled, the CSG2 sends a Service Usage CDR for each service in the session.

   Otherwise, if intermediate CDRs are supported for the session, the CSG2 sends an intermediate CDR for each service in the session. However, if you have enabled fixed-format CDRs, the CSG2 does not generate intermediate CDRs during roaming events.

   The CDR includes:

   - The Cause TLV, indicating that the CDR was generated due to the receipt of a reauthorization trigger
   - The saved subset of attributes from the first RADIUS Start message
   - The list of attributes from the new message

   For more information about service-level CDR summarization, see the "Enabling Service-Level CDR Summarization" section on page 5-10.

   For more information about intermediate CDRs, see the "Intermediate CDRs" section on page 1-38.

For more information about fixed-format CDRs, see the "Configuring Fixed, Variable, or Combined Format CDR Support" section on page 2-17.

To enable Roaming Service Control, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg radius reauthorization attribute {radius-attribute-number | vsa} {vendor-id | 3gpp} radius-subattribute-number}`	(Optional) Defines the RADIUS attributes and VSA subattributes to be monitored by the CSG2, and enables Roaming Service Control.

The attributes are configured by their standard number, as shown in the following example:

```
ip csg radius reauthorization attribute 14
ip csg radius reauthorization attribute vsa 7777 44
ip csg radius reauthorization attribute 26 7778 4
```

If both Roaming Service Control and the reporting of RADIUS attributes are enabled, the CSG2 sends the combined list of attributes in every CDR to the BMA and quota server (but only changes in the Roaming Service Control attributes trigger reauthorization). For example, if the CSG2 is configured to report attributes 1, 3, and 5, and configured to monitor attributes 2, 4, and 6 for Roaming Service Control, then the CSG2 reports attributes 1, 2, 3, 4, 5, and 6 in all CDRs to the BMA and quota server. For more information about the reporting of RADIUS attributes, see the "Reporting RADIUS Attributes and VSA Subattributes" section on page 9-9.

Retrieving the Billing Plan ID from RADIUS

The CSG2 can extract the Billing Plan ID from the RADIUS Access-Accept message or RADIUS Accounting-Request message by using the Cisco subattribute 1 VSA. The format of the VSA is:

- Attribute number: 26 (=vendor specific)
- Vendor ID: 9 (=Cisco)
- Subattribute: 1 (=Cisco generic)
- Format: csg:billing_plan= *billing_plan_name*

  The *billing_plan_name* can be null, indicating that the subscriber is a postpaid subscriber. Otherwise, the billing plan name must be sent as an uppercase string to match a configured billing plan on the CSG2.

If the message includes the billing plan, the user ID (RADIUS attribute 1 or 31, as configured) must also be included; otherwise, the CSG2 cannot associate the billing plan with the subscriber.

If the CSG2 is configured to obtain the billing plan from RADIUS, and the billing plan subattribute is not included in the RADIUS messages, the CSG2 queries the quota server to obtain the attribute (that is, the CSG2 sends a User Profile Request).

To configure the CSG2 to obtain the billing plan from RADIUS, the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg entries user profile radius {remove | pass | timeout timeout}`	(Optional) Specifies that the CSG2 is to obtain the Cisco vendor-specific attribute (VSA) subattribute 1, which contains the billing plan name, from the RADIUS Access-Accept and RADIUS Accounting-Request messages when generating entries for the CSG2 User Table.

To specify the RADIUS attribute that the CSG2 is to use to extract the user identifier from a RADIUS record, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg radius userid {1 | 31 | User-Name | Calling-Station-Id}`	(Optional) Specifies the RADIUS attribute used to extract the user identifier from a RADIUS record.

RADIUS Subscriber Cleanup

A subscriber's connectivity attributes might change over time without a RADIUS Accounting Stop message arriving to close down the previous accounting. Instead, it is possible that a new RADIUS Accounting Start message or a RADIUS Interim Accounting message might arrive with the updated information. Some customers might choose to close all of a subscriber's services if a significant change has occurred in the subscriber's status.

Subscriber cleanup enables the CSG2 to delete the subscriber entry as if it had received a Stop, to close all of the subscriber's services, and to create a new entry.

To clean up the CSG2 User Table entry for a subscriber, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg radius start restart session-id {radius-attribute-number | vsa} {vendor-id | 3gpp} radius-subattribute-number}`	(Optional) Deletes an existing CSG2 User Table entry for a specific subscriber, and creates a new entry for that subscriber.

To avoid deleting the subscriber entry because of a retransmission of the RADIUS message, the **ip csg radius start restart session-id** command specifies an attribute to detect duplicate messages. If the contents of the attribute in the message match the contents of the previous message, the existing entry is not deleted.

RADIUS Error Acknowledgment

By default, the CSG2 acknowledges the following RADIUS parse errors:

- Invalid RADIUS message or attribute length
- RADIUS Authenticator does not match what the CSG2 calculates

- Incorrect RADIUS attribute length
- User profile information such as billing plan or quota server does not match the CSG2 configuration

You can prevent the CSG2 from acknowledging these errors.

To prevent the CSG2 from acknowledging RADIUS parse errors, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# no ip csg radius ack error parse`	(Optional) Prevents the CSG2 from generating a RADIUS response to a RADIUS Accounting Start Request or a RADIUS Accounting Interim Request when it encounters a RADIUS parse error condition.

Note You must use the **no** form of this command, **no ip csg radius ack error parse**, to prevent the CSG2 from acknowledging these RADIUS parse errors.

By default, the CSG2 acknowledges the following user resource errors:

- Maximum number of users reached
- Unable to allocate memory for creating a user entry or for storing RADIUS attribute information (such as report attributes or parsed billing plan information)
- Unable to communicate user information via inter-processor communication
- Load manager prevents allocation of a user

You can prevent the CSG2 from acknowledging these errors.

To prevent the CSG2 from acknowledging user resource errors, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# no ip csg radius ack error user`	(Optional) Prevents the CSG2 from generating a RADIUS response to a RADIUS Accounting Start Request or a RADIUS Accounting Interim Request when it encounters a user resource error condition.

Note You must use the **no** form of this command, **no ip csg radius ack error user**, to prevent the CSG2 from acknowledging these user resource errors.

RADIUS Correlation Processing

A retransmitted RADIUS Stop might cause the CSG2 to remove a subscriber entry from the CSG2 User Table when the entry should not be removed.

To avoid this problem, the CSG2 must be able to associate a session correlator from the RADIUS Start message with a subscriber entry in the User Table, and compare that correlator with the correlator in the RADIUS Stop message. If the correlators match, the CSG2 deletes the subscriber entry; otherwise, the CSG2 retains the entry in the User Table.

The CSG2 can use the Acct-Session-Id (attribute 44) as the correlator, or it can use the following vendor-specific attribute (VSA) subattribute (attribute 26, Vendor-Id 9, subattribute 1):

csg:user_session_correlator=*string*

If both attributes are included in the RADIUS Start or RADIUS Stop message, the CSG2 uses the VSA subattribute.

When RADIUS correlation processing is enabled,:

- If there is no correlator saved in the User Table entry, the CSG2 deletes the entry.
- If there is a correlator saved in the User Table entry, the CSG2 compares it to the correlator in the RADIUS Stop. If the correlators match, the CSG2 deletes the entry; if they do not match, or if there is no correlator in the RADIUS Stop, the CSG2 retains the entry in the User Table.

To enable RADIUS correlation processing by the CSG2, enter the following command in global configuration mode:

Command	Purpose
`csg2(config)# ip csg radius correlation`	(Optional) Enables RADIUS correlation processing by the CSG2.

CHAPTER 10

Configuring Prepaid Support

This chapter contains the following information about Content Service Gateway (CSG2) support for prepaid billing:

- Configuring a Prepaid Billing Plan, page 10-1
- Prepaid WAP Support, page 10-2

Configuring a Prepaid Billing Plan

A billing plan identifies one or more content billing services to be used for prepaid billing.

To define a billing plan, follow these steps, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router (config)# ip csg billing` *billing-plan-name*	Defines a CSG2 billing plan, and enters CSG2 billing configuration mode.
Step 2	`Router (config-csg-billing)# service` *service-name*	Associates a service with a CSG2 billing plan.

The following example shows how to define a prepaid billing plan:

```
ip csg billing REGULAR
 service MOVIES
 service BROWSING
```

When a CSG2 prepaid subscriber initiates a new IP session, a large amount of quota might be reserved for the IP session if the IP session maps to a service configured for **basis byte ip** or **basis byte tcp**. The reservation often greatly exceeds the amount of quota that the session actually uses. This does not result in incorrect charging. However, as a result of one or more large reservations for IP sessions, the CSG2 might make additional requests for quota from the quota server.

Prepaid WAP Support

Some upstream WAP browsing traffic occurs because the CSG2 must inspect the reply before determining whether the traffic is an MMS transaction. However, the downstream WAP browsing replies are discarded if quota is depleted.

Control information is charged against quota for non-MMS transactions. WSP PDU types SUSPEND and RESUME are never charged against quota.

APPENDIX A

CSG2 Command Reference

This appendix documents the commands necessary to configure and monitor the CSG2. Other commands used with the CSG2 are documented in the following publications:

- *Service and Application Module for IP User Guide* for the following commands:
  - Supervisor console commands
  - Power PC console commands
  - Power PC ROM-monitor (ROMmon) console commands
  - Broadcom BCM Linux-based Storage Area Network Operation System (SanOS) console commands
  - Broadcom BCM ROMmon console commands
  - Line Card Processor (LCP) console commands
- *Cisco IOS Server Load Balancing Command Reference* for IOS SLB-specific commands
- Cisco IOS Release 12.2 command reference publications for other IOS commands

All of the CSG2 commands are listed below in alphabetical order:

- **accounting, page A-6**
- **activation, page A-7**
- **aoc append url, page A-9**
- **aoc confirm, page A-10**
- **aoc enable, page A-12**
- **basis, page A-14**
- **block, page A-17**
- **class, page A-18**
- **clear ip csg, page A-19**
- **clear ip iscsi statistics, page A-21**
- **clear record-storage-module stats, page A-22**
- **client-group (CSG2 content), page A-23**
- **content (CSG2 service), page A-25**
- **debug ip csg, page A-27**
- **entries user idle, page A-32**

- flags, page A-34
- idle (CSG2 content), page A-37
- idle (CSG2 service), page A-39
- inservice (CSG2 content), page A-41
- ip (CSG2 content), page A-42
- ip (iSCSI), page A-44
- ip csg billing, page A-46
- ip csg bma, page A-47
- ip csg bma activate, page A-49
- ip csg bma keepalive, page A-51
- ip csg bma local-port, page A-52
- ip csg bma messages, page A-54
- ip csg bma retransmit, page A-56
- ip csg bma retries, page A-57
- ip csg bma window, page A-59
- ip csg case-sensitive, page A-60
- ip csg content, page A-61
- ip csg database, page A-64
- ip csg entries fragment, page A-66
- ip csg entries session user max, page A-68
- ip csg entries user idle, page A-70
- ip csg entries user max, page A-72
- ip csg entries user profile, page A-74
- ip csg ipc crashdump, page A-76
- ip csg ipc keepalive, page A-77
- ip csg ipc retransmit, page A-78
- ip csg ipc retries, page A-79
- ip csg iscsi drain delay, page A-80
- ip csg iscsi drain packet, page A-81
- ip csg iscsi profile, page A-83
- ip csg map, page A-84
- ip csg mode single-tp, page A-86
- ip csg policy, page A-87
- ip csg psd, page A-89
- ip csg psd drain delay, page A-91
- ip csg psd drain packet, page A-92
- ip csg psd keepalive, page A-93
- ip csg psd local-port, page A-94

- ip csg psd margin, page A-96
- ip csg psd retransmit, page A-97
- ip csg psd retries, page A-98
- ip csg psd window, page A-100
- ip csg quota-server, page A-101
- ip csg quota-server activate, page A-104
- ip csg quota-server keepalive, page A-106
- ip csg quota-server local-port, page A-107
- ip csg quota-server messages, page A-109
- ip csg quota-server reassign, page A-110
- ip csg quota-server retransmit, page A-111
- ip csg quota-server retries, page A-112
- ip csg quota-server window, page A-114
- ip csg radius ack error parse, page A-116
- ip csg radius correlation, page A-120
- ip csg radius endpoint, page A-122
- ip csg radius handoff, page A-126
- ip csg radius monitor, page A-128
- ip csg radius monitor nas, page A-131
- ip csg radius on-off purge, page A-133
- ip csg radius pod attribute, page A-134
- ip csg radius pod nas, page A-136
- ip csg radius pod timeout, page A-138
- ip csg radius proxy, page A-139
- ip csg radius reauthorization attribute, page A-143
- ip csg radius start restart session-id, page A-145
- ip csg radius stop purge, page A-147
- ip csg radius userid, page A-149
- ip csg records format, page A-151
- ip csg redirect, page A-152
- ip csg refund, page A-154
- ip csg replicate, page A-155
- ip csg report http header, page A-157
- ip csg report radius attribute, page A-159
- ip csg report smtp rfc2822, page A-161
- ip csg report usage, page A-162
- ip csg report wap actual-pdu, page A-164
- ip csg service, page A-165

- ip csg snmp timer, page A-168
- ip csg subscriber, page A-169
- ip csg transport-type assign, page A-170
- ip iscsi target-profile, page A-171
- map, page A-173
- match header, page A-175
- match method, page A-179
- match url, page A-182
- meter exclude control sip, page A-186
- meter exclude mms wap, page A-188
- meter exclude network-init sip, page A-190
- meter exclude pause rtsp, page A-192
- meter exclude svc-idle, page A-194
- meter include imap, page A-196
- meter increment, page A-199
- meter initial, page A-201
- meter minimum, page A-203
- mode, page A-205
- mode tcp, page A-206
- name (iSCSI), page A-207
- next-hop, page A-209
- owner, page A-211
- parse length, page A-212
- parse protocol, page A-213
- passthrough, page A-215
- pending, page A-216
- policy (CSG2 content), page A-217
- port (iSCSI), page A-219
- reauthorization threshold, page A-221
- reauthorization timeout, page A-223
- records delay, page A-225
- records granularity, page A-226
- records intermediate, page A-228
- refund, page A-230
- replicate, page A-231
- retcode, page A-233
- sami rate all, page A-235
- service, page A-236

- session-timeout (iSCSI), page A-237
- show ip csg, page A-239
- show ip iscsi, page A-252
- show record-storage-module, page A-255
- snmp-server enable traps csg, page A-257
- subscriber-ip http-header forwarded-for, page A-259
- target-portal (iSCSI), page A-261
- verify confirm, page A-263
- verify enable, page A-265
- vlan (CSG2 content), page A-266
- vrf, page A-267

accounting

To specify accounting and an optional customer string for a CSG2 policy, use the **accounting** command in CSG2 policy configuration mode. To remove accounting for a policy, use the **no** form of this command.

accounting [customer-string *string***]**

no accounting [customer-string *string***]**

Syntax Description

customer-string *string*	(Optional) 1- to 16-byte string to be output to the generated accounting records.

Defaults

The default is no accounting.

Command Modes

CSG2 policy configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: All keywords and arguments except **customer-string** *string* were removed.
12.4(15)MD	Support for FTP was added.

Usage Guidelines

This command is required if the CSG2 is to generate call detail records (CDRs) for content that matches the CSG2 policy.

This command is required to enable billing functions (such as CDR generation and prepaid charging) for content that matches a CSG2 policy.

For FTP and Real Time Streaming Protocol (RTSP) accounting, the CSG2 matches prepaid services on the basis of the IP address and port number of the control connection to the FTP or RTSP network IP address.

Examples

The following example shows how to specify accounting and customer strings for a CSG2 policy:

```
ip csg policy MOVIES
 accounting customer-string MOVIES
```

Related Commands

Command	Description
ip csg policy	Defines a policy for qualifying flows for the CSG2 billing services, and enters CSG2 policy configuration mode.

activation

To specify the activation mode for a CSG2 Connection Duration service, use the **activation** command in CSG2 service configuration mode. To restore the default setting, use the **no** form of this command.

activation [**automatic** | **user-profile**]

no activation

Syntax Description

automatic	(Optional) Activates the Connection Duration service, unless the billing profile indicates that no service is to be activated. If you specify the **automatic** keyword, the CSG2 activates the Connection Duration service in the subscriber's billing plan automatically, unless the service name is specified with a zero length as the connect service in the billing profile information. The connect service information must be specified in the same message as the subscriber's billing plan.
user-profile	(Optional) Activates the Connection Duration service only if the billing profile specifies this service as the connect service. This is the default setting. If you specify the **user-profile** keyword, the CSG2 activates the Connection Duration service for a subscriber only if the service name is specified as a connect service in the billing profile information in an authentication, authorization, and accounting (AAA) Access-Accept, an AAA Accounting-Start, or a Quota Server User-Profile Response.

Defaults

The Connection Duration service is activated only if the billing profile specifies this service as the connect service.

Command Modes

CSG2 service configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: None.

Usage Guidelines

This command requires that the service be configured with **basis second connect**.

Examples

The following example specifies **automatic** activation for Connection Duration service CONNECT.

```
ip csg service CONNECT
 basis second connect
 activation automatic
```

Related Commands

Command	Description
ip csg service	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.

aoc append url

To specify that the CSG2 is to append the original URL to the redirect URL sent by the quota server on a Content Authorization REDIRECT_URL response for use in Advice of Charge (AoC) URL-rewriting, use the **aoc append url** command in CSG2 service configuration mode. To restore the default setting, use the **no** form of this command.

aoc append url

no aoc append url

Syntax Description

This command has no arguments or keywords.

Defaults

The CSG2 does not append the original URL to the redirect URL.

Command Modes

CSG2 service configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

Before configuring this command, you must enable AoC by configuring the **aoc enable** command.

The CSG2 performs this function only for content parsed as connectionless or connection-oriented wireless application protocol (WAP 1.x). For other protocols, the CSG2 ignores this configuration option.

Examples

The following example specifies that the CSG2 is to append the original URL to the redirect URL for use in AoC URL-rewriting:

```
ip csg service MOVIES
 aoc enable
 aoc append url
```

Related Commands

Command	Description
aoc confirm	Configures a token for use in Advice of Charge (AoC) URL-rewriting.
aoc enable	Enables Advice of Charge (AoC) URL-rewriting for the CSG2.
ip csg service	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.

aoc confirm

To configure a token for use in Advice of Charge (AoC) URL-rewriting, use the **aoc confirm** command in CSG2 service configuration mode. To remove the token, use the **no** form of this command.

aoc confirm *token*

no aoc confirm

Syntax Description

token	A string of up to 15 alphanumeric characters. The string is not case-sensitive. Acceptable characters include alphanumeric characters and any of the following special characters: $-_.+!*'(),?/:@&=;~%. To enter other special characters not listed, use the URL-escape format with the percent sign (%). To insert a question mark (?) in the string, press Ctrl-v and then press the question mark (**?**) key. To insert a question mark in an editing document, use ASCII code 22. To retain the question mark, use TFTP instead of copy-and-paste.

Defaults

None

Command Modes

CSG2 service configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **aoc confirmation** to **aoc confirm**. • The configuration mode for this command changed from CSG user group configuration to CSG2 service configuration. • The list of supported special characters changed.

Usage Guidelines

Before configuring this command, you must enable AoC by configuring the **aoc enable** command.

URL-rewriting allows a top-off server to append parameters to a URL in order to convey state information to the quota server during a Content Authorization Request. Whenever a Content Authorization Response contains the forward action code, and the URL contains the AoC confirmation token, the token and all trailing characters are removed from the URL before the request is forwarded to the server.

The token is used for HTTP and WAP 1.x content authorization URL-rewriting.

If the token uses the URL-escape format, the redirect URL to which the token is being matched must also use the URL-escape format.

Examples

The following example specifies a token for Advice of Charge (AoC) URL-rewriting:

```
ip csg service MOVIES
 aoc enable
 aoc confirm ?CSG_AOC_OK
```

Related Commands

Command	Description
aoc append url	Specifies that the CSG2 is to append the original URL to the redirect URL sent by the quota server for use in Advice of Charge (AoC) URL-rewriting.
aoc enable	Enables Advice of Charge (AoC) URL-rewriting for the CSG2.
ip csg service	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.

aoc enable

To enable Advice of Charge (AoC) URL-rewriting for the CSG2, use the **aoc enable** command in CSG2 service configuration mode. To restore the default setting, use the **no** form of this command.

aoc enable

no aoc enable

Syntax Description

This command has no arguments or keywords.

Defaults

The CSG2 does not append the original URL to the redirect URL.

Command Modes

CSG2 service configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1.
	Changes from CSG1: The name of this command changed from **authorize content** to **aoc enable**.

Usage Guidelines

This command is not valid if the service is configured with **basis second connect**.

If this command is configured, the CSG2 alerts the quota server of a new transaction, and allows it to direct the CSG2 to perform any of the following mutually exclusive actions:

- **DROP**: Instructs the CSG2 to drop all packets for this flow.
- **FORWARD**: Instructs the CSG2 to forward the flow without altering the destination (a weight might be specified).
- **REDIRECT-URL**: Instructs the CSG2 to redirect subscriber requests to the URL provided by the quota server. The CSG2 sends a Layer 7 redirect to the subscriber (for example, HTTP 302 response) that contains the redirect URL. This applies to both HTTP and WAP 1.x protocols.

Examples

The following example enables AoC URL-rewriting for the CSG2:

```
ip csg service MOVIES
 aoc enable
```

Related Commands

Command	Description
aoc append url	Specifies that the CSG2 is to append the original URL to the redirect URL sent by the quota server for use in Advice of Charge (AoC) URL-rewriting.

Command	Description
aoc confirm	Configures a token for use in Advice of Charge (AoC) URL-rewriting.
ip csg service	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.

basis

To specify the billing basis for a CSG2 content billing service, use the **basis** command in CSG2 service configuration mode. To use the default billing basis, use the **no** form of this command.

basis [**byte** {**ip** | **tcp**} | {**fixed** | **second** [**connect** | **transaction**]}]

no basis [**byte** {**ip** | **tcp**} | {**fixed** | **second** [**connect** | **transaction**]}]

Syntax Description

byte ip	(Optional) Billing charge is a function of the IP data volume processed during the subscriber's session. This is the default setting.
byte tcp	(Optional) Billing charge is a function of the TCP data volume processed during the subscriber's session. **Note** Supplemental usage reporting always reports IP bytes, even if the billing basis is configured for TCP bytes.
fixed	(Optional) Billing charge is a fixed cost, which is deducted each time the first packet for a transaction hits a content-policy pair (that is, deducted for each request).
second	(Optional) Billing charge is duration-based for the CSG2 service. Unless the **connect** keyword is also configured, the billing is for the service duration time.
connect	(Optional) Billing charge is based on connection duration time, not service duration time. **Note** If you specify the **connect** keyword, the **balance** and **consumed** fields in the output of the **show ip csg users** command are updated only when there is a Service Reauthorization Request for new quota.
transaction	(Optional) Billing charge is based on transaction duration time. **Note** The **transaction** keyword is valid for Session Initiation Protocol (SIP) only.

Defaults

The default setting is **byte ip** (billing charge is a function of the IP data volume processed).

Command Modes

CSG2 service configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: The **exclude mms** keyword was removed.
12.4(15)MD	The **transaction** keyword was added.

Usage Guidelines

The **basis** command applies to prepaid and virtual prepaid billing only. It has no impact on postpaid billing.

For TCP billing, configuring **basis byte tcp** allows counting of only TCP payload and exclusion of overhead for network retransmission. With this option, the CSG2 excludes IP and TCP headers from volume counts. The byte counting is limited to TCP payload. Retransmitted packets are not counted.

Services that are configured with the **basis second connect** command (that is, for Connection Duration Billing) are subject to the following restrictions:

- Service verification is not supported for Connection Duration services.
- If redirect is to be performed when the Connection Duration service runs out of quota, the URL location to which the CSG2 redirects must map to a policy that does not have accounting configured. This is because all IP sessions mapped to policies with accounting configured (postpaid or prepaid) are dropped when the Connection Duration service has no quota.

For Service Duration Billing:

- When a Service Duration Billing Service is a member of a billing plan, and an accounting definition is in service and downloaded to a CSG2 module, you cannot modify the basis or meter configuration. You are instructed at the console to configure **no inservice** on the downloaded Accounting definitions.
- If a content configuration is included in a service configured for **basis second**, the CSG2 restricts the content idle timeout to less than or equal to the service idle timeout for the service. The content idle time is not included in the last billable time for the service.
- The CSG2 does not allow you to specify weights for Service Duration Billing.

Note We recommend that you first remove the service from each billing plan, make the basis changes, and add it back to each billing plan. If you delete it, the service is automatically removed from each billing plan, and you must add it back to each plan after configuring it.

To enable Connection Duration Billing for a service, configure the service name as a service under one or more billing plans in CSG2 billing configuration mode, then enter the **basis second connect** command in CSG2 service configuration mode.

Because Internet Message Access Protocol (IMAP) metering is byte-based, you cannot configure both **meter include imap** and **basis fixed** or **basis second** in the same service. Only **basis byte** is meaningful with **meter include imap**.

You cannot configure both **meter exclude svc-idle** and **basis byte** or **basis fixed** in the same service. Only **basis second** is meaningful with **meter exclude svc-idle**.

Examples

The following example shows how to specify fixed billing for the CSG2 service MOVIES:

```
ip csg service MOVIES
 basis fixed
```

The following commands are used to configure Service Duration Billing for the OFF_NET service.

```
ip csg service OFF_NET
 basis second
```

Related Commands

Command	Description
ip csg service	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.
meter exclude svc-idle	Excludes timers from the usage calculation.
meter include imap	Specifies which Internet Message Access Protocol (IMAP) bytes are billed for when doing prepaid debits.
meter increment	Specifies the increments for debiting quota upon completion of a service configured for Service Duration Billing.

block

To force the CSG2 to drop packets that do not match a configured billing policy, use the **block** command in CSG2 content configuration mode. To restore the default behavior, enabling the CSG2 to forward the packets without billing, use the **no** form of this command.

block

no block

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

CSG2 content configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **ip csg block** to **block**. • The configuration mode for this command changed from global to CSG2 content configuration.

Usage Guidelines

By default, if packets do not match any billing policy, the CSG2 forwards the packets without billing. This command causes the CSG2 to drop the packets instead.

Examples

The following example shows how to force the CSG2 to drop packets that do not match any billing policy:

```
ip csg content MOVIES
 block
```

Related Commands

Command	Description
ip csg content	Configures content for CSG2 services, and enters CSG2 content configuration mode.
ip csg policy	Defines a policy for qualifying flows for the CSG2 accounting services, and enters CSG2 policy configuration mode.
parse length	Defines the maximum number of Layer 7 bytes that the CSG2 is to parse when attempting to assign a policy.

class

To specify a service class value, use the **class** command in CSG2 service configuration mode. To remove the service class value, use the **no** form of this command.

class *value*

no class *value*

Syntax Description

value	Specifies a value in the range 1 to 255.

Defaults

None

Command Modes

CSG2 service configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: None.

Usage Guidelines

The **class** command is used with fixed-record format to identify a service class value. This value is opaque to the CSG2 and has meaning only for the administrator. It is reported as tariff-class in fixed-record format call detail records (CDRs).

Examples

The following example specifies a class value for the service:

```
ip csg service FOO
 class 7
```

Related Commands

Command	Description
ip csg service	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.
ip csg transport-type assign	Classifies data traffic on the basis of its access path.
mode	Specifies the mode for a CSG2 billing plan.
ip csg records format	Specifies **variable** or **fixed** CDR format.
owner	Specifies an identifier or name for a service owner.

clear ip csg

To clear the CSG2, use the **clear ip csg** command in privileged EXEC mode.

clear ip csg {counters | sessions user [*application*] [*ip-address ip-mask*] |
user [**all | ip** *ip-address* {**global | vrf** *vrf-name*}]}

Syntax Description

counters	Clears all CSG2 cumulative counters and statistics, but not CSG2 "state" counters. For example, counters such as "current number of sessions" are not cleared.
sessions user	Closes all subscriber sessions.
application	(Optional) Closes subscriber sessions for only the specified application: • **ftp**—Closes FTP subscriber sessions. • **http**—Closes HTTP subscriber sessions. • **imap**—Closes IMAP subscriber sessions. • **other**—Closes other subscriber sessions. • **pop3**—Closes POP3 subscriber sessions. • **rtsp**—Closes RTSP subscriber sessions. • **smtp**—Closes SMTP subscriber sessions. • **wap**—Closes WAP subscriber sessions.
ip-address ip-mask	(Optional) Closes subscriber sessions for only the specified subscriber IP address and subscriber IP address mask. Specify IP address 0.0.0.0 to close subscriber sessions for all subscriber IP addresses. Specify IP address mask 0 to close subscriber sessions for all subscriber IP address masks.
user	Closes all subscriber entries in the CSG2 User Table.
all	(Optional) Closes all subscriber entries in the CSG2 User Table.
ip *ip-address*	(Optional) Closes only those subscriber entries in the CSG2 User Table that are associated with the specified IP address.
global	(Optional) Closes all subscriber entries that are associated with the specified IP address.
vrf *vrf-name*	(Optional) Closes only those subscriber entries that are associated with the specified IP address and that are associated with the specified Virtual Routing and Forwarding (VRF) table. **Note** The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters. The CSG2 does not support the use of the word **forwarding** as a valid VRF name.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(11)MD	This command was introduced.
12.4(15)MD	The **ftp** keyword was added.

Usage Guidelines

By default, the CSG2 deletes 1000 User Table entries per second in response to the **clear ip csg user all** command. To specify a different deletion rate, use the **ip csg radius on-off purge** command in global configuration mode.

Examples

The following example clears all counters and statistics for the CSG2:

```
clear ip csg counters
```

The following example clears all subscriber entries from the CSG2 User Table that are associated with IP address **1.2.3.4**:

```
clear ip csg user ip 1.2.3.4
```

The following example clears all subscriber entries from the CSG2 User Table that are associated with IP address **1.2.3.4** and that are also associated with VRF table **AAA**:

```
clear ip csg user ip 1.2.3.4 vrf AAA
```

The following example clears all sessions for application **http** and IP address mask **1.2.3.4/32**:

```
clear ip csg sessions user http 1.2.3.4/32
```

Related Commands

Command	Description
show ip csg	Displays information about the CSG2.

clear ip iscsi statistics

To clear current iSCSI statistics, use the **clear ip iscsi statistics** command in privileged EXEC configuration mode.

clear ip iscsi statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(15)MD	This command was introduced.

Examples

The following example clears iSCSI-related statistics:

```
clear ip iscsi statistics
```

Related Commands

Command	Description
show ip iscsi	Displays information about the iSCSI.

clear record-storage-module stats

To clear current record storage module (RSM) statistics, use the **clear record-storage-module stats** command in privileged EXEC configuration mode.

clear record-storage-module stats

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(15)MD	This command was introduced.

Examples

The following example clears RSM-related statistics:

```
clear record-storage-module stats
```

Related Commands

Command	Description
show record-storage-module	Displays information about the record storage module (RSM).

client-group (CSG2 content)

To reference a standard access list that is part of a CSG2 content, use the **client-group** command in CSG2 content configuration mode. To delete the reference, use the **no** form of this command.

client-group {*std-access-list-number* | *std-access-list-name*}

no client-group {*std-access-list-number* | *std-access-list-name*}

Syntax Description

std-access-list-number	Standard IP access list number. The ranges are from 1 to 99 and from 1300 to 1999.
std-access-list-name	Standard access list name.

Defaults

All subscribers can access the content.

Command Modes

CSG2 content configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The configuration mode for this command changed from CSG policy configuration to CSG2 content configuration. • The range for the *std-access-list-number* argument increased from 1300 to 1999.

Usage Guidelines

The **client-group** command is used to qualify subscribers for the CSG2 content. The conditions specified in the referenced access list must be true in order for the flows to be processed by the CSG2 content. If the conditions are not true, the CSG2 determines this to be a content mismatch, and normal content match processing continues (that is, the CSG2 tries to match a less specific content). If no contents are matched, the CSG2 does not process the flow (that is, the CSG2 blocks this traffic flow).

If you reference an access list that includes a **deny** statement, and that **deny** statement is matched, then the CSG2 treats the traffic as a content mismatch and normal content processing continues, allowing the traffic to match another less specific content. For example, in the following configuration, packets from from IP address 1.1.1.1 do not match CONTENT1, but they do match CONTENT2:

```
ip csg content CONTENT1
 ip any
 client-group 99
 inservice
!
ip csg content CONTENT2
  ip any
  inservice
!
```

```
access-list 99 deny 1.1.1.1
access-list 99 permit any
```

You can use next-hop with client groups as long as a given client group is always sent to the same next hop. You cannot send a given client group to two or more different next hops based on a content.

The CSG2 searches contents with the same IP and VLAN configuration, but different client groups, in numerical order. For example, given two contents with the same IP/VLAN configuration, one referencing client group 4 and the other client group 7, the CSG2 matches the content that references client group 4.

Examples

The following example shows how to reference client group 44 for the CSG2 content MOVIES:

```
ip csg content MOVIES
 client-group 44
```

Related Commands

Command	Description
ip csg content	Configures content for CSG2 services, and enters CSG2 content configuration mode.
next-hop	Defines a next-hop IP address.

content (CSG2 service)

To configure a content and policy as a member of a CSG2 billing service, and optionally to assign a weight to this content, use the **content** command in CSG2 service configuration mode. To remove a content name from the billing service, use the **no** form of this command.

content *content-name* **policy** *policy-name* [**weight** *weight-value*]

no content *content-name* **policy** *policy-name*

Syntax Description

content-name	Name of the content for this service. The name can be from 1 to 15 characters long, and can include uppercase or lowercase letters (the CSG2 changes all letters to uppercase), numbers, and any special characters.
policy *policy-name*	Name of a configured policy to apply to the content for this service.
weight *weight-value*	(Optional) Number of quadrans to deduct for each transaction. The range is from 0 to 32767. The default *weight-value* is 1 quadran.

Defaults

The default *weight-value* is 1 quadran.

Command Modes

CSG2 service configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1.
	Changes from CSG1: The *weight-name* argument was replaced with the *weight-value* argument.

Usage Guidelines

You must configure a policy before configuring this command.

Content can reference more than one policy. Therefore, you can have multiple **content** commands with the same *content-name* argument, but different *policy-name* arguments.

To make a specific content free, specify a *weight-value* of 0.

Each content billing service is associated with one or more contents and policies.

Multiple services can include the same content/policy pair, as long as the services are not associated with the same billing plan. They cannot be associated with the same billing plan because then the match of content/policy pair to service would not be unique.

Examples

The following example shows how to configure content for the CSG2 service MOVIES. In this example:

- Policy MOVIES_COMEDY is applied to content MOVIES_COMEDY.
- Policy MOVIES_ACTION is applied to content MOVIES_ACTION.
- Content MOVIES_ACTION is given a billing weight of 2.

```
ip csg service MOVIES
 content MOVIES_COMEDY policy MOVIES_COMEDY
 content MOVIES_ACTION policy MOVIES_ACTION weight 2
```

Related Commands

Command	Description
ip csg content	Configures content for CSG2 services, and enters CSG2 content configuration mode.
ip csg policy	Defines a policy for qualifying flows for the CSG2 accounting services, and enters CSG2 policy configuration mode.
ip csg service	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.

debug ip csg

To set the flags to obtain debugging output for the various CSG2 components, use the **debug ip csg** command in privileged EXEC mode. To disable the debugging feature, use the **no** form of this command.

debug ip csg {**all** | **acl** *number* [**vrf** *vrf-name* | **global**] | **configuration sync** | **content** | **crashinfo** | **error** | **frag** | **ftp** | **gtp** {**any** | **bma** [*priority*] | **ipc** | **psd** | **quota-server** [*priority*]} | **http** [**detail**] | **imap** | **interm** | **ipc** [**detail**] | **iscsi** [**detail**] | **other** | **packet** [**dump**] | **policy** | **pop3** | **psd** [**detail**] | **qs** [**detail**] | **radius** [**detail**] | **replicate** | **rtsp** [**detail**] | **service** [**detail** | **ha**] | **session** {**event** | **state** [**detail**]} | **sip** | **smtp** | **stats** | **tlv** | **udb** [**xml**] | **users** | **wap** [**detail**] | **xml**}

no debug ip csg {**all** | **acl** *number* [**vrf** *vrf-name* | **global**] | **configuration sync** | **content** | **crashinfo** | **error** | **frag** | **ftp** | **gtp** {**any** | **bma** [*priority*] | **ipc** | **psd** | **quota-server** [*priority*]} | **http** [**detail**] | **imap** | **interm** | **ipc** [**detail**] | **iscsi** [**detail**] | **other** | **packet** [**dump**] | **policy** | **pop3** | **psd** [**detail**] | **qs** [**detail**] | **radius** [**detail**] | **replicate** | **rtsp** [**detail**] | **service** [**detail** | **ha**] | **session** {**event** | **state** [**detail**]} | **sip** | **smtp** | **stats** | **tlv** | **udb** [**xml**] | **users** | **wap** [**detail**] | **xml**}

Syntax Description

all	Generates debugging output for all CSG2 components.
acl *number*	Generates debugging output for all subscribers in a simple access control list (ACL).
vrf *vrf-name*	(Optional) Generates debugging output for the Virtual Routing and Forwarding (VRF) table with the ACL. **Note** The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters. The CSG2 does not support the use of the word **forwarding** as a valid VRF name.
global	(Optional) Generates debugging output for the default routing table with the ACL.
configuration sync	Generates debugging output for the configuration synchronization component.
content	Generates debugging output for the CSG2 content debug messages, indicating the results of the content match algorithm. This output is filtered if **debug ip csg acl** has been configured.
crashinfo	Generates debugging output for the crash information component.
error	Generates debugging output for situations that might indicate a problem.
frag	Generates debugging output for the CSG2 fragment database.
ftp	Generates debugging output for the FTP component.
gtp any	Generates debugging output for the general packet radio service (GPRS) tunneling protocol (GTP) component's interaction with components other than the Billing Mediation Agent (BMA), the Interprocessor Communication (IPC) component, the Persistent Storage Device (PSD) component, or the quota server.

gtp bma [*priority*]	Generates debugging output for the GTP component's interaction with the BMA. To generate detailed debugging output for the GTP component's interaction with a specific BMA, specify the quota server's *priority*.
gtp ipc	Generates debugging output for the GTP component's interaction with the IPC component.
gtp psd	Generates debugging output for the GTP component's interaction with the PSD component.
gtp quota-server [*priority*]	Generates debugging output for the GTP component's interaction with the quota server. To generate detailed debugging output for the GTP component's interaction with a specific quota server, specify the quota server's *priority*.
http [**detail**]	Generates debugging output for the HTTP component. To generate detailed debugging output for the HTTP component, specify the optional **detail** keyword.
imap	Generates debugging output for the Internet Message Access Protocol (IMAP) component.
interm	Generates debugging output for the intermediate CDR component.
ipc [**detail**]	Generates debugging output for the IPC component. To generate detailed debugging output for the IPC component, specify the optional **detail** keyword.
iscsi [**detail**]	Generates debugging output for the iSCSI component. To generate detailed debugging output for the iSCSI component, specify the optional **detail** keyword.
mail	Generates debugging output for the mail component.
other	Generates debugging output for other components.
packet [**dump**]	Generates debugging output for e-mail packets. To generate a dump of all inbound packets in hexadecimal format, specify the optional **dump** keyword.
policy	Generates debugging output for the policy component.
pop3	Generates debugging output for the Post Office Protocol, version 3 (POP3) component.
psd [**detail**]	Generates debugging output for the PSD component. To generate detailed debugging output for the PSD component, specify the optional **detail** keyword.
qs [**detail**]	Generates debugging output for the quota server component. To generate detailed debugging output for the quota server component, including all packets to and from the quota server in both hexadecimal and ASCII formats, specify the optional **detail** keyword.
radius [**detail**]	Generates debugging output for the RADIUS component. To generate detailed debugging output for the RADIUS component, specify the optional **detail** keyword.

replicate	Generates debugging output for the high availability (HA) component, including stateful messages as well as stateless transitions and the dump/bulk synchronization processes. You can also use the following commands to debug the redundancy facility (RF), the RF for Interdevice redundancy (RF Interdev), and the Hot Standby Router Protocol (HSRP): • **debug redundancy progression** • **debug redundancy interdev** • **debug standby**
service [**detail**]	Generates debugging output for the subscriber services component. To generate detailed debugging output for the subscriber services component, specify the optional **detail** keyword. **Note** If you specify the **detail** keyword, the CSG2 might generate debugging output for every packet mapped to the service.
service [**ha**]	Generates debugging output for the subscriber services component. To generate debugging output for high availability (HA) replication for the subscriber services component, specify the optional **ha** keyword.
session event	Generates debugging output for the session event component.
session state [**detail**]	Generates debugging output for the session state component. To generate detailed debugging output for the session state component, specify the optional **detail** keyword.
rtsp [**detail**]	Generates debugging output for the Real Time Streaming Protocol (RTSP) component. To generate detailed debugging output for the RTSP component, specify the optional **detail** keyword.
sip	Generates debugging output for the Session Initiation Protocol (SIP) component.
smtp	Generates debugging output for the Simple Mail Transfer Protocol (SMTP) component.
stats	Generates debugging output for the statistics component.
tlv	Generates debugging output for the Tag-Length-Values (TLVs) component.
udb [**xml**]	Generates debugging output for the User Database (UDB) component. To generate debugging output for only the XML component, specify the optional **xml** keyword.
users	Generates debugging output for the subscriber component.
wap [**detail**]	Generates debugging output for the wireless application protocol (WAP) component. To generate detailed debugging output for the WAP component, specify the optional **detail** keyword.

Defaults

The CSG2 generates no debugging output.

Command Modes Privileged EXEC

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The **acl** *number*, **configuration sync**, **detail**, **dump**, **error**, **frag**, **global**, **ha**, **http**, **interm**, **ipc**, **mail**, **other**, **packet**, *priority*, **qs**, **replicate**, **service**, **session event**, **session state**, **stats**, and **vrf** *vrf-name*, keywords and arguments were added. • The **any**, **bma**, **ipc**, **psd**, and **quota-server** keywords were added for the **gtp** keyword. • The **agent**, **api**, **cpu**, **module** *number*, **quota**, **prepaid**, **record storage** *slot*, and **timer** keywords and arguments were removed.
12.4(15)MD	The **crashinfo**, **ftp**, **iscsi**, **mail**, and **sip** keywords were added.

Usage Guidelines To see most but not all debugging output, use the **all** option to turn on all debugging flags, and then use the **no** form of this command to exclude debugging output for any options that are not of interest to you.

Restrict the output of other CSG2 debugging commands to subscribers specified in the ACL.

Once the debug flags are set, they are automatically sent to the CSG2 cards when a configuration is downloaded. Similarly, changes in the debug settings are sent to the CSG2 cards that are being debugged.

Generating debugging output for ACL (that is, configuring the **acl** keyword) disables all of the following types of debugging:

- Configuration
- Error
- GTP
- IPC
- PSD
- RADIUS
- Replicate
- Statistics
- TLV
- UDB

You can use the **show debug** command to display the debug flag settings.

Note You must re-enter the **debug** command after every reload because it is not saved in the startup configuration.

Examples The following example shows how to turn on debugging for **rtsp** and **udb**:

```
debug ip csg rtsp
debug ip csg udb
```

entries user idle

To set the time after which entries for idle subscribers are deleted from the CSG2 User Table, use the **entries user idle** command in CSG2 billing configuration mode. To use the default settings, use the **no** form of this command.

entries user idle *duration* [**pod**]

no entries user idle

Syntax Description

idle *duration*	Number of seconds after which entries for idle subscribers are deleted from the CSG2 User Table. The range is from 0 (entries never idle out) to 2147483647. The default setting is 0 (entries never idle out).
pod	(Optional) Specifies whether the CSG2 is to send the RADIUS Packet of Disconnect message when an entry idles out.

Defaults

The default idle duration is 0 seconds, and the CSG2 does not send the RADIUS Packet of Disconnect message when an entry idles out.

Command Modes

CSG2 billing configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1.
	Changes from CSG1: The name of this command changed from **entries idle (CSG2 billing)** to **entries user idle**.

Usage Guidelines

The CSG2 User Table identifies all subscribers known to the CSG2. The table is populated on the basis of the contents of RADIUS Accounting Start messages, or from the user database, if either feature is enabled in your configuration.

When setting the entry idle timer, keep the following considerations in mind:

- You can set the entry idle timer either globally, using the **ip csg entries user idle** command in global configuration mode, or in each billing plan, using the **entries user idle** command. If you do not set the timer in the billing plan, the CSG2 uses the global timer. That is, if there is an entry idle timer value in the billing plan, it is used; otherwise, if there is a global entry idle timer value configured, it is used.
- If set, the idle timer starts when there are no billable sessions, and restarts whenever a RADIUS Accounting Start or an Interim Accounting message is received. The timer stops when a billable session is started.
- If you do not specify the **pod** keyword, the CSG2 deletes the idle entry when the timer expires.
- If you specify the **pod** keyword, and if RADIUS Packet of Disconnect (PoD) is configured for the CSG2, the CSG2 sends a PoD message when the idle timer expires. The CSG2 deletes the idle entry when the PoD message is ACKed, NAKed, or when all retries have been sent.

- If Connection Duration Billing is enabled, you can use either the billing plan entry idle timer or the global entry idle timer to release a subscriber connection.

Examples

The following example shows how to specify an entry idle time of 1 hour for CSG2 billing plan REGULAR:

```
ip csg billing REGULAR
 entries user idle 3600
```

Related Commands

Command	Description
ip csg billing	Defines a CSG2 billing plan, and enters CSG2 billing configuration mode.
ip csg entries user idle	Specifies how long the CSG2 is to retain entries in the CSG2 User Table.
ip csg radius pod attribute	Specifies the RADIUS attributes to be copied from the RADIUS Start message and sent to the NAS in the PoD message.
ip csg radius pod nas	Specifies the NAS port to which the CSG2 is to send the PoD message, and the key to use in calculating the Authenticator.
ip csg radius pod timeout	Specifies the number of times to retry the RADIUS PoD message if it is not acknowledged by means of an ACK message, and the interval between retransmissions.
ip csg radius proxy	Specifies that the CSG2 is to be a proxy for RADIUS messages.
mode	Specifies the mode for a CSG2 billing plan.
service	Associates a service with a CSG2 billing plan.

flags

To specify IP, TCP, or wireless application protocol (WAP) flag bit masks and values for CSG2 Prepaid Error Reimbursement, use the **flags** command in CSG2 refund configuration mode. To remove the flags, use the **no** form of this command.

flags {**ip** *mask* | **tcp** *mask* | **wap**} *value*

no flags {**ip** *mask* | **tcp** *mask* | **wap**} *value*

Syntax Description

ip	All IP protocol connections other than TCP or WAP.
tcp	TCP connections
wap	WAP connections.
mask	The *mask* for an **ip** or **tcp** flag must match that reported to the Billing Mediation Agent (BMA) for connection termination. The range for *mask* is from 0x01 to 0xFF.
value	The *value* for an **ip**, **tcp**, or **wap** flag, which must match that reported to the BMA for connection termination. • For an **ip or tcp** flag, the range for *value* is from 0x00 to 0xFF. • For a **wap** flag, *value* can be 0x00, 0x01, 0x02, or 0x04.

Defaults

None

Command Modes

CSG2 refund configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: None.

Usage Guidelines

The CSG2 supports flag-based refunding for all protocols.

The **ip** flag *values* are:

- 0x01: Connection initiator.
  - 0: The connection was initiated by the subscriber. The source address is associated with the user ID.
  - 1: The connection was initiated by the network. The destination address is associated with the user ID.

- 0x80: Connection terminated because of lack of authorization failure.
  - 0: The connection was not terminated as a result of an authorization failure.
  - 1: The connection was terminated as a result of an authorization failure.
- 0x7E: Reserved.

The **tcp** flag *values* are:

- 0x01: Connection initiator.
  - 0: The connection was initiated by the subscriber. The source address is associated with the user ID.
  - 1: The connection was initiated by the network. The destination address is associated with the user ID.
- 0x02: TCP termination type.
  - 0: Normal TCP termination (FIN or RST).
  - 1: Connection timed out.
- 0x04: Persistent Connection (multiple sequential transactions per TCP connection).
  - 0: The reported connection is not a persistent connection.
  - 1: The reported connection is a persistent connection.
- 0x08: Destination Initiated Close (valid only if TCP termination type is 0).
  - 0: The connection teardown was initiated by the source IP in the flow.
  - 1: The connection teardown was initiated by the destination IP in the flow.
- 0x10: Destination Side FIN (valid only if TCP termination type is 0).
  - 0: The destination side never sent a FIN (it might have sent an RST).
  - 1: The destination side sent a FIN.
- 0x20: Source Side FIN (valid only if TCP termination type is 0).
  - 0: The source side never sent a FIN (it might have sent an RST).
  - 1: The source side sent a FIN.
- 0x40: Connection not closed (valid only for HTTP 1.1).
  - 0: The connection has been closed.
  - 1: The connection is not closed yet, and TCP close bits have no meaning.
- 0x80: Connection terminated because of lack of authorization failure.
  - 0: The connection was not terminated as a result of an authorization failure.
  - 1: The connection was terminated as a result of an authorization failure.

The **wap** flag *values* are:

- 0x00: Normal.
- 0x01: Aborted.
- 0x02: Incomplete.
- 0x04: Forced abort.

Examples

The following example shows how to set flags for IP, TCP, and WAP:

```
ip csg refund COMPANY-REFUND
 flags tcp 43 00
 flags ip 80 80
 flags wap 04
```

Related Commands

Command	Description
ip csg refund	Specifies the CSG2 refund policy to apply to the various services, and enters CSG2 refund configuration mode.
retcode	Specifies the range of application return codes for which the CSG2 refunds quota for Prepaid Error Reimbursement.

idle (CSG2 content)

To specify the minimum amount of time that the CSG2 maintains an idle content connection, use the **idle** command in CSG2 content configuration mode. To restore the default idle duration value, use the **no** form of this command.

idle *duration*

no idle *duration*

Syntax Description

duration	Content idle timer duration in seconds. If no packets are received on a content connection for more than *duration* seconds, the CSG2 assumes the connection is idle and ends the connection. The range is from 4 to 65535. The default is 300.

Defaults

The default idle duration is 300 seconds (5 minutes).

Command Modes

CSG2 content configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: The default setting for the *duration* argument changed from 3600 seconds to 300 seconds.

Usage Guidelines

Real Time Streaming Protocol (RTSP) billing in the CSG2 is based on inspection of the RTSP SETUP and TEARDOWN messages that are exchanged between the subscriber and network. The CSG2 builds the RTSP call detail record (CDR) immediately after the RTSP TEARDOWN signal if the URL exactly matches that from the RTSP SETUP signal. Otherwise, the CSG2 builds the CDR after any condition that causes the flows to be terminated, as when a service_stop is triggered (for example, when the access network sends a RADIUS Accounting Stop for the subscriber).

For RTSP, do not set the idle timer duration to less than 60 seconds.

When using HTTP as the transport for RTSP, the control connection is used sparingly and might time out, causing the stream to become unresponsive. This occurs because the subscriber opens two TCP connections, one for the main content and one for control. The subscriber uses the control connection sparingly, which can cause the connection to time out. To prevent this problem, ensure that the content idle timer has a duration of at least 60 seconds (the default setting is 300 seconds). This is not an issue when using UDP or TCP as the transport.

The CSG2 tracks usage on a per-session basis. User Datagram Protocol (UDP) does not have an end-of-session indicator and simply idles out. For that reason, for UDP and wireless application protocol 1.x (WAP 1.x), setting the content idle timer to a low value (for example, 30) allows the CSG2

to quickly recognize that a session has ended and to generate billing records accordingly. Other service-level features of the CSG2 that count sessions (such as passthrough mode and service-level CDRs) are similarly affected by the content idle timer setting.

For TCP, the CSG2 does not send a reset (RST) until a packet is received.

For a service configured with **basis second**, make sure the idle timeout value for the content configuration, set using the **idle** command in CSG2 content configuration mode, does not exceed the service idle timeout value, set using the **idle** command in CSG2 service configuration mode. Examples of these contents include:

- Non-TCP contents
- TCP contents with policies for HTTP or WAP 2.0 where the subscriber or network does not close the TCP connection at the end of the transaction

Examples

The following example shows how to configure a 120-second idle timer for the CSG2 content MOVIES_COMEDY:

```
ip csg content MOVIES_COMEDY
 idle 120
```

Related Commands

Command	Description
idle (CSG2 service)	Specifies the minimum amount of time that the CSG2 maintains a service with no subscriber sessions.
ip csg content	Configures content for CSG2 services, and enters CSG2 content configuration mode.
pending	Sets the pending connection timeout.

idle (CSG2 service)

To specify the minimum amount of time that the CSG2 maintains a service with no subscriber sessions, use the **idle** command in CSG2 service configuration mode. To restore the default idle duration value, use the **no** form of this command.

idle *duration*

no idle *duration*

Syntax Description

duration	Service idle timer duration, in seconds. The timer begins when there are no sessions. If a subscriber's quota for a service is unused for more than *duration* seconds, the CSG2 assumes that the service is idle and sends a Service Stop to free up the resources. The range is from 1 to 65535. The default is 300.

Defaults

The default idle duration is 300 seconds (5 minutes).

Command Modes

CSG2 service configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: None.

Usage Guidelines

For services configured with **basis second**, make sure the idle timeout value for the content configurations, set using the **idle** command in CSG2 content configuration mode, does not exceed the service idle timeout value, set using the **idle** command in CSG2 service configuration mode. Examples of these contents include:

- Non-TCP contents
- TCP contents with policies for HTTP or WAP 2.0 where the subscriber or network does not close the TCP connection at the end of the transaction

If a subscriber's quota for a service is unused for more than the service idle timer duration, the CSG2 assumes that the service is idle and sends a ServiceStop to free up quota.

For RTSP, do not set the idle timer duration to less than 60 seconds.

Examples

The following example shows how to configure a 120-second idle timer for the CSG2 service MOVIES:

```
ip csg service MOVIES
 idle 120
```

Related Commands

Command	Description
idle (CSG2 content)	Specifies the minimum amount of time that the CSG2 maintains an idle content connection.
ip csg service	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.
pending	Sets the pending connection timeout.

inservice (CSG2 content)

To activate the content service on each CSG2, use the **inservice** command in CSG2 content configuration mode. To suspend the content service, use the **no** form of this command.

inservice

no inservice

Syntax Description

This command has no arguments or keywords.

Defaults

The default value is **no inservice**.

Command Modes

CSG2 content configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: None.

Usage Guidelines

When you activate the **inservice** command, the CSG2 verifies the parameters semantically. If the CSG2 detects an error, the command fails.

If there are sessions on a content, and you take the content out of service (with the **no inservice** command), the CSG2 does not allow the content to be placed back in service (with the **inservice** command) until the sessions have been cleaned up. If you try to enter the **inservice** command before the CSG2 has cleaned up the sessions, the command fails.

Examples

The following example shows how to place the CSG2 content MOVIES_COMEDY in service:

```
ip csg content MOVIES_COMEDY
 inservice
```

Related Commands

Command	Description
ip csg content	Configures content for CSG2 services, and enters CSG2 content configuration mode.

ip (CSG2 content)

To define the subset of Layer 3 and Layer 4 flows that can be processed by the CSG2 accounting services, use the **ip** command in CSG2 content configuration mode. To delete the flow definition, use the **no** form of this command.

ip {**any** | *ip-address* [*netmask*]} [**any** | *protocol* [*port-number* [*last-port-number*]]]

no ip {**any** | *ip-address*}

Syntax Description

any	All Layer 3 and Layer 4 flows can be processed. This is the default setting.
ip-address	IP address for which Layer 3 and Layer 4 flows can be processed.
netmask	(Optional) Mask that identifies the network for which Layer 3 and Layer 4 flows can be processed. You can express the network mask in either IP dotted notation (*n.n.n.n*) or prefix notation (*/nn*, where *nn* is the number of leading 1-bits). For example, 255.255.0.0 and /16 are equivalent network masks. The default network mask is 255.255.255.255 or /32, which means flows to a specific host can be processed.
any	(Optional) All protocol types of Layer 3 and Layer 4 flows can be processed. This is the default setting.
protocol	(Optional) Protocol type of Layer 3 and Layer 4 flows that can be processed: • **any**—Flows of any protocol type can be processed. This is the default setting. • **tcp**—Only TCP flows can be processed. • **udp**—Only User Datagram Protocol (UDP) flows can be processed. • *protocol-number*—Number identifying the protocol whose flows can be processed. The range is from 0 to 255, where 0 means the same as **any**.
port-number	(Optional) Specifies the beginning of the range of port numbers for which Layer 3 and Layer 4 flows can be processed. The range is 0 to 65535, where 0 indicates that flows from any port number can be processed.
last-port-number	(Optional) Specifies the end of the range of port numbers, The range is *port-number* to 65535. If you are specifying a single port number, do not specify *last-port-number*.

Defaults

If you specify an IP address but no network mask, the default network mask is 255.255.255.255 or /32 (flows to a specific host can be processed).

If you do not specify a protocol, flows of any protocol type can be processed.

If you specify a protocol but no port number, the default port number is 0, which means that flows from any port number can be processed.

The CSG2 parses port numbers only when processing TCP and UDP traffic. For all other protocols, the CSG2 does not track the layer 4 port.

Command Modes

CSG2 content configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: None.

Usage Guidelines

This command is required to place content in service.

UDP ports 9200 and 9201 are well-known Wireless Session Protocol (WSP) and Wireless Transaction Protocol (WTP) wireless application protocol (WAP) ports. When a policy with **parse protocol wap** is associated with a content, use even-numbered UDP ports to designate WSP traffic, and use odd-numbered ports to designate WTP traffic.

Although you can use this command to specify a port number for Layer 3 content (**ip any any** *port-number*), the CSG2 does not support Layer 3 content rules. The CSG2 ignores the specified port number, and the **show ip csg content** command displays the port number as 0.

Examples

The following example shows how to specify that, for content MOVIES_COMEDY, only flows for IP address 172.18.45.0/24 and TCP port 8080 are to be processed by the CSG2 accounting services:

```
ip csg content MOVIES_COMEDY
 ip 172.18.45.0/24 tcp 8080
```

Related Commands

Command	Description
ip csg content	Configures content for CSG2 services, and enters CSG2 content configuration mode.

ip (iSCSI)

To specify the IP address of an iSCSI target in the target interface profile on the CSG2, use the **ip** command in iSCSI configuration mode. To remove the IP address configuration, use the **no** form of the command.

ip *ip-address*

no ip *ip-address*

Syntax Description

ip-address	IP address of the iSCSI target.

Command Default

No default behavior or values.

Command Modes

iSCSI configuration

Command History

Release	Modification
12.4(15)MD	This command was introduced.

Usage Guidelines

Only one target can be defined per profile.

Examples

The following example configures an iSCSI target interface profile with the name **targetA** to a SCSI target with the IP address **10.0.0.1**:

```
ip iscsi target-profile targetA
  name iqn.2002-10.edu.abc.iol.iscsi.draft20-target:1
  ip 10.0.0.1
  port 3260
  session-timeout 120
  target-portal 1
```

Related Commands

Command	Description
ip csg iscsi drain delay	Defines the delay interval, in seconds, before draining packets from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) when the Billing Mediation Agent (BMA) becomes active.
ip csg iscsi drain packet	Defines the number of packets to be drained from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) per drain delay interval when the Billing Mediation Agent (BMA) becomes active.

Command	Description
ip csg iscsi profile	Specifies the Internet Small Computer Systems Interface (iSCSI) target to be used as backup storage for the CSG2.
ip iscsi target-profile	Creates an iSCSI profile for an iSCSI target on the CSG2, and enters iSCSI configuration mode.
name (iSCSI)	Specifies the name of an iSCSI target in the target profile on the CSG2
port (iSCSI)	Specifies the number of the port on which to listen for iSCSI traffic in the iSCSI target interface profile on the CSG2.
session-timeout (iSCSI)	Specifies the session timeout for an iSCSI target in the target interface profile on the CSG2.
target-portal (iSCSI)	Specifies the portal group tag for an iSCSI target in the target interface profile on the CSG2.

ip csg billing

To define a CSG2 billing plan, and to enter CSG2 billing configuration mode, use the **ip csg billing** command in global configuration mode. To delete the billing plan, use the **no** form of this command.

ip csg billing *billing-plan-name*

no ip csg billing *billing-plan-name*

Syntax Description

billing-plan-name	Name of the billing plan, which is a set of services. When the CSG2 encounters a new subscriber, the CSG2 retrieves its billing plan. The name can be from 1 to 64 characters long, and can include uppercase or lowercase letters (the CSG2 changes all letters to uppercase), numbers, and any special characters.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: None.

Usage Guidelines

You can define up to 128 billing plans.

The characteristics of each billing plan are defined by the following commands:

- entries user idle
- mode
- service

Examples

The following example shows how to define a CSG2 billing plan named REGULAR:

```
ip csg billing REGULAR
```

Related Commands

Command	Description
entries user idle	Sets the time after which entries for idle subscribers are deleted from the CSG2 User Table.
mode	Specifies the mode for a CSG2 billing plan.
service	Associates a service with a CSG2 billing plan.

ip csg bma

To configure the Billing Mediation Agents (BMAs) to which the CSG2 is to send billing records, use the **ip csg bma** command in CSG2 global configuration mode. To remove a BMA from the list of agents, use the **no** form of this command.

ip csg bma [**vrf** *vrf-name*] *ip-address port-number priority*

no ip csg bma [**vrf** *vrf-name*] *ip-address port-number*

Syntax Description

vrf *vrf-name*	(Optional) Virtual Routing and Forwarding (VRF) table which the CSG2 is to use to communicate with the BMA. **Note** The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters. The CSG2 does not support the use of the word **forwarding** as a valid VRF name.
ip-address	IP address of the BMA you wish to define. When you configure a BMA, make sure that its IP address and port number match on both the active CSG2 and the standby CSG2. You can configure multiple BMAs with the same IP address, but the CSG2 does not support nodealive or redirect for multiple BMAs with the same IP address.
port-number	Port number of the BMA you wish to define. The range is from 1 to 65535. The CSG2 differentiates BMAs on the basis of their port numbers. When you configure a BMA, make sure its port number matches on both the active CSG2 and the standby CSG2.
priority	Priority of the BMA you wish to define. The priority specifies the order of preference of the agents. A lower number indicates a higher priority. If the current agent becomes unusable, the CSG2 uses the highest priority BMA available. Priorities for different agents do not have to be sequential. That is, you can have three agents with priorities 1, 5, and 10. The range of priorities is 1 to 1000.

Defaults

Active and standby BMAs are not defined.
If no VRF table is specified, the CSG2 uses the global routing table to communicate with the BMA.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **agent (CSG2 accounting)** to **ip csg bma**. • The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

You must specify the BMA local port using the **ip csg bma local-port** command before you enter the **ip csg bma** command.

Accounting records are sent only to the agents identified in the **ip csg bma** command. This provides a measure of security to ensure that records are not sent to unauthorized systems.

General packet radio service (GPRS) tunneling protocol (GTP) prime (GTP') does not support nodealive or redirect for multiple agents with the same IP address.

Note The CSG2 does not support multiple BMAs with the same IP address.

Examples

The following example shows how to configure a BMA with priority 10 that uses VRF table BMAVRF:

```
ip csg bma vrf BMAVRF 1.2.3.4 5555 10
```

Related Commands

Command	Description
ip csg bma activate	Enables support for multiple active BMAs.
ip csg bma keepalive	Defines the Billing Mediation Agent (BMA) keepalive time interval for the CSG2.
ip csg bma local-port	Defines the port on which the CSG2 listens for packets from the BMAs.
ip csg bma messages	Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages that the CSG2 can buffer for all Billing Mediation Agents (BMAs).
ip csg bma retransmit	Defines the Billing Mediation Agent (BMA) retransmit time interval for the CSG2.
ip csg bma retries	Defines the maximum number of Billing Mediation Agent (BMA) retries allowed before the CSG2 determines that the link has failed.
ip csg bma window	Defines the Billing Mediation Agent (BMA) transmit window size for the CSG2.

ip csg bma activate

To enable support for multiple active Billing Mediation Agents (BMAs), use the **ip csg bma activate** command in CSG2 global configuration mode. To disable support for multiple active BMAs, use the **no** form of this command.

ip csg bma activate [*number* [**sticky** *seconds*]]

no ip csg bma activate [*number* [**sticky** *seconds*]]

Syntax Description

number	(Optional) Number of BMAs that the CSG2 tries to activate at the same time. If you have defined more BMAs than *number*, and an active BMA fails, the BMA with the highest priority (lowest number) that is not already active is made active. The range is from 1 to 32. The default value is 1.
sticky *seconds*	(Optional) Number of seconds of inactivity after which a sticky object is to be deleted. The CSG2 creates a sticky object to ensure that all the billing records for a subscriber are sent to the same BMA. If the user ID is not available (for example, if the internal table is too small to hold all user ID entries, or if the CSG2 cannot access the user ID database), the CSG2 creates a sticky object for the subscriber IP address. This entry is removed from the table based on inactivity. Entries that contain a user ID do not age out; they are removed only by RADIUS messages. The range is from 1 to 64000. The default value is 30.

Defaults

The default value for *number* is 1.

The default value for *seconds* is 30.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **agent activate** to **ip csg bma activate**. • The range of the *number* argument changed from 1 to 10, to 1 to 32.

Usage Guidelines

Use this command to load-balance CDRs among multiple active BMAs.

When the CSG2 uses multiple active BMAs, it sends all CDRs for a given user to a particular BMA. The CSG2 stores that BMA assignment in the CSG2 User Table entry for that user.

For example, if a configuration has four active BMAs, and one of those BMAs fails, the CSG2 looks for a suitable standby BMA. If the CSG2 finds a suitable standby BMA, it transfers all of the CDRs from the failed BMA to the new BMA, and updates all of the affected User Table entries to reflect the new BMA assignment.

However, if the CSG2 cannot find a suitable standby BMA, it redistributes all of the CDRs from the failed BMA among the remaining three active BMAs. It does so by finding the User Table entries for the affected users in the CDRs. The CSG2 then assigns one of the active BMAs to each affected user, and updates the User Table entries to reflect the new BMA assignments. The CSG2 reassigns all CDRs for a given user to the same BMA.

If the CSG2 cannot find a User Table entry for a user (for example, the user has logged off), it creates a temporary sticky object as a placeholder and assigns a new BMA to the sticky object. This ensures that the remaining CDRs for that user are sent to the same BMA.

Note This command is valid only if your CSG2 uses multiple active BMAs. If your CSG2 uses one and only one active BMA, the default settings are sufficient (that is, **ip csg bma activate 1 sticky 30**).

Examples

The following example shows how to enable support for multiple active BMAs for the CSG2 accounting service A1. In this example, up to two BMAs can be active at the same time, and the CSG2 deletes inactive sticky objects after 60 seconds:

```
ip csg bma activate 2 sticky 60
```

Related Commands

Command	Description
ip csg bma	Defines the Billing Mediation Agents (BMAs) to which the CSG2 is to send billing records
ip csg quota-server activate	Activates one or more quota servers.

ip csg bma keepalive

To define the Billing Mediation Agent (BMA) keepalive time interval for the CSG2, use the **ip csg bma keepalive** command in global configuration mode. To reset the BMA keepalive timer to the default value, use the **no** form of this command.

ip csg bma keepalive *number-of-seconds*

no ip csg bma keepalive

Syntax Description

number-of-seconds	Time, in seconds, between BMA keepalives. The range is 1 to 65535. The default value is 60.

Defaults

The default value is 60 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **keepalive** to **ip csg bma keepalive**. • The configuration mode for this command changed from CSG accounting to global configuration.

Usage Guidelines

We recommend that you change the keepalive time interval only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

Examples

The following example shows how to specify a BMA keepalive time of 300 seconds:

```
ip csg bma keepalive 300
```

Related Commands

Command	Description
ip csg bma	Defines the Billing Mediation Agents (BMAs) to which the CSG2 is to send billing records
ip csg ipc keepalive	Defines the Interprocessor Communication (IPC) keepalive time interval for the CSG2.
ip csg psd keepalive	Defines the Cisco Persistent Storage Device (PSD) keepalive time interval for the CSG2.
ip csg quota-server keepalive	Defines the quota-server keepalive time interval for the CSG2.

ip csg bma local-port

To define the port on which the CSG2 communicates with the Billing Mediation Agent (BMA), use the **ip csg bma local-port** command in CSG2 global configuration mode. To remove the port, use the **no** form of this command.

ip csg bma local-port *port-number*

no ip csg bma local-port

Syntax Description

port-number	Port number on which the BMA will listen. The range is from 1024 to 65535. 5000 is not a valid port number. The BMA local port number must be different from the Persistent Storage Device (PSD) local port number and from the quota server local port number (configured with the **ip csg psd local-port** command and the **ip csg quota-server local-port** command, respectively).

Defaults

No BMA local ports are configured.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: The name of this command changed from **agent local-port** to **ip csg bma local-port**.

Usage Guidelines

You must specify the BMA local port using the **ip csg bma local-port** command before you enter the **ip csg bma** command.

This command accommodates BMAs that configure a port number that is not the general packet radio service (GPRS) tunneling protocol (GTP) prime (GTP') default port (3386).

You must configure a local port to activate BMAs. The local port must be unique with respect to all other configured local ports, such as the quota server local port.

Note The CSG2 drops requests (such as nodealive, echo, and redirect requests) unless they come from a configured BMA IP address. The CSG2 also verifies IP addresses against the configured list of BMAs. If there is no match, the CSG2 drops the request. The CSG2 does not look at a request's source port; instead, the CSG2 replies to the same port from which the request came.

Examples

The following example shows how to specify local port 5555 as the port on which the CSG2 listens for the CSG2 accounting service A1:

```
ip csg bma local-port 5555
```

Related Commands

Command	Description
ip csg bma	Defines the Billing Mediation Agents (BMAs) to which the CSG2 is to send billing records
ip csg psd local-port	Configures the local port on which the CSG2 communicates with the Cisco Persistent Storage Device (PSD).
ip csg quota-server local-port	Configures the local port on which the CSG2 communicates with quota servers.

ip csg bma messages

To specify the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages that the CSG2 can buffer for all Billing Mediation Agents (BMAs), use the **ip csg bma messages** command in global configuration mode. To restore the default setting, use the **no** form of this command.

ip csg bma messages *number*

no ip csg bma messages

Syntax Description

number	Maximum number of GTP' messages that can be buffered for all BMAs. The range is from 1 to 65535. The default is 10000.

Defaults

The CSG2 buffers up to 10000 GTP' messages.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **records max** to **ip csg bma messages**. • The configuration mode for this command changed from CSG accounting to global configuration.

Usage Guidelines

We recommend that you change the number of GTP' messages that can be buffered only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

The CSG2 can buffer GTP' messages in either the Cisco Persistent Storage Device (PSD) or in the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI), as configured. (For more information, see the "Configuring PSD Support" section on page 7-1 and the "Configuring iSCSI Support" section on page 8-1.)

If the BMA GTP' message buffer exceeds 75% of the *number* specified on this command, the CSG2 stops reading GTP' messages from the PSD or SAN. When the buffer drops below the 75% threshold, the CSG2 again begins reading from the PSD or SAN, placing the buffered GTP' messages in the BMA queue. For example, using the default setting for this command of 10,000 messages, the CSG2 can read from the PSD or SAN as long as the buffer contains less than 7,500 GTP' messages—75% of 10,000 messages.

By default, the CSG2 limits the rate at which GTP' messages are read from the PSD to 500 packets/second, and from the SAN to 167 packets/second. However, you can change those default rates. For more information, see the "Configuring the PSD Packet Drain Settings" section on page 7-2 and the "Configuring the iSCSI Packet Drain Settings" section on page 8-4.

Examples

The following example shows how to configure the CSG2 to buffer up to 12345 GTP' messages:

```
ip csg bma messages 12345
```

Related Commands

Command	Description
ip csg bma	Defines the Billing Mediation Agents (BMAs) to which the CSG2 is to send billing records
ip csg iscsi drain delay	Defines the delay interval, in seconds, before draining packets from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) when the Billing Mediation Agent (BMA) becomes active.
ip csg iscsi drain packet	Defines the number of packets to be drained from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) per drain delay interval when the Billing Mediation Agent (BMA) becomes active.
ip csg psd drain delay	Defines the delay interval, in seconds, before draining packets from the Cisco Persistent Storage Device (PSD) when the Billing Mediation Agent (BMA) becomes active.
ip csg psd drain packet	Defines the number of packets to be drained from the Cisco Persistent Storage Device (PSD) per drain delay interval when the Billing Mediation Agent (BMA) becomes active.
ip csg psd margin	Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages, beyond the size of the Billing Mediation Agent (BMA) message queue, that the CSG2 can buffer for the Cisco Persistent Storage Device (PSD).
ip csg quota-server messages	Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages that the CSG2 can buffer for all quota servers.

ip csg bma retransmit

To define the Billing Mediation Agent (BMA) retransmit time interval for the CSG2, use the **ip csg bma retransmit** command in global configuration mode. To reset the BMA retransmit timer to the default value, use the **no** form of this command.

ip csg bma retransmit *number-of-seconds*

no ip csg bma retransmit

Syntax Description

number-of-seconds	Time, in seconds, between BMA retransmits. The range is 2 to 65535. The default value is 4.

Defaults

The default value is 4 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.
12.4(15)MD	The range changed from 1 to 65535 to 2 to 65535.

Usage Guidelines

We recommend that you change the retransmit time interval only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

Examples

The following example shows how to specify a BMA retransmit time of 2 seconds:

```
ip csg bma retransmit 2
```

Related Commands

Command	Description
ip csg bma	Defines the Billing Mediation Agents (BMAs) to which the CSG2 is to send billing records
ip csg ipc retransmit	Defines the Interprocessor Communication (IPC) retransmit time interval for the CSG2.
ip csg psd retransmit	Defines the Cisco Persistent Storage Device (PSD) retransmit time interval for the CSG2.
ip csg quota-server retransmit	Defines the quota server retransmit time interval for the CSG2.

ip csg bma retries

To define the maximum number of Billing Mediation Agent (BMA) retries allowed before the CSG2 determines that the link has failed, use the **ip csg bma retries** command in global configuration mode. To reset the number of BMA retries to the default value, use the **no** form of this command.

ip csg bma retries [**packet**] *number-of-retries*

no ip csg bma retries

Syntax Description

packet	(Optional) Attempt to send a packet to the BMA the specified number of times, then discard the packet.
number-of-retries	Maximum number of BMA retries allowed by the CSG2. The range is 1 to 65535. The default value is 3.

Defaults

The default value is 3 retries.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.
12.4(15)MD	The **packet** keyword was added.

Usage Guidelines

We recommend that you change the number of retries allowed only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

By default, the CSG2 retries a packet forever; it never discards a packet. If you configure the **ip csg bma retries packet** command, the CSG2 tries to send a packet to the BMA the specified number of times, then discards the packet. (The first attempt to send a packet to the BMA is not counted as a retry.) For example, if you configure **ip csg bma retries packet 4**, the CSG2 tries to send a packet to the BMA five times before discarding it (the initial attempt plus four retries).

Examples

The following example shows how to allow two BMA retries:

```
ip csg bma retries 2
```

The following example shows how to allow the CSG2 to try to send a packet to the BMA four times, in addition to the initial attempt:

```
ip csg bma retries packet 4
```

Related Commands

Command	Description
ip csg bma	Defines the Billing Mediation Agents (BMAs) to which the CSG2 is to send billing records
ip csg ipc retries	Defines the maximum number of Interprocessor Communication (IPC) retries allowed before the CSG2 determines that the link has failed.
ip csg psd retries	Defines the maximum number of Cisco Persistent Storage Device (PSD) retries allowed before the CSG2 determines that the link has failed.
ip csg quota-server retries	Defines the maximum number of quota server retries allowed before the CSG2 determines that the link has failed.

ip csg bma window

To define the Billing Mediation Agent (BMA) transmit window size for the CSG2, use the **ip csg bma window** command in global configuration mode. To reset the BMA transmit window size to the default value, use the **no** form of this command.

ip csg bma window {**max** *window-size* | **min** *window-size* | **min auto**}

no ip csg bma window {**max** | **min**}

Syntax Description

max *window-size*	Maximum size, in packets, of the BMA transmit window. The range is 1 to 65535. The default value is 128.
min *window-size*	Minimum size, in packets, of the BMA transmit window. The range is 1 to 65535.
min auto	Specifies that the CSG2 is to determine the minimum size of the BMA transmit window automatically. The CSG2 keeps track of the maximum number of ACKs received in one response and sets that number as the minimum window.

Defaults

The default maximum window size is 128 packets.
The default minimum window size is automatically determined by the CSG2.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

We recommend that you change the transmit window size only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

Examples

The following example shows how to set the maximum BMA transmit window to 64 packets:

```
ip csg bma window max 64
```

Related Commands

Command	Description
ip csg bma	Defines the Billing Mediation Agents (BMAs) to which the CSG2 is to send billing records
ip csg psd window	Defines the Cisco Persistent Storage Device (PSD) transmit window size for the CSG2.
ip csg quota-server window	Defines the quota server transmit window size for the CSG2.

ip csg case-sensitive

To specify whether to treat CSG2 header, method, and URL match patterns as case-sensitive, use the **ip csg case-sensitive** command in global configuration mode. To disable case-sensitivity for CSG2 match patterns, use the **no** form of this command.

ip csg case-sensitive

no ip csg case-sensitive

Syntax Description

This command has no arguments or keywords.

Defaults

CSG2 match patterns are case-sensitive.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Examples

The following example shows how to disable case-sensitivity for CSG2 match patterns:

```
no ip csg case-sensitive
```

Related Commands

Command	Description
match header	Specifies a header match pattern for a CSG2 billing map.
match method	Specifies a method match pattern for a CSG2 billing map.
match url	Specifies a URL match pattern for a CSG2 billing map.

ip csg content

To configure content for CSG2 services, and to enter CSG2 content configuration mode, use the **ip csg content** command in global configuration mode. To delete the content configuration, use the **no** form of this command.

ip csg content *content-name*

no ip csg content ***content-name***

Syntax Description

content-name	Name of the content. The name can be from 1 to 15 characters long, and can include uppercase or lowercase letters (the CSG2 changes all letters to uppercase), numbers, and any special characters.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: None.

Usage Guidelines

You can define up to 2048 contents.

The characteristics of each content configuration are defined by the following commands:

- **block**
- **client-group (CSG2 content)**
- **idle (CSG2 content)**
- **inservice (CSG2 content)**
- **ip (CSG2 content)**
- **mode tcp**
- **next-hop**
- **parse length**
- **parse protocol**
- **pending**
- **policy (CSG2 content)**
- **records delay**
- **records intermediate**
- **replicate**

- **subscriber-ip http-header forwarded-for**
- **vlan (CSG2 content)**
- **vrf**

You cannot change characteristics for a content while it is in service.

In order to determine the service for a subscriber, the CSG2 first matches a content with the first packet in a flow, then matches the policy. The CSG2 then uses the content, policy, and the subscriber's billing plan to determine the service.

If the content configuration does not match any service listed under a subscriber's billing plan, the CSG2 considers the service to be either free or postpaid, and the CSG2 forwards the flow and does not try to authorize the subscriber with the quota server. If BMAs are configured, the CSG2 generates a per-transaction CDR.

The CSG2 supports overlapping contents, as when one content is a subset of another. If one content overlaps another, the CSG2 selects the content that best matches the flow. For example, if you configure Content A with **ip any** and Content B with **ip any tcp 80**, the CSG2 matches TCP port 80 flows to Content B, because **ip any tcp 80** is a more precise match than **ip any**.

The CSG2 does not support duplicate contents. That is, you cannot configure two contents with identical configurations.

Examples

The following example shows how to define the CSG2 content named MOVIES_COMEDY:

```
ip csg content MOVIES_COMEDY
```

Related Commands

Command	Description
block	Forces the CSG2 to drop packets that do not match a configured billing policy.
client-group (CSG2 content)	References a standard access list that is part of a CSG2 content.
idle (CSG2 content)	Specifies the minimum amount of time that the CSG2 maintains an idle content connection.
inservice (CSG2 content)	Activates the content service on each CSG2.
ip (CSG2 content)	Defines the subset of Layer 3 and Layer 4 flows that can be processed by the CSG2 accounting services.
mode tcp	Specifies the mode for CSG2 TCP sessions.
next-hop	Defines a next-hop IP address.
parse length	Defines the maximum number of Layer 7 bytes that the CSG2 is to parse when attempting to assign a policy.
parse protocol	Defines how the CSG2 is to parse traffic for a content.
policy (CSG2 content)	References a CSG2 billing policy.
records delay	Specifies the delay before the CSG2 is to send the HTTP Statistics CDR.
records intermediate	Enables the generation of CSG2 intermediate CDRs.
replicate	Replicates the connection state for all TCP connections to the CSG2 content servers on the standby system.

Command	Description
subscriber-ip http-header forwarded-for	Specifies that the CSG2 is to obtain the subscriber's IP address from the HTTP X-Forwarded-For header.
vlan (CSG2 content)	Restricts the CSG2 billing content to a single source VLAN.
vrf	Restricts the CSG2 content to packets within a single Virtual Routing and Forwarding (VRF) table.

ip csg database

To identify the database server that answers CSG2 user ID queries, use the **ip csg database** command in global configuration mode. To disable the database server, use the **no** form of this command.

ip csg database [**vrf** *vrf-name*] *ip-address port-number local-port*

no ip csg database

Syntax Description

vrf *vrf-name*	(Optional) Specifies the Virtual Routing and Forwarding (VRF) table to be used for communication with the database server. **Note** The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters. The CSG2 does not support the use of the word **forwarding** as a valid VRF name.
ip-address	IP address of the database server that answers user ID queries.
port-number	Port number of the database server that answers user ID queries. The range is from 1 to 65535.
local-port	Local port number that the CSG2 is to use to send queries to the database server. The range is from 1 to 65535.

Defaults

If no VRF table is specified, the CSG2 uses the global routing table to communicate with the database server.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **database** to **ip csg database**. • The configuration mode for this command changed from CSG user group to global configuration. • The **vrf** *vrf-name* and *local-port* keywords and arguments were added.

Usage Guidelines

You can configure one and only one database server to answer CSG2 user ID queries.

The subscriber traffic must flow on an interface in the global routing table (not the VRF table).

Examples

The following example shows how to specify a user database server with IP address 10.1.2.3, port number 11111, and local port number 22222:

```
ip csg database 10.1.2.3 11111 22222
```

ip csg entries fragment

To define the maximum number of entries in the CSG2 fragment database, or to define how long the CSG2 is to retain the entries, use the **ip csg entries fragment** command in global configuration mode. To restore the default settings, use the **no** form of this command.

ip csg entries fragment {**idle** *duration* | **maximum** *entries-number*}

no ip csg entries fragment {**idle** | **max**}

Syntax Description

idle *duration*	Number of seconds after which entries are deleted from the CSG2 fragment database. The range is from 1 to 255. The default setting is 5.
maximum *entries-number*	Maximum number of entries allowed in the CSG2 fragment database. The range is from 1 to 65535. The default number of entries is 16384.

Defaults

The default idle duration is 5 seconds.
The default maximum number of entries is 16384.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

The CSG2 divides the configured maximum number of entries evenly among the traffic processors. For example, if you configure a maximum of 100 entries, the maximum buffer pool size on each traffic processor is 20.

Examples

The following example shows how to specify a maximum CSG2 fragment database size o0f 32,768 entries:

```
ip csg entries fragment maximum 32768
```

Related Commands

Command	Description
ip csg database	Server that answers user ID queries.
ip csg entries user idle	Specifies how long the CSG2 is to retain entries in the CSG2 User Table.
ip csg entries user max	Specifies the maximum number of entries allowed in he CSG2 User Table.

Command	Description
ip csg entries user profile	Specifies the location from which the CSG2 is to obtain the subscriber profile and billing plan when generating entries for the CSG2 User Table.
ip csg entries session user max	Specifies the maximum number of entries allowed in the CSG2 session table.
ip csg psd margin	Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages, beyond the size of the Billing Mediation Agent (BMA) message queue, that the CSG2 can buffer for the Cisco Persistent Storage Device (PSD).
ip csg quota-server messages	Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages that the CSG2 can buffer for all quota servers.

ip csg entries session user max

To specify the maximum number of entries allowed in the CSG2 session table, use the **ip csg entries session user max** command in global configuration mode. To restore the default settings, use the **no** form of this command.

ip csg entries session user max *entries*

no ip csg entries session user max

Syntax Description

entries	Maximum number of entries allowed in the session table. This is the maximum number of sessions that the CSG2 can support. When the number of active sessions reaches the specified maximum, the CSG2 begins dropping incoming new sessions. The range is from 1 to 1800000. The default number of entries is 1000000.

Defaults

The default maximum number of entries is 1000000.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

The maximum number of entries is not enforced on the buffer pool maximum size, it is enforced during allocation of individual subscriber sessions to the table.

Examples

The following example shows how to specify a maximum CSG2 session table size of 100,000 entries:

```
ip csg entries session user max 100000
```

Related Commands

Command	Description
ip csg database	Server that answers user ID queries.
ip csg entries fragment	Defines the maximum number of entries in the CSG2 fragment database, or how long the CSG2 is to retain the entries.
ip csg entries user idle	Specifies how long the CSG2 is to retain entries in the CSG2 User Table.
ip csg entries user max	Specifies the maximum number of entries allowed in he CSG2 User Table.
ip csg entries user profile	Specifies the location from which the CSG2 is to obtain the subscriber profile and billing plan when generating entries for the CSG2 User Table.

Command	Description
ip csg psd margin	Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages, beyond the size of the Billing Mediation Agent (BMA) message queue, that the CSG2 can buffer for the Cisco Persistent Storage Device (PSD).
ip csg quota-server messages	Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages that the CSG2 can buffer for all quota servers.

ip csg entries user idle

To specify how long the CSG2 is to retain entries in the CSG2 User Table, use the **ip csg entries user idle** command in global configuration mode. To restore the default settings, use the **no** form of this command.

ip csg entries user idle *duration* [**pod**]

no ip csg entries user idle

Syntax Description

duration	Number of seconds after which the CSG2 is to delete entries for idle subscribers from the CSG2 User Table. The range is from 0 (entries never idle out) to 2147483647. The default setting is 0.
pod	(Optional) Specifies whether the CSG2 is to send the RADIUS Packet of Disconnect message when an entry idles out.

Defaults

The default idle duration is 0 seconds (entries never idle out), and the CSG2 does not send the RADIUS Packet of Disconnect message when an entry idles out.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

The CSG2 User Table identifies all subscribers known to the CSG2. The table is populated on the basis of the contents of RADIUS Accounting Start messages, or from the user database, if either feature is enabled in your configuration.

When setting the entry idle timer, keep the following considerations in mind:

- You can set the entry idle timer either globally, using the **ip csg entries user idle** command, or in each billing plan, using the **entries user idle** command in CSG2 billing configuration mode. If you do not set the timer in the billing plan, the CSG2 uses the global timer. That is, if there is an entry idle timer value in the billing plan, it is used; otherwise, if there is a global entry idle timer value configured, it is used.
- If set, the idle timer starts when there are no billable sessions, and restarts whenever a RADIUS Accounting Start or an Interim Accounting message is received. The timer stops when a billable session is started.
- If you do not specify the **pod** keyword, the CSG2 deletes the idle entry when the timer expires.
- If you specify the **pod** keyword, and if RADIUS Packet of Disconnect (PoD) is configured for the CSG2, the CSG2 sends a PoD message when the idle timer expires. The CSG2 deletes the idle entry when the PoD message is ACKed, NAKed, or when all retries have been sent.

- If Connection Duration Billing is enabled, you can use either the billing plan entry idle timer or the global entry idle timer to release a subscriber connection.
- The idle timer does not affect sticky user entries.

Examples

The following example shows how to specify a CSG2 User Table entry idle time of 86,400 seconds:

```
ip csg entries user idle 86400
```

Related Commands

Command	Description
entries user idle	Sets the time after which entries for idle subscribers are deleted from the CSG2 User Table.
ip csg database	Server that answers user ID queries.
ip csg entries fragment	Defines the maximum number of entries in the CSG2 fragment database, or how long the CSG2 is to retain the entries.
ip csg entries user max	Specifies the maximum number of entries allowed in he CSG2 User Table.
ip csg entries user profile	Specifies the location from which the CSG2 is to obtain the subscriber profile and billing plan when generating entries for the CSG2 User Table.
ip csg entries session user max	Specifies the maximum number of entries allowed in the CSG2 session table.
ip csg psd margin	Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages, beyond the size of the Billing Mediation Agent (BMA) message queue, that the CSG2 can buffer for the Cisco Persistent Storage Device (PSD).
ip csg quota-server messages	Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages that the CSG2 can buffer for all quota servers.

ip csg entries user max

To specify the maximum number of entries allowed in the CSG2 User Table, use the **ip csg entries user max** command in global configuration mode. To restore the default settings, use the **no** form of this command.

ip csg entries user max *entries*

no ip csg entries user max

Syntax Description

entries	Maximum number of entries allowed in the CSG2 User Table. • For the 2 GB-SAMI option, the range is from 1 to 1250000. The default number of entries is 300000. • For the 1 GB-SAMI option, the range is from 1 to 500000. The default number of entries is 300000. The actual number of entries in the CSG2 User Table depends on several variables, including the traffic model being used and the number of RADIUS attributes reported. Even if you set entries-number to a very large number, such as 300000, the CSG2 might never store that many entries in the CSG2 User Table.

Defaults

The default maximum number of entries is 300000 for both the 1 GB-SAMI and the 2 GB-SAMI options.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.
12.4(15)MD	The range was changed to reflect the differences between the 2 GB-SAMI and 1 GB-SAMI options: • For the 2 GB-SAMI option, the range is from 1 to 1250000. • For the 1 GB-SAMI option, the range is from 1 to 500000.

Usage Guidelines

The maximum number of entries is not enforced on the buffer pool maximum size, it is enforced during allocation of individual entries to the CSG2 User Table.

Examples

The following example shows how to specify a maximum CSG2 User Table size of 500000 entries:

```
ip csg entries user max 500000
```

Related Commands

Command	Description
ip csg database	Server that answers user ID queries.
ip csg entries fragment	Defines the maximum number of entries in the CSG2 fragment database, or how long the CSG2 is to retain the entries.
ip csg entries user idle	Specifies how long the CSG2 is to retain entries in the CSG2 User Table.
ip csg entries user profile	Specifies the location from which the CSG2 is to obtain the subscriber profile and billing plan when generating entries for the CSG2 User Table.
ip csg entries session user max	Specifies the maximum number of entries allowed in the CSG2 session table.
ip csg psd margin	Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages, beyond the size of the Billing Mediation Agent (BMA) message queue, that the CSG2 can buffer for the Cisco Persistent Storage Device (PSD).
ip csg quota-server messages	Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages that the CSG2 can buffer for all quota servers.

ip csg entries user profile

To specify the location from which the CSG2 is to obtain the subscriber profile and billing plan when generating entries for the CSG2 User Table, use the **ip csg entries user profile** command in global configuration mode. To restore the default settings, use the **no** form of this command.

ip csg entries user profile {**quota-server** | **radius** {**pass** | **remove** | **timeout** *timeout*}}

no ip csg entries user profile

Syntax Description

quota-server	The CSG2 obtains the subscriber profile and billing plan from the quota server.
radius	The CSG2 obtains the Cisco vendor-specific attribute (VSA) subattribute 1, which contains the billing plan name, from the RADIUS Access-Accept and RADIUS Accounting-Request messages.
pass	Does not remove the VSA containing the billing plan from the RADIUS Access-Accept message.
remove	Removes the VSA containing the billing plan from the RADIUS Access-Accept message.
timeout *timeout*	Number of seconds to retain cached billing plan data while waiting for a RADIUS Accounting Start message for a user. The range is from 10 to 65535 seconds. The default timeout is 20 seconds.

Defaults

If you do not specify the **ip csg entries user profile** command, the CSG2 obtains the subscriber profile and billing plan from the quota server.
If you do not specify a timeout, the default timeout is 20 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **user-profile server** to **ip csg entries user profile**. • The configuration mode for this command changed from CSG user group to global configuration.
12.4(15)MD	The **timeout** keyword and *timeout* argument were added.

Usage Guidelines

Keep the following considerations in mind:

- The VSA is removed from the RADIUS Access-Accept message only if **remove** is specified. Use the **remove** argument only if the RADIUS client cannot accept the Cisco VSA in the message.
- We recommend that you use **pass** to reduce processing time on the CSG2.
- The user ID must be included in the message that contains the billing plan.

The CSG2 obtains billing plan data from authentication, authorization, and accounting (AAA) RADIUS Access response packets.

- When the CSG2 receives a RADIUS Access response for a user, it caches the billing plan data for that user.
- When the CSG2 receives a RADIUS Accounting Start message from a Network Access Server (NAS) for that same user, it frees the cached billing plan data.
- If the cache timeout expires before the CSG2 receives the RADIUS Accounting Start message, the CSG2 frees the cached billing plan data. If the RADIUS Accounting Start message arrives after the cached billing plan data has been freed, the CSG2 creates the user with an unknown billing plan and sends a User Authorization Request to the quota server.

In most cases, the default timeout of 20 seconds is far greater than the delay between the receipt of the RADIUS Access response and the receipt of the RADIUS Accounting Start message. If the default timeout is not large enough, you can use the **ip csg entries user profile timeout** *timeout* command to increase the timeout.

Examples

The following example shows how to specify that the CSG2 is to obtain billing plan names from the RADIUS Access-Accept and RADIUS Accounting-Request messages, and that the CSG2 is not to remove the VSA containing the billing plan from the messages:

```
ip csg entries user profile radius pass
```

Related Commands

Command	Description
ip csg database	Server that answers user ID queries.
ip csg entries fragment	Defines the maximum number of entries in the CSG2 fragment database, or how long the CSG2 is to retain the entries.
ip csg entries user idle	Specifies how long the CSG2 is to retain entries in the CSG2 User Table.
ip csg entries user max	Specifies the maximum number of entries allowed in he CSG2 User Table.
ip csg entries session user max	Specifies the maximum number of entries allowed in the CSG2 session table.
ip csg psd margin	Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages, beyond the size of the Billing Mediation Agent (BMA) message queue, that the CSG2 can buffer for the Cisco Persistent Storage Device (PSD).
ip csg quota-server messages	Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages that the CSG2 can buffer for all quota servers.
ip csg radius userid	Specifies the RADIUS attribute used to extract the user identifier from a RADIUS record.

ip csg ipc crashdump

To define the action to be taken by the CSG2 if an Interprocessor Communication (IPC) link fails, use the **ip csg ipc crashdump** command in global configuration mode. To restore the default setting, use the **no** form of this command.

ip csg ipc crashdump [**never** | **tolerance** [*number-of-seconds*]]

no ip csg ipc crashdump

Syntax Description

never	(Optional) Never generate a crash dump in an IPC link fails. This is the default setting.
tolerance *number-of-seconds*	(Optional) Time, in seconds, that the CSG2 is to wait after an IPC link fails before generating a crash dump. The range is 60 to 600. The default value is 60.

Defaults

The default setting is to never generate a crash dump.
If you specify the tolerance keyword without specifying a time, the CSG2 generates a crash dump 60 seconds after an IPC link fails.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

We recommend that you change the crash dump setting only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

Examples

The following example shows how to specify that the CSG2 is to generate a crash dump 120 seconds after an IPC link fails:

```
ip csg ipc crashdump tolerance 120
```

ip csg ipc keepalive

To define the Interprocessor Communication (IPC) module keepalive time interval for the CSG2, use the **ip csg ipc keepalive** command in global configuration mode. To reset the IPC keepalive timer to the default value, use the **no** form of this command.

ip csg ipc keepalive *number-of-seconds*

no ip csg ipc keepalive

Syntax Description

number-of-seconds	Time, in seconds, between IPC keepalives. The range is 1 to 65535. The default value is 8.

Defaults

The default value is 8 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

We recommend that you change the keepalive time interval only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

Examples

The following example shows how to specify an IPC keepalive time of 300 seconds:

```
ip csg ipc keepalive 300
```

Related Commands

Command	Description
ip csg bma keepalive	Defines the Billing Mediation Agent (BMA) keepalive time interval for the CSG2.
ip csg psd keepalive	Defines the Cisco Persistent Storage Device (PSD) keepalive time interval for the CSG2.
ip csg quota-server keepalive	Defines the quota-server keepalive time interval for the CSG2.

ip csg ipc retransmit

To define the Interprocessor Communication (IPC) retransmit time interval for the CSG2, use the **ip csg ipc retransmit** command in global configuration mode. To reset the IPC retransmit timer to the default value, use the **no** form of this command.

ip csg ipc retransmit *number-of-seconds*

no ip csg ipc retransmit

Syntax Description

number-of-seconds	Time, in seconds, between IPC retransmits. The range is 1 to 65535. The default value is 4.

Defaults

The default value is 4 second.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

We recommend that you change the retransmit time interval only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

Examples

The following example shows how to specify an IPC retransmit time of 2 seconds:

```
ip csg ipc retransmit 2
```

Related Commands

Command	Description
ip csg bma retransmit	Defines the Billing Mediation Agent (BMA) retransmit time interval for the CSG2.
ip csg psd retransmit	Defines the Cisco Persistent Storage Device (PSD) retransmit time interval for the CSG2.
ip csg quota-server retransmit	Defines the quota server retransmit time interval for the CSG2.

ip csg ipc retries

To define the maximum number of Interprocessor Communication (IPC) retries allowed before the CSG2 determines that the link has failed, use the **ip csg ipc retries** command in global configuration mode. To reset the number of IPC retries to the default value, use the **no** form of this command.

ip csg ipc retries *number-of-retries*

no ip csg ipc retries

Syntax Description

number-of-retries	Maximum number of IPC retries allowed by the CSG2. The range is 1 to 65535. The default value is 20.

Defaults

The default value is 20 retries.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

We recommend that you change the number of retries allowed only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

Examples

The following example shows how to allow two IPC retries:

```
ip csg ipc retries 2
```

Related Commands

Command	Description
ip csg bma retries	Defines the maximum number of Billing Mediation Agent (BMA) retries allowed before the CSG2 determines that the link has failed.
ip csg psd retries	Defines the maximum number of Cisco Persistent Storage Device (PSD) retries allowed before the CSG2 determines that the link has failed.
ip csg quota-server retries	Defines the maximum number of quota server retries allowed before the CSG2 determines that the link has failed.

ip csg iscsi drain delay

To define the delay interval, in seconds, before draining packets from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) when the Billing Mediation Agent (BMA) becomes active, use the **ip csg iscsi drain delay** command in global configuration mode. To delete the drain delay interval, use the **no** form of this command.

ip csg iscsi drain delay *number-of-seconds*

no ip csg iscsi drain delay

Syntax Description

number-of-seconds	Delay interval, in seconds, before draining packets from the SAN. The range is 0 to 3. The default value is 1. A value of 0 means no delay.

Defaults

The default value is 1 second.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)MD	This command was introduced.

Usage Guidelines

The CSG2 can buffer GTP' messages in the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI), if so configured. (For more information, see the "Configuring iSCSI Support" section on page 8-1.) By default, the CSG2 limits the rate at which GTP' messages are read from the SAN to 167 packets/second (500 packets/3 seconds). However, you can use the **ip csg iscsi drain delay** command to change that rate. For example, specifying an interval of 2 seconds yields a rate of 250 packets/second (500 packets/2 seconds).

Examples

The following example shows how to specify a SAN drain delay interval of 2 seconds:

```
ip csg iscsi drain delay 2
```

Related Commands

Command	Description
ip csg iscsi drain packet	Defines the number of packets to be drained from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) per drain delay interval when the Billing Mediation Agent (BMA) becomes active.
ip csg iscsi profile	Specifies the Internet Small Computer Systems Interface (iSCSI) target to be used as backup storage for the CSG2.
ip iscsi target-profile	Creates an iSCSI profile for an iSCSI target on the CSG2, and enters iSCSI configuration mode.

ip csg iscsi drain packet

To define the number of packets to be drained from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) per drain delay interval when the Billing Mediation Agent (BMA) becomes active, use the **ip csg iscsi drain packet** command in global configuration mode. To delete the drain packet, use the **no** form of this command.

ip csg iscsi drain packet *number-of-packets*

no ip csg iscsi drain packet

Syntax Description

number-of-packets	Number of packets to be drained from the SAN per drain delay interval. The range is from 1 to 64000. The default is 500.

Defaults

The default value is 500 packets.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)MD	This command was introduced.

Usage Guidelines

The CSG2 can buffer GTP' messages in the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI), if so configured. (For more information, see the "Configuring iSCSI Support" section on page 8-1.) By default, the CSG2 limits the rate at which GTP' messages are read from the SAN to 167 packets/second (500 packets/3 seconds). However, you can use the **ip csg iscsi drain packet** command to change that rate. For example, specifying that 600 packets are to be drained per interval yields a rate of 200 packets/second (600 packets/3 seconds).

Examples

The following example shows how to specify that 1000 packets are to be drained from the SAN per drain delay interval:

```
ip csg iscsi drain packet 1000
```

Related Commands

Command	Description
ip csg iscsi drain delay	Defines the delay interval, in seconds, before draining packets from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) when the Billing Mediation Agent (BMA) becomes active.

Command	Description
ip csg iscsi profile	Specifies the Internet Small Computer Systems Interface (iSCSI) target to be used as backup storage for the CSG2.
ip iscsi target-profile	Creates an iSCSI profile for an iSCSI target on the CSG2, and enters iSCSI configuration mode.

ip csg iscsi profile

To specify the Internet Small Computer Systems Interface (iSCSI) target to be used as backup storage for the CSG2, use the **ip csg iscsi profile** command in global configuration mode. To delete the iSCSI target, use the **no** form of this command.

ip csg iscsi profile *target-profile-name*

no ip csg iscsi profile

Syntax Description

target-profile-name	Name of the iSCSI target profile to be used as backup storage.

Defaults

No iSCSI target is specified.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)MD	This command was introduced.

Usage Guidelines

You can associate one and only one iSCSI target profile with each CSG2.

Examples

The following example shows how to specify CSG_BACKUP as the iSCSI target:

```
ip csg iscsi profile CSG_BACKUP
```

Related Commands

Command	Description
ip csg iscsi drain delay	Defines the delay interval, in seconds, before draining packets from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) when the Billing Mediation Agent (BMA) becomes active.
ip csg iscsi drain packet	Defines the number of packets to be drained from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) per drain delay interval when the Billing Mediation Agent (BMA) becomes active.
ip iscsi target-profile	Creates an iSCSI profile for an iSCSI target on the CSG2, and enters iSCSI configuration mode.

ip csg map

To define the CSG2 billing content filters (header, method, and URL maps), and to enter CSG2 map configuration mode, use the **ip csg map** command in global configuration mode. To turn off the service, use the **no** form of this command.

ip csg map *map-name*

no ip csg map *map-name*

Syntax Description

map-name	Name of the map. The name can be from 1 to 15 characters long, and can include uppercase or lowercase letters (the CSG2 changes all letters to uppercase), numbers, and any special characters.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1.
	Changes from CSG1: The **header** and **url** keywords were removed.

Usage Guidelines

The CSG2 maps are used to match headers, methods, or URLs against a pattern to determine whether flows are to be processed by the CSG2 accounting services.

The headers, methods, or URLs that are to be matched against a pattern are defined by the following commands:

- **match header**
- **match method**
- **match url**

When configuring a map, keep the following considerations in mind:

- We recommend that you configure the URL match pattern during your maintenance window, or during off-peak hours.
- You cannot specify different types of match patterns in a given map. For example, a map can include one or more **match header** statements, but it cannot include both **match header** statements and **match url** statements.
- You can specify up to three maps in a given policy: one for header matching, one for method matching, and one for URL matching. For example, the following is a valid configuration:

```
ip csg map HOSTMAP
 match header host1 value *.2.*.44
!
```

```
ip csg map URLMAP
 match url */mobile/index.wml
!
ip csg policy MAP-POLICY
 map HOSTMAP
 map URLMAP
```

In this example, a flow must match both HOSTMAP and URLMAP in order to match policy MAP-POLICY.

Examples

The following example shows how to configure a CSG2 URL map named MOVIES:

```
ip csg map MOVIES
 match url *.movies_(comedy|action|drama).com/*.mpeg
```

Related Commands

Command	Description
ip csg case-sensitive	Specifies whether to treat CSG2 sticky objects and header, method, and URL match patterns as case-sensitive.
ip csg policy	Defines a policy for qualifying flows for the CSG2 accounting services, and enters CSG2 policy configuration mode,.
map	References a header, method, or URL map that is part of a CSG2 billing policy.
match header	Specifies a header match pattern for a CSG2 billing map.
match method	Specifies a method match pattern for a CSG2 billing map.
match url	Specifies a URL match pattern for a CSG2 billing map.

ip csg mode single-tp

To enable the CSG2 to use a single traffic processor (TP) instead of multiple TPs, use the **ip csg mode single-tp** command in global configuration mode. To restore the default setting, use the **no** form of this command.

ip csg mode single-tp

no ip csg mode single-tp

Syntax Description

This command has no arguments or keywords.

Defaults

The CSG2 operates in multiple-TP mode.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

In normal multiple-TP mode, the CSG2 distributes subscriber traffic among all of the TPs, based on each subscriber's IP address. In single-TP mode, the CSG2 dispatches traffic for all subscribers to the first TP to be processed.

Single-TP mode is required for HTTP X-Forwarded-For operation. Before configuring the CSG2 for X-Forwarded-For operation, configure the CSG2 for single-TP mode by entering the **ip csg mode single-tp** command, then performing a **write memory**, then restarting the CSG2.

To switch out of single-TP mode, enter the **no ip csg mode single-tp** command, then perform a **write memory**, then restart the CSG2.

If you intend to operate in single-TP mode, the **ip csg mode single-tp** command must be the first command in your CSG2 configuration.

Examples

The following example shows how to configure single-TP mode for the CSG2:

```
ip csg mode single-tp
```

Related Commands

Command	Description
subscriber-ip http-header forwarded-for	Specifies that the CSG2 is to obtain the subscriber's IP address from the HTTP X-Forwarded-For header.

ip csg policy

To define a policy for qualifying flows for the CSG2 billing services, and to enter CSG2 policy configuration mode, use the **ip csg policy** command in global configuration mode. To turn off the service, use the **no** form of this command.

ip csg policy *policy-name*

no ip csg policy *policy-name*

Syntax Description

policy-name	Name of a policy that applies to the content for this service. The name can be from 1 to 15 characters long, and can include uppercase or lowercase letters (the CSG2 changes all letters to uppercase), numbers, and any special characters.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: None.

Usage Guidelines

Because of limitations on the number of URL match patterns that the CSG2 can handle, do not define more than 16,000 policies. For more information on URL match patterns, see the description of the **match url** command.

The characteristics of each policy are defined by the following commands:

- **accounting**
- **map**

When configuring a map, keep the following considerations in mind:

- You cannot specify different types of match patterns in a given map. For example, a map can include one or more **match header** statements, but it cannot include both **match header** statements and **match url** statements.
- You can specify up to three maps in a given policy: one for header matching, one for method matching, and one for URL matching. For example, the following is a valid configuration:

```
ip csg map HOSTMAP
 match header host1 value *.2.*.44
!
ip csg map URLMAP
 match url */mobile/index.wml
!
```

```
ip csg policy MAP-POLICY
 map HOSTMAP
 map URLMAP
```

In this example, a flow must match both HOSTMAP and URLMAP in order to match policy MAP-POLICY.

Examples

The following example shows how to configure a CSG2 policy named MOVIES_COMEDY:

```
ip csg policy MOVIES_COMEDY
```

Related Commands

Command	Description
accounting	Specifies accounting and an optional customer string for a CSG2 policy.
ip csg content	Configures content for CSG2 services, and enters CSG2 content configuration mode.
ip csg map	Defines the CSG2 billing content filters (header, method, and URL maps), and enters CSG2 map configuration mode.
ip csg service	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.
map	References a header, method, or URL map that is part of a CSG2 billing policy.
match header	Specifies a header match pattern for a CSG2 billing map.
match method	Specifies a method match pattern for a CSG2 billing map.
match url	Specifies a URL match pattern for a CSG2 billing map.

ip csg psd

To configure a Cisco Persistent Storage Device (PSD), use the **ip csg psd** command in global configuration mode. To remove the PSD, use the **no** form of this command.

ip csg psd [**vrf** *vrf-name*] *ip-address port-number*

no ip csg psd [**vrf** *vrf-name*] *ip-address port-number*

Syntax Description

vrf *vrf-name*	(Optional) Virtual Routing and Forwarding (VRF) table which the CSG2 is to use to communicate with the PSD. **Note** The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters. The CSG2 does not support the use of the word **forwarding** as a valid VRF name.
ip-address	IP address for packets destined for the PSD. The CSG2 differentiates PSDs on the basis of their IP addresses. When you configure a PSD, make sure that its IP address matches on both the active CSG2 and the standby CSG2.
port-number	Port number for packets destined for the PSD. The CSG2 differentiates PSDs on the basis of their port numbers. When you configure a PSD, make sure that its port number matches on both the active CSG2 and the standby CSG2.

Defaults

No PSDs are configured.
If no VRF table is specified, the CSG2 uses the global routing table to communicate with the PSD.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **records-storage** to **ip csg psd**. • The configuration mode for this command changed from CSG accounting configuration to global configuration. • The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

You must specify the PSD local port using the **ip csg psd local-port** command before you enter the **ip csg psd** command.

Note You can configure one and only one PSD for each CSG2.

Examples

The following example configures a PSD with IP address 1.2.3.4 and port number 7777, that uses VRF table PSDVRF to communicate with the CSG2:

```
ip csg psd vrf PSDVRF 1.2.3.4 7777
```

Related Commands

Command	Description
ip csg psd drain delay	Defines the delay interval, in seconds, before draining packets from the Cisco Persistent Storage Device (PSD) when the Billing Mediation Agent (BMA) becomes active.
ip csg psd drain packet	Defines the number of packets to be drained from the Cisco Persistent Storage Device (PSD) per drain delay interval when the Billing Mediation Agent (BMA) becomes active.
ip csg psd keepalive	Defines the Cisco Persistent Storage Device (PSD) keepalive time interval for the CSG2.
ip csg psd local-port	Configures the local port on which the CSG2 communicates with the Cisco Persistent Storage Device (PSD).
ip csg psd margin	Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages, beyond the size of the Billing Mediation Agent (BMA) message queue, that the CSG2 can buffer for the Cisco Persistent Storage Device (PSD).
ip csg psd margin	Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages, beyond the size of the Billing Mediation Agent (BMA) message queue, that the CSG2 can buffer for the Cisco Persistent Storage Device (PSD).
ip csg psd retransmit	Defines the Cisco Persistent Storage Device (PSD) retransmit time interval for the CSG2.
ip csg psd retries	Defines the maximum number of Cisco Persistent Storage Device (PSD) retries allowed before the CSG2 determines that the link has failed.
ip csg psd window	Defines the Cisco Persistent Storage Device (PSD) transmit window size for the CSG2.

ip csg psd drain delay

To define the delay interval, in seconds, before draining packets from the Cisco Persistent Storage Device (PSD) when the Billing Mediation Agent (BMA) becomes active, use the **ip csg psd drain delay** command in global configuration mode. To delete the drain delay interval, use the **no** form of this command.

ip csg psd drain delay *number-of-seconds*

no ip csg psd drain delay

Syntax Description

number-of-seconds	Delay interval, in seconds, before draining packets from the PSD. The range is 0 to 3. The default value is 1. A value of 0 means no delay.

Defaults

The default value is 1 second.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

The CSG2 can buffer GTP' messages in the Cisco Persistent Storage Device (PSD), if so configured. (For more information, see the "Configuring PSD Support" section on page 7-1.) By default, the CSG2 limits the rate at which GTP' messages are read from the PSD to 500 packets/second. However, you can use the **ip csg psd drain delay** command to change that rate. For example, specifying an interval of 2 seconds yields a rate of 250 packets/second (500 packets/2 seconds).

Examples

The following example shows how to specify a PSD drain delay interval of 2 seconds:

```
ip csg psd drain delay 2
```

Related Commands

Command	Description
ip csg psd	Configures a Cisco Persistent Storage Device (PSD).
ip csg psd drain packet	Defines the number of packets to be drained from the Cisco Persistent Storage Device (PSD) per drain delay interval when the Billing Mediation Agent (BMA) becomes active.

ip csg psd drain packet

To define the number of packets to be drained from the Cisco Persistent Storage Device (PSD) per drain delay interval when the Billing Mediation Agent (BMA) becomes active, use the **ip csg psd drain packet** command in global configuration mode. To delete the drain packet, use the **no** form of this command.

ip csg psd drain packet *number-of-packets*

no ip csg psd drain packet

Syntax Description

number-of-packets	Number of packets to be drained from the PSD per drain delay interval. The range is from 1 to 64000. The default is 500.

Defaults

The default value is 500 packets.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

The CSG2 can buffer GTP' messages in the Cisco Persistent Storage Device (PSD), if so configured. (For more information, see the "Configuring PSD Support" section on page 7-1.) By default, the CSG2 limits the rate at which GTP' messages are read from the PSD to 500 packets/second. However, you can use the **ip csg psd drain packet** command to change that rate. For example, specifying that 1000 packets are to be drained per interval yields a rate of 1000 packets/second (1000 packets/1 second).

Examples

The following example shows how to specify that 1000 packets are to be drained from the PSD per drain delay interval:

```
ip csg psd drain packet 1000
```

Related Commands

Command	Description
ip csg psd	Configures a Cisco Persistent Storage Device (PSD).
ip csg psd drain delay	Defines the delay interval, in seconds, before draining packets from the Cisco Persistent Storage Device (PSD) when the Billing Mediation Agent (BMA) becomes active.

ip csg psd keepalive

To define the Cisco Persistent Storage Device (PSD) keepalive time interval for the CSG2, use the **ip csg psd keepalive** command in global configuration mode. To reset the PSD keepalive timer to the default value, use the **no** form of this command.

ip csg psd keepalive *number-of-seconds*

no ip csg psd keepalive

Syntax Description

number-of-seconds	Time, in seconds, between PSD keepalives. The range is from 1 to 65535. The default value is 60.

Defaults

The default value is 60 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

We recommend that you change the keepalive time interval only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

Examples

The following example shows how to specify a PSD keepalive time of 300 seconds:

```
ip csg psd keepalive 300
```

Related Commands

Command	Description
ip csg bma keepalive	Defines the Billing Mediation Agent (BMA) keepalive time interval for the CSG2.
ip csg ipc keepalive	Defines the Interprocessor Communication (IPC) keepalive time interval for the CSG2.
ip csg psd	Configures a Cisco Persistent Storage Device (PSD).
ip csg quota-server keepalive	Defines the quota-server keepalive time interval for the CSG2.

ip csg psd local-port

To configure the local port on which the CSG2 communicates with the Cisco Persistent Storage Device (PSD), use the **ip csg psd local-port** command in global configuration mode. To remove a quota server local port configuration, use the **no** form of this command.

ip csg psd local-port *port-number*

no ip csg psd local-port

Syntax Description

port-number	Port number on which the CSG2 is to communicate with the PSD. The range is from 1024 to 65535. 5000 is not a valid port number. The PSD local port number must be different from the Billing Mediation Agent (BMA) local port number and from the quota server local port number (configured with the **ip csg bma local-port** command and the **ip csg quota-server local-port** command, respectively).

Defaults

No PSD local port is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **records-storage local-port** to **ip csg psd local-port**. • The configuration mode for this command changed from CSG accounting configuration to global configuration.

Usage Guidelines

You must specify the PSD local port using the **ip csg psd local-port** command before you enter the **ip csg psd** command.

Note You can configure one and only one PSD for each CSG2.

Examples

The following example configures a PSD with local port number 7777:

```
ip csg psd local-port 7777
```

Related Commands

Command	Description
ip csg bma local-port	Configures the local port on which the CSG2 communicates with the Billing Mediation Agent (BMA).
ip csg psd	Configures a Cisco Persistent Storage Device (PSD).
ip csg quota-server local-port	Configures the local port on which the CSG2 communicates with quota servers.

ip csg psd margin

To specify the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages, beyond the size of the Billing Mediation Agent (BMA) message queue, that the CSG2 can buffer for the Cisco Persistent Storage Device (PSD), use the **ip csg psd margin** command in global configuration mode. To restore the default setting, use the **no** form of this command.

ip csg psd margin *number*

no ip csg psd margin

Syntax Description

number	Maximum number of GTP' messages, beyond the size of the BMA message queue, that can be buffered for the PSD. The range is from 100 to 65535. The default is 2000.

Defaults

The CSG2 buffers up to 2000 GTP' messages, beyond the size of the BMA message queue.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

We recommend that you change the number of GTP' messages that can be buffered only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

Examples

The following example shows how to configure the CSG2 to buffer up to 3000 GTP' messages, beyond the size of the BMA message queue:

```
ip csg psd margin 2000
```

Related Commands

Command	Description
ip csg bma messages	Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages that the CSG2 can buffer for all Billing Mediation Agents (BMAs).
ip csg psd	Configures a Cisco Persistent Storage Device (PSD).

ip csg psd retransmit

To define the Cisco Persistent Storage Device (PSD) retransmit time interval for the CSG2, use the **ip csg psd retransmit** command in global configuration mode. To reset the PSD retransmit timer to the default value, use the **no** form of this command.

ip csg psd retransmit *number-of-seconds*

no ip csg psd retransmit

Syntax Description

number-of-seconds	Time, in seconds, between PSD retransmits. The range is 1 to 65535. The default value is 4.

Defaults

The default value is 4 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

We recommend that you change the retransmit time interval only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

Examples

The following example shows how to specify a PSD retransmit time of 2 seconds:

```
ip csg psd retransmit 2
```

Related Commands

Command	Description
ip csg bma retransmit	Defines the Billing Mediation Agent (BMA) retransmit time interval for the CSG2.
ip csg ipc retransmit	Defines the Interprocessor Communication (IPC) retransmit time interval for the CSG2.
ip csg psd	Configures a Cisco Persistent Storage Device (PSD).
ip csg quota-server retransmit	Defines the quota server retransmit time interval for the CSG2.

ip csg psd retries

To define the maximum number of Cisco Persistent Storage Device (PSD) retries allowed before the CSG2 determines that the link has failed, use the **ip csg psd retries** command in global configuration mode. To reset the number of PSD retries to the default value, use the **no** form of this command.

ip csg psd retries [**packet**] *number-of-retries*

no ip csg psd retries

Syntax Description

packet	(Optional) Attempt to send a packet to the PSD the specified number of times, then discard the packet.
number-of-retries	Maximum number of PSD retries allowed by the CSG2. The range is 1 to 65535. The default value is 3.

Defaults

The default value is 3 retries.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.
12.4(15)MD	The **packet** keyword was added.

Usage Guidelines

We recommend that you change the number of retries allowed only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

By default, the CSG2 retries a packet forever; it never discards a packet. If you configure the **ip csg psd retries packet** command, the CSG2 tries to send a packet to the PSD the specified number of times, then discards the packet. (The first attempt to send a packet to the PSD is not counted as a retry.) For example, if you configure **ip csg psd retries packet 4**, the CSG2 tries to send a packet to the PSD five times before discarding it (the initial attempt plus four retries).

Examples

The following example shows how to allow two PSD retries:

```
ip csg psd retries 2
```

The following example shows how to allow the CSG2 to try to send a packet to the PSD four times, in addition to the initial attempt:

```
ip csg psd retries packet 4
```

Related Commands

Command	Description
ip csg bma retries	Defines the maximum number of Billing Mediation Agent (BMA) retries allowed before the CSG2 determines that the link has failed.
ip csg ipc retries	Defines the maximum number of Interprocessor Communication (IPC) retries allowed before the CSG2 determines that the link has failed.
ip csg psd	Configures a Cisco Persistent Storage Device (PSD).
ip csg quota-server retries	Defines the maximum number of Billing Mediation Agent (BMA) retries allowed before the CSG2 determines that the link has failed.

ip csg psd window

To define the Cisco Persistent Storage Device (PSD) transmit window size for the CSG2, use the **ip csg psd window** command in global configuration mode. To reset the PSD transmit window size to the default value, use the **no** form of this command.

ip csg psd window {**max** *window-size* | **min** *window-size* | **min auto**}

no ip csg psd window {**max** | **min**}

Syntax Description

max *window-size*	Maximum size, in packets, of the PSD transmit window. The range is 1 to 65535. The default value is 128.
min *window-size*	Minimum size, in packets, of the PSD transmit window. The range is 1 to 65535.
min auto	Specifies that the CSG2 is to determine the minimum size of the PSD transmit window automatically. The CSG2 keeps track of the maximum number of ACKs received in one response and sets that number as the minimum window.

Defaults

The default maximum window size is 128 packets.
The default minimum window size is automatically determined by the CSG2.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

We recommend that you change the transmit window size only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

Examples

The following example shows how to set the maximum PSD transmit window to 64 packets:

```
ip csg psd window max 64
```

Related Commands

Command	Description
ip csg bma window	Defines the Billing Mediation Agent (BMA) transmit window size for the CSG2.
ip csg psd	Configures a Cisco Persistent Storage Device (PSD).
ip csg quota-server window	Defines the quota server transmit window size for the CSG2.

ip csg quota-server

To configure the CSG2 quota servers that return billing quota values for subscribers, use the **ip csg quota-server** command in global configuration mode. To remove a quota server configuration, use the **no** form of this command.

ip csg quota-server [**vrf** *vrf-name*] *ip-address port-number priority*

no ip csg quota-server [**vrf** *vrf-name*] *ip-address port-number*

Syntax Description

vrf *vrf-name*	(Optional) Virtual Routing and Forwarding (VRF) table which the CSG2 is to use to communicate with the quota server. **Note** The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters. The CSG2 does not support the use of the word **forwarding** as a valid VRF name.
ip-address	IP address of the quota server. When you configure a quota server, make sure that its IP address and port number match on both the active CSG2 and the standby CSG2. You can configure multiple quota servers with the same IP address, but the CSG2 does not support nodealive or redirect for multiple quota servers with the same IP address. You can configure up to 10 quota servers. Each quota server must have a unique IP address (or a unique IP address-VRF name combination, if VRF is configured).
port-number	Port number of the quota server. The range is from 1 to 65535. The CSG2 differentiates quota servers on the basis of their port numbers. When you configure a quota server, make sure that its port number matches on both the active CSG2 and the standby CSG2.
priority	Defines active and standby quota servers. The priority specifies the order of preference of the quota servers. A lower number indicates a higher priority. If the current quota server becomes unusable, the CSG2 uses the highest priority quota server available. The range of priorities is from 1 to 1000, but you can configure only up to 10 quota servers. Each quota server must be configured with a unique priority. Priorities for different quota servers do not have to be sequential. That is, you can have three quota servers with priorities 1, 5, and 10, respectively.

Defaults

No quota servers are configured.
If no VRF table is specified, the CSG2 uses the global routing table to communicate with the quota server.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **quota server** to **ip csg quota-server**. • The configuration mode for this command changed from CSG user group configuration to global configuration. • The **vrf** *vrf-name* keyword and argument were added. • The **reassign** keyword was removed.

Usage Guidelines

For prepaid billing, you must configure at least one quota server.

You can configure up to 10 quota servers. Each quota server must have a unique priority and a unique IP address (or a unique IP address-VRF name combination, if VRF is configured).

Note The CSG2 does not support multiple quota servers that have the same IP address.

A quota server can recognize a duplicate quota-download request, as when general packet radio service (GPRS) tunneling protocol (GTP) retransmits a packet. When the quota server detects a duplicate quota-download request, it resends the same quota that it sent for the original request.

To disable quota server reassignment (that is, to prevent the CSG2 from assigning a new quota server to a subscriber if the original quota server fails), use the **no** form of the **ip csg quota-server reassign** command.

Examples

The following example configures a quota server with IP address 1.2.3.4, port number 6666, and priority 10, that uses VRF table QSVRF to communicate with the CSG2:

```
ip csg quota-server vrf QSVRF 1.2.3.4 6666 10
```

Related Commands

Command	Description
ip csg quota-server activate	Activates one or more quota servers.
ip csg quota-server keepalive	Defines the quota server keepalive time interval for the CSG2.
ip csg quota-server local-port	Configures the local port on which the CSG2 communicates with quota servers.
ip csg quota-server messages	Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages that the CSG2 can buffer for all quota servers.
ip csg quota-server reassign	Reassigns subscribers to a different CSG2 quota server after a failure.
ip csg quota-server retransmit	Defines the quota server retransmit time interval for the CSG2.

Command	Description
ip csg quota-server retries	Defines the maximum number of quota server retries allowed before the CSG2 determines that the link has failed.
ip csg quota-server window	Defines the quota server transmit window size for the CSG2.

ip csg quota-server activate

To activate one or more quota servers, use the **ip csg quota-server activate** command in global configuration mode. To deactivate quota servers, use the **no** form of this command.

ip csg quota-server activate *number*

no ip csg quota-server activate

Syntax Description

number	Number of quota servers to activate. The range is from 1 to 32. The default value is 1.

Defaults

The default value is 1.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **quota activate** to **ip csg quota-server activate**. • The configuration mode for this command changed from CSG user group configuration to global configuration. • The range for the *number* argument changed from 1 to 10, to 1 to 32.

Usage Guidelines

Use this command to load-balance quota transactions among multiple active quota servers.

When the CSG2 uses multiple active quota servers, it sends all quota transactions for a given user to a particular quota server. The CSG2 stores that quota server assignment in the CSG2 User Table entry for that user.

For example, if a configuration has four active quota servers, and one of those quota servers fails, the CSG2 looks for a suitable standby quota server. If the CSG2 finds a suitable standby quota server, it transfers all of the quota transactions from the failed quota server to the new quota server, and updates all of the affected User Table entries to reflect the new quota server assignment.

However, if the CSG2 cannot find a suitable standby quota server, it redistributes all of the quota transactions from the failed quota server among the remaining three active quota servers. It does so by finding the User Table entries for the affected users in the quota transactions. The CSG2 then assigns one of the active quota servers to each affected user, and updates the User Table entries to reflect the new quota server assignments. The CSG2 reassigns all quota transactions for a given user to the same quota server.

If the CSG2 cannot find a User Table entry for a user (for example, the user has logged off), it creates a temporary sticky object as a placeholder and assigns a new quota server to the sticky object. This ensures that the remaining quota transactions for that user are sent to the same quota server.

Note This command is valid only if your CSG2 uses multiple active quota servers. If your CSG2 uses one and only one active quota server, the default settings are sufficient (that is, **ip csg quota-server activate 1 sticky 30**).

Examples

The following example shows how to activate two quota servers:

```
ip csg quota-server activate 2
```

Related Commands

Command	Description
ip csg bma activate	Enables support for multiple active Billing Mediation Agents (BMAs)
ip csg quota-server	Configures the CSG2 quota servers that return billing quota values for subscribers.

ip csg quota-server keepalive

To define the quota server keepalive time interval for the CSG2, use the **ip csg quota-server keepalive** command in global configuration mode. To reset the quota server keepalive timer to the default value, use the **no** form of this command.

ip csg quota-server keepalive *number-of-seconds*

no ip csg quota-server keepalive

Syntax Description

number-of-seconds	Time, in seconds, between quota server keepalives. The range is 1 to 65535. The default value is 60.

Defaults

The default value is 60 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

We recommend that you change the keepalive time interval only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

Examples

The following example shows how to specify a quota server keepalive time of 300 seconds:

```
ip csg quota-server keepalive 300
```

Related Commands

Command	Description
ip csg bma keepalive	Defines the Billing Mediation Agent (BMA) keepalive time interval for the CSG2.
ip csg ipc keepalive	Defines the Interprocessor Communication (IPC) keepalive time interval for the CSG2.
ip csg psd keepalive	Defines the Cisco Persistent Storage Device (PSD) keepalive time interval for the CSG2.
ip csg quota-server	Configures the CSG2 quota servers that return billing quota values for subscribers.

ip csg quota-server local-port

To configure the local port on which the CSG2 communicates with quota servers, use the **ip csg quota-server local-port** command in global configuration mode. To remove a quota server local port configuration, use the **no** form of this command.

ip csg quota-server local-port *port-number*

no ip csg quota-server local-port

Syntax Description

port-number	Port number on which the CSG2 is to communicate with quota servers. The range is from 1024 to 65535. 5000 is not a valid port number. The quota server local port number must be different from the Billing Mediation Agent (BMA) local port number and from the Persistent Storage Device (PSD) local port number (configured with the **ip csg bma local-port** command and the **ip csg psd local-port** command, respectively).

Defaults

No quota server local ports are configured.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **quota local-port** to **ip csg quota-server local-port**. • The configuration mode for this command changed from CSG user group configuration to global configuration. • The range for the *port-number* argument changed from 1 to 65535, to 1024 to 65535.

Usage Guidelines

For prepaid billing, you must configure a quota server local port.

Note The CSG2 drops requests (such as nodealive, echo, and redirect requests) unless they come from a configured quota server IP address. The CSG2 also verifies IP addresses against the configured list of quota servers. If there is no match, the CSG2 drops the request. The CSG2 does not look at a request's source port; the CSG2 replies to the port from which the request came.

Examples

The following example configures quota server local port 6666:

```
ip csg quota-server local-port 6666
```

Related Commands

Command	Description
ip csg bma local-port	Configures the local port on which the CSG2 communicates with the Billing Mediation Agent (BMA).
ip csg psd local-port	Configures the local port on which the CSG2 communicates with the Cisco Persistent Storage Device (PSD).
ip csg quota-server	Configures the CSG2 quota servers that return billing quota values for subscribers.

ip csg quota-server messages

To specify the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages that the CSG2 can buffer for all quota servers, use the **ip csg quota-server messages** command in global configuration mode. To restore the default settings, use the **no** form of this command.

ip csg quota-server messages *number*

no ip csg quota-server messages

Syntax Description

number	Maximum number of GTP' messages that can be buffered for all quota servers. The range is from 1 to 65535. The default is 10000.

Defaults

The CSG2 buffers up to 10000 GTP' messages.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

We recommend that you change the number of GTP' messages that can be buffered only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

Examples

The following example shows how to configure the CSG2 to buffer up to 12345 GTP' messages:

```
ip csg quota-server messages 12345
```

Related Commands

Command	Description
ip csg bma messages	Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages that the CSG2 can buffer for all Billing Mediation Agents (BMAs).
ip csg psd margin	Specifies the maximum number of general packet radio service (GPRS) tunneling protocol prime (GTP') messages, beyond the size of the Billing Mediation Agent (BMA) message queue, that the CSG2 can buffer for the Cisco Persistent Storage Device (PSD).
ip csg quota-server	Configures the CSG2 quota servers that return billing quota values for subscribers.

ip csg quota-server reassign

To reassign subscribers to a different CSG2 quota server after a failure, use the **ip csg quota-server reassign** command in global configuration mode. To disable quota server reassignment for subscribers, use the **no** form of this command.

ip csg quota-server reassign

no ip csg quota-server reassign

Syntax Description

This command has no arguments or keywords.

Defaults

Subscribers are reassigned to a different quota server after a failure.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Examples

The following example reassigns subscribers after a quota server failure:

```
ip csg quota-server reassign
```

Related Commands

Command	Description
ip csg quota-server	Configures the CSG2 quota servers that return billing quota values for subscribers.

ip csg quota-server retransmit

To define the quota server retransmit time interval for the CSG2, use the **ip csg quota-server retransmit** command in global configuration mode. To reset the quota server retransmit timer to the default value, use the **no** form of this command.

ip csg quota-server retransmit *number-of-seconds*

no ip csg quota-server retransmit

Syntax Description

number-of-seconds	Time, in seconds, between quota server retransmits. The range is 1 to 65535. The default value is 4.

Defaults

The default value is 4 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

We recommend that you change the retransmit time interval only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

Examples

The following example shows how to specify a quota server retransmit time of 2 seconds:

```
ip csg quota-server retransmit 2
```

Related Commands

Command	Description
ip csg bma retransmit	Defines the Billing Mediation Agent (BMA) retransmit time interval for the CSG2.
ip csg ipc retransmit	Defines the Interprocessor Communication (IPC) retransmit time interval for the CSG2.
ip csg psd retransmit	Defines the Cisco Persistent Storage Device (PSD) retransmit time interval for the CSG2.
ip csg quota-server	Configures the CSG2 quota servers that return billing quota values for subscribers.

ip csg quota-server retries

To define the maximum number of quota server retries allowed before the CSG2 determines that the link has failed, use the **ip csg quota-server retries** command in global configuration mode. To reset the number of quota server retries to the default value, use the **no** form of this command.

ip csg quota-server retries [**packet**] *number-of-retries*

no ip csg quota-server retries

Syntax Description

packet	(Optional) Attempt to send a packet to the quota server the specified number of times, then discard the packet.
number-of-retries	Maximum number of quota server retries allowed by the CSG2. The range is 1 to 65535. The default value is 3.

Defaults

The default value is 3 retries.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.
12.4(15)MD	The **packet** keyword was added.

Usage Guidelines

We recommend that you change the number of retries allowed only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

By default, the CSG2 retries a packet forever; it never discards a packet. If you configure the **ip csg quota-server retries packet** command, the CSG2 tries to send a packet to the quota server the specified number of times, then discards the packet. (The first attempt to send a packet to the quota server is not counted as a retry.) For example, if you configure **ip csg quota-server retries packet 4**, the CSG2 tries to send a packet to the quota server five times before discarding it (the initial attempt plus four retries).

Examples

The following example shows how to allow two quota server retries:

```
ip csg quota-server retries 2
```

The following example shows how to allow the CSG2 to try to send a packet to the quota server four times, in addition to the initial attempt:

```
ip csg quota-server retries packet 4
```

Related Commands

Command	Description
ip csg bma retries	Defines the maximum number of Billing Mediation Agent (BMA) retries allowed before the CSG2 determines that the link has failed.
ip csg ipc retries	Defines the maximum number of Interprocessor Communication (IPC) retries allowed before the CSG2 determines that the link has failed.
ip csg psd retries	Defines the maximum number of Cisco Persistent Storage Device (PSD) retries allowed before the CSG2 determines that the link has failed.
ip csg quota-server	Configures the CSG2 quota servers that return billing quota values for subscribers.

ip csg quota-server window

To define the quota server transmit window size for the CSG2, use the **ip csg quota-server window** command in global configuration mode. To reset the quota server transmit window size to the default value, use the **no** form of this command.

ip csg quota-server window {**max** *window-size* | **min** *window-size* | **min auto**}

no ip csg quota-server window {**max** | **min**}

Syntax Description

max *window-size*	Maximum size, in packets, of the quota server transmit window. The range is 1 to 65535. The default value is 128.
min *window-size*	Minimum size, in packets, of the quota server transmit window. The range is 1 to 65535.
min auto	Specifies that the CSG2 is to determine the minimum size of the quota server transmit window automatically. The CSG2 keeps track of the maximum number of ACKs received in one response and sets that number as the minimum window.

Defaults

The default maximum window size is 128 packets.
The default minimum window size is automatically determined by the CSG2.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

We recommend that you change the transmit window size only when directed to do so by Cisco Technical Assistance Center (TAC) engineers. In most environments, the default value is the most appropriate setting.

Examples

The following example shows how to set the maximum quota server transmit window to 64 packets:

```
ip csg quota-server window max 64
```

Related Commands

Command	Description
ip csg bma window	Defines the Billing Mediation Agent (BMA) transmit window size for the CSG2.

Command	Description
ip csg psd window	Defines the Cisco Persistent Storage Device (PSD) transmit window size for the CSG2.
ip csg quota-server	Configures the CSG2 quota servers that return billing quota values for subscribers.

ip csg radius ack error parse

To enable the CSG2 to generate a RADIUS response to a RADIUS Accounting Start Request or a RADIUS Accounting Interim Request when it encounters a RADIUS parse error condition, use the **ip csg radius ack error parse** command in global configuration mode. To prevent RADIUS responses to errors, use the **no** form of this command.

ip csg radius ack error parse

no ip csg radius ack error parse

Syntax Description

This command has no arguments or keywords.

Defaults

The CSG2 generates a RADIUS response to a RADIUS Accounting Start Request or a RADIUS Accounting Interim Request when it encounters a RADIUS parse error condition.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The **radius ack error** command split into two new commands—**ip csg radius ack error parse** and **ip csg radius ack error user**. • The configuration mode for this command changed from CSG user group configuration to global configuration.

Usage Guidelines

Use the **no** form of this command, **no ip csg radius ack error parse**, to prevent the CSG2 from acknowledging the following RADIUS parse errors:

- Invalid RADIUS message or attribute length
- RADIUS Authenticator does not match what the CSG2 calculates
- Incorrect RADIUS attribute length
- User profile information such as billing plan or quota server does not match the CSG2 configuration

Examples

The following example shows how to prevent RADIUS responses when RADIUS parse errors are encountered.

```
no ip csg radius ack error parse
```

Related Commands

Command	Description
ip csg radius ack error user	Enables the CSG2 to generate a RADIUS response to a RADIUS Accounting Start Request or a RADIUS Accounting Interim Request when it encounters a user resource error condition.
ip csg radius endpoint	Identifies the CSG2 as an endpoint for RADIUS Accounting messages.
ip csg radius handoff	Configures RADIUS handoff support.
ip csg radius proxy	Specifies that the CSG2 is to be a proxy for RADIUS messages.
ip csg radius start restart session-id	Deletes an existing CSG2 User Table entry for a specific subscriber, and creates a new entry for that subscriber.
ip csg radius stop purge	Specifies the attribute that must be included in the RADIUS Accounting Stop request in order for the CSG2 User Table entry to be deleted.

ip csg radius ack error user

To enable the CSG2 to generate a RADIUS response to a RADIUS Accounting Start Request or a RADIUS Accounting Interim Request when it encounters a user resource error condition, use the **ip csg radius ack error user** command in global configuration mode. To prevent RADIUS responses to errors, use the **no** form of this command.

ip csg radius ack error user

no ip csg radius ack error user

Syntax Description

This command has no arguments or keywords.

Defaults

The CSG2 generates a RADIUS response to a RADIUS Accounting Start Request or a RADIUS Accounting Interim Request when it encounters a user resource error condition.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The **radius ack error** command split into two new commands—**ip csg radius ack error parse** and **ip csg radius ack error user**. • The configuration mode for this command changed from CSG user group configuration to global configuration.

Usage Guidelines

Use the **no** form of this command, **no ip csg radius ack error user**, to prevent the CSG2 from acknowledging the following user resource errors:

- Maximum number of users reached
- Unable to allocate memory for creating a user entry or for storing RADIUS attribute information (such as report attributes or parsed billing plan information)
- Unable to communicate user information via inter-processor communication
- Load manager prevents allocation of a user

Examples

The following example shows how to prevent RADIUS responses when user resource errors are encountered.

```
no ip csg radius ack error user
```

Related Commands

Command	Description
ip csg radius ack error parse	Enables the CSG2 to generate a RADIUS response to a RADIUS Accounting Start Request or a RADIUS Accounting Interim Request when it encounters a RADIUS parse error condition.
ip csg radius endpoint	Identifies the CSG2 as an endpoint for RADIUS Accounting messages.
ip csg radius handoff	Configures RADIUS handoff support.
ip csg radius proxy	Specifies that the CSG2 is to be a proxy for RADIUS messages.
ip csg radius start restart session-id	Deletes an existing CSG2 User Table entry for a specific subscriber, and creates a new entry for that subscriber.
ip csg radius stop purge	Specifies the attribute that must be included in the RADIUS Accounting Stop request in order for the CSG2 User Table entry to be deleted.

ip csg radius correlation

To enable RADIUS correlation processing by the CSG2, use the **ip csg radius correlation** command in global configuration mode. To disable RADIUS correlation processing, use the **no** form of this command.

ip csg radius correlation

no ip csg radius correlation

Syntax Description

This command has no arguments or keywords.

Defaults

The CSG2 does not perform RADIUS correlation processing.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

A retransmitted RADIUS Stop might cause the CSG2 to remove a subscriber entry from the CSG2 User Table when the entry should not be removed.

To avoid this problem, the CSG2 must be able to associate a session correlator from the RADIUS Start message with a subscriber entry in the User Table, and compare that correlator with the correlator in the RADIUS Stop message. If the correlators match, the CSG2 deletes the subscriber entry; otherwise, the CSG2 retains the entry in the User Table.

The CSG2 can use the Acct-Session-Id (attribute 44) as the correlator, or it can use the following vendor-specific attribute (VSA) subattribute (attribute 26, Vendor-Id 9, subattribute 1):

csg:user_session_correlator=<string>

If both attributes are included in the RADIUS Start or RADIUS Stop message, the CSG2 uses the VSA subattribute.

To enable this capability, enter the **ip csg radius correlation** command.

- If there is no correlator saved in the User Table entry, the CSG2 deletes the entry.
- If there is a correlator saved in the User Table entry, the CSG2 compares it to the correlator in the RADIUS Stop. If the correlators match, the CSG2 deletes the entry; if they do not match, or if there is no correlator in the RADIUS Stop, the CSG2 retains the entry in the User Table.

To disable this capability, enter the **no ip csg radius correlation** command. The CSG2 deletes User Table entries without subscriber session correlation.

Examples

The following example shows how to enable RADIUS correlation processing by the CSG2.

```
ip csg radius correlation
```

Related Commands

Command	Description
ip csg radius handoff	Configures RADIUS handoff support.
ip csg radius start restart session-id	Deletes an existing CSG2 User Table entry for a specific subscriber, and creates a new entry for that subscriber.
ip csg radius stop purge	Specifies the attribute that must be included in the RADIUS Accounting Stop request in order for the CSG2 User Table entry to be deleted.
replicate	Replicates the connection state for all connections to the CSG2 content servers on the standby system.

ip csg radius endpoint

To identify the CSG2 as an endpoint for RADIUS Accounting messages, use the **ip csg radius endpoint** command in global configuration mode. To remove the endpoint identification, use the **no** form of this command.

ip csg radius endpoint [**vrf** *csg-vrf-name*] ***csg-address*** **key** [*encrypt*] *secret-string* [**vrf** *sub-vrf-name*]

no ip csg radius endpoint [**vrf** *csg-vrf-name*] ***csg-address***

Syntax Description

vrf *csg-vrf-name*	(Optional) Virtual Routing and Forwarding (VRF) table which the CSG2 IP address is to use for RADIUS communication. **Note** The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters. The CSG2 does not support the use of the word **forwarding** as a valid VRF name.
csg-address	Specifies the CSG2 IP address. The CSG2 IP address must be a virtual IP address, and it must be unique (or the IP address-VRF name combination must be unique, if VRF is configured). The CSG2 IP address (or the IP address-VRF name combination) must not be specified in other CSG2 commands, and it must not match any real IP address, virtual IP address, or alias IP address (or IP address-VRF name combination) configured on the CSG2. If you want the CSG2 RADIUS endpoint IP address to be a member of a CSG2 interface subnet, you must configure the CSG2 IP address as follows: • In non-redundant configurations, you must configure the CSG2 IP address as a secondary IP address configured on the appropriate interface. • In redundant configurations, you must configure the CSG2 IP address as a standby secondary IP address on the appropriate interface. **Note** The CSG2 performs radius endpoint processing only on User Datagram Protocol (UDP) traffic that is destined for the server IP address. The server IP address cannot be used for any other UDP communication with the CSG2.
key	Specifies a RADIUS key.

encrypt	(Optional) Indicates how the *secret-string* is represented when the configuration is displayed (for example, **show run**), or how it is written to nonvolatile memory (for example, **write memory**). The valid values are: • **0**—The *secret-string* is stored in plain text. This is the default setting. • **7**—The *secret-string* is encrypted before it is displayed or written to nonvolatile memory. **Note** If your router is configured to encrypt all passwords, then the password is represented as 7 followed by the encrypted text. See the Cisco IOS **service** command for more details.
secret-string	1- to 64-character clear password value for MD5 authentication. All characters are valid; case is significant. The *secret-string* is always sent in plain text to the CSG2 module when the configuration is downloaded. The *secret-string* must match the secret that is specified on the RADIUS client (for example, the gateway general packet radio service [GPRS] support node [GGSN]).
vrf *sub-vrf-name*	(Optional) Virtual Routing and Forwarding (VRF) table which the subscriber is to use for RADIUS communication. **Note** The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters. The CSG2 does not support the use of the word **forwarding** as a valid VRF name.

Defaults

The *secret-string* is stored in plain text.
If no VRF table is specified for the CSG2, the CSG2 uses the global routing table for RADIUS communication.
If no VRF table is specified for the subscriber, the subscriber uses the global routing table for RADIUS communication.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **radius endpoint** to **ip csg radius endpoint**. • The configuration mode for this command changed from module CSG configuration to global configuration. • The **vrf** *csg-vrf-name* and **vrf** *sub-vrf-name* keywords and arguments were added. • The **table** *table-name* keyword and argument were removed.

Usage Guidelines

A RADIUS Accounting message sent to the specified *csg-address* (and any port) is parsed, and is then acknowledged, by the CSG2.

CSG2 User Table entries created as a result of RADIUS messaging through the **ip csg radius endpoint** definition with a VRF configured are indexed by the configured *sub-vrf-name*. This enables the CSG2 to segment the subscriber space and removes ambiguity if multiple subscribers share the same IP address, provided that their entries were instantiated by RADIUS flows to CSG2 radius definitions bound to different VRFs. If the *sub-vrf-name* is not configured, the User Table entries are indexed via the global routing table.

To change the RADIUS endpoint *csg-vrf-name* or *sub-vrf-name* associated with a given *csg-address*, you must first enter the **no** form of the **ip csg radius endpoint** command for that *csg-address*, then enter the command with the new *csg-vrf-name* or *sub-vrf-name*.

You can specify up to 64 RADIUS endpoints.

Note When the CSG2 is configured as a RADIUS endpoint, the CSG2 drops all RADIUS packets other than RADIUS Accounting-Request messages.

A RADIUS endpoint that is configured with different values for the *csg-address* and *csg-source-address* virtual server IP addresses consumes two RADIUS endpoint resources, not just one. As a result, the maximum number of RADIUS endpoints is reduced by one for each RADIUS endpoint configured with different values for the virtual server IP addresses. In order to configure 64 RADIUS endpoints, each RADIUS endpoint must be configured with the same IP address for *csg-address* and *csg-source-address*. The virtual server IP address must still be different for each RADIUS endpoint command.

You can also configure an optional RADIUS key.

- If you configure a RADIUS key, the CSG2 parses and acts on a message only if the RADIUS Authenticator is correct.
- If you do not configure a RADIUS key, the CSG2 always parses and forwards every message.

Examples

The following example shows how to identify the CSG2 as a RADIUS endpoint:

```
ip csg radius endpoint vrf RADIUSVRF 1.2.3.4 key secret vrf SUBVRF
```

Related Commands

Command	Description
ip csg radius monitor nas	Specifies that the CSG2 is to monitor the RADIUS flows to the specified server.
ip csg radius proxy	Specifies that the CSG2 is to be a proxy for RADIUS messages.
ip csg radius userid	Specifies the RADIUS attribute used to extract the user identifier from a RADIUS record.

ip csg radius handoff

To configure the CSG2 RADIUS handoff timer, use the **ip csg radius handoff** command in global configuration mode. To turn off the timer, use the **no** form of this command.

ip csg radius handoff *duration*

no ip csg radius handoff

Syntax Description

duration	Handoff timer duration, in seconds. The handoff timer is started when a RADIUS Accounting Stop is received. If the handoff timer expires before a RADIUS Accounting Start for a subscriber is seen, the CSG2 assumes that a handoff did not occur and deletes the CSG2 User Table entry for the subscriber. The range is from 1 to 43200.

Defaults

RADIUS handoff is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **radius handoff** to **ip csg radius handoff**. • The configuration mode for this command changed from CSG user group configuration to global configuration.

Usage Guidelines

The handoff timer is started when a RADIUS Accounting Stop is received. If the handoff timer expires before a RADIUS Accounting Start is received for a subscriber, the CSG2 assumes a handoff did not occur and deletes the CSG2 User Table entry for the subscriber.

Examples

The following example shows how to specify a RADIUS handoff timer duration of 1000 seconds:

```
ip csg radius handoff 1000
```

Related Commands

Command	Description
ip csg radius ack error parse	Enables the CSG2 to generate a RADIUS response to a RADIUS Accounting Start Request or a RADIUS Accounting Interim Request when it encounters a RADIUS parse error condition.
ip csg radius ack error user	Enables the CSG2 to generate a RADIUS response to a RADIUS Accounting Start Request or a RADIUS Accounting Interim Request when it encounters a user resource error condition.
ip csg radius proxy	Specifies that the CSG2 is to be a proxy for RADIUS messages.
ip csg radius start restart session-id	Deletes an existing CSG2 User Table entry for a specific subscriber, and creates a new entry for that subscriber.
ip csg radius stop purge	Specifies the attribute that must be included in the RADIUS Accounting Stop request in order for the CSG2 User Table entry to be deleted.

ip csg radius monitor

To specify that the CSG2 is to monitor the RADIUS flows to the specified server, use the **ip csg radius monitor** command in global configuration mode. To stop monitoring the RADIUS flows, use the **no** form of this command.

ip csg radius monitor [**vrf** *vrf-name*] *server-address server-port* [**key** [*encrypt*] *secret-string*] [**vrf** *sub-vrf-name*]

no ip csg radius monitor [**vrf** *vrf-name*] *server-address server-port*

Syntax Description

vrf *csg-vrf-name*	(Optional) Virtual Routing and Forwarding (VRF) table which the CSG2 IP address is to use for RADIUS communication. **Note** The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters. The CSG2 does not support the use of the word **forwarding** as a valid VRF name.
server-address	Specifies the server address to monitor.
server-port	Specifies the server port to monitor.
key	(Optional) Specifies a RADIUS key.
encrypt	(Optional) Indicates how the *secret-string* is represented when the configuration is displayed (for example, **show run**), or how it is written to nonvolatile memory (for example, **write memory**). The valid values are: • **0**—The *secret-string* is stored in plain text. This is the default setting. • **7**—The *secret-string* is encrypted before it is displayed or written to nonvolatile memory. **Note** If your router is configured to encrypt all passwords, then the password is represented as 7 followed by the encrypted text. See the Cisco IOS **service** command for more details.

secret-string	(Optional) 1- to 64-character clear password value for MD5 authentication. All characters are valid; case is significant. The *secret-string* is always sent in plain text to the CSG2 module when the configuration is downloaded. The *secret-string* must match the secret that is specified on the RADIUS client (for example, the gateway general packet radio service [GPRS] support node [GGSN]).
vrf *sub-vrf-name*	(Optional) Virtual Routing and Forwarding (VRF) table which the subscriber is to use for RADIUS communication. **Note** The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters. The CSG2 does not support the use of the word **forwarding** as a valid VRF name.

Defaults

The *secret-string* is stored in plain text.
If no VRF table is specified for the CSG2, the CSG2 uses the global routing table for RADIUS communication.
If no VRF table is specified for the subscriber, the subscriber uses the global routing table for RADIUS communication.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)MD	This command was introduced.

Usage Guidelines

You can configure an optional RADIUS key.

- If you configure a RADIUS key, the CSG2 parses and acts on a message only if the RADIUS Authenticator is correct.
- If you do not configure a RADIUS key, the CSG2 always parses and forwards every message.
- Even if you configure a key, the CSG2 forwards all RADIUS messages (including Access messages), regardless of the configuration or accuracy of the key, unless the IP or UDP headers specify a length larger than the physical packet size.

Examples

The following example shows how to use the **ip csg radius monitor** command to enable the CSG2 to monitor the RADIUS flows:

```
ip csg radius monitor 1.2.3.4 1813 key KEY_TABLE
```

Related Commands

Command	Description
ip csg radius endpoint	Identifies the CSG2 as an endpoint for RADIUS Accounting messages.
ip csg radius monitor nas	Specifies that the CSG2 is to monitor the RADIUS flows to the specified Network Access Server (NAS).
ip csg radius proxy	Specifies that the CSG2 is to be a proxy for RADIUS messages.

ip csg radius monitor nas

To specify that the CSG2 is to monitor the RADIUS flows to the specified Network Access Server (NAS), use the **ip csg radius monitor nas** command in global configuration mode. To stop monitoring the RADIUS flows, use the **no** form of this command.

ip csg radius monitor nas *nas-ip-address* [**vrf** *nas-vrf-name*]

no ip csg radius monitor nas *nas-ip-address* [**vrf** *nas-vrf-name*]

Syntax Description

nas-ip-address	Specifies the NAS IP address to monitor. **Note** The CSG2 performs radius monitor processing only on User Datagram Protocol (UDP) traffic that is destined for the NAS IP address. The NAS IP address cannot be used for any other UDP communication with the CSG2.
vrf *nas-vrf-name*	(Optional) Virtual Routing and Forwarding (VRF) table which the NAS IP address is to use for RADIUS communication. **Note** The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters. The CSG2 does not support the use of the word **forwarding** as a valid VRF name.

Defaults

If no VRF table is specified for the NAS, the CSG2 uses the global routing table for RADIUS communication.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)MD	This command was introduced.

Usage Guidelines

This command is required whenever a RADIUS monitor is configured. Use this command to identify each NAS that is to communicate with the RADIUS monitor server. Each interface on which a NAS server resides must be marked as a subscriber interface.

Examples

The following example shows how to use the **ip csg radius monitor nas** command to enable the CSG2 to monitor the RADIUS flows:

```
ip csg radius monitor nas 1.2.3.4 vrf NAS_TABLE
```

Related Commands

Command	Description
ip csg radius endpoint	Identifies the CSG2 as an endpoint for RADIUS Accounting messages.
ip csg radius proxy	Specifies that the CSG2 is to be a proxy for RADIUS messages.

ip csg radius on-off purge

To specify the rate at which the CSG2 is to delete CSG2 User Table entries in response to a RADIUS Accounting On or RADIUS Accounting Off message, or in response to the **clear ip csg user all** command, use the **ip csg radius on-off purge** command in global configuration mode. To restore the default setting, use the **no** form of this command.

ip csg radius on-off purge *deletions-per-second*

no ip csg radius on-off purge

Syntax Description

deletions-per-second	Number of User Table entry deletions per second. The range is from 50 to 65535. The default rate is 1000.

Defaults

The default rate is 1000 User Table entry deletions per second.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)MD	This command was introduced.

Usage Guidelines

The actual rate at which the CSG2 deletes User Table entries might be slightly higher or lower than the specified rate.

Examples

The following example shows how to specify a User Table deletion rate of 875 entries per second:

```
ip csg radius on-off purge 875
```

ip csg radius pod attribute

To specify the RADIUS attributes and vendor-specific attribute (VSA) subattributes to be copied from the RADIUS Start message and sent to the Network Access Server (NAS) in the Packet of Disconnect (PoD) message, use the **ip csg radius pod attribute** command in global configuration mode. To disable this feature, use the **no** form of this command.

ip csg radius pod attribute {*radius-attribute-number* | **vsa** {*vendor-id* | **3gpp**} *radius-subattribute-number*}

no ip csg radius pod attribute {*radius-attribute-number* | **vsa** {*vendor-id* | **3gpp**} *radius-subattribute-number*}

Syntax Description

radius-attribute-number	RADIUS attribute number to be copied from the RADIUS Start message and sent to the Network Access Server (NAS) in the Packet of Disconnect (PoD) message. The range is from 1 to 255.
vsa	Specifies the VSA.
vendor-id	Specifies the vendor ID number. The range is from 1 to 16777215.
3gpp	Specifies the Third Generation Partnership Project (3GPP) vendor ID.
radius-subattribute-number	Specifies the subattribute number. The range is from 1 to 255.

Defaults

RADIUS attributes sufficient to identify the NAS and subscriber (RFC3576) are sent in the PoD message.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **radius pod attribute** to **ip csg radius pod attribute**. • The configuration mode for this command changed from CSG user group configuration to global configuration. • The **26** keyword was removed.

Usage Guidelines

You can specify up to 256 RADIUS attributes.

If the RADIUS message does not contain an attribute, the PoD message attribute does not contain the attribute, either.

The CSG2 saves and reports attribute and subattribute information for each subscriber.

When the CSG2 receives a new RADIUS Accounting Start or RADIUS Interim Accounting Request, it saves the attribute and subattribute information parsed from the new request.

The CSG2 saves only those attributes or subattributes which meet both of the following criteria:

- They are present in the new RADIUS Accounting Start or RADIUS Interim Accounting Request.
- They are configured for reporting at the time the new request arrives at the CSG2.

All previously stored attribute and subattribute information from previous requests is destroyed, even if the new RADIUS Accounting Start or RADIUS Interim Accounting Request does not contain all of the attributes and subattributes that were present in the previous request. Only the currently stored attributes are reported in CDRs.

If there are multiple instances of an attribute, all instances are included. Attributes are included in the PoD message in random order.

Examples

The following example shows how to specify RADIUS attributes 44 and 26:

```
ip csg radius pod attribute 44
ip csg radius pod attribute 26
```

Related Commands

Command	Description
ip csg radius pod nas	Specifies the NAS port to which the CSG2 is to send the PoD message, and the key to use in calculating the Authenticator.
ip csg radius pod timeout	Specifies the number of times to retry the RADIUS PoD message if it is not acknowledged by means of an ACK message, and the interval between retransmissions.

ip csg radius pod nas

To specify the Network Access Server (NAS) port to which the CSG2 is to send the Packet of Disconnect (PoD) message, and to specify the key to use in calculating the Authenticator, use the **ip csg radius pod nas** command in global configuration mode. To restore the default settings, use the **no** form of this command.

ip csg radius pod nas [**vrf** *vrf-name*] [*start-ip end-ip*] *port* **key [*encrypt*]** *secret-string*

no ip csg radius pod nas [**vrf** *vrf-name*] [*start-ip end-ip*] *port* **key [*encrypt*]** *secret-string*

Syntax Description

vrf *vrf-name*	(Optional) Virtual Routing and Forwarding (VRF) table which the CSG2 is to use for RADIUS communication. **Note** The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters. The CSG2 does not support the use of the word **forwarding** as a valid VRF name.
start-ip	(Optional) Specifies the first NAS IP address in a range of addresses.
end-ip	(Optional) Specifies the last NAS IP address in a range of addresses.
port	Specifies the NAS port number to which the PoD message is sent.
key	Specifies a RADIUS key.
encrypt	(Optional) Indicates how the *secret-string* is represented when the configuration is displayed (for example, **show run**), or how it is written to nonvolatile memory (for example, **write memory**). The possible values are **0** and **7**: • **0**—The *secret-string* is stored in plain text. This is the default setting. • **7**—The *secret-string* is encrypted before it is displayed or written to nonvolatile memory. **Note** If your router is configured to encrypt all passwords, then the password is represented as 7 followed by the encrypted text. See the Cisco IOS **service** command for more details.
secret-string	1- to 64-character clear password value for MD5 authentication. All characters are valid; case is significant. The *secret-string* is always sent in plain text to the CSG2 module when the configuration is downloaded. The *secret-string* must match the secret that is specified on the RADIUS client (for example, the gateway general packet radio service [GPRS] support node [GGSN]).

Defaults

The *secret-string* is stored in plain text.
If no VRF table is specified, the CSG2 uses the global routing table for RADIUS communication.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **radius pod nas** to **ip csg radius pod nas**. • The configuration mode for this command changed from CSG user group configuration to global configuration. • The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The PoD message is sent to the NAS IP address that is specified in the NAS-IP-Address attribute (4) in the RADIUS Accounting Start message. This command specifies the NAS listening port, as well as the key to use in calculating the Authenticator.

The RADIUS Accounting Start message which specifies the NAS IP address to which to send the PoD message must be received on an IP address specified by the **ip csg radius proxy** or **ip csg radius endpoint** command configured in global configuration mode.

In some networks, many NASes might use the same listening port and key. In such networks, you can use this command to specify the range of NAS IP addresses.

If no IP addresses are specified, the port number and key apply to all NASes. The “global” definition is used if a specific range is not configured for the NAS when the PoD message is sent.

Examples

The following example shows how to specify NAS ports and keys:

```
ip csg radius pod nas 1.1.1.0 1.1.1.255 1700 key secret
ip csg radius pod nas 1701 key password
```

Related Commands

Command	Description
ip csg radius pod attribute	Specifies the RADIUS attributes to be copied from the RADIUS Start message and sent to the NAS in the PoD.
ip csg radius pod timeout	Specifies the number of times to retry the RADIUS PoD message if it is not acknowledged by means of an ACK message, and the interval between retransmissions.

ip csg radius pod timeout

To specify the number of times to retry the RADIUS Packet of Disconnect (PoD) message if it is not acknowledged by means of an ACK message, and the interval between retransmissions, use the **ip csg radius pod timeout** command in global configuration mode. To restore the default timeout, use the **no** form of this command.

ip csg radius pod timeout *timeout* **retransmit** *retransmit*

no ip csg radius pod timeout *timeout* **retransmit** *retransmit*

Syntax Description

timeout	Number of seconds to wait for an ACK or NAK before sending another PoD message. The range is from 1 to 1000. The default timeout is 5 seconds.
retransmit *retransmit*	Number of times to retransmit the message. The range is from 1 to 100. The default setting is 3 retransmits.

Defaults

The default timeout is 5 seconds.
The default number of retransmits is 3 retransmits.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **radius pod timeout** to **ip csg radius pod timeout**. • The configuration mode for this command changed from CSG user group configuration to global configuration.

Examples

The following example shows how to specify a RADIUS PoD timeout and the number of times to retransmit the message:

```
ip csg radius pod timeout 30 retransmit 5
```

Related Commands

Command	Description
ip csg radius pod attribute	Specifies the RADIUS attributes to be copied from the RADIUS Start message and sent to the NAS in the PoD.
ip csg radius pod nas	Specifies the NAS port to which the CSG2 is to send the PoD message, and specifies the key to use in calculating the Authenticator.

ip csg radius proxy

To specify that the CSG2 is to be a proxy for RADIUS messages, use the **ip csg radius proxy** command in global configuration mode. To stop the CSG2 from proxying for RADIUS messages, use the **no** form of this command.

ip csg radius proxy [**vrf** *csg-vrf-name*] *csg-address* [**vrf** *server-vrf-name*] *server-address* *csg-source-address* [**key** [*encrypt*] *secret-string*] [**vrf** *sub-vrf-name*]

no ip csg radius proxy [**vrf** *csg-vrf-name*] *csg-address server-addr*ess

Syntax Description

vrf *csg-vrf-name*	(Optional) Virtual Routing and Forwarding (VRF) table which the CSG2 IP address is to use for RADIUS communication. **Note** The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters. The CSG2 does not support the use of the word **forwarding** as a valid VRF name.
csg-address	Specifies the CSG2 IP address. The CSG2 IP address must be a virtual IP address, and it must be unique (or the IP address-VRF name combination must be unique, if VRF is configured). The CSG2 IP address (or the IP address-VRF name combination) must not be specified in other CSG2 commands, and it must not match any real IP address, virtual IP address, or alias IP address (or IP address-VRF name combination) configured on the CSG2. If you want the CSG2 RADIUS proxy IP address to be a member of a CSG2 interface subnet, you must configure the CSG2 IP address as follows: • In non-redundant configurations, you must configure the CSG2 IP address as a secondary IP address configured on the appropriate interface. • In redundant configurations, you must configure the CSG2 IP address as a standby secondary IP address on the appropriate interface. **Note** The CSG2 performs radius proxy processing only on User Datagram Protocol (UDP) traffic that is destined for the server IP address. The server IP address cannot be used for any other UDP communication with the CSG2.
vrf *server-vrf-name*	(Optional) Virtual Routing and Forwarding (VRF) table which the server IP address is to use for RADIUS communication. **Note** The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters. The CSG2 does not support the use of the word **forwarding** as a valid VRF name.
server-address	Specifies the server IP address.

csg-source-address	Specifies the source IP address that the CSG2 is to use when sending packets to the RADIUS server. The CSG2 source IP address must be unique (or the IP address-VRF name combination must be unique, if VRF is configured). If you want the CSG2 RADIUS proxy IP address to be a member of a CSG2 interface subnet, you must configure the CSG2 source IP address as follows: • In non-redundant configurations, you must configure the CSG2 source IP address as a secondary IP address configured on the appropriate interface. • In redundant configurations, you must configure the CSG2 source IP address as a standby secondary IP address on the appropriate interface. **Note** The CSG2 performs radius proxy processing only on User Datagram Protocol (UDP) traffic that is destined for the *csg-source-address*. The *csg-source-address* cannot be used for any other UDP communication with the CSG2.
key	(Optional) Specifies a RADIUS key. **Note** Specify no more than one **key** for each CSG2 IP address.
encrypt	(Optional) Indicates how the *secret-string* is represented when the configuration is displayed (for example, **show run**), or how it is written to nonvolatile memory (for example, **write memory**). The possible values are **0** and **7**: • **0**—The *secret-string* is stored in plain text. This is the default setting. • **7**—The *secret-string* is encrypted before it is displayed or written to nonvolatile memory. **Note** If your router is configured to encrypt all passwords, then the password is represented as 7 followed by the encrypted text. See the Cisco IOS **service** command for more details.
secret-string	(Optional) 1- to 64-character clear password value for MD5 authentication. All characters are valid; case is significant. The *secret-string* is always sent in plain text to the CSG2 module when the configuration is downloaded. The *secret-string* must match the secret that is specified on the RADIUS client (for example, the gateway general packet radio service [GPRS] support node [GGSN]).
vrf *sub-vrf-name*	(Optional) Virtual Routing and Forwarding (VRF) table which the subscriber is to use for RADIUS communication. **Note** The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters. The CSG2 does not support the use of the word **forwarding** as a valid VRF name.

Defaults

The *secret-string* is stored in plain text.
The *csg-source-address* is set to *csg-address*.
If no VRF table is specified for the CSG2, the CSG2 uses the global routing table for RADIUS communication.
If no VRF table is specified for the RADIUS server, the RADIUS server uses the global routing table for RADIUS communication.
If no VRF table is specified for the subscriber, the subscriber uses the global routing table for RADIUS communication.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **radius proxy** to **ip csg radius proxy**. • The configuration mode for this command changed from module CSG configuration to global configuration. • The **vrf** *csg-vrf-name*, **vrf** *server-vrf-name*, and **vrf** *sub-vrf-name* keywords and arguments were added. • The **table** *table-name* keyword and argument were removed.

Usage Guidelines

A message sent to the specified *csg-address* (and any port) is parsed and then forwarded to the specified RADIUS server. When forwarded to the RADIUS server, the source IP address is the *csg-source-address*.

The source port is arbitrarily chosen by the CSG2, and the destination port remains unchanged. When a message is received from the network and forwarded to the subscriber, the source IP address is the *csg-address*, and the source port remains unchanged. The source IP address and port are taken from the destination IP address and port in the original message from the subscriber.

You can configure an optional RADIUS key. If you configure a key, the CSG2 parses and acts on the message only if the RADIUS authenticator is correct. If the key is not configured, the CSG2 always parses the message. Whether you configure a key or not, and whether it is correct or not, the CSG2 always forwards the message.

You can specify up to 64 RADIUS proxies.

Note A RADIUS proxy that is configured with different values for the *csg-address* and *csg-source-address* virtual server IP addresses consumes two RADIUS proxy resources, not just one. As a result, the maximum number of RADIUS proxies is reduced by one for each RADIUS proxy configured with different values for the virtual server IP addresses. In order to configure 64 RADIUS proxies, each RADIUS proxy must be configured with the same IP address for *csg-address* and *csg-source-address*. The virtual server IP address must still be different for each RADIUS proxy command.

You can also configure an optional RADIUS key.

- If you configure a RADIUS key, the CSG2 parses and acts on a message only if the RADIUS Authenticator is correct.
- If you do not configure a RADIUS key, the CSG2 always parses and forwards every message.

You can specify more than one RADIUS **key** by specifying more than one **ip csg radius proxy** command, but each command must specify a unique CSG2 IP address (or IP address-VRF name combination, if VRF is configured).

All RADIUS messages are forwarded, unless the IP or User Datagram Protocol (UDP) headers specify a length larger than the physical packet size.

CSG2 User Table entries created as a result of RADIUS messaging through the **ip csg radius endpoint** definition with a VRF configured are indexed by the configured *sub-vrf-name*. This enables the CSG2 to segment the subscriber space and removes ambiguity if multiple subscribers share the same IP address, provided that their entries were instantiated by RADIUS flows to CSG2 radius definitions bound to different VRFs. If the *sub-vrf-name* is not configured, the User Table entries are indexed via the global routing table.

Note If your network is designed to check the authorization string in RADIUS messages, we recommend that you enter a *secret-string*. Additionally, if you configure the **ip csg entries user profile radius remove** command, you might need to configure a *secret-string*.

To change the RADIUS proxy *csg-vrf-name*, *server-vrf-name*, or *sub-vrf-name* associated with a given *csg-address*, you must first enter the **no** form of the **ip csg radius endpoint** command for that *csg-address*, then enter the command with the new *csg-vrf-name*, *server-vrf-name*, or *sub-vrf-name*.

Examples

The following example illustrates how to create a RADIUS proxy point:

```
ip csg radius proxy vrf RADIUSVRF 1.2.3.4 vrf SERVERVRF 5.6.7.8 1.2.3.4 key secret vrf
SUBVRF
```

Related Commands

Command	Description
ip csg radius endpoint	Identifies the CSG2 as an endpoint for RADIUS Accounting messages.
ip csg radius monitor nas	Specifies that the CSG2 is to monitor the RADIUS flows to the specified server.
ip csg radius userid	Specifies the RADIUS attribute used to extract the user identifier from a RADIUS record.

ip csg radius reauthorization attribute

To define the RADIUS attributes and VSA subattributes to be monitored by the CSG2, and to enable Roaming Service Control, use the **ip csg radius reauthorization attribute** command in global configuration mode. To delete a RADIUS attribute, use the **no** form of this command.

ip csg radius reauthorization attribute {*radius-attribute-number* | **vsa** {*vendor-id* | **3gpp**} *radius-subattribute-number*}

no ip csg radius reauthorization attribute {*radius-attribute-number* | **vsa** {*vendor-id* | **3gpp**} *radius-subattribute-number*}

Syntax Description

radius-attribute-number	Specifies the RADIUS attribute number. The range is from 1 to 255.
vsa	Specifies the vendor-specific attribute (VSA).
vendor-id	Specifies the vendor ID number. The range is from 1 to 16777215.
3gpp	Specifies the Third Generation Partnership Project (3GPP) vendor ID.
radius-subattribute-number	Specifies the subattribute number. The range is from 1 to 255.

Defaults

The default behavior is that no RADIUS attribute is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)MD	This command was introduced.

Usage Guidelines

Roaming Service Control, also known as seamless roaming or RADIUS reauthorization, enables the CSG2 to reauthorize prepaid users, instead of ending the users' sessions, when a configured list of attributes changes.

1. When you enable Roaming Service Control, you also configure a list of RADIUS attributes and VSA subattributes to be monitored and saved by the CSG2.
2. When the CSG2 receives a RADIUS Start message, it saves the subset of attributes that are in both the configured list and the message.
3. When the CSG2 receives a subsequent RADIUS Start or RADIUS Interim Accounting message, it compares the saved subset of attributes to the list of attributes in the new message. (The CSG2 compares only the list of attributes, not the actual contents of those attributes.)
4. If any attribute in the saved subset is missing from the list of attributes in the new message, or if there are any new attributes in the message that are not in the saved subset, the CSG2 reauthorizes prepaid users without ending their sessions.
5. If service-level CDR summarization is enabled, the CSG2 sends a Service Usage CDR for each service in the session.

Otherwise, if intermediate CDRs are supported for the session, the CSG2 sends an intermediate CDR for each service in the session. However, if you have enabled fixed-format CDRs, the CSG2 does not generate intermediate CDRs during roaming events.

The CDR includes:

- The Cause TLV, indicating that the CDR was generated due to the receipt of a reauthorization trigger
- The saved subset of attributes from the first RADIUS Start message
- The list of attributes from the new message

For more information about service-level CDR summarization, see the "Enabling Service-Level CDR Summarization" section on page 5-10.

For more information about intermediate CDRs, see the "Intermediate CDRs" section on page 1-38.

For more information about fixed-format CDRs, see the "Configuring Fixed, Variable, or Combined Format CDR Support" section on page 2-17.

Examples

The following example illustrates how to create a RADIUS proxy point:

```
ip csg radius reauthorization attribute 14
ip csg radius reauthorization attribute vsa 7777 44
ip csg radius reauthorization attribute 26 7778 4
```

Related Commands

Command	Description
ip csg radius proxy	Specifies that the CSG2 is to be a proxy for RADIUS messages.

ip csg radius start restart session-id

To delete an existing CSG2 User Table entry for a specific subscriber, and to create a new entry for that subscriber, use the **ip csg radius start restart session-id** command in global configuration mode.

ip csg radius start restart session-id {*radius-attribute-number* | **vsa** {*vendor-id* | **3gpp**} *radius-subattribute-number*}

Syntax Description

radius-attribute-number	Specifies the RADIUS attribute number. The range is from 1 to 255.
vsa	Specifies the vendor-specific attribute (VSA).
vendor-id	Specifies the vendor ID number. The range is from 1 to 16777215.
3gpp	Specifies the Third Generation Partnership Project (3GPP) vendor ID.
radius-subattribute-number	Specifies the subattribute number. The range is from 1 to 255.

Defaults

The default behavior is that existing CSG2 User Table entries are not deleted.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **radius start restart session-id** to **ip csg radius start restart session-id**. • The configuration mode for this command changed from module CSG configuration to global configuration. • The **26** keyword was removed.

Usage Guidelines

This command:

- Deletes an existing CSG2 User Table entry for a specific subscriber (when a RADIUS Accounting Start or RADIUS Interim Accounting is received).
- Creates a new entry for that subscriber (similar to when a RADIUS Accounting Stop has been received).
- Terminates all sessions for that subscriber.

To detect duplicate RADIUS requests (in this situation, the existing entry is not deleted), specify the attribute (which might be a VSA) to be used. If the contents of the specified attribute in the original request match the contents of the attribute in the current request, the request is a duplicate and the existing entry is not deleted.

Examples

The following example shows how to enable the **ip csg radius start restart session-id** command:

```
ip csg radius start restart session-id 44
```

Related Commands

Command	Description
ip csg radius stop purge	Specifies the attribute that must be included in the RADIUS Accounting Stop request in order for the CSG2 User Table entry to be deleted.

ip csg radius stop purge

To specify the attribute that must be included in the RADIUS Accounting Stop request in order for the CSG2 User Table entry to be deleted, use the **ip csg radius stop purge** command in global configuration mode.

ip csg radius stop purge {*radius-attribute-number* | **vsa** {*vendor-id* | **3gpp**} *radius-subattribute-number*}

Syntax Description

radius-attribute-number	Specifies the RADIUS attribute number. The range is from 1 to 255.
vsa	Specifies the vendor-specific attribute (VSA).
vendor-id	Specifies the vendor ID number. The range is from 1 to 16777215.
3gpp	Specifies the Third Generation Partnership Project (3GPP) vendor ID.
radius-subattribute-number	Specifies the subattribute number. The range is from 1 to 255.

Defaults

The subscriber entry is deleted when a RADIUS Accounting Stop is received.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **radius stop purge** to **ip csg radius stop purge**. • The configuration mode for this command changed from module CSG configuration to global configuration. • The **26** keyword was removed.

Usage Guidelines

The **ip csg radius stop purge command s**pecifies the attribute (which might be a VSA) that must be included in the RADIUS Accounting Stop request in order for the CSG2 User Table entry to be deleted. The contents of the specified attribute are not examined.

Examples

The following example shows how to enable the **ip csg radius stop purge** command:

```
ip csg radius stop purge 44
```

Related Commands

Command	Description
ip csg radius start restart session-id	Deletes an existing CSG2 User Table entry for a specific subscriber, and creates a new entry for that subscriber.

ip csg radius userid

To specify the RADIUS attribute used to extract the user identifier from a RADIUS record, use the **ip csg radius userid** command in global configuration mode. To specify that no RADIUS attributes are to be used, use the **no** form of this command.

ip csg radius userid {1 | 31 | User-Name | Calling-Station-Id}

no ip csg radius userid

Syntax Description

1	RADIUS attribute number 1.
31	RADIUS attribute number 31.
User-Name	Equivalent to RADIUS attribute number 1.
Calling-Station-Id	Equivalent to RADIUS attribute number 31.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **radius userid** to **ip csg radius userid**. • The configuration mode for this command changed from module CSG configuration to global configuration.

Usage Guidelines

The **ip csg radius userid** command specifies that the CSG2 obtains the user ID from either attribute 1 or 31. If the **no** form of this command, **no ip csg radius userid**, is used, user IDs are not obtained from RADIUS messages.

Examples

The following example shows how to specify RADIUS attribute User-Name:

```
ip csg radius userid User-Name
```

Related Commands

Command	Description
ip csg radius ack error parse	Enables the CSG2 to generate a RADIUS response to a RADIUS Accounting Start Request or a RADIUS Accounting Interim Request when it encounters a RADIUS parse error condition.
ip csg radius ack error user	Enables the CSG2 to generate a RADIUS response to a RADIUS Accounting Start Request or a RADIUS Accounting Interim Request when it encounters a user resource error condition.
ip csg radius handoff	Configures RADIUS handoff support.
ip csg radius start restart session-id	Deletes an existing CSG2 User Table entry for a specific subscriber, and creates a new entry for that subscriber.
ip csg radius stop purge	Specifies the attribute that must be included in the RADIUS Accounting Stop request in order for the CSG2 User Table entry to be deleted.

ip csg records format

To specify variable, fixed, or combined (variable-single) call detail record (CDR) format, use the **ip csg records format** command in global configuration mode. To use the default setting, use the **no** form of this command.

ip csg records format [**fixed** | **variable** [**combined** {**http** | **wap**}]]

no ip csg records format [**fixed** | **variable** [**combined** {**http** | **wap**}]]

Syntax Description

fixed	(Optional) Specifies fixed CDR format.
variable	(Optional) Specifies variable CDR format.
combined http	(Optional) Specifies combined (variable-single) CDR format for HTTP traffic.
combined wap	(Optional) Specifies combined (variable-single) CDR format for wireless application protocol (WAP) traffic.

Defaults

The default setting is **variable**.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **records format** to **ip csg records format**. • The configuration mode for this command changed from CSG accounting configuration to global configuration. • The **variable-single-cdr** keyword was replaced with the **combined** keyword. • The **http** and **wap** keywords were added.

Usage Guidelines

This command is valid only for transaction-based CDRs. It is not valid for service-level CDRs.

Fixed record format generates CDRs that always contain the same set of Tag-Length-Values (TLVs). Some might have a length of zero. This format is primarily used for integration with legacy billing systems.

Examples

The following example shows how to specify combined CDR record format for HTTP traffic:

```
ip csg records format variable combined http
```

ip csg redirect

To redirect subscriber flows to an alternate IP address when the subscriber's quota is exhausted, use the **ip csg redirect** command in global configuration mode. To remove the redirect, use the **no** form of this command.

ip csg redirect {**http** *url* | **interval** *seconds* | **maximum** *number* | **sip** *url* | **wap** *url*}

no ip csg redirect [**http** | **sip** | **wap**]

Syntax Description

http *url*	(Optional) Redirects HTTP subscriber flows to the specified redirect URL when quota is depleted, and configures the default URL for use in HTTP redirection.
interval *seconds*	(Optional) Length of time, in seconds, during which the CSG2 redirects an out-of-quota subscriber. After this interval, the CSG2 drops the requests until quota can be requested again. The start of the interval is the time of the first redirect after a quota grant of zero. The range is from 0 to 3600. The default is 8.
maximum *number*	(Optional) Maximum number of times a redirect is to be performed for an out-of-quota subscriber during a redirect interval. The range is from 0 to 255. The default is 15.
sip *url*	(Optional) Redirects Session Initiation Protocol (SIP) call requests (INVITE methods) to the specified redirect URL when quota is depleted.
wap *url*	(Optional) Redirects wireless application protocol (WAP) subscriber flows to the specified redirect URL when quota is depleted.

Defaults

If you do not specify an interval, the CSG2 redirects subscriber flows after 8 seconds.
If you do not specify a maximum, the CSG2 allows up to 15 redirects during the interval.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **redirect** to **ip csg redirect**. • The configuration mode for this command changed from CSG user group configuration to CSG2 service configuration. • The **interval** *seconds* and **maximum** *number* keywords and arguments were added. • The **nat** *ip-address* and *port-number* keyword and arguments were removed.
12.4(15)MD	The **sip** keyword and *url* argument were added.

Examples

The following example shows how to configure CSG2 redirects:

```
ip csg redirect http http://server/topoff.html
ip csg redirect sip sip: 1.2.3.4
ip csg redirect wap http://server/topoff.wml
ip csg redirect interval 30
ip csg redirect maximum 10
```

ip csg refund

To specify the CSG2 refund policy to apply to the various services, and to enter CSG2 refund configuration mode, use the **ip csg refund** command in global configuration mode. To disable this feature, use the **no** form of the command.

ip csg refund *refund-policy-name*

no ip csg refund *refund-policy-name*

Syntax Description

refund-policy-name	Name of the refund policy that applies to the content for this service. The name can be from 1 to 15 characters long, and can include uppercase or lowercase letters (the CSG2 changes all letters to uppercase), numbers, and any special characters.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: None.

Usage Guidelines

The characteristics of each policy are defined by the following commands:

- **flags**—The CSG2 supports flag-based refunding for all protocols.
- **retcode**—The CSG2 supports return code-based refunding for all protocols except RTSP.

Examples

The following example shows how to specify CSG2 refund policy COMPANY-REFUND:

```
ip csg refund COMPANY-REFUND
```

Related Commands

Command	Description
flags	Specifies IP, TCP, or wireless application protocol (WAP) flag bit masks and values for CSG2 Prepaid Error Reimbursement.
ip csg policy	Defines a policy for qualifying flows for the CSG2 accounting services, and enters CSG2 policy configuration mode.
ip csg service	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.
retcode	Specifies the range of application return codes for which the CSG2 refunds quota for Prepaid Error Reimbursement.

ip csg replicate

To enable high availability (HA) state replication between redundant CSG2 systems, use the **ip csg replicate** command in global configuration mode. To disable state replication, use the **no** form of this command.

i**p csg replicate** [**vrf** *vrf-name*] *local-ip remote-ip base-port*

no ip csg replicate

Syntax Description

vrf *vrf-name*	(Optional) Virtual Routing and Forwarding (VRF) table which the redundant CSG2s are to use when sending state synchronization messages. **Note** The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters. The CSG2 does not support the use of the word **forwarding** as a valid VRF name.
local-ip	Local IP address on the CSG2 used as the source IP address for outgoing state synchronization messages, and as the listen IP address for incoming state synchronization messages. You must configure this IP address on the local CSG2 as either an interface or as a secondary IP address.
remote-ip	Remote IP address used as the destination IP address for outgoing state synchronization messages.
base-port	User Datagram Protocol (UDP) port number used as the source and destination port for state synchronization messages. The specified port number is the first of six sequential UDP ports that the CSG2 uses for state synchronization. For example, if you specify port number 2000, the CSG2 uses ports 2000 through 2005 for state synchronization.

Defaults

Replication is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

The i**p csg replicate** command enables stateful replication of the CSG2 state data structures, such as the CSG2 User Table.

To enable replication of session and flows, use the **replicate** command in CSG2 content configuration mode.

Using two separate commands to enable CSG2 replication allows for synchronization of subscriber and quota states independent of per-flow synchronization.

Examples

The following example shows how to enable CSG2 replication to a peer using local IP address 10.10.10.1, remote IP address,10.10.10.2, and UDP ports 2000 through 2005:

```
Ip csg replicate 10.10.10.1 10.10.10.2 2000
```

Related Commands

Command	Description
replicate	Replicates the connection state for all connections to the CSG2 content servers on the standby system.

ip csg report http header

To define the inclusion of multiple HTTP request headers in the CSG2 HTTP_Header call detail record (CDR), use the **ip csg report http header** command in global configuration mode. To disable this configuration, use the **no** form of this command.

ip csg report http header *header-name*

no ip csg report http header *header-name*

Syntax Description

header-name	Name of the request header that you want to include in the CSG2 HTTP_Header CDR. The header name can be from 1 to 224 characters long, and can include uppercase or lowercase letters (the CSG2 changes all letters to uppercase), numbers, and any special characters.

Defaults

The default is to copy only the “host,” “user-agent,” and “from” HTTP headers into the CDRs.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **report http header** to **ip csg report http header**. • The configuration mode for this command changed from CSG accounting configuration to global configuration.

Examples

The following example shows how to enable reporting HTTP header information:

```
ip csg report http header x-subno
ip csg report http header x-al-session-id
```

Related Commands

Command	Description
ip csg report radius attribute	Specifies the RADIUS attributes to be copied from the RADIUS Start message into CSG2 call detail records (CDRs).
ip csg report smtp rfc2822	Specifies that the CSG2 is to include RFC 2822 header Tag-Length-Values (TLVs) in Simple Mail Transfer Protocol (SMTP) call detail records (CDRs).

Command	Description
ip csg report usage	Enables CSG2 supplemental usage reporting to the quota server.
ip csg report wap actual-pdu	Specifies whether actual wireless application protocol (WAP) protocol data units (PDUs) are to be reported in CSG2 call detail records (CDRs).

ip csg report radius attribute

To specify the RADIUS attributes and VSA subattributes to be copied from the RADIUS Start message and sent to the Billing Mediation Agent (BMA) in CSG2 call detail records (CDRs), use the **ip csg report radius attribute** command in global configuration mode. To disable this feature, use the **no** form of this command.

ip csg report radius attribute {*radius-attribute-number* | **vsa** {*vendor-id* | **3gpp**} *radius-subattribute-number*}

no **ip csg report radius attribute** {*radius-attribute-number* | **vsa** {*vendor-id* | **3gpp**} *radius-subattribute-number*}

Syntax Description

radius-attribute-number	RADIUS attribute number to be copied from the RADIUS Start message. The range is from 1 to 255.
vsa	Specifies the vendor-specific attribute (VSA).
vendor-id	Specifies the vendor ID number. The range is from 1 to 16777215.
3gpp	Specifies the Third Generation Partnership Project (3GPP) vendor ID.
radius-subattribute-number	Specifies the RADIUS subattribute number. The range is from 1 to 255.

Defaults

No RADIUS attributes are copied into CDRs.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **report radius attribute** to **ip csg report radius attribute**. • The configuration mode for this command changed from CSG accounting configuration to global configuration. • The **26** keyword was removed.

Usage Guidelines

You can specify up to 256 attributes.

If an attribute is not present in the RADIUS message, it is not present in the CDRs, unless **ip csg records format fixed** is configured.

The CSG2 saves and reports attribute and subattribute information for each subscriber.

When the CSG2 receives a new RADIUS Accounting Start or RADIUS Interim Accounting Request, it saves the attribute and subattribute information parsed from the new request.

The CSG2 saves only those attributes or subattributes which meet both of the following criteria:

- They are present in the new RADIUS Accounting Start or RADIUS Interim Accounting Request.
- They are configured for reporting at the time the new request arrives at the CSG2.

All previously stored attribute and subattribute information from previous requests is destroyed, even if the new RADIUS Accounting Start or RADIUS Interim Accounting Request does not contain all of the attributes and subattributes that were present in the previous request. Only the currently stored attributes are reported in CDRs.

If there are multiple instances of an attribute, they are all reported. Attributes are reported in the order in which they are presented in the RADIUS message.

If both the reporting of RADIUS attributes and Roaming Service Control are enabled, the CSG2 sends the combined list of attributes in every CDR to the BMA and quota server (but only changes in the Roaming Service Control attributes trigger reauthorization). For example, if the CSG2 is configured to report attributes 1, 3, and 5, and configured to monitor attributes 2, 4, and 6 for Roaming Service Control, then the CSG2 reports attributes 1, 2, 3, 4, 5, and 6 in all CDRs to the BMA and quota server. For more information about Roaming Service Control, see the "Enabling Roaming Service Control" section on page 9-10.

Examples

The following example shows how to specify the RADIUS attributes to be copied from the RADIUS Start message into CDRs:

```
ip csg report radius attribute 3
ip csg report radius attribute 5
ip csg report radius attribute 7
ip csg report radius attribute 44
```

Related Commands

Command	Description
ip csg report http header	Defines the inclusion of multiple HTTP request headers in the CSG2 HTTP_Header call detail record (CDR).
ip csg report smtp rfc2822	Specifies that the CSG2 is to include RFC 2822 header Tag-Length-Values (TLVs) in Simple Mail Transfer Protocol (SMTP) call detail records (CDRs).
ip csg report usage	Enables CSG2 supplemental usage reporting to the quota server.
ip csg report wap actual-pdu	Specifies whether actual wireless application protocol (WAP) protocol data units (PDUs) are to be reported in CSG2 call detail records (CDRs).

ip csg report smtp rfc2822

To specify that the CSG2 is to include RFC 2822 header Tag-Length-Values (TLVs) in Simple Mail Transfer Protocol (SMTP) call detail records (CDRs), use the **ip csg report smtp rfc2822** command in global configuration mode. To exclude SMTP headers from CDRs, use the **no** form of this command.

ip csg report smtp rfc2822

no ip csg report smtp rfc2822

Syntax Description

This command has no arguments or keywords.

Defaults

RFC 2822 header TLVs are included in SMTP CDRs.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Examples

The following example shows how to exclude RFC2822 headers from SMTP CDRs:

```
no ip csg report smtp rfc2822
```

Related Commands

Command	Description
ip csg report http header	Defines the inclusion of multiple HTTP request headers in the CSG2 HTTP_Header call detail record (CDR).
ip csg report radius attribute	Specifies the RADIUS attributes to be copied from the RADIUS Start message into CSG2 call detail records (CDRs).
ip csg report usage	Enables CSG2 supplemental usage reporting to the quota server.
ip csg report wap actual-pdu	Specifies whether actual wireless application protocol (WAP) protocol data units (PDUs) are to be reported in CSG2 call detail records (CDRs).

ip csg report usage

To enable CSG2 supplemental usage reporting to the quota server, use the **ip csg report usage** command in global configuration mode. To disable supplemental usage reporting, use the **no** form of this command.

ip csg report usage {**bytes ip** | **seconds**}

no ip csg report usage {**bytes ip** | **seconds**}

Syntax Description

bytes ip	Report the number of IP bytes uploaded and downloaded for each interval.
seconds	Report usage in seconds for the interval, as well as the timestamps of the start of the first and last billable sessions in the interval.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **report usage** to **ip csg report usage**. • The configuration mode for this command changed from CSG accounting configuration to global configuration.

Usage Guidelines

Interval report Tag-Length-Values (TLVs) are generated for Service Reauthorization Request, Service Stop, and Quota Return messages. Reports contain statistics since the last report.

If you want to report both IP bytes and usage in seconds, you can specify both **ip csg report usage bytes ip** and **ip csg report usage seconds**.

Examples

The following example shows how to enable supplemental usage reporting for both IP bytes and seconds:

```
ip csg report usage bytes ip
ip csg report usage seconds
```

Related Commands

Command	Description
ip csg report http header	Defines the inclusion of multiple HTTP request headers in the CSG2 HTTP_Header call detail record (CDR).
ip csg report radius attribute	Specifies the RADIUS attributes to be copied from the RADIUS Start message into call detail records (CDRs).
ip csg report smtp rfc2822	Specifies that the CSG2 is to include RFC 2822 header Tag-Length-Values (TLVs) in Simple Mail Transfer Protocol (SMTP) call detail records (CDRs).
ip csg report wap actual-pdu	Specifies whether actual wireless application protocol (WAP) protocol data units (PDUs) are to be reported in CSG2 call detail records (CDRs).

ip csg report wap actual-pdu

To specify whether actual protocol data units (PDUs) are to be reported in CSG2 wireless application protocol (WAP) call detail records (CDRs), use the **ip csg report wap actual-pdu** command in global configuration mode. To exclude actual PDUs from WAP CDRs, use the **no** form of this command.

ip csg report wap actual-pdu

no ip csg report wap actual-pdu

Syntax Description

This command has no arguments or keywords.

Defaults

Actual PDUs are not reported in WAP CDRs.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Examples

The following example shows how to report actual PDUs in WAP CDRs:

```
ip csg report wap actual-pdu
```

Related Commands

Command	Description
ip csg report http header	Defines the inclusion of multiple HTTP request headers in the CSG2 HTTP_Header call detail record (CDR).
ip csg report radius attribute	Specifies the RADIUS attributes to be copied from the RADIUS Start message into call detail records (CDRs).
ip csg report smtp rfc2822	Specifies that the CSG2 is to include RFC 2822 header Tag-Length-Values (TLVs) in Simple Mail Transfer Protocol (SMTP) call detail records (CDRs).
ip csg report usage	Enables CSG2 supplemental usage reporting to the quota server.

ip csg service

To configure a CSG2 content billing service, and to enter CSG2 service configuration mode, use the **ip csg service** command in global configuration mode. To turn off the content billing service, use the **no** form of this command.

ip csg service *service-name*

no ip csg service *service-name*

Syntax Description

service-name	Name of the content billing service, which is a component of a billing plan that is subscribed to by subscribers. The name can be from 1 to 16 characters long, is not case-sensitive, and can include uppercase or lowercase letters (the CSG2 changes all letters to uppercase), numbers, and any special characters.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: None.

Usage Guidelines

The CSG2 allows you to define a pool of up to 1024 services. You can authorize, for each subscriber, any number of services from that pool, but we recommend that the billing system not authorize more than 10 active services for each subscriber. Exceeding this guideline could lead to the following problems:

- The increase in the number of quota authorizations per subscriber can overload both the quota server and the CSG2.
- As the number of services for which a subscriber is actively authorized increases, the subscriber's quota becomes fragmented. Although the CSG2 allows the billing system to recall and redistribute the quota so that the subscriber is not denied service because of quota fragmentation, the process increases overhead in both the quota server and the CSG2.

The CSG2 supports multiple protocols under a single service definition.

The characteristics of each content billing service are defined by the following commands:

- **activation**
- **aoc append url**
- **aoc confirm**
- **aoc enable**

- basis
- class
- content (CSG2 service)
- idle (CSG2 service)
- meter exclude mms wap
- meter exclude pause rtsp
- meter exclude svc-idle
- meter include imap
- meter increment
- meter initial
- meter minimum
- owner
- passthrough
- reauthorization threshold
- reauthorization timeout
- records granularity
- refund
- verify confirm
- verify enable

Examples

The following example shows how to define a CSG2 content billing service named MOVIES:

```
ip csg service MOVIES
```

Related Commands

Command	Description
activation	Specifies the activation mode for a CSG2 Connection Duration service.
aoc append url	Specifies that the CSG2 is to append the original URL to the redirect URL sent by the quota server for use in Advice of Charge (AoC) URL-rewriting.
aoc confirm	Configures a token for use in Advice of Charge (AoC) URL-rewriting.
aoc enable	Enables Advice of Charge (AoC) URL-rewriting for the CSG2.
basis	Specifies the billing basis for a CSG2 content billing service.
content (CSG2 service)	Configures content as a member of a CSG2 billing service, identifies a policy to apply to this content, and optionally assigns a weight to this content.
idle (CSG2 service)	Specifies the minimum amount of time that the CSG2 maintains a service with no subscriber sessions.
ip csg billing	Defines a CSG2 billing plan, and enters CSG2 billing configuration mode.

Command	Description
ip csg refund	Specifies the CSG2 refund policy to apply to the various services, and enters CSG2 refund configuration mode.
meter exclude mms wap	Excludes bytes for a WAP 1.x Multimedia Messaging Service (MMS) session from the CSG2 usage calculation.
meter exclude pause rtsp	Excludes the Real Time Streaming Protocol (RTSP) PAUSE time from the CSG2 usage calculation.
meter exclude svc-idle	Excludes the final service idle from the CSG2 usage calculation.
meter include imap	Specifies which Internet Message Access Protocol (IMAP) bytes are billed for by the CSG2 when doing prepaid debits.
meter increment	Specifies the increments for debiting quota by the CSG2 upon completion of a service configured for Service Duration Billing.
meter initial	Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing.
meter minimum	Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing.
owner	Specifies an identifier or name for a CSG2 service owner.
passthrough	Enables passthrough mode for a CSG2 service.
reauthorization threshold	Specifies the CSG2 reauthorization threshold.
reauthorization timeout	Specifies the CSG2 reauthorization timeout.
records granularity	Specifies the granularity at which CSG2 billing call detail records (CDRs) are to be generated.
refund	Specifies the refund policy for a CSG2 prepaid service.
verify confirm	Configures a token for use in CSG2 service verification URL-rewriting.
verify enable	Enables CSG2 service verification.

ip csg snmp timer

To define Simple Network Management Protocol (SNMP) timers for lost CSG2 records, use the **ip csg snmp timer** command in global configuration mode. To restore the default setting, use the **no** form of this command.

ip csg snmp timer {**bma** | **psd** | **quota-server**} *interval*

no ip csg snmp timer {**bma** | **psd** | **quota-server**} *interval*

Syntax Description

bma	Defines an SNMP timer for lost CSG2 Billing Mediation Agent (BMA) records.
psd	Defines an SNMP timer for lost CSG2 Persistent Storage Device (PSD) records.
quota-server	Defines an SNMP timer for lost CSG2 quota server records.
interval	Interval, in seconds, of the CSG2 SNMP timer. The range is from 1 to 2,147,483,647. The default is 60.

Defaults

The default SNMP timer interval is 60 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The **psd** keyword was added. • The **agent** keyword was replaced with the **bma** keyword.

Examples

The following example defines a 300-second CSG2 SNMP BMA timer:

```
ip csg snmp timer bma 300
```

Related Commands

Command	Description
snmp-server enable traps csg	Enable Simple Network Management Protocol (SNMP) notification types that are available on the CSG2.

ip csg subscriber

To define a subscriber interface as a CSG2 subscriber interface, use the **ip csg subscriber** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

ip csg subscriber

no ip csg subscriber

Syntax Description

This command has no arguments or keywords.

Defaults

The interface is not a CSG2 subscriber interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

All traffic routed through the CSG2, including peer-to-peer traffic, must flow from a subscriber interface to a network interface, or from a network interface to a subscriber interface. Therefore, configure the **ip csg subscriber** command on only the subscriber interface, never on the network interface.

Examples

The following example defines interface GigabitEthernet0/0.69 as a CSG2 subscriber interface:

```
interface GigabitEthernet0/0.69
 ip csg subscriber
```

ip csg transport-type assign

To classify data traffic on the basis of its access path, use the **ip csg transport-type assign command** in global configuration mode. To remove transport-type information, use the **no** form of this command.

ip csg transport-type assign *ip-address value*

no ip csg transport-type assign *ip-address value*

Syntax Description

ip-address	IP address.
value	Transport-type value in the range 1 to 255.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of the command changed from **ip csg transport-type** to **ip csg transport type assign**. • The *ip-address* and *value* arguments were added.

Usage Guidelines

Use the **ip csg transport-type assign** command to classify data traffic on the basis of its access path, using the Network Access Server (NAS) IP address reported in the RADIUS Accounting Start message. Transport-type information is reported in fixed record format call detail records (CDRs).

Examples

The following example creates a transport-type table and enters transport-type configuration mode:

```
ip csg transport-type assign 1.2.3.4 6
```

Related Commands

Command	Description
class	Specifies a service class value.
owner	Specifies an identifier or name for a service owner.
mode	Specifies the mode for a CSG2 billing plan.
ip csg records format	Specifies **variable** or **fixed** CDR format.

ip iscsi target-profile

To create an iSCSI profile for an iSCSI target on the CSG2, and enter iSCSI configuration mode, use the **ip iscsi target-profile** command in global configuration mode. To remove the iSCSI profile, use the **no** form of the command.

ip iscsi target-profile *target-profile-name*

no ip iscsi target-profile *target-profile-name*

Syntax Description

target-profile-name	Name of the iSCSI profile.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)MD	This command was introduced.

Usage Guidelines

You can configure one and only one iSCSI profile on a given CSG2.

The iSCSI profile enables the CSG2 to read/write to a remote iSCSI device (target) on a SAN via an iSCSI.

Note The CSG2 supports only one type of backup device, either a PSD or an iSCSI device. The PSD and iSCSI features can coexist, but only one can be enabled at a time.

The characteristics of each content billing service are defined by the following commands:

- **ip (iSCSI)**
- **name (iSCSI)**
- **port (iSCSI)**
- **session-timeout (iSCSI)**
- **target-portal (iSCSI)**

Examples

The following example configures an iSCSI profile with the name **targetA** to use to store and retrieve CDRs when a charging gateway (CG) is not available:

```
ip iscsi target-profile targetA
  name iqn.2002-10.edu.abc.iol.iscsi.draft20-target:1
  ip 10.0.0.1
  port 3260
  session-timeout 120
```

```
target-portal 1
```

Related Commands

Command	Description
ip (iSCSI)	Specifies the IP address of an iSCSI target in the target interface profile on the CSG2.
ip csg iscsi drain delay	Defines the delay interval, in seconds, before draining packets from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) when the Billing Mediation Agent (BMA) becomes active.
ip csg iscsi drain packet	Defines the number of packets to be drained from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) per drain delay interval when the Billing Mediation Agent (BMA) becomes active.
ip csg iscsi profile	Specifies the Internet Small Computer Systems Interface (iSCSI) target to be used as backup storage for the CSG2.
name (iSCSI)	Specifies the name of an iSCSI target in the target profile on the CSG2
port (iSCSI)	Specifies the number of the port on which to listen for iSCSI traffic in the iSCSI target interface profile on the CSG2.
session-timeout (iSCSI)	Specifies the session timeout for an iSCSI target in the target interface profile on the CSG2.
target-portal (iSCSI)	Specifies the portal group tag for an iSCSI target in the target interface profile on the CSG2.

map

To reference a header, method, or URL map that is part of a CSG2 billing policy, use the **map** command in CSG2 policy configuration mode. To delete the reference, use the **no** form of this command.

map *map-name*

no map *map-name*

Syntax Description

map-name	Name of a header, method, or URL map, as configured with an **ip csg map** command.

Defaults

None

Command Modes

CSG2 policy configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: This command incorporated the following CSG1 commands: • **header-map** • **url-map**

Usage Guidelines

The conditions specified in the referenced header, method, or URL map must be true in order for the flows to be processed by the CSG2 accounting services. If the conditions are not true, the flows are not processed.

When configuring a map, keep the following considerations in mind:

- You cannot specify different types of match patterns in a given map. For example, a map can include one or more **match header** statements, but it cannot include both **match header** statements and **match url** statements.
- You can specify up to three maps in a given policy: one for header matching, one for method matching, and one for URL matching. For example, the following is a valid configuration:

```
ip csg map HOSTMAP
 match header host1 value *.2.*.44
!
ip csg map URLMAP
 match url */mobile/index.wml
!
ip csg policy MAP-POLICY
 map HOSTMAP
 map URLMAP
```

In this example, a flow must match both HOSTMAP and URLMAP in order to match policy MAP-POLICY.

Examples

The following example shows how to reference maps for CSG2 policies MOVIES and GAMES:

```
ip csg policy MOVIES
 map HORROR
 map COMEDY
ip csg policy GAMES
 map GAMES
```

Related Commands

Command	Description
ip csg map	Defines the CSG2 billing content filters (header, method, and URL maps), and enters CSG2 map configuration mode.
ip csg policy	Defines a policy for qualifying flows for the CSG2 billing services, and enters CSG2 policy configuration mode.
match header	Specifies a header match pattern for a CSG2 billing map.
match method	Specifies a method match pattern for a CSG2 billing map.
match url	Specifies a URL match pattern for a CSG2 billing map.

match header

To specify a header match pattern for a CSG2 billing map, use the **match header** command in CSG2 map configuration mode. To delete the header match pattern, use the **no** form of this command.

match header *header-name value*

no match header *header-name value*

Syntax Description

header-name	Header field that is to be matched against the input header. The *header-name* argument is the name of the HTTP header keyword, such as **Content-Type**, **Host**, **Referer**, **User-Agent**, or an arbitrary header name from 1 to 63 characters long. The header name can include uppercase or lowercase letters (the CSG2 changes all letters to uppercase), numbers, and any special characters. **Note** For Session Initiation Protocol (SIP), you must enter the long form of the header name. The CSG2 does not support the short form of the header name.
value	Regular header pattern that is to be matched against the input header. The pattern can include up to 121 characters, minus the length of the header name. For example, if the header name is 7 characters long, the pattern can be up to 114 characters long. The pattern can include wildcards and UNIX string-matching special characters.

Defaults

None.

Command Modes

CSG2 map configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **match (header map)** to **match header**. • The configuration mode for this command changed from CSG header map configuration to CSG2 map configuration. • The **protocol** *protocol* and **value** keywords and arguments were removed. • The *pattern* argument was replaced with the *value* argument.
12.4(15)MD	Support for Session Initiation Protocol (SIP) headers was added.

Usage Guidelines

This command is valid only for HTTP and Session Initiation Protocol (SIP).

You can use more than one **match header** command in CSG2 map configuration mode to specify multiple header match patterns for a header map as follows:

- You can configure more than one **match header** command in a given header map, but they must reference different headers.

  For example, the following is a valid configuration, because the first **match header** command references header **Host** and the other references header **User-Agent**:

  ```
  ip csg map HDR1
   match header Host www.cisco.com
   match header User-Agent myagent
  ```

  But the following is not a valid configuration, because both **match header** commands reference header **Host**:

  ```
  ip csg map HDR1
   match header Host www.cisco.com
   match header Host my.cisco.com
  ```

- If a flow matches *all* of a map's header match patterns, then the CSG2 accepts and processes the flow (unless another map associated with the flow does not match, of course).
- If a flow *does not* match *even one* of a map's header match patterns, then the match fails and the CSG2 does not accept or process the flow.
- The CSG2 treats each header match pattern as a double-wildcard match, which means that a header match pattern that includes even a single wildcard, such as **match header host* 1.2.3.4**, is treated as a triple-wildcard match. You can include more than one wildcard in a CSG2 header match pattern, but doing so greatly increases the memory used for pattern-matching, effectively limiting the number of match patterns that the CSG2 can ultimately support. Therefore, we highly recommend against the use of multiple wildcards in match patterns.
- By default, the header match patterns are case-sensitive. For example, if you define the following header match pattern:

  match header host1 *.2.*.44

  but the actual HTTP header keyword is **HOST1**, then the match fails and the CSG2 does not accept or process the flow.

  If you do not want the header match patterns to be case-sensitive, configure the **no ip csg case-sensitive** command.

You can specify up to 8192 match patterns.

The following table shows and describes the special characters that you can use in the *value* argument in header match patterns.

Convention	Description
*	Zero or more characters.
+	Zero or more repeated instances of the token preceding the +.
?	Zero or one character.

Convention	Description
character	Escaped character. Examples: \? Match on a question mark (\<ctrl-v>?) \+ Match on a plus sign * Match on an asterisk \a Alert (ASCII 7) \b Backspace (ASCII 8) \f Form-feed (ASCII 12) \n New line (ASCII 10) \r Carriage return (ASCII 13) \t Tab (ASCII 9) \v Vertical tab (ASCC 11) \0 Null (ASCII 0) \\ Back slash
Bracketed range [0-9]	Matching any single character from the range.
A leading ^ in a range	Do not match any in the range. All other characters represent themselves.
.\x##	Any ASCII character as specified in two-digit hex notation. For example, \x3f yields a ? for a one-character wild card match.

When configuring a map, keep the following considerations in mind:

- You cannot specify different types of match patterns in a given map. For example, a map can include one or more **match header** statements, but it cannot include both **match header** statements and **match url** statements.
- You can specify up to three maps in a given policy: one for header matching, one for method matching, and one for URL matching. For example, the following is a valid configuration:

```
ip csg map HOSTMAP
 match header host1 value *.2.*.44
!
ip csg map URLMAP
 match url */mobile/index.wml
!
ip csg policy MAP-POLICY
 map HOSTMAP
 map URLMAP
```

  In this example, a flow must match both HOSTMAP and URLMAP in order to match policy MAP-POLICY.

Examples

The following example shows how to specify HTTP header match patterns for map HDR1. In this example, the header match is TRUE *only* for host **www.cisco.com** and user agent **myagent**. Any other combination of host and IP address matches FALSE:

```
ip csg map HDR1
 match header Host www.cisco.com
```

```
match header User-Agent myagent
```

The following example shows how to specify SIP header match patterns for map SIP-HDR1. In this example, the header match is TRUE *only* for Event **presence** and Content-Type **application/sdp**. Any other combination of Event and Content-Type matches FALSE:

```
ip csg map SIP-HDR1
 match header Event presence
 match header Content-Type application/sdp
```

Related Commands

Command	Description
ip csg case-sensitive	Specifies whether to treat CSG2 header, method, and URL match patterns as case-sensitive.
ip csg map	Defines the CSG2 billing content filters (header, method, and URL maps), and enters CSG2 map configuration mode.
ip csg policy	Defines a policy for qualifying flows for the CSG2 billing services, and enters CSG2 policy configuration mode.
map	References a header, method, or URL map that is part of a CSG2 billing policy.
match method	Specifies a method match pattern for a CSG2 billing map.
match url	Specifies a URL match pattern for a CSG2 billing map.

match method

To specify a method match pattern for a CSG2 billing map, use the **match method** command in CSG2 map configuration mode. To delete the match pattern, use the **no** form of this command.

match method *method-name*

no match method *method-name*

Syntax Description

method-name	Method to be matched. Valid methods are: • **connect**—HTTP CONNECT method • **get** —HTTP GET method • **head**—HTTP HEAD method • **invite**—SIP INVITE method • **message**—SIP MESSAGE method • **notify**—SIP NOTIFY method • **options**—SIP OPTIONS method • **post**—HTTP POST method • **register**—SIP REGISTER method • **subscribe**—SIP SUBSCRIBE method • Any other extension method name of 1 to 15 characters

Defaults

None.

Command Modes

CSG2 map configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.
12.4(15)MD	Support for Session Initiation Protocol (SIP) methods was added.

Usage Guidelines

This command is valid only for HTTP and SIP.

You can use more than one **match method** command in CSG2 map configuration mode to specify multiple method match patterns for a method map:

- If a flow matches *any* of a map's method match patterns, then the CSG2 accepts and processes the flow (unless another map associated with the flow does not match, of course).
- If a flow *does not* match *any* of a map's method match patterns, then the match fails and the CSG2 does not accept or process the flow.

- By default, the method match patterns are case-sensitive. For example, if you define the following method match pattern:

  match method get

  but the actual method keyword is **GET**, then the match fails and the CSG2 does not accept or process the flow.

  If you do not want the method match patterns to be case-sensitive, configure the **no ip csg case-sensitive** command.

You can specify up to 8192 match patterns.

The following table shows and describes the special characters that you can use in the *method-name* argument in method match patterns.

Convention	Description
*	Zero or more characters.
+	Zero or more repeated instances of the token preceding the +.
?	Zero or one character.
character	Escaped character. Examples: \? Match on a question mark (\<ctrl-v>?) \+ Match on a plus sign * Match on an asterisk \a Alert (ASCII 7) \b Backspace (ASCII 8) \f Form-feed (ASCII 12) \n New line (ASCII 10) \r Carriage return (ASCII 13) \t Tab (ASCII 9) \v Vertical tab (ASCC 11) \0 Null (ASCII 0) \\ Back slash
Bracketed range [0-9]	Matching any single character from the range.
A leading ^ in a range	Do not match any in the range. All other characters represent themselves.
.\x##	Any ASCII character as specified in two-digit hex notation. For example, \x3f yields a ? for a one-character wild card match.

When configuring a map, keep the following considerations in mind:

- You cannot specify different types of match patterns in a given map. For example, a map can include one or more **match header** statements, but it cannot include both **match header** statements and **match url** statements.

- You can specify up to three maps in a given policy: one for header matching, one for method matching, and one for URL matching. For example, the following is a valid configuration:

```
ip csg map HOSTMAP
 match header host1 value *.2.*.44
!
ip csg map URLMAP
 match url */mobile/index.wml
!
ip csg policy MAP-POLICY
 map HOSTMAP
 map URLMAP
```

  In this example, a flow must match both HOSTMAP and URLMAP in order to match policy MAP-POLICY.

Examples

The following example shows how to specify a GET method match pattern for map MOVIES:

```
ip csg map MOVIES
 match method GET
```

Related Commands

Command	Description
ip csg case-sensitive	Specifies whether to treat CSG2 header, method, and URL match patterns as case-sensitive.
ip csg map	Defines the CSG2 billing content filters (header, method, and URL maps), and enters CSG2 map configuration mode.
ip csg policy	Defines a policy for qualifying flows for the CSG2 billing services, and enters CSG2 policy configuration mode.
map	References a header, method, or URL map that is part of a CSG2 billing policy.
match header	Specifies a header match pattern for a CSG2 billing map.
match url	Specifies a URL match pattern for a CSG2 billing map.

match url

To specify a URL match pattern for a CSG2 billing map, use the **match url** command in CSG2 map configuration mode. To delete the match pattern, use the **no** form of this command.

match url *pattern*

no match url *pattern*

Syntax Description

pattern	Regular URL pattern to be matched against the input URL. The pattern can include up to 127 characters, including wildcards and UNIX string-matching special characters.

Command Modes

CSG2 map configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **match (URL map)** to **match url**. • The configuration mode for this command changed from CSG2 URL map configuration to CSG2 map configuration. • The **protocol** *protocol* and **method** *method* keywords and arguments were removed.
12.4(15)MD	Support for Session Initiation Protocol (SIP) URLs was added.

Usage Guidelines

You can use more than one **match url** command in CSG2 map configuration mode to specify multiple URL match patterns for a URL map:

- If a flow matches *any* of a map's URL match patterns, then the CSG2 accepts and processes the flow (unless an attribute, header, or method map associated with the flow does not match, of course).
- If a flow *does not* match *any* of a map's URL match patterns, then the match fails and the CSG2 does not accept or process the flow.
- By default, the URL match patterns are case-sensitive, and you must consider uppercase and lowercase combinations carefully when you create URL match patterns. For example, if you define the following URL match pattern:

  match url http://*url-string*

  but a subscriber enters the following URL in a web browser:

  HTTP://*url-string*

  then the match fails and the CSG2 does not accept or process the flow.

  If you do not want the URL match patterns to be case-sensitive, configure the **no ip csg case-sensitive** command.

- As a further example, by default the following URLs do not match:

  http://www.cisco.com/index.html

  http://www.cisco.com/INDEX.html

  However, if you have disabled case-sensitivity by entering the **no ip csg case-sensitive** command, then all of the following URLs match:

  http://www.cisco.com/index.html

  http://www.cisco.com/INDEX.html

  http://www.cisco.com/Index.html

  http://www.cisco.com/IndeX.html

  http://www.cisco.com/INdex.html

- When you configure URL match patterns for Real Time Streaming Protocol (RTSP) streams, be sure to account for trailing stream IDs in RTSP stream names. For example, URL match pattern ***.mpeg** does not match **rtsp://1.1.1.254:554/movie.mpeg/streamid=0** because the stream name has a trailing **/streamid=0**. To match such RTSP stream names, use a URL match pattern such as ***.mpeg***.
- You can include more than one wildcard in a CSG2 URL match pattern, but doing so greatly increases the memory used for pattern-matching, effectively limiting the number of match patterns that the CSG2 can ultimately support. Therefore, we highly recommend against the use of multiple wildcards in match patterns.
- When using wildcards in URL match patterns, observe the following guidelines to optimize the performance of the CSG2:
  - Minimize the number of URL match patterns that are applied to a CSG2 content configuration.
  - Minimize the number of keyword URL match patterns that you use. In general, it is better to use multiple single-wildcard URL match patterns instead of individual keyword URL match patterns.
  - Combine several keyword URL match patterns into a single pattern by using UNIX string-matching special characters. For example, ***.movies_comedy.com/*.mpeg**, ***.movies_action.com/*.mpeg**, and ***.movies_drama.com/*.mpeg** can be combined into the following single pattern:

    ***.movies_(comedy|action|drama).com/*.mpeg**

    And these patterns

    ***.movies_comedy.com/*.mpeg**

    ***.movies_action.com/*.mpeg**

    ***.movies_drama.com/*.mpeg**

    ***.clips_comedy.com/*.mpeg**

    ***.clips_action.com/*.mpeg**

    ***.clips_drama.com/*.mpeg**

    can be combined into the following single pattern:

    ***.(movies|clips)*?*(comedy|action|drama).com/*.mpeg**

– Do not forget that the entire pattern, including wildcards and UNIX string-matching special characters, cannot exceed 128 characters.

You can specify up to 8192 match patterns.

The following table shows and describes the special characters that you can use in the *pattern* argument in URL match patterns.

Convention	Description
*	Zero or more characters.
+	Zero or more repeated instances of the token preceding the +.
?	Zero or one character.
character	Escaped character. Examples: \? Match on a question mark (\<ctrl-v>?) \+ Match on a plus sign * Match on an asterisk \a Alert (ASCII 7) \b Backspace (ASCII 8) \f Form-feed (ASCII 12) \n New line (ASCII 10) \r Carriage return (ASCII 13) \t Tab (ASCII 9) \v Vertical tab (ASCC 11) \0 Null (ASCII 0) \\ Back slash
Bracketed range [0-9]	Matching any single character from the range.
A leading ^ in a range	Do not match any in the range. All other characters represent themselves.
.\x##	Any ASCII character as specified in two-digit hex notation. For example, \x3f yields a ? for a one-character wild card match.

For WAP, the CSG2 supports only URL maps. Header maps and method maps are not supported.

When configuring a map, keep the following considerations in mind:

- We recommend that you configure the URL match pattern during your maintenance window, or during off-peak hours.
- You cannot specify different types of match patterns in a given map. For example, a map can include one or more **match header** statements, but it cannot include both **match header** statements and **match url** statements.
- You can specify up to three maps in a given policy: one for header matching, one for method matching, and one for URL matching. For example, the following is a valid configuration:

```
ip csg map HOSTMAP
 match header host1 value *.2.*.44
!
ip csg map URLMAP
```

```
 match url */mobile/index.wml
!
ip csg policy MAP-POLICY
 map HOSTMAP
 map URLMAP
```

In this example, a flow must match both HOSTMAP and URLMAP in order to match policy MAP-POLICY.

Examples

The following example shows how to specify URL match patterns for map MOVIES. In this example, the URL match is TRUE for ***.movies_comedy.com/*.mpeg**, for ***.movies_action.com/*.mpeg**, for ***.movies_drama.com/*.mpeg**, and for any other URLs that match the pattern:

```
ip csg map MOVIES
 match url *.movies_(comedy|action|drama).com/*.mpeg
ip csg map IMAGES
 match url *.(gif|jpg)
```

Related Commands

Command	Description
ip csg case-sensitive	Specifies whether to treat CSG2 header, method, and URL match patterns as case-sensitive.
ip csg map	Defines the CSG2 billing content filters (header, method, and URL maps), and enters CSG2 map configuration mode.
ip csg policy	Defines a policy for qualifying flows for the CSG2 billing services, and enters CSG2 policy configuration mode.
map	References a header, method, or URL map that is part of a CSG2 billing policy.
match header	Specifies a header match pattern for a CSG2 billing map.
match method	Specifies a method match pattern for a CSG2 billing map.

meter exclude control sip

To exclude call control packets for a Session Initiation Protocol (SIP) session from the CSG2 usage calculation, use the **meter exclude control sip** command in CSG2 service configuration mode. To return to the default behavior, use the **no** form of the command.

meter exclude control sip

no meter exclude control sip

Syntax Description

This command has no arguments or keywords.

Defaults

The default behavior is to include the SIP call control packets in the usage calculation.

Command Modes

CSG2 service configuration

Command History

Release	Modification
12.4(15)MD	This command was introduced.

Usage Guidelines

The **meter exclude control sip** command and the **basis second** command in CSG2 service configuration mode are mutually exclusive. If you configure the **meter exclude control sip** command, do not configure the **basis second** command.

Examples

The following example shows how to exclude the call control packets for a SIP session from the usage calculation for the SERVICE-A service:

```
ip csg service SERVICE-A
 meter exclude control sip
```

Related Commands

Command	Description
ip csg service	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.
meter exclude mms wap	Excludes bytes for a WAP 1.x Multimedia Messaging Service (MMS) session from the CSG2 usage calculation.
meter exclude network-init sip	Excludes incoming Session Initiation Protocol (SIP) transactions (that is, those that are initiated from the network) from the CSG2 usage calculation.
meter exclude pause rtsp	Excludes the Real Time Streaming Protocol (RTSP) PAUSE time from the CSG2 usage calculation.
meter exclude svc-idle	Excludes the final service idle from the CSG2 usage calculation.

Command	Description
meter include imap	Specifies which Internet Message Access Protocol (IMAP) bytes are billed for by the CSG2 when doing prepaid debits.
meter increment	Specifies the increments for debiting quota by the CSG2 upon completion of a service configured for Service Duration Billing.
meter initial	Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing.
meter minimum	Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing.

meter exclude mms wap

To exclude bytes for a WAP 1.x Multimedia Messaging Service (MMS) session from the CSG2 usage calculation, use the **meter exclude mms wap** command in CSG2 service configuration mode. To return to the default behavior, use the **no** form of the command.

meter exclude mms wap

no meter exclude mms wap

Syntax Description

This command has no arguments or keywords.

Defaults

The default behavior is to include the MMS in the usage calculation.

Command Modes

CSG2 service configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1.
	Changes from CSG1: The **meter exclude** command split into three new commands—**meter exclude mms wap**, **meter exclude pause rtsp**, and **meter exclude svc-idle**.

Usage Guidelines

The **meter exclude mms wap** command and the **basis second** command in CSG2 service configuration mode are mutually exclusive. If you configure the **meter exclude mms wap** command, do not configure the **basis second** command.

Examples

The following example shows how to exclude the bytes for a WAP 1.x MMS session from the usage calculation for the SERVICE-A service:

```
ip csg service SERVICE-A
 meter exclude mms wap
```

Related Commands

Command	Description
ip csg service	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.
meter exclude control sip	Excludes call control packets for a Session Initiation Protocol (SIP) session from the CSG2 usage calculation.
meter exclude network-init sip	Excludes incoming Session Initiation Protocol (SIP) transactions (that is, those that are initiated from the network) from the CSG2 usage calculation.

Command	Description
meter exclude pause rtsp	Excludes the Real Time Streaming Protocol (RTSP) PAUSE time from the CSG2 usage calculation.
meter exclude svc-idle	Excludes the final service idle from the CSG2 usage calculation.
meter include imap	Specifies which Internet Message Access Protocol (IMAP) bytes are billed for by the CSG2 when doing prepaid debits.
meter increment	Specifies the increments for debiting quota by the CSG2 upon completion of a service configured for Service Duration Billing.
meter initial	Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing.
meter minimum	Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing.

meter exclude network-init sip

To exclude incoming Session Initiation Protocol (SIP) transactions (that is, those that are initiated from the network) from the CSG2 usage calculation, use the **meter exclude network-init sip** command in CSG2 service configuration mode. To return to the default behavior, use the **no** form of the command.

meter exclude network-init sip

no meter exclude network-init sip

Syntax Description

This command has no arguments or keywords.

Defaults

The default behavior is to include incoming SIP transactions in the usage calculation.

Command Modes

CSG2 service configuration

Command History

Release	Modification
12.4(15)MD	This command was introduced.

Examples

The following example shows how to exclude incoming SIP transactions from the usage calculation for the SERVICE-A service:

```
ip csg service SERVICE-A
 meter exclude network-init sip
```

Related Commands

Command	Description
ip csg service	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.
meter exclude control sip	Excludes call control packets for a Session Initiation Protocol (SIP) session from the CSG2 usage calculation.
meter exclude mms wap	Excludes bytes for a WAP 1.x Multimedia Messaging Service (MMS) session from the CSG2 usage calculation.
meter exclude pause rtsp	Excludes the Real Time Streaming Protocol (RTSP) PAUSE time from the CSG2 usage calculation.
meter exclude svc-idle	Excludes the final service idle from the CSG2 usage calculation.
meter include imap	Specifies which Internet Message Access Protocol (IMAP) bytes are billed for by the CSG2 when doing prepaid debits.
meter increment	Specifies the increments for debiting quota by the CSG2 upon completion of a service configured for Service Duration Billing.

Command	Description
meter initial	Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing.
meter minimum	Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing.

meter exclude pause rtsp

To exclude the Real Time Streaming Protocol (RTSP) PAUSE time from the CSG2 usage calculation, use the **meter exclude pause rtsp** command in CSG2 service configuration mode. To return to the default behavior, use the **no** form of the command.

meter exclude pause rtsp

no meter exclude pause rtsp

Syntax Description

This command has no arguments or keywords.

Defaults

The default behavior is to include the RTSP PAUSE time in the usage calculation.

Command Modes

CSG2 service configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1.
	Changes from CSG1: The **meter exclude** command split into three new commands—**meter exclude mms wap**, **meter exclude pause rtsp**, and **meter exclude svc-idle**.

Usage Guidelines

You must configure **basis second** before configuring this command.

Examples

The following example shows how to exclude the RTSP PAUSE time from the usage calculation for the SERVICE-A service:

```
ip csg service SERVICE-A
 basis second
 meter exclude pause rtsp
```

Related Commands

Command	Description
ip csg service	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.
meter exclude control sip	Excludes call control packets for a Session Initiation Protocol (SIP) session from the CSG2 usage calculation.
meter exclude mms wap	Excludes bytes for a WAP 1.x Multimedia Messaging Service (MMS) session from the CSG2 usage calculation.
meter exclude network-init sip	Excludes incoming Session Initiation Protocol (SIP) transactions (that is, those that are initiated from the network) from the CSG2 usage calculation.

Command	Description
meter exclude svc-idle	Excludes the final service idle from the CSG2 usage calculation.
meter include imap	Specifies which Internet Message Access Protocol (IMAP) bytes are billed for by the CSG2 when doing prepaid debits.
meter increment	Specifies the increments for debiting quota by the CSG2 upon completion of a service configured for Service Duration Billing.
meter initial	Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing.
meter minimum	Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing.

meter exclude svc-idle

To exclude the final service idle from the CSG2 usage calculation, use the **meter exclude svc-idle** command in CSG2 service configuration mode. To return to the default behavior, use the **no** form of the command.

meter exclude svc-idle

no meter exclude svc-idle

Syntax Description

This command has no arguments or keywords.

Defaults

The default behavior is to include the service-idle in the usage calculation.

Command Modes

CSG2 service configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1.
	Changes from CSG1: The **meter exclude** command split into three new commands—**meter exclude mms wap**, **meter exclude pause rtsp**, and **meter exclude svc-idle**.

Usage Guidelines

Configuration of this command can result in reduced charging because the next service access occurs after the service idles, rather than occurring before the service idles.

You cannot configure both **meter exclude svc-idle** and **basis byte** or **basis fixed** in the same service. Only **basis second** is meaningful with **meter exclude svc-idle**.

Examples

The following example shows how to exclude the final service idle from the usage calculation for the OFF_NET service:

```
ip csg service OFF_NET
 meter exclude svc-idle
```

Related Commands

Command	Description
ip csg service	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.
meter exclude control sip	Excludes call control packets for a Session Initiation Protocol (SIP) session from the CSG2 usage calculation.
meter exclude mms wap	Excludes bytes for a WAP 1.x Multimedia Messaging Service (MMS) session from the CSG2 usage calculation.

Command	Description
meter exclude network-init sip	Excludes incoming Session Initiation Protocol (SIP) transactions (that is, those that are initiated from the network) from the CSG2 usage calculation.
meter exclude pause rtsp	Excludes the Real Time Streaming Protocol (RTSP) PAUSE time from the CSG2 usage calculation.
meter include imap	Specifies which Internet Message Access Protocol (IMAP) bytes are billed for by the CSG2 when doing prepaid debits.
meter increment	Specifies the increments for debiting quota by the CSG2 upon completion of a service configured for Service Duration Billing.
meter initial	Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing.
meter minimum	Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing.

meter include imap

To specify which Internet Message Access Protocol (IMAP) bytes are billed for by the CSG2 when doing prepaid debits, use the **meter include imap** command in CSG2 service configuration mode. To return to the default behavior, use the **no** form of the command.

meter include imap body {**header** | **only** | **other**}

no meter include imap

Syntax Description

body header	Only BODY and HEADER IMAP bytes are to be counted when performing prepaid debits.
body only	Only BODY IMAP bytes are to be counted when performing prepaid debits.
body other	Only BODY and OTHER IMAP bytes are to be counted when performing prepaid debits.

Defaults

All IMAP bytes are to be counted when performing prepaid debits.

Command Modes

CSG2 service configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **meter imap** to **meter include imap**. • The **body-header**, **body-only**, and **body-other** keywords changed to **body header**, **body only**, and **body other**, respectively.

Usage Guidelines

You can configure only one **meter include imap** command per service. The billing basis for the service must be **byte**. The three categories of bytes are BODY, HEADER, and OTHER, determined as follows:

- BODY—The bytes are classified as BODY if a fetch request or response is encountered for one of the following specifications (including any appended "<>" subset variants):
  - BODY[]
  - BODY[#]
  - BODY[TEXT]
  - BODY[#.TEXT]
  - BODY.PEEK[]
  - BODY.PEEK[#]
  - BODY.PEEK[TEXT]

  - BODY.PEEK[#.TEXT]
  - RFC822
  - RFC822.TEXT
- HEADER—If the bytes cannot be classified as BODY, then they are classified as HEADER if a fetch request or response is encountered for one of the following specifications (including any appended "<>" subset variants):
  - BODY[HEADER]
  - BODY[#.HEADER]
  - BODY.PEEK[HEADER]
  - BODY.PEEK[#.HEADER]
  - RFC822.HEADER
- OTHER—If request or response cannot be classified as BODY or HEADER, then it is classified as OTHER. OTHER examples include:
  - SYN/FIN/ACK/RST packets that do not contain a payload
  - Non-HEADER or BODY IMAP commands such as **3 select inbox**
  - Retransmitted packets
  - Anything else that is not considered BODY or HEADER
  - If the session becomes encrypted or enters PASSTHRU mode, subsequent packets for the session cannot be parsed and are treated as OTHER.

Because IMAP metering is byte-based, you cannot configure both **meter include imap** and **basis fixed** or **basis second** in the same service. Only **basis byte** is meaningful with **meter include imap**.

Examples

The following example shows how to configure IMAP to count only BODY bytes when performing prepaid debits:

```
ip csg service S1
 meter include imap body only
```

Related Commands

Command	Description
ip csg service	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.
meter exclude control sip	Excludes call control packets for a Session Initiation Protocol (SIP) session from the CSG2 usage calculation.
meter exclude mms wap	Excludes bytes for a WAP 1.x Multimedia Messaging Service (MMS) session from the CSG2 usage calculation.
meter exclude network-init sip	Excludes incoming Session Initiation Protocol (SIP) transactions (that is, those that are initiated from the network) from the CSG2 usage calculation.
meter exclude pause rtsp	Excludes the Real Time Streaming Protocol (RTSP) PAUSE time from the CSG2 usage calculation.
meter exclude svc-idle	Excludes the final service idle from the CSG2 usage calculation.

Command	Description
meter increment	Specifies the increments for debiting quota by the CSG2 upon completion of a service configured for Service Duration Billing.
meter initial	Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing.
meter minimum	Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing.

meter increment

To specify the increments for debiting quota by the CSG2 upon completion of a service configured for Service Duration Billing, use the **meter increment** command in CSG2 service configuration mode. To restore the default behavior, use the **no** form of the command.

meter increment *value*

no meter increment *value*

Syntax Description

value	Increment, in seconds, for debiting quota upon completion of a service configured for Service Duration Billing. For example, to enable the CSG2 to charge quota per minute instead of per second, specify **meter increment 60**. The range is from 1 to 65535. The default value is 1.

Defaults

The default increment is 1 second.

Command Modes

CSG2 service configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: None.

Usage Guidelines

If **basis second** is configured for the service, the network usage (usage excluding the initial charge) is rounded up to the nearest integer multiple of the increment value when the Service Stop is sent. For an increment value of 60, the CSG2 does not round up 120 seconds of network usage; however, the CSG2 does round up, say, 163 seconds of network usage to 180 quadrans before it calculates total usage for reporting in the Service Stop.

Note The rounding-up of network usage is not reflected in calculations for the Usage Tag-Length-Value (TLV) in Service Reauthorization Requests.

The increment value is considered when determining whether sufficient quota exists for granting network access for a session. For instance, if the increment is 60, the network usage is 50, and the balance is 10, network access is permitted. However, if the increment is 60, the network usage is 70, and the balance is 10, network access is not permitted because the balance is not sufficient to satisfy the entire increment (that is, a minimum of 1 minute of quota would be required to allow access for a portion of the minute).

Examples

The following example shows how to configure quota debit increments for Service Duration Billing for the OFF_NET service.

```
ip csg service OFF_NET
 meter increment 100
```

Related Commands

Command	Description
ip csg service	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.
meter exclude control sip	Excludes call control packets for a Session Initiation Protocol (SIP) session from the CSG2 usage calculation.
meter exclude mms wap	Excludes bytes for a WAP 1.x Multimedia Messaging Service (MMS) session from the CSG2 usage calculation.
meter exclude network-init sip	Excludes incoming Session Initiation Protocol (SIP) transactions (that is, those that are initiated from the network) from the CSG2 usage calculation.
meter exclude pause rtsp	Excludes the Real Time Streaming Protocol (RTSP) PAUSE time from the CSG2 usage calculation.
meter exclude svc-idle	Excludes the final service idle from the CSG2 usage calculation.
meter include imap	Specifies which Internet Message Access Protocol (IMAP) bytes are billed for by the CSG2 when doing prepaid debits.
meter initial	Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing.
meter minimum	Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing.

meter initial

To specify the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing, use the **meter initial** command in CSG2 service configuration mode. To restore the default behavior, use the **no** form of the command.

meter initial *value*

no meter initial *value*

Syntax Description

value	Initial quota, in quadrans, debited from the balance at the beginning of a service when the service is configured for Service Duration Billing. The debit occurs when the CSG2 grants the first network access for a session that has been mapped to the service. The initial value is not rounded up to the nearest increment value. The range is from 0 to 65535. The default value is 0.

Defaults

The default quota is 0 quadrans.

Command Modes

CSG2 service configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: None.

Usage Guidelines

This command allows “connection setup charges” to be applied to a service.

The debit occurs when the CSG2 grants the first access for the service. The initial value is not rounded up to the nearest increment value.

Examples

The following example shows how to configure an initial quota debit for the OFF_NET service.

```
ip csg service OFF_NET
 meter initial 60
```

Related Commands

Command	Description
ip csg service	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.
meter exclude control sip	Excludes call control packets for a Session Initiation Protocol (SIP) session from the CSG2 usage calculation.

Command	Description
meter exclude mms wap	Excludes bytes for a WAP 1.x Multimedia Messaging Service (MMS) session from the CSG2 usage calculation.
meter exclude network-init sip	Excludes incoming Session Initiation Protocol (SIP) transactions (that is, those that are initiated from the network) from the CSG2 usage calculation.
meter exclude pause rtsp	Excludes the Real Time Streaming Protocol (RTSP) PAUSE time from the CSG2 usage calculation.
meter exclude svc-idle	Excludes the final service idle from the CSG2 usage calculation.
meter include imap	Specifies which Internet Message Access Protocol (IMAP) bytes are billed for by the CSG2 when doing prepaid debits.
meter increment	Specifies the increments for debiting quota by the CSG2 upon completion of a service configured for Service Duration Billing.
meter minimum	Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing.

meter minimum

To specify the minimum number of quadrans debited by the CSG2 for a service or session, use the **meter minimum** command in CSG2 service configuration mode. To return to the default behavior, use the **no** form of the command.

meter minimum *value*

no meter minimum *value*

Syntax Description

value	Minimum number of quadrans debited for a service or session, excluding the value in **meter initial**. For example, to force the CSG2 to debit 90 quadrans when less than 90 quadrans of network usage were used for the service, specify **meter minimum 90**. If the initial value is 20 quadrans and the minimum is 90 quadrans, then the minimum total charge is 110 quadrans. The minimum value is applied only if at least 1 session is granted network access for the service. The range is from 0 to 65535. The default value is 0.

Defaults

The default number is 0 quadrans.

Command Modes

CSG2 service configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: None.

Usage Guidelines

If **meter initial** is set to 20 quadrans, and **meter minimum** is set to 90 quadrans, then the minimum total charge is 110 quadrans.

If service duration is configured in the **basis** command, the usage is rounded up to the minimum value when the Service Stop is sent. For a minimum value of 90, 150 seconds of network usage is not rounded up for the purpose of calculating usage in the Service Stop, but, for example, 63 seconds of network usage is rounded up to 90 quadrans.

Note The rounding-up of network usage is not reflected in calculations for the Usage Tag-Length-Value (TLV) in Service Reauthorization Requests.

Examples

The following example shows how to configure a minimum debit for the OFF_NET service.

```
ip csg service OFF_NET
 meter minimum 60
```

Related Commands

Command	Description
ip csg service	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.
meter exclude control sip	Excludes call control packets for a Session Initiation Protocol (SIP) session from the CSG2 usage calculation.
meter exclude mms wap	Excludes bytes for a WAP 1.x Multimedia Messaging Service (MMS) session from the CSG2 usage calculation.
meter exclude network-init sip	Excludes incoming Session Initiation Protocol (SIP) transactions (that is, those that are initiated from the network) from the CSG2 usage calculation.
meter exclude pause rtsp	Excludes the Real Time Streaming Protocol (RTSP) PAUSE time from the CSG2 usage calculation.
meter exclude svc-idle	Excludes the final service idle from the CSG2 usage calculation.
meter include imap	Specifies which Internet Message Access Protocol (IMAP) bytes are billed for by the CSG2 when doing prepaid debits.
meter increment	Specifies the increments for debiting quota by the CSG2 upon completion of a service configured for Service Duration Billing.
meter initial	Specifies the initial quota debited by the CSG2 from the balance at the beginning of a service when the service is configured for Service Duration Billing.

mode

To specify the mode for a CSG2 billing plan, use the **mode** command in CSG2 billing configuration mode. To use the default mode, use the **no** form of this command.

mode [**postpaid** | **prepaid**]

no mode

Syntax Description

postpaid	(Optional) Specifies a postpaid billing plan.
prepaid	(Optional) Specifies a prepaid billing plan. This is the default setting.

Defaults

The default mode is **prepaid**.

Command Modes

CSG2 billing configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: None.

Usage Guidelines

The **mode** command with the **postpaid** keyword is used with both fixed-record format and variable-record format to enable service correlation of postpaid CDRs.

Examples

The following example specifies postpaid mode for CSG2 billing plan REGULAR

```
ip csg billing REGULAR
 mode postpaid
```

Related Commands

Command	Description
class	Specifies a service class value.
entries user idle	Sets the time after which entries for idle subscribers are deleted from the CSG2 User Table.
ip csg billing	Defines a CSG2 billing plan, and enters CSG2 billing configuration mode.
ip csg transport-type assign	Classifies data traffic on the basis of its access path.
owner	Specifies an identifier or name for a service owner.
ip csg records format	Specifies **variable** or **fixed** call detail record (CDR) format.
service	Associates a service with a CSG2 billing plan.

mode tcp

To specify the mode for CSG2 TCP sessions, use the **mode tcp** command in CSG2 content configuration mode. To use the default mode, use the **no** form of this command.

mode tcp {**datagram** | **transparent** [**zero**]}

no mode tcp

Syntax Description

datagram	Specifies that the CSG2 is to treat TCP sessions as datagrams.
transparent	Specifies that the CSG2 is to treat TCP sessions as transparent.
zero	(Optional) Specifies that TCP bytes are not to be reported for transparent TCP sessions.

Defaults

If you do not configure this command, the CSG2 treats TCP sessions as transparent, forwarding all TCP packets, including out-of-order packets, and reporting all new and retransmitted TCP payload bytes.

Command Modes

CSG2 content configuration

Command History

Release	Modification
12.4(11)MD6	This command was introduced.

Usage Guidelines

The **mode tcp** command is valid only if the **parse protocol other** command is also specified for the content.

If you configure the **mode tcp transparent** command, the CSG2 forwards all TCP packets, including out-of-order packets, and reports all new and retransmitted TCP payload bytes. If you also configure the optional **zero** keyword, the CSG2 reports zero TCP bytes. The CSG2 uses TCP signals to establish and terminate the TCP sessions.

If you configure the **mode tcp datagram** command, the CSG2 forwards all TCP packets, including out-of-order packets, and reports zero TCP payload bytes. Each TCP session is established by the first SYN, and terminated by the content's idle timer.

Examples

The following example specifies transparent mode for TCP sessions for CSG2 content VPN:

```
ip csg content VPN
 ip any tcp 10000
 mode tcp transparent
```

Related Commands

Command	Description
ip csg content	Configures content for CSG2 services, and enters CSG2 content configuration mode.

name (iSCSI)

To specify the name of an iSCSI target in the target profile on the CSG2, use the **name** command in iSCSI configuration mode. To remove the IP address configuration, use the **no** form of the command.

name *target-name*

no name *target-name*

Syntax Description

target-name	Name of the iSCSI target.

Command Default

No default behavior or values.

Command Modes

iSCSI configuration

Command History

Release	Modification
12.4(15)MD	This command was introduced.

Examples

The following example configures an iSCSI target interface profile with the name **targetA** to a SCSI target named **iqn.2002-10.edu.abc.iol.iscsi.draft20-target:1** :

```
ip iscsi target-profile targetA
  name iqn.2002-10.edu.abc.iol.iscsi.draft20-target:1
  ip 10.0.0.1
  port 3260
  session-timeout 120
  target-portal 1
```

Related Commands

Command	Description
ip (iSCSI)	Specifies the IP address of an iSCSI target in the target interface profile on the CSG2.
ip csg iscsi drain delay	Defines the delay interval, in seconds, before draining packets from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) when the Billing Mediation Agent (BMA) becomes active.
ip csg iscsi drain packet	Defines the number of packets to be drained from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) per drain delay interval when the Billing Mediation Agent (BMA) becomes active.
ip csg iscsi profile	Specifies the Internet Small Computer Systems Interface (iSCSI) target to be used as backup storage for the CSG2.

Command	Description
ip iscsi target-profile	Creates an iSCSI profile for an iSCSI target on the CSG2, and enters iSCSI configuration mode.
port (iSCSI)	Specifies the number of the port on which to listen for iSCSI traffic in the iSCSI target interface profile on the CSG2.
session-timeout (iSCSI)	Specifies the session timeout for an iSCSI target in the target interface profile on the CSG2.
target-portal (iSCSI)	Specifies the portal group tag for an iSCSI target in the target interface profile on the CSG2.

next-hop

To define a next-hop IP address, use the **next-hop** command in CSG2 content configuration mode. To delete the next-hop IP address, use the **no** form of this command.

next-hop *ip-address* [**reverse**] [**subscriber media**]

no next-hop *ip-address* [**reverse**] [**subscriber media**]

Syntax Description

ip-address	IP address of the next hop for packets sourced by the flow initiator.
reverse	(Optional) IP address of the next hop for packets sent to the flow initiator.
subscriber media	(Optional) IP address of the next hop for packets sent from the subscriber for Session Initiation Protocol (SIP) media.

Defaults

None

Command Modes

CSG2 content configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The configuration mode for this command changed from CSG policy configuration to CSG2 content configuration. • The **reverse** keyword was added.
12.4(15)MD	The **subscriber media** keywords were added.

Usage Guidelines

You can configure one forward next-hop, and one reverse next-hop.

Note Even if you have defined a next-hop IP address, traffic that matches the "default" content might not be routed with next-hop.

The **subscriber media** option affects only SIP media sessions (used for subscriber-to-subscriber traffic). If the **subscriber media** option is not configured, SIP media sessions use the values defined for **next-hop** or **next-hop reverse**.

Examples

The following example specifies next-hop for CSG2 content MOVIES:

```
ip csg content MOVIES
 next-hop 1.2.3.4
 next-hop 9.8.7.6 reverse
 Next-hop 2.3.4.5 subscriber media
```

Related Commands

Command	Description
client-group (CSG2 content)	References a standard access list that is part of a CSG2 content.
ip csg content	Configures content for CSG2 services, and enters CSG2 content configuration mode.

owner

To specify an identifier or name for a CSG2 service owner, use the **owner** command in CSG2 service configuration mode. To remove the owner ID or name, use the **no** form of this command.

owner {**id** *id* | **name** *name*}

no owner {**id** | **name**}

Syntax Description

id *id*	1- to 15-character string that identifies a service owner.
name *name*	1- to 38-character string that specifies the name of the service.

Defaults

None

Command Modes

CSG2 service configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: This command incorporated the following CSG1 commands: • **owner id** • **owner name**

Usage Guidelines

Use this command with fixed-record format to identify a service owner.

Examples

The following example specifies an owner ID for the CSG2 service A1:

```
ip csg service A1
 owner id ABC123456
```

Related Commands

Command	Description
class	Specifies a service class value.
ip csg service	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.
ip csg transport-type assign	Classifies data traffic on the basis of its access path.
mode	Specifies the mode for a CSG2 billing plan.
ip csg records format	Specifies variable or fixed CDR format.

parse length

To define the maximum number of Layer 7 bytes that the CSG2 is to parse when attempting to assign a policy, use the **parse length** command in CSG2 content configuration mode. To restore the default setting, use the **no** form of this command.

parse length *number*

no parse length

Syntax Description

number	Maximum number of Layer 7 bytes to parse. The range is from 1 to 65535. The default value is 4000.

Defaults

The CSG2 parses up to 4000 Layer 7 bytes when attempting to assign a policy.

Command Modes

CSG2 content configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

If the parse length is exceeded, the CSG2 blocks or forwards packets on the basis of the **block** command.

This command is valid only if **parse protocol http** is also configured.

Examples

The following example specifies that the CSG2 is to parse up to 1234 Layer 7 bytes when attempting to assign a policy:

```
ip csg content MOVIES
 parse protocol http
 parse length 1234
```

Related Commands

Command	Description
block	Forces the CSG2 to drop packets that do not match a configured billing policy.
ip csg content	Configures content for CSG2 services, and enters CSG2 content configuration mode.
parse protocol	Defines how the CSG2 is to parse traffic for a content.

parse protocol

To define how the CSG2 is to parse traffic for a content, use the **parse protocol** command in CSG2 content configuration mode. To restore the default setting, use the **no** form of this command.

parse protocol {ftp | http | imap | other | pop3 | rtsp | sip | smtp | wap {connection-oriented | connectionless}}

no parse protocol

Syntax Description

ftp	FTP traffic, with Layer 7 inspection of FTP control sessions.
http	HTTP traffic.
imap	Internet Message Access Protocol (IMAP) traffic.
other	Some other type of IP traffic, such as IP, TCP, or User Datagram Protocol (UDP). This is the default setting.
pop3	Post Office Protocol, version 3 (POP3) traffic.
rtsp	Real Time Streaming Protocol (RTSP) traffic.
sip	Session Initiation Protocol (SIP) traffic.
smtp	Simple Mail Transfer Protocol (SMTP) traffic.
wap	Wireless application protocol traffic.
connection-oriented	Defines the WAP traffic as connection-oriented.
connectionless	Defines the WAP traffic as connectionless.

Defaults

The CSG2 parses the traffic as some other type of IP traffic, such as IP, TCP, or User Datagram Protocol (UDP).

Command Modes

CSG2 content configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.
12.4(15)MD	The **ftp** and **sip** keywords were added.

Examples

The following example specifies that the CSG2 is to parse traffic for this content as HTTP traffic:

```
ip csg content MOVIES
 parse protocol http
```

Related Commands

Command	Description
ip csg content	Configures content for CSG2 services, and enters CSG2 content configuration mode.
parse length	Defines the maximum number of Layer 7 bytes that the CSG2 is to parse when attempting to assign a policy.
subscriber-ip http-header forwarded-for	Specifies that the CSG2 is to obtain the subscriber's IP address from the HTTP X-Forwarded-For header.

passthrough

To enable passthrough mode for a CSG2 service, use the **passthrough** command in CSG2 service configuration mode. To disable passthrough mode, use the **no** form of this command.

passthrough *quota-grant*

no passthrough

Syntax Description

quota-grant	Size of each quota grant to give to the service. The *quota-grant* is also called the default quota. The range is from 1 to 2147483647.

Defaults

None

Command Modes

CSG2 service configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: None.

Usage Guidelines

Use this command to enable the CSG2 to grant quota to the service when at least one quota server is configured, but none are active.

Examples

The following example specifies that the CSG2 grants 65535 quadrans of quota to the service NAME each time the service runs low on quota:

```
ip csg service NAME
 passthrough 65535
```

Related Commands

Command	Description
ip csg service	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.

pending

To set the pending connection timeout, use the **pending** command in CSG2 content configuration mode. To restore the default, use the no form of this command.

pending *timeout*

no pending

Syntax Description

timeout	Time, in seconds, to wait for a response to an initial synchronization sequence number (SYN) on a TCP session. The range is from 4 to 65535. The default value is 30.

Defaults

The default pending connection timeout is 30 seconds.

Command Modes

CSG2 content configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: None.

Examples

This example shows how to set the pending connection timer for a CSG2 content:

```
ip csg content MOVIES_COMEDY
 pending 300
```

Related Commands

Command	Description
idle (CSG2 content)	Specifies the minimum amount of time that the CSG2 maintains an idle content connection.
ip csg content	Configures content for CSG2 services, and enters CSG2 content configuration mode.
show ip csg	Displays information about the CSG2.

policy (CSG2 content)

To reference a CSG2 billing policy, use the **policy** command in CSG2 content configuration mode. To delete a policy reference, use the **no** form of this command.

policy *policy-name* [**priority** *priority-number*]

no policy *policy-name*

Syntax Description

policy-name	Name of a configured CSG2 billing policy.
priority *priority-number*	(Optional) Priority of the policy. The priority specifies the order of preference of the policy. A lower number indicates a higher priority. If the current policy becomes unusable, the CSG2 uses the highest priority policy (that is, the policy with the lowest priority number) available. In the same content, all policies must have different priorities. Priorities for different policies do not have to be sequential. That is, you can have three policies with priorities 1, 5, and 10. The range of priorities is 1 to 511.

Defaults

No policy is configured.
If you do not specify a priority for the policy, no priority is configured. The CSG2 lists and prioritizes the policy sequentially, in the order in which it was configured.

Command Modes

CSG2 content configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: None.
12.4(15)MD	The **priority** keyword and the *priority-number* argument were added.

Usage Guidelines

If accounting records are to be generated for flows matching this policy, you must configure the **accounting** command in CSG2 policy configuration mode. If you do not want to bill for flows matching this policy, do not configure the **accounting** command.

To reference more than one policy in a content configuration, use multiple **policy** commands.

All policies in a given content configuration must be configured the same way, either all with priorities, or all without priorities. Policies in the same content configuration must have different priorities.

Examples

The following example shows how to reference policies with and without priorities:

```
ip csg content MOVIES
 policy COMEDY
 policy HORROR

ip csg content MUSIC
 policy HIPHOP priority 1
 policy COUNTRY priority 13
```

Related Commands

Command	Description
ip csg content	Configures content for CSG2 services, and enters CSG2 content configuration mode.
ip csg policy	Defines a policy for qualifying flows for the CSG2 accounting services, and enters CSG2 policy configuration mode.
show ip csg	Displays information about the CSG2.

port (iSCSI)

To specify the number of the port on which to listen for iSCSI traffic in the iSCSI target interface profile on the CSG2, use the **port** command in iSCSI configuration mode. To remove the port number, use the **no** form of the command.

port *port-number*

no port *port-number*

Syntax Description

port-number	Number of the port on which to listen for iSCSI traffic. We recommend that you use port 3260.

Command Default

No default behavior or values.

Command Modes

iSCSI configuration

Command History

Release	Modification
12.4(15)MD	This command was introduced.

Examples

The following example configures an iSCSI target interface profile with the name **targetA** to a iSCSI target with which the CSG2 will communicate using port number **3260**:

```
ip iscsi target-profile targetA
  name iqn.2002-10.edu.abc.iol.iscsi.draft20-target:1
  ip 10.0.0.1
  port 3260
  session-timeout 120
  target-portal 1
```

Related Commands

Command	Description
ip (iSCSI)	Specifies the IP address of an iSCSI target in the target interface profile on the CSG2.
ip csg iscsi drain delay	Defines the delay interval, in seconds, before draining packets from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) when the Billing Mediation Agent (BMA) becomes active.
ip csg iscsi drain packet	Defines the number of packets to be drained from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) per drain delay interval when the Billing Mediation Agent (BMA) becomes active.

Command	Description
ip csg iscsi profile	Specifies the Internet Small Computer Systems Interface (iSCSI) target to be used as backup storage for the CSG2.
ip iscsi target-profile	Creates an iSCSI profile for an iSCSI target on the CSG2, and enters iSCSI configuration mode.
name (iSCSI)	Specifies the name of an iSCSI target in the target profile on the CSG2
session-timeout (iSCSI)	Specifies the session timeout for an iSCSI target in the target interface profile on the CSG2.
target-portal (iSCSI)	Specifies the portal group tag for an iSCSI target in the target interface profile on the CSG2.

reauthorization threshold

To configure the CSG2 reauthorization threshold, use the **reauthorization threshold** command in CSG2 service configuration mode. To restore the default setting, use the **no** form of this command.

reauthorization threshold *threshold*

no reauthorization threshold

Syntax Description

threshold	Number of remaining quadrans or seconds to trigger reauthorization. • For fixed-cost billing (**basis fixed**) or volume-based billing (**basis byte**), the range (in quadrans) is from 0 to 10000000. The default is 10000000. • For duration-based billing (**basis second**), the range (in seconds) is from 0 to 10000000. The default is 10.

Defaults

For fixed-cost billing (**basis fixed**) or volume-based billing (**basis byte**), the default reauthorization threshold is 10000000 quadrans.
For duration-based billing (**basis second**), the default reauthorization threshold is 10 seconds.

Command Modes

CSG2 service configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

Setting the threshold to 0 means that reauthorization is triggered when there are no remaining quadrans or seconds. The quota server can override these settings.

For services configured for fixed-cost billing (**basis fixed**), the reauthorization trigger is the smaller of the following values:

- The threshold configured using the **reauthorization threshold** command
- 25% of the last quota grant returned from the quota server

For services configured for volume-based billing (**basis byte**), the reauthorization trigger is the smaller of the following values:

- The threshold configured using the **reauthorization threshold** command
- 32 KB or 25% of the last quota grant returned from the quota server, whichever is larger

For services configured for duration-based billing (**basis second**), the reauthorization trigger is the threshold configured using the **reauthorization threshold** command.

Examples

The following example shows how to specify a reauthorization threshold of 75 quadrans:

```
ip csg service A1
 reauthorization threshold 75
```

Related Commands

Command	Description
ip csg service	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.
reauthorization timeout	Specifies the CSG2 reauthorization timeout.

reauthorization timeout

To specify the CSG2 reauthorization timeout, use the **reauthorization timeout** command in CSG2 service configuration mode. To restore the default setting, use the **no** form of this command.

reauthorization timeout [**initial** *initial-timeout*] [**maximum** *maximum-timeout*]

no reauthorization timeout

Syntax Description

initial *initial-timeout*	(Optional) Initial timeout, in seconds, for reauthorization after a quota grant of zero. The range is from 1 to 3600 seconds. The default is 4. The value specified for must be less than or equal to the value specified for **maximum** maximum-timeout.
maximum *maximum-timeout*	(Optional) Maximum timeout, in seconds, for reauthorization after a quota grant of zero. The range is from 1 to 3600 seconds. The default is 60.

Defaults

The default initial reauthorization timeout is 4 seconds.
The default maximum reauthorization timeout is 60 seconds.

Command Modes

CSG2 service configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

The quota server can override these settings.

For every quota grant of zero, the reauthorization time doubles, until the maximum timeout is reached. For example, if the initial timeout is set to 30 seconds, and the maximum timeout is set to 250 seconds, the reauthorization times (assuming quota grants of zero) would be:

- 30 seconds
- 60 seconds
- 120 seconds
- 240 seconds
- 250 seconds
- 250 seconds

And so on.

Examples

The following example shows how to specify an initial reauthorization timeout of 10 seconds and a maximum reauthorization timeout of 20 seconds:

```
ip csg service A1
 reauthorization timeout initial 10 maximum 20
```

Related Commands

Command	Description
ip csg service	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.
reauthorization threshold	Specifies the CSG2 reauthorization threshold.

records delay

To specify the delay before the CSG2 is to send the HTTP Statistics CDR, use the **records delay** command in CSG2 content configuration mode. To restore the default setting, use the **no** form of this command.

records delay *seconds*

no records delay

Syntax Description

seconds	Time, in seconds, that the CSG2 is to delay before sending the HTTP statistics CDR. The range is from 0 to 1234 seconds. The default is 0 (no records delay).

Defaults

The default value is 0 (no records delay).

Command Modes

CSG2 content configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

Specifying a records delay enables CSG2 accounting for retransmitted packets and ACKs after the transaction closes, but before the connection closes.

Examples

The following example shows how to specify a records delay of 5 seconds:

```
ip csg content MOVIES
 records delay 5
```

Related Commands

Command	Description
ip csg content	Configures content for CSG2 services, and enters CSG2 content configuration mode.

records granularity

To specify the granularity at which CSG2 billing call detail records (CDRs) are to be generated, use the **records granularity** command in CSG2 service configuration mode. To restore the default granularity, use the **no** form of this command.

records granularity {**transaction** | **service** {**bytes** *bytes* | **seconds** *seconds* | **bytes** *bytes* **seconds** *seconds*}}

no records granularity

Syntax Description

transaction	Generate CDRs for each transaction. This is the default setting.
service	Generate summarized, service-level CDRs.
bytes *bytes*	Number of bytes of data, sent and received by a session, that triggers a CDR. The difference between bytes sent and bytes received in two records might not exactly equal the *bytes* argument, because updates must occur on packet boundaries. The range is from 5000 to 2147483647. If the **bytes** keyword is not specified, there is no maximum.
seconds *seconds*	Maximum time, in seconds, between billing records for a session. Records can be sent more frequently if the number of bytes is reached. When a record is sent because the maximum time has been reached, the byte counts reported in the record are approximate. The range is from 5 to 86400. If the **time** keyword is not specified, there is no time limit.

Defaults

If you do not specify the **records granularity** command, CDRs are generated for each transaction.

If you specify **records granularity service**, you must also specify the **bytes** keyword, the **seconds** keyword, or both:

- If you specify both the **bytes** keyword and the **seconds** keyword, a billing record is sent when either limit is reached. Then both limits are reset.
- If you specify only the **bytes** keyword and not the **seconds** keyword, there is no time limit between billing records for a session.
- If you specify only the **seconds** keyword and not the **bytes** keyword, there is no maximum number of bytes of data that triggers the sending of a billing record.

Command Modes

CSG2 service configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The **time** keyword changed to **seconds**. • The range for the *seconds* argument changed from 60 to 4294967295, to 5 to 86400.

Usage Guidelines

You can use this command to reduce the number of records for services for which transaction-level billing is not required. For example, if a subscriber is accessing the Internet, and the data is to be billed based only on volume, then generating records for each HTTP transaction is of little use. With service-level CDR summarization enabled, the CSG2 generates only consolidated records that contain service-level usage.

To enable service-level CDR summarization in postpaid mode, you must specify that the associated billing plan is postpaid by using the **mode postpaid** command in CSG2 billing configuration mode.

Service-level CDRs are generated only for subscribers with entries in the CSG2 User Table entry. If a subscriber does not have an entry in the User Table, the CSG2 generates transaction-level CDRs.

Examples

The following example shows how to specify a service granularity in both IP bytes and seconds:

```
ip csg service A1
 records granularity service byte 10000 seconds 120
```

Related Commands

Command	Description
ip csg service	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.

records intermediate

To enable the generation of CSG2 intermediate call detail records (CDRs), use the **records intermediate** command in CSG2 content configuration mode. To disable the generation of intermediate CDRs, use the **no** form of this command.

records intermediate {**bytes** *bytes* | **seconds** *seconds* | **bytes** *bytes* **seconds** *seconds*}

no records intermediate {**bytes** *bytes* | **seconds** *seconds* | **bytes** *bytes* **seconds** *seconds*}

Syntax Description

bytes *bytes*	Number of bytes of data, sent and received by a session, that triggers the sending of an intermediate CDR. The difference between bytes sent and received in two records might not exactly equal the *bytes* argument. A trigger can occur only on a packet boundary. Once triggered, a separate process captures a snapshot of the current byte counts for a session. Between the trigger and the snapshot, additional packets might be counted. The range is from 5000 to 4294967295. The default value, if the **bytes** keyword is not specified, is 0, indicating that the number of bytes sent and received will not trigger an intermediate record.
seconds *seconds*	Maximum time, in seconds, between billing records for a session. Records can be sent more frequently if the number of bytes is reached. When a record is sent because the maximum time has been reached, the byte counts reported in the record are approximate. The range is from 5 to 86400. The default value, if the **seconds** keyword is not specified, is 0, indicating no time limit.

Defaults

If you do not specify the **records intermediate** command, or if you specify the **records intermediate** command for a content for a protocol handler that does not support intermediate statistics, intermediate CDRs are not generated.

If you specify the **bytes** keyword but not the **seconds** keyword, the maximum time between billing records for a session is set to 0 seconds, indicating no time limit.

If you specify the **seconds** keyword but not the **bytes** keyword, the number of bytes of data that triggers the sending of an intermediate CDR is set to 0 bytes, indicating that the number of bytes sent and received will not trigger an intermediate record.

If you specify both the **bytes** keyword and the **seconds** keyword, a billing record is sent when either limit is reached. Then both limits are reset.

Command Modes

CSG2 content configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The configuration mode for this command changed from CSG accounting configuration to CSG2 content configuration. • The **time** keyword changed to **seconds**. • The range for the *seconds* argument changed from 5 to 65535, to 5 to 86400.

Usage Guidelines

The CSG2 supports intermediate CDRs for FTP, HTTP, IP, RTSP, SIP, TCP, and UDP.

The CSG2 does not support intermediate CDRs for WAP or e-mail protocols (such as IMAP, POP3, and SMTP).

Examples

The following example shows how to enable intermediate CDRs for the CSG2 content MOVIES. In this example, intermediate records are generated after 100,000 IP bytes of data are sent and received, or after 3600 seconds (1 hour) elapse, whichever occurs first:

```
ip csg content MOVIES
 records intermediate bytes 100000 seconds 3600
```

Related Commands

Command	Description
ip csg content	Configures content for CSG2 services, and enters CSG2 content configuration mode.

refund

To specify the refund policy for a CSG2 prepaid service, use the **refund** command in CSG2 service configuration mode. To disable the refund policy, use the **no** form of this command.

refund *policy-name*

no refund *policy-name*

Syntax Description

policy-name	Name of the refund policy.

Defaults

Refunding is not enabled.

Command Modes

CSG2 service configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1.
	Changes from CSG1: The name of this command changed from **refund-policy** to **refund**.

Examples

The following example specifies refund policy COMPANY-REFUND:

```
ip csg service BILLBYVOLUME
 refund COMPANY-REFUND
```

Related Commands

Command	Description
ip csg refund	Specifies the CSG2 refund policy to apply to the various services, and enters CSG2 refund configuration mode.
ip csg service	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.

replicate

To replicate the connection state for all connections to the CSG2 content servers on the standby system, use the **replicate** command in CSG2 content configuration mode. To disable connection redundancy, use the **no** form of this command.

replicate [**delay** *seconds*]

no replicate [**delay**]

Syntax Description

delay *seconds*	(Optional) Number of seconds to delay state replication. The range is from 1 to 3600. The default value is no delay.

Defaults

Connection redundancy is not enabled.
If you do not specify a delay, there is no delay.

Command Modes

CSG2 content configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **replicate connection tcp** to **replicate**. • The **delay** *seconds* keyword and argument were added.

Usage Guidelines

Replication is not supported for the wireless application protocol 1.x (WAP 1.x) and Real Time Streaming Protocol (RTSP) protocols. Therefore, the CSG2 generates an error message if either of the following situations occurs:

- You have already configured RTSP or WAP 1.x using the **parse protocol** command and you try to enter the **replicate** command.
- You have already configured **replicate** and you try to configure RTSP or WAP 1.x using the **parse protocol** command.

For HTTP, the replicated session is treated as Layer 4. No HTTP parsing is performed when the replicated session on the standby CSG2 becomes active.

Examples

The following example shows how to enable replication for the CSG2 content MOVIES, and replication with a delay of 30 seconds for the CSG2 content GAMES:

```
ip csg content MOVIES
 replicate
ip csg content GAMES
 replicate delay 30
```

Related Commands

Command	Description
ip csg content	Configures content for CSG2 services, and enters CSG2 content configuration mode.
ip csg replicate	Enables state replication between redundant CSG2 systems.

retcode

To specify the range of application return codes for which the CSG2 refunds quota for Prepaid Error Reimbursement, use the **retcode** command in CSG2 refund configuration mode. To disable this feature, use the **no** form of this command.

retcode {**ftp** | **http** | **imap** | **pop3** | **sip** | **smtp** | **wap**} *rc-start* [*rc-end*]

no retcode {**ftp** | **http** | **imap** | **pop3** | **sip** | **smtp** | **wap**} *rc-start* [*rc-end*]

Syntax Description

ftp	The CSG2 refunds quota for FTP application return codes.
http	The CSG2 refunds quota for HTTP and WAP 2.0 application return codes. **Note** The **http** keyword affects only HTTP and WAP 2.0. For WAP 1.x refunds, use the **wap** keyword.
imap	The CSG2 refunds quota for Internet Message Access Protocol (IMAP) application return codes.
pop3	The CSG2 refunds quota for Post Office Protocol, version 3 (POP3) application return codes.
sip	The CSG2 refunds quota for Session Initiation Protocol (SIP) application return codes. **Note** For SIP calls, only the return code to the INVITE method is used. For SIP events, each event is a transaction associated with a single return code.
smtp	The CSG2 refunds quota for Simple Mail Transfer Protocol (SMTP) application return codes.
wap	The CSG2 refunds quota for WAP 1.x application return codes. **Note** The **wap** keyword affects only WAP 1.x. For WAP 2.0 refunds, use the **http** keyword.
rc-start	Specifies the beginning of the range of values for specific application return codes. The range is 1 to 65535 (0xffff).
rc-end	(Optional) Specifies the end of the range of values for specific application return codes. The range is the value of *rc-start* to 65535 (0xffff). If you are specifying a single value as the range, do not specify *rc-end*.

Defaults

None

Command Modes

CSG2 refund configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: None.
12.4(15)MD	The **ftp** and **sip** keywords were added.

Usage Guidelines

The CSG2 supports return code-based refunding for all protocols except RTSP.

The return codes are protocol-specific.

For IMAP, keep in mind the following considerations:

- Only return code 554 is used. Return code 554 is used when a transaction ending in an IMAP tagged response was not flagged **OK**.
- The CSG2 does not support refunding for IMAP. If configured, refunding for IMAP has no effect.

Examples

The following example shows how to **specify ranges of application return codes**:

```
ip csg refund COMPANY-REFUND
 retcode http 500 509
 retcode sip 300 999
 retcode wap 0x44 0x50
```

Related Commands

Command	Description
flags	Specifies IP, TCP, or wireless application protocol (WAP) flag bit masks and values for CSG2 Prepaid Error Reimbursement.
ip csg refund	Specifies the CSG2 refund policy to apply to the various services, and enters CSG2 refund configuration mode.

sami rate all

To specify the bit rate limit to be used by the Service and Application Module for IP (SAMI) for each PowerPC's (PPC's) traffic, CSG2 use the **sami rate all** command in global configuration mode. Use the **no** form of this command to disable this feature.

sami rate *bits-per-second* **all**

no sami rate *bits-per-second* **all**

Syntax Description

bits-per-second	Number of bits per second that the SAMI rate-limiting code is to allow to be forwarded to an individual PPC. The range is 1 bps to 2 Gbps (0x80000000). The default value is 1.9 Gbps (0x70000000).

Defaults

The default rate is 1.9 Gbps (0x70000000).

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Examples

The following example shows how to **specify a bit rate limit of 1 Gbps (0x40000000)**:

```
sami rate 0x40000000 all
```

service

To associate a service with a CSG2 billing plan, use the **service** command in CSG2 billing configuration mode. To remove the association, use the **no** form of this command.

service *service-name*

no service *service-name*

Syntax Description

service-name	Name of a configured CSG2 billing service.

Defaults

None

Command Modes

CSG2 billing configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: None.

Usage Guidelines

To associate more than one service with the same billing plan, use multiple **service** commands.

Examples

The following example shows how to associate services MOVIES and BROWSING with billing plan REGULAR:

```
ip csg billing REGULAR
 service MOVIES
 service BROWSING
```

Related Commands

Command	Description
entries user idle	Sets the time after which entries for idle subscribers are deleted from the CSG2 User Table.
ip csg billing	Defines a CSG2 billing plan, and enters CSG2 billing configuration mode.
ip csg service	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.
mode	Specifies the mode for a CSG2 billing plan.

session-timeout (iSCSI)

To specify the session timeout for an iSCSI target in the target interface profile on the CSG2, use the **session-timeout** command in iSCSI configuration mode. To restore the default timeout, use the **no** form of the command.

session-timeout *duration*

no session-timeout

Syntax Description

duration	Number of seconds the iSCSI initiator waits for a response from the iSCSI target, after which it closes the iSCSI session. The range is from 1 to 600. The default setting is 1 second.

Command Default

The default iSCSI target session timeout is 60 seconds.

Command Modes

iSCSI configuration

Command History

Release	Modification
12.4(15)MD	This command was introduced.

Examples

The following example configures an iSCSI target interface profile with the name **targetA** with a SCSI session timeout of **120** seconds:

```
ip iscsi target-profile targetA
  name iqn.2002-10.edu.abc.iol.iscsi.draft20-target:1
  ip 10.0.0.1
  port 3260
  session-timeout 120
  target-portal 1
```

Related Commands

Command	Description
ip (iSCSI)	Specifies the IP address of an iSCSI target in the target interface profile on the CSG2.
ip csg iscsi drain delay	Defines the delay interval, in seconds, before draining packets from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) when the Billing Mediation Agent (BMA) becomes active.
ip csg iscsi drain packet	Defines the number of packets to be drained from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) per drain delay interval when the Billing Mediation Agent (BMA) becomes active.

Command	Description
ip csg iscsi profile	Specifies the Internet Small Computer Systems Interface (iSCSI) target to be used as backup storage for the CSG2.
ip iscsi target-profile	Creates an iSCSI profile for an iSCSI target on the CSG2, and enters iSCSI configuration mode.
name (iSCSI)	Specifies the name of an iSCSI target in the target profile on the CSG2
port (iSCSI)	Specifies the number of the port on which to listen for iSCSI traffic in the iSCSI target interface profile on the CSG2.
target-portal (iSCSI)	Specifies the portal group tag for an iSCSI target in the target interface profile on the CSG2.

show ip csg

To display information about the CSG2, use the **show ip csg** command in privileged EXEC mode.

show ip csg {**billing [plan** *billing-plan-name*] **| bma | content [name** *content-name*] **[detail | internal] | database | gtp | iscsi | load [history] | psd | quota-server | radius | sessions** {**database | gtp | imap | ipc | radius | replicate | user** [*application* [**internal**]] [*ip-address ip-mask*]} **| stats | users** {*ip-address ip-mask* **| id** *user-name* **| all | sip** [**internal**]}} [**detail**]

Syntax Description

billing	Displays information about billing plans.
plan *billing-plan-name*	(Optional) Displays information about only the specified billing plan.
bma	Displays information about the Billing Mediation Agents (BMAs) to which the CSG2 sends billing records. BMA statistics are reported for each BMA, in addition to an aggregate count for all BMAs.
content	Displays information about the CSG2 content table.
name *content-name*	(Optional) Displays information about only the specified content.
detail	(Optional) Displays detailed information about the CSG2 content.
internal	(Optional) Displays internal CSG2 data structure information for use in debugging. We recommend that you enter this keyword only when directed to do so by Cisco Technical Assistance Center (TAC) engineers.
database	Displays information about the server that answers CSG2 user ID queries.
gtp	Displays information about the general packet radio service (GPRS) tunneling protocol (GTP).
iscsi	Displays information about the Internet Small Computer Systems Interface (iSCSI).
load	Displays information about load management.
history	(Optional) Displays histograms of recent load management activity.
psd	Displays information about the Cisco Persistent Storage Device (PSD) functionality residing on the CSG2.
quota-server	Displays information about the quota servers.
radius	Displays information about RADIUS.
sessions	Displays information about sessions.
database	Displays information about only the user database sessions.
gtp	Displays information about only the GTP sessions.
imap	Displays information about only the Internet Message Access Protocol (IMAP) sessions.
ipc	Displays information about only the Interprocessor Communication (IPC) sessions.
other	Displays information about all other Layer 3 and Layer 4 sessions.
pop3	Displays information about only the Post Office Protocol, version 3 (POP3) sessions.
radius	Displays information about only the RADIUS sessions.

replicate	Displays information about only high availability (HA) sessions.
smtp	Displays information about only the Simple Mail Transfer Protocol (SMTP) sessions.
user	Displays information about only subscriber sessions.
application	(Optional) Displays information about only the specified application: • **ftp**—Closes FTP subscriber sessions. • **http**—Closes HTTP subscriber sessions. • **imap**—Closes IMAP subscriber sessions. • **other**—Closes other subscriber sessions. • **pop3**—Closes POP3 subscriber sessions. • **rtsp**—Closes RTSP subscriber sessions. • **smtp**—Closes SMTP subscriber sessions. • **wap**—Closes WAP subscriber sessions.
internal	(Optional) Displays internal CSG2 data structure information for use in debugging. We recommend that you enter this keyword only when directed to do so by Cisco Technical Assistance Center (TAC) engineers.
ip-address ip-mask	(Optional) Displays information about only the specified subscriber IP address and subscriber IP address mask. Specify IP address 0.0.0.0 to display information about all subscriber IP addresses. Specify IP address mask 0 to display information about all subscriber IP address masks.
stats	Displays performance statistics for the CSG2. You can also use the following commands to monitor CSG2 high availability (HA) configurations: **show redundancy state**, **show redundancy interdev**, and **show ipc sctp**.
users	Displays information about subscribers. **Note** If the **basis second connect** command is configured, the **balance** and **consumed** fields in the output of the **show ip csg users** command are updated only when there is a Service Reauthorization Request for new quota.
ip-address ip-mask	Displays information about only the specified subscriber IP address and subscriber IP address mask. Specify IP address 0.0.0.0 to display information about all subscriber IP addresses. Specify IP address mask 0 to display information about all subscriber IP address masks.
id *user-name*	Displays information about the specified user ID.
all	Displays information about all subscribers.
sip	Displays information about the Session Initiation Protocol (SIP).

internal	(Optional) Displays internal CSG2 data structure information for use in debugging. We recommend that you enter this keyword only when directed to do so by Cisco Technical Assistance Center (TAC) engineers.
detail	(Optional) Displays more detailed information.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: This command incorporated the following CSG1 commands: • **show ip csg accounting** • **show module csg content** • **show module csg stats**
12.4(15)MD	The **billing**, **ftp**, **gtp**, **history**, **iscsi**, **load**, **plan**, and **sip** keywords and *billing-plan-name* argument were added.

Usage Guidelines

In the output for the **show ip csg content** command, the CSG2 might truncate some fields, such as the VRF name and the domain name.

Entering the **show ip csg users all** command might flood your screen with output.

Examples

The following example shows how to display the statistics and counters for CSG2 content:

```
Router# show ip csg content

name            prot destination                  vlan state
--------------------------------------------------------------------------------
ANY             Any  0.0.0.0/0                    ALL  OUTOFSERVICE
CONTENT         Any  0.0.0.0/0                    ALL  INSTALLED
CsgCg01         UDP  0.0.0.0/0:16000              ALL  INSTALLED
CsgCg11         UDP  0.0.0.0/0:16001              ALL  INSTALLED
CsgRadProxy1    UDP  10.18.28.34/32:0             ALL  INSTALLED
CsgRadProxy2    UDP  10.18.28.36/32:0             ALL  INSTALLED
CsgRadProxy3    UDP  10.18.28.37/32:0             ALL  INSTALLED
CsgRadProxy4    UDP  10.18.28.39/32:0             ALL  INSTALLED
CsgRadProxy5    UDP  10.18.28.254/32:0            ALL  INSTALLED
CsgRadProxy6    UDP  10.18.28.2/32:0              ALL  INSTALLED
CsgReplicate    UDP  10.18.28.8/32:6000           ALL  INSTALLED
CsgUDB          UDP  0.0.0.0/0:4444               ALL  INSTALLED
HTTP            TCP  0.0.0.0/0:80                 ALL  INSTALLED
HTTP82          TCP  0.0.0.0/0:82                 ALL  INSTALLED
RADIUS          UDP  11.18.28.16/32:1812          ALL  INSTALLED
RTSP            TCP  0.0.0.0/0:554                ALL  INSTALLED
SMTP            TCP  0.0.0.0/0:2025               ALL  INSTALLED
```

```
TCP             TCP  0.0.0.0/0:0                  ALL  INSTALLED
WAPCONN         UDP  0.0.0.0/0:9201               ALL  INSTALLED
WAPCONNLESS     UDP  0.0.0.0/0:9200               ALL  INSTALLED
```

The following example shows how to display detailed statistics and counters for the CSG2 HTTP content named **HTTP**:

```
Router# show ip csg content name HTTP detail

HTTP, parse type = http, state = INSTALLED, index = 13
 destination = 0.0.0.0/0:80, protocol = TCP, vlan = ANY
 idle = 10, pending = 30, replicate = Session, max parse len = 4000
 total sessions = 48347288, current sessions = 153
 regex memory usage = 98352
 subscriber paks = 187932310, network paks = 261526365



 policy                   transactions
 ------------------------------------
 FILE0K                              0
 FILE16K                             0
 FILE1K                         374104
 FILE4K                         364817
 FILE8K                         365168
 GIF                           4462769
 JPEG                          2982911
 HTML                         13569080
 HTTP                             8535
 (none)                              0
```

The following example shows how to display the CSG2 statistics:

```
Router# show ip csg stats

CSG Replication Stats:
   State: ACTIVE
   Transmit: Packets = 1725627, current sequence = 268220
   Received: Packets = 12014, current sequence = 12015, errors = 0
   Last Bulk Sync Sent: 07:15:01 UTC Jun 6 2007
   Bulk sync in progress on:
     Processor 5
     Processor 8

CSG Clear Stats:
   counters = 0, kut = 0, sessions = 0

IPC PPC Stats:
 init alloc fail = 0
 message block alloc fail = 0
 message block alloc denied = 0
 correlator alloc fail = 0
 message blocks currently allocated = 5020, max allocated = 5200
 message blocks currently queued = 5020, max queued = 5200
 message blocks currently tx queued = 5020, max tx queued = 5200
 message blocks currently hashed = 3600, max hashed = 3663
 dropped messages = 0, null msgs = 0
 failure to respond = 0
 acks = 11251929, timed out responses = 231567
 interrupt acks = 1898906, process acks = 25, no ack = 0
 sent to peer
     unreliable sends = 0, unreliable send failures = 0
     reliable sends = 436, reliable send failures = 0
     request sends = 1902531, request send failures = 0
```

```
     response sends = 11252888, response send failures = 0
 received from peer
     unreliable = 51626, reliable = 97224994, request = 11254924, response =
1667364
     unsupported ipc port = 0, unsupported ipc request port = 0
     uncorrelated = 1138193
 errors
     rtx list = 0, hash list = 0, dealloc = 0
     msg type = 0, ack miss = 0
   ------------------------------
   destination = 127.1.0.4:0, localport = 0
   connection failures = 0
   priority = 0, ACTIVE
   packet rate = 351/sec, ack rate = 351/sec
   data packets sent = 3086282, retransmits = 76, failed acks = 0
   queued = 0, highwater = 586, tx win = 32
   unacked = 0, ack = 138, count = 4

   ------------------------------
   destination = 127.1.0.5:0, localport = 0
   connection failures = 0
   priority = 0, ACTIVE
   packet rate = 304/sec, ack rate = 23/sec
   data packets sent = 1230533, retransmits = 523322, failed acks = 0
   queued = 2490, highwater = 2669, tx win = 32
   unacked = 32, ack = 5, count = 4
   ------------------------------
   destination = 127.1.0.6:0, localport = 0
   connection failures = 0
   priority = 0, ACTIVE
   packet rate = 831/sec, ack rate = 831/sec
   data packets sent = 5280267, retransmits = 114, failed acks = 0
   queued = 0, highwater = 191, tx win = 32
   unacked = 0, ack = 14, count = 1
   ------------------------------
   destination = 127.1.0.7:0, localport = 0
   connection failures = 0
   priority = 0, ACTIVE
   packet rate = 191/sec, ack rate = 191/sec
   data packets sent = 3339431, retransmits = 39339, failed acks = 0
   queued = 0, highwater = 1649, tx win = 32
   unacked = 0, ack = 105, count = 4
   ------------------------------
   destination = 127.1.0.8:0, localport = 0
   connection failures = 0
   priority = 0, ACTIVE
   packet rate = 257/sec, ack rate = 0/sec
   data packets sent = 1281140, retransmits = 506285, failed acks = 0
   queued = 2530, highwater = 2716, tx win = 31
   unacked = 31, ack = 4, count = 0

CSG Distributed Config Stats:
   poll msg sent = 16, online msg rcvd = 5, ack sent = 5
   ack not sent = 4, cmd distributed = 0, rollback = 0
   'no' cmd success = 0, 'no' cmd failure = 0

CSG Load Management Stats:
 Radius Start
   Allowed (per second) = 367872 (21)
   IPC: Queue Depth Tolerance 24000 / 100000 (24 percent)
        Denied (per second) = 0 (0)
 Database Request
   Allowed (per second) = 75197 (10)
   IPC: Queue Depth Tolerance 24000 / 100000 (24 percent)
```

```
        Denied (per second) = 5065121 (0)
    Rate: Limit 1800 per traffic processor
          Denied (per second) = 25193314 (0)
  Session Create
    Allowed (per second) = 49802545 (1872)
    IPC: Queue Depth Tolerance 36000 / 100000 (36 percent)
         Denied (per second) = 21971 (6)
  BMA Messages
    Allowed (per second) = 94475805 (11138)
    IPC: Queue Depth Tolerance 60000 / 100000 (60 percent)
         Denied (per second) = 0 (0)
  Quota Server
    Allowed (per second) = 13725076 (837)
    IPC: Queue Depth Tolerance 60000 / 100000 (60 percent)
         Denied (per second) = 0 (0)

CSG Buffer Management Stats:
 Category    |          Create            Copy            Free            Deny
 ------------------------------------------------------------------------------
 Radius      |               0         1858818         1854161               0
 Application |               0         9422790         9422649               0
 Fragments   |             161            1127            1288               0
 Unlimited   |        95979756               0        95979750               0

CSG User Database Stats:
   errors = 0

CSG Session L4 Stats:
   alloc fail ooo node = 0
   alloc fail pak copy enqueue = 0
   general errors = 0
   FSM errors = 262
   standby FSM errors = 0
   count errors = 0
   term idle = 838696
   term short timer = 10179
   Network interface:
     TCP packets = 266880460
     TCP frags = 0
     datagram packets = 4932124
     datagram frags = 161
     out of order         = 93841
     out of order get     = 91870
     out of order flushed = 1971
     retransmitted = 94873
     set aside         = 56824
     set aside get     = 56412
     set aside flushed = 412
     term closed  = 1003483
     term RST     = 10
     term not SYN = 259
     term mid SYN = 0
     term error   = 0
     dropped OOW = 323808
     dropped set aside = 292592
     dropped queue size = 0
     dropped error = 259
   Subscriber interface
     TCP packets = 192907977
     TCP frags = 0
     datagram packets = 13347893
     datagram frags = 0
     out of order         = 412
     out of order get     = 384
```

```
      out of order flushed = 28
      retransmitted = 485
      set aside         = 9504977
      set aside get     = 9418614
      set aside flushed = 86222
      term closed  = 1362349
      term RST     = 457991
      term not SYN = 0
      term mid SYN = 0
      term error   = 0
      dropped OOW = 0
      dropped set aside = 692663
      dropped queue size = 0
      dropped error = 0

CSG Fragment Stats:
   creates = 161, destroys = 161, timeouts = 0,
   invalids = 0, locked = 0
   Leaders:  rx = 161, tx = 161, dropped = 0, creates = 161
   Trailers: rx = 966, tx = 966, dropped = 0, creates = 0
   Reassemble: invalid = 0
   alloc failures = 0, overlap = 0, missing leader = 0
   failed tx = 0, requeues = 0, failed requeues = 0

CSG Packet Stats:
   packet rcv = 509381050, drop invalid = 0,
   protocol drop = 26408409, no handler = 0, no handler options = 0,
   drop no content = 3, drop no session = 31791002
   local enqueue = 2187, local enqueue failed = 0
   local enqueue copy = 18

CSG Distributed KUT Stats:
   requests = 75197, responses = 62442, resends = 23430
   timeouts = 11652, idle timeouts = 0, corr mismatch = 0
   corr missing = 0, unknown IP = 11652
   unknown ha vrf = 0, tx fail ipc = 0
   alloc failures:
     kut = 0, kut_delete_event = 0, rad attr = 0
     int_stats = 0, kut_svc = 0, svc_stats = 0
     tariff = 0, redir_info = 0, passthru_grant = 0
     refund = 0, txn_abort = 0, ipc = 0

CSG Session Stats:
   user sessions = 531, highwater = 169455, ha_overrun = 0
   max limit = 0, wc fail = 0, no content = 0
   appl fail = 30314998, denied = 1487001, ha no content = 0
   ha no session = 17529
   Resets : subscriber = 46196262, network = 15603410
   Alloc failures : wc = 0, session = 0
     prof event = 0, resolve event = 0, pend quota = 0
     pend aoc = 0
   Resolve : no sess = 1, event fail = 3042, enq fail = 0
     dup quota = 0, dup aoc = 0, aoc fail = 79
     sess lookup fail = 0

CSG LogGen Stats:
   alloc fail = 0, gtp reject = 405
   Billing records: sent = 94591046, fail = 0
   IPC: alloc fail = 0, sent = 94475805, fail = 0, rcv = 94591043

GTP Application: CSG ipc, Local Port: 0
   alloc failures = 0, no standby on CG failure = 0
   packets sent = 14217667, received = 122537872, failed acks = 0
   packets dropped = 0, rejected = 0, retransmits = 1069136, no ip = 0
```

```
   packets outstanding: current = 5022, highwater = 5200
   bad records = 0, unknown CG = 0, CG failures = 0
   send skipped = 0, records dropped during drain = 0
   Charging Gateways: defined = 5, max active = 5
     127.1.0.4:00ACTIVE
     127.1.0.5:00ACTIVE
     127.1.0.6:00ACTIVE
     127.1.0.7:00ACTIVE
     127.1.0.8:00ACTIVE

GTP Application: CSG Billing Agent, Local Port: 16000
   alloc failures = 0, no standby on CG failure = 0
   packets sent = 8096890, received = 809759, failed acks = 0
   packets dropped = 0, rejected = 0, retransmits = 261, no ip = 0
   packets outstanding: current = 4, highwater = 3262
   bad records = 0, unknown CG = 0, CG failures = 0
   send skipped = 0, records dropped during drain = 0
   Charging Gateways: defined = 1, max active = 1
     10.18.28.10:33331ACTIVE

GTP Application: CSG Quota Server, Local Port: 16001
   alloc failures = 0, no standby on CG failure = 81
   packets sent = 4054366, received = 4054405, failed acks = 294
   packets dropped = 2245665, rejected = 405, retransmits = 49, no ip = 0
   packets outstanding: current = 9304, highwater = 10001
   bad records = 0, unknown CG = 0, CG failures = 81
   send skipped = 0, records dropped during drain = 0
   Charging Gateways: defined = 1, max active = 1
     10.18.28.10:33851ACTIVE

GTP Application: CSG PSD, Local Port: 0
   alloc failures = 0, no standby on CG failure = 0
   packets sent = 0, received = 0, failed acks = 0
   packets dropped = 0, rejected = 0, retransmits = 0, no ip = 0
   packets outstanding: current = 0, highwater = 0
   bad records = 0, unknown CG = 0, CG failures = 0
   send skipped = 0, records dropped during drain = 0
   Charging Gateways: defined = 0, max active = 1

CSG User Stats:
   max = 300000, current = 148916, highwater = 169990
   exceed-max = 0
   kut current = 148916, kut highwater = 169990
   sticky current = 0, sticky highwater = 318
   ipc tx fail = 0, ipc response timeouts = 231557
   alloc failures:
     aff = 0, pend event = 0, delete event = 0
     ipc = 0
   ha receive drops:
     no aff = 22, unknown vrf = 0, state = 0

CSG Radius Stats:
   starts = 1548210, stops = 2015870, other = 0
   client msg rcv = 0, client msg sent = 0
   incorrect authentication = 0
   alloc failures:
     billplan = 0, auth = 0, user info = 0
     nas info = 0, pod port = 0, pod info = 0
     proxy elem = 0, proxy port = 0
   proxy source port = 1037
   proxy errors:
     invalid message size = 0, unable to find client = 0
     unable to send to client = 0, unable to send to server = 0
     unable to find proxy blk = 0
```

```
   proxy CSG ip = 10.18.28.34,
     server ip = 11.18.28.17
     client->server = 386484, server->client = 385459
     parse errors = 0, pkt not proxied = 0
   proxy CSG ip = 10.18.28.36,
     server ip = 11.18.28.18
     client->server = 230290, server->client = 229610
     parse errors = 0, pkt not proxied = 0
   proxy CSG ip = 10.18.28.37,
     server ip = 11.18.28.19
     client->server = 304504, server->client = 303612
     parse errors = 0, pkt not proxied = 0
   proxy CSG ip = 10.18.28.39,
     server ip = 11.18.28.20
     client->server = 0, server->client = 0
     parse errors = 0, pkt not proxied = 0
   proxy CSG ip = 10.18.28.254,
     server ip = 11.18.28.16
     client->server = 0, server->client = 0
     parse errors = 0, pkt not proxied = 0
   endpoint CSG ip = 10.18.28.2
     client->CSG = 2642802, CSG->client = 2640636
     unable to send ACK = 0, parse errors = 0
     no ack sent = 0, non-Acct-Req = 0

CSG QS Stats:
   alloc fail:
     req = 0, redir = 0, defer ack = 0, req token = 0
   too frequent requests = 12129585, called on standby = 0
   no defer ack data = 0, no cg affinity = 0
   passthru = 7404738, response no kut svc = 969, no quota = 10034067
   svc auth fail = 6, aoc-verify fail = 0
   badly formatted message:
     aoc verify response = 0, cont auth redir = 458607
     usr auth rsp = 0, svc auth rsp = 0
     svc verify resp = 0, quota return accept = 0
     svc stop req = 0, quota return req = 0
     user disconnect req = 0, quota push req = 0
     invalid req = 0
   QS requests received from QS:
     request = 0, fail to send to tp = 0
   QS responses received from QS:
     response = 4053620, fail to send to tp = 0
     no request = 0, missing request data = 0
   IPC:
     CP alloc fail = 0, sent = 11252881, fail = 0, rcv = 13790207
     TP alloc fail = 0, sent = 13725076, fail = 0, rcv = 11186359
        response no request = 0
   user profile req = 862466, rsp = 181435
   svc auth req = 2533171, re-auth req = 1151422, rsp = 1499012
   quota return = 118566, quota return accept = 0
   auth content req = 6528274, rsp = 1832535
   svc verify req = 0, rsp = 0
   svc stop = 2531177, fail to enqueue qm request process = 0
   svc stop req = 0, user disconnect req = 0
   quota return req = 0, quota push req = 0, rsp = 0
   negative quota grant = 0

CSG OTHER Stats:
   total sessions = 40344, alloc fail = 0
   aoc fail = 0, frags = 0, aborts = 6521, init fail = 2513
   reports = 39937, standby no uid = 0, errors = 0

CSG HTTP Stats:
```

```
   sess = 18052044, txn = 22158257, set-aside resolved = 9367313
   packets:
     sub new = 22418621, retx = 53, payload less = 164830871
     net new = 238215919, retx = 94709, payload less = 22597153
   billing reports:
     header = 6075882, stats = 79933600
   alloc failures = 0
   downgrade:
     parse failures = 8460, status code = 0
     rsp > req = 0, 0.9 method = 3007
   fin terminated = 342, https = 20967, xf4 = 0
   redirects = 450449, redirect failures = 1075
   reset:
     error = 0, no user = 30295243, no quota = 10025299
     exceed max parse len = 0, no policy = 0
     auth drop = 5577073
   svc verify = 0, aoc = 6480351
   unassigned bytes updates:
     no txn = 59360, downgrade = 26308, leak = 16082230
   billing not resolved on standby = 0

CSG RTSP Stats:
   Dyn Sess: add = 32386, fail = 32, delete = 32374, unused = 38
   Allocs: sessions = 8131, ctl_conns = 10405, streams = 16226,
   Timeouts: control = 10402, data = 31359, streams = 1
   Misc: reuse = 0, reuse kills = 0, teardowns = 0
    suspend = 96, patches = 0, interleaved = 0, sess = 0
    http = 0, pauses = 0, no_policy = 0, mismatch = 0
    ip frags = 0, retransmits = 29, resegments = 0
    no user = 4030
   Errors: alloc = 0, dups = 0, ddrops = 0, cdrops = 32
    patch = 0, parse = 0, aoc = 0, reject = 0
    misc = 0
   Reports: tcp = 10402, udp = 32336, stream = 16172

CSG Mail Stats:
   SMTP: messages = 457898, packets = 8701512, reports = 457898
         fsm error = 0
   POP3: messages = 0, packets = 0, reports = 0
         fsm error = 0
   IMAP: header fetches = 0, body fetches = 0
         packets = 0, reports = 0, fsm error = 0
   MAIL: ip frags = 0, aoc bypass = 0, alloc fails = 0
         error = 0, no user = 6754, no policy = 0
         txn drop = 0, aoc drop = 0

CSG WAP Stats:
   parses = 6026562, wap sessions = 978999, mms sessions = 0
   connection oriented paks = 2629846, connectionless paks = 3396716
   total trans = 2087358, incomplete trans = 2962
   billing reports = 3755797, dup packets = 718748, redirects = 972
   disconnects = 0, unknown packets = 98, concat packets = 0
   parse err = 275, alloc fail = 0, refunds = 0
   forced aborts = 19015, concat frags = 0, uid wait = 65571
   seg att = 0, seg succ = 0, seg comp = 0, frags = 161
   send fail = 0, send ok = 50279, no policy = 0
   stateless = 732269, verifys = 0, cont fail = 0
   user fail = 6458, err = 0, pre policy = 0
   Aoc: reqs = 47923, drop = 14006, redir = 6778, fail = 0
   Drops: err = 0, quota = 14290, block = 0, queue = 2521

Timer Stats:
   tmr_intialized = 1
   tmr_ticks = 7160
```

```
   tmr_starts = 4067359
   tmr_stops = 3487837
   tmr_timeouts = 574960
   tmr_active = 4562
   tmr_longest_chain = 505
```

The following example shows how to display information about the quota server:

```
Router# show ip csg quota-server

charging gateway      vrf                                  priority state
-------------------------------------------------------------------------------
10.18.28.10:3385                                           1        ACTIVE
```

The following example shows how to display information about sessions:

```
Router# show ip csg sessions

         subscriber            network       prot  vrf           state
-------------------------------------------------------------------------------
     10.18.28.37:1028      11.18.28.19:1812  17   <none>         ESTAB
     10.18.28.34:1029      11.18.28.17:1812  17   <none>         ESTAB
     10.18.28.11:1813       10.18.28.2:1812  17   <none>         ESTAB
     10.18.28.14:1813       10.18.28.2:1812  17   <none>         ESTAB
     10.18.28.15:1813       10.18.28.2:1812  17   <none>         ESTAB
     10.18.28.13:1813       10.18.28.2:1812  17   <none>         ESTAB
     10.18.28.11:1810       10.18.28.2:5555  17   <none>         ESTAB
     10.18.28.13:1810       10.18.28.2:5555  17   <none>         ESTAB
     10.18.28.14:1810       10.18.28.2:5555  17   <none>         ESTAB
     10.18.28.15:1810       10.18.28.2:5555  17   <none>         ESTAB
     10.18.28.34:1030      11.18.28.17:1812  17   <none>         ESTAB
     10.18.28.13:1814      10.18.28.36:1812  17   <none>         ESTAB
     10.18.28.14:1814      10.18.28.36:1812  17   <none>         ESTAB
     10.18.28.11:1814      10.18.28.36:1812  17   <none>         ESTAB
     10.18.28.34:1031      11.18.28.17:1812  17   <none>         ESTAB
     10.18.28.11:1815       10.18.28.2:5555  17   <none>         ESTAB
     10.18.28.12:1815       10.18.28.2:5555  17   <none>         ESTAB
     10.18.28.13:1815       10.18.28.2:5555  17   <none>         ESTAB
     10.18.28.14:1815       10.18.28.2:5555  17   <none>         ESTAB
     10.18.28.15:1815       10.18.28.2:5555  17   <none>         ESTAB
     10.18.28.36:1025      11.18.28.18:1812  17   <none>         ESTAB
     10.18.28.34:1026      11.18.28.17:1812  17   <none>         ESTAB
     10.18.28.37:1027      11.18.28.19:1812  17   <none>         ESTAB
     10.18.28.11:1812       10.18.28.2:5555  17   <none>         ESTAB
     10.18.28.13:1812       10.18.28.2:5555  17   <none>         ESTAB
     10.18.28.14:1812       10.18.28.2:5555  17   <none>         ESTAB
     10.18.28.15:1812       10.18.28.2:5555  17   <none>         ESTAB
     10.18.28.37:1036      11.18.28.19:1812  17   <none>         ESTAB
     10.18.28.34:1032      11.18.28.17:1812  17   <none>         ESTAB
     10.18.28.13:1816      10.18.28.37:1812  17   <none>         ESTAB
     10.18.28.15:1816      10.18.28.37:1812  17   <none>         ESTAB
     10.18.28.14:1816      10.18.28.37:1812  17   <none>         ESTAB
     10.18.28.11:1816      10.18.28.37:1812  17   <none>         ESTAB
     10.18.28.36:1033      11.18.28.18:1812  17   <none>         ESTAB
     10.18.28.36:1034      11.18.28.18:1812  17   <none>         ESTAB
     10.18.28.11:1818      10.18.28.34:1812  17   <none>         ESTAB
     10.18.28.14:1818      10.18.28.34:1812  17   <none>         ESTAB
     10.18.28.15:1818      10.18.28.34:1812  17   <none>         ESTAB
     10.18.28.12:1818      10.18.28.34:1812  17   <none>         ESTAB
     10.18.28.13:1818      10.18.28.34:1812  17   <none>         ESTAB
     10.18.28.37:1035      11.18.28.19:1812  17   <none>         ESTAB
```

Note The **prot** column displays the IP protocol as described in the Assigned Numbers RFC.

The following table lists and describes the possible states for the **show ip csg sessions user** command:

State[1]	Description
CSG_SSVC_STATE_INIT	The session has been created but no packet has been processed. Short timer.[2]
CSG_SSVC_STATE_SYN_SUB	A SYN packet has been received from the subscriber interface. Short timer.[2]
CSG_SSVC_STATE_SYN_NET	A SYN packet has been received from the network interface. Short timer.[2]
CSG_SSVC_STATE_SYN_BOTH	The session has received a SYN packet from both the subscriber and network interfaces. Short timer.[2]
CSG_SSVC_STATE_SETUP_ACK_SUB_WAIT	The session has received a SYN-ACK from the network interface and is waiting for the ACK from the subscriber interface to complete the TCP 3-way handshake. Short timer.[2]
CSG_SSVC_STATE_SETUP_ACK_NET_WAIT	The session has received a SYN-ACK from the subscriber interface and is waiting for the ACK from the network interface to complete the TCP 3-way handshake. Short timer.[2]
CSG_SSVC_STATE_ESTAB	The TCP session has been established. UDP sessions enter this state on the first packet. This is the only state for UDP sessions after INIT.
CSG_SSVC_STATE_FIN_SUB	The session has received a FIN from the subscriber interface
CSG_SSVC_STATE_FIN_NET	The session has received a FIN from the network interface
CSG_SSVC_STATE_FIN_SUB_WAIT	The session has received an ACK from the subscriber interface and is waiting for a FIN from the subscriber interface
CSG_SSVC_STATE_FIN_NET_WAIT	The session has received an ACK from the network interface and is waiting for a FIN from the network interface
CSG_SSVC_STATE_FIN_BOTH	The session has received a FIN from both the subscriber and network interfaces

State[1]	Description
CSG_SSVC_STATE_CLOSING_ACK_NET_WAIT	The session has received a FIN-ACK or a FIN and an ACK from the subscriber interface and is waiting for the ACK from the network interface to close the connection. Short timer.[2]
CSG_SSVC_STATE_CLOSING_ACK_SUB_WAIT	The session has received a FIN-ACK or a FIN and an ACK from the network interface and is waiting for the ACK from the subscriber interface to close the connection. Short timer.[2]
CSG_SSVC_STATE_CLOSED	The session is closed. Note that closed sessions are destroyed so it is very unlikely that show session will display a session in this state.

1. TCP sessions use all these states. UDP sessions move from INIT state directly to ESTAB state.
2. "Short timer" indicates that the state uses a 5-second idle time regardless of what is configured in the content. All other states use the configured idle time.

The following example displays detailed information about the subscriber at **10.18.28.0/24**:

```
Router# show ip csg users 10.18.28.0/24 detail

10.18.28.11     C-10.18.28.11
   sessions = 1, traffic proc id = 4
   nexthop downlink ip = 0.0.0.0, flags = 0x00000001
   nas = <none>
   idle = 10000, PoD = no
   billing = PREPAID, plan = PERF, handoff timer OFF, idle timer OFF
   bma: ip = 10.18.28.10, port = 3333
   quota-server: ip = 0.0.0.0, port = 0
   affinity state = OPEN
10.18.28.14     C-10.18.28.14
   sessions = 1, traffic proc id = 4
   nexthop downlink ip = 0.0.0.0, flags = 0x00000001
   nas = <none>
   idle = 10000, PoD = no
   billing = PREPAID, plan = PERF, hand
```

Related Commands

Command	Description
ip csg billing	Defines a CSG2 billing plan, and enters CSG2 billing configuration mode.
ip csg content	Configures content for CSG2 services, and enters CSG2 content configuration mode.

show ip iscsi

To display information about the iSCSI, use the **show ip iscsi** command in privileged EXEC mode.

show ip iscsi {name | session [*session-id*] [**detail**] **| stats** [**detail**] **| target}**

Syntax Description

name	Displays the name of an iSCSI initiator.
session	Displays the status of iSCSI sessions on the CSG2.
session-id	(Optional) Displays information for only the specified iSCSI session.
detail	(Optional) Displays detailed information about the iSCSI session.
stats	Displays iSCSI statistics.
detail	(Optional) Displays detailed iSCSI statistics.
target	Displays information about an iSCSI target.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(15)MD	This command was introduced.

Examples

The following example shows output from the **show ip iscsi name** command:

```
Router# show ip iscsi name
iSCSI initiator name: iqn.1987-07.com.cisco:wtbg-sup-09-3
```

The following example shows output from the **show ip iscsi session** command:

```
Router# show ip iscsi session
ID  TARGET  STATE     CONNECTIONS
---------------------------------------------------------------
12  LINUX   Logged In  1
```

The following example shows output from the **show ip iscsi session detail** command:

```
Router# show ip iscsi session detail
ID: 12
Profile: LINUX
State: Logged In
Connections: 1
First Burst Length: 16384
Max Burst Length: 16384
Max Recv Data Segment: 32768
Max Xmit Data Segment: 8192
Initial R2T: Yes
Immediate data: Yes
Data PDU in order: Yes
Data PDU in order: Yes
```

The following example shows output from the **show ip iscsi stats** command:

```
Router# show ip iscsi stats
 iSCSI Stats:
  Login Requests - 2, Login Responses - 2
  Logout Requests - 0, Logout Responses - 0
  Login Timeouts - 0, Logout Timeouts - 0
  SCSI Commands - 27, SCSI Responses - 27
  Data In PDUs - 25, Data Out PDUs - 0
  Immed Data - 1, Unsolicited Data - 0
  NOP Ins - 35, NOP Outs - 35
  Async Requests - 0, Async Req Logout - 0
  Async Drop Conn - 0, Async Drop Conns - 0
  R2t Requests - 0, Rejects - 0

 System Stats:
  TX Queue Overflow - 0, RX Queue Overflow - 0
  Connection Resets - 0, Tasks aborted - 0

 SCSI Stats:
  Total Requests - 27
  Test Unit Ready Requests - 1, Test Unit Ready Failures - 0
  Report Luns Requests - 1, Report Luns Failures - 0
  Lun Inquiry Requests - 5, Lun Inquiry Failures - 0
  Read Capacity Requests - 5, Read Capacity Failures - 0
  Read Requests - 14, Read Failures - 0
  Write Requests - 1, Write Failures - 0
  Blocks Read- 49, Blocks Written - 8
```

The following example shows output from the **show ip iscsi stats detail** command:

```
Router# show ip iscsi stats detail
 iSCSI Stats:
  Login Requests - 2, Login Responses - 2
  Logout Requests - 0, Logout Responses - 0
  Login Timeouts - 0, Logout Timeouts - 0
  SCSI Commands - 27, SCSI Responses - 27
  Data In PDUs - 25, Data Out PDUs - 0
  Immed Data - 1, Unsolicited Data - 0
  NOP Ins - 36, NOP Outs - 36
  Async Requests - 0, Async Req Logout - 0
  Async Drop Conn - 0, Async Drop Conns - 0
  R2t Requests - 0, Rejects - 0

 System Stats:
  TX Queue Overflow - 0, RX Queue Overflow - 0
  Connection Resets - 0, Tasks aborted - 0

 SCSI Stats:
  Total Requests - 27
  Test Unit Ready Requests - 1, Test Unit Ready Failures - 0
  Report Luns Requests - 1, Report Luns Failures - 0
  Lun Inquiry Requests - 5, Lun Inquiry Failures - 0
  Read Capacity Requests - 5, Read Capacity Failures - 0
  Read Requests - 14, Read Failures - 0
  Write Requests - 1, Write Failures - 0
  Blocks Read- 49, Blocks Written - 8
```

The following example shows output from the **show ip iscsi target** command:

```
Router# show ip iscsi target
Target Profile= TARGET_LINUX IN_USE
  Target: name= iqn.2002-10.edu.unh.iol.iscsi.draft20-target:1
  Target: ip= 10.76.43.233, port= 3260, portal group= 0
  vrf= , sync read offset= 100, batch write= 100
  write interval= 5 sec, file size= 100 MB #
```

show record-storage-module

To display information about the record storage module (RSM), use the **show record-storage-module** command in privileged EXEC mode.

show record-storage-module {stats | target-info [all | target-profile *profile-name*] **[detail]}**

Syntax Description

stats	Displays current RSM statistics.
target-info	Displays the number of RSM disks available, and their current status.
all	(Optional) Displays statistics for all targets for which there are profiles.
target-profile *profile-name*	(Optional) Displays statistics for a specific profile.
detail	(Optional) Displays detailed information about the RSM drives.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(15)MD	This command was introduced.

Usage Guidelines

Use the **show record-storage-module stats** command to display RSM statistics.

Examples

The following example shows output from the **show record-storage-module stats** command:

```
Router# show record-storage-module stats
RSM Appl Stats:
 requests:
  open= 1, read= 0, write= 0
  ping= 0, close= 0
 request fail:
  open= 0, read= 0, write= 0
  ping= 0, close= 0 | ta
 alloc fail:
  appl info= 0, appl msg= 0, appl req= 0,
  data buffer= 0, drive= 0
 RSM Clear:
    Statistics = 1
```

The following example shows output from the **show record-storage-module target-info all detail** command:

```
Router# show record-storage-module target-info all detail
  Target profile = TARGET_LINUX
  Application name = GGSN, Target State = Active, Disk = Usable
  Application id = 2, iSCSI handle = 2
```

```
Number of drives = 5, Read drive = sda3, Write drive = sda3
Active drives:
 Drive = sda3
 File system id = 19
 Descriptors: read = -1, write = -1, master = -1
 Current File: bytes written = 0, bytes read = 0
 Master file in memory:
 Drive full = No
 Write: dir = 1, file = 1
 Read: dir = 1, file = 1, offset = 62675
 Salvage file = 0, CRC = 0x91C816C0
Failed drives:
 Drive = sda0
 Reason = Unexpected IFS error (Invalid DOS media or no media in slot)
 Drive = sda1
 Reason = Unexpected IFS error (Invalid DOS media or no media in slot)
 Drive = sda2
 Reason = Unexpected IFS error (Invalid DOS media or no media in slot)
 Drive = sda4
 Reason = Unexpected IFS error (Invalid DOS media or no media in slot)
```

snmp-server enable traps csg

To enable Simple Network Management Protocol (SNMP) notification types that are available on the CSG2, use the **snmp-server enable traps csg** command in global configuration mode. To disable CSG2 notifications, use the **no** form of this command.

snmp-server enable traps csg [**bma** [**records** | **state**] | **database** | **quota-server** [**records** | **state**]]

no snmp-server enable traps csg [**bma** [**records** | **state**] | **database** | **quota-server** [**records** | **state**]]

Syntax Description

bma	(Optional) Enables traps for only the Billing Mediation Agents (BMAs) to which the CSG2 sends billing records.
records	(Optional) Enables only lost records traps for the BMAs.
state	(Optional) Enables only state change traps for the BMAs.
database	(Optional) Enables traps for only the database server that answers CSG2 user ID queries.
quota-server	(Optional) Enables traps for only the CSG2 quota servers.
records	(Optional) Enables only lost records traps for the quota servers.
state	(Optional) Enables only state change traps for the quota servers.

Command Default

If you do not enter the **snmp-server enable traps csg** command, no CSG2 notifications controlled by this command are sent.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The **bma**, **database**, **quota-server**, **records**, and **state** keywords were added. • The **agent**, **database**, and **quota-server** keywords were removed.

Usage Guidelines

Entering the **snmp-server enable traps csg** command enables all CSG2 SNMP traps.

If you then enter the **snmp-server enable traps csg bma** command, the BMA lost records and state change traps are enabled.

If you then enter the **snmp-server enable traps csg quota-server records** command, the quota server lost records trap is enabled.

Examples

The following example enables CSG2 traps:

```
snmp-server enable traps csg
```

Related Commands

Command	Description
ip csg snmp timer	Defines Simple Network Management Protocol (SNMP) timers for lost CSG2 records, and enters CSG2 SNMP timer configuration mode.

subscriber-ip http-header forwarded-for

To specify that the CSG2 is to obtain the subscriber's IP address from the HTTP X-Forwarded-For header, use the **subscriber-ip http-header x-forwarded-for** command in CSG2 content configuration mode. To specify that the CSG2 is to obtain the subscriber's IP address from the IP header, use the **no** form of this command.

subscriber-ip http-header x-forwarded-for [**obscure**]

no subscriber-ip http-header x-forwarded-for

Syntax Description

obscure	(Optional) Overwrite the IP address in the X-Forwarded-For header with blanks.

Defaults

The CSG2 obtains the subscriber's IP address from the IP header.
If you enter the **subscriber-ip http-header x-forwarded-for** command without the **obscure** keyword, the IP address in the X-Forwarded-For header is not obscured with blanks.

Command Modes

CSG2 content configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

If the CSG2 is configured to obtain the subscriber's IP address from the HTTP X-Forwarded-For header, it also automatically recognizes the variant X-UP-Forwarded-For header.

Only content that is configured with **parse protocol http** can be configured with **subscriber-ip http-header x-forwarded-for**.

Single-TP mode is required for HTTP X-Forwarded-For operation.

- Before configuring the CSG2 for X-Forwarded-For operation, configure the CSG2 for single-TP mode by entering the **ip csg mode single-tp** command, then performing a **write memory**, then restarting the CSG2.
- If the CSG2 is not operating in single-TP mode, and you attempt to enter the **subscriber-ip http-header x-forwarded-for** command, the CSG2 rejects the command and issues a warning message.
- If the CSG2 is operating in single-TP mode and you attempt to switch to multiple-TP mode, the CSG2 checks the configuration for the **subscriber-ip http-header x-forwarded-for** command. If the configuration does contain the command (that is, X-Forwarded-For operation is enabled), the CSG2 does not switch to multiple-TP mode, and it issues a warning message.

To prevent exposure of potentially sensitive IP addresses, the CSG2 can obscure the contents of X-Forwarded-For headers, overwriting the contents with blanks.

- If you want to obscure the contents of the X-Forwarded-For header, enter the **subscriber-ip http-header x-forwarded-for** command with the **obscure** keyword.
- If you do not want to obscure the contents of the X-Forwarded-For header, enter the **subscriber-ip http-header x-forwarded-for** command without the **obscure** keyword (the default setting).
- When obscuring the IP address in X-Forwarded-For headers, keep the following considerations in mind:
  - The CSG2 does not obscure the IP address in fragmented request packets that have X-Forwarded-For headers, because the CSG2 does not reassemble the fragments and therefore cannot modify the packets.
  - The CSG2 does not obscure the X-Forwarded-For header for traffic that is downgraded from Layer 7 inspection to Layer 4 inspection.
  - If the active CSG2 fails over to the standby CSG2, the standby CSG2 does not obscure the IP address in X-Forwarded-For header for existing HTTP sessions. However, the standby CSG2 does obscure the IP address in X-Forwarded-For headers for new HTTP sessions.
  - If the subscriber sends more than one GET request with X-Forwarded-For headers, and the content host fails to send a TCP acknowledgement within five seconds, the CSG2 resets the subscriber side connection.

Examples

The following example configures the CSG2 to obtain the subscriber's IP address from the HTTP X-Forwarded-For header, and obscures the IP address in the X-Forwarded-For header:

```
ip csg content MOVIES
 parse protocol http
 subscriber-ip http-header x-forwarded-for obscure
```

Related Commands

Command	Description
ip csg content	Configures content for CSG2 services, and enters CSG2 content configuration mode.
ip csg mode single-tp	Enables the CSG2 to use a single TP instead of multiple TPs.
parse length	Defines the maximum number of Layer 7 bytes that the CSG2 is to parse when attempting to assign a policy.
parse protocol	Defines how the CSG2 is to parse traffic for a content.

target-portal (iSCSI)

To specify the portal group tag for an iSCSI target in the target interface profile on the CSG2, use the **target-portal** command in iSCSI configuration mode. To remove the tag, use the **no** form of the command.

target-portal *duration*

no target-portal

Syntax Description

tag	Portal group tag for the iSCSI target. The iSCSI target portal group tag specifies the IP and TCP port numbers on which an iSCSI target is allowed to bind, and the interface on which the iSCSI target listens. The iSCSI initiator uses the portal group to connect to the target. The range is from 1, which means the iSCSI initiator can connect to the target on any interface, to 65535. The default setting is 1.

Command Default

The iSCSI initiator can connect to the target on any interface.

Command Modes

iSCSI configuration

Command History

Release	Modification
12.4(15)MD	This command was introduced.

Examples

The following example configures an iSCSI target interface profile with the name **targetA** with iSCSI target portal group tag **1**:

```
ip iscsi target-profile targetA
  name iqn.2002-10.edu.abc.iol.iscsi.draft20-target:1
  ip 10.0.0.1
  port 3260
  session-timeout 120
  target-portal 1
```

Related Commands

Command	Description
ip (iSCSI)	Specifies the IP address of an iSCSI target in the target interface profile on the CSG2.
ip csg iscsi drain delay	Defines the delay interval, in seconds, before draining packets from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) when the Billing Mediation Agent (BMA) becomes active.

Command	Description
ip csg iscsi drain packet	Defines the number of packets to be drained from the Storage Area Network (SAN) connected to the Internet Small Computer Systems Interface (iSCSI) per drain delay interval when the Billing Mediation Agent (BMA) becomes active.
ip csg iscsi profile	Specifies the Internet Small Computer Systems Interface (iSCSI) target to be used as backup storage for the CSG2.
ip iscsi target-profile	Creates an iSCSI profile for an iSCSI target on the CSG2, and enters iSCSI configuration mode.
name (iSCSI)	Specifies the name of an iSCSI target in the target profile on the CSG2
port (iSCSI)	Specifies the number of the port on which to listen for iSCSI traffic in the iSCSI target interface profile on the CSG2.
session-timeout (iSCSI)	Specifies the session timeout for an iSCSI target in the target interface profile on the CSG2.

verify confirm

To configure a token for use in CSG2 service verification URL-rewriting, use the **verify confirm** command in CSG2 service configuration mode. To remove the token, use the **no** form of this command.

verify confirm *token*

no verify confirm *token*

Syntax Description

token	A string of up to 15 alphanumeric characters. The string is not case-sensitive. Acceptable characters include alphanumeric characters and any of the following special characters: $-_.+!*'(),?/:@&=;~%. To enter other special characters not listed, use the URL-escape format with the percent sign (%). To insert a question mark (?) in the string, press Ctrl-v and then press the question mark (**?**) key. To insert a question mark in an editing document, use ASCII code 22. To retain the question mark, use TFTP instead of copy-and-paste.

Defaults

None

Command Modes

CSG2 service configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1. Changes from CSG1: • The name of this command changed from **verify confirmation** to **verify confirm**. • The configuration mode for this command changed from CSG user group configuration to CSG2 service configuration. • The list of supported special characters changed.

Usage Guidelines

URL-rewriting allows a top-off server to append parameters to a URL in order to convey state information to the quota server during a Content Authorization Request. Whenever a Service Verification Response contains the forward action code, and the URL contains the verify confirmation token, the token and all trailing characters are removed from the URL before the request is forwarded to the network.

The token is used for HTTP and wireless application protocol (WAP) service verification URL-rewriting.

If the token uses the URL-escape format, the redirect URL to which the token is being matched must also use the URL-escape format.

Examples

The following example specifies a token for service verification URL-rewriting:

```
ip csg service MOVIES
 aoc enable
 verify confirm ?CSG_VERIFY_OK
```

Related Commands

Command	Description
ip csg service	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.
verify enable	Enables CSG2 service verification.

verify enable

To enable CSG2 service verification, use the **verify enable** command in CSG2 service configuration mode. To disable this feature, use the **no** form of this command.

verify enable

no verify enable

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

CSG2 service configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1.
	Changes from CSG1: The name of this command changed from **verify** to **verify enable**.

Usage Guidelines

If this command is configured, the CSG2 uses the Service Verification Request to perform the following actions:

- Alert the quota server of a new transaction.
- Allow the quota server to direct the CSG2 to perform one of the following mutually exclusive actions:
  - **DROP**—Drop all packets for this flow.
  - **FORWARD**—Forward the flow without altering the destination (a weight might be specified).
  - **REDIRECT-URL**—Redirect subscriber requests to the URL provided by the quota server. The CSG2 sends a Layer 7 redirect to the subscriber (for example, HTTP 302 response) that contains the redirect URL.

Examples

The following example specifies a token for service verification URL-rewriting:

```
ip csg service SERVICE_NAME
 verify enable
```

Related Commands

Command	Description
ip csg service	Configures a CSG2 content billing service, and enters CSG2 service configuration mode.
verify confirm	Configures a token for use in CSG2 service verification URL-rewriting.

vlan (CSG2 content)

To restrict the CSG2 billing content to a single source VLAN, use the **vlan** command in CSG2 content configuration mode. To remove the restriction, use the **no** form of this command.

vlan *vlan-number*

no vlan

Syntax Description

vlan-number	Dot1q encapsulation VLAN number.

Defaults

None

Command Modes

CSG2 content configuration

Command History

Release	Modification
12.4(11)MD	This command was migrated from CSG1.
	Changes from CSG1: The *vlan-name* argument was replaced with the *vlan-number* argument.

Usage Guidelines

The VLAN number is dependent on the CSG2 card that receives the content. When the content is downloaded to a CSG2 card, the *vlan-number* argument is mapped to a specific VLAN number.

Examples

The following example shows how to restrict the CSG2 content billing to single-source VLAN number 67:

```
ip csg content MOVIES_COMEDY
 vlan 67
```

Related Commands

Command	Description
ip csg content	Configures content for CSG2 services, and enters CSG2 content configuration mode.

vrf

To restrict the CSG2 content to packets within a single Virtual Routing and Forwarding (VRF) table, use the **vrf** command in CSG2 content configuration mode. To remove the restriction, use the **no** form of this command.

vrf *vrf-name*

no vrf

Syntax Description

vrf-name	VRF within which the content should match packets. **Note** The VRF table name is defined using the **vrf definition** command in global configuration mode. VRF table names supported by the CSG2 can be from 1 to 32 characters long, and can include uppercase or lowercase letters, numbers, and any special characters. The CSG2 does not support the use of the word **forwarding** as a valid VRF name.

Defaults

None

Command Modes

CSG2 content configuration

Command History

Release	Modification
12.4(11)MD	This command was introduced.

Usage Guidelines

VRF configuration and filtering cannot be used in conjunction with VLAN filtering.

If you want to use VRF tables to restrict CSG2 content, we recommend that you define a VRF table for every content. If you do not configure a VRF table for a given content, then that content cannot match traffic to a VRF table, and you cannot use a global content to match traffic in different VRF tables.

Examples

The following example shows how to restrict the CSG2 content to packets within VRF table CONTENTVRF:

```
ip csg content MOVIES_COMEDY
 vrf CONTENTVRF
```

Related Commands

Command	Description
ip csg content	Configures content for CSG2 services, and enters CSG2 content configuration mode.

APPENDIX **B**

CSG2 Command History—CSG1 R7 to CSG2 R1

The following sections document the changes to commands between the CSG1 Release 7 and the CSG2 Release 1:

- Unchanged Commands, page B-1
- New Commands, page B-2
- Deleted Commands, page B-3
- Changed Commands, page B-5
- Changes to Module CSG Configuration Mode, page B-10
- Changes to Module CSG VLAN Configuration Mode, page B-10
- Changes to Accounting Configuration Mode, page B-11
- Changes to Billing Configuration Mode, page B-12
- Changes to Block Configuration Mode, page B-12
- Changes to Content Configuration Mode, page B-12
- Changes to Map Configuration Mode, page B-13
- Changes to Policy Configuration Mode, page B-13
- Changes to Refund Configuration Mode, page B-14
- Changes to Ruleset Configuration Mode, page B-14
- Changes to Service Configuration Mode, page B-14
- Changes to SNMP Timer Configuration Mode, page B-15
- Changes to Transport-Type Configuration Mode, page B-15
- Changes to User Group Configuration Mode, page B-16
- Changes to Weight Configuration Mode, page B-17

Unchanged Commands

The following commands did not change between the CSG1 and the CSG2:

- **activation**
- **class**
- **flags**

- idle (CSG2 service)
- inservice (CSG2 content)
- ip (CSG2 content)
- ip csg billing
- ip csg content
- ip csg policy
- ip csg refund
- ip csg service
- meter increment
- meter initial
- meter minimum
- mode
- passthrough
- pending
- policy (CSG2 content)
- retcode
- service
- show ip csg

New Commands

The following commands are new for the CSG2:

- aoc append url
- clear ip csg
- ip csg bma keepalive
- ip csg bma messages
- ip csg bma retransmit
- ip csg bma retries
- ip csg bma window
- ip csg case-sensitive
- ip csg entries fragment
- ip csg entries session user max
- ip csg entries user idle
- ip csg entries user max
- ip csg ipc crashdump
- ip csg ipc keepalive
- ip csg ipc retransmit
- ip csg ipc retries

- ip csg mode single-tp
- ip csg psd drain delay
- ip csg psd drain packet
- ip csg psd keepalive
- ip csg psd margin
- ip csg psd retransmit
- ip csg psd retries
- ip csg psd window
- ip csg quota-server keepalive
- ip csg quota-server messages
- ip csg quota-server reassign
- ip csg quota-server retransmit
- ip csg quota-server retries
- ip csg quota-server window
- ip csg radius correlation
- ip csg replicate
- ip csg report smtp rfc2822
- ip csg report wap actual-pdu
- ip csg subscriber
- match header
- meter exclude mms wap
- mode tcp
- parse length
- parse protocol
- reauthorization threshold
- reauthorization timeout
- records delay
- sami rate all
- subscriber-ip http-header forwarded-for
- vrf

Deleted Commands

The following CSG1 commands have been deleted from the CSG2:

- **accounting (module CSG2)**
- **alias (module CSG2 VLAN)**
- **assign**
- **clear module csg**

- **clear module csm**
- **client (CSG2 content)**
- **client-ip (CSG2 policy)**
- **content (CSG2 ruleset)**
- **copy**
- **entries**
- **failover**
- **ft group (module CSG2)**
- **gateway (module CSG2 VLAN)**
- **heartbeat-time**
- **hostname**
- **ip address (module CSG2 VLAN)**
- **ip csg accounting**
- **ip csg user-group**
- **ip csg weight**
- **keepalive**
- **module csg**
- **ping**
- **priority**
- **radius acct-port**
- **radius key**
- **radius monitor**
- **radius parse strict**
- **radius server**
- **records batch**
- **records http-statistics**
- **route (module CSG2 VLAN)**
- **ruleset**
- **show module csg arp**
- **show module csg billing**
- **show module csg clock**
- **show module csg conns**
- **show module csg ft**
- **show module csg status**
- **show module csg tech-support**
- **show module csg variable**
- **show module csg vlan**
- **table (module CSG2 VLAN)**

- **upgrade**
- **user-group**
- **variable (module csg)**
- **vlan (module csg)**
- **zero-quota abort type**

Changed Commands

Table B-1 summarizes the changes made to commands between the CSG1 and the CSG2:

Table B-1 Commands That Changed Between CSG1 and CSG2

Command	Change from CSG1
accounting	All keywords and arguments except **customer-string** *string* were removed.
agent (CSG2 accounting)	The name of this command changed to **ip csg bma**. The **vrf** *vrf-name* keyword and argument were added.
agent activate	The name of this command changed to **ip csg bma activate**. The range of the *number* argument changed from 1 to 10, to 1 to 32.
agent local-port	The name of this command changed to **ip csg bma local-port**.
aoc confirmation	The name of this command changed to **aoc confirm**. The configuration mode for this command changed from CSG user group configuration to CSG2 service configuration. The list of supported special characters changed.
authorize content	The name of this command changed to **aoc enable**.
basis	The **exclude mms** keyword was removed.
client-group (CSG2 content)	The configuration mode for this command changed from CSG policy configuration to CSG2 content configuration. The range for the *std-access-list-number* argument increased from 1300 to 1999.
content (CSG2 service)	The *weight-name* argument was replaced with the *weight-value* argument.
database	The name of this command changed to **ip csg database**. The configuration mode for this command changed from CSG user group to global configuration. The **vrf** *vrf-name* and *local-port* keywords and arguments were added.
debug ip csg	The **acl** *number*, **configuration sync**, **detail**, **dump**, **error**, **frag**, **global**, **ha**, **http**, **interm**, **ipc**, **mail**, **other**, **packet**, *priority*, **qs**, **replicate**, **service**, **session event**, **session state**, **stats**, and **vrf** *vrf-name*, keywords and arguments were added. The **any**, **bma**, **ipc**, **psd**, and **quota-server** keywords were added for the **gtp** keyword. The **agent**, **api**, **cpu**, **module** *number*, **quota**, **prepaid**, **record storage** *slot*, and **timer** keywords and arguments were removed.
entries idle (CSG2 billing)	The name of this command changed to **entries user idle**.
header-map	This command, along with the **url-map** command, was incorporated into **map**.

Table B-1 Commands That Changed Between CSG1 and CSG2 (continued)

Command	Change from CSG1
idle (CSG2 content)	The default setting for the *duration* argument changed from 3600 seconds to 300 seconds.
ip csg block	The name of this command changed to **block**. The configuration mode for this command changed from global to CSG content configuration.
ip csg map	The **header** and **url** keywords were removed.
ip csg snmp timer	The **psd** keyword was added. The **agent** keyword was replaced with the **bma** keyword.
ip csg transport-type	The name of the command changed to **ip csg transport-type assign**. The *ip-address* and *value* arguments were added.
keepalive	The name of this command changed to **ip csg bma keepalive**. The configuration mode for this command changed from CSG accounting to global configuration.
match (header map)	The name of this command changed to **match header**. The configuration mode for this command changed from CSG header map configuration to CSG2 map configuration. The **protocol** *protocol* and **value** keywords and arguments were removed. The *pattern* argument was replaced with the *value* argument.
match (url map)	The name of this command changed to **match url**. The configuration mode for this command changed from CSG URL map configuration to CSG2 map configuration. The **protocol** *protocol* and **method** *method* keywords and arguments were removed.
meter exclude	The **meter exclude** command split into three new commands—**meter exclude mms wap**, **meter exclude pause rtsp**, and **meter exclude svc-idle**.
meter imap	The name of this command changed to **meter include imap**. The **body-header**, **body-only**, and **body-other** keywords changed to **body header**, **body only**, and **body other**, respectively.
next-hop	The configuration mode for this command changed from CSG policy configuration to CSG2 content configuration. The **reverse** keyword was added.
owner id	This command, along with the **owner name** command, was incorporated into **owner**.
owner name	This command, along with the **owner id** command, was incorporated into **owner**.
quota activate	The name of this command changed to **ip csg quota-server activate**. The configuration mode for this command changed from CSG user group configuration to global configuration. The range for the *number* argument changed from 1 to 10, to 1 to 32.

Table B-1 Commands That Changed Between CSG1 and CSG2 (continued)

Command	Change from CSG1
quota local-port	– The name of this command changed to **ip csg quota-server local-port**. – The configuration mode for this command changed from CSG user group configuration to global configuration. – The range for the *port-number* argument changed from 1 to 65535, to 1024 to 65535.
quota server	The name of this command changed to **ip csg quota-server**. The configuration mode for this command changed from CSG user group configuration to global configuration. The **vrf** *vrf-name* keyword and argument were added. The **reassign** keyword was removed.
radius ack error	The **radius ack error** command split into two new commands—**ip csg radius ack error parse** and **ip csg radius ack error user**. The configuration mode for this command changed from CSG user group configuration to global configuration.
radius endpoint	The name of this command changed to **ip csg radius endpoint**. The configuration mode for this command changed from module CSG configuration to global configuration. The **vrf** *vrf-name* and **vrf** *sub-vrf-name* keywords and arguments were added. The **table** *table-name* keyword and argument were removed.
radius handoff	The name of this command changed to **ip csg radius handoff**. The configuration mode for this command changed from CSG user group configuration to global configuration.
radius pod attribute	The name of this command changed to **ip csg radius pod attribute**. The configuration mode for this command changed from CSG user group configuration to global configuration. The **26** keyword was removed.
radius pod nas	The name of this command changed to **ip csg radius pod nas**. The configuration mode for this command changed from CSG user group configuration to global configuration. The **vrf** *vrf-name* keyword and argument were added.
radius pod timeout	The name of this command changed to **ip csg radius pod timeout**. The configuration mode for this command changed from CSG user group configuration to global configuration.
radius proxy	The name of this command changed to **ip csg radius proxy**. The configuration mode for this command changed from module CSG configuration to global configuration. The **vrf** *vrf-name* keyword and argument were added. The **table** *table-name* keyword and argument were removed.

Table B-1 Commands That Changed Between CSG1 and CSG2 (continued)

Command	Change from CSG1
radius start restart session-id	The name of this command changed to **ip csg radius start restart session-id**. The configuration mode for this command changed from module CSG configuration to global configuration. The **26** keyword was removed.
radius stop purge	The name of this command changed to **ip csg radius stop purge**. The configuration mode for this command changed from module CSG configuration to global configuration. The **26** keyword was removed.
radius userid	The name of this command changed to **ip csg radius userid**. The configuration mode for this command changed from module CSG configuration to global configuration.
records format	The name of this command changed to **ip csg records format**. The configuration mode for this command changed from CSG accounting configuration to global configuration. The **variable-single-cdr** keyword was replaced with the **combined** keyword. The **http** and **wap** keywords were added.
records granularity	The **time** keyword changed to **seconds**. The range for the *seconds* argument changed from 60 to 4294967295, to 5 to 86400.
records intermediate	The configuration mode for this command changed from CSG accounting configuration to CSG2 content configuration. The **time** keyword changed to **seconds**. The range for the *seconds* argument changed from 5 to 65535, to 5 to 86400.
records max	The name of this command changed to **ip csg bma messages**. The configuration mode for this command changed from CSG accounting configuration to global configuration.
record-storage	The name of this command changed to **ip csg psd**. The configuration mode for this command changed from CSG accounting configuration to global configuration. The **vrf** *vrf-name* keyword and argument were added.
record-storage local-port	The name of this command changed to **ip csg psd local-port**. The configuration mode for this command changed from CSG accounting configuration to global configuration.
redirect	The name of this command changed to **ip csg redirect**. The configuration mode for this command changed from CSG user group configuration to CSG2 service configuration. The **interval** *seconds* and **maximum** *number* keywords and arguments were added. The **nat** *ip-address* and *port-number* keyword and arguments were removed.
refund-policy	The name of this command changed to **refund**.

Table B-1 Commands That Changed Between CSG1 and CSG2 (continued)

Command	Change from CSG1
replicate connection tcp	The name of this command changed to **replicate**. The **delay** *seconds* keyword and argument were added.
report http header	The name of this command changed to **ip csg report http header**. The configuration mode for this command changed from CSG accounting configuration to global configuration.
report radius attribute	The name of this command changed to **ip csg report radius attribute**. The configuration mode for this command changed from CSG accounting configuration to global configuration. The **26** keyword was removed.
report usage	The name of this command changed to **ip csg report usage**. The configuration mode for this command changed from CSG accounting configuration to global configuration.
show module csg accounting	This command, along with the **show module csg content** and **show module csg stats** commands, was incorporated into **show ip csg**.
show module csg content	This command, along with the **show module csg accounting** and **show module csg stats** commands, was incorporated into **show ip csg**.
show module csg stats	This command, along with the **show module csg accounting** and **show module csg content** commands, was incorporated into **show ip csg**.
snmp-server enable traps csg	The **bma**, **database**, **quota-server**, **records**, and **state** keywords were added. The **agent**, **database**, and **quota-server** keywords were removed.
url-map	This command, along with the **header-map** command, was incorporated into **map**.
user-profile server	The name of this command changed to **ip csg entries user profile**. The configuration mode for this command changed from CSG user group to global configuration.
verify	The name of this command changed to **verify enable**.
verify confirmation	The name of this command changed to **verify confirm**. The configuration mode for this command changed from CSG user group configuration to CSG2 service configuration. The list of supported special characters changed.
vlan (CSG2 content)	The *vlan-name* argument was replaced with the *vlan-number* argument.

Changes to Module CSG Configuration Mode

Table B-2 summarizations the changes to module CSG configuration mode between the CSG1 and the CSG2:

Table B-2 Summary of Changes to Module CSG Configuration Mode

Command Name	Status in the CSG2
module csg	Removed. There is no module CSG configuration mode in the CSG2. The old module CSG configuration mode commands have been removed or replaced with global configuration mode commands.
accounting (module CSG)	Removed.
ft group (module CSG)	Removed.
hostname	Removed.
radius endpoint	**ip csg radius endpoint**
radius proxy	**ip csg radius proxy**
ruleset	Removed.
variable	Removed.
vlan (module CSG)	Removed.

Changes to Module CSG VLAN Configuration Mode

Table B-3 summarizations the changes to module CSG VLAN configuration mode between the CSG1 and the CSG2:

Table B-3 Summary of Changes to Module CSG VLAN Configuration Mode

Command Name	Status in the CSG2
vlan (module CSG)	Removed. There is no module CSG VLAN configuration mode in the CSG2.
alias (module CSG VLAN)	Removed.
gateway (module CSG VLAN)	Removed.
ip address (module CDG VLAN)	Removed.
route (module CSG VLAN)	Removed.
table (module CSG VLAN)	Removed.

Changes to Accounting Configuration Mode

Table B-4 summarizations the changes to accounting configuration mode between the CSG1 and the CSG2:

Table B-4 Summary of Changes to Accounting Group Configuration Mode

Command Name	Status in the CSG2
ip csg accounting	Removed. There is no accounting configuration mode in the CSG2. The old accounting configuration mode commands have been removed, moved to other configuration modes, or replaced with global configuration mode commands.
aoc confirmation	**aoc confirm** Moved to CSG2 service configuration mode.
database	**ip csg database**
entries max	**ip csg entries user max**
ip csg entries user idle	New for CSG2.
ip csg quota-server reassign	New for CSG2.
quota activate	**ip csg quota-server activate**
quota local-port	**ip csg quota-server local-port**
quota server	**ip csg quota-server**
radius acct-port	Removed.
radius ack error	**ip csg radius ack error parse** and **ip csg radius ack error user**
radius handoff	**ip csg radius handoff**
radius key	Removed.
radius monitor	Removed.
radius parse strict	Removed.
radius pod attribute	**ip csg radius pod attribute**
radius pod nas	**ip csg radius pod nas**
radius pod timeout	**ip csg radius pod timeout**
radius server	Removed.
radius start restart session-id	**ip csg radius start restart session-id**
radius stop purge	**ip csg radius stop purge**
radius userid	**ip csg radius userid**
redirect	**ip csg redirect**
user-profile server	**ip csg entries user profile**
verify confirmation	**verify confirm**

Changes to Billing Configuration Mode

Table B-5 summarizations the changes to billing configuration mode between the CSG1 and the CSG2:

Table B-5 Summary of Changes to Billing Configuration Mode

Command Name	Status in the CSG2
ip csg billing	Same command name and configuration mode.
entries user idle	New for CSG2.
mode	Same command name and configuration mode.
service	Same command name and configuration mode.

Changes to Block Configuration Mode

Table B-6 summarizations the changes to block configuration mode between the CSG1 and the CSG2:

Table B-6 Summary of Changes to Block Configuration Mode

Command Name	Status in the CSG2
ip csg block	**block** Moved to CSG2 content configuration mode.

Changes to Content Configuration Mode

Table B-7 summarizations the changes to content configuration mode between the CSG1 and the CSG2:

Table B-7 Summary of Changes to Content Configuration Mode

Command Name	Status in the CSG2
ip csg content	Same command name and configuration mode.
block	Moved from block configuration mode.
client (CSG content)	Removed.
client-group (CSG2 content)	Moved from policy configuration mode.
idle (CSG2 content)	Same command name and configuration mode.
inservice (CSG2 content)	Same command name and configuration mode.
ip (CSG2 content)	Same command name and configuration mode.
mode tcp	New for CSG2.
next-hop	Moved from policy configuration mode.
parse length	New for CSG2.
parse protocol	New for CSG2.
pending	Same command name and configuration mode.
policy (CSG2 content)	Same command name and configuration mode.

Table B-7 Summary of Changes to Content Configuration Mode (continued)

Command Name	Status in the CSG2
records delay	New for CSG2.
records intermediate	Moved from accounting configuration mode.
replicate connection tcp	replicate
subscriber-ip http-header forwarded-for	New for CSG2.
vlan (CSG2 content)	Same command name and configuration mode.
vrf	New for CSG2.

Changes to Map Configuration Mode

Table B-8 summarizations the changes to map configuration mode between the CSG1 and the CSG2:

Table B-8 Summary of Changes to Map Configuration Mode

Command Name	Status in the CSG2
ip csg map	Same command name and configuration mode.
match (header map)	match header Moved to CSG2 map configuration mode.
match method	New for CSG2.
match (URL map)	match url Moved to CSG2 map configuration mode.

Changes to Policy Configuration Mode

Table B-9 summarizations the changes to policy configuration mode between the CSG1 and the CSG2:

Table B-9 Summary of Changes to Policy Configuration Mode

Command Name	Status in the CSG2
ip csg policy	Same command name and configuration mode.
accounting	Same command name and configuration mode.
client-group (CSG2 content)	Moved to CSG2 content configuration mode.
client-ip (CSG policy)	Removed.
header-map	map
next-hop	Moved to CSG2 content configuration mode.
url-map	map

Changes to Refund Configuration Mode

Table B-10 summarizations the changes to refund configuration mode between the CSG1 and the CSG2:

Table B-10 Summary of Changes to Refund Configuration Mode

Command Name	Status in the CSG2
ip csg refund	Same command name and configuration mode.
flags	Same command name and configuration mode.
retcode	Same command name and configuration mode.

Changes to Ruleset Configuration Mode

Table B-11 summarizations the changes to ruleset configuration mode between the CSG1 and the CSG2:

Table B-11 Summary of Changes to Ruleset Configuration Mode

Command Name	Status in the CSG2
ip csg ruleset	Removed.

Changes to Service Configuration Mode

Table B-12 summarizations the changes to service configuration mode between the CSG1 and the CSG2:

Table B-12 Summary of Changes to Service Configuration Mode

Command Name	Status in the CSG2
ip csg service	Same command name and configuration mode.
activation	Same command name and configuration mode.
aoc append url	New for CSG2.
aoc confirm	Moved from user group configuration mode.
aoc enable	New for CSG2.
authorize content	**aoc enable**
basis	Same command name and configuration mode.
class	Same command name and configuration mode.
content (CSG2 service)	Same command name and configuration mode.
idle (CSG2 service)	Same command name and configuration mode.
meter exclude	Three new commands for CSG2: **meter exclude mms wap**, **meter exclude pause rtsp**, and **meter exclude svc-idle**.
meter imap	**meter include imap**
meter increment	Same command name and configuration mode.
meter initial	Same command name and configuration mode.

Table B-12 Summary of Changes to Service Configuration Mode (continued)

Command Name	Status in the CSG2
meter minimum	Same command name and configuration mode.
owner id	**owner**
owner name	**owner**
passthrough	Same command name and configuration mode.
reauthorization threshold	New for CSG2.
reauthorization timeout	New for CSG2.
records granularity	Same command name and configuration mode.
refund-policy	**refund**
verify	**verify enable**
verify confirm	New for CSG2.
zero-quota abort type	Removed.

Changes to SNMP Timer Configuration Mode

Table B-13 summarizations the changes to SNMP timer configuration mode between the CSG1 and the CSG2:

Table B-13 Summary of Changes to SNMP Timer Configuration Mode

Command Name	Status in the CSG2
ip csg snmp timer	**ip csg snmp timer**

Changes to Transport-Type Configuration Mode

Table B-14 summarizations the changes to transport-type configuration mode between the CSG1 and the CSG2:

Table B-14 Summary of Changes to Transport-Type Configuration Mode

Command Name	Status in the CSG2
ip csg transport-type	**ip csg transport-type assign**

Changes to User Group Configuration Mode

Table B-15 summarizations the changes to user group configuration mode between the CSG1 and the CSG2:

Table B-15 Summary of Changes to User Group Configuration Mode

Command Name	Status in the CSG2
ip csg user-group	Removed. There is no user group configuration mode in the CSG2. The old user group configuration mode commands have been removed, moved to other configuration modes, or replaced with global configuration mode commands.
aoc confirmation	**aoc confirm** Moved to CSG2 service configuration mode.
database	**ip csg database**
entries max	**ip csg entries user max**
ip csg entries user idle	New for CSG2.
ip csg quota-server reassign	New for CSG2.
quota activate	**ip csg quota-server activate**
quota local-port	**ip csg quota-server local-port**
quota server	**ip csg quota-server**
radius acct-port	Removed.
radius ack error	**ip csg radius ack error parse**
radius handoff	**ip csg radius handoff**
radius key	Removed.
radius monitor	Removed.
radius parse strict	Removed.
radius pod attribute	**ip csg radius pod attribute**
radius pod nas	**ip csg radius pod nas**
radius pod timeout	**ip csg radius pod timeout**
radius server	Removed.
radius start restart session-id	**ip csg radius start restart session-id**
radius stop purge	**ip csg radius stop purge**
radius userid	**ip csg radius userid**
redirect	**ip csg redirect**
user-profile server	**ip csg entries user profile**
verify confirmation	**verify confirm**

Changes to Weight Configuration Mode

Table B-16 summarizations the changes to weight configuration mode between the CSG1 and the CSG2:

Table B-16 Summary of Changes to Weight Configuration Mode

Command Name	Status in the CSG2
ip csg weight	Removed.

APPENDIX C

CSG2 Command History—CSG2 R1 to CSG2 R2

The following sections document the changes to commands between the CSG2 Release 1 and the CSG2 Release 2:

- New Commands, page C-1
- Deleted Commands, page C-2
- Changed Commands, page C-2

New Commands

The following commands are new for the CSG2 Release 2:

- **clear ip iscsi statistics**
  (privileged EXEC configuration mode)
- **clear record-storage-module stats**
  (privileged EXEC configuration mode)
- **ip (iSCSI)**
  (iSCSI configuration mode)
- **ip csg iscsi drain delay**
  (global configuration mode)
- **ip csg iscsi drain packet**
  (global configuration mode)
- **ip csg iscsi profile**
  (global configuration mode)
- **ip csg radius monitor**
  (global configuration mode)
- **ip csg radius monitor nas**
  (global configuration mode)
- **ip csg radius on-off purge**
  (global configuration mode)
- **ip csg radius reauthorization attribute**
  (global configuration mode)
- **ip iscsi target-profile**
  (global configuration mode)

- **meter exclude control sip**
  (CSG2 service configuration mode)
- **meter exclude network-init sip**
  (CSG2 service configuration mode)
- **name (iSCSI)**
  (iSCSI configuration mode)
- **port (iSCSI)**
  (iSCSI configuration mode)
- **session-timeout (iSCSI)**
  (iSCSI configuration mode)
- **show ip iscsi**
  (privileged EXEC configuration mode)
- **show record-storage-module**
  (privileged EXEC configuration mode)
- **target-portal (iSCSI)**
  (iSCSI configuration mode)

Deleted Commands

No CSG2 Release 1 commands were deleted from the CSG2 Release 2.

Changed Commands

Table C-1 summarizes the changes made to commands between the CSG2 Release 1 and the CSG2 Release 2:

Table C-1 Commands That Changed Between CSG2 Release 1 and the CSG2 Release 2

Command	Change from CSG1
accounting	Support for FTP was added.
basis	The **transaction** keyword was added.
clear ip csg	The **ftp** keyword was added.
debug ip csg	The **crashinfo**, **ftp**, **iscsi**, **mail**, and **sip** keywords were added.
ip csg bma retransmit	The range changed from 1 to 65535 to 2 to 65535.
ip csg bma retries	The **packet** keyword was added.
ip csg entries user max	The range was changed to reflect the differences between the 2 GB-SAMI and 1 GB-SAMI options: • For the 2 GB-SAMI option, the range is from 1 to 1250000. • For the 1 GB-SAMI option, the range is from 1 to 500000.
ip csg entries user profile	The **timeout** keyword and *timeout* argument were added.
ip csg psd retries	The **packet** keyword was added.
ip csg quota-server retries	The **packet** keyword was added.

Table C-1 Commands That Changed Between CSG2 Release 1 and the CSG2 Release 2 (continued)

Command	Change from CSG1
ip csg redirect	The **sip** keyword and *url* argument were added.
match header	Support for Session Initiation Protocol (SIP) headers was added.
match method	Support for Session Initiation Protocol (SIP) methods was added.
match url	Support for Session Initiation Protocol (SIP) URLs was added.
next-hop	The **subscriber media** keywords were added.
parse protocol	The **ftp** and **sip** keywords were added.
policy (CSG2 content)	The **priority** keyword and the *priority-number* argument were added.
retcode	The **ftp** and **sip** keywords were added.
show ip csg	The **billing**, **ftp**, **gtp**, **history**, **iscsi**, **load**, **plan**, and **sip** keywords and *billing-plan-name* argument were added.

APPENDIX D

Protocol Compliance Statements for the CSG2

This appendix provides protocol compliance statements for the CSG2. Any RFCs that are not explicitly listed are not supported.

Layer 4 Inspection (parse protocol=other)

The Cisco Content Services Gateway 2 (CSG2) differentiates TCP and User Datagram Protocol (UDP), and classifies all other protocols simply as IP. All protocols can be billed as TCP, UDP, or IP if further protocol-specific processing is not needed (or if deeper inspection for such protocols is not supported).

- IP—Compliant with RFC 791.

  The CSG2 volume counters wrap at 0xFFFFFFFF (4294967295 bytes). The volume counters are 32 bits unsigned.

  The CSG2 supports IP fragmentation for generic Layer 4 flows, regardless of protocol and regardless of the order in which the flows arrive

- UDP—Compliant with RFC 768.
- TCP—Compliant with standard TCP (RFC 3168) and RFC 1323, with the following exceptions:
  - When performing Layer 4 inspection of TCP-based protocols, the CSG2 buffers packets that are received out of order, and processes and forwards them in the proper order.
  - The CSG2 does not support the CLOSING or TIME-WAIT states for TCP connections. When the final ACK is received, the connection is terminated, and the CSG2 does not count or process any out-of-order packets for the connection.

Layer 7 Inspection (parse protocol=specific protocol)

- IP—Compliant with RFC 791.

  The CSG2 supports IP fragmentation for all Layer 7 flows, regardless of protocol and regardless of the order in which the flows arrive

  The CSG2 IP volume counters wrap at 0xFFFFFFFF (4294967295 bytes). The volume counters are 32 bits unsigned.

- UDP—Compliant with RFC 768.

  See the Layer 7 Inspection “IP” bullet for further restrictions.

- TCP—Compliant with standard TCP (RFC 793), with the following exceptions:
  - When performing Layer 7 inspection of TCP-based protocols, the CSG2 buffers packets that are received out of order, and processes and forwards them in the proper order.
  - The CSG2 does not support the CLOSING or TIME-WAIT states for TCP connections. When the final ACK is received, the connection is terminated, and the CSG2 does not count or process any out-of-order packets for the connection.

  The CSG2 TCP volume counters wrap at 0xFFFFFFFF (4294967295 bytes). The volume counters are 32 bits unsigned.

  See the Layer 7 Inspection "IP" bullet for further restrictions.
- HTTP—Compliant with RFC 1945 (HTTP 1.0) and RFC 2616 (HTTP 1.1), with the following exceptions:
  1. Each HTTP method must be initiated by the same endpoint that initiated the TCP connection (that is, by the same side that sent the TCP SYN).

     Impact: Subscriber requests transfer no data (that is, the requests hang). See the "TO-TCP" sub-bullet under the Layer 7 Inspection "MMS for WAP 2.0" bullet for an example.
  2. HTTP request parsing is limited by the setting of the **parse length** command in CSG2 content configuration mode.

     Impact: If a header exceeds the configured limit, the session is ended and the header is not used in matching URL or header maps.
  3. If the HTTP network or subscriber causes improper parsing, the CSG2 reverts to Layer 4 billing for the remainder of the TCP connection. Examples of improper parsing include:

     - If an HTTP response does not begin with "HTTP", the CSG2 increments a Layer 7 error statistic, "Parse failures", and invokes Layer 4 billing. (The CSG2 requires that all HTTP responses begin with the string "HTTP".)

     - If a response contains characters other than ASCII decimal digits (0x30 through 0x39), the CSG2 increments the "Parse failures" statistic and invokes Layer 4 billing. (When parsing the response for an HTTP return code, the CSG2 accepts only ASCII decimal digits.)

     - If the CSG2 cannot parse the status line in the response, it invokes Layer 4 billing for all subsequent traffic.
  4. HTTP status 101 (switching protocols) is not supported. The CSG2 expects all subsequent requests to be unencrypted and parsable by HTTP rules (see the Layer 7 Inspection "HTTPS" bullet for further restrictions).

     Impact: The CSG2 increments the "Status code" statistic and invokes Layer 4 billing.
  5. Error codes 204, 205, and 304 do not require a body. If a response contains one of these error codes, the CSG2 ignores "Content-Type:", "Content-Length:", and "Transfer-Encoding:chunked" headers that might be present in error.
  6. An HTTP message that has a "Content-Type:" header, but no "Content-Length:" or "Transfer-Encoding:chunked" header, causes the CSG2 to invoke Layer 4 billing.
  7. If there are multiple responses for one request, the CSG2 invokes Layer 4 billing.
  8. Multipart content is supported. The CSG2 supports the standard "RANGE" header as well as the earlier "byterange" directive on the URI. In both cases, the "Content-Type: multipart..." header must be present in order for the CSG2 to consider the stream for multipart parsing. The particular subtype in the header does not matter, as long as multipart is specified as the type. If multipart is not specified in the "Content-Type:" header, the CSG2 parses the data as regular HTTP and reverts to Layer 4 billing if any errors in the format are detected.

Compliant with RFC 2774 (HTTP Extension Framework), subject to the restrictions above.

See the Layer Inspection "TCP" bullet for further restrictions.

- HTTPS—Because HTTPS URLs and other headers are encrypted, the CSG2 cannot provide Layer 7 information for HTTPS requests.

  Also, switching from HTTP to HTTPS within the same persistent connection is subject to the following restrictions:

  – Switching via the Connect method (RFC 2817) is supported. The CSG2 detects the Connect method and invokes Layer 4 billing for the remainder of the TCP connection. This Layer 4 charging is reported via the HTTP statistics CDR for the Connect transaction. The CSG2 will not discern any additional transactions after the Connect method is detected. If a method map is configured for the Connect method, the traffic is charged against the matching policy. If no policy exists with the method map, the CSG2 passes the traffic without charge.

  – Switching via the "Upgrade" header (RFC 2817) is ignored. The CSG2 attempts to parse the traffic as normal HTTP. When parsing fails, the CSG2 invokes Layer 4 billing for all subsequent traffic on the TCP connection, charging against the last matching policy.

  See the Layer 7 Inspection "HTTP" bullet for further restrictions.

- WAP 2.0—The CSG2 supports the billing of WAP 2.0 over clear text HTTP and the differential billing of Multimedia Messaging Service (MMS) over WAP 2.0 over clear text HTTP (see the Layer 7 Inspection "MMS for WAP 2.0" for details) as specified by the WAP Forum, with the following exceptions:

  – The CSG2 cannot bill Transport Layer Security (TLS) (encrypted connections) as WAP 2.0 flows. In WAP-235-PushOTA-20010425-a, TLS is referenced as OTA-HTTP-TLS.

  – See the Layer 7 Inspection "HTTPS" bullet for restrictions on switching from HTTP to HTTPS within the same persistent connection. WAP-219-TLS-20010411-a specifies that only the Connect method is supported (that is, portions of RFC 2817 pertaining to Upgrade requests or responses are not supported by WAP 2.0 subscribers).

  See the Layer 7 Inspection "HTTP 1.1," "HTTPS," and "WP-TCP" bullets for further restrictions.

- MMS for WAP 2.0 (HTTP transport)—At present the Multimedia Messaging Service (MMS) standard is very incomplete.

  – For MMS differentiation, the CSG2 requires that the "Content-Type" header in the request be set to "application/vnd.wap.mms-message" on all MMS, WAP 2.0, and HTTP exchanges, except for message retrieval requests.

  – For message retrieval, the "Content-Type" header is not present in the GET request, so the CSG2 uses the URL in the GET request and ignores the "Content-Type" header in the response. This method provides reasonable differentiation, although examining the "Content-Type" in the response is the preferred technique for MMS differentiation, in accordance with the standard.

  MMS over WAP 2.0 allows three types of notification:

  1. Short Message Service (SMS) notification carrying the Uniform Resource Identifier (URI) for the MMS. The handset then initiates a GET request to that URI to retrieve the information.
  2. TO-TCP, which starts with SMS but provides only the IP address of the Push Proxy Gateway (PPG). The terminal must then open a TCP connection and wait for an HTTP request from the PPG. This HTTP request is an OPTIONS method and must succeed before the handset can retrieve the notification.
  3. PO-TCP, which is similar to TO-TCP, except the TCP connection is opened by the PPG and is followed by the OPTIONS method.

The CSG2 Layer 7 billing for MMS relies entirely on notification types 1 and 3. The CSG2 does not support TO-TCP. If a terminal reuses a persistent PO-TCP to initiate a new method request, the packets are dropped and the PO-TCP connection appears to be hung until the TCP retry attempts expire.

See the Layer 7 Inspection "WAP 2.0" bullet for further restrictions.

- POP3—Compliant with RFC 1939. The CSG2 reports the RFC 2822 (Internet Message Format) headers in the body of the POP3 message.

  See the Layer Inspection "TCP" bullet for further restrictions.

- IMAP4—Compliant with RFC 3501.

  See the Layer Inspection "TCP" bullet for further restrictions.

- SMTP—Compliant with RFC 2821. Reports headers in the SMTP are body formatted in accordance with RFC 2822 - Internet Message Format.

  The CSG2 does not support SMTP command pipelining as defined in RFC 2920 - SMTP Service Extension for Command Pipelining.

  Impact: Everything is charged for the first e-mail, and incomplete or no SMTP envelopes and RFC 2822 headers are reported (depending on the e-mail content).

  See the Layer Inspection "TCP" bullet for further restrictions.

- FTP—Compliant with RFC 959. The CSG2 requires that the control connection use port 21 on the server.

  See the Layer Inspection "TCP" bullet for further restrictions.

- RTSP—Compliant with RFC 2326, except that the RFC allows RTSP control flows on either TCP or UDP, but the CSG2 supports RTSP control flows only on TCP. The CSG2 does not parse Synchronized Multimedia Integration Language (SMIL) or Streaming Data Protocol (SDP) files, so correlation is not supported across multiple elements in the file.

  For Interleaved RTSP (in which Control and Stream both share the control connection), the CSG2 parses only the first two SETUP commands.

  For I RTSP over HTTP:554 (with policy of type=rtsp), the CSG2 parses only the first SETUP command.

  See the Layer Inspection "TCP" bullet for further restrictions.

- WAP 1.x—Compliant with the following specifications:

  1. WAP-100, Wireless Application Protocol Architecture Specification (WAP-100-WAPArch-19980430-a)
  2. WAP-165, Push Architectural Overview (WAP-165-PushArchOverview-19991108-a)
  3. WAP-203, Wireless Session Protocol Specification (WAP-203-WSP-20000504-a)
  4. WAP-201, Wireless Transaction Protocol Specification (WAP-201-WTP-20000219-a)

  MMS for Wireless Session Protocol (WSP) is identified via WSP Content Type value 0X3E or via an application/vnd.wap.mms-message.

  See the Layer 7 Inspection "UDP" bullet for further restrictions.

- RADIUS—Compliant with RFC 2865 and RFC 2866. The CSG2 can inspect RADIUS Access and RADIUS Accounting messages.

  For RADIUS inspection, the CSG2 does not support messages that exceed an Ethernet frame size (approximately 1470 bytes). Also, the CSG2 does not police the attributes that it does not use.

  - Specific to RFC 2865—Base RADIUS specification:

    In order to parse information in the Access-Accept message (from the real server), the CSG2 requires attribute 1 (User-Name) or 31 (Calling-Station-Id), as configured. Page 63 of RFC 2865 shows a summary of the attributes for each of the RADIUS messages. It shows that attribute 31 is not included in the RADIUS Access-Accept message, while Attribute 1 can be. The description of attribute 31 says, "It is only used in Access-Request packets." There is no mention of MUST/SHALL/etc.

    For VSA subattribute parsing, we require the String contents to be encoded as a sequence of vendor type / vendor length / value fields. This is a recommendation (SHOULD) on page 48 of RFC 2865. If subattribute parsing is not configured, this restriction does not apply.

  - Specific to RFC 2866—Accounting:

    When operating as a RADIUS Accounting Endpoint, the RADIUS Accounting-Response generated by the CSG2 does not include any attributes, as per page 9 of the RFC:

    "A RADIUS Accounting-Response is not required to have any attributes in it."

    However, on page 5, step 3, of the RFC:

    "The remote server logs the accounting-request (if desired), copies all Proxy-State attributes in order and unmodified from the request to the response packet, and sends the accounting-response to the forwarding server."

    The CSG2 is not compliant with this latter statement, though it is not clear if this is a required element of the RFC.

  - Specific to RFC 2882—Extended practices:

    The CSG2 supports the RADIUS Disconnect messages defined in this RFC:

    40 Disconnect Request

    41 Disconnect Ack

    42 Disconnect Nak

  - Specific to RFC 3576—Dynamic extensions:

    This RFC notes specific ports to which the Disconnect Request is to be sent. The CSG2 allows the customer to configure the NAS port. Also, note specific actions to be taken when the Ack or Nak is received—The CSG2 uses the Ack or Nak only to determine whether it is to send the Request. The CSG2 does not use, process, or report any attributes included in the Ack or Nak. Attributes that the CSG2 sends in the Request are defined by the customer.

    The CSG2 does not support any other message types in this RFC.

  See the Layer 7 Inspection "UDP" bullet for further restrictions.

- SIP—Compliant with RFC 3261 and RFC 4566.
  - Individual SIP/SDP headers are not parsed beyond the first 256 characters.
  - You must enter the long form of the header name when configuring maps for SIP. The CSG2 does not support the short form of the header name.

- Domain names used in headers are not resolved to IP addresses. If domain names are used in headers for which IP addresses are required (such as media connect headers), the CSG2 cannot correctly identify and correlate the SIP media traffic.
- The CSG2 cleans up media sessions for SIP calls when a positive response to a BYE request is processed (200 ok). Media packets that flow after the 200 ok are not associated with the media session.

APPENDIX E

CSG2 System Messages

This appendix lists and describes Cisco CSG2, SAMI, and iSCSI system messages. The system software sends these messages to the console (and, optionally, to a logging server on another system) during operation. Not all system messages indicate problems with your system. Some are purely informational, and others may help diagnose problems with communications lines, internal hardware, or the system software.

This appendix also includes messages that appear when the system crashes.

In these messages, %s indicates a variable text string. For example, the following message:

GTP state change: %s

Can be displayed as:

GTP state change: Communication with CSG Billing Agent 19.19.19.19:2007 established

GTP state change: Communication with CSG Billing Agent 19.19.19.19:2007 failed

This appendix includes the following information:

- CSG2 System Messages, page E-1
- SAMI System Messages, page E-8
- iSCSI System Messages, page E-11

CSG2 System Messages

Message: Configuration download error: %s

Explanation

An unexpected condition was detected in the configuration sync module.

Mnemonic

CFG_DOWNLOAD_ER

Severity

LOG_EMERG - Sev 0

Message: %s

Explanation

An unexpected condition was detected in the configuration module.

Mnemonic

CFG_ERROR

Severity

LOG_WARNING - Sev 4

Message: Startup configuration completed.

Explanation

Startup configuration is completed. Traffic is now allowed.

This indicates CSG2 is done applying startup configuration.

Mnemonic

CFG_STARTUP_DONE

Severity

LOG_NOTICE- Sev 5

Message: Configuration Sync error: %s

Explanation

An unexpected condition was detected in the configuration sync module.

If you see this message after entering the **no** form of a command, continue to retry the command until it succeeds.

Mnemonic

CFG_SYNC_ERROR

Severity

LOG_WARNING - Sev 4

Message: %s

Explanation

An unexpected condition was detected in the CSG2 CG Affinity component.

Mnemonic

CG_AFF_ERROR

Severity
LOG_WARNING - Sev 4

Message: %s packet drop: queue size %d reached, record storage %s is currently %s

Explanation
An unexpected condition was detected while performing CSG2 operation.

Mnemonic
GTP_CDR_DROP

Severity
LOG_ERR - Sev 3

Message: GTP error: %s

Explanation
An error condition was detected while performing GTP operation.

This indicates serious problems within the CSG2 GTP component.

Mnemonic
GTP_ERROR

Severity
LOG_ERR - Sev 3

Message: GTP received reject cause code %d from %i:%u

Explanation
The server rejected a message sent by the CSG.

This indicates that the CSG2 received a reject.

Mnemonic
GTP_REJECT

Severity
LOG_ERR - Sev 3

Message: GTP state change: %s

Explanation

A service affecting state change has occurred in the IPC component.

This indicates problems with communications links between the IOS processors on this module. No action is necessary unless IOS functions are impacted due to unavailability of the IPC links. This message might reflect normal changes in IOS configuration or external network conditions between IOS and the charging gateways. If IPC communications links are being lost and regained frequently, it is important to investigate.

Mnemonic

GTP_STATE_CHANGE

Severity

LOG_WARNING - Sev 4

Message: IPC is link failed to processor %u, state = %u, software reloading card now.

Explanation

A failure in the internal messaging path between the processors on this card has been detected. Configure **no ip csg ipc crashdump** to prevent this action in the future

This indicates a serious problem with communications between the processors on the SAMI. The CSG2 might not be able to correctly bill traffic in this state. Crashing will induce an HA failover. If this is not the desired behavior consider configuring **no ip csg ipc crashdump** or configure a longer interval for **ip csg ipc crashdump tolerance** *seconds*.

Mnemonic

IPC_DROP_CRASH

Severity

LOG_WARNING - Sev 4

Message: %s

Explanation

A service affecting state change has occurred in the IPC component.

This might indicate a serious problem with communications between the processors on the SAMI, if IPC links are lost and do not recover.

Mnemonic

IPC_STATE_CHANGE

Severity

LOG_WARNING - Sev 4

Message: iSCSI device %i:%u is full

Explanation

The iSCSI is full.

This indicates that there is no more disk space on the iSCSI disk.

Mnemonic

iSCSI_FULL

Severity

LOG_ERR - Sev 3

Message: ISCSI state change: %s

Explanation

A service affecting state change has occurred in the ISCSI component.

This indicates problems with communications link with the ISCSI device. If link with remote ISCSI device are being lost and regained frequently it is important to investigate.

Mnemonic

ISCSI_STATE_CHANGE

Severity

LOG_WARNING - Sev 4

Message: %s transaction discarded due to high load.

Explanation

The CSG2 has run out of capacity to service new transactions, the most likely cause of this is system overload due to network activity. Statistics on allowed/denied transactions are under **show ip csg stats**.

This indicates that CSG2 is being overloaded in the customer's network, as a result subscriber packets, and billing information might be lost.

Mnemonic

LOAD_MGMT

Severity

LOG_WARNING - Sev 4

Message: Failed to set %s local port. Either there are no IP addresses configured or port %u is in use.

Explanation

Failed to obtain local port. Either there are no IP addresses configured or the port is in use.

This indicates an issue with reserving a local port for a CSG2 component.

Mnemonic

LOCAL_PORT

Severity

LOG_WARNING - Sev 4

Message: Lock depth %u has crossed threshold.

Explanation

An unexpected condition was detected while performing CSG2 operation.

Mnemonic

LOCKDEPTH

Severity

LOG_WARNING - Sev 4

Message: CSG NTP synchronization is complete

Explanation

CSG2 NTP synchronization is complete.

Mnemonic

NTP_SYNC_COMPLE

Severity

LOG_NOTICE- Sev 5

Message: Error: %s

Explanation

CSG2 detects the clock for the TP is not in sync with SUP.

This might indicate problems with NTP association between TP and SUP due to mis-configuration of NTP on CP or Supervisor.

Mnemonic

NTP_SYNC_ERROR

Severity

LOG_WARNING - Sev 4

Message: PSD device %i:%u is full

Explanation

The PSD is full. There is no more disk space on the PSD.

Mnemonic

PSD_FULL

Severity

LOG_ERR - Sev 3

Message: CSG replicate condition: %s

Explanation

An unexpected condition was detected while performing CSG2 replication operation.

Mnemonic

REPLICATE

Severity

LOG_WARNING - Sev 4

Message: Error: %s

Explanation

An unexpected error occurred while performing CSG2 operation.

Mnemonic

UNEXPECTED

Severity

LOG_WARNING - Sev 4

Message: Unexpected condition: %s

Explanation

An unexpected condition was detected while performing CSG2 operation.

Mnemonic

WARNING

Severity

LOG_WARNING - Sev 4

SAMI System Messages

This section lists SAMI messages (prefix SAMI) alphabetically by mnemonic.

Message: Nvram CRC Failure: %d\n

Explanation

NVRAM Corruption.

Mnemonic

NVRAM_CRC_FAILU

Severity

LOG_INFO - Sev 6

Message: Nvram Erase Failure: handle 0x%x, offset 0x%x, error %s

Explanation
NVRAM Erase Failure.

Mnemonic
NVRAM_ERASE_FAI

Severity
LOG_INFO - Sev 6

Message: Nvram Init Failure of flash device at %d:%s

Explanation
Unable to initialize flash device.

Mnemonic
NVRAM_INIT_FAIL

Severity
LOG_INFO - Sev 6

Message: Nvram Init Failure: %s

Explanation
Unable to initialize flash device: Low Memory.

Mnemonic
NVRAM_INIT_MEMO

Severity
LOG_INFO - Sev 6

Message: Nvram Magic Corrupt: Present %d Expected %d\n

Explanation
NVRAM Corruption.

Mnemonic
NVRAM_MAGIC_COR

Severity
LOG_INFO - Sev 6

Message: Nvram Write Failure: handle 0x%x, offset 0x%x, numbytes 0x%x error %s

Explanation
NVRAM Write Failure.

Mnemonic
NVRAM_WRITE_BLO

Severity
LOG_INFO - Sev 6

Message: Nvram Write Config Failure: \n

Explanation
NVRAM Write Failure.

Mnemonic
NVRAM_WRITE_CON

Severity
LOG_INFO - Sev 6

Message: Unexpected condition: %s

Explanation
An unexpected condition was detected while performing SAMI Platform operation.

Mnemonic
UNEXPECTED

Severity
LOG_WARNING - Sev 4

Message: Unexpected condition: %s

Explanation
An unexpected condition was detected while performing SAMI Platform operation.

Mnemonic
WARNING

Severity
LOG_WARNING - Sev 4

iSCSI System Messages

This section lists iSCSI messages (prefix ISCSI) alphabetically by mnemonic.

Message: Error: %s

Explanation

An unexpected condition was detected in the Record Storage Module.

Mnemonic

ERROR

Severity

LOG_ERR - Sev 3

Message: Error: %s

Explanation

An unexpected error occurred while performing Record Storage Module.

Mnemonic

UNEXPECTED

Severity

LOG_WARNING - Sev 4

Message: Warning: %s

Explanation

An unexpected condition was detected in the Record Storage Module.

Mnemonic

WARNING

Severity

LOG_ERR - Sev 3

APPENDIX F

Monitoring Notifications

This appendix describes enabling and monitoring CSG2 SNMP notifications in order to manage CSG2-related issues. SNMP uses notifications to report events on a managed device. The notifications are traps or informs for different events.

Note This appendix covers enabling and monitoring CSG2 SNMP notifications only. Additional types of SNMP notifications can be enabled on your Cisco router. For more information about the types of SNMP notifications you can enable, see the *Cisco IOS Configuration Fundamentals*, Release 12.4 documentation.

Additionally, to display a list of notifications available on your Cisco router, enter the **snmp-server enable traps ?** command.

This appendix contains the following sections:

- SNMP Overview, page F-1
- Configuring MIB Support, page F-6
- Enabling SNMP Support, page F-8
- Enabling and Disabling SNMP Notifications, page F-9

SNMP Overview

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a standardized framework and a common language used for monitoring and managing devices in a network.

The SNMP framework has three parts:

- SNMP manager—A system used to control and monitor the activities of network hosts using SNMP. The most common managing system is called a Network Management System (NMS). The term NMS can be applied to either a dedicated device used for network management, or the applications used on a network-management device. A variety of network management applications are available for use with SNMP. These features range from simple command-line applications to feature-rich graphical user interfaces (such as the CiscoWorks2000 line of products).

- SNMP agent—A software component in a managed device that maintains the data for the device and reports the data, as needed, to managing systems. The agent and MIB reside on the routing device (router, access server, or switch). To enable the SNMP agent on a managed device, you must define the relationship between the manager and the agent (see the "Enabling SNMP Support" section on page F-8).
- Management Information Base (MIB)—Collection of network-management information, organized hierarchically.

Instead of defining a large set of commands, SNMP places all operations in a get-request, get-next-request, and set-request format. For example, an SNMP manager can get a value from an SNMP agent or set a value in that SNMP agent.

MIB Description

A Management Information Base (MIB) is a collection of network-management information, organized hierarchically. The MIB consists of collections of managed objects identified by object identifiers. MIBs are accessed using a network-management protocol such as SNMP. A managed object (sometimes called a MIB object or an object) is one of a number of characteristics of a managed device, such as a router. Managed objects comprise one or more object instances, which are essentially variables. The Cisco implementation of SNMP uses the definitions of MIB II variables described in RFC 1213.

MIBs can contain two types of managed objects:

- Scalar objects—Define a single object instance (for example, ifNumber in the IF-MIB and bgpVersion in the BGP4-MIB).
- Columnar objects—Defines a MIB table that contains no rows or more than one row, and each row can contain one or more scalar objects, (for example, ifTable in the IF-MIB defines the interface).

System MIB variables are accessible through SNMP as follows:

- Accessing a MIB variable—Function is initiated by the SNMP agent in response to a request from the NMS. The agent retrieves the value of the requested MIB variable and responds to the NMS with that value.
- Setting a MIB variable—Function is initiated by the SNMP agent in response to a message from the NMS. The SNMP agent changes the value of the MIB variable to the value requested by the NMS.

For a list of all MIBs supported by the CSG2 Release 2, see the "MIB Support" section on page 1-4.

SNMP Notifications

An SNMP agent can notify the manager when important system events occur, such as the following:

- An interface or card starts or stops running
- Temperature thresholds are crossed
- Authentication failures occur

When an agent detects an alarm condition, the agent:

- Logs information about the time, type, and severity of the condition
- Generates a notification message, which it then sends to a designated IP host

SNMP notifications are sent as either:

- Traps—Unreliable messages, which do not require receipt acknowledgment from the SNMP manager.
- Informs—Reliable messages, which are stored in memory until the SNMP manager issues a response. Informs use more system resources than traps.

Note Many commands use the word traps in the command syntax. Unless there is an option in the command to select either traps or informs, the keyword traps refers to either traps, informs, or both. Use the **snmp-server host** command to specify whether to send SNMP notifications as traps or informs.

When an agent detects an alarm condition, it logs information about the time, type, and severity of the condition and generates a notification message, which it then sends to a designated IP host.

SNMP notifications can be sent as either *traps* or *informs*. See the "Enabling SNMP Support" section on page F-8 for instructions on how to enable traps on the CSG2.

The Cisco implementation of SNMP uses the definitions of SNMP traps described in RFC 1215.

SNMP Versions

Cisco IOS software supports the following versions of SNMP:

- SNMPv1—The Simple Network Management Protocol: An Internet standard, defined in RFC 1157. Security is based on community strings.
- SNMPv2c—The community-string based administrative framework for SNMPv2. SNMPv2c is an update of the protocol operations and data types of SNMPv2p (SNMPv2 classic), and uses the community-based security model of SNMPv1.
- SNMPv3—Version 3 of SNMP. SNMPv3 uses the following security features to provide secure access to devices:
  - Message integrity—Ensuring that a packet has not been tampered with in transit.
  - Authentication—Determining that the message is from a valid source.
  - Encryption—Scrambling the contents of a packet to prevent it from being learned by an unauthorized source.

SNMPv1 and SNMPv2c

Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers who are able to access the agent MIB is defined by an IP address Access Control List and password.

SNMPv2c support includes a bulk-retrieval mechanism and more detailed error message reporting to management stations. The bulk-retrieval mechanism supports the retrieval of tables and large quantities of information, minimizing the number of round-trip transmissions required. SNMPv2c improved error handling support includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes now report the error type.

Three kinds of exceptions are also reported:

- **no such object** exceptions
- **no such instance** exceptions
- **end of MIB view** exceptions

SNMPv3

SNMPv3 provides the following security models and security levels:

- Security model—Authentication strategy that is set up for a user and the group in which the user resides.
- Security level—Permitted level of security within a security model.

A combination of a security model and a security level determines the security mechanism to be employed when handling an SNMP packet.

SNMP Security Models and Levels

Table 6-1 describes the security models and levels provided by the different SNMP versions.

Table 6-1 SNMP Security Models and Levels

Model	Level	Authentication	Encryption	Description
v1	noAuthNoPriv	Community string	No	Uses match on community string for authentication.
v2c	noAuthNoPriv	Community string	No	Uses match on community string for authentication.
v3	noAuthNoPriv	User name	No	Uses match on user name for authentication.
v3	authNoPriv	MD5 or SHA	No	Provides authentication based on HMAC-MD5 or HMAC-SHA algorithm.
v3	authPriv	MD5 or SHA	DES	Provides authentication based on HMAC-MD5 or HMAC-SHA algorithm. Also provides DES 56-bit encryption based on CBC-DES (DES-56) standard.

You must configure the SNMP agent to use the version of SNMP supported by the management station. An agent can communicate with multiple managers; for this reason, you can configure the Cisco IOS software to support communications with one management station using the SNMPv1 protocol, one using the SNMPv2c protocol, and another using SMNPv3.

Requests for Comments

MIB modules are written in the SNMP MIB module language, and are typically defined in Request For Comments (RFC) documents submitted to the Internet Engineering Task Force (IETF). RFCs are written by individuals or groups for consideration by the Internet Society and the Internet community as a whole.

Before being given RFC status, recommendations are published as Internet Draft (I-D) documents. RFCs that have become recommended standards are also labeled as standards (STD) documents. For more information, see the Internet Society and IETF websites (http://www.isoc.org and http://www.ietf.org).

We provide private MIB extensions with each Cisco system. Cisco enterprise MIBs comply with the guidelines described in the relevant RFCs unless otherwise noted in the documentation.

Object Identifiers

An object identifier (OID) uniquely identifies a MIB object on a managed network device. The OID identifies the MIB object's location in the MIB hierarchy, and provides a means of accessing the MIB object in a network of managed devices:

- Standard RFC MIB OIDs are assigned by the Internet Assigned Numbers Authority (IANA)
- Enterprise MIB OIDs are assigned by Cisco Assigned Numbers Authority (CANA).

Each number in the OID corresponds to a level of MIB hierarchy. For example, the OID 1.3.6.1.4.1.9.9.xyz represents the *xyz*-MIB whose location in the MIB hierarchy is as follows. Note that the numbers in parentheses are included only to help show correspondence to the MIB hierarchy. In actual use, OIDs are represented as numerical values only.

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).cisco(9).ciscoMgt(9).*nn*-MIB

You can uniquely identify a managed object, such as ifNumber in the IF-MIB, by its object name (iso.org.dod.internet.mgmt.enterprises.interfaces.ifNumber) or by its OID (1.3.6.1.2.1.2.1).

For a list of OIDs assigned to MIB objects, go to the following URL:

ftp://ftp.cisco.com/pub/mibs/oid/

Related Information and Useful Links

The following URL provides access to general information about Cisco MIBs. Use the links on this page to access MIBs for download, and to access related information (such as application notes and OID listings).

- http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

TAC Information and FAQs

The following URLs provide access to SNMP information developed by the Cisco Technical Assistance Center (TAC):

- http://www.cisco.com/warp/public/477/SNMP/index.html is the Cisco TAC page for SNMP. It provides links to general SNMP information and tips for using SNMP to gather data.
- http://www.cisco.com/warp/public/477/SNMP/mibs_9226.shtml is a list of frequently asked questions (FAQs) about Cisco MIBs.

SNMP Configuration Information

The following URLs provide information about configuring SNMP:

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/fun_c/fcprt3/fcmonitr.htm provides general information about configuring SNMP support. It is part of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/fun_r/frprt3/frmonitr.htm provides information about SNMP commands. It is part of the *Cisco IOS Configuration Fundamentals Command Reference*.

Configuring MIB Support

This chapter describes how to configure SNMP and MIB support on a Cisco router. It includes the following sections:

- Determining MIBs Included for Cisco IOS Releases, page F-6
- Downloading and Compiling MIBs, page F-6
- Enabling SNMP Support, page F-8

Determining MIBs Included for Cisco IOS Releases

Follow these steps to determine which MIBs are included in the Cisco IOS release you are using:

Step 1 Go to the Feature Navigator home page http://tools.cisco.com/ITDIT/MIBS/servlet/index.

Step 2 Click **MIB Locator** to launch the application. The MIB Locator application allows you to find a MIB in the following three ways:

a. By release, platform family, and feature set—From the MIB Locator page:

- Click the drop-down menu and select the desired Cisco IOS software release.
- From the Platform Family menu, select **7600-SAMI**. If you select the platform first, the system displays only those releases and feature sets that apply to the platform you have selected.
- From the Feature Set menu, select the appropriate CSG2 release.

b. By image name—From the MIB Locator page, enter the CSG2 image name you are using in the Search by Image Name field and click **Submit**.

c. By MIB name—From the MIB Locator page, search for the MIB from the list of MIBs in the Search for a MIB menu. You can select one, or for a multiple selection, hold down the **CTRL** key, then click **Submit**.

Note After you make a selection, follow the links and instructions.

Downloading and Compiling MIBs

The following sections provide information about how to download and compile MIBs for the CSG2:

- Considerations for Working with MIBs
- Downloading MIBs
- Compiling MIBs

Considerations for Working with MIBs

While working with MIBs, consider the following:

Mismatches on Datatype Definitions

- Mismatches on datatype definitions might cause compiler errors or warning messages. Although Cisco MIB datatype definitions are not mismatched, standard RFC MIBs do mismatch. For example:

```
MIB A defines: SomeDatatype : := INTEGER(0. .100)
MIB B defines: SomeDatatype : := INTEGER(1. .50)
```

  This example is considered to be a trivial error and the MIB loads successfully with a warning message.

  The next example is considered a nontrivial error (even though the two definitions are essentially equivalent), and the MIB is not successfully parsed.

```
MIB A defines: SomeDatatype : := DisplayString
MIB B defines: SomeDatatype : := OCTET STRING (SIZE(0. .255))
```

  If your MIB compiler treats these as errors, or you want to delete the warning messages, edit one of the MIBs that define this same datatype so that the definitions match.

- Many MIBs import definitions from other MIBs. If your management application requires MIBs to be loaded, and you experience problems with undefined objects, you might want to load the following MIBs in this order:

  SNMPv2-SMI.my
  SNMPv2-TC.my
  SNMPv2-MIB.my
  RFC1213-MIB.my
  IF-MIB.my
  CISCO-SMI.my
  CISCO-PRODUCTS-MIB.my
  CISCO-TC.my

- For additional information and SNMP technical tips, from the Locator page, click **SNMP MIB Technical Tips** and follow the links or go to the following URL:

  http://www.cisco.com/pcgi-bin/Support/browse/psp_view.pl?p=Internetworking:SNMP&s=Implementation_and_Configuration#Samples_and_Tips

- For a list of SNMP object identifiers (OIDs) assigned to MIB objects, go to the following URL and click on **SNMP Object Navigator** and follow the links:

  http://tools.cisco.com/ITDIT/MIBS/servlet/index

Note You must have a Cisco CCO name and password to access the MIB Locator.

- For information about how to download and compile Cisco MIBs, go to the following URL:

  http://www.cisco.com/warp/public/477/SNMP/mibcompilers.html

Downloading MIBs

Follow these steps to download the MIBs onto your system if they are not already there:

Step 1 Review the considerations in the previous section ("Considerations for Working with MIBs").

Step 2 Go to one of the following Cisco URLs. If the MIB you want to download is not there, try the other URL; otherwise, go to one of the URLs in Step 5.

- ftp://ftp.cisco.com/pub/mibs/v2
- ftp://ftp.cisco.com/pub/mibs/v1

Step 3 Click the link for a MIB to download that MIB to your system.

Step 4 Select **File > Save** or **File > Save As** to save the MIB on your system.

Step 5 You can download industry-standard MIBs from the following URLs:

- http://www.ietf.org
- http://www.atmforum.com

Compiling MIBs

If you plan to integrate the Cisco router with an SNMP-based management application, then you must also compile the MIBs for that platform. For example, if you are running HP OpenView on a UNIX operating system, you must compile platform MIBs with the HP OpenView Network Management System (NMS). For instructions, see the NMS documentation.

Enabling SNMP Support

The following procedure summarizes how to configure the Cisco router for SNMP support.

For detailed information about SNMP commands, see the following Cisco documents:

- *Cisco IOS Release 12.3 Configuration Fundamentals Configuration Guide*, "Monitoring the Router and Network" section, available at the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/index.htm

- *Cisco IOS Release 12.3 Configuration Fundamentals Command Reference*, Part 3: System Management Commands, "Router and Network Configuration Commands" section, available at the the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_r/index.htm

To configure the Cisco router for SNMP support, you must set up your basic SNMP configuration through the command line interface (CLI) on the router.

Note These basic configuration commands are for SNMPv2c. For SNMPv3, you must also set up SNMP users and groups. (See the preceding list of documents for command and setup information.)

Step 1 Define SNMP read-only and read-write communities:

```
Router (config)# snmp-server community Read_Only_Community_Name ro
Router (config)# snmp-server community Read_Write_Community_Name rw
```

Step 2 Configure SNMP views (to limit the range of objects accessible to different SNMP user groups):

```
Router (config)# snmp-server view view_name oid-tree {included | excluded}
```

Enabling and Disabling SNMP Notifications

To enable and disable SNMP Notifications, perform the tasks in the following sections:

- Enabling and Disabling CSG2 Notifications via the CLI, page F-9
- Enabling and Disabling CSG2 SNMP Notifications via SNMP, page F-10

Enabling and Disabling CSG2 Notifications via the CLI

To use the command line interface (CLI) to enable the Cisco router to send CSG2 SNMP notifications (traps or informs), perform the following steps.

Step 1 Make sure SNMP is configured on the router (see the "Enabling SNMP Support" section on page F-8).

Step 2 Identify (by IP address) the host to receive traps from the Cisco router:

```
Router(config)# snmp-server host host-address version SNMP version community/user(V3)
udp-port <UDP port No>
```

Step 3 Enable CSG2 SNMP notifications on the Cisco router using the following command (enter a separate command for each type of notification you want to enable):

```
Router(config)# snmp-server enable traps csg [bma [records | state] | database |
quota-server [records | state]]
```

Where:

- **bma—**Enables traps for only the Billing Mediation Agents (BMAs) to which the CSG2 sends billing records.
  - **records**—Enables only lost records traps for the BMAs.
  - **state**—Enables only state change traps for the BMAs.
- **database—**Enables traps for only the database server that answers CSG2 user ID queries.
- **quota-server**—Enables traps for only the CSG2 quota servers.
  - **records**—Enables only lost records traps for the quota servers.
  - **state**—Enables only state change traps for the quota servers.

Note Entering the **snmp-server enable traps csg** command without a keyword option enables all CSG2 SNMP notifications.

Step 4 To disable CSG2 SNMP notifications on the Cisco router, enter the following command.

```
Router(config)# no snmp-server enable traps csg
```

If you omit the notification type keyword (**csg** in this example), all notifications are disabled.

Enabling and Disabling CSG2 SNMP Notifications via SNMP

Note The set operation is not yet valid for these objects. We recommend that you use the CLI to enable and disable CSG2 SNMP notifications.

Additionally, CSG2 SNMP Notifications can be enabled or disabled by setting the following objects to true(1) or false(2).

- ccsBMAStateChangeNotifEnabled—Enables/disables the generation of the Billing Mediation Agent (BMA) state change notification (ciscoContentServicesBMAStateChange)
- ccsQuotaMgrStateChangeNotifEnabled—Enables/disables the generation of the Quota Manager state change notification (ciscoContentServicesQuotaMgrStateChange)
- ccsUserDbStateChangeNotifEnabled—Enables/disables the generation of the User Database Server state change notification (ciscoContentServicesUserDbStateChange)
- ccsBMALostRecordEventNotifEnabled—Enables/disables the generation of the Billing Mediation Agent Lost Reocrd notification (ciscoContentServicesBMALostRecordEvent)
- ccsQuotaMgrLostRecordEventNotifEnabled—Enables/disables the generation of the Quota Manager Lost Record notification (ciscoContentServicesQuotaMgrLostRecordEvent)